Commutative Algebra

Pete L. Clark

Contents

Introduction

1. What is Commutative Algebra?

Commutative algebra is the study of commutative rings and attendant structures, especially ideals and modules.

This is the only possible short answer I can think of, but it is not completely satisfying. We might as well say that *Hamlet, Prince of Denmark* is about a fictional royal family in late medieval Denmark and especially about the crown prince, whose father (i.e., the King) has recently died and whose father's brother has married the prince's mother (i.e., the Queen). Informative, but not the whole story!

2. Why study Commutative Algebra?

What are the intellectual reasons for studying any subject of pure mathematics? I can think of two:

I. Commutative algebra is a necessary and/or useful prerequisite for the study of other fields of mathematics in which we are interested.

II. We find commutative algebra to be intrinsically interesting and we want to learn more. Perhaps we even wish to *discover* new results in this area.

Most beginning students of commutative algebra can relate to the first reason: they need, or are told they need, to learn some commutative algebra for their study of other subjects. If so, they are likely being told correctly: commutative algebra has come to occupy a remarkably central role in modern pure mathematics, perhaps second only to category theory in its ubiquitousness, but in a different way. Category theory provides a common language and builds bridges between different areas of mathematics: it is something like a circulatory system. Commutative algebra provides core results and structures that other results and structures draw upon are overlayed upon: it is something like a skeleton.

The branch of mathematics that draws most of all upon commutative algebra for its structural integrity is *algebraic geometry*, the study of geometric properties of manifolds and singular spaces which arise as solution sets to systems of polynomial equations. There is a hard lesson here: in the 19th century algebraic geometry split off from complex function theory and differential geometry as its own discipline and then burgeoned dramatically at the turn of the century. But by 1920 or so the practitioners of the subject had found their way into territory in which "purely geometric" reasoning led to serious errors. In particular they had been making

arguments about how algebraic varieties behave *generically*, but they lacked the technology to even give a precise meaning to the term. Thus the subject eventually became invertebrate and began to collapse under its own weight. Then (starting in about 1930) came a heroic shoring up process in which the foundations of the subject were recast with commutative algebraic methods at the core. This was done, several times over and in several different ways, by Zariski, Weil, Serre and Grothendieck, among others. For the last 60 years it has been impossible to deeply study algebraic geometry without knowing commutative algebra – a lot of commutative algebra. (More than is contained in these notes!)

The other branch of mathematics that draws upon commutative algebra in an essential way is algebraic number theory. One sees this from the beginning in that the Fundamental Theorem of Arithmetic is the assertion that the ring $\mathbb{Z}$ is a unique factorization domain (UFD), a basic commutative algebraic concept. Moreover number theory was one of the historical sources of the subject. Notably the concept of Dedekind domain came from Dedekind's number-theoretic investigations. At the student level, algebraic number theory does not embrace commutative algebra as early or as thoroughly as algebraic geometry. This seems to me to be a pedagogical mistake: although one can do a good amount of algebraic number theory without explicit reliance on commutative algebra, this seems to come at the expense of not properly explaining what is going on. A modicum of commutative algebra greatly enriches the study of algebraic number theory: it clarifies it, generalizes it and (I believe) makes it more interesting.

The interplay among number theory, algebraic geometry and commutative algebra flows in all directions. What Grothendieck did in the 1960s (with important contributions from Chevalley, Serre and others) was to create a single field of mathematics that encompassed commutative algebra, classical algebraic geometry and algebraic number theory: the theory of schemes. As a result, most contemporary number theorists are also partly commutative algebraists and partly algebraic geometers: we call this cosmopolitan take on the subject **arithmetic geometry**.

There are other areas of mathematics that draw upon commutative algebra in important ways. To mention some which will show up in later in these notes:

- Differential topology: vector bundles on a compact base.
- General topology.
- Invariant theory.
- Order theory.

3. What distinguishes this text

The most straightforward *raison d'être* for a commutative algebra text would be to provide a foundation for the subjects of algebraic geometry, arithmetic geometry and algebraic number theory. The bad news is that this task – even, restricted to providing foundations for the single, seminal text of Hartshorne [**Ha**] – is dauntingly large. The good news is that this has nevertheless been achieved some time ago by David Eisenbud (a leading contemporary expert on the interface of commutative algebra and algebraic geometry) in his text [**Ei**]. This work is highly recommended.

It is 797 pages long, so contains enough material for many courses in the subject. It would be folly to try to improve upon Eisenbud's work here, and I certainly have not tried.

The other standard commutative algebra texts are those by Atiyah-Macdonald [**AM**] and by Matsumura [**M**]. Any reader who is halfway serious in their study of commutative algebra should have access to all of [**AM**], [**M**] and [**Ei**] and consult them frequently. While the current text does not rely on them in the logical sense, I am – at best – a part time commutative algebraist, and much of what I know comes from these texts. (Reading only "derivative" sources is rarely a good idea.) On the other hand, precisely because there are three standard excellent texts I have at times allowed my choice of topics to be much less standard.

The topics covered in Atiyah-Macdonald's text in particular have become a *de facto* standard for a first course in commutative algebra. Here are the chapter titles from [**AM**]: 1. Rings and Ideals 2. Modules 3. Rings and Modules of Fractions 4. Primary Decomposition 5. Integral Dependence and Valuations 6. Chain Conditions 7. Noetherian Rings 8. Artin Rings 9. Discrete Valuation Rings and Dedekind Domains 10. Completions 11. Dimension Theory. The text is 126 pages, and a substantial portion of the text is devoted to exercises, making [**AM**] one of the most amenable to student study graduate level mathematics texts I have ever seen. The exercises are especially attractive: some are easy, some are very challenging, and they treat both core topics and side attractions.

Much of the present text covers the material of **the first nine chapters** of [**AM**] but with a more leisurely, detailed exposition. Many exercises in [**AM**] appear as proved results here. To give a specific example, Boolean rings appear in Exercises 1.11, 1.23, 1.24, 1.25, 3.28 of [**AM**], in which in particular proofs of the Stone Representation Theorem and Stone Duality Theorems are sketched. In this text Chapter 9 is devoted to Boolean rings, including proofs of these two results. The failure to cover completions and basic dimension theory in this text would be unforgivable were it not the case that [**AM**] covers it so nicely.

Let us also compare to [**M**]. Here we treat the material of the first 12 sections of [**M**] except §8 (Completion and the Artin-Rees Lemma) as well as some material from §20 (UFDs). This is less than one third of the material covered in [**M**].

4. More on the contents

As mentioned above, one of the distinguishing features of this text – and one of the things which makes it much lengthier compared to the portions of [**AM**] and [**M**] that cover the same material – is that we digress to include many "applications" to other parts of mathematics. At one point I had the idea that every section of "core material" should be followed by a section giving applications. This conceit was not fully feasible, but there are still some entire sections devoted to applications (generally characterized by making contact with topics outside of commutative algebra by their relative independence from the rest of the text):

• §2 on Galois connections.

- §6 on vector bundles and Swan's Theorem.
- §9 on Boolean rings, Boolean spaces and Stone Duality.

As for significant parts of sections, we have:

- §5.2 on rings of continuous functions.
- §5.3 on rings of holomorphic functions.
- §11.3 on the real Nullstellensatz.
- §11.4 on the combinatorial Nullstellensatz.
- §11.5 on the finite field Nullstellensatz.
- §11.6 on Terjanian's Nullstellensatz.
- §13.6 on Hochster's Theorem.
- §14.6 on invariant theory and the Shephard-Todd-Chevalley Theorem.

5. Acknowledgments

Thanks to Kasper Andersen, Ufuoma Asarhasa, Pablo Barenbaum, Max Bender, Martin Brandenburg, Tom Church, John Doyle, Georges Elencwajg, Amelia Ernst, Tyler Genao, Ernest Guico, Emil Jerabek, Jason Joseph, Keenan Kidwell, David Krumm, Allan Lacy, Casey LaRue, Andrew Lott, Stacy Musgrave, Kedar Nadkarni, Hans Parshall, Davide Pierrat, Alon Regev, Tomasz Rzepecki, Frederick Saia, Christopher Padilla Sandoval, Jacob Schlather, Jack Schmidt, Mariano Suárez-Álvarez, James Taylor, Peter Tamaroff, Matthé van der Lee and Lori D. Watson for catching errors[1] and making other useful suggestions.

[1]Of which many, many remain: your name could go here!

CHAPTER 1

Commutative Rings

1. Fixing terminology

We are interested in studying properties of **commutative rings with unity**.

By a **general algebra** R, we mean a triple $(R, +, \cdot)$ where R is a set endowed with a binary operation $+ : R \times R \to R$ – called **addition** – and a binary operation $\cdot : R \times R \to R$ – called **multiplication** – satisfying the following:

(CG) $(R, +)$ is a commutative group,

(D) For all $a, b, c \in R$, $(a + b) \cdot c = a \cdot c + b \cdot c,\ a \cdot (b + c) = a \cdot b + a \cdot c$.

For at least fifty years, there has been agreement that in order for an algebra to be a **ring**, it must satisfy the additional axiom of associativity of multiplication:

(AM) For all $a, b, c \in R$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.

A general algebra that satisfies (AM) will be called simply an **algebra**. A similar convention that is prevalent in the literature is the use of the term **nonassociative algebra** to mean what we have called a general algebra: i.e., a not *necessarily* associative algebra.

A ring R is said to be **with unity** if there exists a multiplicative identity, i.e., an element e of R such that for all $a \in R$ we have $e \cdot a = a \cdot e = a$. If e and e' are two such elements, then $e = e \cdot e' = e'$. In other words, if a unity exists, it is unique, and we will denote it by 1.

A ring R is **commutative** if for all $x,\ y \in R, x \cdot y = y \cdot x$.

In these notes we will be (almost) always working in the category of commutative rings with unity. In a sense which will shortly be made precise, this means that the identity 1 is regarded as part of the structure of a ring and must therefore be *preserved* by all homomorphisms.

Probably it would be more natural to study the class of possibly non-commutative rings with unity, since, as we will see, many of the fundamental constructions of rings give rise, in general, to non-commutative rings. But if the restriction to commutative rings (with unity!) is an artifice, it is a very useful one, since two of the most fundamental notions in the theory, that of ideal and module, become

significantly different and more complicated in the non-commutative case. It is nevertheless true that many individual results have simple analogues in the non-commutative case. But it does not seem necessary to carry along the extra generality of non-commutative rings; rather, when one is interested in the non-commutative case, one can simply remark "Proposition X.Y holds for (left) R-modules over a noncommutative ring R."

Notation: Generally we shall abbreviate $x \cdot y$ to xy. Moreover, we usually do not use different symbols to denote the operations of addition and multiplication in different rings: it will be seen that this leads to simplicity rather than confusion.

For a ring R, we put

$$R^\bullet := R \backslash \{0\}$$

to be the set of nonzero elements of R. If for all $x, y \in R^\bullet$ we have $xy \in R^\bullet$ we say that R is a **domain**. (The older, and still popular terminology is "integral domain." However, on the one hand the word *integral* does not have any independent meaning here, and on the other hand later in this text we will define integral *extensions* of rings, a distinct concept. So we will stick to just "domain.")

Group of units: Let R be a ring with unity. An element $x \in R$ is said to be a **unit** if there exists an element y such that $xy = yx = 1$.

CONVENTION ON EXERCISES: Throughout the exercises, a "ring" means a commutative ring unless explicit mention is made to the contrary. Some but not all of the results in the exercises still hold for non-commutative rings, and it is left to the interested reader to explore this.

EXERCISE 1.1.

a) *Show: if x is a unit, the element y with $xy = yx = 1$ is unique, denoted x^{-1}.*
b) *Show: if x is a unit, so is x^{-1}.*
c) *Show that, for all $x, y \in R$, xy is a unit $\iff$ x and y are both units.*
d) *Show: the units form a group, denoted $R^\times$, under multiplication.*

REMARK 1. *For elements x, y in a non-commutative ring R, if x and y are units so is xy, but the converse need not hold. (Thus Exercise 1.1c) is an instance of a result in which commutativity is essential.) Nevertheless this is enough to deduce that in any ring the units $R^\times$ form a group...which is not necessarily commutative.*

EXAMPLE 1.1 (Zero ring). *Our rings come with two distinguished elements, the additive identity 0 and the multiplicative identity 1. Suppose that $0 = 1$. Then for $x \in R$, $x = 1 \cdot x = 0 \cdot x$, whereas in any ring $0 \cdot x = (0 + 0) \cdot x = 0 \cdot x + 0 \cdot x$, so $0 \cdot x = 0$. In other words, if $0 = 1$, then this is the only element in the ring. It is clear that for any one element set $R = \{0\}$, $0 + 0 = 0 \cdot 0 = 0$ endows R with the structure of a ring. We call this ring the **zero ring**.*

The zero ring exhibits some strange behavior, such that it must be explicitly excluded in many results. For instance, the zero element is a unit in the zero ring, which is obviously not the case in any nonzero ring. A nonzero ring in which every nonzero element is a unit is called a **division ring**. A commutative division ring

is called a **field**.

Let R and S be rings. A **homomorphism** $f : R \to S$ is a function such that:

(HOM1) For all $x, y \in R$, $f(x + y) = f(x) + f(y)$.
(HOM2) For all $x, y \in R$, $f(xy) = f(x)f(y)$.
(HOM3) $f(1) = 1$.

We observe that (HOM1) implies $f(0) = f(0 + 0) = f(0) + f(0)$, so $f(0) = 0$. Thus we do not need to explcitly include $f(0) = 0$ in the definition of a group homomorphism. For the multiplicative identity however, this argument only shows that if $f(1)$ is a unit, then $f(1) = 1$. Therefore, if we did not require (HOM3), then for instance the map $f : R \to R$, $f(x) = 0$ for all x, would be a homomorphism, and we do not want this.

EXERCISE 1.2. *Suppose R and S are rings, and let $f : R \to S$ be a map satisfying (HOM1) and (HOM2). Show that f is a homomorphism of rings (i.e., satisfies also $f(1) = 1$) if and only if $f(1) \in S^\times$.*

A homomorphism $f : R \to S$ is an **isomorphism** if there exists a homomorphism $g : S \to R$ such that: for all $x \in R$, $g(f(x)) = x$; and for all $y \in S$, $f(g(y)) = y$.

EXERCISE 1.3. *Let $f : R \to S$ be a homomorphism of rings. Show the following are equivalent:*

(i) *f is a bijection.*
(ii) *f is an isomorphism.*

In many algebra texts, an isomorphism of rings (or groups, etc.) is *defined* to be a bijective homomorphism, but this gives the wrong idea of what an isomorphism should be in other mathematical contexts (e.g. for topological spaces). Rather, having defined the notion of a morphism of any kind, one defines isomorphism in the way we have above.

EXERCISE 1.4.

a) *Suppose R and S are both rings on a set containing exactly one element. Show that there is a unique ring isomorphism from R to S. (This is a triviality, but explains why are we able to speak of **the zero ring**, rather than simply the zero ring associated to one element set. We will therefore denote the zero ring just by 0.)*
b) *Show that any ring R admits a unique homomorphism to the zero ring. One says that the zero ring is **the final object** in the category of rings.*

EXERCISE 1.5. *Show: for a not-necessarily-commutative-ring S there exists a unique homomorphism from the ring $\mathbb{Z}$ of integers to S. (Thus $\mathbb{Z}$ is the **initial object** in the category of not-necessarily-commutative-rings. It follows immediately that it is also the initial object in the category of rings.)*

A **subring** R of a ring S is a subset R of S such that

(SR1) $1 \in R$.
(SR2) For all $r, s \in R$, $r + s \in R$, $r - s \in R$, and $rs \in R$.

Here (SR2) expresses that the subset R is an algebra under the operations of addition and multiplication defined on S. Working, as we are, with rings with unity, we have to be a bit more careful: in the presence of (SR2) but not (SR1) it is possible that R *either* does not have a multiplicative identity or, more subtly, that it has a multiplicative identity which is not the element $1 \in S$.

An example of the first phenomenon is $S = \mathbb{Z}$, $R = 2\mathbb{Z}$. An example of the second is $S = \mathbb{Z}$, $R = 0$. A more interesting example is $S = \mathbb{Z} \times \mathbb{Z}$ – i.e., the set of all ordered pairs (x, y), $x, y \in \mathbb{Z}$ with $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$, $(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2, y_1 y_2)$ – and $R = \{(0, y) \mid y \in \mathbb{Z}\}$. Then with the induced addition and multiplication from S, R is isomorphic to the ring $\mathbb{Z}$ and the element $(0, 1)$ serves as a multiplicative identity on R which is different from the (always unique) multiplicative identity $1_S = (1, 1)$, so according to our conventions R is not a subring of S.

Notice that if R is a subring of S, the inclusion map $R \hookrightarrow S$ is an injective homomorphism of rings. Conversely, if $\iota : R \hookrightarrow S$ is an injective ring homomorphism, then $R \cong \iota(R)$ and $\iota(R)$ is a subring of S, so essentially we may use ι to view R as a subring of S. The only proviso here is that this certainly depends on ι: in general there may be other injective homomorphisms $\iota : R \hookrightarrow S$ which realize R as a different subset of S, hence a different subring.

2. Adjoining elements

Let $\iota : R \hookrightarrow S$ be an injective ring homomorphism. As above, let us use ι to view R as a subring of S; we also say that S is an **extension ring** of R and write S/R for this (note: this has nothing to do with cosets or quotients!) We wish now to consider rings T such that $R \subseteq T \subseteq S$; such a ring T might be called a **subextension** of S/R or an **intermediate ring**.

For $\iota : R \hookrightarrow S$ as above, let $X = \{x_i\}$ be a subset of S. Then the partially ordered set of all subrings of S containing R and X is nonempty (since S is in it) and contains a bottom element, given (as usual!) by taking the intersection of all of its elements. We call this the ring obtained by **adjoining** the elements of X to R. In the commutative case, we denote this ring by $R[\{x_i\}]$, for reasons that will become more clear when we discuss polynomial rings in §5.4.

EXAMPLE 1.2. *Take $R = \mathbb{Z}$, $S = \mathbb{C}$. Then $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ is the smallest subring of $\mathbb{C}$ containing ($\mathbb{Z}$ and) $\sqrt{-1}$.*

EXAMPLE 1.3. *Take $R = \mathbb{Z}$, $S = \mathbb{Q}$, let $\mathcal{P}$ be any set of prime numbers, and put $X = \{\frac{1}{p}\}_{p \in \mathcal{P}}$. Then there is a subring $\mathbb{Z}_{\mathcal{P}} := \mathbb{Z}[\{\frac{1}{p}\}_{p \in \mathcal{P}}]$ of $\mathbb{Q}$.*

EXERCISE 1.6. *Let $\mathcal{P}$, $\mathcal{Q}$ be two sets of prime numbers. Show the following are equivalent:*

(i) $\mathbb{Z}_{\mathcal{P}} \cong \mathbb{Z}_{\mathcal{Q}}$.
(ii) $\mathbb{Z}_{\mathcal{P}} = \mathbb{Z}_{\mathcal{Q}}$.
(iii) $\mathcal{P} = \mathcal{Q}$.

EXERCISE 1.7. *Show: every subring of $\mathbb{Q}$ is of the form $\mathbb{Z}_{\mathcal{P}}$ for some $\mathcal{P}$.*

The adjunction process $R \mapsto R[X]$ is defined only relative to some extension ring S of R, although the notation hides this. In fact, one of the recurrent themes of the subject is the expression of the adjunction process in a way which depends only on R itself. In the first example, this is achieved by identifying $\sqrt{-1}$ with its minimal polynomial t^2+1 and replacing $\mathbb{Z}[\sqrt{-1}]$ with the quotient ring $\mathbb{Z}[t]/(t^2+1)$. The second example will eventually be turned around: we will be able to give an independent definition of $\mathbb{Z}_{\mathcal{P}}$ as a certain "ring of fractions" formed from $\mathbb{Z}$ and then $\mathbb{Q}$ will be the ring of fractions obtained by taking $\mathcal{P}$ to be the set of all prime numbers.

Nevertheless, the existence of such turnabouts should not cause us to forget that adjunction is relative to an extension; indeed forgetting this can lead to serious trouble. For instance, if $\sqrt[3]{2}$ is the unique real cube root of 2 and ζ_3 is a primitive cube root of unity, then the three complex numbers with cube 2 are $z_1 = \sqrt[3]{2}$, $z_2 = \sqrt[3]{2}\zeta_3$ and $z_3 = \sqrt[3]{2}\zeta_3^2$. Each of the rings $\mathbb{Q}[z_1]$, $\mathbb{Q}[z_2]$, $\mathbb{Q}[z_3]$ is isomorphic to the ring $\mathbb{Q}[t]/(t^3-2)$, so all three are isomorphic to each other. But they are not *the same* ring: on the one hand $\mathbb{Q}[z_1]$ is contained in $\mathbb{R}$ and the other two are not. More seriously $\mathbb{Q}[z_1, z_2, z_3] = \mathbb{Q}[\sqrt[3]{2}, \zeta_3]$, which strictly contains any one of $\mathbb{Q}[z_1]$, $\mathbb{Q}[z_2]$ and $\mathbb{Q}[z_3]$.

3. Ideals and quotient rings

Let $f : R \to S$ be a homomorphism of rings, and put

$$I = f^{-1}(0) = \{x \in R \mid f(x) = 0\}.$$

In particular f is a homomorphism of commutative groups $(R,+) \to (S,+)$, I is a subgroup of $(R,+)$. Moreover, it enjoys both of the following properties:

(LI) For all $j \in I$ and $x \in R$, $xj \in I$.
(RI) For all $i \in I$ and $y \in R$, $iy \in I$.

Indeed,

$$f(xj) = f(x)f(j) = f(x) \cdot 0 = 0 = 0 \cdot f(y) = f(i)f(y) = f(iy).$$

In general, let R be a ring. An **ideal** is a subset $I \subseteq R$ which is a subgroup of $(R,+)$ (in particular, $0 \in I$) and that satisfies (LI) and (RI).

THEOREM 1.4. *Let R be a ring, and let I be a subgroup of $(R,+)$. The following are equivalent:*

(i) *The group I is an ideal of R.*
(ii) *There is a ring structure on the quotient group R/I making the additive homomorphism $R \to R/I$ into a homomorphism of rings.*

When these conditions hold, the ring structure on R/I in (ii) is unique, and R/I is called the quotient of R by the ideal I.

PROOF. Consider the group homomorphism $q : R \to R/I$. If we wish R/I to be a ring in such a way so that q is a ring homomorphism, we need

$$(x+I)(y+I) = q(x)q(y) = q(xy) = (xy+I).$$

This shows that there is only one possible ring structure, and the only question is whether it is well-defined. For this we need that for all $i, j \in I$, $(x+i)(y+j) - xy =$

$xj + iy + ij \in I$. Evidently this holds for all x, y, i, j if and only if (LI) and (RI) both hold. □

Remark: If R is commutative, then of course there is no difference between (LI) and (RI). For a non-commutative ring R, an additive subgroup I satisfying condition (LI) but not necessarily (RI) (resp. (RI) but not necessarily (LI)) is called a **left ideal** (resp. a **right ideal**). Often one says **two-sided ideal** to emphasize that (LI) and (RI) both hold. Much of the additional complexity of the non-commutative theory comes from the need to distinguish between left, right and two-sided ideals.

We do not wish to discuss such complexities here, so henceforth in this section we assume (except in exercises, when indicated) that our rings are commutative.

EXAMPLE 1.5. *In $R = \mathbb{Z}$, for any integer n, consider the subset $(n) = n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$ of all multiples of n. This is easily seen to be an ideal.*[1] *The quotient $\mathbb{Z}/n\mathbb{Z}$ is the ring of integers modulo n.*

An ideal $I \subsetneq R$ is called **proper**.

EXERCISE 1.8. *Let R be a ring and I an ideal of R. Show: the following are equivalent:*

(i) $I \cap R^\times \neq \emptyset$.
(ii) $I = R$.

EXERCISE 1.9.

a) *Let R be a commutative ring. Show that R is a field if and only if R has exactly two ideals, 0 and R.*
b) *Let R be a not necessarily commutative ring. Show the following are equivalent:*
   (i) *The only one-sided ideals of R are 0 and R.*
   (ii) *R is a division ring.*
c) *For a field k and an integer $n > 1$, show that the matrix ring $M_n(k)$ has no two-sided ideals but is not a division ring.*

EXERCISE 1.10. *Some contemporary undergraduate algebra texts define the finite ring $\mathbb{Z}/n\mathbb{Z}$ in a different and apparently simpler way: put $Z_n = \{0, 1, \ldots, n-1\}$. For any integer x, there is a unique integer k such that $x - kn \in Z_n$. Define a function $\mod n : \mathbb{Z} \to Z_n$ by $\mod n(x) := x - kn$. We then define $+$ and $\cdot$ on Z_n by $x + y := \mod n(x + y)$, $xy = \mod n(xy)$. Thus we have avoided any mention of ideals, equivalence classes, quotients, etc. Is this actually simpler? (Hint: how do we know that Z_n satisfies the ring axioms?)*

For any commutative ring R and any element $y \in R$, the subset $(y) = yR = \{xy \mid x \in R\}$ is an ideal of R. Such ideals are called **principal**. A **principal ideal ring** is a commutative ring in which each ideal is principal.

EXERCISE 1.11.

a) *The intersection of any family of (left, right or two-sided) ideals in a not-necessarily-commutative-ring is a (left, right or two-sided) ideal.*

[1] If this is not known and/or obvious to the reader, these notes will probably be too brisk.

b) *Let $\{I_i\}$ be a set of ideals in the commutative ring R. Show that $\bigcap_i I_i$ has the following property: for any ideal J of R such that $J \subseteq I_i$ for all i, $J \subseteq \bigcap_i I$.*

Let R be a ring and S a subset of R. There is then a smallest ideal of R containing S, namely $\bigcap I_i$, where I_i are all the ideals of R containing S. We call this the ideal **generated** by S. This is a "top-down" description; as usual, there is a complementary "bottom-up" description that is not quite as clean but often more useful. Namely, put

$$\langle S \rangle := \{\sum r_i s_i \mid r_i \in R, s_i \in S\}$$

i.e., the set of all finite sums of an element of R times an element of S. In practice, when $S = \{x_1, \ldots, x_n\}$ is finite, we write $\langle x_1, \ldots, x_n \rangle$ instead of $\langle \{x_1, \ldots, x_n\} \rangle$.

PROPOSITION 1.6. *For a subset S of a commutative ring R, the set $\langle S \rangle$ is an ideal, the intersection of all ideals containing S.*

EXERCISE 1.12. *Prove Proposition 1.6.*

When S is a subset of R such that $I = \langle S \rangle$, we say S is a **set of generators** for I. In general the same ideal will have many (most often infinitely many) sets of generators. Just above we defined for each $x \in R$ the principal ideal (x). This is also the ideal $\langle x \; rangle$, i.e., the least ideal of R that contains x. In any ring, the zero ideal $0 = \langle 0 \rangle$ and the entire ring $R = \langle 1 \rangle$ are principal. For $x \in R$, we tend to denote the principal ideal generated by x as either Rx or (x) rather than $\langle x \rangle$.

EXERCISE 1.13. *Let R be a ring. For elements $x, y \in R$ we say that x and y are **associates** if there is a unit $u \in R^\times$ such that $y = ux$.*

a) *Show: being associates is an equivalence relation on R.*
b) *Show: if x and y are associates, then $(x) = (y)$.*
c) *Show: if R is a domain and for $x, y \in R$ we have $(x) = (y)$, then x and y are associates.*
d) *Find a ring R and elements x and y such that $(x) = (y)$, but x and y are not associates.*
(Suggestions: take $R = C(\mathbb{R}, \mathbb{R})$ to be the the ring of continuous functions $f : \mathbb{R} \to \mathbb{R}$ under pointwise addition and multiplication. One can take f_1 and f_2 to be piecewise linear functions with $|f_1| = |f_2|$ and such that each vanishes on $[-1, 1]$.)

An ideal I is **finitely generated** if...it admits a finite set of generators.[2]

Stop and think for a moment: do you know an example of an ideal that is *not* finitely generated? You may well find that you do not. It turns out that there is a very large class of rings – including most or all of the rings you are likely to meet in undergraduate algebra – for which every ideal is finitely generated. A ring R in which every ideal is finitely generated is called **Noetherian**. This is probably the single most important class of rings, as we will come to appreciate slowly but surely over the course of these notes.

EXERCISE 1.14. *Let R be a ring.*

[2]Well, obviously. Nevertheless this definition is so critically important that it would have been a disservice to omit it.

a) *For ideals I and J of R, define $I + J = \{i + j \mid i \in I,\ j \in J\}$. Show that $I + J = \langle I \cup J \rangle$ is the smallest ideal containing both I and J.*
b) *Extend part a) to any finite number of ideals $I_1, \ldots, I_n$.*
c) *Suppose $\{I_i\}$ is a set of ideals of I. Give an explicit description of the ideal $\langle I_i \rangle$.*

The preceding considerations show that the collection of all ideals of a commutative ring R, partially ordered by inclusion, form a **complete lattice**.

If I is an ideal in the ring R, then there is a correspondence between ideals J of R containing I and ideals of the quotient ring R/I, exactly as in the case of a normal subgroup of a group:

THEOREM 1.7. *(Correspondence Theorem) Let I be an ideal of a ring R, and denote the quotient map $R \to R/I$ by q. Let $\mathcal{I}(R)$ be the lattice of ideals of R, $\mathcal{I}_I(R)$ be the sublattice of ideals containing I and $\mathcal{I}(R/I)$ the lattice of ideals of the quotient ring R/I. Define maps*

$$\Phi : \mathcal{I}(R) \to \mathcal{I}(R/I),\ J \mapsto (I + J)/I,$$
$$\Psi : \mathcal{I}(R/I) \to \mathcal{I}(R),\ J \mapsto q^{-1}(J).$$

Then $\Psi \circ \Phi(J) = I + J$ and $\Phi \circ \Psi(J) = J$. In particular Ψ induces an isomorphism of lattices from $\mathcal{I}(R/I)$ to $\mathcal{I}_I(R)$.

PROOF. For all the abstraction, the proof is almost trivial. For $J \in \mathcal{I}(R)$, we check that $\Psi(\Phi(J)) = \Psi(J + I \pmod I) = \{x \in R \mid x + I \in J + I\} = J + I \in \mathcal{I}_I(R)$. Similarly, for $J \in \mathcal{I}(R/I)$, we have $\Phi(\Psi(J)) = J$. □

Remark: In fancier language, the pair (Φ, Ψ) give an **isotone Galois connection** between the partially ordered sets $\mathcal{I}(R)$ and $\mathcal{I}(R/I)$. The associated closure operator $\Phi \circ \Psi$ on $\mathcal{I}(R/I)$ is the identity, whereas the closure operator $\Psi \circ \Phi$ on $\mathcal{I}(R)$ carries each ideal J to the smallest ideal containing both J and I.[3]

The Correspondence Theorem will be our constant companion. As is common, we will often use the map Ψ to identify the sets $\mathcal{I}(R/I)$ and $\mathcal{I}_I(R)$.

EXERCISE 1.15. *Let I be an ideal of R and $\{J_i\}$ be a set of ideals of R. Show: Φ preserves suprema and Ψ preserves infima:*

$$\Phi(\langle J_i \rangle) = \langle \Phi(J_i) \rangle$$

and

$$\Psi(\bigcap J_i) = \bigcap \Psi(J_i).$$

4. The monoid of ideals of R

Let I and J be ideals of the ring R. The **product ideal** IJ is the least ideal containing all elements of the form xy for $x \in I$ and $y \in J$. It is easy to see that

$$IJ = \{\sum x_i y_i \mid x_i \in I,\ y_i \in J\}$$

is precisely the set of all finite sums of such products. Recall that we have written $\mathcal{I}(R)$ for the lattice of all ideals of R. Then $(I, J) \mapsto IJ$ gives a binary operation on $\mathcal{I}(R)$, the **ideal product**.

[3]This point of view will be explored in more detail in §2.

EXERCISE 1.16. *Show: $\mathcal{I}(R)$ under the ideal product is a commutative monoid, with identity element R and absorbing element the (0) ideal of R.*[4]

If you are given a commutative monoid M, then invariably the property you are hoping it has is **cancellation**: for all $x, y, z \in M$, $xz = yz \implies x = y$.[5] For example, if R is a ring, then the set $R^\bullet$ of nonzero elements of R is cancellative if and only if R is a domain. In $(R, \cdot)$ 0 is an absorbing element, so we remove it to get a hope of cancellativity.

EXERCISE 1.17.

a) *Let M be a cancellative monoid of cardinality greater than one. Show: M does not have any absorbing elements.*
b) *Let R be a ring that is not the zero ring. Show: the monoid $\mathcal{I}(R)$ is not cancellative.*

In light of the previous exercise, for a domain R we define $\mathcal{I}^\bullet(R)$ to be the monoid of *nonzero ideals* of R under multiplication.

Warning: Just because R is a domain, $\mathcal{I}^\bullet(R)$ need not be cancellative!

EXERCISE 1.18. *Let $R = \mathbb{Z}[\sqrt{-3}]$, and let $\mathfrak{p}_2 = \langle 1 + \sqrt{-3}, 1 - \sqrt{-3} \rangle$.*

a) *Show: $\#R/(2) = 4$ and $R/\mathfrak{p}_2 \cong \mathbb{Z}/2\mathbb{Z}$.*
b) *Show: $\mathfrak{p}_2^2 = \mathfrak{p}_2 \cdot (2)$.*
c) *Conclude: $\mathcal{I}^\bullet(R)$ is* not *cancellative.*

EXERCISE 1.19. *Let R be a PID. Show: $\mathcal{I}^\bullet(R)$ is cancellative.*

EXERCISE 1.20. *Show: for a commutative monoid M, the following are equivalent:*

(i) *The monoid M is cancellative.*
(ii) *There is a commutative group G and an injective monoid homomorphism $\iota : M \hookrightarrow G$.*

EXERCISE 1.21. *Let M be a commutative monoid. A **group completion** of M consists of a commutative group $G(M)$ and a monoid homomorphism $c : M \to G(M)$ that is* universal *for monoid homomorphisms into a commutative group. That is, for any commutative group G and monoid homomorphism $f : M \to G$, there is a unique homomorphism of groups $F : G(M) \to G$ such that $f = F \circ c$.*

a) *Show: any two group completions are isomorphic.*
b) *Show: any commutative monoid has a group completion.*
c) *Show: a commutative monoid injects into its group completion if and only if it is cancellative.*

5. Pushing and pulling ideals

Let $f : R \to S$ be a homomorphism of commutative rings. We can use f to transport ideals from R to S and also to transport ideals from S to R.

More precisely, for I an ideal of R, consider $f(I)$ as a subset of S.

EXERCISE 1.22.

[4]An element z of a monoid M is called **absorbing** if for all $x \in M$, $zx = xz = z$.

[5]Well, obviously this is an exaggeration, but you would be surprised how often it is true.

a) *Give an example to show that $f(I)$ need not be an ideal of S.*
b) *Suppose f is surjective. Show: $f(I)$ is an ideal of S.*

Nevertheless we can consider the ideal it generates: we define

$$f_*(I) = \langle f(I) \rangle,$$

and we call $f_*(I)$ the **pushforward of I to S**.

Similarly, let J be an ideal of S, and consider its complete preimage in R, i.e., $f^{-1}(J) = \{x \in R \mid f(x) \in J\}$. As you are probably already aware, preimages have much nicer algebraic properties than direct images, and indeed $f^{-1}(J)$ is necessarily an ideal of R. We denote it by $f^*(J)$ and call it the **pullback of J to R**.

Suppose that I is an ideal of R, $S = R/I$ and $f : R \to R/I$ is the quotient map. In this case, pushforwards and pullbacks were studied in detail in Theorem 1.7. In this case $f^* : \mathcal{I}(S) \hookrightarrow \mathcal{I}(R)$ is an injection, which allows us to view the lattice of ideals of S as a sublattice of the lattice of ideals of R. Moreover we have a **push-pull formula**: for all ideals J of R,

$$f^* f_* J = J + I$$

and also a **pull-push formula**: for all ideals J of R/I,

$$f_* f^* J = J.$$

These formulas are extremely useful at all points in the study of ring theory. More generally, whenever one meets a homomorphism $f : R \to S$ of rings (or better, a certain class of homomorphisms), it is fruitful to ask about properties of f_* and f^*: in particular, is f^* necessarily injective, or surjective? Can we identify the composite maps $f^* f_*$ and/or $f_* f^*$?

In these notes, the most satisfying and important answers will come for **localizations** and **integral extensions**.

6. Maximal and prime ideals

An ideal $\mathfrak{m}$ of R is **maximal** if it is proper and there is no proper ideal of R strictly containing $\mathfrak{m}$. An ideal $\mathfrak{p}$ of R is **prime** if for all $x, y \in R$, $xy \in \mathfrak{p}$ implies $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$ or both.

EXERCISE 1.23. *For an ideal I in a ring R, show: the following are equivalent:*
(i) *The ideal I is maximal.*
(ii) *The ring R/I is a field.*

EXERCISE 1.24. *For an ideal I in a ring R, show: the following are equivalent:*
(i) *The ideal I is prime.*
(ii) *The ring $R/\mathfrak{p}$ is a domain.*

EXERCISE 1.25. *Show: maximal ideals are prime.*

EXERCISE 1.26. *Let $f : R \to S$ be a homomorphism of rings.*
a) *Let I be a prime ideal of R. Show: $f_* I$ need* not *be a prime ideal of S.*
b) *Let J be a prime ideal of S. Show: $f^* J$ is a prime ideal of R.*
c) *Let J be a maximal ideal of S. Show: $f^* J$ need* not *be maximal in R.*

If I and J are ideals of a ring R, we define the **colon ideal**[6]

$$(I : J) = \{x \in R \mid xJ \subseteq I\}.$$

EXERCISE 1.27. *Show: $(I : J)$ is indeed an ideal of R.*

7. Products of rings

Let R_1 and R_2 be rngs. The Cartesian product $R_1 \times R_2$ has the structure of a ring with "componentwise" addition and multiplication:

$$(r_1, r_2) + (s_1, s_2) := (r_1 + s_1, r_2 + s_2).$$
$$(r_1, r_2) \cdot (s_1, s_2) := (r_1 s_1, r_2 s_2).$$

EXERCISE 1.28.

a) *Show: $R_1 \times R_2$ is commutative if and only if both R_1 and R_2 are commutative.*

b) *Show: $R_1 \times R_2$ has a multiplciative identity if and only if both R_1 and R_2 do, in which case $1 := (1, e_1)$ is the identity of $R_1 \times R_2$.*

As for any Cartesian product, $R_1 \times R_2$ comes equipped with its projections

$$\pi_1 : R_1 \times R_2 \to R_1, \mid (r_1, r_2) \mapsto r_1$$
$$\pi_2 : R_1 \times R_2 \to R_2, \mid (r_1, r_2) \mapsto r_2.$$

The Cartesian product $X_1 \times X_2$ of sets X_1 and X_2 satisfies the following universal property: for any set Z and any maps $f_1 : Z \to X_1$, $f_2 : Z \to X_2$, there exists a unique map $f : Z \to X_1 \times X_2$ such that $f_1 = \pi_1 \circ f$, $f_2 = \pi_2 \circ f$. The Cartesian product $R_1 \times R_2$ satisfies the analogous universal property in the category of rings.

EXERCISE 1.29. *For rings R_1, R_2, S and ring homomorphisms $f_i : S \to R_i$, there exists a unique homomorphism of rings $f : S \to R_1 \times R_2$ such that $f_i = \pi_i \circ f$.*

So the Cartesian product of R_1 and R_2 is also the product in the categorical sense.

As with sets, we can equally well take the Cartesian product over an arbitrary indexed family of rings: if $\{R_i\}_{i \in I}$ is a family of rings, their Cartesian product $\prod_{i \in I} R_i$ becomes a ring under coordinatewise addition and multiplication, and satisfies the universal property of the product. Details are left to the reader.

It is natural to ask whether the category of rings has a direct sum as well. In other words, given rings R_1 and R_2 we are looking for a ring R together with ring homomorphisms $\iota_i : R_i \to R$ such that for any ring S and homomorphisms $f_i : R_i \to S$, there exists a unique homomorphism $f : R \to S$ such that $f_i = f \circ \iota_i$. We recall that in the category of commutative groups, the Cartesian product group $G_1 \times G_2$ also the categorical direct sum, with $\iota_1 : g \mapsto (g, 0)$ and $\iota_2 : g \mapsto (0, g)$. Since each ring has in particular the structure of a commutative group, it is natural to wonder whether the same might hold true for rings. However, the map $\iota_1 : R_1 \to R_1 \times R_2$ does not preserve the multiplicative identity (unless $R_2 = 0$), so is not a homomorphism of rings when identities are present. Moreover, even

[6]The terminology is unpleasant and is generally avoided as much as possible. One should think of $(I : J)$ as being something like the "ideal quotient" I/J (which of course has no formal meaning). Its uses will gradually become clear.

in the category of algebras, in order to satisfy the universal property on the underlying additive subgroups, the homomorphism f is uniquely determined to be $(r_1, r_2) \mapsto f_1(r_1) + f_2(r_2)$, and it is easily checked that this generally does not preserve the product.

REMARK 2. *The category of rings* does *have categorical direct sums: for rings R_1 and R_2, the universal property of the direct sum is satisfied by the tensor product $R_1 \otimes_{\mathbb{Z}} R_2$.*

Now returning to the case of commutative rings, let us consider the ideal structure of the product $R = R_1 \times R_2$. If I_1 is an ideal of R_1, then $I_1 \times \{0\} = \{(i, 0) \mid i \in I\}$ is an ideal of the product; moreover the quotient $R/(I_1 \times \{0\}$ is isomorphic to $R_1/I_1 \times R_2$. Similarly, if I_2 is an ideal, $\{0\} \times I_2$ is an ideal of R_2. Finally, if I_1 is an ideal of R_1 and I_2 is an ideal of R_2, then

$$I_1 \times I_2 \coloneqq \{(i_1, i_2) \mid i_1 \in I_1,\ i_2 \in I_2\}$$

is an ideal of R. In fact we have already found all the ideals of the product ring:

PROPOSITION 1.8. *Let R_1 and R_2 be commutative rings, and let I be an ideal of $R \coloneqq R_1 \times R_2$. For $i = 1, 2$, put $I_i \coloneqq \pi_i(I)$. Then for $i = 1, 2$ we have that $\pi_i(I)$ is an ideal of R_i and $I = \pi_1(I) \times \pi_2(I)$. Then $I = I_1 \times I_2 = \{(i_1, i_2) \mid i_1 \in I_1,\ i_2 \in I_2\}$.*

PROOF. Since $\pi_i : R_1 \times R_2 \to R_i$ is a surjective ring homomorphism, by Exercise 1.22b) we have that $\pi_i(I)$ is an ideal of R_i, and thus $\pi_1(I) \times \pi_2(I)$ is an ideal of $R_1 \times R_2$.

For any subset S of a Cartesian product $X_1 \times X_2$ we have $S \subseteq \pi_1(S) \times \pi_2(S)$, so certainly

$$I \subseteq \pi_1(I) \times \pi_2(I).$$

The reverse inclusion certainly does not hold in general for subsets of Cartesian products, but it does hold here: if $x \in \pi_1(I)$ then there is $(x, y) \in I$ and then $(x, 0) = (x, y) \cdot (1, 0) \in I$. Similarly we get that if $y \in \pi_2(I)$ then $(0, y) \in I$, so $(x, y) = (x, 0) + (0, y) \in I + I = I$. □

Another way to express the result is that, corresponding to a decomposition $R = R_1 \times R_2$, we get a decomposition $\mathcal{I}(R) = \mathcal{I}(R_1) \times \mathcal{I}(R_2)$.

Let us call a commutative ring R **disconnected** if there exists nonzero rings R_1, R_2 such that $R \cong R_1 \times R_2$, and **connected** otherwise.[7] If R is disconnected, then choosing such an isomorphism φ, we may put $I_1 = \varphi^{-1}(R_1 \times \{0\})$ and $I_2 = \varphi^{-1}(\{0\} \times R_2)$. Evidently I_1 and I_2 are ideals of R such that $I_1 \cap I_2 = \{0\}$ and $I_1 + I_2 = R$. Conversely, if in a ring R we can find a pair of ideals I_1, I_2 with these properties then it will follow from the Chinese Remainder Theorem (Theorem 4.22) that the natural map $\Phi : R \to R/I_2 \times R/I_1$, $r \mapsto (r + I_2, r + I_1)$ is an isomorphism.

Now Φ restricted to I_1 induces an isomorphism of groups onto R/I_2 (and similarly with the roles of I_1 and I_2 reversed). We therefore have a distinguished element of I_1, $e_1 \coloneqq \Phi^{-1}(1)$. This element e_1 is an identity for the multiplication on R restricted to I_1; in particular $e_1^2 = e_1$; such an element is called an **idempotent**. In

[7] We will see later that there is a topological space Spec R associated to every ring, and Spec R is a disconnected topological space if and only if R can be written as a nontrivial product of rings

any ring the elements 0 and 1 are idempotents, called trivial; since $e_1 = \Phi^{-1}(1,0)$ – and not the preimage of $(0,0)$ or of $(1,1)$ – e_1 is a **nontrivial idempotent**. Thus a nontrivial decomposition of a ring implies the presence of nontrivial idempotents.

The converse is also true:

PROPOSITION 1.9. *Suppose R is a ring and e is a nontrivial idempotent element of R: $e^2 = e$ but $e \neq 0, 1$. Put $I_1 = Re$ and $I_2 = R(1-e)$. Then I_1 and I_2 are ideals of R such that $I_1 \cap I_2 = 0$ and $R = I_1 + I_2$, and therefore $R \cong R/I_1 \times R/I_2$ is a nontrivial decomposition of R.*

EXERCISE 1.30. *Prove Proposition 1.9.*

EXERCISE 1.31. *Generalize the preceding discussion to decompositions into a finite number of factors: $R = R_1 \times \cdots \times R_n$.*

8. A cheatsheet

Let R be a commutative ring. Here are some terms that we will analyze in loving detail later, but would like to be able to mention in passing whenever necessary.

R is a **domain** if $xy = 0 \implies x = 0$ or $y = 0$.

An ideal $\mathfrak{p}$ of R is **prime** if the quotient ring $R/\mathfrak{p}$ is a domain. Equivalently, $\mathfrak{p}$ is an ideal such that $xy \in \mathfrak{p} \implies x \in \mathfrak{p}$ or $y \in \mathfrak{p}$.

An ideal $\mathfrak{m}$ of R is **maximal** if it is proper – i.e., not R itself – and not strictly contained in any larger proper ideal. Equivalently, $\mathfrak{m}$ is an ideal such that the quotient ring $R/\mathfrak{m}$ is a field.

R is **Noetherian** if it satisfies any of the following equivalent conditions:[8]

(i) For any nonempty set S of ideals of R, there exists $I \in S$ that is not properly contained in any $J \in S$.
(ii) There is no infinite sequence of ideals $I_1 \subsetneq I_2 \subsetneq \ldots$ in R.
(iii) Every ideal of R is finitely generated.

R is **Artinian** (or sometimes, an **Artin ring**) if the partially ordered set of ideals of R satisfies the descending chain condition: there is no infinite sequence of ideals $I_1 \supsetneq I_2 \supsetneq \ldots$.

Let $R \subseteq S$ be an inclusion of rings. We say that $s \in S$ is **integral over R** if there are $a_0, \ldots, a_{n-1} \in R$ such that

$$s^n + a_{n-1}s^{n-1} + \ldots + a_1 s + a_0 = 0.$$

We say that **S is integral over R** if every element of S is integral over R. This is the appropriate generalization to rings of the notion of an algebraic field extension. We will study integral elements and extensions, um, extensively in § 14, but there is one easy result that we will need earlier, so we give it now.

PROPOSITION 1.10. *Let $R \subseteq S$ be an integral extension of domains. If S is a field then R is a field.*

[8]See Theorem 8.24 for a proof of their equivalence.

PROOF. Let $\alpha \in R^\bullet$. Then α^{-1} is integral over R: there are $a_i \in R$ such that

$$\alpha^{-n} = a_{n-1}\alpha^{-n+1} + \ldots + a_1\alpha^{-1} + a_0.$$

Multiplying through by α^{n-1} gives

$$\alpha^{-1} = a_{n-1} + a_{n-2}\alpha + \ldots + a_1\alpha^{n-2} + a_0\alpha^{n-1} \in R. \qquad \square$$

CHAPTER 2

Galois Connections

1. The basic formalism

Let $(X, \leqslant)$ be a partially ordered set. We denote by $X^\vee$ the **order dual** of X: it has the same underlying set as X but the inverse order relation: $x \preceq y \iff y \leqslant x$.

Let $(X, \leqslant)$ and $(Y, \leqslant)$ be partially ordered sets. A map $f : X \to Y$ is **isotone** (or **order-preserving**) if for all $x_1, x_2 \in X$, $x_1 \leqslant x_2 \implies f(x_1) \leqslant f(x_2)$; f is **antitone** (or **order-reversing**) if for all $x_1, x_2 \in X$, $x_1 \leqslant x_2 \implies f(x_1) \geqslant f(x_2)$.

EXERCISE 2.1. *Let X, Y, Z be partially ordered sets, and let $f : X \to Y$, $g : Y \to Z$ be functions. Show:*

a) *If f and g are isotone, then $g \circ f$ is isotone.*
b) *If f and g are antitone, then $g \circ f$ is isotone.*
c) *If one of f and g is isotone and the other is antitone, then $g \circ f$ is antitone.*

Let $(X, \leqslant)$ and $(Y, \leqslant)$ be partially ordered sets. An **antitone Galois connection between X and Y** is a pair of maps $\Phi : X \to Y$ and $\Psi : Y \to X$ such that:

(GC1) Φ and Ψ are both antitone maps, and
(GC2) For all $x \in X$ and all $y \in Y$, $x \leqslant \Psi(y) \iff y \leqslant \Phi(x)$.

There is a pleasant symmetry in the definition: if (Φ, Ψ) is a Galois connection between X and Y, then (Ψ, Φ) is a Galois connection between Y and X.

EXERCISE 2.2. *Let $(X, \leqslant)$ be a partially ordered set. Let $f : X \to X$ be an antitone map such that*

$$\forall x \in X,\ x \leqslant f(f(x)).$$

Show: (f, f) is a Galois connection between X and X.

If $(X, \leqslant)$ is a partially ordered set, then a mapping $f : X \to X$ is called a **closure operator** if it satisfies all of the following properties:

(C1) For all $x \in X$, $x \leqslant f(x)$.
(C2) For all $x_1, x_2 \in X$, $x_1 \leqslant x_2 \implies f(x_1) \leqslant f(x_2)$.
(C3) For all $x \in X$, $f(f(x)) = f(x)$.

PROPOSITION 2.1. *The mapping $\Psi \circ \Phi$ is a closure operator on $(X, \leqslant)$ and the mapping $\Phi \circ \Psi$ is a closure operator on $(Y, \leqslant)$.*

PROOF. By symmetry, it is enough to consider the mapping $x \mapsto \Psi(\Phi(x))$ on X. If $x_1 \leqslant x_2$, then since both Φ and Ψ are antitone, we have $\Phi(x_1) \geqslant \Phi(x_2)$ and thus $\Psi(\Phi(x_1)) \leqslant \Psi(\Phi(x_1))$: (C2).

For $x \in X$, $\Phi(x) \geqslant \Phi(x)$, and by (GC2) this implies $x \leqslant \Psi(\Phi(x))$: (C1).
Finally, for $x \in X$, applying (C1) to the element $\Psi(\Phi(x))$ of X gives

$$\Psi(\Phi(x)) \leqslant \Psi(\Phi(\Psi(\Phi(x)))).$$

Conversely, we have

$$\Psi(\Phi(x)) \leqslant \Psi(\Phi(x)),$$

so by (GC2)

$$\Phi(\Psi(\Phi(x)) \geqslant \Phi(x),$$

and applying the order-reversing map Ψ gives

$$\Psi(\Phi(\Psi(\Phi(x)))) \leqslant \Psi(\Phi(x)).$$

Thus

$$\Psi(\Phi(x)) = \Psi(\Phi(\Psi(\Phi(x))).$$

□

COROLLARY 2.2. *Φ and Ψ satisfy the following **tridempotence** properties:*

a) *For all $x \in X$, $\Phi\Psi\Phi x = \Phi x$.*
b) *For all $y \in X$, $\Psi\Phi\Psi y = \Psi y$.*

PROOF. By symmetry, it suffices to prove a). Since $\Phi \circ \Psi$ is a closure operator, $\Phi\Psi\Phi x \geqslant \Phi x$. Moreover, since $\Psi \circ \Phi$ is a closure operator, $\Psi\Phi x \geqslant x$, and since Φ is antitone, $\Phi\Psi\Phi x \leqslant \Phi x$. So $\Phi\Psi\Phi x = \Phi x$. □

PROPOSITION 2.3. *Let (Φ, Ψ) be a Galois connection between partially ordered sets X and Y. Let $\overline{X} = \Psi(\Phi(X))$ and $\overline{Y} = \Psi(\Phi(Y))$. Then:*

a) *$\overline{X}$ and $\overline{Y}$ are precisely the subsets of closed elements of X and Y respectively.*
b) *We have $\Phi(X) \subseteq \overline{Y}$ and $\Psi(Y) \subseteq \overline{X}$.*
c) *$\Phi : \overline{X} \to \overline{Y}$ and $\Psi : \overline{Y} \to \overline{X}$ are mutually inverse bijections.*

PROOF. a) If $x = \Psi(\Phi(x))$ then $x \in \overline{X}$. Conversely, if $x \in \overline{X}$, then $x = \Psi(\Phi(x'))$ for some $x' \in X$, so

$$\Psi(\Phi(x))) = \Psi(\Phi(\Psi(\Phi(x')))) = \Psi(\Phi(x')) = x,$$

so X is closed.
b) This is just a reformulation of Corollary 2.2.
c) If $x \in \overline{X}$ and $y \in \overline{Y}$, then $\Psi(\Phi(x)) = x$ and $\Psi(\Phi(y)) = y$. □

We speak of the mutually inverse antitone bijections $\Phi : \overline{X} \to \overline{Y}$ and $\Psi : \overline{Y} \to \overline{X}$ as the **Galois correspondence** induced by the Galois connection (Φ, Ψ).

EXAMPLE 2.4. *Let K/F be a field extension, and G a subgroup of $\mathrm{Aut}(K/F)$. Then there is a Galois connection between the set of subextensions of K/F and the set of subgroups of G, given by*

$$\Phi : L \to G_L = \{\sigma \in G \mid \sigma x = x \ \forall x \in L\},$$

$$\Psi : H \to K^H = \{x \in K \mid \sigma x = x \ \forall \sigma \in H\}.$$

Having established the basic results, we will now generally abbreviate the closure operators $\Psi \circ \Phi$ and $\Phi \circ \Psi$ to $x \mapsto \overline{x}$ and $y \mapsto \overline{y}$.

2. Lattice properties

Recall that a partially ordered set X is a **lattice** if for all $x_1, x_2 \in X$, there is a greatest lower bound $x_1 \wedge x_2$ and a least upper bound $x_1 \vee x_2$. A partially ordered set is a **complete lattice** if for every subset A of X, the greatest lower bound $\bigwedge A$ and the least upper bound $\bigvee A$ both exist.

LEMMA 2.5. *Let (X, Y, Φ, Ψ) be a Galois connection.*

a) *If X and Y are both lattices, then for all $x_1, x_2 \in X$, we have*

$$\Phi(x_1 \vee x_2) = \Phi(x_1) \wedge \Phi(x_2).$$

b) *If X and Y are both complete lattices, then for all subsets $A \subseteq X$, we have*

$$\Phi(\bigvee A) = \bigwedge \Phi(A).$$

PROOF. We will prove part a) and leave the proof of part b) as an exercise.

For $y \in Y$, we have $y \leqslant \Phi(x_1 \vee x_2)$ if only if $x_1 \vee x_2 \leqslant \Psi(y)$ if and only if $x_i \leqslant \Psi(y)$ for $i = 1, 2$ if and only if $y \leqslant \Phi(x_i)$ for $i = 1, 2$ if and only if $y \leqslant \Phi(x_1) \wedge \Phi(x_2)$. □

EXERCISE 2.3. *Prove Lemma 2.5b).*

Unfortunately, in a Galois connection (X, Y, Φ, Ψ) in which X and Y are lattices, we need *not* have

$$\forall x_1, x_2 \in X,\ \Phi(x_1 \wedge x_2) = \Phi(x_1) \vee \Phi(x_2),$$

even if X and Y are complete lattices. The following counterexample was communicated anonymously [**msegc**].

EXAMPLE 2.6. *We consider a partially ordered set X with five elements, called $0, a, b, c, 1$. We define the partial ordering as follows: 0 is the bottom element (i.e., less than every other element) and 1 is the top element (i.e., greater than every other element); the ordering restricted to $\{a, b, c\}$ is given by $a, b \leqslant c$. This is a complete lattice. We define $f : X \to X$ by*

$$f(0) = 1,\ f(a) = b,\ f(b) = a,\ f(c) = f(1) = 0.$$

Using Exercise 2.2 it is almost immediate to see that (f, f) is a Galois connection from X to X. However, we have

$$f(a) \vee f(b) = b \vee a = c < 1 = f(0) = f(a \wedge b).$$

Complete lattices also intervene in this subject in the following way.

PROPOSITION 2.7. *Let A be a set and let $X = (2^A, \subset)$ be the power set of A, partially ordered by inclusion. Let $c : X \to X$ be a closure operator. Then the collection $c(X)$ of closed subsets of A forms a complete lattice, with $\bigwedge S = \bigcap_{B \in S} B$ and $\bigvee S = c(\bigcup_{B \in S} B)$.*

EXERCISE 2.4. *Prove Proposition 2.7.*

3. Examples of Antitone Galois Connections

EXAMPLE 2.8. *(Indiscretion) Let $(X, \leqslant)$, $(Y, \leqslant)$ be partially ordered sets with top elements T_X, T_Y. Define $\Phi : X \to Y$, $x \mapsto T_Y$ and $\Psi : Y \to X$, $y \mapsto T_X$. Then (X, Y, Φ, Ψ) is a Galois connection. The induced closure operators are "indiscrete": they send every element of X (resp. Y) to the top element T_X (resp. T_Y).*

EXAMPLE 2.9. *(Perfection) Let $(X, \leqslant)$ and $(Y, \leqslant)$ be **anti-isomorphic partially ordered sets**, i.e., suppose that there exists a bijection $\Phi : X \to Y$ with $x_1 \leqslant x_2 \iff \Phi(x_2) \leqslant \Phi(x_1)$. Then the inverse map $\Psi : Y \to X$ satisfies $y_1 \leqslant y_2 \iff \Psi(y_2) \leqslant \Psi(y_1)$. Moreover, for $x \in X$, $y \in Y$, $x \leqslant \Psi(y) \iff y = \Psi(\Phi(y)) \leqslant \Phi(x)$, so (X, Y, Φ, Ψ) is a Galois connection. Then $\overline{X} = X$ and $\overline{Y} = Y$. As we saw above, the converse also holds: if $\overline{X} = X$ and $\overline{Y} = Y$ then Φ and Ψ are mutually inverse bijections. Such a Galois connection is called **perfect**.*[1]

EXAMPLE 2.10. *(Trope-Namer) Let L/K be a field extension. Let X be the set of all subextensions M of L/K, i.e., fields usch that $K \subseteq M \subseteq L$, partially ordered under inclusion. Let Y be the set of all subgroups of $\mathrm{Aut}(L/K)$, partially ordered under inclusion. Define $\Phi : X \to Y$ and $\Psi : Y \to X$ as follows:*

$$\Phi(L) \coloneqq \mathrm{Aut}(M/L) \text{ and } \Psi(H) \coloneqq L^H \coloneqq \{x \in L \mid \forall \sigma \in H, \sigma(x) = x\}.$$

It is immediate that Φ and Ψ are antitone. For all $M \in X$ and $H \in Y$ we have

$$M \leqslant \Psi(H) \iff M \subseteq L^H$$

$$\iff \forall x \in M,\ \forall \sigma \in H, \sigma(x) = x \iff$$

$$H \subseteq \mathrm{Aut}(L/M) \iff \Phi(M) \leqslant H.$$

So far we have introduced the formalism of Galois theory but not the content. The content is the assertion that if L/K is normal, separable and of finite degree, then the Galois connection (Φ, Ψ) is perfect. By the way, the converse of this is also true: if for a field extension L/K the Galois connection (Φ, Ψ) is perfect, then L/K is normal, separable and of finite degree. We leave this to the interested reader as a nontrivial field-theoretic exercise.

The remaining examples of this section make use of some important ring-theoretic concepts that will be treated in more detail later on in the text.

EXAMPLE 2.11. *Let R be a commutative ring. Let X be the set of all ideals of R and $Y = 2^{\mathrm{Spec}\, R}$ the power set of the set of prime ideals of R. For $I \in X$, put*

$$\Phi(I) = V(I) = \{\mathfrak{p} \in \mathrm{Spec}\, R \mid I \subseteq \mathfrak{p}\}.$$

For $V \in Y$, put

$$\Psi(V) = \bigcap_{\mathfrak{p} \in V} \mathfrak{p}.$$

[1] There is a small paradox here: in purely order-theoretic terms this example is not any more interesting than the previous one. But in practice given two partially ordered sets it is infinitely more useful to have a pair of mutually inverse antitone maps running between them than the trivial operators of the previous example. The paradox already shows up in the distinction between indiscrete spaces and discrete spaces: although neither topology looks more interesting than the other, the discrete topology is natural and useful (as we shall see...) whereas the indiscrete topology entirely deserves its alternate name "trivial".

The maps Φ and Ψ are antitone, and for $I \in \mathcal{X}$, $V \in \mathcal{Y}$,

$$I \subseteq \Psi(V) \iff I \subseteq \bigcap_{\mathfrak{p} \in V} \mathfrak{p} \iff \forall \mathfrak{p} \in V, I \subseteq \mathfrak{p} \iff V \subseteq \Phi(I), \tag{1}$$

so (Φ, Ψ) is a Galois connection. Then $\overline{X}$ consists of all ideals which can be written as the intersection of a family of prime ideals. For all $I \in X$,

$$\overline{I} = \bigcap_{\mathfrak{p} \supset I} \mathfrak{p} = \operatorname{rad} I = \{x \in R \mid \exists n \in \mathbb{Z}^+ \ x^n \in I\};$$

that is, the induced closure operation on X takes any ideal to its ***radical*** *$r(I)$. In particular $\overline{X}$ consists precisely of the radical ideals.*

It is not so easy to describe the closure operator on Y or even the subset $\overline{Y}$ explicitly, but there is still something nice to say. Since:

$$V((0)) = \operatorname{Spec} R, \ V(R) = \varnothing, \tag{2}$$

$$V(I_1) \cup V(I_2) = V(I_1 I_2), \tag{3}$$

$$\bigcap_{\alpha \in A} V(I_\alpha) = V(\sum_{\alpha \in A} I_\alpha), \tag{4}$$

the elements of $\overline{Y}$ are the closed subsets for a topology, the ***Zariski topology****.*

Example 2.12. *Take R and X as above, but now let S be any set of ideals of R and put $Y = 2^S$. For $I \in X$, put*

$$\Phi(I) = V(I) = \{\mathfrak{s} \in S \mid I \subseteq \mathfrak{s}\}$$

and for $V \in \mathcal{Y}$, put

$$\Psi(V) = \bigcap_{\mathfrak{s} \in V} \mathfrak{s}.$$

Once again Φ and Ψ are antitone maps and (1) holds, so we get a Galois connection. The associated closure operation on X is

$$I \mapsto \overline{I} = \bigcap_{\mathfrak{s} \in S} \mathfrak{s}.$$

The relation (4) holds for any S, and the relation (2) holds so long as $R \notin S$. The verification of (3) for $R = \operatorname{Spec} R$ uses the fact that a prime ideal $\mathfrak{p}$ contains $I_1 I_2$ if and only if it contains I_1 or I_2, so as long as $S \subseteq \operatorname{Spec} S$, $\overline{Y} = \{V(I) \mid I \in X\}$ are the closed subsets for a topology on S. This is indeed the topology S inherits as a subspace of $\operatorname{Spec} R$, so we call it the ***(relative) Zariski topology****.*

Various particular choices of $S \subseteq \operatorname{Spec} R$ have been considered. Of these the most important is certainly $S = \operatorname{MaxSpec} R$, the set of all maximal ideals of R. In this case, $\overline{X}$ consists of all ideals that can be written as the intersection of some family of maximal ideals. Such ideals are necessarily radical, but in a general ring not all radical ideals are obtained in this way. Observe that in a general ring every radical ideal is the intersection of the maximal ideals containing it if and only if every prime ideal is the intersection of maximal ideals containing it; a ring satisfying these equivalent conditions is called a ***Jacobson ring****.*

EXAMPLE 2.13. *Let k be a field and put $R = k[t_1, \ldots, t_n]$. Then R is a Jacobson ring (Proposition 11.3).*

*Suppose that k is algebraically closed. Then Zariski's Lemma assumes a stronger form: for all $\mathfrak{m} \in \operatorname{MaxSpec} R$, the k-algebra $R/\mathfrak{m}$ is equal to k. Let $q : R \to R/\mathfrak{m} = k$ be the quotient map, and for $1 \leqslant i \leqslant n$, put $x_i = q(t_i)$ and $x = (x_1, \ldots, x_n)$. It follows that $\mathfrak{m}$ contains the ideal $\mathfrak{m}_x = \langle t_1 - x_1, \ldots, t_n - x_n \rangle$, and since $\mathfrak{m}_x$ is maximal, $\mathfrak{m} = \mathfrak{m}_x$. This gives the following description of the Galois connection between the set X of ideals of R and $Y = 2^{\operatorname{MaxSpec} R}$, **Hilbert's Nullstellensatz**:*

(i) *Maximal ideals of R are canonically in bijection with n-tuples of points of k, i.e., with points of **affine n-space** $\mathbb{A}^n_{/k}$.*
(ii) *The closure operation on ideals takes I to its radical ideal $\operatorname{rad} I$.*
(iii) *The closure operation on subsets of $\mathbb{A}^n$ coincides with topological closure with respect to the Zariski topology, i.e., the topology on $\mathbb{A}^n$ for which the closed subsets are the intersections of the zero sets of polynomial functions.*

EXAMPLE 2.14. *Let K be a field, let $X = 2^K$, let $\operatorname{RSpec} K$ be the set of orderings on K, and let $Y = 2^{\operatorname{RSpec} K}$. Let $H : X \to Y$ by*

$$S \mapsto H(S) = \{P \in \operatorname{RSpec} K \mid \forall x \in S \ x >_P 0\}.$$

Let $\Psi : Y \to X$ by

$$T \mapsto \Psi(T) = \{x \in \operatorname{RSpec} K \mid \forall P \in T \ x >_P 0\}.$$

Then (X, Y, H, Ψ) is a Galois connection.

*The set $\operatorname{RSpec} K$ carries a natural topology. Namely, we may view any ordering P as an element of $\{\pm 1\}^{K^\times}$: $P : x \in K^\times \mapsto +1$ if $P(x) > 0$ and -1 is $P(x) < 0$. Giving $\{\pm 1\}$ the discrete topology and $\{\pm 1\}^{K^\times}$, it is a compact (by Tychonoff's Theorem) zero-dimensional space, hence a **Boolean space** in the sense of §9.5. It is easy to see that $\operatorname{RSpec} K$ embeds in $\{\pm 1\}^{K^\times}$ as a closed subspace, and therefore $\operatorname{RSpec} K$ is itself a **Boolean space**.*

EXAMPLE 2.15. *Let $\mathcal{L}$ be a language, let X be the set of $\mathcal{L}$-theories, and let Y be the class of all classes $\mathcal{C}$ of $\mathcal{L}$-structures, partially ordered by inclusion.*[2] *For a theory $\mathcal{T}$, let $\Phi(\mathcal{T}) = \mathcal{C}_\mathcal{T}$ be the class of all models of $\mathcal{T}$, whereas for a class $\mathcal{C}$, we define $\Psi(\mathcal{C})$ to be the collection of all sentences φ such that for all $X \in \mathcal{C}$, $X \models \varphi$.*

4. Antitone Galois Connections Decorticated: Relations

Example: Let S and T be sets, and let $R \subseteq S \times T$ be a **relation** between S and T. As is traditional, we use the notation xRy for $(x, y) \in R$. For $A \subseteq S$ and $y \in T$, we let us write ARy if xRy for all $x \in A$; and dually, for $x \in S$ and $B \subseteq T$, let us write xRB if xRy for all $y \in B$. Finally, for $A \subseteq S$, $B \subseteq T$, let us write ARB if xRy for all $x \in A$ and all $y \in B$.

Let $X = (2^S, \subset)$, $Y = (2^T, \subset)$. For $A \subseteq S$ and $B \subseteq T$, we put

$$\Phi_R(A) = \{y \in T \mid ARy\},$$

$$\Psi_R(B) = \{x \in S \mid xRB\}.$$

[2]Here we are cheating a bit by taking instead of a partially ordered set, a *partially ordered class*. We leave it to the interested reader to devise a remedy.

We claim that $\mathcal{G}_R = (X, Y, \Phi_R, \Psi_R)$ is a Galois connection. Indeed, it is immediate that Φ_R and Ψ_R are both antitone maps; moreover, for all $A \subseteq S,\ B \subseteq T$ we have

$$A \subseteq \Psi_R(B) \iff ARB \iff B \subseteq \Phi_R(A).$$

Remarkably, this example includes most of the Galois connections above. Indeed:

• In Example 2.2, take X to be 2^K and $Y = 2^{\mathrm{Aut}(K/F)}$. The induced Galois connection is the one associated to the relation $gx = x$ on $K \times \mathrm{Aut}(K/F)$.
• In Example 2.5, take X to be 2^R. The induced Galois connection is the one associated to the relation $x \in \mathfrak{p}$ on $R \times \operatorname{Spec} R$. Similarly for Examples 2.7 and 2.8.
• The Galois connection of Example 2.8 is the one associated to the relation $x \in P$ on $K \times \operatorname{RSpec} K$.
• The Galois connection of Example 2.9 is the one associated to the relation $X \models \varphi$.

THEOREM 2.16. *Let S and T be sets, let $X = (2^S, \subset)$, $Y = (2^S, \subset)$, and let $\mathcal{G} = (X, Y, \Phi, \Psi)$ be any Galois connection. Define a relation $R \subseteq S \times T$ by xRy if $y \in \Phi(\{x\})$. Then $\mathcal{G} = \mathcal{G}_R$.*

PROOF. Note first that X and Y are complete lattices, so Lemma 2.5b) applies. Indeed, for $A \subseteq S$, $A = \bigcup_{x\in A}\{x\} = \bigvee_{x\in A}\{x\}$, so

$$\Phi(A) = \bigcap_{x\in A} \Phi(\{x\}) = \bigcap_{x\in A} \{y \in T \mid xRy\} = \{y \in T \mid ARy\} = \Phi_R(A).$$

Moreover, since $\mathcal{G}$ is a Galois connection we have $\{x\} \subseteq \Psi(\{y\}) \iff \{y\} \subseteq \Phi(\{x\}) \iff xRy$. Thus for $B \subseteq T$, $B = \bigcup_{y\in B}\{y\} = \bigvee_{y\in B}\{y\}$, so

$$\Psi(B) = \bigcap_{y\in B} \Psi(\{y\}) = \bigcap_{y\in A} \{x \in S \mid xRy\} = \{x \in S \mid xRB\} = \Psi_R(B). \qquad \square$$

For any partially ordered set $(X, \leqslant)$, a **downset** is a subset $Y \subseteq X$ such that for all $x_1, x_2 \in X$, if $x_2 \in Y$ and $x_1 \leqslant x_2$ then $x_1 \in Y$. Let $D(X)$ be the collection of all downsets of X, viewed as a subset of $(2^X, \subset)$. To each $x \in X$ we may associate the **principal downset** $d(x) = \{y \in X \mid y \leqslant x\}$. The map $d : X \to D(X)$ is an order embedding; composing this with the inclusion $D(X) \subseteq 2^X$ we see that every partially ordered set embeds into a power set lattice.

Let $\mathcal{G} = (X, Y, \Phi, \Psi)$ be a Galois connection with X and Y complete lattices. Then we may extend $\mathcal{G}$ to a Galois conection between 2^X and 2^Y as follows: for $A \subseteq X$, put $\Phi(A) = \bigwedge\{\Phi(x)\}_{x\in A}$, and simialrly for $B \subseteq Y$, put $\Psi(B) = \bigwedge\{\Psi(y)\}_{y\in B}$. Thus every Galois connection between complete lattices may be viewed as the Galois connection induced by a relation between sets.

5. Isotone Galois Connections

Let $(X, \leqslant)$ and $(Y, \leqslant)$ be partially ordered sets. An **isotone Galois connection between X and Y** is a pair of maps $\Phi : X \to Y$ and $\Psi : Y \to X$ such that:

(IGC1) Φ and Ψ are both isotone maps, and
(IGC2) For all $x \in X$ and all $y \in Y$, $\Phi(x) \leqslant y \iff x \leqslant \Psi(y)$.

In contrast to the antitone case, this time there is an *asymmetry* between Φ and Ψ. We call Φ the **lower adjoint** and Ψ the **upper adjoint**.

At the abstract level, the concepts of antitone and isotone Galois connection are manifestly equivalent.

EXERCISE 2.5. *Let X, Y be partially ordered sets, and let $\Phi : X \to Y$, $\Psi : Y \to X$ be functions.*

a) *Show: (Φ, Ψ) is an antitone Galois connection between X and Y if and only if (Φ, Ψ) is an isotone Galois connection between $X^\vee$ and Y.*
b) *Show: (Φ, Ψ) is an antitone Galois connection between X and Y if and only if (Ψ, Φ) is an isotone Galois connection between $Y^\vee$ and X.*

If $(X, \leqslant)$ is a partially ordered set, then a mapping $f : X \to X$ is called an **interior operator** if it satisfies all of the following properties:

(I1) For all $x \in X$, $x \geqslant f(x)$.
(C2) For all $x_1, x_2 \in X$, $x_1 \leqslant x_2 \implies f(x_1) \leqslant f(x_2)$.
(C3) For all $x \in X$, $f(f(x)) = f(x)$.

EXERCISE 2.6. *Let $(X, \leqslant)$ be a partially ordered set, and let $f : X \to X$ be a function. Show: f is a closure operator if and only if $f : X^\vee \to X^\vee$ is an interior operator.*

PROPOSITION 2.17. *Let (Φ, Ψ) be an isotone Galois connection. Then $\Psi \circ \Phi$ is an interior operator on $(X, \leqslant)$, and $\Phi \circ \Psi$ is a closure operator on $(Y, \leqslant)$.*

PROOF. By Exercise 2.5, (Φ, Ψ) is an antitone Galois connection between $X^\vee$ and Y, so by Proposition 2.1, $\Phi \circ \Psi$ is a closure operator on Y and $\Psi \circ \Phi$ is a closure operator on $X^\vee$ and thus, by Exercise 2.6, an interior operator on X. □

6. Examples of Isotone Galois Connections

Example (Galois connection of a function): Let $f : S \to T$ be a function. Let $X = (2^S, \subset)$ and $Y = (2^T, \subset)$. For $A \subseteq S$ and $B \subseteq T$, put

$$f_*(S) = f(S) = \{f(s) \mid s \in S\}, \ f^*(T) = f^{-1}(B) = \{s \in S \mid f(s) \in B\}.$$

EXERCISE 2.7.
a) *Show: (f^*, f_*) is an isotone Galois connection between 2^T and 2^S.*
b) *Show that the interior operator $f_* \circ f^* : B \subseteq T \mapsto B \cap f(S)$. In particular the Galois connection is **left perfect** if and only if f is surjective.*
c) *Show that the Galois connection is **right perfect** – i.e., $f^* f_* A = A$ for all $A \subseteq S$ – if and only if f is injective.*
d) *Interpret this isotone Galois connection in terms of the "universal" antitone Galois connection of §2.4.*

EXAMPLE 2.18. *(Galois Connection of a Ring Homomorphism): Let $f : R \to S$ be a homomorphism of rings, and let $\mathcal{I}(R)$ and $\mathcal{I}(S)$ be the lattices of ideals of R and S. In §1.5 we defined a pushforward map*

$$f_* : \mathcal{I}(R) \to \mathcal{I}(S), \ f_*(I) = \langle f(I) \rangle$$

and a pullback map

$$f^* : \mathcal{I}(S) \to \mathcal{I}(R), \ f^*(J) = f^{-1}(J).$$

PROPOSITION 2.19. *The maps* (f^*, f_*) *give an isotone Galois connection between* $\mathcal{I}(S)$ *and* $\mathcal{I}(T)$.

EXERCISE 2.8. *Prove Proposition 2.19.*

CHAPTER 3

Modules

1. Basic definitions

Suppose $(M, +)$ is a commutative group. For any $m \in M$ and any integer n, one can make sense of $n \bullet m$. If n is a positive integer, this means $m + \cdots + m$ (n times); if $n = 0$ it means 0, and if n is negative, then $n \bullet m = -(-n) \bullet m$. Thus we have defined a function $\bullet : \mathbb{Z} \times M \to M$ that enjoys the following properties: for all $n,\ n_1,\ n_2 \in \mathbb{Z},\ m,\ m_1,\ m_2 \in M$, we have

(ZMOD1) $1 \bullet m = m$.
(ZMOD2) $n \bullet (m_1 + m_2) = n \bullet m_1 + n \bullet m_2$.
(ZMOD3) $(n_1 + n_2) \bullet m = n_1 \bullet m + n_2 \bullet m$.
(ZMOD4) $(n_1 n_2) \bullet m = n_1 \bullet (n_2 \bullet m)$

It should be clear that this is some kind of ring-theoretic analogue of a group action on a set. In fact, consider the slightly more general construction of a monoid $(M, \cdot)$ acting on a set S: that is, for all $n_1,\ n_2 \in M$ and $s \in S$, we require $1 \bullet s = s$ and $(n_1 n_2) \bullet s = n_1 \bullet (n_2 \bullet s)$.

For a group action G on S, each function $g\bullet : S \to S$ is a bijection. For monoidal actions, this need not hold for all elements: e.g. taking the natural multiplication action of $M = (\mathbb{Z}, \cdot)$ on $S = \mathbb{Z}$, we find that $0\bullet : \mathbb{Z} \to \{0\}$ is neither injective nor surjective, $\pm 1\bullet : \mathbb{Z} \to \mathbb{Z}$ is bijective, and for $|n| > 1$, $n\bullet : \mathbb{Z} \to \mathbb{Z}$ is injective but not surjective.

EXERCISE 3.1. *Let $\bullet : M \times S \to S$ be a monoidal action on a set. Let $M^\times$ be the group of units of M: that is, the subset of elements $x \in M$ for which there is $y \in M$ such that $xy = yx = 1$. Show: for each $u \in M^\times$, the map $u\bullet : S \to S$ is a bijection.*

Then the above "action" of $\mathbb{Z}$ on a commutative group M is in particular a monoidal action of $(\mathbb{Z}, \cdot)$ on the set M. But it is more: M has an additive structure, and (ZMOD2) asserts that for each $n \in \mathbb{Z}$, $n\bullet$ respects this structure – i.e., is a homomorphism of groups; also (ZMOD3) is a compatibility between the additive structure on $\mathbb{Z}$ and the additive structure on M.

These axioms can be restated in a much more compact form. For a commutative group M, an **endomorphism** of M is just a group homomorphism from M to itself: $f : M \to M$. We write $\mathrm{End}(M)$ for the set of all endomorphisms of M. But $\mathrm{End}(M)$ has lots of additional structure: for $f, g \in \mathrm{End}(M)$ we define $f + g \in \mathrm{End}(M)$ by

$$(f + g)(m) \coloneqq f(m) + g(m),$$

i.e., pointwise addition. We can also define $f \cdot g \in \mathrm{End}(M)$ by composition:

$$(f \cdot g)(m) := f(g(m)).$$

PROPOSITION 3.1. *For any commutative group M, the set $\mathrm{End}(M)$ of group endomorphisms of M, endowed with pointwise addition and multiplication by composition, has the structure of a ring.*

EXERCISE 3.2. *Prove Proposition 3.1.*

EXERCISE 3.3. *Show: $\mathrm{End}(\mathbb{Z}) = \mathbb{Z}$, and for any $n \in \mathbb{Z}$, $\mathrm{End}(\mathbb{Z}/n\mathbb{Z}) = \mathbb{Z}/n\mathbb{Z}$. (More precisely, find canonical isomorphisms.)*

These simple examples are potentially misleading: we did not say that the multiplication was commutative, and of course there is no reason to expect composition of functions to be commutative.

EXERCISE 3.4.

a) *Show: $\mathrm{End}(\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}) = M_2(\mathbb{Z}/2\mathbb{Z})$, the (noncommutative!) ring of 2×2 matrices with $\mathbb{Z}/2\mathbb{Z}$-coefficients.*

b) *If M is a commutative group and $n \in \mathbb{Z}^+$, show $\mathrm{End}(M^n) = M_n(\mathrm{End}(M))$.*

Now observe that the statement that the action of $\mathbb{Z}$ on M satisfes (ZMOD1) through (ZMOD4) is equivalent to the following much more succinct statement:

For any commutative group M, the map $n \in \mathbb{Z} \mapsto (n\bullet) : M \to M$ is a homomorphism of rings $\mathbb{Z} \to \mathrm{End}(M)$.

This generalizes very cleanly: if R is any ring (not necessarily commuative) and M is a commutative group, a homomorphism $\bullet : R \to \mathrm{End}(M)$ will satisfy: for all $r \in R,\ m, m_1, m_2 \in M$:

(LRMOD1) $1 \bullet m = m$.
(LRMOD2) $r \bullet (m_1 + m_2) = r \bullet m_1 + r \bullet m_2$.
(LRMOD3) $(r_1 + r_2) \bullet m = r_1 \bullet m + r_2 \bullet m$.
(LRMOD4) $(r_1 r_2) \bullet m = r_1 \bullet (r_2 \bullet m)$.

The terminology here is that such a homomorphism $r \mapsto (r\bullet)$ is a **left R-module structure** on the commutative group M.

What then is a **right R-module structure** on M? The pithy version is that it is a ring homomorphism from R^{op}, the opposite ring of R to $\mathrm{End}(M)$. This definition makes clear (only?) that if R is commutative, there is no difference between left and right R-module structures. Since our interest is in the commutative case, we may therefore not worry too much. But for the record:

EXERCISE 3.5. *Show: a homomorphism $R^{\mathrm{op}} \to \mathrm{End}(M)$ is equivalent to a mapping $\bullet : M \times R \to M$ satisfying*

$$m \bullet 1 = m,$$
$$(m_1 + m_2) \bullet r = m_1 \bullet r + m_2 \bullet r,$$
$$m \bullet (r_1 + r_2) = m \bullet r_1 + m \bullet r_2,$$
$$m \bullet (r_1 r_2) = (m \bullet r_1) \bullet r_2.$$

As usual for multiplicative notation, we will generally suppress the bullet, writing rm for left R-modules and mr for right R-modules.

The calculus of left and right actions is at the same time confusing and somewhat miraculous: it is a somewhat disturbing example of a purely lexicographical convention that has – or looks like it has – actual mathematical content. Especially, suppose we have a commutative group M and two rings R and S, such that M simultaneously has the structure of a left R-module and a right S-module. Thus we wish to entertain expressions such as rms for $m \in M$, $r \in R$, $s \in S$. But as stands this expression is ambiguous: it could mean either

$$(r \bullet m) \bullet s$$

or

$$r \bullet (m \bullet s).$$

We say that M is an **R-S bimodule** if both of these expressions agree. Here is what is strange about this: lexicographically, it is an associativity condition. But "really" it is a commutativity condition: it expresses the fact that for all $r \in R$, $s \in S$, $(r\bullet) \circ (\bullet s) = (\bullet s) \circ (r\bullet)$: every endomorphism coming from an element of R commutes with every endomorphism coming from an element of S. Thus for instance:

EXERCISE 3.6. *Show: any ring R is naturally an $R - R$-bimodule.*

We will not deal with bimodules further in these notes. In fact, when we say R-module at all, it will be understood to mean a left R-module, and again, since we shall only be talking about commutative rings soon enough, the distinction between left and right need not be made at all.

For M a left R-module, we define its **annihilator**

$$\operatorname{ann}(M) = \{r \in R \mid \forall m \in M, rm = 0\}.$$

Equivalently, $\operatorname{ann}(M)$ is the set of all r such that $r\cdot = 0 \in \operatorname{End}(M)$, so that it is precisely the kernel of the associated ring homomorphism $R \to \operatorname{End}(M)$. It follows that $\operatorname{ann}(M)$ is an ideal of R (note: two-sided, in the noncommutative case). If $m \in M$, we put

$$\operatorname{ann}(m) := \{r \in R \mid rm = 0\}.$$

Then $\operatorname{ann}(m)$ is a left ideal of R. To see that it need not be an ideal in general, consider the case $R = M_2(F)$ is the ring of 2×2 matrices over a field F. Then R naturally acts on F^2 by viewing the elements as column vectors. The annihilator of $(1, 0)$ is

$$I := \begin{bmatrix} 0 & b \\ 0 & d \end{bmatrix}.$$

Then I is a left ideal but not a right ideal of $M_2(F)$. In fact, for any $n \in \mathbb{Z}^+$ the ring $M_n(F)$ of $n \times n$ matrices over a field is **simple**: it has no nonzero, proper two-sided ideals.

EXERCISE 3.7. *Let R be a commutative ring, and let M be a left R-module. Let $\mathcal{R} \subseteq R \times M$ be the relation in which $(r, m) \in \mathcal{R}$ if and only if $rm = 0$. This defines an antitone Galois connection from 2^R to 2^M.*

a) *Show: let X be the set of ideals of R and let Y be the set of R-submodules of M, both partially ordered under inclusion. Show: the relation restricts to an antitone Galois connection $(\Phi : X \to Y, \Psi : Y \to X)$.*
b) *Show: $\Psi(M) = \operatorname{ann} M$ and for all $m \in M$, $\Psi(\{m\}) = \operatorname{ann} m$.*

A left R-module M is **faithful** if $\operatorname{ann}(M) = 0$. Explicitly, this means that for all $0 \neq r \in R$, there exists $m \in M$ such that $rm \neq 0$.

EXERCISE 3.8. *Let M be an R-module. Show that M has the natural structure of a faithful $R/\operatorname{ann}(M)$-module.*

Definition: Let M be a left R-module. A **submodule** of M is a subgroup N of $(M, +)$ such that $RN \subseteq N$. The following result is extremely easy and all-important:

THEOREM 3.2. *Let R be a ring. The left R-submodules of R are precisely the left ideals of R.*

EXERCISE 3.9. *Prove Theorem 3.2.*

Definition: Let M and N be left R-modules. A **homomorphism** of R-modules is a homomorphism of commutative groups $f : M \to N$ such that for all $r \in R,\ m \in M,\ n \in N,\ f(rm) = rf(m)$.

EXERCISE 3.10.

a) *Define an isomorphism of R-modules in the correct way, i.e.,* not *as a bijective homomorphism of R-modules.*
b) *Show: a homomorphism of R-modules is an isomorphism if and only if it is bijective.*

If N is a submodule of a left R-module M, then the quotient group M/N has a natural R-module structure. More precisely, there is a unique left R-module structure on M/N such that the quotient map $M \to M/N$ is a homomorphism of R-modules.

EXERCISE 3.11. *Let I be a two-sided ideal of the not-necessarily-commutative ring R, so the quotient ring R/I has the structure of a left R-module. Show:*

$$\operatorname{ann}(R/I) = I.$$

In particular, every two-sided ideal of R occurs as the annihilator of a left R-module.

EXERCISE 3.12.

a) *Let R be a ring and $\{M_i\}_{i \in I}$ a family of R-modules. Consider the commutative group $M = \bigoplus_{i \in I} M_i$. Show that putting $r(m_i) = (rm_i)$ makes R into an R-module. Show that the usual inclusion map $\iota_i : M_i \to M$ is a homomorphism of R-modules.*
b) *Show: for any R-module N and R-module maps $f_i : M_i \to N$, there exists a unique R-module map $f : M \to N$ such that $f_i = f \circ \iota_i$ for all $i \in I$. Thus M satisfies the universal mapping property of the direct sum.*

As a matter of notation, for $n \in \mathbb{Z}^+$, $R^n := \bigoplus_{i=1}^n R$, $R^0 = 0$.

EXERCISE 3.13. *Work out the analogue of Exercise 3.12 for direct products.*

EXERCISE 3.14. a) *Suppose M is an R-module and S is a subset of M. Show that the intersection of all R-submodules of M containing S is an R-submodule, and is contained in every R-submodule that contains S. We call it the R-submodule* ***generated*** *by S and denote it by $\langle S \rangle$. If $S = \{x_1, \ldots, x_n\}$ is finite, we usually write $\langle x_1, ..., x_n \rangle$ instead of $\langle \{x_1, \ldots, x_n\} \rangle$.*

b) *If $S = \{s_i\}_{i \in I}$, show that the R-module generated by S is the set of all sums $\sum_{i \in J} r_i s_i$, where J is a finite subset of S.*

An R-module M is **cyclic** (or **monogenic**) if $M = \langle x \rangle$ for some $x \in X$.

EXERCISE 3.15. *Show: for an R-module M, the following are equivalent:*

(i) $M \cong R/\operatorname{ann}(M)$.

(ii) *M is cyclic.*

EXERCISE 3.16. *Suppose k is a field. Show: the terms "k-module" and "vector space over k" are synonymous.*

One can therefore view the theory of R-modules as a generalization of vector spaces to arbitrary rings. But really this is something like a zeroth order approximation of the truth: for a general ring R, the theory of R-modules is incomparably richer than the theory of vector spaces over a field. There are two explanations for this. First, even when working with very simple R-modules such as R^n, the usual linear algebra notions of linear independence, span and basis remain meaningful, but behave in unfamiliar ways:

Call a subset S of an R-module M **linearly independent** if for every finite subset $m_1, \ldots, m_n$ of S and any $r_1, \ldots, r_n \in R$, $r_1 m_1 + \ldots + r_n m_n = 0$ implies $r_1 = \ldots = r_n = 0$. Say that S **spans** R if the R-submodule generated by S is R, and finally a **basis** for an R-module is a subset that is both linearly independent and spanning. For example, for any set I, the R-module $\bigoplus_i R$ has a basis e_i.

In linear algebra – i.e., when R is a field – every R-module has a basis.[1] However the situation is quite different over a general ring:

THEOREM 3.3. a) *Let M be an R-module. Suppose that $S \subseteq R$ is a basis. Then M is isomorphic as an R-module to $\bigoplus_{s \in S} R$.*

b) *Let S be any set, and consider the R-module $R_S := \bigoplus_{s \in S} R$. For each $s \in S$, let $e_s \in \bigoplus_{s \in S} R$ be the element whose s-coordinate is 1 and all of whose other coordinates are 0. Then set $\{e_s\}_{s \in S}$ is a basis for R_S.*

EXERCISE 3.17. *Prove Theorem 3.3.*

A module that has a basis – so, by the theorem, admits an isomorphism to $\bigoplus_{s \in S} R$ for some index set S – is called **free**.

EXERCISE 3.18. *Show: a nonzero free R-module is faithful.*

Let us examine the case of modules over $R = \mathbb{Z}$, i.e., of commutative groups. Here the term **free commutative group** is synonymous with "free $\mathbb{Z}$-module". Needless to say (right?), not all commutative groups are free: for any integer $n > 1$, $\mathbb{Z}/n\mathbb{Z}$

[1]This uses, and is in fact equivalent to, the Axiom of Choice, but the special case that any vector space with a finite spanning set has a basis does not.

is not free, since it has nonzero annihilator $n\mathbb{Z}$. Thus $\mathbb{Z}/n\mathbb{Z}$ does not have a basis as a $\mathbb{Z}$-module, and indeed has no nonempty linearly independent subsets!

PROPOSITION 3.4. *For a commutative ring R, the following are equivalent:*

(i) *Every R-module is free.*
(ii) *The ring R is a field.*

PROOF. As discussed above, (ii) $\implies$ (i) is a fundamental theorem of linear algebra, so we need only concern ourselves with the converse. But if R is not a field, then there exists a nonzero proper ideal I, and then R/I is a nontrivial R-module with $0 \neq I = \mathrm{ann}(R/I)$, so by Exercise 3.18 R/I is not free. □

Remark: If R is a not-necessarily-commutative ring such that every left R-module is free, then the above argument shows R has no nonzero proper twosided ideals, so is what is called a **simple ring**. But a noncommutative simple ring may still admit a nonfree module. For instance, let k be a field and take $R = M_2(k)$, the 2×2 matrix ring over k. Then $k \oplus k$ is a left R-module that is not free. However, suppose R is a ring with no proper nontrivial one-sided ideals. Then R is a division ring – i.e., every nonzero element of R is a unit – and every R-module is free.

In linear algebra – i.e., when R is a field – every linearly independent subset of an R-module can be extended to a basis. Over a general ring this does not hold even for free R-modules. For instance, take $R = M = \mathbb{Z}$. A moment's thought reveals that the only two bases are $\{1\}$ and $\{-1\}$, whereas the linearly independent sets are precisely the singleton sets $\{n\}$ as n ranges over the nonzero integers.

Note well the form of Proposition 3.4: we assume that R is a commutative ring for which R-modules satisfy some nice property, and we deduce a result on the structure of R. Such "inverse problems" have a broad appeal throughout mathematics and provide one of the major motivations for studying modules above and beyond their linear algebraic origins. We will see other such characterizations later on.

2. Finitely presented modules

One of the major differences between commutative groups and noncommutative groups is that a subgroup N of a finitely generated commutative group M remains finitely generated, and indeed, the minimal number of generators of the subgroup N cannot exceed the minimal number of generators of M, whereas this is not true for nonabelian groups: e.g. the free group of rank 2 has as subgroups free groups of every rank $0 \leqslant r \leqslant \aleph_0$. (For instance, the commutator subgroup is not finitely generated.)

Since a commutative group is a $\mathbb{Z}$-module and every R-module has an underlying commutative group structure, one might well expect the situation for R-modules to be similar to that of commutative groups. We will see later that this is true in many but not all cases: an R-module is called **Noetherian** if all of its submodules are finitely generated. Certainly a Noetherian module is itself finitely generated. The basic fact here – which we will prove in §8.7 – is a partial converse: if the ring R is Noetherian, any finitely generated R-module is Noetherian. We can already see that the Noetherianity of R is necessary: if R is not Noetherian, then by definition there exists an ideal I of R that is not finitely generated, and this is nothing else

than a non-finitely generated R-submodule of R (that is itself generated by the single element 1.) Thus the aforementioned fact about subgroups of finitely generated commutative groups being finitely generated holds because $\mathbb{Z}$ is a Noetherian ring.

When R is not Noetherian, it becomes necessary to impose stronger conditions than finite generation on modules. One such condition indeed comes from group theory: recall that a group G is **finitely presented** if it is isomorphic to the quotient of a finitely generated free group F by the least normal subgroup N generated by a finite subset $x_1, \ldots, x_m$ of F.

PROPOSITION 3.5. *For a finitely generated R-module M, the following are equivalent:*

(i) *There are non-negative integers m, n and an exact sequence*
$$R^m \to R^n \to M \to 0.$$
(ii) *M is the quotient of a finitely generated free R-module by a finitely generated submodule.*

*A module M satisfying these equivalent conditions is said to be **finitely presented**.*

PROOF. (i) $\implies$ (ii) is immediate. Conversely, let $M = R^n/N$ where N is finitely generated. Then there exists a surjection $R^m \to N$ and thus the sequence
$$R^m \to R^n \to M \to 0$$
is exact. □

PROPOSITION 3.6. *Let*
$$0 \to K \xrightarrow{\psi} N \xrightarrow{\phi} M \to 0$$
be a short exact sequence of R-modules, with M finitely presented and N finitely generated. Then K is finitely generated.

PROOF. (Matsumura) By definition of finitely presented, we can place M in an exact sequence
$$R^m \to R^n \xrightarrow{f} M \to 0 \tag{5}$$
for some $m, n \in \mathbb{N}$. For $1 \leqslant i \leqslant n$, let e_i be the ith standard basis element of M, let $m_i = f(e_i)$ be the image in M, and choose $n_i \in N$ any element in $\phi^{-1}(m_i)$. Then there is a unique R-module homomorphism $\alpha : R^n \to N$ given by $\alpha(e_i) = n_i$, that restricts to an R-module homomorphism $\beta : B^m \to K$. Altogether we get a commutative diagram
$$R^m \longrightarrow R^n \xrightarrow{f} M \longrightarrow 0$$
$$0 \longrightarrow K \xrightarrow{\psi} N \xrightarrow{\phi} M.$$
The rest of the proof is essentially a diagram chase. Suppose $N = \langle \xi_1, \ldots, \xi_k \rangle_R$, and choose $v_1, \ldots, v_k \in R^n$ such that $\phi(\xi_i) = f(v_i)$. Put
$$\xi_i' = \xi_i - \alpha(v_i).$$
Then $\varphi(\xi_i') = 0$, so there exist unique $\eta_i \in K$ such that
$$\xi_i' = \psi(\eta_i).$$

We CLAIM that K is generated as an R-module by $\beta(R^m)$ and $\eta_1, \ldots, \eta_k$ and thus is finitely generated. Indeed, for $\eta \in K$, there are $r_1, \ldots, r_k \in R$ such that

$$\psi(\eta) = \sum_i r_i \xi_i.$$

Then

$$\psi(\eta - \sum_i r_i \eta_i) = \sum_i r_i(\xi_i - \xi_i') = \alpha(\sum_i r_i v_i).$$

Since

$$0 = \phi(\alpha(\sum_i r_i v_i)) = f(\sum_i r_i v_i),$$

we may write $\sum_i r_i v_i = g(u)$ with $u \in R^m$. Then

$$\psi(\beta(u)) = \alpha(g(u)) = \alpha(\sum_i r_i v_i) = \psi(\eta - \sum_i r_i \eta_i).$$

Since ψ is injective, we conclude

$$\eta = \beta(u) + \sum_i r_i \eta_i. \qquad \square$$

EXERCISE 3.19. *Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules.*

a) *Show: if M' and M'' are both finitely presented, so is M.*
b) *Show: if M is finitely presented and M' is finitely generated, then M'' is finitely presented.*

A stronger condition still is the following: an R-module M is **coherent** if it is finitely generated and every finitely generated submodule is finitely presented. Evidently coherent implies finitely presented implies finitely generated, and all three coincide over a Noetherian ring. The significance of coherence lies in the following:

THEOREM 3.7. *Let R be a not-necessarily-commutative ring.*

a) *The category of all left R-modules is an abelian category.*
b) *The category of all coherent left R-modules is an abelian category.*
c) *In particular, if R is left Noetherian, the category of all finitely generated left R-modules is an abelian category.*
d) *There exists a commutative ring R for which the category of all finitely generated (left) R-modules is **not** abelian.*

We will make absolutely no future use of this result, so we omit the proof here: the reader may consult e.g. `https://stacks.math.columbia.edu/tag/0AZ5`. Nevertheless we hope that it will be of some use to students of algebraic geometry: for instance, it explains why in some algebraic geometry texts coherent sheaves of $\mathcal{O}_X$-modules on a scheme X are defined only for Noetherian schemes.

3. Torsion and torsionfree modules

Let R be a domain, and let M be an R-module. An element $x \in M$ is said to be **torsion** if there exists $0 \neq a \in R$ such that $ax = 0$. Equivalently, the annihilator $\operatorname{ann}(x) = \{a \in R \mid ax = 0\}$ is a nonzero ideal of R. We define $M[\text{tors}]$ to be the set of all torsion elements of M. It is immediate to see that $M[\text{tors}]$ is a submodule of M. We say that M is a **torsion** R-module if $M = M[\text{tors}]$ and that M is **torsionfree** if $M[\text{tors}] = 0$.

EXERCISE 3.20. *Let $0 \to M_1 \to M \to M_2 \to 0$ be an exact sequence.*

a) *Show that if M is torsion, so are M_1 and M_2.*
b) *If M_1 and M_2 are torsion modules, must M be torsion?*
c) *Show that if M is torsionfree, show that so is M_1, but M_2 need not be.*
d) *If M_1 and M_2 are torsionfree, must M be torsionfree?*

PROPOSITION 3.8. *Let R be a domain and M an R-module.*

a) *The quotient $M/M[\text{tors}]$ is torsionfree.*
b) *If M is finitely generated, the following are equivalent:*
   (i) *M embeds in a finitely generated free R-module.*
   (ii) *M is torsionfree.*

PROOF. a) Put $N = M/M[\text{tors}]$, and let $\overline{x} \in N$ be such that there exists $0 \neq a \in R$ with $a\overline{x} = 0$. Let x be any lift of $\overline{x}$ to M; then there exists $t \in M[\text{tors}]$ such that $ax = t$. By definition of torsion, there exists $a' \in R$ such that $a't = 0$, so $a'ax = a't = 0$. Since R is a domain, $a'a$ is nonzero, so $x \in M[\text{tors}]$ and $\overline{x} = 0$.
b) (i) $\implies$ (ii) is very easy: free modules are torsionfree and submodules of torsionfree modules are torsionfree.
(ii) $\implies$ (i): We may assume $M \neq 0$. Let $M = \langle x_1, \ldots, x_r \rangle$ with $r \geqslant 1$ and all the x_i are nonzero. Further, after reordering the x_i's if necessary, there exists a unique s, $1 \leqslant s \leqslant r$, such that $\{x_1, \ldots, x_s\}$ is linearly independent over R but for all i with $s < i \leqslant r$, $\{x_1, \ldots x_s, x_i\}$ is linearly dependent over R. Then $F = \langle x_1, \ldots, x_s \rangle \cong R^s$, so we are done if $s = r$. If $s < r$, then for each $i > s$ there exists $0 \neq a_i \in R$ such that $a_i x_i \in F$. Put $a = \prod_{s<i\leqslant r} a_i$: then $aM \subseteq F$. Let $[a] : M \to M$ denote multiplication by a. Since M is torsionfree, $[a]$ is injective hence gives an R-module isomorphism from M to a submodule of the finitely generated free module F. □

EXERCISE 3.21. *Show: the torsionfree $\mathbb{Z}$-module $(\mathbb{Q}, +)$ is not isomorphic to a submodule of any finitely generated free $\mathbb{Z}$-module.*
(Thus – even for very nice rings! – the hypothesis of finite generation is necessary in Proposition 3.8.)

4. Tensor and Hom

4.1. Tensor products.

We assume that the reader has some prior familiarity with tensor products, say of vector spaces and/or of abelian groups. The first is an instance of tensor products of k-modules, for some field k, and the second is an instance of tensor products of $\mathbb{Z}$-modules. We want to give a general definition of $M \otimes_R N$, where M and N are two R-modules.

There are two ways to view the tensor product construction: as a solution to a universal mapping problem, and as a generators and relations construction. They are quite complementary, so it is a matter of taste as to which one takes as "the" definition. So we will follow our taste by introducing the mapping problem first:

Suppose M, N, P are R-modules. By an R-**bilinear** map $f : M \times N \to P$ we mean a function that is separately R-linear in each variable: for all $m \in M$, the mapping $n \mapsto f(m, n)$ is R-linear, and for each $n \in N$, the mapping $m \mapsto f(m, n)$ is

R-linear. Now consider all pairs (T, ι), where T is an R-module and $\iota : M \times N \to T$ is an R-bilinear map. A morphism from (T, ι) to (T', ι') will be an R-module homomorphism $h : T \to T'$ such that $\iota' = h \circ \iota$. By definition, a tensor product $M \otimes_R N$ is an initial object in this category: i.e., it comes equipped with an R-bilinear map $M \times N \to M \otimes_R N$ such that any R-bilinear map $f : M \times N \to P$ factors through it. As usual, the initial object of a category is unique up to unique isomorphism provided it exists.

As for the existence, we fall back on the generators and relations construction. Namely, we begin with the free R-module F whose basis is $M \times N$, and we write the basis elements (purely formally) as $m \otimes n$. We then take the quotient by the submodule generated by the following relations R:

$$(x + x') \otimes y - x \otimes y - x' \otimes y,$$

$$x \otimes (y + y') - x \otimes y - x \otimes y',$$

$$(ax) \otimes y - a(x \otimes y),$$

$$x \otimes (ay) - a(x \otimes y).$$

It is then easy to see that the quotient map $M \times N \to F/N$ satisfies all the properties of a tensor product (details left to the reader).

Note that the general element of $M \otimes_R N$ is not a single element of the form $x \otimes y$ but rather a finite sum of such elements. (Indeed, from the free R-module, every element can be represented by a finite R-linear combination of elements of the form $x \otimes y$, but the last two defining relations in the tensor product allow us to change $r_i(x \otimes y)$ to either $(r_i x) \otimes y$ or $x \otimes (r_i y)$.) Of course, this representation of an element of the tensor product need not be (and will never be, except in trivial cases) unique.

One can also take the tensor product of R-algebras: if R is a (commutative!) ring and A and B are commutative R-algebras, then on the tensor product $A \otimes_R B$ we have a naturally defined product, induced by $(a_1 \otimes b_1) \cdot (a_2 \otimes b_2) \coloneqq (a_1 a_2 \otimes b_1 b_2)$. We have to check that this is well-defined, a task that we leave to the reader (or see [**AM**, pp. 30-31])). The tensor product of algebras is a powerful tool – e.g. in the structure theory of finite-dimensional algebras over a field, or in the theory of linear disjointness of field extensions – and is given misleadingly short shrift in most elementary treatments.

Base change: Suppose that M is an R-module and $f : R \to S$ is a ring homomorphism. Then S is in particular an R-module, so that we can form the tensor product $S \otimes_R M$. This is still an R-module, but it is also an S-module in an evident way: $s \bullet (\sum_i s_i \otimes m_i) \coloneqq \sum_i s s_i \otimes m_i$. This is process is variously called **scalar extension**, **base extension** or **base change**. Note that this process is functorial, in the following sense: if $f : M \to M'$ is an R-algebra homomorphism, then there exists an induced S-algebra homomorphism $S \otimes_R M \to S \otimes_R M'$, given by $s \otimes m \mapsto s \otimes f(m)$.

EXERCISE 3.22. *If M is a finitely generated R-module and $f : R \to S$ is a ring homomorphism, then $S \otimes_R M$ is a finitely generated S-module.*

EXERCISE 3.23. *Let A and B be rings, M an A-module, P a B-module, and N an (A,B)-bimodule. Then $M \otimes_A N$ is naturally a B-module, $N \otimes_B P$ is naturally an A-module, and*

$$(M \otimes_A N) \otimes_B P \cong M \otimes_A (N \otimes_B P).$$

EXERCISE 3.24. *Let R be a commutative ring, I an ideal of R and M an R-module.*

a) *Show: there is a well-defined R-bilinear map $R/I \times M \to M/IM$ given by $(r+I, m) \mapsto rm + I$. Thus there is an induced homomorphism of R-modules*

$$\varphi : R/I \otimes_R M \to M/IM.$$

b) *Show: φ is an isomorphism of R-modules.*

PROPOSITION 3.9. *Let R be a commutative ring, M an R-module and $\{N_i\}_{i\in I}$ a directed system of R-modules. Then the R-modules $\varinjlim(M \otimes N_i)$ and $M \otimes (\varinjlim N_i)$ are canonically isomorphic.*

EXERCISE 3.25. *Prove Proposition 3.24.*

EXERCISE 3.26. *Let M and N be R-modules.*

a) *Show* $\operatorname{ann} M \otimes N \supset \operatorname{ann} M + \operatorname{ann} N$.

b) *Suppose M and N are cyclic R-modules. Show: $M \otimes N$ is cyclic and* $\operatorname{ann}(M \otimes N) = \operatorname{ann} M + \operatorname{ann} N$. *Equivalently, show that for all ideals I, J of R we have*

$$R/I \otimes R/J = R/(I+J).$$

c) *Deduce: for all $m, n \in \mathbb{Z}$ we have*

$$\mathbb{Z}/m\mathbb{Z} \otimes \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\langle m, n\rangle\mathbb{Z}.$$

d) *Let*[2] *k be a field, let $R := k[t^2, t^3]$, $M := k[t]$, $I = t^2R$, $N := R/I$. Show:*

$$t^3 \in \operatorname{ann}(M/IM) \setminus \operatorname{ann} M + I = I$$

and thus

$$\operatorname{ann}(M \otimes N) \supsetneq \operatorname{ann} M + \operatorname{ann} N.$$

5. Projective modules

5.1. Basic equivalences.

PROPOSITION 3.10. *For an R-module P, the following are equivalent:*

(i) *There exists an R-module Q such that $P \oplus Q$ is a free R-module.*

(ii) *If $\pi : M \to N$ is a surjective R-module homomorphism and $\varphi : P \to N$ is a homomorphism, then there exists at least one R-module homomorphism $\Phi : P \to M$ such that $\varphi = \pi \circ \Phi$.*

(iii) *If $\pi : M \to N$ is a surjection, then the natural map* $\operatorname{Hom}(P, M) \to \operatorname{Hom}(P, N)$ *given by $\Phi \mapsto \pi \circ \Phi$ is surjective.*

(iv) *The functor* $\operatorname{Hom}(P, \ )$ *is exact.*

[2]This is taken from `https://math.stackexchange.com/questions/79538/`.

(v) *Every short exact sequence of R-modules*

$$0 \to N \to M \xrightarrow{q} P \to 0$$

splits: there exists an R-module map $\sigma : P \to M$ such that $q \circ \sigma = 1_P$ and thus an internal direct sum decomposition $M = N \oplus \sigma(P)$.

A module satisfying these equivalent conditions is called ***projective****.*

PROOF. (i) $\implies$ (ii): Let $F \cong P \oplus Q$ be a free module. Let $\{f_i\}$ be a free basis for F and let $\{p_i\}$ be the corresponding generating set for P, where p_i is the image of f_i under the natural projection $P \oplus Q \to P$. Put $n_i = \varphi(p_i)$. By surjectivity of π, let $m_i \in \pi^{-1}(n_i)$. By the freeness of F, there is a unique R-module homomorphism $h : F \to M$ carrying each f_i to m_i. Pull h back to P via the natural inclusion $P \hookrightarrow F$. Then $h : P \to M$ is such that $\pi \circ f = \varphi$.
(ii) $\implies$ (i): As for any R-module, there exists a free R-module F and a surjection $\pi : F \to P$. Applying (ii) with $N = p$ and $\varphi : P \to N$ the identity map, we get a homomorphism $\Phi : P \to F$ such that $\pi \circ \varphi = 1_P$. It follows that $F = \Phi(P) \oplus \ker(\pi)$ is an internal direct sum decomposition.
(ii) $\iff$ (iii): (iii) is nothing more than a restatement of (ii), as we leave it to the reader to check.
(iii) $\iff$ (iv): To spell out (iv), it says: if

$$0 \to M' \to M \to M'' \to 0$$

is a short exact sequence of R-modules, then the corresponding sequence

$$0 \to \mathrm{Hom}(P, M') \to \mathrm{Hom}(P, M) \to \mathrm{Hom}(P, M'') \to 0$$

is exact. Now for any R-module P, the sequence

$$0 \to \mathrm{Hom}(P, M') \to \mathrm{Hom}(P, M) \to \mathrm{Hom}(P, M'')$$

is exact – i.e., $\mathrm{Hom}(P, \ )$ is left exact – so (iv) amounts to: for any surjection $M \to M''$, the corresponding map $\mathrm{Hom}(P, M) \to \mathrm{Hom}(P, M'')$ is surjective, and this is condition (iii).
(ii) $\implies$ (v): Given

$$0 \to N \to M \to P \xrightarrow{q} 0,$$

we apply (ii) to the identity map $1_P : P \to P$ and the surjection $q : M \to P$, getting a map $\sigma : P \to M$ such that $q \circ \sigma = 1_P$, so σ is a section as required.
(v) $\implies$ (i): Choosing a set of generators for P gives rise to a surjective homomorphism $q : F \to P$ from a free R-module F to P and thus a short exact sequence

$$0 \to \mathrm{Ker}\, q \to F \xrightarrow{q} P \to 0.$$

By hypothesis, there exists a section $\sigma : P \to F$ and thus an internal direct sum decomposition $F \cong \mathrm{Ker}(q) \oplus \sigma(P) \cong \mathrm{Ker}(q) \oplus P$. □

EXERCISE 3.27. *Give a direct proof that (v) $\implies$ (ii) in Proposition 3.10. (Suggestion: Given the surjection $q : M \to N$ and the map $\pi : P \to N$, form the short exact sequence $0 \to K \to M \to N \to 0$ and show that it is mapped to by a short exact sequence $0 \to K \to M \times_N P \to P \to 0$, where*

$$M \times_N P = \{(x, y) \in M \times P \mid q(x) = \pi(y)\}$$

is the ***fiber product*** *of M and P over N.)*

EXERCISE 3.28. *Use Proposition 3.10 to show, several times over, that a free R-module is projective.*

EXERCISE 3.29. *Let $\{M_i\}_{i\in I}$ be an index family of R-modules. Show that the direct sum $M = \bigoplus_{i\in I} M_i$ is projective if and only if each M_i is projective.*

EXERCISE 3.30. a) *Show: the tensor product of two free R-modules is free.*

b) *Show: the tensor product of two projective R-modules is projective.*

EXERCISE 3.31. *Show: a finitely generated projective module is finitely presented. (Hint: the problem is that over a not-necessarily-Noetherian ring, a submodule of a finitely generated module need not be finitely generated. However, a* direct summand *of a finitely generated module is always finitely generated: why?)*

5.2. Linear algebraic characterization of projective modules.

Let R be a commutative ring, $n \in \mathbb{Z}^+$, and let P be an element of the (non-commutative!) ring $M_n(R)$ of $n \times n$ matrices with entries in R such that $P^2 = P$. There are several names for such a matrix. The pure algebraist would call such a matrix **idempotent**, for that is the name of an element in any ring that is equal to its square. A geometrically minded algebraist however may call such a matrix a **projection**, the idea being that the corresponding R-module endomorphism of R^n "projects" R^n onto the submodule $P(R^n)$.

PROPOSITION 3.11. *An R-module M is finitely generated and projective if and only if it is, up to isomorphism, the image of a projection: i.e., if and only if there exists $n \in \mathbb{Z}^+$ and a matrix $P \in M_n(R)$ with $P = P^2$ such that $M \cong P(R^n)$.*

PROOF. Suppose first that M is a finitely generated projective R-module. Since M is finitely generated,, there exists $n \in \mathbb{Z}^+$ and a surjective R-module homorphism $\pi : R^n \to M$. Since M is projective, this homomorphism has a section $\sigma : M \to R^n$, and we may thus write $R^n = \sigma(M) \oplus M'$. Put $P = \sigma \circ \pi \in \mathrm{End}_R(R^n)$. Then $P(R^n) = \sigma(\pi(R^n)) = \sigma(M) \cong M$ and

$$P^2 = \sigma \circ (\pi \circ \sigma) \circ \pi = \sigma \circ 1_M \circ \pi = \sigma \circ \pi = P.$$

Conversely, suppose that there exists $P \in \mathrm{End}_R(R^n)$ with $P^2 = P$ and let $M \cong P(R^n)$. Then – since $P(1-P) = 0$ – $R^n = P(R^n) \oplus (1-P)(R^n)$, exhibiting $P(R^n)$ as a direct summand of a free module.[3] □

5.3. The Dual Basis Lemma.

PROPOSITION 3.12. *(Dual Basis Lemma) For an R-module M, the following are equivalent:*

(i) *There is an index set I, elements $\{a_i\}_{i\in I}$ of M and homomorphisms $\{f_i : M \to R\}_{i\in I}$ such that for each $a \in M$, $\{i \in I \mid f_i(a) \neq 0\}$ is finite, and*

$$a = \sum_{i\in I} f_i(a) a_i.$$

(ii) *M is projective.*

[3]This part of the proof redeems the pure algebraist: this the decomposition afforded by the pair of orthogonal idempotents $P, 1-P$.

PROOF. (i) $\implies$ (ii): Let F be the free R-module with basis elements $\{e_i\}_{i\in I}$, and define $f : F \to M$ by $f(e_i) = a_i$. Then the map $\iota : M \to F$ given by $\iota(a) = \sum_{i\in I} f_i(a)e_i$ is a section of f, so M is a direct summand of F.
(ii) $\implies$ (i): Let $f : F = \bigoplus_{i\in I} R \to M$ be an epimorphism from a free R-module onto M. Since M is projective, there exists a section $\iota : M \hookrightarrow F$. If $\{e_i\}_{i\in I}$ is the standard basis of F, then for all $a \in M$, the expression

$$\iota(a) = \sum_{i\in I} f_i(a)e_i$$

defines the necessary family of functions $f_i : M \to R$. □

EXERCISE 3.32. *Let P be a projective R-module. Show: one can can find a* finite *index set I satisfying condition (i) of the Dual Basis Lemma if and only if P is finitely generated.*

EXERCISE 3.33. *Let P be a finitely generated projective R-module, so that by Exercise 3.32 there are $a_1, \ldots, a_n \in P$ and $f_1, \ldots, f_n \in P^\vee$ such that for all $a \in P$ we have $a = \sum_{i=1}^n f_i(a)a_i$. Show: $\langle f_1, \ldots, f_n\rangle = P^\vee$.*

EXERCISE 3.34. *For any R-module M we have a natural map*

$$\iota_M : M \to M^{\vee\vee}, (x, f) \in M \times M^\vee \mapsto f(x) \in R.$$

*We say that M is **torsionless** if ι_M is an injection and that M is **reflexive** if ι_M is an isomorphism.*

a) *Show: a projective module is torsionless.*
b) *Show: a submodule of a torsionless module is torsionless.*
c) *Show: a finitely generated free module is reflexive.*
d) *Show: a finitely generated projective module is reflexive.*

5.4. Projective versus free.

Having established some basic facts about projective modules, we should now seek examples in nature: which modules are projective? By Exercise 3.28 any free module is projective. But this surely counts as a not very interesting example! Indeed the following turns out to be one of the deepest questions of the subject.

QUESTION 1. *When is a projective module free?*

We want to give examples to show that the answer to Question 1 is *not* "always". But even by giving examples one wades into somewhat deep waters. The following is the one truly "easy" example of a non-free projective module I know.

Example: Suppose R_1 and R_2 are nontrivial rings. Then the product $R = R_1 \times R_2$ admits nonfree projective modules. Indeed, let P be the ideal $R_1 \times \{0\}$ and Q the ideal $\{0\} \times R_2$. Since $R = P \oplus Q$, P and Q are projective. On the other hand P cannot be free because taking $e := (0, 1) \in R$, we have $eP = 0$, whereas $eF \neq 0$ for any nonzero free R-module F (and of course, Q is not free either for similar reasons).

Question 1 may be construed in various ways. One way is to ask for the class of rings over which every projective module is free, or over which every finitely generated projective module is free. I actually do not myself know a complete answer to this question, but there are many interesting and important special cases.

Recall the following result from undergraduate algebra.

THEOREM 3.13. *A finitely generated module over a PID is free if and only if it is torsionfree.*

(We will deduce this result as a consequence of other module-theoretic facts in Corollary 3.64.) Of course submodules of torsionfree modules are torsionfree, so projective implies torsionfree. We deduce:

COROLLARY 3.14. *A finitely generated projective module over a PID is free.*

Theorem 3.13 does not extend to all torsionfree modules: for instance, the $\mathbb{Z}$-module $\mathbb{Q}$ is torsionfree but not free. However Corollary 3.14 *does* extend to all modules over a PID. The proof requires transfinite methods and is given in §3.10.

Recall that a ring R is local if it has a unique maximal ideal. It is convenient to reserve the notation $\mathfrak{m}$ for the unique maximal ideal of a local ring and speak of "the local ring $(R, \mathfrak{m})$". We want to show that every finitely generated projective module over a local ring is free. First a few preliminaries.

Let $f : R \to S$ be a homomorphism of rings. Then necessarily f induces a homomorphism $f^\times : R^\times \to S^\times$ on unit groups: if $xy = 1$, then $f(x)f(y) = f(1) = 1$, so units get mapped to units. But what about the converse: if $x \in R$ is such that $f(x)$ is a unit in S, must x be a unit in R?

It's a nice idea, but it's easy to see that this need not be the case. For instance, let $a > 1$ be any positive integer. Then a is not a unit of $\mathbb{Z}$, but for each prime $p > a$, the image of a in the quotient ring $\mathbb{Z}/p\mathbb{Z}$ is a unit. Too bad! Let us not give up so soon: a conjecture may fail, but a definition cannot: say a homomorphism $f : R \to S$ of rings is **unit-faithful** if for all $x \in R$, $f(x) \in S^\times \implies x \in R^\times$.

LEMMA 3.15. *If $(R, \mathfrak{m})$ is a local ring, the quotient map $q : R \to R/\mathfrak{m}$ is unit-faithful.*

PROOF. An element of any ring is a unit if and only if it is contained in no maximal ideal, so in a local ring we have $R^\times = R \backslash \mathfrak{m}$. Moreover, since $\mathfrak{m}$ is maximal, $R/\mathfrak{m}$ is a field. Thus, for $x \in R$,

$$q(x) \in (R/\mathfrak{m})^\times \iff x \notin \mathfrak{m} \iff x \in R^\times. \qquad \square$$

Later we will see a generalization: if J is any ideal contained the *Jacobson radical* of R, then $q : R \to R/J$ is unit-faithful.

THEOREM 3.16. *A finitely generated projective module over a local ring is free.*

PROOF. Let P be a finitely generated projective module over the local ring $(R, \mathfrak{m})$. We may find Q and $n \in \mathbb{Z}^+$ such that $P \oplus Q = R^n$. Now tensor with $R/\mathfrak{m}$: we get a direct sum decomposition $P/\mathfrak{m}P \oplus Q/\mathfrak{m}Q = (R/\mathfrak{m})^n$. Since $R/\mathfrak{m}$ is a field, all $R/\mathfrak{m}$-modules are free. Choose bases $\{\overline{p_i}\}$ for $P/\mathfrak{m}P$ and $\{\overline{q_j}\}$ for $Q/\mathfrak{m}Q$, and for all i, j, lift each $\overline{p_i}$ to an element p_i of P and each $\overline{q_j}$ to an element q_j of Q. Consider the $n \times n$ matrix A with coefficients in R whose columns are $p_1, \ldots, p_a, q_1, \ldots, q_b$. The reduction modulo $\mathfrak{m}$ of A is a matrix over the field $R/\mathfrak{m}$ whose columns form a basis for $(R/\mathfrak{m})^n$, so its determinant is a unit in $(R/\mathfrak{m})^\times$. Since $\det(M \pmod{\mathfrak{m}}) = \det(M) \pmod{\mathfrak{m}}$, Lemma 3.15 implies that $\det(M) \in R^\times$, i.e., M is invertible.

But this means that its columns are linearly independent. By a consequence of Nakayama's Lemma (Corollary 3.44) we have that $p_1, \ldots, p_a$ spans P, so in fact it forms a basis for P. □

Once again, in Section 3.9 this result will be improved upon: it is a celebrated theorem of Kaplansky that *any* projective module over a local ring is free.

Much more interesting is an example of a finitely generated projective, nonfree module over a domain. Probably the first such examples come from nonprincipal ideals in rings of integers of number fields with class number greater than 1. To give such an example with proof of its projectivity this early in the day, we require a little preparation.[4]

Two ideals I and J in a ring R are **comaximal** if $I + J = R$. More generally, a family $\{I_i\}$ of ideals in a ring is **pairwise comaximal** if for all $i \neq j$, $I + J = R$.

LEMMA 3.17. *Let I, J, $K_1, \ldots, K_n$ be ideals in the ring R.*

a) *We have $(I + J)(I \cap J) \subseteq IJ$.*
b) *If I and J are comaximal, $IJ = I \cap J$.*
c) *If $I + K_i = R$ for all $1 \leqslant i \leqslant n$, then $I + K_1 \cdots K_n = R$.*

PROOF. a) $(I + J)(I \cap J) = I(I \cap J) + J(I \cap J) \subseteq IJ + IJ = IJ$.
b) If $I + J = R$, the identity of part a) becomes $I \cap J \subseteq IJ$. Since the converse inclusion is valid for all I and J, the conclusion follows. c) We go by induction on n, the case $n = 1$ being trivial. If $n = 2$, then for $i = 1, 2$, let $a_i \in I$ and $b_i \in K_i$ be such that $1 = a_i + b_i$. Then

$$1 = a_1 + a_2 - a_1 a_2 + b_1 b_2 \in I + K_1 K_2.$$

Now assume $n \geqslant 3$ and that the result holds for $n - 1$. By induction,

$$I + K_1 \cdots K_{n-1} = R.$$

and by hypothesis $I + K_n = R$, so by the $n = 2$ case we have

$$I + K_1 \cdots K_n = R.$$ □

PROPOSITION 3.18. *Let I and J be comaximal ideals in a domain R, and consider the R-module map $q : I \oplus J \to R$ given by $(x, y) \mapsto x + y$. Then:*

a) *The map q is surjective.*
b) *We have $\mathrm{Ker}(q) = \{(x, -x) \mid x \in I \cap J\}$, hence is isomorphic as an R-module to $I \cap J$.*
c) *We have an isomorphism of R-modules*

$$I \oplus J \cong IJ \oplus R.$$

d) *Thus if IJ is a principal ideal, I and J are projective modules.*

PROOF. It is clear that for any ideals I and J, the image of the map q is the ideal $I + J$, and we are assuming $I + J = R$, whence part a).
Part b) is essentially immediate: details are left to the reader.
Combining parts a) and b) we get a short exact sequence

$$0 \to I \cap J \to I \oplus J \to R \to 0.$$

[4]Here we wish to acknowledge our indebtedness to K. Conrad: we took our inspiration for Proposition 3.18 and the following Exercise from Example 3.1 of http://www.math.uconn.edu/∼kconrad/blurbs/linmultialg/splittingmodules.pdf.

But R is free, hence projective, and thus the sequence splits, giving part c). Finally, a nonzero principal ideal (x) in a domain R is isomorphic as an R-module to R itself: indeed, multiplication by x gives the isomorphism $R \to (x)$. So if IJ is principal, $I \oplus J \cong R^2$ and I and J are both direct summands of a free module. □

In particular, if we can find in a domain R two comaximal nonprincipal ideals I and J with IJ principal, then I and J are finitely generated projective nonfree R-modules. The following exercise asks you to work through an example.

EXERCISE 3.35. *Let $R = \mathbb{Z}[\sqrt{-5}]$, and put*

$$\mathfrak{p}_1 = \langle 3, 1 + \sqrt{-5} \rangle, \ \mathfrak{p}_2 = \langle 3, 1 - \sqrt{-5} \rangle.$$

a) *Show that $R/\mathfrak{p}_1 \cong R/\mathfrak{p}_2 \cong \mathbb{Z}/3\mathbb{Z}$, so $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are maximal ideals of R.*
b) *Show that $\mathfrak{p}_1 + \mathfrak{p}_2 = R$ (or equivalently, that $\mathfrak{p}_1 \neq \mathfrak{p}_2$).*
c) *Show that $\mathfrak{p}_1\mathfrak{p}_2 = (3)$.*
d) *Show that neither $\mathfrak{p}_1$ nor $\mathfrak{p}_2$ is principal.*
(Suggestion: show that if $\mathfrak{p}_1 = (x + \sqrt{-5}y)$ then $\mathfrak{p}_2 = (x - \sqrt{-5}y)$ and thus there are integers x, y such that $x^2 + 5y^2 = \pm 3$.)
e) *Conclude that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are (in fact isomorphic) nonfree finitely generated projective modules over the domain R.*
f) *Show that $\mathfrak{p}^2$ is principal, and thus that the class of $\mathfrak{p}$ in $\widetilde{K_0(R)}$ is 2-torsion.*

This construction looks very specific, and the number-theoretically inclined reader is warmly invited to play around with other quadratic rings and more general rings of integers of number fields to try to figure out what is really going on. From our perspective, we will (much later on) gain a deeper understanding of this in terms of the concepts of invertible ideals, the Picard group and Dedekind domains.

EXAMPLE 3.19. *Let X be a compact space, and let $C(X)$ be the ring of continuous real-valued functions on X. The basic structure of these rings is studied in §5.2. Let $E \to X$ be a real topological vector bundle over X. Then the group $\Gamma(E)$ of global sections is naturally a module over $C(X)$. In fact it is a finitely generated projective module, and all finitely generated projective $C(X)$-modules arise faithfully in this way: the global section functor gives a categorical equivalence between vector bundles on X and finitely generated projective modules over $C(X)$. This is a celebrated theorem of R.G. Swan, and Chapter 6 is devoted to giving a self-contained discussion of it, starting from the definition of a vector bundle. In particular, via Swan's Theorem basic results on the tangent bundles of compact manifolds translate into examples of finitely generated projective modules: for instance, an Euler characteristic argument shows that the tangent bundle of any even-dimensional sphere S^{2k} is nontrivial, and thus $\Gamma(TS^{2k})$ is a finitely generated nonfree $C(S^{2k})$-module! Following Swan, we will show that examples of nonfree projective modules over more traditional rings like finitely generated $\mathbb{R}$-algebras follow from examples like these.*

EXAMPLE 3.20. *Let k be a field and $R = k[t_1, \ldots, t_n]$ be the polynomial ring over k in n indeterminates. When $n = 1$, R is a PID, so indeed every finitely generated R-module is projective. For $n > 1$, the situation is much less clear, but the problem of freeness of finitely generated projective R-modules can be stated geometrically as follows: is any algebraic vector bundle on affine n-space $\mathbb{A}^n_{/k}$ algebraically*

trivial? When $k = \mathbb{C}$, the space $\mathbb{A}^n_{/\mathbb{C}} = \mathbb{C}^n$ in its usual, Euclidean topology is contractible, which by basic topology implies that any continuous $\mathbb{C}$-vector bundle on $\mathbb{A}^n$ is (continuously) trivial. Moreover, relatively classical complex variable theory shows that any holomorphic *vector bundle on $\mathbb{A}^n$ is (holomorphically) trivial. But asking the transition functions and the trivialization to be algebraic – i.e., polynomial functions – is a much more stringent problem. In his landmark 1955 paper FAC, J.-P. Serre noted that this natural problem remained open for algebraic vector bundles: he was able to prove only the weaker result that a finitely generated projective R-module M is* ***stably free*** *– i.e., there exists a finitely generated free module F such that $M \oplus F$ is free. This became known as* ***Serre's Conjecture*** *(to his dismay) and was finally resolved independently in 1976 by D. Quillen* [**Qu76**] *and A. Suslin* [**Su76**]*: indeed, every finitely generated projective R-module is free. Quillen received the Fields Medal in 1978. Fields Medals are not awarded for the solution of any single problem, but the prize committee writes an official document describing the work of each winner that they found particularly meritorious. In this case, it was made clear that Quillen's resolution of Serre's Conjecture was one of the reasons he received the prize. All this for modules over a polynomial ring!*

For more information on Serre's Conjecture, the reader can do no better than to consult a book of T.Y. Lam [**La06**].

EXERCISE 3.36. *($K_0(R)$): From a commutative ring R, we will construct another commutative ring $K_0(R)$ whose elements correspond to formal differences of finite rank projective modules. More precisely:*

a) *Let $M_0(R)$ denote the set of all isomorphism classes of finitely generated projective modules. For finitely generated projective modules P and Q we define*

$$[P] + [Q] = [P \oplus Q],$$
$$[P] \cdot [Q] = [P \otimes Q].$$

Check that this construction is well-defined on isomorphism classes and endows $M_0(R)$ with the structure of a commutative semiring with unity. What are the additive and mulitplicative identity elements?

b) *Define $K_0(R)$ as the Grothendieck group of $M_0(R)$, i.e., as the group completion of the commutative monoid $M_0(R)$. Convince yourself that $K_0(R)$ has the structure of a semiring. The elements are of the form $[P] - [Q]$, and we have $[P_1] - [Q_1] = [P_2] - [Q_2] \iff$ there exists a finitely generated projective R-module M with*

$$P_1 \oplus Q_2 \oplus M \cong P_2 \oplus Q_1 \oplus M.$$

Thus if P and Q are projective modules, then $[P] = [Q]$ in $K_0(R)$ if and only if $[P]$ and $[Q]$ are ***stably isomorphic****, i.e., if and only if they become isomorphic after taking the direct sum with some other finitely generated projective module M. item[c)] Show: we also have $[P] = [Q]$ if and only if there exists a finitely generated* free *module R^n such that $P \oplus R^n \cong Q \oplus R^n$. In particular, $[P] = [0] = 0$ if and only if P is* ***stably free****: there exists a finitely generated free module F such that $P \oplus F$ is free.*

d) *Show that $M_0(R)$ is cancellative if and only if every stably free finitely generated projective module is free.*

e) *Find a ring R admitting a finitely generated projectve module which is stably free but not free.*
f) *Show that the mapping $R^n \mapsto [R^n]$ induces an injective homomorphism of rings $\mathbb{Z} \to K_0(R)$. Define $\tilde{K}_0(R)$ to be the quotient $K_0(R)/\mathbb{Z}$. Show that if R is a PID then $\tilde{K}_0(R) = 0$.*

6. Injective modules

6.1. Basic equivalences.

Although we will have no use for them in the sequel of these notes, in both commutative and (especially) homological algebra there is an important class of modules "dual" to the projective modules. They are characterized as follows.

PROPOSITION 3.21. *For a module E over a ring R, the following are equivalent:*
(i) *If $\iota : M \to N$ is an injective R-module homomorphism and $\varphi : M \to E$ is any homomorphism, there is at least one extension of φ to a homomorphism $\Phi : N \to E$.*
(ii) *If $M \hookrightarrow N$, the natural map $\mathrm{Hom}(N, E) \to \mathrm{Hom}(M, E)$ is surjective.*
(iii) *The (contravariant) functor $\mathrm{Hom}(\ , E)$ is exact.*
(iv) *Each short exact sequence of R-modules*

$$0 \to E \xrightarrow{\iota} M \to N \to 0$$

splits: there is an R-module map $\pi : M \to E$ such that $\pi \circ \iota = 1_E$ and thus an internal direct sum decomposition $M = \iota(E) \oplus \ker(\pi) \cong E \oplus N$.

*A module satisfying these equivalent conditions is called **injective**.*

EXERCISE 3.37. *Prove Proposition 3.21.*

EXERCISE 3.38. *Show: an R-module E is injective if and only if whenever E is a submodule of a module M, E is a direct summand of M.*

Notice that the set of equivalent conditions starts with (ii)! This is to facilitate direct comparison to Proposition 3.10 on projective modules. Indeed, one should check that each of the properties (ii) through (v) are *duals* of the corresponding properties for projective modules: i.e., they are obtained by reversing all arrows. The difficulty here with property (i) is that if one literally reverses the arrows in the definition of free R-module to arrive at a "cofree" R-module, one gets a definition that is unhelpfully strong: the "cofree R-module on a set X" does not exist when $\#X > 1$! This can be remedied by giving a more refined definition of *cofree* module. For the sake of curiosity, we will give it later on in the exercises, but to the best of my knowledge, cofree R-modules by any definition do not play the fundamental role that free R-modules do.

EXERCISE 3.39. *Show: every module over a field is injective.*

EXERCISE 3.40. *Show: $\mathbb{Z}$ is* not *an injective $\mathbb{Z}$-module.*
(Injectivity is the most important property of modules that is not necessarily satisfied by free modules.)

EXERCISE 3.41. *Let $\{M_i\}_{i \in I}$ be any family of R-modules and put $M = \prod_{i \in I} M_i$. Show that M is injective if and only if M_i is injective for all $i \in I$.*

EXERCISE 3.42. *For a ring R, show the following are equivalent:*

(i) *The ring R is **absolutely projective**: every R-module is projective.*
(ii) *The ring R is **absolutely injective**: every R-module is injective.*

6.2. Baer's Criterion.

THEOREM 3.22. *(Baer's Criterion* [**Ba40**]*) For a module E over a ring R, the following are equivalent:*

(i) *E is injective.*
(ii) *For every ideal nonzero I of R, every R-module map $\varphi : I \to E$ extends to an R-module map $\Phi : R \to E$.*

PROOF. (i) $\implies$ (ii): this is a special case of condition (ii) of Proposition 3.21: take $M = I$, $N = R$.
(ii) $\implies$ (i): Let M be an R-submodule of N and $\varphi : M \to E$ an R-module map. We need to show that φ may be extended to N. Now the set $\mathcal{P}$ of pairs (N', φ') with $M \subseteq N' \subseteq N$ and $\varphi : N' \to E$ a map extending φ is nonempty and has an evident partial ordering, with respect to which the union of any chain of elements in $\mathcal{P}$ is again an element of $\mathcal{P}$. So by Zorn's Lemma, there is a maximal element $\varphi' : N' \to E$. Our task is to show that $N' = N$.

Assume not, and choose $x \in N \backslash N'$. Put

$$I = (N' : x) = \{r \in R \mid rx \subseteq N'\};$$

one checks immediately that I is an ideal of R (a generalization to modules of the *colon ideal* we have encountered before). Consider the composite map

$$I \xrightarrow{\cdot x} N' \xrightarrow{\varphi} E;$$

by our hypothesis, this extends to a map $\psi : R \to E$. Now put $N'' = \langle N', x \rangle$ and define[5] $\varphi'' : N'' \to E$ by

$$\varphi''(x' + rx) = \varphi'(x') + \psi(r).$$

Thus φ'' is an extension of φ' to a strictly larger submodule of N than N', contradicting maximality. □

EXERCISE 3.43. *Verify that the map φ'' is well-defined.*

6.3. Divisible modules.

Recall that a module M over a domain R is **divisible** if for all $r \in R^\bullet$ the endomorphism $r\bullet : M \to M, x \mapsto rx$, is surjective. Further, we define M to be **uniquely divisible** if for all $r \in R^\bullet$, the endomorphism $r\bullet : M \to M$ is a bijection.

EXAMPLE 3.23. *The $\mathbb{Z}$-modules $\mathbb{Q}$ and $\mathbb{Q}/\mathbb{Z}$ are divisible. $\mathbb{Q}$ is moreover uniquely divisible but $\mathbb{Q}/\mathbb{Z}$ is not.*

EXERCISE 3.44. *Show: a divisible module is uniquely divisible if and only if it is torsionfree.*

EXERCISE 3.45.

a) *Show: a quotient of a divisible module is divisible.*

[5]Since N'' need not be the direct sum of N' and $\langle x \rangle$, one does need to check that φ'' is well-defined; we ask the reader to do so in an exercise following the proof.

b) *Show: arbitrary direct sums and direct products of divisible modules are divisible.*

EXERCISE 3.46. *Let R be a domain with fraction field K.*

a) *Show: K is a uniquely divisible R-module.*
b) *Let M be any R-module. Show that the natural map $M \to M \otimes_R K$ is injective if and only if M is torsionfree.*
c) *Show: for any R-module M, $M \otimes_R K$ is uniquely divisible.*
d) *Show: K/R is divisible but not uniquely divisible.*

EXERCISE 3.47. a) *Show: a $\mathbb{Z}$-module is uniquely divisible if and only if it can be endowed with the compatible structure of a $\mathbb{Q}$-module, and if so this $\mathbb{Q}$-module structure is unique.*
b) *Show: a $\mathbb{Z}$-module M is a subgroup of a uniquely divisible divisible $\mathbb{Z}$-module if and only if it is torsionfree.*

EXERCISE 3.48. *For a domain R, show that the following are equivalent:*

(i) *There is a nonzero finitely generated divisible R-module.*
(ii) *R is a field.*

PROPOSITION 3.24. *Let R be a domain and E an R-module.*

a) *If E is injective, then it is divisible.*
b) *If E is torsionfree and divisible, then it is injective.*
c) *If R is a PID and E is divisible, thenit is injective.*

PROOF. a) Let $r \in R^\bullet$. For $x \in E$, consider the R-module homomorphism $\varphi : rR \to E$ given by $r \mapsto x$. Since E is injective, this extends to an R-module map $\varphi : R \to E$. Then $r\varphi(1) = \varphi(r \cdot 1) = \varphi(r) = x$, so $r\bullet$ is surjective on E.
b) Let I be a nonzero ideal of R and $\varphi : I \to E$ be an R-module map. For each $a \in I^\bullet$, there is a unique $e_a \in E$ such that $\varphi(a) = ae_a$. For $b \in I^\bullet$, we have

$$bae_a = b\varphi(a) = \varphi(ba) = a\varphi(b) = abe_b;$$

since E is torsionfree we conclude $e_a = e_b = e$, say. Thus we may extend φ to a map $\Phi : R \to E$ by $\Phi(r) = re$. Thus E is injective by Baer's Criterion.
c) As above it is enough to show that given a nonzero ideal I of R, every homomorphism $\varphi : I \to E$ extends to a homomorphism $R \to E$. Since R is a PID, we may write $I = xR$ for $x \in R^\bullet$. Then, as in part a), one checks that φ extends to Φ if and only if multiplication by x is surjective on M, which it is since M is divisible. □

By combining Proposition 3.24 with Exercise 3.46, we are able to show an important special case of the desired fact that every R-module can be realized as a submodule of an injective module. Namely, if M is a torsionfree module over a domain R, then M is a submodule of the uniquely divisible – hence injective – module $M \otimes_R K$.

EXERCISE 3.49. *Let $n \in \mathbb{Z}^+$.*

a) *Show: $\mathbb{Z}/n\mathbb{Z}$ is not a divisible $\mathbb{Z}$-module, hence not an injectivve $\mathbb{Z}$-module.*
b) *Show: $\mathbb{Z}/n\mathbb{Z}$ is a divisible $\mathbb{Z}/n\mathbb{Z}$-module if and only if n is prime.*
c) *Show: $\mathbb{Z}/n\mathbb{Z}$ is an injective $\mathbb{Z}/n\mathbb{Z}$-module.*

EXERCISE 3.50. *Let $R = \mathbb{Z}[t]$ and let K be its fraction field. Show: the R-module K/R is divisible but not injective.*

EXERCISE 3.51. *Let R be a domain with fraction field K.*

a) *If $R = K$, show: all R-modules are both injective and projective.*
b) *If $R \neq K$, show: the only R-module that is both projective and injective is 0.*

6.4. Enough injectives.

The idea of this section is to pursue the dual version of the statement "Every R-module is a quotient of a projective module": namely we wish to show that every R-module is a *submodule* of an injective module. This is a good example of a statement which remains true upon dualization but becomes more elaborate to show. The projective version is almost obvious: indeed, we have the stronger result that every module is a quotient of a *free* module, and – as we have seen – to realize M as a quotent of a free R-module is equivalent to simply choosing a set of generators for M. (But again, if we choose the most obvious definition of "cofree", then this statement will be false.)

Let k be a ring, R a k-algebra, M an R-module and N a k-module. Consider the commutative group $\mathrm{Hom}_k(M, N)$. We may endow it with the structure of an R-module as follows: for $r \in R$ and $f \in \mathrm{Hom}_{\mathbb{Z}}(M, N)$, $(rf)(x) := f(rx)$.

Consider the special case $k = \mathbb{Z}$ and $N = \mathbb{Q}/\mathbb{Z}$ of the above construction. It gives $\mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ the structure of an R-module, which we denote by M^* and call the **Pontrjagin dual** of M.[6] Because $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module, the (contravariant) functor $M \mapsto M^*$ – or in other words $\mathrm{Hom}_{\mathbb{Z}}(\ , \mathbb{Q}/\mathbb{Z})$ – is exact.[7] In particular, if $f : M \to N$ is an R-module map, then f injective implies f^* surjective and f surjective implies f^* injective.

As is often the case for "duals", we have a natural map $M \to M^{**}$: namely $x \mapsto (f \mapsto f(x))$.

Lemma 3.25. *For any R-module M, the natural map $\Psi_M : M \to M^{**}$ is injective.*

Proof. Seeking a contradiction, let $x \in M^\bullet$ be such that $\Psi(x) = 0$. Unpacking the definition, this means that for all $f \in \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$, $f(x) = 0$. But since $\mathbb{Q}/\mathbb{Z}$ is an injective $\mathbb{Z}$-module, it suffices to find a nontrivial homomorphism $\mathbb{Z}x \to \mathbb{Q}/\mathbb{Z}$, and this is easy: if x has finite order $n > 1$, we may map x to $\frac{1}{n}$, whereas if x has infinite order we may map it to any nonzero element of $\mathbb{Q}/\mathbb{Z}$. □

Lemma 3.26. *Every $\mathbb{Z}$-module M can be embedded into an injective $\mathbb{Z}$-module.*

Proof. Let $I \subseteq M$ be a generating set and let $\bigoplus_{i \in I} \mathbb{Z} \to M$ be the corresponding surjection, with kernel K, so $M \cong (\bigoplus_{i \in I} \mathbb{Z})/K$. The natural map $\bigoplus_{i \in I} \mathbb{Z} \hookrightarrow \bigoplus_{i \in I} \mathbb{Q}$ induces an injection $M \hookrightarrow (\bigoplus_{i \in I} \mathbb{Q})/K$, and the latter $\mathbb{Z}$-module is divisible, hence injective since $\mathbb{Z}$ is a PID. □

Lemma 3.27. *(Injective Production Lemma) Let R be a k-algebra, E an injective k-module and F a free R-module. Then $\mathrm{Hom}_k(F, E)$ is an injective R-module.*

[6] Recall that the notation $M^\vee$ has already been taken: this is the *linear dual* $\mathrm{Hom}_R(M, R)$.

[7] Here we are using the (obvious) fact that a sequence of R-modules is exact if and only if it is exact when viewed merely as a sequence of $\mathbb{Z}$-modules.

PROOF. We will show that the functor $\mathrm{Hom}_R(\ , \mathrm{Hom}_k(F, E))$ is exact. For any R-module M, the adjointness of $\otimes$ and Hom gives

$$\mathrm{Hom}_R(M, \mathrm{Hom}_k(F, E)) = \mathrm{Hom}_k(F \otimes_R M, E)$$

so we may look at the functor $M \mapsto \mathrm{Hom}_k(F \otimes_R M, E)$ instead. This is the composition of the functor $M \mapsto F \otimes_R M$ with the functor $N \mapsto \mathrm{Hom}_k(N, E)$. But both functors are exact – in the former case a moment's thought shows this to be true, and the latter case is one of our defining properties of injective modules. □

Remark: Soon enough we will define a *flat* R-module to be an R-module N such that the functor $M \mapsto M \otimes_R N$ is exact. Then Lemma 3.27 can be rephrased with the hypothesis that F is a flat R-module, and (since as we have just seen, free R-modules are flat) this gives a somewhat more general result.

THEOREM 3.28. *Every R-module can be embedded into an injective R-module.*

PROOF. Let M be an R-module. Viewing M as a $\mathbb{Z}$-module, by Lemma 3.26 there is an injective $\mathbb{Z}$-module E_1 and a $\mathbb{Z}$-module map $\varphi_1 : M \hookrightarrow E_1$. Further, by Lemma 3.27, $\mathrm{Hom}_{\mathbb{Z}}(R, E_1)$ is an injective R-module. Now consider the R-module map

$$\varphi : M \to \mathrm{Hom}_{\mathbb{Z}}(R, E_1),\ x \mapsto (r \mapsto \varphi_1(rx)).$$

We claim that φ is a monomorphism into the injective R-module $\mathrm{Hom}_{\mathbb{Z}}(R, E_1)$. Indeed, if $\varphi(x) = 0$ then for all $r \in R$, $\varphi_1(rx) = 0$. In particular $\varphi_1(x) = 0$, so since φ_1 is a monomorphism, we conclude $x = 0$. □

EXERCISE 3.52. *We say a $\mathbb{Z}$-module is **cofree** if it is of the form F^* for a free $\mathbb{Z}$-module F. Then the proof of Lemma 3.26 gives the stronger statement that every $\mathbb{Z}$-module can be embedded into a cofree $\mathbb{Z}$-module. Formulate a definition of **cofree R-module** so that the proof of Theorem 3.28 gives the stronger statement that every R-module can be embedded into a cofree R-module. (Hint: remember to pay attention to the difference between direct sums and direct products.)*

6.5. Essential extensions and injective envelopes.

The results of this section are all due to B. Eckmann and A. Schopf [**ES53**].

PROPOSITION 3.29. *For R modules $M \subseteq N$, the following are equivalent:*

(i) *If X is any nonzero R-submodule of N, then $X \cap M$ is nonzero.*
(ii) *If $x \in N^\bullet$, there exists $r \in R$ such that $rx \in M^\bullet$.*
(iii) *If $\varphi : N \to Y$ is an R-module map, then φ is injective if and only if $\varphi|_M$ is injective.*

*An extension $M \subseteq N$ satisfying these equivalent conditions is called **essential**.*

PROOF. (i) $\implies$ (ii): Apply (i) with $X = \langle x \rangle$.
(ii) $\implies$ (iii): Assuming (ii), let $\varphi : N \to Y$ be a homomorphism with $\varphi|_M$ is injective. It is enough to show that φ is injective. Seeking a contradiction, let $x \in N^\bullet$ be such that $\varphi(x) = 0$. By (ii), there exists $r \in R$ such that $rx \in M^\bullet$. But then by assumption $r\varphi(x) = \varphi(rx) \neq 0$, so $\varphi(x) \neq 0$, contradiction.
(iii) $\implies$ (i): We go by contraposition. Suppose there exists a nonzero submodule X of N such that $X \cap M = 0$. Then the map $\varphi : N \to N/X$ is not an injection but its restriction to M is an injection. □

PROPOSITION 3.30. *(Tower Property of Essential Extensions) Let $L \subseteq M \subseteq N$ be R-modules. Then $L \subseteq N$ is an essential extension if and only if $L \subseteq M$ and $M \subseteq N$ are both essential extensions.*

PROOF. Suppose first that $L \subseteq N$ is an essential extension. Then for any nonzero submodule X of N, we have $X \cap L \neq 0$. In particular this holds for $X \subseteq M$, so $L \subseteq M$ is essential. Moreover, since $L \subseteq M$, $X \cap L \neq 0$ implies $X \cap M \neq 0$, so $M \subseteq N$ is essential. Conversely, suppose $L \subseteq M$ and $M \subseteq N$ are both essential, and let X be a nonzero submodule of N. Then $X \cap M$ is a nonzero submodule of M and thus $(X \cap M) \cap L = X \cap L$ is a nonzero submodule of L. So $L \subseteq N$ is essential. □

So why are we talking about essential extensions when we are supposed to be talking about injective modules? The following result explains the connection.

THEOREM 3.31. *For an R-module M, the following are equivalent:*

(i) *M is injective.*
(ii) *M has no proper essential extensions: i.e., if $M \subseteq N$ is an essential extension, then $M = N$.*

PROOF. (i) $\implies$ (ii): Let M be injective and $M \subsetneq N$. Then M is a direct summand of N: there exists M' such that $M \oplus M' = N$. Thus M has zero intersection with M', and by criterion (ii) of Proposition 3.29, we must have $M' = 0$ and thus $M = N$.
(ii) $\implies$ (i): It suffices to show: if N is an R-module and $M \subseteq N$, then M is a direct summand of N. Now consider the family of submodules M' of N with the property that $M \cap M' = 0$. This family is partially ordered by inclusion, nonempty, and closed under unions of chains, so by Zorn's Lemma there exists a maximal such element M'. Now consider the extension $M \hookrightarrow N/M'$: we claim it is essential. Indeed, if not, there exists $x \in N \backslash M'$ such that $\langle M', x \rangle \cap M = 0$, contradicting maximality of M'. But by hypothesis, M has no proper essential extensions: thus $M = N/M'$, i.e., $M \oplus M' = N$ and M is a direct summand of N. □

We say that an extension $M \subseteq N$ is **maximal essential** if it is essential and there is no proper extension N' of N such that $M \subseteq N'$ is essential. Combining Proposition 3.30 and Theorem 3.31 yields the following important result.

THEOREM 3.32. *For an essential extension $M \subseteq N$ of R-modules, the following are equivalent:*

(i) *$M \subseteq N$ is maximal essential.*
(ii) *N is injective.*

EXERCISE 3.53. *To be sure you're following along, prove Theorem 3.32.*

Once again we have a purpose in life – or at least, this subsection of it – we would like to show that every R-module admits a maximal essential extension and that such extensions are unique up to isomorphism over M. Moreover, a plausible strategy of proof is the following: let M be an R-module. By Theorem 3.28 there exists an extension $M \subseteq E$ with E injective. Certainly this extension need not be essential, but we may seek to construct within it a maximal essential subextension N and then hope to show that $M \subseteq E'$ is injective.

THEOREM 3.33. *Let M be an R-module and $M \subseteq E$ an extension with E injective. Let $\mathcal{P}$ be the set of all essential subextensions N of $M \subseteq E$. Then:*

a) *$\mathcal{P}$ contains at least one maximal element.*
b) *Every maximal element E' of $\mathcal{P}$ is injective.*

PROOF. The proof of part a) is the usual Zorn's Lemma argument: what we need to check is that the union N of any chain $\{N_i\}$ of essential subextensions is again an essential subextension. Suppose for a contradiction that there exists a nonzero submodule X of N such that $X \cap M = 0$. Choose $x \in X^\bullet$ and put $X' = \langle x \rangle$. Then $X' \subseteq tN_i$ for some i and $X' \cap M \subseteq X \cap M = 0$, contradicting the essentialness (?!) of the extension $M \subseteq N_i$.
Now let E' be a maximal essential *subextension* of $M \subseteq E$. We need to show that $M \subseteq E'$ is actually a maximal essential extension: so suppose there is an essential extension $E' \subseteq N$. Let $\iota : M \subseteq E' \subseteq N$ be the composite map. It is a monomorphism, so by the injectivity of E the injection $M \subseteq E$ extends to a homomorphism $\varphi : N \to E$. But $\varphi|_M$ is an injection and $M \subseteq N$ is an essential extension, so by condition (iii) of Proposition 3.29 this implies that φ itself is an injection. By maximality of E' among essential subextensions of $M \subseteq E$ we must have $E' = N$. □

For an R-module M, we say that an extension $M \subseteq E$ is an **injective envelope** (other common name: **injective hull**) of M if $M \subseteq E$ is a maximal essential extension; equivalently, an essential extension with E injective. Thus Theorem 3.33 shows that any R-module admits an injective envelope.

PROPOSITION 3.34. *Let R be a domain with fraction field K. Then $R \subseteq K$ is an injective envelope of R.*

EXERCISE 3.54. *Prove Proposition 3.34.*
(Suggestion: use the relationship between injective modules and divisible modules.)

EXERCISE 3.55. *More generally, let M be a torsionfree module over a domain R. Show that $M \subseteq M \otimes_R K$ is an injective envelope of M.*

Let us touch up our characterization of injective envelopes a bit.

PROPOSITION 3.35. *(Equivalent Properties of an Injective Envelope) For an extension $M \subseteq E$ of R-modules, the following are equivalent:*

(i) *$M \subseteq E$ is a maximal essential extension.*
(ii) *$M \subseteq E$ is essential and E is injective.*
(iii) *E is minimal injective over M: there does not exist any proper subextension $M \subseteq E' \subseteq E$ with E' injective.*

PROOF. We have already seen that (i) $\iff$ (ii).
(ii) $\implies$ (iii): Assume that E is injective and E' is an injective subextension of $M \subseteq E$. Since E' is injective, there exists $N \subseteq E$ such that $E' \oplus N = E$. Moreover, $M \cap N \subseteq E' \cap N = 0$, so $M \cap N = 0$. Since $M \subseteq E$ is essential, we must have $N = 0$, i.e., $E' = E$.
(iii) $\implies$ (ii): Suppose that $M \subseteq E$ is minimal injective. The proof of Theorem 3.33 gives us a subextension E' of $M \subseteq E$ such that E' is injective and $M \subseteq E'$ is essential. Thus by minimality $E = E'$, i.e., $M \subseteq E$ is essential. □

THEOREM 3.36. *(Uniqueness of Injective Envelopes) Let M be an R-module and let $\iota_1 : M \subseteq E_1$, $\iota_2 : M \subseteq E_2$ be two injective envelopes of M. Then E_1 and E_2 are isomorphic as R-module extensions of M: i.e., there exists an R-module isomorphism $\Phi : E_1 \to E_2$ such that $\Phi \circ \iota_1 = \iota_2$.*

PROOF. Since $\iota_1 : M \to E_1$ is a monomorphism and E_2 is injective, the map $\iota_2 : M \to E_2$ extends to a map $\Phi : E_1 \to E_2$ such that $\Phi \circ \iota_1 = \iota_2$. Since the restriction of Φ to the essential submodule M is a monomorphism, so is Φ. The image $\Phi(E_1)$ is an essential subextension of $M \subseteq E_2$, so by condition (iii) of Proposition 3.35 we must have $E_2 = \Phi(E_1)$. Thus $\Phi : E_1 \to E_2$ is an isomorphism. □

In view of Theorem 3.36, it is reasonable to speak of "the" injective envelope of M and denote it by $M \to E(M)$. Reasonable, that is, but not ideal: it is not true that any two injective envelopes are canonically isomorphic.[8] Otherwise put, formation of the injective envelope is not functorial. For more on this in a more general category-theoretic context, see [**AHRT**].

EXERCISE 3.56. *Let M be a submodule of an injective module E. Show: E contains an isomorphic copy of the injective envelope $E(M)$.*

EXERCISE 3.57. *If $M \subseteq N$ is an essential extension of modules, then $E(M) = E(N)$.*

7. Flat modules

Suppose we have a short exact sequence

$$0 \to M' \to M \to M'' \to 0$$

of R-modules. If N is any R-module, we can tensor each element of the sequence with N, getting maps

$$0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0.$$

Unfortunately this new sequence need not be exact. It is easy to see that it is **right exact**: that is, the piece of the sequence

$$M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$$

remains exact. This follows because of the canonical "adjunction" isomorphism

$$\mathrm{Hom}(M \otimes N, P) = \mathrm{Hom}(M, \mathrm{Hom}(N, P))$$

and the left-exactness of the sequence $\mathrm{Hom}(\ , Y)$ for all R-modules Y. However, tensoring an injection need not give an injection. Indeed, consider the exact sequence

$$0 \to \mathbb{Z} \stackrel{[2]}{\to} \mathbb{Z}.$$

If we tensor this with $\mathbb{Z}/2\mathbb{Z}$, we get a sequence

$$0 \to \mathbb{Z}/2\mathbb{Z} \stackrel{[2]}{\to} \mathbb{Z}/2\mathbb{Z},$$

but now the map $\mathbb{Z} \otimes Z/2\mathbb{Z} \to \mathbb{Z} \otimes \mathbb{Z}/2\mathbb{Z}$ takes $n \otimes i \to (2n \otimes i) = n \otimes 2i = 0$, so is not injective.

Definition: A module M over a ring R is **flat** if the functor $N \mapsto N \otimes_R M$ is

[8] The situation here is the same as for "the" splitting field of an algebraic field extension or "the" algebraic closure of a field.

exact. This means, equivalently, that if $M \hookrightarrow M'$ then $M \otimes N \hookrightarrow M' \otimes N$, or also that tensoring a short exact sequence with M gives a short exact sequence.

It will probably seem unlikely at first, but in fact this is one of the most important and useful properties of an R-module.

So, which R-modules are flat?

PROPOSITION 3.37. *Let $\{M_i\}_{i \in I}$ be a family of R-modules. The following are equivalent:*

(i) *For all i, M_i is flat.*
(ii) *The direct sum $M = \bigoplus_i M_i$ is flat.*

EXERCISE 3.58. *Prove Proposition 3.37.*

PROPOSITION 3.38. *Let R be a domain. Then flat R-modules are torsionfree.*

PROOF. We will prove the contrapositive. Suppose that $0 \neq m \in R[\text{tors}]$, and let $0 \neq r \in R$ be such that $rm = 0$ Since R is a domain, we have a short exact sequence

$$0 \to R \xrightarrow{[r]} R \to R/rR \to 0$$

and tensoring it with M gives

$$0 \to M \xrightarrow{[r]} M \to M/rM \to 0,$$

but since $rm = 0$ the first map is not injective. □

EXAMPLE 3.39. *Let k be a field, and let $R := k[x, y]$, the polynomial ring in two indeterminates over k. Let $I := \langle x, y \rangle$; then I is a maximal ideal such that $R/I = k$. Like every ideal of a domain, I is a torsionfree module. We claim that I is not flat.*[9] *It suffices to show that the map*

$$\varphi : I \otimes I \to I \otimes_R R = I$$

obtained by tensoring the injection $I \hookrightarrow R$ with I is not an injection. This map is nothing else than the induced map from the R-bilinear multiplication map $I \times I \to I$: it sends $\sum_{i=1}^n a_i \otimes b_i$ to $\sum_{i=1}^n a_i b_i$. Evidently the element

$$\theta := x \otimes y - y \otimes x$$

lies in the kernel of φ; the crux of the matter is to show that $\theta \neq 0$. For this, let

$$D_x : k[x, y] \to k = k[x, y]/I$$

by taking the partial derivative with respect to x and then evaluating at $(0, 0)$ and let

$$D_y : k[x, y] \to k = k[x, y]/I$$

by taking the partial derivative with respect to y and then evaluating at $(0, 0)$. Finally, put

$$\mathbb{D} : I \times I \to k, \ (a, b) \mapsto D_x(a) D_y(b).$$

[9] Much later we will learn that because I is a prime ideal of height greater than 1 in a Noetherian ring, it cannot be flat.

Then $\mathbb{D}$ is R-bilinear: e.g. for $a, b \in I = \langle x, y \rangle$ and $c, d \in k[x, y]$ we have

$$\mathbb{D}(ca, db) = D_x(ca)D_y(db) = \left(c\frac{\partial a}{\partial x} + a\frac{\partial c}{\partial x}\right)\left(d\frac{\partial b}{\partial y} + b\frac{\partial d}{\partial y}\right) + \langle x, y \rangle$$

$$= cd\frac{\partial a}{\partial x}\frac{\partial b}{\partial y} + \langle x, y \rangle.$$

So $\mathbb{D}$ factors through an R-linear map $D : I \otimes I \to k$. Since

$$D(\theta) = D(x \otimes y - y \otimes x) = \mathbb{D}((x, y)) - \mathbb{D}((y, x)) = 1 - 0 = 1,$$

it follows that $\theta \neq 0$.

PROPOSITION 3.40. *Projective R-modules are flat.*

PROOF. A projective R-module is a module P such that there exists P' with $P \oplus P' \cong F$ a free module. Therefore, by Proposition 3.37, it is enough to show that free modules are flat. By abuse of notation, we will abbreviate the infinite direct sum of d copies of R as R^d. Since for any R-module M we have $M \otimes_R R^d = M^d$, it follows that tensoring a short exact sequence

$$0 \to M' \to M \to M'' \to 0$$

with $F = R^d$ just yields

$$0 \to (M')^d \to (M)^d \to (M'')^d \to 0.$$

This is still exact. □

8. Nakayama's Lemma

8.1. Nakayama's Lemma.

PROPOSITION 3.41. *Let M be a finitely generated R-module, I an ideal of R, and φ be an R-endomorphism of M such that $\varphi(M) \subseteq IM$. Then φ satisfies an equation of the form*

$$\varphi^n + a_{n-1}\varphi^{n-1} + \ldots + a_1\varphi + a_0 = 0,$$

with $a_i \in I$.

PROOF. Let $x_1, \ldots, x_n$ be a set of generators for M as an R-module. Since each $\varphi(x_i) \in IM$, we may write $\varphi(x_i) = \sum_j a_{ij}x_j$, with $a_{ij} \in I$. Equivalently, for all i,

$$\sum_{j=1}^{n} (\delta_{ij}\varphi - a_{ij})x_j = 0.$$

By multiplying on the left by the adjugate of the matrix $M = (\delta_{ij}\varphi - a_{ij})$, we get that $\det(\delta_{ij}\varphi - a_{ij})$ kills each x_i, hence is the zero endomorphism of M. Expanding out the determinant gives the desired polynomial relation satisfied by φ. □

EXERCISE 3.59. *Some refer to Proposition 3.41 as the Cayley-Hamilton Theorem. Discuss.*

THEOREM 3.42 (Nakayama's Lemma). *Let R be a ring, J an ideal of R, and M a finitely generated R-module such that $JM = M$.*

a) *There is $x \in R$ such that $x \equiv 1 \pmod{J}$ and $xM = \{0\}$.*
b) *If moreover J is contained in every maximal ideal of R, then $M = \{0\}$.*

PROOF. Applying Proposition 3.41 to the identity endomorphism $\varphi = 1_M$ gives $a_1, \ldots, a_{n-1} \in J$ such that for $x := 1 + a_1 + \ldots + a_{n-1}$, we have $xM = \{0\}$ and $x \equiv 1 \pmod{J}$, proving part a). If moreover J lies in every maximal ideal $\mathfrak{m}$ of R, then $x \equiv 1 \pmod{\mathfrak{m}}$ for all maximal ideals $\mathfrak{m}$, hence x lies in no maximal ideal of R. Therefore x is a unit and multiplying $xM = \{0\}$ by x^{-1} gives $M = \{0\}$. □

COROLLARY 3.43. *Let R be a ring, J an ideal of R which is contained in every maximal ideal of R, M a finitely generated R-module and N a submodule of M such that $JM + N = M$. Then $M = N$.*

PROOF. We have $J(M/N) = (JM + N)/N = M/N$. Applying Nakayama's Lemma to M/N, we conclude $M/N = 0$, i.e., $N = M$. □

COROLLARY 3.44. *Let R be a ring, let J be an ideal of R which is contained in every maximal ideal of R, and let M be a finitely generated R-module. Let $x_1, \ldots, x_n \in M$ be such that their images in M/JM span M/JM as an R/J-module. Then the x_i's span M.*

PROOF. Let $N = \langle x_1, \ldots, x_n \rangle_R$, and apply Corollary 3.43. □

COROLLARY 3.45. *Let R be a ring, and let J be an ideal that is contained in every maximal ideal of R. Let M and N be R-modules, with N finitely generated, and let $u : M \to N$ be an R-module map. Suppose that the map $u_J : M/JM \to N/JN$ is surjective. Then u is surjective.*

PROOF. Apply Nakayama's Lemma to J and N/M. □

Recall that an element x in a ring R such that $x^2 = x$ is called **idempotent**. Similarly, an ideal I of R such that $I^2 = I$ is called **idempotent**.

EXERCISE 3.60. *Let R be a ring and I an ideal of R.*

a) *Suppose $I = (e)$ for an idempotent element e. Show that I is idempotent.*
b) *Give an example of a nonidempotent x such that (x) is idempotent.*
c) *Is every idempotent ideal generated by some idempotent element?*

COROLLARY 3.46. *Let R be a ring, and let I be a* finitely generated *idempotent ideal of R. Then there is an idempotent $e \in R$ such that $I = (e)$. Thus in a Noetherian ring every idempotent ideal is generated by an idempotent element.*

EXERCISE 3.61. *Prove Corollary 3.46. (Hint: apply Theorem 3.42!)*

8.2. Hopfian modules.

A group G is **Hopfian** if every surjective group homomorphism $f : G \to G$ is an isomorphism – equivalently, G is not isomorphic to any of its proper quotients.

This concept has some currency in combinatorial and geometric group theory. Clearly any finite group is Hopfian. A free group is Hopfian if and only if it is finitely generated, and more generally a finitely generated residually finite group is Hopfian. An obvious example of a non-Hopfian group is $\prod_{i=1}^{\infty} G$ for any nontrivial group G. A more interesting example is the **Baumslag-Solitar group**

$$B(2,3) = \langle x, y \mid yx^2y^{-1} = x^3 \rangle.$$

More generally, let $\mathcal{C}$ be a concrete category: that is, $\mathrm{Ob}\,\mathcal{C}$ is a class of sets and for all $X, Y \in \mathrm{Ob}\,\mathcal{C}$, $\mathrm{Hom}_{\mathcal{C}}(X,Y) \subseteq \mathrm{Hom}_{\mathrm{Set}}(X,Y)$, i.e., the morphisms between X

and Y are certain functions from X to Y. We may define an object X in $\mathcal{C}$ to be **Hopfian** if every surjective endomorphism of X is an isomorphism.

EXERCISE 3.62.

a) *(C. LaRue) Show: any finite object in a concrete category is Hopfian.*
b) *In the category of sets, the Hopfian objects are precisely the finite sets.*

Remark: Our discussion of "Hopfian objects" in categories more general than R-Mod is not particularly serious or well thought out. So far as I know there is not a completely agreed upon definition of a Hopfian object, but Martin Brandenburg has suggested (instead) the following: $X \in \mathcal{C}$ is Hopfian if every **extremal epimorphism** $X \to X$ is an isomorphism.

THEOREM 3.47. *Let R be a ring and M a finitely generated R-module. Then M is a Hopfian object in the category of R-modules.*

PROOF. ([**M**, p. 9]) Let $f : M \to M$ be a surjective R-module map. We show f is injective.

There is a unique $R[t]$-module structure on M extending the given R-module structure and such that for all $m \in$M, $tm = f(m)$. Let $I = tR[t]$. By hypothesis $IM = M$, so by Nakayama's Lemma there exists $P(t) \in R[t]$ such that

$$(1 + P(t)t)M = 0.$$

Let $y \in \ker f$. Then

$$0 = (1 + P(t)t)y = y + P(t)f(y) = y + P(t)0 = y.$$

So f is injective. □

EXERCISE 3.63. *Show: $(\mathbb{Q}, +)$ is a Hopfian $\mathbb{Z}$-module which is not finitely generated.*

EXERCISE 3.64. *Do there exist Hopfian $\mathbb{Z}$-modules of all cardinalities? (An affirmative answer was claim in* [**Ba62**]*, but it was announced in* [**Ba63**] *that the construction is not valid. So far as I know the problem remains open lo these many years later.)*

8.3. A variant.

The results of this section are taken from [**DM71**, §I.1].

THEOREM 3.48 (Nakayama's Lemma). *Let R be a ring, J an ideal of R and M a finitely generated R-module. the following are equivalent:*

(i) $J + \operatorname{ann} M = R$.
(ii) $JM = M$.

PROOF. (i) $\implies$ (ii): The annihilator of M/JM contains J and $\operatorname{ann} M$, so it contains $J + \operatorname{ann} M = R$. This means that $M/JM = 0$ and $JM = M$.
(ii) $\implies$ (i): Conversely, suppose $M = \langle m_1, \ldots, m_n \rangle$. For $1 \leqslant i \leqslant n$, put $M_i = \langle m_i, \ldots, m_n \rangle$ and $M_{n+1} = 0$. We claim that for all $1 \leqslant i \leqslant n+1$ there exists $a_i \in J$ with $(1 - a_i)M \subseteq M_i$, and we will prove this by induction on n. We may take $a_1 = 0$. Having chosen $a_1, \ldots, a_i$, we have

$$(1 - a_i)M = (1 - a_i)JM = J(1 - a_i)M \subseteq M_i,$$

so there exist $a_{ij} \in J$ such that

$$(1 - a_i)m_j = \sum_{j=i}^{n} a_{ij} m_j,$$

or

$$(1 - a_i - a_{ii})m_i \in M_{i+1}.$$

Thus

$$\left(1 - (2a_i + a_{ii} - a_i^2 - a_i a_i i)\right) M = (1-a_i)(1-a_i-a_{ii})M \subseteq (1-a_i-a_{ii})M_i \subseteq M_{i+1},$$

and we may take

$$a_{i+1} = 2a_i + a_{ii} - a_i^2 - a_i a_i i.$$

So there is $a_n \in J$ such that $1 - a_n \in \operatorname{ann} M$, and thus $1 \in J + \operatorname{ann} M$. □

EXERCISE 3.65. *Explain why Theorem 3.48 is an equivalent (but nicer?) reformulation of Theorem 3.42a).*

COROLLARY 3.49. *Let M be a finitely generated R-module such that $\mathfrak{m}M = M$ for all maximal ideals of R. Then $M = 0$.*

EXERCISE 3.66. *Prove Corollary 3.49.*

For an R-module M, we define its **trace ideal** to be the ideal $\mathcal{T}(M)$ of R generated by all the images $f(M)$ of R-module maps $f \in M^\vee = \operatorname{Hom}_R(M, R)$.

EXERCISE 3.67. *Let R be a ring.*

a) *Show: $\mathcal{T}(R) = R$.*
b) *Show: $\mathcal{T}(M_1 \oplus M_2) = \langle \mathcal{T}(M_1), \mathcal{T}(M_2) \rangle$.*
c) *Show: if M is an R-module such that $\mathcal{T}(M) = R$, then M is faithful.*

THEOREM 3.50. *Let P be a projective module, and let $\mathcal{T}(P)$ be its trace ideal.*

a) *We have $\mathcal{T}(P)P = P$, $\mathcal{T}(P)^2 = \mathcal{T}(P)$ and $\operatorname{ann} \mathcal{T}(P) = \operatorname{ann} P$.*
b) *Suppose that P is moreover finitely generated. Then $\mathcal{T}(P)$ is finitely generated, and R decomposes as a direct product of rings:*

$$R = \mathcal{T}(P) \times \operatorname{ann} P.$$

PROOF. a) Let $\{(a_i, f_i)\}_{i \in I}$ be as in the Dual Basis Lemma: for all $a \in P$ we have $a = \sum_{i \in I} f_i(a) a_i$. This shows that $\mathcal{T}(P)P = P$. For $f \in P^\vee$ we have

$$\forall a \in P,\ f(a) = \sum_{i \in I} f_i(a) f(a_i),$$

which shows that $\mathcal{T}(P)^2 = \mathcal{T}(P)$. If $s \in \operatorname{ann} P$ and $f \in P^\vee$ then for all $a \in P$ we have $sf(a) = f(sa) = 0$, so $s \in \operatorname{ann} \mathcal{T}(P)$. If $s \in \operatorname{ann} \mathcal{T}(P)$ and $a \in P$, then

$$sa = s(\sum_i f_i(a) a_i) = 0,$$

so $s \in \operatorname{ann} P$.
b) By Exercise 3.32 we may take the index set I to be $\{1, \ldots, n\}$. We claim that $\mathcal{T}(P)$ is generated by the set $\{f_j(a_i)\}$. By Exercise 3.33 we have $P^\vee = \langle f_1, \ldots, f_n \rangle$, so for $f \in P^\vee$ there are $x_1, \ldots, x_n \in R$ such that $f = \sum_{j=1}^n x_j f_j$, and then for any $a \in P$ we have

$$f(a) = \sum_{j=1}^{n} x_j f_j(a) = \sum_{1 \leqslant i,j \leqslant n} x_j f_i(a) f_j(a_i).$$

Therefore $\mathcal{T}(P)$ is a finitely generated idempotent ideal, so by Corollary 3.46 it is principal and generated by an idempotent element, say e. As with any idempotent element, this gives us a direct product decomposition

$$R = eR \times (1-e)R = (e) \times \operatorname{ann}(e) = \mathcal{T}(P) \times \operatorname{ann}\mathcal{T}(P) = \mathcal{T}(P) \times \operatorname{ann} P. \quad \square$$

COROLLARY 3.51. *A nonzero finitely generated projective module over a connected ring R (i.e., without idempotents other than 0 and 1) is faithful.*

EXERCISE 3.68. *Prove Corollary 3.51.*

COROLLARY 3.52. *Let $R \subseteq S$ be an extension of rings.*

a) *We have that R is a direct summand of the R-module S if and only if $\mathcal{T}(S) = R$.*
b) *If S is finitely generated an projective as an R-module, then R is a direct summand of S.*

PROOF. a) First suppose that we have an R-module decomposition $S = R \oplus A$. Then by Exercise 3.67 we have $\mathcal{T}(S) \supseteq \mathcal{T}(R) = R$.

Now suppose that $\mathcal{T}(S) = R$, so there are elements $a_1, \ldots, a_n \in S$ and $f_1, \ldots, f_n \in S^\vee$ such that $\sum_{i=1}^n f_i(a_i) = 1$. Define $\ell \in S^\vee$ by

$$\ell(s) := \sum_{i=1}^n f_i(sa_i).$$

Then for all $r \in R$ we have

$$\ell(r) = \sum_{i=1}^n f_i(ra_i) = r\left(\sum_{i=1}^n f_i(a_i)\right) = r,$$

so if $\iota : R \hookrightarrow S$ is the inclusion map we have $\ell \circ \iota = 1_R$ and thus $S = R \oplus \operatorname{Ker} \ell$.
b) By Theorem 3.50, we have $R = \mathcal{T}(S) \times \operatorname{ann} S$. Since R is a faithful R-module, so is the larger R-module S: $\operatorname{ann} S = (0)$. Thus $\mathcal{T}(S) = R$, so part a) applies. $\square$

Later on we will study Dedekind domains, and in particular characterize them as the Noetherian domains for which every finitely generated torsionfree module is projective. Thus Corollary 3.52 has the following application that is useful in number theory: let R be a Dedeknd domain, with fraction field K. Let V be a finite-dimensional K-vector space. An **R-order** in V is a ring $R \subseteq \mathcal{O} \subseteq V$ such that $\mathcal{O}$ is finitely generated as an R-module. Since $\mathcal{O}$ is torsionfree, it then follows that R is a direct summand of $\mathcal{O}$.

8.4. Applications to modules over local rings.

LEMMA 3.53. *Let R be a ring and J an ideal which is contained in every maximal ideal of R, and let M be a finitely presented R-module. Suppose that:*

(i) *M/JM is a free R/J-module, and*
(ii) *The canonical map $J \otimes_R M \to JM$ is injective.*

Then M is a free R-module.

PROOF. We may choose a family $\{x_i\}_{i \in I}$ of elements of M such that the images in M/JM give a R/J-basis. (Since M is finitely generated over R, M/JM is finitely generated over R/J, so the index set I is necessarily finite.) Consider the finitely generated free R-module $L = \bigoplus_{i \in I} R$, with canonical basis $\{e_i\}$. Let $u : L \to M$ be the unique R-linear mapping each e_i to x_i, and let $K = \ker(u)$. Since M is finitely

presented, by Proposition 3.6 K is finitely generated. We have a commutative diagram with exact rows:

$$J \otimes K \to J \otimes L \to J \otimes M \to 0$$
$$0 \to K \to L \to M \to 0,$$

where each vertical map – $a : J \otimes K \to K$, $b : J \otimes L \to L$, $c : J \otimes M \to M$ – is the natural multiplication map. Our hypothesis is that the the map $J \otimes_R M \to JM$ is injective, so by the Snake Lemma we get an exact sequence

$$0 \to \operatorname{coker}(a) \to \operatorname{coker}(b) \xrightarrow{\overline{u}} \operatorname{coker}(c).$$

Now observe that $\operatorname{coker}(b) = (R/J) \otimes_R L$ and $\operatorname{coker}(c) = (R/J) \otimes_R M$, and by definition the mapping $u : L \to M$ gives, upon passage to the quotient modulo J, a mapping from one R/J-module basis to another. So $\overline{u}$ is an isomorphism and thus $\operatorname{coker}(a) = 0$, i.e., $K/JK = 0$. By Nakayama's Lemma we conclude $K = 0$, i.e., u gives an isomorphism from the free module L to M, so M is free. □

We can now prove the following result, which is one that we will build upon in our future studies of modules over commutative rings.

THEOREM 3.54. *Let R be a ring with a unique maximal ideal $\mathfrak{m}$ – i.e., a* local ring. *For a* finitely presented *R-module M, the following are equivalent:*

(i) *M is free.*
(ii) *M is projective.*
(iii) *$M$is flat.*
(iv) *The natural map $\mathfrak{m} \otimes_R M \to \mathfrak{m}M$ is an injection.*

PROOF. Each of the implications (i) $\implies$ (ii) $\implies$ (iii) $\implies$ (iv) is immediate. Assume (iv). Then, since $\mathfrak{m}$ is maximal, $R/\mathfrak{m}$ is a field, so every $R/\mathfrak{m}$-module is free. Therefore Lemma 3.53 applies to complete the proof. □

9. Ordinal Filtrations and Applications

9.1. The Transfinite Dévissage Lemma.

Let M be an R-module. By an **ordinal filtration** on M we mean an ordinal number α and for each $i \leqslant \alpha$ a submodule M_i of M satisfying all of the following:
(OF1) $M_0 = 0$, $M_\alpha = M$.
(OF2) For all $i, j \in \alpha + 1$, $i \leqslant j \implies M_i \subseteq M_j$.
(OF3) For all limit ordinals $i \leqslant \alpha$, $M_i = \bigcup_{j<i} M_j$.

So for instance, taking $\alpha = \omega = \{1, 2, 3, \ldots\}$ the first infinite ordinal, we recover the usual notion of an exhaustive filtration by submodules M_n, with the additional convention that $M_\omega = \bigcup_{n \in \omega} M_n$.

For $i < \alpha$, we call M_{i+1}/M_i the **ith successive quotient**. If for a class $\mathcal{C}$ of R-modules each successive quotient lies in $\mathcal{C}$, we say the filtration is of **class** $\mathcal{C}$.

Define the **associated graded module** $\operatorname{Gr}(M) = \bigoplus_{i<\alpha} M_{i+1}/M_i$.

LEMMA 3.55. *(Transfinite Dévissage Lemma) Let M be an R-module and $\{M_i\}_{i \leqslant \alpha}$ an ordinal filtration of M.*

a) *Suppose we make the following hypothesis: (DS) For all $i < \alpha$ the submodule M_i is a direct summand of M_{i+1}. Then*

$$M \cong \mathrm{Gr}(M) = \bigoplus_{i<\alpha} M_{i+1}/M_i.$$

b) *Hypothesis (DS) holds if each successive quotient M_{i+1}/M_i is projective.*
c) *Hypothesis (DS) holds if each M_i is injective.*

EXERCISE 3.69. *Prove Lemma 3.55. (Hint: use transfinite induction.)*

COROLLARY 3.56. *For an R-module M, the following are equivalent:*

(i) *M is free.*
(ii) *M admits an ordinal filtration with successive quotients isomorphic to R.*
(iii) *M admits an ordinal filtration with free successive quotients.*

PROOF. (i) $\implies$ (ii): If M is free, then $M \cong \bigoplus_{i\in I} R$. By the Well-Ordering Principle[10], I is in bijection with an ordinal α, so we may write $M \cong \bigoplus_{i<\alpha} R$, and put $M_i = \bigoplus_{j<i} R$.
(ii) $\implies$ (iii) is immediate.
(iii) $\implies$ (i) follows from Lemma 3.55 since free modules are projective. □

9.2. Hereditary and semihereditary rings.

An R-module is **hereditary** if every submodule is projective. (In particular a hereditary module is projective, and thus the property of being projective is "inherited" by its submodules.) We say that a ring R is **hereditary** if R is a hereditary R-module, or equivalently every ideal of R is projective as an R-module.

EXERCISE 3.70.
a) *Show: every submodule of a hereditary module is hereditary.*
b) *Show: the zero module is hereditary.*
c) *Show: there are nonzero rings R for which the only hereditary R-module is the zero module.*

EXAMPLE 3.57. *A PID is a hereditary ring. Indeed, any nonzero ideal of a PID R is isomorphic as an R-module to R.*

THEOREM 3.58.

a) *For $i \in I$, let M_i be a hereditary R-module, and let N be an R-submodule of $\bigoplus_{i\in I} M_i$. Then there is for all $i \in I$ an R-submodule H_i of M_i such that $N \cong \bigoplus_{i\in I} H_i$.*
b) *For R hereditary and M an R-module, the following are equivalent:*
   (i) *M is isomorphic to to a direct sum of ideals of R.*
   (ii) *M can be embedded in a free R-module.*
   (iii) *M can be embedded in a projective R-module.*

PROOF. a) Let $M = \bigoplus_{i\in I}$ be a direct sum of hereditary modules, and let N be an R-submodule of M. By the Well-Ordering Principle there is a bijection from I to some ordinal α, and without loss of generality we may assume $M = \bigoplus_{i\in\alpha} M_i$.

[10]This set-theoretic axiom is equivalent to the Axiom of Choice and also to Zorn's Lemma. Our running convention in these notes is to freely use these axioms when necessary.

For $j \in \alpha^+$, put $P_j = \bigoplus_{i<j^+} M_i$, so that $\{M_j\}$ is an ordinal-indexed chain of R-submodules of M with final element $P_\alpha = M$. For each $j \in \alpha^+$, put

$$N_j = N \cap P_j,$$

so $\{N_j\}$ is an ordinal filtration on N with $N_\alpha = N$. Moreover, for all $i \in \alpha$ we have $N_i = N_{i+1} \cap P_i$ and thus

$$N_{i+1}/N_i = N_i/(N_{i+1} \cap P_i) \cong (N_{i+1} + P_i)/P_i.$$

Thus N_{i+1}/N_i is isomorphic to a submodule H_i of $P_{i+1}/P_i \cong M_i$. For $i \in I$, since M_i is hereditary, so is $H_i \cong N_{i+1}/N_i$. In particular each N_{i+1}/N_i is projective, and the Transfinite Dévissage Lemma (Lemma 3.55) applies to show that

$$N \cong \operatorname{Gr} N = \bigoplus_{i<\alpha} N_{i+1}/N_i \cong \bigoplus_{i \in I} H_i.$$

b) (i) $\implies$ (ii): Since an ideal is precisely an R-submodule of a free R-module of rank 1, this holds over any ring.
(ii) $\iff$ (iii): Since every projective module is a direct summand of a free R-module, this also holds over any ring.
(ii) $\implies$ (i): This follows from part a). □

COROLLARY 3.59. *Let $\{M_i\}_{i \in I}$ be a family of R-modules. Then $M = \bigoplus_{i \in I} M_i$ is hereditary if and only if M_i is hereditary for all i.*

PROOF. Suppose each M_i is hereditary, and let N be a submodule of M. By Theorem 3.58a), there is for all $i \in I$ an R-submodule H_i of M_i such that $N \cong \bigoplus_{i \in I} H_i$. Each H_i, being a submodule of the hereditary module M_i, is itself hereditary, hence projective. Thus N is a direct sum of projective modules, hence projective. Conversely, if M is hereditary, so are all of its submodules M_i. □

LEMMA 3.60.

a) *(Checking Projectivity With Injectives) Let P be an R-module such that: for every injective module I, surjection $q : I \to Q$ and module map $f : P \to Q$, there is $F : P \to I$ such that $q \circ F = f$. Then P is projective.*
b) *(Checking Injectivity With Projectives) Let I be an R-module such that: for every projective R-module P, injection $\iota : S \to P$ and module map $f : S \to I$, there is $F : P \to I$ such that $F \circ \iota = f$. Then I is injective.*

PROOF. a) Let $0 \to A' \xrightarrow{\iota} A \xrightarrow{\tau} A'' \to 0$ be a short exact sequence of R-modules, and let $f : P \to A''$ be a module map. Let $\sigma : A \to I$ be an embedding into an injective module, and consider the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A' & \xrightarrow{\iota} & A & \xrightarrow{\tau} & A'' & \longrightarrow & 0 \\ & & \| & & \downarrow{\scriptstyle \sigma} & & & & \\ 0 & \longrightarrow & A' & \xrightarrow{\sigma \circ \iota} & I & \xrightarrow{q} & Q & \longrightarrow & 0 \end{array}$$

Step 1: We claim there is $\rho : A'' \to Q$ making the diagram commute.
Proof: This is a routine diagram chase: choose $y \in A''$, lift to x in A, and put $\rho(y) = (q \circ \sigma)(x)$. Let us check that this is well-defined: if we chose a different lift x' in A, then $x - x' \in A'$, so $(q \circ \sigma)(x - x') = 0$.
Step 2: By hypothesis, the map $\rho \circ f : P \to Q$ can be lifted to $G : P \to I$. To

complete the proof it suffices to show $G(P) \subset \sigma(A)$. To see this, let $x \in P$ and choose $a \in A$ such that $\tau(a) = f(x)$. Then

$$q(G(x)) = \rho(f(x)) = \rho(\tau(a)) = q(\sigma(a)),$$

so $G(x) - \sigma(a) \in \operatorname{Ker} q = \operatorname{Im}(\sigma \circ q)$. That is, there is $a' \in A'$ such that $\sigma(\iota(a')) = G(x) - \sigma(a)$, so

$$G(x) = \sigma(\iota(a') + a) \in \sigma(A).$$

b) This is the dual version of part a), i.e., obtained by reversing all the arrows. The above proof also dualizes, as we leave it to the reader to check. □

COROLLARY 3.61. *(Cartan-Eilenberg)*
For a ring R, the following are equivalent:

(i) *R is hereditary.*
(ii) *Every free R-module is hereditary.*
(iii) *Every projective R-module is hereditary.*
(iv) *Every quotient of an injective R-module is injective.*

PROOF. (i) $\implies$ (ii) is immediate from Corollary 3.59.
(ii) $\implies$ (iii): Suppose that every free R-module is hereditary. Then if P is a projective R-module, P is a submodule of a free module, hence a submodule of a hereditary module, hence itself hereditary.
(iii) $\implies$ (i): R is a projective R-module.
(iv) $\iff$ (iii): Let P' be a submodule of a projective R-module P; call the inclusion j. We will use Lemma 3.60a) : let I be an injective module, $q : I \to I'$ a surjection, and $f : P' \to I'$ a module map. By assumption I' is injective, so there is $h : P \to I'$ such that $h \circ j = f$. Since P is projective, there is $k : P \to I$ such that $q \circ k = h$. Then $F = k \circ j : P' \to I$ lifts f: $q \circ F = q \circ k \circ j = h \circ j = f$.
(iii) $\implies$ (iv): Using Lemma 3.60b) we may dualize the proof of (iv) $\implies$ (iii). □

THEOREM 3.62. *Let R be a a PID and F a free R-module. Then any submodule M of F is again free, of rank less than or equal to the rank of F. In particular R is a hereditary ring.*

PROOF. Let N be a submodule of $F = \bigoplus_{i \in I} R$. By Theorem 3.58b) for all $i \in I$ there is an ideal J_i of R such that $N \cong \bigoplus_{i \in I} J_i$. Since R is a PID, each J_i is is a free R-module of rank 0 or 1, so N is free of rank at most $\#I$. □

COROLLARY 3.63. *A projective module over a PID is free.*

COROLLARY 3.64. *For a finitely generated module M over a PID R, the folowing are equivalent:*

(i) *M is free.*
(ii) *M is torsionfree.*

PROOF. (i) Over any domain R, a free R-module is torsionfree. (ii) $\implies$ (i): Let M be a finitely generated module over a PID. By Proposition 3.8b), M is a submodule of a finitely generated free R-module. Applying Theorem 3.62 we deduce that M is free. □

EXERCISE 3.71. *Let R be a ring with the following property: every submodule of a finitely generated free R-module is free. Show that R is a principal ring (i.e., every ideal of R is principal).*

An R-module M is **semihereditary** if every finitely generated R-submodule N of M is projective. Thus a Noetherian semihereditary module is hereditary. A ring R is **semihereditary** if R is a semihereditary R-module, or equivalently every finitely generated ideal of R is projective as an R-module.

EXAMPLE 3.65. *A domain in which every finitely generated ideal is principal is semihereditary. These are called* ***Bézout domains*** *and will be studied later on.*

THEOREM 3.66. *Let $\{M_i\}_{i\in I}$ a family of semihereditary R-modules, and let N be a finitely generated R-submodule of $\bigoplus_{i\in I} M_i$. Then for all $i \in I$ there is an R-submodule H_i of M_i such that $N \cong \bigoplus_{i\in I} H_i$.*

PROOF. The proof of Theorem 3.58a) goes through verbatim. □

THEOREM 3.67. *Let R be a domain in which every finitely generated ideal is principal, and let F be a free R-module. Then any finitely generated submodule N of F is free, of rank less than or equal to the rank of F.*

PROOF. One can adapt the proof of Theorem 3.63, using Theorem 3.66 in place of Theorem 3.58. □

THEOREM 3.68. *Let R be a domain in which every finitely generated ideal is principal. Then every finitely generated torsionfree R-module is free.*

PROOF. The argument is the same as that of Proposition 3.64 (a special case), using Theorem 3.67 in place of Theorem 3.62. □

THEOREM 3.69 (F. Albrecht). *Let R be a semihereditary ring, F a free R-module, and P a finitely generated submodule of F.*

a) *P is isomorphic to a finite direct sum of finitely generated ideals of R.*
b) *In particular, P is a finitely generated projective module.*
c) *If R is a domain with fraction field K and F is free of finite rank n, then the rank of P – i.e., $\dim_K P \otimes_R K$ – is at most n.*

EXERCISE 3.72. *Use Theorem 3.66 to prove Theorem 3.69.*

9.3. Big modules.

LEMMA 3.70. *(Kaplansky) Let R be a ring, and let F be an R-module which is a direct sum of countably generated submodules: say $F = \bigoplus_{\lambda\in\Lambda} E_\lambda$. Then every direct summand of F is again a direct sum of countably generated submodules.*

PROOF. We CLAIM that there is an ordinal filtration $\{F_i\}_{i\leqslant\alpha}$ on F satisfying all of the following properties. (i) For all $i < \alpha$, F_{i+1}/F_i is countably generated.
(ii) If $M_i = F_i \cap M$, $N_i = F_i \cap N$, then $F_i = M_i \oplus N_i$.
(iii) For each i there is a subset Λ_i of Λ such that $F_i = \bigoplus_{\lambda\in\Lambda_i} \Lambda_i$.
SUFFICIENCY OF CLAIM: If so, $\{M_i\}_{i\leqslant\alpha}$ is an ordinal filtration on M. Moreover, since $M_i \subseteq M_{i+1}$ are both direct summands of F, M_i is a direct summand of M_{i+1}. The Transfinite Dévissage Lemma (Lemma 3.55) applies to give

$$M \cong \mathrm{Gr}(M) = \bigoplus_{i<\alpha} M_{i+1}/M_i.$$

Moreover, for all $i < \alpha$ we have

$$F_{i+1}/F_i = (M_{i+1} \oplus N_{i+1})/(M_i \oplus N_i) \cong M_{i+1}/M_i \oplus N_{i+1}/N_i,$$

which shows that each successive quotient M_{i+1}/M_i is countably generated. Therefore M is a direct sum of countably generated submodules.
PROOF OF CLAIM: We will construct the filtration by transfinite induction. The base case and the limit ordinal induction step are forced upon us by the definition of ordinal filtration: we must have $F_0 = \{0\}$, and for any limit ordinal $\beta \leqslant \alpha$, assuming we have defined F_i for all $i < \beta$ we must have $F_\beta = \bigcup_{i<\beta} F_i$.

So consider the case of a successor ordinal $\beta = \beta' + 1$. Let Q_1 be any E_λ which is not contained in $F_{\beta'}$. (Otherwise we have $F_{\beta'} = F$ and we may just define $F_i = F$ for all $\beta \leqslant i \leqslant \alpha$.) Let $x_{11}, x_{12}, \ldots$ be a sequence of generators of Q_1, and decompose x_{11} into its M- and N-components. Let Q_2 be the direct sum of the finitely many E_λ which are necessary to write both of these components, and let $x_{21}, x_{22}, \ldots$ be a sequence of generators for Q_2. Similarly decompose x_{12} into M and N components, and let Q_3 be the direct sum of the finitely many E_λ needed to write out these components, and let $x_{31}, x_{32}, \ldots$ be a sequence of generators of Q_3. We continue to carry out this procedure for all x_{ij}, proceeding according to a diagonal enumeration of $\mathbb{Z}^+ \times \mathbb{Z}^+$: i.e., $x_{11}, x_{12}, x_{21}, x_{13}, x_{22}, x_{31}, \ldots$. Put $F_\beta = \langle F_{\beta'}, \{x_{ij}\}_{i,j\in\mathbb{Z}^+}\rangle_R$. This works! □

For a cardinal number κ, we say that a module is **κ-generated** if it admits a generating set of cardinality at most κ.

EXERCISE 3.73. *(Warfield) Let κ be an infinite cardinal. Formulate and prove a version of Lemma 3.70 in which "countably generated" is replaced by "κ-generated".*

THEOREM 3.71. *(Kaplansky) For a ring R, let $\mathcal{P}_c$ be the class of countably generated projective R-modules. For an R-module M, the following are equivalent:*

(i) *M admits an ordinal filtration of class $\mathcal{P}_c$.*
(ii) *M is a direct sum of countably generated projective submodules.*
(iii) *M is projective.*

PROOF. (i) $\iff$ (ii) follows immediately from Lemma 3.55.
(ii) $\implies$ (iii): any direct sum of projective modules is projective.
(iii) $\implies$ (ii): If M is projective, let F be a free R-module with $F = M \oplus N$. Certainly F is a direct sum of countably generated submodules (indeed, of singly generated submodules!), so by Lemma 3.70 M is a direct sum of a family of countably generated submodules, each of which must be projective. □

While pondering the significance of this result, one naturally inquires:

QUESTION 2. *Is there a ring R and an R-module M which is* not *a direct sum of countably generated submodules?*

THEOREM 3.72. *(Cohen-Kaplansky [**CK51**], Griffith) For a ring R, the following are equivalent:*

(i) *Every R-module is a direct sum of cyclic (i.e., singly generated) R-modules.*
(ii) *Every R-module is a direct sum of finitely generated submodules.*
(iii) *The ring R is an Artinian principal ring.*

Building on these results as well as work of Faith and Walker [**FW67**], R.B. Warfield Jr. proved the following striking results.

THEOREM 3.73. *(Warfield [**Wa**]) Let R be a Noetherian ring which is not a principal Artinian ring. Then for any cardinal κ, there is a module M with the following properties:*

(i) *M is not κ-generated.*
(ii) *Any decomposition of M into the direct sum of nonzero submodules has only finitely many direct summands.*

The hypotheses of Theorem 3.73 apply for instance to the ring $\mathbb{Z}$ of integers and yields, in particular, for any infinite cardinal κ a commutative group M which is not a direct sum of κ-generated submodules.

THEOREM 3.74. *(Warfield [**Wa**]) For a ring R, the following are equivalent:*
(i) *Every R-module is a direct sum of cyclic submodules.*
(ii) *There exists a cardinal number κ such that every R-module is a direct sum of κ-generated submodules.*
(iii) *R is a principal Artinian ring.*

It is natural to wonder whether Theorem 3.73 can be strengthened in the following way: an R-module M is **indecomposable** if it cannot be expressed as a direct sum of two nonzero submodules.

QUESTION 3. *For which rings R do there exist indecomposable R-modules of all infinite cardinalities?*

However, Question 3 has turned out to be bound up with sophisticated set-theoretic considerations. Namely, in a 1959 paper [**Fu59**], L. Fuchs claimed that there exist indecomposable commutative groups of all infinite cardinalties, thus giving an affirmative answer to Question 3 for the ring $R = \mathbb{Z}$. However, it was later observed (by A.L.S. Corner) that Fuchs' argument is valid only for cardinals κ less than the first **inaccessible cardinal**. Exactly what an inaccessible cardinal is we do not wish to say, but we mention that the nonexistence of inaccessible cardinals is equiconsistent with the standard ZFC axioms of set theory (in other words, if the ZFC axioms are themselves consistent, then ZFC plus the additional axiom that there are no inaccessible cardinals remains consistent) but that nevertheless set theorists have reasons to believe in them. See also [**Fu74**] in which these issues are addressed and he proves that there is an indecomposable commutative group of any infinite **nonmeasurable** cardinality (note: accessible implies nonmeasurable).

QUESTION 4. *Is there a ring R and a projective R-module M which is* not *a direct sum of finitely generated submodules?*

Again the answer is *yes*. A very elegant example was given by Kaplansky (unpublished, apparently).[11] Namely that R be the ring of all real-valued continuous functions on the unit interval $[0,1]$, and let I be the ideal of functions $f : [0,1] \to \mathbb{R}$ which vanish near zero: i.e., for which there exists $\epsilon = \epsilon(f) > 0$ such that $f|_{[0,\epsilon(f)]} = 0$.

EXERCISE 3.74. *Show the ideal I defined above gives a projective R-module which is not the direct sum of finitely generated submodules.*
(Suggestions: (i) to show that I is projective, use the Dual Basis Lemma. (ii) A slick proof of the fact that I is not a direct sum of finitely generated submodules can be given by Swan's Theorem using the contractibility of the unit interval.)

LEMMA 3.75. *Let M be a projective module over the local ring R, and let $x \in M$. There is a direct summand M' of M such that M' contains x and M' is free.*

[11] Warm thanks to Gjergji Zaimi for bringing this important example to my attention.

PROOF. Let F be a free module with $F = M \oplus N$. Choose a basis $B = \{u_i\}_{i \in I}$ of F with respect to which the element x of M has the minimal possible number of nonzero coordinates. Write

$$x = r_1 u_1 + \ldots + r_n u_n,\ r_i \in R^\bullet.$$

Then for all $1 \leqslant i \leqslant n$, $r_i \notin \sum_{j \neq i} R r_j$. Indeed, if say $r_n = \sum_{i=1}^{n-1} s_i r_i$, then $x = \sum_{i=1}^{n-1} r_i(u_i + s_i u_n)$, contradicting the minimality of the chosen basis.
Now write $u_i = y_i + z_i$ with $y_i \in M,\ z_i \in N$, so

$$x = \sum_i r_i u_i = \sum_i r_i y_i. \tag{6}$$

We may write

$$y_i = \sum_{j=1}^{n} c_{ij} u_j + t_i, \tag{7}$$

with t_i a linear combination of elements of $B \backslash \{u_1, \ldots, u_n\}$. Substituting (7) into (6) and projecting onto M gives the relations

$$r_i = \sum_{j=1}^{n} c_{ji} r_j,$$

or equivalently, for all i,

$$(1 - c_{ii}) r_i = \sum_{j \neq i} c_{ji} r_j.$$

If for any i and j, then one of the coefficients of r_j in the above equation is a unit of R, then dividing through by it expresses r_j as an R-linear combination of the other r_i's, which as above is impossible. Therefore, since R is local, each coefficient must lie in the maximal ideal of R:

$$\forall i,\ 1 - c_{ii} \in \mathfrak{m}, \quad \forall i \neq j,\ c_{ij} \in \mathfrak{m}.$$

It follows that the determinant of the matrix $C = (c_{ij})$ is congruent to 1 modulo $\mathfrak{m}$, hence invertible: if $x \in \mathfrak{m}$ and $1 + x$ is not invertible, then $1 + x = y$ for $y \in \mathfrak{m}$, so $1 = y - x \in \mathfrak{m}$, contradiction. Therefore replacing $u_1, \ldots, u_n$ in B with $y_1, \ldots, y_n$ still yields a basis of F. It follows that $M' = \langle y_1, \ldots, y_n \rangle_R$ is a direct summand of F hence also of M which is a free module containing x. □

THEOREM 3.76. *(Kaplansky) Let $(R, \mathfrak{m})$ be a local ring, and let P be any projective R-module. Then P is free.*

PROOF. Step 1: Since by Theorem 3.71 P is a direct sum of countably generated projective submodules, we may as well assume that P itself is countably generated.
Step 2: Suppose $M = \langle \{x_n\}_{n=1}^{\infty} \rangle_R$ is a countably generated projective module over the local ring R. By Lemma 3.75, $M = F_1 \oplus M_1$ with F_1 free containing x_1. Note that M_1 is again projective and is generated by the images $\{x_n'\}_{n=2}^{\infty}$ of the elements x_n under the natural projection map $M \to M_1$. So reasoning as above, we may write $M_2 = F_2 \oplus M_2$ with F_2 free containing x_2'. Continuing in this manner, we get

$$M = \bigoplus_{n=1}^{\infty} F_n,$$

so M is free. □

EXERCISE 3.75. *Give an example of a (necessarily infinitely generated) module over a local PID which is flat but not free.*

10. Tor and Ext

10.1. Co/chain complexes.

Let R be a ring. A **chain complex** $C_\bullet$ of R-modules is a family $\{C_n\}_{n\in\mathbb{Z}}$ of R-modules together with for all $n \in \mathbb{Z}$, an R-module map $d_n : C_n \to C_{n-1}$ such that for all n, $d_{n-1} \circ d_n = 0$. (It is often the case that $C_n = 0$ for all $n < 0$, but this is not a required part of the definition.)

An example of a chain complex of R-modules is any long exact sequence. However, from the perspective of homology theory this is a trivial example in the following precise sense: for any chain complex we may define its **homology modules**: for all $n \in \mathbb{Z}$, we put

$$H_n(C) = \operatorname{Ker}(d_n)/\operatorname{Im}(d_{n+1}).$$

EXAMPLE 3.77. *Let X be any topological space. For any ring R, we have the **singular chain complex** $S(X)_\bullet$: $S(X)_n = 0$ for $n < 0$, and for $n \geqslant 0$, $S(X)_n$ is the free R-module with basis the set of all continuous maps $\Delta_n \to X$, where Δ_n is the standard n-dimensional simplex. A certain carefully defined alternating sum of restrictions to faces of Δ_n gives rise to a boundary map $d_n : S(X)_n \to S(X)_{n-1}$, and the indeed the homology groups of this complex are nothing else than the singular homology groups $H_n(X, R)$ with coefficients in R.*

If $C_\bullet$ and $D_\bullet$ are two chain complexes of R-modules, a **homomorphism** $\eta : C_\bullet \to D_\bullet$ is given by maps $\eta_n : C_n \to D_n$ for all n rendering the following infinite ladder commutative:

INSERT ME!.

In this way one has evident notions of a **monomorphism** and **epimorphisms** of chain complexes. In fact the chain complexes of R-modules form an abelian category and thus these notions have a general categorical meaning, but it turns out they are equivalent to the more concrete naive conditions: η is a monomorphism if and only if each η_n is injective and is an epiomorphism if and only if each η_n is surjective.

In particular we may consider a short exact sequence of chain complexes:

$$0 \longrightarrow A_\bullet \longrightarrow B_\bullet \longrightarrow C_\bullet \longrightarrow 0.$$

Here is the first basic theorem of homological algebra.

THEOREM 3.78. *Let*

$$0 \longrightarrow A_\bullet \xrightarrow{f} B_\bullet \xrightarrow{g} C_\bullet \longrightarrow 0$$

*be a short exact sequence of chain complexes of R-modules. Then for all $n \in \mathbb{Z}$ there is a natural **connecting homomorphism** $\partial : H_n(C) \to H_{n-1}(A)$ such that*

$$\ldots \xrightarrow{g} H_{n+1}(C) \xrightarrow{\partial} H_n(A) \xrightarrow{f} H_n(B) \xrightarrow{g} H_n(C) \xrightarrow{\partial} H_{n-1}(A) \xrightarrow{f} \ldots$$

is exact.

PROOF. No way. See [**W**, Thm. 1.3.1]. □

Moreover, the homology modules H_n are functors: if $f : C_\bullet \to D_\bullet$ is a morphism of chain complexes, there are induced maps on the homology groups

$$H_n(f) : H_n(C) \to H_n(D).$$

EXAMPLE 3.79. *Let $f : X \to Y$ be a continuous map of topological spaces. Then for any basic n-chain $\Delta_n \to X$ in $S(X)_n$, composition with f gives a basic n-chain $\Delta_n \to Y$ in $S(Y)_n$ and thus a homomorphism of chain complexes $S(f) : S(X)_\bullet \to S(Y)_\bullet$. There are induced maps on homology, namely the usual maps*

$$H_n(f) : H_n(X, R) \to H_n(Y, R).$$

There is an entirely parallel story for **cochain complexes** of R-modules, which are exactly the same as chain complexes but with a different indexing convention: a cochain complex $C^\bullet$ consists of for each $n \in \mathbb{Z}^+$ an R-module C^n and a "coboundary map" $d^n : C^n \to C^{n+1}$. To any cochain complex we get **cohomology modules**: for all $n \in \mathbb{Z}$, put

$$H^n(C) = \operatorname{Ker}(d^n)/\operatorname{Im}(d^{n-1}).$$

The rest of the discussion proceeds in parallel to that of chain complexes (including the realization of singular cohomology as a special case of this construction).

10.2. Chain homotopies.

Let $C_\bullet, D_\bullet$ be two chain complexes, and let $f, g : C_\bullet \to D_\bullet$ be two homomorphisms between them. We say that f and g are **chain homotopic** if there exist for all $n \in \mathbb{Z}^+$ R-module maps $s_n : C_n \to D_{n+1}$ such that

$$f_n - g_n = d_{n+1}s_n + s_{n-1}d_n.$$

The sequence $\{s_n\}$ is called a **chain homotopy** from f to g.

EXERCISE 3.76. *Show: chain homotopy is an equivalence relation on morphisms from $C_\bullet$ to $D_\bullet$.*

What on earth is going on here? Again topology is a good motivating example: we say that two maps $f, g : X \to Y$ are **homotopic** if there exists a continuous map $F : X \times [0,1] \to Y$ such that for all $x \in X$, $F(x,0) = f(x)$ and $F(x,1) = g(x)$. This is an equivalence relation and is generally denoted by $f \sim g$. We then define two topological spaces to be **homotopy equivalent** if there exist maps $\varphi : X \to Y$ and $\psi : Y \to X$ such that

$$\psi \circ \varphi \sim 1_X, \ \varphi \circ \psi \sim 1_Y.$$

(We say that $\varphi : X \to Y$ is a **homotopy equivalence** if there exists a map ψ as above.) E.g. a space is **contractible** if it is homotopy equivalent to a single point.

One of the basic tenets of algebraic topology is that it aspires to study topological spaces only up to homotopy equivalence. That is, all of the fundamental invariants of spaces should be the same on homotopy equivalent spaces and homomorphisms between these invariants induced by homotopic maps should be identical. Especially, if $f : X \to Y$ is a homotopy equivalence, the induced maps $H_n(f) : H_n(X) \to H_n(Y)$ should be isomorphisms. In fact, if $f, g : X \to Y$ are homotopic, the induced morphisms $S(f), S(g) : S(X)_\bullet \to S(Y)_\bullet$ are chain homotopic. So the following result ensures that the induced maps on homology are equal.

PROPOSITION 3.80. *If $f, g : C_\bullet \to D_\bullet$ are chain homotopic, then for all $n \in \mathbb{Z}$, $H_n(f) = H_n(g)$.*

PROOF. Replacing f and g by $f-g$ and 0, it is enough to assume that there exists a chain homotopy s from f to the zero map – i.e., for all n $f_n = d_{n+1}s_n + s_{n-1}d_n$ – and show that f induces the zero map on homology. So take $x \in H_n(C)$. Then x is represented by an element of C_n lying in the kernel of d_n, so

$$f_n(x) = d_{n+1}s_n x + s_{n-1}d_n x = d_{n+1}s_n x + 0 = d_{n+1}s_n x.$$

Thus $f_n(x)$ lies in the image of $d_{n+1}D_{n+1} \to D_n$ so represents $0 \in H_n(D)$. □

10.3. Resolutions.

Let M be an R-module. A **left resolution** of M is an infinite sequence $\{A_i\}_{i=0}^{\infty}$ of R-modules, for all $n \in \mathbb{N}$ an R-module map $A_{n+1} \to A_n$ and an R-module map $A_0 \to M$ such that the sequence

$$\ldots \longrightarrow A_{n+1} \to A_n \longrightarrow \ldots \longrightarrow A_1 \longrightarrow A_0 \longrightarrow M \longrightarrow 0$$

is exact. By abuse of notation, we often speak of "the resolution $A_\bullet$. Dually, a **right resolution** of M is an infinite sequence $\{B^i\}_{i=0}^{\infty}$ of R-modules, for all $n \in \mathbb{N}$ an R-module map $B^n \to B^{n+1}$ and an R-module map $M \to B^0$ such that the sequence

$$0 \longrightarrow M \longrightarrow B^0 \longrightarrow B^1 \longrightarrow \ldots \longrightarrow B^n \longrightarrow B^{n1} \ldots$$

is exact. We speak of "the resolution $B^\bullet$".

A **projective resolution** of M is a left resolution $A_\bullet$ such that each A_n is projective. A **injective resolution** of M is a right resolution $B^\bullet$ such that each B^n is injective. (Exactly why we are not interested in left injective resolutions and right projective resolutions will shortly become clear.)

THEOREM 3.81. *(Existence of resolutions) Let M be an R-module.*

a) *Since every R-module is the quotient of a projective (indeed, of a free) module, M admits a projective resolution.*
b) *Since every R-module can be embedded in an injective module, M admits an injective resolution.*

PROOF. a) Choose a projective module P_0, a surjection $\epsilon_0 : P_0 \to M$, and put $M_0 = \ker(\epsilon_0)$. Inductively, given M_{n-1}, we choose a projective module P_n, a surjection $\epsilon_n : P_n \to M_{n-1}$, and put $M_n = \ker(\epsilon_0)$. As our map $d_n : P_n \to P_{n-1}$ we take the composite

$$P_n \xrightarrow{\epsilon_n} M_{n-1} \xrightarrow{\ker(\epsilon_{n-1})} P_{n-1}.$$

We claim that the resulting sequence

$$\ldots \longrightarrow P_{n+1} \to P_n \longrightarrow \ldots \longrightarrow P_1 \longrightarrow P_0 \longrightarrow M \longrightarrow 0$$

is exact. It is certainly exact at M. If $x \in P_0$ and $\epsilon_0(x) = 0$, then $x_0 \in M_0$. Lifting x_0 via the surjection ϵ_1 to $x_1 \in P_1$, we find $d_1(x_1) = \epsilon_1(x_1) = x_0$, so $\ker(\epsilon_0) \subseteq \mathrm{Im}(d_1)$. Conversely, since d_1 factors through $\ker(\epsilon_0)$, it is clear that $\mathrm{Im}(d_1) \subseteq \ker(\epsilon_0)$. Exactly the same argument verifies exactness at P_n for each $n > 0$, so $P_\bullet$ is a projective resolution of M.
b) We leave the proof of this part to the reader as an exercise, with the following comforting remark: the notion of an injective module is obtained from the notion of a projective module by "reversing all the arrows", which is the same relationship

that a left resolution bears to a right resolution. Therefore it should be possible to prove part b) simply by holding up the proof of part a) to a mirror. (And it is.) □

THEOREM 3.82. *(Comparison theorem for resolutions)*

a) *Let $P_\bullet$ be a projective resolution of the R-module M. Let N be another R-module and $f_{-1} : M \to N$ be an R-module map. Then for every left resolution $A_\bullet$ of N there exists a homomorphism η from the chain complex $P_\bullet \to M \to 0$ to the chain complex $A_\bullet \to N \to 0$. Moreover η is unique up to chain homotopy.*

b) *Let $E^\bullet$ be an injective resolution of the R-module N. Let M be another R-module and $f' : M \to N$ be an R-module map. Then for every right resolution $A^\bullet$ of M there exists a homomorphism η from the chain complex $0 \to M \to A^\bullet$ to the chain complex $0 \to N \to E^\bullet$. Moreover η is unique up to chain homotopy.*

PROOF. See [**W**, Thms. 2.2.6 and 2.3.7]. □

EXERCISE 3.77. *Let F be a covariant additive functor on the category of R-modules. Let $C_\bullet$ and $D_\bullet$ be two chain complexes of R-modules and $f, g : C_\bullet \to D_\bullet$ be two homomorphisms between them.*

a) *Show: $FC_\bullet$ and $FD_\bullet$ are chain complexes and there are induced chain homomorphisms Ff, $Fg : FC_\bullet \to FD_\bullet$.*

b) *Show: if f and g are chain homotopic, so are Ff and Fg. (Suggestion: Show that it makes sense to apply F to a chain homotopy s.)*

10.4. Derived functors.

Let us consider covariant, additive functors F from the category of R-modules to itself. (Recall that additive means that for any M, N, the induced map $\mathrm{Hom}(M, N) \to \mathrm{Hom}(F(M), F(N))$ is a homomorphism of commutative groups.)

EXERCISE 3.78. *For any additive functor F and any chain complex $C_\bullet$ of R-modules, $FC_\bullet$ is again a chain complex.*
(Hint: an additive functor takes the zero homomorphism to the zero homomorphism.)

Thus if

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0$$

is a short exact sequence of R-modules, then

$$0 \longrightarrow F(M_1) \longrightarrow F(M_2) \longrightarrow F(M_3) \longrightarrow 0$$

is necessarily a *complex* of modules but not necessarily exact: it may have nonzero homology.

EXAMPLE 3.83. *For any ring R, the functor $F(M) = M \oplus M$ is exact. For $R = \mathbb{Z}$ the functor $F(M) = M \otimes \mathbb{Z}/2\mathbb{Z}$ is not exact: for instance it takes the short exact sequence*

$$0 \longrightarrow \mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z} \longrightarrow \mathbb{Z}/2\mathbb{Z} \longrightarrow 0$$

to the complex

$$0 \longrightarrow \mathbb{Z}/2\mathbb{Z} \xrightarrow{\cdot 2} \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \longrightarrow 0,$$

but multiplication by 2 on $\mathbb{Z}/2\mathbb{Z}$ is not an injection.

Although an exact functor is a thing of beauty and usefulness to all, it turns out that from a homological algebraic point of view, it is the functors which are "half exact" which are more interesting: they give rise to co/homology theories.

An additive functor F is **right exact** if for any exact sequence of the form

$$M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0,$$

the induced sequence

$$FM_1 \longrightarrow FM_2 \longrightarrow FM_3 \longrightarrow 0$$

is again exact. This much was true for the functor $F(M) = M \otimes \mathbb{Z}/2\mathbb{Z}$, at least for the sequence we chose above. In fact this holds for all tensor products.

PROPOSITION 3.84. *For any ring R and any R-module N, the functor $F(M) = M \otimes_R N$ is right exact.*

EXERCISE 3.79. *Prove Proposition 3.84*

We have also the dual notion of an additive functor F being **left exact**: for any exact sequence of the form

$$0 \to M_1 \to M_2 \to M_3,$$

the induced sequence

$$0 \to FM_1 \to FM_2 \to FM_3$$

is again exact.

We now wish to press our luck a bit by extending this definition to contravariant functors. Here a little abstraction actually makes me less confused, so I will pass it along to you: we say that a contravariant functor F from the abelian category $\mathcal{C}$ to the abelian category $\mathcal{D}$ is left exact (resp. right exact) if the associated covariant functor $F^{\text{opp}} : \mathcal{C}^{\text{opp}} \to \mathcal{D}$ is left exact (resp. right exact). Concretely, a contravariant functor F from R-modules to R-modules is **left exact** if every exact sequence of the form

$$M_1 \to M_2 \to M_3 \to 0$$

is transformed to an exact sequence

$$0 \to FM_3 \to FM_2 \to FM_1.$$

(And similarly for right exact contravariant functors.)

PROPOSITION 3.85. *Let R be a ring and X be an R-module.*

a) *The functor $M \mapsto \text{Hom}(X, M)$ is covariant and left exact. (Recall that it is exact if and only if X if projective.)*
b) *The functor $M \mapsto \text{Hom}(M, X)$ is contravariant and left exact. (Recall that it is exact if and only if X is injective.)*

EXERCISE 3.80. *Prove Proposition 3.85.*

Let F be a right exact additive functor on the category of R-modules. We will define a sequence $\{L_nF\}_{n\in\mathbb{N}}$ of functors, with $L_0F = F$, called the **left derived functors** of F. The idea here is that the left-derived functors quantify the failure of F to be exact.

Let M be an R-module. We define all the functors L^nF at once, as follows: first we choose any projective resolution $P_\bullet \to M \to 0$ of M. Second we take away the M, getting a complex $P_\bullet$ which is exact except at P_0, i.e.,

$$H_0(P) = P_0/\operatorname{Im}(P_1 \to P_0) = P_0/\operatorname{Ker}(P_0 \to M) = M,$$

$$\forall n > 0, H_n(P) = 0.$$

Third we apply the functor F getting a new complex $FP_\bullet$. And finally, we take homology of this new complex, defining

$$(L_nF)(M) \coloneqq H_n(FP_\bullet).$$

Now there is (exactly?) one thing which is relatively clear at this point.

PROPOSITION 3.86. *We have* $(L_0F)(M) = FM$.

PROOF. Since $P_1 \to P_0 \to M \to 0$ is exact and F is right exact, $FP_1 \to FP_0 \to FM \to 0$ is exact, hence

$$\operatorname{Im}(FP_1 \to FP_0) = \operatorname{Ker}(FP_0 \to FM).$$

Thus

$$\begin{aligned}(L_0F)(M) = H_0(FP_\bullet) &= \operatorname{Ker}(FP_0 \to 0)/\operatorname{Im}(FP_1 \to FP_0)\\ &= FP_0/\operatorname{Ker}(FP_0 \to FM) = FM.\end{aligned}$$

□

Before saying anything else about the left derived functors L_nF, there is an obvious point to be addressed: how do we know they are well-defined? On the face of it, they seem to depend upon the chosen projective resolution $P_\bullet$ of M, which is very far from being unique. To address this point we need to bring in the Comparison Theorem for Resolutions (Theorem 3.82). Namely, let $P'_\bullet \to M \to 0$ be any other projective resolution of M. By Theorem 3.82, there exists a homomorphism of chain complexes $\eta : P_\bullet \to P'_\bullet$ which is unique up to chain homotopy. Interchanging the roles of $P'_\bullet$ and $P_\bullet$, we get a homomorphism $\eta' : P'_\bullet \to P_\bullet$. Moreover, the composition $\eta' \circ \eta$ is a homomorphism from $P_\bullet$ to itself, so by the uniqueness $\eta' \circ \eta$ is chain homotopic to the identity map on $P_\bullet$. Similarly $\eta \circ \eta'$ is chain homotopic to the identity map on $P'_\bullet$, so that η is a chain homotopy equivalence. By Exercise 3.77, $F\eta : FP_\bullet \to FP'_\bullet$ is a chain homotopy equivalence, and therefore the induced maps on homology $H_n(F\eta) : H_n(FP_\bullet) \to H_n(FP'_\bullet)$ are isomorphisms. Thus we have shown that two different choices of projective resolutions for M lead to *canonically* isomorphic modules $(L_nF)(M)$.

EXERCISE 3.81. *Suppose M is projective. Show: for any right exact functor F and all $n > 0$, $(L_nF)(M) = 0$.*

The next important result shows that a short exact sequence of R-modules induces a long exact sequence involving the left-derived functors and certain connecting homomorphisms (which we have not defined and will not define here).

THEOREM 3.87. *Let*

$$0 \longrightarrow M_1 \longrightarrow M_2 \longrightarrow M_3 \longrightarrow 0 \tag{8}$$

be a short exact sequence of R-modules, and let F be any left exact functor on the category of R-modules. Then:

a) *There is a long exact sequence*

(9)
$$\ldots \to (L_2F)(M_3) \xrightarrow{\partial} (L_1F)(M_1) \to (L_1F)(M_2) \to (L_1F)(M_3) \xrightarrow{\partial} FM_1 \to FM_2 \to FM_3 \to 0.$$

b) *The above construction is functorial in the following sense: if* $0 \longrightarrow N_1 \longrightarrow N_2 \longrightarrow N_3 \longrightarrow 0$ *is another short exact sequence of* R*-modules and we have maps* $M_i \to N_i$ *making a "short commutative ladder", then there is an induced "long commutative latter" with top row the long exact sequence associated to the first short exact sequence and the bottom row the long exact sequence associated to the second short exact sequence.*

PROOF. See [**W**, Thm. 2.4.6]. □

Remark: One says that (9) is the **long exact homology sequence** associated to the short exact sequence (8).

Now, dually, if F is a right exact functor on the category of R-modules, we may define **right derived functors** R^nF. Namely, for an R-module M, first choose an injective resolution $0 \to M \to E^\bullet$, then take M away to get a cochain complex $E^\bullet$, then apply F to get a cochain complex $FE^\bullet$, and then finally define $(R^nF)(M) = H^n(FE^\bullet)$. In this case, a short exact sequence of modules (8) induces a **long exact cohomology sequence**

(10)
$$0 \to FM_1 \to FM_2 \to FM_3 \xrightarrow{\partial} (R^1F)(M_1) \to (R^1F)(M_2) \to (R^1F)(M_3) \xrightarrow{\partial} (R^2F)(M_1)\ldots$$

EXERCISE 3.82. *Suppose* M *is injective. Show: for any left exact functor* F *and all* $n > 0$*, we have* $(R^nF)(M) = 0$*.*

10.5. Tor.

Let M, N be R-modules, and let $F : N \to M \otimes_R N$ be the functor "tensor with M". Then F is right exact so has left derived functors (L_nF). By definition, for all $n \in \mathbb{N}$,
$$\mathrm{Tor}_n(M, N) := (L_nF)(N).$$
Now un/fortunately the situation is even a little richer than the general case of left-derived functors discussed above. Namely, the tensor product is really a **bifunctor**: i.e., a functor in M as well as in N, additive and covariant in each variable separately. So suppose we took the right-derived functors of $M \mapsto M \otimes_R N$ and applied them to M: this would give us $\mathrm{Tor}_n(N, M)$. So it is natural to ask: how does $\mathrm{Tor}_n(M, N)$ compare to $\mathrm{Tor}_n(N, M)$? Since for $n = 0$ we have that $M \otimes_R N$ is canonically isomorphic to $N \otimes_R M$, it is natural to hope that the Tor functors are symmetric. And indeed this turns out to be the case.

THEOREM 3.88. *(Balancing Tor) For any* R*-modules* M *and* N *and all* $n \geqslant 0$*, there are natural isomorphisms* $\mathrm{Tor}_n(M, N) = \mathrm{Tor}_n(N, M)$*.*

PROOF. No way. See [**W**, Thm. 2.7.2]. □

EXERCISE 3.83. *In order to use the Universal Coefficient Theorem (for homology) in algebraic topology, one needs to know the values of* $\mathrm{Tor}_1(M, N)$ *for any two finitely generated* $\mathbb{Z}$*-modules* M *and* N*.*

a) *Show that for any* $m, n \in \mathbb{Z}^+$*,* $\mathrm{Tor}_1(\mathbb{Z}/m\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/\gcd(m, n)\mathbb{Z}$*.*

b) *Show that for all $\mathbb{Z}$-modules N, $\mathrm{Tor}_1(\mathbb{Z}, N) = 0$.*
c) *Explain how the structure theorem for finitely generated $\mathbb{Z}$-modules reduces the problem of computation of $\mathrm{Tor}_1(M, N)$ for any finitely generated M and N to the two special cases done in parts a) and b).*

EXERCISE 3.84. *Show: the Tor functors commute with direct limits in the sense that for all $n \in \mathbb{N}$, any directed system $\{M_i\}_{i \in I}$ of R-modules M and any R-module N we have a canonical isomorphism*

$$\mathrm{Tor}_n(\varinjlim_i M_i, N) \to \varinjlim_i \mathrm{Tor}_n(M_i, N).$$

(Suggestion: the case $n = 0$ is Proposition 3.9. Use this to show the general case by brute force: i.e., take a projective resolution of N and track these isomorphisms through the definition of Tor_n.)

10.6. Ext.

Let M, N be R-modules, and let $F : N \to \mathrm{Hom}(M, N)$, so F is covariant and left exact. By definition, for all $n \in \mathbb{N}$,

$$\mathrm{Ext}^n(M, N) = (R^n F)(N).$$

But again, we have an embarrassment of riches: why didn't we define the Ext functors as the right-derived functors of the contravariant left exact functor $G : N \to \mathrm{Hom}(N, M)$? Again, we can do this.

THEOREM 3.89. *(Balancing Ext) Let M and N be R-modules. Define functors $F_M : N \to \mathrm{Hom}(M, N)$ and $G_N : M \to \mathrm{Hom}(M, N)$. Then for all $n \geqslant 0$,*

$$(R^n F_M)(N) = (R^n G_N)(M).$$

PROOF. No way. See [**W**, Thm. 2.7.6]. □

EXERCISE 3.85. *In order to use the Universal Coefficient Theorem (for cohomology) in algebraic topology, one needs to know the values of $\mathrm{Ext}^1(M, N)$ for any two finitely generated $\mathbb{Z}$-modules M and N. Compute them.*

THEOREM 3.90.
a) *For an R-module P, the following are equivalent:*
  (i) *P is projective.*
  (ii) *$\mathrm{Ext}^1_R(P, B) = 0$ for all R-modules B.*
b) *For an R-module E, the following are equivalent:*
  (i) *E is injective.*
  (ii) *$\mathrm{Ext}^1_R(A, E) = 0$ for all R-modules A.*

EXERCISE 3.86. *Prove Theorem 3.100.*

THEOREM 3.91.
a) *For a ring R, the following are equivalent:*
  (i) *R is hereditary.*
  (ii) *Every R-module M admits a projective resolution of the form $0 \to P_1 \to P_0 \to M \to 0$.*
  (iii) *For all R-modules M and N and all $n \geqslant 2$, we have $\mathrm{Ext}^n_R(M, N) = 0$.*
b) *The conditions of part a) imply:*
  (iv) *For all R-modules M and N and all $n \geqslant 2$, $\mathrm{Tor}^n_R(M, N) = 0$.*
c) *If R is Noetherian, then (iv) $\implies$ (i) and thus all are equivalent.*

EXERCISE 3.87. *Prove Theorem 3.101.*

THEOREM 3.92. *For R-modules A and C, the following are equivalent:*

(i) *Every short exact sequence $0 \to A \to B \twoheadrightarrow C \to 0$ splits.*
(ii) $\mathrm{Ext}^1_R(C, A) = 0$.

PROOF. See e.g. [**Ro**, Thm. 7.31]. □

11. More on flat modules

THEOREM 3.93. *(Tensorial Criterion for Flatness) For an R-module M, the following are equivalent:*

(i) *The R-module M is flat.*
(ii) *For every finitely generated ideal I of R the canonical map $I \otimes_R M \to IM$ is an isomorphism.*

PROOF. First note that the canonical map $I \otimes_R M \to IM$ is always a surjection.
(i) $\implies$ (ii): if M is flat, then since $I \hookrightarrow R$, $I \otimes_R M \hookrightarrow R \otimes_R M = M$, so $I \otimes_R M \xrightarrow{\sim} IM$.
(ii) $\implies$ (i): Every ideal of R is the direct limit of its finitely generated subideals, so it follows from Proposition 3.9 and the exactness of direct limits that $I \otimes M \to M$ is injective for *all* ideals I. Moreover, if N is an R-module and $N' \subseteq N$ is an R-submodule, then since N is the direct limit of submodule $N' + F$ with F finitely generated, to show that $N' \otimes M \to N \otimes M$ is injective we may assume

$$N = N' + \langle \omega_1, \ldots, \omega_n \rangle_R.$$

We now proceed by dévissage: putting $N_i = N' + \langle \omega_1, \ldots, \omega_i \rangle_R$, it is enough to show injectivity at each step of the chain

$$N' \otimes M \to N_1 \otimes M \to \ldots \to N \otimes M,$$

and further simplifying, it is enough to show that if $N = N' + R\omega$, then $N' \otimes M \hookrightarrow N \otimes M$. Let I be the "conductor ideal of N/N'", i.e., $I = \{x \in R \mid x\omega \in N'\}$, so that we get a short exact sequence of R-modules

$$0 \to N' \to N \to R/I \to 0$$

which gives rise to a long exact homology sequence

$$\ldots \to \mathrm{Tor}^R_1(M, R/I) \to N' \otimes M \to N \otimes M \to M/IM \to 0.$$

Thus it suffices to prove $\mathrm{Tor}^R_1(M, R/I) = 0$. For this we consider the homology sequence associated to

$$0 \to I \to R \to R/I \to 0,$$

namely

$$\ldots \to \mathrm{Tor}^R_1(M, R) = 0 \to \mathrm{Tor}^R_1(M/R/I) \to I \otimes M \to M \to \ldots,$$

and from the injectivity of $I \otimes M \to M$ we deduce $\mathrm{Tor}^R_1(M, R/I) = 0$. □

THEOREM 3.94. *(Homological Criterion for Flatness) For an R-module M, the following are equivalent:*

(i) *The R-module M is flat.*
(ii) *For every R-module N all $i > 0$, we have $\mathrm{Tor}^R_i(M, N) = 0$.*
(ii′) *For every R-module N, we have $\mathrm{Tor}^R_1(M, N) = 0$.*
(iii) *For every finitely generated ideal I of R, we have $\mathrm{Tor}^R_1(M, R/I) = 0$.*

PROOF. (i) $\implies$ (ii): This is a statement about projective resolutions, but given that it is just about the most basic possible one. Namely, let $L_\bullet \to N \to 0$ be a projective resolution of N. Then

$$\ldots \to L_n \otimes M \to L_{n-1} \otimes M \to \ldots \to L_0 \otimes M$$

is exact, so $\mathrm{Tor}_i^R(M,N) = 0$ for all $i > 0$.
(ii) $\implies$ (ii$'$) and (ii$'$) $\implies$ (iii) are both immediate.
(iii) $\implies$ (i): For each finitely generated ideal I of R, the short exat sequence

$$0 \to I \to R \to R/I \to 0$$

of R-modules induces a long exact sequence in homology, which ends

$$\ldots \to \mathrm{Tor}_1^R(M, R/I) = 0 \to I \otimes M \to M \to M/IM \to 0,$$

i.e., the map $I \otimes M \to M$ is injective and thus induces an isomorphism $I \otimes M \xrightarrow{\sim} IM$. Using the Tensorial Criterion for Flatness (Theorem 3.93), we conclude M is flat. □

COROLLARY 3.95. *(Direct limits preserve flatness) Let R be a ring and $\{M_i\}_{i \in I}$ a directed system of flat R-modules. Then $M = \varinjlim M_i$ is a flat R-module.*

PROOF. For every R-module N, we have

$$\mathrm{Tor}_1^R(\varinjlim M_i, N) \cong \mathrm{Tor}_1^R(N, \varinjlim M_i) = \varinjlim \mathrm{Tor}_1^R(N, M_i) \cong \varinjlim \mathrm{Tor}_1^R(M_i, N) = \varinjlim 0 = 0.$$

Now apply the Homological Criterion for Flatness. □

COROLLARY 3.96. *For a domain R, the following are equivalent:*

(i) *Every finitely generated torsionfree R-module is flat.*
(ii) *Every torsionfree R-module is flat.*

PROOF. Every submodule of a torsionfree R-module is torsionfree, and every R-module is the direct limit of its finitely generated submodules. So the result follows immediately from Proposition 3.95. □

COROLLARY 3.97. *Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules, with M'' flat. Then M' is flat if and only if M is flat.*

EXERCISE 3.88. *Use the Homological Criterion of Flatness to prove Corollary 3.97.*

EXERCISE 3.89. *In a short exact sequence of R-modules as in Corollary 3.97, if M' and M are flat, must M'' be flat?*

Now recall that a finitely generated torsion free module over a PID is free (Proposition 3.64). From this we deduce:

COROLLARY 3.98. *A module over a PID is flat if and only if it is torsionfree.*

EXERCISE 3.90. *Let R be a domain and M a torsion R-module. Show that for all R-modules N and all $n \geqslant 0$, $\mathrm{Tor}_n(M,N)$ is a torsion R-module.*

THEOREM 3.99. *Let R be a PID and let M, N be R-modules.*

a) *For all $n \geqslant 2$, $\mathrm{Tor}_n(M,N) = 0$.*
b) *$\mathrm{Tor}_1(M,N)$ is a torsion R-module.*

PROOF. a) Choose a free module F_0 and a surjection $d_0 : F_0 \to N$. We have that $F_1 = \mathrm{Ker}(d_0)$ is free, so we get a **finite free resolution of N**:

$$0 \to F_1 \to F_0 \to N \to 0.$$

Therefore we certainly have $\mathrm{Tor}_n(M, N)$ for all M and all $n \geqslant 2$.
b) Let $\{M_i\}_{i \in I}$ be the direct system of all finitely generated submodules of M. As above, we have $M = \varinjlim M_i$, so

$$\mathrm{Tor}_1(M, N) = \mathrm{Tor}_1(\varinjlim M_i, N)) = \varinjlim \mathrm{Tor}_1(M_i, N).$$

By Corollary 3.98, each M_i which is torsionfree is flat, hence $\mathrm{Tor}_1(M_i, N) = 0$. Thus the only possible contribution to $\varinjlim \mathrm{Tor}_1(M_i, N)$ comes from torsion modules M_i, and by Exercise 3.90, M_i torsion implies $\mathrm{Tor}_1(M_i, N)$ torsion. Thus $\mathrm{Tor}_1(M, N)$ is a direct limit of torsion modules, hence itself a torsion module. □

THEOREM 3.100. *(Equational Criterion for Flatness) Let M be an R-module.*

a) *Suppose M is flat, and that we are given $r, n \in \mathbb{Z}^+$, a matrix $A = (a_{ij}) \in M_{r \times n}(R)$ and elements $x_1, \ldots, x_n \in M$ such that*

$$\forall 1 \leqslant i \leqslant r, \ \sum_j a_{ij} x_j = 0.$$

Then there are $s \in \mathbb{Z}^+$, $b_{jk} \in R$ and $y_k \in M$ (for $1 \leqslant j \leqslant n$ and $1 \leqslant k \leqslant s$) such that

$$\forall i, k, \ \sum_j a_{ij} b_{jk} = 0$$

and

$$\forall j, \ x_j = \sum_j b_{jk} y_k.$$

Thus the solutions in a flat module of a system of linear equations with R-coefficients can be expressed as a linear combination of solutions of the system in R.

b) *Conversely, if the above conditions hold for a single equation (i.e., with $r = 1$), then M is a flat R-module.*

PROOF. a) Let $\varphi : R^n \to R^r$ be the linear map corresponding to multiplication by the matrix A and let $\varphi_M : M^n \to M^r$ be the same for M, so that $\varphi_M = \varphi \otimes 1_M$. Let $K = \mathrm{Ker}\, \varphi$. Since M is flat, tensoring with M preserves exact sequences, thus the sequence

$$K \otimes_R M \overset{\iota \otimes 1}{\to} M^n \overset{\varphi}{\to} M^r$$

is exact. By our hypothesis we have $\varphi_M(x_1, \ldots, x_n) = 0$, so that we may write

$$(x_1, \ldots, x_n) = (\iota \otimes 1) \left(\sum_{k=1}^{s} \beta_k \otimes y_k \right)$$

with $\beta_k \in K$ and $y_k \in M$. Writing out each β_k as an element $(b_{1k}, \ldots, b_{nk}) \in R^n$ gives the desired conclusion.
b) We will use the Tensorial Criterion for Flatness to show that M is flat. Let $I = \langle a_1, \ldots, a_n \rangle$ be a finitely generated ideal of R. We may write an arbitrary element z of $I \otimes M$ as $\sum_{i=1}^n a_i \otimes m_i$ with $m_i \in M$. Let $\overline{z} = \sum_{i=1}^n a_i m_i$ denote the image of z in $IM \subseteq M$. We want to show that $\overline{z} = 0$ implies $z = 0$, so suppose

that $\sum_i a_i m_i = 0$. By hypothesis, there exist $b_{ij} \in R$ and $y_j \in M$ such that for all j, $\sum_i a_i b_{ij} = 0$ and for all i, $m_i = \sum_j b_{ij} y_j$. Thus

$$z = \sum_i a_i \otimes m_i = \sum_i \sum_j a_i b_{ij} \otimes y_j = \sum_j \left(\sum_i a_i b_{ij} \right) \otimes y_j = \sum_j 0 \otimes y_j = 0.$$

□

As an application, we can now improve Theorem 3.54 by weakening the hypothesis of "finite presentation" to the simpler one of "finite generation".

THEOREM 3.101. *Let M be a* finitely generated *flat module over the local ring $(R, \mathfrak{m})$. Then for all $n \in \mathbb{Z}^+$, $x_1, \ldots, x_n$ are elements of M such that the images in $R/\mathfrak{m}$ are $R/\mathfrak{m}$-linearly independent, then $x_1, \ldots, x_n$ are R-linearly independent.*

PROOF. We go by induction on n. Suppose first that $n = 1$, in which case it is sufficient to show that $a_1 \in R$, $a_1 x_1 \neq 0$ implies $a_1 = 0$. By the Equational Criterion for Flatness, there exist $b_1, \ldots, b_s \in R$ such that $ab_i = 0$ for all i and $x_1 \in \sum_i b_i M$. By assumption, x_1 does not lie in $\mathfrak{m}M$, so that for some i we must have $b_i \in R^\times$, and then $ab_i = 0$ implies $a = 0$.

Now suppose $n > 1$, and let $a_1, \ldots, a_n \in R$ are such that $a_1 x_1 + \ldots + a_n x_n = 0$. Again using the Equational Criterion for Flatness, there are $b_{ij} \in R$ and $y_1, \ldots, y_s \in M$ such that for all j, $\sum a_i b_{ij} = 0$ and $x_i = \sum b_{ij} y_j$. Since the set of generators is minimal, by Nakayama's Lemma their images in $M/\mathfrak{m}M$ must be $R/\mathfrak{m}$-linearly independent. In particular $x_n \notin \mathfrak{m}M$, so that at least one b_{nj} is a unit. It follows that there exist $c_1, \ldots, c_{n-1} \in R$ such that $a_n = \sum_{i=1}^{n-1} a_i c_i$. Therefore

$$a_1(x_1 + c_1 x_n) + \ldots + a_{n-1}(x_{n-1} + c_{n-1} x_n) = 0.$$

The images in $M/\mathfrak{m}M$ of the $n-1$ elements $x_1 + c_1 x_n, \ldots, x_{n-1} + c_{n-1} x_n$ are $R/\mathfrak{m}$-linearly independent, so by induction $a_1 = \ldots = a_{n-1} = 0$. Thus $a_n = 0$. □

THEOREM 3.102. *For a finitely generated module M over a local ring R, the following are equivalent:*

(i) *The R-module M is free.*
(ii) *The R-module M is projective.*
(iii) *The R-module M is flat.*

PROOF. For any module over any ring we have (i) $\implies$ (ii) $\implies$ (iii). So suppose that M is a finitely generated flat module over the local ring $(R, \mathfrak{m})$. Let $(x_1, \ldots, x_n)$ be a set of R-module generators for M of minimal cardinality. By Nakayama's Lemma the images of $x_1, \ldots, x_n$ in $R/\mathfrak{m}$ are $R/\mathfrak{m}$-linearly independent, and then Theorem 3.101 implies that $x_1, \ldots, x_n$ is a basis for M as an R-module. □

A ring R is called **absolutely flat** if every R-module is flat.

EXERCISE 3.91. *Show: a quotient of an absolutely flat ring is absolutely flat.*

PROPOSITION 3.103. *For a ring R, the following are equivalent:*

(i) *The ring R is absolutely flat.*
(ii) *For every principal ideal I of R, $I^2 = I$.*
(iii) *Every finitely generated ideal of R is a direct summand of R.*

PROOF. (i) $\implies$ (ii): Assume R is absolutely flat, and let $I = (x)$ be a principal ideal. Tensoring the natural inclusion $(x) \to R$ with $R/(x)$, we get a an injection $(x) \otimes_R R/(x) \to R/(x)$. But this map sends $x \otimes r \mapsto xr + (x) = (x)$, so it is identically zero. Therefore its injectivity implies that $0 = (x) \otimes_R R/(x) \cong (x)/(x^2)$, so $(x) = (x^2)$.

(ii) $\implies$ (iii): Let $x \in R$. Then $x = ax^2$ for some $a \in R$, so putting $e = ax$ we have $e^2 = a^2x^2 = a(ax^2) = ax = e$, so e is idempotent, and $(e) = (x)$. In general, for any two idempotents e, f, we have $\langle e, f \rangle = (e + f - ef)$. Hence every finitely generated ideal is principal, generated by an idempotent element, and thus a direct summand.

(iii) $\implies$ (i): Let M be an R-module, and let I be any finitely generated ideal of R. By assumption, we may choose J such that $R = I \oplus J$. Therefore J is projective, so $\mathrm{Tor}_1(R/I, M) = \mathrm{Tor}_1(J, M) = 0$. By the Homological Criterion for Flatness, M is flat. □

EXERCISE 3.92. *Show: a (finite or infinite) product of absolutely flat rings is absolutely flat.*

The following striking result came relatively late in the game: it is due independently to Govorov [**Gov65**] and Lazard [**La64**].

THEOREM 3.104. *(Govorov-Lazard) For a module M over a ring R, the following are equivalent:*

(i) *The R-module M is flat.*
(ii) *There is a directed family $\{F_i\}_{i \in I}$ of finitely generated free submodules of M such that $M = \varinjlim F_i$.*

PROOF. (i) $\implies$ (ii): Suppose $M = \varinjlim F_i$ is a direct limit of free modules. Then in particular M is a direct limit of flat modules, so by Corollary 3.95 M is flat.
(ii) $\implies$ (i): see [**Ei**, Thm. A6.6]. □

11.1. Flat Base Change.

PROPOSITION 3.105. *(Stability of flatness under base change) Let M be a flat R-module, and $f : R \to S$ a ring homomorphism. Then $S \otimes_R M$ is a flat S-module.*

EXERCISE 3.93. *Prove Proposition 3.105.*

EXERCISE 3.94. *Show: the tensor product of flat R-modules is a flat R-module.*

EXERCISE 3.95. *Let R be a nonzero commutative ring, and $n, m \in \mathbb{N}$.*

a) *Show that $R^m \cong R^n$ if and only if $m = n$.*
b) *Suppose that $\varphi : R^m \to R^n$ is a surjective R-module map. Show that $m \geqslant n$.*
c) [12] *Suppose that $\varphi : R^m \to R^n$ is an injective R-module map. Show that $m \leqslant n$.*
d) *Find a noncommutative ring R for which part a) fails.*

THEOREM 3.106. *(Hom commutes with flat base change) Let S be a flat R-algebra and M, N R-modules with M finitely presented. Then the canonical map*

$$\Phi_M : S \otimes_R \mathrm{Hom}_R(M, N) \to \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S)$$

[12] This is actually quite challenging.

induced by $(s, f) \mapsto (m \otimes t) \mapsto f(m) \otimes st$ *is an isomorphism.*

PROOF. (Hochster) It is immediate that Φ_R is an isomorphism and that $\Phi_{M_1 \oplus M_2} = \Phi_{M_1} \oplus \Phi_{M_2}$, and thus Φ_M is an isomorphism when M is finitely generated free. For finitely presented M, there is an exact sequence

$$H \to G \to M \to 0$$

with H and G finitely generated free modules. Now we have the following commutative diagram:

$$\begin{array}{c} 0 \longrightarrow 0 \\ S \otimes_R \operatorname{Hom}_R(M, N) \xrightarrow{\theta_M} \operatorname{Hom}_S(M \otimes_R S, N \otimes_R S) \\ S \otimes_R \operatorname{Hom}_R(G, N) \xrightarrow{\theta_G} \operatorname{Hom}_S(G \otimes_R S, N \otimes_R S) \\ S \otimes_R \operatorname{Hom}_R(H, N) \xrightarrow{\theta_H} \operatorname{Hom}_S(H \otimes_R S, N \otimes_R S). \end{array}$$

The right column is obtained by first applying the exact functor $A \mapsto A \otimes_R S$ and then applying the right exact cofunctor $U \mapsto \operatorname{Hom}_S(U, N \otimes_R S)$, so it is exact. Similarly, the left column is obtained by first applying the right exact cofunctor $A \mapsto \operatorname{Hom}_R(A, N)$ and then applying the exact (since R is flat) functor $A \mapsto A \otimes_R S$, so is exact. Since G and H are finitely generated free, θ_G and θ_H are isomorphisms, and a diagram chase shows that θ_M is an isomorphism. □

12. Faithful flatness

PROPOSITION 3.107. *For an R-module M, the following are equivalent:*

(i) *For a sequence*

$$N_1 \xrightarrow{\alpha} N_2 \xrightarrow{\beta} N_3 \tag{11}$$

of left R-modules to be exact it is necessary and sufficient that

$$M \otimes_R N_1 \xrightarrow{A} M \otimes_R N_2 \xrightarrow{B} M \otimes_R N_3 \tag{12}$$

be exact.

(ii) *M is flat and for all nonzero R-modules N, we have $M \otimes_R N \neq 0$.*

(iii) *M is flat and for all nonzero R-module maps $u : N \to N'$,*

$$1_M \otimes u : M \otimes_R N \to M \otimes_R N' \text{ is not zero .}$$

(iv) *M is flat and for every $\mathfrak{m} \in \operatorname{MaxSpec} R$, $\mathfrak{m}M \subsetneq M$.*

(v) *M is flat and for every $\mathfrak{p} \in \operatorname{Spec} R$, $\mathfrak{p}M \subsetneq M$.*

A module satisfying these equivalent conditions is ***faithfully flat****.*

PROOF. (i) $\implies$ (ii): Certainly (i) implies that M is flat. Moreover, if N is a nonzero R-module such that $M \otimes N = 0$, then $0 \to N \to 0$ is not exact but its tensor product with M is exact, contradicting (i).
(ii) $\implies$ (iii): Let $I = \operatorname{Im}(u)$; then $M \otimes I = \operatorname{Im}(1_M \otimes u)$. So assuming (ii) and that $I \neq 0$, we conclude $\operatorname{Im}(1_M \otimes u) \neq 0$.
(iii) $\implies$ (i): Assume (iii). Then, since M is flat, if (11) is exact, so is (12). Conversely, suppose (12) is exact, and put $I = \operatorname{Im}(\alpha)$, $K = \ker(\beta)$. Then $B \circ A = 1_M \otimes (\beta \circ \alpha) = 0$, so $\beta \circ \alpha = 0$, or in other words, $I \subseteq K$. We may therefore form the exact sequence

$$0 \to I \to K \to K/I \to 0,$$

and tensoring with the flat module M gives an exact sequence

$$0 \to M \otimes I \to M \otimes K \to M \otimes K/I \to 0.$$

But $M \otimes K = M \otimes I$ by hypothesis, so $K/I = 0$ and $I = K$.
(ii) $\implies$ (iv): Let $\mathfrak{m} \in \operatorname{MaxSpec} R$. Then $R/\mathfrak{m}$ is a nonzero R-module, so by (ii) so is $M \otimes R/\mathfrak{m} = M/\mathfrak{m}M$, i.e., $\mathfrak{m}M \subsetneq M$.
(iv) $\implies$ (ii): Assume (iv) holds. Then, since every proper ideal is contained in a maximal ideal, we have moreover that for all proper ideals I of R, $IM \subsetneq M$, or equivalently $M \otimes (R/I) \neq 0$. But the modules of the form R/I as I ranges over all proper ideals of R are precisely all the *cyclic* (a.k.a. monogenic) R-modules, up to isomorphism. Now if N is any nonzero R-module, choose $0 \neq x \in M$ and let $N' = \langle x \rangle$ by the cyclic submodule spanned by x. It follows that $M \otimes N' \neq 0$. Since M is flat, $N' \hookrightarrow N$ implies $M \otimes N' \hookrightarrow M \otimes N$, so $M \otimes N \neq 0$.
(iv) $\iff$ (v): this follows immediately from the proofs of the last two implications, as we leave it to the reader to check. □

Exercise 3.96. *Show: (iv) $\iff$ (v) in Proposition 3.107.*

Corollary 3.108. *Let M be a faithfully flat and $u : N \to N'$ an R-module map. Then:*

a) *u is injective if and only if $1_M \otimes u : M \otimes N \to M' \otimes N$ is injective.*
b) *u is surjective if and only if $1_M \otimes u$ is surjective.*
c) *u is an isomorphism if and only if $1_M \otimes u$ is an isomorphism.*

Exercise 3.97. *Deduce Corollary 3.108 from Proposition 3.107.*

Exercise 3.98. *Use each of the criteria of Proposition 3.107 to show that the (flat) $\mathbb{Z}$-module $\mathbb{Q}$ is not faithfully flat.*

Exercise 3.99. *Show: a faithfully flat module is faithful and flat, and that – unfortunately! – a flat, faithful module need not be faithfully flat.*

Exercise 3.100. *Show: a nonzero free module is faithfully flat but that a nonzero (even finitely generated) projective module need not be.*

Exercise 3.101. *Let $\{M_i\}_{i \in I}$ be a family of flat R-modules, and put $M = \bigoplus_{i \in I} M_i$.*

a) *Suppose that for some i, M_i is faithfully flat. Show that M is faithfully flat.*
b) *Give an example where no M_i is faithfully flat yet M is faithfully flat.*

Proposition 3.109. *Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules. Suppose M' and M'' are flat and that at least one is faithfully flat. Then M is faithfully flat.*

Proof. By Proposition 3.97, M is flat. Now let N be any R-module. Since M'' is flat, $\operatorname{Tor}_1(M'', N) = 0$ so

$$0 \to M' \otimes N \to M \otimes N \to M'' \otimes N \to 0$$

is exact. Thus if $M \otimes N = 0$ then $M' \otimes N = M'' \otimes N = 0$. Since one of M', M'' is faithfully flat, by criterion (ii) of Proposition 3.107 we have $N = 0$, and then that same criterion shows that M is faithfully flat. □

By a **faithfully flat R-algebra**, we mean a ring S equipped with a ring homomorphism $R \to S$ making S into a faithfully flat R-module.

PROPOSITION 3.110. *Let $f : R \to S$ be a ring map and M an R-module. Then M is faithfully flat if and only if $M \otimes_R S$ is faithfully flat.*

PROOF. The key fact is that for any S-module N, we have

$$(M \otimes_R S) \otimes_S N \cong_R M \otimes_R N.$$

With this, the proof becomes straightforward and is left to the reader. □

EXERCISE 3.102. *Complete the proof of Proposition 3.110.*

THEOREM 3.111. *For a flat algebra $f : R \to S$, the following are equivalent:*

(i) *S is faithfully flat over R.*
(ii) *The map $f^* : \operatorname{MaxSpec} S \to \operatorname{MaxSpec} R$ is surjective.*
(iii) *The map $f^* : \operatorname{Spec} S \to \operatorname{Spec} R$ is surjective.*

PROOF. (i) $\iff$ (ii): Let $\mathfrak{m}$ be any maximal ideal of R. Then $\mathfrak{m}S \subsetneq S$ holds if and only if there is a maximal ideal $\mathcal{M}$ of S containing $\mathfrak{m}S$ if and only if $f^*(\mathcal{M}) = \mathfrak{m}$. The equivalence now follows from criterion (iv) of Proposition 3.107.
(i) $\implies$ (iii): Let $\mathfrak{p} \in \operatorname{Spec} R$, and let $k(\mathfrak{p})$ be the fraction field of the domain $R/\mathfrak{p}$. By faithful flatness, $S \otimes_R k(\mathfrak{p})$ is a nonzero $k(\mathfrak{p})$-algebra so has a prime ideal $\mathcal{P}$. Consider the composite map $h : R \xrightarrow{f} S \xrightarrow{g} S \otimes_R k(\mathfrak{p})$. We CLAIM that $g^* : \operatorname{Spec}(S \otimes_R k(\mathfrak{p})) \to \operatorname{Spec} R$ has image precisely $\{\mathfrak{p}\}$. The proof of this result, a spectral description of the **fiber of the morphism** $f : R \to S$ over $\mathfrak{p}$, will have to wait until we have developed the theory of localization in §7.3. Assuming it for now, we get that $g^*(\mathcal{P})$ is a prime ideal of $\operatorname{Spec} S$ such that $f^*g^*(\mathcal{P}) = (g \circ f)^*(\mathcal{P}) = \mathfrak{p}$, so $f^* : \operatorname{Spec} S \to \operatorname{Spec} R$ is surjective.
(iii) $\implies$ (ii): Let $\mathfrak{m} \in \operatorname{MaxSpec} R \subseteq \operatorname{Spec} R$. By assumption, the set of prime ideals $\mathcal{P}$ of S such that $f^*\mathcal{P} = \mathfrak{m}$ is nonempty. Moreover the union of any chain of prime ideals pulling back to $\mathfrak{m}$ is again a prime ideal pulling back to $\mathfrak{p}$, so by Zorn's Lemma there exists an ideal $\mathcal{M}$ which is maximal with respect to the property that $f^*\mathcal{M} = \mathfrak{m}$. Suppose $\mathcal{M}$ is not maximal and let $\mathcal{M}'$ be a maximal ideal properly containing $\mathcal{M}$. Then by construction $f^*(\mathcal{M}')$ properly contains the maximal ideal $\mathfrak{m}$ of R, i.e., $f^*(\mathcal{M})') = R$, contradicting the fact that prime ideals pull back to prime ideals. So $\mathcal{M}$ is indeed maximal in S. □

PROPOSITION 3.112. *Let $f : R \hookrightarrow S$ be a ring extension such that S is a faithfully flat R-module, and let M be an R-module. Then:*

a) *M is finitely generated if and only if $M \otimes_R S$ is finitely generated.*
b) *M is finitely presented if and only if $M \otimes_R S$ is finitely presented.*

PROOF. Note first that the properties of finite generation and finite presentation are preserved by arbitrary base change $f : R \to S$. So it suffices to prove that if $M \otimes_R S$ is finitely generated (resp. finitely presented), then M is finitely generated (resp. finitely presented).
a) Since $M \otimes_R S$ is finitely generated over S, it has a finite set of S-module generators of the form $x_i \otimes 1$. Let $N = \langle x_1, \ldots, x_n \rangle_R$ and $\iota : N \hookrightarrow M$ the canonical injection. Then $\iota_S : N \otimes_R S \to M \otimes_R S$ is an isomorphism, so by faithful flatness ι was itself an isomorphism and thus $M = \langle x_1, \ldots, x_n \rangle$ is finitely generated.
b) By part a), M is finitely generated over R, so let $u : R^n \to M$ be a surjection.

Since $M \otimes_R S$ is finitely presented, the kernel of $u_S : S^n \to M \otimes_R S$ is finitely generated over S. Since by flatness $\ker u_S = (\ker u)_S$, part a) shows that $\ker u$ is finitely generated and thus that M is finitely presented. □

LEMMA 3.113. *Let $f : R \to S$ be a ring map, and let M, N be R-modules.*

a) *There is a canonical S-module map*

$$\omega : \mathrm{Hom}_R(M, N) \otimes_R S \to \mathrm{Hom}_S(M \otimes_R S, N \otimes_R S)$$

such that for all $u \in \mathrm{Hom}_R(M, N)$, $\omega(u \otimes 1) = u \otimes 1_B$.

b) *If S is flat over R and M is finitely generated, then ω is injective.*

c) *If S is flat over R and M is finitely presented, then ω is an isomorphism.*

EXERCISE 3.103. *Prove Lemma 3.113. (It is not difficult, really, but it is somewhat technical. Feel free to consult* [**B**, p. 23] *for the details.)*

THEOREM 3.114. *(Faithfully flat descent for projective modules) Let $f : R \hookrightarrow S$ be a faithfully flat ring extension, and let P be an R-module. Then P is finitely generated and projective if and only if $P \otimes_R S$ is finitely generated and projective.*

PROOF. Begin, once again the implication P finitely generated projective implies $P \otimes_R S$ is finitely generated projective holds for any base change. So suppose $P \otimes_R S$ is finitely generated projective. Then $P \otimes_R S$ is finitely presented, so by Proposition 3.112, M is finitely presented. It remains to show that M is projective.

Let $v : M \to N$ be a surjection of R-modules. We wish to show that the natural map $\mathrm{Hom}_R(P, M) \to \mathrm{Hom}_R(P, N)$ is surjective. Because of the faithful flatness of S/R, it is sufficient to show that $\mathrm{Hom}_R(P, M) \otimes_R S \to \mathrm{Hom}_R(P, N) \otimes_R S$ is surjective, and by Lemma 3.113 this holds if and only if

$$\mathrm{Hom}_S(P \otimes_R S, M \otimes_R S) \to \mathrm{Hom}_S(P \otimes_R S, N \otimes_R S)$$

is surjective. But this latter map is surjective because $M \otimes_R S \to N \otimes_R S$ is surjective and the S-module $P \otimes_R S$ is projective by assumption. □

CHAPTER 4

First Properties of Ideals in a Commutative Ring

1. Introducing maximal and prime ideals

Consider again the set $\mathcal{I}(R)$ of all ideals of R, partially ordered by inclusion. The maximal element is the ideal R itself, and the minimal element is the ideal (0).

In general our attitude to the ideal R of R is as follows: although we must grudgingly admit its existence – otherwise, given a subset S of R it would be in general a difficult question to tell whether the ideal $\langle S \rangle$ generated by S "exists" (i.e., is proper) or not – nevertheless we regard it as exceptional and try to ignore it as much as possible. Because of this we define an ideal I of R to be **maximal** if it is maximal among all *proper* ideals of R, i.e., $I \subsetneq R$ and there does not exist J such that $I \subsetneq J \subsetneq R$. That this is a more interesting concept than the literally maximal ideal R of R is indicated by the following result.

PROPOSITION 4.1. *For an ideal I of R, the following are equivalent:*

(i) *The ideal I is maximal.*
(ii) *The quotient ring R/I is a field.*

PROOF. Indeed, R/I is a field if and only if it has precisely two ideals, I and R, which by the Correspondence Theorem says precisely that there is no proper ideal strictly containing I. □

EXAMPLE 4.2. *In $R = \mathbb{Z}$, the maximal ideals are those of the form (p) for p a prime number. The quotient $\mathbb{Z}/p\mathbb{Z}$ is the finite field of order p.*

Does every ring have a maximal ideal? With a single (trivial) exception, the answer is yes, assuming – as we must, in order to develop the theory as it is used in other branches of mathematics – suitable transfinite tools.

PROPOSITION 4.3. *Let R be a nonzero ring and I a proper ideal of R. Then there exists a maximal ideal of R containing I.*

PROOF. Consider the set S of all proper ideals of R containing I, partially ordered by inclusion. Since $I \in S$, S is nonempty. Moreover the union of a chain of ideals is an ideal, and the union of a chain of proper ideals is proper (for if 1 were in the union, it would have to lie in one of the ideals of the chain). Therefore by Zorn's Lemma we are entitled to a maximal element of S, which is indeed a maximal ideal of R that contains I. □

COROLLARY 4.4. *A nonzero ring R contains at least one maximal ideal.*

PROOF. Apply Proposition 4.3 with $I = (0)$. □

Remark: The zero ring has the disquieting property of having no maximal ideals.

Remark: The appeal to Zorn's Lemma cannot be avoided, in the sense that Corollary 4.4 implies the Axiom of Choice (AC). In fact, W. Hodges has shown that the axioms of ZF set theory together with the statement that every UFD (see §15) has a maximal ideal already implies AC [**Ho79**].

A proper ideal I of a ring R is **prime** if $xy \in I$ implies $x \in I$ or $y \in I$.

EXERCISE 4.1. *Let $\mathfrak{p}$ be a prime ideal of R.*

a) *Suppose $x_1, \ldots, x_n$ are elements of R such that $x_1 \cdots x_n \in \mathfrak{p}$. Then $x_i \in \mathfrak{p}$ for some at least one i.*
b) *In particular, for $x \in R$ and $n \in \mathbb{Z}^+$ we have $x^n \in \mathfrak{p}$, then $x \in \mathfrak{p}$.*

PROPOSITION 4.5. *Let $f : R \to S$ be a homomorphism of rings, and let J be an ideal of S.*

a) *Put $f^*(J) := f^{-1}(J) = \{x \in R \mid f(x) \in J\}$. Then $f^*(J)$ is an ideal of R.*
b) *If J is a prime ideal, so is $f^*(J)$.*

EXERCISE 4.2. *Prove Proposition 4.5.*

PROPOSITION 4.6. *For a commutative ring R, the following are equivalent:*

(i) *If $x, y \in R$ are such that $xy = 0$, then $x = 0$ or $y = 0$.*
(ii) *If $0 \neq x \in R$ and $y, z \in R$ are such that $xy = xz$, then $y = z$.*

*A nontrivial ring satisfying either of these two properties is called a **domain**.*

PROOF. Assume (i), and consider $xy = xz$ with $x \neq 0$. We have $x(y - z) = 0$, and since $x \neq 0$, (i) implies $y - z = 0$, i.e., $y = z$. Assuming (ii) suppose $xy = 0$ with $x \neq 0$. Then $xy = 0 = x \cdot 0$, so applying cancellation we get $y = 0$. □

A **zero-divisor** in a ring R is an element x such that there exists $0 \neq y \in R$ with $xy = 0$. In particular, in any nontrivial ring the element 0 *is* a zero-divisor. Thus a domain is a nontrivial ring in which 0 is the only zero-divisor.[1] Property (ii) makes sense in any commutative monoid and is called **cancellation**.

EXERCISE 4.3. *Let R be a ring, and let $x, y \in R$ be zero-divisors. Show: xy is a zero-divisor.*

The following result of Ganesan [**Ga64**, Thm. I] is easy to prove but is somewhat surprising.

THEOREM 4.7 (Ganesan). *Let R be a ring having exactly n zero-divisors for some integer $n \geqslant 2$. Then $\#R \leqslant n^2$. In particular, a ring that is not a domain and has only finitely many zero-divisors must be finite.*

PROOF. Let $z \in R^\bullet$ be a zero-divisor of R. Then the map

$$\varphi : R \to R, x \mapsto xz$$

is an endomorphism of the additive group $(R, +)$ for which every element of both the kernel and image is a zero-divisor. Since for every group homomorphism f :

[1]It is a common convention to exclude zero from being a zero-divisor. With this convention, one can say that a domain is a nontrivial ring without zero-divisors, which is a little cleaner than "a domain is a nontrivial ring in which 0 is the only zero-divisor." However, in the further study of zero-divisors, we think our convention establishes itself as being the better one.

$G \to H$, partitioning G into the set of cosets of its kernel gives the cardinal equality $\#G = (\#\operatorname{Ker} f) \cdot (\#f(G))$, the reuslt follows. □

PROPOSITION 4.8. *For an ideal I in a ring R, the following are equivalent:*

(i) *The ideal I is prime.*
(ii) *The quotient ring R/I is a domain.*

EXERCISE 4.4. *Prove Proposition 4.8.*

COROLLARY 4.9. *A maximal ideal is prime.*

PROOF. If I is maximal, R/I is a field, hence a domain, so I is prime. □

Corollary 4.9 is the first instance of a somewhat mysterious meta-principle in ideal theory: for some property P of ideals in a ring, it is very often the case that an ideal which is maximal with respect to the satisfaction of property P (i.e., is not strictly contained in any other ideal satisfying P) must be prime. In the above, we saw this with P = "proper". Here is another instance:

PROPOSITION 4.10. *(Multiplicative Avoidance) Let R be a ring and $S \subseteq R$. Suppose: 1 is in S; 0 is not in S; and S is closed under multiplication: $S \cdot S \subseteq S$. Let $\mathcal{I}_S$ be the set of ideals of R which are disjoint from S. Then:*

a) *The set $\mathcal{I}_S$ is nonempty.*
b) *Every element of $\mathcal{I}_S$ is contained in a maximal element of $\mathcal{I}_S$.*
c) *Every maximal element of $\mathcal{I}_S$ is prime.*

PROOF. a) $(0) \in \mathcal{I}_S$. b) Let $I \in \mathcal{I}_S$. Consider the subset P_I of $\mathcal{I}_S$ consisting of ideals which contain I. Since $I \in P_I$, P_I is nonempty; moreover, any chain in P_I has an upper bound, namely the union of all of its elements. Therefore by Zorn's Lemma, P_I has a maximal element, which is clearly also a maximal element of $\mathcal{I}_S$. c) Let I be a maximal element of $\mathcal{I}_S$; suppose that $x, y \in R$ are such that $xy \in I$. If x is not in I, then $\langle I, x\rangle \supsetneq I$ and therefore contains an element s_1 of S, say

$$s_1 = i_1 + ax.$$

Similarly, if y is not in I, then we get an element s_2 of S of the form

$$s_2 = i_2 + by.$$

But then

$$s_1 s_2 = i_1 i_2 + (by) i_1 + (ax) i_2 + (ab) xy \in I \cap S,$$

a contradiction. □

In fact Corollary 4.9 is precisely the special case $S = \{1\}$ of Proposition 4.10.

If I and J are ideals of R, we define the **product** IJ to be the ideal generated by all elements of the form xy with $x \in I, y \in J$. Every element of IJ is of the form $\sum_{i=1}^n x_i y_i$ with $x_1, \ldots, x_n \in I,\ y_1, \ldots, y_n \in J$.

The following simple result will be used many times in the sequel.

PROPOSITION 4.11. *Let $\mathfrak{p}$ be a prime ideal and $I_1, \ldots, I_n$ be ideals of a ring R. If $\mathfrak{p} \supset I_1 \cdots I_n$, then $\mathfrak{p} \supset I_i$ for at least one i.*

PROOF. An easy induction argument reduces us to the case of $n = 2$. So suppose for a contradiction that $\mathfrak{p} \supset I_1 I_2$ but there exists $x \in I_1 \backslash \mathfrak{p}$ and $y \in I_2 \backslash \mathfrak{p}$. Then $xy \in I_1 I_2 \subseteq \mathfrak{p}$; since $\mathfrak{p}$ is prime we must have $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$, contradiction. □

EXERCISE 4.5. *Show: Proposition 4.11 characterizes prime ideals, in the sense that if $\mathfrak{p}$ is any ideal such that for all ideals I, J of R, $\mathfrak{p} \subseteq IJ$ implies $\mathfrak{p} \subseteq I$ or $\mathfrak{p} \subseteq JJ$, then $\mathfrak{p}$ is a prime ideal.*

For an ideal I and $n \in \mathbb{Z}^+$, we denote the n-fold product of I with itself by I^n.

COROLLARY 4.12. *If $\mathfrak{p}, I$ are ideals and $\mathfrak{p}$ is prime, then $\mathfrak{p} \supset I^n \implies \mathfrak{p} \supset I$.*

2. Radicals

An element x of a ring R is **nilpotent** if $x^n = 0$ for some $n \in \mathbb{Z}^+$. Obviously 0 is a nilpotent element; a ring in which 0 is the only nilpotent element is called **reduced**. An ideal I of R is **nil** if every element of I is nilpotent. An ideal I is **nilpotent** if there exists $n \in \mathbb{Z}^+$ such that $I^n = (0)$.

PROPOSITION 4.13. *Let I be an ideal of a ring R.*

a) *If I is nilpotent, then I is a nil ideal.*
b) *If I is finitely generated and nil, then I is nilpotent.*

PROOF. Part a) is immediate from the definition.

Suppose $I = \langle a_1, \ldots, a_n \rangle_R$. Since I is nil, for each i, $1 \leqslant i \leqslant r$, there exists n_i such that $a_i^{n_i} = 0$. Let $N = n_1 + \ldots + n_r$. We claim $I^N = 0$. Indeed, an arbitrary element of I is of the form $x_1 a_1 + \ldots + x_n a_n$. Raising this element to the nth power yields a sum of monomials of the form $x_1^{j_1} \cdots x_r^{j_r} a_1^{j_1} \cdots a_r^{j_r}$, where $\sum_{i=1}^r j_i = N$. If we had for all i that $j_i < n_i$, then certainly $j_1 + \ldots + j_r < N$. So for at least one i we have $j_i \geqslant n_i$ and thus $x_i^{j_i} = 0$; so every monomial term equals zero. □

EXERCISE 4.6. *The bound on the nilpotency index of $\langle a_1, \ldots, a_n \rangle$ we gave in the preceding argument is a bit lazy: we can do better.*

a) *Let $a_1, \ldots, a_r$ be elements of a ring and let $n_1, \ldots, n_r \in \mathbb{Z}^+$ be such that $a_1^{n_1} = \ldots = a_r^{n_r} = 0$. Show:*
$$\langle a_1, \ldots, a_r \rangle^{n_1 + \ldots + n_r - (r-1)} = (0).$$
b) *Show that the bound of part a)* is *best possible for all positive integers $r, n_1, \ldots, n_r$.*
(Suggestion: for a field k, consider $k[t_1, \ldots, t_r]/\langle t_1^{n_1}, \ldots, t_r^{n_r} \rangle$.)

EXERCISE 4.7. *Find a ring R and an ideal I of R which is nil but not nilpotent.*

The **nilradical** $\mathcal{N}$ of R is the set of all nilpotent elements of R.

PROPOSITION 4.14. *Let R be a ring.*

a) *The nilradical $\mathcal{N}$ is a nil ideal of R.*
b) *The quotient $R/\mathcal{N}$ is reduced.*
c) *The map $q : R \to R/\mathcal{N}$ is* universal *for maps from R into a reduced ring.*
d) *The nilradical is the intersection of all prime ideals of R.*

PROOF. a) It suffices to show that $\mathcal{N}$ is an ideal. The only part of this that is not absolutely immediate is closure under addition. But by Proposition 4.13 the ideal generated by two nilpotent elements is nilpotent, hence nil, hence consists of

nilpotent elements, so in particular the sum of two nilpotent elements is nilpotent.
b) Let $r + \mathcal{N}$ be a nilpotent element of $R/\mathcal{N}$, so there exists $n \in \mathbb{Z}^+$ such that $r^n \in \mathcal{N}$. But this means there exists $m \in \mathbb{Z}^+$ such that $0 = (r^n)^m = r^{nm}$, and thus r itself is a nilpotent element.
c) In plainer terms: if S is a reduced ring and $f : R \to S$ is a ring homomorphism, then there exists a unique homomorphism $\overline{f} : R/\mathcal{N} \to S$ such that $f = \overline{f} \circ q$. Given this, the proof is straightforward, and we leave it to the reader.
d) Suppose x is a nilpotent element of R, i.e., $\exists n \in \mathbb{Z}^+$ such that $x^n = 0$. If $\mathfrak{p}$ is a prime ideal, then since $0 = x \cdots x \in \mathfrak{p}$, we conclude $x \in \mathfrak{p}$: this shows $\mathcal{N} \subseteq \bigcap \mathfrak{p}$. Conversely, suppose x is not nilpotent. Then the set $S_x := \{x^n \mid n \in \mathbb{N}\}$ satisfies (i) and (ii) of Proposition 5.26, so we may apply that result to get a prime ideal $\mathfrak{p}$ which is disjoint from S_x, hence not containing x. □

EXERCISE 4.8. *Prove Proposition 4.14c).*

EXERCISE 4.9. *Let $f : R \to T$ be a ring homomorphism. Show:*

$$f_*(\operatorname{nil} R) \subseteq \operatorname{nil} T.$$

For a ring R, what are the units in the polynomial ring $R[t]$? If R is a domain, then the leading coefficient of any nonzero polynomial is nonzero hence not a zero-divisor. This implies that for nonzero $f, g \in R[t]$ we have $\deg(fg) = \deg(f) + \deg(g)$, from which it follows that every unit has degree zero, i.e., is a constant polynomial and then that $R[t]^\times = R^\times$. The following result treats the general case by reduction to this case.

PROPOSITION 4.15. *Let R be a nonzero ring, and let $R[t]$ be the polynomial ring over R. Let f be a nonzero element of $R[t]$ and write*

$$f = a_n t^n + \ldots + a_1 t + a_0, \ a_n \neq 0.$$

Then $f \in R[t]^\times$ if and only if $a_0 \in R^\times$ and for all $1 \leqslant i \leqslant n$ we have $a_i \in \operatorname{nil} R$.

PROOF. Put $g := a_n t^n + \ldots + a_1 t$.

First suppose that $a_0 \in R^\times$ and $a_i \in \operatorname{nil} R$ for all $1 \leqslant i \leqslant n$. Then is g nilpotent by Exercise 4.9, so $f = g + a_0$ is the sum of a nilpotent element and a unit. If $\mathfrak{m}$ is any maximal ideal of $R[t]$ then if $f \in \mathfrak{m}$ then $a_0 = f - g \in \mathfrak{m}$, contradiction. So f lies in no maximal ideal, hence is a unit of $R[t]$.

Now suppose that $f \in R[t]^\times$. For a prime ideal $\mathfrak{p}$ of R, let

$$q_\mathfrak{p} : R[t] \to R[t]/(\mathfrak{p}R[t]) \cong (R/\mathfrak{p})[t]$$

be the quotient map. Then $q_\mathfrak{p}(f)$ is a unit in $(R/\mathfrak{p})[t]$, which implies that $a_i \in \mathfrak{p}$ for all $1 \leqslant i \leqslant n$. Since this holds for all prime ideals $\mathfrak{p}$ we have $a_i \in \operatorname{nil} R$. Moreover $q_\mathfrak{p}(a_0) \in (R/\mathfrak{p})^\times$, hence $a_0 \notin \mathfrak{p}$. As above, this means that a_0 lies in no maximal ideal, hence $a_0 \in R^\times$. □

PROPOSITION 4.16. *(Lifting Idempotents Modulo a Nil Ideal) Let R be a ring, let N be a nil ideal of R, and let $\overline{e} = \overline{e}^2$ be an idempotent element of R/N. Then there is a unique idempotent e of R such that $e \pmod N = \overline{e}$.*

PROOF. (Jacobson [**J2**, Prop. 7.14])
Step 1: We will prove the existence of e.[2] First let $x \in R$ be such that $x \pmod N =$

[2]This step holds for not-necessarily-commutative rings.

$\overline{e}$. Then $z = x - x^2$ is nilpotent: there is $n \in \mathbb{Z}^+$ such that $z^n = 0$. Put $y = 1 - x$. Then

$$0 = z^n = (x(1-x))^n = x^n y^n,$$

so

$$1 = 1^{2n-1} = (x+y)^{2n-1} = e + f,$$

where e is a sum of terms $x^i y^{2n-1-i}$ with $n \leqslant i \leqslant 2n-1$ and f is a sum of the terms $x^i y^{2n-1-i}$ with $0 \leqslant i \leqslant n-1$. Since $x^n y^n = 0$, any term in e annihilates any term in f. Hence $ef = 0 = fe$. Since $e + f = 1$, we have

$$e = e(e+f) = e^2 + ef = e^2, \ f = (e+f)f = ef + f^2 = f^2.$$

Every term in e except x^{2n-1} contains the factor $xy = z$, so $x^{2n-1} \equiv e \pmod{N}$. Since $x \equiv x^2 \equiv x^3 \equiv \ldots \equiv x^{2n-1} \pmod{N}$, we have $e \equiv x \equiv \overline{e} \pmod{N}$.

Step 2: Let $e, z \in R$ with e idempotent, z nilpotent and $e + z$ idempotent. Then

$$e + z = (e+z)^2 = e^2 + 2ez + z^2 = e + 2ez + z^2$$

so

$$z^2 = (1 - 2e)z.$$

It follows that

$$z^3 = (1-2e)z^2 = (1-2e)^2 z = (1 - 4e + 4e^2)z = (1 - 4e + 4e)z = z$$

and thus

$$z^{2k+1} = z \ \forall k \in \mathbb{Z}^+.$$

Since z is nilpotent, it follows that $z = 0$. □

An ideal I of a ring R is **radical** if for all $x \in R$, $n \in \mathbb{Z}^+$, $x^n \in I$ implies $x \in I$.

EXERCISE 4.10. a) *Show: a prime ideal is radical.*
b) *Exhibit a radical ideal that is not prime.*
c) *Find all radical ideals in $R = \mathbb{Z}$.*
d) *Show: R is reduced if and only if (0) is a radical ideal.*
e) *Let $\{I_i\}$ be a set of radical ideals in a ring R. Show $I = \bigcap_i I_i$ is a radical ideal.*

EXERCISE 4.11. *Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be prime ideals of a ring R. By Exercise 4.10, we have $\mathfrak{p}_1 \cap \mathfrak{p}_2$ is a radical ideal.*
a) *Show: if $\mathfrak{p}_1 + \mathfrak{p}_2 = R$ then $\mathfrak{p}_1\mathfrak{p}_2$ is radical.*
b) *Give an example in which $\mathfrak{p}_1 \neq \mathfrak{p}_2$ and $\mathfrak{p}_1\mathfrak{p}_2$ is not radical.*

For any ideal I of R, we define the **radical** of I:

$$r(I) = \{x \in R \mid \exists n \in \mathbb{Z}^+ \ x^n \in I\}.$$

PROPOSITION 4.17. *Let R be a commutative ring and I, J ideals of R.*
a) *$r(I)$ is the intersection of all prime ideals containing I, and is a radical ideal.*
b) *(i) $I \subseteq r(I)$; (ii) $r(r(I)) = r(I)$; (iii) $I \subseteq J \implies r(I) \subseteq r(J)$.*
c) *$r(IJ) = r(I \cap J) = r(I) \cap r(J)$.*
d) *$r(I + J) = r(r(I) + r(J))$.*
e) *$r(I) = R \iff I = R$.*
f) *For all $n \in \mathbb{Z}^+$, $r(I^n) = r(I)$.*
g) *If J is finitely generated and $r(I) \supset J$, then there is $n \in \mathbb{Z}^+$ such that $I \supset J^n$.*

PROOF. Under the canonical homomorphism $q : R \to R/I$, $r(I) = q^{-1}(\mathcal{N}(R/I))$. By Proposition 4.5a), $r(I)$ is an ideal.
a) Since $\mathcal{N}$ is the intersection of all prime ideals of R/I, $r(I)$ is the intersection of all prime ideals containing I, which is, by Exericse 4.10e), a radical ideal.
b) (i) is immediate from the definition, and (ii) and (iii) follow from the characterization of $r(I)$ as the intersection of all radical ideals containing I.
c) Since $IJ \subseteq I \cap J$, $r(IJ) \subseteq r(I \cap J)$. If $x^n \in I \cap J$, then $x^{2n} = x^n x^n \in IJ$, so $x \in r(IJ)$; therefore $r(IJ) = r(I \cap J)$. Since $I \cap J$ is a subset of both I and J, $r(I \cap J) \subseteq r(I) \cap r(J)$. Conversely, if $x \in r(I) \cap r(J)$, then there exist m and n such that $x^m \in I$ and $x^n \in J$, so $x^{mn} \in I \cap J$ and $x \in r(I \cap J)$.
d) Since $I + J \subseteq r(I) + r(J)$, $r(I + J) \subseteq r(r(I) + r(J))$. A general element of $r(I)+r(J)$ is of the form $x+y$, where $x^m \in I$ and $y^n \in J$. Then $(x+y)^{m+n} \in I+J$, so $x + y \in r(I + J)$.
e) Evidently $r(R) = R$. Conversely, if $r(I) = R$, then there exists $n \in \mathbb{Z}^+$ such that $1 = 1^n \in I$.
f) By part a), $r(I^n)$ is the intersection of all prime ideals $\mathfrak{p} \supset I^n$. But by Corollary 4.12, a prime contains I^n if and only if it contains I, so $r(I^n) = r(I)$.
g) Replacing R with R/I we may assume $I = 0$. Then J is a finitely generated nil ideal, so it is nilpotent. □

Remark: Proposition 4.17b) asserts that the mapping $I \mapsto r(I)$ is a **closure operator** on the lattice $\mathcal{I}(R)$ of ideals of R.

An ideal $\mathfrak{p}$ of a ring R is **primary** if every zero divisor of $R/\mathfrak{p}$ is nilpotent. Equivalently, $xy \in \mathfrak{p}$, $x \notin \mathfrak{p} \implies y^n \in \mathfrak{p}$ for some $n \in \mathbb{Z}^+$. More on primary ideals in §10.3.

We also define the **Jacobson radical** $J(R)$ as the intersection of all maximal ideals of R. Evidently we have $\mathcal{N} \subseteq J(R)$.

PROPOSITION 4.18. *Let R be a ring. An element x of R lies in the Jacobson radical $J(R)$ if and only if $1 - xy \in R^\times$ for all $y \in R$.*

PROOF. Suppose x lies in every maximal ideal of R. If there is y such that $1 - xy \notin R^\times$, then $1 - xy$ lies in some maximal ideal $\mathfrak{m}$, and then $x \in \mathfrak{m}$ implies $xy \in \mathfrak{m}$ and then $1 = (1 - xy) + xy \in \mathfrak{m}$, a contradiction. Conversely, suppose that there is a maximal ideal $\mathfrak{m}$ of R which does not contain x. Then $\langle \mathfrak{m}, x \rangle = R$, so $1 = m + xy$ for some $m \in \mathfrak{m}$ and $y \in R$, and thus $1 - xy$ is not a unit. □

PROPOSITION 4.19. *Let J be an ideal of R contained in the Jacobson radical, and let $\varphi : R \to R/J$ be the natural map.*

a) *For all $x \in R$, we have $x \in R^\times \iff \varphi(x) \in (R/J)^\times$: φ is **unit-faithful**.*
b) *The map $\varphi^\times : R^\times \to (R/J)^\times$ is surjective.*

PROOF. a) For any homomorphism of rings $\varphi : R \to S$, if $x \in R^\times$ then there is $y \in R$ with $xy = 1$, so $1 = \varphi(1) = \varphi(xy) = \varphi(x)\varphi(y)$, and thus $\varphi(x) \in S^\times$. For the converse we assume $S = R/J$ and let $x \in R$ be such that $\varphi(x) \in (R/J)^\times$. Then there is $y \in R$ such that $xy-1 \in J$. Thus for each maximal ideal $\mathfrak{m}$ of R, $xy-1 \in \mathfrak{m}$. It follows that $x \notin \mathfrak{m}$, for otherwise $xy \in \mathfrak{m}$ and thus $1 = xy - (xy - 1) \in \mathfrak{m}$. So x is not contained in any maximal ideal and thus $x \in R^\times$.
b) This is immediate from part a): in fact we've shown that *every* preimage under φ of a unit in R/J is a unit in R. □

EXERCISE 4.12. *For a ring R, let $\iota : R \hookrightarrow R[t]$ be the inclusion into the polynomial ring $R[t]$.*

a) *Show:*

$$J(R[t]) = \iota_*(\operatorname{nil} R).$$

b) *Thus $J(R[t]) = (0)$ if R is a domain. Give a simpler direct proof of this.*

Remark: It is not yet clear why we have defined these two different notions of "radical." Neither is it so easy to explain in advance, but nevertheless let us make a few remarks. First, the Jacobson radical plays a very important role in the theory of noncommutative rings, especially that of finite dimensional algebras over a field. (Indeed, a finite dimensional k-algebra is semisimple – i.e., a direct product of algebras without nontrivial two-sided ideals – if and only if its Jacobson radical is zero. In the special case of commutative algebras this comes down to the simpler result that a finite dimensional commutative k-algebra is reduced if and only if it is a product of fields.) One important place in commutative algebra in which the Jacobson radical $J(R)$ appears – albeit not by name, because of the necessity of putting the results in a fixed linear order – is in the statement of Nakayama's Lemma. In general, the defining condition of $\operatorname{nil}(R)$ – i.e., as the intersection of all prime ideals of R – together with the fact that the radical of an arbitrary ideal I corresponds to the nilradical of R/I, makes the nilradical more widely useful in commutative algebra (or so it seems to the author of these notes). It is also important to consider when the nil and Jacobson radicals of a ring coincide. A ring R for which every homomorphic image S has $\operatorname{nil}(S) = J(S)$ is called a **Jacobson ring**; such rings will be studied in detail in §12.

3. Comaximal ideals

Two ideals I and J in a ring R are **comaximal** if $I + J = R$. A family of ideals in R is **pairwise comaximal** if any two members of the family are comaximal.

EXERCISE 4.13. *Let $I_1, \ldots, I_n$ be pairwise comaximal. Show: $\sum_{j=1}^n \prod_{i \neq j} I_i = R$.*

PROPOSITION 4.20. *Let I and J be ideals in R. If $r(I)$ and $r(J)$ are comaximal, so are I and J.*

PROOF. Apply Proposition 4.17d) and 4.17e) to $r(I) + r(J) = R$:

$$R = r(r(I) + r(J)) = r(I + J) = I + J. \qquad \square$$

An immediate corollary of Proposition 4.20 is that if $\{I_i\}$ are pairwise comaximal and $\{n_i\}$ are any positive integers, then $\{I_i^{n_i}\}$ are pairwise comaximal.

LEMMA 4.21. *Let $K_1, \ldots, K_n$ be pairwise comaximal ideals in the ring R. Then $K_1 \cdots K_n = \bigcap_{i=1}^n K_i$.*

PROOF. We go by induction on n: $n = 1$ is trivial and $n = 2$ is Lemma 3.17b). Suppose the theorem is true for any family of $n-1$ pairwise comaximal ideals. Let $K' = \bigcap_{i=2}^n K_i$; by induction, $K' = K_2 \cdots K_n$. By Lemma 3.17c), $K_1 + K' = R$, so by the $n = 2$ case $\bigcap_{i=1}^n K_i = K_1 \cap K' = K_1 K' = K_1 \cdots K_n$. $\square$

THEOREM 4.22. *(Chinese Remainder Theorem, or "CRT") Let R be a ring and $I_1, \ldots, I_n$ a finite set of pairwise comaximal ideals. Consider the natural map*

$$\Phi : R \to \prod_{i=1}^{n} R/I_i,$$

$x \mapsto (x + I_i)_{i=1}^n$. Then Φ is surjective with kernel $I_1 \cdots I_n$, so that there is an induced isomorphism

$$\Phi : R/(I_1 \cdots I_n) \xrightarrow{\sim} \prod_{i=1}^{n} R/I_i. \tag{13}$$

PROOF. The map Φ is well-defined and has kernel $\bigcap_{i=1}^n I_i$. Since the I_i's are pairwise comaximal, Lemma 4.21 gives $\bigcap_{i=1}^n I_i = I_1 \cdots I_n$. So it remains to show that Φ is surjective. We prove this by induction on n, the case $n = 1$ being trivial. So we may assume that the natural map $\Phi' : R \to R' := \prod_{i=1}^{n-1} R/I_i$ is surjective, with kernel $I' := I_1 \cdots I_{n-1}$. Let $(r', \overline{s})$ be any element of $R' \times R/I_n$. By assumption, there exists $r \in R$ such that $\Phi'(r + I') = r'$. Let s be any element of R mapping to $\overline{s} \in R/I_n$. By Lemma 3.17c) we have $I' + I_n = R$, so there exist $x \in I'$, $y \in I_n$ such that $s - r = x + y$. Then $\Phi'(r + x) = r'$, and $r + x \equiv r + x + y \equiv s \pmod{I_n}$, so $\Phi(r + x) = (r', \overline{s})$ and Φ is surjective. □

In the classical case $R = \mathbb{Z}$, we can write $I_i = (n_i)$ and then we are trying to prove – under the assumption that the n_i's are coprime in pairs in the sense of elementary number theory – that the injective ring homomorphism $\mathbb{Z}/(n_1 \cdots n_n) \to \mathbb{Z}/n_1 \times \cdots \times \mathbb{Z}/n_n$ is an isomorphism. But both sides are finite rings of order $n_1 \cdots n_n$, so since the map is an injection it must be an isomorphism! Nevertheless the usual proof of CRT in elementary number theory is much closer to the one we gave in the general case: in particular, it is constructive.

EXERCISE 4.14 (Converse to CRT). *Let $I_1, \ldots, I_n$ be ideals in a ring R. Show: if $\prod_{i=1}^n R/I_i$ is a cyclic R-module, then $I_1, \ldots, I_n$ are pairwise comaximal.*

The following *modulization* of CRT is sometimes useful.

THEOREM 4.23. *(Module-theoretic CRT) Let R be a ring, $I_1, \ldots, I_n$ a finite set of pairwise comaximal ideals, and let M be an R-module. Then $(I_1 \cdots I_n)M = \bigcap_{i=1}^r I_i M$, and there is an induced R-module isomorphism*

$$\Phi_M : M/(I_1 \cdots I_r)M \to \prod_{i=1}^{n} M/I_i M. \tag{14}$$

PROOF. Indeed $\Phi_M = \Phi \otimes_R M$, so it is an isomorphism. Thus

$$\bigcap_{i=1}^{r} I_i M = \ker\left(M \to \prod_{i=1}^{n} M/I_i M\right) = (I_1 \cdots I_r)M.$$ □

EXERCISE 4.15. *Let R be a ring and $I_1, \ldots, I_n$ any finite sequence of ideals. Consider the map $\Phi : R \to \prod_{i=1}^n R/I_i$ as in CRT.*

a) *Show that Φ is surjective only if the $\{I_i\}$ are pairwise comaximal.*
b) *Show that Φ is injective if and onl if $\bigcap_{i=1}^n I_i = (0)$.*

EXERCISE 4.16.

a) *Let G be a finite commutative group with exactly one element z of order 2. Show: $\sum_{x \in G} x = z$.*
b) *Let G be a finite commutative group that does not have exactly one element of order 2. Show: $\sum_{x \in G} x = 0$.*
c) *Prove the following result of Gauss (a generalization of **Wilson's Theorem**): let $N \in \mathbb{Z}^+$, and put*

$$P(N) = \prod_{x \in (\mathbb{Z}/N\mathbb{Z})^\times} x.$$

Then: $P(N) = \pm 1$, and the minus sign holds if and only if $N = 4$ or is of the form p^m or $2p^m$ for an odd prime p and $m \in \mathbb{Z}^+$.
d) *For a generalization to the case of $(\mathbb{Z}_K/A)^\times$, where A is an ideal in the ring $\mathbb{Z}_K$ of integers of a number field K, see* [**Da09**]. *Can you extend Dalawat's results to the function field case?*

EXERCISE 4.17. *Let K be a field, and put $R = K[t]$.*

a) *Let $n_1, \ldots, n_k$ be a sequence of non-negative integers and $\{x_1, \ldots, x_k\}$ a k-element subset of K. For $1 \leqslant i \leqslant k$, let $c_{i0}, \ldots, c_{in_i}$ be a finite sequence of $n_i + 1$ elements of k (not necessarily distinct). By applying the Chinese Remainder Theorem, show that there is a polynomial $P(t)$ such that for $1 \leqslant i \leqslant k$ and $0 \leqslant j \leqslant n_i$ we have $P^{(j)}(x_i) = c_{ij}$, where $P^{(j)}(x_i)$ denotes the jth "formal" derivative of P evaluated at x_i. Indeed, find all such polynomials; what can be said about the least degree of such a polynomial?*
b) *Use the proof of the Chinese Remainder Theorem to give an explicit formula for such a polynomial P.*

EXERCISE 4.18. *Let $(M, \cdot)$ be a monoid and k a field. A **character** on M with values in k is a homomorphism of monoids from M to the multiplicative group $k^\times$ of k. Each character lies in the k-vector space k^M of all functions from M to k.*

a) *(Dedekind) Show: any finite set of characters is k-linearly independent.*
b) *What does this have to do with CRT? Well, the wikipedia article on CRT*[3] *contains a proof of part a) using CRT. This is the proof I had in mind when I originally wrote this exercise. But it seems to me now that this argument requires M to be finite. Discuss.*

EXERCISE 4.19. *Show: for a ring R, the following are equivalent:*

(i) *The ring R has finitely many maximal ideals.*[4]
(ii) *The quotient of R by its Jacobson radical $J(R)$ is a finite product of fields.*

We now give a commutative algebraic version of Euclid's proof of the infinitude of prime numbers. A special case for domains appears in [**K**, § 1.1, Exc. 8]. The case in which R is infinite and $R^\times$ is finite has appeared on an algebra qualifying exam at UGA; the appearance of this unusually interesting and challenging problem on a qual was remarked to me by both D. Lorenzini and B. Cook. I learned the stronger version presented here from W.G. Dubuque.

THEOREM 4.24. *If R is infinite and $\#R > \#R^\times$, then* $\operatorname{MaxSpec} R$ *is infinite.*

[3] `https://en.wikipedia.org/wiki/Chinese_remainder_theorem#Dedekind.27s_theorem`

[4] Such rings are typically called **semilocal**. I am not a fan of the terminology – it seems to either suggest that R has one half a maximal ideal (whatever that could mean) or two maximal ideals. But it is well entrenched, and I will not campaign to change it.

PROOF. Since R is not the zero ring, it has at least one maximal ideal $\mathfrak{m}_1$. We proceed by induction: given maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$, we construct another maximal ideal. Let $J := \bigcap_{i=1}^n \mathfrak{m}_i = \prod_{i=1}^n \mathfrak{m}_i$ be the Jacobson radical. By Proposition 4.18 we have $J + 1 \subseteq R^\times$, so

$$\#J = \#(J+1) \leqslant \#R^\times < \#R.$$

Moreover, by Proposition 4.19, the map $R^\times \to (R/J)^\times$ is surjective. It follows that $\#(R/J)^\times \leqslant \#R^\times < \#R$: by the Chinese remainder Theorem, $R/J \cong \prod_{i=1}^n R/\mathfrak{m}_i$, hence for all $1 \leqslant i \leqslant n$ there is an injection $(R/\mathfrak{m}_i)^\times \hookrightarrow (R/J)^\times$. Putting the last two sentences together we conclude that for all $1 \leqslant i \leqslant n$ we have $\#(R/\mathfrak{m}_i)^\times < \#R$, and since each $R/\mathfrak{m}_i$ is a field and R is infinite, we get

$$\#R/\mathfrak{m}_i = \#(R/\mathfrak{m}_i)^\times + 1 < \#R.$$

Finally this gives

$$\#R = \#J \cdot \#R/J = \#J \cdot \prod_{i=1}^n \#R/\mathfrak{m}_i < (\#R)^{n+1} = \#R,$$

a contradiction. □

In §15.11, following a discussion of factorization in domains, we will give a variant on this result that gives a sufficient condition for a domain R to have infinitely many pairwise nonassociate irreducible elements.

4. Local rings

PROPOSITION 4.25. *For a ring R, the following are equivalent:*

(i) *There is exactly one maximal ideal $\mathfrak{m}$.*
(ii) *The set $R \backslash R^\times$ of nonunits forms a subgroup of $(R, +)$.*
(iii) *The set $R \backslash R^\times$ is a maximal ideal.*

A ring satisfying these equivalent conditions is called a ***local ring****.*

PROOF. Since $R^\times = R \backslash \bigcup_{\mathfrak{m}} \mathfrak{m}$, the union extending over all maximal ideals of R, it follows that if there is only one maximal ideal $\mathfrak{m}$ then $\mathfrak{m} = R \backslash R^\times$. This shows (i) $\implies$ (iii) and certainly (iii) $\implies$ (ii). Conversely, since the set of nonunits of a ring is a union of ideals, it is closed under multiplication by all elements of the ring. Thus it is itself an ideal if and only if it is an additive subgroup: (ii) $\implies$ (iii). The implication (iii) implies (i) is very similar and left to the reader. □

Warning: In many older texts, a ring with a unique maximal ideal is called "quasi-local" and a local ring is a Noetherian quasi-local ring. This is not our convention.

Local rings (especially Noetherian local rings) play a vital role in commutative algebra: the property of having a single maximal ideal simplifies many ideal-theoretic considerations, and many ring theoretic considerations can be reduced to the study of local rings (via a process called, logically enough, *localization*: see Chapter 7).

A field is certainly a local ring. The following simple result builds on this trivial observation to give some further examples of local rings:

PROPOSITION 4.26. *Let I be an ideal in the ring R.*

a) *If $\mathrm{rad}(I)$ is maximal, then R/I is a local ring.*

b) *In particular, if* $\mathfrak{m}$ *is a maximal ideal and* $n \in \mathbb{Z}^+$*, then* $R/\mathfrak{m}^n$ *is a local ring.*

PROOF. a) We know that $\operatorname{rad}(I) = \bigcap_{\mathfrak{p} \supset I} \mathfrak{p}$, so if $\operatorname{rad}(I) = \mathfrak{m}$ is maximal it must be the *only* prime ideal containing I. Therefore, by correspondence R/I is a local ring. (In fact it is a ring with a unique prime ideal.)

b) By Proposition 4.17f), $r(\mathfrak{m}^n) = r(\mathfrak{m}) = \mathfrak{m}$, so part a) applies. □

So, for instance, for any prime number p, $\mathbb{Z}/(p^k)$ is a local ring, whose maximal ideal is generated by p. It is easy to see (using, e.g. the Chinese Remainder Theorem) that conversely, if $\mathbb{Z}/(n)$ is a local ring then n is a prime power.

EXAMPLE 4.27. *The ring* $\mathbb{Z}_p$ *of p-adic integers is a local ring. For any field* k*, the ring* $k[[t]]$ *of formal power series with coefficients in* k *is a local ring. Both of these rings are also PIDs. A ring which is a local PID is called a* ***discrete valuation ring****; these especially simple and important rings will be studied in detail later.*

EXERCISE 4.20. *Show: a local ring is connected, i.e.,* $e^2 = e \implies e \in \{0, 1\}$.

5. The Prime Ideal Principle of Lam and Reyes

A recurrent meta-principle in commutative algebra is that if $\mathcal{F}$ is a naturally given family of ideals in commutative ring R, then it is often the case that every maximal element of $\mathcal{F}$ is prime. In this section we review some known examples, give some further classical ones, and then discuss a beautiful theorem of T.-Y. Lam and M. Reyes which gives a general criterion for this phemenon to occur.

Recall that for a ring R, $\mathcal{I}(R)$ is the monoid of ideals of R under multiplication. For any $\mathcal{F} \subseteq \mathcal{I}(R)$, let $\operatorname{Max} \mathcal{F}$ denote the maximal elements of $\mathcal{F}$ (to be sure, this means the elements of $\mathcal{F}$ which are not properly contained in any other element of $\mathcal{F}$, not the elements of $\mathcal{F}$ which are not contained in any other proper ideal!). We say that $\mathcal{F}$ is an **MP family** if $\operatorname{Max} \mathcal{F} \subseteq \operatorname{Spec} R$.

EXAMPLE 4.28.
a) *Every maximal ideal is prime (Corollary 4.9), so the family of all proper ideals in a ring* R *is an MP family.*
b) *If* $S \subseteq R$ *is a multiplicative set, an ideal that is maximal with the property of being disjoint from* S *is prime (Proposition 5.26), so the family of all ideals in* R *that are disjoint from* S *is an MP family.*
c) *As we will see shortly, the family of all* non-*principal ideals in a ring* R *is an MP family. Thus if every prime ideal is principal, every ideal is principal: Theorem 4.31.*
d) *As we will see shortly, the family of all infinitely generated ideals in a ring* R *is an MP family. This implies a result of Cohen (Theorem 4.32): if every prime ideal is finitely generated, then* R *is Noetherian.*

The challenge is to come up with a common explanation and proof for all of these examples. One first observation is that there is a complementation phenomenon in play here: for $\mathcal{F} \subseteq \mathcal{I}(R)$, put $\mathcal{F}' = \mathcal{I}(R) \backslash \mathcal{F}$. Then in each of the last three cases it is most natural to view the MP family as $\mathcal{F}'$ for a suitable $\mathcal{F}$: in the second case, $\mathcal{F}$ is the set of ideals meeting S; in the third case, $\mathcal{F}$ is the set of all principal ideals; in the fourth case $\mathcal{F}$ is the set of all finitely generated ideals.

Let us also recall that for $I, J \in \mathcal{I}(R)$,

$$(I : J) = \{x \in R \mid xJ \subseteq I\}.$$

For $a, b \in R$, we write $(I : b)$ for $(I : Rb)$ and $(a : J)$ for $(aR : J)$.

EXERCISE 4.21. *For ideals I, J in R, show that*

$$(I : J)\langle I, J\rangle \subseteq I. \tag{15}$$

EXERCISE 4.22. *Let R be a PID, and let $a, b \in R^\bullet$. Then (a) and (b) can be factored into products of principal prime ideals, say*

$$(a) = (\pi_1^{a_1} \cdots (\pi_i^{a_r}),\ b = (\pi_1^{b_1}) \cdots (\pi_r^{b_r}),\ a_i, b_i \in \mathbb{N}.$$

a) *Show $\langle a, b\rangle = \langle \pi_1^{\min(a_1,b_1)} \cdots \pi_r^{\min(a_r,b_r)}\rangle$.*
b) *Show $(a : b) = \langle \pi_1^{\max(a_1-b_1,0)} \cdots \pi_r^{\max(a_r-b_r,0)}\rangle$.*
c) *Show $\langle a\rangle \subseteq (a : b)$.*
d) *Show $(a : b)\langle a, b\rangle = \langle a\rangle$.*
e) *Suppose $\#MaxSpecR \geqslant 2$. Find $a, b \in R^\bullet$ such that:*
   (i) *We have $(a : b) \subseteq \langle a, b\rangle$.*
   (ii) *We have $\langle a, b\rangle \subseteq (a : b)$.*
   (iii) *Neither of $(a : b)$, $\langle a, b\rangle$ contains the other.*

We say a partially ordered set $(X, \leqslant)$ has the **weak maximum** property if for every $x \in X$ there is a maximal element $m \in X$ with $x \leqslant m$. Zorn's Lemma implies that if every chain in X has an upper bound then X has the weak maximum property.

EXERCISE 4.23. *Let $\mathcal{F} \subseteq \mathcal{I}(R)$ be a family of finitely generated ideals of R. (This applies to all $\mathcal{F}$ if and only if R is Noetherian.) Show: $\mathcal{F}'$ has the weak maximum property.*

A family $\mathcal{F} \subseteq \mathcal{I}(R)$ is an **Oka family** if $R \in \mathcal{F}$ and for all $x \in R$ and $I \in \mathcal{I}(R)$, if $\langle I, x\rangle,\ (I : x) \in \mathcal{F}$, then $I \in \mathcal{F}$.

A family $\mathcal{F} \subseteq \mathcal{I}(R)$ is an **Ako family** if $R \in \mathcal{F}$ and for all $x_1, .x_2 \in R$ and $I \in \mathcal{I}(R)$, if $\langle I, x_1\rangle,\ \langle I, x_2\rangle \in \mathcal{F}$, then $\langle I, x_1x_2\rangle \in \mathcal{F}$.

A family $\mathcal{F} \subseteq \mathcal{I}(R)$ is **increasing** if for all $I, J \in \mathcal{I}(R)$, if $I \in \mathcal{F}$ and $J \supset I$ then $J \in \mathcal{F}$.

THEOREM 4.29. *(Prime Ideal Principle of Lam-Reyes [**LR08**]) Let R be a ring and let $\mathcal{F} \subseteq \mathcal{I}(R)$ be a family of ideals that is either Oka or Ako.*

a) *The complementary family $\mathcal{F}' := \mathcal{I}(R)\backslash\mathcal{F}$ is an MP family.*
b) *Suppose moreover that $\mathcal{F}'$ has the weak maximum property. Then:*
   (i) *Let $\mathfrak{f} \subseteq \mathcal{I}(R)$ be an increasing family. If $\mathfrak{f} \cap \operatorname{Spec} R \subseteq \mathcal{F}$, then $\mathfrak{f} \subseteq \mathcal{F}$.*
   (ii) *Suppose that $I \in \mathcal{I}(R)$ is such that every prime ideal $\mathfrak{p}$ that contains I (resp. properly contains I) lies in $\mathcal{F}$. Then every ideal that contains I (resp. properly contains I) lies in $\mathcal{F}$.*
   (iii) *If $\operatorname{Spec} R \subseteq \mathcal{F}$ then $\mathcal{F} = \mathcal{I}(R)$.*

PROOF. a) We go by contraposition: let $I \in \operatorname{Max}\mathcal{F}'$ be an ideal which is not prime, so there are $a, b \in R\backslash I$ with $ab \in I$. Since $b \in (I : a)$, the ideals $\langle I, a\rangle, (I : a)$ each properly contain I, so by maximality of I we have $\langle I, a\rangle,\ \langle I, b\rangle,\ (I : a) \in \mathcal{F}$.

Since $I = \langle I, ab\rangle \notin \mathcal{F}$, the family $\mathcal{F}$ is neither Oka nor Ako.
b) (i) Suppose there is $I \in \mathfrak{f}\backslash\mathcal{F}$. Since $\mathcal{F}'$ has the weak maximum property, I is contained in a maximal element $\mathfrak{p}$ of $\mathcal{F}'$, which by part a) is prime. Since $\mathfrak{f}$ is increasing, this gives $\mathfrak{p} \in \mathfrak{f} \cap \operatorname{Spec} R \subseteq \mathcal{F}$, a contradiction.
(ii) Apply (i) with $\mathfrak{f}$ the family of ideals containing (resp. properly containing) I.
(iii) Apply (i) with $\mathfrak{f} = \operatorname{Spec} R$. □

PROPOSITION 4.30. *Let R be a ring. Each of the following families $\mathcal{F}$ is Oka and the complementary family $\mathcal{F}'$ is closed under taking unions of chains hence satisfies the weak maximum property:*

(i) *The set of all ideals meeting a multiplicatively closed subset $S \subseteq R$.*
(ii) *The set of all principal ideals.*
(iii) *The set of all finitely generated ideals.*

PROOF. (i) Let $x \in R$, $I \in \mathcal{I}(R)$ be such that $\langle I, x\rangle, (I : x) \in \mathcal{F}$. Then there are $s_1, s_2 \in S$, $i_1, i_2 \in I$ and $a, b \in R$ such that

$$s_1 = ai_1 + bx,\ s_2x = i_2.$$

Then

$$s_2s_2 = as_2i_1 + bs_2x = as_2i_1 + bi_2 \in S \cap I.$$

The union of a chain of ideals disjoint from S is an ideal disjoint from S.
(ii) Suppose $(I : x) = \langle a\rangle$ and $\langle I, x\rangle = \langle b\rangle$. Exercise 4.22d) gives us a useful hint: we will show $I = \langle ab\rangle$. Equation (15) gives the containment

$$\langle ab\rangle = \langle a\rangle\langle b\rangle(I : x)\langle I, x\rangle \subseteq I.$$

Conversely, let $i \in I$. Since $I \subseteq \langle I, x\rangle = \langle b\rangle$, we may write $i = \alpha b$ for some $\alpha \in R$. We have $\alpha(b) \subseteq I$ hence also $\alpha\langle x\rangle \subseteq I$ and thus $\alpha \in (I : x) = \langle a\rangle$. So

$$i = \alpha b \in \langle ab\rangle.$$

The union I of a chain $\{I_j\}$ of nonprincipal ideals must be nonprincipal: if $I = \langle a\rangle$ then $a \in I_j$ for some j and thus $\langle a\rangle \subseteq I_j \subseteq I = \langle a$, so $I_j = \langle a\rangle$ is principal.
(iii) Suppose $(I : x) = \langle a_1, \ldots, a_m\rangle$ and $\langle I, x\rangle = \langle i_1 + \alpha_1 x, \ldots, i_n + \alpha_n x\rangle$. Let $J = \langle i_1, \ldots, i_n, xa_1, \ldots, xa_m\rangle$. We will show $I = J$, hence I is finitely generated. It is immediate that $J \subseteq I$. Conversely $z \in I$; since $I \subseteq \langle I, x\rangle$, we may write

$$z = \beta_1(i_1 + \alpha_1 x) + \ldots + \beta_n(i_1 + \alpha_n x) = (\beta_1 i_1 + \ldots + \beta_n i_n) + (\alpha_1\beta_1 + \ldots + \alpha_n\beta_n)x.$$

Since z and $\beta_1 i_1 + \ldots + \beta_n i_n \in I$, so is $(\alpha_1\beta_1 + \ldots + \alpha_n\beta_n)x$, i.e., $\alpha_1\beta_1 + \ldots + \alpha_n\beta_n \in (I : x) = \langle a_1, \ldots, a_m\rangle$, so $(\alpha_1\beta_1 + \ldots + \alpha_n\beta_n)x \in \langle xa_1, \ldots, xa_m\rangle$ and thus $z \in J$.

The union I of a chain $\{I_j\}$ of infinitely generated ideals must be infinitely generated: if $I = \langle x_1, \ldots, x_n\rangle$, then for all $1 \leqslant i \leqslant n$ we have $x_i \in I_{j_i}$ for some index j_i. Then

$$\langle x_1, \ldots, x_n\rangle \subseteq I_{\max(j_1,\ldots,j_n)} \subseteq I = \langle x_1, \ldots, x_n\rangle,$$

so $I_j = \langle x_1, \ldots, x_n\rangle$ is finitely generated. □

Combining Proposition 4.34 and Theorem 4.29 we deduce a new proof of Multiplicative Avoidance as well as immediate proofs of the following results.

THEOREM 4.31. *If every prime ideal of R is principal, every ideal of R is principal.*

What about maximal ideals? Later we will encounter local rings with maximal principal ideals that are not principal ideal rings, but they will be non-Noetherian. Indeed they need to be: by a result of Kaplansky (Theorem 16.11), if in a Noetherian ring every maximal ideal is principal, then every ideal is principal. The proof will draw significantly on aspects of the structure theory of Noetherian rings.

THEOREM 4.32. *(Cohen [**?**]) If every prime ideal of R is finitely generated, then every ideal of R is finitely generated.*

Looking back at the above approach, the only cloud in the sky may be that directly checking whether a family is Oka or Ako is neither completely trivial nor especially enlightening. Following Lam-Reyes, we introduce some further conditions on a family that will allow us to prove more easily that it is either Oka or Ako.

A family $\mathcal{F} \subseteq \mathcal{I}(R)$ is a **strongly Oka family** if $R \in \mathcal{F}$ and for $I, J \in \mathcal{I}(R)$, if $\langle I, J\rangle,\ (I : J) \in \mathcal{F}$, then $I \in \mathcal{F}$.

A family $\mathcal{F} \subseteq \mathcal{I}(R)$ is a **strongly Ako family** if $R \in \mathcal{F}$ and for all $x \in R$ and $I,\ J \in \mathcal{I}(R)$, if $\langle I, x\rangle,\ \langle I, J\rangle \in \mathcal{F}$, then $\langle I, xJ\rangle \in \mathcal{F}$.

A family $\mathcal{F} \subseteq \mathcal{I}(R)$ is a **very strongly Ako family** if $R \in \mathcal{F}$ and for all $I,\ J_1, J_2 \in \mathcal{I}(R)$, if $\langle I, J_1\rangle,\ \langle I, J_2\rangle \in \mathcal{F}$, then $\langle I, J_1J_2\rangle \in \mathcal{F}$.

A family $\mathcal{F} \subseteq \mathcal{I}(R)$ is a **filter** if $\mathcal{F}$ is increasing, $\mathcal{F}$ is closed under finite intersections and $R \in \mathcal{F}$.[5] A family $\mathcal{F} \subseteq \mathcal{I}(R)$ is **monoidal** if $R \in \mathcal{F}$ and for all $I, J \in \mathcal{F}$ we have $IJ \in \mathcal{F}$.

EXERCISE 4.24.
a) *Show: a monoidal increasing family $\mathcal{F} \subseteq \mathcal{I}(R)$ is a monoidal filter.*
b) *Let (P) be any of the following properties: Oka, Ako, strongly Oka, strongly Ako, monoidal filter. For each $i \in I$, let $\mathcal{F}_i$ be a family satisfying (P). Show that $\mathcal{F} := \bigcap_{i\in I}$ satsisfies property (P). Deduce: that for any family $\mathcal{F} \subseteq \mathcal{I}(R)$ there is a unique minimal family $\overline{\mathcal{F}}$ containing $\mathcal{F}$ and satisfying property (P).*
c) *Let (P) be the property of being a monoidal filter, and let $\mathcal{F} \subseteq \mathcal{I}(R)$ be any family of ideals. Show that $\overline{\mathcal{F}}$ is the collection of ideals of R that contain a finite product $I_1 \cdots I_n$ with each $I_i \in \mathcal{F}$.*

PROPOSITION 4.33. *Let R be a ring, and let $\mathcal{F} \subseteq \mathcal{I}(R)$ be a family of ideals.*
a) *Strongly Oka implies Oka, and very strongly Ako implies strongly Ako implies Ako.*
b) *Monoidal filter implies very strongly Ako.*
c) *Very strongly Ako implies strongly Oka.*
d) *Strongly Ako implies Oka.*

PROOF. a) These implications are immediate from the definitions.
b) Let $I, J_1, J_2 \in \mathcal{I}(R)$. If $\langle I, J_1\rangle,\ \langle I, J_2\rangle \in \mathcal{F}$, then since $\mathcal{F}$ is monoidal, we have

$$\langle I, J_1\rangle\langle I, J_2\rangle = \langle I^2, IJ_1, IJ_2, J_1J_2\rangle \in \mathcal{F}.$$

[5]This is the usual set-theoretic notion of a filter on 2^R each of whose elements is an ideal. To be slick about it, closure under finite intersections should include closure under the empty intersection which should itself imply that $R \in \mathcal{F}$.

Since $\langle I^2, IJ_1, IJ_2, J_1J_2\rangle \subseteq \langle I, J_1J_2\rangle$ and $\mathcal{F}$ is monoidal, we get that $\langle I, J_1J_2\rangle \in \mathcal{F}$, so $\mathcal{F}$ is very strongly Ako.
c) Let $\mathcal{F}$ be very strongly Ako. Let $I, J \in \mathcal{I}(R)$ be such that $\langle I, J\rangle$, $\langle I : J\rangle \in \mathcal{F}$. Then $(I : J) = \langle I, (I : J)\rangle$, and the very strong Ako condition gives

$$I = \langle I, J(I : J)\rangle \in \mathcal{F}.$$

d) Taking $J =]\langle x\rangle$ in the proof of part c) shows that strongly Ako implies Oka. □

We now revisit some of the above examples with these further conditions in mind.

EXAMPLE 4.34. a) *If $S \subseteq R$ is a multiplicative subset, the family $\mathcal{F}_S$ of all ideals in R that meet S is a monoidal filter, as is almost immediate to check. This is the strongest of the conditions we have introduced, so in particular $\mathcal{F}_S$ is both Oka and Ako.*

b) *Let $\mathcal{F}_1$ be the family of all principal ideals of R. Except in the trivial case where every ideal of R is principal, $\mathcal{F}_1$ is not increasing, so is not a filter. However it is monoidal and strongly Oka: the former is immediate and the proof of Oka-ness given in Proposition adapts to show strong Oka-ness.*

In fact the family $\mathcal{F}_1$ need not be Ako. Let R be a ring admitting principal ideals $\langle a\rangle$, $\langle b\rangle$ whose intersection is not finitely generated (see [**LR08**, Remark 3.18]*) and the references therein for a specific example). Then $\langle I, a\rangle = \langle a\rangle$, $\langle I, b\rangle = \langle b\rangle \in \mathcal{F}_1$ but $\langle I, ab\rangle = I \notin \mathcal{F}_1$. This also gives a ring in which the family of finitely generated ideals is not Ako (but is strongly Oka, as we will now see).*

c) *For an infinite cardinal κ, let $\mathcal{F}_{<\kappa}$ (resp. $\mathcal{F}_{\leqslant\kappa}$) be the family of ideals of R that admit a generating set of cardinality less than α (resp. of cardinality at most α). These families are monoidal: for $\mathcal{F}_{<\kappa}$ this is because if α, β, κ are cardinals with κ infinite and $\alpha, \beta < \kappa$ then*

$$\alpha\beta \leqslant \max(\alpha, \beta)^2 < \kappa^2 = \kappa,$$

and the case of $\mathcal{F}_{\leqslant\kappa}$ is because $\kappa^2 = \kappa$. They are also monoidal: we will treat the slightly more difficult case of $\mathcal{F}_{<\kappa}$. For an ideal I of R, we write $\mu(I)$ for its minimal number of generators. Let $I \in \mathcal{I}(R)$ and $x \in R$. Then there are infinite cardinals $\alpha, \beta < \kappa$ such that $\mu(I, x) \leqslant \alpha < \kappa$ and $\mu((I : x)) \leqslant \beta < \kappa$. Then there is an ideal $I_0 \subseteq I$ with $\mu(I_0) \leqslant \alpha$ and $\langle I, x\rangle = \langle I_0, x\rangle$. We claim that

$$I_0 + (I : x)\langle x\rangle = I.$$

Indeed, both I_0 and $(I : x)\langle x\rangle$ are contained in I, so $I_0 + (I : x)\langle x\rangle \subseteq I$. If $i \in I$ there is $i_0 \in I_0$ and $a \in R$ such that $i = i_0 + ax$; since $ax = i - i_0 \in I$, we have $a \in (I : x)$, and thus $i \in I_0 + (I : x)\langle x\rangle$. Thus $\mu(I) \leqslant \alpha + \beta \leqslant \max(\alpha, \beta) < \kappa$, so $I \in \mathcal{F}_\alpha$.

EXERCISE 4.25. *Let κ be an infinite cardinal, and let $\mathcal{F}$ be either $\mathcal{F}_{<\kappa}$ or $\mathcal{F}_{\leqslant\kappa}$ as defined in Example 4.34c) above. We showed that* $\operatorname{Max}\mathcal{F}' \subseteq \operatorname{Spec}\mathcal{F}$. *Is it true that if every prime ideal in R can be generated by fewer than κ elements (resp. by at most κ elements) then every ideal in R can be generated be fewer than κ elements (resp. by at most κ elements)?*

6. Minimal Primes

Let R be a ring. A **minimal prime** $\mathfrak{p}$ of R is just what it sounds like: a minimal element of the set $\operatorname{Spec} R$ of prime ideals of R, partially ordered by inclusion.

EXERCISE 4.26. *Let $\mathcal{C}$ be a chain of prime ideals in a ring R. Show: $\bigcap_{\mathfrak{p}\in\mathcal{C}} \mathfrak{p}$ is a prime ideal.*

PROPOSITION 4.35. *Let $I \subseteq \mathcal{P}$ be ideals of R, with $\mathcal{P}$ prime. Then the set $\mathcal{S}$ of all prime ideals $\mathfrak{p}$ of R with $I \subseteq \mathfrak{p} \subseteq \mathcal{P}$ has a minimal element.*

PROOF. We partially order $\mathcal{S}$ by reverse inclusion i.e., $\mathfrak{p}_1 \leqslant \mathfrak{p}_2 \iff \mathfrak{p}_1 \supset \mathfrak{p}_2$. Let C be any chain in $\mathcal{S}$. By Exercise 4.26, $\bigcap_{\mathfrak{p}\in\mathcal{C}} \mathfrak{p}$ is a prime ideal and thus it is an upper bound for $\mathcal{C}$ in $\mathcal{S}$. By Zorn's Lemma, $\mathcal{S}$ contains a maximal element, i.e., a minimal element under ordinary containment. □

COROLLARY 4.36. *Every nonzero ring has at least one minimal prime.*

EXERCISE 4.27. *Prove Corollary 4.29.*

We write $\operatorname{MinSpec} R$ for the set of all minimal primes of R and $\operatorname{ZD}(R)$ for the set of all zerodivisors in R.

EXERCISE 4.28. *Show: in a ring R, $r(R) = \bigcap_{\mathfrak{p}\in\operatorname{MinSpec} R} \mathfrak{p}$.*

In order to prove the next result, it is convenient to use the theory of localization, which we will not develop until § 7. Nevertheless we have decided to place the proof here, as it fits thematically with the other results of the section.

THEOREM 4.37. *Let R be a ring.*

a) *We have $\bigcup_{\mathfrak{p}\in\operatorname{MinSpec} R} \mathfrak{p} \subseteq \operatorname{ZD}(R)$.*

b) *If R is reduced, then equality holds:*

$$\bigcup_{\mathfrak{p}\in\operatorname{MinSpec} R} \mathfrak{p} = \operatorname{ZD}(R). \tag{16}$$

PROOF. a) Let $\mathfrak{p} \in \operatorname{MinSpec} R$ and let $x \in \mathfrak{p}$. Then $\mathfrak{p}R_{\mathfrak{p}}$ is the unique prime ideal of $R_{\mathfrak{p}}$, so $x \in r(\mathfrak{p}A_{\mathfrak{p}})$ is nilpotent. By Exercise 7.6, this implies that there is $y \in R\backslash\mathfrak{p}$ such that $yx^n = 0$. Since $y \neq 0$, x^n – and thus also x – is a zero-divisor.
b) Suppose $a \in \operatorname{ZD}(R)$, so there is $b \in R^\bullet$ with $ab = 0$. Since $b \neq 0$ and R is reduced, by Exercise 4.28 we have

$$b \notin \bigcap_{\mathfrak{p}\in\operatorname{MinSpec} R} \mathfrak{p},$$

so there is $\mathfrak{p} \in \operatorname{MinSpec} R$ not containing b. Since $ab = 0 \in \mathfrak{p}$, we have $a \in \mathfrak{p}$. □

PROPOSITION 4.38. *Let $\mathcal{I} := \{I_j\}_{j\in J}$ be any family of ideals in a ring R, and let $\mathcal{F}$ be the family of ideals that contain some finite product $I_{j_1} \cdots I_{j_n}$ (taking the empty product, we get that $R \in \mathcal{F}$). Let $\mathcal{F}'$ be the complementary family of ideals not containing any product of the I_j's.*

a) *Any maximal element of $\mathcal{F}'$ is a prime ideal.*

b) *Suppose moreover that each I_i is finitely generated and that every prime ideal of R contains some I_i. Then there are $j_1, \ldots, j_n \in J$ such that $I_{j_1} \cdots I_{j_n} = (0)$.*

PROOF. a) The family $\mathcal{F}$ is a monoidal filter: indeed, it is the monoidal filter generated by the family $\{I_j\}_{j \in I}$. By Theorem 4.29a), every maximal element of $\mathcal{F}'$ is prime.
b) Let $\{J_k\}$ be a chain in $\mathcal{F}'$, and let $J := \bigcup_k J_k$ be its union. If $J \supset I_{j_1} \cdots I_{j_n}$, then since each I_{j_i} is finitely generated, so is $I_{j_1} \cdots I_{j_n}$, and as we have seen before, if the union of a chain of ideals contains a finitely generated ideal, then so does some element of the chain. So by Zorn's Lemma $\mathcal{F}'$ has the weak maximum property, so by Theorem 4.29b)(iii) since every prime ideal of R lies in $\mathcal{F}$ we conclude that every ideal lies in $\mathcal{F}$. In particular the zero ideal lies in $\mathcal{F}$, giving the desired conclusion. □

COROLLARY 4.39 (Anderson).

a) *Suppose that in a ring R every minimal prime ideal is finitely generated. Then* $\operatorname{MinSpec} R$ *is finite.*
b) *If R is Noetherian, then* $\operatorname{MinSpec} R$ *is finite.*

PROOF. a) We apply Proposition 4.38b) with $\mathcal{I} = \operatorname{MinSpec} R$. There are then distinct minimal prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ and $a_1, \ldots, a_n \in \mathbb{Z}^+$ such that $\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n} = (0)$. If now $\mathfrak{q} \in \operatorname{MinSpec} R$ then $\mathfrak{q} \supset \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n}$ so $\mathfrak{q} \supset \mathfrak{p}_i$ for some $1 \leqslant i \leqslant n$. It follows that $\operatorname{MinSpec} R = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.
b) If R is Noetherian then every ideal is finitely generated, so part a) applies. □

7. An application to unit groups

The following useful generalization of Proposition 4.19 is due to MathOverflow user zcn: see `http://mathoverflow.net/users/44201/zcn`.

THEOREM 4.40. *Let $f : R \to S$ be a surjective ring homomorphism, with kernel I. Suppose that all but finitely many maximal ideals of R contain I. Then the induced group homomorphism on unit groups $f^\times : R^\times \to S^\times$ is surjective.*

PROOF. We may identify S with R/I. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ be the maximal ideals of R that do not contain I. Then the ideals $I, \mathfrak{m}_1, \ldots, \mathfrak{m}_n$ are pairwise comaximal. Let $y \in S^\times$, and choose $x \in R$ such that $f(x) = y$. By the Chinese Remainder Theorem there is $a \in I$ such that $a \equiv 1 - x \pmod{\mathfrak{m}_i}$ for all $1 \leqslant i \leqslant n$. Then $f(x+a) = f(x) + f(a) = f(x) = y$. Moreover, for all $1 \leqslant i \leqslant n$ we have $x + a \notin \mathfrak{m}_i$. If $\mathfrak{m} \in \operatorname{MaxSpec} R \backslash \{\mathfrak{m}_1, \ldots, \mathfrak{m}_n\}$ then $\mathfrak{m} \supset I$, so if $x + a \in \mathfrak{m}$, then $x \in \mathfrak{m}$, so $y = f(x) \in \mathfrak{m}/I$, a proper ideal of R/I: contradiction. So $x + a \in R^\times$. □

The hypothesis of Theorem 4.40 applies to every surjective homomorphism $f : R \to S$ when R is semilocal, so in particular when R is finite or – as we will see later in Theorem 8.37 – when R is Artinian.

CHAPTER 5

Examples of Rings

1. Rings of numbers

The most familiar examples of rings are probably rings of numbers, e.g.

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}.$$

These are, respectively, the integers, the rational numbers, the real numbers and the complex numbers. For any positive integer N the ring integers modulo N, denoted $\mathbb{Z}/N\mathbb{Z}$. We assume that the reader has seen all these rings before.

Historically, the concept of a ring as an abstract structure seems to have arisen as an attempt formalize common algebraic properties of number rings of various sorts. It is my understanding that the term "ring" comes from Hilbert's *Zahlring* ("Zahl" means "number" in German). Indeed, various sorts of extension rings of $\mathbb{C}$ – most famously Hamilton's quaternions $\mathbb{H}$ – have been referred to as systems of **hypercomplex numbers**. This terminology seems no longer to be widely used.

The adjunction process gives rise to many rings and fields of numbers, as already seen in §2.2. For instance, for a nonsquare integer D, let $\sqrt{D}$ be a complex number whose square is D: then $\mathbb{Z}[\sqrt{D}]$ is an interesting ring.

EXERCISE 5.1. *Show:* $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$.

In particular, $(\mathbb{Z}[\sqrt{D}], +) \cong (\mathbb{Z}^2, +)$ as commutative groups, although not as rings, since $\mathbb{Z}[\sqrt{D}]$ is a domain and $\mathbb{Z}^2$ has nontrivial idempotents.

More generally, let K be any number field (a finite degree field extension of $\mathbb{Q}$), and let $\mathbb{Z}_K$ be the set of elements $x \in K$ which satisfy a monic polynomial with $\mathbb{Z}$-coefficients. It turns out that $\mathbb{Z}_K$ is a ring, the **ring of algebraic integers in K**. This is a special case of the theory of integral closure: see §14.

Algebraic number theory proper begins with the observation that in general the rings $\mathbb{Z}_K$ need not be UFDs but are otherwise as nice as possible from a commutative algebraic standpoint. That is, every ring $\mathbb{Z}_K$ is a **Dedekind domain**, which among many other characterizations, means that every nonzero ideal factors into a product of prime ideals. That the rings $\mathbb{Z}_K$ are Dedekind domains is an example of a *normalization theorem*, more specifically a very special case of the **Krull-Akizuki Theorem** of §18.

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$. (This is *not* a number field, being an infinite degree algebraic extension of $\mathbb{Q}$.) We may define $\overline{\mathbb{Z}}$ to be the set of all elements of $\overline{\mathbb{Q}}$ which satsify a monic polynomial with integer coefficients: this is **the ring of**

all algebraic integers. In particular,

$$\overline{\mathbb{Z}} = \varinjlim \mathbb{Z}_K$$

is the direct limit of all rings of integers in fixed number fields.

EXERCISE 5.2. *Let $\overline{\mathbb{Z}}$ be the set of all algebraic integers.*

a) *Taking as given that for any number field K, the algebraic integers in K form a subring of K, show that $\overline{\mathbb{Z}}$ is a subring of $\overline{\mathbb{Q}}$.*[1]

b) *Show: $\overline{\mathbb{Z}}$ is a domain that is* not *Noetherian. Hint: use the fact that the nth root of an algebraic integer is an algebraic integer to construct an infinite strictly ascending chain of principal ideals in $\overline{\mathbb{Z}}$.*

THEOREM 5.1. *Every finitely generated ideal in the ring $\overline{\mathbb{Z}}$ is principal.*

Thus, if only $\overline{\mathbb{Z}}$ were Noetherian, it would be a principal ideal domain! Later on we will prove a more general theorem, due to Kaplansky, in the context of limits of Dedekind domains with torsion Picard groups.

2. Rings of continuous functions

2.1. The ring of real-valued functions.

Let R be a ring, X a set, and consider the set R^X of all functions $f : X \to R$. We may endow R^X with the structure of a ring by defining addition and multiplication "pointwise", i.e.,

$$(f + g) : x \mapsto f(x) + g(x),$$
$$(fg) : x \mapsto f(x)g(x).$$

EXERCISE 5.3. *Show: this makes R^X into a ring with additive identity the constant function 0 and multiplicative identity the constant function 1.*

However, this is not really a "new" example of a ring.

EXERCISE 5.4. *Show: R^X is isomorphic as a ring, to $\prod_{x \in X} R$.*

Later on we will see this construction in the special case $R = \mathbb{F}_2$, in which case we get an important subclass of **Boolean rings**. However, in general R^X is quite a roomy ring. It contains many interesting subrings, some of which can be nicely consructed and analyzed using topological, geometric and analytic considerations.

2.2. Separation axioms and $C(X)$.

We specialize to the following situation: $R = \mathbb{R}$, X is a topological space, and instead of the ring $\mathbb{R}^X$ we look at the subring $C(X)$ of *continuous* $f : X \to \mathbb{R}$.

EXERCISE 5.5. *Show: for a topological space X, the following are equivalent:*

(i) *For every $x, y \in X$ with $x \neq y$, there exists $f \in C(X)$ with $f(x) \neq f(y)$.*

(ii) *For every $x, y \in X$ with $x \neq y$ and every $\alpha, \beta \in \mathbb{R}$, there exists $f \in C(X)$ with $f(x) = \alpha,\ f(y) = \beta$.*

(iii) *For every finite subset S of X and any function $g : S \to \mathbb{R}$, there is $f \in C(X)$ such that $f|_S = g$.*

A space that satisfies these equivalent conditions is called ***C-separated***.[2]

[1] Both the "given" and the conclusion of this part of the exercise will follow from our study of integral extensions in Chapter 14.

[2] More standard terminology: "the continuous functions on X separate points".

Recall the following chains of implications from general topology:

LEMMA 5.2. *For any topological space, the following implications hold (and none of the arrows may be reversed)):*

a) *X compact $\implies$ X normal $\implies$ X Tychonoff $\implies$ X regular $\implies$ X Hausdorff $\implies$ X separated $\implies$ X Kolmogorov.*
b) *X locally compact $\implies$ X Tychonoff.*

EXERCISE 5.6.

a) *Show: a Tychonoff space is C-separated.*
b) *Show: a C-separated space is Hausdorff.*
c) *Show: a regular space need not be C-separated. (Suggestion: see* [**Ga71**]*.)*

For a topological space X, a **zero set** is a set of the form $f^{-1}(0)$ for some continuous function $f : X \to \mathbb{R}$. A **cozero set** is a complement of a zero set. The cozero sets in fact form a base for a topology on X; we call it the **Z-topology** and write X_Z for X endowed with the Z-topology. Since every cozero set is an open set in the given topology on X, X_Z is a coarser topology than the given topology on X. Of course we allow the possibility that the two topologies coincide. The following basic (but not so widely known) result gives a condition for this.

THEOREM 5.3.

a) *For a Hausdorff topological space X, the following are equivalent:*
   (i) *$X_Z = X$: every closed set is an intersection of zero sets of continuous functions.*
   (ii) *X is Tychonoff, i.e., if Y is a closed subset of X and $x \in X \backslash Y$, then there exists a continuous function $f : X \to [0,1]$ with $f(x) = 0$, $f|_Y \equiv 1$.*
b) *For any topological space X, the space X_Z is quasi-Tychonoff*[3] *and is the finest quasi-Tychonoff topology on the underlying set of X which is coarser than X.*

PROOF. [**GJ76**, p. 38]. □

Let X be a topological space, and let $x \in X$ be any point. Consider the set

$$\mathfrak{m}_x = \{f \in C(X) \mid f(x) = 0\}.$$

Evidently $\mathfrak{m}_x$ is an ideal of $C(X)$. But more is true.

PROPOSITION 5.4. *Evaluation at x gives a canonical isomorphism $C(X)/\mathfrak{m}_x \xrightarrow{\sim} \mathbb{R}$. In particular, $\mathfrak{m}_x$ is a* maximal *ideal of $C(X)$.*

EXERCISE 5.7. *Prove Proposition 5.4.*

For a topological space X, we let

$$M(X) \coloneqq \operatorname{MaxSpec} C(X)$$

be the set of maximal ideals in the ring of continuous real-valued functions on X. Thus $x \mapsto \mathfrak{m}_x$ gives a map of sets $\mathcal{M} : X \to M(X)$.

[3]That is, points can be separated from closed subsets by continuous functions. Quasi-Tychonoff is often called "completely regular," and Tychonoff means quasi-Tychonoff and Hausdorff.

PROPOSITION 5.5. *The map $\mathfrak{m} : X \to M(X)$ is injective if and only if X is C-separated.*

EXERCISE 5.8. *Prove Proposition 5.5.*

2.3. Quasi-compactness and $C(X)$.

PROPOSITION 5.6. *If X is quasi-compact, then $\mathfrak{m}$ is surjective, i.e., every maximal ideal of $C(X)$ is of the form $\mathfrak{m}_x$ for at least one point $x \in X$.*

PROOF. It suffices to show: let I be an ideal of $C(X)$ such that for no $x \in X$ do we have $I \subseteq \mathfrak{m}_x$. Then $I = C(X)$. By hypothesis, for every $x \in X$ there is $f_x \in I$ such that $f_x(x) \neq 0$. Since f_x is continuous, there is an open neighborhood U_x of x such f_x is nowhere vanishing on U_x. By quasi-compactness of X, there is a finite set $x_1, \ldots, x_N$ such $X = \bigcup_{i=1}^N U_{x_i}$. Then the function $f = f_{x_1}^2 + \ldots + f_{x_n}^2$ is an element of $\mathfrak{m}$ which is positive at every $x \in X$. But then $\frac{1}{f}$ is also a continuous function on X, i.e., $f \in C(X)^\times$, so $I = R$. □

A compact space is quasi-compact and C-separated. Thus previous results yield:

THEOREM 5.7. *If X is compact, then $\mathfrak{m} : X \to M(X)$ is a bijection: every maximal ideal of $C(X)$ is of the form $\mathfrak{m}_x$ for a unique $x \in X$.*

If X is quasi-compact, there is a natural topology on $M(X)$, the **initial topology**: each $f \in C(X)$ induces a function $M_f : M(X) \to \mathbb{R}$, by mapping $\mathfrak{m}$ to the image of f in $C(X)/\mathfrak{m} = \mathbb{R}$. We endow $M(X)$ with the coarsest topology which makes each M_f continuous. It follows that for a topological space W, a function $g : W \to M(X)$ is continuous if and only if $M_f \circ g : W \to \mathbb{R}$ is continuous for all $f \in C(X)$. In particular the function $\mathfrak{m} : X \to M(X)$ is continuous because for all $f \in C(X)$, we have $M_f \circ \mathfrak{m} = f$ is continuous.

LEMMA 5.8. *For a compact space X, the initial topology on $M(X)$ is Hausdorff.*

PROOF. For distinct $x, x' \in X$, consider the maximal ideals $\mathfrak{m}_x, \mathfrak{m}_{x'}$. By C-separatedness, there exists $f \in C(X)$ with $f(x) = 0$, $f(x') \neq 0$. Thus choose disjoint neighborhoods V, V' of $f(x), f(x') \in \mathbb{R}$. The sets

$$U_{f,V} = \{x \in X \mid f(x) \in V\},\ U_{f,V'} = \{x \in X \mid f(x) \in V'\}$$

are disjoint open neighborhoods of x and x'. □

THEOREM 5.9. *If X is a compact space, then $\mathfrak{m} : X \to M(X)$ is a homeomorphism.*

PROOF. The map $\mathfrak{m}$ is a continuous bijection from a compact space to a Hausdorff space. Any such map is a homeomorphism. Indeed, let Y be a closed subset of X. Then Y is compact, so $\mathfrak{m}(Y)$ is compact in the Hausdorff space $M(X)$, so $\mathfrak{m}(Y)$ is closed, and it follows that $\mathfrak{m}^{-1}$ is continuous. □

2.4. The Zariski topology on $C(X)$.

For any commutative ring R, we define a topology on the set MaxSpec R of maximal ideals of R. For an ideal I of R, we put

$$V(I) := \{\mathfrak{m} \in \operatorname{MaxSpec} R \mid I \subseteq \mathfrak{m}\}.$$

As we will pursue in much more detail in Chapter 13, the sets $V(I)$ are the closed sets for a unique topology on $\operatorname{MaxSpec} R$, the **Zariski topology**. (The Zariski topology on the set $\operatorname{Spec} R$ of all prime ideals of R is defined in exactly the analogous way and later on will be our primary object of study. For the class of rings $C(X)$ it turns out to be sufficient – and easier – to study maximal ideals only.) Another way to say it is that the closed sets in the Zariski topology are precisely all sets obtained by intersecting sets of the form

$$V(f) = \{\mathfrak{m} \in \operatorname{MaxSpec} R \mid f \in \mathfrak{m}\}.$$

To see this, note first that for any ideal I of R,

$$V(I) = \bigcap_{f \in I} V(f)$$

and for any subset S of R,

$$\bigcap_{f \in S} V(f) = \bigcap_{f \in \langle S \rangle_R} V(f).$$

It is virtually immediate that the Zariski topology on $\operatorname{MaxSpec} R$ is **separated**, i.e., satisfies the T_1 separation axiom: singleton sets are closed. Indeed, for any subset $S \subseteq \operatorname{MaxSpec} S$, the Zariski closure $\overline{S}$ of S is $\bigcap_{f \in S} V(f) = V(S) = V(\langle S \rangle)$, so if $S = \{\mathfrak{m}\}$ then $\overline{S} = V(\mathfrak{m}) = \{\mathfrak{m}\} = S$. It also also easy to see that the Zariski topology on $\operatorname{MaxSpec} R$ is quasi-compact: indeed, suppose we have a family of ideals $\{I_i\}_{I \in S}$ of ideals of R such that $\bigcap_{i \in S} V(I_i) = \varnothing$. This means that there is no maximal ideal $\mathfrak{m}$ of R containing each I_i, which means that $\langle I_i \mid i \in S \rangle = R$. But the ideal generated by any family of ideals is the set of all *finite* sums of elements from the ideals, so therefore there is a finite subset T of S such that $\langle I_i \mid i \in T \rangle = R$, so $\bigcap_{i \in T} V(I_i) = \varnothing$. Thus the closed subsets in $\operatorname{MaxSpec} R$ satisfy the finite intersection condition, which is a characteristic property of quasi-compact spaces.

The Zariski topology on $\operatorname{MaxSpec} C(X)$ was first defined by M. Stone.

PROPOSITION 5.10. *Let X be any topological space. The map $\mathfrak{m} : X \to M(X)$ is continuous when $M(X)$ is given the Zariski topology.*

PROOF. As above, it is enough to show that for all $f \in C(X)$, the preimage $\mathfrak{m}^{-1}(V(f))$ is closed in X. Unpacking the definitions, we find

$$\mathfrak{m}^{-1}(V(f)) = f^{-1}(0),$$

which is closed because f is continuous. □

COROLLARY 5.11. *For a compact space X, the Zariski topology on $M(X)$ coincides with the initial topology.*

PROOF. By Theorem 5.9, we may compare the *Zariski topology on X* – the topology obtained by pulling back the Zariski topology on $M(X)$ via $\mathfrak{m}$ – with the given topology on X. But the proof of Proposition 5.10 shows that the Zariski topology on X is precisely the Z-topology, i.e., the one in which the closed subsets are the intersections of zero sets. But X is compact hence quasi-Tychonoff, so by Theorem 5.3 the Z-topology on X coincides with the given topology on X. □

Let $\pi : X \to Y$ be a continuous map of topological spaces. There is an induced map $C(\pi) : C(Y) \to C(X)$: given $g : Y \to \mathbb{R}$, we pull back by π to get $g \circ \pi : X \to \mathbb{R}$. It is no problem to see that $C(\pi)$ is a homomorphism of rings. For $x \in X$ we find:

$$C(\pi)^*(\mathfrak{m}_x) = \{g \in C(Y) \mid \pi \circ g \in \mathfrak{m}_x\} = \{g \in C(Y) \mid \pi(g(x)) = 0\} = \mathfrak{m}_{\pi(x)}.$$

In other words, maximal ideals in the image $\mathfrak{m}(X)$ pull back to maximal ideals in the image $\mathfrak{m}(Y)$, and moreover on the image this pullback map is just π. If X and Y are compact, $\mathfrak{m} : X \to M(X)$ and $\mathfrak{m} : Y \to M(Y)$ are homeomorphisms and therefore in this case we have

$$C(\pi)^* = \pi.$$

It follows that C and M are inverse anti-equivalences from the category of compact spaces to the category of rings of continuous functions on compact spaces. This gives a first glimpse at a class of very fruitful connections between topological spaces and rings of functions on them that recurs throughout several brances of mathematics. We will see another instance of this in Chapter 9.

2.5. When X is not compact. In this section we will discuss some results on $C(X)$ when the topological space is *not* compact. Unfrotunately we will have to skip many proofs, referring instead to the excellent text of Gillman-Jerison [**GJ76**].

EXAMPLE 5.12. *Let X be an infinite discrete space, so $C(X) = \mathbb{R}^X$ is the ring of* all *functions from X to $\mathbb{R}$. Thus X is a noncompact Tychonoff space. So it follows from our work so far that $\mathfrak{m} : X \to M(X)$ is a continuous injection. In fact $\mathfrak{m}$ is an embedding: for any subset $Y \subseteq X$, let I_Y be the ideal of functions vanishing identically on Y. Then*

$$V(I) \cap \mathfrak{m}(X) = \mathfrak{m}(Y),$$

so $\mathfrak{m}(Y)$ is closed in $\mathfrak{m}(X)$. Therefore $\mathfrak{m}(X)$ is an infinite discrete subspace of the quasi-compact space $M(X)$, so the map $\mathfrak{m}$ cannot be surjective.

The next result implies that we may restrict to considering Tychonoff spaces X without shrinking the class of rings $C(X)$.

THEOREM 5.13. *Let X be a topological space, let $\mathfrak{m} : X \to M(X)$ be the map $x \mapsto \mathfrak{m}_x$, and let $X_T = \mathfrak{m}(X)$, viewed as a subspace of $M(X)$.*

a) *The space X_T is Tychonoff.*
b) *The map $\mathfrak{m} : X \to X_T$ is the Tychonoff completion of X: i.e., it is universal for continuous maps from X to a Tychonoff space.*
c) *The induced map $C(\mathfrak{m}) : C(X_T) \to C(X)$ is an isomorphism of rings.*

PROOF. See [**GJ76**, §3.9]. □

Henceforth we restrict to Tychonoff spaces.

THEOREM 5.14. *Let X be a Tychonoff space.*

a) *The space $M(X)$ endowed with the Zariski topology is compact.*
b) *The map $\mathfrak{m} : X \to M(X)$ is the Stone-Čech compactification of X.*

PROOF. See [**GJ76**, §7.11]. □

%endcor

EXERCISE 5.9.

a) *Show: $C(X)$ is an $\mathbb{R}$-subalgebra of $\mathbb{R}^X$.*

b) *Show: $C(X)$ is reduced: it contains no nonzero nilpotent elements.*
c) *(T. Rzepecki) Show: for a topological space, the following are equivalent:*
(i) *The Tychonoff completion X_T of X is a one-point space.*
(ii) *We have $C(X) = \mathbb{R}$.*
(iii) *The ring $C(X)$ is a domain.*
(Suggestion: (ii) $\iff$ (i) $\implies$ (iii) are straightforward. For (iii) $\implies$ (ii), let $f \in C(X)$ be nonconstant, so $f(x) \neq f(y)$ for some $x, y \in X$. Show that for suitable real numbers C_1 and C_2 the functions $g_1 = \max(0, f_1 + C_1)$ and $g_2 = \max(0, -f_1 + C_2)$ give nonzero elements of $C(X)$ with $g_1 g_2 = 0$.)

EXERCISE 5.10. *Show $C(X)$ is connected in the algebraic sense – i.e., there are no idempotents other than 0 and 1 – if and only if the topological space X is connected.*

EXERCISE 5.11. *Show: there is an antitone Galois connection between 2^X and the set of ideals of $C(X)$, as follows:*
$S \subseteq X \mapsto I_S = \{f \in C(X) \mid f|_S \equiv 0\}$ and
$I \mapsto Y_I = \{x \in X \mid \forall f \in I, f(x) = 0\}$.

EXERCISE 5.12. *Let X be a Tychonoff space.*
a) *Let $\mathfrak{p}$ be a prime ideal of $C(X)$. Show: $\#Y_{\mathfrak{p}} \leqslant 1$.*
b) *Suppose X is moreover compact. Deduce:*
(i) *The space $Y_{\mathfrak{p}}$ consists of exactly one point.*
(ii) *A prime ideal $\mathfrak{p}$ of $C(X)$ is closed in the sense of the Galois connection – i.e., $\mathfrak{p} = I_{Y_{\mathfrak{p}}}$ if and only if $\mathfrak{p}$ is maximal.*
(iii) *Each prime ideal $\mathfrak{p}$ of $C(X)$ is contained in a* unique *maximal ideal.*

A commutative ring in which each prime ideal is contained in a unique maximal ideal is called a **Gelfand ring** (or sometimes an **h-local ring**, though I don't know what the "h" is for); this class of rings will be studied in Chapter 13. Two evident classes of Gelfand rings are the local rings (i.e., there is a unique maximal ideal) and the zero-dimensional rings (i.e., every prime ideal is maximal).

EXERCISE 5.13. *Let X be a finite topological space. Show:* $\dim C(X) = 0$.
(Hint: the conclusion holds for any ring that is finite-dimensional as an algebra over a field.)

If X is an infinite compact space, then since $M(X) \cong X$ is infinite, evidently $C(X)$ is not local. It is less immediately clear whether $C(X)$ is zero-dimensional.

EXAMPLE 5.15. *Let X be an infinite compact subset of $\mathbb{R}^N$ that is Zariski-dense: a polynomial $f \in \mathbb{R}[t_1, \ldots, t_N]$ that vanishes identically on X must vanish identically on $\mathbb{R}^N$ and must therefore be the zero polynomial. (Notice that every infinite subset of $\mathbb{R}$ is Zariski-dense.) Let S be the submonoid of $\mathbb{R}[t_1, \ldots, t_N]$ generated by polynomials of the form $t_i - x_i$ for some $1 \leqslant i \leqslant N$ and $x_i \in \mathbb{R}$. Because X is Zariski-dense in $\mathbb{R}^N$, each element of S induces a nonzero element of $C(X)$. Therefore we may apply Theorem 4.9 to get a prime ideal $\mathfrak{p}$ of $C(X)$ that is disjoint from S. In particular, for all $x = (x_1, \ldots, x_N) \in X$, we have $(t_1 - x_1) \cdots (t - N - x_N) \in \mathfrak{m}_x \backslash \mathfrak{p}$. Since every maximal ideal of $C(X)$ is of the form $\mathfrak{m}_x$ for some $x \in X$, it follows that $\mathfrak{p}$ is not maximal. So* $\dim X \geqslant 1$.

But this is just the tip of the iceberg.

THEOREM 5.16. *(Wofsey) Let X be a topological space.*

a) *The following are equivalent:*
   (i) *Every prime ideal of $C(X)$ is maximal.*
   (ii) *Every chain of prime ideals in $\operatorname{Spec} C(X)$ has length less than $\mathfrak{c} = \#\mathbb{R}$.*
   (iii) *Every $f \in C(X)$ is locally constant.*

PROOF. Notice that (i) $\implies$ (ii) is immediate. We will give the proof of (iii) $\implies$ (i) now. Later in the chapter, after developing some machinery for a similar result, we will show that if there is $f \in C(X)$ that is not locally constant, then $\operatorname{Spec} C(X)$ has a chain that is order-isomorphic to $\mathbb{R}$, which by contraposition gives (ii) $\implies$ (iii), completing the proof.

The proof of (iii) $\implies$ (i) is short but uses a result that we will prove in Chapter 7. Namely, we CLAIM that if every $f \in C(X)$ is locally constant, then every principal ideal of $C(X)$ is idempotent, so by Proposition 3.103 the ring $C(X)$ is absolutely flat. Let $\mathfrak{p}$ be a prime ideal of $C(X)$. By Exercise 3.91 the quotient $C(X)/\mathfrak{p}$ is an absolutely flat domain. Let x be a nonzero element of $C(X)/\mathfrak{p}$. Since the principal ideal (x) is idempotent, we have $(x) = (x)^2 = (x^2)$. Since we are in a domain, this implies $x = ux^2$ for some $u \in (C(X)/\mathfrak{p})^\times$, and since x is not a zero-divisor we may cancel it to get $ux = 1$, so $x \in (C(X)/\mathfrak{p})^\times$. This implies that $C(X)/\mathfrak{p}$ is a field and thus that $\mathfrak{p}$ is maximal.

Now let us establish the claim. If $f \in C(X)$ is locally constant, then

$$g : x \mapsto \begin{cases} \frac{1}{f(x)} & \text{if } f(x) \neq 0 \\ 0 & \text{if } f(x) = 0 \end{cases}$$

is also an element of $C(X)$. We get immediately that $f = gf^2$, so $(f) = (f^2)$, completing this part of the proof. □

In Theorem 5.16, the equivalence of (i) and (iii) already appears in the text of Gillman-Jerison [**GJ76**]. They call a Tychonoff space X for which every $f \in C(X)$ is locally constant a **P-space** and show that this is equivalent to each of the following properties: (i) every zero-set in X is open; (ii) every G_δ-set (i.e., countable intersection of open sets) is open; every ideal of $C(X)$ is a radical ideal; (ii) for all $f, g \in C(X)$ we have $\langle f, g\rangle = \langle f^2 + g^2\rangle$, hence in particular all finitely generated idals of $C(X)$ are principal; $C(X)$ is absolutely flat.

COROLLARY 5.17. *(Wofsey) Let X be an infinite space. Suppose that X is either compact or is both Tychonoff and connected. Then X is a P-space, and thus*

$$\dim C(X) \geqslant \mathfrak{c}.$$

PROOF. In each case, we will construct a continuous function $f : X \to \mathbb{R}$ that is not locally constant. The conclusion then follows from Theorem 5.16.

Suppose first that X is an infinite, connected Tychonoff space. Since X is connected, every locally constant function on X is constant. But since X is Tychonoff, it is C-separated, which since it has more than one point, means that $C(X) \supsetneq \mathbb{R}$. So there is $f \in C(X)$ that is not locally constant.

Next suppose that X is compact. Let us first address the case in which X is moreover metrizable, since we can make a simpler argument here. Choose any infinite subset of X, and form an injective sequence with its terms. Since X is alsosequentially compact, this sequence admits a convergent subsequence. This

shows that there is an injective convergence sequence $\{x_n\}_{n=1}^{\infty}$ converging to some $x_\bullet \in X$. The function $x \mapsto d(x, x_\bullet)$ (where d is some metric inducing the topology on X) is then 0 at $x_\bullet$ but not in any ϵ-ball around $x_\bullet$, so is continuous and not locally constant.

Now let X be any infinite compact space. Being an infinite Hausdorff space, X admits a countably infinite discrete subspace Y, which we may arrange into the terms of an injective sequence $\{x_n\}$. By Tietze"s Extension Theorem, for all $n \in \mathbb{Z}^+$ there is a continuous function $f : X \to [0, 2^{-n}]$ such that $f(x) = 2^{-n}$ if $x \in \{x_1, \ldots, x_n\}$ and $f(x) = 0$ otherwise. Then $f := \sum_{n=1}^{\infty} f_n$ is an element of $C(X)$, since each partial sum is continuous and f is the uniform limit of the sequence of partial sums. We have $f(x_n) = 2^{1-n}$, so $f|_Y$ is injective. Since X it is compact, the infinite subset Y has a limit point: that is, there is $x_\bullet \in X$ such that every neighborhood U of $x_\bullet$ contains a point of $Y \backslash \{x_\bullet\}$, and indeed, since X is Hausdorff, infinitely many such points. The function f is therefore not locally constant at $x_\bullet$. □

EXERCISE 5.14. *Let $X = [0,1]$ with the standard Euclidean topology. Let $\mathfrak{r}_0$ be the ideal of all functions $f \in C(X)$ such that for all $k \in \mathbb{N}$, $\lim_{x \to 0^+} \frac{f(x)}{x^k} = 0$. Equivalently $\mathfrak{r}_0$ is the ideal of all functions which are infinitely differentiable at 0 and have identically zero Taylor series at zero.*

a) *Show: $\mathfrak{r}_0$ is radical but not prime.*
b) *Show: the only maximal ideal containing $\mathfrak{r}_0$ is*
$$\mathfrak{m}_0 := \{f \in C([0,1]) \mid f(0) = 0\}.$$
c) *Deduce: there are ideals of $C(X)$ that are prime but not maximal.*

EXERCISE 5.15. *Let X be a C-separated topological space.*

a) *Let $S \subseteq X$ with $\#S > 1$. Show: I_S is not maximal.*
b) *Suppose X is Tychonoff and $S, T \subseteq X$. Show: $I_S \subseteq I_T \iff \overline{T} \subseteq \overline{S}$.*
c) *Show: if X is Tychonoff, then for closed $S, T \subseteq X$, we have $I_S = I_T \iff S = T$.*

EXERCISE 5.16. *Let $\varphi : X \to Y$ be a continuous function between topological spaces.*

a) *Show: φ induces a ring homomorphism $C(\varphi) : C(Y) \to C(X)$ by $g \in C(Y) \mapsto \varphi^* g = g \circ \varphi$.*
b) *Suppose Y is normal, that X is a closed subspace of X and $\varphi : X \to Y$ is the inclusion map. Show: $C(\varphi)$ is surjective.*

EXERCISE 5.17. *Let X be a normal topological space. Show: the closure operator on subsets of X given by the Galois connection is the topological closure.*

EXERCISE 5.18. *Let $X = \{0\} \cup \{\frac{1}{n}\}_{n \in \mathbb{Z}^+} \subseteq \mathbb{R}$, and let $\mathfrak{m}$ be the maximal ideal of functions vanishing at 0. Fill in the details of the following proof that $\mathfrak{m}$ is* not *finitely generated.*[4] *Assume not: $\mathfrak{m} = \langle a_1, \ldots, a_n \rangle$. Then for all $g \in \mathfrak{m}$, $\lim_{x \to 0} \frac{g^2(x)}{|a_1(x)| + \ldots + |a_n(x)|} = 0$. (Show also that there is $\delta > 0$ such that the denominator is strictly positive on $(0, \delta)$.) Now choose $g \in \mathfrak{m}$ so as to get a contradiction.*

EXERCISE 5.19. *Let X be a normal space, and let $x \in X$.*

[4]Or, if you like, give your own proof that $\mathfrak{m}$ is not finitely generated!

a) *Show that the following are equivalent:*
   (i) *The ideal I_x is finitely generated.*
   (ii) *The ideal I_x is principal.*
   (iii) *The point x is isolated in X (i.e., $\{x\}$ is open).*
b) *Suppose X is compact. Show that the following are equivalent:*
   (i) *The ring $C(X)$ is Noetherian.*
   (ii) *The ring $C(X)$ is finite-dimensional as an $\mathbb{R}$-vector space.*
   (iii) *The set X is finite.*

EXERCISE 5.20. *Show: if we worked throughout with rings $C(X, \mathbb{C})$ of continuous $\mathbb{C}$-valued functions, then all of the above results continue to hold.*

EXERCISE 5.21. *Suppose we looked at rings of continuous functions from a topological space X to $\mathbb{Q}_p$. To what extent to the results of the section continue to hold?*

EXERCISE 5.22. *Let X be a compact smooth manifold and consider the ring $C^\infty(X)$ of smooth functions $f : X \to \mathbb{R}$.*

a) *Show: for $x \in X$, $\{f \in C^\infty(X) \mid f(x) = 0\}$ is a* finitely generated *maximal ideal.*
b) *The phenomenon of part a) is in contrast to the case of maximal ideals in the ring $C([0,1])$, say. However, I believe that with this sole exception, all of the results of this section hold for the rings $C^\infty(X)$ just as for the rings $C(X)$. Try it and see.*

2.6. A theorem of B. Sury.

THEOREM 5.18. *(Sury) Let $c \in [0,1]$, and let $\mathfrak{m}_c = \{f \in C([0,1]) \mid f(c) = 0\}$. Then $\mathfrak{m}_c$ admits no* countable *generating set.*

PROOF. Let $\{f_n\}_{n=1}^\infty$ be a countably infinite subset of $\mathfrak{m}_c$, and let $J = \langle \{f_n\}_{n=1}^\infty \rangle$. It suffices to exhibit $f \in \mathfrak{m}_c \backslash J$. By rescaling, we may assume $||f_n|| \leqslant 1$ for all n. And we may assume $\bigcap_{n=1}^\infty f_n^{-1}(0) = \{c\}$: otherwise $x \mapsto |x - c|$ lies in $\mathfrak{m}_c \backslash J$. Put

$$f(x) = \sum_{n=1}^\infty \sqrt{\frac{|f_n(x)|}{2^n}}.$$

The series is uniformly convergent (by "Weierstrass's M-Test") and thus f, being the uniform limit of continuous functions, is itself continuous. Moreover $f^{-1}(0) = \{c\}$, and in particular $f \in \mathfrak{m}_c$. Seeking a contradiction, we suppose $f \in J$: then there is $r \in \mathbb{Z}^+$ and $g_1, \ldots, g_r \in C([0,1])$ such that

$$f = \sum_{n=1}^r g_n f_n.$$

Let $M = \max_{1 \leqslant n \leqslant r} ||g_n||$, so $||f|| \leqslant M \sum_{n=1}^r ||f_n||$. Let U be a neighborhood of c such that $||\sqrt{f_n}||_U < \frac{1}{2^n M}$ for $1 \leqslant n \leqslant r$. Since $f = \sum_{n=1}^r g_n f_n$ vanishes only at c, for each $x \in U \backslash \{c\}$, there exists $1 \leqslant N \leqslant r$ such that $f_N(x) \neq 0$ and thus

$$|f_N(x)| < \frac{\sqrt{|f_N(x)|}}{2^N M}.$$

Hence

$$|f(x)| \leqslant M \sum_{n=1}^r |f_n(x)| < \sum_{n=1}^r \frac{\sqrt{|f_n(x)|}}{2^n} \leqslant |f(x)|,$$

a contradiction. □

EXERCISE 5.23. *Let X be a compact topological space, and let $c \in X$ be such that there is $f \in C(X)$ such that $f^{-1}(0) = \{c\}$. (Note: this condition holds for all points $c \in X$ if X is perfectly normal, which in turn holds if X is metrizable.) For the maximal ideal $\mathfrak{m}_c := \{f \in C(X) \mid f(c) = 0\}$, show that the following are equivalent:*

(i) *The point c is isolated in X.*
(ii) *The ideal $\mathfrak{m}_c$ is principal.*
(iii) *The ideal $\mathfrak{m}_c$ is countably generated.*

3. Rings of holomorphic functions

We have just seen that the ring of continuous functions on a topological space is very rarely a domain. A remedy for this is to consider more "rigid" collections of functions. Let U be an open subset of the complex plane $\mathbb{C}$, and let $\mathrm{Hol}(U)$ be the set of holomorphic functions $f : U \to \mathbb{C}$. (A holomorphic function on U is one for which the complex derivative $f'(z)$ exists for each $z \in U$. Equivalently, for each $z \in U$ f admits a power series expansion with positive radius of convergence.) Then $\mathrm{Hol}(U) \subseteq \mathbb{C}^U$, the ring of all $\mathbb{C}$-valued functions on U.

PROPOSITION 5.19. *For nonempty open $U \subseteq \mathbb{C}$, the following are equivalent:*

(i) *The set U is connected.*
(ii) *The ring $\mathrm{Hol}(U)$ is a domain.*

PROOF. (i) $\implies$ (ii): For any $f \in C(U, \mathbb{C})$ let $Z(f) = \{z \in U \mid f(z) = 0\}$ be the zero set of f. Since f is continuous, $Z(f)$ is a closed subset of U. If f is moreover holomorphic, then $Z(f)$ has no accumulation point in U, i.e., $f \neq 0 \implies Z(f)$ is discrete – in particular $Z(f)$ is countable. Moreover, for any $f, g \in C(U, \mathbb{C})$ we have $Z(fg) = Z(f) \cup Z(g)$, so if $f, g \in \mathrm{Hol}(U)^\bullet$ then $Z(fg)$ is at most countable, whereas U is uncountable, so $fg \neq 0$.
$\neg$ (i) $\implies$ $\neg$ (ii): If U is not connected, then $U = V_1 \cup V_2$ where V_1 and V_2 are disjoint open subsets. Let χ_i be the characteristic function of V_i for $i = 1, 2$. Then each χ_i is locally constant on U – hence holomorphic, and nonzero, but $\chi_1 \chi_2 = 0$. □

In complex function theory it is common to call a nonempty connected open $U \subseteq \mathbb{C}$ a **domain**. Henceforth we assume that U is a domain. For $z \in U$ there is a function $\mathrm{ord}_z : \mathrm{Hol}(U)^\bullet \to \mathbb{N}$, the **order of vanishing of f at z**: we expand f into a power series at z: $f(\zeta) = \sum_{n=0}^{\infty} a_n (\zeta - z)^n$ and let $\mathrm{ord}_z(f)$ be the least n for which $a_n \neq 0$. Compiling these we associate to each $f \in \mathrm{Hol}(U)^\bullet$ its **total order** $\mathrm{Ord}(f) : U \to \mathbb{N}$ given by $\mathrm{Ord}(f)(z) = \mathrm{ord}_z(f)$. Consider the set $\mathbb{N}^U$ of all functions from U to $\mathbb{N}$. For $O \in \mathbb{N}^U$, we define the **support** of O to be the set of $z \in U$ such that $O(z) > 0$.

A *meromorphic function* on U is a function which is holomorphic on U except for isolated finite order singularities. More precisely, a meromorphic function is a function which is holomorphic on $U \backslash Z$ for some discrete closed subset Z of U and such that for all $z_0 \in Z$, there exists $n \in \mathbb{Z}^+$ such that $(z - z_0)^n f(z)$ extends to a holomorphic function on a neighborhood of z. If the least n as above is positive, we say that f has a pole at z_0, and we employ the convention that $f(z_0) = \infty$. Let

$\mathrm{Mer}(U)$ be the set of all meromorphic functions on U; it is a ring under pointwise addition and multiplication, under the conventions that for all $z \in \mathbb{C}$,

$$z + \infty = \infty + \infty = z \cdot \infty = \infty \cdot \infty = \infty.$$

THEOREM 5.20. *(Weierstrass + Mittag-Leffler) Let $U \subseteq \mathbb{C}$ be a domain.*

a) *If $O \in \mathbb{N}^U$ has closed, discrete support, there is $f \in \mathrm{Hol}(U)^\bullet$ with $\mathrm{Ord}(f) = O$.*

b) *Let $Z \subseteq U$ be a closed subset without limit points. To each $z \in Z$ we associate $n_z \in \mathbb{N}$ and $w_{z,k} \in \mathbb{C}$ for all $0 \leqslant k \leqslant n_z$. Then there is $f \in \mathrm{Hol}(U)$ such that for all $z \in Z$ and $0 \leqslant k \leqslant n_z$, $f^{(k)}(z) = k! w_{z,k}$.*

PROOF. Part a) is part of Weierstrass' Factorization Theory [**Ru87**, Thm. 15.11]. To get part b), combine part a) with Mittag-Leffler's result on the existence of meromorphic functions with prescribed principal parts [**Ru87**, Thm. 15.13]. □

COROLLARY 5.21. *The ring $\mathrm{Mer}(U)$ of meromorphic functions on U is a field, and indeed is the field of fractions of $\mathrm{Hol}(U)$.*

EXERCISE 5.24. *Prove Proposition 5.21.*

EXERCISE 5.25. *Fix $z_0 \in U$. For $f \in \mathrm{Mer}(U)$, choose $n \in \mathbb{N}$ such that $(z - z_0)^n f$ is holomorphic at z_0, and put $\mathrm{ord}_{z_0}(f) = \mathrm{ord}_{z_0}((z - z_0)^n f) - n$.*

a) *Show that this gives a well-defined function $\mathrm{ord}_{z_0} : \mathrm{Mer}(U)^\bullet \to \mathbb{Z}$ (i.e., independent of the choice of n in the definition).*

b) *Show that for all $f, g \in \mathrm{Mer}(U)^\times$, $\mathrm{ord}_{z_0}(fg) = \mathrm{ord}_{z_0}(f) + \mathrm{ord}_{z_0}(g)$.*

c) *We formally extend ord_{z_0} to a function from $\mathrm{Mer}(U)$ to $\mathbb{Z} \cup \{\infty\}$ by setting $\mathrm{ord}_{z_0}(0) = \infty$. Show that, under the convention that $\infty + n = \infty + \infty = \infty$, we have for all $f, g \in \mathrm{Mer}(U)$ that $\mathrm{ord}_{z_0}(f + g) \geqslant \min \mathrm{ord}_{z_0}(f), \mathrm{ord}_{z_0}(g)$.*

d) *Show that if $\mathrm{ord}_{z_0}(f) \neq \mathrm{ord}_{z_0}(g)$ then $\mathrm{ord}_{z_0}(f+g) = \min \mathrm{ord}_{z_0} f, \mathrm{ord}_{z_0}(g)$.*

Similarly we may extend Ord to a function from $\mathrm{Mer}(U)^\bullet$ to $\mathbb{Z}^U$.

LEMMA 5.22. *For $f, g \in \mathrm{Hol}(U)^\bullet$, the following are equivalent:*

(i) $\mathrm{Ord}(f) = \mathrm{Ord}(g)$.
(ii) *$f = ug$ for $u \in \mathrm{Hol}(U)^\times$.*
(iii) $(f) = (g)$.

PROOF. (ii) $\iff$ (iii) for elements of any domain.
(ii) $\implies$ (i) is easy and left to the reader.
(i) $\implies$ (ii): The meromorphic function $\frac{f}{g}$ has identically zero order, hence is nowhere vanishing and is thus a unit u in $\mathrm{Hol}(U)$. □

THEOREM 5.23. *(Helmer [**He40**]) For a domain U in the complex plane, every finitely generated ideal of $\mathrm{Hol}(U)$ is principal. More precisely, for any $f_1, \ldots, f_n \in \mathrm{Hol}(U)^\bullet$, there exists $f \in \mathrm{Hol}(U)$ such that $\mathrm{Ord}(f) = \min_i \mathrm{Ord}(f_i)$, unique up to associates, and then $\langle f_1, \ldots, f_n \rangle = \langle f \rangle$.*

PROOF. Step 1: Suppose $f_1, f_2 \in \mathrm{Hol}(U)^\bullet$ don't both vanish at any $z \in U$. Let Z be the zero set of f_1, so for all $z \in Z$, $f_2(z) \neq 0$. Theorem 5.20b) gives $g_2 \in \mathrm{Hol}(U)$ such that for all $z \in Z$, $\mathrm{ord}_z(1 - g_2 f_2) \geqslant \mathrm{ord}_z(f_1)$. Thus $\mathrm{Ord}(1 - g_2 f_2) \geqslant \mathrm{Ord}(f_1)$, so $g_1 := \frac{1 - g_2 f_2}{f_1} \in \mathrm{Hol}(U)$, $f_1 g_1 + f_2 g_2 = 1$ and $\langle f_1, f_2 \rangle = \mathrm{Hol}(U)$.
Step 2: Now let $f_1, f_2 \in \mathrm{Hol}(U)^\bullet$ be arbitrary. By Theorem 5.20a), there exists

$f \in \mathrm{Hol}(U)$ with $\mathrm{Ord}(f) = \min \mathrm{Ord}(f_1), \mathrm{Ord}(f_2)$. For $i = 1, 2$, put $g_i = \frac{f_i}{f}$. Then g_1 and g_2 are holomorphic and without a common zero, so by Step 1 $\langle g_1, g_2 \rangle = \mathrm{Hol}(U)$. Multiplying through by f gives $\langle f_1, f_2 \rangle = \langle f \rangle$.
Step 3: If in a ring every ideal of the form $\langle x_1, x_2 \rangle$ is principal, then every finitely generated ideal is principal. By Step 2, this applies in particular to $\mathrm{Hol}(U)$. Moreover, if the ideal $\langle f_1, \ldots, f_n \rangle = \langle f \rangle$, then we must have $\mathrm{Ord}\, f = \min \mathrm{Ord}\, f_i$. □

EXERCISE 5.26. *Explain why in Step 1 above, Theorem 5.20b) implies that g_2 exists.*

The most familiar domains in which every finitely generated ideal is principal are those in which *every* ideal is principal: PIDs! But as the reader may have already suspected, if $\mathrm{Hol}(U)$ were a PID, we would have said so by now: indeed it is not. One way to see this is to show that $\mathrm{Hol}(U)$ is not even a UFD. Remarkably, this is a consequence of the Weierstrass Factorization Theory, which expresses every holomorphic function as a product of prime elements! The catch is that most holomorphic functions require *infinite* products, a phenomenon which is not countenanced in the algebraic theory of factorization.

EXERCISE 5.27. *Let $f \in \mathrm{Hol}(U)^\bullet$.*

a) *Show that f is an irreducible element of $\mathrm{Hol}(U)$ – i.e., if $f = g_1 g_2$ then exactly one of g_1, g_2 is a unit – if and only if it has exactly one simple zero.*
b) *Suppose f is irreducible. Show: $\mathrm{Hol}(U)/(f) = \mathbb{C}$. In particular, (f) is prime.*
c) *Show: f admits a (finite!) factorization into irreducible elements if and only if f has only finitely many zeros. Conclude that $\mathrm{Hol}(U)$ is not a UFD.*

EXERCISE 5.28.

a) *Show: all the results of this section extend to the ring of holomorphic functions on a noncompact Riemann surface.*
b) *Investigate which of the results of this section hold for all Stein manifolds.*[5]

4. Kapovich's Theorem and Wofsey's Theorem

4.1. The cardinal Krull dimension of a partially ordered set.

Throughout, all rings are commutative and with multiplicative identity. For a ring R, $\mathrm{Spec}\, R$ is the set of prime ideals of R, partially ordered under inclusion.

A **chain** is a linearly ordered set; its **length** is its cardinality minus one. The **cardinal Krull dimension** $\mathrm{carddim}\, X$ of a partially ordered set X is the supremum of lengths of its chains. For a ring R we put $\mathrm{carddim}\, R = \mathrm{carddim}\, \mathrm{Spec}\, R$.

REMARK 3. *The prime spectrum $\mathrm{Spec}\, R$ of a ring is endowed with the Zariski topology, in which the closed sets are $V(I) = \{\mathfrak{p} \in \mathrm{Spec}\, R \mid \mathfrak{p} \supset I\}$ as I ranges over all ideals of R. For $\mathfrak{p}_1, \mathfrak{p}_2 \in \mathrm{Spec}\, R$ we have $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \iff \mathfrak{p}_2 \in \overline{\{\mathfrak{p}_1\}}$. Thus $\mathrm{carddim}\, R$ is a topological invariant of $\mathrm{Spec}\, R$.*

For a topological space X, define the cardinal Krull dimension $\mathrm{carddim}\, X$ as

[5]Step 1: learn the definition of a Stein manifold!

the supremum of lengths of chains of closed irreducible subspaces of X. Since for a ring R the map $\mathfrak{p} \mapsto V(\mathfrak{p})$ gives an antitone bijection from $\operatorname{Spec} R$ *to the set of closed irreducible subspaces of* $\operatorname{Spec} R$*, we have* $\operatorname{carddim} R = \operatorname{carddim} \operatorname{Spec} R$.

Our use of the word "cardinal" is twofold: (i) it is common to say "$\dim R$ is infinite" if there are arbitrarily long finite chains in $\operatorname{Spec} R$. For the class of rings considered here we will show the Krull dimension is zero or infinite, but we will not completely answer the more refined question of how infinite it is. (ii) There is also a notion of **ordinal Krull dimension** of rings [**GoRo**] that we do not discuss here.

REMARK 4.

a) *Let X and Y bre partially ordered sets. If there is an injective isotone map $\iota : Y \to X$, then* $\operatorname{carddim} Y \leqslant \operatorname{carddim} X$.
b) *If $f : R_1 \to R_2$ is surjective or a localization map, then $f^* : \operatorname{Spec} R_2 \to \operatorname{Spec} R_1$ is an injective isotone map, so* $\operatorname{carddim} R_2 \leqslant \operatorname{carddim} R_1$.

4.2. Holomorphic functions on a $\mathbb{C}$-manifold.

Let M be a $\mathbb{C}$-manifold. (Our definition includes that M is Hausdorff and second countable.) Let $\operatorname{Hol}(M)$ be the ring of global holomorphic functions $f : M \to \mathbb{C}$. We have $\mathbb{C} \hookrightarrow \operatorname{Hol}(M)$ via the constant functions.

LEMMA 5.24. *The ring* $\operatorname{Hol}(M)$ *is a domain if and only if M is connected.*

PROOF. If $M = M_1 \coprod M_2$ with $M_1, M_2 \neq \varnothing$, let f_i be the characteristic function of M_i. Then $f_1, f_2 \in \operatorname{Hol}(M)^\bullet$ and $f_1 f_2 = 0$.

Conversely, let $f \in \operatorname{Hol}(M)^\bullet$, and let U be the set of $x \in M$ such that the power series expansion at x is zero (as a formal series: i.e., every term is zero). For all $x \in U$, f vanishes identically in some neighborhood of x, so U is open. If $x \in M \backslash U$, then some mixed partial derivative of f is nonvanishing at x. These mixed partials are continuous, so there is a neighborhood N_x of x on which this condition continues to hold, and thus $N_x \subseteq M \backslash U$ and U is closed. Since M is connected and $U \subsetneq M$, we have $U = \varnothing$. For $f, g \in \operatorname{Hol}(M)^\bullet$, let $x \in M$. The power series of f and g at x are each nonzero, hence the same holds for fg. So fg does not vanish identically on any neighborhood of x: thus $fg \neq 0$. □

From now on we will assume that all our $\mathbb{C}$-manifolds are connected.

4.3. Kapovich's Theorems: Statements.

THEOREM 5.25. *(Kapovich* [**Ka17**]*) Let M be a $\mathbb{C}$-manifold. Then either* $\operatorname{Hol}(M) = \mathbb{C}$ *or* $\operatorname{carddim} \operatorname{Hol}(M) \geqslant \mathfrak{c} = 2^{\aleph_0}$.

A **discrete valuation** on a ring R is a surjective function

$$v : R \to \mathbb{N} \cup \{\infty\}$$

such that
(DV0) For all $x \in R$, $v(x) = \infty \iff x = 0$.
(DV1) For all $x, y \in R$, $v(xy) = v(x) + v(y)$.
(DV2) For all $x, y \in R$, $v(x + y) \geqslant \min v(x), v(y)$.

Here we use some standard conventions on arithmetic in the extended real numbers: for all $x \in [0, \infty]$, $x + \infty = \infty$ and $\min(x, \infty) = x$. Conditions (DV0) and (DV1)

ensure that a ring that admitting a discrete valuation is a domain.

A V_∞**-ring** is a ring R admitting a sequence $\{v_k\}_{k\in\mathbb{Z}^+}$ of discrete valuations such that for any sequence $\{n_k\}_{k=1}^\infty$ of natural numbers there is $x \in R^\bullet$ such that $v_k(x) = n_k$ for all $k \in \mathbb{Z}^+$. The following results together imply Theorem 5.25.

THEOREM 5.26. *If R is a V_∞-ring, then* $\operatorname{carddim} R \geqslant \mathfrak{c}$.

THEOREM 5.27. *Let M be a $\mathbb{C}$-manifold. If M admits a nonconstant holomorphic function, then* $\operatorname{Hol}(M)$ *is a V_∞-ring.*

4.4. Preliminaries on ultralimits.

Let I be a set, let X be a topological space, and let $x_\bullet : I \to X$ be a function. Let $\mathcal{F}$ be an ultrafilter on I. We say $x \in X$ is an **ultralimit** of $x_\bullet$ and write $\mathcal{F}\lim x_\bullet = x$ if $x_\bullet(\mathcal{F}) \to x$: that is, for every neighborhood U of $x \in X$, we have $x_\bullet^{-1}(U) \in \mathcal{F}$. From the general theory of filter convergence, we deduce: (i) If X is Hausdorff, then every I-indexed sequence $x_\bullet : I \to X$ has at most one ultralimit. (ii) If X is quasi-compact, then every I-indexed sequence has at least one ultralimit. Thus (iii) If X is compact, then every I-indexed sequence has a unique ultralimit. In our application we will have $I = \mathbb{N}$, ω a fixed nonprincipal ultrafilter and $X = [0, \infty]$. Thus we have an ordinary sequence $\{x_n\}$ in $[0, \infty]$; let us spell out what $\omega \lim x_n = x$ means. If $x < \infty$, it means that for all $\epsilon > 0$, we have

$$\{n \in \mathbb{N} \mid |x_n - x| < \epsilon\} \in \omega.$$

If $x = \infty$, it means that for all $M \in [0, \infty)$, we have

$$\{n \in \mathbb{N} \mid x_n > M\} \in \omega.$$

Because $[0, \infty]$ is compact, any sequence in $[0, \infty]$ has a unique ultralimit.

EXERCISE 5.29. *Let ω be a nonprincipal ultrafilter on $\mathbb{Z}^+$.*

a) *Show: if $\lim_{k\to\infty} x_k = x$ in the usual sense, then also $\omega \lim_k x_k = x$.*
b) *Let $\{x_k\}$, $\{y_k\}$ be sequences in $[0, \infty]$. Show:*
   (i) $\omega \lim_k (x_k + y_k) = \omega \lim_k x_k + \omega \lim_k y_k$.
   (ii) $\omega \lim_k \min(x_k, y_k) = \min(\omega \lim_k x_k, \omega \lim_k y_k)$.
   (iii) $\omega \lim_k \max(x_k, y_k) = \max(\omega \lim_k x_k, \omega \lim_k y_k)$.

4.5. Proof of Theorem 5.26.

For $t \in (0, \infty)$, put

$$\mathfrak{p}_t = \{x \in R^\bullet \mid \omega \lim_k \frac{v_k(x)}{k^t} > 0\}.$$

Each $\mathfrak{p}_t$ is a prime ideal, and for all $t_1 \geqslant t_2$ we have $\mathfrak{p}_{t_1} \subseteq \mathfrak{p}_{t_2}$. Since R is a V_∞-ring, there is $x_t \in R^\bullet$ such that $v_k(x_t) = \lceil k^t \rceil$ for all $k \in \mathbb{Z}^+$, and we have $x_t \in \mathfrak{p}_t$, $x_t \notin \mathfrak{p}_s$ for all $s > t$. So $\{\mathfrak{p}_t \mid t \in (0, \infty)\}$ is a chain of prime ideals of R of cardinality $\mathfrak{c}$.

4.6. Proof of Theorem 5.27.

Let $h : M \to \mathbb{C}$ be holomorphic and nonconstant. By the Open Mapping Theorem, $U = h(M)$ is a connected open subset of $\mathbb{C}$. In particular U is metrizable and not compact, so there is a sequence $\{z_k\}_{k=1}^\infty$ of distinct points of U with no accumulation point in U. We do not disturb the latter property by successively

replacing each z_k with any point in a sufficiently small open ball, so by Sard's Theorem we may assume that each z_k is a regular value of h. For $k \in \mathbb{Z}^+$, let $p_k \in h^{-1}(z_k)$ and let $v_k : \mathrm{Hol}(M)^\bullet \to \mathbb{N}$ be the order of vanishing of h at p_k: that is, the least N such that there is a mixed partial derivative of order N which is nonvanishing at p_k. Then v_k is a discrete valuation. Let $\{n_k\}_{k=1}^\infty$ be as sequence of natural numbers. By Theorem 5.20a), there is $g \in \mathrm{Hol}(U)$ such that $\mathrm{ord}_{z_k}(g) = n_k$ and thus – since p_k is a regular value for h – for all $k \in \mathbb{Z}^+$ we have $v_k(g \circ h) = n_k$.

4.7. The cardinal Krull dimension of a Stein manifold.

We will now prove a stronger lower bound on the cardinal Krull dimension of $\mathrm{Hol}(M)$ for when M is a **Stein manifold**: a $\mathbb{C}$-manifold which admits a closed (equivalently proper) holomorphic embedding into $\mathbb{C}^N$ for some $N \in \mathbb{Z}^+$. Stein manifolds play the role in the biholomorphic category that affine varieties play in the algebraic category (of quasi-projective varieties $V_{/\mathbb{C}}$, say) – and a nonsingular affine variety over $\mathbb{C}$ is a Stein manifold – namely the $\mathbb{C}$-manifolds which have "enough" global holomorphic functions: in particular, for points $x \neq y$ on a Stein manifold M, there is $f \in \mathrm{Hol}(M)$ with $f(x) \neq f(y)$. At the other extreme lie the compact $\mathbb{C}$-manifolds, which play the role in the biholomorphic category that projective varieties play in the algebraic category – and a nonsingular projective variety over $\mathbb{C}$ is a compact $\mathbb{C}$-manifold). In dimension one this is a simple dichotomy: a Riemann surface is a Stein manifold if and only if it is noncompact [**GuRo**, p. 209].

THEOREM 5.28. *If S_1, S_2 are noncompact Riemann surfaces then*

$$\mathrm{carddim}\,\mathrm{Hol}(S_1) = \mathrm{carddim}\,\mathrm{Hol}(S_2) \geqslant 2^{\aleph_1}.$$

PROOF. Henriksen showed $\mathrm{Hol}(\mathbb{C}) \geqslant 2^{\aleph_1}$ [**He53**]. For noncompact Riemann surfaces S and T, Alling showed $\mathrm{Spec}\,\mathrm{Hol}(S)$ and $\mathrm{Spec}\,\mathrm{Hol}(T)$ are homeomorphic [**Al63**]. By Remark 3 it follows that $\mathrm{carddim}\,\mathrm{Hol}(S) = \mathrm{carddim}\,\mathrm{Hol}(\mathbb{C}) \geqslant 2^{\aleph_1}$. □

LEMMA 5.29. *Let M_1, M_2 be $\mathbb{C}$-manifolds. Then*

$$\mathrm{carddim}\,\mathrm{Hol}(M_1 \times M_2) \geqslant \mathrm{carddim}\,\mathrm{Hol}(M_1).$$

PROOF. Fix $y_0 \in M_2$. Pulling back holomorphic functions via the embedding

$$\iota : M_1 \hookrightarrow M_1 \times M_2,\ x \mapsto (x, y_0)$$

gives a ring homomorphism $\iota^* : \mathrm{Hol}(M_1 \times M_2) \to \mathrm{Hol}(M_1)$. If $f \in \mathrm{Hol}(M_1)$ put

$$F : M_1 \times M_2 \to \mathbb{C},\ (x, y) \mapsto f(x).$$

Then $F \in \mathrm{Hol}(M_1 \times M_2)$ and $\iota^*(F) = f$. So we may apply Remark 4b). □

THEOREM 5.30. *Let M be a $\mathbb{C}$-manifold of the form $V \times N$ for a Stein manifold V. Then* $\mathrm{carddim}\,\mathrm{Hol}(M) \geqslant \mathrm{carddim}\,\mathrm{Hol}(\mathbb{C}) \geqslant 2^{\aleph_1}$.

PROOF. Lemma 5.29 reduces us to the case in which M is a Stein manifold. If $f : M \to \mathbb{C}$ is a nonconstant holomorphic function, then a connected component M' of the preimage of a regular value is a closed submanifold with $\dim_{\mathbb{C}} M' = \dim_{\mathbb{C}} M - 1$. A closed $\mathbb{C}$-submanifold of a Stein manifold is a Stein manifold [**GuRo**, p. 210], so we may repeat the process, eventually obtaining a closed embedding $\iota : S \hookrightarrow M$ with S a connected, one-dimensional Stein manifold, hence a connected, noncompact Riemann surface. Now if Y is a closed $\mathbb{C}$-submanifold of a Stein manifold X then the map $\mathrm{Hol}\,X \to \mathrm{Hol}\,Y$ obtained by

restricting holomorphic functions to Y is surjective [**GuRo**, Thm. VIII.18], so $\iota^* : \mathrm{Hol}(M) \to \mathrm{Hol}(S)$ is surjective. By Remark 4b) and Theorem 5.28 we have $\mathrm{carddim}\, M \geqslant \mathrm{carddim}\, S \geqslant 2^{\aleph_1}$. □

4.8. Further Remarks on Kapovich's Theorem.

A little set theory: For a $\mathbb{C}$-manifold M, the ring $\mathrm{Hol}(M)$ is a subring of the ring of all continuous $\mathbb{C}$-valued functions. For any separable topological space X, the set of continuous functions $f : X \to \mathbb{C}$ has cardinality at most $\mathfrak{c}^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \times \aleph_0} = 2^{\aleph_0} = \mathfrak{c}$. Since $\mathbb{C} \subseteq \mathrm{Hol}(M)$ we have $\#\,\mathrm{Hol}(M) = \mathfrak{c}$. It follows that $\mathrm{Hol}(M)$ has at most $2^{\mathfrak{c}}$ ideals and thus $\mathrm{carddim}\,\mathrm{Hol}(M) \leqslant 2^{\mathfrak{c}}$. Moreover

$$\mathfrak{c} = 2^{\aleph_0} \leqslant 2^{\aleph_1} \leqslant 2^{\mathfrak{c}}.$$

Whether either inequality is strict is independent of the ZFC axioms, but e.g. the Continuum Hypothesis (CH) gives $\mathfrak{c} < 2^{\aleph_1} = 2^{\mathfrak{c}}$. Thus under CH we have $\mathrm{carddim}\,\mathrm{Hol}(M) = 2^{\mathfrak{c}}$ for any Stein manifold M. It may well be the case that the determination of $\mathrm{carddim}\,\mathrm{Hol}(\mathbb{C})$ is independent of the ZFC axioms.

A little history: Theorem 5.25 is a result of M. Kapovich. It answers a question of G. Elencwajg: is there a $\mathbb{C}$-manifold M with $\mathrm{carddim}\,\mathrm{Hol}(M)$ finite and positive?[6] The question was asked on April 19, 2012 and answered the following day. Kapovich's construction draws from work of Henriksen [**He53**] and Sasane [**Sa08**]. Kapovich's first proof of Theorem 5.26 was closely modelled on a criterion of Sasane [**Sa08**, Thm. 2.2] which was used by Sasane to show that the Krull dimension of a noncompact Riemann surface is infinite (which had earlier been established by Alling). I believe Sasane's proof is faulty: [**Sa08**, (2.6)] assumes that the Multiplicative Avoidance Theorem gives a *unique* ideal. I corresponded with Kapovich, and he immediately replaced the limsup with an ultralimit.

The proof of Theorem 5.25 given here is directly inspired by Kapovich's proof. The proof of Theorem 5.27 is identical to Kapovich's, but the proof of Theorem 5.26 is a bit different. Kapovich uses hyperreals and hypernaturals, but in an earlier version he used ultralimits to show $\mathrm{carddim}\,\mathrm{Hol}(M) \geqslant 1 \implies \mathrm{carddim}\,\mathrm{Hol}(M) \geqslant \aleph_0$; we adapt this argument to show the stronger result by following a construction of Henriksen [**He53**]. Henriksen's proof is not couched in the language of ultralimits, but this is just an expository difference: crucially, it uses a nonprincipal ultrafilter on $\mathbb{Z}^+$. Our perspective is that ultrafilters are a nice way to package this argument, as it makes the bookkeeping virtually automatic.

4.9. Proof of Wofsey's Theorem. We will now complete the proof of Theorem 5.16 by showing: for a topological space X admitting a continuous function $f : X \to \mathbb{R}$ that is not locally constant, there is a chain of prime ideals in X that is order isomorphic to $\mathbb{R}$. In fact, we will construct a chain that is order isomorphic to $(0, \infty)$, which is itself order isomorphic to $\mathbb{R}$.

Let $f_0 \in C(X)$ be a function that is constant in no neighborhood of a point $x_0 \in X$. The same property then holds for $f_0 - f_0(x_0)$, so without loss of generality we may assume that $f_0(x_0) = 0$. Put

$$U := f_0^{-1}(\mathbb{R} \backslash \{0\}).$$

[6] See `https://mathoverflow.net/questions/94537`.

Then U is an open subset of $X\backslash\{x_0\}$, and since f_0 does not vanish identically on any neighborhood of x_0, the point x_0 lies in the closure $\overline{U}$ of U. Let ω be an ultrafilter on U converging to x_0. If $g \in C(X)$, then by restriction g defines a continuous function $g : U \to \mathbb{R}$. We can therefore consider ultralimits: for $L \in \mathbb{R}$, recall that $\omega \lim g = L$ means that the ultrafilter $g(\omega)$ converges to L in $\mathbb{R}$: for all $\epsilon > 0$, the set $\{x \in U \mid |g(x) - L| < \epsilon\}$ lies in ω. Notice that since we are now looking at ultrafilters on the noncompact space $\mathbb{R}$, the ultralimit $\omega \lim g$ need not exist; however it is still true that if $\lim_{x\to x_0} g(x) = L$ in the usual sense – even upon restriction to U – then $\omega \lim g = L$.

Now, for $\alpha \in (0, \infty)$, we define

$$\mathfrak{p}_\alpha := \{f \in C(X) \mid \forall a \in \mathbb{R}, \omega \lim e^{a|f_0|^{-\alpha}} f = 0\}.$$

The intuition here is that $\mathfrak{p}_\alpha$ consists of functions f that, as x approaches x_0, converge to 0 much faster than $e^{-|f_0|^\alpha}$.
Step 1: Let $0 < \alpha < \beta$ be real numbers. It is immediate that $\mathfrak{p}_\beta \subseteq \mathfrak{p}_\alpha$. Moreover, consider the function

$$f_\alpha : x \mapsto \begin{cases} e^{-|f_0(x)|^{-\alpha-1}} & \text{if } f_0(x) \neq 0 \\ 0 & \text{if } f_0(x) = 0 \end{cases}.$$

Then since f_0, being continuous, converges to $f_0(x_0) = 0$, so for all $a \in \mathbb{R}$ we have that $e^{a|f_0(x)|^{-\alpha} - |f_0(x)|^{-\alpha-1}}$ converges to 0 as $x \to x_0$ along U, so $f_\alpha \in \mathfrak{p}_\alpha$. Similarly, since $e^{2|f_0(x)|^{-\alpha-1} - |f_0(x)|^{-\alpha-1}}$ approaches ∞ as $x \to x_0$ along U. Thus the chain $\{\mathfrak{p}_\alpha\}_{\alpha\in(0,\infty)}$ is order-anti-isomorphic to $(0, \infty)$, hence order-anti-isomorphic to $\mathbb{R}$, but $\mathbb{R}$ is order-anti-isomorphic to itself via $x \mapsto -x$.
Step 2: Let $\alpha > 0$. We will show that $\mathfrak{p}_\alpha$ is a prime ideal of $C(X)$. It is clear that $\mathfrak{p}_\alpha$ is an additive subgroup of $C(X)$, and the fact that every continuous function is bounded on some neighborhood of x_0 implies that if $f \in \mathfrak{p}_\alpha$ and $g \in C(X)$ then $gf \in \mathfrak{p}_\alpha$, so $\mathfrak{p}_\alpha$ is an ideal of $C(X)$. Finally we show that $\mathfrak{p}_\alpha$ is prime, and notice that it is here that the magic of ultrafilters must come in: for everything we did so far we could have taken ω simply to be the *filter* of all neighborhoods of x_0 and used limits in th usual sense. Suppose $g, h \in C(X)\backslash\mathfrak{p}_\alpha$. Because ω is an ultrafilter, there are $a, b \in \mathbb{R}$ and $\epsilon > 0$ such that

$$S := \{x \in U \mid |e^{a|f_0(x)|^{-\alpha}} g(x)| \geqslant \epsilon\}$$

and

$$T := \{X \in U \mid |e^{b|f_0(x)|^{-\alpha}} h(x)| \geqslant \epsilon\}$$

both lie in ω, hence also $S \cap T$ lies in ω. But for all $x \in S \cap T$, we have

$$|e^{(a+b)|f_0(x)|^{-\alpha}} g(x)h(x)| \geqslant \epsilon^2.$$

Therefore the set of $x \in U$ for which

$$|e^{(a+b)|f_0(x)|^{-\alpha}} g(x)h(x)| < \epsilon^2$$

is disjoint from $S \cap T$ so cannot lie in ω because any two elements of a filter have nonempty intersection. It follows that $gh \notin \mathfrak{p}_\alpha$. Therefore $\mathfrak{p}_\alpha$ is a prime ideal, which completes the proof.

4.10. Further Remarks on Wofsey's Theorem. Theorem 5.16 can be summarized as follows: for any topological space X, we have either $\operatorname{carddim} C(X) = 0$ or $\operatorname{carddim} C(X) \geqslant \mathfrak{c}$ and the former holds if and only if every $f \in C(X)$ is locally constant. Because our definition of $\mathbb{C}$-manifold includes connectedness, all locally constant continuous functions on a $\mathbb{C}$-manifold are constant and in particular all locally onstant holomorphic functions are constant. So Kapovich's Theorem can be summarized in a completely analogous way: for a $\mathbb{C}$-manifold X, we have either $\operatorname{carddim} \operatorname{Hol}(M) = 0$ or $\operatorname{carddim} \operatorname{Hol}(M) \geqslant \mathfrak{c}$.

Wofsey's Theorem also arose as an answer to a question on a website.[7] The question was asked on December 31, 2016 and answered a few hours later. In both cases it seems likely that these questions would have been readily answered by experts in the fields of rings of continuous and holomorphic functions already in the 1950's, but to the best of my knowledge they did not explicitly appear until much more recently.

If X is a discrete space, then $C(X) = \mathbb{R}^X$ and every element is locally constant, so it follows that $\operatorname{carddim} \mathbb{R}^X = 0$. In Chapter 9 we will prove by different methods that for any set X, we have $\operatorname{carddim} \mathbb{F}_2^X = 0$. In fact prime ideals are maximal in any product of fields, although we will unfortunately not prove that result in this text.

Gillman-Jerison showed that for any topological space X (but one reduces to the case in which X is Tychonoff), for any $\mathfrak{p} \in \operatorname{Spec} C(X)$, the set of prime ideals containing $\mathfrak{p}$ forms a chain. In particular, every prime ideal is contained in a unique maximal ideal: this was shown in Exercise 5.12 when X is compact and will be shown in general in Chapter 13. The classical study of $C(X)$ – especially in the case when X is compact – emphasizes maximal ideals over prime ideals. Because of the aforementioned uniqueness result, we can think of the maximal ideals of $C(X)$ as "rocks" under which all the other prime ideals are hiding, but by Wofsey's Theorem, if $C(X)$ carries a function that is not locally constant then every rock is hiding at least continuum-many nonmaximal prime ideals! (Note that this result leaves open the possibility that $\operatorname{carddim} C(X) > \mathfrak{c}$; unlike for the case of $\mathbb{C}$-manifolds, as we range over all topological spaces X, it is not even clear that the cardinal Krull dimension of $C(X)$ must be bounded above by any fixed cardinal.)

Very broadly speaking, the moral here is that it is interesting to consider rings of functions arising from topology and analysis, but these rings are often bewilderingly large: non-Noetherian to say the least! This tends not to happen when we consider rings of functions arising from algebra, a topic to which we now turn.

5. Polynomial rings

Let R be a ring (possibly non-commutative, but – as ever – with identity). Then $R[t]$ denotes the ring of univariate polynomials with R-coefficients.

We assume the reader knows what this means in at least an informal sense: an element of R will be an expression of the form $a_n t^n + \ldots + a_1 t + a_0$, where n is some non-negative integer and $a_n, \ldots, a_0$ are in R. The degree of a polynomial is the

[7] See `https://math.stackexchange.com/questions/2078755/`

supremum over all numbers n such that $a_n \neq 0$. We say "supremum" rather than "maximum" as an attempt to justify the convention that the degree of the 0 polynomial should be $-\infty$ (for that is the supremum of the empty set). A polynomial of degree 0 is called **constant**, and we can view R as a subset of $R[t]$ by mapping $a \in R$ to the constant polynomial a. As an commutative group, $R[t]$ is canonically isomorphic to $\bigoplus_{n=0}^{\infty} R$, the isomorphism being given by $\sum_n a_n t^n \mapsto (a_0, a_1, \ldots)$. (The key point here is that on both sides we have $a_n = 0$ for all sufficiently large n.) Multiplication of polynomials is obtained by applying the relations

$$t^0 = 1,$$

$$\forall i, j \in \mathbb{N},\ t^{i+j} = t^i t^j,$$

$$\forall a \in R,\ at = ta$$

and distributivity, i.e.,

$$(a_n t^n + \ldots + a_n t^1 + a_0) \cdot (b_m t^m + \ldots + b_1 t + b_0) = \sum_{0 \leqslant i \leqslant n,\ 0 \leqslant j \leqslant m} a_i b_j t^{i+j}.$$

For any $P \in R[t]$, the identity $1 \in R$ has the property $1 \cdot P = P \cdot 1 = 1$.

Unfortunately there are some minor annoyances of rigor in the previous description. The first one – which a sufficiently experienced reader will immediately either dismiss as silly or know how to correct – is that it is not *set-theoretically correct*: technically speaking, we need to say what $R[t]$ is as a set and this involves saying what t "really is." It is common in abstract algebra to refer to t is an **indeterminate**, a practice which is remarkably useful despite being formally meaningless: essentially it means "Don't worry about what t is; it can be anything that is not an element of R. All we need to know about t is encapsulated in the multiplication rules $at = ta$, $t^0 = 1$, $t^i t^j = t^{i+j}$." In other words, t is what in the uncomplicated days of high school algebra was referred to as a **variable**.

If someone insists that $R[t]$ be some particular set – a rather unenlighened attitude that we will further combat later on – then the solution has already been given: we can take $R[t] = \bigoplus_{n=0}^{\infty} R$. (It is fair to assume that we already know what direct sums of commutative groups "really are", but in the next section we will give a particular construction which is in fact rather useful.) This disposes of the set-theoretic objections.

Not to be laughed away completely is the following point: we said $R[t]$ was a ring, but how do we know this? We did explain the group structure, defined a multiplication operation, and identified a multiplicative identity. It remains to verify the distributivity of multiplication over addition (special cases of which motivated our definition of multiplication, but nevertheless needs to be checked in general) and also the *associativity* of multiplication.

Neither of these properties are at all difficult to verify. In fact:

EXERCISE 5.30.

a) *Show: $R[t]$ is a ring.*
b) *Show: $R[t]$ is commutative if and only if R is commutative.*

Let us now attempt a "conceptual proof" of the associativity of polynomial multiplication. For this we shall assume that R is commutative – this is the only case we will be exploring further anyway. Then we can, as the $P(t)$ notation suggests, view an element of $R[t]$ as a function from R to R. Namely, we just plug in values:

$$a \in R \mapsto P(a) \in R.$$

To be clear about things, let us denote this associated function from R to R by $\underline{P}$. As we saw above, the set of all functions R^R from R to R forms a commutative ring under pointwise addition and multiplication: $(f+g)(a) := f(a)+g(a)$, $(fg)(a) := f(a) \cdot g(a)$. In particular, it really is obvious that the multiplication of functions is associative. Let $\mathcal{P}$ be the subset of R^R of functions of the form $\underline{P}$ for some $P \in R[t]$. More concretely, we are mapping the constant elements of $R[t]$ to constant functions and mapping t to the identity function. This makes it clear that $\mathcal{P}$ is a subring of R^R: in fact it is the subring of R^R generated by the constant functions and the identity function.

So why don't we just define $R[t]$ to be $\mathcal{P}$, i.e., identify a polynomial with its associated function?

The problem is that the map $R[t] \to \mathcal{P}$ need not be an injection. Indeed, if R is finite (but not the zero ring), $\mathcal{P}$ is a subring of the finite ring R^R so is obviously finite, whereas $R[t]$ is just as obviously infinite. If R is a domain this turns out to be the only restriction.

PROPOSITION 5.31. *Let R be a domain.*

a) *Suppose that R is infinite. Then the canonical mapping $R[t] \to \mathcal{P}$ is a bijection.*
b) *Suppose that R is finite, say of order q, and is therefore a field. Then the kernel of the canonical mapping $R[t] \to \mathcal{P}$ is the principal ideal generated by $t^q - t$.*

We leave the proof as a (nontrivial) exercise for the interested reader.

EXERCISE 5.31. *Exhibit an infinite commutative ring R for which the map $R[t] \to \mathcal{P}$ is not injective. (Suggestion: find an infinite ring all of whose elements x satisfy $x^2 = x$.)*

EXERCISE 5.32. *Show: the map $R[t] \to \mathcal{P}$ is a homomorphism of rings.*

So if we restrict to infinite domains, the map $R[t] \to \mathcal{P}$ is an isomorphism of rings. Thus we see, after the fact, that we could have defined the ring structure in terms of pointwise multiplication.

6. Semigroup algebras

A **semigroup** M is a set equipped with a single binary operation $\cdot$, which is required (only!) to be associative. A **monoid** is a semigroup with a two-sided identity.

EXERCISE 5.33. *Show: a semigroup has at most one two-sided identity, so it is unambiguous to speak of "the" identity element in a monoid. We will denote it by e (so as not to favor either addditive or multiplicative notation).*

EXAMPLE 5.32. *Let $(R, +, \cdot)$ be an algebra. Then $(R, \cdot)$ is a semigroup. If R is a ring (i.e., has an identity 1) then $(R, \cdot)$ is a monoid, with identity element 1.*

EXAMPLE 5.33. *Any group is a monoid. In fact a group is precisely a monoid in which each element has a two-sided inverse.*

EXAMPLE 5.34. *The structure* $(\mathbb{N}, +)$ *of natural numbers under addition is a monoid; the identity element is* 0.

EXAMPLE 5.35. *The structure* $(\mathbb{Z}^+, \cdot)$ *of positive integers under multiplication is a monoid; the identity element is* 1.

Let M and N be two semigroups. Then the Cartesian product $M \times N$ becomes a semigroup in an obvious way: $(m_1, n_1) \cdot (m_2, n_2) := (m_1 \cdot m_2, n_1 \cdot n_2)$. If M and N are monoids with identity elements e_M and e_N, then $M \times N$ is a monoid, with identity element (e_M, e_N). Exactly the same discussion holds for any finite set $M_1, \ldots, M_N$ of semigroups: we can form the direct sum $M = \bigoplus_{i=1}^n M_i$, i.e., the Cartesian product of sets with componentwise operations; if all the M_i's are monoids, so is M.

If we instead have an infinite family $\{M_i\}_{i \in I}$ of semigroups indexed by a set I, we can define a semigroup structure on the Cartesian product $\prod_{i \in I} M_i$ in the obvious way, and if each M_i is a monoid with identity e_i, then the product semigroup is a monoid with identity $(e_i)_{i \in I}$. If each M_i is a monoid, we can also define the **direct sum** $\bigoplus_{i \in I} M_i$, which is the subset of the direct product $\prod_{i \in I} M_i$ consisting of all I-tuples $(m_i \in M_i)_{i \in I}$ such that $m_i = e_i$ for all but finitely many i. Then we have that $\bigoplus_{i \in I} M_i$ is a submonoid of the **direct product** monoid $\prod_{i \in I} M_i$.

If M and N are semigroups, then a map $f : M \to N$ is a homomorphism of semigroups if $f(m_1 \cdot m_2) = f(m_1) \cdot f(m_2)$ for all $m_1,\ m_2 \in M$. If M and N are monoids, a homomorphism of monoids is a homomorphism of semigroups such that moreover $f(e_M) = e_N$. A homomorphism $f : M \to N$ of semigroups (resp. of monoids) is an isomorphism if and only if there is a homomorphism of semigroups (resp. monoids) $g : N \to M$ such that $g \circ f = \mathrm{Id}_M$, $f \circ g = \mathrm{Id}_N$.

EXERCISE 5.34.

a) *Exhibit monoids* M *and* N *and a homomorphism of semigroups* $f : M \to N$ *that is not a homomorphism of monoids.*
b) *Show: a homomorphism of semigroups* $f : M \to N$ *is an isomorphism if and only if it is bijective. Show the same result for monoids.*

EXERCISE 5.35. *Show: the monoid* $(\mathbb{Z}^+, \cdot)$ *of positive integers under multiplication is isomorphic to* $\bigoplus_{i=1}^{\infty} (\mathbb{N}, +)$*, i.e., the direct sum of infinitely many copies of the natural numbers under addition. (Hint: a more natural indexing set for the direct sum is the set of all prime numbers.)*

Now let R be an algebra and M be a semigroup. We suppose first that M is finite. Denote by $R[M]$ the set of all functions $f : M \to R$.

As we saw, using the operations of pointwise addition and multiplication endow this set with the structure of an associative algebra (which has an identity if and only if M does). We are going to keep the pointwise addition but take a different binary operation $* : R[M] \times R[M] \to R[M]$.

Namely, for $f, g \in R[M]$, we define the **convolution product** $f * g$ as follows:

$$(f * g)(m) := \sum_{(a,b) \in M^2 \mid ab=m} f(a)g(b).$$

In other words, the sum extends over all ordered pairs (a, b) of elements of M whose product (in M, of course), is m.

PROPOSITION 5.36. *Let R be an associative algebra and M a finite semigroup. The structure $(R[M], +, *)$ whose underlying set is the set of all functions from M to R, and endowed with the binary operations of pointwise addition and convolution product, is an associative algebra. If R is a ring and M is a monoid with identity e, then $R[M]$ is a ring with multiplicative identity the function I which takes e_M to 1_R and every other element of M to 0_R.*

PROOF. First, suppose that R is a ring and M is a monoid, then for any $f \in R[M]$ and $m \in M$, we have

$$(f*I)(m) = \sum_{(a,b) \in M^2 \mid ab=m} f(a)I(b) = f(m)I(1) = f(m) = I(1)f(m) = \ldots = (I*f)(m).$$

We still need to check the associativity of the convolution product and the distributivity of convolution over addition. We leave the latter to the reader but check the former: if $f, g, h \in R[M]$, then

$$((f * g) * h)(m) = \sum_{xc=m} (f * g)(x)h(c) = \sum_{xc=m} \sum_{ab=x} f(a)g(b)h(c)$$

$$= \sum_{abc=m} f(a)g(b)h(c)$$

$$= \sum_{ay=m} \sum_{bc=y} f(a)g(b)h(c) = \sum_{ay=m} f(a)(g * h)(y) = (f * (g * h))(m).$$

□

A special case of this construction which is important in the representation theory of finite groups is the ring $k[G]$, where k is a field and G is a finite group.

Now suppose that M is an infinite semigroup. Unless we have some sort of extra structure on R which allows us to deal with convergence of sums – and, in this level of generality, we do not – the above definition of the convolution product $f * g$ is problematic because the sum might be infinite. For instance, if $M = G$ is any group, then our previous definition of $(f * g)(m)$ would come out to be $\sum_{x \in G} f(x)g(x^{-1}m)$, which is, if G is infinite, an infinite sum.

Our task therefore is to modify the construction of the convolution product so as to give a meaningful answer when the semigroup M is infinite, but in such a way that agrees with the previous definition for finite M.

Taking our cue from the infinite direct sum, we restrict our domain: define $R[M]$ to be subset of all functions $f : M \to R$ such that $f(m) = 0$ except for finitely many m (or, for short, **finitely nonzero functions**). Restricting to such functions,

$$(f * g)(m) := \sum_{ab=m} f(a)g(b)$$

makes sense: although the sum is apparently infinite, all but finitely terms are zero.

PROPOSITION 5.37. *Let R be an associative algebra and M a semigroup. The structure $(R[M], +, *)$ whose underlying set is the set of all finitely nonzero functions from M to R, and endowed with the binary operations of pointwise addition and convolution product, is an associative algebra. If R is a ring and M is a monoid with identity element e, then $R[M]$ is a ring with multiplicative identity the function I which takes e_M to 1_R and every other element of M to 0_R.*

EXERCISE 5.36. *Prove Proposition 5.37. More precisely, verify that the proof of Proposition 5.36 goes through unchanged.*

As a commutative group, $R[M]$ is naturally isomorphic to the direct sum $\bigoplus_{m \in M} R$, i.e., of copies of R indexed by M. One can therefore equally well view an element $R[M]$ as a formal finite expressions of the form $\sum_{m \in M} a_m m$, where $a_m \in R$ and all but finitely many are 0. Written in this form, there is a natural way to define the product

$$\left(\sum_{m \in M} a_m m \right) \left(\sum_{m \in M} b_m m \right)$$

of two elements f and g of $R[M]$: namely we apply distributivity, use the multiplication law in R to multiply the a_m's and the b_m's, use the operation in M to multiply the elements of M, and then finally use the addition law in R to rewrite the expression in the form $\sum_m c_m m$. But a moment's thought shows that c_m is nothing else than $(f * g)(m)$. On the one hand, this makes the convolution product look very natural. Conversely, it makes clear:

The polynomial ring $R[t]$ is canonically isomorphic to the monoid ring $R[\mathbb{N}]$. Indeed, the explict isomorphism is given by sending a polynomial $\sum_n a_n t^n$ to the function $n \mapsto a_n$.

This gives a new proof of the associativity of the product in the polynomial ring $R[t]$. We leave it to the reader to decide whether this proof is any easier than direct verification.. Rather the merit is that this associativity computation has been done once and for all in a very general context.

The semigroup algebra construction can be used to define several generalizations of the polynomial ring $R[t]$.

EXERCISE 5.37. *For a ring R, identify the monoid ring $R[\mathbb{Z}]$ with the ring $R[t, t^{-1}]$ of Laurent polynomials.*

First, let $T = \{t_i\}$ be a set. Let $FA(T) := \bigoplus_{i \in T} (\mathbb{N}, +)$ be the direct sum of a number of copies of $(\mathbb{N}, +)$ indexed by T. Let R be a ring, and consider the monoid ring $R[FA(T)]$. Let us write the composition law in $FA(T)$ multiplicatively; moreover, viewing an arbitrary element I of $FA(T)$ as a finitely nonzero function from T to $\mathbb{N}$, we use the notation t^I for $\prod_{t \in T} t^{I(t)}$. Then an arbitrary element of $R[FA(T)]$ is a finite sum of the form $\sum_{k=1}^n r_k t^{I_k}$, where $I_1, \ldots, I_k$ are elements of $FA(t)$. This representation of the elements should make clear that we can view $R[FA(T)]$ as a polynomial ring in the indeterminates $t \in T$: we use the alternate notation $R[\{t_i\}]$.

THEOREM 5.38. *Let R be a ring and G a group. Then the group ring $R[G]$ is a domain – i.e., a* commutative *ring without nonzero zero-divisors – if and only if R is a domain and G is commutative and torsionfree.*

PROOF. Step 1: The ring $R[G]$ is commutative if and only if both R and G are. Since R is a subring of $R[G]$, if $R[G]$ is a domain then so is R. If there is $g \in G$ and $n > 1$ such that $g^n = 1$, then $(g-1)(g^{n-1} + \ldots + g + 1) = 0$, so $R[G]$ is not a domain.
Step 2: Suppose R is a domain and G is torsionfree commutative. Let K be the fraction field of R. Then $R[G]$ is a subring of $K[G]$, so it is enough to show that $K[G]$ is a domain. Here is the key observation: for $x, y \in K[G]^\bullet$, there is a finitely generated subgroup H of G such that $x, y \in K[H]$. Since H is also torsionfree, we have $H \cong \mathbb{Z}^n$ so $K[H]$ is isomorphic to the ring of Laurent polynomials $K[t_1, t_1^{-1}, \ldots, t_n, t_n^{-1}]$, which itself lies in function field $K(t_1, \ldots, t_n)$ so is a domain.

Somewhere in here we must have used that $K[t_1, \ldots, t_n]$ is a domain, so that it has a field of fractions. This is no problem to establish directly: write $K[t_1, \ldots, t_n] = K[t_1, \ldots, t_{n-1}][t_n]$ to reduce to the case of a polynomial ring in one variable over a domain. If $\deg(f) = d_1$ and $\deg(g) = d_2$, then $\deg(fg) = d_1 + d_2$.) □

REMARK 5. *Our convention that a domain is a* commutative *ring saved us from considering the following question: if R is a ring without (nonzero) zero-divisors and G is a group without (nontrivial) elements of finite order, is $R[G]$ a ring without zero-divisors? This question remains wide open even in the case when R is a field, in which case it is known as the* ***Kaplansky Zero Divisor Conjecture****.*

Let us go back to the monoid ring $R[\mathbb{N}]$, whose elements are finitely nonzero functions $f : R \to \mathbb{N}$. Notice that in this case the precaution of restricting finitely nonzero functions is not necessary: the monoid $(\mathbb{N}, +)$, although infinite, has the property that for any $m \in \mathbb{N}$, the set of all $x, y \in \mathbb{N}$ such that $x + y = m$ is finite (indeed, of cardinality $m + 1$). Let us call an arbitrary monoid M **divisor-finite** if for each m in M, the set $\{(x, y) \in M^2 \mid xy = m\}$ is finite.

EXERCISE 5.38.

a) *For a set T, $FA(T) = \bigoplus_{t \in T} (\mathbb{N}, +)$ is divisor-finite.*
b) *A group is divisor-finite if and only if it is finite.*

For a divisor-finite monoid M, and any ring R, we may define the **big monoid ring** $R[[M]]$ to be the collection of all functions $M \to R$, with pointwise addition and convolution product.

For example, if $M = (\mathbb{N}, +)$, then writing M multiplicatively with $n \in N \mapsto t^n$ for some formal generator t, an element of the ring $R[[M]]$ is an infinite formal sum $\sum_{n \in \mathbb{N}} r_n t^n$. Such sums are added coordinatewise and multiplied by distributivity:

$$(\sum_{n \in \mathbb{N}} r_n t^n)(\sum_{n \in \mathbb{N}} s_n t^n) = r_0 s_0 + (r_0 s_1 + r_1 s_0)t + \ldots + (\sum_{k=0}^{n} r_k s_{n-k})t^n + \ldots.$$

This ring is denoted by $R[[t]]$ and called the **formal power series ring** over R.

EXERCISE 5.39. *Using Exercise 5.38, define, for any set $T = \{t_i\}$ and any ring R, a formal power series ring $R[[\{t_i\}]]$.*

Here is yet another variation on the construction: suppose M is a commutative, cancellative divisor-finite monoid endowed with a total order relation $\leqslant$. (Example: $(\mathbb{N}, +)$ or $FA(T)$ for any T.) There is then a group completion $G(M)$ together with an injective homomorphism of monoids $M \to G(M)$. If M is finite and cancellative, it is already a group. If M is infinite, then so is $G(M)$, so it cannot be divisor-finite. Nevertheless, the ordering $\leqslant$ extends uniquely to an ordering on $G(M)$, and we can define a ring $R((G(M))$ whose elements are the functions from $f : G(M) \to R$ such that $\{x \in G(M) \mid x < 0,\ f(x) \neq 0\}$ is finite, i.e., f is finitely nonzero on the negative values of $G(M)$.

EXERCISE 5.40.

a) *Show: under the above hypotheses, the convolution product on $R((G(M))$ is well-defined, and endows $R((G(M))$ with the structure of a ring.*
b) *When $M = (\mathbb{N}, +)$, identify $R((M))$ as $R((t))$, the ring of formal finite-tailed Laurent series with coefficients in R. Give a multi-variable analogue of this by taking $M = FA(T)$ for arbitrary T.*

EXERCISE 5.41. *Let R be a not-necessarily-commutative ring. Give a rigorous definition of the ring $R\langle t_1, t_2\rangle$ of "noncommutative polynomials" – each t_i commutes with each element of R, but t_1 and t_2 do not commute – as an example of a small monoid ring $R[M]$ for a suitable monoid M. Same question but with an arbitrary set $T = \{t_i\}$ of noncommuting indeterminates.*

The universal property of semigroup rings: Fix a commutative ring R. Let B be a commutative R-algebra and M a commutative monoid. Let $f : R[M] \to B$ be an R-algebra homomorphism. Consider f restricted to M; it is a homomorphism of monoids $M \to (B, \cdot)$. Thus we have defined a mapping

$$\mathrm{Hom}_{\text{R-alg}}(R[M], B) \to \mathrm{Hom}_{\text{Monoid}}(M, (B, \cdot)).$$

Interestingly, this map has an inverse. If $g : M \to B$ is any homomorphism satisfying $g(0) = 0$, $g(m_1 + m_2) = g(m_1) + g(m_2)$, then g extends to a unique R-algebra homomorphism $R[M] \to B$: $\sum_{m \in M} r_m m \mapsto \sum_m r_m g(m)$. The uniqueness of the extension is immediate, and that the extended map is indeed an R-algebra homomorphism can be checked directly (please do so).

In more categorical language, this canonical bijection shows that the functor $M \mapsto R[M]$ is the **left adjoint** to the forgetful functor $(S, +, \cdot) \mapsto (S, \cdot)$ from R-algebras to commutative monoids. Yet further terminology would express this by saying that $R[M]$ is a "free object" of a certain type.

THEOREM 5.39. *(Universal property of polynomial rings) Let $T = \{t_i\}$ be a set of indeterminates. Let R be a commutative ring, and S an R-algebra. Then each map of sets $T \mapsto S$ extends to a unique R-algebra homomorphism $R[T] \to S$.*

Proof: By the previous result, each monoid map from the free commutative monoid $\bigoplus_{t \in T} \mathbb{Z}$ to S extends to a unique R-algebra homomorhpism. So what is needed is the fact that every set map $T \to M$ to a commutative monoid extends uniquely to a homomorphism $\bigoplus_{t \in T} \mathbb{Z} \to M$ (in other words, we pass from the category of sets to the category of commutative R-algebras by passing through the category of commutative monoids, taking the free commutative monoid associated to a set and then the free R-algebra associated to the monoid). As before, the uniqueness of the extension is easy to verify.

EXERCISE 5.42.

a) *Formulate analogous universal properties for Laurent polynomial rings, and non-commutative polynomial rings.*
b) *Suppose M is a divisor-finite monoid. Is there an analogous extension property for the big monoid ring $R[\![M]\!]$?*

This result is of basic importance in the study of R-algebras. For instance, let S be an R-algebra. A generating set for S, as an R-algebra, consists of a subset T of S such that the least R-subalgebra of S containing T is S itself. This definition is not very concrete. Fortunately, it is equivalent to the following:

THEOREM 5.40. *Let R be a commutative ring, S a commutative R-algebra, and T a subset of S. the following are equivalent:*

(i) *The set T generates S as an R-algebra.*
(ii) *The canonical homomorphism of R-algebras $R[T] \to S$ – i.e., the unique one sending $t \mapsto t$ – is a surjection.*

EXERCISE 5.43. *Prove Theorem 5.40.*

In particular, a commutative R-algebra S is finitely generated if and only if it is a quotient ring of some polynomial ring $R[t_1, \ldots, t_n]$.

Another application is that every commutative ring whatsoever is a quotient of a polynomial ring (possibly in infinitely many indeterminates) over $\mathbb{Z}$. Indeed, for a ring R, there is an obvious surjective homomorphism from the polynomial ring $\mathbb{Z}[R]$ – here R is being viewed as a set of indeterminates – to R, namely the one carrying $r \mapsto r$.

A ring R is said to be **absolutely finitely generated** if it is finitely generated as a $\mathbb{Z}$-algebra; equivalently, there exists an $n \in \mathbb{N}$ and an ideal I in $\mathbb{Z}[t_1, \ldots, t_n]$ such that $\mathbb{Z}[t_1, \ldots, t_n]$ is isomorphic to R.

EXERCISE 5.44.

a) *Show: a finitely generated ring has finite or countably infinite cardinality.*
b) *Find all fields which are finitely generated as rings.*
(N.B.: In field theory there is a notion of absolute finite generation for a field. This a much weaker notion: e.g. $\mathbb{Q}(x)$ is absolutely finitely generated as a field but not as a ring.)

CHAPTER 6

Swan's Theorem

We now digress to discuss an important theorem of R.G. Swan on projective modules over rings of continuous functions.

Throughout this section K denotes either the field $\mathbb{R}$ or the field $\mathbb{C}$, each endowed with their standard Euclidean topology. For a topological space X, the set $C(X)$ of all continuous functions $f : X \to K$ forms a commutative ring under pointwise addition and multiplication.

1. Introduction to (topological) vector bundles

Recall[1] the notion of a **K-vector bundle** over a topological space X. This is given by a topological space E (the "total space"), a surjective continuous map $\pi : E \to X$ and on each fiber $E_x := \pi^{-1}(x)$ the structure of a finite-dimensional K-vector space satisfying the following local triviality property: for each $x \in X$, there exists an open neighborhood U containing x and a homeomorphism $f : \pi^{-1}U \to U \times K^n$ such that for all $y \in U$ f carries the fiber E_y over y to $\{y\} \times K^n$ and induces on these fibers an isomorphism of K-vector spaces. (Such an isomorphism is called a **local trivialization** at x.) As a matter of terminology we often speak of "the vector bundle E on X" although this omits mention of some of the structure.

On any K-vector bundle E over X we have a **rank function** $r : X \to \mathbb{N}$, namely we define $r(x)$ to be the dimension of the fiber E_x. We say that E is a **rank n** vector bundle if the rank function is constantly equal to n. The existence of local trivializations implies that the rank function is locally constant – or equivalently, continuous when $\mathbb{N}$ is given the discrete topology, so if the base space X is connected the rank function is constant.

As a basic and important example, for any $n \in \mathbb{N}$ we have the **trivial rank n vector bundle** on X, with total space $X \times K^n$ and such that π is just projection onto the first factor.

If $\pi : E \to X$ and $\pi' : E' \to X$ are two vector bundles over X, a **morphism** of vector bundles $f : E \to E'$ is a continuous map of topological spaces from E to E' *over* X in the sense that $\pi = \pi' \circ f$ – equivalently f sends the fiber E_x to the fiber E'_x – and induces a K-linear map on each fiber. In this way we get a category $\mathrm{Vec}(X)$ of K-vector bundles on X. If we restrict only to rank n vector bundles and morphisms between them we get a subcategory $\mathrm{Vec}_n(X)$. A vector bundle E on X is said to be trivial (or, for emphasis, "globally trivial") if it is isomorphic to the

[1] from a previous life, if necessary

trivial rank n vector bundle for some n.

Many of the usual linear algebraic operations on vector spaces extend immediately to vector bundles. Most importantly of all, if E and E' are two vector bundles on X, we can define a direct sum $E \oplus E'$, whose defininining property is that its fiber over each point $x \in X$ is isomorphic to $E_x \oplus E_{x'}$. This not being a topology/geometry course, we would like to evade the precise construction, but here is the idea: it is obvious how to define the direct sum of trivial bundles. So in the general case, we define the direct sum by first restricting to a covering family $\{U_i\}_{i \in I}$ of simultaneous local trivializations of E and E' and then *glue together* these vector bundles over the U_i's. In a similar way one can define the tensor product $E \otimes E'$ and the dual bundle $E^\vee$.

For our purposes though the direct sum construction is the most important. It gives $\mathrm{Vec}(X)$ the structure of an additive category: in addition to the existence of direct sums, this means that each of the sets $\mathrm{Hom}(E, E')$ of morphisms from E to E' form a commutative group. (In fact $\mathrm{Hom}(E, E')$ naturally has the structure of a K-vector space.) Decategorifying, the set of all isomorphism classes of vector bundles on X naturally forms a commutative monoid under direct sum (the identity is the trivial vector bundle $X \to X$ where each one point fiber is identified – uniquely! – with the zero vector space). The Grothendieck group of this monoid is $K(X)$: this is the beginning of **topological K-theory**.

2. Swan's Theorem

But we digress from our digression. A **(global) section** of a vector bundle $\pi : E \to X$ is indeed a continuous section σ of the map π, i.e., a continuous map $\sigma : X \to E$ such that $\pi \circ \sigma = 1_X$. The collection of all sections to E will be denoted $\Gamma(E)$. Again this is a commutative group and indeed a K-vector space, since we can add two sections and scale by elements of K.

But in fact more is true. The global sections form a module over the ring $C(X)$ of continuous K-valued functions, in a very natural way: given a section $\sigma : X \to E$ and $f : X \to K$, we simply define $f\sigma : X \to E$ by $x \mapsto f(x)\sigma(x)$. Thus $\Gamma : E \to \Gamma(E)$ gives a map from vector bundles over X to $C(X)$-modules.

In fancier language, Γ gives an additive functor from the category of vector bundles on X to the category of $C(X)$-modules; let us call it the **global section functor**. (Indeed, if we have a section $\sigma : E \to X$ of E and a morphism of vector bundles $f : E \to E'$, $f(\sigma) = f \circ \sigma$ is a section of E'. No big deal!)

THEOREM 6.1. *(Swan* [**Sw62**]*) Let X be a compact space. Then the global section functor Γ gives an equivalence of categories from $\mathrm{Vec}(X)$ to the category of finitely generated projective $C(X)$-modules.*

In other words, at least for this very topologically influenced class of rings $C(X)$, we may entirely identify finitely generated projective bundles with a basic and important class of geometric objects, namely vector bundles.

There is a special case of this result which is almost immediately evident. Namely, suppose that E is a trivial vector bundle on X, i.e., up to isomorphism E is simply $X \times K^n$ with $\pi = \pi_1$. Thus a section σ is nothing else than a continuous function

$\sigma : X \to K^n$, which in turn is nothing else than an n-tuple $(f_1, \ldots, f_n)$ of elements of $C(X)$. Thus if we define $\sigma_i \in \Gamma(E)$ simply to be the section which takes each point to the ith standard basis vector e_i of K^n, we see immediately that $(\sigma_1, \ldots, \sigma_n)$ is a basis for $\Gamma(E)$, i.e., $\Gamma(E)$ is a free $C(X)$-module of rank n. Moreover, we have

$$\mathrm{Hom}(X \times K^n, X \times K^m) \cong \mathrm{Map}(X, \mathrm{Hom}_K(K^n, K^m))$$
$$\cong C(X) \otimes_K \mathrm{Hom}(K^n, K^w) \cong \mathrm{Hom}_{C(X)}(\Gamma(X \times K^n), \Gamma(X \times K^m)).$$

Thus we have established that Γ gives an additive equivalence from the category of trivial vector bundles on X to the category of finitely generated free $C(X)$-modules. We wish to promote this to an equivalence from locally trivial vector bundles (i.e., all vector bundles) to finitely generated projective modules. Oh, if only we had some nice "geometric" characterization of finitely generated projective modules!

But we do: namely Proposition 3.11 characterizes finitely generated projective modules over any commutative ring R as being precisely the images of projection operators on finitely generated free modules. Thus the essence of what we want to show is that for any vector bundle E over X (a compact space), there exists a trivial vector bundle T and a projection $P : T \to T$ – i.e., an element of $\mathrm{Hom}(T, T)$ with $P^2 = P$ such that the image of P is a vector bundle isomorphic to E. Indeed, if we can establish this, then just as in the proof of 3.11 we get an internal direct sum decomposition $T = P(T) \oplus (1 - P)(T)$ and an isomorphism $P(T) \cong E$, and applying the additive functor Γ this gives us that $\Gamma(E)$ is isomorphic to a direct summand of the finitely generated free $C(X)$-module $\Gamma(T)$. A little thought shows that in fact this proves the entire result, because we have characterized $\mathrm{Vec}(X)$ as the "projection category" of the additive category trivial vector bundles, so it must be equivalent to the "projection category" of the equivalent additive category of finitely generated free $C(X)$-modules. So from this point on we can forget about projective modules and concentrate on proving this purely topological statement about vector bundles on a compact space.[2]

3. Proof of Swan's Theorem

Unfortunately the category of vector bundles over X is not an abelian category. In particular, it can happen that a morphism of vector bundles does not have either a kernel or image. Swan gives the following simple example: let $X = [0, 1]$, $E = X \times K$ the trivial bundle, and $f : E \to E$ be the map given by $f(x, y) = (x, xy)$. Then the image of f has rank one at every $x \neq 0$ but has rank 0 at $x = 0$. Since X is connected, a vector bundle over X should have constant rank function. Exactly the same considerations show that the kernel of f is not a vector bundle. However, nothing other than this can go wrong, in the following sense:

PROPOSITION 6.2. *For a morphism $f : E \to E'$ of vector bundles over X, the following are equivalent:*

(i) *The image of f is a subbundle of E'.*
(ii) *The kernel of f is a subbundle of E.*

[2]We note that [**Sw62**] takes a more direct approach, for instance proving by hand that the global section functor Γ is fully faithful. In our use of projection operators and projection categories to prove Swan's theorem we follow Atiyah [**At89**, §1.4]. Aside from being a bit shorter and slicker, this approach really brings life to Proposition 3.11 and thus seems thematic in a commutative algebra course. But it is not really more than a repackaging of Swan's proof.

(iii) *The function* $x \mapsto \dim_K(\operatorname{Im} f)_x$ *is locally constant.*
(iv) *The function* $x \mapsto \dim_K(\operatorname{Ker} f)_x$ *is locally constant.*

PROOF. Step 1: We first wish to prove a special case: namely that if $f : E \to E'$ is a monomorphism of vector bundles (i.e., it induces an injection on all fibers) then $(\operatorname{Im} f)$ is a subbundle of E' and $f : E \to (\operatorname{Im} f)$ is an isomorphism. The issues of whether $\operatorname{Im} f$ is a vector bundle and f is an isomorphism are both local ones, so it suffices to treat the case where E and E' are trivial bundles. Suppose $E' = X \times V$, and let $x \in X$. Choose $W_x \subseteq V$ a subspace complementary to $(\operatorname{Im} f)_x$. Then $G := X \times W_x$ is a sub-bundle of E; let $\iota : G \to E$ be the inclusion map. Define $\theta : E \oplus G \to E'$ by $\theta((a,b)) = f(a) + \iota(b)$. Then θ_x is an isomorphism, so there exists an open neighborhood U of x such that $\theta|_U$ is an isomorphism. Since E is a subbundle of $E \oplus G$, $\theta(E) = f(E)$ is a subbundle of $\theta(E \oplus G) = E'$ on U.
Step 2: Since the rank function on a vector bundle is locally constant, (i) $\implies$ (iii), (ii) $\implies$ (iv), and (by simple linear algebra!) (iii) $\iff$ (iv).
(iv) $\implies$ (i): Again the issue of whether $\operatorname{Im} f$ is a vector bundle is a local one, so we may assume that $E = X \times V$ is a trivial bundle. For $x \in X$, let $W_x \subseteq V$ be a complementary subspace to $(\operatorname{Ker} f)_x$. Let $G = X \times W_x$, so that f induces a homomorphism $\psi : G \to E'$ whose fiber at x is a monomorphism. Thus ψ is a monomorphism on some neighborhood U of x, so $\psi(G)|_U$ is a subbundle of $E'|_U$. However $\Psi(G) \subseteq f(E)$, and since $f(E)$ has constant rank, and

$$\dim \psi(G)_y = \dim \psi(G)_x = \dim f(E)_x = \dim f(E)_y$$

for all $y \in U$, $\psi(G)|_U = f(E)|_U$. so $f(E)$ is a subbundle of E'.
(iv) $\implies$ (ii): here we exploit dual bundles. The hypothesis implies that the kernel of $f^\vee : (E')^\vee \to E^\vee$ has constant rank function. Since $E^\vee \to \operatorname{Coker} f^\vee$ is an epimorphism, $(\operatorname{Coker} f^\vee)^\vee \to E^{\vee\vee}$ is a monomorphism: by Step 1, its image is a subbundle. But the natural map $E \to E^{\vee\vee}$ is an isomorphism, the restriction of which to $\operatorname{Ker} f$ gives an isomorphism to the vector bundle $(\operatorname{Coker} f^\vee)^\vee$. So $\operatorname{Ker} f$ is a vector bundle. □

The proof yields the following additional information.

COROLLARY 6.3. *For any morphism of vector bundles, the rank function of the image is upper semi-continuous: that is, for any* $x \in X$*, there exists a neighborhood* U *of* x *such that for all* $y \in U$*,* $\dim_K(\operatorname{Im} f)_y \geqslant \dim_K(\operatorname{Im} f)_x$*.*

EXERCISE 6.1. *Prove Corollary 6.3.*

PROPOSITION 6.4. *Let* E *be a vector bundle over* X*, and let* $P \in \operatorname{End}(E) = \operatorname{Hom}(E,E)$ *be a projection, i.e.,* $P^2 = P$*. Then:*

a) *We have* $\operatorname{Ker}(P) = \operatorname{Im}(1-P)$.
b) $\operatorname{Im} P$ *and* $\operatorname{Im}(1-P)$ *are both subbundles of* E.
c) *There is an internal direct sum decomposition* $E = \operatorname{Im} P \oplus \operatorname{Im}(1-P)$.

PROOF. a) For all $x \in X$ linear algebra gives us an equality of fibers $\operatorname{Ker}(P)_x = \operatorname{Im}(1-P)_x$. This suffices!
b) From part a) we deduce an equality of rank functions

$$r_{\operatorname{Im} P} + r_{\operatorname{Im}(1-P)} = r_E.$$

By Corollary 6.3, for all $x \in X$, there is a neighborhood U of x on which $r_{\operatorname{Im} P}$ is at least as large as $r_{\operatorname{Im} P}(x)$, $r_{\operatorname{Im}(1-P)}$ is at least as large as $r_{\operatorname{Im}(1-P)}(x)$ and r_E is

constantly equal to $r_E(x)$. On this neighborhood the ranks of $\operatorname{Im} P$ and $\operatorname{Im}(1-P)$ must be constant, and therefore by Proposition 6.2 $\operatorname{Im} P$ and $\operatorname{Im}(1-P)$ are both subbundles.
c) Again it is enough to check this fiber by fiber, which is simple linear algebra. □

An inner product on a finite-dimensional $\mathbb{R}$-vector space V is, as usual, a symmetric $\mathbb{R}$-bilinear form $\langle , \rangle : V \times V \to \mathbb{R}$ which is positive definite in the sense that for all $x \in V \backslash \{0\}$, $\langle x, x \rangle = 0$. An inner product on a finite-dimensional $\mathbb{C}$-vector space V is a positive definite sesquilinear form: i.e., it is $\mathbb{C}$-linear in the first variable, conjugate-linear in the second variable and again we have $\langle x, x \rangle > 0$ for all $x \in V \backslash \{0\}$.

Now let E be a K-vector bundle on X. An **inner product** on E is a collection of inner products $\langle , \rangle_x : E_x \times E_x \to K$ on each of the fibers which vary continuously in x. Formally this means the following: let $E \times_X E$ be the subset of $(e_1, e_2) \in E \times E$ such that $\pi(e_1) = \pi(e_2)$; then such a fiberwise family of inner products defines a function from $E \times_X E$ to K, and this function is required to be continuous.

Let us say that a **metrized vector bundle** E on X is a vector bundle together with an inner product. (Again, this is an abuse of terminology: we do not speak of the inner product by name.)

PROPOSITION 6.5. *Let E be a metrized line bundle on X.*

a) *If E' is a subbundle of E, fiberwise orthogonal projection onto E' defines a projection operator $P \in \operatorname{End}(E)$ with image E'.*
b) *All short exact sequences $0 \to E' \to E \to E'' \to 0$ of vector bundles are split.*
c) *If M is another vector bundle on X and there exists an epimorphism of bundles $q : E \to M$, then M is isomorphic to the image of a projection operator on E.*

PROOF. a) This is mostly a matter of understanding and unwinding the definitions, and we leave it to the reader.
b) Let P be orthogonal projection onto E'. The restriction of the map $E \to E''$ to $\operatorname{Ker} P$ is an isomorphism of vector bundles. The inverse of this isomorphism gives a splitting of the sequence.
c) By Proposition 6.2, since $\operatorname{Im} q = M$ is a vector bundle, so is $\operatorname{Ker} q$, whence a short exact sequence

$$0 \to \operatorname{Ker} q \to E \to M \to 0.$$

By part b), there exists a splitting $\sigma : M \to E$ of this sequence. Then, as usual, $P = \sigma \circ q$ is a projection operator on E and $q|_{\operatorname{Im} P} : \operatorname{Im} P \xrightarrow{\sim} M$. □

PROPOSITION 6.6. *If X is a paracompact topological space, then every vector bundle over X admits an inner product.*

PROOF. This is a rather standard topological argument which we just sketch here. Let M be a vector bundle on X, and let $\{U_i\}_{i \in I}$ be an open covering of X such that the restriction of M to each U_i is a trivial bundle. On a trivial bundle there is an obvious inner product, say $\langle , \rangle_x$. Now, since X is paracompact, there exists a partition of unity $\{\varphi_i\}_{i \in I}$ subordinate to the open covering $\{U_x\}$: that is,
• each $\varphi_i : X \to [0, 1]$ is continuous,

• for all $x \in X$ we have $\mathrm{supp}(\varphi_i) \subseteq U_i$
• for all $x \in X$ there exists an open neighborhood V of x on which all but finitely many φ_i's vanish identically, and
• for all $x \in X$, $\sum_{i \in I} \varphi_i(x) = 1$.[3]
Then, for $x \in X$ and $e_1, e_2 \in M_x$, define

$$\langle e_1, e_2 \rangle_x := \sum_i \varphi_i(x) \langle e_1, e_2 \rangle_i;$$

the sum extends over all $i \in I$ such that $x \in U_i$. This is an inner product on M. □

To complete the proof of Swan's Theorem, it suffices to show that if X is compact, every vector bundle M on X is the epimorphic image of a trivial bundle. In particular, Proposition 6.5 then shows that M is a direct summand of a trivial vector bundle T and thus $\Gamma(M)$ is a direct summand of the finitely generated free $C(X)$-module $\Gamma(T)$, hence is finitely generated projective.

PROPOSITION 6.7. *Let X be a compact space and M a vector bundle on X. Then there exists an epimorphism of bundles from a trivial vector bundle $X \times V$ to M.*

PROOF. Step 1: We CLAIM that for each $x \in X$, there exists a neighborhood U_x of x and finite set of global sections $S_x = \{s_{x,1}, \ldots, s_{x,k_x}\}$ of M such that for all $y \in U$, $s_{x,1}(y), \ldots, s_{x,k_x}(y)$ is a K-basis for M_y.
PROOF OF CLAIM: Let U be an open neighborhood of x on which M is a trivial bundle. Certainly then there exist finitely many sections $s_1, \ldots, s_n$ of M over U which when evaluated at any $y \in U$ give a basis of M_y. We need to show that there exists an open set W with $x \in W \subseteq U$ and global sections $s_1', \ldots, s_n'$ such that for all i, $s_i'|_W = s_i|_W$. For this it suffices to work one section at a time: let s be a section of M over U. Since X is paracompact, it is normal, so there exist open neighborhoods W and V of x with $\overline{W} \subseteq V$ and $\overline{V} \subseteq U$. By Urysohn's Lemma, there is a continuous function $\omega : X \to [0,1]$ such that $\omega|_{\overline{W}} \equiv 1$ and $\omega|_{X \setminus V} \equiv 0$. If we then define $s' : X \to M$ by $s'(y) = \omega(y)s(y)$ for $y \in U$ and $s'(y) = 0$ for $y \in X \setminus U$, then this s does the job.
Step 2: By compactness of X, there exists a finite subset I of X such that $\{U_x\}_{x \in I}$ covers X. So $S = \bigcup_{i \in I} S_x$ is a finite set of global sections of M which when evaluated at any $x \in X$, span the fiber M_x. So the K-subspace V of $\Gamma(M)$ spanned by S is finite-dimensional. We define a map $q : X \times V \to M$ by $q(x,s) = s(x)$. This is a surjective bundle map from a trivial vector bundle to M! □

Remark: In the above proof the paracompactness of X seems to have been fully exploited, but the need for compactness is less clear. In fact, at the end of [**Sw62**], Swan remarks that if you replace the last step of the proof by an argument from Milnor's 1958 lecture notes *Differential Topology*, one gets a categorical equivalence between vector bundles *with bounded rank function* on a paracompact space X and finitely generated projective $C(X)$-modules.

Remark: A more straightforward variant of Swan's theorem concerns the case where X is a compact differentiable manifold (say of class C^∞). In this case the equivalence is between differentiable K-vector bundles on X and modules over the ring of K-valued C^∞-functions. Looking over the proof, one sees that the only part that

[3]See e.g. Exercise 5 in §4.5 of Munkres' *Topology: a first course* for a proof of this fact.

needs additional attention is the existence of differentiable partitions of unity. Such things indeed exist and are constructed in many of the standard texts on geometry and analysis on manifolds. We recommend [**We80**], which has a particularly clear and complete discussion.

4. Applications of Swan's Theorem

4.1. Vector bundles and homotopy.

Vector bundles on a space are of interest not only to differential topologists and geometers but also to algebraic geometers. This is because pullback of vector bundles behaves well under homotopy.

First, suppose that $f : X \to Y$ is a continuous map of topological spaces and $\pi : E \to Y$ is a vector bundle on Y. We may **pullback** π to a vector bundle $\pi_X : E \times_Y X \to X$ just by taking $E \times_Y X$ to be the fiber product of the maps f and π, namely the subspace of $X \times E$ consisting of all pairs (x, v) such that $f(x) = \pi(v) \in Y$. The map $\pi_X : E \times_Y X \to X$ is just restriction of the projection map: $(x, v) \mapsto x$.

EXERCISE 6.2. *Show: $\pi_X : E \times_Y X \to X$ is indeed a vector bundle on X. We abbreviate it by either $f^*\pi$ or (more abusively) f^*E.*

EXERCISE 6.3. *Show: the pullback of a trivial bundle is a trivial bundle.*

THEOREM 6.8. *(Covering Homotopy Theorem) Let X and Y be topological spaces with X paracompact. Let $\pi : E \to Y$ be a vector bundle on Y, and let $f, g : X \to Y$ be homotopic maps. Then the pullbacks $f^*\pi$ and $g^*\pi$ are isomorphic vector bundles on X.*

PROOF. See for instance [**Hs66**, Thm. 4.7]. □

For our applications, it is enough to know that compact spaces are paracompact. But for culture we also remark that any regular σ-compact space is paracompact, e.g. any CW-complex with only finitely many cells of any given dimension.

COROLLARY 6.9. *If X is a contractible paracompact space, then every vector bundle on X is trivial.*

PROOF. Choose any point $x_0 \in X$, let $f : X \to X$ be the map which sends every point of X to x_0,and let $g : X \to X$ be the identity map. If $\pi : E \to X$ is any vector bundle on X, then by Theorem 6.8 we have $f^*\pi = g^*\pi$. Since g is the identity map, $g^*\pi = \pi$. On the other hand, tracking through the definitions shows $f^*\pi = X \times \pi^{-1}(x_0)$, a trivial bundle. So π is trivial. □

5. Stably free modules

Recall that an R-module M is **stably free** if there is a finitely generated free module F such that $M \oplus F$ is free. This definition is natural from the perspective of K-theory: the class $[P]$ in $\widetilde{K_0(R)}$ of a finitely generated projective module P is trivial iff P is stably free.

EXERCISE 6.4. *Let $0 \to A \to B \to P \to 0$ be a short exact sequence of R-modules, with P stably free. Show: A is stably free $\iff$ B is stably free.*

Certainly we have

$$\text{free} \implies \text{stably free} \implies \text{projective}.$$

Asking to what extent these implications can be reversed brings us quickly to some deep and beautiful mathematics.

5.1. Finite Generation.

We begin by addressing finite generation conditions.

EXERCISE 6.5. *(**Eilenberg Swindle**): Let us say that a projective module P is **weakly stably free** if there exists a not necessarily finitely generated free module F such that $P \oplus F$ is free. Show that every projective module is weakly stably free. (Hint: if $P \oplus Q$ is free, take $F = P \oplus Q \oplus P \oplus Q \oplus \ldots$.)*

EXERCISE 6.6. *Show: for a finitely generated projective module P, the following are equivalent:*

(i) *P is stably free.*

(ii) *P admits a **finite free resolution**: for some $n \in \mathbb{N}$ there is an exact sequence*

$$0 \to F_n \to \ldots \to F_0 \to P \to 0,$$

with each F_i a finitely generated free module.

This explains why the free module we take the direct sum with in the definition of stably free is required to be finitely generated. What happens if we take the module P to be infinitely generated? Here let us be sure that by an **infinitely generated R-module**, we mean an R-module which is *not* finitely generated.[4]

THEOREM 6.10. *(Gabel) Each infinitely generated stably free module is free.*

PROOF. Let M be infinitely generated and stably free. Choose $a \in \mathbb{N}$ such that $F = M \oplus R^a$ is free. Let $\{a_i\}_{i \in I}$ be a basis for F. Since F has an infinitely generated homomorphic image, I is infinite. Let $p : F \to R^a$ be the natural projection map $(x, y) \mapsto y$. For each standard basis element e_k of R^a lift it to $\widetilde{e_k}$ in F and let J_k be the "support" of $\widetilde{e_k}$, i.e., the set of indices i such that the coefficient of a_i in $\widetilde{e_k}$ is nonzero. Then $J = \bigcup_{k=1}^{a} J_k$ is finite. Let $F' = \langle a_i \rangle_{i \in J}$, so that F' is free of finite rank and F/F' is free of infinite rank. By construction $q(F') = R^a$; it follows that

$$F = F' + M.$$

Put $N = M \cap F'$, so

$$F'/N \cong R^a.$$

Since R^a is projective, the sequence

$$0 \to N \to F' \to R^a \to 0$$

splits, giving

$$F' \cong N \oplus R^a.$$

Further

$$F/F' \cong M/N,$$

[4] *A priori* it would be reasonable to take "infinitely generated R-module" to mean a module which possesses an infinite generating set, but a moment's thought shows that an R-module has this property if and onl if it is infinite, so it is more useful to define "infinitely generated" as we have.

so M/N is infinitely generated free: $M/N \cong R^a \oplus F''$ for a free module F''. In particular M/N is projective, so the sequence

$$0 \to N \to M \to M/N \to 0$$

splits. Putting all this together we get

$$M \cong N \oplus M/N \cong N \oplus R^a \oplus F'' \cong F' \oplus F''. \qquad \square$$

The following result – which we will not prove here – shows that for a large class of "reasonable rings" infinitely generated projective modules are much less interesting objects than finitely generated projectives, and thus gives further motivation to our restriction to the finitely generated case.

THEOREM 6.11. *(Bass* [**Ba63**]*) Let R be a connected Noetherian ring. Then any infinitely generated projective R-module is free.*

However, we can use Swan's Theorem to exhibit a nonfree infinitely generated projective module. Let $[0,1]$ be the closed unit interval with its topology: a compact, contractible space. By Corollary 6.9, every vector bundle over $[0,1]$ is trivial. By Swan's Theorem, this implies that every finitely generated projective module over the ring $R = C([0,1])$ of continuous functions $f : [0,1] \to \mathbb{R}$ is free.

But now – as in §3.9 – consider the ideal I of all functions $f \in R$ which vanish *near zero*, i.e., for which there exists $\epsilon(f) > 0$ such that $f|_{[0,\epsilon(f)]} \equiv 0$. Exercise 3.74 tells us that I is a projective R-module. Moreover, I is not a free R-module: indeed, any $f \in I$ is annihilated by any continuous function with support lying in $[0, \epsilon(f)]$, and nonzero such functions clearly exist. On the other hand, any nonzero free module has elements with zero annihilator: take any basis element.

Thus $C([0,1])$ is a connected ring over which every finitely generated projective module is free, but the infinitely generated projective module I is not free. (Theorem 6.11 says that no such modules exist over connected *Noetherian* rings.) Moreover I is therefore clearly not a direct sum of finitely generated modules, since by what we have established any such module over $C([0,1])$ would be free!

EXERCISE 6.7. *Use Corollary 3.51 to give a purely algebraic proof that I is not a direct sum of finitely generated submodules.*

EXERCISE 6.8. *Find necessary and sufficient conditions on a compact, contractible space X for there to exist a nonfree projective module.*

5.2. Ranks.

Later we will attach to a finitely generated projective module over any ring R a rank *function* (on $\operatorname{Spec} R$). However, for a stably free module we can – as for free modules – simply assign a rank. Namely, if we put $\operatorname{rank} P = b - a$.

EXERCISE 6.9. *Show: the rank of a finitely generated stably free module is well-defined.*

EXERCISE 6.10. *Show: for an R-module M, the following are equivalent:*

(i) *M is stably free of rank zero.*
(ii) *$M = 0$.*

Comment: This will be quite routine once we have the theory of localization. If you have trouble with the general case now, just show that $M \oplus R \cong R \implies M = 0$*, which is easier: every cyclic module is isomorphic to* R/I *for some ideal* I *of* R*; now consider annihilators.*

5.3. The least number of generators.

For a finitely generated R-module M we denote by $\operatorname{mg} M$ the minimal number of generators of M, i.e., the least n such that $R^n \twoheadrightarrow M$.

From a naive perspective this is perhaps the most natural numerical invariant associated to a finitely generated R-module. But in fact it behaves badly. Essentially its only good property is the obvious one: if $M_1 \twoheadrightarrow M_2$, then $\operatorname{mg}(M_2) \leqslant \operatorname{mg}(M_1)$. However, if $M_1 \hookrightarrow M_2$, then we certainly *need not have* $\operatorname{mg}(M_1) \leqslant \operatorname{mg}(M_2)$: let I be a finitely generated but nonprincipal ideal, and let $M_1 = I$, $M_2 = R$. One may momentarily hope that for finitely generated R-modules M_1 and M_2 we at least have $\operatorname{mg}(M_1 \oplus M_2) = \operatorname{mg}(M_1) + \operatorname{mg}(M_2)$ but in fact this is false even over the simplest rings: take $R = \mathbb{Z}$, $M_1 = \mathbb{Z}/2\mathbb{Z}$, $M_2 = \mathbb{Z}/3\mathbb{Z}$. But it gets even worse:

Exercise 6.11. *Let* R *be a ring and* M_1*,* M_2 *be finitely generated* R*-modules.*

a) *Suppose* R *is local. Show:* $\operatorname{mg}(M_1 \oplus M_2) = \operatorname{mg}(M_1) + \operatorname{mg}(M_2)$*. In fact, show that if* $0 \to M' \to M \to M'' \to 0$ *is a short exact sequence of finitely generated* R*-modules then* $\operatorname{mg}(M) = \operatorname{mg}(M') + \operatorname{mg}(M'')$*.*

b) *Suppose* R *is a PID. Show:* $\operatorname{mg}(M_1 \oplus M_1) = 2\operatorname{mg}(M_1)$*.*

c) *Suppose* R *is a Dedekind domain,*[5] *and* l I *is a nonzero proper ideal of* R*. Show:*

(i) • *If* I *is principal,* $\operatorname{mg}(I) = 1$*.*
• *If* I *is not principal,* $\operatorname{mg}(I) = 2$*.*

(ii) • *If* I^2 *is principal,* $\operatorname{mg}(I \oplus I) = 2$*.*

(iii) • *If* I^2 *is not principal,* $\operatorname{mg}(I \oplus I) = 3$*.*

d) *Deduce: For a nonprincipal ideal* I *in a Dedekind domain* R*,* $\operatorname{mg}(I \oplus I) < 2\operatorname{mg}(I)$*.*

Later we will see "better" invariants for certain subclasses of finitely generated R-modules, namely the rank for projective modules and the length for...finite length modules. Over a Dedekind domain every finitely generated module can be decomposed into the direct sum of a projective module and a finite length module. This does not hold over more general rings, e.g. the $\mathbb{C}[x,y]$-module $\mathbb{C}[x]$ is a torsion module of infinite length so cannot be so expressed.

Proposition 6.12. *A rank one stably free module is free.*

We will come back to prove this later once we have developed localization.

5.4. Around Hermite's Lemma.

In number theory and related branches of mathematics one studies sublattices Λ of the standard integral lattice $\mathbb{Z}^n$, i.e., rank n $\mathbb{Z}$-submodules of $\mathbb{Z}^n$. Their structure is surprisingly rich – for instance, the function $L_n(k)$ which counts the number of

[5]This exercise is stated now for continuity purposes, but to solve it you will probably want to use the theory of finitely generated modules over a Dedekind domain detailed in § 20.6.

index k sublattices of $\mathbb{Z}^n$ is arithmetically interesting and nontrivial. In particular, one question that comes up in the study of integer lattices is: which vectors $v \in \mathbb{Z}^n$ can be part of a $\mathbb{Z}$-basis of $\mathbb{Z}^n$? Unlike the answer for modules over a field (all nonzero vectors), there is an obvious obstruction: for instance there is no basis (v_1, v_2) of $\mathbb{Z}^2$ with $v_1 = (2, 0)$. For if so, the linear transformation $T : \mathbb{Z}^2 \to \mathbb{Z}^2$ given by $T((1,0)) = (2,0)$, $T((0,1)) = v_2 = (a,b)$ has determinant $2b$. Since this is not a unit in $\mathbb{Z}$, T is not invertible, which is a contradiction (make sure you see why, e.g. by using the universal property of free modules).

This observation can be vastly generalized, as follows: for a domain R and $n \in \mathbb{Z}^+$, we say $v = (x_1, \ldots, x_n) \in R^n$ is **a primitive vector** if $v \neq 0$ and $\langle x_1, \ldots, x_n \rangle = R$.

EXERCISE 6.12. *Let K be the fraction field of R. Show that $v \in (R^n)^\bullet$ is primitive if and only if $Kv \cap R^n = Rv$.*

EXERCISE 6.13. *Let R be a domain, and let $(b_1, \ldots, b_n)$ be a basis for R^n. Show that each b_i is a primitive vector.*

In 1850 Hermite proved that for integer lattices this is the only obstruction.

PROPOSITION 6.13. *(Classical Hermite Lemma) For a vector $v \in \mathbb{Z}^n$, the following are equivalent:*

(i) *There is $M \in \mathrm{GL}_n(\mathbb{Z})$ with $M(e_1) = v$, i.e., the first column of M is v.*
(ii) *There is a basis for $\mathbb{Z}^n$ containing v.*
(iii) *The vector v is primitive.*

For a proof of Proposition 6.13 in the classical style, see [**GoN**, § 1.3.3]. In fact the methods of module theory allow for a slicker proof of a more general result.

PROPOSITION 6.14.
Let R be a PID. For a vector $v \in R^n$, the following are equivalent:

(i) *There is $M \in \mathrm{GL}_n(R)$ with $M(e_1) = v$, i.e., the first column of M is v.*
(ii) *There is a basis for R^n containing v.*
(iii) *v is a primitive vector.*

PROOF. Any two bases of R^n are equivalent under $\mathrm{GL}_n(R)$. So (i) $\iff$ (ii).
(ii) $\implies$ (iii): If $v, v_2, \ldots, v_n$ is a basis for R^n and v were not primitive, then we would have $v = \alpha w$ for some $\alpha \in R^\bullet \backslash R^\times$. Then $w = \frac{1}{\alpha} v$ expresses w as a K-linear combination of the basis vectors with a nonintegral coefficient: contradiction.
(iii) $\implies$ (ii): Step 1: For a domain R and $v \in (R^n)^\bullet$, we claim that v is a primitive vector if and only if $R^n/\langle v \rangle$ is torsionfree.
Proof: Suppose v is not primitive: $v = \alpha v'$ for some $\alpha \in R^\bullet \backslash R^\times$. Then v' is a torsion element of $R^n/\langle v \rangle$. Conversely, suppose v is primitive. If$n = 1$ then $\langle v \rangle = R$ and the result holds trivially, so assume $n \geqslant 2$. Suppose there is $w \in R^n$ and $\alpha \in \mathbb{R}^\bullet$ such that $\alpha w = \beta v$ for some $\beta \in R$. Thus $w = \frac{\beta}{\alpha} v$. Since v is primitive, $\alpha \mid \beta$ and the image of w in $R^n/\langle v \rangle$ is zero.
Step 2: Consider the short exact sequence

$$0 \to \langle v \rangle \to R^n \to M \to 0,$$

with $M = R^n/\langle v \rangle$. By Step 1, M is a finitely generated torsionfree module over a PID, so it is free: indeed, tensoring to K and applying linear algebra we see that $M \cong R^{n-1}$. Thus the sequence splits: $R^n = \langle v \rangle \oplus M'$, with $M' \cong R^{n-1}$. Thus if $v_2, \ldots, v_n$ is an R-basis for M', $v, v_2, \ldots, v_n$ is an R-basis for R^n. $\square$

PROPOSITION 6.15. *Let R be a commutative ring, and let $n \in \mathbb{Z}^+$. the following are equivalent:*

(i) *If for an R-module M we have $M \oplus R \cong R^n$ then M is free.*
(ii) *Every primitive vector $v \in R^n$ is part of a basis for R^n.*

PROOF. We follow a treatment of K. Conrad [**Cd-SF**]. First we observe that when $n = 1$ both (i) and (ii) hold for all R-modules M: indeed, by Exercise 6.10, if $M \oplus R \cong R$ then $M = 0$, whereas (ii) is completely vacuous in this case.
(i) $\implies$ (ii): Assume (i). For $\mathbf{v} = (v_1, \ldots, v_n)$, $\mathbf{w} = (w_1, \ldots, w_n) \in R^n$, let $\mathbf{v} \cdot \mathbf{w} = \sum_{i=1}^n v_i w_i$. Let $\mathfrak{a} = (a_1, \ldots, a_n) \in R^n$ be a primitive vector. Observe that this is equivalent to the existence of $\mathfrak{b} = (b_1, \ldots, b_n) \in R^n$ with $\mathfrak{a} \cdot \mathfrak{b} = 1$ and fix such a $\mathfrak{b}$. Consider the R-linear functional $f : R^n \to R$ given by $\mathbf{v} \mapsto \mathbf{v} \cdot \mathfrak{b}$. Since $f(\mathfrak{a}) = 1$ it is nonzero and thus there is a short exact sequence

$$0 \to \operatorname{Ker} f \to R^n \xrightarrow{f} R \to 0.$$

Since R is projective, this sequence splits, giving $R^n \cong \operatorname{Ker} f \oplus R$. More concretely a splitting is given by a section $\sigma : R \to R^n$ of f which is determined by mapping $1 \in R$ to any $v \in R^n$ with $f(v) = 1$. Thus $1 \mapsto \mathfrak{a}$ gives an internal direct sum decomposition

$$R^n = \operatorname{Ker} f \oplus \langle \mathfrak{a} \rangle \cong \operatorname{Ker} f \oplus R.$$

By our hypothesis (i), $\operatorname{Ker} f$ is free, and if $\mathfrak{b}_2, \ldots, \mathfrak{b}_n$ is a basis for $\operatorname{Ker} f$ then $\mathfrak{a}, \mathfrak{b}_2, \ldots, \mathfrak{b}_n$ is a basis for R^n containing $\mathfrak{a}$.
(ii) $\implies$ (i): Let $g : M \oplus R \xrightarrow{\sim} R^n$ be an R-module isomorphism. Put $\mathfrak{a} = (a_1, \ldots, a_n) = g(0, 1)$. We claim that $\mathfrak{a}$ is a primitive vector. If not, there is a maximal ideal $\mathfrak{m}$ such that $\langle a_1, \ldots, a_n \rangle \subseteq \mathfrak{m}$. But

$$g|_{\mathfrak{m}(M \oplus R^n)} : \mathfrak{m}M \oplus \mathfrak{m} \xrightarrow{\sim} (\mathfrak{m}R)^n,$$

and $g(0, 1) = \mathfrak{a} \in (\mathfrak{m}R)^n$, so $(0, 1) \in \mathfrak{m}M \oplus (\mathfrak{m}R)^n$, a contradiction. Thus by (ii) there is a basis $\mathfrak{a}, \mathfrak{b}_2, \ldots, \mathfrak{b}_n$ of R^n, so that $g^{-1}(\mathfrak{a}), g^{-1}(\mathfrak{b}_2), \ldots, g^{-1}(\mathfrak{b}_n)$ is a basis of $M \oplus R$. For $2 \leqslant i \leqslant n$ we write $g^{-1}(\mathfrak{b}_i) = (x_i, c_i)$. Subtracting off from each of these vectors a suitable scalar multiple of $g^{-1}(\mathfrak{a}) = (0, 1)$ we get a new basis $(0, 1), (x_2, 0), \ldots, (x_n, 0)$ of $M \oplus R$. Then $x_2, \ldots, x_n$ is a basis for M. □

THEOREM 6.16. *For a commutative ring R, the following are equivalent:*

(i) *For all R-modules M, if $M \oplus R$ is free, then M is free.*
(ii) *For all $n \in \mathbb{Z}^+$, every primitive vector $v \in R^n$ is an element of some basis of R^n.*
(iii) *Every stably free R-module M is free.*

*A ring satisfying these equivalent conditions will be called an **L-Hermite ring**.*

PROOF. Since an infinitely generated stably free module is free (Theorem 6.10), in parts (i) and (iii) we may – and shall – assume M is finitely generated. Then:
(i) $\iff$ (ii) is immediate from Proposition 6.15.
(i) $\implies$ (iii): It suffices to show that for all finitely generated modules M and all $a \in \mathbb{N}$, if $M \oplus R^a$ is free then M is free. We go by induction on n, the case $n = 0$ being trivial. Suppose the result holds for $a \in \mathbb{N}$. Then $M \oplus R^{a+1} \cong (M \oplus R^a) \oplus R$ is free, so by (i) $M \oplus R^a$ is free, and then by induction M is free.
(iii) $\implies$ (i) is immediate. □

5.5. Swan's Construction.

For $n \in \mathbb{N}$, let

$$R_n = \mathbb{R}[t_0, \ldots, t_n]/\langle t_0^2 + \ldots + t_n^2 - 1\rangle.$$

EXERCISE 6.14. *Show: R_n is a domain if and only if $n \geq 1$.*

Consider the map $H : R_n^{n+1} \to R_n$ obtained by taking the dot product of $\mathbf{v} = (v_1, \ldots, v_{n+1})$ with $\mathbf{t} = (t_0, \ldots, t_n)$. For $0 \leq i \leq n$, let e_i be the ith standard basis vector of R_n^{n+1}; then $H(e_i) = t_i$, so the image of H contains $\langle t_0, \ldots, t_n\rangle = R_n$: H is surjective. Let $P_n = \operatorname{Ker} H$, so we have a short exact sequence

$$0 \to P_n \to R_n^{n+1} \xrightarrow{H} R_n \to 0.$$

As above, this sequence splits and since $\mathbf{t} \cdot \mathbf{t} = 1$, a canonical section is given by mapping $1 \in R_n$ to $\mathbf{t}$. In particular

$$P_n \oplus R_n \cong R_n^{n+1}$$

so P_n is stably free. When is it free?

THEOREM 6.17. *(Swan) The stably free R_n-module P_n is free if and only if $n = 0, 1, 3$ or 7.*

PROOF. Step 0: Since $P_0 = 0$, it is free. Moreover P_1 has rank 1 so is free by general principles (Proposition 6.12). But this is overkill: in fact one sees that $-t_1 e_0 + t_0 e_1$ is a basis for P_1. Similarly one can simply write down bases for P_3 and P_7 in a concrete manner: we leave this as an exercise for the reader.
Step 1: Suppose $n \notin \{0, 1, 3, 7\}$. We wish to show that P_n is *not* free. The key observation is that it is enough to do so after any base change: that is, if $R_n \to S$ is a ring map and M is an R-module such that $M \otimes_{R_n} S$ is not a free S-module, then M is not a free R-module. What is the natural base change to make?

Notice that R_n is nothing else than the ring of polynomial functions on the unit sphere $S^n \subseteq \mathbb{R}^{n+1}$. For those unitiated in the above jargon we spell it out more explicitly: every $f \in \mathbb{R}[t_0, \ldots, t_{n+1}]$ induces a function from $\mathbb{R}^{n+1} \to \mathbb{R}$ and thus by restriction a function $S^n \to \mathbb{R}$. We wish to identify polynomials which define the same function on S^n, and to do so we should at least impose the relation $t_0^2 + \ldots + t_n^2 - 1 = 0$ since this function vanishes identically on S^n. As we will see later when we study the Nullstellensatz, since by Exercise 6.14 the ideal $I = \langle t_0^2 + \ldots + t_n^2 - 1\rangle$ is prime, it is radical and thus the relation $I(V(I)) = I$ tells us that the only polynomials which vanish identically on S^n are those in I.

Since every polynomial function is a continuous function for the Euclidean topology on S^n, we get an extension of rings $R_n \to C(S^n)$. So our bright idea is to show insteaad that the finitely generated projective $C(S^n)$-module

$$T_n = P_n \otimes_{R_n} C(S^n)$$

is not free. By Swan's Theorem, T_n corresponds to a vector bundle on S^n and it is equivalent to show that this vector bundle is nontrivial. [6]
Step 3: We claim that in fact T_n is nothing else but the tangent bundle of S^n. Indeed, we have $S^n \subseteq \mathbb{R}^{n+1}$. The tangent bundle to $\mathbb{R}^{n+1}$ is trivial, hence so is its

[6]Thus in summary we have just accomplished the following exciting maneuver: using basic affine algebraic geometry, we have completely transferred our problem from the domain of commutative algebra to that of differential topology!

pullback to S^n, say F^{n+1}. Further, there is a surjective bundle map from F^{n+1} to the rank one trivial bundle F^1: at every point of S^n we orthogonally project to the outward normal vector. The kernel of this bundle map is $T(S^n)$. Thus we have a short exact sequence of vector bundles

$$0 \to TS^n \to F^{n+1} \to F \to 0.$$

We claim that under the Swan's Theorem equivalence of categories, this split exact sequence corresponds to the split exact sequence

$$0 \to T_n \to C(S^n)^{n+1} \stackrel{H}{\to\to} C(S^n) \to 0$$

which is the base change to $C(S^n)$ of the defining short exact sequence of S^n. We leave it to the interested reader to piece this together from our consruction of P_n. Step 4: By a classical theorem of Bott and Milnor [**BM58**], the tangent bundle of S^n is trivial if and only if $n \in \{0, 1, 3, 7\}$. □

EXERCISE 6.15. *Show: P_n is free for $n = 3$ and $n = 7$.*

EXERCISE 6.16. *Find stably free but not free modules of ranks 3 and 7.*

The Bott-Milnor Theorem is a deep and celebrated result. Their original proof used the recently developed tools of midcentury differential topology: Stiefel-Whitney and Pontrjagin classes, cohomology operations, and so forth. In 1962 J.F. Adams determined for each n the largest rank of a trivial subbundle of $T(S^n)$ [**Ad62**]. The K-theory developed in the 1960's gave more graceful proofs: we recommend that the interested reader consult, for instance, [**Ka**, § V.2].

If one merely wants *some* values of n for which P_n is not free, one can use much lower technology. for instance, the Poincaré-Hopf Theorem [**Mi**, p. 35] implies that a closed n-manifold which admits a nowhere vanishing vector field (equivalently a trivial rank one subbundle of its tangent bundle; this is much weaker than the tangent bundle being trivial) must have zero Euler characteristic. The Euler characteristic of S^n is $1 + (-1)^n$, so it is nonzero for all even n.

CHAPTER 7

Localization

1. Definition and first properties

As we have seen, one way to "simplify" the study of ideals in a ring R is to pass to a quotient ring R/I: as we have seen, this has the (often useful) effect of "cutting off the bottom" of the ideal lattice by keeping only ideals $J \supset I$. There is another procedure, **localization**, which effects the opposite kind of simplification: given a **prime** ideal P of R, there is a ring R_P together with a canonical map $\iota : R \to R_P$ such that $\iota^* : \mathcal{I}(R_P) \to \mathcal{I}(R)$ is an injection whose image is precisely the ideals $J \subseteq P$. As usual, ι^* carries prime ideals to prime ideals. In particular, assuming only that P is prime, we get a corresponding ideal – rather inelegantly but standardly denoted PR_P – which is the **unique maximal** ideal of R_P. If we can take $P = (0)$ – i.e., if R is a domain – this means that PR_P is the only ideal of R_P, which is therefore a field. In fact it is nothing else than the quotient field of the domain R, and – with one exception – all the secrets of localization are already present in this very familiar special case.

In fact the localization construction is a bit more general than this: given an arbitrary ring R (of course commutative with unity!) and an arbitrary **multiplicative subset** S of R – this just means that $1 \in S$ and $SS \subseteq S$ – we will define a new ring R_S together with a canonical homomorphism $\iota : R \to R_S$ (for which ι^* will still be an injection with explicitly given image). Just as in the case of quotients, ι satisfies a certain universal mapping property, but let us sacrifice some elegance for intelligibility by working our way up to this crisp definition.

Indeed, first consider the special case in which R is a domain, with fraction field F. Then R_S will be an extension ring of R, still with fraction field F, which is obtained by adjoining to R all elements $\frac{1}{s}$ for $s \in S$.

EXAMPLE 7.1. *Suppose $R = \mathbb{Z}$, $S = \{2^n\}_{n \in \mathbb{N}}$. Then $R_S = \mathbb{Z}[\frac{1}{2}]$. Indeed we see that for any nonzero element f, we can take S to be the multiplicative set consisting of the powers of f, and then the localization is just $R[\frac{1}{f}]$.*

What if in the example above, instead of taking the multiplicative subset generated by 2, we took the multiplicative subset generated by 2^2, or 2^{127}? Clearly it wouldn't matter: if we have $\frac{1}{2^k}$ for any k in our subring of $\mathbb{Q}$, we also have $\frac{2^{k-1}}{2^k} = \frac{1}{2}$. To generalize this idea, define the **saturation** $\mathbb{S}$ of a multiplicatively closed subset S of a domain R to be the set $\{a \in R \mid \exists b \in R \mid ab \in S\}$, i.e., the set of all divisors of elements of S. The same observation as above shows that $R_S = R_{\mathbb{S}}$, so if we like we can restrict to consideration of saturated multiplicatively closed subsets.

Example, continued: The saturated, multiplicatively closed subsets of $\mathbb{Z}$ correspond to (arbitary) subsets $\mathcal{P}$ of the prime numbers (exercise!). In particular $\mathbb{Z}$ itself corresponds to $\mathcal{P} = \varnothing$, $\mathbb{Z}[\frac{1}{p}]$ corresponds to $\mathcal{P} = \{p\}$, $\mathbb{Q}$ corresponds to the set of all primes. Most interestingly, fix any prime p and let $\mathcal{P}$ be the set of all primes **except** p: then the corresponding ring, which is confusingly denoted $\mathbb{Z}_{(p)}$ is the set of all rational numbers of the form $\frac{x}{y}$ where p does not divide y. Notice that such rings are the maximal subrings of $\mathbb{Q}$ which are not fields. Moreover, the units of $\mathbb{Z}_{(p)}$ are precisely the elements of the form $\frac{x}{y}$ with $(p, x) = 1$. The nonunits a are all of the form pa' for $a' \in \mathbb{Z}_{(p)}$, so therefore the unique maximal ideal is the principal ideal $(p) = p\mathbb{Z}_{(p)}$.

EXERCISE 7.1. *Show: the only ideals in $\mathbb{Z}_{(p)}$ are those of the form $(p)^k$ for some $k \in \mathbb{N}$.*

Now let R be any ring and S a multiplicatively closed subset of R. We would still like to define a ring $S^{-1}R$ which is, roughly speaking, obtained by adjoining to R all inverses of elements of S. We can still define $S^{-1}R$ in terms of formal quotients, i.e., as equivalence classes of elements (a, b) with $a \in R$, $b \in S$. However, if we define $(a, b) \sim (c, d)$ to be $ad = bc$, then unfortunately we find that this need not be an equivalence relation! Indeed:

EXERCISE 7.2. *Let R be a nonzero ring that is not a domain: thus there are $a, b \in R\backslash\{0\}$ such that $ab = 0$. Let $S = \{a^n \mid a \in \mathbb{N}\}$. Show that the relation $\sim$ on $R \times S$ defined by*

$$(r_1, s_1) \sim (r_2, s_2) \text{ if } s_1 r_2 = s_2 r_1$$

is not *transitive.*

Therefore we need to enlarge the relation a bit: we put $(a, b) \sim (c, d)$ if and only if there is $s \in S$ such that $sad = sbc$. We then define

$$\frac{a}{s} + \frac{b}{t} := \frac{at + bs}{st},$$
$$\frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}.$$

We must check that these operations are well-defined on equivalence classes; this is left as a (perhaps somewhat tedious, but not difficult) exercise for the reader.

EXERCISE 7.3. *Let R be a ring, and let $S \subseteq R$ be a multiplicative subset. We wish to consider three relations on $R \times S$: the first relation $\sim_1$ i the "wrong" relation considered above:*

$$(r_1, s_1) \sim_1 (r_2, s_2) \text{ if } s_1 r_2 = s_2 r_1.$$

By Exercise 7.2, the relation $\sim_1$ can fail to be transitive when R is not a domain. So we define the relation $\sim_2$ to be the transitive closure of $\sim_1$, i.e., the smallest transitive relation on $R \times S$ that contains $\sim_1$. We define $\sim_3$ to be the "right relation":

$$(r_1, s_1) \sim (r_2, s_2) \text{ if there is } s \in S \text{ such that } ss_1 r_2 = ss_2 r_1.$$

a) *Show: $\sim_1$ is reflexive and symmetric, and deduce that $\sim_2$ is an equivalence relation.*
b) *Show: $\sim_2 = \sim_3$. Deduce: the "right relation" $\sim_3$ is the equivalence relation generated by (i.e., the smallest equivalence relation containing) the "wrong relation" $\sim_1$.*

EXERCISE 7.4. *Indeed, check that $S^{-1}R$ is a ring and that $x \mapsto \frac{x}{1}$ defines a homomorphism of rings $R \to S^{-1}R$. Thus $S^{-1}R$ is an R-algebra, and in particular an R-module.*

EXERCISE 7.5. *Let R be a domain and $S = R^\bullet = R\backslash\{0\}$. Show: $S^{-1}R$ is indeed the fraction field of R.*

When $f \in R$, we denote the localization of R at the multiplicative subset generated by f as R_f.

EXAMPLE 7.2. *Suppose $f \in R$ is a nilpotent element: $f^n = 0$ for some $n \in \mathbb{Z}^+$. Then $1 = \frac{f^{n-1}}{f^{n-1}}$ whereas $0 = \frac{0}{f}$. Since $(f^{n-1} \cdot f - f^{n-1} \cdot 0) = 0$, we have that $1 = 0$, i.e., R_f is the zero ring. Conversely, if $1 = 0$ in R_f, then there is $s \in \{f^n \mid n \in \mathbb{N}\}$ such that $0 = s \cdot 1 = s$, so f is nilpotent. The same argument shows that for any multiplicative subset S, we have that $S^{-1}R$ is the zero ring if and only if $0 \in S$.*

EXERCISE 7.6.

a) *Show: the kernel of the natural map $R \to S^{-1}(R)$ is the set of all $r \in R$ such that for some $s \in S$, $sr = 0$.*
b) *The map $R \to S^{-1}(R)$ is injective if and only if S has no zerodivisors.*
c) *Show that the subset Q of all nonzerodivisors of a ring R is multiplicatively closed. The localization $Q^{-1}R$ is called the **total fraction ring** of R. Show that $Q^{-1}(R)$ is a field if and only if R is a domain.*

EXERCISE 7.7. *Show: the homomorphism $R \to S^{-1}R$ is universal for homomorphisms $R \to T$ with $f(S) \subseteq T^\times$.*

EXERCISE 7.8. *A multiplicatively closed subset S of a ring R is **saturated** if for all $s \in S$ and all $t \in R$, if $t \mid s$ then $t \in S$.*

a) *For a multiplicatively closed subset $S \subseteq R$, define its **saturation** $\mathbf{S} = \{t \in R \mid t \mid s \text{ for some } s \in S\}$. Show that $\mathbf{S}$ contains S, is multiplicatively closed and saturated, and is minimal with these properties: if $T \supset S$ is saturated and multiplicatively closed, then $T \supset \mathbf{S}$.*
b) *Show: the rings $\mathbf{S}^{-1}R$ and $S^{-1}R$ are canonically isomorphic.*
c) *Let I be an ideal of R. Show that the following are equivalent:*
   (i) *$R\backslash I$ is multiplicatively closed.*
   (ii) *$R\backslash I$ is multiplicatively closed and saturated.*
   (iii) *I is a prime ideal.*
d) *Let $\mathbf{S} \subseteq R$ be a saturated multiplicatively closed subset. Show: there is a subset $Y \subseteq \operatorname{Spec} R$ such that $\mathbf{S} = \bigcap_{\mathfrak{p} \in Y} (R\backslash\mathfrak{p})$.*
   (Hint: use Multiplicative Avoidance.)

EXERCISE 7.9. *Let S be a multiplicative subset of a domain R, with saturation $\mathbf{S}$. Show:*

$$(S^{-1}R)^\times \cap R = \mathbf{S}.$$

2. Pushing and pulling via a localization map

Let R be a ring and S a multiplicatively closed subset. Let $\iota : R \to S^{-1}R$ be the natural map. As for any homomorphism of rings, ι induces maps between the sets of ideals of R and the set of ideals of $S^{-1}R$, in both directions:

$$\iota_* : \mathcal{I}_R \to \mathcal{I}_{S^{-1}R},\ I \mapsto IS^{-1}R,$$

$$\iota^* : \mathcal{I}_{S^{-1}R} \to \mathcal{I}_R,\ J \mapsto \iota^{-1}(J).$$

LEMMA 7.3. *Let $\iota : R \to S^{-1}R$ be as above. For an ideal I of R, we have*

$$\iota_*(I) = \{\frac{x}{s} \in S^{-1}R \mid x \in I,\ s \in S\}.$$

PROOF. Let us temporarily write

$$\mathcal{I} = \{\frac{x}{s} \in S^{-1}R \mid x \in I,\ s \in S\}.$$

We want to show that $\mathcal{I} = \iota_*(I) = \langle \iota(I) \rangle_{S^{-1}R}$. It is clear that $\iota(I) \subseteq \mathcal{I} \subset \iota_*(I)$, so it is enough to show that $\mathcal{I}$ is itself an ideal of $S^{-1}R$. No problem: if $\frac{x_1}{s_1},\ \frac{x_2}{s_2} \in \mathcal{I}$,

$$\frac{x_1}{s_1} + \frac{x_2}{s_2} = \frac{x_1 s_2 + x_2 s_1}{s_1 s_2} \in \mathcal{I},$$

and if $\frac{y}{s} \in S^{-1}R$, then

$$\frac{y}{s}\frac{x_1}{s_1} = \frac{x_1 y}{s s_1} \in \mathcal{I}.$$ □

Like quotient maps, any localization map has the **pull-push property**.

PROPOSITION 7.4. *Let $\iota : R \to S^{-1}R$ be as above. For an ideal J of $S^{-1}R$, we have*

$$J = \iota_* \iota^* J.$$

PROOF. We have seen before that for any homomorphism $\iota : R \to R'$ of rings and any ideal J of R' we have

$$\overline{J} := \iota_* \iota^* J \subseteq J.$$

Thus it is enough to show the reverse containment. For this, consider an arbitrary element $\frac{x}{s} \in J$. Then $x = s\frac{x}{s} \in J$ hence also $x \in \iota^*(J)$, so $\iota(x) \in \overline{J}$. But since $\overline{J}$ is an ideal and s is a unit in $S^{-1}R$, we then also have $\frac{1}{s}x = \frac{x}{s} \in \overline{J}$. □

LEMMA 7.5. *Let $\iota : R \to S^{-1}R$ be as above and I an ideal of R. The following are equivalent:*

(i) $I \cap S \neq \varnothing$.
(ii) $\iota_*(I) = S^{-1}R$.

PROOF. (i) $\implies$ (ii): If $s \in S \cap I$, then $s \in IS^{-1}R$, so $1 = \frac{s}{s} \in \iota_*(I)$.
(ii) $\implies$ (i): Suppose $1 \in \iota_*(I)$. By Lemma 7.3, $\frac{1}{1} = \frac{x}{s}$ for some $x \in I$ and $s \in S$. Clearing denominators, there is $s' \in S$ such that $ss' = s'x$ and thus $ss' \in I \cap S$. □

PROPOSITION 7.6. *Let $\iota : R \to S^{-1}R$ be a localization homomorphism.*

a) *For a prime ideal $\mathfrak{p}$ of R, the following are equivalent:*
   (i) *The pushforward $\iota_*\mathfrak{p}$ is prime in $S^{-1}R$.*
   (ii) *The pushforward $\iota_*\mathfrak{p}$ is proper in $S^{-1}R$.*
   (iii) *We have $\mathfrak{p} \cap S = \varnothing$.*
b) *If $\mathfrak{p}$ is prime and disjoint from S, then $\iota^*(\iota_*\mathfrak{p}) = \mathfrak{p}$.*

PROOF. a) (i) $\implies$ (ii) since prime ideals are proper.
(ii) $\iff$ (iii) for all ideals of R by Lemma 7.5.
(iii) $\implies$ (i): Suppose $\mathfrak{p}$ is a prime ideal of R, and suppose we have $\frac{a_1}{s_1},\ \frac{a_2}{s_2} \in S^{-1}R$ with $\frac{a_1}{s_1}\frac{a_2}{s_2} = \frac{x}{s} \in \iota_*(\mathfrak{p})$. Clearing denominators, there is $s' \in S$ such that

$$ss'a_1a_2 = s's_1s_2x \in \mathfrak{p}.$$

Since $S \cap \mathfrak{p} = \varnothing$, $(ss') \notin \mathfrak{p}$, and since $\mathfrak{p}$ is prime, we conclude that $a_1 a_2 \in \mathfrak{p}$ and then that $a_i \in \mathfrak{p}$ for some i, hence $\frac{a_i}{s_i} \in \iota_* \mathfrak{p}$ for some i and $\iota_*(\mathfrak{p})$ is prime. This completes the proof of part a).
b) Recall: for any homomorphism $\iota : R \to R'$ and any ideal I of R we have

$$\iota^*(\iota_*(I)) \supset I,$$

so taking $I = \mathfrak{p}$ to be prime it suffices to show the inverse inclusion. Suppose $x \in \iota^* \iota_* \mathfrak{p}$, i.e., there exist $a \in \mathfrak{p}$, $s \in S$ such that $\iota(x) = \frac{x}{1} = \frac{a}{s}$. By definition, this means that there exists some $s' \in S$ such that $s'sx = s'a \in \mathfrak{p}$. Therefore either $s's \in \mathfrak{p}$ or $x \in \mathfrak{p}$, but since $s's \in S$ and S is disjoint from $\mathfrak{p}$, we must have $x \in \mathfrak{p}$. □

COROLLARY 7.7. *The maps ι^* and ι_* give mutually inverse bijections from the set of prime ideals of $S^{-1}R$ to the set of prime ideals of R that are disjoint from S.*

Therefore we may – and shall – view $\operatorname{Spec} S^{-1}R$ as a subset of $\operatorname{Spec} R$.

EXERCISE 7.10.

a) *Show: the results of Proposition 7.6 extend to all* primary *ideals of R.*[1]
b) *Let I be* any *ideal of R. Show that*

$$\iota^* \iota_* I = \{x \in R \mid \exists s \in S \text{ such that } sx \in I\}.$$

c) *Exhibit a map $\iota : R \to S^{-1}R$ and a (nonprimary) ideal I of R such that $\iota^* \iota_* I \supsetneq I$.*

EXERCISE 7.11. *Let R be a ring, let $S \subseteq R$ be a multiplicative subset, and let I, J be ideals of R. Recall:*

$$(I :_R J) := \{x \in R \mid xJ \subseteq I\}.$$

a) *Show: $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$.*
b) *Show: $S^{-1}(I + J) = S^{-1}I + S^{-1}J$.*
c) *Show: $S^{-1}(IJ) = (S^{-1}I)(S^{-1}(J)$.*
d) *Show: if J is finitely generated, then we have $S^{-1}(I : J) = (S^{-1}I : S^{-1}J)$.*

3. The fibers of a morphism

Let $f : R \to S$ be a homomorphism of rings, and let $\mathfrak{p} \in \operatorname{Spec} R$. Consider the "fiber of $f^* : \operatorname{Spec} S \to \operatorname{Spec} R$ over $\mathfrak{p}$", i.e.,

$$f_{\mathfrak{p}} = (f^*)^{-1}(\mathfrak{p}) = \{\mathcal{P} \in \operatorname{Spec} S \mid f^*(\mathcal{P}) = \mathfrak{p}\}.$$

We claim that $f_{\mathfrak{p}}$ is canonically isomorphic to the spectrum of a certain ring. Namely, let $k(\mathfrak{p})$ be the fraction field of the domain $R/\mathfrak{p}$. Then we wish to identify $f_{\mathfrak{p}}$ with $\operatorname{Spec}(S \otimes_R k(\mathfrak{p}))$.

Let $\iota_1 : S \to S \otimes_R k(\mathfrak{p})$ and $\iota_2 : k(\mathfrak{p}) \to S \otimes_R k(\mathfrak{p})$ be the canonical maps. The tensor product of R-algebras fits into a commutative square (INSERT) and is indeed the categorical **pushout**: in other words, given any ring A and homomorphisms $\varphi_1 : A \to S$ $\varphi_2 : A \to k(\mathfrak{p})$ such that the composite homomorphisms $\iota_1 \circ \varphi_1 = \iota_2 \circ \varphi_2$ are equal, there exists a unique homomorphism $\Phi : A \to R$ such that $f \circ \Phi = \varphi_1$ and $q \circ \Phi = \varphi_2$, where $q : R \to R/\mathfrak{p}$ is the quotient map.

[1]Recall $\mathfrak{p}$ is primary if for $a, b \in R$ such that $ab \in \mathfrak{p}$, either $a \in \mathfrak{p}$ or $b^n \in \mathfrak{p}$ for some $n \in \mathbb{Z}^+$. We have not yet done much with this concept, and will not really address it squarely until the section on primary decomposition.

On the spectral side, all the arrows reverse, and the corresponding diagram is (INSERT), which expresses $\operatorname{Spec}(S \otimes_R k(\mathfrak{p}))$ as the fiber product of $\operatorname{Spec} S$ and $\operatorname{Spec} k(\mathfrak{p})$ over $\operatorname{Spec} R$.

Observe that the map $\iota_1 : S \to S \otimes_R k(\mathfrak{p})$ is the composite of the surjective map $q_1 : S \to S \otimes_R R/\mathfrak{p}$ with the map $\ell_2 : S \otimes_R R/\mathfrak{p} \to (S \otimes_R R/\mathfrak{p}) \otimes_{R/\mathfrak{p}} k(\mathfrak{p})$, the latter map being localization with respect to the multiplicatively closed subset $q_1(R\backslash\mathfrak{p})$. Both q_1^* and ℓ_2^* are injections, and therefore $\iota_{1*} = q_1^* \circ \ell_2^*$ is injective. Similarly $\operatorname{Spec} k(\mathfrak{p}) \hookrightarrow \operatorname{Spec} R$ (this is just the special case of the above with $R = S$). It follows that the above diagram identifies $\operatorname{Spec} S \otimes_R k(\mathfrak{p})$ with the prime ideals $\mathcal{P}$ of $\operatorname{Spec} S$ such that $f^*\mathcal{P} = \mathfrak{p}$.

4. Commutativity of localization and passage to a quotient

LEMMA 7.8. *Let R be a ring, $S \subseteq R$ a multiplicatively closed subset, and I an ideal of R. Write $q : R \to R/I$ for the quotient map and put $\overline{S} := q(S)$. Then there is a canonical isomorphism*

$$S^{-1}R/IS^{-1}R \cong \overline{S}^{-1}(R/I).$$

PROOF. Explicitly, we send $\frac{a}{s} \pmod{I}S^{-1}R$ to $\frac{\overline{a}}{\overline{s}}$, where $\overline{a} = a + I$, $\overline{s} = s + I$. It is straightforward to check that this an isomorphism. □

Matsumura makes the following nice comment: both sides satisfy the universal property for homomorphisms $f : R \to R'$ such that $f(S) \subseteq (R')^\times$ and $f(I) = 0$. Therefore they must be canonically isomorphic.

5. Localization at a prime ideal

An extremely important example of a multiplicative subset of R is the complement $R\backslash\mathfrak{p}$ of a prime ideal $\mathfrak{p}$. As a matter of notation, we write $R_\mathfrak{p}$ for $(R\backslash\mathfrak{p})^{-1}R$.[2]

PROPOSITION 7.9. *If $\mathfrak{p}$ is a prime ideal of R, then the localization $R_\mathfrak{p}$ is a local ring with unique maximal ideal $\mathfrak{p}R_\mathfrak{p}$.*

PROOF. We know that the primes of the localized ring are precisely the push-forwards of the prime ideals of R which are disjoint from the muliplicatively closed set. Here $S = R\backslash\mathfrak{p}$, so being disjoint from S is equivalent to being contained in $\mathfrak{p}$. Thus the unique maximal such element is indeed $\mathfrak{p}R_\mathfrak{p}$. □

Remark: We will simply write $\mathfrak{p}$ for the maximal ideal $\mathfrak{p}R_\mathfrak{p}$ of $R_\mathfrak{p}$.

Proposition 7.9, simple though it is, is of inestimable importance. It shows that the effect of localization at a prime ideal on the lattice of ideals is dual to that of passage to the quotient: if we mod out by a prime $\mathfrak{p}$, we get a ring $R/\mathfrak{p}$ whose ideals are precisely the ideals of R containing $\mathfrak{p}$. However, if we localize at $R\backslash\mathfrak{p}$, we get a ring whose ideals are precisely the ideals of R contained in $\mathfrak{p}$. In particular, this

[2]This is inevitably a bit confusing at first, but our choice of notation for a loacalization is designed to make this less confusing. The other common notation for the localization, R_S, creates a notational nightmare. As a mnemonic, remember that we gain nothing by localizing at a subset S containing 0, since the corresponding localization is the trivial ring.

construction motivates us to develop an especially detailed theory of local rings, by assuring us that such a theory could be put to good use in the general case.

EXERCISE 7.12. *True or false: If $(R, \mathfrak{m})$ is a local ring and $S \subseteq R^\bullet$ is a multiplicatively closed set, then $S^{-1}R$ is a local ring (or the zero ring).*

EXERCISE 7.13. *Let R be a ring, and let $S \subseteq R^\bullet$ be a saturated multiplicatively closed subset such that the localization $S^{-1}R$ is a local ring with maximal ideal $\mathfrak{m}$. Write $\iota : R \to S^{-1}R$ be the localization map. Show:*

$$S = R \backslash \iota^*(\mathfrak{m}).$$

6. Localization of modules

If S is any multiplicative subset and M is any R-module, we can also construct a localized R-module $S^{-1}M$. One the one hand, we can construct this exactly as we did $S^{-1}R$, by considering the appropriate equivalence relation on pairs $(m, s) \in M \times S$. On the other hand, we can just take the base extension $S^{-1}R \otimes M$. We are left with the task of showing that these two constructions are "the same".

EXERCISE 7.14. *Formulate a universal mapping property for the localization morphism $M \to S^{-1}M$. Check that both of the above constructions satisfy this universal mapping property, and deduce that they are canonically isomorphic.*

EXERCISE 7.15.

a) *Show: the kernel of $M \to S^{-1}M$ is the set of $m \in M$ such that $\operatorname{ann}(m) \cap S \neq \varnothing$.*

b) *Let R be a domain with fraction field K. Let M be an R-module. Show:*

$$\operatorname{Ker}(M \to M \otimes K) = M[\text{tors}].$$

c) *Use part b) to give a new proof of Proposition 3.8b).*

EXERCISE 7.16. *Let N be any $S^{-1}R$-module. Show that there exists an R-module M such that $N \cong S^{-1}R \otimes_R M$.*

Generally speaking, thinking of $S^{-1}M$ as $S^{-1}R \otimes_R M$ is more convenient for proving results, because it allows us to employ the theory of tensor products of modules. For example:

PROPOSITION 7.10. *For any ring R and multiplicatively closed subset S of R, $S^{-1}R$ is a flat R-module. Equivalently, if*

$$0 \to M' \to M \to M'' \to 0$$

is a short exact sequence of R-modules, then

$$0 \to S^{-1}M' \to S^{-1}M \to S^{-1}M'' \to 0$$

is a short exact sequence of R-modules (or equivalently, of $S^{-1}R$-modules).

PROOF. Tensor products are always right exact, so we need only show $S^{-1}M' \hookrightarrow S^{-1}M$. Suppose not: then there exists $m' \in M'$ and $s \in S$ such that $\frac{m'}{s} = 0 \in M$. Thus there is $g \in S$ such that $gm' = 0$, but if so, then $\frac{m'}{s} = 0$ in M'.[3] □

[3]Note also that the exactness of a sequence of R-modules does not depend on the R-module structure but only on the underlying commutative group structure. Thus if we have a sequence of commutative groups which can be viewed as a sequence of R-modules and also as a sequence of R'-modules, then exactness as R-modules is equivalent to exactness as R'-modules.

COROLLARY 7.11. *Let N and P be submodules of an R-module M. Then:*

a) $S^{-1}(N+P) = S^{-1}N + S^{-1}P$.

b) $S^{-1}(N \cap P) = S^{-1}N \cap S^{-1}P$.

c) $S^{-1}(M/N) \cong_{S^{-1}R} S^{-1}M/S^{-1}N$.

EXERCISE 7.17. *Prove Corollary 7.11.*

PROPOSITION 7.12. *Let M and N be R-modules and S a multiplicatively closed subset of R. Then the mapping*

$$\frac{m}{s} \otimes \frac{n}{t} \mapsto \frac{m \otimes n}{st}$$

induces an isomorphism of $S^{-1}(R)$-modules

$$S^{-1}M \otimes_{S^{-1}R} S^{-1}N \xrightarrow{\sim} S^{-1}(M \otimes_R N).$$

In particular, for any prime ideal $\mathfrak{p}$ of R, we have

$$M_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} N_{\mathfrak{p}} \xrightarrow{\sim} (M \otimes_R N)_{\mathfrak{p}}.$$

EXERCISE 7.18. *Prove Proposition 7.12.*

EXERCISE 7.19. *Let R be a ring, $S \subseteq R$ multiplicative, and M an R-module.*

a) *If M is finitely generated, then $S^{-1}M$ is a finitely generated $S^{-1}R$-module.*

b) *If M is finitely presented, then $S^{-1}M$ is a finitely presented $S^{-1}R$-module.*[4]

Recall that if M_1 and M_2 are R-submodules of an R-module M, then

$$(M_1 : M_2) = \{x \in R \mid xM_2 \subseteq M_1\}$$

and thus

$$(M_1 : M_2) = \operatorname{ann}((M_1 + M_2)/M_1)).$$

PROPOSITION 7.13. *Let $S \subseteq R$ be a multiplicatively closed subset.*

a) *Let M be a finitely generated R-module. Then*

$$S^{-1} \operatorname{ann} M = \operatorname{ann} S^{-1}M.$$

b) *If M_1, M_2 are submodules of an R-module M and M_2 is finitely generated, then*

$$S^{-1}(M_1 : M_2) = (S^{-1}M_1 : S^{-1}M_2).$$

PROOF. a) We go by induction on the number n of generators of M.
Base Case: If $n = 1$ then $M \cong R/I$ for some ideal I, so

$$S^{-1} \operatorname{ann} M = S^{-1}I = \operatorname{ann} S^{-1}R/S^{-1}I = \operatorname{ann} S^{-1}M.$$

Induction Step: Suppose $n \geqslant 2$ and that the result holds for all modules that can be generated by n elements. Write $M = M_1 + M_2$ with M_1 generated by n elements and M_2 generated by 1 element. Then

$$S^{-1} \operatorname{ann} M = S^{-1} \operatorname{ann}(M_1 + M_2) = S^{-1}(\operatorname{ann} M_1 \cap \operatorname{ann} M_2) = S^{-1} \operatorname{ann} M_1 \cap S^{-1} \operatorname{ann} M_2$$
$$= \operatorname{ann} S^{-1}M_1 \cap \operatorname{ann} S^{-1}M_2 = \operatorname{ann} S^{-1}M_1 + S^{-1}M_2 = \operatorname{ann} S^{-1}M.$$

b) Put $M \coloneqq (M_1 + M_2)/M_1$. Then M is a quotient of M_2 hence finitely generated, so by part a) we have

$$S^{-1}(M_1 : M_2) = S^{-1} \operatorname{ann}(M_1 + M_2)/M_1 = \operatorname{ann} S^{-1}(M_1 + M_2)/M_1$$

[4]Actually both parts hold for any base change $R \to R'$! We record it in this form since it will be used later.

$$= \operatorname{ann}(S^{-1}(M_1 + M_2)/S^{-1}M_1) = (S^{-1}M_1 : S^{-1}M_2). \qquad \square$$

7. Local properties

We say that a property P of a ring R is **localizable** if whenever R satisfies property P, so does $R_\mathfrak{p}$ for every prime ideal $\mathfrak{p}$ of R. We say that a property P is **local-to-global** if whenever $R_\mathfrak{p}$ has property P for all prime ideals $\mathfrak{p}$ of R, then R has that property. Finally, we say a property is **local** if it is both localizable and local-to-global. There are similar definitions for properties of R-modules.

EXERCISE 7.20.

a) *Show the following properties of rings are localizable: being a field, having characteristic* 0*, having prime characteristic* p*, being a domain, being reduced.*

b) *Show that the following properties of modules are localizable: freeness, projectivity, flatness, cyclicity, finite generation, finite presentation.*

For a property P of rings, we say that a ring R is **locally P** if for all $\mathfrak{p} \in \operatorname{Spec} R$, $R_\mathfrak{p}$ has the property P. Similarly, if Q is a property of modules, we say that an R-module M is **locally P** if for all $\mathfrak{p} \in \operatorname{Spec} R$, $M_\mathfrak{p}$ has property Q.

Warning: It would also be reasonable to define "locally P" to mean that for all $\mathfrak{p} \in \operatorname{Spec} R$, there is $f \in R \backslash \mathfrak{p}$ such that R_f (or M_f) has property P. In the case of rings, as we shall see later this latter definition means that $\operatorname{Spec} R$ has property P locally with respect to the Zariski topology. We will consider this property as well, but we call it **Z-locally P** instead.

EXERCISE 7.21. *Let P be a property of rings (or modules). Show: "locally P" is a local property.*

One of the most important themes in commutative algebra is the recognition of the importance of local properties for rings and modules.

Remark: Very often it is true that if P is a local property, then R has property P if and only if $R_\mathfrak{m}$ has property P for all maximal ideals $\mathfrak{m}$ of R. We will not introduce terminology for this, but watch for it in the upcoming results.

First of all, for an R-module, **being zero** is a local property.

PROPOSITION 7.14. *For an R-module M, the following are equivalent:*

(i) $M = 0$.
(ii) $M_\mathfrak{p} = 0$ *for all primes* $\mathfrak{p}$ *of* R.
(iii) $M_\mathfrak{m} = 0$ *for all maximal ideals* $\mathfrak{m}$ *of* R.

PROOF. Clearly (i) $\implies$ (ii) $\implies$ (iii), so asume that $M_\mathfrak{m} = 0$ for all maximal ideals $\mathfrak{m}$ of R. Suppose there exists $0 \neq x \in M$, and let I be the annihilator of x, so that I is a proper ideal of R and thus contained in some maximal ideal $\mathfrak{m}$. Then x is not killed by any element of the multiplicative subset $R \backslash \mathfrak{m}$ and therefore maps to a nonzero element of $M_\mathfrak{m}$: contradiction. $\square$

EXERCISE 7.22. *Let M be an R-module, and let N_1, N_2 be R-submodules of M.*

a) *Show: the following are equivalent:*

(i) *We have* $N_1 \subseteq N_2$.
(ii) *For all* $\mathfrak{p} \in \operatorname{Spec} R$, *we have* $(N_1)_{\mathfrak{p}} \subseteq (N_2)_{\mathfrak{p}}$.
(iii) *For all* $\mathfrak{m} \in \operatorname{MaxSpec} R$, *we have* $(N_1)_{\mathfrak{m}} \subseteq (N_2)_{\mathfrak{m}}$.
(Hint: $N_1 \subseteq N_2$ *if and only if* $(N_1 + N_2)/N_2 = 0$.*)*

b) *Show: the following are equivalent:*
(i) *We have* $N_1 = N_2$.
(ii) *For all* $\mathfrak{p} \in \operatorname{Spec} R$, *we have* $(N_1)_{\mathfrak{p}} = (N_2)_{\mathfrak{p}}$.
(iii) *For all* $\mathfrak{m} \in \operatorname{MaxSpec} R$, *we have* $(N_1)_{\mathfrak{m}} = (N_2)_{\mathfrak{m}}$.

PROPOSITION 7.15. *Let* $f : M \to N$ *be an* R*-module homomorphism.*

a) *The following are equivalent:*
(i) f *is injective.*
(ii) *For all prime ideals* $\mathfrak{p}$ *of* R, $f_{\mathfrak{p}} : M_{\mathfrak{p}} \to N_{\mathfrak{p}}$ *is injective.*
(iii) *For all maximal ideals* $\mathfrak{m}$ *of* R, $f_{\mathfrak{m}} : M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ *is injective.*

b) *Part a) holds with "injective" replaced everywhere by "surjective", and thus also if "injective" is replaced everywhere by "is an isomorphism."*

PROOF. a) (i) $\implies$ (ii) by the exactness of localization, and obviously (ii) $\implies$ (iii). Assume (iii), and let $M' = \operatorname{Ker}(f)$. Then $0 \to M' \to M \to N$ is exact, hence for all $\mathfrak{m}$ we have $0 \to M'_{\mathfrak{m}} \to M_{\mathfrak{m}} \to N_{\mathfrak{m}}$ is exact. So, by our assumption, $M'_{\mathfrak{m}} = 0$ for all maximal ideals $\mathfrak{m}$, and thus by Proposition 7.14 we have $M' = 0$. The proof of part b) is virtually identical and left to the reader. □

Warning: Proposition 7.15 **does not say**: if M and N are R-modules such that $M_{\mathfrak{p}} \cong N_{\mathfrak{p}}$ as $R_{\mathfrak{p}}$ modules for all $\mathfrak{p} \in \operatorname{Spec} R$, then $M \cong N$. This is being asserted only when there is a map $f : M \to N$ inducing all the isomorphisms between localized modules.

EXERCISE 7.23. *Exhibit finitely generated* R*-modules* M *and* N *which are "locally isomorphic" – i.e.,* $M_{\mathfrak{p}} \cong N_{\mathfrak{p}}$ *for all* $\mathfrak{p} \in \operatorname{Spec} R$ *– but are not isomorphic.*[5]

COROLLARY 7.16. *Let* R *be a domain with fraction field* K. *Then we have*

$$\bigcap_{\mathfrak{m} \in \operatorname{MaxSpec} R} R_{\mathfrak{m}} = R.$$

PROOF. Certainly $R \hookrightarrow \bigcap_{\mathfrak{m} \in \operatorname{MaxSpec} R} R_{\mathfrak{m}}$. Conversely, if $x \in K \backslash R$ then

$$I := (R : Rx)$$

is a proper ideal, hence contained in some maximal ideal $\mathfrak{m}$. Because Rx is a finitely generated R-module, by Proposition 7.13 we have

$$(R_{\mathfrak{m}} : R_{\mathfrak{m}} x) = I_{\mathfrak{m}} \subsetneq R_{\mathfrak{m}}.$$

Thus $x \notin R_{\mathfrak{m}}$. □

Let R be a domain with fraction field K, and let V be a finite-dimensional K-vector space. An **R-lattice in V** is a finitely generated R-submodule Λ of V such that $\langle \Lambda \rangle_K = V$. Since K is a torsionfree R-module, every R-lattice in K is a finitely generated, torsionfree R-module. Convesrsely, if Λ is a finitely generated torsionfree R-module, let $V := \Lambda \otimes_R K$. Then by Exercise 3.46 the natural R-module map $\Lambda \hookrightarrow \Lambda \otimes_R K$ is injective and makes Λ into an R-lattice in the finite-dimensional

[5]In mantra form: "being isomorphic" is not a local property, but "being an isomorphism" is.

K-vector space $\Lambda \otimes_R K$. Such lattices are ubiquitous in algebra and number theory.

Corollary 7.16 extends to a **local-global principle for lattices**.

THEOREM 7.17. *Let R be a domain with fraction field K, let V be a finite-dimensional K-vector space, and let Λ be a finitely generated R-submodule of K. Then, inside V we have*

$$\bigcap_{\mathfrak{m} \in \operatorname{MaxSpec} R} \Lambda_{\mathfrak{m}} = \Lambda.$$

PROOF. Put $L := \bigcap_{\mathfrak{m} \in \operatorname{MaxSpec} R} \Lambda_{\mathfrak{m}}$. Clearly $\Lambda \hookrightarrow L$. Seeking a contradiction, suppose there is $x \in L \backslash \Lambda$, and put $\tilde{\Lambda} = \langle \Lambda, x \rangle$. Then

$$I := (\Lambda : \tilde{\Lambda})$$

is a proper ideal of R, hence contained in a maximal ideal $\mathfrak{m}$. Since Λ is finitely generated, so is $\tilde{\Lambda}$, so by Proposition 7.13 we have

$$(\Lambda_{\mathfrak{m}} : \tilde{\Lambda}_{\mathfrak{m}}) = I_{\mathfrak{m}} \subsetneq R_{\mathfrak{m}}.$$

It follows that $\tilde{\Lambda}_{\mathfrak{m}} = \langle \Lambda, x \rangle_{R_{\mathfrak{m}}} \supsetneq \Lambda_{\mathfrak{m}}$ so $x \notin \Lambda_{\mathfrak{m}}$, hence $x \notin L$: contradiction. □

We give an application in the theory of stably free modules.

PROPOSITION 7.18. *A stably free module of rank one is free.*

PROOF. The natural proof uses exterior products of modules, which we have unfortunately not defined in these notes. For the basics here see BOURBAKI or [**Ei**, Appendix A2]. Especially, all the properties of exterior powers that we use appear in [**Ei**, Prop. A2.2].

Now suppose P is such that $P \oplus R^{n-1} \cong R^n$. Taking top exterior powers we get

$$R \cong \bigwedge^n R^n \cong \bigwedge^n (P \oplus R^{n-1}) \cong \bigoplus_{i+j=n} \bigwedge^i P \otimes \bigwedge^j R^{n-1}$$

$$\cong M \oplus \left(\bigwedge^2 M \otimes \bigwedge^{n-2} R^{n-1} \right) \oplus \dots.$$

For any $\mathfrak{p} \in \operatorname{Spec} R$, $M_{\mathfrak{p}}$ is free of rank one over $R_{\mathfrak{p}}$. Thus $\bigwedge^i M_{\mathfrak{p}} = (\bigwedge^i M)_{\mathfrak{p}} = 0$ for all $i \geqslant 2$. By Proposition 7.14, $\bigwedge^i M = 0$ for all $i \geqslant 2$, so $R \cong M$. □

One of the most important local properties of an R-module M is the condition of being **locally free**: for all $\mathfrak{p} \in \operatorname{Spec} M$, $M_{\mathfrak{p}}$ is free. We had better repeat the previous warning in this special case: some people say that M is locally free if and only if for all $\mathfrak{p} \in \operatorname{Spec} R$ there is $f \in R \backslash \mathfrak{p}$ such that M_f is free. This is in general a stronger property, which we call **Z-locally free**.

In light of the fact the being projective is a localizable property, Theorem 3.76 can be rephrased as follows.

THEOREM 7.19. *(Kaplansky) A projective module is locally free.*

From our study of vector bundles it is natural to wonder about the converse: must a finitely generated locally free module be projective? In complete generality the answer is negative (we will meet counterexamples later on), but morally it is right: cf. Theorem 7.30.

7.1. Rank Functions.

Let M be a finitely generated module. There is an associated **rank function** $\text{rank}_M : \text{Spec}\, R \to \mathbb{N}$, given by

$$\text{rank}_M(\mathfrak{p}) = \dim_{k(\mathfrak{p})} M \otimes k(\mathfrak{p}).$$

Here $k(\mathfrak{p})$ is the fraction field of the domain $R/\mathfrak{p}$, and since M is a finitely generated R-module, $M \otimes k(\mathfrak{p})$ is a finite-dimensional $k(\mathfrak{p})$-vector space.

EXERCISE 7.24.

a) *Show: for finitely generated R-modules M and N, we have*

$$\text{rank}_{M\oplus N} = \text{rank}_M + \text{rank}_N$$

and

$$\text{rank}_{M\otimes_R N} = \text{rank}_M \cdot \text{rank}_N .$$

b) *Compute the rank function on the $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$.*

c) *Compute the rank function on any finitely generated module over a PID.*

EXERCISE 7.25. *Let M be a finitely generated R-module.*

a) *Show: if M is locally free, then for all $\mathfrak{p} \in \text{Spec}\, R$, $M_\mathfrak{p} \cong R_\mathfrak{p}^{\text{rank}_M(\mathfrak{p})}$.*

b) *Suppose M is stably free of rank n: i.e., there are $m, n \in \mathbb{N}$ such that $M \oplus R^m \cong R^{m+n}$. Show: for all $\mathfrak{p} \in \text{Spec}\, R$, we have $\text{rank}_M(\mathfrak{p}) = n$.*

We will mostly be interested in the rank function on a finitely generated projective module. As in §6, we view a finitely generated projective module as being analogous to a vector bundle, and then the rank at $\mathfrak{p}$ plays the role of the dimension of the fiber at $\mathfrak{p}$. In the case of a vector bundle on a topological space X, the rank function is locally constant, hence constant if X is connected. Once we study the Zariski topology on $\text{Spec}\, R$ in earnest, we can and will prove the analogous statement: the rank function on a finitely generated projective module M is locally constant. Its failure to be constant is somehow the coarsest possible obstruction to M being free: if the rank function is not constant, then M cannot even be stably free: equivalently, its class in the reduced K-group $\widetilde{K_0(R)}$ is nontrivial.

Here is a (not so deep) criterion for a projective module to be free.

PROPOSITION 7.20. *Let M be a projective R-module of constant rank n. Then M is free if and only if M can be generated by n elements.*

PROOF. If M is free then $M \cong R^n$. Conversely, that M can be generated by n elements means there is a surjective R-module map $\varphi : R^n \to M$. Let $K = \ker \varphi$; since M is projective, we have

$$R^n \cong K \oplus M.$$

Thus K is also finitely generated projective, so for all $\mathfrak{p} \in \text{Spec}\, R$ we have

$$R_\mathfrak{p}^n \cong K_\mathfrak{p} \oplus M_\mathfrak{p}$$

with $K_\mathfrak{p} \cong R_\mathfrak{p}^{r(\mathfrak{p})}$ and $M_\mathfrak{p} \cong R_\mathfrak{p}^n$. It follows (by tensoring to $k(\mathfrak{p})$) that $K_\mathfrak{p} = 0$. Being zero is a local property, so $K = 0$ and $\varphi : R^n \to M$ is an isomorphism. □

We can now give a situation in which our coarsest possible obstruction to freeness is the only one.

LEMMA 7.21. *Let M be a finitely generated projective R-module, and let I be an ideal contained in the Jacobson radical. If M/IM is free, then so is M.*

PROOF. If $M/IM \cong (R/I)^n$, then by Nakayama's Lemma n is the least number of generators of M. Moreover, for all $\mathfrak{m} \in \operatorname{MaxSpec} R$, since the map $M \to M/\mathfrak{m}M$ factors through M/IM we have $\operatorname{rank}_M(\mathfrak{m}) = n$. Now observe that if $\mathfrak{p}_1 \subseteq \mathfrak{p}_2 \in \operatorname{Spec} R$, then

$$R_{\mathfrak{p}_1}^{\operatorname{rk}_M(\mathfrak{p}_1)} \cong M_{\mathfrak{p}_1} \cong M_{\mathfrak{p}_2} \otimes_{R_{\mathfrak{p}_2}} R_{\mathfrak{p}_1} \cong R_{\mathfrak{p}_2}^{\operatorname{rk}_M(\mathfrak{p}_2)} \otimes_{R_{\mathfrak{p}_2}} R_{\mathfrak{p}_1} \cong R_{\mathfrak{p}_1}^{\operatorname{rk}_M(\mathfrak{p}_2)},$$

so $\operatorname{rk}_M(\mathfrak{p}_1) = \operatorname{rk}_M(\mathfrak{p}_2)$. It follows that M has constant rank n and can be generated by n elements, so by Proposition 7.20 we have that M is free. □

EXERCISE 7.26. *Let $I \subseteq J(R)$ be an ideal of R. Let P_1, P_2 be two finitely generated projective R-modules. Show: if $P_1/IP_1 \cong_{R/I} P_2/IP_2$ then $P_1 \cong P_2$.*
(Hint: use the projectivity of P_1 to factor the map $P_1 \to P_1/IP_1 \xrightarrow{\sim} P_2/IP_2$ through P_2.)

COROLLARY 7.22. *Let R be a semilocal ring ($\operatorname{MaxSpec} R$ is finite). Let M be a finitely generated projective R-module. Then M is free if and only if it has constant rank.*

PROOF. We know that free modules have constant rank. Conversely, suppose M is projective of constant rank n, and let $\mathfrak{m}_1, \ldots, \mathfrak{m}_N$ be the distinct maximal ideals of R, so $J(R) = \bigcap_{i=1}^N \mathfrak{m}_i = \prod_{i=1}^N \mathfrak{m}_i$. By the Chinese Remainder Theorem for modules we have

$$M/J(R) \cong \prod_{i=1}^N M/\mathfrak{m}_i M.$$

Since M has constant rank n, we have $\dim_{R/\mathfrak{m}_i} M\mathfrak{m}_i M = n$ for all i, so $M/J(R)M$ is a free $R/J(R)$-module of rank n. Apply Lemma 7.21. □

The topological analogue of Corollary 7.22 is, roughly, that a vector bundle on a discrete space is trivial if and only if it has constant rank. (However that is a triviality whereas Corollary 7.22 is actually rather useful.)

7.2. Local nature of flatness.

PROPOSITION 7.23. *For an R-module M, the following are equivalent:*

(i) *M is flat.*
(ii) *For all prime ideals $\mathfrak{p}$ of R, the $R_{\mathfrak{p}}$-module $M_{\mathfrak{p}}$ is flat.*
(iii) *For all maximal ideals $\mathfrak{m}$ of R, the $R_{\mathfrak{m}}$-module $M_{\mathfrak{m}}$ is flat.*

PROOF. (i) $\implies$ (ii) is a special case of Proposition 7.10; (ii) $\implies$ (iii) is immediate. So assume (iii), and let $N \hookrightarrow P$ be any injective R-module homomorphism. Then, by exactness of localization, for all maximal ideals $\mathfrak{m}$ we have $N_{\mathfrak{m}} \hookrightarrow P_{\mathfrak{m}}$. Since $M_{\mathfrak{m}}$ is assumed to be flat, we have $(N \otimes_R M)_{\mathfrak{m}} = N_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} M_{\mathfrak{m}} \hookrightarrow P_{\mathfrak{m}} \otimes_{R_{\mathfrak{m}}} M_{\mathfrak{m}} = (P \otimes_R M)_{\mathfrak{m}}$. Applying Proposition 7.15 we conclude that $N \otimes_R M \to P \otimes_R P$ is injective, and therefore M is flat over R. □

COROLLARY 7.24. *Let R be a ring, $S \subseteq R$ a multiplicative subset. If M is a flat R-module, then $S^{-1}M$ is a flat $S^{-1}R$-module.*

PROOF. If M is flat, so is $M_{\mathfrak{p}}$ for each prime ideal $\mathfrak{p}$ of M, but since the primes of $S^{-1}R$ are a subset of the primes of R, this implies that $S^{-1}M$ is flat. □

When a property P of rings or modules is *not* local, it is often of interest to study also its "localized version": we say that an R-module M is **locally P** if for all prime ideals $\mathfrak{p}$ of R, $M_{\mathfrak{p}}$ has property $\mathfrak{p}$ (and similarly for rings).

7.3. Absolute flatness revisited.

LEMMA 7.25. *Suppose an absolutely flat ring R is either local or a domain. Then R is a field.*

PROOF. Suppose R is not a field, and let $x \in R$ be a nonzero, nonunit. Then $(0) \subsetneq (x) \subsetneq R$. Proposition 3.103 gives $R \cong (x) \oplus J$: contradiction. □

LEMMA 7.26. *Let R be a ring.*

a) *If R is absolutely flat and $S \subseteq R$ is any multiplicative subset, then $S^{-1}R$ is absolutely flat.*
b) *The ring R is absolutely flat if and only if $R_{\mathfrak{m}}$ is a field for all maximal ideals $\mathfrak{m}$ of R.*

PROOF. a) By Exercise 7.16 every $S^{-1}R$-module is of the form $S^{-1}R \otimes_R M$ for some R-module M. By hypothesis M is flat, so by Corollary 7.24, so is $S^{-1}M$. b) If R is absolutely flat, and $\mathfrak{m}$ is a maximal ideal of R, then by part a) $R_{\mathfrak{m}}$ is absolutely flat. On the other hand it is a local ring, so by Lemma 7.25, $R_{\mathfrak{m}}$ is a field. Conversely, assume that each $R_{\mathfrak{m}}$ is a field, and let M be an R-module. Then for all $\mathfrak{m} \in \operatorname{MaxSpec} R$, $M_{\mathfrak{m}}$ is a flat $R_{\mathfrak{m}}$-module, so M is a flat R-module. □

THEOREM 7.27. *For a ring R, the following are equivalent:*

(i) *The ring $R/\operatorname{nil} R$ is absolutely flat, i.e., every $R/\operatorname{nil} R$-module is flat.*
(ii) *Every prime ideal of R is maximal.*

‘

PROOF. Since the prime ideals of R are the same as those of $R/\operatorname{nil} R$, it is equivalent to prove the following simpler assertion: if R is reduced, it is absolutely flat if and only if every prime ideal of R is maximal. Suppose R is absolutely flat and $\mathfrak{p} \in \operatorname{Spec} R$. Then $R/\mathfrak{p}$ is an absolutely flat domain, hence a field by Lemma 7.25, hence $\mathfrak{p}$ is maximal. Let $\mathfrak{m}$ be a maximal ideal of R. Then $R_{\mathfrak{m}}$ is a reduced local ring, hence a field. By Lemma 7.26, R is absolutely flat. □

8. Local characterization of finitely generated projective modules

Let us call a family of $\{f_i\}_{i \in I}$ of elements of R a **Z-family** if $\langle f_i \rangle = 1$. Clearly for every Z-family there is a finite subset $J \subseteq I$ such that $\{f_i\}_{i \in J}$ is also a Z-family. (Later on, this trivial observation will be dressed up in rather fancy attire: this gives the quasi-compactness of the Zariski topology on $\operatorname{Spec} R$.)

A property P of rings or modules will be said to be **Z-local** if it holds over R if and only if it holds over all R_{f_i} for some Z-family $\{f_i\}$ of R.

PROPOSITION 7.28.
Let $u : M \to N$ be a homomorphism of R-modules, and let $\mathfrak{p} \in \operatorname{Spec} R$.

a) *If N is finitely generated and $u_{\mathfrak{p}}$ is surjective, there exists $f \in R \backslash \mathfrak{p}$ such that $u_f : M_f \to N_f$ is surjective.*
b) *The surjectivity of u is a Z-local property.*

c) *If M is finitely generated, N is finitely presented and $u_{\mathfrak{p}}$ is an isomorphism, then there exists $f \in R\backslash\mathfrak{p}$ such that $u_f : M_f \to N_f$ is an isomorphism.*
d) *If M is finitely generated and N is finitely presented, then the bijectivity of u is a Z-local property.*

PROOF. Write out the exact sequence

$$0 \to \ker u \to M \xrightarrow{u} N \to \operatorname{coker} u \to 0.$$

By the flatness of localization, this sequence remains exact upon being tensored with R_f for any $f \in R$ or with $R_{\mathfrak{p}}$ for any $\mathfrak{p} \in R$. It follows that passage to the kernel and cokernel commutes with localization.
a) We're assuming $0 = \operatorname{coker}(u_{\mathfrak{p}}) = (\operatorname{coker} u)_{\mathfrak{p}}$, i.e., for each $x \in \operatorname{coker} u$ there exists $f_x \in R\backslash\mathfrak{p}$ such that $f_x x = 0$. Since $\operatorname{coker} u$ is a quotient of the finitely generated module N, it is finitely generated, say by $x_1, \ldots, x_n$. Then $f = f_{x_1} \cdots f_{x_n} \in R\backslash\mathfrak{p}$ is such that $f \operatorname{coker} u = 0$, so $0 = (\operatorname{coker} u)_f = \operatorname{coker}(u_f)$ and u_f is surjective.
b) It is clear that if u is surjective, then for any $f \in R$, u_f is surjective. Conversely, let $\{f_i\}_{i\in I}$ be a Z-family such that u_{f_i} is surjective for all i. Then for any $\mathfrak{p} \in \operatorname{Spec} R$ there exists $i \in I$ such that $f_i \in R\backslash\mathfrak{p}$, so that $u_{\mathfrak{p}}$ is a further localization of u_{f_i} and thus the surjectivity of u_{f_i} implies that of $u_{\mathfrak{p}}$. By Proposition 7.15, u is surjective.
c) By part a), there exists $f_1 \in R\backslash\mathfrak{p}$ such that $\operatorname{coker} u_{f_1} = 0$, and thus we have an exact sequence

$$0 \to (\ker u)_{f_1} \to M_{f_1} \to N_{f_1} \to 0.$$

Since N is finitely presented over R, N_{f_1} is finitely presented over R_{f_1} and thus $(\ker u)_{f_1}$ is finitely generated. Arguing as in part b), we get $f_2 \in R\backslash\mathfrak{p}$ such that $f_1 f_2 \ker u = 0$. Taking $f = f_1 f_2$ we get $u_f : M_f \xrightarrow{\sim} N_f$.
d) This is proved analogously to part b) and is left to the reader. □

COROLLARY 7.29. *For a finitely presented R-module M, the following are equivalent:*

(i) *There is a Z-family $\{f_i\}_{i\in I}$ of R such that for all $i \in I$, M_{f_i} is a free R_{f_i}-module.*
(ii) *M is locally free: for all $\mathfrak{p} \in \operatorname{Spec} R$, $M_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$-module.*
(ii′) *For every $\mathfrak{m} \in \operatorname{MaxSpec} R$, $M_{\mathfrak{m}}$ is a free $R_{\mathfrak{m}}$-module.*

PROOF. (i) $\implies$ (ii): For each prime ideal $\mathfrak{p}$ there exists at least one i such that $f_i \notin \mathfrak{p}$; equivalently, the multiplicative subset generated by f_i is contained in $R\backslash\mathfrak{p}$. Thus $M_{\mathfrak{p}} = M_{f_i} \otimes_{R_{f_i}} R_{\mathfrak{p}}$ and since M_{f_i} is free, so is $M_{\mathfrak{p}}$.
(ii) $\implies$ (i): It is enough to find for each prime ideal $\mathfrak{p}$ an element $f_{\mathfrak{p}} \in R\backslash\mathfrak{p}$ such that $M_{f_{\mathfrak{p}}}$ is free: for if so, then $\{f_{\mathfrak{p}}\}_{\mathfrak{p}\in\operatorname{Spec} R}$ is a Z-family. Choose $x_1, \ldots, x_n \in M$ whose images in $M_{\mathfrak{p}}$ give an $R_{\mathfrak{p}}$-basis, and define $u : R^n \to M$ via $e_i \mapsto x_i$. Then $u_{\mathfrak{p}}$ is an isomorphism, so by Proposition 7.28c) we may choose $f_{\mathfrak{p}} \in R\backslash\mathfrak{p}$ such that $u_{f_{\mathfrak{p}}}$ is an isomorphism and thus $M_{f_{\mathfrak{p}}}$ is free.
(ii) $\iff$ (ii′): Since freeness is localizable, this follows from Exercise 7.22. □

REMARK 6. *(M. Brandenburg) The proof of (ii) $\implies$ (i) shows something a bit stronger: if M is a finitely presented module over a ring R and for some $\mathfrak{p} \in \operatorname{Spec} R$ we have that $M_{\mathfrak{p}}$ is free, then there is $f_{\mathfrak{p}} \in R$ such that $M_{f_{\mathfrak{p}}}$ is free.*

EXERCISE 7.27. *For $1 \leqslant i \leqslant n$, let M_i be a finitely generated proejctive R_i-module. Show: $\prod_{i=1}^n M_i$ is a finitely generated projective $\prod_{i=1}^n R_i$-module.*

We can now prove one of the major results of this text.

THEOREM 7.30. *For an R-module M, the following are equivalent:*

(i) *M is finitely generated and projective.*
(ii) *M is finitely* presented *and locally free.*
(iii) *For every maximal ideal $\mathfrak{m}$ of R, there exists $f \in R\backslash\mathfrak{m}$ such that M_f is a locally free R_f-module of finite rank.*
(iv) *There is a finite Z-family $\{f_1, \ldots, f_n\}$ of R such that $\langle f_1, \ldots, f_n\rangle = R$ and for all i, M_{f_i} is a finitely generated free R_{f_i}-module.*

PROOF. (i) $\implies$ (ii): Let M be finitely generated and projective. There exists a finitely generated free module F and a surjection $q : F \to M$. Since M is projective, q splits and $\mathrm{Ker}(q)$ is not just a submodule of F but also a quotient and thus finitely generated. So M is finitely presented. Since projectivity is preserved by base change and any finitely generated projective module over a local ring is free (Theorem 3.16), for all maximal ideals $\mathfrak{m}$ of R, $M_\mathfrak{m}$ is free.
(ii) $\implies$ (iii): this follows immediately from Corollary 7.29.
(iii) $\implies$ (iv): For each $\mathfrak{m} \in \operatorname{MaxSpec} R$, choose $f_\mathfrak{m} \in R\backslash\mathfrak{m}$ such that $M_{f_\mathfrak{m}}$ is a finitely generated free $R_{f_\mathfrak{m}}$-module. Then $\{f_\mathfrak{m}\}_{\mathfrak{m}\in\operatorname{MaxSpec} R}$ is a Z-family of R, and as remarked above, every Z-family contains a finite subfamily.
(iv) $\implies$ (i): Put $S = \prod_{i=1}^n R_{f_i}$ and let $f : R \to S$ be the natural map.
Step 1: First note that

$$\ker f = \bigcap_{i=1}^n \ker(R \to R_{f_i}) = \bigcap_{i=1}^n \operatorname{ann}(f_i) = f \operatorname{ann}\langle f_1, \ldots, f_n\rangle = \operatorname{ann} R = 0,$$

so f is injective, and thus S is an extension ring of R.
Step 2: We CLAIM $f : R \hookrightarrow S$ is a faithfully flat extension. Since localizations are flat and direct sums of flat algebras are flat, S/R is a flat extension. So by Theorem 3.111, it is enough to show that $f^* : \operatorname{Spec} S \to \operatorname{Spec} R$ is surjective. But $\operatorname{Spec} S = \coprod_{i=1}^n \operatorname{Spec} R_{f_i}$ and $f^*(\operatorname{Spec} R_{f_i})$ is the subset of $\mathfrak{p} \in \operatorname{Spec} R$ such that $f_i \notin \mathfrak{p}$. Since $\{f_1, \ldots, f_n\}$ forms a Z-family, no proper ideal can contain all the f_i's, and therefore $\mathfrak{p}$ lies in at least one $f^*(\operatorname{Spec} R_{f_i})$.
Step 3: We have a faithfully flat ring extension $f : R \hookrightarrow S$ and an R-module M such that $M \otimes_R S = \prod_{i=1}^n M_{f_i}$ is a finitely generated projective $S = \prod_{i=1}^n R_{f_i}$-module (Exercise 7.27). By Theorem 3.114, M is finitely generated and projective! □

COROLLARY 7.31. *Every finitely presented flat R-module is projective.*

PROOF. Let M be a finitely presented, flat R-module. For each maximal ideal $\mathfrak{m}$ of R, $M_\mathfrak{m}$ is a finitely presented flat module over the local ring $R_\mathfrak{m}$, hence is free by Theorem 3.54. Therefore by criterion (iii) of Theorem 7.30, M is projective. □

COROLLARY 7.32. *Let R be a Noetherian ring, and let M be a finitely generated R-module. The following are equivalent:*

(i) *M is projective.*
(ii) *M is locally free.*
(iii) *M is flat.*

EXERCISE 7.28. *Prove Corollary 7.32.*

THEOREM 7.33. *For an R-module A, the following are equivalent:*

(i) *A is finitely generated projective.*

(ii) *For all R-modules B, the natural map*

$$\Phi : A^\vee \otimes_R B \to \mathrm{Hom}_R(A, B)$$

induced by $(f, b) \mapsto (a \mapsto f(a)b)$ is an isomorphism.

(iii) *The map $\Phi : A^\vee \otimes_R A \to \mathrm{Hom}_R(A, A)$ is an isomorphism.*

PROOF. (i) $\implies$ (ii): It is enough to show that for all $\mathfrak{p} \in \mathrm{Spec}\, R$, $\Phi_{\mathfrak{p}}$ is an isomorphism. Since A is finitely generated projective, it is finitely presented; moreover $R_{\mathfrak{p}}$ is a flat R-module, so by Theorem 3.106 we have a canonical isomorphism $\mathrm{Hom}_R(A, N) \otimes_R R_{\mathfrak{p}} = \mathrm{Hom}_{R_{\mathfrak{p}}}(A_{\mathfrak{p}}, N_{\mathfrak{p}})$. Also tensor products commute with base change, so it is enough to show

$$\Phi_{\mathfrak{p}} : A_{\mathfrak{p}}^\vee \otimes_{R_{\mathfrak{p}}} B_{\mathfrak{p}} \to \mathrm{Hom}_{R_{\mathfrak{p}}}(A_{\mathfrak{p}}, B_{\mathfrak{p}})$$

is an isomorphism. Since A is finitely generated projective, $A_{\mathfrak{p}}$ is finitely generated and free. We are thus essentially reduced to a familiar fact from linear algebra, namely the canonical isomorphism $V^\vee \otimes W \xrightarrow{\sim} \mathrm{Hom}(V, W)$ for vector spaces over a field, with V finite-dimensional. We leave the details to the reader as an exercise.
(ii) $\implies$ (iii): This is immediate.
(iii) $\implies$ (i): Let $\Phi^{-1}(1_A) = \sum_{i=1}^m f_i \otimes a_i$. Then we have that for all $a \in A$, $a = \sum_{i=1}^m f_i(a)a_i$. By the Dual Basis Lemma, A is finitely generated projective. □

We end by showing that without the Noetherian hypothesis, a finitely generated locally free module need not be projective.

PROPOSITION 7.34. *For a ring R, the following are equivalent:*

(i) *R is absolutely flat.*

(ii) *Every R-module is locally free.*

PROOF. (i) $\implies$ (ii): By Lemma 7.26, for $\mathfrak{m} \in \mathrm{MaxSpec}\, R$, $R_{\mathfrak{m}}$ is a field, so every $R_{\mathfrak{m}}$-module is free. By Theorem 7.27 every prime ideal of R is maximal, so every R-module is locally free.
(ii) $\implies$ (i): Applying Lemma 7.26 again, if R is *not* absolutely flat, there is $\mathfrak{m} \in \mathrm{MaxSpec}\, R$ such that $R_{\mathfrak{m}}$ is not a field, and thus there exists a nonfree $R_{\mathfrak{m}}$-module $M_{\mathfrak{m}}$. By Exercise 7.16 there is an R-module M such that $M \otimes_R R_{\mathfrak{m}} \cong M_{\mathfrak{m}}$ and thus M is not locally free. □

EXERCISE 7.29. *(G. Elencwajg) Let R be a ring, and let I be an ideal of R.*

a) *Show: if R/I is a projective R-module, then I is principal.*

b) *Suppose that R is absolutely flat and not Noetherian (e.g. an infinite product of fields) and that I is infinitely generated. Show: the R-module R/I is finitely generated, flat,* not *projective, locally free and* not *Z-locally free.*

CHAPTER 8

Noetherian rings

We have already encountered the notion of a Noetherian ring, i.e., a ring in which each ideal is finitely generated; or equivalently, a ring which satisfies the ascending chain condition (ACC) on ideals. Our results so far have given little clue as to the importance of this notion. But in fact, as Emmy Noether showed, consideration of rings satisfying (ACC) is a major unifying force in commutative algebra.

In this section we begin to see why this is the case. After giving an introductory examination of chain conditions on rings and modules, we are able to make the key definitions of *height* of a prime ideal and *dimension* of a ring. We begin by giving a reasonably complete analysis of the structure theory of Artinian rings, which, as we will show, really is our first order of business in attempting the systematic study of Noetherian rings, since according to the Akizuki-Hopkins theorem the Artinian rings are precisely the Noetherian rings of dimension zero. We are then able to state and prove three of the most important and useful theorems in the entire subject. Whereas the first theorem, the Hilbert basis theorem, gives us a large supply of Noetherian rings, the latter two theorems, Krull's intersection theorem and Krull's principal ideal theorem, are basic results about the structure theory of Noetherian rings.

1. Chain conditions on partially ordered sets

PROPOSITION 8.1.
For a partially ordered set $(S, \leqslant)$, the following are equivalent:

(i) *The set S satisfies the **Ascending Chain Condition** (ACC): there is no infinite sequence $\{x_i\}_{n=1}^{\infty}$ of elements of S with $x_n < x_{n+1}$ for all $n \in \mathbb{Z}^+$.*
(ii) *Every nonempty subset $T \subseteq S$ has a maximal element.*

*A partially ordered set satisfying these equivalent conditions is called **Noetherian**.*

PROOF. (i) $\implies$ (ii): Let T be a nonempty subset of S without a maximal element. Since T is nonempty, choose $x_1 \in T$. Since T has no maximal elements, choose $x_2 > x_1$. Since T has no maximal elements, choose $x_3 > x_2$. And so on: we get an infinite strictly ascending chain in S.
(ii) $\implies$ (i): Indeed, an infinite strictly ascending chain is a nonempty subset without a maximal element. □

Similarly, we say that a partially ordered set satisfies the **Descending Chain Condition** (DCC) –if there is no infinite sequence $\{y_j\}_{j=1}^{\infty}$ of elements of S such that $y_j > y_{j+1}$ for all $j \in \mathbb{Z}^+$. As above, this holds if and only if every nonempty subset of S has a minimal element, and a partially ordered set satisfying these equivalent conditions is called **Artinian**.

Every partially ordered set $(S, \leqslant)$ has an **order dual** $S^\vee$: the underlying set is S, and we put $x \leqslant_\vee y \iff y \leqslant x$. Clearly S is Noetherian (resp. Artinian) if and only if $S^\vee$ is Artinian (resp. Noetherian). Thus at this level of abstraction we really have one notion here, not two. Nevertheless in our applications to rings and modules the two conditions remain quite distinct.

Examples: If S is finite it satisfies both ACC and DCC. With the usual orderings, the positive integers $\mathbb{Z}^+$ satisfy DCC but not ACC, the negative integers $\mathbb{Z}^-$ (or equivalently, $\mathbb{Z}^+$ with the opposite ordering) satisfy ACC but not DCC, and the integers $\mathbb{Z}$ satisfy neither.

EXERCISE 8.1. *Let S be a partially ordered set.*

a) *Show that S satisfies (ACC) (resp. (DCC)) if and only if there is no order embedding $\mathbb{Z}^+ \hookrightarrow S$ (resp. $\mathbb{Z}^- \hookrightarrow S$).*

b) *Suppose S is totally ordered. Show that S satisfies (DCC) if and only if it is well-ordered: i.e., every nonempty subset has a minimal element.*

2. Chain conditions on modules

Let R be a ring, and M a (left) R-module. It makes sense to speak of the (ACC) and (DCC) for R-submodules of M. Indeed, we will call M a **Noetherian module** if it satisfies (ACC) and an **Artinian module** if it satisfies (DCC).

EXERCISE 8.2. *Show: an R-module M is Noetherian if and only if every R-submodule M' of M is finitely generated.*

EXAMPLE 8.2. *As a $\mathbb{Z}$-module, the integers $\mathbb{Z}$ are Noetherian but not Artinian.*

EXAMPLE 8.3. *As a $\mathbb{Z}$-module, the group of all p-power roots of unity in the complex numbers – in other words, $\lim_{n\to\infty} \mu_{p^n}$ – is Artinian but not Noetherian.*

Every ring R is naturally an R-module, and the R-submodules of R are precisely the ideals. Thus it makes sense to say whether R is a Noetherian or Artinian R-module, and – thank goodness – this is visibly consistent with the previous terminology.

EXERCISE 8.3. *Let $M' \subseteq M$ be R-modules, and $\varphi : M \to M/M'$ be the quotient map. If N_1 and N_2 are submodules of M such that $N_1 \subseteq N_2$, $N_1 \cap M' = N_2 \cap M'$ and $\varphi(N_1) = \varphi(N_2)$, show that $N_1 = N_2$.*

THEOREM 8.4. *Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules. Then M is Noetherian (resp. Artinian) if and only if both M' and M'' are Noetherian (resp. Artinian).*

PROOF. We do the Noetherian case, leaving the similar Artinian case as an exercise for the reader. First, since an infinite ascending chain in a submodule or quotient module of M gives rise to an infinite ascending chain in M, if M is Noetherian, both M' and M'' are. Conversely, suppose $N_1 \subsetneq N_2 \subsetneq \dots$ is an infinite ascending chain of submodules of M. Consider the chain $(N_i + M')/M'$ in $M'' = M/M'$. By hypothesis, this chain eventually stabilizes, i.e., for sufficiently large i and j, $N_i + M' = N_j + M'$. Similarly, by intersecting with M' we get that for sufficiently large i and j $N_i \cap M' = N_j \cap M'$. Applying Exercise 8.3 we conclude $N_i = N_j$ for all sufficiently large i, j. □

A ring R is **Noetherian** if R is a Noetherian R-module. A ring R is **Artinian** if R is an Artinian R-module.

EXERCISE 8.4. *Let R be a ring.*

a) *Show: R is Noetherian if and only if every finitely generated R-module is Noetherian.*
b) *Show: R is Artinian if and only if every finitely generated R-module is Artinian.*
c) *Exhibit a ring R that is Noetherian but not Artinian.*
d) *Can you find a ring R which is Artinian but not Noetherian?*[1]

3. Semisimple modules and rings

In this section we allow *not necessarily commutative rings* R. By a "module over R" we mean a *left* R-module unless otherwise indicated.

A module M is **simple** if it is nonzero and has no proper, nonzero submodules.

This definition is of course made in analogy to that of a *simple group*, namely a nontrivial group possessing no nontrivial proper normal subgroups. And indeed many of the results in this and subsequent sections were first proved in the context of groups. It is even possible to work in a single context that simultaneously generalizes the case of groups and modules (over a not necessarily commutative ring), the key concept being that of **groups with operators**. For more on this perspective we invite the reader to consult any sufficiently thick all-purpose graduate level algebra text, the gold standard here being [**J1**], [**J2**].

EXERCISE 8.5. *(**Schur's Lemma**): Let M be a simple R-module. Show: $\mathrm{End}_R(M)$ is a division ring.*

THEOREM 8.5. *For an R-module M, the following are equivalent:*

(i) *M is a direct sum of simple submodules.*
(ii) *Every submodule of M is a direct summand.*
(iii) *M is a sum of simple submodules.*

*A modules satisfying these equivalent conditions is called **semisimple**.*

PROOF. (i) $\implies$ (ii): Suppose $M = \bigoplus_{i \in I} S_i$, with each S_i a simple submodule. For each $J \subseteq I$, put $M_J = \bigoplus_{i \in J} S_i$. Now let N be an R-submodule of M. An easy Zorn's Lemma argument gives us a maximal subset $J \subseteq I$ such that $N \cap M_J = 0$. For $i \notin J$ we have $(M_J \oplus S_i) \cap N \neq 0$, so choose $0 \neq x = y + z$, $x \in N$, $y \in M_J$, $z \in S_i$. Then $z = x - y \in (M_j + N) \cap S_i$, and if $z = 0$, then $x = y \in N \cap M_j = 0$, contradiction. So $(M_J \oplus N) \cap S_i \neq 0$. Since S_i is simple, this forces $S_i \subseteq M_J \oplus N$. It follows that $M = M_J \oplus N$.
(ii) $\implies$ (i): First observe that the hypothesis on M necessarily passes to all submodules of M. Next we CLAIM that every nonzero submodule $C \subseteq M$ contains a simple module.

PROOF OF CLAIM: Choose $0 \neq c \in C$, and let D be a submodule of C which is maximal with respect to not containing c. By the observation of the previous paragraph, we may write $C = D \oplus E$. Then E is simple. Indeed, suppose not and

[1] More on this later!

let $0 \subsetneq F \subsetneq E$. Then $E = F \oplus G$ so $C = D \oplus F \oplus G$. If both $D \oplus F$ and $D \oplus G$ contained c, then $c \in (D \oplus F) \cap (D \oplus G) = D$, contradiction. So either $D \oplus F$ or $D \oplus G$ is a strictly larger submodule of C than D which does not contain c, contradiction. So E is simple, establishing our claim.

Now let $N \subseteq M$ be maximal with respect to being a direct sum of simple submodules, and write $M = N \oplus C$. If $C \neq 0$, then by the claim C contains a nonzero simple submodule, contradicting the maximality of N. Thus $C = 0$ and M is a direct sum of simple submodules.
(i) $\implies$ (iii) is immediate.
(iii) $\implies$ (i): as above, by Zorn's Lemma there exists a submodule N of M which is maximal with respect to being a direct sum of simple submodules. We must show $N = M$. If not, since M is assumed to be generated by its simple submodules, there exists a simple submodule $S \subseteq M$ which is not contained in N. But since S is simple, it follows that $S \cap N = 0$ and thus $N \oplus S$ is a strictly larger direct sum of simple submodules: contradiction. □

COROLLARY 8.6. *An R-module M has a unique maximal semisimple submodule, called the* ***socle of M*** *and written* $\operatorname{Soc} M$. *Thus M is semisimple iff* $M = \operatorname{Soc} M$.

EXERCISE 8.6. *Prove Corollary 8.6.*

EXERCISE 8.7. *Let $N \in \mathbb{Z}^+$. Compute the socle of the $\mathbb{Z}$-module $\mathbb{Z}/N\mathbb{Z}$. Show in particular that $\mathbb{Z}/N\mathbb{Z}$ is semisimple if and only if N is squarefree.*

A not-necessarily-commutative ring R is **left semisimple** if R is semisimple as a left R-module.

THEOREM 8.7. *For a nonzero not necessarily commutative ring R, the following are equivalent:*

(i) *R is left semisimple.*
(ii) *Every left ideal of R is a direct summand.*
(iii) *Every left ideal of R is an injective module.*
(iv) *All left R-modules are semisimple.*
(v) *All short exact sequences of left R-modules split.*
(vi) *All left R-modules are projective.*
(vii) *All left R-modules are injective.*

PROOF. We will show (i) $\iff$ (ii), (iv) $\iff$ (v) $\iff$ (vi) $\iff$ (vii) and (ii) $\implies$ (vii) $\implies$ (iii) $\implies$ (ii), which suffices.
(i) $\implies$ (ii) follows immediately from Theorem 8.5.
(iv) $\iff$ (v) follows immediately from Theorem 8.5.
(v) $\iff$ (vi) and (v) $\iff$ (vii) are immediate from the definitions of projective and injective modules.
(ii) $\implies$ (vii): Let I be a left ideal of R and $f : I \to M$ an R-module map. By hypothesis, there exists J such that $I \oplus J = R$, so f extends to $F : R = I \oplus J \xrightarrow{\pi_1} I \to M$. By Baer's Criterion, M is injective.
(vii) $\implies$ (iii) is immediate.
(iii) $\implies$ (ii) is immediate from the definition of injective modules. □

LEMMA 8.8. *Let R be a ring and $\{M_j\}_{j \in J}$ be an indexed family of nonzero R-modules. The following are equivalent:*

(i) *I is finite and each M_j is finitely generated.*
(ii) *$M = \bigoplus_{j \in J} M_j$ is finitely generated.*

PROOF. (i) $\implies$ (ii) is left to the reader as an easy exercise.
(ii) $\implies$ (i): Each M_j is isomorphic to a quotient of M, so if M is finitely generated, so is M_j. Now let $X = \{x_1, \ldots, x_n\}$ be a finite generating set for M, and for each $1 \leqslant 1 \leqslant n$, let x_{ij} be the j-component of x_i, so $x_i = \sum_{j \in J} x_{ij}$. This sum is of course finite, and therefore the set $J' \subseteq J$ of indices j such that $x_{ij} \neq 0$ for some $1 \leqslant i \leqslant n$ is finite. It follows that $\langle X \rangle \subseteq \bigoplus_{j \in J'} M_j \subsetneq M$, contradiction. □

LEMMA 8.9. *Let $R_1, \ldots, R_n$ be finitely many not necessarily commutative rings, and put $R = \prod_{i=1}^n R_i$. Then R is semisimple if and only if $R_i$is semisimple for all $1 \leqslant i \leqslant n$.*

EXERCISE 8.8. *Prove Lemma 8.9.*

We now quote the following basic result from noncommutative algebra.

THEOREM 8.10. *(Wedderburn-Artin) For a ring R, the following are equivalent:*

(i) *R is semisimple as a left R-module (left semisimple).*
(ii) *R is semisimple as a right R-module (right semisimple).*
(iii) *There are $N, n_1, \ldots, n_N \in \mathbb{Z}^+$ and division rings $D_1, \ldots, D_N$ such that*

$$R \cong \prod_{i=1}^N M_{n_i}(D_i).$$

Combining Theorems 8.7 and 8.10 gives us a tremendous amount of information. First of all, a ring is left semisimple iff it is right semisimple, so we may as well speak of **semisimple rings**. A ring is semisimple if and only if it is **absolutely projective** if and only if it is **absolutely injective**.

Coming back to the commutative case, the Wedderburn-Artin theorem tells us that the class of semisimple / absolutely projective / absolutely injective rings is extremely restricted.

COROLLARY 8.11. *A commutative ring is semisimple if and only if it is a finite product of fields.*

However it is significantly easier to give a proof of Wedderburn-Artin in the commutative case, so we will give a direct proof of Corollary 8.11

PROOF. Step -1: Officially speaking the theorem holds for the zero ring because it is an empty product of fields. In any event, we may and shall assume henceforth that our semisimple ring is nonzero.
Step 0: A field is a semisimple ring: e.g. every module over a field is free, hence projective. By Lemma 8.9, a finite direct product of fields is therefore semisimple.
Step 1: Let R be a semisimple ring, and let $R = \bigoplus_{i \in I} M_i$ be a direct sum decomposition into simple R-modules. R is a finitely generated R-module, by Lemma 8.8 I is finite, and we may identify it with $\{1, \ldots, n\}$ for some $n \in \mathbb{Z}^+$: $R = M_1 \oplus \ldots \oplus M_n$.
Step 2: We may uniquely write $1 = e_1 + \ldots + e_n$ with $e_i \in M_i$. Then for all $i \neq j$, $e_i e_j = 0$, and this together with the identity $1 \cdot 1 = 1$ implies that $e_i^2 = e_i$ for all i. As usual for idempotent decompositions, this expresses R as a direct product of

the subrings $R_i = M_i = e_iR$. Moreover, since M_i is a simple R-module, R_i has no proper nonzero ideals, and thus it is a field, say k_i. □

EXERCISE 8.9. *Exhibit an absolutely flat commutative ring that is not semisimple.*

4. Normal Series

If M is an R-module a **normal series** is a finite ascending chain of R-submodules $0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_n = M$. We say that n is the **length** of the series. (The terminology is borrowed from group theory, in which one wants a finite ascending chain of subgroups with each normal in the next. Of course there is no notion of "normal submodule", but we keep the group-theoretic terminology.)

There is an evident partial ordering on the set of normal series of a fixed R-module M: one normal series $\{M_i\}_{i=0}^n$ is less than another normal series $\{M'_j\}_{j=0}^{n'}$ if for all $1 \leqslant i \leqslant n$, M_i is equal to M'_j for some (necessarily unique) j. Rather than saying that $\{M_i\} \leqslant \{M'_j\}$, it is traditional to say that the larger series $\{M'_j\}$ **refines** the smaller series $\{M_i\}$.

Given any normal series $\{M_i\}$ we may form the associated **factor sequence** $M_1/M_0 = M_1, M_2/M_1, \ldots, M_n/M_{n-1} = M/M_{n-1}$. Two normal series $\{M_i\}_{i=0}^n, \{M'_j\}_{j=0}^{n'}$ are **equivalent** if $n = n'$ and there is a permutation σ of $\{1, \ldots, n\}$ such that for all $1 \leqslant i \leqslant n$, the factors M_i/M_{i-1} and $M'_{\sigma(i)}/M'_{\sigma(i)-1}$ are isomorphic. In other words, if we think of the factor sequence of a normal series as a **multiset** of isomorphism classes of modules, then two normal series are equivalent if the associated multisets of factors are equal.

EXERCISE 8.10. *Show: refinement descends to a partial ordering on equivalence classes of normal series of a fixed R-module M.*

The following theorem is the basic result in this area.

THEOREM 8.12. *(Schreier Refinement) For any R-module M, the partially ordered set of equivalence classes of normal series of submodules of M is* directed*: that is, any two normal series admit equivalent refinements.*

PROOF. For the proof in a context that simultaneously generalizes that of modules and groups, see e.g. [**J2**, §3.3]. □

For an R-module M, a **composition series** is a maximal element in the partially ordered set of normal series: that is, a composition series which admits no proper refinement.

EXERCISE 8.11. *Show: a normal series $\{M_i\}_{i=0}^n$ for an R-module M is a composition series if and only if for all $1 \leqslant i \leqslant n$, the factor module M_i/M_{i-1} is simple.*

THEOREM 8.13. *(Jordan-Hölder) Let M be an R-module. Then any two composition series for M are* equivalent*: up to a permutation, their associated factor series are term-by-term isomorphic.*

PROOF. This is an immediate consequence of Schreier Refinement: any two normal series admit equivalent refinements, but no composition series admits a proper refinement, so any two composition series must already be equivalent. □

Thus for a module M which admits a composition series, we may define the **length** $\ell(M)$ of M to be the length of any composition series. One also speaks of the **Jordan-Hölder factors of M** or the **composition factors of M**, i.e., the unique multiset of isomorphism classes of simple R-modules which must appear as the successive quotients of any composition series for M.

If a module does not admit a composition series, we say that it has infinite length.

And now a basic question: which R-modules admit a composition series?

EXERCISE 8.12. *Let M be an R-module.*

a) *Suppose M is finite: recall that for us this mean that the underlying set of M is finite (which is* much *stronger than being finitely generated). Show: M admits a composition series.*
b) *Show: if M admits a composition series, then M is finitely generated.*
c) *Let $R = \mathbb{Z}$. Show: M admits a composition series and only if M is finite.*
d) *Let $R = k$ be a field. Show: M admits a composition series if and only if M is finitely generated (in other words, finite-dimensional).*

EXERCISE 8.13. *Show: an R-module M admits a composition series if and only if there is $L \in \mathbb{Z}^+$ such that every normal series in M has length at most L. (Hint: use Schreier Refinement.)*

THEOREM 8.14. *Show: for an R-module M, the following are equivalent:*

(i) *M is both Noetherian and Artinian.*
(ii) *M admits a composition series.*

PROOF. Assume (i). Since M satisfies (DCC), there is a minimal nonzero submodule, say M_1. If M_1 is a maximal proper submodule, we have a composition series. Otherwise among all proper R-submodules strictly containing M_1, by (DCC) we can choose a minimal one M_2. We continue in this way: since M also satisfies (ACC) the process must eventually terminate, yielding a composition series.

(ii) $\implies$ (i): This follows easily from Exercise 8.13. □

EXERCISE 8.14. *Exercise 8.13 makes use of Schreier Refinement. Give a proof that (ii) $\implies$ (i) in Theorem 8.14 that is independent of Schreier Refinement. (Suggestion: try induction on the length of a composition series.)*

PROPOSITION 8.15. *Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of R-modules.*

a) *M admits a composition series if and only if both M' and M'' admit composition series.*
b) *If M admits a composition series, then*

$$\ell(M) = \ell(M') + \ell(M'').$$

EXERCISE 8.15. *Prove Proposition 8.15.*

Although it will not play a prominent role in our course, the length of an R-module M is an extremely important invariant, especially in algebraic geometry: it is is used, among other things, to keep track of intersection multiplicities and to quantitatively measure the degree of singularity of a point.

5. The Krull-Schmidt Theorem

The material in this section follows [**J2**, §3.4] very closely. In particular, very exceptionally for us – but as in *loc. cit.* – in this section we work with left modules over a *possibly noncommutative ring* R. The reason: not only does the desired result carry over verbatim to the noncommutative case (this is not in itself a good enough reason, as the same holds for a positive proportion of the results in these notes) but the proof requires us to consider noncommutative rings!

A module M is **decomposable** if there are nonzero submodules $M_1, M_2 \subseteq M$ such that $M = M_1 \oplus M_2$; otherwise M is **indecomposable**.

THEOREM 8.16. *(Krull-Schmidt) Let M be an R-module of finite length.*

a) *There are indecomposable submodules $M_1, \ldots, M_m$ such that $M = \bigoplus_{i=1}^m M_i$.*
b) *If there are indecomposable submodules $N_1, \ldots, N_n$ such that $M = \bigoplus_{i=1}^n N_i$, then $m = n$ and there exists a bijection σ of $\{1, \ldots, n\}$ such that for all i, $M_i \cong N_{\sigma(i)}$.*

The *Proof* of Theorem 8.16a) is easy, and we give it now. If M is a finite length module and we write $M = M_1 \oplus M_2$ then $0 < \ell(M_1), \ell(M_2) < \ell(M)$. Thus an evident induction argument shows that any sequence of moves, each one of which splits a direct summand of M into two nontrivial direct subsummands of M, must terminate after finitely many steps, leaving us with a decomposition of M into a finite direct sum of indecomposable submodules. □

As one might suspect, the second part of Theorem 8.16 concerning the uniqueness of the indecomposable decomposition is more subtle. Indeed, before giving the proof we need some preparatory considerations on endomorphism rings of modules.

PROPOSITION 8.17. *For an R-module M, the following are equivalent:*

(i) *M is decomposable.*
(ii) *The (possibly noncommutative, even if R is commutative) ring $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$ has a nontrivial idempotent, i.e., an element $e \neq 0, 1$ with $e^2 = e$.*

EXERCISE 8.16. *Prove Proposition 8.17.*

A not-necessarily-commutative ring R is **local** if the set of nonunits $R \backslash R^\times$ forms a two-sided ideal of R.

EXERCISE 8.17. *Let R be a local, not necessarily commutative ring.*

a) *Show: $R \neq 0$.*
b) *Show: R has no nontrivial idempotents.*

An R-module M is **strongly indecomposable** if $\mathrm{End}_R(M)$ is local. Thus it follows from Proposition 8.17 and Exercise 8.17 that a strongly indecomposable module is indecomposable.

EXAMPLE 8.18. *The $\mathbb{Z}$-module $\mathbb{Z}$ is indecomposable: any two nonzero submodules (a) and (b) have a nontrivial intersection (ab). On the other hand $\mathrm{End}_{\mathbb{Z}}(\mathbb{Z}) = \mathbb{Z}$ is not a local ring, so $\mathbb{Z}$ is not strongly indecomposable.*

Thus "strongly indecomposable" is, in general, a stronger concept than merely "indecomposable". Notice though that the Krull-Schmidt theorem applies only to finite length modules – equivalently to modules which are both Noetherian and Artinian – and $\mathbb{Z}$ is not an Artinian $\mathbb{Z}$-module. In fact, it shall turn out that any finite length indecomposable module is strongly indecomposable, and this will be a major step towards the proof of the Krull-Schmidt Theorem.

But we are not quite ready to prove this either! First some Fitting theory.

For an R-module M and $f \in \mathrm{End}_R(M)$, we put

$$f^\infty(M) = \bigcap_{n=1}^{\infty} f^n(M).$$

The set $f^\infty(M)$ is the intersection of a descending chain

$$M \supset f(M) \supset f^2(M) \supset \ldots \supset f^n(M) \supset \ldots$$

of submodules of M, and is thus an f-stable submodule of M. The restriction of f to $f^\infty(M)$ is surjective. Moreover, if M is an Artinian module, there exists $s \in \mathbb{Z}^+$ such that $f^s(M) = f^{s+1}(M) = \ldots$.

EXERCISE 8.18. *Find a commutative ring R, an R-module M and $f \in \mathrm{End}_R(M)$ such that for no $n \in \mathbb{Z}^+$ is the submodule $f^n(M)$ f-stable.*

Similarly, for M and f as above, we put

$$f_{-\infty}(0) = \bigcup_{n=1}^{\infty} \ker f^n.$$

Here each $\ker f^n$ is an f-stable submodule of M on which f is *nilpotent*. The set $f_{-\infty}(0)$ is the union of an ascending chain of submodules

$$0 \subseteq \ker f \subseteq \ker f^2 \subseteq \ldots \subseteq \ker f^n \subseteq \ldots$$

of M and is thus an f-stable submodule of M on which f acts as a *nil* endomorphism: i.e., every element of M is killed by some power of f. Moreover, if M is a Noetherian module, there exists $t \in \mathbb{Z}^+$ such that $\ker f^t = \ker f^{t+1} = \ldots$ and thus f is a nilpotent endomorphism of $f_{-\infty}(0)$.

EXERCISE 8.19. *Find a commutative ring R, an R-module M and $f \in \mathrm{End}_R(M)$ such that f is* not *a nilpotent endomorphism of $f_{-\infty}(0)$.*

THEOREM 8.19. *(Fitting's Lemma) Let M be a finite length module over the not necessarily commutative ring R, and let $f \in \mathrm{End}_R(M)$.*

a) *There is a* ***Fitting Decomposition***

$$M = f^\infty(M) \oplus f^{-\infty}(0). \tag{17}$$

b) *$f|_{f^\infty(M)}$ is an isomorphism and $f|_{f_{-\infty}(0)}$ is nilpotent.*

PROOF. Since M has finite length it is both Noetherian and Artinian. Thus there exists $r \in \mathbb{Z}^+$ such that

$$f^r(M) = f^{r+1}(M) = \ldots = f^\infty(M)$$

and

$$\ker f^r = \ker f^{r+1} = \ldots = f_{-\infty}(0).$$

Let $x \in f^{\infty}(M) \cap f_{-\infty}(0)$. Then there is $y \in M$ such that $x = f^r(y)$; moreover $0 = f^r(x) = f^{2r}(y)$. But $f^{2r}(y) = 0$ implies $x = f^r(y) = 0$, so $f^{\infty}(M) \cap f_{-\infty}(0) = 0$.

Let $x \in M$. Then $f^r(x) \in f^r(M) = f^{2r}(M)$, so there exists $y \in M$ with $f^r(x) = f^{2r}(y)$ and thus $f^r(x - f^r(y)) = 0$. so

$$x = f^r(y) + (x - f^r(y)) \in f^{\infty}(M) + f^{-\infty}(0),$$

completing the proof of part a). As for part b), we saw above that the restriction of f to $f^{\infty}(M)$ is surjective. It must also be injective since every element of the kernel lies in $f^{-\infty}(0)$. Thus $f|_{f^{\infty}(M)}$ is an isomorphism. Finally, as observed above, since $f_{-\infty}(0) = \ker f^r$, $f|_{f_{-\infty}(0)}$ is nilpotent. □

COROLLARY 8.20. *Let M be a finite length indecomposable R-module. Then every $f \in \mathrm{End}_R(M)$ is either an automorphism or nilpotent. Moreover M is strongly indecomposable.*

PROOF. Since M is indecomposable, Fitting's Lemma implies that for $f \in \mathrm{End}_R(M)$ we must have either $M = f^{\infty}(M)$ – in which case f is an automorphism – or $M = f^{-\infty}(0)$ – in which case f is nilpotent. We must show that

$$I := \mathrm{End}_R(M) \setminus \mathrm{End}_R(M)^{\times}$$

is a two-sided ideal of $\mathrm{End}_R(M)$. We observe that I consists precisely of the nilpotent elements of $\mathrm{End}_R(M)$.

For $f \in I$ and $g \in \mathrm{End}_R(M)$, since f is neither injective nor surjective, we have gf is not injective and fg is not surjective, hence $fg,\ gf \in I$.

Let $f_1, f_2 \in I$, and seeking a contradiction we suppose that $f_1 + f_2 \notin I$, so $u := f_1 + f_2 \in \mathrm{End}_R(M)^{\times}$. For $i = 1, 2$, we put $h_i = f_i u_i^{-1}$, so $h_1 + h_2 = 1$. Then h_2 is non-invertible hence nilpotent: we have $h_2^n = 0$ for some $n \in \mathbb{Z}^+$ and thus

$$(1 - h_2)(1 + h_2 + \ldots + h_2^{n-1}) = 1 = (1 + h_2 + \ldots + h_2^{n-1})(1 - h_2),$$

contradicting that $h_1 = 1 - h_2 \in I$ □

LEMMA 8.21. *Let M be a nonzero R-module and N an indecomposable R-module. Suppose we have homomorphisms $f : M \to N,\ g : N \to M$ such that gf is an automorphism of M. Then both f and g are isomorphisms.*

PROOF. Let $h = (gf)^{-1}$, $l = hg : N \to M$ and $e = fl : N \to N$. Then $lf = hgf = 1_M$ and $e^2 = flfl = f1_M l = fl = e$. Since M is indecomposable, either $e = 1$ or $e = 0$, and the latter implies $1_M = 1_M^2 = lflf = lef = 0$, i.e., $M = 0$. So $fl = e = 1_N$, so f is an isomorphism and thus so too is $(f(gf)^{-1})^{-1} = g$. □

THEOREM 8.22. *Let $M \cong N$ be isomorphic modules, and let $M = \bigoplus_{i=1}^m M_i$ and $N = \bigoplus_{i=1}^n N_i'$ with each M_i strongly indecomposable and each N_i indecomposable. Then $m = n$ and there is a bijection σ of $\{1, \ldots, m\}$ such that for all i, $M_i \cong N_{\sigma(i)}$.*

PROOF. By induction on m: $m = 1$ is clear. Suppose the result holds for all direct sums of fewer than m strongly indecomposable submodules.

Step 1: Let $e_1, \ldots, e_m \in \mathrm{End}_R(M)$ and $f_1, \ldots, f_n \in \mathrm{End}_R(N)$ be the idempotent elements corresponding to the given direct sum decompositions (i.e., projection onto the corresponding factor). Let $g : M \xrightarrow{\sim} N$, and put

$$h_j := f_j g e_1 \in \mathrm{Hom}_R(M, N),\ k_j = e_1 g^{-1} f_j \in \mathrm{Hom}_R(N, M),\ 1 \leqslant j \leqslant n.$$

Then

$$\sum_{j=1}^{n} k_j h_j = \sum_j e_1 g^{-1} f_j g e_1 = e_1 g^{-1} \sum_j f_j g e_1 = e_1 g^{-1} 1_N g e_1 = e_1.$$

The restrictions of e_1 and $k_j h_j$ to M_1 stabilize M_1 so may be regarded as endomorphisms of M_1, say e_1' and $(k_j h_j)'$, and we have

$$\sum_{j=1}^{n} (k_j h_j)' = e_1' = 1_{M_1}.$$

By assumption $\mathrm{End}_R M_1$ is local, so for at least one j, $(k_j h_j)'$ is a unit, i.e., an automorphism of M_1. By reordering the N_j's we may assume that $j = 1$, so $(k_1 h_1)' \in \mathrm{Aut}_R M_1$. We may regard the restriction h_1' of h_1 to M_1 as a homomorphism from M_1 to N_1 and similarly the restriction k_1' of k_1 to N_1 as a homomorphism from N_1 to M_1, and then $k_1' h_1' = (k_1 h_1)'$ is an automorphism. By Lemma 8.21, $h_1' = (f_1 g e_1') : M_1 \xrightarrow{\sim} N_1$ and $k_1' = (e_1 g^{-1} f_1)' : N_1 \xrightarrow{\sim} M_1$.
Step 2: We claim that

$$M = g^{-1}(N_1) \oplus \bigoplus_{i=2}^{m} M_i. \tag{18}$$

To see this, let $x \in g^{-1}N_1 \cap (\bigoplus_{i=2}^m M_i)$, so $x = g^{-1}y$ for some $y \in N_1$. Because $x \in \bigoplus_{i=2}^m M_i$, $e_1 x = 0$. Thus

$$0 = e_1 x = e_1 g^{-1} y = e_1 g^{-1} f_1 y = k_1 y = k_1' y.$$

Since k_1' is an isomorphism, $y = 0$ and thus $x = 0$, so the sum in (18) is direct. Now put $M' = g^{-1}(N_1) \oplus \bigoplus_{i=2}^m M_i$, so we wish to show $M' = M$. Let $x \in g^{-1}N_1$. Then $x, e_2 x, \ldots, e_m x \in M'$, so $e_1 x = (1 - e_2 - \ldots - e_m)x \in M'$. So

$$M' \supset e_1 g^{-1} N_1 = e_1 g^{-1} f_1 N_1 = k_1 N_1 = k_1' N_1 = M_1$$

and thus $M' \supset \bigoplus_{i=1}^m M_i = M$.
Step 3: The isomorphism $g : M \xrightarrow{\sim} N$ carries $g^{-1}N_1$ onto N_1 hence induces an isomorphism $\frac{M}{g^{-1}N_1} \overset{sim}{\to} N/N_1$. Using Step 2, we have

$$\bigoplus_{j=2}^{n} N_i = \frac{N}{N_1} \cong \frac{M}{g^{-1}N_1} \cong \bigoplus_{i=2}^{m} M_i.$$

We are done by induction. □

EXERCISE 8.20. *Please confirm that we have proved the Krull-Schmidt Theorem!*

EXERCISE 8.21. *Let M and N be R-modules such that $M \times M \cong N \times N$.*

a) *If M and N are both of finite length, show that $M \cong N$.*
b) *Must we have $M \cong N$ in general?*

Part b) is far from easy! If you give up, see [**Co64**].

6. Some important terminology

All we aspire to do in this section is to introduce some terminology, but it is so important that we have isolated it for future reference.

Let R be a ring and $\mathfrak{p}$ a prime ideal of R. The **height** of $\mathfrak{p}$ is the supremum of all lengths of finite chains of prime ideals of the form $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n = \mathfrak{p}$ (the length of the indicated chain being n; i.e., it is the number of $\subsetneq$'s appearing, which is one less than the number of elements). Thus the height is either a non-negative integer or ∞; the latter transpires if and only if there are arbitrarily long finite chains of prime ideals descending from $\mathfrak{p}$ (and of course, this need not imply the existence of an infinite chain of prime ideals descending from $\mathfrak{p}$).

A prime ideal of height 0 is called a **minimal prime**. In a domain R, the unique minimal prime is (0), so the concept is of interest only for rings which are not domains. If I is a proper ideal of R, we also speak of a **minimal prime over** I, which means a prime $\mathfrak{p} \supset I$ such that there is no prime ideal $\mathfrak{q}$ with $I \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$. Note that $\mathfrak{p}$ is a minimal prime over I if and only if $\mathfrak{p}$ is a minimal prime in the quotient ring R/I. This remark simultaneously explains the terminology "minimal over" and gives a hint why it is useful to study minimal prime ideals even if one is ultimately most interested in domains.

The **dimension** of a ring R is the supremum of all the heights of its prime ideals. The full proper name here is **Krull dimension** of R, which is of course useful when one has other notions of dimension at hand. Such things certainly do exist but will not be considered here. Moreover, as will shortly become apparent, the need to include Krull's name here so as to ensure that he gets proper recognition for his seminal work in this area is less than pressing. Therefore we use the full name "Krull dimension" only rarely as a sort of rhetorical flourish.

One also often speaks of the **codimension** of a prime ideal $\mathfrak{p}$ of R, which is the dimension of R minus the height of $\mathfrak{p}$. This is especially natural in applications to algebraic geometry, of which the present notes allude to only in passing. Note that this is *not* necessarily equal to the Krull dimension of $R/\mathfrak{p}$ – or what is the same as that, the maximal length of a finite chain of prime ideals ascending from $\mathfrak{p}$ – although in reasonable applications, and especially in geometry, one is certainly entitled to hope (and often, to prove) that this is the case.

Remark: All of these definitions would make perfect sense for arbitrary partially ordered sets and their elements, but the terminology is not completely consistent with order theory. Namely, the height of an element in an arbitrary partially ordered set *is* defined as the supremum of lengths of chains descending from that element, but the order theorists would cringe to hear the supremum of all heights of elements called the "dimension" of the partially ordered set. They would call that quantity the height of the partially ordered set, and would reserve dimension for any of several more interesting invariants. (Roughly, the idea is that a chain of any finite length is one-dimensional, whereas a product of d chains should have dimension d.)

7. Introducing Noetherian rings

The following is probably the most important single definition in all of ring theory.

A ring R is said to be **Noetherian** if the partially ordered set $\mathcal{I}(R)$ of all ideals of R satisfies the ascending chain condition.

THEOREM 8.23. *A finitely generated module over a Noetherian ring is Noetherian.*

PROOF. If M is a finitely generated module over R, then we may represent it as R^n/K for some submodule K of R^n. An immediate corollary of the preceding theorem is that finite direct sums of Noetherian modules are Noetherian, and by assumption R itself is a Noetherian R-module, hence so is R^n and hence so is the quotient $R^n/K = M$. □

Thus so long as we restrict to Noetherian rings, submodules of finitely generated modules remain finitely generated. This is extremely useful even in the case of $R = \mathbb{Z}$: a subgroup of a finitely generated commutative group remains finitely generated. This does not hold for all noncommutative groups, e.g. not for a finitely generated free group of rank greater than 1.

THEOREM 8.24. *(Characterization of Noetherian rings) For a ring R, the following are equivalent:*

(i) *Every nonempty set of ideals of R has a maximal element.*
(ii) *There are no infinite ascending chains*

$$I_1 \subsetneq I_2 \subsetneq \ldots \subsetneq I_n \subsetneq \ldots$$

of ideals of R.
(iii) *Every ideal of R is finitely generated.*
(iv) *Every prime ideal of R is finitely generated.*

PROOF. (i) $\iff$ (ii) is a special case of Proposition 8.1.
(ii) $\iff$ (iii) is a special case of Exercise 8.2.
(iii) $\iff$ (iv) is Cohen's Theorem (Theorem 4.25). □

EXERCISE 8.22. *Suppose a ring R satisfies the ascending chain condition on prime ideals. Must R be Noetherian?*

PROPOSITION 8.25. *Let R be a Noetherian ring.*

a) *If I is an ideal of R, the quotient R/I is Noetherian.*
b) *If $S \subseteq R$ is any multiplicative subset, the localization $S^{-1}R$ is Noetherian.*

PROOF. Any ideal of R/I is of the form J/I for some ideal $J \supset I$ of R. By assumption J is finitely generated, hence J/I is finitely generated, so R/I is Noetherian. A similar argument holds for the localization; details are left to the reader. □

EXERCISE 8.23. *Let k be a field, let S be an infinite set, and put $R = \prod_{s \in S} k$, i.e., the infinite product of $\#S$ copies of k. Show that R is not Noetherian, but the localization $R_{\mathfrak{p}}$ at each prime ideal is Noetherian.*

Thus Noetherianity is a localizable property but not a local property.

8. Theorems of Eakin-Nagata, Formanek and Jothilingam

In 1968, P.M. Eakin, Jr. [**Ea68**] and M. Nagata [**Na68**] independently showed that if a ring R admits an extension ring S which is Noetherian and finitely generated as an R-module, then R is Noetherian.

Several years later, E. Formanek [**Fo73**] gave a stronger result. His improvement is a nice instance of the philosophy of "modulization": where possible one should replace theorems about rings with theorems about modules over rings. He writes: "The object of this paper is to present a simple and elementary proof of the Eakin-Nagata theorem which generalizes the original version in a new direction. The proof is essentially a contraction of Eakin's proof as presented by Kaplansky in [**K**, Exc. 14-15, p. 54] based on the observation that much of the proof disappears if one is not 'handicapped' by the hypothesis that T is a ring."

More recently, P. Jothilingam [**Jo00**] gave a result which simultaneously generalizes Formanek's Theorem and Cohen's Theorem that a ring in which all prime ideals are finitely generated is Noetherian. Finally(?), several years ago A. Naghipour [**Na05**] found a significantly shorter, simpler proof of Jothilingam's Theorem, which we will present here. All in all, this provides a nice case study of how even very basic results get improved and simplified as time passes.

Having told the story in correct chronological order, we now reverse it: we will prove Jothilingam's Theorem and swiftly deduce the earlier results as corollaries. First a couple of easy preliminaries.

LEMMA 8.26 (Kaplansky). *For a ring R, the following are equivalent:*

(i) *R is Noetherian.*
(ii) *R admits a* faithful *Noetherian module.*

PROOF. (i) $\implies$ (ii): If R is Noetherian, then R is a faithful Noetherian R-module.
(ii) $\implies$ (i): Let M be a faithful Noetherian R-module. In particular M is finitely generated, say by $x_1, \ldots, x_n$. Let $\varphi : R \to M^n$ by $r \mapsto (rx_1, \ldots, rx_n)$. Since M is Noetherian, so is M^n, and since M is faithful, φ is injective, and thus R is isomorphic to a submodule of a Noetherian module, hence Noetherian. □

EXERCISE 8.24.

a) *Show: any ring R admits a Noetherian module.*
b) *Show: if M is a Noetherian R-module, then $R/\operatorname{ann} M$ is Noetherian.*

Let M be an R-module. An R-submodule of M is **extended** if it is of the form IM for some ideal I of R. This is a generalization of a previous use of the term: if $\iota : R \to T$ is a map of rings, then the *extended ideals* of T are those of the form $\iota_* I = IT$ for an ideal I of R.

PROPOSITION 8.27. *For a finitely generated R-module M, let $\mathcal{E}_M$ be the family of extended submodules of M, partially ordered under inclusion. the following are equivalent:*

(i) *$\mathcal{E}_M$ is Noetherian: i.e., extended submodules satisfy (ACC).*
(ii) *Every extended submodule of M is finitely generated.*

PROOF. $\neg$ (ii) $\implies$ $\neg$ (i): Let I be an ideal of R such that IM is not finitely generated. Let $a_1 \in I$. Then, since M is finitely generated, $a_1 M$ is a finitely generated submodule of IM, hence proper: there exists $a_2 \in I$ such that

$a_1M \subsetneq \langle a_1, a_2\rangle M$. Again, $\langle a_1, a_2\rangle M$ is finitely generated, so is proper in IM. Continuing in this way we get a sequence $\{a_n\}_{n=1}^{\infty}$ in I such that

$$a_1M \subsetneq \langle a_1, a_2\rangle M \subsetneq \ldots \subsetneq \langle a_1, \ldots, a_n\rangle M \subsetneq \ldots,$$

so $\mathcal{E}_M$ is not Noetherian.
(ii) $\implies$ (i): Let $I_1M \subseteq I_2M \subseteq \ldots \subseteq I_nM \subseteq \ldots$ be an ascending chain in $\mathcal{E}_M$. Let $N = \sum_n I_nM$ and $I = \sum_n I_n$, so $N = IM \in \mathcal{E}_M$. By assumption, N is finite generated, so there is $n \in \mathbb{Z}^+$ with $N = I_1M + \ldots + I_nM$. Since $I_kM \subseteq I_{k+1}M$ for all k, $N = I_nM$ and thus $I_nM = I_{n+k}M$ for $k \in \mathbb{N}$: the chain stabilizes at n. □

THEOREM 8.28 (Jothilingam). *For a finitely generated R-module M, the following are equivalent:*

(i) *M is Noetherian.*
(ii) *For every prime ideal $\mathfrak{p}$ of R, the submodule $\mathfrak{p}M$ is finitely generated.*

PROOF. We follow [**Na05**].
(i) $\implies$ (ii): If M is Noetherian, then every submodule of M is finitely generated.
$\neg$ (i) $\implies$ $\neg$ (ii): Suppose M is not Noetherian: we will find a prime ideal $\mathfrak{p}$ of R such that $\mathfrak{p}M$ is infinitely generated.
Step 0: Since the union of a chain of infinitely generated submodules of M is an infinitely generated submodule of M, by Zorn's Lemma there is a submodule $N \subseteq M$ maximal with respect to being infinitely generated.
Step 1: Let $\mathfrak{p} = \operatorname{ann}(M/N) = \{x \in R \mid xM \subseteq N\}$. We will show that $\mathfrak{p}$ is a prime ideal: indeed, seeking a contradiction suppose there are $a, b \in R\backslash\mathfrak{p}$ such that $ab \in \mathfrak{p}$. Then $N + aM, B + bM \supsetneq N$ so are both finitely generated: write $N + aM = \langle n_1 + am_1, \ldots, n_\ell + am_\ell\rangle$ with $n_i \in N$, $m_i \in M$. Put

$$L = \{m \in M : am \in N\};$$

then L is an R-submodule of M containing N and bM and hence also $N + bM \supsetneq N$, so L is finitely generated. We CLAIM

$$N = \sum_{i=1}^{\ell} Rn_i + aL.$$

If so, then N is finitely generated, a contradiction, and thus $\mathfrak{p}$ is prime. Since $abM \subseteq N$, we have $\sum_{i=1}^{\ell} Rn_i + aL \subseteq N$. Conversely, let $y \in N$. Since $y \in N + aM$, there are $b_1, \ldots, b_\ell \in R$ such that

$$y = \sum_{i=1}^{\ell} b_i(n_i + am_i) = \sum_{i=1}^{\ell} b_in_i + a\sum_{i=1}^{\ell} b_im_i.$$

Thus

$$a\sum_{i=1}^{\ell} b_im_i = y - \sum_{i=1}^{\ell} b_in_i \in N,$$

so $\sum_{i=1}^{\ell} b_im_i \in L$ and $y \in \sum_{i=1}^{\ell} Rn_i + aL$.
Step 2: For $x \in M$, write $\overline{x}$ for the canonical image of x in M/N. Now we use that M is finitely generated: write $M = \langle x_1, \ldots, x_n\rangle_R$, so $M/N = \langle \overline{x_1}, \ldots, \overline{x_n}\rangle_R$, so $\mathfrak{p} = \bigcap_{i=1}^{n} \operatorname{ann} R\overline{x_i}$. Because $\mathfrak{p}$ is prime, we must have $\mathfrak{p} = \operatorname{ann} R\overline{x_j}$ for some j.

Since $N + Rx_i \supsetneq N$, $N + Rx_i$ is finitely generated, say by $y_1 + r_1x_j, \ldots, y_k + r_kx_j$, with $y_i \in N$, $r_i \in R$. Arguing as in Step 1 we get

$$N = \sum_{i=1}^{k} Ry_i + \mathfrak{p}x_j.$$

Since $\mathfrak{p}M \subseteq N$, we have

$$N = \sum_{i=1}^{k} Ry_i + \mathfrak{p}x_j \subseteq \sum_{i=1}^{k} Ry_i + \mathfrak{p}M \subseteq \sum_{i=1}^{k} Ry_i + N \subseteq N,$$

and thus

$$N = \sum_{i=1}^{k} Ry_i + \mathfrak{p}M. \tag{19}$$

Since N is infinitely generated, (19) implies $\mathfrak{p}M$ is infinitely generated. □

COROLLARY 8.29. *(Formanek's Theorem) Let R be a ring, and let $M = \langle a_1, \ldots, a_n \rangle$ be a faithful finitely generated R-module. Suppose M satisfies (ACC) on "extended submodules" – i.e., submodules of the form IM for I an ideal of R. Then M is Noetherian, hence so is R.*

PROOF. By Proposition 8.27, all extended submodules are finitely generated, hence *a fortiori* all submodules of the form $\mathfrak{p}M$ for $\mathfrak{p} \in \operatorname{Spec} R$ are finitely generated. By Theorem 8.28, M is Noetherian, and then by Lemma 8.26, R is Noetherian. □

COROLLARY 8.30. *(Eakin-Nagata Theorem) Let $R \subseteq S$ be an ring extension, with S finitely generated as an R-module. Then R is Noetherian if and only if S is Noetherian.*

PROOF. $\Longrightarrow$ If R is Noetherian, then S is a finitely generated module over a Noetherian ring so S is a Noetherian R-module. That is, (ACC) holds on R-submodules of S, hence *a fortiori* it holds on S-submodules of S.
$\Longleftarrow$ Apply Formanek's Theorem with $M = S$. □

EXERCISE 8.25. *Investigate the possibility of proving Jothilingam's Theorem using the Prime Ideal Principle of* §4.5.

9. The Bass-Papp Theorem

We now present a beautiful characterization of Noetherian rings in terms of properties of injective modules, due independently to Z. Papp [**Pa59**] and H. Bass [**Ba59**].

THEOREM 8.31. *(Bass-Papp) For a ring R, the following are equivalent:*

(i) *A direct limit of injective modules is injective.*
(ii) *A direct sum of injective modules is injective.*
(iii) *A countable direct sum of injective modules is injective.*
(iv) *R is Noetherian.*

PROOF.
(i) $\Longrightarrow$ (ii): A direct sum is a kind of direct limit.
(ii) $\Longrightarrow$ (iii) is immediate.

(iii) $\implies$ (iv): Let $I_1 \subseteq I_2 \subseteq \ldots \subseteq I_n \subseteq \ldots$ be an infinite ascending chain of ideals of R, and let $I = \bigcup_n I_n$. We define

$$E = \bigoplus_{n=1}^{\infty} E(R/I_n).$$

For $n \in \mathbb{Z}^+$, let $f_n : I \to E(R/I_n)$ be the composite map $I \to R \to R/I_n \to E(R/I_n)$. There is then a unique map $\prod f : I \to \prod_{n=1}^{\infty} E(R/I_n)$. But indeed, for each fixed $x \in I$, x lies in I_n for sufficiently large n and thus $f_n(x) = 0$. It follows that $\prod f$ actually lands in the direct sum, and we have thus defined a map

$$f : I \to E.$$

By hypothesis, E is a countable direct sum of injective modules and therefore injective, so f extends to an R-module map with domain all of R and is thus of the form $f(x) = xf(1) = xe$ for some fixed $e \in E$. Let N be sufficiently large so that for $n \geqslant N$, the nth component e_n of e is zero. Then for all $x \in I$,

$$0 = xe_n = f_n(x) = x + I_n \in R/I_n,$$

and thus $x \in I_n$. That is, for all $n \geqslant N$, $I_n = I$.
(iv) $\implies$ (i): let $\{E_\alpha\}$ be a directed system of injective modules with direct limit E. For $\alpha \leqslant \beta$ we denote the transition map from E_α to E_β by $\iota_{\alpha\beta}$ and the natural map from E_α to E by ι_α. We will show E is injective by Baer's Criterion (Theorem 3.22), so let I be any ideal of R and consider an R-module map $f : I \to E$. Since R is Noetherian, I is finitely generated, and it follows that there exists an index α such that $f(I) \subseteq \iota_\alpha(E_\alpha)$. Let M be a finitely generated submodule of E_α such that $f(I) \subseteq \iota_\alpha(M)$. Consider the short exact sequence

$$0 \to K \to M \xrightarrow{\iota_\alpha} f(I) \to 0.$$

Since M is finitely generated and R is Noetherian, K is finitely generated. Moreover K maps to 0 in the direct limit, so there exists $\beta \geqslant \alpha$ such that $\iota_{\alpha\beta} K = 0$. Let $M' = \iota_{\alpha\beta} M$, so by construction

$$\iota_\beta : M' \xrightarrow{\sim} f(I).$$

Taking $g = \iota_\beta|_{M'}^{-1} \circ f$ we get a map $g : I \to E_\beta$ such that $f = \iota_\beta \circ g$. Since E_β is injective, g extends to a map $G : R \to E_\beta$ and thus $F = \iota_\beta \circ G$ extends f to R. $\square$

10. Artinian rings: structure theory

A ring R which satisfies the descending chain condition (DCC) on ideals is called **Artinian** (or sometimes, "an Artin ring").

Exercise 8.26.

a) *Show: a ring with only finitely many ideals is Artinian.*
b) *Show: the ring of integers $\mathbb{Z}$ is* not *Artinian.*
c) *Show: a quotient of an Artinian ring is Artinian.*
d) *Show: a localization of an Artinian ring is Artinian.*

Obviously any finite ring has only finitely many ideals and is Artinian. It is not difficult to give examples of infinite rings with finitely many ideals. For instance, let k be a field and let $0 \neq f \in k[t]$. Then $R = k[t]/(f)$ has only finitely many

ideals. Indeed, if we factor $f = f_1^{a_1} \cdots f_r^{a_r}$ into irreducible factors, then the Chinese Remainder Theorem gives

$$k[t]/(f) \cong k[t]/(f_1^{a_1}) \times \ldots \times k[t]/(f_r^{a_r}).$$

Each factor ring $k[t]/(f_i^{a_i})$ is a local ring with maximal ideal (f_1), and the ideals are precisely

$$(0) \subsetneq (f_i)^{a_i - 1} \subsetneq \ldots \subsetneq f_i.$$

Since every ideal in a product is a direct sum of ideals of the factors, there are then precisely $\prod_{i=1}^r (a_i + 1)$ ideals of R.

A bit of reflection reveals that – notwithstanding their very similar definitions – requiring (DCC) on ideals of a ring is considerably more restrictive than the (ACC) condition. For instance:

PROPOSITION 8.32. *A domain R is Artinian if and only if it is a field.*

PROOF. Obviously a field satisfies (DCC) on ideals. Conversely, if R is a domain and not a field, there exists a nonzero nonunit element a, and then we have $(a) \supsetneq (a^2) \supsetneq (a^3) \supsetneq \ldots$. Indeed, if $(a^k) = (a^l)$, suppose $k \leqslant l$ and write $l = k + n$, and then we have $ua^k = a^k a^n$ for some $u \in A^\times$, and then by cancellation we get $a^n = u$, so a^n is unit and thus a is a unit, contradiction. □

The result collects several simple but important properties of Artinian rings.

THEOREM 8.33. *Let R be an Artinian ring.*

a) *R has dimension zero: prime ideals are maximal.*
b) *Therefore the Jacobson radical of R coincides with its nilradical.*
c) *The ring R has only finitely many maximal ideals, say $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$.*
d) *Let $\mathcal{N} = \bigcap_{i=1}^n \mathfrak{m}_i$ be the nilradical. Then it is a nilpotent ideal: there is $k \in \mathbb{Z}^+$ such that $\mathcal{N}^k = 0$.*

PROOF. a) If $\mathfrak{p}$ is a prime ideal of A, then $A/\mathfrak{p}$ is an Artinian domain, which by Proposition 8.32 is a field, so $\mathfrak{p}$ is maximal.
b) The Jacobson radical is the intersection of all maximal ideals and the nilradical is the intersection of all prime ideals. So their coincidence follows from part a).
c) Suppose $\mathfrak{m}_i$ is an infinite sequence of maximal ideals. Then

$$R \supsetneq \mathfrak{m}_1 \supsetneq \mathfrak{m}_1 \cap \mathfrak{m}_2 \cdots$$

is an infinite descending chain. Indeed, equality at any step would mean $\mathfrak{m}_{N+1} \supset \bigcap_{i=1}^N \mathfrak{m}_i = \prod_{i=1}^N \mathfrak{m}_i$, and then since $\mathfrak{m}_{N+1}$ is prime it contains $\mathfrak{m}_i$ for some $1 \leqslant i \leqslant N$, contradiction.
d) By DCC, it must be the case that there exists some k with $\mathcal{N}^k = \mathcal{N}^{k+n}$ for all $n \in \mathbb{Z}^+$. Put $I = \mathcal{N}^k$. Suppose $I \neq 0$, and let Σ be the set of ideals J such that $IJ \neq 0$. Evidently $\Sigma \neq \varnothing$, for $I \in \Sigma$. By DCC we are entitled to a minimal element J of Σ. There exists $0 \neq x \in J$ such that $xI \neq 0$. For such an x, we have $(x) \in \Sigma$ and by minimality we must have $J = (x)$. But $(xI)I = xI \neq 0$, so $xI \subseteq (x)$ and thus $xI = (x)$ by minimality. So there exists $y \in I$ with $xy = x$ and thus we have

$$x = xy = xy^2 = \ldots = xy^k = \ldots. \tag{20}$$

But $y \in I \subseteq \mathcal{N}$, so y is nilpotent and (20) gives $x = 0$, a contradiction. □

LEMMA 8.34. *Suppose that in a ring R there exists a finite sequence $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ of maximal ideals such that $0 = \prod_i \mathfrak{m}_i$. Then R is Noetherian if and only if it is Artinian.*

PROOF. Recall from §8.4 that an R-module M is Noetherian and Artinian if and only if it has finite length. Consider

$$0 = \mathfrak{m}_1 \cdots \mathfrak{m}_n \subsetneq \mathfrak{m}_1 \cdots \mathfrak{m}_{n-1} \subsetneq \ldots \subsetneq \mathfrak{m}_1 \subsetneq R.$$

For R to have finite length, it is necessary and sufficient that each quotient

$$Q_i = \mathfrak{m}_1 \cdots \mathfrak{m}_{i-1}/\mathfrak{m}_1 \cdots \mathfrak{m}_i$$

be a finite length R-module. (Since we do not assume that the $\mathfrak{m}_i$'s are distinct, it is possible – and harmless – that some Q_i's may be zero.) But each Q_i is canonically a module over the *field* $R/\mathfrak{m}_i$, i.e., a vector space, so it has finite length if and only if it is finite-dimensional. So we win: R is Noetherian if and only if each Q_i is if and only if each Q_i is finite-dimensional if and only if each Q_i is Artinian if and only if R is Artinian. □

THEOREM 8.35. *(Akizuki-Hopkins) For a ring R, the following are equivalent:*

(i) *R is Artinian.*

(ii) *R is Noetherian, and prime ideals are maximal.*

PROOF. (i) $\implies$ (ii): Suppose R is Artinian. By Theorem 8.33, prime ideals in R are maximal, so it suffices to show that R is Noetherian. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ be the distinct maximal ideals of R. For any $k \in \mathbb{Z}^+$ we have (using CRT) $\prod_{i=1}^n \mathfrak{m}_i^k = \left(\bigcap_{i=1}^n \mathfrak{m}_i\right)^k$. Applying Theorem 8.33d), this shows that for sufficiently large k we have $\prod_{i=1}^n \mathfrak{m}_i^k = 0$. We can now apply Lemma 8.34 to conclude that R is Artinian. (ii) $\implies$ (i): Suppose R is Noetherian and zero-dimensional. A bit later on (sorry!) we will see that any Noetherian ring has only finitely many minimal prime ideals (Theorem 10.14 and again in Corollary 13.21), so R has only finitely many minimal prime ideals, each of which is maximal by zero-dimensionality. Therefore $\mathcal{N} = \bigcap_{i=1}^n \mathfrak{m}_i$ is the nilradical of a Noetherian ring, hence a nilpotent ideal by Proposition 4.12. As above, we deduce that $\prod_{i=1}^n \mathfrak{m}_i^k = 0$ for sufficiently large k. By Lemma 8.34, R is Artinian. □

EXERCISE 8.27. *Consider the ring $R = \mathbb{C}[x,y]/(x^2, xy, y^2) = \mathbb{C}[x,y]/I$.*

a) *Show that $\dim_{\mathbb{C}} R = 3$ and that a $\mathbb{C}$-basis is given by $1 + I$, $x + I$, $y + I$.*

b) *Deduce: R is Artinian.*

c) *Show: the proper ideals of R are precisely the $\mathbb{C}$-subspaces of $\langle x+I, y+I\rangle_{\mathbb{C}}$.*

d) *Deduce: R has infinitely many ideals.*[2]

EXERCISE 8.28. *Let k be a field and $A = k[\{x_i\}_{i=1}^{\infty}]$ a polynomial ring over k in a countable infinite number of indeterminates. Let $\mathfrak{m} = (\{x_i\})$ be the ideal of all polynomials with zero constant term, and put $R = A/\mathfrak{m}^2$. Show that R is a ring with a unique prime ideal which is not Noetherian (so also not Artinian).*

EXERCISE 8.29. *Let $n \in \mathbb{Z}^+$. Suppose R is a Noetherian domain with exactly n prime ideals. Must R be Artinian?*

[2]Indeed, the number of maximal ideals if $\mathfrak{c}$, the cardinality of the continuum. Replacing $\mathbb{C}$ by an arbitrary field k, we find that for every infinite cardinal κ, there is an Artinian ring with κ maximal ideals.

PROPOSITION 8.36. *Let $(R, \mathfrak{m})$ be a Noetherian local ring.*

a) *Either:*
   (i) $\mathfrak{m}^k \neq \mathfrak{m}^{k+1}$ *for all* $k \in \mathbb{Z}^+$, *or*
   (ii) $\mathfrak{m}^k = 0$ *for some* k.

b) *Moreover, condition (ii) holds if and only if R is Artinian.*

PROOF. a) Suppose there exists k such that $\mathfrak{m}^k = \mathfrak{m}^{k+1}$. By Nakayama's Lemma, we have $\mathfrak{m}^k = 0$. If $\mathfrak{p}$ is any prime ideal of R, then $\mathfrak{m}^k \subseteq \mathfrak{p}$, and taking radicals we have $\mathfrak{m} \subseteq \mathfrak{p}$, so $\mathfrak{p} = \mathfrak{m}$ and R is a Noetherian ring with a unique prime ideal, hence an Artinian local ring. b) If R is Artinian, then (i) cannot hold, so (ii) must hold. Conversely, if (ii) holds then $\mathfrak{m}$ is a nil ideal, hence contained in the intersection of all prime ideals of R, which implies that $\mathfrak{m}$ is the only prime ideal of R, and R is Artinian by the Akizuki-Hopkins theorem. □

THEOREM 8.37. *Let R be an Artinian ring.*

a) *There are $n \in \mathbb{Z}^+$ and local Artinian rings $R_1, \ldots, R_n$ such that $R \cong \prod_{i=1}^n R_i$.*

b) *Moreover, the decomposition is unique in the sense that if $R \cong \prod_{j=1}^m S_j$ is another decomposition, then $n = m$ and there exists a permutation σ of $\{1, \ldots, n\}$ such that $R_i \cong S_{\sigma(i)}$ for all i.*

PROOF. a) Let $(\mathfrak{m}_i)_{i=1}^n$ be the distinct maximal ideals of R. We have seen that there exists $k \in \mathbb{Z}^+$ such that $\prod_{i=1}^n \mathfrak{m}_i^k = 0$. By Proposition 4.16, the ideals $\mathfrak{m}_i^k$ are pairwise comaximal, so so $\bigcap_i \mathfrak{m}_i^k = \prod_i \mathfrak{m}_i^k$. Therefore by CRT the natural mapping

$$R \to \prod_{i=1}^n \frac{R}{\mathfrak{m}_i^k}$$

is an isomorphism. Each $\frac{R}{\mathfrak{m}_i^k}$ is local Artinian, so this gives part a).

b) The proof requires **primary decomposition**, so must be deferred to §10.5. □

EXERCISE 8.30. *Let R be an Artinian ring.*

a) *Show: every element of R is either a unit or a zero divisor.*

b) *Show: R is its own total fraction ring.*

EXERCISE 8.31. *Let R be a ring, and let $J(R)$ be its Jacobson radical. The following are equivalent:*

(i) *R is semilocal, i.e.,* $\operatorname{MaxSpec} R$ *is finite.*
(ii) *The ring $R/J(R)$ is a finite product of fields.*
(iii) *The ring $R/J(R)$ has only finitely many ideals.*
(iv) *The ring $R/J(R)$ is Artinian.*

11. The Hilbert Basis Theorem

The following result shows in one fell swoop that the majority of the rings that one encounters in classical algebraic geometry and number theory are Noetherian.

THEOREM 8.38. *(Hilbert Basis Theorem) If R is Noetherian, so is $R[t]$.*

PROOF. Seeking a contradiction, suppose J is an ideal of $R[t]$ which is not finitely generated. We inductively construct a sequence $f_0, f_1, \ldots, f_n, \ldots$ of elements of J and a sequence of ideals $J_n = \langle f_0, \ldots, f_n \rangle$ of $R[t]$ as follows: $f_0 = 0$, and for all $i \in \mathbb{N}$, f_{i+1} is an element of minimal degree in $J \backslash J_i$. Thus for all positive

integers i we have $\deg f_i \leqslant \deg f_{i+1}$. Moreover, for all $i \in \mathbb{Z}^+$ let a_i be the leading coefficient of f_i, and let I be the ideal $\langle a_1, a_2, \ldots, a_N, \ldots \rangle$ of R. However, R is Noetherian, so there exists $N \in \mathbb{Z}^+$ such that $I = \langle a_1, \ldots, a_N \rangle$. In particular, there are $u_1, \ldots, u_N \in R$ such that $a_{N+1} = u_1 a_1 + \ldots + u_N a_N$. Define

$$g = \sum_{i=1}^{N} u_i f_i t^{\deg f_{N+1} - \deg f_i}.$$

Since $g \in J_N$ and $f_{N+1} \in J \backslash J_N$, we have $f_{N+1} - g \in J \backslash J_N$. Moreover g and f_{N+1} have the same degree and the same leading term, so $\deg f_{N+1} - g < \deg f_{N+1}$, hence f_{N+1} does not have minimal degree among polynomials in $J \backslash J_N$, contradiction. □

EXERCISE 8.32. *Prove the converse of the Hilbert Basis Theorem: if R is a ring such that either $R[t]$ or $R[[t]]$ is Noetherian, then R is Noetherian.*

COROLLARY 8.39. *A finitely generated algebra over a Noetherian ring is Noetherian.*

PROOF. Let R be Noetherian and S a finitely generated R-algebra, $S \cong R[t_1, \ldots, t_n]/I$ for some $n \in \mathbb{Z}^+$ and some ideal I. By induction on the Hilbert Basis Theorem, the ring $R[t_1, \ldots, t_n]$ is Noetherian, hence so is its quotient ring S. □

THEOREM 8.40. *Let R be a ring, let $\mathcal{P}$ be a prime ideal of $R[[t]]$, and let $\mathfrak{p}$ be the set of constant coefficients of elements of $\mathcal{P}$.*

a) *Suppose that for some $k \in \mathbb{N}$, $\mathfrak{p}$ can be generated by k elements. Then $\mathcal{P}$ can be generated by $k+1$ elements. Moreover, if $t \notin \mathcal{P}$, $\mathcal{P}$ can be generated by k elements.*

b) *If R is Noetherian, then so is $R[[t]]$.*

PROOF. Let $q : R[[t]] \to R[[t]]/(t) = R$ be the quotient map, so $\mathfrak{p} = q_* \mathcal{P}$.
a) Suppose $\mathfrak{p} = \langle a_1, \ldots, a_k \rangle$, and let I be the ideal $\langle a_1, \ldots, a_k, t \rangle$ of $R[[t]]$.
Case 1: If $t \in \mathcal{P}$, we claim $I = \mathcal{P}$, which suffices. That $I \subseteq \mathcal{P}$ is clear; conversely, writing $f = \sum_{n=0}^{\infty} a_n t^n \in \mathcal{P}$ as $a_0 + t(a_1 + a_2 t + \ldots)$ shows $f \in I$.
Case 2: Suppose $t \notin \mathcal{P}$. Let $f_1, \ldots, f_k \in \mathcal{P}$ with constant terms $a_1, \ldots, a_k$, respectively. We CLAIM $\mathcal{P} = \langle f_1, \ldots, f_k \rangle$. To see this, let $g_1 = \sum_{n=0}^{\infty} b_n t^n \in \mathcal{P}$. Since $b_0 \in \mathfrak{p}$, there are $r_{1,1}, \ldots, r_{k,1} \in R$ with

$$b_0 = r_{1,1} a_1 + \ldots + r_{k,1} a_k,$$

and thus

$$g_1 - (r_{1,1} f_1 + \ldots + r_{k,1} f_k) = t g_2$$

for some $g_2 \in R[[t]]$. Since $\mathcal{P}$ is prime, $t g_2 \in \mathcal{P}$ and $t \notin \mathcal{P}$, we must have $g_2 \in \mathcal{P}$. Applying the above argument to g_2 we find $r_{1,2}, \ldots, r_{k,2} \in R$ and $g_3 \in \mathcal{P}$ such that $g_2 - (r_{1,2} f_1 + \ldots + r_{1,k} f_k) = t g_3$. Continuing in this way, we generate, for $1 \leqslant i \leqslant k$, a power series $h_i = \sum_{n=0}^{\infty} r_{i,n} t^n$, such that

$$g = h_1 f_1 + \ldots + h_k f_k,$$

establishing the claim.
b) If R is Noetherian, then by part a) every prime ideal of $R[[t]]$ is finitely generated. By Cohen's Theorem (Theorem 4.25), $R[[t]]$ is Noetherian. □

EXERCISE 8.33. *Show: for a ring R, the following are equivalent:*

(i) *R is Noetherian.*

(ii) *For all* $n \geqslant 1$, $R[t_1, \ldots, t_n]$ *is Noetherian.*
(iii) *For all* $n \geqslant 1$, $R[[t_1, \ldots, t_n]]$ *is Noetherian.*

EXERCISE 8.34. *Let* k *be a field, and consider the subring* $R = k[y, xy, x^2y, \ldots]$ *of* $k[x, y]$. *Show that* R *is not Noetherian.*

Therefore, a subring of a Noetherian ring need not be Noetherian. Thinking that this ought to be the case is one of the classic "rookie mistakes" in commutative algebra. In general though, it is the exception rather than the rule that a nice property of a ring R is inherited by all subrings of R, and one gets used to this.

12. Monomial Ideals

Let k be a field, and let $R := k[t_1, \ldots, t_N]$.

Let $\mathrm{Mon}(R)$ denote the set of monomials $t_1^{n_1} \cdots t_N^{n_N}$ of R. There is a natural bijection from $\mathrm{Mon}(R)$ to the commutative monoid $\mathbb{N}^N$: $t_1^{n_1} \cdots t_N^{n_N} \mapsto (n_1, \ldots, n_N)$. The set $\mathbb{N}^N$ has a natural, product partial ordering, in which $(m_1, \ldots, m_N) \leqslant (n_1, \ldots, n_N)$ if and only if $m_i \leqslant n_i$ for all $1 \leqslant i \leqslant N$. This is a total ordering if and only if $N = 1$. By transport of structure, we get a natural partial ordering on $\mathrm{Mon}(R)$ that is nothing else than the divisibility relation restricted to monomials.

For $f \in R$, we define the **support** $\mathrm{supp}(f) \subseteq \mathrm{Mon}(R)$ to be the set of monomials appearing in f with nonzero coefficient. For an ideal I of R, let

$$\mathcal{M}(I) := \mathrm{Mon}(R) \cap I$$

be the set of monomials that lie in I. With respect to the aforementioned partial ordering on $\mathrm{Mon}(R)$, the subset $\mathcal{M}(I)$ is an **up-set**: that is, for monomials $m_1 \leqslant m_2$, if $m_1 \in \mathcal{M}(I)$, then also $m_2 \in \mathcal{M}(I)$: this is just because if $m_1 \leqslant m_2$ then $m_2 = m_1 f$ for some $f \in R$.

An ideal I of R is a **monomial ideal** if it can be generated by monomials: that is, if there is $S \subseteq \mathrm{Mon}(R)$ such that $I = \langle S \rangle$. Notice that by the Hilbert Basis Theorem, I has a finite set of generators, but the definition of a monomial ideal allows the set of monomial generators to be infinite, and it is not immediately clear from the definition that a monomial ideal is always generated by a finite set of monomials. But the following result implies that this is the case.

PROPOSITION 8.41. *Let* I *be a monomial ideal of* $R = k[t_1, \ldots, t_N]$, *and let* $f \in R$. *Then* $f \in I$ *if and only if* $m \in I$ *for each monomial* $m \in \mathrm{supp}(f)$.

PROOF. If every monomial in the support of a polynomial f lies in *any* ideal J of R, then evidently f lies in J. Conversely, suppose that $f \in I$. Since I is a monomial ideal there are $m_1, \ldots, m_k \in \mathcal{M}(I)$ and $g_1, \ldots, g_k \in R$ such that

$$f = \sum_{i=1}^{k} g_i m_i.$$

We have

$$\mathrm{supp}(f) \subseteq \bigcup_{i=1}^{k} \mathrm{supp}(g_i m_i).$$

Because $m_i \in \mathcal{M}(I)$, for all $1 \leqslant i \leqslant k$ and all $u \in \mathrm{supp}(g_i m_i)$ we have $m_i \leqslant u$, so $u \in \mathcal{M}(I)$. It follows that $\mathrm{supp}(f) \subseteq \mathcal{M}(I)$, which is what we wanted to show. □

LEMMA 8.42. *Let $\{m_x\}_{x\in X}$ be a set of monomials in $R = k[t_1 \dots, t_N]$, and let m be a monomial in R. Then m lies in $I := \langle m_x \mid x \in X\rangle$ if and only if $m_x \mid m$ for some $x \in X$.*

PROOF. Clearly if $m_x \mid m$ for some $x \in X$, then $m \in I$. Conversely, suppose $m \in I$. Then there are $x_1, \dots, x_n \in X$ and $g_1, \dots, g_n \in R$ such that $m = g_1 m_{x_1} + \dots + g_n m_{x_n}$. Multiplying out the right hand side, we see that every monomial term that appears is divisible by some m_{x_i}, hence the same is true for the left hand side, which is m. □

EXERCISE 8.35. *Let I be an ideal of $R = k[t_1, \dots, t_N]$ with the property of Proposition 8.41: for all $f \in R$, we have $f \in I$ if and only if $m \in I$ for each monomial $m \in \mathrm{supp}(f)$. Show: I is a monomial ideal.*

EXERCISE 8.36. *Let I be a monomial ideal of $R = k[t_1, \dots, t_N]$. Show: $\mathcal{M}(I)$ is a k-basis for I.*

COROLLARY 8.43. *For a subset $M \subseteq \mathrm{Mon}(R)$, let*

$$M^{\uparrow} := \{u \in \mathrm{Mon}(R) \mid m \leqslant u \text{ for some } m \in M\};$$

this is the smallest up-set of $\mathrm{Mon}(R)$ containing M. Then

$$\mathcal{M}(\langle M\rangle) = M^{\uparrow}.$$

PROOF. Since $\mathcal{M}(\langle M\rangle)$ is an up-set in $\mathrm{Mon}(R)$ containing M, it must also contain $M^{\uparrow}$. The proof of the converse is very similar to that of Proposition 8.41 indeed, let m be a monomial in $\langle M\rangle$. We may write

$$m = \sum_{i=1}^{k} g_i m_i$$

with $m_1, \dots, _k \in M$, which shows that $\{m\} = \mathrm{supp}(m) \subseteq M^{\uparrow}$, so $m \in M^{\uparrow}$. □

For each element $\mathbf{n} = (n_1, \dots, n_N) \in \mathbb{N}^N$, the principal downset

$$\mathbf{n}^{\downarrow} := \{(m_1, \dots, m_N) \in \mathbb{N}^N \mid m_i \leqslant n_i \ \forall 1 \leqslant i \leqslant N\}$$

is finite: indeed, it has size $\prod_{i=1}^{N}(n_i + 1)$. In particular, the partially ordered set $\mathbb{N}^N$ is **Artinian**: that is, it has no infinite descending chains. For $S \subseteq \mathbb{N}^N$, let $\min(S)$ be the set of minimal elements of S: i.e., elements that are not strictly smaller than any other element of S.

LEMMA 8.44. *Let $(X, \leqslant)$ be an Artinian partially ordered set, and let $S, T \subseteq X$.*

b) *We have $S^{\uparrow} = (\min S)^{\uparrow}$.*
b) *If $S^{\uparrow} = T^{\uparrow}$, then $\min(S) = \min(T)$.*
c) *We have $\min(S^{\uparrow}) = \min(S)$.*

PROOF. a) For subsets $S \subseteq T \subseteq X$ of any partially ordered set, we have $S^{\uparrow} \subseteq T^{\uparrow}$. If $x \in S^{\uparrow}$ there is $s \in S$ with $s \leqslant x$. Since X is Artinian, there is some $m \in \min(S)$ with $m \leqslant s$. Then $m \leqslant x$, so $x \in (\min S)^{\uparrow}$.
b) By symmetry, it suffices to show that every $s \in \min(S)$ is also a minimal element of T. Since $s \in T^{\uparrow} = (\min T)^{\uparrow}$, there is $t \in \min T$ with $t \leqslant s$. Since $T = S^{\uparrow}$ there is $s' \in S$ with $s' \leqslant t \leqslant s$. Since $s \in \min(S)$ we have $s' = t = s$ and thus $s \in \min T$.
c) For instance, we can apply part b) with $T = S^{\uparrow}$, since $(S^{\uparrow})^{\uparrow} = S^{\uparrow}$. □

Now let $M \subseteq \mathrm{Mon}(R)$, and let $I := \langle M \rangle$ be the associated monomial ideal. If M' is another set of monomial generators for I, then by Corollary 8.43 we have $M^{\uparrow} = (M')^{\uparrow}$, so by Lemma 8.44 we have $\min(M) = \min(M')$ and $I = \langle \min(M) \rangle$. Thus every monomial ideal has a *unique minimal* set of monomial generators, which is precisely the set of minimal elements of any monomial generating set. Moreover, by the Hilbert Basis Theorem we have $I = \langle f_1, \ldots, f_k \rangle$, so by Proposition 8.41, if $M' = \bigcup_{i=1}^{k} \mathrm{supp}(f_i)$, then $M' \subseteq I$ and thus $I = \langle M' \rangle$. So as promised earlier, every monomial ideal has a finite set of monomial generators that is easily determined from any finite set of generators: write out the monomials appearing in the support of the generators in a finite list, and proceeding from left to right, cross out monomials that are multiples of monomials appearing earlier in the list.

This discussion has an important purely order-theoretic consequence:

COROLLARY 8.45 (Dickson's Lemma). *Let $N \in \mathbb{Z}^+$. Each subset of $\mathbb{N}^N$ has finitely many minimal elements.*

PROOF. Let $S \subseteq \mathbb{N}^N$, and let $M_S \subseteq \mathrm{Mon}(R)$ be the corresponding set of monomials. As explained above, the set $\min(M_S)$ is the unique, minimal set of monomial generators for $\langle M_S \rangle$, and it is finite. Our canonical bijection between $\mathbb{N}^N$ and $\mathrm{Mon}(R)$ identifies $\min(S)$ with $\min(M_S)$, so $\min(S)$ is finite. □

EXERCISE 8.37. *A partially ordered set $(X, \leqslant)$ is a **well partial ordering** if it is Artinian and has no infinite antichains: that is, for any infinite subset $Y \subseteq X$ there are elements $y_1, y_2 \in Y$ with $y_1 < y_2$. Show that Dickson's Lemma is equivalent to the assertion that for all $N \in \mathbb{Z}^+$, the product ordering on $\mathbb{N}^N$ is a well partial ordering.*

We have made very little use of k being a field: indeed, Proposition 8.41 and Corollary 8.43 manifestly hold verbatim with k any ring. In order to show that the unique minimal monomial generating set of a monomial ideal was finite, we appealed to the Hilbert Basis Theorem, for which k should be a Noetherian ring. However, after applying this to the case of k a field we got Dickson's Lemma, which we can then turn around and apply to monomial ideals over any coefficient ring k to see that the unique minimal monomial generating set of any monomial ideal is finite.

We will end our discussion of monomial ideals here: in fact it was included mostly as another instance of the interaction between commutative algebra and order theory. But it is no exaggeration to say that the importance of monomial ideals in contemporary commutative algebra is such that one could write an entire book on them. Indeed this has already been done at least twice: [**HH**] and [**MRSW**].

EXERCISE 8.38. *Let k be a field, and let $R = k[t_1, \ldots, t_N]$.*

a) *Show that there is exactly one monomial ideal $\mathfrak{m} \in \mathrm{MaxSpec}\, R$.*
b) *Show that there are precisely 2^N monomial ideals $\mathfrak{p} \in \mathrm{Spec}\, R$ (and find them all).*

EXERCISE 8.39. *Let k be a field, and let $R = k[t_1, \ldots, t_N]$. For a monomial $u = t_1^{a_1} \cdots t_n^{a_n}$, put $\mathrm{rad}(u) := \prod_{i | a_i > 0} t_i$.*

a) *Show: for all $u \in \mathrm{Mon}(R)$, we have $\mathrm{rad}(u) = (\mathrm{rad}(u))$.*
b) *For any subset $S \subseteq \mathrm{Mon}(R)$, show: $\mathrm{rad}\langle S \rangle = \langle \mathrm{rad}(u) \mid u \in S \rangle$.*

c) *Deduce: the radical of a monomial ideal is again a monomial ideal.*
d) *Deduce: there are only finitely many radical monomial ideals. Can you determine the number in terms of N?*

13. The Krull Intersection Theorem

13.1. Preliminaries on Graded Rings.

In the proof of the theorem of this section we will need a little fact about homogeneous polynomials. So here we discuss some rudiments of this theory by embedding it into its natural context: **graded rings**. The notion of graded ring is of the utmost importance in various applications of algebra, from algebraic geometry to algebraic topology and beyond. It would certainly be nice to give a comprehensive exposition of graded algebra but at the moment this is beyond the ambition of these notes, so we content ourselves with the bare minimum needed for our work in the next section.

Let R be a ring, $n \in \mathbb{Z}^+$, and denote by $R[t] = R[t_1, \ldots, t_n]$ the polynomial ring in n indeterminates over R. For a polynomial $P = P(t)$ in several variables, we have the notion of the **degree of P** with respect to the variable t_i: thinking of P as an element of $R[t_1, \ldots, t_{i-1}, t_{i+1}, \ldots, t_n][t_i]$ it is just the largest m such that the coefficient of t_i^m is nonzero, as usual. For any monomial term $c_I t_1^{i_1} \cdots t_n^{i_n}$ we define the **total degree** to be $d = i_1 + \ldots + i_n$.

A nonzero polynomial $P = \sum_I c_I t_1^{i_1} \cdots t_n^{i_n}$ is **homogeneous** if all of its monomial terms have the same total degree, and this common number is called the **degree of the homogeneous polynomial** P. By convention the zero polynomial is regarded as being homogeneous total degree d for all $d \in \mathbb{N}$.

A general polynomial $P \in R[t]$ can be written as a sum of homogeneous polynomials $P = \sum_{d=0}^{\infty} P_d(t)$ with each P_d homogeneous of degree d (and of course $P_d = 0$ for all sufficiently large d). This sum is *unique*. One way to see this is to establish the following more structural fact: for any $d \in \mathbb{N}$, let $P[t]_d$ be the set of all polynomials which are homogeneous of degree d. Then each $P[t]_d$ is an R-submodule of $P[t]$ and we have a direct sum decomposition

$$P[t] = \bigoplus_{d=0}^{\infty} P[t]_d. \tag{21}$$

Moreover, for all $d_1, d_2 \in \mathbb{N}$ we have

$$P[t]_{d_1} \cdot P[t]_{d_2} \subseteq P[t]_{d_1+d_2}. \tag{22}$$

In general, if R is a ring and S is an algebra admitting an R-module direct sum decomposition $S = \bigoplus_{d=0}^{\infty} S_d$ satisfying $S_{d_1} \cdot S_{d_2} \subseteq S_{d_1+d_2}$, then we say that S is an $(\mathbb{N})$-**graded R-algebra**. Taking $R = \mathbb{Z}$ we get the notion of a **graded ring**.

Exercise 8.40. *Let $S = \bigoplus_{d=0}^{\infty} S_d$ be a graded R-algebra. Show: the R-submodule S_0 is in fact an R-algebra.*

Let $S = \bigoplus_{d=0}^{\infty} S_d$ be a graded ring. We say that $x \in S$ is **homogeneous of degree d** if $x \in S_d$. An ideal I of S is **homogeneous** if it has a generating set $I = \langle x_i \rangle$ with each x_i a homogeneous element.

EXERCISE 8.41. *Let S be a graded R-algebra and let I be a homogeneous ideal of S. Show:*

$$S/I = \bigoplus_{d=0}^{\infty} (S_d + I)/I$$

and thus S/I is a graded R-algebra.

Now back to the case of polynomial rings.

LEMMA 8.46. *Let S be a graded ring, let $f_1, \ldots, f_n$ be homogeneous elements of S, and put $I = \langle f_1, \ldots, f_n \rangle$. Let $f \in I$ be homogeneous. Then there are homogeneous elements $g_1, \ldots, g_n \in R$ such that*

$$f = \sum_{i=1}^{n} g_i f_i$$

and for all $1 \leqslant i \leqslant n$,

$$\deg g_i = \deg f - \deg f_i.$$

PROOF. Since $f \in I$, there exist $X_1, \ldots, X_n \in S$ such that

$$f = X_1 f_1 + \ldots + X_n f_n.$$

For each $1 \leqslant i \leqslant n$, let $X_i = \sum_j x_{i,j}$ with $\deg x_{i,j} = j$ be the canonical decomposition of X_i into a sum of homogeneous elements: i.e., $\deg x_{i,j} = j$. Then

$$f = \sum_{d=0}^{\infty} \sum_{i=1}^{n} x_{i,d-\deg f_i} f_i. \tag{23}$$

Since f is homogeneous of degree $\deg(f)$, only the $d = \deg(f)$ in the right hand side of (23) is nonzero, so

$$f = \sum_{i=1}^{n} x_{i,\deg f - \deg f_i} f_i. \qquad \square$$

13.2. The Krull Intersection Theorem.

THEOREM 8.47. *Let R be a Noetherian ring, and I an ideal of R. Suppose there is an element x of R such that $x \in \bigcap_{n=1}^{\infty} I^n$. Then $x \in xI$.*

PROOF. The following miraculously short proof is due to H. Perdry [**Pe04**]. Suppose $I = \langle a_1, \ldots, a_r \rangle$. For each $n \geqslant 1$, since $x \in I^n$ there is a homogeneous degree n polynomial $P_n(t_1, \ldots, t_r) \in R[t_1, \ldots, t_r]$ such that

$$x = P_n(a_1, \ldots, a_r).$$

By the Hilbert Basis Theorem (Theorem 8.38), the ring $R[t_1, \ldots, t_r]$ is Noetherian. Therefore, definining $J_n = \langle P_1, \ldots, P_n \rangle$, there exists N such that $J_N = J_{N+1}$. By Lemma 8.46 we may write

$$P_{N+1} = Q_N P_1 + \ldots + Q_1 P_N,$$

with Q_i homogeneous of degree $i > 0$. Plugging in $t_i = a_i$ for $1 \leqslant i \leqslant n$, we get

$$x = P_{N+1}(a_1, \ldots, a_r) = x \left(Q_1(a_1, \ldots, a_r) + \ldots + Q_N(a_1, \ldots, a_r) \right).$$

Since each Q_i is homogeneous of positive degree, we have $Q_i(a_1, \ldots, a_r) \in I$. $\square$

COROLLARY 8.48. *Let I be an ideal in a Noetherian ring R. Suppose* either

(i) *R is a domain and I is a proper ideal;* or
(ii) *I is contained in the Jacobson radical $J(R)$ of R.*

Then $\bigcap_{n=1}^{\infty} I^n = 0$.

PROOF. Either way, let $x \in \bigcap_{n=1}^{\infty} I^n$ and apply Theorem 8.47 to obtain an element $a \in I$ such that $x = xa$. Thus $(a-1)x = 0$. Under assumption (i), we obtain either $a = 1$ – so $I = R$, contradicting the properness of I – or $x = 0$. Under assumption (ii), $a \in J(R)$ implies $a - 1 \in R^\times$, so that we may multiply through by $(a-1)^{-1}$, again getting $x = 0$.F □

EXERCISE 8.42. *(Suárez-Alvarez) Exhibit an ideal I in a Noetherian ring such that $\bigcap_{n=1}^{\infty} I^n \supsetneq \{0\}$. (Hint: idempotents!)*

EXERCISE 8.43. *Let R be the ring of all C^∞ functions $f : \mathbb{R} \to \mathbb{R}$.*
Let $\mathfrak{m} = \{f \in R \mid f(0) = 0\}$.

a) *Show that $\mathfrak{m} = xR$ is a maximal ideal of R.*
b) *Show that for all $n \in \mathbb{Z}^+$, $\mathfrak{m}^n = \{f \in R \mid f(0) = f'(0) = \ldots = f^{(n-1)}(0)\}$.*
c) *Deduce that $\bigcap_{n=1}^{\infty} \mathfrak{m}^n$ is the ideal of all smooth functions with identically zero Taylor series expansion at $x = 0$. Conclude that $\bigcap_{n=1}^{\infty} \mathfrak{m}^n \neq 0$.*
d) *Let $f(x) = e^{\frac{-1}{x^2}}$ for $x \neq 0$ and 0 for $x = 0$. Show that $f \notin f\mathfrak{m}$.*
e) *Deduce: R is not Noetherian.*

EXERCISE 8.44. *Let $R = \bigcup_{n=1}^{\infty} \mathbb{C}[[t^{\frac{1}{n}}]]$ be the Puiseux series ring. Show that R is a domain with a unique maximal ideal $\mathfrak{m}$ and that for all $n \in \mathbb{Z}^+$, $\mathfrak{m}^n = \mathfrak{m}$. Deduce from the Krull Intersection Theorem that R is not Noetherian.*

The preceding exercise will become much more routine when we study valuation rings in §17. In that language, one can show that if R is a valuation ring with divisible value group, then $(R, \mathfrak{m})$ is a local domain and $\bigcap_{n=1}^{\infty} \mathfrak{m}^n = \mathfrak{m}$.

EXERCISE 8.45 (Kearnes-Oman [**KeOm10**]). *Let I be an ideal in a Noetherian ring R, and suppose that either R is a domain and I is proper or I is contained in the Jacobson radical of R. Show: $\#R \leqslant (\#R/I)^{\aleph_0}$.*
(Suggestion: Show $\#\prod_{n=1}^{\infty} R/I^n \leqslant (\#R/I)^{\aleph_0}$ and apply Krull Intersection.)

The following exercise was conveyed to me by J.H. Silverman.

EXERCISE 8.46. *Let $(R, \mathfrak{m})$ be a local ring with residue field $k = R/\mathfrak{m}$. Let $n \in \mathbb{Z}^+$ be indivisible by the characteristic of k (i.e., $n \cdot 1$ is a unit in k), and let*

$$\mu_n(R) \coloneqq \{x \in R \mid x^n = 1\}$$

be the group of nth roots of unity in R.

a) *Show:*

$$\mu_n(R) \cap (1 + \mathfrak{m}) \subseteq \bigcap_{k=1}^{\infty} \mathfrak{m}^l.$$

(Hint: Let $r \in \mathbb{Z}^+$, and let $y \in \mathfrak{m}^r$ be such that $(1+y)^n = 1$. Show: $y \in \mathfrak{m}^{2r}$.)
b) *Deduce: if R is Noetherian, then $\mu_n(R) \cap (1 + \mathfrak{m}) = \{1\}$.*
c) *Exhibit a Noetherian local ring $(R, \mathfrak{m})$ of residue characteristic $p > 0$ such that $\mu_p(R) \cap (1 + \mathfrak{m}) \supsetneq \{1\}$.*
d) *(Open) Must we have $\mu_n(R) \cap (1 + \mathfrak{m}) = \{1\}$ if R is not Noetherian?*

14. Krull's Principal Ideal Theorem

THEOREM 8.49. *(The Principal Ideal Theorem, a.k.a. Krull's Hauptidealsatz) Let x be a nonunit in a Noetherian ring R, and let $\mathfrak{p}$ be minimal among prime ideals containing x. Then $\mathfrak{p}$ has height at most one.*

Remark: A prime $\mathfrak{p}$ which is minimal among primes containing x will be called a **minimal prime over x**. Note that an equivalent condition is that $\mathfrak{p}$ is a minimal prime in the quotient ring $R/(x)$. Note also that if x is nilpotent, every prime of $\mathfrak{p}$ contains x so the height of any minimal prime is 0.

Our strategy of proof follows Kaplansky, who follows D. Rees. We need a preliminary result:

LEMMA 8.50. *Let u and y be nonzero elements in a domain R. Then:*

a) *The R-modules $\langle u, y\rangle/(u)$ and $\langle u^2, uy\rangle/(u^2)$ are isomorphic.*
b) *If we assume further that for all $t \in R$, $tu^2 \in (y)$ implies $tu \in (y)$, then the R-modules $(u)/(u^2)$ and $\langle u^2, y\rangle/\langle u^2, uy\rangle$ are isomorphic.*

PROOF. a) The isomorphism is simply induced by multiplication by u.
b) The module $(u)/(u^2)$ is cyclic with annihilator (u), and conversely any such module is isomorphic to $R/(u)$. Moreover $M := \langle u^2, y\rangle/\langle u^2, uy\rangle$ is also cyclic, being generated simply by y. Certainly u annihilates M, so it suffices to show that the annihilator is exactly (u). More concretely, given $ky = au^2 + buy$, we must deduce that $k \in (u)$. But we certainly have $au^2 \in (y)$, so by hypothesis $au \in (y)$, say $au = cy$. Then $ky = cuy + buy$. Since $0 \neq y$ in our domain R, we may cancel y to get $k = (c + b)u \in (u)$. □

Proof of Krull's Hauptidealsatz: Under the given hypotheses, assume for a contradiction that we have

$$\mathfrak{p}_2 \subsetneq \mathfrak{p}_1 \subsetneq \mathfrak{p}.$$

Note first that we can safely pass to the quotient $R/\mathfrak{p}_2$ and thus assume that R is a domain. Dually, it does not hurt any to localize at $\mathfrak{p}$. Therefore we may assume that we have a Noetherian local domain R with maximal ideal $\mathfrak{m}$, an element $x \in \mathfrak{m}$, and a nonzero prime ideal, say $\mathfrak{p}$, with $x \in \mathfrak{p} \subsetneq \mathfrak{m}$, and our task is now to show that this setup is impossible. Now for the clever part: let $0 \neq y$ be any element of $\mathfrak{p}$, and for $k \in \mathbb{Z}^+$, let I_k denote the ideal of all elements t with $tx^k \in (y)$. Then $\{I_k\}_{k=1}^{\infty}$ is an ascending chain of ideals in the Noetherian ring R so must stabilize, say at $k = n$. In particular, $tx^{2n} \in (y)$ implies $tx^n \in (y)$. Putting $u = x^n$, we have $tu^2 \in (y)$ implies $(tu) \in (y)$.

Since $\mathfrak{m}$ is a minimal prime over (x), the quotient ring $T = R/(u^2)$ has exactly one prime ideal, $\mathfrak{m}$, and is therefore, by the Akizuki-Hopkins Theorem, an Artinian ring, so that any finitely generated T-module has finite length. In particular, $M := \langle u, y\rangle/(u^2)$, which can naturally be viewed as a T-module, has finite length, and hence so does its T-submodule $M' := \langle u^2, y\rangle/(u^2)$. Put $N = \langle u^2, y\rangle\langle u^2, uy\rangle$. Then

$$\ell(M') = \ell(N) + \ell(\langle u^2, uy/(u^2)) = \ell((u)/(u^2)) + \ell(\langle u, y\rangle/(u)) = \ell(M);$$

in the second equality we have used Lemma 8.50. The only way that M could have the same length as its submodule M' is if $\langle u, y\rangle = \langle u^2, y\rangle$, i.e., if there exist $c, d \in R$ such that $u = cu^2 + dy$, or $u(1 - cu) = -dy$. Since u lies in the maximal ideal of

the local ring R, $1 - cu \in R^\times$, and thus $u \in (y) \subseteq \mathfrak{p}$. But $\mathfrak{m}$ is minimal over x and hence, being prime, also minimal over $u = x^n$, contradiction! $\square$

COROLLARY 8.51. *With hypotheses as in Theorem 8.49, suppose that x is not a zero-divisor. Then any prime $\mathfrak{p}$ which is minimal over x has height one.*

EXERCISE 8.47. *Use the Akizuki-Hopkins theorem and Proposition 8.36 to give a proof of Corollary 8.51.*

Again we need a small preliminary result.

LEMMA 8.52. *(Prime Avoidance) Let R be a ring, and $I_1, \ldots, I_n, J$ be ideals of R. Suppose that all but at most two of the I_i's are prime and that $J \subseteq \bigcup_{i=1}^n I_i$. Then $J \subseteq I_i$ for some i.*

PROOF. We go by induction on n, the case $n = 1$ being trivial.
$n = 2$: Seeking a contradiction, suppose there is $x_1 \in J \backslash I_2$ and $x_2 \in J \backslash I_1$. Since $J \subseteq I_1 \cup I_2$ we must have $x_1 \in I_1$ and $x_2 \in I_2$. Then $x_1 + x_2 \in J \subseteq I_1 \cup I_2$. If $x_1 + x_2 \in I_1$, then since $x_1 + x_2, x_1 \in I_1$, so is x_2, contradiction; whereas if $x_1 + x_2 \in I_2$, then since $x_1 + x_2, x_2 \in I_1$, so is x_1.[3]
$n \geqslant 3$: We may suppose that I_n is prime and also that for all proper subsets $S \subseteq \{1, \ldots, n\}$, $J \nsubseteq \bigcup_{i \in S} I_i$; otherwise we would be done by induction. So for $1 \leqslant i \leqslant n$, there is $x_i \in J \backslash \bigcup_{j \neq i} I_j$, and then $x_i \in I_i$. Consider $x = x_1 \cdots x_{n-1} + x_n$. Then $x \in J$, so $x \in I_i$ for some i.
Case 1: $x \in I_n$. Then since $x_n \in I_n$, $x_1 \cdot x_{n-1} \in I_n$, and since I_n is prime $x_i \in I_n$ for some $1 \leqslant i \leqslant n-1$, contradiction.
Case 2: $x \in I_j$ for some $1 \leqslant j \leqslant n-1$. Then $x_1 \cdots x_{n-1} \in I_j$, so $x_n \in I_j$, contradiction. $\square$

EXERCISE 8.48. *(*[**CDVM13**, Prop. 2.2]*) Let R be a UFD and not a field. Suppose $R^\times$ is finite. Show: R has infinitely many principal prime ideals.*
*(*HINT: *Suppose R has finitely many principal nonzero principal prime ideals, say $(\pi_1), \ldots, (\pi_n)$. Let $\mathfrak{m} \in \operatorname{MaxSpec} R$. By choosing $x \in \mathfrak{m}^\bullet$ and applying unique factorization, show $\mathfrak{m} \subseteq \bigcup_{i=1}^n (\pi_i)$. Apply Prime Avoidance and then Theorem 4.24.)*

We can now give a striking structural result about primes in a Noetherian ring. First a piece of notation: for any elements x, y in a partially ordered set S we define the "interval" (x, y) to be the set of all $z \in S$ such that $x < z < y$. For prime ideals $\mathfrak{p}$ and $\mathfrak{q}$, we denote by $(\mathfrak{p}, \mathfrak{q})$ the set of all prime ideals $\mathcal{P}$ with $\mathfrak{p} \subseteq \mathcal{P} \subseteq \mathfrak{q}$.

COROLLARY 8.53. *Let $\mathfrak{p} \subseteq \mathfrak{q}$ be prime ideals in a Noetherian ring R. Then the interval $(\mathfrak{p}, \mathfrak{q})$ is either empty or infinite.*

PROOF. As usual, by correspondence we may pass to $R/\mathfrak{p}$ and therefore assume that $\mathfrak{p} = 0$. Suppose that for some $n \geqslant 1$ we have $(0, \mathfrak{q}) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$. By Prime Avoidance (Lemma 8.52) we cannot then have $\mathfrak{q} \subseteq \bigcup_{i=1}^n \mathfrak{p}_i$, so choose $x \in \mathfrak{q} \backslash \bigcup_{i=1}^n \mathfrak{p}_i$. Then $\mathfrak{q}$ is a prime of R, of height at least 2, which is minimal over (x), contradicting Theorem 8.49. $\square$

In particular, if R is Noetherian and $\operatorname{Spec} R$ is finite, then $\dim R \leqslant 1$.

[3] In fact this works for any subgroups I_1, I_2, J of a group G with $J \subseteq I_1 \cup I_2$.

THEOREM 8.54. *(Generalized Principal Ideal Theorem) Let R be a Noetherian ring, and let $I = \langle a_1, \ldots, a_n \rangle$ be a proper ideal of R. Let $\mathfrak{p}$ be a minimal element of the set of all prime ideals containing I. Then $\mathfrak{p}$ has height at most n.*

PROOF. As usual, we may localize at $\mathfrak{p}$ and suppose that R is local with $\mathfrak{p}$ as its maximal ideal. Suppose to the contrary that there exists a chain $\mathfrak{p} = \mathfrak{p}_0 \supsetneq \mathfrak{p}_1 \supsetneq \ldots \supsetneq \mathfrak{p}_{n+1}$. Because R is Noetherian, we may arrange for $(\mathfrak{p}_1, \mathfrak{p}) = \varnothing$. Because $\mathfrak{p}$ is minimal over I, I cannot be contained in $\mathfrak{p}_1$; without loss of generality we may suppose that a_1 is not in $\mathfrak{p}_1$. Put $J := \langle \mathfrak{p}_1, a_1 \rangle$; then J strictly contains $\mathfrak{p}_1$ so $\mathfrak{p}$ is the unique prime of R containing J. So the ring R/J is an Artin local ring, and then by Proposition 8.36 for sufficiently large k we have $\mathfrak{p}^k \subseteq J$. Then by taking t to be sufficiently large we can write, for $2 \leqslant i \leqslant n$,

$$a_i^t = c_i a_1 + b_i,\ c_i \in R, b_i \in \mathfrak{p}_1.$$

Put $K = \langle b_2, \ldots, b_n \rangle \subseteq \mathfrak{p}_1$. Since the height of $\mathfrak{p}_1$ exceeds $n-1$, by induction on n we may assume that $\mathfrak{p}_1$ properly contains a prime ideal Q which contains J. The ideal $Q' := \langle a_1, Q \rangle$ contains some power of each a_i and therefore $\mathfrak{p}$ is the unique prime ideal containing Q'. So in the quotient R/Q, the prime $\mathfrak{p}/Q$ is minimal over the principal ideal Q'/Q. By Krull's Hauptidealsatz (Theorem 8.49) $\mathfrak{p}/Q$ has height 1. On the other hand, we have $\mathfrak{p}/Q \supsetneq \mathfrak{p}_1/Q \supsetneq 0$, a contradiction. □

Thus every prime ideal in a Noetherian ring has finite height. More precisely:

COROLLARY 8.55. *Let R be a Noetherian ring, and let $\mathfrak{p} \in \operatorname{Spec} R$ be a non-minimal prime ideal. Then the height of $\mathfrak{p}$ is the least $n \in \mathbb{Z}^+$ such that there are $x_1, \ldots, x_n \in \mathfrak{p}$ such that $\mathfrak{p}$ is a minimal prime over the ideal $\langle x_1, \ldots, x_n \rangle$.*

PROOF. Let $\mathfrak{p}$ have height $m \geqslant 1$, and let n be the least positive integer such that $\mathfrak{p}$ is a minimal prime over an ideal with n generators. By Theorem 8.54 we have $m \leqslant n$. Conversely, we'll show that $n \leqslant m$ by induction on m: suppose the claim holds for every prime ideal in a Noetherian ring of height less than m. By Corollary 4.32b), the set of minimal primes of R is finite, so by Prime Avoidance (Lemma 8.52) there is x_1 that lies in $\mathfrak{p}$ and does not lie in any minimal prime of R, so any prime ideal containing x_1 has positive height, so any finite chain of prime ideals in R with smallest element $\mathfrak{p}$ can be extended in length by adjoining a minimal prime contained in $\mathfrak{p}$ (which exists by Proposition 4.26). It follows that the ideal $\mathfrak{p}/\langle x_1 \rangle$ of $R/\langle x_1 \rangle$ has height at most $m-1$. By induction, there are $\overline{x_2}, \ldots, \overline{x_m} \in \mathfrak{p}/\langle x_1 \rangle$ such that $\mathfrak{p}/\langle x_1 \rangle$ is a minimal prime over $\langle \overline{x_2}, \ldots, \overline{x_m} \rangle$ in $R/\langle x_1 \rangle$. For $2 \leqslant i \leqslant m$, lifting each $\overline{x_j}$ to $x_j \in \mathfrak{p}$, we get that $\mathfrak{p}$ is a minimal prime over $\langle x_1, \ldots, x_m \rangle$ in R. □

Suppose in particular that $(R, \mathfrak{m})$ is a Noetherian local ring of dimension n. By Corollary **??** there are $x_1, \ldots, x_n \in \mathfrak{m}$ such that $\operatorname{rad}\langle x_1, \ldots, x_n \rangle = \mathfrak{m}$. (In the terminology of Chapter 10, this means that the ideal $\langle x_1, \ldots, x_n \rangle$ is $\mathfrak{m}$-primary.) The finite sequence $x_1, \ldots, x_n$ is then called a **system of parameters** of $\mathfrak{m}$.

An important special case of the Generalized Principal Ideal Theorem is that if $\mathfrak{p}$ is a height n prime in a Noetherian ring, then $\mathfrak{p}$ requires at least n generators. It is natural to ask about the converse, and this certainly need not be true. For instance, we will see in §15.1 that a Noetherian domain is a UFD if and only if every height one prime is principal – most Noetherian domains are *not* UFDs. It is especially important to ask this question after localization: if $(R, \mathfrak{m})$ is a Noetherian local ring of dimension n, then there are $x_1, \ldots, x_n$ such that the radical of

$\langle x_1, \ldots, x_n \rangle$ is $\mathfrak{m}$, but when can we find $x_1, \ldots, x_n$ such that $\langle x_1, \ldots, x_n \rangle = \mathfrak{m}$? By Nakayama's Lemma, the minimal number of generators for $\mathfrak{m}$ is

$$z(R) := \dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2,$$

so for a Noetherian local ring R we have

$$z(R) \leqslant \dim R$$

and are asking about equality. By definition, equality holds if R is a **regular local ring**. Moreover, a Noetherian ring R is **regular** if for all $\mathfrak{m} \in \operatorname{MaxSpec} R$, the localization $R_{\mathfrak{m}}$ is a regular local ring. Regularity is a vitally important concept in commutative algebra and algebraic geometry: it is perhaps the first example of a purely algebraic concept that must be appreciated geometrically to be properly understood, which makes it mostly out of scope of the present text.

However, let us at least discuss two important examples; we will quote some later results in this text. Let k be a field. First consider the polynomial ring $R_n := k[t_1, \ldots, t_n]$. Then every maximal ideal of R_n has height n (Theorem 14.31) and can be generated by n elements (Theorem 12.21). In particular the ring R_n is regular (with room to spare: in this ring, maximal ideals $\mathfrak{m}$ are *globally* generated by $\operatorname{ht} \mathfrak{m}$ elements, whereas for regularity they only need to be *locally* generated by $\operatorname{ht} \mathfrak{m}$ elements). Also R_n is a UFD (§15.6), so every height one prime of R_n is principal (Corollary 15.2a)). Thus if $n \leqslant 2$ then indeed every prime ideal $\mathfrak{p}$ of R_n can be generated by $\operatorname{ht}(\mathfrak{p})$ elements. The early algebraist F.S. Macaulay showed in 1916 that for all $r \in \mathbb{Z}^{\geqslant 2}$ there is a height 2 prime ideal in $\mathbb{C}[t_1, t_2, t_3]$ that needs at least r generators. See [**Ab73**] for a modern take on this, with $\mathbb{C}$ replaced by any algebraically closed field. I expect that for any field k and $h, k, r \in \mathbb{Z}^+$ with $2 \leqslant h \leqslant n-1$ there is a prime ideal $\mathfrak{p} \in k[t_1, \ldots, t_n]$ of height h and needing at least r generators: it would be nice to have a reference.

Now let $n \geqslant 2$ and let $f \in k[t_1, \ldots, t_n]$ be a polynomial of degree at least 2 having no constant and no linear term, and consider the ring $R_f := k[t_1, \ldots, t_n]/(f)$. By Krull's Hauptidealsatz, every minimal prime of R_f is a height one prime of $R = k[t_1, \ldots, t_n]$; since every maximal ideal of R has height n, every maximal ideal of R_f has height $n-1$ and thus R_f has dimension $n-1$. The maximal ideal $\mathfrak{m} := \langle t_1, \ldots, t_n \rangle$ of R contains f, so $\overline{\mathfrak{m}} := \mathfrak{m} + (f)$ is a maximal ideal of R_f. Clearly it is still generated by the images of $t_1, \ldots, t_n$, but we claim that even in the localization $(R_f)_{\overline{\mathfrak{m}}}$ the maximal ideal $\overline{\mathfrak{m}}_{\overline{\mathfrak{m}}}$ requires n generators, so R_f is not a regular ring. Again, by Nakayama the minimal number of generators of $\overline{\mathfrak{m}}_{\overline{\mathfrak{m}}}$ is $\dim_{R_f/\overline{\mathfrak{m}}} \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2$. We have $R_f/\overline{\mathfrak{m}} = R/\mathfrak{m} = k$ and $f \in \mathfrak{m}^2$, so the natural map

$$\mathfrak{m}/\mathfrak{m}^2 \to \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2$$

is a k-vector space isomorphism. It follows that the minimal number of generators for $\overline{\mathfrak{m}}_{\overline{\mathfrak{m}}}$ is n, so $(R_f)_{\overline{\mathfrak{m}}}$ is not a regular local ring.

EXERCISE 8.49. *Let R be a Noetherian ring.*

a) *Suppose R is semilocal. Show:* $\dim R$ *is finite.*
b) *Suppose R is local, with maximal ideal $\mathfrak{m}$. Show:* $\dim R$ *is the least $n \in \mathbb{N}$ such that that there are $x_1, \ldots, x_n$ with* $\operatorname{rad}\langle x_1, \ldots, x_n \rangle = \mathfrak{m}$.

EXERCISE 8.50. *Let k be a field. Let $R = k[t_1, \ldots, t_n, \ldots]$ be a polynomial ring over k in a countably infinite set of indeterminates. Find a prime ideal of R of infinite height.*

However, it does not follow from Theorem 8.54 that a Noetherian ring necessarily has finite Krull dimension, and in fact this is false: the first counterexample was constructed by Nagata in 1962.

15. The Dimension Theorem

THEOREM 8.56. *Let R be a ring.*

a) *Let $\mathcal{M}$ be a maximal ideal in $R[t]$, and **suppose** that its contraction $\mathfrak{m} := \mathcal{M} \cap R$ is maximal in R. Then $\mathcal{M}$ can be generated by $\mathfrak{m}$ and by one additional element f, which can be taken to be a monic polynomial which maps modulo $\mathfrak{m}$ to an irreducible polynomial in $R/\mathfrak{m}[t]$.*

b) *If, moreover, we suppose that $R/\mathfrak{m}$ is algebraically closed, then $\mathcal{M} = \langle \mathfrak{m}, t - a \rangle$ for some $a \in R$.*

PROOF. a) Since $\mathcal{M}$ contains $\mathfrak{m}$, by correspondence $\mathcal{M}$ may be viewed as a maximal ideal of $R[t]/\mathfrak{m}R[t] \cong (R/\mathfrak{m})[t]$, a PID, so corresponds to an irreducible polynomial $\overline{f} \in R/\mathfrak{m}[t]$, which we may take to be monic. If f is any monic lift of f to $R[t]$, then $\mathcal{M} = \langle \mathfrak{m}, f \rangle$. Part b) follows immediately from the observation that an irreducible univariate polynomial over an algebraically closed field is linear. □

The following result covers the other extreme.

THEOREM 8.57. *Let R be a domain, with fraction field K. Let $\iota : R[t] \to K[t]$ be the natural inclusion. Then ι_* and ι^* induce mutually inverse bijections between the set of prime ideals $\mathcal{P}$ of $R[t]$ such that $\mathcal{P} \cap R = (0)$ and the set of prime ideals of $K[t]$. It follows that every nonzero prime ideal $\mathcal{P}$ of $R[t]$ such that $\mathcal{P}capR = (0)$ has height one.*

PROOF. Let $S := R^\bullet$. The key observation is that $S^{-1}R[t] = K[t]$. A prime ideal $\mathcal{P}$ of $R[t]$ is disjoint from S if and only if $\mathcal{P} \cap R = (0)$, so by Proposition 7.6 and Corollary 7.7, the maps ι_* and ι^* are mutually inverse bijections from the set of $\mathcal{P} \in \operatorname{Spec} R[t]$ such that $\mathcal{P} \cap R = (0)$ to the set of prime ideals of $K[t]$. Moreover the bijections ι_* and ι^* are height-preserving: they are order-preserving, and if $\mathcal{P}$ is disjoint from S then so is every prime ideal contained in $\mathcal{P}$. So the last statement follows because in the PID $K[t]$, every nonzero prime ideal has height one. □

COROLLARY 8.58. *Let R be a domain, let I be an ideal of $R[t]$ and let $\mathcal{P}$ be a prime ideal of $R[t]$ such that $(0) \subsetneq \mathcal{P} \subsetneq I$. Then $I \cap R \neq (0)$.*

PROOF. Seeking a contradiction, suppose that $I \cap R = (0)$. Then I is disjoint from $R^\bullet$, so by Multiplicative Avoidance I is contained in a prime ideal $\mathcal{Q}$ that is disjoint from $R^\bullet$. Then $\mathcal{Q} \supsetneq \mathcal{P} \supsetneq (0)$ shows that $\mathcal{Q}$ is a prime ideal of $R[t]$ of height at least two such that $\mathcal{Q} \cap R = (0)$, contradicting Theorem 8.57. □

LEMMA 8.59. *Let R be a ring, and let $I_1 \subsetneq \mathcal{P} \subsetneq I_2$ be ideals of R with $\mathcal{P}$ a prime ideal. Then $I_1 \cap R \subsetneq I_2 \cap R$.*

PROOF. The conclusion certainly holds if $I_1 \cap R \subsetneq \mathcal{P} \cap R$, so we may assume

$$\mathfrak{p} := \mathcal{P} \cap R = I_1 \cap R \in \operatorname{Spec} R.$$

We may replace R by $R/\mathfrak{p}$ and $R[t]$ by $R[t]/\mathfrak{p}R[t] = (R/\mathfrak{p})[t]$ and thereby assume that R is a domain and $I_1 \cap R = \mathcal{P} \cap R = (0)$. Corollary 8.58 applies to show that $I_2 \cap R \neq (0)$, so $I_1 \cap R \subsetneq I_2 \cap R$. □

THEOREM 8.60 (Dimension Theorem). *Let R be a ring of finite Krull dimension d, and let $n \in \mathbb{Z}^+$.*

a) *We have $d + 1 \leqslant \dim R[t] \leqslant 2d + 1$.*

b) *Suppose that R is Noetherian. Then*

$$\dim R[t_1, \ldots, t_n] = d + n.$$

c) *Suppose that R is Noetherian. Then*

$$\dim R[[t_1, \ldots, t_n]] = d + n.$$

PROOF. a) Since R has dimension d, there is a chain $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_d$ of prime ideals in R. Since for every $\mathfrak{p} \in \operatorname{Spec} R$ we have $R[t]/\mathfrak{p}R[t] = (R/\mathfrak{p})[t]$, which is a domain, also $\mathfrak{p}R[t] \in \operatorname{Spec} R[t]$. Since $(\mathfrak{p}R[t]) \cap R = \mathfrak{p}$, it follows that $\mathfrak{p}_0 R[t] \subsetneq \ldots \subsetneq \mathfrak{p}_d R[t]$ is a chain of prime ideals in $R[t]$ of length d. Moreover $\langle \mathfrak{p}_d R[t], t \rangle$ is a prime ideal of $R[t]$ properly containing $\mathfrak{p}_d R[t]$, so $\dim R[t] \geqslant d + 1$.

Now let $\mathcal{P}_0 \subsetneq P_1 \subsetneq \ldots \subsetneq \mathcal{P}_r$ be a chain of prime ideals of $R[t]$ of length $r \geqslant 1$. If r is even, then by Lemma 8.59, we have that

$$\mathcal{P}_0 \cap R \subsetneq \mathcal{P}_2 \cap R \subsetneq \ldots \subsetneq \mathcal{P}_r \cap R$$

is a chain of prime ideals of R of length $\frac{r}{2}$, so $r \leqslant 2d$. Similarly, if r is odd then by Lemma 8.59 we have that

$$\mathcal{P}_0 \cap R \subsetneq \mathcal{P}_2 \cap R \subsetneq \ldots \subsetneq \mathcal{P}_{r-1} \cap R$$

is a chain of prime ideals of R of length $\frac{r-1}{2}$, so $r \leqslant 2d+1$. Thus $\dim R[t] \leqslant 2d+1$.
b) Suppose R is Noetherian. By induction and the Hilbert Basis Theorem it is enough to show that $\dim R[t] = d+1$, and by part a) we know that $\dim R[t] \geqslant d+1$. Let $\mathcal{P} \in \operatorname{Spec} R[t]$. By Corollary 8.55 (note that we use here that R is Noetherian), it is enough to show that $\mathcal{P}$ is minimal over an ideal I that can be generated by at most $d + 1$ elements.

Let $\mathfrak{p} := \mathcal{P} \cap R$. Since $\mathfrak{p}$ has height $d' \leqslant d$, by Corollary 8.55 there are $x_1, \ldots, x_{d'} \in R$ such that $\mathfrak{p}$ is a minimal prime over $I := \langle x_1, \ldots, x_{d'} \rangle$.

Let $\mathcal{P}_1$ be a prime ideal of $R[t]$ such that

$$IR[t] \subseteq \mathcal{P}_1 \subseteq \mathfrak{p}R[t],$$

so $\mathcal{P}_1 \subseteq \mathcal{P}$. Then $I \subseteq \mathcal{P}_1 \cap R \subseteq \mathcal{P} \cap R = \mathfrak{p}$, so $\mathcal{P}_1 \cap R = \mathfrak{p}$ and $\mathcal{P}_1 = \mathfrak{p}R[t]$. Thus $\mathfrak{p}R[t]$ is a minimal prime over $IR[t]$. Since $IR[t]$ can be generated by d' elements, $\mathfrak{p}R[t]$ has height at most $d' \leqslant d$. Thus if $\mathfrak{p}R[t] = \mathcal{P}$, then $\mathcal{P}$ has height at most d.

Now suppose that $\mathfrak{p}R[t] \subsetneq \mathcal{P}$, let $f \in \mathcal{P} \backslash \mathfrak{p}R[t]$, and let $\mathcal{Q}$ be a minimal prime over $IR[t] + (f) = \langle a_1, \ldots, a_d, f \rangle$ that is contained in $\mathcal{P}$. Since $I \subseteq \mathcal{Q} \cap R \subseteq \mathfrak{p}$ and $\mathfrak{p}$ is minimal over I, we have $\mathcal{Q} \cap R = \mathfrak{p}$ and thus $\mathfrak{p}R[t] \subseteq \mathcal{Q}$. Indeed, because $f \in \mathcal{Q} \backslash \mathfrak{p}R[t]$ we have $\mathfrak{p}R[t] \subsetneq \mathcal{Q}$. Since

$$(\mathfrak{p}R[t]) \cap R = \mathcal{Q} \cap R = \mathcal{P} \cap R,$$

Lemma 8.59 gives $\mathcal{Q} = \mathcal{P}$, and thus $\mathcal{P}$ is minimal over $\langle a_1, \ldots, a_d, f \rangle$ so has height at most $d + 1$.
c) Again, induction and the power series analogue of the Hilbert Basis Theorem (Theorem 8.40b) reduces us to the case of $n = 1$. Let $\mathcal{M} \in \operatorname{MaxSpec} R[[t]]$. We claim that $t \in \mathcal{M}$. Indeed, this is equivalent to showing that t lies in the Jacbson radical of $R[[t]]$. which by Proposition 4.18 is equivalent to showing that for all $f \in R[[t]]$ we have $1 - ft \in R[[t]]^\times$. But an element $\sum_{n=0}^{\infty} a_n t^n$ of $R[[t]]$ is a unit if and only if the constant coefficient a_0 is a unit of R, and the constant coefficient of $1 - ft$

is 1, establishing the claim. Then Theorem 8.40a) tells us that if $\mathfrak{m} := \mathcal{M} \cap R$ is the set of constant coefficients of elements of $\mathcal{M}$, then $\mathcal{M} = \langle \mathfrak{m}, t \rangle$. Since $\mathcal{M}$ is maximal and $R[[t]]/\mathcal{M} \cong R/\mathfrak{m}$, also $\mathfrak{m}$ is a maximal ideal of the Noetherian ring R. Suppose $\mathfrak{m}$ has height h (so $h \leqslant d = \dim R$). Then there is a chain

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_h = \mathfrak{m}$$

of prime ideals of R. For any $\mathfrak{p} \in \operatorname{Spec} R$, we have $R[[t]]/\mathfrak{p}R[[t]] \cong (R/\mathfrak{p})[[t]]$ is a power series ring over a domain, hence a domain, so $\mathfrak{p}R[[t]]$ is a prime ideal. Also if $I \subsetneq J$ are ideals of R then $IR[t]] \subsetneq JR[[t]]$ are ideals of $R[[t]]$, so

$$\mathfrak{p}_0 R[[t]] \subsetneq \mathfrak{p}_1 R[[t]] \subsetneq \ldots \subsetneq \mathfrak{p}_h R[[t]] \subseteq \mathcal{M}$$

shows that $\mathcal{M}$ has height at least $h+1$, and it follows that $\dim R[[t]] \geqslant d+1$.

To complete the proof it suffices to show that $\mathcal{M}$ has height at most $h+1$. As we saw in §8.13, the height of any maximal ideal M in a Noetherian ring A is the minimal $h \in \mathbb{N}$ such that there are $x_1, \ldots, x_h \in A$ such that $M = \operatorname{rad}\langle x_1, \ldots, x_h \rangle$, or equivalently such that M is the only prime ideal of A containing $x_1, \ldots, x_h$. Applying this remark to the height h maximal ideal $\mathfrak{m}$ of R, there are $x_1, \ldots, x_h \in R$ such that $\mathfrak{m} = \operatorname{rad}\langle x_1, \ldots, x_h \rangle$. We claim that $\mathcal{M} = \operatorname{rad}\langle x_1, \ldots, x_h, t \rangle$, which will therefore show that $\mathcal{M}$ has height at most $d+1$. Establishing the claim is easy: if $\mathcal{P}$ is any prime ideal of $R[[t]]$ containing $x_1, \ldots, x_h, t$ then for any $x \in R$ and $n \in \mathbb{Z}^+$ such that $x^n \in \langle x_1, \ldots, x_h \rangle_R$ we have $x^n \in \mathcal{P}$ hence $x \in \mathcal{P}$; thus $\mathcal{P}$ contains $\mathfrak{m}$, and by assumption it contains t, so it contains $\langle \mathfrak{m}, t \rangle = \mathcal{M}$. □

The proofs of parts b) and c) of Theorem 8.60 use Corollary 8.55, whch is one of the deeper results in this text. In contrast, the proof of part a) is much more elementary. If I didn't know any better, comparing parts a) and b) would make me want to work harder to try to show that $\dim R[t] = 1 + \dim R$ for any ring R of finite Krull dimension. But in fact Theorem 8.60a) is sharp! That is, for any $d, D \in \mathbb{N}$ with $d+1 \leqslant D \leqslant 2d+1$, there is a ring R of Krull dimension d such that $R[t]$ has Krull dimension D. Moreover, the class of rings R of Krull dimension d such that $R[t]$ has Krull dimension $d+1$ is well understood. A domain with this property is called a **Jaffard domain**, and a domain R of dimension d with fraction field K is Jaffard if and only if for every T with $R \subseteq T \subseteq K$ we have $\dim T \leqslant d$ if and only if for every valuation ring T (see Chapter 17) with $R \subseteq T \subseteq K$ we have $\dim T \leqslant d$. It turns out that e.g. any Prüfer domain (see Chapter 20) is a Jaffard domain, though we will not prove that here. In general, the dimension of $R[t]$ can be understood in terms of the **valuative dimension** of R, which is the largest Krull dimension of any valuation overring of R.

When one proves a result about polynomial rings, it is usually fruitful to pursue analogues in formal power series rings, but the situation with the Hilbert Basis Theorem perhaps gives the wrong impression: the formal power series story need not be fully parallel with the polynomial ring story, and in many cases the formal power series story turns out to be more complicated. For instance, in Chapter 14 we will study "integrally closed domains" and prove that if R is an integrally closed domain then so is $R[t]$, but it will turn out that $R[[t]]$ need not be. Moreover, in Chapter 15 we will study unique factorization domains (UFDs) and prove that if R is a UFD then so is $R[t]$; in this case it is a major result of Samuel that $R[[t]]$ need not be (we will see the ring R but not the proof). In the present context, parts

b) and c) of Theorem 8.60 are in perfect analogue and the proof was even a little easier in the formal power series case. But...what about the formal power series analogue of part a)? This turns out to be fals

THEOREM 8.61. *(Arnold) For any $d \in \mathbb{N}$, there is a ring R of Krull dimension d such that $R[[t]]$ has infinite Krull dimension.*

PROOF. See [**Ar73**]. □

Let us just mention one example from Arnold's paper: he shows that if R is a valuation ring of rank 1 that is not discrete (see Chapter 17), then R has dimension 1 but $R[[t]]$ has infinite Krull dimension.

16. The Artin-Tate Lemma

THEOREM 8.62. *(Artin-Tate [**AT51**]) Let $R \subseteq T \subseteq S$ be a tower of rings with:*

(i) *R Noetherian,*
(ii) *S finitely generated as an R-algebra, and*
(iii) *S finitely generated as a T-module.*

Then T is finitely generated as an R-algebra.

PROOF. Let $x_1, \ldots, x_n$ be a set of generators for S as an R-algebra, and let $\omega_1, \ldots, \omega_m$ be a set of generators for S as a T-module. For all $1 \leqslant i \leqslant n$, we may write

$$x_i = \sum_j a_{ij}\omega_j, \ a_{ij} \in T. \tag{24}$$

Similarly, for all $1 \leqslant i, j \leqslant m$, we may write

$$\omega_i\omega_j = \sum_{i,j,k} b_{ijk}\omega_k, \ b_{ijk} \in T. \tag{25}$$

Let T_0 be the R-subalgebra of T generated by the a_{ij} and b_{ijk}. Since T_0 is a finitely generated algebra over the Noetherian ring R, the ring T_0 is Noetherian by the Hilbert Basis Theorem. Each element of S may be expressed as a polynomial in the x_i's with R-coefficients. Making substitutions using (24) and then (25), we see S is generated as a T_0-module by $\omega_1, \ldots, \omega_m$, and in particular that S is a finitely generated T_0-module. Since T_0 is Noetherian, the submodule T is also finitely generated as a T_0-module. This immediately implies that T is finitely generated as a T_0-algebra and then in turn that T is finitely generated as an R-algebra. □

CHAPTER 9

Boolean Rings

1. First Properties

Just for a second, let us break our rule by considering a not-necessarily-commutative ring R, but let us suppose that this ring has the property that every element is idempotent: we have $x^2 = x$ for all $x \in R$. Then:

$$(1+1) = (1+1)^2 = 1+1+1+1,$$

so $1+1=0$ and thus $-x = x$ for all $x \in R$. Moreover for all $x, y \in R$ we have

$$x + y = (x+y)^2 = x^2 + xy + yx + y^2 = x + y + xy + yx,$$

so $xy + yx = 0$ and thus $xy = -yx = yx$. It turns out that we haven't broken our rule at all: such a ring is necessarily commutative. In this chapter we study this class of rings: a ring is **Boolean** if every element is idempotent. Although this is clearly a very special class of rings, it is still interesting: in particular, there are important connections to both order theory and topology.

EXERCISE 9.1. *Show: if R is a Boolean ring, then its unit group $R^\times$ is trivial.*

EXERCISE 9.2.

a) *Show: a subring of a Boolean ring is Boolean.*
b)) *Show: a quotient of a Boolean ring is Boolean.*
c) *Show: let I be a nonempty set, and for each $i \in I$ let R_i be a Boolean ring. Show: the product $R := \prod_{i \in I} R_i$ is Boolean.*

EXERCISE 9.3. *Show: a Boolean ring is absolutely flat (cf. §3.11).*

EXERCISE 9.4. *Let R be a Boolean ring, and let $x, y \in R$.*

a) *Show: the following are equivalent:*
   (i) *We have $x \mid y$: that is, there is $z \in R$ such that $xz = y$.*
   (ii) *We have $xy = y$.*
b) *Show: if $(x) = (y)$, then $x = y$.*

2. Ideal Theory in Boolean Rings

PROPOSITION 9.1. *Let R be a Boolean ring.*

a) *For all $x \in \mathbb{N}$ and all $n \geqslant 2$, we have $x^n = x$.*
b) *A Boolean ring is reduced, i.e., has no nonzero nilpotent elements.*
c) *Every ideal in a Boolean ring is a radical ideal.*

PROOF. a) The case $n = 2$ is the definition of a Boolean ring, so we may assume $n \geqslant 3$. Assume the result holds for all $x \in R$ and all $2 \leqslant k < n$. Then $x^n = x^{n-1}x = x \cdot x = x$.

b) If $x \in R$ is such that $x^n = 0$ for some positive integer n, then either $n = 1$

or $n \geqslant 2$ and $x^n = x$; either way $x = 0$.
c) Let I be an ideal in the Boolean ring R. Then $I = \operatorname{rad}(I)$ if and only if R/I is reduced, but R/I is again a Boolean ring and part b) applies. □

Of course $\mathbb{Z}/2\mathbb{Z}$ is a Boolean ring. It is also a field, hence certainly a local ring and a domain. We will now show that $\mathbb{Z}/2\mathbb{Z}$ is the unique Boolean ring possessing *either* of these latter two properties.

PROPOSITION 9.2. *Let R be a Boolean ring.*

a) *If R is a domain, then $R \cong \mathbb{Z}/2\mathbb{Z}$.*
b) *We have $\dim R = 0$: i.e., every prime ideal of R is maximal.*
c) *If $(R, \mathfrak{m})$ is a local ring, then $R \cong \mathbb{Z}/2\mathbb{Z}$*
d) *R is semiprimitive: the Jacobson radical $J(R) := \bigcap_{\mathfrak{m} \in \operatorname{MaxSpec} R} \mathfrak{m} = (0)$.*

PROOF. a) Let $x \in R$. Then $x(x-1) = 0$, so in a domain R this implies $x = 0$ or $x = 1$, so $R \cong \mathbb{Z}/2\mathbb{Z}$.
b) If $\mathfrak{p} \in \operatorname{Spec} R$ then $R/\mathfrak{p}$ is a Boolean domain, hence by part a) is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, which is a field, so $\mathfrak{p} \in \operatorname{MaxSpec} R$.
c) By part b), we have $\operatorname{Spec} R = \{\mathfrak{m}\}$, so by Proposition 4.14d) we have that the set of nilpotents in R is $\mathfrak{m}$. Combining with Proposition 9.1 we conclude that $\mathfrak{m} = 0$, so R is a field, so by part a) we have $R \cong \mathbb{Z}/2\mathbb{Z}$.
d) By part b) and Proposition 4.14d), we have

$$J(R) = \bigcap_{\mathfrak{m} \in \operatorname{MaxSpec} R} \mathfrak{m} = \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p} = \operatorname{nil} R = (0). \qquad \square$$

EXERCISE 9.5. *Let R be a Boolean ring, and let $x, y \in R$.*

a) *Show: $\langle x, y \rangle = \langle xy + x + y \rangle$.*
b) *Deduce: any finitely generated ideal of R is principal.*

PROPOSITION 9.3.

a) *For a Boolean ring R, the following are equivalent:*
   (i) *R is finite.*
   (ii) *R is Noetherian.*
   (iii) *Every prime ideal of R is finitely generated.*
   (iv) *$\operatorname{Spec} R$ is finite.*
b) *If these equivalent conditions hold, then $R \cong (\mathbb{Z}/2\mathbb{Z})^n$ with $n = \#\operatorname{Spec} R$.*

PROOF. By Proposition 9.2b) we know that R is zero-dimensional:

$$\operatorname{MinSpec} R = \operatorname{Spec} R = \operatorname{MaxSpec} R.$$

a) (i) $\implies$ (ii) $\implies$ (iii) holds immediately in any ring.
(iii) $\implies$ (iv) by Corollary 4.32b).
(iv) $\implies$ (i): Suppose $\operatorname{Spec} R$ is finite. By Proposition 9.2d) we have $J(R) = 0$, so Exercise 8.31 gives $R \cong \prod_{i=1}^n k_i$ is a finite product of fields. Each k_i is a quotient of R, hence a Boolean field, hence $k_i \cong \mathbb{Z}/2\mathbb{Z}$ by Proposition 9.2a), so $R \cong (\mathbb{Z}/2\mathbb{Z})^n$.
b) While proving part a) we also showed that the conditions imply $R \cong \prod_{i=1}^n \mathbb{Z}/2\mathbb{Z}$. The prime ideals in $\prod_{i=1}^n \mathbb{Z}/2\mathbb{Z}$ are the ideals of the form $\prod_{i=1}^n I_i$ in which exactly one I_i is zero and the others are $\mathbb{Z}/2\mathbb{Z}$, so there are precisely n of them. □

LEMMA 9.4. *For an ideal $\mathfrak{m}$ in a Boolean ring R, the following are equivalent:*

(i) *$\mathfrak{m}$ is maximal.*

(ii) *For all $x \in R$, exactly one of x and $1-x$ lies in $\mathfrak{m}$.*

PROOF. (i) $\implies$ (ii): Suppose $\mathfrak{m}$ is maximal, and let $x \in R$. Of course we cannot have both $x, 1-x \in \mathfrak{m}$ for then $1 \in \mathfrak{m}$ and $\mathfrak{m} = R$. We may assume that x is neither 0 nor 1, so by Proposition 1.9 we get a decomposition $R = xR \times (1-x)R$. By Proposition 1.8 we have $\mathfrak{m} = I_1 \times I_2$ with $I_1 \subseteq xR$ and $I_2 \subseteq (1-x)R$, so $R/\mathfrak{m} \cong (xR)/I_1 \times (1-x)R/I_2$. For this quotient to be a field we need either $I_1 = xR$ – in which case $x \in \mathfrak{m}$ – or $I_2 = (1-x)R$ – in which case $1-x \in \mathfrak{m}$.
(ii) $\implies$ (i): This implication holds in any ring. We will show the contrapositive: suppose $\mathfrak{m}$ is not maximal. If $\mathfrak{m} = R$ then for all $x \in R$ both x and $1-x$ lie in $\mathfrak{m}$, so we may assume that $\mathfrak{m}$ is properly contained in $\mathcal{M} \in \operatorname{MaxSpec} R$. Let $x \in \mathcal{M} \backslash \mathfrak{m}$. Then ineed $x \notin \mathfrak{m}$, and because $\mathcal{M}$ is a proper ideal containing x, it does not contain $1-x$ and hence neither does the smaller ideal $\mathfrak{m}$. □

3. The Stone Representation Theorem

Let R be a Boolean ring. We would like to find an embedding of R into a Boolean ring of the form $(\mathbb{Z}/2\mathbb{Z})^X$. For this the key question is what X should be. Can we find any clues in our prior work on Boolean rings?
indent We understand finite Boolean rings very well: from Proposition 9.3, we know that every finite Boolean ring R is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$, where n is the number of maximal ideals of R. We claim that there is in fact a canonical isomorphism $\varphi : R \xrightarrow{\sim} (\mathbb{Z}/2\mathbb{Z})^{\operatorname{MaxSpec} R}$. Indeed, for any finite set $\mathcal{S}$ of maximal ideals of a ring R, the Chinese Remainder Theorem gives an isomorphism

$$R/\bigcap_{\mathfrak{m} \in \mathcal{S}} \mathfrak{m} \xrightarrow{\sim} \prod_{\mathfrak{m} \in \mathcal{S}} R/\mathfrak{m}.$$

In any semilocal ring – e.g. any finite ring – we may take $\mathcal{S} = \operatorname{MaxSpec} R$, getting

$$R/J(R) \xrightarrow{\sim} \prod_{\mathfrak{m} \in \operatorname{MaxSpec} R} R/\mathfrak{m}.$$

In a Boolean ring, we know that $J(R) = (0)$ and for all $\mathfrak{m} \in \operatorname{MaxSpec} R$ we have $R/\mathfrak{m} \cong \mathbb{Z}/2\mathbb{Z}$ – in fact, uniquely isomorphic, since 0 must go to 0 and 1 must go to 1. So in a finite Boolean ring the CRT map gives a canonical isomorphism

$$\varphi : R \xrightarrow{\sim} (\mathbb{Z}/2\mathbb{Z})^{\operatorname{MaxSpec} R}.$$

Another way of viewing φ is that for $x \in R$, the vector $\varphi(x)$ is, precisely, recording which maximal ideals contain x: for $\mathfrak{m} \in \operatorname{MaxSpec} R$, the $\mathfrak{m}$-component of $\varphi(x)$ is 0 if and only if $x \in \mathfrak{m}$.

In the above construction, the only real use of CRT was to get the surjectivity of φ. For any ring R we have an injective ring homomorphism

$$R/J(R) \hookrightarrow \prod_{\mathfrak{m} \in \operatorname{MaxSpec} R} R/\mathfrak{m}.$$

If R is Boolean, then once again we have $J(R) = 0$ and $R/\mathfrak{m} = \mathbb{Z}/2\mathbb{Z}$, so we get:

THEOREM 9.5. *(Stone Representation Theorem) Let R be a Boolean ring. We define a map*

$$E : R \to \mathbb{Z}/2\mathbb{Z}^{\operatorname{MaxSpec} R}$$

as follows: for $x \in R$ and $\mathfrak{m} \in \operatorname{MaxSpec} R$, $E(x)$ maps $\mathfrak{m}$ to 0 if and only if $x \in \mathfrak{m}$. Then E is an injective homomorphism of Boolean rings.

4. Boolean Algebras

A Boolean ring is an object of commutative algebra. It turns out that there is a completely equivalent class of structures of an order-theoretic nature, called **Boolean algebras**. In some ways the concept of a Boolean algebra is more intuitive and transparent – e.g., starting directly from the definition, it is perhaps easier to give examples of Boolean algebras.

A **Boolean algebra** is a certain very nice partially ordered set $(B, \leqslant)$. Recall that for any partially ordered set B and any subset S, we have the notion of the **supremum** $\sup S$ and the **infimum** $\inf S$. To define these it is convenient to extend the inequality notation as follows: if S, T are subsets of B, we write

$$S < T$$

to mean that for all $s \in S$ and $t \in T$, $s < t$, and similarly

$$S \leqslant T$$

to mean that for all $s \in S$ and $t \in T$, $s \leqslant t$.
Then we say that $z = \sup S$ if $S \leqslant z$ and if w is any element of B with $S \leqslant w$, then $z \leqslant w$. Similarly $z = \inf S$ if $z \leqslant S$ and if w is any element of B with $w \leqslant S$ then $w \leqslant Z$. For a given subset S, neither $\sup S$ nor $\inf S$ need exist, but if either exists it it is plainly unique. In particular if $\sup \varnothing$ exists, it is necessarily a bottom element, called 0, and if $\inf \varnothing$ exists, it is necessarily a top element called 0.
A partially ordered set $(L, \leqslant)$ is called a **lattice** if for all $x, y \in L$, $\sup\{x, y\}$ and $\inf\{x, y\}$ both exist. We give new notation for this: we write

$$x \vee y := \sup\{x, y\},$$

the **join** of x and y and

$$x \wedge y := \inf\{x, y\},$$

the **meet** of x and y.
A lattice is said to be **bounded** if it contains a bottom element 0 and a top element 1: each of these is unique if it exists. Notice that

$$0 = \sup \varnothing \text{ and } 1 = \inf \varnothing,$$

so a lattice is bounded if and only every finite subset has both a supremum and infimum.

EXERCISE 9.6. *Let L be a lattice containing 0 and 1, and let $x \in L$.*

a) *Show:* $x \vee 1 = 1$.
b) *Show:* $x \wedge 1 = x$.
c) *Show:* $x \vee 0 = x$.
d) *Show:* $x \wedge 0 = 0$.

A lattice L is **complemented** if it has a bottom element 0, a top element 1, and for each $x \in L$ there exists $y \in L$ such that $x \vee y = 1$, $x \wedge y = 0$.

A lattice is **distributive** if $\forall x, y, z \in L$,

$$(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z),$$

$$(x \wedge y) \vee z = (x \vee z) \wedge (y \vee z).$$

PROPOSITION 9.6. *Let L be a distributive complemented lattice. Then for all $x \in L$, the complement of x is unique.*

PROOF. Suppose that y_1 and y_2 are both complements to x, so

$$x \vee y_1 = x \vee y_2 = 1, \ x \wedge y_1 = x \wedge y_2 = 0.$$

Then

$$y_2 = 1 \wedge y_2 = (x \vee y_1) \wedge y_2 = (x \wedge y_2) \vee (y_1 \wedge y_2) = 0 \vee (y_1 \wedge y_2) = y_1 \wedge y_2,$$

so $y_2 \leqslant y_1$. Reasoning similarly, we get $y_1 \leqslant y_2$, so $y_1 = y_2$. □

By virtue of Proposition 9.6 we denote the complement of an element x in a distributive complemented lattice as x^*.

EXERCISE 9.7. *Show: for every element x of a distributive complemented lattice we have $(x^*)^* = x$.*

A **Boolean algebra** is a complemented distributive lattice with 0 and 1. (We allow $0 = 1$.)

EXERCISE 9.8. *(DeMorgan's Laws) Let B be a Boolean algebra.*

a) *Show: for all $x, y \in B$, we have $(x \wedge y)^* = x^* \vee y^*$.*
b) *Show: for all $x, y \in B$, we have $(x \vee y)^* = x^* \wedge y^*$.*

The shining example of a Boolean algebra is the powerset algebra 2^S for a nonempty set S. In the special case in which $|S| = 1$, we denote the corresponding Boolean algebra (the unique totally ordered set on two elements) simply as 2.

Not every Boolean algebra is isomorphic to a power set Boolean algebra.

EXAMPLE 9.7. *Let S be a set, and let $Z(S) \subseteq 2^S$ be the collection of all finite and cofinite subsets of S. Then $(Z(S), \subseteq) \subseteq (2^S, \subseteq)$ is a sub-Boolean algebra. However, $\#Z(S) = \#S$, so if S is countably infinite, then $Z(S)$ is not isomorphic to any power set Boolean algebra.*

Boolean algebras form a full subcategory of the category of partially ordered sets. In other words, we define a morphism $f : B \to B'$ of Boolean algebras simply to be an isotone (or order-preserving) map: $\forall x, y \in B, x \leqslant y \implies f(x) \leqslant f(y)$. One can also axiomatize Boolean algebras as a structure $(B, \vee, \wedge, *, 0, 1)$, the point being that $x \leqslant y$ if and only if $x \vee y = y$ if and only if $x \wedge y = x$, so the partial ordering can be recovered from either the wedge or the join.

PROPOSITION 9.8. *The category of Boolean rings is equivalent to the category of Boolean algebras.*

In other words, we can define a functor F from Boolean rings to Boolean algebras and a functor G from Boolean algebras to Boolean rings such that for every Boolean ring R, R is naturally isomorphic to $G(F(R))$ and for every Boolean algebra B, B is naturally isomorphic to $F(G(B))$.

Let us sketch the basic construction, leaving the details to the reader. Suppose first that R is a Boolean ring. Then we associate a Boolean algebra $F(R)$ with the same underlying set as R, endowed with the following operations: $\forall x, y \in R$,

$$x \wedge y = xy \tag{26}$$

and

$$x^* = 1 - x = 1 + x. \tag{27}$$

The join operation is then forced on us by DeMorgan's Laws:

$$x \vee y = (x^* \wedge y^*)^* = x + y - xy = x + y + xy. \tag{28}$$

EXERCISE 9.9. *Check that $(F(R), \wedge, \vee, *)$ is indeed a Boolean algebra, and that the bottom element 0 in $F(R)$ (resp. the top element 1) is indeed the additive identity 0 (resp. the multiplicative identity 1).*

Conversely, suppose that we have a Boolean algebra $(B, \wedge, \vee, *)$. Then we define a Boolean ring $G(B)$ on the same underlying set B, by taking

$$x + y := (x \wedge y^*) \vee (y \wedge x^*) \tag{29}$$

and

$$xy := x \wedge y. \tag{30}$$

The formula for addition may look a bit opaque. If B is a Boolean algebra of sets – i.e., a subalgebra of 2^S – then for $x, y \subseteq S$, $x + y$ is the **symmetric difference** of x and y: the set of all elements of S that lie in exactly one of x and y.

EXERCISE 9.10. *Let B be a Boolean algebra. Show: $(G(B), +, \cdot)$ is indeed a Boolean ring with additive identity the bottom element 0 of B and multiplicative identity the top element 1 of B.*

EXERCISE 9.11.

a) *Let R be a Boolean ring. Show: the identity map 1_R on R is an isomorphism of Boolean rings $R \to G(F(R))$.*
b) *Let B be a Boolean algebra. Show that the identity map 1_B on B is an isomorphism of Boolean algebras $B \to G(F(B))$.*

Let B be a Boolean algebra. A subset I of B is an **ideal** if $0 \in I$, for all $x, y \in I$ we have $x \vee y \in I$ and for all $x \in I$ and $a \in B$ we have $a \wedge x \in I$. Because for $x, y \in B$ we have $x \leqslant y$ if and only if $x \wedge y = x$, every ideal I is a downset of $(B, \leqslant)$.

PROPOSITION 9.9.

a) *Let I be an ideal of the Boolean algebra B. Then I is also an ideal of the Boolean ring $R := F(B)$.*
b) *Let I be an ideal of the Boolean ring R. Then I is also an ideal of the Boolean algebra $B := G(R)$.*

PROOF. a) Suppose I is an ideal of B. Then for all $x \in I$ and $a \in B$ we have $ax = a \wedge x \in I$. Now let $x, y \in I$. We have $x \wedge y^*, y \wedge x^* \in I$, hence $x + y = (x \wedge y^*) \vee (y \wedge x^*) \in I$.
b) Suppose I is an ideal of R. Then for all $x, y \in I$ and $a \in R$ we have $x + y \in I$ and $ax \in I$. So if $x, y \in I$ then $x \wedge y = xy + x + y \in I$ and if $x \in I$ and $a \in B$ then $a \wedge x = ax \in I$. □

Because the categories of Boolean rings and Boolean algebras are equivalent, every part of the theory of Boolean rings – definitions, theorems, and so forth – has a perfect analogue in the theory of Boolean algebras. However, it may happen that something is easier to understand or to prove in one category than the other. In

fact the theory of Boolean algebras predates the theory of Boolean rings, and for the most part things seem simpler on the ring side – at least, that is the perspective that we take in this text! But the Boolean algebras perspective is sometimes extremely enlightening: indeed, the main result of this chapter (Stone Duality) will be stated for Boolean algebras.

It is easy to express the conditions of prime and maximal ideals on the Boolean algebra side. An ideal I of a Boolean algebra B is prime if for all $x, y \in B$, $x \wedge y \in I$ implies that at least one of x, y lies in I. An ideal I is maximal if it is a proper ideal – i.e., it does not contain 1 – and is not properly contained in any other proper ideal. We will write $M(B)$ for the set of maximal ideals of a Boolean algebra. To be sure, we have immediately that $M(B) = \mathrm{MaxSpec}(G(B))$.

EXAMPLE 9.10. *Let S be a set, and let 2^S be the Boolean algebra of all subsets of S, partially ordered under inclusion. This Boolean algebra is canonically isomorphic to the Boolean algebra $F((\mathbb{Z}/2\mathbb{Z})^S)$. Indeed, to a function $f : S \to \mathbb{Z}/2\mathbb{Z}$, we attach the subset $S(f) := \{x \in S \mid f(x) = 1\}$. This correspondence is (a very well-known) bijection: the inverse function maps a subset X of S to the "indicator function" 1_X: $1_X(s) = 1$ if and only if $s \in X$. Moreover, for $f_1, f_2 : S \to \mathbb{Z}/2\mathbb{Z}$, we have $f_1 \leqslant f_2$ if and only if $f_1 \wedge f_2 = f_1$ if and only if ((by Exercise 9.4)) f_2 divides f_1 if and only if for all $s \in S$, $f_2(s) = 0$ implies $f_1(s) = 0$ if and only if for all $s \in S$, $f_1(s) = 1$ implies $f_2(s) = 1$ if and only if $S_{f_1} \subseteq S_{f_2}$. Because of this we will allow ourselves to say that $(2^S, \subseteq)$ is the Boolean algebra associated to $(\mathbb{Z}/2\mathbb{Z})^S$.*

We can then state the Stone Representation Theorem in terms of Boolean algebras as follows: every Boolean algebra is isomorphic to an algebra of sets (i.e., a subalgebra of some $(2^S, \subseteq)$). More precisely, we have an injective homomorphism of Boolean algebras

$$E : B \hookrightarrow 2^{M(B)}$$

obtained by mapping $x \in B$ to the set of maximal ideals $\mathfrak{m}$ of B that do not *contain x. Thus for instance since 0 is contained in every maximal ideal, we have $E(0) = \varnothing$, and since 1 is not contained in any maximal ideal, we have $E(1) = M(B)$. This is the form in which the Stone Representation Theorem was originally proved.*

Let us explore the ideal theory of Boolean algebras just a little further. The critierion for an ideal to be maximal given by Lemma 9.4 comes out nicely on the Boolean algebra side: it says that an ideal I in a Boolean algebra B is maximal if and only if for all $x \in B$, I contains exactly one of x, x^*. Using this we can give an "algebra side" proof that an ideal is maximal if and only if it is prime: suppose I is a maximal ideal of the Boolean algebra B, let $x, y \in B$ be such that $x \wedge y \in I$, and suppose that $x \notin I$. Then by maximality we have $x^* \in I$, hence I contains

$$(x^* \wedge y) \vee (x \wedge y) = (x \vee x^*) \wedge y = y.$$

Conversely, suppose that I is prime and let $x \in B$. Then $0 = x \wedge (x^*) \in I$, so I contains one of x and x^*, and if it contained both then it would contain $x \vee x^* = 1$.

For a subset X of a Boolean algebra B, let $\langle X \rangle$ be the ideal generated by X: by definition, this is the intersection of all ideals containing X and thus the unique minimal ideal containing X. As usual, this "top-down" description is easy to give but insufficiently concrete for many purposes. The next several results address this.

PROPOSITION 9.11. *Let B be a Boolean algebra, let X be a subset of B, and let $p \in B$. Then the ideal of B generated by X contains p if and only if there is a finite subset Y of X such that $p \leqslant \bigvee Y$.*

PROOF. Since for any finite subset Y of X we have $\bigvee Y \subseteq \langle X \rangle$, one direction is clear. For the converse, let J be the set of elements of $p \in B$ such that there is a finite subset Y of X with $p \leqslant \bigvee Y$. Clearly $X \subseteq J$, so it is enough to show that J is an ideal of B, for then I, being the unique minimal ideal of B containing X, must be contained in J. If $p_1, p_2 \in B$, there are finite subsets Y_1, Y_2 of X such that $p_i \leqslant \bigvee y_i$ for $i = 1, 2$, and then $Y_1 \cup Y_2$ is a finite subset of X such that $p_1 \vee p_2 \leqslant \bigvee(Y_1 \cup Y_2)$. Moreover if $x \in J$ and $p \in B$, there is a finite subset Y of X such that $x \leqslant \bigvee Y$ and then $p \wedge x \leqslant x \leqslant \bigvee Y$, so $p \wedge x \in J$. □

COROLLARY 9.12. *Let B be a Boolean algebra, let I be an ideal of B, and let $x_0 \in B$.*

a) *We have*
$$\langle I, x_0 \rangle = \{x \vee y \mid x \leqslant x_0 \text{ and } y \in I\}.$$
b) *If $x_0^* \notin I$, then $x_0^* \notin \langle I, x_0 \rangle$.*

PROOF. a) Let $J := \langle I, x_0 \rangle$. It is clear that every element $x \vee y$ with $x \leqslant x_0$ and $y \in I$ lies in J. Conversely, let $p \in J$: applying Proposition 9.11 with $X := I \cup \{x_0\}$, we get that there is a finite subset Y of I such that $p \leqslant \bigvee(Y \cup \{x_0\}) = y \vee x_0$ for some $y \in I$, which implies
$$p = p \wedge (y \vee x_0) = (p \wedge y) \vee (p \wedge x_0).$$
Since $p \wedge y \in I$ and $p \wedge x_0 \leqslant x_0$, we're done.
b) Seeking a contradiction, suppose $x_0^* \in \langle I, x_0 \rangle$. By part a), there is $x \leqslant x_0$ and $y \in I$ such that
$$x^* = x \vee y \leqslant x_0 \vee y.$$
Thus we have
$$x_0^* = x_0^* \wedge (x_0 \vee y) = (x_0^* \wedge x_0) \vee (x_0^* \wedge y) = (x_0^* \wedge y),$$
which implies that $x_0^* \leqslant y$, hence $x_0^* \in I$, contradiction. □

We can now give an "algebra side" proof of Lemma 9.4: namely, we will show that an ideal I in a Boolean algebra B is maximal if and only if for all $x \in B$ exactly one of x and x^* lies in I. One direction is easy: an ideal that contains exactly one of x, x^* for all $x \in R$ contains 0 so does not contain 1 so is proper, and it must be maximal, because for any element $x \in R \backslash I$ we have $x^* \in I$ so the $\langle I, x \rangle \supseteq \langle x^*, x \rangle = B$. Inversely, suppose there is $x \in B$ such that I contains neither x nor x^*. By Corollary 9.12b), we have $I \subsetneq \langle I, x_0 \rangle \subseteq B$, so I is not maximal.

COROLLARY 9.13. *Let x and y be distinct elements of a Boolean algebra B.*

a) *If $y \not\leqslant x$, then there is a maximal ideal of B containing x and not containing y.*
b) *There is a maximal ideal of B containing exactly one of x and y.*

PROOF. a) Suppose $y \not\leqslant x$, so $y \notin \langle x \rangle$. By Corollary 9.12b), we have $y \notin I := \langle x, y^* \rangle$. By the usual Zorn's Lemma argument, there is a maximal ideal $\mathfrak{m}$ of B containing I. Then $\mathfrak{m}$ contains x and y^* hence does not contain y.
b) Since $x \neq y$, part a) can be applied after interchanging them if necessary. □

Corollary 6 is the necessary ingredient to give an "algebra side" proof of the Stone Representation Theorem: namely, for any Boolean algebra B, we may certainly define the map

$$E : B \to 2^{M(B)}$$

by mapping $x \in B$ to the set of maximal ideals that do not contain x. If $x \leqslant y$, then every maximal ideal that contains y also contains x, so the set $B(x)$ of maximal ideals that *do not* contain x is a subset of the set of maximal ideals that *do not* contain y, showing that E is a homomorphism of Boolean algebras. The injectivity of B is the assertion that an element of B is determined by the set of maximal ideals that contain it, which is precisely the content of Corollary 6.

For elements x and y in a partially ordered set $(X, \leqslant)$, we say that **y covers x** if $x < y$ and there is no $z \in X$ with $x < z < y$. This relation comes up for instance in the **Hasse diagram** of X which is a directed graph with vertex set X and there is a direted edge from x to y if and only if y covers x.

An atom in a Boolean algebra B is an element x that covers 0: in other words, x is a minimal nonezero element of B. For any nonzero element x of a Boolean algebra, there is either an atom $y \leqslant x$ or an infinite descending chain $x > x_2 > \ldots$. A Boolean algebra B is **atomic** if for every nonzero $x \in B$ there is an atom $a \leqslant x$. A Boolean algebra is **atomless** if it contains no atoms.

EXAMPLE 9.14.

a) *Let S be a set, and let $B = (2^S, \subseteq)$ be the Boolean algebra of all subsets of S. Then B is atomic, and the atoms are the singleton sets $\{s\}$ for $s \in S$. Since every finite Boolean algebra is isomorphic to such a Boolean algebra, every finite Boolean algebra is atomic. This was however already clear from the definition.*

b) *Let S be an infinite set, and let $B \subseteq 2^S$ be the Boolean algebra of subsets that are either finite or have finite complement. Again the atoms are the singleton sets and this Boolean algebra is atomic.*

c) *Let $B \subseteq 2^{\mathbb{R}}$ be the set of subsets of $\mathbb{R}$ that are finite unions of any of the following subsets: $\varnothing$, $\mathbb{R}$, $[a, b)$ for any real numbers $a < b$, $[a, \infty)$ for any $a \in \mathbb{R}$ and $(-\infty, b)$ for any $b \in \mathbb{R}$. This is an atomless Boolean algebra of cardinality $\beth = \#\mathbb{R}$. More generally, if we replace $\mathbb{R}$ by any dense totally ordered set X (dense means: for all $x, y \in X$ with $x < y$, there is z in X with $x < z < x$) with at least two elements, then we get an atomless Boolean algebra I_X of cardinality $\#X$ called the **interval algebra of X**. Taking $X = \mathbb{Q}$ we get a countably infinite atomless Boolean algebra.*

d) *Let B_2 be an atomless Boolean algebra, and let $B := \{0, 1\} \times B_2$ with the product partial ordering: $(a_1, b_1) \leqslant (a_2, b_2)$ if and only if $a_1 \leqslant a_2$ and $b_1 \leqslant b_2$. This is again a Boolean algebra. The unique atom in B is $(1, 0)$, so there is no atom $a \leqslant x$ for any element x of B with nonzero second coordinate. Thus B is neither atomless nor atomic.*

The following is an important early result in the theory of Boolean algebras:

THEOREM 9.15. *Any two countably infinite atomless Boolean algebras are isomorphic.*

Theorem 9.15 bears a strong family resemblance to the result that any two countably infinite dense linear orders without endpoints are isomorphic. The proof is via

the "back-and-forth" method. The reader who is familiar with the back-and-forth method may wish to try to prove Theorem 9.15. We will not give a proof here, but later we will deduce it from a result in topology.

EXERCISE 9.12. *(Kernel of a homomorphism) Let $f : R \to \mathbb{Z}/2\mathbb{Z}$ be a homomorphism of Boolean rings.*

a) *Show:* $\operatorname{Ker} f$ *is $\vee$-closed: if $x, y \in \operatorname{Ker} f$, then $x \vee y \in \operatorname{Ker} f$.*
b) *Show:* $\operatorname{Ker} f$ *is downward-closed: if $x \in \operatorname{Ker} f$ and $y \leqslant x$, then $y \in \operatorname{Ker} f$.*
c) *Explain why parts a) and b) are equivalent to showing that* $\operatorname{Ker} f$ *is an ideal of the Boolean ring R.*
d) *Show:* $\operatorname{Ker} f$ *is in fact a maximal ideal of R.*
e) *Conversely, for every maximal ideal $\mathfrak{m}$ of R, show that $R/\mathfrak{m} = \mathbb{Z}/2\mathbb{Z}$ and thus the quotient map $q : R \to R/\mathfrak{m}$ is a homomorphism from R to $\mathbb{Z}/2\mathbb{Z}$.*

EXERCISE 9.13. *(Shell of a homomorphism) Let $f : R \to \mathbb{Z}/2\mathbb{Z}$ be a homomorphism of Boolean rings. Define the* ***shell*** $\operatorname{Sh} f$ *to be $f^{-1}(1)$.*

a) *Show:* $\operatorname{Sh} f$ *is wedge-closed: if $x, y \in \operatorname{Sh} f$, so is $x \wedge y$.*
b) *Show:* $\operatorname{Sh} f$ *is upward-closed: if $x \in \operatorname{Sh} f$ and $x \leqslant y$, then $y \in \operatorname{Sh} f$.*
c) *A nonempty, proper subset of a Boolean algebra that is wedge-closed and upward-closed is called a* ***filter****, so by parts a) and b)* $\operatorname{Sh} f$ *is a filter on B. Show that in fact it is an* ***ultrafilter*** *on B, i.e., that it is not properly contained in any other filter. (Suggestion: use Lemma 9.4.)*
d) *Show: every ultrafilter on B is the shell of a unique homomorphism of Boolean algebras $f : B \to \mathbb{Z}/2\mathbb{Z}$.*

5. Boolean Spaces

We will now digress a bit to talk (not for the first or last time!) about topological spaces. Following Bourbaki, for us **compact** means quasi-compact and Hausdorff. Further a **locally compact space** is a Hausdorff space in which each point admits a local base of compact neighborhoods. A subset of a topological space is **clopen** if it is both closed and open.

A topological space X is **totally disconnected** if the only connected subsets of X are the singleton sets $\{x\}$.[1] A totally disconnected space is necessarily **separated**: singleton sets are closed. Indeed, the closure of every connected set is connected, so the closure of a non-closed point would give a connected set which is larger than a point. On the other hand a space X is **zero-dimensional** if it admits a base of clopen sets.

PROPOSITION 9.16. *Let X be a locally compact space. Then X is totally disconnected if and only if it is zero-dimensional.*

PROOF. It is an exercise to show that every zero-dimensional Hausdorff space is totally disconnected. For a proof that every locally compact totally disconnected space is zero-dimensional, see e.g. [**Cl-GT**, Thm. 5.48]. □

A space X is called **Boolean**[2] if it is compact and zero-dimensional; in particular a Boolean space admits a base for the topology consisting of *compact open* sets.

[1]Following Qiaochu Yuan, we take the convention that the empty space is *not* connected: it has zero connected components, not one!

[2]There are many synonyms: e.g. **Stone space**, **profinite space**.

EXERCISE 9.14.

a) *A finite space is Boolean if and only if it is discrete.*
b) *A Boolean space is discrete if and only if it is finite.*
c) *An arbitrary direct product of Boolean spaces is Boolean.*
d) *The usual Cantor space is homeomorphic to a countably infinite direct product of copes of a discrete, two-point space and thus is a Boolean space.*

EXERCISE 9.15. *Show: a topological space is Boolean if and only if it is homeomorphic to an inverse limit of finite, discrete spaces.*

EXERCISE 9.16. *Let X be a Boolean space. Show: the following are equivalent:*

(i) *The space X has a countable base for its topology.*
(ii) *The space X is metrizable.*
(iii) *There is a sequence of finite discrete spaces X_n and for each $m \leqslant n$ a map $\varphi_{n,m} : X_n \to X_m$ such that X is homemorphic to the inverse limit $\varprojlim_n X_n$.*
(iv) *The set of clopen subsets of X is countable.*

To every topological space X we may associate a Boolean algebra: namely, the subalgebra of 2^X consisting of compact open subsets. Thus in particular we may associate a Boolean algebra $\mathcal{C}(X)$, the **characteristic algebra** of X.

EXERCISE 9.17. *Show: the assignment $X \mapsto \mathcal{C}(X)$ extends to a contravariant functor from the category of topological spaces to the category of Boolean algebras. (In other words, show that a continuous map $f : X \to Y$ of topological spaces induces a "pullback" ring homomorphism $\mathcal{C}(f) : \mathcal{C}(Y) \to \mathcal{C}(X)$.)*

If X is itself a Boolean space, then the characteristic algebra $\mathcal{C}(X)$ is indeed *characteristic* of X in the following sense.

PROPOSITION 9.17. *Let X be a Boolean space, and let $\mathcal{A}$ be a Boolean algebra of subsets of X that is also a base for the topology of X. Then $\mathcal{A} = \mathcal{C}(X)$.*

PROOF. By hypothesis the elements of $\mathcal{A}$ are open sets in X. Moreover, since $\mathcal{A}$ is closed under complementation, the elements are also closed. Thus $\mathcal{A} \subseteq \mathcal{C}(X)$.

Conversely, suppose $Y \in \mathcal{C}(X)$. Since Y is open and $\mathcal{A}$ is a base for the topology on X, for each $y \in Y$ there is $A_y \in \mathcal{A}$ with $y \in A_y \subseteq Y$. Thus $\{A_y\}_{y \in Y}$ is an open cover for Y. But Y is also closed in a compact space hence itself compact, so we may extract a finite subcover, say $Y = \bigcup_{i=1}^n A_{y_i}$. Since $\mathcal{A}$ is a subalgebra, it is closed under finite unions, so $Y \in \mathcal{A}$. Thus $\mathcal{C}(X) \subseteq \mathcal{A}$. □

To every Boolean algebra B we will now endow the set $M(B)$ of maximal ideals of B with a topology that makes it into a Boolean space.

By the Stone Representation Theorem we have an embedding

$$B \hookrightarrow 2^{M(B)}$$

and thus every element $x \in B$ determines a function $x : M(B) \to \{0,1\}$: $x(\mathfrak{m}) = 1 \iff x \notin \mathfrak{m}$. Endowing $\{0,1\}$ with the discrete topology, we may give $M(B)$ the **initial topology** for the family of maps $\{x : M(B) \to \{0,1\}\}_{x \in R}$: the coarsest topology that makes each of these maps continuous. Because a for a topological

space X, a map $f : X \to \{0,1\}$ is continuous if and only if $f^{-1}(0)$ and $f^{-1}(1)$ are open, the initial topology on $M(B)$ is the one generated by $\{U_x, V_x\}_{x \in X}$ where

$$U_x = \{\mathfrak{m} \in M(B) \mid x \notin \mathfrak{m}\}$$

and

$$V_x = \{\mathfrak{m} \in M(B) \mid x \in \mathfrak{m}\}.$$

Because for all $x \in B$ and all $\mathfrak{m} \in M(B)$ we have that $\mathfrak{m}$ contains exactly one of x and x^*, it follows that

$$V_x = U_{x^*}.$$

Moreover, for $x, y \in B$ we have

$$U_x \cap U_y = U_{x \wedge y}.$$

Thus the set $\{U_x\}_{x \in B}$ is a base for this topology on $M(B)$. In Chapter 13 we will study the Zariski topology on $\operatorname{Spec} R$ for any ring R and see right away that a base for it is

$$\{U(f) := \{\mathfrak{p} \in \operatorname{Spec} R \mid f \notin \mathfrak{p}\}\}_{f \in R},$$

so the topology we've defined on $M(B)$ is the Zariski topology on the associated Boolean ring $R = F(B)$. For $x \in B$ we have $U_x = M(B) \backslash V_x = M(B) \backslash U_{x^*}$, so each U_x is a clopen set. Le tus now show that $M(R)$ is a Boolean space.

Hausdorff: Let $\mathfrak{m}_1$ and $\mathfrak{m}_2$ be distinct maximal ideals of R. Choose $x \in \mathfrak{m}_2 \backslash \mathfrak{m}_1$, so by Lemma 9.4 we have $x^* \in \mathfrak{m}_1 \backslash \mathfrak{m}_2$. Thus $\mathfrak{m}_1 \in U_x$, $\mathfrak{m}_2 \in U_{x^*}$ and

$$U_x \cap U_{x^*} = U_{x \wedge x^*} = U_0 = \varnothing,$$

so we have separated $\mathfrak{m}_1$ and $\mathfrak{m}_2$ by open sets.

Quasi-compactness: It suffices to check quasicompactness using open covers taken from any given base, so let's use $\{U_x\}_{x \in B}$: suppose that we have a family $\{x_i\}_{i \in I}$ such that $\bigcup_{i \in I} U_{x_i} = M(B)$. Now

$$M(B) = \bigcup_i U_{x_i} = \bigcup_i (M(B) \backslash V_{x_i}) = M(B) \backslash \bigcap_i V_{x_i},$$

so that $\bigcap_i V_{x_i} = \varnothing$. Thus we have $\langle x_i \mid i \in I \rangle = B$. By Propoisition 9.11 there is a finite subset J of I such that $1 \in \langle x_i \mid i \in J \rangle$ and thus $\bigcup_{i \in J} U_{x_i} = M(B)$.

Thus $M(B)$ is a Boolean space, which we call the **Stone space** of the Boolean algebra B. If R is the corresponding Boolean ring (on the same underlying set as R) then we have $\operatorname{Spec} R = M(B)$ as topological spaces.

EXERCISE 9.18. *Show: the assignment $B \mapsto M(B)$ extends to a contravariant functor from the category of Boolean algebras to the category of Boolean spaces: that is, a homomorphism $f : B_1 \to B_2$ canonically induces a continuous map $M(f) : M(B_2) \to M(B_1)$ of Stone spaces.*

6. Stone Duality

THEOREM 9.18. *(Stone Duality) The functors $\mathcal{C}$ and M give a duality between the category of Boolean spaces and the category of Boolean algebras. That is:*

a) *For every Boolean algebra B, the map $B \to \mathcal{C}(M(B))$ given by $x \in B \mapsto U_x$ is an isomorphism of Boolean algebras.*

b) *For every Boolean space X, the map $m : X \to M(\mathcal{C}(X))$ given by $x \in X \mapsto \mathfrak{m}_x := \{U \in \mathcal{C}(X) \mid x \notin U\}$ is a homeomorphism of Boolean spaces.*

PROOF. a) The map $e : x \in B \mapsto U_x \in 2^{M(B)}$ is the embedding e of the Stone Representation Theorem. In particular it is an embedding of Boolean algebras. Its image $e(B)$ is a subalgebra of the characteristic algebra of the Boolean space $M(B)$ which is, by definition, a base for the topology of $M(B)$. By Proposition 9.17 we have $e(B) = \mathcal{C}(M(B))$ so e is an isomorphism of Boolean algebras.
b) First we need to show that $\mathfrak{m}_x$ is a maximal ideal in the characteristic ring $\mathcal{C}(X)$. It seems more natural to show this on the Boolean algebra side, i.e., to show that $\mathfrak{m}_x$ is downward closed and union-closed. Indeed, $U \in \mathfrak{m}_x$ means $x \notin U$, so if $V \subseteq X$ then certainly $x \notin V$, i.e., $V \in \mathfrak{m}_x$; moreover, $U, V \in \mathfrak{m}_x \iff x \notin U$ and $x \notin V \iff x \notin U \cup V \iff U \cup V \in \mathfrak{m}_x$. Thus $\mathfrak{m}_x$ is an ideal of $\mathcal{C}(X)$. Applying Lemma 9.4, one easily sees that is maximal, so the map m is well-defined.
indent The injectivity of m follows immediately from the Hausdorff property of X.

Surjectivity: Let $\mathfrak{m} \in M(\mathcal{C}(X))$. We may identify $\mathfrak{m}$ with a homomorphism of Boolean algebras $f_{\mathfrak{m}} : \mathcal{C}(X) \to \mathbb{Z}/2\mathbb{Z}$. Let $\mathcal{F} = f_{\mathfrak{m}}^{-1}(1)$ be the shell of $f_{\mathfrak{m}}$, an ultrafilter on the Boolean algebra of sets $\mathcal{C}(X)$. In particular $\mathcal{F}$ is wedge-closed, i.e., it is a family of clopen subsets of the compact space X satisfying the finite intersection property. Therefore there exists $x \in \bigcap_{U \in \mathcal{F}} U$. On the other hand, the collection $\mathcal{F}_x$ of all clopen sets in X containing x is also a filter on $\mathcal{C}(X)$ with $\mathcal{F} \subseteq \mathcal{F}_x$. But since $\mathcal{F}$ is an *ultra*filter – i.e., a maximal filter – we have $\mathcal{F} = \mathcal{F}_x$. Thus $\mathfrak{m}$ and $\mathcal{F}_x$ are respectively the kernel and shell of the homomorphism $f : \mathcal{C}(X) \to \mathbb{Z}/2\mathbb{Z}$, so

$$\mathfrak{m} = \mathcal{C}(X) \backslash \mathcal{F}_x = \{U \in \mathcal{C}(X) \mid x \notin U\} = m(x).$$

Finally, since m is surjective, we have that for each $A \in \mathcal{C}(X)$,

$$\{U \in M(\mathcal{C}(X)) \mid A \in U\} = \{m(x) \mid x \in A\},$$

so that m maps the base $\mathcal{C}(X)$ for the topology on X onto the base $\mathcal{C}(M(\mathcal{C}(X)))$. □

Thus at this point we know that the category of Boolean spaces is anti-equivalent to the category of Boolean algebras, which is equivalent to the category of Boolean rings. It follows, of course, that the category of Boolean spaces is anti-equivalent to the category of Boolean rings. We can state this a bit more directly, as follows: for a topological space X, let $C(X, 2)$ be the ring of all continuous functions $f : X \to \mathbb{Z}/2\mathbb{Z}$ (with $\mathbb{Z}/2\mathbb{Z}$ being given the discrete topology). The ring $C(X, 2)$ is a Boolean ring under pointwise addition and multiplication. Letting $\mathcal{C}(X)$ be the characteristic algebra of X, the map

$$C(X, 2) \to \mathcal{C}(X), \ f \in C(X, 2) \mapsto f^{-1}(1)$$

is an isomorphism from $G(C(X, 2))$, the Boolean algebra of $C(X, 2)$, to the Boolean algebra $\mathcal{C}(X)$. It follows that:

THEOREM 9.19 (Stone Duality, version II). a) *For every Boolean ring R, the map $R \to C(\operatorname{Spec} R, 2)$ given by $x \mapsto (\mathfrak{m} \mapsto x \pmod{\mathfrak{m}} \in \mathbb{Z}/2\mathbb{Z})$ is an isomorphism of Boolean rings.*

b) *For every Boolean space X, the map $X \to \operatorname{Spec}(C(X, 2))$ given by $x \mapsto \mathfrak{m}_x := \{f \in C(X, 2) \mid f(x) = 0\}$ is a homeomorphism.*

The map $x \mapsto \mathfrak{m}_x$ of Theorem 9.19 is an analogue of the map $X \to \operatorname{MaxSpec} C(X)$ that we defined for the ring of $\mathbb{R}$-valued continuous functions on any topological space X. (For any topological field F, we can define such a map $X \to \operatorname{MaxSpec} C(X, F)$, where $C(X, F)$ is the ring continuous functions $f : X \to F$.) Theorem 9.19 is closely analogous to the anti-equivalence from the category of compact spaces to the category of continuous real-valued functions on those spaces.

However, in Chapter 5 we did not give a ring-theoretic characterization of the class of rings $C(X)$ for X a compact space, whereas the class of rings $C(X, 2)$ obtained by varying over all topological spaces X is simply the class of all Boolean rings. There is a better duality theorem on the class of compact spaces, but it takes us out of our subject matter: for a compact space X, there is more structure on $C(X, \mathbb{C}) = \{\text{continuous } f : X \to \mathbb{C}\}$ than just that of a commutative ring: it is a commutative, unital C^*-algebra. Gelfand showed that there is a categorical anti-equivalence between compact spaces and commutative, unital C^*-algebras.

THEOREM 9.20. *Let B be a Boolean algebra, with associated Boolean ring R and Stone space $M(B) = \operatorname{Spec} R$.*

a) *For $\mathfrak{m} \in M(B)$, the following are equivalent:*
   (i) *$\mathfrak{m}$ is an isolated point of $M(B)$: that is, $\{\mathfrak{m}\}$ is open.*
   (ii) *The ideal $\mathfrak{m}$ is principal.*

b) *For $x \in B$, the following are equivalent:*
   (i) *The ideal $\langle x \rangle$ is maximal.*
   (ii) *The element x^* is an atom of B.*

PROOF. a) (i) $\implies$ (ii): Suppose that $\mathfrak{m} \in M(B)$ is isolated: then there is $x \in B$ such that $\{\mathfrak{m}\} = U_x$, i.e., $\mathfrak{m}$ is the unique maximal ideal that does not contain x. Equivalently, $\mathfrak{m}$ is the unique maximal ideal containing x^*. If $\mathfrak{m}$ contained an element y with $y \nleq x^*$ then by Corollary a) there would be a maximal ideal of B containing x^* and not y, which is a contradiction: the only maximal ideal that contains x^* also contains y. It follows that $\mathfrak{m} = \langle x^* \rangle$ is principal.
(ii) $\implies$ (i): If $\mathfrak{m} = \langle x \rangle$, then every maximal ideal that does not contain x^* must contain $\mathfrak{m}$, so $U_{x^*} = \{\mathfrak{m}\}$.
b) (i) $\implies$ (ii): We go by contraposition: suppose that x^* is not an atom, so there is $y \in B$ with $0 < y < x^*$. Then $x < y^* < 1$, so $\langle x \rangle \supsetneq \langle y^* \rangle \subsetneq B$.
(ii) $\implies$ (i): Again, we go by contraposition: if $\langle x \rangle$ is not maximal, then there is $y \in B$ such that

$$\langle x \rangle \subsetneq \langle x, y \rangle \subsetneq B.$$

But $\langle x, y \rangle = \langle x \vee y \rangle$, so we have $x < x \vee y < 1$ and thus $0 < (x \vee y)^* < x^*$. It follows that x^* is not an atom. □

Here is another take on Theorem 9.20b): an element x of a Boolean algebra B is an atom if and only if $\langle x \rangle$ is minimal among nonzero principal ideals if and only if $\langle x^* \rangle$ is maximal among proper principal ideals. Because finitely generated ideals in a Boolean ring are principal, an ideal that is maximal among proper principal ideals must actually be a maximal ideal. (In a domain R, an element that generates an ideal that is maximal among proper principal ideals is called **irreducible**. Such elements will be studied in great detail in Chapter 15. The ideal generated by an irreducible element need not be prime, and if it is prime it need not be maximal.) Because principal ideals in a Boolean algebra B have unique generators (Exercise

9.4b)), the map

$$a \mapsto (a^*)$$

gives a bijection from the set of atoms of B to the set $\mathrm{PM}(B)$ of principal maximal ideals of B, which by Theorem 9.20a) is an open, discrete subset of $M(B)$.

EXERCISE 9.19. *Let B be a Boolean algebra. Show: the set $\mathrm{PM}(B)$ is dense in the set $M(B)$ of all maximal ideals of B if and only if B is atomic.*

Earlier, in Proposition 9.3 we showed that every infinite Boolean ring has a prime ideal that is not principal (equivalently, not finitely generated, since all finitely generated ideals of a Boolean ring are not principal). Theorem 9.20 gives a nice topological proof of this: if R is a Boolean ring in which every prime ideal is principal, then every point of $\operatorname{Spec} R$ is isolated, so $\operatorname{Spec} R$ is discrete. But it is also compact, hence it is finite.

We also immediately deduce:

COROLLARY 9.21. *For a Boolean algebra B with corresponding Boolean ring R, the following are equivalent:*

(i) *B is atomless.*
(ii) *R has no principal prime ideals.*
(iii) *The Stone space $M(B) = \operatorname{Spec} R$ is perfect: no point is isolated.*

Thus atomless Boolean algebras correspond to perfect Boolean spaces. The most famous perfect Boolean space is the **Cantor space**,. The Cantor *set* C is the set of real numbers in $[0,1]$ admitting a ternary (base 3) expansion in which 1 does not appear. Any real number has at most one such expansion, so C is in canonical bijection with $\{0,2\}^{\mathbb{Z}^+}$. If we give each $\{0,2\}$ the discrete topology and $\{0,2\}^{\mathbb{Z}^+}$ the product topology, then this caononical bijection is a homeomorphism. One also sees easily that $\{0,2\}^{\mathbb{Z}^+}$ is Boolean, perfect and second-countable. In fact, any infinite topological space that is Boolean, perfect and second-countable is homeomorphic to the Cantor space [**Cl-GT**, Thm. 9.4]. Using Exercise 9.16, the "Stone dual" of this result is the assertion that any two countably infinite atomless Boolean algebras are isomorphic: this is Theorem 9.15.

EXERCISE 9.20. *Let S be a nonempty set, and let $R := (\mathbb{Z}/2\mathbb{Z})^S$.*

a) *Show: the atoms of R are the elements x all of whose coordinates except for exactly one are 0.*
b) *For $s \in S$, let x_s be the element all of whose coordinates except for the sth coordinate are 1 and for which the sth coordinate is 0. Show: the map $\iota : S \hookrightarrow \operatorname{MaxSpec} R$ given by $s \mapsto (x_s)$ is an injection with image the set of principal maximal ideals of R.*
c) *As mentioned above, $\iota(S)$ is a discrete, open subspace of $\operatorname{MaxSpec} R$. Show: $\iota : S \hookrightarrow \operatorname{MaxSpec} R$ is the Stone-Cech compactification of the discrete space S.*

In the examples of infinite Boolean algebras that we've seen so far, "most" maximal ideals were not principal. This need not be the case:

EXERCISE 9.21. *Let κ be a countable cardinal. Show: there is a countably infinite Boolean algebra with exactly κ nonprincipal maximal ideals.*

CHAPTER 10

Associated Primes and Primary Decomposition

1. Associated Primes

Let M be an R-module. A prime ideal $\mathfrak{p}$ of R is an **associated prime** of M if there is $m \in M$ with $\mathfrak{p} = \operatorname{ann} m = \{x \in R \mid xm = 0\}$. The set of associated primes of M is denoted (unfortunately) by $\operatorname{Ass} M$.

Thus when R is a domain and M is torsionfree, (0) is the only associated prime of M. In particular this holds for ideals of R. We hope this motivates the following definition: for an ideal I of a ring R, the associated primes of the ideal I are the associated primes of the module R/I.

PROPOSITION 10.1.
For an R-module M and $\mathfrak{p} \in \operatorname{Spec} R$, the following are equivalent:

(i) $\mathfrak{p} \in \operatorname{Ass} M$.
(ii) *There is an injection of R-modules $R/\mathfrak{p} \hookrightarrow M$.*

PROOF. (i) $\implies$ (ii): Let $\mathfrak{p} \in \operatorname{Ass} M$, and let $m \in M$ with $\mathfrak{p} = \operatorname{ann} m$. Define $\iota : R \to M$ by $x \mapsto xm$. Then $\operatorname{Ker} \iota = \mathfrak{p}$, so ι gives an injection from $R/\mathfrak{p}$ to M.
(ii) $\implies$ (i): If $\iota : R/\mathfrak{p} \hookrightarrow M$, let $m = \iota(1 + \mathfrak{p})$. Then $\mathfrak{p} = \operatorname{ann} m$. □

We immediately deduce:

COROLLARY 10.2. *If $N \subseteq M$ are R-modules, then $\operatorname{Ass} N \subseteq \operatorname{Ass} M$.*

PROPOSITION 10.3. *For a prime ideal $\mathfrak{p}$ of R, $\operatorname{Ass} R/\mathfrak{p} = \{\mathfrak{p}\}$.*

PROOF. Proposition 10.1 gives $\mathfrak{p} \in \operatorname{Ass} R/\mathfrak{p}$. Conversely, let $x \in R$ be such that $\operatorname{ann}(x + \mathfrak{p}) = \mathfrak{q}$ is a prime ideal. Since $\mathfrak{p}$ is prime, $y \in \mathfrak{q} \iff yx \in \mathfrak{p} \iff y \in \mathfrak{p}$. □

For an R-module M, a **zero divisor** of M is an element $x \in R$ such that $xm = 0$ for some $m \in M^\bullet$. We write $\operatorname{ZD}(M)$ for the set of all zero divisors of M.

PROPOSITION 10.4. *For a nonzero R-module M, let $\mathcal{F} = \{\operatorname{ann} m \mid m \in M^\bullet\}$.*

a) *Every maximal element of $\mathcal{F}$ is a prime ideal.*
b) *If R is Noetherian, then $\operatorname{Ass} M \neq \varnothing$.*

PROOF. a) Let I be an ideal of R of the form $\operatorname{ann} m$ for some $x \in M^\bullet$ and not properly contained in $\operatorname{ann} x'$ for any $x' \in M^\bullet$. Let $a, b \in R$ be such that $ab \in I$ but $b \notin I$. Then $bx \in M^\bullet$. Since $0 = abx = a(bx)$, $a \in \operatorname{ann}(bx)$. But clearly $I = \operatorname{ann} x \subseteq \operatorname{ann}(bx)$, so by maximality of I we have $I = \operatorname{ann}(bx)$ and thus $a \in I$.
b) If $M \neq 0$, then $\mathcal{F}$ is a nonempty family of ideals in a Noetherian ring so has a maximal element. Apply part a). □

EXERCISE 10.1. *Let M be a nonzero R-module, and let $S \subseteq R$ be a multiplicative subset. Following* [**LR08**, Prop. 3.5]*, we consider the family $\mathcal{F}$ of ideals I of R with the following propery: for all $m \in M$, if $Im = 0$ then $sm = 0$ for some $s \in S$.*

a) *Show: $\mathcal{F}$ is increasing and strongly Ako.*
b) *Show: an ideal I of R is maximal with respect to being disjoint from S and of the form $\operatorname{ann}(m)$ for some nonzero element $m \in M$ if and only if it is a maximal element of $\mathcal{F}'$.*
c) *(Herstein) Show: an ideal that is maximal among annihilators of nonzero points of M is prime.*
d) *Suppose that either R or M is Noetherian. Show: $\mathcal{F}$ is a monoidal filter.*

PROPOSITION 10.5. *Let M be an R-module.*

a) *We have $\bigcup_{\mathfrak{p} \in \operatorname{Ass} M} \mathfrak{p} \subseteq \operatorname{ZD}(M)$.*
b) *If R is Noetherian, then $\bigcup_{\mathfrak{p} \in \operatorname{Ass} M} \mathfrak{p} = \operatorname{ZD}(M)$.*

PROOF. a) If $\mathfrak{p} = \operatorname{ann} m$, then $xm = 0$ for all $x \in \mathfrak{p}$, so $\mathfrak{p} \subseteq \operatorname{ZD}(M)$.
b) Let $x \in \operatorname{ZD}(M)$, so that there is $m \in M^\bullet$ with $xm = 0$. By Proposition 10.4 applied to $N = \langle m \rangle$, there is $\mathfrak{p} \in \operatorname{Ass} N$, i.e., there is $y \in R$ such that $ym \neq 0$ and $\mathfrak{p} = \operatorname{ann} ym$. Since $xm = 0$, $xym = 0$ and $x \in \mathfrak{p}$. By Proposition 10.2 $\mathfrak{p} \in \operatorname{Ass} M$ and thus $x \in \bigcup_{\mathfrak{p} \in \operatorname{Ass} M} \mathfrak{p}$. □

PROPOSITION 10.6. *Let $N \subseteq M$ be R-modules. Then:*

a) *We have $\operatorname{Ass} M \subseteq \operatorname{Ass} N \cup \operatorname{Ass} M/N$.*
b) *We have $\operatorname{Ass}\left(\bigoplus_{i \in I} M_i\right) = \bigcup_{i \in I} \operatorname{Ass} M_i$.*

PROOF. a) For $\mathfrak{p} \in \operatorname{Ass} M$, let $\iota : R/\mathfrak{p} \subseteq M$ be an R-module monomorphism. Put $H = \iota(R/\mathfrak{p})$ and $L = H \cap N$.
Case 1: Suppose $L = 0$. Then the natural map $\alpha : H \to M/N$ is a monomorphism, so $\alpha \circ \iota : R/\mathfrak{p} \to M/N$ is a monomorphism and $\mathfrak{p} \in \operatorname{Ass} M/N$.
Case 2: Let $x \in L^\bullet$. Then $x \in H^\bullet \cong (R/\mathfrak{p})^\bullet$, so $\operatorname{ann} x = \mathfrak{p}$. Since $x \in N$, $\mathfrak{p} \in \operatorname{Ass} N$.
b) Put $M = \bigoplus_{i \in I} M_i$. Since each M_i is a submodule of $\bigoplus_{i \in I} M_i$, $\bigcup_{i \in I} \operatorname{Ass} M_i \subseteq \operatorname{Ass} M$ follows from Proposition 10.2. The containment $\operatorname{Ass} M \subseteq \bigcup_{i \in I} \operatorname{Ass} M_i$ follows from part a) when I is finite. In the general case, let $\mathfrak{p} \in \operatorname{Ass} M$. Then there is an R-module monomorphism $\iota : R/\mathfrak{p} \hookrightarrow M = \bigoplus_{i \in I} M_i$. The image $\iota(R/\mathfrak{p})$ lies in the submodule generated by $\iota(1 + \mathfrak{p})$, hence lies in $\bigoplus_{i \in J} M_i$ for some finite subset $J \subseteq I$. This reduces us to the finite case. □

THEOREM 10.7. *Let R be a Noetherian ring, and let M be a nonzero, finitely generated R-module.*

a) *There is a chain of submodules*

$$0 = M_0 \subsetneq M_1 \subsetneq \ldots \subsetneq M_n = M$$

such that for all $0 \leqslant i \leqslant n-1$ there is a prime ideal $\mathfrak{p}_i$ of R with $M_{i+1}/M_i \cong \mathfrak{p}_i$.
b) *For any such chain, we have $\operatorname{Ass} M \subseteq \{\mathfrak{p}_0, \ldots, \mathfrak{p}_{n-1}\}$.*
c) *In particular, $\operatorname{Ass} M$ is finite.*

PROOF. a) By Proposition 10.5 M has an associated prime $\mathfrak{p}_1 = \operatorname{ann} m_1$. Put $M_0 = \{0\}$ and $M_1 = \langle m_1 \rangle$; note $M_1/M_0 = M_1 \cong R/\mathfrak{p}_1$. If $M_1 = M$ we're done; if not, M/M_1 is finitely generated and nonzero so has an associated prime $\mathfrak{p}_2 = \operatorname{ann}(m_2 + M_1)$. Put $M_2 = \langle m_1, m_2 \rangle$, so that $M_2/M_1 \cong R/\mathfrak{p}_2$. We continue in this way, getting an increasing chain of submodules M_i in M. Since M is

Noetherian, we must have $M_n = M$ for some m.
b) By Proposition 10.3, for all $0 \leqslant i \leqslant n-1$ we have

$$\operatorname{Ass} M_{i+1}/M_i = \operatorname{Ass} R/\mathfrak{p}_i = \{\mathfrak{p}_i\}.$$

By Proposition 10.6 we have for all $0 \leqslant i \leqslant n-1$, $\operatorname{Ass} M_{i+1} \subseteq \operatorname{Ass} M_i \cup \{\mathfrak{p}_{i+1}\}$, and from this $\operatorname{Ass} M = \operatorname{Ass} M_n \subseteq \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ follows.
c) This follows immediately. □

COROLLARY 10.8. *Let $(R, \mathfrak{m})$ be a Noetherian local ring. If $\mathfrak{m}\backslash\mathfrak{m}^2$ consists entirely of zero-divisors, then there is $x \in R^\bullet$ with $x\mathfrak{m} = 0$.*

PROOF. If $\mathfrak{m} = 0$ we may take $x = 1$. Henceforth we assume $\mathfrak{m} \neq 0$, so by Nakayama's Lemma there is $a \in \mathfrak{m}\backslash\mathfrak{m}^2$. By Theorem 10.7 and Proposition 10.5, $\operatorname{Ass} R = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ is finite and $\operatorname{ZD}(R) = \bigcup_{i=1}^n \mathfrak{p}_i$. Thus by hypothesis

$$\mathfrak{m}\backslash\mathfrak{m}^2 \subseteq \bigcup_{i=1}^n \mathfrak{p}_i.$$

For $y \in \mathfrak{m}^2$ and $p \in \mathbb{Z}^+$, $a + y^p \in \mathfrak{m}\backslash\mathfrak{m}^2$, so by the Pigeonhole Principle there are $1 \leqslant p < q \in \mathbb{Z}^+$ such that $a + y^p, a + y^q \in \mathfrak{p}_i$ for some i. Then $y^p(1 - y^{q-p}) \in \mathfrak{p}_i$; since $y^{q-p} \in \mathfrak{m}$ and R is local, $1 - y^{q-p} \in R^\times$; thus $y^p \in \mathfrak{p}_i$ and, since $\mathfrak{p}_i$ is prime, $y \in \mathfrak{p}_i$. This shows

$$\mathfrak{m} \subseteq \bigcup_{i=1}^n \mathfrak{p}_i.$$

By Prime Avoidance (Lemma 8.52), there is at least one i such that $\mathfrak{m} \subseteq \mathfrak{p}_i$. By definition $\mathfrak{p}_i = \operatorname{ann} x$ for some $x \in R^\bullet$: we're done. □

PROPOSITION 10.9. *Let $S \subseteq R$ be multiplicatively closed.*

a) *If M is an $S^{-1}R$-module, then $\operatorname{Ass}_R M = \operatorname{Ass}_{S^{-1}R} M$.*
b) *If M is an R-module, then*

$$\operatorname{Ass}_R M \cap \operatorname{Spec} S^{-1}R \subseteq \operatorname{Ass}_{S^{-1}R} S^{-1}M.$$

c) *If R is Noetherian and M is an R-module, then*

$$\operatorname{Ass}_R M \cap \operatorname{Spec} S^{-1}R = \operatorname{Ass}_{S^{-1}R} S^{-1}M.$$

Let M be an R-module. A **weakly associated prime of M** is a prime ideal $\mathfrak{p}$ of R such that there is $x \in M$ with $\mathfrak{p} = r(\operatorname{ann} x)$. Thus the definition differs from the usual one in that we are permitted to pass from $\operatorname{ann} x$ to its radical. We denote by $\operatorname{weakAss} M$ the set of weakly associated primes of M.

EXERCISE 10.2. *Show: for an R-module M and $\mathfrak{p} \in \operatorname{Spec} R$, the following are equivalent:*

(i) *$\mathfrak{p}$ is weakly associated to M.*
(ii) *There is an ideal I of R with $r(I) = \mathfrak{p}$ and an R-module injection $R/I \hookrightarrow M$.*

EXERCISE 10.3. *Show: parts a) and b) of Proposition 10.9b) hold if we replace* Ass *by* weakAss *throughout.*

PROPOSITION 10.10. *Let M be an R-module.*

a) *We have $\operatorname{Ass} M \subseteq \operatorname{weakAss} M$.*
b) *If R is Noetherian, then $\operatorname{Ass} M = \operatorname{weakAss} M$.*

PROOF. a) As the terminology suggests, this is immediate: if $\mathfrak{p} = \operatorname{ann} x$, then $\operatorname{ann} x$ is prime, hence radical, so $\mathfrak{p} = r(\operatorname{ann} x)$.
b) By Proposition 10.9 it is enough to show that $\mathfrak{p} \in \operatorname{Ass}_{R_\mathfrak{p}} M_\mathfrak{p}$: replacing R by $R_\mathfrak{p}$ we may assume R is Noetherian local with maximal ideal $\mathfrak{p}$. Since $\mathfrak{p} \in \operatorname{weakAss} M$, there is $x \in M$ with $r(\operatorname{ann} x) = \mathfrak{p}$. Since R is Noetherian, by Proposition 4.17g) we have that $\mathfrak{p}^n \subseteq \operatorname{ann} x$ for some $n \in \mathbb{Z}^+$. Again using the Noetherian hypothesis, the set $\{\operatorname{ann} y \mid y \in R \text{ is such that } \operatorname{ann} y \supset \operatorname{ann} x\}$ has a maximal element $\operatorname{ann} y$, and by Proposition 10.4, $\mathfrak{q} = \operatorname{ann} y$ is prime. Then we have $\mathfrak{p}^n \subseteq \operatorname{ann} x \subseteq \mathfrak{q}$, and since $\mathfrak{q}$ is prime and $\mathfrak{p}$ is maximal, we have $\mathfrak{q} = \mathfrak{p}$ and thus $\mathfrak{p} \in \operatorname{Ass} M$. □

EXERCISE 10.4. *Let k be a field and $R = k[t_1, t_2, \ldots]$ be the polynomial ring in a countably infinite set of indeterminates over k. Let $I = \langle t_1^2, t_2^2, \ldots \rangle$, and let $\mathfrak{p} = r(I) = \langle t_1, t_2, \ldots \rangle$. Show: $\mathfrak{p} \in \operatorname{weakAss} R/I \setminus \operatorname{Ass} R/I$.*

2. The support of a module

For a module M over a ring R, we define its **support**

$$\operatorname{supp} M = \{\mathfrak{p} \in \operatorname{Spec} R \mid M_\mathfrak{p} \neq 0\}.$$

PROPOSITION 10.11. *For a finitely generated R-module M,*

$$\operatorname{supp} M = \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \supset \operatorname{ann} M\}.$$

PROOF. Write $M = \langle \omega_1, \ldots, \omega_n \rangle_R$. For $\mathfrak{p} \in \operatorname{Spec} R$, we have $\mathfrak{p} \in \operatorname{supp} M$ if and only if $M_\mathfrak{p} \neq 0$ iff for some $1 \leqslant i \leqslant n$ we have $\operatorname{ann}(\omega_i) \subseteq \mathfrak{p}$. If these conditions hold then

$$\operatorname{ann} M = \bigcap_{i=1}^n \operatorname{ann}(\omega_i) \subseteq \mathfrak{p}.$$

Conversely, if $\mathfrak{p}$ contains $\operatorname{ann}(M) = \bigcap_{i=1}^n \operatorname{ann}(\omega_i)$ then $\mathfrak{p}$ contains $\prod_{i=1}^n \operatorname{ann}(\omega_i)$ hence it contains $\operatorname{ann}(\omega_i)$ for some i, so $\mathfrak{p} \in \operatorname{supp} M$. □

We record the following result here, even though it involves some ideas from Chapter 13.

COROLLARY 10.12. *Let M be a finitely generated R-module.*

a) *The set* $\operatorname{supp} M$ *is a Zariski-closed subset of* $\operatorname{Spec} R$.
b) *If $\mathfrak{q} \supseteq \mathfrak{p}$ are prime ideals of R and $\mathfrak{p} \in \operatorname{supp} M$, then also $\mathfrak{q} \in \operatorname{supp} M$.*

PROOF. a) Indeed, Proposition 10.11 gives that $\operatorname{supp} M$ is the set of all prime ideals containing the ideal $\operatorname{ann} M$, which makes its Zariski-closed by definition. b) If $\mathfrak{q} \supseteq \mathfrak{p}$, then $\mathfrak{q}$ lies in the closure of $\mathfrak{p}$ (cf. §13.4), so this follows from part a). □

THEOREM 10.13. *Let M be an R-module.*

a) *We have* $\operatorname{weakAss} M \subseteq \operatorname{supp} M$.
b) *If R is Noetherian, the minimal elements of* $\operatorname{Ass} M$ *are the minimal elements of* $\operatorname{supp} M$.
c) *The minimal associated primes of R are the minimal primes of R.*

PROOF. a) Let $\mathfrak{p} \in \operatorname{weakAss} M$. By Exercise 10.2, there is an ideal I of R with $r(I) = \mathfrak{p}$ and an R-module embedding $R/I \hookrightarrow M$. Tensoring with the flat R-module $R_\mathfrak{p}$ gives an injection $R_\mathfrak{p}/IR_\mathfrak{p} \hookrightarrow M_\mathfrak{p}$. Since $r(I) = \mathfrak{p}$, $I \subseteq \mathfrak{p}$ and thus $IR_\mathfrak{p} \subseteq \mathfrak{p}R_\mathfrak{p} \subsetneq R_\mathfrak{p}$ and $M_\mathfrak{p} \supset R_\mathfrak{p}/IR_\mathfrak{p} \neq 0$.
b) Recall that under the Noetherian assumption $\operatorname{weakAss} M = \operatorname{Ass} M$.

Step 1: Each $\mathfrak{p} \in \operatorname{supp} M$ contains an element of $\operatorname{Ass} M$: indeed, let $\mathfrak{p} \in \operatorname{supp} M$, so $M_{\mathfrak{p}} \neq 0$. Since $R_{\mathfrak{p}}$ is Noetherian, Propositions 10.4b) and 10.9c) give

$$\varnothing \neq \operatorname{Ass}_{R_{\mathfrak{p}}} M_{\mathfrak{p}} = \operatorname{Ass}_R M \cap \operatorname{Spec} R_{\mathfrak{p}},$$

and an element of the latter set is precisely an associated prime $\mathfrak{q}$ of M with $\mathfrak{q} \subseteq \mathfrak{p}$.
Step 2: Let $\mathfrak{p} \in \operatorname{Ass} M$ be minimal, so by part a) $\mathfrak{p} \in \operatorname{supp} M$. If there were $\mathfrak{p}' \in \operatorname{supp} M$ with $\mathfrak{p}' \subsetneq \mathfrak{p}$ then there is no element in $\operatorname{Ass} M$ which is contained in $\mathfrak{p}'$, contradicting Step 1.
Step 3: Let $\mathfrak{p} \in \operatorname{supp} M$ be minimal. By Step 1, $\mathfrak{p}$ contains an element $\mathfrak{p}'$ of $\operatorname{Ass} M$, but since $\operatorname{Ass} M \subseteq \operatorname{supp} M$ and $\mathfrak{p}$ is minimal we must have $\mathfrak{p} = \mathfrak{p}'$.
c) Apply part b) to $M = R$. □

THEOREM 10.14. *If R is Noetherian,* $\operatorname{MinSpec} R$ *is finite.*

PROOF. Combine Theorem 10.7c) and Theorem 10.13c). □

Later we will give a *topological* proof of Theorem 10.14!

3. Primary Ideals

A proper ideal $\mathfrak{q}$ of a ring R is **primary** if for all $x, y \in R$, $xy \in \mathfrak{q}$ implies $x \in \mathfrak{q}$ or $y^n \in \mathfrak{q}$ for some $n \in \mathbb{Z}^+$.

EXERCISE 10.5.

a) *Show: a prime ideal is primary. (Trivial but important!)*
b) *Show: an ideal $\mathfrak{q}$ of R is primary if and only if every zero-divisor in $R/\mathfrak{q}$ is nilpotent.*

Neither the definition or primary ideal nor the characterization given in the above exercise is particularly enlightening, so one natural question is: which ideals are primary? (And, of course, another natural question is: what's the significance of a primary ideal?) Here are some simple results which give some information on primary ideals, sufficient to determine all the primary ideals in some simple rings.

PROPOSITION 10.15. *Let $\mathfrak{q}$ be an ideal in a ring R. If $r(\mathfrak{q}) = \mathfrak{m}$ is a maximal ideal, then $\mathfrak{q}$ is primary. In particular, any power of a maximal ideal is primary.*

PROOF. Since $r(\mathfrak{q})$ is the intersection of all prime ideals containing $\mathfrak{q}$, if this intersection is a maximal ideal $\mathfrak{m}$, then $\mathfrak{m}$ is the unique prime ideal containing $\mathfrak{q}$ and $R/\mathfrak{q}$ is a local ring with $\operatorname{nil}(R/\mathfrak{q}) = J(R/\mathfrak{q}) = \mathfrak{m}/\mathfrak{q}$. In such a ring an element is a zero-divisor if and only if it is a nonunit if and only if it is nilpotent, so $\mathfrak{q}$ is primary. The "in particular" follows since by Proposition 4.17f), $r(\mathfrak{m}^n) = r(\mathfrak{m}) = \mathfrak{m}$. □

PROPOSITION 10.16. *If $\mathfrak{q}$ is a primary ideal, then its radical $r(\mathfrak{q})$ is a prime ideal, the smallest prime ideal containing $\mathfrak{q}$.*

PROOF. Let $xy \in r(\mathfrak{q})$, so that $(xy)^m = x^m y^m \in \mathfrak{p}$ for some $m \in \mathbb{Z}^+$. If x^m is in $\mathfrak{q}$ then $x \in r(\mathfrak{q})$, so assume that x^m is not in $\mathfrak{q}$. Then y^m is a zero divisor in $R/\mathfrak{q}$, so by definition of primary there exists $n \in \mathbb{Z}^+$ such that $(y^m)^n \in \mathfrak{q}$, and then $y \in r(\mathfrak{q})$. The second statement holds for any ideal I whose radical is prime, since $r(I)$ is the intersection of all prime ideals containing I. □

A primary ideal is said to be $\mathfrak{p}$-**primary** if its radical is the prime ideal $\mathfrak{p}$.

LEMMA 10.17. *If $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$ are $\mathfrak{p}$-primary ideals, then $\mathfrak{q} = \bigcap_{i=1}^n \mathfrak{q}_i$ is $\mathfrak{p}$-primary.*

PROOF. Let x, y be elements of the ring R such that $xy \in \mathfrak{q}$ and $x \in R \backslash \mathfrak{q}$. Then for all $1 \leqslant i \leqslant n$, since $xy \in \mathfrak{q}_i$ there is $a_i \in \mathbb{Z}^+$ such that $y^{a_i} \in \mathfrak{q}_i$, and then $y^{a_1+\ldots+a_n} \in \mathfrak{q}$, so $\mathfrak{q}$ is primary. Moreover, by Proposition 4.17b) we have

$$r(\mathfrak{q}) = r(\bigcap_{i=1}^n \mathfrak{q}_i) = \bigcap_{i=1}^n r(\mathfrak{q}_i) = \bigcap_{i=1}^n \mathfrak{p} = \mathfrak{p}. \qquad \square$$

EXERCISE 10.6. *Give an example of primary ideals $\mathfrak{q}, \mathfrak{q}'$ such that $\mathfrak{q} \cap \mathfrak{q}'$ is not primary.*

PROPOSITION 10.18. *If $\mathfrak{q}$ is a primary ideal, the quotient ring $R/\mathfrak{q}$ is connected.*

PROOF. Indeed, a ring is disconnected if and only if it has an idempotent element e different from 0 or 1. Such an element is certainly not nilpotent $e^n = e$ for all n – but is a zero-divisor, since $e(1-e) = e - e^2 = 0$. $\square$

EXERCISE 10.7. *Let k be a field, let $R = k[x,y]$ and put $I = (xy)$. Show: I is not primary but "nevertheless" R/I is connected.*

EXAMPLE 10.19. *We will find all primary ideals in the ring $\mathbb{Z}$ of integers. Evidently (0) is prime and hence primary. If $\mathfrak{q}$ is any nonzero primary ideal, then its radical $\mathfrak{p} = r(\mathfrak{q})$ is a nonzero prime ideal, hence maximal. So, combining Propositions 10.15 and 10.16 we find that a nonzero ideal in $\mathbb{Z}$ is primary if and only if its radical is maximal. Moreover, for any prime power (p^n), $r((p^n)) = r((p)) = (p)$ is maximal – we use here the elementary and (we hope) familiar fact that if p is a prime number, (p) is a prime ideal (Euclid's Lemma); such matters will be studied in more generality in Chapter 15 – so (p^n) is a primary ideal. Conversely, if n is divisible by more than one prime power, then applying the Chinese Remainder Theorem, we get that $\mathbb{Z}/n$ is disconnected.*

EXERCISE 10.8.

a) *Let R be an domain for which each nonzero ideal is a (finite, of course) product of maximal ideals. Use the above argument to show that an ideal $\mathfrak{q}$ of R is primary if and only if it is a prime power.*
b) *(For those who know something about PIDs) Deduce in particular that primary = prime power in any principal ideal domain.*

Consider the following property of an domain:

(DD) Every ideal can be expressed as a product of prime ideals.

This is *a priori* weaker than the hypothesis of Exericse 10.8a). Later we will devote quite a lot of attention to the class of domains satisfying (DD), the **Dedekind domains**. Among their many properties is that a Dedekind domain is (either a field or) a domain in which each nonzero prime ideal is maximal. Thus in fact the hypothesis of Exercise 10.8a) is equivalent to assuming that R is a Dedekind domain.

Remark(ably): Another characterization theorem says that any Noetherian domain in which each primary ideal is a prime power is a Dedekind domain. In particular, any polynomial ring $k[x_1, \ldots, x_n]$ in $2 \leqslant n < \infty$ variables over a field admits primary ideals which are not prime powers.

EXERCISE 10.9. *Let $R = \mathbb{Z}[t]/(t^2+3)$ (or, equivalently, $\mathbb{Z}[\sqrt{-3}]$). Let $\mathfrak{q} = (2)$.*

a) *Show: there is a unique ideal $\mathfrak{p}_2$ with $R/\mathfrak{p}_2 = \mathbb{Z}/2\mathbb{Z}$. Evidently $\mathfrak{p}_2$ is maximal.*
b) *Show that $r(\mathfrak{q}) = \mathfrak{p}_2$, and deduce that I is primary.*
c) *Show that $\mathfrak{q}$ is not a prime power, and indeed, cannot be expressed as a product of prime ideals.*

Thus a primary ideal need not be a prime power. Conversely? It is a special case of Proposition 10.15 that any power of a maximal ideal is primary, but in general a power of prime ideal need not be primary:

EXAMPLE 10.20. [**AM**, p. 51] *Let k be a field; put $R = k[x,y,z]/(xy - z^2)$. Denote by $\overline{x}$, $\overline{y}$, and $\overline{z}$ the images of x, y, z in R. Put $\mathfrak{p} = \langle \overline{x}, \overline{z} \rangle$. Since $R/\mathfrak{p} = k[x,y,z]/(x, z, xy - z^2) = k[y]$ is a domain, $\mathfrak{p}$ is a prime ideal. Now consider the ideal $\mathfrak{p}^2$: we have $\overline{x}\,\overline{y} = \overline{z}^2 \in \mathfrak{p}^2$, but $\overline{x} \notin \mathfrak{p}^2$ and $\overline{y} \notin \mathfrak{p} = r(\mathfrak{p}^2)$, so $\mathfrak{p}^2$ is not primary.*

4. Primary Decomposition, Lasker and Noether

Let R be a ring and I an ideal of R. A **primary decomposition** of I is an expression of I as a finite intersection of primary ideals, say $I = \bigcap_{i=1}^n \mathfrak{q}_i$.

An ideal that admits at least one primary decomposition is said to be **decomposable**. This is not a piece of terminology that we will use often, but the reader should be aware of its existence.

For any ring R, let us either agree that R itself admits the "empty" primary decomposition or that R has no primary decomposition (i.e., it doesn't matter either way) and thereafter restrict our attention to proper ideals.

It may not be too surprising that not every ideal in every ring admits a primary decomposition. Indeed, we will see later that if R is a ring for which (0) admits a primary decomposition, then the ring R has finitely many minimal primes.

The first important result in this area was proved by Emanuel Lasker in 1905, roughly in the middle of his 27 year reign as world chess champion. Here it is.

THEOREM 10.21. *(Lasker [**La05**]) Let R be a polynomial ring in finitely many variables over a field. Every proper ideal I of R admits a primary decomposition.*

Lasker's proof of this theorem was a long and intricate calculation. As we will shortly see, a broader perspective yields considerably more for considerably less effort. In Lasker's honor a ring R in which every proper ideal admits a primary decomposition is called a **Laskerian ring**.

EXERCISE 10.10. *If R is Laskerian and I is an ideal of R, then R/I is Laskerian.*

Combining Lasker's theorem with this exercise, we get that every finitely generated algebra over a field admits a primary decomposition. This result is of fundamental (indeed, foundational) importance in algebraic geometry.

However, in 1921 Lasker's triumph was undeniably trumped by Emmy Noether.

To see how, we need one further concept. An ideal I is **irreducible** if whenever I is written as an intersection of two ideals – i.e., $I = J \cap K$ – then $I = J$ or $I = K$.

EXERCISE 10.11. *Let I be a proper ideal in a principal ideal domain R. Show: the following are equivalent:*

(i) *I is primary.*
(ii) *I is irreducible.*
(iii) *I is a prime power: there exists a in R and $n \in \mathbb{Z}^+$ such that (a) is prime and $I = (a)^n = (a^n)$.*

PROPOSITION 10.22.

a) *A prime ideal is irreducible.*
b) *An irreducible ideal in a Noetherian ring is primary.*

PROOF. a) Let $\mathfrak{p}$ be a prime ideal, and write $\mathfrak{p} = I \cap J$. Since then $\mathfrak{p} \supset IJ$, by Proposition 4.11 we have $\mathfrak{p} \supset I$ or $\mathfrak{p} \supset J$; WLOG say $\mathfrak{p} \supset I$. Then $\mathfrak{p} = I \cap J \subseteq I \subseteq \mathfrak{p}$, so that we must have $I = \mathfrak{p}$.

b) By passage to the quotient, we may assume that (0) is irreducible and show that it is primary. So suppose $xy = 0$ and $x \neq 0$. Consider the chain of ideals

$$\operatorname{ann}(y) \subseteq \operatorname{ann}(y^2) \subseteq \ldots \subseteq \operatorname{ann}(y^n) \subseteq \ldots.$$

Since R is Noetherian, this chain stabilizes: there exists n such that $\operatorname{ann}(y^n) = \operatorname{ann}(y^{n+k})$ for all k. We claim that $(x) \cap (y^n) = 0$. Indeed, if $a \in (x)$ then $ay = 0$, and if $a \in (y^n)$ then $a = by^n$ for some $b \in R$, hence $by^{n+1} = ay = 0$, so $b \in \operatorname{ann}(y^{n+1}) = \operatorname{ann}(y^n)$, hence $a = by^n = 0$. Since the (0) ideal is irreducible, we must then have $y^n = 0$, and this shows that (0) is primary. □

EXERCISE 10.12. *This exercise is taken from a post of E. Merkulova on http://math.stackexchange.com/questions/28620. Let k be a field, $R = k[x, y]$ and $I = \langle x^2, xy, y^2 \rangle$.*

a) *Show: I is primary. (Hint: use Proposition 10.15.)*
b) *Show: $I = \langle x, y^2 \rangle \cap \langle x^2, y \rangle$.*
c) *Deduce: I is an ideal in a (very nice) Noetherian domain which is primary but not irreducible.*

THEOREM 10.23. *(Noether) A proper ideal in a Noetherian ring admits a primary decomposition.*

PROOF. Let I be a proper ideal in the Noetherian ring R. We claim I is a finite intersection of *irreducible* ideals; in view of Proposition 10.22 this gives the desired result. To see this: suppose that the set of proper ideals that cannot be written as a finite intersection of irreducible ideals is nonempty, and choose a maximal element I. Then I is reducible, so we may write $I = J \cap K$ where each of J and K is strictly larger than I. Being strictly larger than I, each of J and K can be written as a finite intersection of irreducible ideals, hence so can I. Contradiction! □

In other words, a Noetherian ring is Laskerian. Therefore Lasker's Theorem is an immediate consequence of Noether's Theorem together with the Hilbert Basis Theorem, which we recall, was proved in 1888 and whose remarkably short and simple – but nonconstructive – proof engendered first controversy and later deep admiration. The same is true for Noether's theorem: it is from this theorem, and the ridiculous simplicity of its proof, that Noetherian rings get their name.

EXERCISE 10.13. *Let R be a Noetherian ring, with minimal primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$. Show: there is $N \in \mathbb{Z}^+$ such that $(0) = \bigcap_{i=1}^r \mathfrak{p}_i^N$. (Hint: use Proposition 4.17g).)*

5. Irredundant primary decompositions

If an ideal can be expressed as a product of prime ideals, that product is in fact unique. We would like to have similar results for primary decomposition. Unfortunately such a uniqueness result is clearly impossible. Indeed, if $I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n$ is a primary decomposition of I and $\mathfrak{p}$ is any prime containing I, then $\mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_n \cap \mathfrak{p}$ is also a primary decomposition, and clearly a different one if $\mathfrak{p} \neq \mathfrak{q}_i$ for any i. A proper ideal I may well be contained in infinitely many primes – e.g. this occurs with $I = (0)$ for any Noetherian domain of dimension at least 2 – so there may well be infinitely many different primary decompositions.

But of course throwing in extra primes is both frivolous and wasteful. The following definition formalizes the idea of a primary decomposition which is "frugal" in two reasonable ways.

A primary decomposition is said to be **irredundant**[1] (or **minimal**, or **reduced**) if both of the following properties hold:

(IPD1) For all $i \neq j$, $r(\mathfrak{q}_i) \neq r(\mathfrak{q}_j)$.
(IPD2) For all i, $\mathfrak{q}_i$ does not contain $\bigcap_{j \neq i} \mathfrak{q}_j$.

If wastefulness succeeds, so does frugality:

LEMMA 10.24. *An ideal that admits a primary decomposition admits an irredundant primary decomposition.*

PROOF. By Lemma 10.17, we may replace any collection of primary ideals $\mathfrak{q}_i$ with a common radical with their intersection and still have a primary ideal, thus satisfying (IPD1). Then if (IPD2) is not satisfied, there is some $\mathfrak{q}_i$ which contains the intersection of all the other $\mathfrak{q}_j$'s, hence it can be removed to obtain a primary decomposition satisfying (IPD1) and with a smaller number of primary ideals. Proceeding in this way we eventually arrive at an irredundant primary decomposition. □

The question is now to what extent an irredundant primary decomposition is unique. The situation here is significantly better: although the primary decomposition is not in all cases unique, it turns out that there are some important quantities which are defined in terms of a primary decomposition and which can be shown to be independent of the choice of irredundant decomposition, i.e., are invariants of the ideal. Such uniqueness results are pursued in the next section.

6. Uniqueness properties of primary decomposition

Recall that for ideals I and J of a ring R, $(I : J) = \{x \in R \mid xJ \subseteq I\}$, which is also an ideal of R. We abbreviate $(I : (x))$ to $(I : x)$ and $((x) : J)$ to $(x : J)$.

EXERCISE 10.14. *Show: for ideals I and J, we have $I \subseteq (I : J)$.*

[1]It is amusing to note that most dictionaries do not recognize "irredundant" as an English word, but mathematicians have been using it in this and other contexts for many years.

LEMMA 10.25. *Let $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal and $x \in R$.*

a) *If $x \in \mathfrak{q}$ then $(\mathfrak{q} : x) = R$.*
b) *If $x \notin \mathfrak{q}$ then $(\mathfrak{q} : x)$ is $\mathfrak{p}$-primary.*
c) *If $x \notin \mathfrak{p}$ then $(\mathfrak{q} : x) = \mathfrak{q}$.*

PROOF. a) If $x \in \mathfrak{q}$ then $1(x) = x \subseteq \mathfrak{q}$, so $1 \in (\mathfrak{q} : x)$.
b) If $y \in (\mathfrak{q} : x)$, then $xy \in \mathfrak{q}$; by assumption $x \notin \mathfrak{q}$, so $y^n \in \mathfrak{q}$ for some n and thus $y \in r(\mathfrak{q}) = \mathfrak{p}$. So $\mathfrak{q} \subseteq (\mathfrak{q} : x) \subseteq \mathfrak{p}$; taking radicals we get $r((\mathfrak{q} : x)) = \mathfrak{p}$. Moreover, if $yz \in (\mathfrak{q} : x)$ with $y \notin (\mathfrak{q} : x)$, then $xyz = y(xz) \in \mathfrak{q}$, so $(xz)^n = x^n z^n \in \mathfrak{q}$ for some n, and $x^n \notin \mathfrak{q} \implies (z^m)^n \in \mathfrak{q}$ for some $n \in \mathbb{Z}^+$, thus $z^{mn} \in \mathfrak{q} \subseteq (\mathfrak{q} : x)$.
c) We have in all cases that $\mathfrak{q} \subseteq (\mathfrak{q} : x)$. If $x \notin \mathfrak{p} = r(\mathfrak{q})$ and $y \in (\mathfrak{q} : x)$, then $xy \in \mathfrak{q}$; since no power of x is $\mathfrak{q}$, we must have $y \in \mathfrak{q}$. □

THEOREM 10.26. *(First Uniqueness Theorem) Let $I = \bigcap_{i=1}^n \mathfrak{q}_i$ be any irredundant primary decomposition of the ideal I. Let $\mathfrak{p}_i = r(\mathfrak{q}_i)$. Then the $\mathfrak{p}_i$'s are precisely the prime ideals of the form $r((I : x))$ as x ranges through elements of R. In particular, they are independent of the choice of irredundant primary decomposition.*

PROOF. For $x \in R$ we have $(I : x) = (\bigcap_i \mathfrak{q}_i : x) = \bigcap_i (\mathfrak{q}_i : x)$, so

$$r((I : x)) = \bigcap_i r((q_i : x)) = \bigcap_{x \notin \mathfrak{q}_j} \mathfrak{p}_j$$

by Lemma 10.25. If $r(I : x)$ is prime, then $r(I : x) =$
p_j for some j. Conversely, for each i, by irredundancy of the decomposition there exists $x_i \in \bigcap_{j \neq i} \mathfrak{q}_j \backslash \mathfrak{q}_i$ and then the Lemma implies $r(I : x_i) = \mathfrak{p}_i$. □

COROLLARY 10.27. *Let R be Noetherian, and let $I \subsetneq R$ be a proper ideal. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the radicals of the primary ideals in an(y) irredundant primary decomposition of I. Then*

$$\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\} = \operatorname{Ass} R/I.$$

PROOF. By Theorem 10.26 the $\mathfrak{p}_i$'s are precisely the elements of $\operatorname{weakAss} R/I$. Since R is Noetherian, so is R/I and thus by Proposition 10.10b) $\operatorname{weakAss} R/I = \operatorname{Ass} R/I$. □

PROPOSITION 10.28. *Let $I = \bigcap_{i=1}^n \mathfrak{q}_i$ be a primary decomposition of an ideal I, with $\mathfrak{p}_i = r(\mathfrak{q}_i)$. Then any prime ideal $\mathfrak{p}$ containing I contains $\mathfrak{p}_i$ for some i.*

PROOF. If $\mathfrak{p} \supset I = \bigcap_i \mathfrak{q}_i$, then

$$\mathfrak{p} = r(\mathfrak{p}) \supset \bigcap_i r(\mathfrak{q}_i) = \bigcap_i \mathfrak{p}_i.$$

Since $\mathfrak{p}$ is prime, $\mathfrak{p} \supset \mathfrak{p}_i$ for some i. □

EXERCISE 10.15. *Show: an infinite Boolean ring is not Laskerian.*

PROPOSITION 10.29. *Let $I \subseteq R$ be a decomposable ideal, $I = \bigcap_{i=1}^n \mathfrak{q}_i$ an irredundant primary decomposition, and $\mathfrak{p}_i = r(\mathfrak{q}_i)$. Then*

$$\bigcup_{i=1}^n \mathfrak{p}_i = \{x \in R : (I : x) \neq I\}.$$

In particular, if the zero ideal is decomposable, then the set of zero divisors of R is the union of the minimal associated primes of R.

PROOF. By passage to the quotient ring R/I, we may assume that $I = 0$. Let $0 = \bigcap_{i=1}^r \mathfrak{q}_i$ be a primary decomposition, with $\mathfrak{p}_i = r(\mathfrak{q}_i)$. For $x \in R$, $((0) : x) \neq (0)$ if and only if x is a zero-divisor, so it suffices to show the last statement of the proposition, that the union of the minimal primes is the set of all zero-divisors. Let D be the set of all zero divisors, so from Exercise 3.X and the proof of Theorem 10.26 we have

$$D = r(D) = \bigcup_{0 \neq x} r((0 : x)) = \bigcup_{0 \neq x} \bigcap_{x \notin \mathfrak{q}_j} \mathfrak{p}_j \subset \bigcup_j \mathfrak{p}_j.$$

Conversely, by Theorem 10.26 each $\mathfrak{p}_i$ is of the form $r((0 : x))$ for some $x \in R$. □

THEOREM 10.30. *(Second Uniqueness Theorem) Let I be an ideal of R, and let*

$$\bigcap_{i=1}^n \mathfrak{q}_i = I = \bigcap_{j=1}^m \mathfrak{r}_j$$

be two irredundant primary decompositions for an ideal I. By Theorem 10.26 we know that $m = n$ and that there is a reordering $\mathfrak{r}_1, \ldots, \mathfrak{r}_n$ of the $\mathfrak{r}_j$'s such that for $1 \leqslant i \leqslant n$, $r(\mathfrak{q}_i) = \mathfrak{p}_i = r(\mathfrak{r}_i)$. Moreover, if $\mathfrak{p}_i$ is minimal, then $\mathfrak{q}_i = \mathfrak{r}_j$.

In other words, the primary ideals corresponding to the minimal primes are independent of the primary decomposition.

We will use the technique of localization to prove this result, so first we need some preliminaries on the effect of localization on a primary decomposition.

PROPOSITION 10.31. *Let R be a ring, $S \subseteq R$ a multiplicatively closed set, and $\mathfrak{q}$ be a $\mathfrak{p}$-primary ideal. Write $\iota : R \to S^{-1}R$ for the localization map.*

a) *If $S \cap \mathfrak{p} \neq \varnothing$, then $\iota_*(\mathfrak{q}) = S^{-1}R$.*
b) *If $S \cap \mathfrak{p} = \varnothing$, then $\iota_*(\mathfrak{q})$ is $\iota_*(\mathfrak{p})$-primary, and $\iota^*(\iota_*(\mathfrak{q})) = \mathfrak{q}$.*

PROOF. a) If $x \in S \cap \mathfrak{p}$, then for some $n \in \mathbb{Z}^+$, $x^n \in S \cap \mathfrak{q}$, so $\iota_*(\mathfrak{q})$ contains a unit of $S^{-1}R$ and is therefore $S^{-1}R$. Part b) follows immediately from Proposition 7.4 and Proposition 7.6a). □

PROPOSITION 10.32. *Let $S \subseteq R$ be a multiplicatively closed set, and let $I = \bigcap_{i=1}^n \mathfrak{q}_i$ be an irredundant primary decomposition of an ideal I. Put $\mathfrak{p}_i = r(\mathfrak{q}_i)$ and suppose that the numbering is such that $S \cap \mathfrak{p}_i = \varnothing$ for $i \leqslant m$ and $S \cap \mathfrak{p}_i \neq \varnothing$ for $i > m$. Then:*

$$\iota_*(I) = \bigcap_{i=1}^m \iota_*(\mathfrak{q}_i),$$

$$\iota^*\iota_*(I) = \bigcap_{i=1}^m \mathfrak{q}_i,$$

and both of these are irredundant primary decompositions.

EXERCISE 10.16. *Prove Proposition 10.32.*

Proof of Theorem 10.30: let $\mathfrak{p}_i$ be a minimal associated prime, and put $S = R\backslash\mathfrak{p}_i$. Certainly S is a multiplicatively closed set, and moreover by minimality $\mathfrak{p}_i$ is the unique associated prime which is disjoint from S. Applying Proposition 10.32 to both primary decompositions gives

$$\mathfrak{q}_i = \iota^* \iota_* (I) = \mathfrak{r}_i.$$

□

7. Applications in dimension zero

We now give the proof of the uniqueness portion of Theorem 8.37. Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_n$ be the distinct maximal ideals of the Artinian ring R. As in the proof of Theorem 8.37a) there exists $k \in \mathbb{Z}^+$ such that $\prod_{i=1}^n \mathfrak{m}_i^k = \cap_{i=1}^n \mathfrak{m}_i^k = 0$. For each i, the radical $r(\mathfrak{m}_i^k)$ is the maximal ideal $\mathfrak{m}_i$, so by Proposition 10.15 each $\mathfrak{m}_i^k$ is an $\mathfrak{m}_i$-primary ideal. Thus $0 = \bigcap_{i=1}^n \mathfrak{m}_i^k$ is a primary decomposition of the zero ideal which is moreover immediately seen to be irredundant. Since all the primes $\mathfrak{m}_i$ are maximal, the desired uniqueness statement of Theorem 8.37b) follows from the Second Uniqueness Theorem (Theorem 10.30) for primary decompositions.

8. Applications in dimension one

Let R be a one-dimensional Noetherian domain, and I a nonzero ideal. Then by Theorem 10.23, I has a primary decomposition: $I = \bigcap_{i=1}^n \mathfrak{q}_i$, where $\mathfrak{p}_i = r(\mathfrak{q}_i) \supset \mathfrak{q}_i \supset I$ is a nonzero prime ideal. But therefore each $\mathfrak{p}_i$ is maximal, so that the $\mathfrak{p}_i$'s are pairwise comaximal. By Proposition 4.20, so too are the $\mathfrak{q}_i$'s, so the Chinese Remainder Theorem applies to give

$$I = \bigcap_{i=1}^n \mathfrak{q}_i = \prod_{i=1}^n \mathfrak{q}_i,$$

and

$$R/I \cong \prod_{i=1}^n R/\mathfrak{q}_i.$$

Thus in this case we can decompose any proper ideal as a finite *product* of primary ideals and not just a finite intersection. Moreover, for $I \neq 0$, all the associated primes are minimal over I, so the Uniqueness Theorems (Theorems 10.26 and 10.30) simply assert that the ideals $\mathfrak{q}_i$ are unique. This observation will be very useful in our later study of ideal theory in one dimensional Noetherian domains.

CHAPTER 11

Nullstellensätze

Let k be a field. By an **affine algebra over k** we simply mean a finitely generated k-algebra. Of all the various and sundry classes of commutative rings we have met and will meet later in these notes, affine algebras are probably the most important and most heavily studied, because of their connection to algebraic geometry.

1. Zariski's Lemma

In 1947 Oscar Zariski published a short note [**Za47**] proving the following result.

THEOREM 11.1. *(Zariski's Lemma) Let k be a field, A a finitely generated k-algebra, and $\mathfrak{m} \in \operatorname{MaxSpec} A$. Then $A/\mathfrak{m}$ is a finite degree field extension of k.*

EXERCISE 11.1. *Show: the following is an equivalent restatement of Zariski's Lemma: let K/k be a field extension such that K is finitely generated as a k-algebra. Then K/k is an algebraic field extension.*

Notwithstanding its innocuous appearance, Zariski's Lemma is a useful result on affine algebras over any field. Further, when k is algebraically closed, it carries all of the content of Hilbert's Nullstellensatz, the main theorem of this section.

So how do we prove Zariski's Lemma?

Oh, let us count the ways! The literature contains many interesting proofs, employing an impressively wide range of ideas and prior technology. We will in fact give several different proofs during the course of these notes. Of course some pride of place goes to the *first proof* that we give, so after much thought (and after changing our mind at least once!) we have decided on the following.

1.1. Proof of Zariski's Lemma via the Artin-Tate Lemma.

As in Exercise 11.1, it suffices to prove the following: let K/k be a field extension that is finitely generated as a k-algebra. We claim K/k is algebraic.

Indeed, if not, let $x_1, \ldots, x_n$ be a transcendence basis for K/k ($n \geq 1$ since K/k is transcendental), put $k(x) = k(x_1, \ldots, x_n)$ and consider the tower of rings

$$k \subset k(x) \subset K. \tag{31}$$

To be sure, we recall the definition of a transcendence basis: the elements x_i are algebraically independent over k and $K/k(x)$ is algebraic. But since K is a finitely generated k-algebra, it is certainly a finitely generated $k(x)$-algebra and thus $K/k(x)$ is a finite degree field extension. Thus the Artin-Tate Lemma applies to (31): we conclude that $k(x)/k$ is a finitely generated k-algebra. But this is absurd. It implies the much weaker statement that $k(x) = k(x_1, \ldots, x_{n-1})(x_n)$ is finitely generated

as a $k(x_1, \ldots, x_{n-1})[x_n]$-algebra, or weaker yet, that there exists some field F such that $F(t)$ is finitely generated as an $F[t]$-algebra: i.e., there exist finitely many rational functions $\{r_i(t) = \frac{p_i(t)}{q_i(t)}\}_{i=1}^N$ such that every rational function is a polynomial in the r_i's with k-coefficients. But $F[t]$ is a PID with infinitely many nonassociate nonzero prime elements q (e.g. adapt Euclid's argument of the infinitude of the primes), so we may choose a nonzero prime element q which does not divide $q_i(t)$ for any i. It is then clear that $\frac{1}{q}$ cannot be a polynomial in the $r_i(t)$'s: for instance, evaluation at a root of q in $\overline{F}$ leads to a contradiction. □

Remark: The phenomenon encountered in the endgame of the preceding proof will be studied in great detail in §12. What we are actually showing is that for any field F, the polynomial ring $F[t]$ is not a **Goldman domain**, and indeed this is closely related to the fact that $\operatorname{Spec} F[t]$ is infinite. More on this later.

1.2. McCabe's Proof of Zariski's Lemma.

We will give one further proof of Zariski's Lemma now (and more later...), an extremely elegant and simple one due to J. McCabe [**McC76**].

Let K/k be a field extension that is finitely generated as a k-algebra, say by $x_1, \ldots, x_n$. Reorder the x_i's so that $x_1, \ldots, x_t$ are algebraically independent over k and $x_{t+1}, \ldots, x_n$ are algebraic over $k(x_1, \ldots, x_n)$. We may assume $t \geqslant 1$, for otherwise K/k is finitely generated algebraic field extension, hence of finite degree.

Let $S = k[x_1, \ldots, x_t]$, so S is a polynomial ring and *is not* a field. There is $y \in S^\bullet$ such that $yx_{t+1}, \ldots, yx_n$ are all integral over $S[\frac{1}{y}]$. We have $k \subset S[\frac{1}{y}]$ and $x_1, \ldots, x_t \in S[\frac{1}{y}]$, so $K = k[x_1, \ldots, x_n]$ is integral over $S[\frac{1}{y}]$. Since K is a field, by Proposition 1.10 so is $S[\frac{1}{y}]$.

Let $\mathfrak{m} \in \operatorname{MaxSpec} S$. Since $t \geqslant 1$, $\mathfrak{m} \neq (0)$, so let $f \in \mathfrak{m}^\bullet$. Then f is invertible in the field $S[\frac{1}{y}]$ so there is $g \in S$ and $N \in \mathbb{Z}^+$ such that $\frac{1}{f} = \frac{g}{y^N}$ and thus $y^N = fg$. Since $f \in \mathfrak{m}$ and maximal ideals are prime, $y \in \mathfrak{m}$. It follows that y lies in every maximal ideal of S, hence $1 + y$ lies in no maximal ideal and is thus a unit in S. But $S^\times = k[x_1, \ldots, x_n]^\times = k^\times$, so $1 + y \in k^\times$ and $y \in k^\bullet$. Thus $k[x_1, \ldots, x_t] = k[x_1, \ldots, x_t, \frac{1}{y}] = S[\frac{1}{y}]$ is a field: contradiction!

2. Hilbert's Nullstellensatz

Let k be a field, let $R_n = k[t_1, \ldots, t_n]$, and write $\mathbb{A}^n$ for k^n. We introduce an antitone Galois connection (V, I) between subsets of R_n and subsets of $\mathbb{A}^n$. Namely:

For $S \subset \mathbb{A}^n$, we put

$$I(S) = \{f \in R_n \mid \forall x \in S,\ f(x) = 0\}.$$

In other words, $I(S)$ is the set of polynomials which vanish at every element of S. Conversely, for $J \subset R_n$, we put

$$V(J) = \{x \in \mathbb{A}^n \mid \forall f \in J,\ f(x) = 0\}.$$

This is nothing else than the Galois relation associated to the relation $f(x) = 0$ on the Cartesian product $R_n \times \mathbb{A}^n$.

As usual, we would like to say something about the induced closure operators on R_n and $\mathbb{A}^n$. First, for any subset S of $\mathbb{A}^n$, $I(S)$ is not just a subset but an ideal of R_n. In fact $I(S)$ is a radical ideal: indeed, if $f^n \in I(S)$ then f^n vanishes on every point of S, so f vanishes at every point of S.

This little bit of structure pulled from thin air will quicken the heart of any Bourbakiste. But beyond the formalism, the key question is: exactly which sets are closed? Without knowing this, we haven't proved the Nullstellensatz any more than the analogous formalities between sets and groups of automorphisms prove the Galois correspondence for Galois field extensions.

Indeed, an ideal I is radical if $f^n \in I$ implies $f \in I$. But if f^n vanishes identically on S, then so does f.

The closed subsets of $\mathbb{A}^n$ are closed under arbitrary intersections (including the "empty intersection": $\mathbb{A}^n = V((0))$ and under finite unions (including the "empty union": $\varnothing = V(\{1\}) = V(R_n)$, and therefore form the closed sets for a unique topology on $\mathbb{A}^n$, the **Zariski topology**.

Exercise 11.2.

a) *Prove these facts.*
b) *Show: the Zariski topology on $\mathbb{A}^n_{/k}$ coincides with the topology it inherits as a subset of $\mathbb{A}^n_{/\overline{k}}$.*
c) *Show: the Zariski topology is separated: i.e., singleton subsets are closed.*
d) *Show: when $n = 1$, the Zariski topology is the coarsest T_1 topology on k: namely, the topology in which a proper subset is closed if and only if it is finite.*
e) *For any $n \geq 1$, show: the Zariski topology on k^n is discrete if and only if k is finite.*
f) *For any infinite field and $m, n \geq 1$, show: the Zariski topology on k^{m+n} is strictly finer than the product of the Zariski topologies on k^m and k^n.*

Exercise 11.3. *Let k be a field and $n \in \mathbb{Z}^+$ as above. Explicitly compute the ideal $I(k^n)$, i.e., the set of all polynomials which vanish at* every *point of k^n. Do we necessarily have $I(k^n) = \{0\}$?*

Lemma 11.2. *For $a = (a_1, \ldots, a_n) \in k^n$, put $\mathfrak{m}_a = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$. Then:*

a) *We have $R_n/\mathfrak{m}_a = k$. In particular $\mathfrak{m}_a$ is maximal.*
b) *$\mathfrak{m}_a = I(\{a\})$ is the ideal of all functions vanishing at a.*
c) *The assignment $a \mapsto \mathfrak{m}_a$ is a bijection from k^n to the set of all maximal ideals $\mathfrak{m}$ of R_n such that $R_n/\mathfrak{m} = k$.*

Proof. Part a) is obvious (but important).
b) Certainly each $x_i - a_i$ vanishes at a, so $\mathfrak{m}_a \subset I(\{a\})$. But by part a) $\mathfrak{m}_a$ is a maximal ideal, whereas $1 \notin I(\{a\})$, so we must have $\mathfrak{m}_a = I(\{a\})$.
c) The mapping $a \mapsto \mathfrak{m}_a$ is an injection from k^n to the set of maximal ideals with residue field k. Conversely, let $\mathfrak{m}$ be an ideal of R_n with $R_n/\mathfrak{m} = k$. For $1 \leq i \leq n$ let a_i be the image of x_i in $R_n/\mathfrak{m} = k$. Then $\mathfrak{m} \supset \mathfrak{m}_a$ so we must have equality. □

We now pause for a very important definition. A ring R is a **Jacobson ring** if it is "sufficiently many maximal ideals": more precisely, such that every prime ideal $\mathfrak{p}$ of R is the intersection of the maximal ideals that contain it.

EXERCISE 11.4.

a) *Show: a ring R is a Jacobson ring if and only if for every ideal I, the intersection of all maximal ideals containing I is* $\operatorname{rad}(I)$.
b) *Show: every homomorphic image of a Jacobson ring is Jacobson.*

PROPOSITION 11.3. *(Rabinowitsch Trick* [**Ra30**]*) Let k be a field and $n \in \mathbb{Z}^+$.*

a) *The ring $R = k[x_1, \ldots, x_n]$ is a Jacobson ring.*
b) *It follows that any affine k-algebra is a Jacobson ring.*

PROOF. a) It is sufficient to show that for each prime ideal $\mathfrak{p}$ of R and $a \in R \backslash \mathfrak{p}$, there exists a maximal ideal $\mathfrak{m}$ containing $\mathfrak{p}$ and not containing a.

To show this, put $R_a := R[\frac{1}{a}]$, and let $\mathfrak{p}_a = \mathfrak{p}R_a$ be the pushed forward ideal. Since $\mathfrak{p}$ does not meet the multiplicative set generated by a, $\mathfrak{p}_a$ is still prime in R_a. Let $\mathfrak{m}_a$ be any maximal ideal of R_a containing $\mathfrak{p}_a$, and let $\mathfrak{m} = \mathfrak{m}_a \cap R$ be its contraction to R: *a priori*, this is a prime ideal. There is an induced k-algebra embedding $R/\mathfrak{m} \hookrightarrow R_a/\mathfrak{m}_a$. But R_a is still a finitely generated algebra so by Zariski's Lemma (Theorem 11.1) $R_a/\mathfrak{m}_a$ is finite dimensional as a k-vector space, hence so is the subspace $R/\mathfrak{m}$. Thus the domain $R/\mathfrak{m}$ must be a field: let $x \in (R/\mathfrak{m})^\bullet$, and write out a linear dependence relation of minimal degree among the powers of x:

$$x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0, \ c_i \in k, \ c_0 \neq 0.$$

Thus

$$x\left(x^{n-1} + c_{n-1}x^{n-2} + \ldots + c_1\right) = \frac{-1}{c_0},$$

so x is invertible. Thus $\mathfrak{m}$ is the desired maximal ideal.
b) This follows immediately from Exercise 11.4. □

Remark: It seems that the author "J.L. Rabinowitsch," the author of [**Ra30**] is in fact *George Yuri Rainich*, a distinguished Russian-American mathematician.

We prove one last fact before imposing the hypothesis that k is algebraically closed.

PROPOSITION 11.4. *Let k be any field and J an ideal of $k[x] = k[x_1, \ldots, x_n]$.*

a) *We have $V(J) = V(\operatorname{rad} J)$.*
b) *For any subset $S \subset k^n$, the ideal $I(S)$ is radical.*
c) *$I(V(J))$ is a radical ideal containing* $\operatorname{rad} J$.

PROOF. The underlying mechanism here is the following truly basic observation: for $f \in k[x]$, $P \in k^n$ and $m \in \mathbb{Z}^+$, we have

$$f(P) = 0 \iff f^m(P) = 0.$$

a) Since $J \subset \operatorname{rad} J$ we have $V(J) \supset V(\operatorname{rad} J)$. Conversely, let $P \in V(J)$ and $f \in \operatorname{rad} J$. Then there is $m \in \mathbb{Z}^+$ such that $f^m \in J$, so $f^m(P) = 0$ and thus $f(P) = 0$. It follows that $P \in V(\operatorname{rad} J)$.
b) Similarly, for any $f \in k[x]$ and $m \in \mathbb{Z}^+$, if $f^m \in I(S)$, then for all $P \in S$, $f^m(P) = 0$. But this implies $f(P) = 0$ for all $P \in S$ and thus $f \in I(S)$.
c) This follows immediately from parts a) and b) and the tautological fact that for any ideal J of $k[x]$, $I(V(J)) \supset J$. □

Finally we specialize to the case in which the field k is algebraically closed. We have done almost all the work necessary to establish the following fundamental result.

THEOREM 11.5. *(Hilbert's Nullstellensatz) Let k be an algebraically closed field, let $k[x] = k[x_1, \ldots, x_n]$. Then:*

a) *I induces a bijective correspondence between the singleton sets of k^n and the maximal ideals: $a \in k^n \mapsto \mathfrak{m}_a = \langle x_1 - a_1, \ldots, x_n - a_n \rangle$.*
b) *For any Zariski-closed subset $S \subset k^n$, we have $V(I(S)) = S$.*
c) *For any ideal J of R_n, we have $I(V(J)) = \mathrm{rad}(J)$.*
*Thus there is an inclusion-reversing, bijective correspondence between Zariski-closed subsets of k^n and **radical** ideals of $k[x]$.*

PROOF. a) Let $\mathfrak{m}$ be a maximal ideal of $k[x]$. By Theorem 11.1, the residue field $k[x]/\mathfrak{m}$ is a finite degree extension of k. Since k is algebraically closed, this forces $k[x]/\mathfrak{m} = k$, and now Lemma 11.2 applies.
b) There is no content here: it is part of the formalism of Galois connections.
c) By Proposition 11.4, it is no loss of generality to assume that J is a radical ideal. Further, by Proposition 11.3, $k[x]$ is a Jacobson ring, so any radical ideal J is the intersection of the maximal ideals $\mathfrak{m}$ containing it. This is true over any field k. But combining with part a), we get that J is an intersection of maximal ideals of the form $\mathfrak{m}_a$ for certain points $a \in k^n$. Since $\mathfrak{m}_a = I(\{a\})$, $J \subset \mathfrak{m}_a$ if and only if every element of J vanishes at a, in other words if and only if $a \in V(J)$. Thus J is equal to the set of all polynomials $f \in R_n$ which vanish at every point of $V(J)$: $J = I(V(J))$! □

EXERCISE 11.5. *Let k be a field. Show that if either part a) or part c) of Theorem 11.5 holds for the rings $k[x_1, \ldots, x_n]$, then k is algebraically closed. (Hint: in fact both parts fail for each $n \in \mathbb{Z}^+$, including $n = 1$.)*

EXERCISE 11.6. *Show: Zariski's Lemma in the case that k is algebraically closed is equivalent to the following statement: let $J = \langle f_1, \ldots, f_m \rangle$ be an ideal in $k[x_1, \ldots, x_n]$. Then either there exists a simultaneous zero a of $f_1, \ldots, f_m$ or there exist polynomials $g_1, \ldots, g_m$ such that $g_1 f_1 + \ldots + g_m f_m = 1$.*

2.1. The Semirational Nullstellensatz.

LEMMA 11.6. *(Lang's Lemma) Let k be a field, L an algebraically closed field, $\varphi : k \to L$ a field embedding, and R a finitely generated k-algebra. Then there is a homomorphism $\Phi : R \to L$ extending φ.*

PROOF. Let $\mathfrak{m}$ be a maximal ideal of k. By Zariski's Lemma, $R/\mathfrak{m}$ is a finite degree field extension of k, so by basic field theory it embeds as a k-algebra into any algebraically closed field containing k. □

Remark: In [**Lg02**, § IX.1], Lang gives a direct proof of Lemma 11.6. It is easy to see that Lemma 11.6 implies Zariski's Lemma, so this gives another way to proceed.

COROLLARY 11.7. *Let k be a field, and let R be a domain that is finitely generated as a k-algebra. For any $y_1, \ldots, y_n \in R^\bullet$, there is a homomorphism $\psi : R \to \overline{k}$ such that $\psi(y_i) \neq 0$ for $1 \leqslant i \leqslant n$.*

PROOF. Apply Lang's Lemma to the ring $R[\frac{1}{y_1}, \ldots, \frac{1}{y_n}]$. □

COROLLARY 11.8. *Let J be a proper ideal of $k[t_1, \ldots, t_n]$. Then there is $x \in \overline{k}^n$ such that for all $f \in J$, $f(x) = 0$.*

PROOF. Let $\mathfrak{m}$ be a maximal ideal containing J. Zariski's Lemma gives a k-algebra embedding $\psi : k[t_1, \ldots, t_n]/\mathfrak{m} \hookrightarrow \overline{k}$. Let $(x_1, \ldots, x_n) = (\psi(t_1), \ldots, \psi(t_n))$. □

For an ideal J of $k[t_1, \ldots, t_n]$, let $V^a(J)$ be the set of $x = (x_1, \ldots, x_n) \in \overline{k}^n$ with $g(x) = 0$ for all $g \in J$. For $S \subset \overline{k}^n$, let $I(S)$ be the set of $g \in k[t_1, \ldots, t_n]$ such that $g(x) = 0$ for all $x \in S$. (Notice that we are extending to the algebraic closure on the affine space side but not on the ring side, hence the term "semirational".)

THEOREM 11.9. *(Semirational Nullstellensatz) For all ideals J of $k[t_1, \ldots, t_n]$, we have $I(V^a(J)) = \operatorname{rad} J$.*

PROOF. It is easy to see that $I(V^a(J))$ is a radical ideal containing J and thus $I(V^a(J)) \supset \operatorname{rad} J$. Conversely, let $f \in I(V^a(J))$. We must show that there is $N \in \mathbb{Z}^+$ such that $f^m \in J$. We may assume $f \neq 0$. We introduce a new indeterminate t_{n+1} and let J' be the ideal $\langle J, 1 - t_{n+1}f \rangle$ of $k[t_1, \ldots, t_n, t_{n+1}]$. Let $Z \subset \overline{k}^n$ be the zero set of J, so $f|_Z \equiv 0$. Let $(x_1, \ldots, x_n, x_{n+1}) \in \overline{k}^{n+1}$. If $(x_1, \ldots, x_n) \notin Z$, then there is $g \in J \subset J'$ such that $g(x_1, \ldots, x_n, x_{n+1}) \neq 0$. If $(x_1, \ldots, x_n) \in Z$, then $1 - x_{n+1}f(x_1, \ldots, x_n) = 1 \neq 0$. By Corollary 11.8, $J' = k[t_1, \ldots, t_n, t_{n+1}]$, so there are $g_i \in k[t_1, \ldots, t_n, t_{n+1}]$ and $h_i \in J$ such that

$$1 = g_0(1 - t_{n+1}f) + g_1h_1 + \ldots + g_rh_r.$$

Now substitute $t_{n+1} = f^{-1}$ and multiply by an appropriate power f^N of f to clear denominators: we get $f^N \in J$. □

EXERCISE 11.7. *The argument used in the proof of Theorem 11.9 is also called the **Rabinowitsch Trick**. Explain its relation to the proof of Proposition 11.3.*

EXERCISE 11.8. *Can you deduce Theorem 11.9 from Hilbert's Nullstellensatz?*

EXERCISE 11.9. *Let R be a subring of an algebraically closed field k, and let $f_1, \ldots, f_r \in R[t_1, \ldots, t_n]$. Show that exactly one of the following holds:*

(i) *There is $x \in k^n$ such that $f_1(x) = \ldots = f_r(x) = 0$.*

(ii) *There are $g_1, \ldots, g_r \in R[t_1, ..., t_n]$ and $a \in R^\bullet$ such that $\sum_{i=1}^r g_i f_i = a$.*

In the case of $R = \mathbb{Z}$ and $k = \mathbb{C}$, Exercise 11.9 is often called the "Arithmetic Nullstellensatz." A more interesting version of it would ask in Case (ii) for explicit upper bounds on the degrees of the polynomials g_j.

3. The Real Nullstellensatz

Recall that a field k is **formally real** if it is *not* possible to express -1 as a sum of (any finite number of) squares in k.

EXERCISE 11.10. *Let k be a formally real field.*

a) *Show: k is not algebraically closed.*

b) *Show: each subfield of k is formally real.*

A field k is **real closed** if it is formally real and admits no proper formally real algebraic extension. So e.g. $\mathbb{R}$ is real closed and $\mathbb{Q}$ is formally real but not real closed.

As we saw, even the weak Nullstellensatz fails for polynomial rings over any non-algebraically closed field k. However, when k is formally real one can find counterexamples to the Nullstellensatz of a particular form, and when k is real closed one can show that these counterexamples are in a certain precise sense the only ones, leading to an identification of the closure operation $J \mapsto I(V(J))$ in this case.

In any commutative ring R, an ideal I is **real** if for all $n \in \mathbb{Z}^+$ and $x_1, \ldots, x_n \in R$, $x_1^2 + \ldots + x_n^2 \in I$ implies $x_1, \ldots, x_n \in I$.

A domain R is **real** if the zero ideal is real.

EXERCISE 11.11.

a) *Show: a domain is real if and only if its fraction field is formally real.*
b) *Let R be a ring. Show: $\mathfrak{p} \in \operatorname{Spec} R$ is real if and only if the fraction field of $R/\mathfrak{p}$ is formally real.*

EXERCISE 11.12. *Show: any real ideal is a radical ideal.*

So what? The following result gives the connection to the closure operator on ideals in $k[t_1, \ldots, t_n]$.

PROPOSITION 11.10. *Let k be a formally real field and $k[x] = k[x_1, \ldots, x_n]$. For any ideal J of $k[x]$, its closure $\overline{J} = I(V(J))$ is a real ideal.*

PROOF. Let $f_1, \ldots, f_m \in k[x]$ be such that $f_1^2 + \ldots + f_m^2 \in \overline{J}$. Then for any $P \in V(J)$, we have $f_1(P)^2 + \ldots + f_m(P)^2 = 0$. Since k is formally real, this implies $f_1(P) = \ldots = f_m(P) = 0$, and thus $f_1, \ldots, f_m \in I(V(J)) = \overline{J}$. □

EXERCISE 11.13. *Find a real prime ideal $\mathfrak{p} \in \mathbb{Q}[t]$ which is not closed.*

For an ideal I of a ring R, define the **real radical**

$$\mathbb{R}\operatorname{ad}(I) = \{x \in R \mid \exists n \in \mathbb{Z}^+ \ \exists b_1, \ldots, b_m \in R \mid x^{2n} + b_1^2 + \ldots + b_m^2 \in I\}.$$

PROPOSITION 11.11. [**BCR**, Prop. 4.1.7] *Let I be an ideal in a ring R.*

a) *A real ideal J contains I if and only if $J \supset \mathbb{R}\operatorname{ad}(I)$ i.e., $\mathbb{R}\operatorname{ad}(I)$ is the unique minimal real ideal containing I.*
b) *The ideal $\mathbb{R}\operatorname{ad}(I)$ is the intersection of all real prime ideals $\mathfrak{p} \supset I$.*
c) *It follows that every real ideal is equal to the intersection of all the real prime ideals containing it.*

Remark: If there are no real prime ideals containing I, then the intersection over this empty set is taken to be R.

PROOF. Step 1: we show that $\mathbb{R}\operatorname{ad}(I)$ is an ideal. The only nonobvious part of this is closure under addition. Suppose that

$$a^{2n} + b_1^2 + \ldots + b_m^2, \ A^{2N} + B_1^2 + \ldots + B_M^2 \in I.$$

We may write

$$(a + A)^{2(n+N)} + (a - A)^{2(n+N)} = a^{2m}c + A^{2M}C,$$

with c, C sums of squares in R. Then

$$(a + A)^{2(n+N)} + (a - A)^{2(n+N)} + c(b_1^2 + \ldots + b_m^2) + C(B_1^2 + \ldots + B_M^2) \in I,$$

so $a + A \in \mathbb{R}\,\mathrm{ad}(I)$.
Step 2: $\mathbb{R}\,\mathrm{ad}(I)$ is a real ideal. Indeed, if $x_1^2 + \ldots + x_k^2 \in \mathbb{R}\,\mathrm{ad}(I)$, then there exists $n \in \mathbb{Z}^+$ and $b_1, \ldots, b_m \in R$ such that

$$(x_1^2 + \ldots + x_k^2)^{2m} + b_1^2 + \ldots + b_m^2 \in I;$$

for each $1 \leqslant i \leqslant k$, we may rewrite this as $x_i^{4m} + B_1^2 + \ldots + B_N^2$, so $x_i \in \mathbb{R}\,\mathrm{ad}(I)$.
Step 3: Since every real ideal is radical, it is clear that any real ideal containing I also contains $\mathbb{R}\,\mathrm{ad}(I)$.
Step 4: Let $a \in R \backslash \mathbb{R}\,\mathrm{ad}(I)$. By Zorn's Lemma, the set of real ideals containing I but not a has a maximal element, say J. We claim that J is prime. If not, there exist $b, b' \in R \backslash J$ such that $bb' \in J$. Then $a \in \mathbb{R}\,\mathrm{ad}(J + bR)$ and $a \in \mathbb{R}\,\mathrm{ad}(J + b'R)$, hence there are $j, j' \in J$ such that

$$a^{2m} + c_1^2 + \ldots + c_q^2 = j + bd,\ a^{2m'} + c_1'^2 + \ldots + c_q'^2 = j' + b'd'.$$

It follows that

$$a^{2(m+m')} + \text{ a sum of squares } = jj' + jb'd' + j'bd + bb'dd' \in J,$$

and thus $a \in \mathbb{R}\,\mathrm{ad}(J) = J$, contradiction. Thus $\mathbb{R}\,\mathrm{ad}(I)$ is the intersection of all real prime ideals containing I. □

THEOREM 11.12. *(Artin-Lang Homomorphism Theorem)*

a) *Let $k \hookrightarrow L$ be a map of real-closed fields, and let R be a finitely generated k-algebra. If there is a k-algebra homomorphism $\varphi : R \to L$, then there is a k-algebra homomorphism $\psi : R \to k$.*
b) *Let k be a real-closed field, and let R be a domain which is a finitely generated k-algebra. If R is real, there is a k-algebra homomorphism $\varphi : R \to k$.*

PROOF. a) For a proof using model-theoretic methods, see e.g. [**BCR**, Thm. 4.1.2].
b) The fraction field K of R is formally real: let L be a real closure of K. Apply part a) to the composite k-algebra homomorphism $\varphi : R \to K \to L$. □

Remark: For a direct algebraic proof of Theorem 11.12b), see e.g. [**S**, § 3.3].

EXERCISE 11.14. *Let $R = \mathbb{R}[x, y]/(x^2 + y^2)$.*

a) *Show: R is a domain.*
b) *Show: R is not real.*
c) *Show: there is a (unique!) $\mathbb{R}$-algebra homomorphism $\varphi : R \to \mathbb{R}$. (Thus the converse of Theorem 11.12b) does not hold.)*

In [**Lg53**], Lang actually proved the following stronger result than Theorem 11.12b), which we state in more geometric language: the domain R above corresponds to an integral affine variety V over the real closed field k, and Lang showed that the function field $k(V)$ is formally real if and only if V has a *nonsingular* k-rational point.

THEOREM 11.13. *(The Nullstellensatz for Real-Closed Fields) Let k be a real-closed field, and J an ideal in $k[t] = k[t_1, \ldots, t_n]$. Then $\overline{J} = \mathbb{R}\,\mathrm{ad}(J)$.*

PROOF. Step 1: Suppose J is a real prime ideal. Let $R = k[t]/J$, and let K be the fraction field of R; by Exercise 11.X, K is formally real; let L be a real closure of K. For $f \in R\backslash J$, let S be the localization $R[\frac{1}{q(f)}]$, so $S \subset L$. By Theorem 11.12a) there is a k-algebra homomorphism $\psi : S \to k$; let $x = (\psi(\overline{t_1}), \ldots, \psi(\overline{t_n}))$. Then $x \in V(J)$ and $f(x) \neq 0$, so $f \notin I(V(J))$. It follows that $\overline{J} = I(V(J)) = J$.
Step 2: Suppose J is a real ideal, and let X_J be the set of all real prime ideals containing J. By Proposition 11.11c), $J = \bigcap_{\mathfrak{p} \in X_J} \mathfrak{p}$, and thus

$$\overline{J} = I(V(J)) = I(V(\bigcap_{\mathfrak{p} \in X_J} \mathfrak{p})) = I(\bigcup_{\mathfrak{p} \in X_J} V(\mathfrak{p})) = \bigcap_{\mathfrak{p} \in X_J} I(V(\mathfrak{p})) = \bigcap_{\mathfrak{p} \in X_J} \mathfrak{p} = J.$$

Step 3: Now let J be arbitrary. By Proposition 11.10, $\overline{J}$ is a real ideal containing J, so by Proposition 11.11a), $\mathbb{R}\operatorname{ad}(J) \subset \overline{J}$. On the other hand, part b) gives

$$\overline{J} \subset \overline{\mathbb{R}\operatorname{ad}(J)} = \mathbb{R}\operatorname{ad}(J),$$

so $\overline{J} = \mathbb{R}\operatorname{ad}(J)$. □

4. The Finite Field Nullstellensatz

For a prime power q, let $\mathbb{F}_q$ be a finite field of cardinality q. We will characterize the closure operation $J \mapsto \overline{J} = I(V(J))$ for ideals in $\mathbb{F}_q[t] = \mathbb{F}_q[t_1, \ldots, t_n]$.

Let $I_0 = \langle t_1^q - t_1, \ldots, t_n^q - t_n \rangle$. Then the key observation is that for any ideal J of $\mathbb{F}_q[t]$, $\overline{J} \supset I_0$. Indeed, since $x^q = x$ for all $x \in \mathbb{F}_q$, the polynomials $t_1^q - t_1, \ldots, t_n^q - t_n$ each vanish at every point of $\mathbb{F}_q^n$, so $\overline{J} = I(V(J)) \supset I(\mathbb{F}_q^n) \supset I_0$. Since of course $\overline{J} \supset J$, it follows that for all ideals J of $k[t]$ we have

$$\overline{J} \supset J + I_0. \tag{32}$$

PROPOSITION 11.14. *(Finite Field Weak Nullstellensatz) Let $\mathbb{F}_q$ be a finite field, and let $n \in \mathbb{Z}^+$. For $1 \leqslant i \leqslant n$, let $g_i = t_i^q - t_i \in \mathbb{F}_q[t_1, \ldots, t_n]$, and put $I_0 = \langle g_1, \ldots, g_n \rangle$. Then $I_0 = I(\mathbb{F}_q^n)$ is the ideal of all functions vanishing at every point of $\mathbb{F}_q^n$.*

EXERCISE 11.15. *Deduce Proposition 11.14 from the Combinatorial Nullstellensatz.*

Proposition 11.14 asserts that the containment of (32) is an equality when $J = (0)$. In fact, this holds in all cases.

LEMMA 11.15. *Let J be an ideal of $\mathbb{F}_q[t_1, \ldots, t_n]$. If J contains the ideal $I_0 = \langle t_1^q - t_1, \ldots, t_n^q - t_n \rangle$, then* $\operatorname{rad} J = J$.

PROOF. Suppose that for $x \in R$, there is $n \in \mathbb{Z}^+$ with $x^n \in J$. Then also $x^{q^n} = (x^{q^{n-1}})^q \in J$. By Corollary 11.14, for all $x \in R$, $f^q - f \in I_0 \subset J$: applying this with $f = x^{q^{n-1}}$, we find that $x^{q^n} - x \in I$ and thus $x^{q^n} - (x^{q^n} - x) = x \in J$. □

THEOREM 11.16. *(Finite Field Nullstellensatz) For any ideal J of $R = \mathbb{F}_q[t_1, \ldots, t_n]$,*

$$\overline{J} = I(V(J)) = J + I_0 = \langle J, t_1^q - t_1, \ldots, t_n^q - t_n \rangle.$$

We will give two proofs: one using the Semirational Nullstellensatz, and one using the Finite Field Weak Nullstellensatz.

PROOF. By the Semirational Nullstellensatz (Theorem 11.9) and Lemma 11.15,

$$I(V^a(J + I_0)) = \operatorname{rad}(J + I_0) = J + I_0.$$

Since $V^a(I_0) = \mathbb{F}_q^n$, we have

$$I(V(J)) = I(V^a(J) \cap \mathbb{F}_q^n) = I(V^a(J) \cap V^a(I_0)) = I(V^a(J + I_0)) = J + I_0.$$

□

PROOF. By (32) $\overline{J} \supset J + I_0$, it suffices to show that for all $J \supseteq I_0$, $J = \overline{J}$. By Proposition 11.14, $I_0 = I(\mathbb{F}_q^n)$. For $P = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$, let

$$\mathfrak{m}_P = I(\{P\}) = \langle t_1 - x_1, \ldots, t_n - x_n \rangle.$$

Thus $\{\mathfrak{m}_P\}_{P \in \mathbb{F}_q^n}$ are finitely many pairwise comaximal ideals with $I_0 = \bigcap_{P \in \mathbb{F}_q^n} \mathfrak{m}_P$. By the Chinese Remainder Theorem,

$$R/I_0 = R/\bigcap_{P \in \mathbb{F}_q^n} \mathfrak{m}_P \cong \prod_{P \in \mathbb{F}_q^n} R/\mathfrak{m}_P \cong k^{\#\mathbb{F}_q^n}. \tag{33}$$

The Correspondence Theorem now gives us canonical bijections between the set of ideals containing I_0 and the set of subsets of $\mathbb{F}_q^n$. Since every subset of the finite set $\mathbb{F}_q^n$ is Zariski closed, there are precisely $2^{\#\mathbb{F}_q^n}$ Zariski-closed subsets and therefore precisely $2^{\#\mathbb{F}_q^n}$ ideals J with $J = \overline{J}$. By (33) there are precisely $2^{\#\mathbb{F}_q^n}$ ideals J containing I_0, so we must have $J = \overline{J}$ for all such ideals. □

Remark: It seems that Theorem 11.16 was first stated and proved (as in the first proof above) in a 1991 technical report of R. Germundsson [**Ge91**].

5. Terjanian's Homogeneous p-Nullstellensatz

THEOREM 11.17. *Let k be an algebraically closed field, let $1 \leqslant m < n$ be integers, and let $f_1, \ldots, f_m \in k[t_1, \ldots, t_n]$. Put*

$$V := V(f_1, \ldots, f_m) = \{x = (x_1, \ldots, x_n) \in k^n \mid f_1(x) = \ldots = f_m(x) = 0\}.$$

Then V is either empty or infinite.

PROOF. Put $I := \langle f_1, \ldots, f_m \rangle$. Seeking a contradiction, we suppose that $V = \{p_1, \ldots, p_N\}$ is nonempty and finite. For $x \in k^n$ we have $x \in V$ if and only if I is contained in the maximal ideal $\mathfrak{m}_x$ of polynomials that vanish at x, so the maximal ideals contaning I are precisely $\mathfrak{m}_{p_1}, \ldots, \mathfrak{m}_{p_N}$. Since $k[t_1, ..., t_n]$ is Jacobson, we have

$$\operatorname{rad} I = \bigcap_{i=1}^N \mathfrak{m}_{p_i} = \prod_{i=1}^N \mathfrak{m}_{p_i}.$$

Let $\mathfrak{p}$ be a minimal prime ideal over I. Then $\mathfrak{p} \supset \operatorname{rad} I = \prod_{i=1}^N \mathfrak{m}_{p_i}$, so $\mathfrak{p} = \mathfrak{m}_x$ for some $x = (x_1, \ldots, x_n) \in k^n$. Applying the Generalized Principal Ideal Theorem to $\mathfrak{p} = \mathfrak{m}_x$ we get that $\operatorname{ht} \mathfrak{m}_{x_i} \leqslant m < n$. But

$$(0) \subsetneq \langle t_1 - x_1 \rangle \subsetneq \langle t_1 - x_1, t_2 - x_2 \rangle \subsetneq \ldots \subsetneq \langle t_1 - x_1, \ldots, t_n - x_n \rangle = \mathfrak{m}_x$$

shows that $\mathfrak{m}_x$ has height at least n, a contradiction. □

EXERCISE 11.16. *For which fields k does the conclusion of Theorem 11.17 hold? Evidently not when k is finite!*

a) *Let $f = t_1^2 + t_2^2 \in \mathbb{R}[t_1, t_2]$. Show: $V(f) = \{(0, 0)\}$ is nonempty and finite.*

b) *Show: if k is not algebraically closed, there is $f \in k[t_1, t_2]$ such that $V(f) = \{(0,0)\}$.*

COROLLARY 11.18 (Homogeneous Nullstellensatz). *Let k be an algebraically closed field, $m, n \in \mathbb{Z}^+$, and let $f_1, \ldots, f_m \in k[t_0, \ldots, t_n]$ be homogeneous polynomials of positive degree. If $m \leq n$, then there is $0 \neq x \in k^{n+1}$ such that*

$$f_1(x) = \ldots = f_n(x) = 0.$$

PROOF. Let V be as in Theorem 11.17. Since each f_i is homogeneous we have $0 \in V$, and thus by Theorem 11.17 the set V is infinite. □

While Theorem 11.18 is a very classical result – it was used (not necessarily with proper justification) by 19th century mathematicians studying varieties in projective space – the following generalization is a 1972 theorem of G. Terjanian.

Let p be a prime number. We say that a field k is a **p-field** if every every finite extension l/k has degree a power of p.

EXAMPLE 11.19.

a) *Every separably closed field is a p-field.*
b) *l Every real-closed field is a 2-field.*
c) *A perfect field k is a p-field if and only if $\mathrm{Gal}(\overline{k}/k)$ is a pro-p-group.*

THEOREM 11.20. *(Terjanian's Homogeneous p-Nullstellensatz) Let k be a p-field, and let $n \in \mathbb{Z}^+$. For $1 \leqslant i \leqslant n$, let $f_i \in k[t_0, \ldots, t_n]$ be homogeneous of degree d_i indivisible by p. Then there is $0 \neq x = (x_1, \ldots, x_n) \in k^n$ such that*

$$f_1(x) = \ldots = f_n(x) = 0.$$

The proof given in [**Te72**] was rather involved; a significantly simpler proof is given in [**P**], but even this involves more graded algebra than we wish to discuss here. However, following Arason and Pfister [**AP82**] we will now deduce some striking consequences of the Homogeneous 2-Nullstellensatz for real-closed fields.

EXERCISE 11.17. *Let k be a field of characteristic different from 2, and let $f \in k[t_1, \ldots, t_n]$. We say that f is an **odd polynomial** if $f(-t) = -f(t)$. Show: an odd polynomial is a sum of monomials each of odd total degree.*

THEOREM 11.21. *(Algebraic Borsuk-Ulam) Let k be a real closed field, $n \in \mathbb{Z}^+$, and for $1 \leqslant i \leqslant n$, let $f_i \in k[t_1, \ldots, t_{n+1}]$ be an* odd *polynomial: $f_i(-t) = -f_i(t)$. Then there is $x = (x_1, \ldots, x_{n+1}) \in k^{n+1}$ such that*

$$x_1^2 + \ldots + x_{n+1}^2 = 1,\ f_1(x) = \ldots = f_n(x) = 0.$$

PROOF. So as to be able to apply Terjanian's Homogeneous p-Nullstellensatz, we homogenize: let t_0 be an additional indeterminate and let $\tilde{f}_i \in k[t_0, \ldots, t_{n+1}]$ be the unique homogeneous polynomial such that $\tilde{f}_i(1, t_1, \ldots, t_{n+1}) = f_i$, of degree $d_i = \deg f_i$. Being an odd polynomial, each f_i only contains monomials of odd degree; thus each d_i is odd and t_0 occurs in $\tilde{f}_i$ to even powers only. Thus we may make the change of variables $t_0^2 \mapsto t_1^2 + \ldots + t_{n+1}^2$ in each $\tilde{f}_i$, leading to homogeneous polynomials $g_1, \ldots, g_n \in k[t_1, \ldots, t_{n+1}]$ of odd degrees $d_1, \ldots, d_n$. Applying Theorem 11.20 with $p = 2$, we get $0 \neq a \in k^{n+1}$ such that $g_1(a) = \ldots = g_n(a) = 0$. Since the g_i's are homogeneous, we may scale by $\left(a_1^2 + \ldots + a_{n+1}^2\right)^{-1}$

to get an a such that $a_1^2 + \ldots + a_{n+1}^2 = 1$ and $g_1(a) = \ldots = g_n(a) = 0$. Thus $f_i(a) = \tilde{f}_i(1, a) = g_i(a) = 0$ for all i, and we're done. □

We now revert to the case of $k = \mathbb{R}$. As usual, for $x = (x_1, \ldots, x_n) \in \mathbb{R}^n$, we put

$$||x|| = \sqrt{x_1^2 + \ldots + x_n^2}\};$$

for $x, y \in \mathbb{R}^n$, we put

$$d(x, y) = ||x - y||,$$

and we define the **unit sphere**

$$S^n = \{x \in \mathbb{R}^n \mid ||x|| = 1\}$$

and the **unit disk**

$$D^n = \{x \in \mathbb{R}^n \mid ||x|| \leqslant 1\}.$$

A subset $S \subset \mathbb{R}^n$ is **symmetric** if $x \in S \implies -x \in S$. If $S \subset \mathbb{R}^m$ and $T \subset \mathbb{R}^n$ are symmetric subsets, then $f : S \to T$ is **odd** if for all $x \in S$, $f(-x) = -f(x)$. For $x \in S^n$, x and $-x$ are **antipodal**, and $\{x, -x\}$ is called an **antipodal pair**.

COROLLARY 11.22. *(Topological Borsuk-Ulam)*
Let $f : S^n \to \mathbb{R}^n$ be a continuous, odd map. Then there is $x \in S^n$ with $f(x) = 0$.

PROOF. Write $f = (f_1, \ldots, f_n)$, for $f_i : S^n \to \mathbb{R}$ an odd continuous map. Seeking a contradiction, we suppose f has no zero. Since S^n is compact, there is $\delta > 0$ such that for all $x \in S^n$, $\max_i |f_i(x)| \geqslant \delta$. Choose $0 < \epsilon < \delta$ and apply the Weierstrass Approximation Theorem to the continuous functions $f_1, \ldots, f_n$ on the compact space S^n: there are $p_1, \ldots, p_n \in \mathbb{R}[t_1, \ldots, t_{n+1}]$ such that $|f_i(x) - p_i(x)| < \epsilon$ for all i and all $x \in S^n$. Put $q_i(t) = \frac{1}{2}(p_i(t) - p_i(-t))$; then for $x \in S^n$,

$$\begin{aligned} |f_i(x) - q_i(x)| &= \frac{|f_i(x) - f_i(-x) - p_i(x) + p_i(-x)|}{2} \\ &\leqslant \frac{|f_i(x) - p_i(x)| + |f_i(-x) - p_i(-x)|}{2} < \epsilon. \end{aligned}$$

It follows that for all $x \in S^n$, $\max_i |q_i(x)| \geqslant \delta - \epsilon > 0$, so the q_i's have no simultaneous zero on S^n, contradicting Theorem 11.21. □

COROLLARY 11.23.
The following statements are equivalent – and hence, by Corollary 11.22, all true.

(i) *Every continuous, odd map $f : S^n \to \mathbb{R}^n$ has a zero.*
(ii) *There is no continuous, odd map $g : S^n \to S^{n-1}$.*
(iii *) Every continuous map $f : S^n \to \mathbb{R}^n$ identifies some antipodal pair.*
(iv) *(Lusternik-Schnirelmann-Borsuk) Let $\{F_1, \ldots, F_{n+1}\}$ be a covering family of closed subsets of S^n. Then some member of the family contains an antipodal pair.*

PROOF. (i) $\implies$ (ii): Let $\iota : S^{n-1} \hookrightarrow \mathbb{R}^n$ be the natural inclusion. If $g : S^n \to S^{n-1}$ is continuous and odd, $\iota \circ g : S^n \to \mathbb{R}^n$ is continuous and odd with no zero.
(ii) $\implies$ (iii): If f identifies no antipodal pair, then $g : S^n \to S^{n-1}$ by $x \mapsto \frac{f(x) - f(-x)}{||f(x) - f(-x)||}$ is continuous and odd.
(iii) $\implies$ (i): Let $f : \mathbb{R}^n \to S^n$ be odd. By assumption, there is $x \in S^n$ such that $f(x) = f(-x)$, but since also $f(x) = -f(-x)$, we conclude $f(x) = 0$.
(iii) $\implies$ (iv): Let $F_1, \ldots, F_{n+1}$ be closed subsets of S^n such that $\bigcup_{i=1}^{n+1} F_i = S^n$;

suppose that none of the sets $F_1, \ldots, F_n$ contains an antipodal pair: equivalently, putting $E_i = -F_i$, we have that $E_i \cap F_i = \varnothing$ for $1 \leqslant i \leqslant n$. For a point x and a subset Y of S^n, put $d(x, Y) = \inf\{d(x, y) \mid y \in Y\}$. For $1 \leqslant i \leqslant n+1$, define $f_i : S^n \to \mathbb{R}$ by $f_i(x) = d(x, E_i) - d(x, F_i)$. Observe that

$$x \in F_i \implies f_i(-x) < 0 < f_i(x),$$

$$x \in E_i \implies f_i(x) < 0 < f_i(-x).$$

Applying condition (iii) to $f = (f_1, \ldots, f_n) : S^n \to \mathbb{R}^n$, we get $x_0 \in S^n$ such that $f(-x_0) = f(x_0)$. Thus neither x_0 nor $-x_0$ lies in any F_i with $1 \leqslant i \leqslant n$, hence both x_0 and $-x_0$ must lie in F_{n+1}.
(iv) $\implies$ (ii): Let $f : S^n \to S^{n-1}$ be continuous. Observe the following "converse" to Lusternik-Schnirelmann-Borsuk: there is a covering family $\{E_i\}_{i=1}^{n+1}$ of closed subsets of S^{n-1}, each of diameter less than 2. (We leave the verification of this as an exercise.) For $1 \leqslant i \leqslant n+1$, put $F_i = f^{-1}(E_i)$. Thus $\{F_i\}_{i=1}^{n+1}$ is a covering of S^n by closed subsets, so by condition (iv) for some $1 \leqslant i \leqslant n+1$ and $x_0 \in S^n$ we have $x_0, -x_0 \in F_i$, i.e., $f(x_0), f(-x_0) \in E_i$. Since E_i has diameter less than 2, it contains no antipodal pair, and thus f cannot be odd, for otherwirse $f(x_0), -f(x_0) \in E_i$. □

EXERCISE 11.18. *Verify: for any $n \in \mathbb{Z}^+$, S^n can be covered by $n+2$ closed subsets each of diameter less than 2.*
(Suggestion: take a regular simplex inscribed in D^n and consider the projections of its faces onto S^n.)

For a function $f : \mathbb{R}^n \to \mathbb{R}$, let us put

$$f^+ = \{x \in \mathbb{R}^n \mid f(x) > 0\},$$

$$f^0 = \{x \in \mathbb{R}^n \mid f(x) = 0\},$$

$$f^- = \{x \in \mathbb{R}^n \mid f(x) < 0\}.$$

For a Lebesgue measurable subset $S \subset \mathbb{R}^n$, we denote its measure by $\mathrm{Vol}(S)$.

The following result is due to Stone and Tukey [**ST42**].

COROLLARY 11.24. *(Polynomial Ham Sandwich Theorem) Let $d, n \in \mathbb{Z}^+$ and put $N = \binom{n+d}{d} - 1$. Let $U_1, \ldots, U_N \in \mathbb{R}^n$ be measurable, finite volume subsets. There is a polynomial $P \in \mathbb{R}[t_1, \ldots, t_n]$ of degree at most d which **bisects** each U_i:*

$$\forall 1 \leqslant i \leqslant N,\ \mathrm{Vol}(U_i \cap P^+) = \mathrm{Vol}(U_i \cap P^-).$$

PROOF. Let $V_d \subset \mathbb{R}[t_1, \ldots, t_n]$ be the $\mathbb{R}$-subspace of polynomials of total degree at most d, so $\dim V_d = N + 1$. Endow V_d with a norm $||\cdot||$ (all norms on a finite-dimensional real vector space are *equivalent*, so we need not be more specific than this). Let S^N be the unit sphere in V_d. We define a function

$$f = (f_1, \ldots, f_N) : S^N \to \mathbb{R}^N$$

by

$$f_i(P) = \mathrm{Vol}(U_i \cap P^+) - \mathrm{Vol}(U_i \cap P^-).$$

Step 1: We CLAIM that f is continous.
PROOF OF CLAIM: One easily reduces to the claim that for any measurable, finite volume subset $U \subset \mathbb{R}^n$, the mapping

$$M : P \in V_d^\bullet \mapsto \mathrm{Vol}(U \cap P^+)$$

is continuous. For this, let $\{P_n\}$ be a sequence in V_d such that $P_n \to P$ with respect to $||\cdot||$. It follows that $P_n \to P$ pointwise on ($\mathbb{R}^n$ hence in particular on) U. Since $\mathrm{Vol}(U) < \infty$, we may apply Egorov's Theorem: for each $\epsilon > 0$, there is a measurable subset $E \subset U$ with $\mathrm{Vol}(E) < \epsilon$ and such that $P_n \to P$ uniformly on $U \backslash E$. Since $\mathrm{Vol}(P^0) = 0$ and $\mathrm{Vol}(U) < \infty$, there is $\delta > 0$ such that

$$\mathrm{Vol}(\{x \in U \mid |P(x)| < \delta\}) < \epsilon.$$

Take $N \in \mathbb{Z}^+$ such that for all $n \geqslant N$, $|P_n(x) - P(x)| < \delta$ for all $x \in U \backslash E$. Then

$$|\mathrm{Vol}(U \cap P_n^+) - \mathrm{Vol}(U \cap P^+)| < 2\epsilon.$$

Step 2: It is immediate that f is odd. By Corollary 11.22, there is $P \in S^N$ such that $f(P) = 0$, and such a P bisects each U_i. □

COROLLARY 11.25. *(No Retraction Theorem) There is no* ***retraction*** *from D^n to S^{n-1}, i.e., no continuous map $r : D^n \to S^{n-1}$ such that $r|_{S^{n-1}} = 1_{S^{n-1}}$.*

PROOF. Let $\pi : \mathbb{R}^{n+1} \to \mathbb{R}^n$, $(x_1, \ldots, x_n, x_{n+1}) \mapsto (x_1, \ldots, x_n)$, and let

$$H_n^+ = \{(x_1, \ldots, x_{n+1}) \in S^n \mid x_{n+1} \geqslant 0\},\ H_n^- = \{(x_1, \ldots, x_{n+1}) \in S^n \mid x_{n+1} \leqslant 0\}.$$

Suppose $r : D^n \to S^{n-1}$ is a retraction, and define $g : S^n \to S^{n-1}$ by

$$g(x) = \begin{cases} r(-\pi(x)),\ x \in H_n^+, \\ -r(\pi(x)),\ x \in H_n^- \end{cases}$$

Then g is well-defined, continuous and odd, contradicting Corollary 11.23b). □

COROLLARY 11.26. *(Brouwer Fixed Point Theorem) Each continuous function $f : D^n \to D^n$ has a fixed point.*

PROOF. Suppose $f : D^n \to D^n$ is continuous with $f(x) \neq x$ for all $x \in D^n$. For $x \in D^n$, consider the ray $\mathfrak{r}_x$ with initial point $f(x)$ and lying on the line determined by $f(x)$ and x. Then $\mathfrak{r}_x$ intersects S^{n-1} at a unique point, say $r(x)$, and $x \mapsto r(x)$ defines a retraction $r : D^n \to S^{n-1}$, contradicting Corollary 11.25. □

CHAPTER 12

Goldman Domains and Hilbert-Jacobson rings

1. Goldman domains

LEMMA 12.1.
For a domain R with fraction field K, the following are equivalent:

(i) *K is finitely generated as an R-algebra.*
(ii) *There is $f \in K$ such that $K = R[f]$.*

PROOF. Of course (ii) $\implies$ (i). Conversely, if $K = R[f_1, \ldots, f_n]$, then write $f_i = \frac{p_i}{q_i}$, and then $K = R[\frac{1}{q_1 \cdots q_n}]$. □

A ring satisfying the conditions of Lemma 12.1 will be called a **Goldman domain**.

EXERCISE 12.1. *Show: an overring*[1] *of a Goldman domain is a Goldman domain.*

LEMMA 12.2. *Let R be a domain with fraction field K, and $0 \neq x \in R$. the following are equivalent:*

(i) *Every nonzero prime ideal of R contains x.*
(ii) *Every nonzero ideal contains x^n for some $n \in \mathbb{Z}^+$.*
(iii) *We have $K = R[x^{-1}]$.*

PROOF. (i) $\implies$ (ii): let I be a nonzero ideal. If I is disjoint from $\{x^n\}$, then by Multiplicative Avoidance (5.26), I can be extended to a prime ideal disjoint from $\{x^n\}$, contradicting (i).

(ii) $\implies$ (iii): Let $0 \neq y \in R$. By (ii), we have (y) contains some power of x, say $x^k = yz$. But this implies that y is a unit in $R[x^{-1}]$.

(iii) $\implies$ (i): The prime ideals killed in the localization map $R \mapsto R[x^{-1}]$ are precisely those which meet the multiplicatively closed set $\{x^k\}$, i.e., contain x. □

COROLLARY 12.3. *For a domain R, the following are equivalent:*

(i) *R is a Goldman domain.*
(ii) *The intersection of all nonzero prime ideals of R is nonzero.*

EXERCISE 12.2. *Prove Corollary 12.3.*

Easy examples of Goldman domains: a field, $k[[t]]$, $\mathbb{Z}_{(p)}$. In fact we have developed enough technology to give a remarkably clean characterization of Noetherian Goldman domains.

THEOREM 12.4. *Let R be a domain.*

a) *If R has only finitely many primes, then R is a Goldman domain.*
b) *If R is a Noetherian Goldman domain, then R has finitely many primes.*

[1] An overring of a domain R is a ring intermediate between R and its fraction field K.

c) *A Noetherian Goldman domain is either a field or a one-dimensional domain.*

PROOF. Throughout we may – and shall – assume that R is not a field.

a) Suppose that R has only finitely many primes, and let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be the nonzero prime ideals of R. For $1 \leqslant i \leqslant n$, let $0 \neq x_i \in \mathfrak{p}_i$, and put $x = x_1 \cdots x_n$. Then the multiplicative set S generated by x meets every nonzero prime of R, so that $S^{-1}R$ has only the zero ideal. In other words, $R[\frac{1}{x}]$ is the fraction field of R, so R is a Goldman domain. (Alternately, this follows quickly from Corollary 12.3.)

b) Similarly, for a Goldman domain R we can write $K = R[\frac{1}{x}]$ for $x \in R$ and then every nonzero prime of R contains x. Suppose first that (x) itself is prime, necessarily of height one by the Hauptidealsatz (Theorem 8.49), hence if R has any primes other than (0) and (x) – especially, if it has infinitely many primes – then it has a height two prime $\mathfrak{q}$. But by Corollary 8.53 a Noetherian ring cannot have a height two prime unless it has infinitely many height one primes, a contradiction. So we may assume that (x) is not prime, and then the minimal primes of the Noetherian ring $R/(x)$ are finite in number – say $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ – and correspond to the primes of R which are minimal over x, so again by the Hauptidealsatz they all have height one. Similarly, if R has infinitely many primes there would be, for at least one i (say $i = 1$), a height two prime $\mathfrak{q} \supset \mathfrak{p}_1$. But then by Corollary 8.53 the "interval" $(0, \mathfrak{q})$ is infinite. Each element of this set is a height one prime ideal containing (x), i.e., is one of the $\mathfrak{p}_i$'s, a contradiction. Part c) follows by again applying Corollary 8.53: a Noetherian ring of dimension at least two must have infinitely many primes. □

Remark: a non-Noetherian Goldman domain can have infinitely many primes and/or primes of arbitrarily large height.

PROPOSITION 12.5. *Let R be a domain. Then the polynomial ring $R[t]$ is* not *a Goldman domain.*

PROOF. Let K be the fraction field of R. If $R[t]$ is a Goldman domain, then by Exercise 12.1, so is $K[t]$. But $K[t]$ is a Noetherian domain with infinitely many primes – e.g., Euclid's proof of the infinitude of primes in $\mathbb{Z}$ carries over verbatim to $K[t]$ – so Theorem 12.4 applies to show that $K[t]$ is not a Goldman domain. □

PROPOSITION 12.6. *Let R be a domain, and $T \supset R$ an extension domain which is algebraic and finitely generated as an R-algebra. Then R is a Goldman domain if and only if T is a Goldman domain.*

PROOF. Let K and L be the fraction fields of R and T, respectively. Suppose first that R is a Goldman domain: say $K = R[\frac{1}{u}]$. Then $T[\frac{1}{u}]$ is algebraic over the field K, so is a field, hence we have $L = T[\frac{1}{u}]$. Conversely, suppose that T is a Goldman domain: say $L = T[\frac{1}{v}]$; also write $T = R[x_1, \ldots, x_k]$. The elements $v^{-1}, x_1, \ldots, x_k$ are algebraic over R hence satisfy polynomial equations with coefficients in R. Let a be the leading coefficient of a polynomial equation for v^{-1} and $b_1, \ldots, b_k$ be the leading coefficients of polynomial equations for $x_1, \ldots, x_k$. Let $R_1 := R[a^{-1}, b_1^{-1}, \ldots, b_k^{-1}]$. Now L is generated over R_1 by $x_1, \ldots, x_k, v^{-1}$, all of which are integral over R_1, so L is integral over R_1. Since L is a field, it follows that R_1 is a field, necessarily equal to K, and this shows R is a Goldman domain. □

COROLLARY 12.7. *Let $R \subset S$ be an inclusion of domains, with R a Goldman domain. Suppose that $u \in S$ is such that $R[u]$ is a Goldman domain. Then u is algebraic over R, and R is a Goldman domain.*

THEOREM 12.8. *For a domain R, the following are equivalent:*

(i) *R is a Goldman domain.*

(ii) *There is a maximal ideal $\mathfrak{m}$ of $R[t]$ such that $\mathfrak{m} \cap R = (0)$.*

PROOF. (i) $\implies$ (ii): We may assume WLOG that R is not a field. Write $K = R[\frac{1}{u}]$. Define a homomorphism $\varphi : R[t] \to K$ by sending $t \mapsto \frac{1}{u}$. Evidently φ is surjective, so its kernel $\mathfrak{m}$ is a maximal ideal, and clearly we have $\mathfrak{m} \cap R = 0$.

(ii) $\implies$ (i): Suppose $\mathfrak{m}$ is a maximal ideal of $R[t]$ such that $\mathfrak{m} \cap R = (0)$. Let v be the image of t under the natural homomorphism $R[t] \to R[t]/\mathfrak{m}$. Then $R[v]$ is a field, so by Corollary 12.7, R is a Goldman domain. □

We define a prime ideal $\mathfrak{p}$ of a ring R to be a **Goldman ideal** if $R/\mathfrak{p}$ is a Goldman domain. Write $G\operatorname{Spec} R$ for the set of all Goldman ideals. Thus a Goldman ideal is more general than a maximal ideal but much more special than a prime ideal.

PROPOSITION 12.9. *Let R be a ring and I an ideal of R.*

a) *The nilradical of R is the intersection of all Goldman ideals of R.*

b) *The radical of I is the intersection of all Goldman ideals containing I.*

PROOF. a) We know that $N = \bigcap_{\mathfrak{p} \in \operatorname{Spec} R} \mathfrak{p}$, so certainly $N \subset \bigcap_{\mathfrak{p} \in G\operatorname{Spec} R} \mathfrak{p}$. Conversely, suppose $x \in R \backslash N$. The ideal (0) is then disjoint from the multiplicative set $S = \{x^n\}$. By multiplicative avoidance, we can extend (0) to an ideal $\mathfrak{p}$ maximal with respect to disjointness from S. We showed earlier that $\mathfrak{p}$ is prime; we now claim that it is a Goldman ideal. Indeed, let $\overline{x}$ denote the image of x in $\overline{R} = R/\mathfrak{p}$. By maximality of $\mathfrak{p}$, every nonzero prime of $\overline{R}$ contains $\overline{x}$. By Lemma 12.2, this implies $\overline{R}[\overline{x}^{-1}]$ is a field, thus $\overline{R}$ is a Goldman domain, and therefore $\mathfrak{p}$ is a Goldman ideal which does not contain x. Part b) follows by correspondence, as usual. □

The following result may seem completely abstruse at the moment, but soon enough it will turn out to be the key:

COROLLARY 12.10. *An ideal I in a ring R is a Goldman ideal if and only if it is the contraction of a maximal ideal in the polynomial ring $R[t]$.*

PROOF. This follows from Theorem 12.8 by applying the correspondence principle to the quotient ring R/I. □

2. Hilbert rings

To put Theorem 8.56 to good use, we need to have a class of rings for which the contraction of a maximal ideal from a polynomial ring is again a maximal ideal. It turns out that the following is the right class of rings:

Definition: A **Hilbert ring** is a ring in which every Goldman ideal is maximal.

PROPOSITION 12.11. *Any quotient ring of a Hilbert ring is a Hilbert ring.*

PROOF. This follows immediately from the correspondence between ideals of R/I and ideals of R containing I. □

A direct consequence of the definition and Proposition 12.9 is the following:

PROPOSITION 12.12. *Let I be an ideal in a Hilbert ring R. Then the intersection $\bigcap_{\mathfrak{m} \sup I} \mathfrak{m}$ of all maximal ideals $\mathfrak{m}$ containing I is* $\operatorname{rad}(I)$.

Any zero dimensional ring is a Hilbert ring. Especially, a field is a Hilbert ring, as is any Artinian ring or any Boolean ring.

EXERCISE 12.3.

a) *Let R be a one-dimensional Noetherian domain. The following are equivalent:*
   (i) *The ring R is a Hilbert ring.*
   (ii) *The Jacobson radical of R is* 0.
   (iii) *The ring R has infinitely many prime ideals.*
   (iv) *The ring R is not a Goldman domain.*

b) *Deduce: the ring $\mathbb{Z}$ of integers is a Hilbert domain.*

THEOREM 12.13. *Let R be a Hilbert ring, and S a finitely generated R-algebra. Then:*

a) *The ring S is also a Hilbert ring.*
b) *For every maximal ideal $\mathfrak{P}$ of S, the ideal $\mathfrak{p} := \mathfrak{P} \cap R$ is a maximal ideal of R.*
c) *The degree $[S/\mathfrak{P} : R/\mathfrak{p}]$ is finite.*

PROOF. a) It suffices to show that R is a Hilbert ring if and only if $R[t]$ is a Hilbert ring, for then, if R is a Hilbert ring, by induction any polynomial ring $R[t_1, \ldots, t_n]$ is a Hilbert ring, and any finitely generated R-algebra is a quotient of $R[t_1, \ldots, t_n]$ and thus a Hilbert ring. Note also that since R is a homomorphic image of $R[t]$, if $R[t]$ is a Hilbert domain, then so also is R.

So suppose R is a Hilbert ring, and let $\mathfrak{q}$ be a Goldman ideal in $R[t]$; we must show $\mathfrak{q}$ is maximal. Put $\mathfrak{p} = \mathfrak{q} \cap R$. As above, we can reduce to the case $\mathfrak{p} = 0$, so in particular R is a domain. Let a be the image of t in the natural homomorphism $R[t] \to R[t]/\mathfrak{q}$. Then $R[a]$ is a Goldman domain. By Corollary 12.7, a is algebraic over R, and R is a Goldman domain. But since we assumed that R was a Hilbert ring, this means that R is a field, and thus $R[a] = R[t]/\mathfrak{q}$ is a field, so $\mathfrak{q}$ is maximal.

b) We may write $S = R[t_1, \ldots, t_n]/I$. A maximal ideal $\mathfrak{m}$ of S is just a maximal ideal of $R[t_1, \ldots, t_n]$ containing I. By Corollary 12.10, the contraction $\mathfrak{m}'$ of $\mathfrak{m}$ to $R[t_1, \ldots, t_{n-1}]$ is a Goldman ideal of the Hilbert ring $R[t_1, \ldots, t_{n-1}]$, so is therefore maximal. Moreover, by Theorem 8.56, $\mathfrak{m}$ is generated by $\mathfrak{m}'$ and an irreducible polynomial in $R/\mathfrak{m}'[t]$, so that the residual extension $R[t_1, \ldots, t_n]/\mathfrak{m}$ has finite degree over $R[t_1, \ldots, t_{n-1}/\mathfrak{m}'$. Again, induction gives the full result. □

Applying Theorem 12.13c) in the case $R = k$ is a field, we deduce our second proof of **Zariski's Lemma** (Lemma 11.1).

THEOREM 12.14. *Let R be a Noetherian Hilbert ring. Then*

$$\dim(R[t]) = \dim R + 1.$$

PROOF. Let $0 = \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_d$ be a chain of prime ideals in R. Then, with $\iota : R \hookrightarrow R[t]$ the natural inclusion,

$$\iota_* \mathfrak{p}_0 \subsetneq \ldots \subsetneq \iota_* \mathfrak{p}_n \subsetneq \langle \iota_*(\mathfrak{p}_n), t \rangle$$

is a chain of prime ideals of $R[t]$ of length $d + 1$, hence for any ring R we have $\dim R[t] \geqslant \dim R + 1$. Conversely, it suffices to show that the height of any maximal

ideal $\mathcal{P}$ of $R[t]$ is at most $d+1$. For this, put $\mathfrak{p} = \mathcal{P} \cap R$. By Theorem 12.13, $\mathfrak{p}$ is maximal in R, so Theorem 8.56 tells us that there exists $f \in R[t]$ such that $\mathcal{P} = \langle \iota_* \mathfrak{p}, f \rangle$. Applying Krull's Hauptidealsatz (Theorem 8.49) in the quotient ring $R[t]/\iota_*\mathfrak{p}$, we get that the height of $\mathcal{P}$ is at most one more than the height of $\mathfrak{p}$. □

COROLLARY 12.15. *Let k be a field, and put $R = k[t_1, \ldots, t_n]$.*

a) *Every maximal ideal of R has height n and can be generated by n elements (and no fewer, by Theorem 8.54).*
b) *We have* $\dim R = n$.

EXERCISE 12.4. *Prove Corollary 12.15.*

3. Jacobson Rings

THEOREM 12.16. *For a ring R, the following are equivalent:*

(i) *For all $I \in \mathcal{I}(R)$, $r(I)$ is the intersection of all* maximal *ideals containing I.*
(i′) *In every quotient ring of R, the nilradical equals the Jacobson radical.*
(ii) *Every prime ideal $\mathfrak{p}$ of R is the intersection of all maximal ideals containing $\mathfrak{p}$.*
(iii) *Every* non*maximal prime ideal $\mathfrak{p}$ of R is equal to the intersection of all prime ideals strictly containing $\mathfrak{p}$.*

If R satisfies these equivalent properties it is called a ***Jacobson ring****.*

PROOF. (i) $\iff$ (i′) is immediate from the Correspondence Theorem.
(i) $\implies$ (ii): If (i) holds, then in particular for any radical ideal I, $I = \bigcap_{\mathfrak{m} \supset I} \mathfrak{m}$, and prime ideals are radical.
(ii) $\implies$ (i): for any ideal I of R,

$$\operatorname{rad} I = \bigcap_{\mathfrak{p} \supset I} \mathfrak{p} = \bigcap_{\mathfrak{p} \supset I} \bigcap_{\mathfrak{m} \supset \mathfrak{p}} \mathfrak{m} = \bigcap_{\mathfrak{m} \supset I} \mathfrak{m}.$$

(ii) $\implies$ (iii): If $\mathfrak{p}$ is prime but not maximal, then $\mathfrak{p} = \bigcap_{\mathfrak{m} \supset \mathfrak{p}} \mathfrak{m}$ and all the maximal ideals containing $\mathfrak{p}$ strictly contain $\mathfrak{p}$.
$\neg$ (ii) $\implies$ $\neg$ (iii): Let $\mathfrak{p}$ be a prime which is *not* the intersection of the maximal ideals containing it. Replacing R with $R/\mathfrak{p}$, we may assume R is a domain with nonzero Jacobson radical $J(R)$. Let $x \in J(R) \backslash \{0\}$, and choose, by Multiplicative Avoidance, an ideal $\mathfrak{p}$ which is maximal with respect to the property that $x \notin \mathfrak{p}$. Since $x \notin J(R) \backslash \mathfrak{p}$, $\mathfrak{p}$ is not maximal; since x lies in every ideal properly containing $\mathfrak{p}$, $\mathfrak{p}$ is not equal to the intersection of prime ideals strictly containing it. □

COROLLARY 12.17. *Every quotient ring of a Jacobson ring is Jacobson.*

PROOF. This is immediate from condition (i′) of Theorem 12.16. □

4. Hilbert-Jacobson Rings

PROPOSITION 12.18. *Suppose R is both a Goldman domain and a Jacobson ring. Then R is a field.*

PROOF. Let K be the fraction field of R, and suppose for a conradiction that $R \neq K$. Then there is a nonzero nonunit $f \in R$ such that K is the localization of R at the multiplicative subset $S = \{f, f^2, \ldots\}$. Let $\mathfrak{m}$ be a maximal ideal of R. Since R is not a field, $\mathfrak{m}$ is not zero, and thus the pushforward of R to $S^{-1}R$ is the unit

ideal. By Proposition 7.6, $\mathfrak{m}$ meets S. Since $\mathfrak{m}$ is prime, we conclude $f \in \mathfrak{m}$. It follows that the Jacobson radical of R contains f is accordingly nonzero. On the other hand R, being a domain, has zero nilradical. Thus R is not Jacobson. □

THEOREM 12.19. *For a commutative ring R, the following are equivalent:*

(i) *R is a Hilbert ring.*
(ii) *R is a Jacobson ring.*
(iii) *For all maximal ideals $\mathfrak{m}$ of $R[t]$, the ideal $\mathfrak{m} \cap R$ is a maximal ideal of R.*
(iv) *(Zariski's Lemma) Let K be a field that is finitely generated as an R-algebra. Then K is finitely generated as a R-module.*

PROOF. (i) $\implies$ (ii) by Proposition 12.12.
(ii) $\implies$ (i): Suppose R is Jacobson and $\mathfrak{p}$ is a Goldman ideal of R. Then $R/\mathfrak{p}$ is a Goldman domain (by definition of Goldman ideal) and a Jacobson ring (by Corollary 12.17), hence a field (by Proposition 12.18), so $\mathfrak{p}$ is maximal.
(ii) $\implies$ (iii) is Theorem 12.13b).
(iii) $\implies$ (i): Suppose R is a ring such that every maximal ideal of $R[t]$ contracts to a maximal ideal of R, and let $\mathfrak{p}$ be a Goldman ideal of R. By Corollary 12.10, $\mathfrak{p}$ is the contraction of a maximal ideal of $R[t]$, hence by assumption $\mathfrak{p}$ is maximal.
(i) $\implies$ (iv) by Theorem 12.13c).
(iv) $\implies$ (ii): By Theorem 12.16, it suffices to show that every nonmaximal prime $\mathfrak{p}$ is the intersection of the prime ideals strictly containing it. That is, let $x \in R \backslash \mathfrak{p}$: we will find a prime ideal $\mathfrak{q} \supsetneq \mathfrak{p}$ such that $x \notin \mathfrak{q}$. Let B be the domain $R/\mathfrak{p}$, so the image of x in B (which we continue to denote by x) is nonzero. Then $B' = B[\frac{1}{x}]$ is a finitely generated R-algebra. If B' is a field, then by hypothesis B' is finitely generated as an R-module and thus, equivalently, finitely generated as a B-module. But this implies that B is a field, a basic fact about integral extensions which will be proved later on in the notes (Theorem 14.1, Propostion 14.8a)) and thus $\mathfrak{p}$ is maximal, contradiction. So B' is not a field and thus it contains a nonzero maximal ideal, whose pullback to B is a prime ideal $\overline{\mathfrak{q}}$ not containing x. The ideal $\overline{\mathfrak{q}}$ corresponds to a prime ideal $\mathfrak{q} \supsetneq \mathfrak{p}$ of R not containing x. □

In the sequel we will use the consolidated terminology **Hilbert-Jacobson ring** for a ring satisfying the equivalent conditions of Theorem 12.19.

5. Application: Zero-Dimensional Ideals in Polynomial Rings

Let k be a field with algebraic closure $\overline{k}$, and let I be an ideal of the polynomial ring $k[t_1, \ldots, t_n]$. Recall (from §11.2.1) that $V^a(I)$ denotes the set of simultaneous zeros of I in $\overline{k}^n$.

THEOREM 12.20. *For an ideal I of $k[t_1, \ldots, t_n]$, the following are equivalent:*

(i) *$\dim_k k[t_1, \ldots, t_n]/I$ is finite.*
(ii) *The ring $k[t_1, \ldots, t_n]/I$ is Artinian.*
(iii) *The ring $k[t_1, \ldots, t_n]/I$ has Krull dimension 0.*
(iv) *The ring $k[t_1, \ldots, t_n]/I$ has only finitely many prime ideals.*
(v) *The ring $k[t_1, \ldots, t_n]/I$ has only finitely many maximal ideals.*
(vi) *The set $V^a(I)$ is finite.*

*An ideal satisfying these conditions is called **zero-dimensional**.*

PROOF. (i) $\implies$ (ii): A finite dimensional k-algebra A has no infinite descending chains of k-submodules, let alone A-submodules.
(ii) $\iff$ (iii): By the Hilbert Basis Theorem the ring $k[t_1, \ldots, t_n]$ is Noetherian hence so is its quotient $k[t_1, \ldots, t_n]$. A ring is Artinian if and only if it is Noetherian of Krull dimension zero.
(ii) $\implies$ (iv): An Artinian ring has finitely many prime ideals, all of which are maximal.
(iv) $\implies$ (v) is immediate.
(v) $\implies$ (vi): We have $V^a(I) = V^a(\operatorname{rad} I)$. Since $k[t_1, \ldots, t_n]$ is a Hilbert-Jacobson ring, $\operatorname{rad} I$ is the intersection of all maximal ideals containing I, so I satisfies condition (v) if and only if $\operatorname{rad} I$ does and we may assume that I is a radical ideal. Because there are finitely many maximal ideals $\mathfrak{m}_1, \ldots, \mathfrak{m}_N$, we have $I = \bigcap_{i=1}^N \mathfrak{m}_i$, so

$$V^a(I) = \bigcup_{i=1}^n V^a(\mathfrak{m}_i),$$

so it suffices to show that $V^a(\mathfrak{m})$ is finite for a maximal ideal $\mathfrak{m}$. By Zariski's Lemma, $k[t_1, \ldots, t_n]/\mathfrak{m}$ is a finite-degree field extension of k, so there are only finitely many k-algebra homomorphisms $k[t_1, \ldots, t_n]/\mathfrak{m} \hookrightarrow \overline{k}^n$. However, if $x = (x_1, \ldots, x_n) \in V^a(\mathfrak{m})$ then the k-algebra homomorphism $E_x : k[t_1, \ldots, t_n] \to \overline{k}$ that maps each t_i to x_i has $\mathfrak{m}$ in its kernel, hence induces a k-algebra homomorphism $E_x : k[t_1, \ldots, t_n]/\mathfrak{m} \to \overline{k}$, and the association $x \in V^a(\mathfrak{m}) \mapsto E_x$ is injective since $x = (E_x(t_1), \ldots, E_x(t_n))$. Thus $V^a(\mathfrak{m})$ is finite.
(vi) $\implies$ (i): Let $\overline{I} = I\overline{k}[t_1, \ldots, t_n]$. Then $V^a(I) = V(\overline{I})$ and

$$\overline{k}[t_1, \ldots_n]/\overline{I} = k[t_1, \ldots, t_n]/I \otimes_k \overline{k}$$

and thus $\dim_k k[t_1, \ldots, t_n]/I$ is finite if and only if $\dim_{\overline{k}} \overline{k}[t_1, \ldots, t_n]/\overline{I}$ is finite. So we may assume that k is algebraically closed, and thus the points x of $V(I)$ correspond precisely to the maximal ideals of $k[t_1, \ldots, t_n]$ containing I, so we are assuming that I is contained in only finitely many maximal ideals, say $\mathfrak{m}_1, \ldots, \mathfrak{m}_N$. Thus

$$k[t_1, \ldots, t_n]/\operatorname{rad} I \cong k[t_1, \ldots, t_n]/\mathfrak{m}_1 \times \ldots \times k[t_1, \ldots, t_n]/\mathfrak{m}_N,$$

so $\dim_k k[t_1, \ldots, t_n]/\operatorname{rad} I$ is finite by Zariski's Lemma. In particular $k[t_1, \ldots, t_n]/\operatorname{rad} I$ has Krull dimension zero, hence so does $k[t_1, \ldots, t_n]/I$, hence it is Artinian. By Theorem 8.37, for all sufficiently large a we have

$$k[t_1, \ldots, t_n]/I \cong \prod_{i=1}^n k[t_1, \ldots, t_n]/\mathfrak{m}_i^a.$$

For each $0 \leqslant j \leqslant a-1$, $\mathfrak{m}_i^j/\mathfrak{m}_i^{j+1}$ is finitely generated over $k[t_1, \ldots, t_n]/\mathfrak{m}_i$, hence finite-dimensional over k, and thus $\dim_k k[t_1, \ldots, t_n]/I$ is finite. □

EXERCISE 12.5. *Let I be an ideal of $k[t_1, \ldots, t_n]$.*

a) *Show: I is zero-dimensional if and only if $\operatorname{rad} I$ is zero-dimensional.*
b) *Show: if $S \subset \overline{k}^n$ is finite, then $I(S)$ is a radical zero-dimensional ideal.*
c) *Show: every radical zero-dimensional ideal of $k[t_1, \ldots, t_n]$ is of the form $I(S)$ if and only if k is algebraically closed.*

EXERCISE 12.6.

a) *Let I be an ideal of $k[t_1, \ldots, t_n]$. Show: I is zero-dimensional radical if and only if $k[t_1, \ldots, t_n]/I$ is a finite product of fields (equivalently, is semisimple).*
b) *Let $I \subset J$ be ideals of $k[t_1, \ldots, t_n]$. Show: if I is zero-dimensional, so is J. If I is zero-dimensional radical, so is J.*

According to Corollary 12.15, every maximal ideal of $k[t_1, \ldots, t_n]$ can be generated by n elements. In general, if $I_1, \ldots, I_N$ are ideals and for each $1 \leqslant j \leqslant N$, S_j is a finite set of generators of I_j, then $\{f_1 \cdots f_n \mid f_j \in S_j\}$ is a finite set of generators of $I_1 \cdots I_N$. Thus a radical zero-dimensional ideal I of $k[t_1, \ldots, t_n]$ that is contained in N maximal ideals has a generating set of cardinality n^N. But actually we can do much better than this.

THEOREM 12.21. *Let I be a radical zero-dimensional ideal of $R = k[t_1, \ldots, t_n]$. Then I can be generated by n elements.*

PROOF. (Vasconcelos) Let $I = \bigcap_{i=1}^N \mathfrak{m}_i$ with $\mathfrak{m}_i$ maximal ideals of $k[t_1, \ldots, t_n]$. Consider the ideal $I \cap k[t_1] = \bigcap_{I=1}^N \mathfrak{m}_i \cap k[t_1]$. By Theorem 12.13, each $\mathfrak{m}_i \cap k[t_1]$ is a maximal ideal of $k[t_1]$, so $I \cap k[t_1]$ is a radical ideal of the PID $k[t_1]$, so it is generated by a product of nonassociate irreducible polynomials, say

$$f(t_1) = g_1(t_1) \cdots g_s(t_1).$$

For $1 \leqslant i \leqslant s$, let $l_i = k[t_1]/g_i$, a finite degree field extension of k. By CRT, we have

$$R/(fR) = k[t_1]/(f)[t_2, \ldots, t_n] \cong \prod_{i=1}^s l_i[t_2, \ldots, t_n].$$

For $1 \leqslant i \leqslant s$, let $I_i := IR/g_iR = Il_i[t_2, \ldots, t_n]$. Since $(R/g_iR)/I_i = R/\langle I, g_i\rangle$, by Exercise 12.6 each I_i is a radical zero-dimensional ideal of $l_i[t_2, \ldots, t_n]$, so by induction there are $f_{i,1}, \ldots, f_{i,n-1} \in I$ such that $\langle f_{i,1}, \ldots, f_{i,n-1}\rangle R/g_iR = I_i$.

For $1 \leqslant i \leqslant n$, put

$$G_i(t_1) := \prod_{j \neq i} g_j(t_1),$$

and for $1 \leqslant k \leqslant n-1$ put

$$H_k = \sum_{1 \leqslant j \leqslant s} G_j(t_1) f_{j,k}.$$

We claim that

$$I = \langle f(t_1), H_1, \ldots, H_{n-1}\rangle.$$

Certainly we have

$$\langle f(t_1)\rangle \subset \langle f(t_1), G_1, \ldots, G_{n-1}\rangle \subset I,$$

so passing to $R/(f(t_1))$ it is enough to show equality after localizating at each prime ideal $\mathfrak{p}$ containing $f(t_1)$. Let $\mathfrak{p}$ be such a prime ideal. Then $\mathfrak{p}$ contains $g_i(t_1)$ for some j, and since the g_j's are pairwise comaximal, for all $j \neq i$, we have that $g_j(t_1)$ is a unit modulo $\mathfrak{p}$, hence $G_i(t_1)$ is a unit modulo $\mathfrak{p}$, whereas $G_j(t_1) \in (g_i)$ for all $j \neq i$. Therefore

$$\langle f(t_1), H_1, \ldots, H_{n-1}\rangle_{\mathfrak{p}} = \langle g_i(t_1), f_{i,1}, \ldots, f_{i,n-1}\rangle_{\mathfrak{p}}.$$

Since $f_{i,1}, \ldots, f_{i,n-1}$ generate I modulo (g_i), they generate I modulo $\mathfrak{p}$ and thus $I_{\mathfrak{p}}$ modulo $R_{\mathfrak{p}}$, so by Nakayama's Lemma they generate $I_{\mathfrak{p}}$, completing the proof. □

In particular, if $S \subset k^n$ is any finite subset, there are polynomials $f_1, \ldots, f_n \in k[t_1, \ldots, t_n]$ such that

$$\{x \in k^n \mid f_1(x) = \ldots = f_n(x) = 0\} = S.$$

EXERCISE 12.7. *Let $I = \langle t_1, t_2 \rangle^2 = \langle t_1^2, t_1 t_2, t_2^2 \rangle$ in $k[t_1, t_2]$. Show: I is zero-dimensional and cannot be generated by 2 elements. (Thus the word "radical" in the statement of Theorem 12.21 is essential.)*

CHAPTER 13

Spec R as a Topological Space

1. The Prime Spectrum

For a ring R, we denote the set of all prime ideals of R by $\operatorname{Spec} R$. Moreover, we refer to $\operatorname{Spec} R$ as the **Zariski spectrum** – or **prime spectrum** – of R.

It is important to notice that $\operatorname{Spec} R$ comes with additional structure. First, it has a natural partial ordering, in which the maximal elements are the maximal ideals, and the minimal elements are (by definition) the **minimal primes**. Also, as O. Zariski first observed, $\operatorname{Spec} R$ can be endowed with a **topology**. To see this, for any ideal I of R, put $V(I) = \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \supseteq I\}$.

PROPOSITION 13.1. *For ideals I, J of R, we have $V(I) = V(J)$ if and only if $\operatorname{rad} I = \operatorname{rad} J$.*

PROOF. For any ideal I and any prime ideal $\mathfrak{p}$, we have $\mathfrak{p} \supseteq I$ if and only if $\mathfrak{p} \supseteq \operatorname{rad} I$, and therefore $V(I) = V(\operatorname{rad} I)$. Conversely, if $V(I) = V(J)$, then the set of prime ideals containing I is the same as the set of prime ideals containing J. So

$$\operatorname{rad} I = \bigcap_{\mathfrak{p} \supseteq I} \mathfrak{p} = \bigcap_{\mathfrak{p} \supseteq J} \mathfrak{p} = \operatorname{rad} J. \qquad \square$$

EXERCISE 13.1. *Let I and J be ideals of a ring R. Show:*

$$V(I) \subseteq V(J) \iff \operatorname{rad} I \supseteq \operatorname{rad} J.$$

Now we claim that the family of subsets $V(I)$ of $\operatorname{Spec} R$ has the following properties:

(ZT1) We have $\varnothing = V(R)$ and $\operatorname{Spec} R = V((0))$.
(ZT2) If $\{I_i\}$ is any collection of ideals of R, then $\bigcap_i V(I_i) = V(\langle I_i \rangle)$.
(ZT3) If $I_1, \ldots, I_n$ are ideals of R, then $\bigcup_{i=1}^n V(I_i) = V(I_1 \cdots I_n) = V(\bigcap_{i=1}^n I_i)$.

(ZT1) is clear. As for (ZT2), let $\mathfrak{p}$ be a prime ideal of R. Then $\mathfrak{p} \in \bigcap_i V(I_i)$ for all i if and only if $\mathfrak{p} \supseteq I_i$ for all i if and only if $\mathfrak{p}$ contains the ideal generated by all I_i. As for (ZT3), $\mathfrak{p}$ contains a product of ideals if and only if it contains one of the ideals of the product.

Therefore there is a unique topology on $\operatorname{Spec} R$ in which the closed sets are precisely those of the form $V(I)$. This is called the **Zariski topology**.

We will now give a characterization of the open sets in the Zariski topology. Recall that a **base** for the open sets of a topology is a collection $\{B_i\}$ of open sets such that:

(BT1) for any point $x \in B_i \cap B_j$, there exists a k such that $x \in B_k \subset B_i \cap B_j$;

(BT2) every open set is a union of the B_i's contained in it.

For $f \in R$, we define $U(f) := \operatorname{Spec} R \backslash V((f))$. In other words, $U(f)$ is the collection of all prime ideals which *do not* contain the element f. For $f, g \in R$, $U(f) \cap U(g)$ is the set of prime ideals $\mathfrak{p}$ containing neither f nor g; since $\mathfrak{p}$ is prime, this is equivalent to $\mathfrak{p}$ not containing fg, thus

$$U(f) \cap U(g) = U(fg),$$

which is a stronger property than (BT1). Moreover, any open set U is of the form $\operatorname{Spec} R \backslash V(I)$. Each ideal I is the union of all of its elements f_i, so $V(I) = \bigcap_i V(f_i)$, so that

$$U = \operatorname{Spec} R \backslash V(I) = \operatorname{Spec} R \backslash \bigcap_i V(f_i) = \bigcup_i (\operatorname{Spec} R \backslash V(f_i)) = \bigcup_i U(f_i).$$

Recall that for a subset A of a topological space X, the closure $\overline{A}$ is defined to be the intersection of all closed subsets of X containing A, and $\overline{A}$ is characterized as the unique minimal closed subset of X that contains A. (It has several other characterizations, e.g. as the set of all limits of convergent nets with terms in X.)

PROPOSITION 13.2. *Let R be a ring, and let $A \subseteq \operatorname{Spec} R$. Then the closure of A in the Zariski topology is*

$$\overline{A} = V(\bigcap_{\mathfrak{p} \in A} \mathfrak{p}).$$

PROOF. It is clear that $V(\bigcap_{\mathfrak{p} \in A} \mathfrak{p})$ is a Zariski-closed subset of $\operatorname{Spec} R$ that contains A. Conversely, a Zariski-closed subset of $\operatorname{Spec} R$ that contains A is of the form $V(I)$ such that $I \subseteq \mathfrak{p}$ for all $\mathfrak{p} \in A$, so $I \subseteq \bigcap_{\mathfrak{p} \in A} \mathfrak{p}$ and thus $V(I) \subseteq V(\bigcap_{\mathfrak{p} \in A} \mathfrak{p})$. Thus $V(\bigcap_{\mathfrak{p} \in A} \mathfrak{p})$ is the unique minimal Zariski-closed subset of $\operatorname{Spec} R$ that contains A, so $V(\bigcap_{\mathfrak{p} \in A} \mathfrak{p}) = \overline{A}$. □

In particular, for $\mathfrak{p} \in \operatorname{Spec} R$, the closure of the singleton set $\{\mathfrak{p}\}$ is the set of prime ideals of R that contain $\mathfrak{p}$. It follows that $\mathfrak{p}$ is a closed point (i.e., the set $\{\mathfrak{p}\}$ is a closed subset) of $\operatorname{Spec} R$ if and only if $\mathfrak{p}$ is maximal, so all points of $\operatorname{Spec} R$ are closed if and only if $\dim R = 0$. Closures of points in the Zariski topology are studied in detail in §4.

PROPOSITION 13.3. *Let R be any ring, and consider the canonical homomorphism $f : R \to R^{\mathrm{red}} = R/\operatorname{nil}(R)$. Then $f^{-1} : \operatorname{Spec} R^{\mathrm{red}} \to \operatorname{Spec} R$ is a homeomorphism.*

EXERCISE 13.2. *Prove Proposition 13.3.*

EXERCISE 13.3. *Let $R_1, \ldots, R_n$ be finitely many rings. Show:* $\operatorname{Spec}(R_1 \times \ldots \times R_n)$ *is canonically homeomorphic to the topological space* $\coprod_{i=1}^n \operatorname{Spec} R_i$.

EXERCISE 13.4. *Let R be a Boolean ring. Earlier we defined a topology on the set "$M(R)$" of all maximal ideals of R. But, as we know, a Boolean ring all prime ideals are maximal, so as sets $M(R) = \operatorname{Spec} R$. Show that moreover the topology we defined on $M(R)$ is the Zariski topology on* $\operatorname{Spec} R$.

2. Properties of the spectrum: quasi-compactness

More than sixty years ago now, N. Bourbaki introduced the term **quasi-compact** for a topological space X for which any open covering has a finite subcovering. The point of this terminology is to reserve **compact** for a space which is both quasi-compact and Hausdorff, and thus emphasize that most of the nice properties of compact spaces in classical topology do rely on the Hausdorff axiom. Nowhere is this terminology more appropriate than in the class of spectral spaces, which as we have seen above, are only Hausdorff in the comparatively trivial case of a zero-dimensional ring. On the other hand:

PROPOSITION 13.4. *For any commutative ring R,* $\operatorname{Spec} R$ *is quasi-compact.*

PROOF. Let $\{U_i\}$ be any open covering of $\operatorname{Spec} R$. For each $\mathfrak{p} \in \operatorname{Spec} R$, there exists an element U of the cover containing $\mathfrak{p}$, and thus a principal open set $X(f)$ containing $\mathfrak{p}$ and contained in U. Therefore there is a refinement of the cover consisting of principal open subsets, and if this refinement has a finite cover, then the original cover certainly does as well. Thus it suffices to assume that the U_i's are basic open sets.[1] So now suppose that $\operatorname{Spec} R = \bigcup_i U(f_i)$. Then we have

$$\operatorname{Spec} R = \bigcup_i U(f_i) = \bigcup_i (\operatorname{Spec} R \backslash V(f_i)) = \operatorname{Spec} R \backslash \bigcap_i V(f_i),$$

so that $\varnothing = \bigcap_i V(f_i) = V(\langle f_i \rangle)$. Therefore the ideal $I = \langle f_i \rangle$ contains 1, and this means that there is some finite subset $f_1, \ldots, f_n$ of I such that $\langle f_1, \ldots, f_n \rangle = R$. Thus $\bigcap_{i=1}^n V(f_i) = \varnothing$, or equivalently, $\operatorname{Spec} R = \bigcup_{i=1}^n U(f_i)$. □

3. Properties of the spectrum: connectedness

LEMMA 13.5. *Let $\mathcal{E}(R)$ be the set of idempotents in a ring R. Then:*

a) *If $e, f \in \mathcal{E}(R)$, then*
   (i) $e^* := 1 - e \in \mathcal{E}(R)$;
   (ii) $e \wedge f := ef \in \mathcal{E}(R)$;
   (iii) $e \vee f := (e^* \wedge f^*)^* = e + f - ef \in \mathcal{E}(R)$.

b) $(\mathcal{E}, \wedge, \vee, *)$ *is a Boolean algebra.*

EXERCISE 13.5. *Prove Lemma 13.5.*

EXERCISE 13.6. *For a topological space X, let* $\operatorname{Clopen}(X)$ *be the family of clopen subsets of X.*

a) *Show:* $\operatorname{Clopen}(X)$ *is a Boolean subalgebra of* 2^X.
b) *Show: if X is compact, then* $\operatorname{Clopen}(X)$ *is the characteristic algebra of X.*

THEOREM 13.6. *Let R be a ring.*

a) *If $e \in \mathcal{E}(R)$ is an idempotent, then $U(e)$ is a clopen subset of* $\operatorname{Spec} R$.
b) *The map $U : \mathcal{E}(R) \to \operatorname{Clopen}(\operatorname{Spec} R)$ given by*

$$e \mapsto U(e)$$

is an isomorphism of Boolean algebras.

[1] This is just the familiar, and easy, fact that it suffices to verify quasi-compactness on any base for the topology. It is also true, but deeper, that one can verify quasi-compactness on any subbase: Alexander's Subbase Theorem.

PROOF. a) For any element $f \in R$, the set $U(f) = \operatorname{Spec} R \backslash V(f)$ is open by definition of the Zariski topology on $\operatorname{Spec} R$. If e is idempotent then $e(1-e) = 0$, so every $\mathfrak{p} \in \operatorname{Spec} R$ contains exactly one of e and $1-e$ and it follows that

$$U(e) = V(1-e),\ U(1-e) = V(e).$$

Thus $U(e)$ is clopen.
b) It is straightforward to see that U is a homomorphism of Boolean algebras: for an idempotent e, we have $U(e^*) = U(1-e) = \operatorname{Spec} R \backslash U(e)$, and for idempotents e, f we have $U(e \wedge f) = U(ef) = U(e) \cap U(f)$. It then follows formally that

$$U(e \vee f) = U((e^* \wedge f^*)^*) = U(e^* \wedge f^*)^* = (U(e)^* \wedge U(f)^*)^*$$

$$= U(e)^{**} \vee U(f)^{**} = U(e) \vee U(f).$$

Indeed a bijective homomorphism of Boolean algebras is an isomorphism.

To check the surjectivity, it will be convenient to work also in $\overline{R} = R/\operatorname{nil} R$. Letting $q : R \to \overline{R}$ be the quotient map, we know that for all $\mathfrak{p} \in \operatorname{Spec} R$, $q(\mathfrak{p}) \in \operatorname{Spec} \overline{R}$ and the map $q_* : \operatorname{Spec} R \to \operatorname{Spec} \overline{R}$ is a homeomorphism. Let Y be a clopen set of $\operatorname{Spec} R$, so also $Y^* = \operatorname{Spec} R \backslash Y$ is clopen and $q(Y), q(Y)^* = q(Y^*)$ are clopen subsets of $\operatorname{Spec} \overline{R}$. For any ring A and a subset Z of $\operatorname{Spec} A$, we put

$$\Delta_A := \bigcap_{\mathfrak{p} \in A} \mathfrak{p},$$

so $\overline{A} = V(\Delta_A)$. Since $v(Y)$, $v(Y^*)$ are clopen subsets, we have

$$V(\Delta_{q(Y)}) = q(Y) \text{ and } V(\Delta_{q(Y^*)}) = q(Y^*).$$

For $\overline{\mathfrak{p}} \in \operatorname{Spec} \overline{R}$, if $\overline{\mathfrak{p}} \supseteq \Delta_{q(Y)} + \Delta_{q(Y^*)}$, then $\overline{\mathfrak{p}} \supseteq \Delta_{q(Y)}$ and $\overline{\mathfrak{p}} \supseteq \Delta_{q(Y^*)}$, so $\overline{\mathfrak{p}} \in q(Y) \cap q(Y^*) = q(Y) \cap q(Y)^* = \varnothing$; this shows $\Delta_{q(Y)} + \Delta_{q(Y^*)} = \overline{R}$. Any $\overline{\mathfrak{p}} \in \operatorname{Spec} \overline{R}$ lies in eaxctly one of $q(Y)$ and $q(Y^*)$ so contains exactly one of $\Delta_{q(Y)}$ and $\Delta_{q(Y^*)}$; thus $\overline{\mathfrak{p}} \supseteq \Delta_{q(Y)} \cap \Delta_{q(Y^*)}$. Thus $\Delta_{q(Y)} \cap \Delta_{q(Y^*)}$ is contained in every prime ideal of $\overline{R}$ hence is contained in the nilradical of $\overline{R}$....which is (0), so

$$\Delta_{q(Y)} \cap \Delta_{q(Y^*)} = (0).$$

By CRT we get

$$\overline{R} = \overline{R}/\Delta_{q(Y^*)} \times \overline{R}/\Delta_{q(Y)} = \Delta_{q(Y)} \times \Delta_{q(Y^*)}.$$

Let $\overline{e} := (0,1)$ be the second idempotent coming from this decomposition. By Proposition 4.16 there is a unique idempotent e of R such that $q(e) = \overline{e}$. For $\mathfrak{p} \in \operatorname{Spec} R$, we have $e \in \mathfrak{p}$ if and only if $\overline{e} \in \overline{\mathfrak{p}}$ if and only if $\overline{\mathfrak{p}} \supseteq \Delta_{q(Y^*)}$ if and only if $\overline{\mathfrak{p}} \in q(Y^*)$ if and only if $\mathfrak{p} \in Y^*$: thus $Y^* = V(e) = U(e^*)$, so $Y = U(e)$.

Now let $e \in \mathcal{E}(R)$. Then $q(U(e))$ is the set of prime ideals of $\overline{R}$ containing $1-\overline{e}$ and $q(U(1-e))$ is the set of prime ideals of $\overline{R}$ containing $\overline{e}$, so

$$\overline{R} = \Delta_{q(U(e))} \times \Delta_{q(U(1-e))}.$$

Since $\Delta_{q(U(e))} \supseteq (1-\overline{e})$ and $\Delta_{q(U(1-e))} \supseteq (\overline{e})$ and

$$\overline{R} = (\overline{e}) \times (1-\overline{e}),$$

we must have

$$\Delta_{q(U(e))} = (1-\overline{e}).$$

An ideal can have at most one idempotent generator: if $(e_1) = (e_2)$ then $e_1 = xe_2$ and $e_2 = ye_1$, so

$$e_1 = xe_2 = xe_2e_2 = e_1e_2 = e_1(ye_1) = ye_1 = e_2.$$

So $U(e)$ determines $\overline{e}$ and thus determines e as the unique idempotent element of R such that $q(e) = \overline{e}$. This shows that the map U is injective. □

COROLLARY 13.7. *For a nonzero ring R, the following are equivalent:*

(i) *R is connected: $\mathcal{E}(R) = \{0, 1\}$.*
(ii) *$\operatorname{Spec} R$ is connected.*

EXERCISE 13.7. *Prove it.*

For the zero ring, we take the convention that it is not connected. This is compatible with the convention that the empty topological space is not connected.

4. Properties of the spectrum: separation and specialization

For the reader's convenience we recall the "lower" separation axioms:

A topological space X is **Kolmogorov** – or T_0 – if for any distinct points $x, y \in X$, the **system of neighborhoods** $\mathcal{N}_x$ and $\mathcal{N}_y$ do not coincide. In plainer language, either there exists an open set U containing x and not containing y, or conversely.

A topological space X is **separated** – or T_1 – if for any distinct points $x, y \in X$, there exists both an open set U containing x and not y and an open set V containing y and not x. A space is separated if and only if all singleton sets $\{x\}$ are closed if and only if for all $x \in X$, $\bigcap_{U \in \mathcal{N}_x} U = \{x\}$.

A topological space X is **Hausdorff** – or T_2 – if for any distinct points $x, y \in X$, there exist open neighborhoods U of x and V of y with $U \cap V = \varnothing$. A space is Hausdorff if and only if for all $x \in X$, the intersection of all closed neighborhoods of x is $\{x\}$.

Hausdorff implies separated implies Kolmogorov. In a general topology course one learns that neither of the converse implications holds in general. On the other hand most of the spaces one encounters in analysis and geometry are Hausdorff, and certainly are if they are Kolmogorov. We are about to see that yet a third state of affairs transpires when we restrict attention to spectra of rings.

Let X be a topological space. We define a relation $\mapsto$ on X by decreeing that for $x, y \in X$, $x \mapsto y$ iff y lies in the closure of the singleton set $\{x\}$. This relation is called **specialization**, and we read $x \mapsto y$ as "x specializes to y".

The reader who is familiar with topology but has not seen the specialization relation before will find an explanation in part f) of the following exercise.

EXERCISE 13.8.

a) *Show: $x \mapsto y$ if and only if $\mathcal{N}_x \subset \mathcal{N}_y$.*
b) *Show: specialization satisfies the following properties:*
   (i) *Reflexivity: $x \mapsto x$; and*

(ii) *Transitivity* $x \mapsto y,\ y \mapsto z \implies x \mapsto z$.

A relation R with these properties is called a ***quasi-ordering****. A partial ordering is a quasi-ordering with the additional axiom of anti-symmetry:* $xRy,\ yRx \implies x = y$.

c) *Show: specialization is a partial ordering on X if and only if X is Kolmogorov.*

d) *Show: a point y is closed*[2] *if and only if $y \mapsto x \implies x = y$.*

e) *A point x for which $x \mapsto y$ holds for all $y \in X$ is called* ***generic****. Give an example of a topological space in which every point is generic.*

f) *Show: X is separated if and only if $x \mapsto y \implies x = y$.*

EXERCISE 13.9. *Let X be a set endowed with a quasi-ordering R. Define a new relation $x \equiv y$ if $x\ R\ y$ and $y\ R\ x$.*

a) *Show: $\equiv$ is an equivalence relation on X.*

b) *Write X' for the set of $\equiv$ equivalence classes, and let $q : X \to X'$ be the natural map – i.e., $x \mapsto \{y \in X \mid y \equiv x\}$. Show that the relation R descends to a relation $\leqslant$ on X': i.e., for $s_1,\ s_2 \in X'$, then by choosing $x_1 \in s_1, x_2 \in s_2$ and putting*

$$s_1 \leqslant s_2 \iff x_1\ R\ x_2,$$

the relation $\leqslant$ is well-defined independent of the choices of x_1 and x_2. Show that moreover $\leqslant$ is a partial ordering on X'.

c) *Let X be a topological space and R be the specialization relation. Endowing X' with the quotient topology via q, show that the induced relation $\leqslant$ on X' is the specialization relation on X', and accordingly by the previous exercise X' is a Kolmogorov space. If it pleases you, show that $q : X \to X'$ is* ***universal*** *for maps from X into a Kolmogorov space Y, hence X' (or rather, $q : X \to X'$) can be regarded as the* ***Kolmogorov quotient*** *of X.*

EXERCISE 13.10. *Let (X, μ) be a measure space, and let $\mathcal{L}^1$ be the space of all measurable functions $f : X \to \mathbb{R}$ with $\int_X |f| d\mu < \infty$. For $f \in \mathcal{L}^1$, define $||f|| := \int_X |f| d\mu$, and for $\epsilon > 0$, put $B(f, \epsilon) = \{g \in \mathcal{L}^1 \mid ||g - f|| < \epsilon\}$. Show that the $B(f, \epsilon)$'s form a base for a topology on $\mathcal{L}^1$, but that this topology is, in general, not Kolmogorov. Show that the Kolmogorov quotient is precisely the usual Lebesgue space L^1, whose elements are not functions but classes of functions modulo μ a.e. equivalence.*

PROPOSITION 13.8. *For any ring R, the spectrum* $\operatorname{Spec} R$ *is a Kolmogorov space. Indeed, for $\mathfrak{p}, \mathfrak{q} \in \operatorname{Spec} R$ we have $\mathfrak{p} \mapsto \mathfrak{q}$ if and only if $\mathfrak{p} \subset \mathfrak{q}$.*

PROOF. For prime ideals $\mathfrak{p}$ and $\mathfrak{q}$ we have

$$\mathfrak{p} \mapsto \mathfrak{q} \iff \mathfrak{q} \in \overline{\{\mathfrak{p}\}} = \{\mathfrak{f} \in \operatorname{Spec} R \mid \mathfrak{f} \supseteq \mathfrak{p}\} \iff \mathfrak{p} \subset \mathfrak{q}.$$

Thus the specialization relation is just containment of ideals, which certainly satisfies antisymmetry: $\mathfrak{p} \subset \mathfrak{q},\ \mathfrak{p} \subset \mathfrak{q} \implies \mathfrak{p} = \mathfrak{q}$. Now apply Exercise 13.9c). □

THEOREM 13.9. *For a commutative ring R, the following are equivalent:*

(i) *The ring $R/\operatorname{nil} R$ is absolutely flat, i.e., every $R/\operatorname{nil} R$-module is flat.*

(ii) *The ring R has Krull dimension zero.*

(iii) *The topological space* $\operatorname{Spec} R$ *is separated.*

[2]Strictly speaking we mean $\{y\}$ is closed, but this terminology is common and convenient.

(iv) *The topological space* $\operatorname{Spec} R$ *is Hausdorff.*
(v) *The topological space* $\operatorname{Spec} R$ *is Boolean.*

PROOF. (i) $\iff$ (ii) This is Theorem 7.27.
(ii) $\iff$ (iii): A space is separated if and only if all of its singleton sets are closed. But if $\mathfrak{p}$ is prime, $V(\mathfrak{p})$ consists of all primes containing $\mathfrak{p}$, so $V(\mathfrak{p}) = \{\mathfrak{p}\}$ if and only if $\mathfrak{p}$ is maximal.
Certainly (v) $\implies$ (iv) $\implies$ (iii).
(i) $\implies$ (v): Since $\operatorname{Spec} R = \operatorname{Spec}(R/\operatorname{nil} R)$, we may well assume that R itself is absolutely flat. Let $\mathfrak{p}$ and $\mathfrak{q}$ be distinct prime ideals; since both are maximal, there exists an element $f \in \mathfrak{p}\backslash\mathfrak{q}$. By Proposition 3.103, there is an idempotent e with $(e) = (f)$, and therefore $e \in \mathfrak{p}\backslash\mathfrak{q}$. Then $D(1-e)$, $D(e)$ is a separation of $\operatorname{Spec} R$. More precisely, $D(e) \cap D(1-e) = D(e(1-e)) = D(e-e^2) = D(0) = \varnothing$, whereas for any prime ideal $\mathfrak{p}$, since $0 = e(1-e) \in \mathfrak{p}$, we must have $e \in \mathfrak{p}$ or $1-e \in \mathfrak{p}$. By construction, $\mathfrak{p} \in D(1-e)$, $\mathfrak{q} \in D(e)$. This shows $\operatorname{Spec} R$ is Hausdorff, and more: given points $P \neq Q$ of X, we found a separation $X = U \coprod V$ with $P \in U$, $Q \in V$, so X is zero-dimensional. By Proposition 13.4, every ring has quasi-compact spectrum, so $\operatorname{Spec} R$ is Hausdorff, zero-dimensional and quasi-compact, i.e., Boolean. □

EXERCISE 13.11.

a) *Let R be a product of fields. Show:* $\operatorname{Spec} R$ *is a Boolean space.*
b) *Let $\{R_i\}_{i\in I}$ be a family of rings, each of which has Krull dimension 0, and put $R = \prod_i R_i$. Must* $\operatorname{Spec} R$ *be Boolean?*

4.1. Gelfand Rings. Let R be any ring, let $\mathfrak{m} \in \operatorname{MaxSpec} R$, and put

$$O_{\mathfrak{m}} := \bigcap_{\mathfrak{p}\in\operatorname{Spec} R,\ \mathfrak{p}\subseteq\mathfrak{m}} \mathfrak{p}$$

be the intersection of all prime ideals contained in $\mathfrak{m}$. We claim that $O_{\mathfrak{m}}$ is the set of all $x \in R$ such that there is $y \in R\backslash\mathfrak{m}$ such that xy is nilpotent. To see this, suppose that $x \in R$ is such that xy is nilpotent for some $y \in R\backslash\mathfrak{m}$. Then x is nilpotent in $R/\mathfrak{m}$, so $x^N \in \mathfrak{m}$ for some $N \in \mathbb{Z}^+$, so $x \in \mathfrak{m}$. Conversely, if $x \in R$ is such that xy is not nilpotent for any $y \in R\backslash\mathfrak{m}$, then the multiplicative set $S = \{x^n y \mid n \in \mathbb{N}, y \in R\backslash\mathfrak{m}\}$ does not contain 0 and contains $R\backslash\mathfrak{m}$, so there is $\mathfrak{p} \in \operatorname{Spec} R$ such that $\mathfrak{p} \subseteq R\backslash S \subseteq \mathfrak{m}$ and $x \notin \mathfrak{p}$, so $x \notin O_{\mathfrak{m}}$.

THEOREM 13.10. *For a ring R, the following are equivalent:*

(i) *Every prime ideal of R is contained in a unique maximal ideal.*
(ii) *For all $\mathfrak{m}_1 \neq \mathfrak{m}_2 \in \operatorname{MaxSpec} R$, there is $x_1 \in \mathfrak{m}_1\backslash\mathfrak{m}_2$ and $x_2 \in \mathfrak{m}_2\backslash\mathfrak{m}_1$ such that $x_1x_2 = 0$.*
(iii) $\operatorname{MaxSpec} R$ *is a retract of* $\operatorname{Spec} R$.
(iv) *For all $\mathfrak{m} \in \operatorname{MaxSpec} R$, the only maximal ideal containing $O_{\mathfrak{m}}$ is $\mathfrak{m}$.*
(v) $\operatorname{Spec} R$ *is quasi-normal: two disjoint closed sets can be separated by two disjoint open sets.*
(vi) *For all $x \in R$, there are $r, s \in R$ such that $(1+rx)(1+s(1-x)) = 0$.*

A ring satisfying these equivalent conditions is called a ***Gelfand ring****.*

PROOF. (i) $\implies$ (ii): Assume (i), let $\mathfrak{m}_1$ and $\mathfrak{m}_2$ be distinct maximal ideals and consider the multiplicative subset

$$S := (R\backslash\mathfrak{m}_1) \cdot (R\backslash\mathfrak{m}_2).$$

If S did not contain 0, then by Multiplicative Avoidance there would be a prime ideal $\mathfrak{p} \subseteq R\backslash S \subseteq \mathfrak{m}_1 \cap \mathfrak{m}_2$, contradicting our assumption. Thus there are $x_2 \in R\backslash\mathfrak{m}_1$ and $x_1 \in R\backslash\mathfrak{m}_2$ such that $x_1x_2 = 0$. Because $\mathfrak{m}_1$ and $\mathfrak{m}_2$ are prime, it follows that $x_1 \in \mathfrak{m}_1$ and $x_2 \in \mathfrak{m}_2$.

(ii) $\implies$ (i): Suppose that (ii) holds, and seeking a contradiction, suppose there is a prime ideal $\mathfrak{p}$ and distinct maximal ideals $\mathfrak{m}_1 \neq \mathfrak{m}_2$ such that $\mathfrak{p} \subseteq \mathfrak{m}_1 \cap \mathfrak{m}_2$. Then we may write $0 = x_1x_2$ with $x_1 \notin mm_2$ and $x_2 \notin \mathfrak{m}_1$, and since $0 \in \mathfrak{p}$ we have that $\mathfrak{p}$ contains either x_1 or x_2, but since $\mathfrak{p}$ is contained in both $\mathfrak{m}_1$ and $\mathfrak{m}_2$, this is a contradiction.

(iii) $\implies$ (i): Let $\tau : \operatorname{Spec} R \to \operatorname{MaxSpec} R$ be a retraction. Let $\mathfrak{p} \in \operatorname{Spec} R$, and put $\mathfrak{m} \coloneqq \tau(\mathfrak{p})$. Then $\mathfrak{p} \in \tau^{-1}(\{\mathfrak{m}\})$, and since $\tau^{-1}(\{\mathfrak{m}\})$ is closed, also for any specialization $\mathfrak{q}$ of $\mathfrak{p}$ we have $\tau(\mathfrak{q}) = \mathfrak{m}$. Because τ fixes every maximal ideal, we conclude that the only maximal ideal containign $\mathfrak{p}$ is $\mathfrak{m}$.

(iv) $\implies$ (i): Suppose that (iii) holds, and let $\mathfrak{p} \subseteq \mathfrak{m}$ be a prime ideal contained in a maximal ideal. If $\mathfrak{m}'$ is another maximal ideal containing $\mathfrak{p}$ then $\mathfrak{m}' \supseteq O_{\mathfrak{m}}$, so $\mathfrak{m}' = \mathfrak{m}$ by hypothesis.

(i) $\implies$ (iii) and (iv): Suppose that (i) holds, and let $\mu : \operatorname{Spec} R \to \operatorname{MaxSpec} R$ be the function that maps $\mathfrak{p} \in \operatorname{Spec} R$ to the unique maximal ideal that contains it. We CLAIM that μ is continuous. If so, since $\mu(\mathfrak{m}) = \mathfrak{m}$ for all $\mathfrak{m} \in \operatorname{MaxSpec} R$, the map $\mu : \operatorname{Spec} R \to \operatorname{MaxSpec} R$ is a retraction, establishing (iii). Also if so, we have that $\mu^{-1}(\{\mathfrak{m}\}) = \{\mathfrak{p} \in \operatorname{Spec} R \mid \mathfrak{p} \subseteq \mathfrak{m}\}$ is closed in $\operatorname{Spec} R$, so

$$\mu^{-1}(\{\mathfrak{m}\}) = \overline{\mu^{-1}(\{\mathfrak{m}\})} = V(O_{\mathfrak{m}}),$$

so no maximal ideal other than $\mathfrak{m}$ contains $\mathcal{O}_{\mathfrak{m}}$, establishing (iv).

Now we establish that μ is continuous. Let W be a closed subset of $\operatorname{MaxSpec} R$, and put $J \coloneqq \bigcap_{\mathfrak{m}\in W} \mathfrak{m}$, so $W = Z_{\operatorname{MaxSpec}}(J)$ (i.e., the set of maximal ideals containing J). Put $V \coloneqq \mu^{-1}(W)$ and put $I \coloneqq \bigcap_{\mathfrak{p}\in\operatorname{Spec} R|\mu(\mathfrak{p})\in V} \mathfrak{p}$. We want to show that $V = V(I)$: that is, if for $\mathfrak{p} \in \operatorname{Spec} R$ we have $\mathfrak{p} \supseteq I$ then $\mu(\mathfrak{p}) \in W$. If $\mathfrak{q} \in \operatorname{Spec} R$ and $\mathfrak{q} \subseteq B \coloneqq \bigcup_{\mathfrak{m}\in W} \mathfrak{m}$, then $\mu(\mathfrak{q}) \in W$: indeed, $\mathfrak{q} + J \subseteq B \subsetneq R$, so there is $\mathfrak{m} \in \operatorname{MaxSpec} R$ such that $\mathfrak{q} + J \subseteq \mathfrak{m}$; since $\mathfrak{m} \supseteq J$ and $W = Z_{\operatorname{MaxSpec}}(J)$, we have $\mathfrak{m} \in W$, and since $\mathfrak{q} \subseteq \mathfrak{m}$ we have $\mu(\mathfrak{q}) = \mathfrak{m}$. Now let $\mathfrak{p}$ be a prime ideal containing I: we will show that $\mathfrak{p}$ contains a prime ideal $\mathfrak{q}$ such that $\mathfrak{q} \subseteq B$, hence by what was just done we get $\mu(\mathfrak{p}) = \mu(\mathfrak{q}) \in W$. Put

$$S \coloneqq R\backslash B \text{ and } T \coloneqq R\backslash\mathfrak{p}$$

and choose $s \in S$ and $t \in T$. Since $\mathfrak{p} \supseteq I$, there is $\mathfrak{p}' \in \mu^{-1}(W)$ such that $t \notin \mathfrak{p}'$, and since $s \notin \mathfrak{p}'$ we have $st \notin \mathfrak{p}'$, so $st \notin I$. Thus the multiplicative system ST does not meet I, so by Multiplicative Avoidance there is a prime ideal $\mathfrak{q}$ containing I and disjoint from ST, and we have $\mathfrak{q} \cap \mathfrak{p} \cap B$, establishing the continuity of μ. This completes the proof of the equivalence of conditions (i) through (iv).

(i) $\implies$ (v): Suppose (i) holds. Then $\operatorname{MaxSpec} R$ is Hausdorff: let $\mathfrak{m}_1$ and $\mathfrak{m}_2$ be distinct maximal ideals of R, and since (i) $\implies$ (ii) there is $x_1 \in \mathfrak{m}_1\backslash\mathfrak{m}_2$ and $x_2 \in \mathfrak{m}_2\backslash\mathfrak{m}_1$ such that $x_1x_2 = 0$. Then $U_{\operatorname{MaxSpec}}(x_2)$ is an open neighborhood of $\mathfrak{m}_1$ and $U_{\operatorname{MaxSpec}}(x_1)$ is an open neighborhood of $\mathfrak{m}_2$, and $U_{\operatorname{MaxSpec}}(x_1) \cap U_{\operatorname{MaxSpec}}(x_2) = U_{\operatorname{MaxSpec}}(x_1x_2) = U_{\operatorname{MaxSpec}}(0) = \varnothing$. Now let V_1 and V_2 be disjoint closed subsets of $\operatorname{Spec} R$. Since $\operatorname{Spec} R$ is quasi-compact, V_1 and V_2 are both quasi-compact. If $\mathfrak{m} \in \mu(V_1) \cap \mu(V_2)$, then for $i = 1, 2$ there is $\mathfrak{p}_i \in V_i$ such that $\mu(\mathfrak{p}_i) = \mathfrak{m}$. Since $\mathfrak{m}$ is a specialization of $\mathfrak{p}_i$ and V_i is closed, we have $\mathfrak{m} \in V_1 \cap V_2$, a contradiction. So $\mu(V_1)$ and $\mu(V_2)$ are disjoint quasi-compact subsets of the compact space $\operatorname{MaxSpec} R$, so

they are closed. Since compact spaces are normal, there are disjoint open subsets $U_1 \supseteq \mu(V_1)$ and $U_2 \supseteq \mu(V_2)$, and then $\mu^{-1}(U_1)$ and $\mu^{-1}(U_2)$ are disjoint open subsets containing V_1 and V_2 respectively.

(v) $\implies$ (i): Suppose $\operatorname{Spec} R$ is quasi-normal, and let $\mathfrak{m}_1$ and $\mathfrak{m}_2$ be disjoint maximal ideals of R. Then $\{\mathfrak{m}_1\}$ and $\{\mathfrak{m}_2\}$ are disjoint closed subsets of $\operatorname{Spec} R$, so there are disjoint open subsets U_1 and U_2 with $\mathfrak{m}_1 \in U_1$ and $\mathfrak{m}_2 \in U_2$. Let $\mathfrak{p} \in \operatorname{Spec} R$. Then $\mathfrak{p}$ cannot lie in both of U_1 and U_2, so $\mathfrak{p}$ must lie in at least one of the cloesd subsets $\operatorname{Spec} R \backslash U_1$ and $\operatorname{Spec} R \backslash U_2$. If $\mathfrak{p}$ lies in $\operatorname{Spec} R \backslash U_1$, then this is a closed subset containing $\mathfrak{p}$ and not containing $\mathfrak{m}_1$, so $\mathfrak{m}_1$ does not lie in the closure of $\mathfrak{p}$ and thus $\mathfrak{m}_1$ does not contain $\mathfrak{p}$; similarly, if $\mathfrak{p}$ lies in $\operatorname{Spec} R \backslash U_2$ then $\mathfrak{m}_2$ does not contain $\mathfrak{p}$. Thus $\mathfrak{p}$ cannot be contained in more than one maximal ideal.

(i) $\implies$ (vi): Suppose (i) holds, and let $x \in R$. Put $x' := 1 - x$. Let S (resp. S') be the multiplicative subset of R consisting of elements that are congruent to 1 modulo x (resp. modulo x'), and put $T := SS'$. If T did not contain 0, then there is a prime ideal $\mathfrak{p}$ of R that is disjoint from T. Moreover the ideal $\mathfrak{p} + (x)$ is proper: if not we would have $1 = p + ax$ with $p \in \mathfrak{p}$ and $a \in R$ and then $p \in S \subseteq T$. Similarly the ideal $\mathfrak{p} + (x')$ is proper. So there is a maximal ideal $\mathfrak{m}$ containing $\mathfrak{p} + (x)$ and a maximal ideal $\mathfrak{m}'$ containing $\mathfrak{p} + (x')$. We must have $\mathfrak{m} \neq \mathfrak{m}'$, for otherwise $\mathfrak{m}$ would contain $x + x' = 1$, and thus $\mathfrak{p}$ is contained in two different maximal ideals: contradiction. So there are $r, s \in R$ such that

$$0 = (1 + rx)(1 + s(1 - x)).$$

(vi) $\implies$ (i): Suppose (vi) holds, and, seeking a contradiction, that some prime ideal $\mathfrak{p}$ is contained in distinct maximal ideals $\mathfrak{m}$ and $\mathfrak{m}'$. Then there are $m \in \mathfrak{m}$ and $m' \in \mathfrak{m}'$ such that $m + m' = 1$, so there are $r, s \in R$ such that $0 = (1 + rm)(1 + sm')$. Then $\mathfrak{p}$ contains either $1 + rm$ or $1 + sm'$; in the former case $1 \in \mathfrak{m}$, while in the latter case $1 \in \mathfrak{m}'$: either way, a contradiction. □

EXERCISE 13.12. *Show: the class of Gelfand rings is closed under quotients, localizations and direct products.*

EXERCISE 13.13. *(E. Wofsey[3]) Show: if R is a Gelfand ring, then* $\operatorname{MaxSpec} R$ *is a deformation retract of* $\operatorname{Spec} R$. *In particular, the two spaces are homotopy equivalent.*

Any local ring is a Gelfand ring, and a Gelfand domain must be local: in a domain, (0) is a prime ideal contained in every maximal ideal. The following result gives a much more interesting class of Gelfand rings:

COROLLARY 13.11. *Let X be a topological space. The ring $C(X)$ of real-valued continuous functions on X is a Gelfand ring.*

PROOF. We will verify condition (vi) of Theorem 13.10. Let $f \in C(X)$. Put $u := \max(f, 1 - f)$. First of all, $u \in C(X)$, e.g. because for $a, b \in \mathbb{R}$ we have $\max(a, b) = \frac{a+b+|a-b|}{2}$. Moreover $u(x) > 0$ for all $x \in \mathbb{R}$, so $u \in C(X)^\times$. Consider

$$g := (1 + \left(\frac{-1}{u}\right) f)(1 + \left(\frac{-1}{u}\right)(1 - f)).$$

Then for all $x \in X$, either $u(x) = f(x)$ and the first factor of g is 0 or $u(x) = (1 - f)(x)$ and the second factor of g is 0. So condition (vi) applies with $r = s = \frac{-1}{u}$. □

[3]Cf. `http://math.stackexchange.com/questions/1586745`

In the course of the proof of Theorem 13.10 we saw that for any Gelfand ring R, the space $\operatorname{MaxSpec} R$ is compact (once again we emphasize: quasi-compact plus Hausdorff!). Conversely, if X is a compact space, then we saw in §5.2 that $\operatorname{MaxSpec} C(X)$, when endowed with the Zariski topology, is homeomorphic to X. Thus the spaces that are homeomorphic to $\operatorname{MaxSpec} R$ for a Gelfand ring R are precisely the compact spaces. This raises several further questions: (i) which non-Hausdorff spaces are homeomorphic to $\operatorname{MaxSpec} R$ for some ring R; and (ii) what is the class of rings R for which $\operatorname{MaxSpec} R$ is compact? We will state the answer to the first question later in this chapter, and we will now answer the second question:

THEOREM 13.12. *For a ring R, the following are equivalent:*

(i) *The ring $R/J(R)$ is Gelfand.*
(ii) *The topological space $\operatorname{MaxSpec} R$ is compact*
(iii) *The topological space $\operatorname{MaxSpec} R$ is Hausdorff.*

PROOF. (i) $\implies$ (ii): For a ring R, let $q : R \to R/J(R)$ be the quotient map. Then $q^* : \operatorname{MaxSpec} R/J(R) \to \operatorname{MaxSpec} R$ is essentially the identity map: it is certainly a homeomorphism. So if $R/J(R)$ is Gelfand, then by the proof of Theorem 13.10 the space $\operatorname{MaxSpec} R/J(R)$ is compact, hence so is $\operatorname{MaxSpec} R$.
(ii) $\iff$ (iii): We know that $\operatorname{MaxSpec} R$ is quasi-compact, so this is immediate.
(ii) $\implies$ (i): Suppose that $\operatorname{MaxSpec} R$ is Hausdorff. Let $\mathfrak{m}_1 \neq \mathfrak{m}_2$ be distinct maximal ideals of R; beacuse $\operatorname{MaxSpec} R$ is Hausdorff and the principal open sets $\{U(f)\}_{f \in R}$ form a base for the topology, there must be $x_1, x_2 \in R$ such that $U(x_1) \cap U(x_2) = \varnothing$, $\mathfrak{m}_1 \in U(x_2)$ and $\mathfrak{m}_2 \in U(x_1)$. Then $U(x_1x_2) = U(x_1) \cap U(x_2) = \varnothing$, which means that every maximal ideal of R contains x_1x_2, i.e., $x_1x_2 \in J(R)$, so $x_1 \in \mathfrak{m}_1$ and $x_2 \in \mathfrak{m}_2$. Keeping in mind the canonical homeomorphism $\operatorname{MaxSpec} R/J(R) \to \operatorname{MaxSpec} R$, this shows that $R/J(R)$ satisfies condition (ii) of Theorem 13.10 and is thus a Gelfand ring. □

EXERCISE 13.14. *Show: a Boolean ring is a Gelfand ring.*

A **clean ring** (also called an **exchange ring**) is a ring in R in which for all $x \in R$ there is an idempotent $e \in R$ such that $x + e \in R^\times$.

EXERCISE 13.15.

a) *Show: every Boolean ring is a clean ring.*
b) *Show: every clean ring is a Gelfand ring. (Hint: for $x \in R$, let e be an idempotent such that $e - x \in R^\times$. Show: $\left(1 + \frac{x}{e-x}\right)\left(1 - \frac{1-x}{e-x}\right) = 0$.)*
c) *Show: every local ring is a clean ring.*
d) *Show: if $\operatorname{Spec} R$ is connected, then R is clean if and only if it is local.*

5. Irreducible spaces

A topological space is **irreducible** if it is nonempty and if it cannot be expressed as the union of two proper closed subsets.

EXERCISE 13.16. *Show: for a Hausdorff topological space X, the following are equivalent:*

(i) *The space X is irreducible.*
(ii) *We have $\#X = 1$.*

PROPOSITION 13.13. *For a topological space X, the following are equivalent:*

(i) *The space X is irreducible.*
(ii) *Every finite intersection of nonempty open subsets (including the empty intersection!) is nonempty.*
(iii) *Every nonempty open subset of X is dense.*
(iv) *Every open subset of X is connected.*

EXERCISE 13.17. *Prove Proposition 13.13.*

PROPOSITION 13.14. *Let X be a nonempty topological space.*

a) *If X is irreducible, then every nonempty open subset of X is irreducible.*
b) *If a subset Y of X is irreducible, so is its closure $\overline{Y}$.*
c) *If $\{U_i\}$ is an open covering of X such that $U_i \cap U_j \neq \varnothing$ for all i, j and each U_i is irreducible, then X is irreducible.*
d) *If $f : X \to Y$ is continuous and X is irreducible, then $f(X)$ is irreducible in Y.*

PROOF. a) Let U be a nonempty open subset of X. By Proposition 13.13, it suffices to show that any nonempty open subset V of U is dense. But V is also a nonempty open subset of the irreducible space X.
b) Suppose $\overline{Y} = A \cup B$ where A and B are each proper closed subsets of $\overline{Y}$; since $\overline{Y}$ is itself closed, A and B are closed in X, and then $Y = (Y \cap A) \cup (Y \cap B)$. If $Y \cap A = Y$ then $Y \subset A$ and hence $\overline{Y} \subset \overline{A} = A$, contradiction. So A is proper in Y and similarly so is B, thus Y is not irreducible.
c) Let V be a nonempty open subset of X. Since the U_i's are a covering of X, there exists at least one i such that $V \cap U_i \neq \varnothing$, and thus by irreducibility $V \cap U_i$ is a dense open subset of U_i. Therefore, for any index j, $V \cap U_i$ intersects the nonempty open subset $U_j \cap U_i$, so in particular V intersects every element U_j of the covering. Thus for all sets U_i in an open covering, $V \cap U_i$ is dense in U_i, so V is dense in X.
d) If $f(X)$ is not irreducible, there exist closed subsets A and B of Y such that $A \cap f(X)$ and $B \cap f(X)$ are both proper subsets of $f(X)$ and $f(X) \subset A \cup B$. Then $f^{-1}(A)$ and $f^{-1}(B)$ are proper closed subsets of X whose union is all of X. □

PROPOSITION 13.15. *Let R be a ring. Let $V \subset \operatorname{Spec} R$ be a Zariski-closed subset, so $V = V(I)$ for a unique radical ideal I. The following are equivalent:*

(i) *The subspace $V(I)$ is irreducible.*
(ii) *The ideal I is prime.*

PROOF. $\neg$ (ii) $\implies$ $\neg$ (i): Let $a, b \in R$ such that $ab \in R$ and $a, b \in R \backslash I$. Then I contains neither $\operatorname{rad}(a)$ nor $\operatorname{rad}(b)$, so $V(I)$ is contained in neither $V(a)$ nor $V(b)$, but $V(a) \cup V(b) = V(ab) \supseteq V(I)$. Thus $V(a) \cap V(I)$ and $V(b) \cap V(I)$ are two proper closed subsets whose union is $V(I)$, so $V(I)$ is reducible.
(ii) $\implies$ (i): Suppose $\mathfrak{p}$ is a prime ideal. We claim that $V(\mathfrak{p})$ is irreducible. If not, there are ideals I and J such that $V(I)$ and $V(J)$ are both proper subsets of $V(\mathfrak{p})$ and $V(\mathfrak{p}) = V(I) \cup V(J) = V(IJ)$. But then $\mathfrak{p} = \operatorname{rad}(IJ) \supseteq IJ$ and since $\mathfrak{p}$ is prime this implies $\mathfrak{p} \supseteq I$ or $\mathfrak{p} \supseteq J$. Without loss of generality, suppose $\mathfrak{p} \supseteq I$; then $V(\mathfrak{p}) \subset V(I)$, so that $V(I)$ is not proper in $V(\mathfrak{p})$, contradiction. □

Let x be a point of a topological space, and consider the set of all irreducible subspaces of X containing x. (Since $\{x\}$ itself is irreducible, this set is nonempty.) The union of a chain of irreducible subspaces being irreducible, Zorn's Lemma says that

there exists at least one maximal irreducible subset containing x. A maximal irreducible subset (which, by the above, is necessarily closed) is called an **irreducible component** of X. Since irreducible subsets are connected, each irreducible component lies in a unique connected component. It is *not* true in general that the connected component of x is the union of the irreducible components containing x: the way that irreducible components are combined to form connected components is slightly more complicated and explored in Exercise 13.22.

However, unlike connected components, it is possible for a given point to lie in more than one irreducible component. We will see examples shortly.

In the case of the Zariski topology on $\operatorname{Spec} R$, it follows from Proposition 13.15 that the irreducible components of $\operatorname{Spec} R$ are the subsets $V(\mathfrak{p})$ for a minimal prime ideal $\mathfrak{p}$. Above we showed that every nonempty topological space has at least one irreducible component, so this argument shows that every nonzero ring admits minimal primes. Thus we have deduced a commutative algebraic result as a consequence of a topological result. However we showed this earlier in Proposition 4.26 and the two proofs are essentially the same Zorn's Lemma argument. A more interesting topological argument is coming up soon.

6. Noetherianity

6.1. Noetherian topological spaces. We now introduce a property of topological spaces which, from the standpoint of conventional geometry, looks completely bizarre:

PROPOSITION 13.16. *For a topological space X, the following are equivalent:*

(i) *Every ascending chain of open subsets is eventually constant.*
(ibis) *Every descending chain of closed subsets is eventually constant.*
(ii) *Every nonempty family of open subsets has a maximal element.*
(iibis) *Every nonempty family of closed subsets has a minimal element.*
(iii) *Every open subset is quasi-compact.*
(iv) *Every subset is quasi-compact.*

A space satisfying any (and hence all) of these conditions is called ***Noetherian****.*

PROOF. The equivalence of (i) and (ibis), and of (ii) and (iibis) is immediate from taking complements. The equivalence of (i) and (ii) is a general property of partially ordered sets.

(i) $\iff$ (iii): Assume (i), let U be any open set in X and let $\{V_j\}$ be an open covering of U. We assume for a contradiction that there is no finite subcovering. Choose any j_1 and put $U_1 := V_{j_1}$. Since $U_1 \neq U$, there exists j_2 such that U_1 does not contain V_{j_2}, and put $U_2 = U_1 \cup V_{j_2}$. Again our assumpion implies that $U_2 \supsetneq U$, and continuing in this fashion we will construct an infinite properly ascending chain of open subsets of X, contradiction. Conversely, assume (iii) and let $\{U_i\}_{i=1}^{\infty}$ be an infinite properly ascending chain of subsets. Then $U = \bigcup_i U_i$ is not quasi-compact.

Obviously (iv) $\implies$ (iii), so finally we will show that (iii) $\implies$ (iv). Suppose that $Y \subset X$ is not quasi-compact, and let $\{V_i\}_{i \in I}$ be a covering of Y by relatively open subsets without a finite subcover. We may write each V_i as $U_i \cap Y$ with U_i open in Y. Put $U = \bigcup_i U_i$. Then, since U is quasi-compact, there exists a finite subset $J \subset I$ such that $U = \bigcup_{j \in J} U_j$, and then $Y = U \cap Y = \bigcup_{j \in J} U_j \cap Y = \bigcup_{j \in J} V_j$. $\square$

COROLLARY 13.17. *A Noetherian Hausdorff space is finite.*

PROOF. In a Hausdorff space every quasi-compact subset is closed. Therefore, using the equivalence (i) $\iff$ (iv) in Proposition 13.16, in a Noetherian Hausdorff space every subset is closed, so such a space is discrete. But it is also quasi-compact, so it is finite. □

PROPOSITION 13.18. *Let X be a topological space.*

a) *The following are equivalent:*
   (i) *There is a finite partition of X into connected clopen subsets.*
   (ii) *The space X has finitely many connected components.*
   (iii) *The space X has finitely many clopen subsets.*

b) *The equivalent conditions of part a) hold when X is Noetherian.*

PROOF. a) (i) $\implies$ (ii): Whenever a topological space admits a partition into connected clopen subsets, these subsets are the connected components of X.
(ii) $\implies$ (i): In any topological space, each connected component is closed. If there are only finitely many connected components then the complement of each component is a finite union of closed sets, so each connected component is clopen.
(i) $\implies$ (iii): Intersecting any clopen set with a connected component $C(x)$ gives either the empty set or $C(x)$, and the result follows easily from this.
(iii) $\implies$ (i): A partition of X into clopen sets is maximal if and only if each clopen set in the partition is connected, so in any nonmaximal partition we can partition one of the clopen sets in the partition into two clopen subsets, increasing the number of clopen sets in the partition by 1. So if X has finitely many clopen subsets then this process, starting with $\{X\}$, must terminate after finitely many steps, yielding a finite partition into connected clopen subsets.
b) Suppose X is Noetherian, and let $\mathcal{F}$ be the family of closed subsets of X which have infinitely many connected components. If $\mathcal{F}$ is nonempty, then since X is Noetherian, $\mathcal{F}$ has a minimal element Y. Then Y is nonempty and disconnected, so $Y = Y_1 \coprod Y_2$ with Y_1, Y_2 nonempty. By minimality of Y, the proper closed subsets Y_1 and Y_2 each have finitely many connected components, hence so does Y: contradiction. Applying this to X, we get that X has finitely many connected components. □

Just to be sure: if a topological space X has infinitely many connected components, it may or may not admit a partition into clopen subsets. This does hold if X is a paracompact topological manifold. Notice though that this holds for a totally disconnected space iff the space is discrete, and there are many totally disconnected spaces that are not discrete, e.g. any infinite boolean space or the rational numbers as a subspace of the real numbers.

PROPOSITION 13.19. *Let X be a Noetherian topological space.*

a) *There are finitely many closed irreducible subsets $\{A_i\}_{i=1}^n$ such that $X = \bigcup_{i=1}^n A_i$.*

b) *Starting with any finite family $\{A_i\}_{i=1}^n$ as in part a) and eliminating all redundant sets – i.e., all A_i such that $A_i \subset A_j$ for some $j \neq i$ – we arrive at the set of irreducible components of X. In particular, the irreducible components of a Noetherian space are finite in number.*

PROOF. a) Let X be a Noetherian topological space. We first claim that X can be expressed as a finite union of irreducible closed subsets. Indeed, consider

the collection of closed subsets of X which cannot be expressed as a finite union of irreducible closed subsets. If this collection is nonempty, then by Proposition 13.16 there exists a minimal element Y. Certainly Y is not itself irreducible, so is the union of two strictly smaller closed subsets Z_1 and Z_2. But Z_1 and Z_2, being strictly smaller than Y, must therefore be expressible as finite unions of irreducible closed subsets and therefore so also can Y be so expressed, contradiction.

b) So write

$$X = A_1 \cup \ldots \cup A_n$$

where each A_i is closed and irreducible. If for some $i \neq j$ we have $A_i \subset A_j$, then we call A_i **redundant** and remove it from our list. After a finite number of such removals, we may assume that the above finite covering of X by closed irreducibles is **irredundant** in the sense that there are no containment relations between distinct A_i's. Now let Z be any irreducible closed subset. Since $Z = \bigcup_{i=1}^n (Z \cap A_i)$ and Z is irreducible, we must have $Z = Z \cap A_i$ for some i, i.e., $Z \subset A_i$. It follows that the "irredundant" A_i's are precisely the maximal irreducible closed subsets, i.e., the irreducible components. □

6.2. Applications to Noetherian rings.

PROPOSITION 13.20. *For a ring R, the following are equivalent:*

(i) *R satisfies the ascending chain condition on radical ideals.*
(ii) *$\operatorname{Spec} R$ is a Noetherian space.*

In particular if R – or even $R^{\mathrm{red}} = R/\operatorname{nil}(R)$ – is a Noetherian ring, then $\operatorname{Spec} R$ is a Noetherian space.

PROOF. Since $I \mapsto V(I)$ gives a bijection between radical ideals and Zariski closed subsets, (ACC) on radical ideals is equivalent to (DCC) on closed subsets. Evidently these conditions occur if R is itself Noetherian, or, since $\operatorname{Spec} R$ is canonically homeomorphic to $\operatorname{Spec} R^{\mathrm{red}}$, if R^{red} is Noetherian. □

COROLLARY 13.21. *Let I be a proper ideal in a Noetherian ring R. The set of prime ideals $\mathfrak{p}$ which are minimal over I (i.e., minimal among all prime ideals containing I) is finite and nonempty.*

EXERCISE 13.18. *Prove Corollary 13.21.*

EXERCISE 13.19. *Let I be an infinite set, and for all $i \in I$, let $\mathfrak{r}_i$ be a nonzero ring. Show: the ring $\prod_{i \in I} \mathfrak{r}_i$ is not Noetherian.*

The following result shows that every Noetherian ring is a finite product of connected Noetherian rings in an essentially unique way.

THEOREM 13.22. *Let R be a nonzero Noetherian ring.*

a) *There is a unique $n \in \mathbb{Z}^+$ for which there are $I_1, \ldots, I_n \in \mathcal{I}(R)$ such that:*
   (i) *For all $1 \leqslant i \leqslant n$ the ring R/I_i is connected.*
   (ii) *For all $1 \leqslant i \leqslant n$ there is an idempotent $e_i \in R$ such that $I_i = \langle e_i \rangle$.*
   (iii) *We have $\bigcap_{i=1}^n I_i = (0)$ and $I_i + I_j = Rf$ or all $1 \leqslant i \neq j \leqslant n$. Thus we have a canonical isomorphism*

$$R \xrightarrow{\sim} \prod_{i=1}^n R/I_i. \tag{34}$$

b) *Let $N \in \mathbb{Z}^+$ and let $\mathfrak{r}_1, \ldots, \mathfrak{r}_N$ be nonzero rings such that $R \cong \prod_{i=1}^N \mathfrak{r}_i$. Then $N \leqslant n$. Moreover, if each $\mathfrak{r}_i$ is connected, then we have $N = n$ and after reordering the $\mathfrak{r}_i$'s we have for all $1 \leqslant i \leqslant n$ an R-algebra isomorphsim $\mathfrak{r}_i \cong R/I_i$.*

PROOF. a) By Proposition 13.18 there is $n \in \mathbb{Z}^+$ such that $\operatorname{Spec} R = \coprod_{i=1}^n X_i$ with each X_i nonempty connected, and the Boolean algebra $\operatorname{Clopen} \operatorname{Spec} R$ has order 2^n. For $1 \leqslant i \leqslant n$, put $Y_i := \operatorname{Spec} R \backslash X_i = \coprod_{1 \leqslant j \leqslant n,\ j \neq i} X_j \in \operatorname{Clopen} \operatorname{Spec} R$. By Theorem 13.6, for all $1 \leqslant i \leqslant n$ there is an idempotent $e_i \in R$ such that $Y_i = U(e_i)$. We know that $e \mapsto U(e)$ gives an isomorphism of Boolean algebras, so for all $1 \leqslant i \neq j \leqslant n$ we have

$$U(e_1 \cdots e_n) = U(e_1 \wedge \ldots \wedge e_n) = \bigcap_{i=1}^n U(e_i) = \bigcap_{i=1}^n Y_i = \varnothing = U(0),$$

so $e_1 \cdots e_n = 0$. If $x \in \bigcap_{i=1}^n I_i$, then for all $1 \leqslant i \leqslant n$ we have $x = e_i x_i$ for some $x_i \in R$ and thus $e_i x = e_i^2 x_i = e_i x_i = x$. It follows that $x = e_1 \cdots e_n x = 0$, so $\bigcap_{i=1}^n I_i = (0)$. For $1 \leqslant i \neq j \leqslant n$ we have

$$U(e_i \wedge e_j) = U(e_i) \cup U(e_j) = Y_i \cup Y_j = X = U(1),$$

so $e_i \wedge e_j = 1$. Thus

$$1 = e_i \wedge e_j = e_i + e_j - e_i e_j \in I_i + I_j.$$

So we may apply the Chinese Remainder Theorem to get (34). Moreover we have

$$\operatorname{Spec} R/I_i = \operatorname{Spec} R/\langle e_i \rangle = V(e_i) = \operatorname{Spec} R \backslash U(e_i) = \operatorname{Spec} R \backslash Y_i = X_i.$$

Finally, (34) implies that n must be the number of connected components of $\operatorname{Spec} R$.
b) Suppose there are nonzero rings $\mathfrak{r}_1, \ldots, \mathfrak{r}_N$ such that $R \cong \prod_{i=1}^N \mathfrak{r}_i$. Each $\mathfrak{r}_i$ is a quotient of R hence Noetherian, so by part a) is itself a finite product of connected nonzero rings. So if $N > n$ then this would express R as a product of more than n connected nonzero rings, contradicting part a). Let us now assume that each $\mathfrak{r}_i$ is connected. Again, this forces $N = n$. For $1 \leqslant i \leqslant n$ let J_i be the kernel of the natural map $R \to \mathfrak{r}_i$, so we get an R-algebra isomorphism $\mathfrak{r}_i \cong R/J_i$. By Exercise 4.14 we have $J_i + J_j = R$ for all $1 \leqslant i \neq j \leqslant n$. Thus for all $1 \leqslant i \neq j \leqslant n$ we have

$$\bigcup_{i=1}^n \operatorname{Spec} R/J_i = \bigcup_{i=1}^n V(J_i) = V(\bigcap_{i=1}^n J_i) = V(0) = \operatorname{Spec} R$$

and

$$\operatorname{Spec} R/J_i \cap \operatorname{Spec} R/J_j = V(J_i) \cap V(J_j) = V(J_i + J_j) = V(R) = \varnothing.$$

Thus the $V(J_i)$'s are precisely the connected components of $\operatorname{Spec} R$, so after reordering we have $V(J_i) = V(I_i)$ and thus $\operatorname{rad} J_i = \operatorname{rad} I_i$ for all $1 \leqslant i \leqslant n$. Both I_i and J_i are ideals genearted by an idempotent element: this was the construction of I_i, while $J_i = \{(r_1, \ldots, r_{i-1}, 0, r_{i+1}, \ldots, r_n) \mid r_j \in \mathfrak{r}_j\}$ so it is generated by the element of R corresponding to $(1, 1, \ldots, 0, 1, \ldots, 1) \in \prod_{i=1}^n \mathfrak{r}_i$. Since both I_i and J_i are finitely generated, by Proposition 4.17g) this implies that there is $M \in \mathbb{Z}^+$ such that $I_i^M \subset J_i$ and $J_i^M \subset I_i$. It follows that $J_i = I_i$ for all $1 \leqslant i \leqslant n$. □

The above result continues to hold under weaker hypotheses.

EXERCISE 13.20. *Let R be a nonzero ring, and let κ be the number of connected components of* $\operatorname{Spec} R$.

a) *Show that the following are equivalent:*
   (i) *We have* $\kappa < \aleph_0$.
   (ii) *The ring* R *has* $2^\kappa < \aleph_0$ *idempotents.*
   (iii) *The ring* R *is a finite product of connected rings.*

b) *When the equivalent conditions of part a) hold, if* R *is a product of* α *nonzero rings, then* $\alpha \leqslant \kappa$. *If* R *is a product of* β *connected rings, then* $\beta = \kappa$. *Moreover if we have connected rings* $\mathfrak{r}_1, \ldots, \mathfrak{r}_\kappa, \mathfrak{s}_1, \ldots, \mathfrak{s}_\kappa$ *such that*

$$\prod_{i=1}^{\kappa} \mathfrak{r}_i \cong R \cong \prod_{i=1}^{\kappa} \mathfrak{s}_\mathfrak{i},$$

then after permuting the indices we have R*-algebra isomorphisms* $\mathfrak{r}_i \cong \mathfrak{s}_i$ *for all* $1 \leqslant i \leqslant \kappa$.

EXERCISE 13.21. *Let* R_1, R_2, R_3 *be nonzero rings such that* $R_1 \times R_2 \cong R_1 \times R_3$.

a) *Show: if each* R_i *is Noetherian (or indeed is a finite product of connected rings), show that* $R_2 \cong R_3$.

b) *Give an example to show that we need not have* $R_2 \cong R_3$ *in general.*

EXERCISE 13.22. *Let* X *be a Noetherian topological space, and let* $x \in X$.

a) *Show: every irreducible component containing* x *is contained in the connected component of* x. *Deduce: every connected component is a finite union of irreducible components.*

b) *Show: the union of the irreducible components containing* x *may be a proper subset of the connected component of* x.

c) *For two irreducible components of* X, *write* $A_i \sim A_j$ *if* $A_i \cap A_j \neq \varnothing$. *Show:* $\sim$ *need not be transitive. Let* $\approx$ *be the transitive closure of* $\sim$*: explicitly,* $A \approx B$ *if there is a finite chain* $A \sim A_1 \sim \ldots \sim A_n \sim B$. *Show:* $\approx$ *is an equivalence relation on the set of irreducible components of* X *and the unions of the components in any one equivalence class are precisely the connected components of* X.

7. Krull Dimension of Topological Spaces

The Krull dimension $\dim X$ of a topological space is the supremum of lengths of chains of irreducible closed subsets of X. This is a cardinal number. In a ring R we have a bijective correspondence between prime ideals of R and irreducible closed subspaces of $\operatorname{Spec} R$, which gives

$$\dim R = \dim \operatorname{Spec} R.$$

EXAMPLE 13.23. *Let* X *be the topological space with underlying set* $\mathbb{Z}^+$ *and with nonempty open sets*

$$U(n) = \{m \in \mathbb{Z}^+ \mid m \geqslant n\}$$

as n *ranges over all positive integers. Then families of nonempty open sets are indexed by subsets* $A \subset \mathbb{Z}^+$. *If* $A \neq \varnothing$ *then* $\bigcup_{n \in A} U(n) = U(\min A)$. *If* A *is finite, then* $\bigcap_{n \in A} U(n) = U(\max A)$, *whereas if* A *is infinite then* $\bigcap_{n \in A} U(n) = \varnothing$. *Thus* X *is an Alexandroff topological space: the family of open sets is closed under arbitrary unions and intersections.*

Since every nonempty open subset of X *is cofinite,* X *is Noetherian. For* $n \in \mathbb{Z}^+$, *the proper closed sets containing* x *are the intervals* $[1, m] = \{1, \ldots, m\}$ *with*

$n \leqslant m$, so $\overline{n} = [1, n]$. Thus every nonempty closed subset of X is irreducible, and an irreducible closed subset has a generic point if and only if it is proper, and $\dim X = \aleph_0$.

Let $\tilde{X} = X \coprod \{\eta\}$, where η is some point not in X. We define a nonempty subset of $\tilde{X}$ to be open if it is of the form $U(n) \cup \{\eta\}$ for some $n \in \mathbb{Z}^+$. This gives a topology on $\tilde{X}$. Since every nonempty open subset of $\tilde{X}$ contains η, we have $\overline{\eta} = \tilde{X}$. Let $\iota : X \hookrightarrow \tilde{X}$. The map ι^{-1} gives an order-preserving bijection from the open subsets of $\tilde{X}$ to the open substs of X. Thus $\tilde{X}$ is Noetherian and $\dim \tilde{X} = \aleph_0$.

8. Jacobson spaces

Let X be a topological space. We denote by X_0 the subset of closed points of X. We endow X_0 with the subspace topology.

EXERCISE 13.23. *Let X be a topological space.*

a) *Show: if X is finite, then X_0 is closed in X.*
b) *Exhibit a topological space X for which X_0 is not closed in X. (Suggestion: take $X = \operatorname{Spec} R$ for a suitable ring!)*

A subset $Y \subset X$ is **locally closed** if it is the intersection of an open set with a closed subset. A subset $Z \subset X$ is **strongly dense** if $Z \cap Y \neq \varnothing$ for all nonempty locally closed subsets $Y \subset X$. A topological space X is **Jacobson** if X_0 is strongly dense in X.

Notice that X is separated if and only if $X_0 = X$; such spaces are certainly Jacobson. The concept is only interesting when not all points are closed.

LEMMA 13.24. *For a topological space X, the following are equivalent:*

(i) *X_0 is strongly dense in X.*
(ii) *For all closed subsets $Z \subset X$, we have $Z = \overline{Z \cap X_0}$.*
(iii) *For all $x \in X$, we have $\overline{\{x\}} = \overline{\overline{\{x\}} \cap X_0}$.*

*A space satisfying these equivalent properties is called a **Jacobson space**.*

EXERCISE 13.24. *Prove Lemma 13.24*

EXERCISE 13.25.

a) *Let X be at topological space, and let $\{U_i\}_{i \in I}$ be an open cover of X. Show: X is Jacobson if and only if U_i is Jacobson for all i.*
b) *Suppose X is Jacobson and $Y \subset X$ is a union of locally closed subspaces of X. Show: Y is Jacobson.*
c) *Show: a finite Jacobson space is discete.*

EXERCISE 13.26. *For a topological space X, we define the **Jacobson subspace***

$$J(X) = \{x \in X \mid \overline{\{x\}} = \overline{\overline{\{x\}} \cap X_0}\}.$$

a) *Show: X is Jacobson if and only if $J(X) = X$.*
b) *Show: $J(X)$ is a Jacobson space.*

LEMMA 13.25. *Let X be a Jacobson topological space, and let $\iota : X_0 \to X$ be the inclusion map.*

a) *The map $Y \subset X \mapsto \iota^{-1}(Y) = Y \cap X_0$ s a bijection from the closed subspaces of X to the closed subspaces of X_0.*

b) *A closed subset $Y \subset X$ is irreducible if and only if $Y \cap X_0$ is irreducible.*
c) *We have* $\dim X_0 = \dim X$.

PROOF. a) Certainly if $Y \subset X$ is closed in X, then $Y \cap X_0$ is closed in X_0, and by definition of the subspace topology every closed subset of X_0 is of the form $Y \cap X_0$ for some closed $Y \subset X$. Suppose Y_1, Y_2 are closed in X and $Y_1 \cap X_0 = Y_2 \cap X_0$. If $Y_1 \neq Y_2$, then $(Y_1 \backslash Y_2) \cup (Y_2 \backslash Y_1)$ is a nonempty locally closed set, so it meets X_0: contradiction.
b), c) Left to the reader. □

PROPOSITION 13.26. *For a ring R, the following are equivalent:*
(i) *R is a Jacobson ring.*
(ii) Spec R *is a Jacobson space.*

PROOF. Let $\mathfrak{p} \in \operatorname{Spec} R$. Then $\overline{\mathfrak{p}} = \{\mathfrak{q} \in \operatorname{Spec} R \mid \mathfrak{q} \supseteq \mathfrak{p}\}$ and

$$\overline{\{\mathfrak{p}\}} \cap \operatorname{MaxSpec} R = \bigcap_{\mathfrak{m} \in \operatorname{MaxSpec} R,\ \mathfrak{m} \supseteq \mathfrak{p}} \mathfrak{m},$$

so the equivalence follows from Lemma 13.25. □

For a ring R, we define the **Jacobson spectrum** $\operatorname{JSpec} R$ to be the set of all prime ideals which are intersections of maximal ideals.[4] Thus $\operatorname{MaxSpec} R \subset \operatorname{JSpec} R \subset \operatorname{Spec} R$, and $\operatorname{JSpec} R = \operatorname{Spec} R$ if and only if R is Jacobson. We endow $\operatorname{JSpec} R$ with the topology it receives as a subspace of $\operatorname{Spec} R$. Since $\operatorname{JSpec} R$ consists precisely of the prime ideals of R which lie in the closure of the set of maximal ideals containing them, we have that

$$\operatorname{JSpec} R = J(\operatorname{Spec} R),$$

i.e., $\operatorname{JSpec} R$ is the Jacobson subspace of $\operatorname{Spec} R$. In particular, $\operatorname{JSpec} R$ is a Jacobson space.

A topological space X is **sober** if for every irreducible closed subspace Y of X, there exists a unique point $y \in Y$ such that $Y = \overline{\{y\}}$. Equivalently, a sober space is one for which every irreducible closed subset has a unique generic point.

EXERCISE 13.27.
a) *Show that a Hausdorff space is sober.*
b) *Show that a sobser space is Kolmogorov.*
c) *Show that the cofinite topology on an infinite set is separated but not sober.*

A map $f : (X, \tau_X) \to (Y, \tau_Y)$ of topological spaces is a **quasi-homeomorphism** if it is continuous and $f^{-1} : V \in \tau_Y \mapsto f^{-1}(V) \in \tau_X$ is a bijection.

EXERCISE 13.28. *(Sobrification) For a topological space X, let X^+ denote the set of irreducible closed subspaces of X. If $Y \subset X$ is closed, then $Y^+ \subset X^+$. Consider the family $\mathcal{C} = \{Y^+ \mid Y \subset X \text{ is closed }\}$ of subsets of X^+.*
a) *Show: $\mathcal{C}$ contains $\varnothing$ and X^+ and is closed under finite unions and arbitrary intersections, thus forms the closed sets for a unique topology on X^+.*

[4]The Jacobson spectrum was introduced by R.G. Swan [**Sw67**].

b) *Define a map $j : X \to X^+$ by $j : x \mapsto \overline{\{x\}}$. Show: if $Y \subset X$ is closed, then $j^{-1}(Y^+) = Y$. Deduce: $V \mapsto V^+$ is a bijection from the family of closed subsets of X to the family of closed subsets of X^+, with inverse bijection $V^+ \mapsto f^{-1}(V^+) = V$. In particular, j is quasi-homeomorphism.*

c) *Show: X has the initial topology coming from the map $j : X \to X^+$, i.e., the coarsest topology that makes j continuous.*

d) *Show: if $V \subset X$ is closed, then V is irreducible if and only if V^+ is irreducible, so $V \mapsto V^+$ gives a bijection from the closed irreducible subsets of X to the closed irreducible subsets of X^+. Deduce: X^+ is sober.*

e) *Show: the map $j : X \to X^+$ is the universal continuous function from X into a sober topological space: if $f : X \to Y$ is continuous and Y is sober, then there is a unique $F : X^+ \to Y$ such that $f = F \circ j$. We say that $j : X \to X^+$ (and, by a standard abuse of terminology, X^+ itself) is the* ***sobrification*** *of X.*

f) *Show: j is injective if and only if X is Kolmogorov and j is surjective if and only if every irreducible closed subset of X has a generic point (****quasi-sober****).*

g) *Show: the following are equivalent:*
   (i) *X is sober.*
   (ii) *j is a homeomorphism.*
   (iii) *j is bijection.*
   (iv) *j is a closed injection.*

PROPOSITION 13.27. *Let $f : X \to Y$ be a quasi-homeomorphism.*

a) *If X is Kolmogorov, then f is injective.*

b) *If X is sober and Y is Kolmogorov, then f is a homeomorphism.*

PROOF. a) Seeking a contradiction, we suppose there are $x_1 \neq x_2$ in X such that $f(x_1) = f(x_2)$. After interchanging x_1 and x_2 if necessary, we may assume there is an open subset $U \subset X$ containing x_1 and not x_2. Let $V \subset Y$ be open such that $q^{-1}(V) = U$. Then $q(x_1) \in V$ and $q(x_2) \notin V$: contradiction.
b) It suffices to show f is bijective, since a bijective quasi-homeomorphism is a homeomorphism. By part a), f is injective. Let $y \in Y$. Then $f^{-1}(\overline{\{y\}})$ is irreducible and closed in the sober space X, so it has a generic point x. Thus

$$\overline{\{x\}} \subset f^{-1}(\overline{\{f(x)\}}) \subset f^{-1}(\overline{\{y\}}) = \overline{\{x\}},$$

so $f^{-1}(\overline{\{f(x)\}}) = f^{-1}(\overline{\{y\}})$. Since f is quasi-homeomorphism, we have $\overline{\{f(x)\}} = \overline{\{y\}}$, and since Y is Kolmogorov we conclude $f(x) = y$. □

COROLLARY 13.28. *If $f : X \to Y$ is a quasi-homeomorphism and Y is sober, then f is the sobrification of X.*

PROOF. The universal property of the sobrification $j : X \to X^+$ gives us a factorization $f = F \circ j$ for a continuous map $F : X^+ \to Y$. We have $f^{-1} = j^{-1} \circ F^{-1}$. Since f^{-1} and j^{-1} are each bijections between lattices of open sets, so is F^{-1}. Thus F is a quasi-homeomorphism of sober spaces, hence a homeomorphism. □

EXAMPLE 13.29. *Let X be a topological space which is Kolmogorov but not sober: e.g. take X to be an inifnite endowed with the cofinite topology. Let $j : X \to X^+$ be the sobrification, so j is a quasi-homeomorphism. There is no quasi-homeomorphism $f : X^+ \to X$: indeed, the previous result implies that f would have*

to be a homeomorphism and thus X would be sober, contradiction.

So beware: as a relation, quasi-homeomorphism is not symmetric, hence not an equivalence relation. However, if $\equiv$ is the equivalence relation on topological spaces generated by quasi-homeomorphism, then it is easy to see that $X \equiv Y$ if and only if X^+ and Y^+ are homeomorphic.

We come now to the following result, which is the main payoff of the material of this section and will be used in our treatment of the Forster-Swan Theorem.

THEOREM 13.30. *For any ring R, the inclusion map $\iota : \operatorname{MaxSpec} R \hookrightarrow \operatorname{JSpec} R$ is the sobrification of* $\operatorname{MaxSpec} R$.

PROOF. We leave it to the reader to check that the argument that shows $\operatorname{Spec} R$ is sober carries over to show the sobriety of $\operatorname{JSpec} R$. By the above corollay it is enough to show that ι is a quasi-homeomorphism. Since ι is an inclusion map, certainly ι^{-1} is surjective on closed sets, so it's enough to see injectivity. If Z is a closed subset of $\operatorname{JSpec} R$, then since $\operatorname{JSpec} R$ is Jacobson, we have $Z = \overline{Z \cap \operatorname{MaxSpec} R} = \overline{\iota^{-1}(Z)}$, giving the injectivity. □

COROLLARY 13.31. *Let R be a ring.*

a) *The following conditions are equivalent:*
   (i) *The space* $\operatorname{MaxSpec} R$ *is Noetherian.*
   (ii) *The space* $\operatorname{JSpec} R$ *is Noetherian.*
   (iii) *The ascending chain condition holds on intersections of maximal ideals in R.*

b) *If* $\operatorname{Spec} R$ *is Noetherian, then the conditions of part a) hold.*

c) *The supremum of lengths of chains in* $\operatorname{JSpec} R$ *is the Krull dimension of both* $\operatorname{JSpec} R$ *and of* $\operatorname{MaxSpec} R$.

d) *We have* $\dim \operatorname{MaxSpec} R \leqslant \dim \operatorname{Spec} R$.

EXERCISE 13.29. *Prove Corollary 13.31.*

9. Hochster's Theorem

A topological space X is **spectral** if:
(SS1) X is quasi-compact,
(SS2) X is sober, and
(SS3) The family of quasi-compact open subsets of X is closed under finite intersections and is a base for the topology.

EXERCISE 13.30. *Show: a finite topological space is spectral if and only if it iis Kolmogorov (or T_0).*

The following result gives an arguably cleaner characterization of spectral spaces.

PROPOSITION 13.32. *For a topological space X, the following are equivalent:*

(i) *The space X is homeomorphic to an inverse limit of finite T_0 spaces.*
(ii) *The space X is spectral.*

EXERCISE 13.31. *Prove Proposition 13.16.*

PROPOSITION 13.33. *For every ring R, the space* $\operatorname{Spec} R$ *is spectral.*

EXERCISE 13.32. *Prove Proposition 13.33.*
(Hint: you will find the needed results in the previous subsections. Especially, use Proposition 13.15 to prove sobriety.)

For any ring R we endow the set $\mathrm{MaxSpec}(R)$ of maximal ideals of R with the topology it inherits as a subset of $\mathrm{Spec}(R)$. When necessary, we describe $\mathrm{MaxSpec}\, R$ as the "maximal spectrum" of R.

PROPOSITION 13.34. *For any ring R, the space $\mathrm{MaxSpec}\, R$ is separated and quasi-compact.*

EXERCISE 13.33. *Prove Proposition 13.34.*

THEOREM 13.35. *(Hochster's Thesis* [**Ho69**]*) Let X be a topological space.*

a) *The following are equivalent:*
   (i) *The space X is homeomorphic to $\mathrm{Spec}\, R$ for some ring R.*
   (ii) *The space X is spectral.*

b) *The following are equivalent:*
   (i) *The space is homeomorphic to $\mathrm{MaxSpec}\, R$ for some ring R.*
   (ii) *The space X is quasi-compact and separated.*

We do not aspire to give a proof of Theorem 13.35 at this time.

EXERCISE 13.34.

a) *Show: the specialization relation gives an equivalence of categories between the category of T_0 finite spaces and the category of finite partially ordered sets.*

b) *Formulate a generalization of part a) in which T_0 finite spaces are replaced by T_0 **Alexandroff spaces**. (A topological space is Alexandroff if an arbitrary intersection of closed subsets is closed.)*

EXERCISE 13.35. *Let $n \in \mathbb{Z}^+$.*

a) *Use Hochster's Thesis and the previous exercise to show: there exists a ring R with exactly n prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ such that $\mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \ldots \subset \mathfrak{p}_n$.*

b) *For $n = 1, 2$, exhibit Noetherian rings with these properties. For $n \geq 3$, show: there is no such Noetherian ring.*

10. Rank functions revisited

THEOREM 13.36. *Let M be a finitely generated module over a ring R.*

a) *For each $n \in \mathbb{N}$, the set*

$$U_r = \{\mathfrak{p} \in \mathrm{Spec}\, R \mid M_{\mathfrak{p}} \text{ can be generated over } R_{\mathfrak{p}} \text{ by at most } r \text{ elements}\}$$

is open in $\mathrm{Spec}\, R$.

b) *If M is finitely presented (e.g. if R is Noetherian), then the set*

$$U_F = \{\mathfrak{p} \in \mathrm{Spec}\, R \mid M_{\mathfrak{p}} \text{ is a free } R_{\mathfrak{p}}\text{-module}\}$$

is open in $\mathrm{Spec}\, R$.

PROOF. (Matsumura) Suppose $M_{\mathfrak{p}} = \langle \omega_1, \ldots, \omega_r \rangle_{R_{\mathfrak{p}}}$. Each ω_i is of the form $\frac{m_i}{s_i}$ with $m_i \in M$ and $s_i \in R \backslash \mathfrak{p}$. But since $s_i \in R_{\mathfrak{p}}^{\times}$ for all i, we also have $\langle m_1, \ldots, m_r \rangle_{R_{\mathfrak{p}}} = M_{\mathfrak{p}}$. Thus it is no loss of generality to assume that each ω_i

is the image in $M_{\mathfrak{p}}$ of an element of M. Let $\varphi : R^r \to M$ be the R-linear map given by $(a_1, \ldots, a_r) \mapsto \sum_i a_i \omega_i$, and put $C = \operatorname{coker} \varphi$, whence an exact sequence

$$R^r \to M \to C \to 0.$$

Localizing this at a prime $\mathfrak{q}$ of R gives an exact sequence

$$R_{\mathfrak{q}}^r \to M_{\mathfrak{q}} \to C_{\mathfrak{q}} \to 0.$$

When $\mathfrak{q} = \mathfrak{p}$ we of course have $C_{\mathfrak{q}} = 0$. Moreover, C is a quotient of M hence a finitely generated R-module, so by Proposition 10.11 its support $\operatorname{supp} C$ is a Zariski-closed set. It follows that there exists an open neighborhood V of $\mathfrak{p}$ such that $C_{\mathfrak{q}} = 0$ for all $\mathfrak{q} \in V$.

b) Suppose that $M_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$-module with basis $\omega_1, \ldots, \omega_r$. As above it is no loss of generality to assume that each ω_i is the image in $M_{\mathfrak{p}}$ of an element of M. Moreover, as we have also just seen, there exists a basic open neighborhood $U(f)$ such that for all $\mathfrak{q} \in U(f)$, the images of $\omega_1, \ldots, \omega_r$ in $M_{\mathfrak{q}}$ generate $M_{\mathfrak{q}}$ as an $R_{\mathfrak{q}}$-module. Replacing R by R_f and M by M_f we may assume that this occurs for all $\mathfrak{q} \in \operatorname{Spec} R$. Thus $M/\langle \omega_1, \ldots, \omega_r \rangle_R$ is everywhere locally zero, so it is locally zero: $M = \langle \omega_1, \ldots, \omega_r \rangle$. Defining an R-linear map $\varphi : R^r \to M$ as above and setting $K = \operatorname{Ker} \varphi$, we have the exact sequence

$$0 \to K \to R^r \to M \to 0.$$

Since M is finitely *presented*, according to Proposition 3.6 K is a finitely generated R-module. Moreover we have $K_{\mathfrak{p}} = 0$ hence as above $K_{\mathfrak{q}} = 0$ for all $\mathfrak{q}$ on some open neighborhood V of $\mathfrak{p}$. By construction, for each $\mathfrak{q} \in V$, the images of $\omega_1, \ldots, \omega_r$ in $M_{\mathfrak{q}}$ give an $R_{\mathfrak{q}}$-basis for $M_{\mathfrak{q}}$. □

Let M be a finitely generated, locally free module over a ring R. Earlier we defined the rank function $r : \operatorname{Spec} R \to \mathbb{N}$. Applying Theorem 13.36a) to the locally free module M says that the rank function is *upper semicontinuous*: it can jump up upon specialization, but not jump down.

We now ask the reader to look back at Theorem 7.30 and see that for a finitely generated module M over a general ring R, M is projective if and only if it is locally free and finitely presented. When R is Noetherian, being finitely presented is equivalent to being finitely generated, so being projective is the same as being locally free. We have had little to say about the distinction between finitely generated and finitely presented modules. Is there some way to rephrase the subtly stronger property of finite presentation, perhaps a more geometric way?

Indeed there is:

THEOREM 13.37. *Let M be a finitely generated locally free R-module. the following are equivalent:*

(i) *The rank function $r_M : \operatorname{Spec} R \to \mathbb{N}$ is locally constant.*
(ii) *M is a projective module.*

PROOF. (i) $\implies$ (ii): By Theorem 7.30, it is enough to show that for all $\mathfrak{m} \in \operatorname{MaxSpec} R$, there is $f \in R \backslash \mathfrak{m}$ such that M_f is a free module. Let $n = r(\mathfrak{m})$, and let $x_1, \ldots, x_n$ be an $R_{\mathfrak{m}}$-basis for $M_{\mathfrak{m}}$. Choose $X_1, \ldots, X_n \in M$ such that for all i, the image of X_i in $M_{\mathfrak{m}}$ is of the form $u_i x_i$ for $u_u \in R_{\mathfrak{m}}^{\times}$. Let $u : R^n \to M$ be the map sending the ith standard basis element e_i to X_i. Since M is finitely generated,

by Proposition 7.28 there is $f \in R\backslash\mathfrak{m}$ such that $u_f : R_f^n \to M_f$ is surjective. It follows that for all $g \in R\backslash\mathfrak{m}$, u_{fg} is surjective. Moreover, by hypothesis there is some such g such that $r(\mathfrak{p}) = n$ for all $\mathfrak{p} \in X(g)$. Replacing f by fg we may assume that $r(\mathfrak{p}) = n$ for all $\mathfrak{p} \in X(f)$. For all such $\mathfrak{p}$, $u_{\mathfrak{p}} : R_{\mathfrak{p}}^n \to M_{\mathfrak{p}}$ is therefore a surjective endomorphism from a rank n free module to itself. Since finitely generated modules are Hopfian, $u_{\mathfrak{p}}$ is an isomorphism. By the local nature of isomorphisms (Proposition 7.15) we conclude u_f is an isomorphism, so M_f is free.
(ii) $\implies$ (i): By Theorem 7.30, M is Z-locally free: there exists a finite Z-family $\{f_i\}_{i\in I}$ such that for all $i \in I$, M_{f_i} is finitely generated and free. Thus the module $\prod_{i=1}^n M_{f_i}$ is finitely generated and projective over the faithfully flat R-algebra $\prod_{i=1}^n R_{f_i}$, so by faithfully flat descent (Theorem 3.114) M itself is projective. □

Corollary 13.38. *Let R be a ring with* $\operatorname{Spec} R$ *irreducible (e.g. a domain). For a finitely generated R-module M, the following are equivalent:*

(i) *The module M is projective.*
(ii) *The module M is Z-locally free.*
(iii) *The module M is locally free.*

Exercise 13.36. *Prove Corollary 13.24.*

11. The Forster-Swan Theorem

For a prime ideal $\mathfrak{p}$ of a ring R, put $k(\mathfrak{p}) = R_{\mathfrak{p}}/\mathfrak{p}R_{\mathfrak{p}}$. For a fnitely generated R-module M, we let $\mu(M)$ denote the minimal cardinality of a set of R-module generators for M. Recall that if $(R, \mathfrak{m})$ is local, then by Nakayama's Lemma we have

$$\mu(M) = \dim_{R/\mathfrak{m}} M/\mathfrak{m}M.$$

For $\mathfrak{p} \in \operatorname{Spec} R$ let $\mu_{\mathfrak{p}}(M)$ be the minimal cardinality of a set of generators for the $R_{\mathfrak{p}}$-module $M_{\mathfrak{p}}$.

Lemma 13.39. *Let M be a finitely generated R-module, and let S be a finite subset of* $\operatorname{supp} M$. *Then there is $m \in M$ such that for all $\mathfrak{p} \in S$, the image of M in $M_{\mathfrak{p}}/\mathfrak{p}M_{\mathfrak{p}}$ is nonzero, and thus*

$$\forall \mathfrak{p} \in S,\ \mu_{\mathfrak{p}}(M/\langle m\rangle) = \mu_{\mathfrak{p}}(M) - 1.$$

Proof. We go by induction on the number of elements s of S. The base case $s = 0$ is clear, so let $s \geqslant 1$ and suppose the statement holds when $\#S = s - 1$. We may order the elements of S as $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ so as to have $\mathfrak{p}_1 \cdots \mathfrak{p}_{s-1} \not\subset \mathfrak{p}_s$; choose $x_s \in \mathfrak{p}_1 \cdots \mathfrak{p}_{s-1}\backslash\mathfrak{p}_s$. By induction, there is $m_1 \in M$ such that for all $1 \leqslant i \leqslant s-1$, the image of m_1 in $M_{\mathfrak{p}_i}/\mathfrak{p}_i M_{\mathfrak{p}_i}$ is nonzero. We are done if the image of m_1 in $M_{\mathfrak{p}_s}/\mathfrak{p}_s M_{\mathfrak{p}_s}$ is nonzero, so assume otherwise. Let $m_2 \in M$ have nonzero image in $M_{\mathfrak{p}_s}/\mathfrak{p}_s M_{\mathfrak{p}_s}$. Then $m_1 + x_s m_2$ has nonzero image in $M_{\mathfrak{p}_i}/\mathfrak{p}_i M_{\mathfrak{p}_i}$ for all $1 \leqslant i \leqslant s$. □

Theorem 13.40. *(Forster-Swan* [**Fo64**], [**Sw67**]*) Let R be a ring such that the space* $\operatorname{MaxSpec} R$ *is Noetherian, and let M be a finitely generated R-module. Then*

$$\mu(M) \leqslant \sup_{\mathfrak{p}\in \operatorname{JSpec} R} \left(\mu_{\mathfrak{p}}(M) + \dim \operatorname{JSpec} R/\mathfrak{p}\right). \tag{35}$$

PROOF. We follow an exposition of Swan's proof due to C.-L. Chai.

We may assume that $\sup_{\mathfrak{p} \in \operatorname{JSpec} R} \dim \operatorname{JSpec} R/\mathfrak{p} < \aleph_0$, for otherwise the conclusion is trivial. Since $\mu_{\mathfrak{p}}(M) \leqslant \mu(M)$ for all $\mathfrak{p} \in \operatorname{Spec} R$, we have

$$\mu_{\mathrm{FS}}(M) := \sup_{\mathfrak{p} \in \operatorname{JSpec} R} (\mu_{\mathfrak{p}}(M) + \dim \operatorname{JSpec} R/\mathfrak{p}) < \aleph_0.$$

We go by induction on μ_{FS}. If $\mu_{FS}(M) = 0$ then $\mu_{\mathfrak{m}}(M) = 0$ for all $\mathfrak{m} \in \operatorname{MaxSpec} R$, so $M = 0$ and thus $\mu(M) = 0$.

Induction Step: Suppose $\mu_{\mathrm{FS}}(M) \geqslant 1$ and suppose the result holds for finitely generated modules R-modules N with $\mu_{\mathrm{FS}}(N) < \mu_{\mathrm{FS}}(M)$. Let

$$S = \{\mathfrak{p} \in \operatorname{JSpec} R \mid \mu_{\mathfrak{p}}(M) + \dim \operatorname{JSpec} R/\mathfrak{p} = \mu_{\mathrm{FS}}(M)\}.$$

For $n \in \mathbb{N}$, put

$$X_n(M) = \{\mathfrak{p} \in \operatorname{JSpec} R \mid \mu_{\mathfrak{p}}(M) \geqslant n\}.$$

Theorem 13.21 implies that $X_n(M)$ is closed in $\operatorname{JSpec} R$. For $\mathfrak{q} \in S$, put $n = \mu_{\mathfrak{q}}(M)$ and $Z = \overline{\{\mathfrak{q}\}}$, so $Z \subset X_n(M)$. We claim that Z is an irreducible component of $X_n(M)$: if not, there is $\mathfrak{p} \in X_n(M)$ such that $\mathfrak{p} \subsetneq \mathfrak{q}$ and

$$\mu_{\mathfrak{p}}(M) + \dim \operatorname{JSpec} R/\mathfrak{p} > \mu_{\mathfrak{q}}(M) + \dim \operatorname{JSpec} R/\mathfrak{q} = \mu_{\mathrm{FS}}(M),$$

contradiction. Because $\operatorname{MaxSpec} R$ is Noetherian, so is $\operatorname{JSpec} R$ and thus also $X_n(M)$. It follows ($\operatorname{JSpec} R$ is sober, hence Kolmogorov) that S is finite. By Lemma 13.39, there is $m \in M$ such that $\mu_q(M/\langle m \rangle) = \mu_q(M) - 1$ for all $\mathfrak{q} \in S$. Thus for all $\mathfrak{p} \in \operatorname{JSpec} R$ we have

$$\mu_{\mathrm{FS}}(M/\langle m \rangle) \leqslant k - 1,$$

so $\mu(M/\langle m \rangle) \leqslant k - 1$ by induction. It follows that $\mu(M) \leqslant k$. □

COROLLARY 13.41. *Let M be a finitely generated module over a semilocal ring.*

a) *We have $\mu(M) = \sup_{\mathfrak{m} \in \operatorname{MaxSpec} R} \mu_{\mathfrak{m}}(M)$.*
b) *If M is projective, then M is free if and only if the rank function r_M is constant.*

PROOF. a) Since $\operatorname{MaxSpec} R$ is finite and separated, it is Noetherian and discrete. So $\dim \operatorname{JSpec} R = 0$ and $\operatorname{JSpec} R = \operatorname{MaxSpec} R$. Apply Forster-Swan.

b) Free modules have constant rank. Conversely, suppose $r_M(\mathfrak{m}) = n$ for all $\mathfrak{m} \in \operatorname{MaxSpec} R$. By part a), $\mu(M) = n$, so M is free by Proposition 7.20. □

CHAPTER 14

Integral Extensions

1. First properties of integral extensions

If S is a ring extension of R – i.e., $R \subset S$ – we will say that an element α of S is **integral** over R if there exist $a_0, \ldots, a_{n-1} \in R$ such that

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0.$$

Note that every element $\alpha \in R$ satisfies the monic polynomial $t - \alpha = 0$, so is integral over R.

THEOREM 14.1. *Let $R \subset T$ be an inclusion of rings, and $\alpha \in T$. The following are equivalent:*

(i) *The element α is integral over R.*
(ii) *$R[\alpha]$ is finitely generated as an R-module.*
(iii) *There is an intermediate ring $R \subset S \subset T$ such that $\alpha \in S$ and S is finitely generated as an R-module.*
(iv) *There is a faithful $R[\alpha]$-submodule M of T that is finitely generated as an R-module.*

PROOF. (i) $\implies$ (ii): If α is integral over R, there are $a_0, \ldots, a_{n-1} \in R$ such that

$$\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0,$$

or equivalently

$$\alpha^n = -a_{n-1}\alpha^{n-1} - \ldots - a_1\alpha - a_0.$$

This relation allows us to rewrite any element of $R[\alpha]$ as a polynomial of degree at most $n-1$, so that $1, \alpha, \ldots, \alpha^{n-1}$ generates $R[\alpha]$ as an R-module.
(ii) $\implies$ (iii): Take $S := R[\alpha]$.
(iii) $\implies$ (iv): Take $M := S$.
(iv) $\implies$ (i): Let $m_1, \ldots, m_n$ be a finite set of generators for M over R, and express each of the elements $m_i\alpha$ in terms of these generators:

$$\alpha m_i = \sum_{j=1}^{n} r_{ij} m_j, \ r_{ij} \in R.$$

Let A be the $n \times n$ matrix $\alpha I_n - (r_{ij})$; then recall from linear algebra that

$$AA^* = \det(A) \cdot I_n,$$

where A^* is the "adjugate" matrix (of cofactors). If $m = (m_1, \ldots, m_n)$ (the row vector), then the above equation implies $0 = mA = mAA^* = m\det(A) \cdot I_n$. The latter matrix equation amounts to $m_i \det(A) = 0$ for all i. Thus $\bullet \det(A) = \bullet 0$ on M, and by faithfulness this means $\det(A) = 0$. Since so that α is a root of the monic polynomial $\det(T \cdot I_n - (a_{ij}))$. □

EXERCISE 14.1. *Let S be a finitely generated R-algebra. Show that the following are equivalent:*

(i) *S/R is integral.*
(ii) *S is a finitely generated R-module.*

Deduce: if S/R is an extension and $\alpha_1, \ldots, \alpha_n$ are all integral over R, then $R[\alpha_1, \ldots, \alpha_n]$ is a finitely generated R-module.

PROPOSITION 14.2. *(Integrality is preserved under quotients and localizations) Let S/R be an integral ring extension.*

a) *Let J be an ideal of S. Then S/J is an integral extension of $R/(J \cap R)$.*
b) *Let T be a multiplicatively closed subset of nonzero elements of R. Then S_T is an integral extension of R_T.*

PROOF. a) First note that the kernel of the composite map $R \hookrightarrow S \to S/J$ is $J \cap R$, so that $R/(J \cap R) \hookrightarrow S/J$ is indeed a ring extension. Any element of S/J is of the form $x + J$ for $x \in S$, and if $P(t)t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 = 0 \in R[t]$ is a polynomial satisfied by x, then reducing coefficientwise gives a monic polynomial $\overline{P}(t) \in R/(J \cap R)$ satisfied by x.

b) Let $J = \{s \in S \mid \exists t \in T \mid ts = 0\}$, an ideal of S. Let $\overline{T}$ be the image of T in $R/(J \cap R)$. Then $S_T \cong (S/J)_{\overline{T}}$ and $J_T \cong (R/(J \cap R))_{\overline{T}}$, so we may assume that the maps $R \to R_T$ and $S \to S_T$ are injective. Let $\frac{x}{y} \in S_T$ with $x \in S,\ y \in T$. Let $P(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0 \in R[t]$ be a monic polynomial satisfied by x. Then

$$\left(\frac{x}{y}\right)^n + \frac{a_{n-1}}{y}\left(\frac{x}{y}\right)^{n-1} + \ldots + \frac{a_0}{y^n} = 0,$$

showing that $\frac{x}{y}$ is integral over R_T. □

LEMMA 14.3. *Let $R \subset S \subset T$ be an inclusion of rings. If $\alpha \in T$ is integral over R, then it is also integral over S.*

PROOF. If α is integral over R, there exists a monic polynomial $P \in R[t]$ such that $P(\alpha) = 0$. But P is also a monic polynomial in $S[t]$ such that $P(\alpha) = 0$, so α is also integral over S. □

LEMMA 14.4. *Let $R \subset S \subset T$ be rings. If S is a finitely generated R-module and T is a finitely generated S-module, then T is a finitely generated R-module.*

PROOF. If $\alpha_1, \ldots, \alpha_r$ generates S as an R-module and $\beta_1, \ldots, \beta_s$ generates T as an S-module, $\{\alpha_i\beta_j\}_{1 \leqslant i \leqslant r, 1 \leqslant j \leqslant s}$ generates T as an R-module: for $\alpha \in T$,

$$\alpha = \sum_j b_j\beta_j = \sum_i \sum_j (a_{ij}\alpha_i)\beta_j,$$

with $b_j \in S$ and $a_{ij} \in R$. □

COROLLARY 14.5. *(Transitivity of integrality) If $R \subset S \subset T$ are ring extensions such that S/R and T/S are both integral, then T/R is integral.*

PROOF. For $\alpha \in T$, let $\alpha^n + b_{n-1}\alpha^{n-1} + \ldots + b_1\alpha + b_0 = 0$ be an integral dependence relation, with $b_i \in S$. Thus $R[b_1, \ldots, b_{n-1}, \alpha]$ is finitely generated over $R[b_1, \ldots, b_{n-1}]$. Since S/R is integral, $R[b_1, \ldots, b_{n-1}]$ is finite over R. By Lemma 14.4, $R[b_1, \ldots, b_{n-1}, \alpha]$ is a subring of T containing α and finitely generated over R, so by Theorem 14.1, α is integral over R. □

COROLLARY 14.6. *If S/R is a ring extension, then the set $I_S(R)$ of elements of S which are integral over R is a subring of S, the **integral closure of** R **in** S. Thus $R \subset I_S(R) \subset S$.*

PROOF. If $\alpha \in S$ is integral over R, $R[\alpha_1]$ is a finitely generated R-module. If α_2 is integral over R it is also integral over $R[\alpha_1]$, so that $R[\alpha_1][\alpha_2]$ is finitely generated as an $R[\alpha_1]$-module. By Lemmma 14.4, this implies that $R[\alpha_1,\ \alpha_2]$ is a finitely generated R-module containing $\alpha_1 \pm \alpha_2$ and $\alpha_1 \cdot \alpha_2$. By Theorem 14.1, this implies that $\alpha_1 \pm \alpha_2$ and $\alpha_1\alpha_2$ are integral over R. □

If $R \subset S$ such that $I_S(R) = R$, we say R is **integrally closed** in S.

PROPOSITION 14.7. *Let S be a ring. The operator $R \mapsto I_S(R)$ on subrings of R is a closure operator in the abstract sense, namely it satisfies:*
(CL1) $R \subset I_S(R)$,
(CL2) $R_1 \subset R_2 \implies I_S(R_1) \subset I_S(R_2)$.
(CL3) $I_S(I_S(R)) = I_S(R)$.

PROOF. (CL1) is the (trivial) Remark 1.1. (CL2) is obvious: evidently if $R_1 \subset R_2$, then every element of S which satisfies a monic polynomial with R_1-coefficients also satisfies a monic polynomial with R_2-coefficients. Finally, suppose that $\alpha \in S$ is such that $\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1\alpha + a_0 = 0$ for $a_i \in I_S(R)$. Then each a_i is integral over R, so $R[a_1, \ldots, a_n]$ is finitely generated as an R-module, and since $R[a_1, \ldots, a_n, \alpha]$ is finitely generated as an $R[a_1, \ldots, a_n]$-module, applying Lemma 14.4 again, we deduce that α lies in the finitely generated R-module $R[a_1, \ldots, a_n, \alpha]$ and hence by Theorem 14.1 is integral over R. □

2. Integral closure of domains

Until further notice we restrict to the case in which $R \subset S$ are **domains**.

PROPOSITION 14.8. *Let $R \subset S$ be an integral extension of domains.*

a) *R is a field if and only if S is a field.*
b) *An extension of fields is integral if and only if it is algebraic.*

PROOF. a) Suppose first that R is a field, and let $0 \neq \alpha \in S$. Since α is integral over R, $R[\alpha]$ is finitely generated as an R-module, and it is well-known in field theory that this implies $R[\alpha] = R(\alpha)$. Indeed, taking the polynomial of least degree satisfied by α, say $\alpha(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \ldots + a_1) = -a_0$, then $0 \neq a_0 \in R$ is invertible, so

$$\frac{-(\alpha^{n-1} + a_{n-1}\alpha^{n-2} + \ldots + a_1)}{a_0} = \frac{1}{\alpha},$$

and S is a field. Conversely, if S is a field and $a \in R$, then $R[a^{-1}]$ is finite-dimensional over R, i.e., there exist $a_i \in R$ such that

$$a^{-n} = a_{n-1}a^{-n+1} + \ldots + a_1a^{-1} + a_0.$$

Multiplying through by a^{n-1} gives

$$a^{-1} = a_{n-1} + a_{n-2}a + \ldots + a_1a^{n-2} + a_0a^{n-1} \in R,$$

completing the proof of part a). Over a field every polynomial relation can be rescaled to give a monic polynomial relation, whence part b). □

Remark: A more sophisticated way of expressing Proposition 14.8 is that if S/R is an integral extension of domains, then $\dim R = 0$ if and only if $\dim S = 0$. Later we will see that in fact $\dim R = \dim S$ under the same hypotheses.

If $R \subset S$ are fields, $I_S(R)$ is called the **algebraic closure** of R in S.

EXERCISE 14.2.

a) *Let L/K be a field extension. Show: if L is algebraically closed, so is $I_L(K)$.*
b) *Deduce: if $K = \mathbb{Q}$ and $L = \mathbb{C}$, then $I_{\mathbb{C}}(\mathbb{Q})$ is an algebraically closed field extension of $\mathbb{Q}$. This field is denoted $\overline{\mathbb{Q}}$ and called the field of algebraic numbers.*

THEOREM 14.9. *Let S/R be an extension of domains, and let $T \subset R$ be a multiplicatively closed subset. Then $I_{T^{-1}S}(T^{-1}R) = T^{-1}I_S(R)$. In other words, localization commutes with integral closure.*

PROOF. Let K be the fraction field of R and L the fraction field of S. Then $T^{-1}I_S(R)$ is the subring of L generated by T^{-1} and the elements of S which are integral over R. Since both of these kinds of elements of $T-1S$ are integral over $T^{-1}R$ and integral elements form a subring, we must have $T^{-1}I_S(R) \subset I_{T^{-1}S}(T^{-1}R)$. Conversely, let $x \in T^{-1}S$ be integral over $T^{-1}(R)$, so there are $b_0, \ldots, b_{n-1} \in T^{-1}(R)$ such that

$$x^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0 = 0.$$

We may take a common denominator $t \in T$ such that $x = \frac{s}{t}$ and for all $0 \leqslant i \leqslant n-1$, $b_i = \frac{a_i}{t}$. Making this substitution and multiplying through by t^n, we get

$$s^n + a_{n-1}s^{n-1} + ta_{n-2}s^{n-2} + \ldots + t^{n-2}a_1s + t^{n-1} = 0.$$

Thus s is integral over R and $x = \frac{s}{t} \in T^{-1}I_S(R)$. □

PROPOSITION 14.10. *Let R be a domain with fraction field K, let L/K be a field extension, and let S be the integral closure of R in L. Then the fraction field of S is $I_L(K)$.*

PROOF. We write M for the fraction field of S.
Step 1: Every element of S is an element of L that is integral over R, hence also integral over K, so $S \subseteq I_L(K)$. Proposition 14.8 gives that $I_L(K)$ is a field, so also the fraction field M of S is contained in $I_L(K)$.
Step 2: Let $x \in I_L(K)$, so there are $a_0, \ldots, a_{n-1} \in K$ such that

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0.$$

Each a_i may be written as quotient of two elements of R; multiplying by the product of the denominators of these elements and relabelling, there are $b_0, \ldots, b_n \in R$ with $b_n \neq 0$ such that

$$b_nx^n + \ldots + b_1x + b_0 = 0.$$

Multiplying through by b_n^{n-1}, we get

$$(b_nx)^n + b_{n-1}(b_nx)^{n-1} + \ldots + b_1b_n^{n-2}(b_nx) + b_n^{n-1}b_0 = 0,$$

and thus $b_nx \in S$. Also $b_n \in R \subset S$, so $b_nx, b_n^{-1} \in L$, so $x \in L$. □

REMARK 7. *The proof of Proposition* **??** *establishes the following result, which is occasionally useful in its own right: let R be a domain with fraction field K, let L/K be an algebraoc field extension, and let T be the integral closure of R in L. Then for all $x \in L$, there is $a \in R^\bullet$ such that $ax \in T$.*

EXAMPLE 14.11. *If $R = \mathbb{Z}$, $S = \mathbb{C}$, then $I_S(R) = \overline{\mathbb{Z}}$, the ring of all algebraic integers.*

EXERCISE 14.3. *Show: $\overline{\mathbb{Z}}$ is not finitely generated as a $\mathbb{Z}$-module.*[1]

Let R be a domain with fraction field K. We say that R is **integrally closed** if $I_K(R) = R$, i.e., if any element of the fraction field satisfying a monic integral polynomial with R-coefficients already belongs to R.

COROLLARY 14.12. *Let R be a domain with fraction field K, let L/K be a field extension, and let $S = I_L(R)$. Then S is integrally closed.*

PROOF. Let M be the fraction field of S, and let $\tilde{S}$ be the integral closure of S in M. By Corollary 14.5, $\tilde{S}/R$ is integral, so $\tilde{S} \subseteq S$ and thus $\tilde{S} = S$. □

EXERCISE 14.4. *Let $R = \mathbb{Z}[\sqrt{-3}] = \mathbb{Z}[t]/(t^2+3)$. Show that R is not integrally closed, and compute its integral closure.*

The geometric terminology for an integrally closed domain is **normal**. The process of replacing R by its integral closure $I_K(R)$ is often called **normalization**.

EXERCISE 14.5. *Let R be a domain.*

a) *Suppose the polynomial ring $R[t]$ is integrally closed. Show: R is integrally closed.*
b) *Suppose the formal power series ring $R[[t]]$ is integrally closed. Show: R is integrally closed.*

THEOREM 14.13. *Let R be an integrally closed domain. Then the polynomial ring $R[t]$ is integrally closed.*

PROOF. Let K be the fraction field of R, so $K(t)$ is the fraction field of $R[t]$. The ring $K[t]$ is a PID, hence a UFD, hence integrally closed (these facts will be reviewed in Chapter 15). Let $f \in K(t)^\bullet$ be integral over R; then f is also integral over $K[t]$, so f lies in $K[t]$. We must show that $f \in R[t]$, which we do by induction on $n = deg(f)$. The base case is $n = 0$: then f lies in K and is integral over R, so $f \in R \subseteq R[t]$ because R is integrally closed. Now suppose $n \geqslant 1$ and that every $g \in K[t]$ that is integral over R and of degree less than n lies in $R[t]$. The ring $R[t][f]$ is finitely generated as an R-algebra and integral over R so is finitely generated as an R-module. It follows from this that the ring T of leading coefficients of elements of $(R[t][f])^\bullet$ is finitely generated over R. For

$$f = a_n t^n + \ldots + a_1 t + a_0,$$

we have that $R[a_n] \subseteq T$, so a_n is integral over R and thus – because R is integrally closed – we have $a_n \in R$. Then $f - a_n t^n$ is integral over $R[t]$ and has degree less than n, so by induction $f - a_n t^n \in R[t]$, hence $f \in R[t]$. □

[1]In fact it is not even a Noetherian ring, so not even finitely generated as a $\mathbb{Z}$-algebra.

It is now natural to ask: if R is an integrally closed domain, must $R[[t]]$ be integrally closed? Surprisingly, the answer is in general negative. Before adddressing this, we make an important remark: let K be the fraction field of R. Then the fraction field of $K[[t]]$ is $K[[t]][\frac{1}{t}] =: K((t))$, the field of formal finite-tailed Laurent series. (The ring $K[[t]]$ is a local PID, hence its fraction field is obtained by adjoining a generator of its maximal ideal.) However, the fraction field of $R[[t]]$ may be a proper subfield of $K((t))$. Now here is the first piece of the answer:

THEOREM 14.14. *(Seidenberg* [**Se66**]*) Let R be an integrally closed domain containing a field k. Suppose there is $x \in R \backslash R^\times$ such that $\bigcap_{n \in \mathbb{Z}^+} (x^n) \supsetneq (0)$. Then the formal power series domain $R[[t]]$ is* not *integrally closed.*

PROOF. Let K be the fraction field Choose an integer $n \geqslant 2$ that is not divisible by the characteristic of k, so $n \in R^\times$. There is a sequence $\{c_n\}_{n=1}^\infty$ in the prime subfield of k such that $c_1 \neq 0$ and

$$\left(1 + c_1(\frac{t}{x^2}) + \ldots + c_m(\frac{t}{x^2})^m + \ldots\right)^n = 1 + \frac{t}{x^2},$$

so taking

$$\alpha := x\left(1 + c_1(\frac{t}{x^2}) + \ldots + c_m(\frac{t}{x^2})^m + \ldots\right),$$

we have

$$\alpha^n = x^n(1 + \frac{t}{x^2}) = x^n + tx^{n-2}.$$

Let $a \in \bigcap_{n \neq \mathbb{Z}^+} (x^n) \backslash \{0\}$. Then $a\alpha \in R[[t]]$, so α lies in the fraction field of $R[[t]]$, but α does not lie in $R[[t]]$ since its coefficient of t is $\frac{c_1}{x}$ and we have $c_1 \in R^\times$ and $x \notin R^\times$. □

We still need to find a domain satisfying the hypotheses of Theorem 14.14. We will do so in Chapter 17 in the course of our study of valuation rings. Later in this chapter we will see that if R is integrally closed and Noetherian, then $R[[t]]$ is integrally closed.

3. Spectral properties of integral extensions

Going down (GD): If we have $I_1 \supseteq I_2$ of R and $J_1 \in \operatorname{Spec} S$ such that $J_1 \cap R = I_1$, there exists $J_2 \in \operatorname{Spec} S$ such that $J_2 \subset J_1$ and $J_2 \cap R = I_2$.

LEMMA 14.15. *Let R be a local ring with maximal ideal $\mathfrak{p}$ and S/R an integral extension. Then the pushed forward ideal $\mathfrak{p}S$ is proper.*

PROOF. Suppose not: then there exist $p_i \in \mathfrak{p}$, $s_i \in S$ such that $1 = \sum_i s_i p_i$. Therefore any counterxample would take place already in the finite R-module $R[s_1, \ldots, s_d]$. By induction on d, it is enough to consider the case of $n = 1$: $S = R[s]$. Consider as usual a relation

$$s^n = a_{n-1}s^{n-1} + \ldots + a_1 s + a_0,\ a_i \in R \tag{36}$$

of minimal possible degree n. If $1 \in \mathfrak{p}S$ then we have

$$1 = p_0 + p_1 s + \ldots + p_k s^k,\ p_i \in \mathfrak{p}. \tag{37}$$

In view of (36) we may assume $k \leqslant n-1$. Since $1-p_0$ is not in the maximal ideal of the local ring R, it is therefore a unit; we may therefore divide (37) by $1-p_0$ and get an equation of the form

$$1 = p_1's + \ldots + p_q's^q,\ p_i' \in \mathfrak{p}.$$

This shows that $s \in S^\times$. Replacing $a_0 = a_0 \cdot 1$ in (36) by $a_0(p_1's + \ldots + p_q's^q)$, we get an integral dependence relation which is a polynomial in s with no constant term. Since s is a unit, we may divide through by it and get an integral dependence relation of smaller degree, contradiction. □

THEOREM 14.16. *An integral ring extension S/R satisfies property (LO):*[2] *every prime ideal $\mathfrak{p}$ of R is of the form $S \cap \mathcal{P}$ for a prime ideal $\mathcal{P}$ of S.*

PROOF. For $\mathfrak{p}$ a prime ideal of R, we denote – as usual – by $R_\mathfrak{p}$ the localization of R at the multiplicatively closed subset $R\backslash\mathfrak{p}$. Then $R_\mathfrak{p}$ is local with unique maximal ideal $\mathfrak{p}R_\mathfrak{p}$, and if we can show that there exists a prime ideal $\mathcal{Q}$ of $S_\mathfrak{p}$ lying over $\mathfrak{p}R_\mathfrak{p}$, then the pullback $\mathcal{P} = \mathcal{Q} \cap S$ to S is a prime ideal of S lying over $\mathfrak{p}$. By Lemma 14.15, there exists a maximal ideal $\mathcal{Q} \supset \mathfrak{p}S$ and then $\mathcal{Q} \cap R$ is a proper ideal containing the maximal ideal $\mathfrak{p}$ and therefore equal to it. □

COROLLARY 14.17. *(Going Up Theorem of Cohen-Seidenberg* [**CS46**]*) Let S/R be an integral extension and $\mathfrak{p} \subset \mathfrak{q}$ be two prime ideals of R. Let $\mathcal{P}$ be a prime ideal of S lying over $\mathfrak{p}$ (which necessarily exists by Theorem 14.16). Then there exists a prime ideal $\mathcal{Q}$ of S containing $\mathcal{P}$ and lying over $\mathfrak{q}$.*

PROOF. Apply Theorem 14.16 with $R = R/\mathfrak{p}$ $S = S/\mathcal{P}$ and $\mathfrak{p} = \mathfrak{q}/\mathfrak{p}$. □

COROLLARY 14.18. *(Incomparability) Suppose S/R is integral and $\mathcal{P} \subset \mathcal{Q}$ are two primes of S. Then $\mathcal{P} \cap R \neq \mathcal{Q} \cap R$.*

PROOF. By passage to $S/\mathcal{P}$, we may assume that $\mathcal{P} = 0$ and S is a domain, and our task is to show that any nonzero prime ideal $\mathcal{P}$ of S lies over a nonzero ideal of R. Indeed, let $0 \neq x \in \mathcal{P}$, and let $P(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0 \in R[t]$ be a monic polynomial satisfied by x; we may assume $a_0 \neq 0$ (otherwise divide by t). Then $a_0 \in xS \cap R \subset \mathcal{P} \cap R$. □

COROLLARY 14.19. *Let S/R be an integral extension, $\mathcal{P}$ a prime ideal of S lying over $\mathfrak{p}$. Then $\mathcal{P}$ is maximal if and only if $\mathfrak{p}$ is maximal.*

PROOF. FIRST PROOF: Consider the integral extension $S/\mathcal{P}/(R/\mathfrak{p})$; we want to show that $S/\mathcal{P}$ is a field if and only if $R/\mathfrak{p}$ is a field. This is precisely Proposition 14.8a).
SECOND PROOF: If $\mathfrak{p}$ is not maximal, it is properly contained in some maximal ideal $\mathfrak{q}$. By the Going Up Theorem, there exists a prime $\mathcal{Q} \supset \mathcal{P}$ lying over $\mathfrak{q}$, so $\mathcal{P}$ is not maximal. Conversely, suppose that $\mathfrak{p}$ is maximal but $\mathcal{P}$ is not, so there exists $\mathcal{Q} \supsetneq \mathcal{P}$. Then $\mathcal{Q} \cap R$ is a proper ideal containing the maximal ideal $\mathfrak{p}$, so $\mathcal{Q} \cap R = \mathfrak{p} = \mathcal{P} \cap R$, contradicting the Incomparability Theorem. □

Invoking Going Up and Incomparability to (re)prove the elementary Corollary 14.19 is overkill, but these more sophisticated tools also prove the following

COROLLARY 14.20. *Let S/R be an integral extension of rings. Then the Krull dimensions of R and S are equal.*

[2]Or, **lying over**.

PROOF. Suppose $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_d$ are primes in R. Applying Theorem 14.1, we get a prime $\mathcal{P}_0$ of S lying over $\mathfrak{p}_0$, and then repeated application of the Going Up Theorem yields a chain of primes $\mathcal{P}_0 \subsetneq \mathcal{P}_1 \subsetneq \ldots \subsetneq \mathcal{P}_d$, so that $\dim(S) \geqslant \dim(R)$. Similarly, if we have a chain of prime ideals $\mathcal{P}_0 \subsetneq \ldots \subsetneq \mathcal{P}_d$ of length d in S, then Theorem 14.18 implies that for all $0 \leqslant i < d$, $\mathcal{P}_i \cap R \subsetneq \mathcal{P}_{i+1}$. □

4. Integrally closed domains

Let $R \subset S$ be domains. Immediately from the definition of integrality, there is a concrete way to show that $x \in S$ is integral over R: it suffices to exhibit a monic polynomial $P \in R[t]$ with $P(x) = 0$. What if we want to show that $x \in S$ is *not* integral over R? It would suffice to show that $R[x]$ is not a finitely generated R-module, but exactly how to do this is not clear.

As an example, it is obvious that $\alpha = \sqrt{2}$ is an algebraic integer, but unfortunately it is not obvious that $\beta = \frac{\sqrt{2}}{2}$ is not an algebraic integer. (And of course we need to be careful, because e.g. $\gamma = \frac{1+\sqrt{5}}{2}$ is an algebraic integer, since it satisfies $t^2 + t - 1 = 0$.) One thing to notice is that unlike α and γ, the minimal polynomial of β, $t^2 - \frac{1}{2}$, does not have $\mathbb{Z}$-coefficients. According to the next result, this is enough to know that β is not integral over $\mathbb{Z}$.

THEOREM 14.21. *Let R be a domain with fraction field K, let S/R be an extension domain, and $x \in S$ an integral element over R.*

a) *Let $P(t) \in K[t]$ be the minimal polynomial of x over K. Then $P(t) \in I_K(R)[t]$.*

b) *If R is integrally closed, the minimal polynomial of x has R-coefficients.*

PROOF. a) Let $g \in R[t]$ be a monic polynomial satisfied by x. Let K be the fraction field of R, and let $P \in K[t]$ be the minimal polynomial of x over K, and let M/K be the splitting field of P, so there are $\alpha_1, \ldots, \alpha_d \in M$ such that $P = \prod_{i=1}^d (t - \alpha_i)$. There is $h \in K[t]$ such that $g = Ph$ in $K[t]$. For all $1 \leqslant i \leqslant d$ we have $g(\alpha_i) = 0$, so each α_i is integral over R. Since the roots of P lie among the α_i's they are also integral over R, hence so too are the coefficients of P, being polynomial expressions in the roots.
b) This follows immediately from part a). □

EXERCISE 14.6. *Let R be a domain with fraction field K. Let S/R be an extension such that for every $x \in S$ that is integral over R, the minimal polynomial $P(t) \in K[t]$ has R-coefficients. Show: R is integrally closed.*

THEOREM 14.22. *(Local nature of integral closure) For a domain R, the following are equivalent:*

(i) *R is integrally closed.*

(ii) *For all prime ideals $\mathfrak{p}$ of R, $R_{\mathfrak{p}}$ is integrally closed.*

(iii) *For all maximal ideals $\mathfrak{m}$ of R, $R_{\mathfrak{m}}$ is integrally closed.*

PROOF. Let K be the fraction field of R. Assume (i), and let $\mathfrak{p} \in \operatorname{Spec} R$. By Theorem 14.9, the integral closure of $R_{\mathfrak{p}}$ in K is $R_{\mathfrak{p}}$. Evidently (ii) $\implies$ (iii). Assume (iii), and let x be an element of K which is integral over R. Then for every maximal ideal $\mathfrak{m}$ of R, certainly x is integral over $R_{\mathfrak{m}}$, so by assumption $x \in R_{\mathfrak{m}}$ and thus $x \in \bigcap_{\mathfrak{m}} R_{\mathfrak{m}}$. By Corollary 7.16 we have $\bigcap_{\mathfrak{m}} R_{\mathfrak{m}} = R$. □

EXERCISE 14.7. *Let R be an integrally closed domain with fraction field K, L/K an algebraic field extension, S the integral closure of R in L and $G = \mathrm{Aut}(L/K)$.*

a) *Show: for every $\sigma \in G$, $\sigma(S) = S$.*
b) *For $\mathcal{P} \in \operatorname{Spec} S$ and $\sigma \in G$, show $\sigma(\mathcal{P}) = \{\sigma(x) \mid x \in \mathcal{P}\}$ is a prime ideal of S.*
c) *Show: $\mathcal{P} \cap R = \sigma(\mathcal{P}) \cap R$.*

In conclusion, for every $\mathfrak{p} \in \operatorname{Spec} R$, there is a well-defined action of G on the (nonempty!) set of prime ideals $\mathcal{P}$ of S lying over $\mathfrak{p}$.

LEMMA 14.23. *Let R be a domain with fraction field K of characteristic $p > 0$, let L/K be a purely inseparable algebraic extension of K (possibly of infinite degree), and let S be the integral closure of R in L. For any $\mathfrak{p} \in \operatorname{Spec} R$, $\mathrm{rad}(\mathfrak{p}R)$ is the unique prime of S lying over $\mathfrak{p}$.*

EXERCISE 14.8. *Prove Lemma 14.23.*
(Suggestions: recall that since L/K is purely inseparable, for every $x \in L$, there exists $a \in \mathbb{N}$ such that $x^{p^a} \in K$. First observe that $\mathrm{rad}(\mathfrak{p}R)$ contains every prime ideal of S which lies over $\mathfrak{p}$ and then show that $\mathrm{rad}(\mathfrak{p}R)$ is itself a prime ideal.)

THEOREM 14.24. *(Going Down Theorem of Cohen-Seidenberg [**CS46**]) Let R be an integrally closed domain with fraction field K, and let S be an integral extension of R. If $\mathfrak{p}_1 \subset \mathfrak{p}_2$ are prime ideals of R and $\mathcal{P}_2$ is a prime ideal of S lying over $\mathfrak{p}_2$, then there is a prime ideal $\mathcal{P}_1$ of S which is contained in $\mathcal{P}_2$ and lies over $\mathfrak{p}_1$.*

PROOF. Let L be a normal extension of K containing S, and let T be the integral closure of R in L. In particular T is integral over S, so we may choose $\mathcal{Q}_2 \in \operatorname{Spec} T$ lying over $\mathcal{P}_2$ and also $\mathcal{Q}_1 \in \operatorname{Spec} T$ lying over $\mathfrak{p}_1$. By the Going Up Theorem there exists $\mathcal{Q}' \in \operatorname{Spec} T$ containing $\mathcal{Q}_1$ and lying over $\mathfrak{p}_2$. Both $\mathcal{Q}_2$ and $\mathcal{Q}'$ lie over $\mathfrak{p}_2$, so by Theorem 14.42 there exists $\sigma \in \mathrm{Aut}(L/K)$ such that $\sigma(\mathcal{Q}') = \mathcal{Q}_2$. Thus $\sigma(\mathcal{Q}_1) \subset \sigma(\mathcal{Q}') = \mathcal{Q}_2$ and $\sigma(\mathcal{Q}_1)$ lies over $\mathfrak{p}_1$, so that setting $\mathcal{P}_1 = \sigma(\mathcal{Q}_1) \cap S$ we have $\mathcal{P}_1 \cap R = \mathfrak{p}_1$ and $\mathcal{P}_1 \subset \sigma(\mathcal{Q}') \cap S = \mathcal{Q}_2 \cap S = \mathcal{P}_2$. □

Remark: In [**AM**, Chapter 5] one finds a proof of Theorem 14.24 which avoids all Galois-theoretic considerations. However it is significantly longer than the given proofs of Theorems 14.42 and 14.24 combined and – to me at least – rather opaque.

COROLLARY 14.25. *Let R be an integrally closed domain, and let S be a domain that is an integral extension of R. If $\mathcal{Q} \in \operatorname{Spec} S$, then the height of the ideal $\mathcal{Q}$ of S is the height of the ideal $\mathcal{P} := \mathcal{Q} \cap R$ of R.*

PROOF. Let

$$\mathcal{Q}_0 \subsetneq \mathcal{Q}_1 \subsetneq \ldots \mathcal{Q}_{n-1} \subsetneq \mathcal{Q}$$

be a chain of prime ideals of S having length n and terminating in $\mathcal{Q}$. By Corollary 14.18, the contraction of this chain to R (i.e., we intersect each ideal with R) is a chain of prime ideals of R having length n and terminating in $\mathcal{P}$, so the height of $\mathcal{P}$ is at least that of $\mathcal{Q}$.

Conversely, let

$$\mathcal{P}_0 \subsetneq \mathcal{P}_1 \subsetneq \ldots \mathcal{P}_{n-1} \subsetneq \mathcal{P}$$

be a chain of prime ideals of R having length n and terminating in $\mathcal{P}$. By Theorem 14.24 and Corollary 14.18, this is the contraction of a chain of prime ideals of S having length n and terminating in $\mathcal{Q}$, so the height of $\mathcal{Q}$ is at least that of $\mathcal{P}$. □

5. The Noether Normalization Theorem

5.1. The classic version.

THEOREM 14.26. *(Noether Normalization) Let k be a field, and let R be a domain with fraction field K. Suppose that R is moreover a finitely generated k-algebra, generated say by elements $x_1, \ldots, x_m$. Then:*

a) *There is $d \in \mathbb{Z}$, $0 \leqslant d \leqslant m$, and algebraically independent elements $y_1, \ldots, y_d \in R$ such that R is finitely generated as a module over the polynomial ring $k[y_1, \ldots, y_d]$ – or equivalently, that $R/k[y_1, \ldots, y_d]$ is an integral extension.*

b) *We have $\dim R = d = \operatorname{trdeg}(K/k)$ (the transcendence degree of K/k).*

PROOF. a) (Jacobson) The result is trivial if $m = d$, so we may suppose $m > d$. Then the y_i are algebraically dependent over k: there exists a nonzero polynomial

$$f(s_1, \ldots, s_m) = \sum a_J s_1^{j_1} \cdots s_m^{j_m}, a_J \in k[s_1, \ldots, s_m]$$

with $f(x_1, \ldots, x_m) = 0$. Let X be the set of monomials $s^J = s_1^{j_1} \cdots s_m^{j_m}$ occuring in f with nonzero coefficients. To each such monomial we associate the univariate polynomial

$$j_1 + j_2 t + \ldots + j_m t^{m-1} \in \mathbb{Z}[t].$$

The polynomials obtained in this way from the elements of X are distinct. Since a univariate polynomial over a field has only finitely many zeroes, it follows that there exists $a \geqslant 0$ such that the integers $j_1 + j_2 a + \ldots + j_m a^{m-1}$ obtained from the monomials in X are distinct. Now consider the polynomial

$$f(s_1, s_1^a + t_1, \ldots, s_1^{a^{m-1}} + t_m) \in k[s, t].$$

We have

$$f(s_1, s_1^a + t_1, \ldots, s_1^{a^{m-1}} + t_m) = \sum_J a_J s_1^{j_1} (s_1^d + t_2)^{j_2} \cdots (s_1^{a^{m-1}} + t_m)^{j_m}$$

$$= \sum_J a_J s_1^{j_1 + j_2 a + \ldots + j_m a^{m-1}} + g(s_1, t_2, \ldots, y_m),$$

in which the degree of g in s_1 is less than that of $\sum_J a_J s_1^{j_1 + j_2 a + \ldots + j^m a^{m-1}}$. Hence for suitable $\beta \in k^\times$, $\beta f(s_1, s_1^a + t_2, \ldots, s_1^{a^{m-1}} + t_m)$ is a monic polynomial in x_1 with $k[t_2, \ldots, t_m]$-coefficients. Putting $w_i = x_i - x_1^{a^{i-1}}$ for $2 \leqslant i \leqslant m$, we get

$$\beta f(x_1, x_1^d + w_2, \ldots, x_1^{a^{m-1}} + w_m) = 0,$$

so that x_1 is integral over $R' = k[w_2, \ldots, w_m]$. By induction on the number of generators, R' has a transcendence base $\{y_i\}_{i=1}^d$ such that R' is integral over $k[y_1, \ldots, y_d]$. Thus R is integral over $k[y_1, \ldots, y_d]$ by transitivity of integrality.

b) Since $R/k[y_1, \ldots, y_d]$ is integral, by Corollary 14.20 the Krull dimension of R is equal to the Krull dimension of $k[y_1, \ldots, y_d]$, which by Corollary 12.15 is d. Since R is finitely generated as a $k[y_1, \ldots, y_d]$ algebra, by Proposition 14.10 K is finitely generated as a $k(y_1, \ldots, y_d)$-module, so $\operatorname{trdeg} K/k = \operatorname{trdeg} k(y_1, \ldots, y_d) = d$. □

5.2. Separable Noether Normalization.

Let K be a field and let $\overline{K}$ an algebraic closure of K. A field extension L/K is **regular** if $L \otimes_K \overline{K}$ is a field (equivalently, a domain).

For a field extension L/K, we say **K is algebraically closed in L** if any element of L which is algebraic over K lies in K. It is an easy exercise to show that if L/K is regular, K is algebraically closed in L. The converse is true in characteristic zero, but in positive characteristic we need a further hypothesis:

THEOREM 14.27. *Let L/K be a field extension.*

a) *The following are equivalent:*
   (i) *The extension L/K is regular.*
   (ii) *The extension L/K is separable and K is algebraically closed in L.*

b) *In particular, if K is perfect and algebraically closed in L, then L/K is regular.*

PROOF. a) The key result here is **Mac Lane's Theorem** [**FT**, §12]: a field extension L/K is separable if and only if L and $K^{p^{-\infty}}$ are linearly disjoint over K. (i) $\implies$ (ii): If L/K is regular, then K is algebraically closed in L. Further, L and $\overline{K}$ are linearly disjoint over K, hence L and $K^{p^{-\infty}}$ are linearly disjoint over K. (ii) $\implies$ (i): Let $K' = K^{p^{-\infty}}$ and $L' = L \otimes_K K'$. Since $L \otimes_K \overline{K} = (L \otimes_K K') \otimes_{K'} \overline{K} = L' \otimes_{K'} \overline{K}$, it is enough to show that L' is a field and $L' \otimes_{K'} \overline{K}$ is a field. Now L' is a field by Mac Lane's Theorem, and since K' is perfect, $\overline{K}/K'$ is a Galois extension, and thus by [**FT**, §12.3], since $L' \cap \overline{K} = K'$, L' and $\overline{K}$ are linearly disjoint over K'. b) If K is perfect, every extension of K is separable. Apply part a). □

THEOREM 14.28. *(Separable Noether Normalization) Let k be a field, and let R be a domain that is finitely generated as a k-algebra. Assume moreover that the fraction field L of R is a* regular *extension of k.*

a) *There is $d \in \mathbb{Z}$, $0 \leqslant d \leqslant m$, and algebraically independent elements $y_1, \ldots, y_d \in R$ such that R is finitely generated as a $k[y_1, \ldots, y_d]$-module and $L/k(y_1, \ldots, y_d)$ is a finite* separable *field extension.*

b) *The integer d is equal to both the Krull dimension of R and the transcendence degree of K/k.*

For now we refer the reader to [**Ei**, Cor. 16.18] for the proof.

5.3. Noether normalization over a domain.

THEOREM 14.29. *(Noether Normalization II) Let $R \subset S$ be domains with S finitely generated as an R-algebra. There exists $a \in R^\bullet$ and $y_1, \ldots, y_d \in S$ algebraically independent over the fraction field of R such that S_a (the localization of S at the multiplicative subset generated by a) is finitely generated as a module over $T = R_a[y_1, \ldots, y_d]$.*

PROOF. (K.M. Sampath) Let K be the fraction field of R and let $x_1, \ldots, x_m$ be a set of R-algebra generators for S. Then

$$S' := S \otimes_R K = K[x_1, \ldots, x_m]$$

is finitely generated over K (as above, the x_i's need not be algebraically independent). Applying Theorem 14.26, we get algebraically independent elements $y_1, \ldots, y_d \in S'$ such that S' is a finitely generated $T' := K[y_1, \ldots, y_d]$-module.

Multiplying by a suitable element of $R^\times$, we may assume $y_i \in S$ for all i.

Since S' is finitely generated as a T'-module, it is integral over T'. For $1 \leqslant i \leqslant m$, x_i satisfies a monic polynomial equation with coefficients in T':

$$y_1^n + P_{i,1}(y_1, \ldots, y_d)y_i^{n-1} + \ldots + P_{i,n} = 0.$$

Let a be the product of the denominators of all coefficients of all the polynomials $P_{i,k}$. It follows that S_a is integral and finitely generated as a $T = R_a[y_1, \ldots, y_d]$-algebra, hence it is finitely generated as a T-module. □

EXERCISE 14.9. *In the setting of Theorem 14.29 suppose S is a graded R-algebra. Show: we may take all the y_i to be homogeneous elements.*

5.4. Applications.

The Noether Normalization Theorem is one of the foundational results in algebraic geometry: geometrically, it says that every integral affine variety of dimension d is a finite covering of affine d-space $\mathbb{A}^d$. Thus it allows us to study arbitrary varieties in terms of rational varieties via branched covering maps. It is almost as important as a theorem of pure algebra, as even the "soft" part of the result, that the Krull dimension of an integral affine k-algebra is equal to the transcendence degree of its fraction field, is basic and useful.

One of the traditional applications of Noether Normalization is to prove Hilbert's Nullstellensatz. As we have seen, it is fruitful to channel proofs of the Nullstellensatz through Zariski's Lemma, and this is no exception.

PROPOSITION 14.30. *Noether Normalization implies Zariski's Lemma.*

EXERCISE 14.10. *Prove Proposition 14.30.*

For the next result, we write $\mathrm{ht}(\mathfrak{p})$ for the height of a prime ideal $\mathfrak{p}$.

THEOREM 14.31. *Let k be a field, and let R be a domain that is finitely generated as a k-algebra.*

a) *For all $\mathfrak{p} \in \operatorname{Spec} R$, we have*

$$\dim R = \mathrm{ht}(\mathfrak{p}) + \dim R/\mathfrak{p}. \tag{38}$$

b) *Every maximal chain of prime ideals in R has length $\dim R$.*

PROOF. a) We claim that in any Noetherian ring R of finite Krull dimension, for any $\mathfrak{p} \in \operatorname{Spec} R$ we have

$$\dim R \geqslant \mathrm{ht}(\mathfrak{p}) + \dim R/\mathfrak{p}.$$

Indeed, let $\mathcal{C}_1$ be a chain of prime ideals teminating at $\mathfrak{p}$ of length $\mathrm{ht}(\mathfrak{p})$, and let $\mathcal{C}_2$ be a chain of prime ideals starting at $\mathfrak{p}$ of length $\dim R/\mathfrak{p}$. Then $\mathcal{C}_1 \cup \mathcal{C}_2$ is a chain of prime ideals of length $\mathrm{ht}(\mathfrak{p}) + \dim R/\mathfrak{p}$, so $\mathrm{ht}(\mathfrak{p}) + \dim R/\mathfrak{p} \leqslant \dim R$.

Let $d = \dim R$. We will prove that

$$d \leqslant \mathrm{ht}(\mathfrak{p}) + \dim R/\mathfrak{p}$$

by induction on d. The case $d = 0$ is trivial. Let us inductively suppose that the inequality holds for all finitely generated k-algebras of dimension less than d.

Step 1: By Noether normalization, there are algebraically independent elements

$x_1, \ldots, x_d$ of R such that R is finitely generated as a $k[x_1, \ldots, x_d]$-module, hence R is integral over $k[x_1, \ldots, x_d]$. Let $\underline{\mathfrak{p}} := \mathfrak{p} \cap k[x_1, \ldots, x_d]$. The natural map

$$k[x_1, \ldots, x_d]/\underline{\mathfrak{p}} \to R/\mathfrak{p}$$

is an integral extension of domains, so $\dim R/\mathfrak{p} = \dim k[x_1, \ldots, x_d]/\underline{\mathfrak{p}}$. Moreover by Corollary 14.25 we have $\mathrm{ht}(\mathfrak{p}) = \mathrm{ht}(\underline{\mathfrak{p}})$. Thus we may assume without loss of generality that $R = k[t_1, \ldots, t_d]$ is a polynomial ring.

Step 2: Since $\mathfrak{p}$ is a nonzero prime ideal of the UFD $k[t_1, \ldots, t_d]$, there is a nonzero prime element $f \in \mathfrak{p}$, and by Krull's Hauptidealsatz, (f) is a height one prime ideal. We claim that $\dim k[t_1, \ldots, t_d]/(f) = d - 1$. By Noether Normalization, it suffices to show that if K is the fraction field of the domain $k[t_1, \ldots, t_d]/(f)$, then the transcendence degree of K/k is $d-1$. The polynomial f must have positive degree in at least one indterminate; without loss of generality, suppose it has positive x_d-degree. For $1 \leqslant i \leqslant d$ let $\overline{x_i}$ be the image of x_i in K. We claim that $\overline{x_1}, \ldots, \overline{x_d} = 0$. The polynomial f itself shows that $\overline{x_d}$ is algebraic over $k(\overline{x_1}, \ldots, \overline{x_{d-1}})$. Now let $Q \in k[x_1, \ldots, x_{d-1}]$ be a polynomial such that $Q(\overline{x_1}, \ldots, \overline{x_{d-1}}) = 0$. This means $Q \in (f)$, but then if Q were nonzero its degree in t_d would be be positive since the degree of f in x_d is positive...so $Q = 0$. Thus $\overline{x_1}, \ldots, \overline{x_{d-1}}$ is a transcendence basis for K/k, so $\dim k[x_1, \ldots, t_d]/(f) = d - 1$ as claimed.

Step 3: Put $R' := k[x_1, \ldots, x_d]/\langle f \rangle$ and $\mathfrak{p}' := \mathfrak{p}/\langle f \rangle$. Then $R/\mathfrak{p} \cong R'/\mathfrak{p}'$ and

$$\mathrm{ht}(\mathfrak{p}) \geqslant \mathrm{ht}(\mathfrak{p}') + 1,$$

so by induction we have

$$\dim R = 1 + \dim R' = 1 + \mathrm{ht}(\mathfrak{p}') + \dim R/\mathfrak{p}' = 1 + \mathrm{ht}(\mathfrak{p}') + \dim R/\mathfrak{p} \leqslant \mathrm{ht}(\mathfrak{p}) + \dim R/\mathfrak{p},$$

completing the proof of part a).

b) Let

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_n$$

be a maximal chain of prime ideals of R. Then $\mathfrak{p}_0 = (0)$ and $\mathfrak{p}_n \in \mathrm{MaxSpec}\, R$. We argue by induction on n.

If $n = 0$, then $\mathfrak{p}_n = (0)$, so R is a field and $n = \dim R$. Now suppose that $n \geqslant 1$. The chain $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1$ must be maximal among chains terminating at $\mathfrak{p}_1$, so $\mathrm{ht}(\mathfrak{p}_1) = 1$. Then

$$\mathfrak{p}_1/\mathfrak{p}_1 \subsetneq \mathfrak{p}_2/\mathfrak{p}_1 \subsetneq \mathfrak{p}_n/\mathfrak{p}_1$$

is a maximal chain of length $n-1$ in $R/\mathfrak{p}_1$, so by induction and part a) we have

$$n - 1 = \dim R/\mathfrak{p}_1 = \dim R - \mathrm{ht}(\mathfrak{p}_1) = \dim R - 1,$$

so $n = \dim R$. □

We say that a partially ordered set $(X, \leqslant)$ is **catenary** if for two elements $x_1 \leqslant x_2$ there is a uniform bound on lengths of finite chains starting at x_1 and ending at x_2 and all maximal finite chains from x_1 to x_2 have the same length.

Exercise 14.11.

a) *Let A be a set, and let $X = 2^A$ be the set of all finite subsets of X, partially ordered under inclusion. If $Y_1 \subseteq Y_2$ are finite subsets of A, show that every chain from Y_1 to Y_2 in X is finite and every maximal such chain has length $\#Y_2 - \#Y_1$. Thus X is catenary.*

b) *Let κ be a cardinal number. Show: if $\kappa \leqslant 2$ then every partially ordered set of cardinality κ is catenary, while if $\kappa \geqslant 3$ there is a partially ordered set of cardinality κ that is not catenary.*

EXERCISE 14.12. *Let $(X, \leqslant)$ be a partially ordered set. Suppose there is $d \in \mathbb{N}$ such that every finite chain in X has length at most d and that every maximal finite chain in X has length d. Show: X is catenary.*

We say that a ring R is **catenary** if $\operatorname{Spec} R$, partially ordered under inclusion, is catenary.

EXERCISE 14.13. *Let k be a field, and let R be a finitely generated k-algebra. Let $\mathfrak{p} \subsetneq \mathfrak{q}$ be prime ideals of R. Show: every maximal chain of primes from $\mathfrak{p}$ to $\mathfrak{q}$ has length $\operatorname{ht}(\mathfrak{q}) - \operatorname{ht}(\mathfrak{p})$. Deduce: R is caternary.*

EXERCISE 14.14. *Let R be a ring that is* not *catenary. Show that there is an ideal I such that R/I is a non-catenary domain with $\dim R = \dim(R/I)$.*

By the previous exercise, to look for noncatenary rings we may restrict attention to domains. Clearly any domain of Krull dimension 0 or 1 is catenary. Already there are noncatenary domains of dimension 2: by Exercise 15.16b), if R is a semilocal PID, then $R[t]$ is a noncatenary domain of Krull dimension 2. Notice that $R[t]$ is otherwise a very nice ring: e.g. it is a UFD. Catenarity is in fact a very strong property; that finitely generated algebras over a field satisfy it is an important foundational result for algebraic geometry.

6. Some Classical Invariant Theory

Let R be a commutative ring, let G be a finite group, and suppose G acts on R by automorphisms, i.e., we have a homomorphism $\rho : G \to \operatorname{Aut}(R)$. We define

$$R^G = \{x \in R \mid \forall g \in G,\ gx = x\},$$

the **ring of G-invariants** – it is indeed a subring of R.

Remark: As in the case of rings acting on commutative groups, we say that G-action on R is **faithful** if the induced homomorphism $\rho : G \to \operatorname{Aut}(R)$ is injective. Any G-action induces a faithful action of $G/\ker(\rho)$, so it is no real loss of generality to restrict to faithful G-actions. We will do so when convenient and in such a situation identify G with its isomorphic image in $\operatorname{Aut} R$.

The simplest case is that in which $R = K$ is a field. Then K^G is again a field and K/K^G is a finite Galois extension. Conversely, for any finite Galois extension K/F, $F = K^{\operatorname{Aut}(K/F)}$. This characterization of Galois extensions was used by E. Artin as the foundation for an especially elegant development of Galois theory (which swiftly became the standard one). Note also the analogy to topology: we have the notion of a finite Galois covering $Y \to X$ of topological spaces as one for which the group $G = \operatorname{Aut}(Y/X)$ of deck transformations acts freely and properly discontinuously on Y such that $Y/G = X$.

The branch of mathematics that deals with invariant rings under linear group actions is called **classical invariant theory**. Historically it was developed along with basic commutative algebra and basic algebraic geometry in the early 20th

century, particularly by Hilbert. Especially, Hilbert's work on the finite generation of invariant rings was tied up with his work on the Basis Theorem.

For $a \in R$, put $N_G(a) = \prod_{\sigma \in G} \sigma(a)$. Then $N_G(a) \in R^G$, so we have a map

$$N_G : R \to R^G.$$

Note that N_G is *not* a homomorphism of additive groups. However, when R is a domain, there is an induced map

$$N_G : R^\bullet \to (R^G)^\bullet$$

which is a homomorphism of monoids, so induces a homomorphism on unit groups.

EXERCISE 14.15. *Let $R[t]$ be the univariate polynomial ring over R. Show: there is a unique action of G by automorphisms of G on $R[t]$ extending the G-action on R and such that $gt = t$. Show that $(R[t])^G = R^G[t]$.*

PROPOSITION 14.32. *For a finite group G acting on R, R/R^G is integral.*

PROOF. For $x \in R$, define

$$\Phi_x(t) = N_G(t - x) = \prod_{g \in G} (t - gx),$$

so $\Phi_x(t) \in (R[t])^G = R^G[t]$. Thus $\Phi_x(t)$ is a monic polynomial with R^G-coefficients which is satisfied by x. □

Base extension: Suppose that G is a finite group acting faithfully on R. Moreover, let A be a ring and $f : A \to R$ be a ring homomorphism, so R is an A-algebra. Suppose moreover that $f(A) \subset R^G$. In such a situation we say that G acts on R by A-automorphisms and write $G \subset \mathrm{Aut}(R/A)$.

Suppose we have another A-algebra A'. We can define an action of G on $R \otimes_A A'$ by putting $g(x \otimes y) := gx \otimes y$. We say that the G-action is **extended to** A'.

PROPOSITION 14.33. *In the above setup, suppose that A' is a flat A-algebra. Then there is a natural isomorphism*

$$R^G \otimes_A A' \xrightarrow{\sim} (R \otimes_A A')^G.$$

PROOF. Madapusi p. 65-66. □

COROLLARY 14.34. *Let G be a finite group acting on the ring R, and let $S \subset R^G$ be a multiplicatively closed set. Then $(S^{-1}R)^G = S^{-1}R^G$.*

EXERCISE 14.16. *Prove Corollary 14.34.*

In particular, suppose R is a domain with fraction field K, and let F be the fraction field of R^G. Then the G-action on R extends to a G-action on K, and Corollary 14.34 gives $K^G = F$. Thus the invariant theory of domains is compatible with the Galois theory of the fraction fields.

PROPOSITION 14.35. *If R is integrally closed, so is R^G.*

PROOF. Let $x \in K$ be integral over R^G. Then x is also integral over R, and since R is integally closed in L we have $x \in R$. Thus $x \in R \cap K = R \cap L^G = R^G$. □

THEOREM 14.36. *(Noether* [**No26**]*) Suppose that R is a finitely generated algebra over some field k with $k = k^G$. Then:*

a) *R is finitely generated as an R^G-module.*
b) *R^G is a finitely generated k-algebra.*

PROOF. a) Since R is a finitely generated k-algebra and $k \subset R^G$, R is a finitely generated R^G-algebra. But by Proposition 14.32 R/R^G is integral. So R is finitely generated as an R^G-module.
b) By part a), the Artin-Tate Lemma (Theorem 8.62) applies to the tower of rings $k \subset R^G \subset R$. The conclusion is as desired: R^G is a finitely generated k-algebra. □

Remark: The title of [**No26**] mentions "characteristic p". In fact, when k has characteristic 0 the result had been proven by Hilbert significantly earlier [**Hi90**], and moreover for certain actions of infinite linear groups, like $\mathrm{SL}_n(k)$. But Noether's formulation and proof give an excellent illustration of the economy and power of the commutative algebraic perspective.

Let us make contact with the setup of *classical invariant theory*: let k be a field, V a finite-dimensional vector space and $\rho : G \to \mathrm{Aut}_k(V)$ a linear representation of G on V. Let $k[V] = \mathrm{Sym}(V^\vee)$ be the algebra of polynomial functions on V. If we choose a k-basis $e_1, \ldots, e_n$ of V and let $x_1, \ldots, x_n$ be the dual basis of $V^\vee$, then $k[V] = k[x_1, \ldots, x_n]$ is a polynomial ring in n independent indeterminates. There is an induced action of G on $k[V]$, namely for $f \in k[V]$ we put $(gf)(x) = f(g^{-1}x)$.

All of our above results apply in this situation. Especially, Theorem 14.36 applies to tell us that the ring $k[V]^G$ is finitely generated as a k-algebra, or a **finite system of invariants**. Of course, we did not so much as crease our sleeves, let alone roll them up, to establish this: for a concretely given finite group G and action on a k-vector space V, it is of interest to explicitly compute such a finite system. Moreover, the polynomial ring $k[V]$ is integrally closed: in the next section we will see that it is a unique factorization domain and that this is a stronger property. Therefore Proposition 14.35 applies to show that $k[V]^G$ is integrally closed. This is actually quite a robust and useful procedure for producing integrally closed rings.

EXAMPLE 14.37. *Let k be a field, $n \in \mathbb{Z}^+$, let $V = k^n$, $G = S_n$ be the symmetric group, and let G act on V by permuting the standard basis elements $e_1, \ldots, e_n$. We will compute $k[V]^G$. Namely, for $1 \leqslant i \leqslant n$, we define the* ***ith elementary symmetric function*** *$s_i(t_1, \ldots, t_n)$ as follows: let X be an independent indeterminate and put*

$$f(X) := \prod_{i=1}^{n}(X - t_i) = X^n + \sum_{i=1}^{n}(-1)^i s_i(t_1, \ldots, t_n)X^{n-i}.$$

THEOREM 14.38. *The invariant ring $k[V]^{S_n}$ is a polynomial k-algebra on the elementary symmetric functions $s_1, \ldots, s_n$.*

PROOF. Step 1: Explicitly, we have

$$s_1 = t_1 + \ldots + t_n,$$

$$s_2 = \sum_{i<j} t_i t_j;$$

each s_i is the sum of all $\binom{n}{k}$ monomials of degree k. Clearly $k[s_1, \ldots, s_n] \subset k[V]^{S_n}$.
Step 2: For any finite group G of automorphisms of a field L, L/K^G is a Galois extension with $\mathrm{Aut}(L/L^G) = G$. Take $L = k(V)$ and note that $k(V)$ is the splitting field of the separable polynomial $f \in k(s_1, \ldots, s_n)[x]$, so $k(V)^G = k(s_1, \ldots, s_n)$.
Step 3: Because $k(t_1, \ldots, t_n)/k(s_1, \ldots, s_n)$ is a finite extension, the transcendence degree of $k(s_1, \ldots, s_n)/k$ is equal to the transcendence degree of $k(t_1, \ldots, t_n)/k$, namely n. It follows that the elements $s_1, \ldots, s_n$ are algebraically independent, i.e., $k[s_1, \ldots, s_n]$ is a polynomial ring.
Step 4: As in the proof of Proposition 14.35,

$$k[t_1, \ldots, t_n]^{S_n} = k[t_1, \ldots, t_n] \cap k(s_1, \ldots, s_n) = k[s_1, \ldots, s_n]. \qquad \square$$

The above example is well-known and extremely useful, but gives a misleadingly simple impression of classical invariant theory. One can ask how often the ring of invariants of a finite group action on a polynomial ring is again a polynomial ring, and there is a nice answer to this. But let's back up a step and go back to "rational invariant theory": if G acts on $k[x_1, \ldots, x_n]$, then as above it also acts on the fraction field $k(x_1, \ldots, x_n)$ and we know that $k(x_1, \ldots, x_n)/k(x_1, \ldots, x_n)^G$ is a finite Galois extension. But must $k(x_1, \ldots, x_n)^G$ itself be a rational function field, as it was in the example above? This is known as **Noether's Problem**: it was first posed by E. Noether in 1913. It is natural and important, for an affirmative answer would allow us to realize every finite group as a Galois group (i.e., the automorphism group of a Galois extension) of $\mathbb{Q}$ thanks to a famous theorem of Hilbert. For more than half of the twentieth century, Noether's problem remained open. Finally, in 1969 R.G. Swan (yes, the same Swan as before!) found a representation of the cyclic group of order 47 on a finite-dimensional $\mathbb{Q}$-vector space for which the invariant field is not a rational function field [**Sw69**]. Too bad – this was arguably the best shot that anyone has ever taken at the Inverse Galois Problem over $\mathbb{Q}$.[3]

EXAMPLE 14.39. *Let k be a field of characteristic different from 2, let $V = k^2$, and consider the action of the two-element group $G = \{\pm 1\}$ on V by -1 acting as the scalar matrix -1. The induced action on $k[V] = k[x, y]$ takes $x \mapsto -x$ and $y \mapsto -y$. This is, apparently, a not very interesting representation of a not very interesting group. But the invariant theory is very interesting!*

EXERCISE 14.17.

a) *Show: $k[V]^G$ is generated as a k-algebra by x^2, y^2 and xy.*
b) *Show: $k[V]^G$ is isomorphic to the k-algebra $k[A, B, C]/(AB - C^2)$.*
c) *Show: $k[V]^G$ is* not *isomorphic to $k[x, y]$.*[4]
d) *Show that nevertheless the fraction field of $k[V]^G$ is rational, i.e., is isomorphic to $k(X, Y)$ for independent indeterminates X and Y.*

Before signing off on our quick glimpse of classical invariant theory, we cannot resist mentioning one more classic theorem in the subject. It answers the question: when is the invariant subalgebra $k[V]^G$ isomorphic to a polynomial algebra over k?

---

[3]Serre's *Topics in Galois Theory* describes a conjecture of J.-L. Colliot-Thélène – roughly a weaker form of Noether's problem – that would still imply that every finite group is a Galois group over $\mathbb{Q}$. I am not aware of any progress on this conjecture.

[4]Suggestion: the proof of Theorem 15.62 shows that $\mathbb{C}[A, B, C]/(AB - C^2)$ is not a unique factorization domain. The argument goes through with $\mathbb{C}$ replaced by k.

Let $\rho : G \hookrightarrow \mathrm{GL}(V)$ be a faithful representation of G on a finite-dimensional k-vector space V. An element $g \in \mathrm{GL}(V)$ is a **pseudoreflection** if it has finite order and pointwise fixes a hyperplane W in V. (Equivalently, a pseudoreflection has characteristic polynomial $(t-1)^{\dim V - 1}(t-\zeta)$, where ζ is a root of unity in k.)

EXERCISE 14.18. *If k is formally real, any nontrivial pseudoreflection has order 2 – i.e., it really is a hyperplane reflection.*

A faithful representation ρ of G is a **pseudoreflection representation** of G if $\rho(G)$ is generated by pseudorflections.

THEOREM 14.40. *(Shephard-Todd-Chevalley-Serre) Let k be a field, and let $\rho : G \hookrightarrow \mathrm{GL}(V)$ be a faithful finite-dimensional k-linear representation.*

a) *If $k[V]^G$ is a polynomial algebra, then ρ is a pseudoreflection representation.*
b) *If ρ is a pseudoreflection representation and $\mathrm{char}\, k \nmid \#G$, then $k[V]^G$ is a polynomial algebra.*

PROOF. See [**Be**, §7.2]. □

In the **modular** case $\mathrm{char}\, k \mid \#G$, there are pseudoreflection representations for which $k[V]^G$ is not a polynomial algebra. However, work of Kemper and Malle [**KM99**] shows that even in the modular case, if ρ is an irreducible pseudoreflection representation then the invariant *field* $k(V)^G$ is purely transcendental over k.

EXERCISE 14.19. *It follows from Theorem 14.40 the fundamental theorem on symmetric functions that the standard permutation representation of the symmetric group S_n on k^n is a pseudoreflection representation. Show this directly.*

7. Galois extensions of integrally closed domains

PROPOSITION 14.41. *Let G be a finite group acting by automorphisms on a ring R, with invariant subring R^G. Let $\iota : R^G \hookrightarrow R$, and let $\mathfrak{p} \in \mathrm{Spec}\, R^G$.*

a) *There is a natural action of G on the fiber $(\iota^*)^{-1}(\mathfrak{p})$ – i.e., on the set of primes $\mathcal{P}$ of R such that $\iota^*\mathcal{P} = \mathfrak{p}$.*
b) *The G-action on the fiber $(\iota^*)^{-1}(\mathfrak{p})$ is transitive.*

PROOF. Let $\mathcal{P} \in \mathrm{Spec}\, R$ and $\sigma \in G$. Define

$$\sigma\mathcal{P} = \{\sigma x \mid x \in \mathcal{P}\}.$$

It is straightforward to verify that $\sigma\mathcal{P}$ is a prime ideal of R (if you like, this follows from the fact that Spec is a functor). Moreover $(\sigma\mathcal{P}) \cap R^G$ is the set of all elements σx with $x \in \mathcal{P}$ such that for all $g \in G$, $g\sigma x = \sigma x$. As g runs through all elements of G, so does $g\sigma^{-1}$, hence $(\sigma\mathcal{P}) \cap R^G = \mathcal{P} \cap R^G = \mathfrak{p}$.
b) Let $\mathcal{P}_1, \mathcal{P}_2$ be two primes of R lying over a prime $\mathfrak{p}$ of R^G. Let $x \in \mathcal{P}_1$. Then $N_G(x) \in \mathcal{P}_1 \cap R^G = \mathfrak{p} \subset \mathcal{P}_2$. Since $\mathcal{P}_2$ is prime, there exists at least one $\sigma \in G$ such that $\sigma x \in \mathcal{P}_2$, and thus $\mathcal{P}_1 \subset \bigcup_{\sigma \in G} \sigma\mathcal{P}_2$. By Prime Avoidance (Lemma 8.52), there exists $\sigma \in G$ such that $\mathcal{P}_1 \subset \sigma\mathcal{P}_2$. Since R/R^G is integral, Incomparability (Corollary 14.18) yields $\mathcal{P}_1 = \sigma\mathcal{P}_2$. □

THEOREM 14.42. *Let R be an integrally closed domain with fraction field K, let L/K be a normal algebraic field extension (possibly of infinite degree), and let S be the integral closure of R in L. Let $\mathfrak{p} \in \mathrm{Spec}\, R$, and let $X_\mathfrak{p}$ be the set of all prime ideals of S lying over $\mathfrak{p}$. Then $G = \mathrm{Aut}(L/K)$ acts transitively on $X_\mathfrak{p}$.*

PROOF. Step 1: Suppose $[L:K] = n < \infty$, and write $G = \{\sigma_1 = 1, \ldots, \sigma_r\}$.[5] Seeking a contradiction, suppose there are $\mathcal{P}_1, \mathcal{P}_2 \in X_{\mathfrak{p}}$ such that $\mathcal{P}_2 \neq \sigma_j^{-1}\mathcal{P}_1$ for all j. By Corollary 14.18, $\mathcal{P}_2$ is not contained in any $\sigma_j^{-1}\mathcal{P}_1$, so by Prime Avoidance (Lemma 8.52) there is $x \in \mathcal{P}_2 \setminus \bigcup_j \sigma_j^{-1}\mathcal{P}_1$. Let q be the inseparable degree of L/K and put $y = \left(\prod_j \sigma_j(x)\right)^q$. Thus $y = N_{L/K}(x)$, so $y \in K$. Moreover y is integral over R, so $y \in R$. Since $\sigma_1 = 1$, $y \in \mathcal{P}_2$, so $y \in \mathcal{P}_2 \cap R = \mathfrak{p} \subset \mathcal{P}_1$, and thus, since $\mathcal{P}_1$ is prime, $\sigma_j(x) \in \mathcal{P}_1$ for some j: contradiction!
Step 2: We will reduce to the case in which L/K is a Galois extension. Let $G = \mathrm{Aut}(L/K)$ and $K' = L^G$, so that L/K' is Galois and K'/K is purely inseparable. Let R' be the integral closure of R in K'. Then by Lemma 14.23 $\operatorname{Spec} R' \to \operatorname{Spec} R$ is a bijection. So we may as well assume that $K' = K$ and L/K is Galois.
Step 3: For each finite Galois subextension M of L/K, consider the subset

$$F(M) := \{\sigma \in G \mid \sigma(\mathcal{P}_1 \cap M) = \mathcal{P}_2 \cap M\}.$$

Observe that $F(M)$ is a union of cosets of $\mathrm{Gal}(L/M)$ hence is (open and) closed in the Krull topology. By Step 1, we have $F(M) \neq \varnothing$. Moreover, the compositum $M = \prod_i M_i$ of any finite number $\{M_i\}$ of finite Galois subextenions is again a finite Galois subextension, and we have $\bigcap_i F(M_i) \supset F(M) \neq \varnothing$. Therefore as M_i ranges through all finite Galois subextensions of L/K, $\{F(M_i)\}_{i \in I}$ is a family of closed subsets of the compact space G satisfying the finite intersection condition, and it follows that there exists $\sigma \in \bigcap_i F(M_i) = F(L)$ i.e., $\sigma \in G$ such that $\sigma\mathcal{P}_1 = \mathcal{P}_2$. □

8. Almost Integral Extensions

We come now to a technical variant of the notion of integrality. This variant will not be used until §19.4 on divisorial ideals. We honestly recommend that the reader skip past this section for now and return only when the concept of complete integral closure is needed and used.

Let $R \subseteq T$ be rings. An element $x \in T$ is **almost integral** over R if there is a finitely generated R-submodule of T that contains x^n for all $n \in \mathbb{Z}^+$. We say that T is **almost integral** over R if every element of S is almost integral over R.

PROPOSITION 14.43. *Let R be a domain with fraction field K. For $x \in K^\times$, the following are equivalent:*

(i) *The element x is almost integral over R.*
(ii) *There is $a \in R^\bullet$ such that for all $n \in \mathbb{Z}^+$ we have $ax^n \in R$.*
(iii) *There is a nonzero ideal I of R such that $x \in (I : I)$.*

PROOF. (i) $\implies$ (ii): If x is almost integral over R, then there are elements $y_1, \ldots, y_N \in K$ and for all $n \in \mathbb{Z}^+$ elements $a_{n,1}, \ldots, a_{n,N} \in R$ such that

$$x^n = a_{n,1}y_1 + \ldots + a_{N,n}y_N.$$

We may assume that each y_i is nonzero and then write $y_i = \frac{b_i}{c_i}$ with $b_i, c_i \in R^\bullet$. Clearing denominators, we get

$$c_1 \cdots c_N x^n = c_2 \cdots c_N a_{n,1} b_1 + \ldots + c_1 \cdots c_{N-1} a_{N,N} b_N \in R.$$

[5] We are assuming that L/K is normal, so L/K is separable if and only if L/K is Galois if and only if $r = n$.

(ii) $\implies$ (i): If $a \in R^\bullet$ is such that $ax^n \in R$ for all $n \in \mathbb{Z}^+$, then $\langle \frac{1}{a} \rangle_R$ is a finitely generated R-submodule of K that contains x^n for all $n \in \mathbb{Z}^+$.
(ii) $\implies$ (iii): Suppose there is $a \in R^\bullet$ such that $ax^n \in R$ for all $n \in \mathbb{Z}^+$. Then if we take $I := \langle ax^n \mid n \in \mathbb{Z}^+ \rangle$, then I is a nonzero ideal of R such that $xI \subseteq I$.
(iii) $\implies$ (ii): Suppose there is a nonzero ideal I of R such that $x \in (I : I)$. Since $(I : I)$ is a subring of K, we have $x^n \in (I : I)$ for all $n \in \mathbb{Z}^+$, and let $a \in I^\bullet$. Then for all $n \in \mathbb{Z}^+$ we have $ax^n \in I \subseteq R$. □

PROPOSITION 14.44. *Let $R \subset S$ be rings, and let $x \in S$.*

a) *If x is integral over R, then it is almost integral over R.*
b) *If R is Noetherian and x is almost integral over R, then x is integral over R.*

PROOF. Let $M = \langle R, x \rangle$. By Theorem 14.1, x is integral over R if and only if M is a finitely generated R-module.
a) If x is integral over R, then M is a finitely generated R-submodule of S containing x^n for all $n \in \mathbb{Z}^+$, so x is almost integral over R.
b) Suppose x is almost integral over R: there is a finitely generated R-submodule N of S containing x^n for all $n \in \mathbb{Z}^+$. Then $M \subset N$, and since R is Noetherian and N is finitely generated, M is finitely generated and x is integral over R. □

Remark: As the proof shows, an equivalent – and perhaps more perspicuous – way of expressing the almost integrality condition is that, while integrality of x means that $M = \langle R, x \rangle_R$ is a finitely generated submodule of S, almost integrality means that there is *some* finitely generated R-submodule of S containing M.

For rings $R \subseteq T$, the **complete integral closure** of R in T is the set of all elements of T that are almost integral over R.

EXERCISE 14.20. *Let $R \subseteq T$ be rings. Show: the complete integral closure of R in T is an R-subalgebra of T.*

A domain R is **completely integrally closed** if its complete integral closure in its fraction field is R itself. By Proposition 14.43, the complete integral closure of a domain R with fraction field K is the set of elements $x \in K$ for which there is $a \in R^\bullet$ such that $ax^n \in R$ for all $n \in \mathbb{Z}^+$.

EXERCISE 14.21. *Show: a UFD is completely integrally closed.*

EXERCISE 14.22. *Let $U \subseteq \mathbb{C}$ be a domain (i.e., a connected open subset). Show: the ring $\mathrm{Hol}\, U$ of holomorphic functions on U is completely integrally closed.*

EXERCISE 14.23. *Let R be a domain.*

a) *(Seidenberg) Suppose R is completely integrally closed. Show: $R[[t]]$ is completely integrally closed.*
b) *(Nagata) Deduce: if R is Noetherian and integrally closed, then $R[[t]]$ is integrally closed.*

PROPOSITION 14.45. *Let $R \subseteq T$ be rings, and let $\tilde{R}$ be the complete integral closure of R in T. Then $\tilde{R}$ is integrally closed in T.*

PROOF. Let $x \in T$ be integral over $\tilde{R}$, so there are $a_0, \ldots, a_{n-1} \in \tilde{R}$ such that $x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$. Then x is also integral over the ring

$R[a_0, \ldots, a_{n-1}]$. For $0 \leqslant i \leqslant n-1$, there is a finitely generated R-submodule M_i of T containing all non-negative powers of a_i. Let M be the R-submodule of T generated by all products $b_0 \cdots b_{n-1}$ with $b_i \in M_i$. Then M is a finitely generated R-module and

$$R[a_0, \ldots, a_{n-1}] \subseteq M \subseteq T.$$

Let $\tilde{M}$ be the R-module generated by elements mx^i for $m \in M$ and $0 \leqslant i \leqslant n-1$. Because M is finitely generated, so is $\tilde{M}$. Moreover

$$R[x] \subseteq \langle x^0, \ldots, x^{n-1} \rangle_{R[a_0,\ldots,a_{n-1}]} \subseteq \tilde{M},$$

so $R[x]$ is contained in a finitely generated R-submodule of T. Thus x is almost integral over R and $x \in \tilde{R}$. □

However, complete integral closure lacks of some of the good properties of integral closure. First of all, Proposition 14.45 is not what one probably would have wanted to show: rather it is natural to expect that the complete integral closure of R in T is *completely* integrally closed. Unfortunately this is not generally true: in fact there is a domain R whose complete integral closure in its fraction field is not completely integrally closed [**LM**, p. 98, Exc. IV.14]. Thus complete integral closure is somewhat of a misnomer in that it is not a closure operator on the set of subrings of a field in the sense given in §2.1. Moreover, whereas being integrally closed is a local property, being completely integrally closed is not even a localizable property: by Exercise 14.22, the ring $\operatorname{Hol} \mathbb{C}$ of entire functions is completely integrally closed, but Exercise d) shows that the localization at one of its maximal ideals is not.

This makes one wonder whether and how much business we should have with the complete integral closure concept. It will make exactly two more crucial appearances in this text: it will turn out that complete integral closure is the necessary and sufficient on a domain for the divisorial fractional ideals modulo the prinicpal fractional ideals to form a group, the **divisor class group** of R. It also appears in a characterization theorem of **Krull domains**.

CHAPTER 15

Factorization

Let R be a domain, and x a nonzero, nonunit element of R. We say that x is **irreducible** if for any $y, z \in R$ such that $x = yz$, one of y or z is a unit.

For any unit $u \in R^\times$, we get factorizations of the form $x = u \cdot (u^{-1}x)$, so every x has at least these factorizations, which we wish to regard as "trivial". On the other hand, y and z cannot both be units, for then x would also be a unit. Let us then define a **factorization** of a nonzero nonunit $a \in R$ as a product

$$a = x_1 \cdots x_n,$$

such that each x_i is irreducible. We say that two factorizations

$$a = x_1 \cdots x_n = y_1 \cdots y_m$$

are **equivalent** if the multisets of associated principal ideals $\{\{(x_i)\}\} = \{\{(y_j)\}\}$ are equal. More concretely, this means that $m = n$ and that there is a bijection $\sigma : \{1, \ldots, n\} \to \{1, \ldots, m\}$ such that $(y_{\sigma(i)}) = (x_i)$ for all $1 \leqslant i \leqslant n$.

If factorizations always exist and any two factorizations of a given element are equivalent, we say R is a **unique factorization domain** (UFD).

1. Kaplansky's Theorem (II)

A basic and important result that ought to get covered at the undergraduate level is that PID implies UFD. In fact this is easy to prove. What is more difficult is to get a sense of exactly how UFDs are a more general class of rings than PIDs. In this regard, an elegant theorem of Kaplansky seems enlightening.

EXERCISE 15.1. *Let x be an element of a domain which can be expressed as*

$$x = p_1 \cdots p_n,$$

such that for $1 \leqslant i \leqslant n$, $\mathfrak{p}_i = (p_i)$ is a prime ideal. If then there exist principal prime ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ such that $(x) = \mathfrak{q}_1 \cdots \mathfrak{q}_m$, then $m = n$ and there exists a permutation σ of the integers from 1 to n such that $\mathfrak{q}_i = \mathfrak{p}_{\sigma(i)}$ for all i.

EXERCISE 15.2. *Let R be a domain, and let S be the set of all nonzero elements x in R such that (x) can be expressed as a product of principal prime ideals. Show: S is a saturated multiplicatively closed subset.*

THEOREM 15.1. *(Kaplansky) A domain is a UFD if and only if every nonzero prime ideal in R contains a prime element.*

PROOF. Suppose R is a UFD and $0 \neq \mathfrak{p} \in \operatorname{Spec} R$. Let $x \in \mathfrak{p}^\bullet$, and write

$$x = p_1 \cdots p_r$$

a product of prime elements. Then $x \in \mathfrak{p}$ implies $p_i \in \mathfrak{p}$ for some i, so $(p_i) \subset \mathfrak{p}$.

Conversely, assume each nonzero prime ideal of R contains a principal prime. Let S be the set of all products of prime elements, so that by Exercise 15.2, S is a saturated multiplicative subset. By Exercise 15.1, it is enough to show that S contains all nonzero nonunits of R. Suppose for a contradiction that there exists a nonzero nonunit $x \in R \backslash S$. The saturation of S implies $S \cap (x) = \varnothing$, and then by Theorem 5.26 there is a prime ideal $\mathfrak{p}$ containing x and disjoint from S. But by hypothesis, $\mathfrak{p}$ contains a prime element p, contradicting its disjointness from S. □

COROLLARY 15.2. *Let R be a domain.*

a) *If R is a UFD, then every height one prime ideal is principal. If R is Noetherian and every height one prime ideal is principal, then R is a UFD.*
b) *If every ideal of R is principal, R is a UFD.*
c) *Conversely, if R is a UFD of dimension one, every ideal of R is principal.*

PROOF. We begin by recalling that in a domain R the height one primes are the nonzero prime ideals $\mathfrak{p}$ such that there is no prime ideal $\mathfrak{q}$ with $(0) \subsetneq \mathfrak{q} \subsetneq \mathfrak{p}$.
a) If R is a UFD and $\mathfrak{p}$ is a height one prime ideal, then by Theorem 15.1 $\mathfrak{p}$ has a prime element (π). Then $(\pi) \subset \mathfrak{p}$ is a containment of prime ideals, and since $\mathfrak{p}$ has height one we have $\mathfrak{p} = (\pi)$ is principal. Conversely, suppose R is Noetherian and every height one prime ideal is principal. Let $x \in R$ be irreducible: i.e., x is a nonzero nonunit and $x = yz$ implies $y \in R^\times$ or $z \in R^\times$. Let $\mathfrak{p}$ be a minimal prime over (x). By Krull's Hauptidealsatz, $\mathfrak{p}$ has height one and so by assumption $\mathfrak{p} = (\pi)$. Thus $\pi \mid x$ and since x is irreducible we must have $(\pi) = (x)$. Thus we have shown that every irreducible element of R is prime. As we will see §3 (and as the reader may know from "general algebra"), a Noetherian domain in which each irreducible element is prime is a UFD.
b) If every ideal of R is principal, then every ideal of R is finitely generated. So R is Noetherian and part a) applies.
c) In a UFD of dimension one, part a) implies that every prime ideal is principal. By Theorem 4.30, every ideal is principal. □

One may ask: in a not necessarily Noetherian domain, if every height one prime is principal, must R be a UFD? The answer turns out to be negative. Later on, when we study valuation rings, we will be able to construct: (i) a domain R in which every nonzero prime ideal has infinite height. Such a domain vacuously has the property that every height one prime is principal, has no nonzero prime elements (and is not a field!) so cannot be a UFD. And we will be able to construct (ii): for each $n \geqslant 2$ a domain of Krull dimension n with a unique height one prime ideal, that is principal. In a UFD R with a unique height one prime $\mathfrak{p}$, we must have $\mathfrak{p} = (\pi)$ and then every nonunit element of R is divisible by π, so $\mathfrak{p}$ is maximal and $\dim R = 1$.

Corollary 15.2 shows in particular that a one-dimensional UFD is Noetherian. We will see later in this chapter that a UFD need not be Noetherian: indeed, we will show that for any UFD R, the polynomial ring $R[t_1, \ldots, t_n, \ldots]$ in infinitely many indeterminates is also a UFD, and this ring is certainly not Noetherian. The ring $R[t_1, \ldots, t_n, \ldots]$ moreover has infinite Krull dimension: indeed the prime ideal $\mathfrak{p} = \langle t_1, \ldots, t_n, \ldots \rangle$ has infinite height. So one may then ask whether there are

non-Noetherian UFDs of finite Krull dimension. In fact, for all $n \in \mathbb{Z}^{\geq 2}$, Gilmer constructed a non-Noetherian UFD of Krull dimension n [**Gi74**, Thm. 2].

EXERCISE 15.3. *Let R be a UFD with finitely many height one primes. Show: R is a semilocal PID.*
(Hint: every prime ideal in a UFD is generated by prime elements.)

2. Atomic domains, ACCP

A domain in which every nonzero nonunit can be factored into irreducibles is an **atomic domain**.

EXERCISE 15.4. *Show: the ring $\overline{\mathbb{Z}}$ of all algebraic integers is not an atomic domain. Indeed, since for every algebraic integer x, there exists an algebraic integer y such that $y^2 = x$, there are no irreducible elements in $\overline{\mathbb{Z}}$!*

The condition of factorization into irreducibles (in at least one way) holds in every Noetherian domain. In fact, a much weaker condition than Noetherianity suffices:

PROPOSITION 15.3. *Let R be a domain in which every ascending chain of **principal** ideals stabilizes. Then every nonzero nonunit factors into a product of irreducible elements. In particular, a Noetherian domain is atomic.*

PROOF. Let R be a domain satisfying the ascending chain condition for principal ideals (ACCP for short), and suppose for a contradiction that R is *not* an atomic domain. Then the set of principal ideals generated by unfactorable elements is nonempty, so by our assumption there exists a maximal such element, say $I = (a)$. Evidently a is not irreducible, so we can begin to factor a: $a = xy$ where x and y are nonunits. But this means precisely that both principal ideals (x) and (y) properly contain (a), so that by the assumed maximality of (a), we can factor both x and y into irreducibles: $x = x_1 \cdots x_m$, $y = y_1 \cdots y_n$. But then

$$a = x_1 \cdots x_m y_1 \cdots y_n$$

is a factorization of a, contradiction. □

This proposition motivates us to consider also the class of domains which satisfy the **ascending chain condition for principal ideals** (ACCP).

EXERCISE 15.5. *Suppose $R \hookrightarrow S$ is an extension of rings such that $S^\times \cap R = R^\times$. (In particular, this holds for integral extensions.) Show that S satisfies (ACCP) implies R satisfies (ACCP). Does the converse hold?*

We have just seen that (ACCP) implies atomicity. The proof shows that under (ACCP) we can always obtain an expression of a given nonzero nonunit by a finite sequence of "binary factorizations" i.e., replacing an element x with $y_1 \cdot y_2$, where y_1 and y_2 are nonunits whose product is x. After a bit of thought, one is inclined to worry that it may be possible that this factorization procedure fails but nevertheless irreducible factorizations exist. This worry turns out to be justified:

THEOREM 15.4. *There is an atomic domain that is not an ACCP-domain.*

PROOF. See [**Gr74**]. □

However, the following strenghtening of atomicity does imply ACCP:

A domain R is a **bounded factorization domain** BFD if it is atomic and for each nonzero nonunit $a \in R$, there exists a positive integer $N(a)$ such that in any irreducible factorization $a = x_1 \cdots x_r$ we have $r \leqslant N(a)$.

PROPOSITION 15.5. *A UFD is a BFD.*

PROOF. An immediate consequence of the definitions. □

PROPOSITION 15.6. *A BFD satisfies (ACCP).*

PROOF. Let R be a BFD. Suppose for a contradiction that $(x_i)_{i \in \mathbb{Z}^+}$ is a strictly ascending chain of principal ideals. We therefore have

$$x_0 = y_1 x_1 = y_1 y_2 x_2 = \ldots = y_1 \cdots y_n x_n = \cdots,$$

with each x_i, y_i a nonunit. Since R is atomic, we can refine each factorization into an irreducible factorization, but clearly an irreducible refinement of $y_1 \cdots y_n x_n$ has at least $n+1$ irreducible factors, contradicting BFD. □

3. EL-domains

An element x of a domain R is **prime** if the principal ideal (x) is a prime ideal. Equivalently, x satisfies **Euclid's Lemma**: if $x \mid yz$, then $x \mid y$ or $x \mid z$.

PROPOSITION 15.7. *A prime element is irreducible.*

PROOF. If x is reducible, then $x = yz$ with neither y nor z a unit, so that $yz \in (x)$ but $y \notin (x)$, $z \notin (x)$. □

However, it need not be the case that irreducible elements are prime!

Example: Let $R = \mathbb{Z}[\sqrt{-5}]$. Then $2, 3$ and $1 \pm \sqrt{-5}$ are all irreducible, but

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

shows that none of them are prime.

EXERCISE 15.6. *Check all these assertions. Hint: Define $N(a + b\sqrt{-5}) = a^2 + 5b^2$. Check that $N((a + b\sqrt{-5})(c + d\sqrt{-5})) = N(a + b\sqrt{-5})N(c + d\sqrt{-5})$. Show that $\alpha \mid \beta$ (in R) $\implies$ $N(\alpha) \mid N(\beta)$ (in $\mathbb{Z}$), and use this to show that $2, 3, 1 \pm \sqrt{-5}$ are irreducible but not prime.*

It is tempting to call a domain in which all irreducible elements are prime "Euclidean," but this terminology is already taken for domains satisfying a generalization of the Euclidean algorithm (c.f. §16.3). So we will, provisionally, call a ring in which irreducible elements are prime an **EL-domain**. (EL = Euclid's Lemma).

THEOREM 15.8. *For a domain R, the following are equivalent:*

(i) *R is a UFD.*
(ii) *R satisfies (ACCP) and is an EL-domain.*
(iii) *R is an atomic EL-domain.*

PROOF. i) $\implies$ (ii): In the previous section we saw UFD $\implies$ BFD $\implies$ (ACCP). We show UFD implies EL-domain: let $x \in R$ be irreducible and suppose $x \mid yz$. Let $y = y_1 \cdots y_m$ and $z = z_1 \cdots z_n$ be irreducible factorizations of y and z. Then the uniqueness of irreducible factorization means that x must be associate to some y_i or to some z_j, and hence $x \mid y$ or $x \mid z$: R is an EL-domain.

(ii) $\implies$ (iii) follows immediately from Proposition 15.3.

(iii) $\implies$ (i): This is nothing else than the usual deduction of the fundamental theorem of arithmetic from Euclid's Lemma: in an atomic domain we have at least one irreducible factorization of a given nonzero nonunit x. If we also assume irreducibles are prime, we may compare any two irreducible factorizations: suppose

$$x = y_1 \cdots y_m = z_1 \cdots z_n.$$

Then y_1 is a prime element so divides z_j for some j. WLOG, relabel to assume $j = 1$. Since z_1 is irreducible, we have $y_1 = u_1 z_1$ and thus we may cancel to get

$$y_2 \cdots y_m = (u_1^{-1} z_2) z_3 \cdots z_n.$$

Continuing in this way we find that each y_i is associate to some z_j; when we get down to $1 = \prod_j z_j$ we must have no factors of z_j left, so $m = n$ and R is a UFD. □

We can now deduce the following important result, a characterization of Noetherian UFDs among all Noetherian domains.

THEOREM 15.9. *For a Noetherian domain R, the following are equivalent:*

(i) *Every height one prime ideal of R is principal.*

(ii) *R is a UFD.*

PROOF. (i) $\implies$ (ii): By Theorem 15.8, it is sufficient to prove that R is an EL-domain, so let $x \in R$ be irreducible. Let $\mathfrak{p}$ be a minimal prime containing x. By Krull's Hauptidealsatz (Theorem 8.49), $\mathfrak{p}$ has height one, so by assumption $\mathfrak{p} = (p)$ is principal. Thus $x = up$ for some $u \in R$, and since x and p are both irreducible, $u \in R^\times$, $(x) = \mathfrak{p}$, and x is a prime element.

(ii) $\implies$ (i): This implication is a special case of Kaplansky's Theorem 15.1 (and thus holds without the Noetherian assumption on R). □

4. GCD-domains

For elements a and b of a domain R, a **greatest common divisor** is an element d of R such that: $d \mid a$, $d \mid b$ and for $e \in R$ with $e \mid a$, $e \mid b$, $e \mid d$.

EXERCISE 15.7. *Show: if d is a gcd of a and b, then an element d' of R is a gcd of a and b if and only if $(d) = (d')$. In particular, any two gcd's are associate.*

If a and b have a gcd, it would be more logically sound to write $\gcd(a, b)$ to mean the unique principal ideal whose generators are the various gcd's of a and b. It is traditional however to use the notation $\gcd(a, b)$ to denote an element, with the understanding that in general it is only well-defined up to multiplication by a unit.[1]

More generally, for elements $a_1, \ldots, a_n$ in a domain R, a greatest common divisor is an element d of R such that $d \mid a_i$ for all i and if $e \mid a_i$ for all i then $e \mid d$.

[1]In some rings, principal ideals have canonical generators: e.g. in the integers we may take the unique positive generator and in $k[t]$ we may take the unique monic generator. Under these circumstances, a common convention is to let $\gcd(a, b)$ stand for this canonical generator.

If a GCD of $(a_1, \ldots, a_n)$ exists, it is unique up to associates, and we denote it by $\gcd(a_1, \ldots, a_n)$. As above, it can be characterized as the unique minimal *principal* ideal containing $\langle a_1, \ldots, a_n \rangle$. Moreover, these setwise GCDs can be reduced to pairwise GCDs.

EXERCISE 15.8. *Let a, b, c be elements of a domain R and assume that all pairwise GCD's exist in R. Then $\gcd(a, b, c)$ exists and we have $\gcd(a, \gcd(b, c)) = \gcd(a, b, c) = \gcd(\gcd(a, b), c)$.*

A domain R is a **GCD-domain** if for all $a, b \in R$, $\gcd(a, b)$ exists. By the above remarks, it would be equivalent to require that $\gcd(a_1, \ldots, a_n)$ for all n-tuples of elements in R.

PROPOSITION 15.10. *(GCD Identities) Let R be a GCD-domain. Then:*

a) *For all $a, b, c \in R$, $\gcd(ab, ac) = a \gcd(b, c)$.*
b) *For all $a, b \in R \backslash \{0\}$, $\gcd(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}) = 1$.*
c) *For all $a, b, c \in R$, $\gcd(a, b) = \gcd(a, c) = 1$, then $\gcd(a, bc) = 1$.*
d) *For all $a, b, c \in R$, $\gcd(a, b + ac) = gcd(a, b)$.*
e) *For all $a, a_1, \ldots, a_n, b_1, \ldots, b_n, c \in R$, $\gcd(a, b_1 + ca_1, \ldots, b_n + ca_n) = \gcd(a, b_1, \ldots, b_n)$.*

PROOF. a) Let $x = \gcd(ab, ac)$. Then $a \mid ab$ and $a \mid ac$ so $a \mid x$: say $ay = x$. Since $x \mid ab$ and $x \mid ac$, $y \mid b$ and $y \mid c$, so $y \mid \gcd(b, c)$. If $z \mid b$ and $z \mid c$, then $az \mid ab$ and $az \mid ac$, so $az \mid x = ay$ and $z \mid y$. Therefore $\gcd(b, c) = y = \frac{1}{a} \gcd(ab, ac)$.
b) This follows immediately from part a).
c) Suppose $\gcd(a, b) = \gcd(a, c) = 1$, and let t divide a and bc. Then t divides ab and bc so $t \mid \gcd(ab, bc) = b \gcd(a, c) = b$. So t divides $\gcd(a, b) = 1$.
d) If d divides both a and b, it divides both a and $b + ac$. If d divides both a and $b + ac$, it divides $b + ac - c(a) = b$.
e) We have

$$\begin{aligned}\gcd(a, b_1 + ca_1, \ldots, b_n + ca_n) &= \gcd(a, \gcd(a, b_1 + ac_1), \ldots, \gcd(a, b_n + ac_n)) \\ &= \gcd(a, \gcd(a, b_1), \ldots, \gcd(a, b_n)) = \gcd(a, b_1, \ldots, b_n).\end{aligned}$$

□

PROPOSITION 15.11. *A GCD-domain is an EL-domain.*

PROOF. This follows from: $\gcd(x, y) = \gcd(x, z) = 1 \implies \gcd(x, yz) = 1$. □

THEOREM 15.12. *Consider the following conditions on a domain R:*

(i) *R is a UFD.*
(ii) *R is a GCD-domain.*
(iii) *R is an EL-domain: irreducible elements are prime.*

a) *We have (i) $\implies$ (ii) $\implies$ (iii).*
b) *If R is an ACCP-domain, (iii) $\implies$ (i).*

PROOF. a) (i) $\implies$ (ii): Let x, y be nonzero elements of R. We may write

$$x = f_1 \cdots f_r g_1 \cdots g_s, \ y = u f_1 \cdots f_r h_1 \cdots h_t,$$

where the f's, g's and h's are prime elements, $(g_j) \neq (h_k)$ for all j, k and $u \in R^\times$. Then $f_1 \cdots f_r$ is a gcd for x and y.
(ii) $\implies$ (iii): This is Proposition 15.11.
b) (iii) + (ACCP) $\implies$ (i): This is Theorem 15.8. □

COROLLARY 15.13. *For a Noetherian domain R, the following are equivalent:*
(i) *R is a UFD.*
(ii) *R is a GCD-domain.*
(iii) *R is an EL-domain.*

We now present some simple results that are long overdue. An extremely useful fact in algebra is that any UFD is integrally closed in its fraction field. We give a slightly stronger result and then recall a classical application.

THEOREM 15.14. *A GCD-domain is integrally closed.*

PROOF. Let R be a GCD-domain with fraction field K. Suppose $x \in K$ satisfies

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0,\ a_i \in R.$$

Write $x = \frac{s}{t}$ with $s, t \in R,\ t \neq 0$. By Proposition 15.10b), after dividing by the gcd we may assume $\gcd(s,t) = 1$. Plugging in $x = \frac{s}{t}$ and clearing denominators gives

$$s^n = -\left(a_{n-1}ts^{n-1} + \ldots + a_1 t^{n-1}s + a_0 t^n\right),$$

so $t \mid s^n$. But by Proposition 15.10c) $\gcd(s^n, t) = 1$, so $t \in R^\times$ and $x \in R$. □

COROLLARY 15.15. *An algebraic integer which is a rational number is an integer: $\overline{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$.*

EXERCISE 15.9. *Prove Corollary 15.15.*

Thus e.g. one can derive the irrationality of $\sqrt{2}$: it is a root of the monic polynomial equation $t^2 - 2 = 0$ but evidently not an integer, so cannot be rational.

PROPOSITION 15.16. *(Compatibility of GCD's with localization) Let R be a GCD-domain and S a multiplicative subset of R. Then:*
a) *The localization $S^{-1}R$ is again a GCD-domain.*
b) *For all $x, y \in R^\bullet$, if d is a GCD for x and y in R, then it is also a GCD for x and y in $S^{-1}R$.*

EXERCISE 15.10. *Prove Proposition 15.16.*

THEOREM 15.17. *Let R be a UFD with $2 \in R^\times$. Let $f \in R$ be squarefree – i.e., not divisible by the square of any nonunit – and not a square. Then*

$$S = R[\sqrt{f}] := R[x]/\langle x^2 - f\rangle$$

is an integrally closed domain.

PROOF. Let K be the fraction field of R. By Theorem 15.14 R is integrally closed, and thus f is not a square in K – if so, it would also be a square in R – so $x^2 - f$ is irreducible in $K[x]$ and thus $L := K[x]/(x^2 - f)$ is a quadratic field extension of K. Write $\sqrt{f}$ for the element $x + (x^2 - f)$ of L, so $L = K(\sqrt{f})$ and $S = R[\sqrt{f}]$. In particular, S is a domain.

Let α be an element of L that is integral over R, so $\alpha = a + b\sqrt{f}$ with $a, b \in K$. If $b = 0$ then $\alpha \in K$ hence $\alpha \in R$ since R is integrally closed in K, so assume $b \neq 0$. Then the minimal polynomial of α is

$$P(t) = t^2 - 2at + (a^2 - b^2 f).$$

By Theorem 14.21 we have $-2a \in R$ and $a^2 - b^2 f \in R$. Since $2 \in R^\times$, we get that $a \in R$ and then that $b^2 f \in R$. Since f is squarefree, this implies that $b \in R$:

otherwise, $\mathrm{ord}_p(b) \leqslant -1$ for some prime element p, so $\mathrm{ord}_p(b^2 f) \leqslant -2 + 1 < 0$. So $\alpha \in S$. Thus S is integrally closed. □

EXERCISE 15.11. *Show: in Theorem 15.17 the hypothesis $2 \in R^\times$ is necessary. (E.g. show: $\mathbb{Z}[\sqrt{3}]$ is not integrally closed.)*

5. GCDs versus LCMs

The definition of GCDs in a domain has an evident analogue for least common multiples. Namely, if a and b are elements of a domain R, a **least common multiple** of a and b is an element l such that for all $m \in R$ with $a \mid m$ and $b \mid m$ then $l \mid m$.

Many of the properties of GCD's carry over immediately to LCM's. For instance, if l is an LCM of a and b, then $l' \in R$ is an LCM of a and b if and only if l' is associate to l.

PROPOSITION 15.18. *Let a and b be elements in a domain R. Then $\mathrm{lcm}(a,b)$ exists if and only if the ideal $(a) \cap (b)$ is principal, in which case the set of all LCM's of a and b is the set of all generators of $(a) \cap (b)$.*

PROOF. This is straightforward and left to the reader. □

LCM's exist in any UFD: if

$$a = x_1^{a_1} \cdots x_r^{a_r},\ b = x_1^{b_1} \cdots x_r^{b_r},$$

with $a_i, b_i \in \mathbb{N}$. Then

$$l = x_1^{\max(a_1,b_1)} \cdots x_r^{\max(a_r,b_r)}$$

is a greatest common divisor of a and b. Now the simple identity

$$\forall a, b \in \mathbb{N}, \min(a,b) + \max(a,b) = a + b$$

implies that for a, b in any UFD R we have

$$\gcd(a,b)\,\mathrm{lcm}(a,b) \sim ab.$$

This identity further suggests that the existence of either one of $\gcd(a,b)$, $\mathrm{lcm}(a,b)$ implies the existence of the other. However, this turns out only to be half correct!

THEOREM 15.19. *For a, b in a domain R, the following are equivalent:*

(i) $\mathrm{lcm}(a,b)$ *exists.*
(ii) *For all $r \in R\backslash\{0\}$, $\gcd(ra,rb)$ exists.*

PROOF. Step 1: i) $\Longrightarrow$ (ii). Suppose that there exists a least common multiple of a and b, say l. We claim that $d := \frac{ab}{l}$ is a greatest common divisor of a and b. (Since ab is a common divisor of a and b, $l \mid ab$, so indeed $d \in R$.) Indeed, suppose that $e \mid a$ and $e \mid b$. Then since $\frac{ab}{e}$ is a common multiple of a and b, we must have $l \mid \frac{ab}{e}$ and this implies $e \mid \frac{ab}{l}$. Thus d is a GCD of a and b.
Step 2: Suppose that for $r \in R\backslash\{0\}$ and $a, b \in R$, $\gcd(ra,rb)$ exists. Then we claim that $\gcd(a,b)$ exists and $\gcd(ra,rb) = r\gcd(a,b)$. Put $g := \frac{\gcd(ra,rb)}{r}$, which is clearly an element of D. Since $\gcd(ra,rb)$ divides ra and rb, g divides a and b. Conversely, if $e \mid a$ and $e \mid b$, then $re \mid ra$ and $re \mid rb$ so $er \mid \gcd(ra,rb)$ and $e \mid g$.
Step 3: We claim that if $l := \mathrm{lcm}(a,b)$ exists then so does $\mathrm{lcm}(ra,rb)$ for all $r \in R\backslash\{0\}$. First observe that rl is a common multiple of ra and rb. Now suppose m is a common multiple of ra and rb, say $m = xra = yrb = r(xa - yb)$. Thus $r \mid m$

and $a \mid \frac{m}{r}$, $b \mid \frac{m}{r}$. So $l \mid \frac{m}{r}$ and $rl \mid m$. Thus $\operatorname{lcm}(ra, rb) = r \operatorname{lcm}(a, b)$.
Step 4: (ii) $\implies$ (i). We may assume that a and b are nonzero, since the other cases are trivial. Suppose $\gcd(ra, rb)$ exists for all $r \in R\backslash\{0\}$. We claim that $l := \frac{ab}{\gcd(a,b)}$ is an LCM of a and b. Clearly l is a common multiple of a and b. Now suppose that m is a common multiple of a and b. Then ab divides both ma and mb, so $ab \mid \gcd(ma, mb)$. By Step 2, $\gcd(ma, mb) = m \gcd(a, b)$. Thus $\frac{ab}{\gcd(a,b)} \mid m$. □

THEOREM 15.20. *(Khurana,* [**Kh03**, Thm. 4]*) Let $d \geqslant 3$ be an integer such that $d + 1$ is not prime, and write $d + 1 = pk$ for a prime number p and $k \geqslant 2$. Then in the domain $R = \mathbb{Z}[\sqrt{-d}]$, the elements p and $1 + \sqrt{-d}$ have a GCD but no LCM.*

PROOF. Step 1: We claim that p is irreducible as an element of R. Indeed, if it were reducible, then by the multiplicativity of the norm map $N(a + b\sqrt{-d}) = a^2 + dp^2$ we could write it as $p = \alpha\beta$, with

$$p^2 = N(p) = N(\alpha\beta) = N(\alpha)N(\beta),$$

and, since α, β are nonunits, $N(\alpha), N(\beta) > 1$. But then $N(\alpha) = N(\beta) = p$, i.e., there would be $a, b \in \mathbb{Z}$ such that $a^2 + db^2 = p$. But this is not possible: either $ab = 0$, in which the left hand side is a perfect square, or $a^2 + db^2 \geqslant d + 1 > p$.
Step 2: $\gcd(p, 1 + \sqrt{-d}) = 1$. Indeed, since $\frac{1}{p} + \frac{1}{p}\sqrt{-d} \notin R$, $p \nmid 1 + \sqrt{-d}$.
Step 3: We claim that kp and $k(1 + \sqrt{-d})$ do not have a GCD. Indeed, by Step 2 of the proof of Theorem 15.19, if any GCD exists then k is a GCD. Then, since $1 + \sqrt{-d}$ divides both $(1 - \sqrt{-d})(1 + \sqrt{-d}) = 1 + d = kp$ and $k(1 + \sqrt{-d})$, $1 + \sqrt{-d}$ divides $\gcd(kp, k(1 + \sqrt{-d}) = k$, i.e., there exist $a, b \in \mathbb{Z}$ such that

$$k = (1 + \sqrt{-d})(a + b\sqrt{-d}) = (a - db) + (a + b)\sqrt{-d},$$

i.e., $a = -b$ and $k = a - db = a + da = a(1 + d)$ and $d + 1 \mid k$, contradicting the fact that $1 < k < d + 1$.
Step 4: It follows from Theorem 15.19 that $\operatorname{lcm}(p, 1 + \sqrt{-d})$ does not exist. □

Khurana produces similar examples even when $d + 1$ is prime, which implies that for no $d \geqslant 3$ is $R_d = \mathbb{Z}[\sqrt{-d}]$ a GCD-domain. (In fact, since $(R_d, +) \cong \mathbb{Z}^2$, R_d is an abstract number ring and hence Noetherian, so the notions of EL-domain, GCD-domain and UFD are all equivalent.) Let us give an independent proof:

THEOREM 15.21. *For no $d \geqslant 3$ is $R_d = \mathbb{Z}[\sqrt{-d}]$ an EL-domain.*

PROOF. As in the proof of Theorem 15.20 above, the easy observation that the equation $a^2 + db^2 = 2$ has no integral solutions implies that the element 2 is irreducible in R_d. Now, since (quite trivially) $-d$ is a square modulo 2, there exists $x \in \mathbb{Z}$ such that $2 \mid x^2 + d = (x + \sqrt{-d})(x - \sqrt{-d})$. But now, if R_d were an EL-domain, the irreducible element 2 would be prime and hence Euclid's Lemma would apply to show that $2 \mid x \pm \sqrt{-d}$, i.e., that $\frac{x}{2} + \frac{1}{2}\sqrt{-d} \in R_d$, which is a clear contradiction ($\frac{1}{2}$ is not an integer!). □

Theorem 15.19 has the following immediate consequence:

COROLLARY 15.22. *(Cohn,* [**?**, Thm. 2.1]*) For a domain R, the following are equivalent:*

(i) *Any two elements of R have a greatest common divisor.*
(ii) *Any two elements of R have a least common multiple.*

Thus we need not define an "LCM-domain": these are precisely the GCD domains.

6. Polynomial rings over UFDs

Our goal in this section to show that if R is a UFD, then a polynomial ring in any number (possibly infinite) of indeterminates is again a UFD. This result generalizes a familiar fact from undergraduate algebra: if k is a field, $k[t]$ is a UFD. The corresponding fact that polynomials in $k[t_1, \ldots, t_n]$ factor uniquely into irreducibles is equally basic and important, and arguably underemphasized at the pre-graduate level (including high school, where factorizations of polynomials in at least two variables certainly do arise).

If we can establish that R a UFD implies $R[t]$ a UFD, then an evident induction argument using $R[t_1, \ldots, t_n, t_{n+1}] = R[t_1, \ldots, t_n][t_{n+1}]$ gives us the result for polynomials in finitely many indeterminates over a UFD. It is then straightforward to deduce the case for an arbitrary set of indeterminates.

There are several ways to prove the univariate case. Probably the most famous is via Gauss's Lemma. For this we need some preliminary terminology.

Let R be a domain, and consider a nonzero polynomial

$$f = a_n t^n + \ldots + a_1 t + a_0 \in R[t].$$

We say f is **primitive** if $x \in R$, $x \mid a_i$ for all i implies $x \in R^\times$. In a GCD-domain, this is equivalent to $\gcd(a_1, \ldots, a_n) = 1$. In a PID, this is equivalent to $\langle a_0, \ldots, a_n \rangle = R$. For a general domain, this latter condition is considerably stronger: e.g. the polynomial $xt + y \in k[x, y][t]$ is primitive but the coefficients do not generate the unit ideal. Let us call this latter – usually too strong condition – **naively primitive**.

PROPOSITION 15.23. *Let R be a domain, and $f, g \in R[t]$ be naively primitive. Then fg is naively primitive.*

PROOF. We go by contraposition: suppose that fg is *not* naively primitive, so there is a maximal ideal $\mathfrak{m}$ of R such that $f, g \in \mathfrak{m}[t]$. For $h \in R[t]$, write $\overline{h}$ for its image in the quotient ring $R[t]/\mathfrak{m}[t] = R/\mathfrak{m}[t]$, which is a domain. Then we have

$$\overline{f}\,\overline{g} = \overline{fg} = 0,$$

so at least one of $\overline{f}, \overline{g}$ is 0, and thus at least one of f, g is not naively primitive. □

If R is a GCD-domain and $0 \neq f \in R[t]$, we define the **content** $c(f)$ of f to be the gcd of the coefficients of f, which we view as a principal ideal of R, but by a slight abuse of notation we will often write $c(f) = a$ to mean that a is a generator of this ideal. Thus a polynomial is primitive if and only if $c(f) = 1$.

EXERCISE 15.12. *Let R be a GCD-domain and $0 \neq f \in R[t]$.*

a) *Show: f factors as cf_1, where f_1 is primitive and $c(f) = c$.*
b) *Let $a \in R^\bullet$. Show: $c(af) = ac(f)$.*

THEOREM 15.24 (Gauss's Lemma). *Let R be a GCD-domain. If $f, g \in R[t]$ are nonzero polynomials, we have $c(fg) = c(f)c(g)$.*

If we assume the stronger hypothesis that R is a UFD, we can give a very transparent proof along the lines of that of Proposition 15.23 above. Since this special case may be sufficient for the needs of many readers, we will give this simpler proof first, followed by the proof in the general case.

PROOF. (Classical proof for UFDs) The factorization $f = cf_1$ of Exercise 15.12 reduces us to the following special case: if f and g are primitive, then so is fg. Suppose that fg is not primitive, i.e., there exists a nonzero nonunit x which divides all of the coefficients of fg. Since R is a UFD, we may choose a prime element $\pi \mid x$. Now we may argue exactly as in the proof of Proposition 15.23: $(R/(\pi)[t]$ is a domain, $\overline{f}$ and $\overline{g}$ are nonzero, but $\overline{f}\overline{g} = \overline{fg} = 0$, a contradiction. □

The proof of the general case uses the GCD identities of Proposition 15.10.

PROOF. (Haible) As above, we may assume that $f = a_n t^n + \ldots + a_1 t + a_0, g = b_m t^m + \ldots + b_1 t + b_0 \in R[t]$ are both primitive, and we wish to show that $fg = c_{m+n}t^{m+n} + \ldots + c_1 t + c_0$ is primitive. We go by induction on n. Since a primitive polynomial of degree 0 is simply a unit in R, the cases $m = 0$ and $n = 0$ are both trivial; therefore the base case $m + n = 0$ is doubly so. So assume $m, n > 0$. By Proposition 15.10, we have

$$c(fg) = \gcd(c_{n+m}, \ldots, c_0) =$$

$$\gcd(a_n b_m, \gcd(c_{n+m-1}, \ldots, c_0)) \mid \gcd(a_n, \gcd(c_{n+m-1}, \ldots, c_0)) \cdot \gcd(b_m, \gcd(c_{n+m-1}, \ldots, c_0)).$$

Now

$$\gcd(a_n, \gcd(c_{n+m-1}, \ldots, c_0)) = \gcd(a_n, c_{n+m-1}, \ldots, c_0)$$
$$= \gcd(a_n, c_{n+m-1} - a_n b_{m-1}, \ldots, c_n - a_n b_0, c_{n-1}, \ldots, c_0)$$
$$= \gcd(a_n, c((f - a_n t^n)g).$$

Our induction hypothesis gives $c((f - a_n t^n)g) = c(f - a_n t^n)c(g) = c(f - a_n t^n)$, so

$$\gcd(a_n, c_{n+m-1} - a_n b_{m-1}, \ldots, c_n - a_n b_0, c_{n-1}, \ldots, c_0) = \gcd(a_n, c(f - a_n t^n)) = c(f) = 1.$$

Similarly we have $\gcd(b_m, \gcd(c_{n+m-1}, \ldots, c_0)) = 1$, so $c(fg) = 1$. □

COROLLARY 15.25. *Let R be a GCD-domain with fraction field K, and let $f \in R[t]$ be a polynomial of positive degree.*

a) *The following are equivalent:*
   (i) *f is irreducible in $R[t]$.*
   (ii) *f is primitive and irreducible in $K[t]$.*

b) *The following are equivalent:*
   (i) *f is reducible in $K[t]$.*
   (ii) *There are $g, h \in R[t]$ such that $\deg(g), \deg(h) < \deg(f)$ and $f = gh$.*

PROOF. a) (i) $\implies$ (ii): Suppose that f is irreducible in $R[t]$. If f is not primitive, then the factorization $f = cf_1$ of Exercise 15.12a) shows that f is reducible. Now suppose that f is reducible in $K[t]$: i.e., it is a product of two polynomials of smaller degree. If both polynomials have coefficients in R, we have a contradiction. Otherwise we can multiply by $a \in R^\bullet$ to get a factorization

$$af = gh \text{ with } g, h \in R[t],$$

and uising Exercise 15.12a) we may write

$$af = c_f c_g g_1 h_1$$

with $c_f, c_g \in R^\bullet$ and $g_1, h_1 \in R[t]$ primitive polynomials. By Gauss's Lemma, $g_1 h_1$ is primitive, so taking contents of both sides gives

$$(a) = (c_f c_g).$$

Thus $\frac{c_f c_g}{a} \in R^\times$ and the factorization

$$f = (\frac{c_f c_g}{a} g_1) h_1$$

shows that f is reducible.
(ii) $\implies$ (i) is similar but much simpler and left to the reader.
b) That (ii) $\implies$ (i) is obvious, so assume (i). Because we can factor out the content, it is no loss of generality to assume that f is primitive. Let $f = g_1 h_1$ with $g_1, h_1 \in K[t]$ and $\deg(g_1), \deg(h_1) < \deg(f)$. Because R is a GCD-domain, we may write $g = \frac{\tilde{g}}{d_1}$, $h = \frac{\tilde{h}}{d_2}$ with $\tilde{g}, \tilde{h} \in R[t]$ primitive. Then we have $d_1 d_2 f = \tilde{g}\tilde{h}$, and equating contents gives $(d_1 d_2) = (1)$, so $d_1, d_2 \in R^\times$ and thus the factorization $f = gh$ has the properties we seek. □

We now give Gauss's proof that a univariate polynomial ring over a UFD is a UFD.

THEOREM 15.26. *If R is a UFD, so is $R[t]$.*

PROOF. Let K be the fraction field of R, and let $f \in R[t]^\bullet$. We know that $K[t]$ is a PID hence a UFD, so we get a factorization

$$f = c g_1 \cdots g_r,$$

with $c \in R$ and each $g_i \in R[t]$ is primitive and irreducible. Then factoring c into irreducibles gives an irreducible factorization of f. If we had another irreducible factorization $f = d h_1 \cdots h_s$, then unique factorization in $K[t]$ gives that we have $r = s$ and after permuting the factors have $g_i = u_i h_i$ for all i, where $u_i \in K^\times$. Since both g_i and h_i are primitive, we must have $u_i \in R^\times$, whence the uniqueness of the factorization. □

This proof relies on knowing that $K[t]$ is a UFD, which of course follows from the fact that polynomial division gives a Euclidean algorithm, as one learns in an undergraduate course. This is of course an adaptation of the proof that the ring $\mathbb{Z}$ is a UFD (the **Fundamental Theorem of Arithmetic**) essentially due to Euclid.

It is interesting to find alternate routes to such basic and important results.

THEOREM 15.27. *Let R be a domain with fraction field K.*

a) *If R is an ACCP-domain, so is $R[t]$.*
b) *If R is a GCD-domain, so is $R[t]$.*
c) *Thus, once again, if R is a UFD, so is $R[t]$.*

PROOF. a) In an infinite ascending chain $\{(P_i)\}$ of principal ideals of $R[t]$, $\deg P_i$ is a descending chain of non-negative integers, hence eventually constant. Therefore for sufficiently large n we have $P_n = a_n P_{n+1}$ with $a_n \in R$ and $(a_{n+1}) \supset (a_n)$. Since R is an ACCP domain, we have $(a_n) = (a_{n+1})$ for sufficiently large n, hence also $(P_n) = (P_{n+1})$ for sufficiently large n.
b) (Haible, [**Ha94**]) Let $f, g \in R[t]$. We may assume that $fg \neq 0$. As usual, write $f = c(f)\tilde{f}$ and $g = c(g)\tilde{g}$. Since $K[t]$ is a PID, may take the gcd of $\tilde{f}$ and $\tilde{g}$ in $K[t]$, say $\tilde{d}$. The choice of $\tilde{d}$ is unique only up to an element of $K^\times$, so by choosing the unit appropriately we may assume that $\tilde{d}$ lies in $R[t]$ and is primitive. We put

$d = \gcd(c(f), c(g)))\tilde{d}$.

Step 1: We claim that $\tilde{d}$ is a gcd of $\tilde{f}$ and $\tilde{g}$ in $R[t]$. Since $\tilde{d} \mid f$ in $K[t]$, we may write $\frac{\tilde{f}}{\tilde{d}} = \frac{a}{b}q$ with $a, b \in R\backslash\{0\}$ and $q \in R[t]$ primitive. Since $b\tilde{f} = a\tilde{d}$, we have $(b) = c(b\tilde{f}) = c(a\tilde{d}) = (a)$, i.e., $\frac{b}{a} \in R^\times$ and thus $\tilde{d} \mid \tilde{f}$ in $R[t]$. Similarly $\tilde{d} \mid \tilde{g}$. Moreover, sice $\tilde{d} \in \tilde{f}K[t] + \tilde{g}K[t]$, there exist $u, v \in R[t]$ and $c \in R\backslash\{0\}$ with $c\tilde{d} = u\tilde{f} + v\tilde{g}$. Suppose $h \in R[t]$ divides both $\tilde{f}$ and $\tilde{g}$. Then $h \mid c\tilde{d}$, and $c(h) \mid c(\tilde{f}) = (1)$. Writing $\frac{cd}{h} = \frac{a}{b}q$ with $q \in R[t]$ primitive, and equating contents in $bc\tilde{d} = ahq$, we get $(bc) = (a)$, hence $\frac{\tilde{d}}{h} = \frac{ab}{c}q \in R[t]$, so $h \mid \tilde{d}$.

Step 2: We claim that d is a gcd of f and g in $R[t]$. Certainly we have

$$(d) = (\gcd(c(f), c(g)\tilde{d}) \mid (c(f)\tilde{f}) = (f),$$

so $d \mid f$. Similarly $d \mid g$. Conversely, let $h \in R[t]$ divide f and g. Write $h = c(h)\tilde{h}$ for $\tilde{h} \in R[t]$ primitive. From $h \mid f$ it follows that $c(h) \mid c(f)$ and thus $\tilde{h} \mid \tilde{f}$. Similarly $h \mid f$ so $\tilde{h} \mid \tilde{g}$. Thus $c(h) \mid \gcd(c(f), c(g))$, $\tilde{h} \mid \tilde{d}$ and thus finally $h \mid d$.

c) If R is a GCD domain and an ACCP domain, it is also an atomic EL-domain, hence a UFD by Theorem 15.8. □

Lindemann [**Li33**] and Zermelo [**Ze34**] (independently) gave (similar) striking proofs of the Fundamental Theorem of Arithmetic avoiding all lemmas and packaging the Euclidean division into a single inductive argument. Later several authors have recorded analogous proofs of Gauss's Theorem (Theorem 15.26): the earliest instance we are aware of in the literature is due to S. Borofsky [**Bo50**]. We give a third, "lemmaless" proof of Theorem 15.26 here.

Proof. It suffices to show that $R[t]$ is an ACCP domain and an EL-domain. By Theorem 15.27a), $R[t]$ is an ACCP domain. Now, seeking a contradiction, we suppose that $R[t]$ is not an EL-domain. Among the set of all elements in $R[t]$ admitting inequivalent irreducible factorizations, let p be one of minimal degree. We may assume

$$p = f_1 \cdots f_r = g_1 \cdots g_s,$$

where for all i, j, $(f_i) \neq (g_j)$ and

$$m = \deg f_1 \geqslant \deg f_2 \geqslant \ldots \geqslant \deg f_r,$$

$$n = \deg g_1 \geqslant \deg g_2 \geqslant \ldots \geqslant \deg g_s,$$

with $n \geqslant m > 0$. Suppose the leading coefficient of f_1 (resp. g_1) is a (resp. b). Put

$$q = ap - bf_1x^{n-m}g_2 \cdots g_s = f_1(af_2 \cdots f_r - bx^{n-m}g_2 \cdots g_s) = (ag_1 - bf_1x^{n-m})g_2 \cdots g_s.$$

Thus $q = 0$ implies $ag_1 = bf_1x^{n-m}$. If, however, $q \neq 0$, then

$$\deg(ag_1 - bf_1x^{n-m}) < \deg g_1,$$

hence $\deg q < \deg p$ and q has a unique factorization into irreducibles, certainly including $g_2, \cdots, g_s$ and f_1. But then f_1 must be a factor of $ag_1 - bf_1x^{n-m}$ and thus also of ag_1. Either way $ag_1 = f_1h$ for some $h \in R[t]$. Because a is constant, it can be factored into a product of prime elements $a = p_1 \cdots p_r$ of R, each of which remains prime in $R[t]$: $R[t]/(p_i) \cong R/(p_i)[t]$ is a domain. Since each p_i is constant and f_1 is irreducible, we have $p_i \nmid f_1$ for all i and it follows that $h = ah_2$. So $ag_1 = f_1ah_2$, or $g_1 = f_1h_2$, contradiction. □

THEOREM 15.28. *Let R be a domain and let $\{t_i\}_{i \in I}$ be any set of indeterminates. We will write $R[\mathbf{t}]_I$ for the polynomial ring $R[\{t_i\}_{i \in I}$. Then:*

a) *R is an ACCP-domain $\iff$ $R[\mathbf{t}]_I$ is an ACCP-domain.*
b) *R is a GCD-domain $\iff$ $R[\mathbf{t}]_I$ is a GCD-domain.*
c) *R is a UFD $\iff$ $R[\mathbf{t}]_I$ is a UFD.*

PROOF. The following simple facts will be useful to us: let $\{t_j\}_{j \in J}$ be a set of indeterminates, let R be a domain, let $f, g \in R$. Then f divides g in R if and only if f divides g in $R[\mathbf{t}]_J$. The implication $\implies$ holds for any extension of domains. Conversely, suppose that there is $P \in R[\mathbf{t}]_J$ such that $g = fP$. Then

$$0 = \deg(g) = \deg(fP) = \deg(f) + \deg(P) = \deg(P),$$

so $\deg P = 0$, i.e., $P \in R$. Similarly, if $f, g \in R[\mathbf{t}]_J^\bullet$ such that f divides g and moreover g lies in R, then the same degree considerations show that f lies in R.

From this it follows: (i) for $f \in R$ we have $f \in R^\times \iff f \in R[\mathbf{t}]_J^\times$. (ii) For a nonzero nonunit $f \in R$, we have that f is irreducible as an element of R if and only if f is irreducible as an element of $R[\mathbf{t}]_J$. (iii) For $f, g \in R^\bullet$, f and g have a GCD in R if and only if they have a GCD in $R[]_J$. (iv) If $\{a_n\}_{n=1}^\infty$ is a sequence in R then $\{a_n R\}_{n=1}^\infty$ is a strictly ascending chain of principal ideals in R if and only if $\{a_n R[\mathbf{t}]_J\}_{n=1}^\infty$ is a strictly ascending chain of prinicpal ideals in $R[\mathbf{t}]_J$.

Thus if $R[\mathbf{t}]_I$ is an ACCP-domain then so is R, and if $R[\mathbf{t}]_I$ is a GCD-domain then so is R. Since a UFD is precisely a domain that is an ACCP-domain and a GCD-domain, we also get that if $R[\mathbf{t}]_I$ is a UFD, then so is R.

Suppose that R is an ACCP-domain. Theorem 15.27a) asserts that $R[t]$ is an ACCP-domain. The proof works verbatim to show that $R[\mathbf{t}]_I$ is an ACCP-domain. Alternately, using Theorem 15.27a) we get that a polynomial ring over R in any finite number of indeterminates is an ACCP-domain. If $R[\mathbf{t}]_I$ is not an ACCP-domain, then we have an infinite strictly ascending chain $(f_1) \subsetneq (f_2) \subsetneq \ldots$ of principal ideals of $R[\mathbf{t}]_I$. Let J be a finite subset of I such that $f_1 \in R[\mathbf{t}]_J$. For $n \in \mathbb{Z}^+$ we have that f_n strictly divides f_1, so each f_n lies in $R[\mathbf{t}]_J$ and strictly divides f_1 in $R[\mathbf{t}]_J$. Thus $R[\mathbf{t}]_J$ does not satisfy ACCP, contradiction. This completes the proof of part a).

Suppose that R is a GCD-domain and let $f, g \in R[\mathbf{t}]_I$. There is a finite subset J of I such that f and g lie in $R[\mathbf{t}]_J$. By induction on Theorem 15.27b), the ring $R[\mathbf{t}]_J$ is a GCD-domain, so $h = \gcd(f, g)$ exists in $R[\mathbf{t}]_J$. Since $R[\mathbf{t}]_I = (R[\mathbf{t}]_J)[\mathbf{t}]_{I \setminus J}$, it follows that h is also a GCD of f and g in $R[\mathbf{t}]_I$. This completes the proof of part b), and part c) is immediate from parts a) and b). □

In particular, for any field k and any set I, the polynomial ring $k[\mathbf{t}]_I$ is a UFD. By totally ordering the elements of I and defining for $i \in I$ the ideal $\mathfrak{p}_i$ to be the ideal generated by the indeterminates t_j with $j < i$, we get a chain $\{\mathfrak{p}_i\}_{i \in I}$ of prime ideals in $k[\mathbf{t}]_I$, so $\operatorname{carddim} k[\mathbf{t}]_I \geq \#I$. Thus not only are there UFDs that are not Noetherian, but there are UFDs of arbitrarily large cardinal Krull dimension.

EXERCISE 15.13. *Let $f : R \to S$ be a homomorphism of domains.*

a) *Find examples in which:*
   (i) *f is injective, S is an ACCP-domain, and R is not an ACCP-domain.*
   (ii) *f is surjective, S is an ACCP-domain, and R is not an ACCP-domain.*

(iii) *f is surjective, R is an ACCP-domain, and S is not an ACCP-domain.*
(iv) *f is injective, R is an ACCP-domain, and S is not an ACCP-domain.*

b) *Suppose that is injective and unit-faithful (for $x \in R$ we have $x \in R^\times \iff f(x) \in S^\times$). Show: if S is an ACCP-domain, then R is an ACCP-domain.*

c) *Let I be a set, and for $i \in I$ let $f_i : R \to S_i$ be a unit-faithful homomorphism to an ACCP-domain S_i. Suppose also that for each $x \in R^\bullet$ there is $i \in I$ such that $f_i(x) \neq 0$. Show: R is an ACCP-domain.*[2]

EXERCISE 15.14. *Let $(I, \leqslant)$ be a directed set, and let $\{R_i, \varphi_{ij}\}$ be a directed system of UFDs with injective transition maps. Let $R = \varinjlim R_i$ be the direct limit, which is a domain. We may identify each R_i with a subring of R, and then $R = \bigcup_{i \in I} R_i$.*

a) *Show: R need* not *be a UFD. (Hint: cf. Exercise 8.44.)*

b) *Suppose: for all $i \leqslant j$ and all prime elements p_i of R_i, the element $\varphi_{ij}(p_i)$ is a prime element of R_j. Show: R is a UFD.*

c) *Let R be a domain, let I be a set, and let $R[\mathbf{t}]_I$ be a polynomial ring in indeterminates t_i indexed by $i \in I$. Show: if p is a prime element of R, then p is a prime element of $R[\mathbf{t}]_I$.*
(Hint: $R[\mathbf{t}]_I/(p) \cong R/(p)[\mathbf{t}]_I$.)

d) *Use parts b) and c) to give a different proof (still using Theorem 15.26) that if R is a UFD, then $R[\mathbf{t}]_I$ is a UFD.*

EXERCISE 15.15. *Let R be a domain, let I be a set, and let $R[\mathbf{t}]_I$ be a polynomial ring in indeterminates t_i indexed by $i \in I$.*

a) *Show: if $R[\mathbf{t}]_I$ is atomic, then so is R.*

b) *Show: if $R[\mathbf{t}]_I$ is an EL-domain, then so is R.*

The conspiciuously missing converses of the previous exercise are addressed by the following results, which we quote without proof.

THEOREM 15.29.

a) *(Roitman [**Ro93**]) There is an integrally closed atomic domain R such that $R[t]$ is not atomic.*

b) *(Anderson-Quintero-Zafrullah) There is an EL-domain R such that $R[t]$ is not an EL-domain.*

7. Application: the Schönemann-Eisenstein Criterion

The most famous criterion for irreducibility of univariate polynomials is named after Ferdinand Eisenstein [**Ei50**]. However, the version for polynomials over $\mathbb{Z}$ was proven several years earlier by Theodor Schönemann [**Sc45**], [**Sc46**]. Few anglophone texts have associated Schönemann's name with this result, and his contribution might have been in real danger of being forgotten were it not for the beautiful recent article of Cox [**Co11**] on the early history of this result.

Nowadays it is common to state and prove a version of Eisenstein's criterion with respect to a prime ideal in a UFD. We give a slight generalization:

[2]Notice that this is a generalization of part b).

THEOREM 15.30. *(Schönemann-Eisenstein Criterion) Let R be a domain with fraction field K, and let $f(t) = a_d t^d + \ldots + a_1 t + a_0 \in R[t]$. Suppose that there exists a prime ideal $\mathfrak{p}$ of R such that $a_d \notin \mathfrak{p}$, $a_i \in \mathfrak{p}$ for all $0 \leqslant i < d$ and $a_0 \notin \mathfrak{p}^2$.*

a) *If f is primitive, then f is irreducible over $R[t]$.*

b) *If R is a GCD-domain, then f is irreducible over $K[t]$.*

PROOF. a) Suppose to the contrary that f is primitive and reducible over $R[t]$: i.e., there exists a factorization $f = gh$ with $g(t) = b_m t^m + \ldots + b_1 t + b_0$, $h(t) = c_n t^m + \ldots + c_1 t + c_0$, $\deg(g), \deg(h) < \deg(f)$ and $b_m c_n \neq 0$. Since $a_0 = b_0 c_0 \in \mathfrak{p} \backslash \mathfrak{p}^2$, it follows that exactly one of b_0, c_0 lies in $\mathfrak{p}$: say it is c_0 and not b_0. Moreover, since $a_d = b_m c_n \notin \mathfrak{p}$, $c_n \notin \mathfrak{p}$. Let k be the least index such that $c_k \notin \mathfrak{p}$, so $0 < k \leqslant n$. Then $b_0 c_k = a_k - (b_1 c_{k-1} + \ldots + b_k c_0) \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime, it follows that at least one of b_0, c_k lies in $\mathfrak{p}$, a contradiction.
b) Suppose R is a GCD-domain and (seeking a contradiction) that f is reducible over $K[t]$. By Corollary 15.25b), we may write $f = gh$ with $g, h \in R[t]$ and $\deg(g), \deg(h) < \deg(f)$. Then the proof of part a) goes gives a contradiction. □

COROLLARY 15.31. *Let R be a GCD-domain containing a prime element π. Then the fraction field K of R is not separably closed.*

PROOF. The element π is prime if and only if the principal ideal $\mathfrak{p} = (\pi)$ is a nonzero prime ideal. Then $\pi \notin \mathfrak{p}^2$, so for all $n > 1$, $P_n(t) = t^n - \pi$ is Eisenstein with respect to $\mathfrak{p}$ and hence irreducible in $K[t]$. Choosing n to be prime to the characteristic of K yields a degree n separable field extension $L_n := K[t]/(P_n)$. □

8. Application: Determination of $\operatorname{Spec} R[t]$ for a PID R

Let R be a PID. We wish to determine all prime ideals of the ring $R[t]$. Let us begin with some general structural considerations. First, R is a one-dimensional Noetherian UFD; so by Theorems 8.38, 15.27 and 8.60, $R[t]$ is a two-dimensional Noetherian UFD. Being a UFD, its height one ideals are all principal. Since it has dimension two, every nonprincipal prime ideal is maximal. Therefore it comes down to finding all the maximal ideals.

It turns out that we can proceed without using the Dimension Theorem, following [**R**, pp. 22-23]. Namely, let $\mathcal{P}$ be a nonzero prime ideal of $R[t]$. We assume – only! – that $\mathcal{P}$ is not principal. By Theorem 15.1, we are entitled to a prime element f_1 of $\mathcal{P}$. Since $\mathcal{P} \neq (f_1)$, let $f_2 \in \mathcal{P} \backslash (f_1)$. Then $\gcd(f_1, f_2) = 1$: since $\gcd(f_1, f_2) \mid f_1$, the only other possibility is $(\gcd(f_1, f_2)) = (f_1)$, so $f_1 \mid f_2$ and $f_2 \in (f_1)$, contradiction.

FIRST CLAIM Let K be the fraction field of R. The elements f_1 and f_2 are also relatively prime in the GCD-domain $K[t]$. Indeed, suppose that $f_1 = h g_1$, $f_2 = h g_2$ with $h, g_1, g_2 \in K[t]$ and h a nonunit. By Gauss' Lemma, we may write $h = a h_0$, $g_1 = b_1 \gamma_1$, $g_2 = b_2 \gamma_2$ with $a_1, b_1, b_2 \in K$ and h_0, γ_1, γ_2 primitive elements of $R[t]$. Again by Gauss' Lemma, $h_0 \gamma_1$ and $h_0 \gamma_2$ are also primitive, so $f_1 = h g_1 = (a b_1)(h_0 \gamma_1) \in R[t]$, which implies that $a b_1 \in R$. Similarly, $a b_2 \in R$, so h_0 is a nonunit of $R[t]$ which divides both f_1 and f_2, contradiction.

Let $\mathcal{M} := \langle f_1, f_2 \rangle$, and put $\mathfrak{m} = \mathcal{M} \cap R$. It remains to show that, as the notation suggests, $\mathcal{M}$ is a maximal ideal of $R[t]$ and $\mathfrak{m}$ is a maximal ideal of R.

SECOND CLAIM $\mathfrak{m} \neq 0$. Since $K[t]$ is a PID and f_1, f_2 are relatively prime in

$K[t]$, there exist $a, b \in K[t]$ such that $af_1 + bf_2 = 1$. Let $0 \neq c \in R$ be an element which is divisible by the denominator of each coefficient of a and b: then $(ca)f_1 + (cb)f_2 = c$ with $ca, cb \in R$, so that $c \in \mathfrak{m}$.

Now put $\mathfrak{p} = \mathcal{P} \cap R$, so $\mathfrak{p} = (p)$ is a prime ideal of the PID R. Moreover,

$$\mathfrak{p} = \mathcal{P} \cap R \supset \mathcal{M} \cap R = \mathfrak{m} \supsetneq 0,$$

so $\mathfrak{p}$ is maximal. Since $\mathcal{P} \supset \mathfrak{p}$, $\mathcal{P}$ corresponds to a prime ideal in $R[t]/\mathfrak{p}R[t] = (R/\mathfrak{p})[t]$, a PID. Therefore $\mathcal{P}$ is generated by $p \in \mathfrak{p}$ and an element $f \in R[t]$ whose image in $(R/\mathfrak{p})[t]$ is irreducible.

We therefore have proved:

THEOREM 15.32. *Let R be a PID, and let $\mathcal{P} \in \operatorname{Spec} R[t]$. Exactly one of the following holds:*

(0) *$\mathcal{P}$ has height 0: $\mathcal{P} = (0)$.*
(i) *$\mathcal{P}$ has height one: $\mathcal{P} = (f)$, for a prime element $f \in R[t]$.*
(ii) *$\mathcal{P}$ has height two: $\mathcal{P} = \langle p, f \rangle$, where p is a prime element of R and $f \in R[t]$ is an element whose image in $(R/p)[t]$ is irreducible. Moreover both $\mathcal{P}$ and $\mathfrak{p} := \mathcal{P} \cap R$ are maximal, and $[R[t]/\mathcal{P} : R/\mathfrak{p}] < \infty$.*

EXERCISE 15.16.

a) *Suppose R has only finitely prime ideals, so is not a Hilbert-Jacobson ring. By Theorem 12.19, there is $\mathfrak{m} \in \operatorname{MaxSpec} R[t]$ such that $\mathfrak{m} \cap R = (0)$. Find one, and explain where $\mathfrak{m}$ fits in to the classification of Theorem 15.32.*
b) *(Zanello [**Za04**]) Deduce: for a PID R, the following are equivalent:*
   (i) *R has infinitely many prime ideals.*
   (ii) *Every maximal ideal of $R[t]$ has height two.*

9. The Weierstrass-Bourbaki Preparation Theorem

In this section we will discuss a result involving complete local rings, despite the fact that (unlike most commutative algebra texts) we do not discuss the completion of a ring with respect to an ideal. The situation is (more than) analogous to that of discussing complete metric spaces but not the completion of a metric space.

Still we need to define and briefly discuss I-adic topologies, so here goes: let R be a ring, and let I be an ideal of R. Then the **I-adic topology on R** is the topology for which for $x \in R$, a neighborhood base at x is given by $\{x + I^n \mid n \in \mathbb{N}\}$. In more words, the neighborhoods of 0 in the I-adic topology are precisely the subsets containing some power of I, and this topology is "homogeneous" in the sense that for all $x \in R$, a subset $U \subseteq R$ is a neighborhood of x if and only if $-x + U$ is a neighborhood of 0. The I-adic topology makes R into a topological ring: that is,

$$+ : R \times R \to R, - : R \to R \text{ by } x \mapsto -x, \cdot : R \times R \to R$$

are all continuous. Moreover this topology is manifestly first-countable, since it is defined by a countable neighborhood base at each point, hence it is a sequential space in the sense of [**Cl-GT**, §5.2.2].

EXERCISE 15.17. *Let I be an ideal of R.*

a) *Show: the I-adic topology on R is indiscrete (i.e., the only nonempty open subset of R is R itself) if and only if $I = R$.*
b) *Show: the I-adic topology on R is discrete if and only if I is nilpotent.*

LEMMA 15.33. *Let I be an ideal of R, and let τ be the I-adic topology on R. The following are equivalent:*

(i) *The space (R, τ) is Hausdorff.*
(ii) *The space (R, τ) is separated: that is, for all $x \in R$, $\{x\}$ is closed.*
(iii) *The space (R, τ) is Kolmogorov: for all $x, y \in R$, if x and y have the same open neighborhoods, then $x = y$.*
(iv) *We have $\bigcap_{n=1}^{\infty} I^n = \{0\}$.*

*When these equivalent conditions hold, we say that R is **I-adically separated**.*

PROOF. (i) $\implies$ (ii) $\implies$ (iii) holds for all topological spaces.
(iii) $\implies$ (i) holds in any topological group G. We show this by arguing the contrapositive: suppose that G is not Hausdorff. Then the diagonal $\Delta := \{(x, x) \mid x \in G\}$ is not closed in G. On the other hand, the map $M : G \times G \to G$ by $(g_1, g_2) \mapsto g_1^{-1} g_2$ is continuous, and $\Delta = M^{-1}(\{e\})$, so it follows that $\{e\}$ is not closed, so G is not separated; that is, the closed normal subgroup $K := \overline{\{e\}}$ is nontrivial. In any topological space, the closure of a point consists of the intersection of all neighborhoods of that point: indeed, for x in a topological space X, a net $x_\bullet : I \to X$ such that $x_i = x$ for all $i \in I$ converges to $y \in X$ if and only if y lies in every open neighborhood of x. So the subgroup K is the set of points of G having the same neighborhoods as the identity e, and thus the nontriviality of K means that G is not Kolmogorov.
(iii) $\iff$ (iv): We just saw that a topological group G is Kolmogorov if and only if the intersection of all neighborhoods of e is precisely $\{e\}$. For our topological group (R, τ), this condition is precisely that $\bigcap_{n=1}^{\infty} I^n = \{0\}$. □

Every topological space X has a Kolmogorov quotient $\overline{X}$: this a topological space equipped with a continuous map $q : X \to \overline{X}$ that is universal for continuous maps into a Kolmogorov space. More explicitly, $q : X \to \tilde{X}$ is the quotient under the equivalence relation $\sim$ of topological indistinguishability: $x \sim y$ if and only if x and y have precisely the same neighborhoods. Thus for a topological group G, if $K := \overline{\{e\}}$, then its Kolmogorov quotient is the quotient topological group $\overline{G} := G/K$. In particular: R is not I-adically separated, we may replace (R, I) with $(\overline{R}, \overline{I})$ with $R := R + \bigcap_{n=1}^{\infty} I^n$ and $\overline{I} = I + \bigcap_{n=1}^{\infty} I^n$, and then $\overline{R}$ is $\overline{I}$-adically separated.

However, being I-adically separated is a mild condition at least when R is Noetherian. Indeed, the Krull Intersection Theorem immediately implies:

COROLLARY 15.34. *Let I be a proper ideal of the Noetherian ring R. If either R is a domain or I is contained in the Jacobson radical $J(R)$ of R, then the I-adic topology on R is separated.*

In fact, the true business of this section concerns a Noetherian local ring $(R, \mathfrak{m})$, which as above will always be $\mathfrak{m}$-adically separated.

Let I be an ideal of R. The I-adic topology of course allows us to define convergence of sequences in R. We cannot of course define Cauchy sequences in an arbitrary topological space. The most familiar setting in which Cauchy sequences can be defined is that of metric spaces. We can also define Cauchy sequences in

any commutative topological group $(G,+)$, as follows: we say that $\{x_n\}$ is Cauchy if and only if for every open neighborhood U of 0, there is $N \in \mathbb{Z}^+$ such that for all $m,n \geqslant N$ we have $x_m - x_n \in U$. As usual, it is easy to see that convergent sequences are Cauchy, and the more interesting question is whether the converse holds. In a commutative topological group $(G,+)$ we can also define convergence (resp. Cauchyness) of infinite series $\sum_{n=1}^{\infty} x_n$ just be requiring the sequence of partial sums to be convergent (resp. Cauchy).

In the case of the I-adic topology on R, this simplifies to: the squence $\{x_n\}$ is Cauchy if for all $E \in \mathbb{Z}^+$ there is $N \in \mathbb{Z}^+$ such that for all $m,n \geqslant N$ we have $x_m - x_n \in I^E$. Moreover, the condition of Cauchyness of an infinite series turns out to be remarkably simple in this context:

LEMMA 15.35. *Let I be a proper ideal of the ring R. For an infinite series $\sum_n x_n$ in R, the following are equivalent:*

(i) *The series $\sum_n x_n$ is Cauchy in the I-adic topology.*
(ii) *In the I-adic topology, we have $x_n \to 0$.*

PROOF. (i) $\implies$ (ii): This holds in any commutative topological group $(G,+)$, using the familiar argument from freshman calculus: let $S_n := \sum_{k=1}^{n} x_k$. If the sequence $\{S_n\}$ is Cauchy, then in particular, for every open neighborhood U of 0, there is $N \in \mathbb{Z}^+$ such that for all $n \geqslant N$ we have $x_n = S_n - S_{n-1} \in U$. So $x_n \to 0$. (Of course the converse does not hold in every commutative topological group: e.g. it does not hold in $\mathbb{R}$!)
(ii) $\implies$ (i): Suppose $x_n \to 0$, and let $E \in \mathbb{Z}^+$. Then there is $N \in \mathbb{Z}^+$ such that for all $n \geqslant N$ we have $x_n \in I^E$. Let $m,n \geqslant N$; we may suppose that $m \geqslant n$. Then $S_m - S_n = x_{n+1} + \ldots + x_m \in I^E$, so the series $\sum_n x_n$ is Cauchy. □

This last result suggetss the presence of an ultrametric, which is very nearly the case. For a proper ideal I of R and $x,y \in R$, we can define $V(x,y)$ to be the least $n \in \mathbb{N}$ such that $x - y \notin I^n$ or ∞ if $x - y \in \bigcap_{n=1}^{\infty} I^n$. Then we can define

$$d : R \times R \to R,\ (x,y) \mapsto 2^{-V(x,y)}.$$

EXERCISE 15.18. *With notation as above:*

a) *Show: for all x,y,z, show: $d(x,z) \leqslant \max d(x,y), d(y,z)$.*
b) *Show: d is a metric on R if and only if R is I-adically separated.*
c) *Show: if R is I-adically separated, the I-adic topology is the topology induced by the ultrametric d.*

When R is not I-adically separated, the function d is what is called a *pseudo-metric*: it satisfies every property of a metric except we may have $d(x,y) = 0$ for $x \neq y$. A pseudo-metric that is not a metric also induces a topology, that is not Kolmogorov. It induces a metric on the Kolmogorov quotient, which is the quotient under the equivalence relation $x \sim y$ if and only if $d(x,y) = 0$.

For an ideal I of a ring R, we say that R is **I-adically complete** if in the I-adic pseudometric, every Cauchy sequence in convergent. When $(R,\mathfrak{m})$ is local ring, we say that R is **complete** if it is complete for the $\mathfrak{m}$-adic topology and **separated** if it is separated for the $\mathfrak{m}$-adic topology.

All of this is highly formal. To come back to earth, let k be a field, let $R := k[t]$, and let $I = (t)$. In this case t is a prime element of the PID $k[t]$, which gives rise to a valuation v_t on $k(t)$. For $x, y \in k[t]$ we have $V(x,y) = v_t(x-y)$ and the above metric is (one normalization of) the ultrametric induced by a discrete valuation. We find that a series $\sum_n f_n(t)$ is Cauchy if and only if for all $N \in \mathbb{Z}^+$, all but finitely many of the terms $f_n(t)$ are diviisble by t^N. So for instance $\sum_{n=0}^{\infty} t^n$ is Cauchy. If in the I-adic topology on $k[t]$ we have a convergent sequence $x_n \to x$, then for all $N \in \mathbb{Z}^+$ and all sufficiently large n we have $x_n - x$ is divisible by t^N. Equivalently, for all $d \geqslant 0$, for all sufficiently large n we have that the coefficient of t^d in x_n is equal to the coefficient of t^d in x. In the sequence of partial sums $\sum_{k=0}^{n} t^k$ indeed we have that for all d, the sequence of coefficients of t^d is eventually constant: indeed, all but finitely many of these coefficients are equal to 1. This however means that the series *does not* converge in $k[t]$, because it would have to converge to $1 + t + t^2 + \ldots + t^n + \ldots$, which is not a polynomial. This $k[t]$ is not complete for the t-adic topology.

This example suggests a clear remedy: instead of considering the t-adic valuation on $k[t]$, we consider the t-adic valuation on the formal power series ring $k[[t]]$, which is again a PID. Almost the same argument as above now shows that Cauchy sequences converge: again, being Cauchy means that for each $d \in \mathbb{N}$ the sequence of coefficients of t^d is eventually constant, say to c_d; then the Cauchy sequence converges to $\sum_{n=0}^{\infty} c_d t^d$. It is easy to see that $k[[t]]$ with the (t)-adic metric is the completion of $k[t]$ with the (t)-adic metric: that is, the map $k[t] \hookrightarrow k[[t]]$ is an isometric embedding with dense image.

PROPOSITION 15.36. *Let $(R, \mathfrak{m})$ be a local ring, let $N \in \mathbb{Z}^+$ and put $T := R[[t_1, \ldots, t_N]]$.*

a) *The ring T is local, with maximal ideal $\mathcal{M} := \langle \mathfrak{m}, t_1, \ldots, t_N \rangle$.*
b) *The ring T is Noetherian if and only if the ring R is Noetherian.*
c) *If R is $\mathfrak{m}$-adically complete, then T is $\mathcal{M}$-adically complete.*
d) *If R is $\mathfrak{m}$-adically separated, then T is $\mathcal{M}$-adically separated.*

EXERCISE 15.19. *Prove Proposition 10.*

With these preliminaries in place, we now come to the actual setup of this section. Let $(R, \mathfrak{m})$ be a local ring that is complete and separated for the $\mathfrak{m}$-adic topology (recall the latter is automatic if R is Noetherian), and put $T := R[[t]]$ and $\mathcal{M} := \langle \mathfrak{m}, t \rangle$. By Proposition 10 we have that $(T, \mathcal{M})$ is a complete, separated local ring that is Noetherian if and only if R is. Put $k := R/\mathfrak{m}$.

There is an evident map $T = R[[t]] \to k[[t]]$; namely we mod out by $\mathfrak{m}T$. For any power series $f = \sum_{n=0}^{\infty} a_n t^n \in T$, we define the **reduced series** $\overline{f} = \sum_{n=0}^{\infty} \overline{a_n} t^n \in k[[t]]$. We say that $f \in T$ is **regular** if $\overline{f} \neq 0$ – that is, if not all coefficients of f lie in $\mathfrak{m}$ – and if so we define the **order** $\operatorname{ord}(f)$ of f to be the least $n \in \mathbb{N}$ such that $a_n \notin \mathfrak{m}$. If f is not regular, we put $\operatorname{ord}(f) = \infty$. In other words, the order of a regular element f is the t-adic valuation of $\overline{f} \in k[[t]]$.

EXERCISE 15.20. *Let $f, g \in T$.*

a) *Show: $f \in T^\times$ if and only if $\operatorname{ord}(f) = 0$.*
b) *Show: $\operatorname{ord}(fg) = \operatorname{ord}(f) + \operatorname{ord}(g)$. Deduce that fg is regular if and only if f and g are both regular.*

c) *Show:* $\mathrm{ord}(f+g) \geqslant \min(\mathrm{ord}(f), \mathrm{ord}(g))$.
c) *Show: if* $\mathrm{ord}(g) < \mathrm{ord}(f)$, *then* $\mathrm{ord}(f+g) = \mathrm{ord}(g)$.

THEOREM 15.37 (Weierstrass-Bourbaki Division Theorem). *Let $f \in T$ be regular of order $s \geqslant 1$, and put $M := \langle 1, t, \ldots, t^{s-1} \rangle_R$. Then:*

a) *For all $g \in T$, there is unique $q \in T$ and $r \in M$ such that $g = qf + r$.*
b) *It follows that f is not a zero-divisor in T and that the R-module T/fT is free of rank s.*

PROOF. a) Step 1: Suppose that $q \in T$ is such that $qf \in M$. We CLAIM that $q = 0$. Suppose for the moment that this claim holds. Then, if we have $q_1, q_2 \in T$ and $r_1, r_2 \in M$ such that $q_1 f + r_1 = g = q_2 f + r_2$, then

$$(q_1 - q_2)f = (r_2 - r_1) \in M,$$

so the claim implies that $q_1 = q_2$ and that $r_1 = r_2$.
Now we prove the claim. Let us be more concrete: suppose $m_0, \ldots, m_{s-1} b_0, b_1, \ldots, b_n, \in A$ are such that

$$(\sum_{n=0}^{\infty} b_n t^n) f = m_0 + m_1 t + \ldots + m_{s-1} t^{s-1}. \tag{39}$$

We need to show that $b_n = 0$ for all n. Because A is separated, it suffices to show that $b_i \in \mathfrak{m}^n$ for all $i, n \in \mathbb{N}$. Inductively, we may assume that $b_i \in \mathfrak{m}^{n-1}$ for all i and that $b_i \in \mathfrak{m}^n$ for all $i < k$ and show that $b_k \in \mathfrak{m}^n$. For this, we write $f = \sum_{n=0}^{\infty} a_i t^i$ and equate coefficients of t^{s+k} in (39) to get:

$$(b_0 a_{s+k} + \ldots + b_{k-1} a_{s+1}) + b_k a_s + (b_{k+1} a_{s-1} + \ldots + b_{k+s} a_0) = 0. \tag{40}$$

In the above equation, each term in the first parenthesized group lies in $\mathfrak{m}^n$ because $b_i \in \mathfrak{m}^n$ for $i < k$ and every term in the second parenthesized group lies in $\mathfrak{m}^n$ because $b_i \in \mathfrak{m}^{n-1}$ for all i and $a_j \in \mathfrak{m}$ for $j < s$. Thus $b_k a_s \in\in \mathfrak{m}^n$, and because $a_s \in R^\times$ we get $b_k \in \mathfrak{m}^n$, completing the induction.
Step 2: We show that $fT + M = T$. Still taking $f = \sum_{n=0}^{\infty} a_n t^n$, we put

$$g := \sum_{n=s}^{\infty} a_n t^{n-s} = a_s + a_{s+1} t + \ldots \in T^\times,$$

so

$$f - t^s g = a_0 + a_1 t + \ldots + a_{s-1} t^{s-1} \in \mathfrak{m}[t].$$

Put

$$\sum_{n=0}^{\infty} h_n t^n = h := t^s - f g^{-1} = -(f - t^s g) g^{-1} \in \mathfrak{m}[[t]].$$

Now let $r \in T$. We will recursively define a sequence $\{q^{(m)}\}_{m=0}^{\infty}$ in T. Let $q^{(0)}$ be the unique element of T satisfying

$$r - t^s q^{(0)} \in M. \tag{41}$$

Then we put

$$q_i^{(m)} := \sum_{j=0}^{i+s} h_j q_{i+s-j}^{(m-1)}$$

and

$$q^{(m)} := \sum_{n=0}^{\infty} q_n^{(m)} t^n. \tag{42}$$

Immediately from (42) we get for all $m \geqslant 1$ that

$$t^s q^{(m)} \equiv h q^{(m-1)} \pmod{M}. \tag{43}$$

Since $h_n \in \mathfrak{m}$ for all n, (42) and induction gives $q_n^{(m)} \in \mathfrak{m}^m$ for all m, n. Because T is complete, the series

$$q := \sum_{m=0}^{\infty} q^{(m)}$$

converges to an element of T. Using (41) and (43) we get:

$$t^s(q^{(0)} + q^{(1)} + \ldots + q^{(m)} \equiv r + h(q^{(0)} + \ldots + q^{(m-1)}) \pmod{M}. \tag{44}$$

Since M is closed in T, the quotient space T/M is Hausdorff, so limits of convergent sequences are unique, and thus from (44) we deduce $r - (t^s - h)q \in M$, so $r \in M + (t^s - h)qT = M + fg^{-1}qT \subseteq M + fT$.

Step 3: By Step 2, there is $q \in T$ such that $g - fq \in M$, and Step 1 implies the uniqueness of this q, establishing part a). In particular, if for $q \in T$ we have $qf = 0 \in M$, so by Step 1 we have $q = 0$ and thus f is not a zero-divisor. Part a) implies that $T = fT \oplus M$. Since $M \cong_R R^s$, we get $T/fT \cong M^s$. □

Let $f \in T = R[[t]]$ be regular of order $s \geqslant 1$. We say that f is **distinguished** if $f = t^s + a_{s-1}t^{s-1} + \ldots a_1 t + a_0$ with $a_0, \ldots, a_{s-1} \in \mathfrak{m}$. Thus a polynomial of positive degree is distinguished if and only if it is monic and regular of order equal to its degree.

THEOREM 15.38 (Weierstrass-Bourbaki Preparation Theorem). *Let $f \in T = R[[t]]$ be regular of order s. Then there is a unique $u \in T^\times$ such that uf is a distinguished polynomial (necessarily of degree s).*

PROOF. Apply Theorem 15.37a) with $f := t^s$ and $g := f$: there is a unique $q \in T$ and a unique $r \in R[t]$ of degree less than s such that $t^s = qf + r$. Thus

$$qf = t^s - r.$$

Since $\deg(r) < s$, if $\underline{r} \neq 0$ then $\mathrm{ord}(r) < s$ and thus by Exercise 15.20 we have

$$s = \mathrm{ord}(f) \leqslant \mathrm{ord}(f) + \mathrm{ord}(q) = \mathrm{ord}(qf) = \mathrm{ord}(t^s - r) = \mathrm{ord}(r) < s,$$

a contradiction. So $\underline{r} = 0$ and thus $t^s - r$ is a distinguished polynomial. Moreover we have

$$\mathrm{ord}(q) + s = \mathrm{ord}(qf) = \mathrm{ord}(t^s - r) = s,$$

so $\mathrm{ord}(q) = 0$ and thus $q \in T^\times$ by Exercise 15.20. So we may take $u := q$.

Conversely, suppose $u' \in T^\times$ is such that $u'f$ is dstinguished polynomial, necessarily of degree f, so we may write $u'f = t^s - r'$ where $\deg(r') < s$. Then $t^s = u'f + r'$, so by the uniqueness part of Theorem 15.37 we have $u' = u$ and $r' = r$. □

Above we mentioned that if $f, g, h \in R[[t]]$ with $f = gh$, then f is regular if and only if both g and h are regular. If $g, h \in R[t]$ are distinguished polynomials, then gh is also distinguished. However, the converse is not true for rather trivial reasons: if $g, h \in R[t]$ are distinguished polynomials and $f = gh$, then also $f = (ug)(u^{-1}h)$ for any $u \in R^\times$, and if $u \neq 1$ then ug fails to be distinguished precisely insofar as it is not monic. Being monic is clearly needed for the uniqueness part of Theorem 15.38. For many other purposes it will be convenient to make use of a slightly weaker property: a polynomial $f \in R[t]$ of positive degree is **quasi-distiguished**

if it is regular of order equal to its degree. A polynomial of degree $s \geqslant 1$ is quasidistinguished if and only if it is of the form $ut^s + r$ with $u \in R^\times$, $\deg(r) < s$ and $\underline{r} = 0$ if and only if it is a unit times a distinguished polynomial.

LEMMA 15.39. *If R is a domain and $f, g, h \in R[\![t]\!]$ are polynomials of positive degree such that $f = gh$, then f is quasi-distinguished if and only if g and h are both quasi-distinguished.*

PROOF. If g and h are quasi-distinguished, then there are $u_1, u_2 \in R^\times$ such that $u_1 g$ and $u_2 h$ are distinguished, so $u_1 u_2 f = (u_1 g_1)(u_2 h_2)$ is distinguished, so f is quasi-distinguished.

Suppose f is quasi-distinguished of degree d, so $\underline{f} = \underline{u}t^d$ for some $u \in R^\times$. Since $\underline{f} = \underline{g}\underline{h}$, we must have $\underline{g} = \underline{u_1}t^{s_1}$ and $\underline{h} = \underline{u_2}t^{s_2}$ for $u_1, u_2 \in R^\times$ and $s_1 + s_2 = d$. Thus g is regular of order s_1, so has degree $d_1 \geqslant s_1$ and h is regular of order s_2, so has degree $d_2 \geqslant s_2$. Since R is a domain, we have $d = d_1 + d_2 = s_1 + s_2$, so we must have $s_1 = d_1$ and $s_2 = d_2$ and thus g and h are quasi-distinguished. □

COROLLARY 15.40. *Let $f, g_1, g_2 \in T = R[\![t]\!]$, and suppose that f is a distinguished polynomial and $f = g_1 g_2$. Then there is $u \in T^\times$ such that ug_1 and $u^{-1}g_2$ are distinguished polynomials and $f = (ug_1)(u^{-1}g_2)$.*

PROOF. By Theorem 15.38 there are $u_1, u_2 \in T^\times$ such that for $i = 1, 2$ we have that $u_i g_i$ is a distinguished polynomial. Thus

$$u_1 u_2 f = (u_1 g_1)(u_2 g_2)$$

is a product of distinguished polynomials and thus itself a distinguished polynomial. Since f is also a distinguished polynomial, the uniqueness part of Theorem 15.38 gives $u_1 u_2 = 1$, so we may take $u = u_1$. □

COROLLARY 15.41. *Let $f \in R[t]$ be a quasi-distinguished polynomial. Then f is a prime element of $R[t]$ if and only if f is a prime element of $R[\![t]\!]$.*

PROOF. Suppose f has order $s \geqslant 1$. Because f is distinguished, its degree is also s. Consider the natural R-algebra homomorphism

$$\iota : R[t]/fR[t] \hookrightarrow R[\![t]\!]/fR[\![t]\!]. \tag{45}$$

It follows from Theorem 15.37a) that ι is surjective: indeed, for any $g \in R[\![t]\!]$ there is $q \in R[\![t]\!]$ and $r \in R[t]$ such that $g = qf + r$, so $g + fR[\![t]\!] = \iota(r + fR[t])$. Moreover, as an R-module, $R[t]/fR[t]$ is isomorphic to $R^{\deg(f)}$, while by Theorem 15.37b) we have $R[\![t]\!]/fR[\![t]\!] \cong R^{\mathrm{ord}(f)} \cong R^{\deg(f)}$. So there is an isomorphism of R-modules $\alpha : R[\![t]\!]/fR[\![t]\!] \xrightarrow{\sim} R[t]/fR[t]$, and thus $\alpha \circ \iota$ is a surjective R-module endomorphism of $R[t]/fR[t]$. By Theorem 3.47 the map $\alpha \circ \iota$ is an isomorphism, and thus also ι is an isomorphism. Thus f is a prime element of R if any only if $R[t]/fR[t]$ is a domain if and only if $R[\![t]\!]/fR[\![t]\!]$ is a domain if and only if f is a prime element of $R[\![t]\!]$. □

10. Power series rings over UFDs

For a ring R and a set I, we let $R[\![\mathbf{t}]\!]_{i \in I}$ be the ring of formal power series indeterminates t_i indexed by $i \in I$, with coefficients in R. These can be defined as "big monoid rings" as in §5.6 (see especially Exercises 5.38 and 5.39), but let us give some further details.

First we define the formal power series ring $R[[t_1, \ldots, t_n, \ldots]]$ in a countably infinite set of indeterminates as follows: let $\underline{d} = (d_1, d_2, \ldots, d_n, \ldots)$ be a sequence of natural numbers such that $d_n = 0$ for all but finitely many n, and we define the monomial

$$\underline{t}^{\underline{d}} := \prod_{n=1}^{\infty} t_n^{d_n}.$$

The key here is that this is not really an infinite product, because for all but finitely many n we have $t_n^{d_n} = t_n^0 = 1$. For two monomials $\underline{t}^{\underline{d}}$ and $\underline{t}^{\underline{e}}$, we say that $\underline{t}^{\underline{d}}$ divides $\underline{t}^{\underline{e}}$ if $\underline{d} \leqslant \underline{e}$, meaning that $d_n \leqslant e_n$ for all n. Then $R[[t_1, \ldots, t_n, \ldots]]$ is the free R-module with basis $\{\underline{t}^{\underline{d}}\}$. We multiply basis elements in the most evident way: $\underline{t}^{\underline{d}} \cdot \underline{t}^{\underline{e}} := \underline{t}^{\underline{d}+\underline{e}}$, and we "extend R-linearly" to get a product on $R[[t_1, \ldots, t_n, \ldots]]$. The scare quotes are there because multiplication requires us to distribute over infinite sums, so we need to take a moment to be sure that this product is well-defined. It is: for $x, y \in R[[t_1, \ldots, t_n, \ldots]]$ and any monomial $\underline{t}^{\underline{d}}$, in order to compute the coefficient of $\underline{t}^{\underline{d}}$ in the product xy, we only need to consider the coefficients of the monomials of x and y that divide $\underline{t}^{\underline{d}}$, and the number of monomials that divide $\underline{t}^{\underline{d}}$ is $\prod_{n=1}^{\infty}(d_n + 1)$, which is finite.

Here the set of monomials is indexed by $\bigoplus_{n \in \mathbb{Z}^+}(\mathbb{N}, +)$, which is a free commutative semigroup. The elements of $R[[t_1, \ldots, t_n, \ldots]]$ may be viewed as functions $f : \bigoplus_{n \in \mathbb{Z}^+}(\mathbb{N}, +)$: namely the value of the function at $\underline{d}$ is the coefficient of $\underline{d}$. This evidently gives an isomorphism of R-modules from $R[[t_1, \ldots, t_n, \ldots]$ to $R^{\bigoplus_{n \in \mathbb{Z}^+} \mathbb{N}}$. Moreover the product operation can nicely be expressed in terms of these functions: namely, for $f, g : \bigoplus_{n \in \mathbb{Z}^+} \mathbb{N} \to R$, we define

$$(f \cdot g)(\underline{d}) := \sum_{\underline{d_1} + \underline{d_2} = \underline{d}} f(\underline{d_1}) g(\underline{d_2}). \tag{46}$$

Again, this sum is well-defined because we need only sum over pairs $\overline{d_1}, \overline{d_2}$ such that $\overline{d_i} \leqslant \overline{d}$ in the natural "componentwise" partial ordering on $\bigoplus_{n \in \mathbb{Z}^+}(\mathbb{N}, +)$, and for each fixed $\overline{d}$ there are only many $\underline{e}$ with $\underline{e} \leqslant \underline{d}$.

Looking back at this construction, we see that the fact that the index set of the set of indeterminates is $\mathbb{Z}^+$ is not playing a crucial role. Now for any set I, we define a formal power series ring $R[[\mathbf{t}]]_I$ in indeterminates t_i with $i \in I$ and coefficients lying in a ring R. From the first perspective, our definition of monomial is very similar: $\underline{t}^{\underline{d}} := \prod_{i \in I} t_i^{d_i}$ with again the condition that $d_i = 0$ for all but finitely many $i \in I$. Still each monomial $\underline{t}^{\underline{d}}$ has a degree $\sum_{i \in I} d_i$. And again we may regard the elements as functions from $\bigoplus_{i \in I} \mathbb{N}$ to R and define the product via the same equation (46). Now, even though each $\underline{d}$ may have uncountably many components, still all but finitely many of them are 0 so the number of $\underline{e}$ with $\underline{e} \leqslant \underline{d}$ is again $\prod_{i \in I}(d_i + 1)$. One minor comment: we have $\#\bigoplus_{i \in I} \mathbb{N} = \max(\#I, \aleph_0)$, so when I is uncountable, a single element of $R[[\mathbf{t}]]_I$ is allowed to have uncountably many nonzero terms, thus stretching the traditional meaning of the term "series." Also, if $\#I_1 = \#I_2$ then $R[[\mathbf{t}]]_{I_1}$ and $R[[\mathbf{t}]]_{I_2}$ are isomorphic.

EXERCISE 15.21. a) *Let I_1 and I_2 be disjoint sets. Show: there is a canonical isomorphism from $(R[\mathbf{t}]_{I})[\mathbf{t}_J]$ to $R[\mathbf{t}]_{I \cup J}$, which we will use to identify them.*

b) *Exhibit a ring R such that for all $m, n \in \mathbb{N}$ we have $R[[t_1, \ldots, t_m]] \cong R[[t_1, \ldots, t_n]]$.*

EXERCISE 15.22. *Let R be a ring, and let $R[\mathbf{t}]_I$ be a formal power series ring, as above. For $f \in R[\mathbf{t}]_I$, let $a_0(f)$ denote its constant coefficient. Let $\mathcal{T} := \langle t_i \mid i \in I \rangle$.*

a) *Let $f \in R[\mathbf{t}]_I$. Show: $f \in R[\mathbf{t}]_I^\times \iff a_0(f) \in R[\mathbf{t}]_I^\times$. Observe that we may identify $a_0(f)$ with the image of f in $R[\mathbf{t}]_I/\mathcal{T}$. Deduce that the homomorphism $q : R[\mathbf{t}]_I \to R[\mathbf{t}]_I/\mathcal{T}$ is unit-faithful (cf. §4.2).*

b) *(Recall that for a ring A, $J(A)$ denotes its Jacobson radical.) Show: $f \in J(R[\mathbf{t}]_I) \iff a_0(f) \in J(R)$. Deduce:*

$$J(R[[\mathbf{t}]]_I) = \langle J(R), \mathcal{T} \rangle.$$

c) *Deduce: R is local if and only if $R[[\mathbf{t}]]_I$ is local.*

LEMMA 15.42. *Let I be a set. Then the formal power series ring $R[[\mathbf{t}]]_I$ is a domain if and only if R is domain.*

PROOF. Since R is a subring of $R[[\mathbf{t}]]_I$, certainly R must be a domain if $R[[\mathbf{t}]]_I$ is a domain. The converse is not as obvious as for polynomial rings. We proceed as follows:
Step 1: If R is a domain, then $R[[t]]$ is domain. We define a function $\mathrm{ord} : R[[t]] \to \mathbb{N} \cup \{\infty\}$ as follows: if $f \neq 0$, we define $\mathrm{ord}(f)$ to be the least $n \in \mathbb{N}$ such that t^n appears in f with nonzero coefficient; also we define $\mathrm{ord}(0) = \infty$. It is immediate that for all $f, g \in R[[t]]^\bullet$ we have $\mathrm{ord}(fg) = \mathrm{ord}(f) + \mathrm{ord}(g)$, which shows that for $f, g \neq 0$ we have $fg \neq 0$. Step 2: Since $R[[t_1, \ldots, t_{n+1}]] = (R[[t_1, \ldots, t_n]])[[t_{n+1}]]$, it follows by induction that $R[[\mathbf{t}]]_I$ is a domain for all finite sets I.
Step 3: Let I be an infinite set, and let $f, g \in R[[\mathbf{t}]]_I^\bullet$. There is a finite subset J of I such that $r_J(f), r_J(g) \in R[[\mathbf{t}]]_J^\bullet$. (This is true because only finitely many indeterminates appear in any given monomial hence also in any finite number of monomials.) Step 2 gives $r_J(fg) = r_J(f) r_J(g) \neq 0$, so certainly $fg \neq 0$. □

Henceforth we assume that R is a domain.

PROPOSITION 15.43. *Let R be a domain, and let I be a set. Then R is an ACCP-domain if and only if $R[[\mathbf{t}]]_I$ is an ACCP-domain.*

PROOF. First suppose that $R[[\mathbf{t}]]_I$ is an ACCP-domain. The inclusion map $\iota : R \hookrightarrow R[[\mathbf{t}]]_I$ is unit-faithful, so if $R[[\mathbf{t}]]_I$ is an ACCP-domain, then also R is an ACCP-domain by Exercise 15.13b). Let's spell it out: under ι, an ascending chain $(a_1) \subseteq (a_2) \subseteq \ldots \subseteq (a_n) \subseteq$ of nonzero principal ideals of R pushes forward to an ascending chain of principal ideals of $R[[\mathbf{t}]]_I$, which must stabilize since $R[[\mathbf{t}]]_I$ satisfies ACCP. So there is $N \in \mathbb{Z}^+$ such that for all $n \geqslant N$ we have that $\iota(\frac{a_{n+1}}{a_n})$ is a unit of $R[[\mathbf{t}]]_I$, hence $\frac{a_{n+1}}{a_n}$ is a unit of R and the sequence stabilizes.

Now suppose that R is an ACCP-domain. Since the map $r : R[[\mathbf{t}]]_I \to R$ is unit-faithful, one might try to apply the above argument to show that $R[[\mathbf{t}]]_I$ is an ACCP-domain. This will work *unless* each a_n lies in $\mathcal{T} = \mathrm{Ker}(r)$. This is what Exercise 15.13c) is for: for every $f \in R[[\mathbf{t}]]_I^\bullet$, there is a finite subset J of I such that $r_J(f) \neq 0$ (and then also if $g \mid f$ then $r_J(g) \neq 0$), and moreover each $r_J : R[[\mathbf{t}]]_I \to R[[\mathbf{t}]]_J$ is unit-faithful. So it suffices to show that each $R[[\mathbf{t}]]_J$ is an ACCP-domain for each finite J. By induction, it suffices to show that if R is an ACCP-domain then so is $R[[t]]$.

Suppose we have a sequence $\{f_n\}_{n=1}^\infty$ of elements of $R[[t]]^\bullet$ such that $f_{n+1} \mid f_n$

for all $n \in \mathbb{Z}^+$. Then the sequence $\{\mathrm{ord}(f_n)\}_{n=1}^{\infty}$ is a descending sequence in $\mathbb{N}$, so there is $N_1 \in \mathbb{Z}^+$ and $o \in \mathbb{N}$ such that $\mathrm{ord}(f_n) = o$ for all $n \geqslant N_1$. For $n \geqslant N_1$, $f_{n+1} \mid f_n$ implies $a_o(f_{n+1}) \mid a_o(f_n)$. So we get an ascending chain of nonzero principal ideals $\{a_o(f_n)\}$ in the ACCP-domain R, which must therefore stabilize: for all $n \geqslant N_2 \geqslant N_1$ we have $\frac{a_o(f_{n+1})}{a_o(f_n)} \in R^\times$. For all $n \geqslant N_2$ the element $\frac{f_{n+1}}{f_n}$ of $R[[t]]$ has order 0 and leading term a unit of R, hence is a unit of $R[[t]]$, so the sequence (f_n) stabilizes. □

LEMMA 15.44. *Let R be a domain, let I be a set, and let $a \in R$ be a nonzero, nonunit element.*

a) *The element a is irreducible in R if and only if it is irreducible in $R[[\mathbf{t}]]_I$.*
b) *The element a is prime in R if and only if it is prime in $R[\mathbf{t}]]_I$.*

PROOF. a) Suppose a is irreducible in R and that there are $g_1, g_2 \in R[[\mathbf{t}]]_I$ such that $a = g_1 g_2$. Let $r : R[[\mathbf{t}]]_I \to R$ be the quotient map by the ideal $\mathcal{T}$, which is unit-faithful. In R we have

$$a = r(a) = r(g_1)r(g_2),$$

so one of $r(g_1)$ and $r(g_2)$ is a unit, so by unit-faithfulness at least one of g_1 and g_2 is a unit, so a is irreducible in $R[[\mathbf{t}]]_I$.

Suppose a is reducible in R: $a = b_1 b_2$ for $b_1, b_2 \in R \backslash R^\times$. By Exercise 15.22, neither b_1 nor b_2 lies in $R[[\mathbf{t}]]_I^\times$, so a remains irreducible in $R[[\mathbf{t}]]_I$.
b) For any $a \in R$ we have $R[[[\mathbf{t}]]]_I/(a) \cong (R/(a))[[\mathbf{t}]]_I$, so $R/(a)$ is a domain if and only if $R[\mathbf{t}]]_I/(a)$ is a domain. □

All of this was just warmup. The real questions are: if R is a UFD, must $R[[t]]$ be a UFD? If so, can we prove that for any set I, the ring $R[[\mathbf{t}]_I$ is a UFD?

In contrast to the case of UFDs, whereas the argument to prove that R a UFD implies $R[t]$ a UFD even predated the modern definitions involved, whether a univariate formal power series ring over a UFD must be a UFD was a perplexing problem that remained open well into the 20th century. Some special cases were known relatively early on.

THEOREM 15.45. *If R is a PID, then $R[[t]]$ is a UFD.*

PROOF. By Theorem 15.1, it suffices to show that every nonzero prime ideal $\mathcal{P}$ of $R[[t]]$ has a prime element. If $t \in \mathcal{P}$, we're done. Otherwise, let $q : R[[t]] \to R$ be the quotient map and $\mathfrak{p} = q_* \mathcal{P}$. Since R is a PID, $\mathfrak{p}$ can be generated by one element, and then by Theorem 8.40a), so can $\mathcal{P}$. □

In particular, if k is a field then $k[[t_1]]$ is a PID, so $k[[t_1, t_2]] = k[[t_1]][[t_2]]$ is a UFD.

The following result shows a potential plan of attack in the local case:

THEOREM 15.46. *Let $(R, \mathfrak{m})$ be a local UFD that is complete and separated. Let $f \in R[[t]]$ be regular of order $s \geqslant 1$. Then f is a product of prime elements.*

PROOF. By Theorem 15.38, there is $u \in R[[t]]^\times$ such that $g := uf$ is a distinguished polynomial of degree s. By Theorem 15.26, since R is a UFD so is $R[t]$, so there are prime elements $p_1, \ldots, p_r$ of $R[t]$ such that $g = p_1 \cdots p_r$. By Lemma 15.39 each p_i is quasi-distinguished, so by Corollary 15.41 each p_i is also a prime element of $R[[t]]$. Thus $f = (u^{-1}p_1)p_2 \cdots p_r$ is a product of prime elements of $R[[t]]$. □

In order to use Theorem 15.46 to show that $R[[t]]$ is a UFD, we would need to somehow show that if every regular element of $R[[t]]$ is a product of prime elements, then every nonzero nonunit is a product of prime elements. In the case where $R = k$ is a field, this is trivial: every nonzero element of $k[[t]]$ is regular. One step up from this is if R is a PID, so the maximal ideal is principal, say $\mathfrak{m} = (\pi)$. Then π is prime element. Since $\bigcap_{n=1}^{\infty} \mathfrak{m}^n = (0)$, every nonzero element f of $R[[t]]$ is of the form $\pi^n g$ with g a regular element. Since g is a product of prime elements, so is f. This is the special case of Theorem 15.45 in which R is moreover a complete local ring: e.g. it applies to show that $\mathbb{Z}_p[[t]]$ is a UFD, where $\mathbb{Z}_p$ is the ring of p-adic integers.

Bourbaki employs this strategy more cleverly to prove the following result:

THEOREM 15.47. *(Rückert* [**Rü33**]*, Krull* [**Kr37**]*) Let k be a field, and let $n \in \mathbb{Z}^+$. Then $k[[t_1, \ldots, t_n]]$ is a UFD.*

PROOF. By Proposition , the ring $k[[t_1, \ldots, t_n]]$ is a Noetherian local ring with maximal ideal $\langle t_1, \ldots, t_n \rangle$ that is complete and separated. We will go by induction on n. We already know the cases $n = 0, 1$ (also $n = 2$, but the present argument will prove this again), so suppose that $n \geqslant 2$ and that we already know that $R := k[[t_1, \ldots, t_{n-1}]]$ is a UFD. Put $T := R[[t_n]]$; since $T \cong k[[t_1, \ldots, t_n]]$, our task is to show that T is a UFD. Let $f \in T$ be a nonzero nonunit. If f is regular (necessarily of order $s \geqslant 1$ since it is not a unit) then by Theorem 15.46 we know that f is a product of prime elements. We CLAIM that there is an automorphism α of T such that $\alpha(f)$ is regular. If so, then there are prime elements $p_1 \cdots p_r$ such that $\alpha(f) = p_1 \cdots p_r$, and then $f = \alpha^{-1}(p_1) \cdots \alpha^{-1}(p_n)$ is also a product of prime elements, completing the proof.
Step 1: Let A be a ring, and let $f \in A[[t_1, \ldots, t_n]]^\bullet$. We will show that there are $u_1, \ldots, u_{n-1} \in \mathbb{Z}^+$ such that $f(t^{u_1}, \ldots, t^{u_{n-1}}, t) \neq 0$.
To show this, we proceed inductively: assuming there are $u_1, \ldots, u_{k-1} \in \mathbb{Z}^+$ such that $f(t_n^{u_1}, \ldots, t_n^{u_{k-1}}, t_k, \ldots, t_n) \neq 0$, it suffices to find $u_k \in \mathbb{Z}^+$ such that $f(t_n^{u_1}, \ldots, t_n^{u_k}, t_{k+1}, \ldots, t_n) \neq 0$. Moreover, viewing $f(t_n^{u_1}, \ldots, t_n^{u_{k-1}}, t_k, \ldots, t_n)$ as an element of $R[[t_{k+1}, \ldots, t_{n-1}]][[t_k, t_n]]$, we reduce to the case $n = 2$.

Thus let $f = \sum_{i,j} e_{ij} x^i y^k \in A[[x, y]]^\bullet$. Let G be the support of f, i.e., the set of $(i, j) \in \mathbb{N}^2$ such that $e_{ij} \neq 0$. We order $\mathbb{N} \times \mathbb{N}$ lexicographically, let (c, d) be the least element of G and choose an integer $p > d$. In the expression

$$f(t^p, t) = \sum_{(i,j) \in G} e_{ij} t^{ip+j},$$

let us consider the coefficient of $cp + d$: it is the sum of the e_{ij}'s iwth $ip + j = cp + d$. We claim that the only such term is $(i, j) = (c, d)$. Indeed, if $i \geqslant c + 1$ then

$$ip + j \geqslant (c + 1)p_j \geqslant (c + 1)p > cp + d,$$

while if $i < c$ then because (c, d) is the lexicographically least element in the support of G we must have $e_{ij} = 0$. Therefore we must have $i = c$ and then $ip + j = cp + d$ implies $j = d$. Therefore the coefficient of t^{cp+d} in $f(t^p, t)$ is $e_{(c,d)} \neq 0$, so $f(t^p, t) = 0$, completing this step of the proof.
Step 2: Let A be a ring, and let $\mathcal{T}$ be the ideal $\langle t_1, \ldots, t_n \rangle$ of the ring $A[[t_1, \ldots, t_n]]$, and let $w_1, \ldots, w_n \in \mathcal{T}$. If $f \in A[[t_1, \ldots, t_n]]$, then $f(w_1, \ldots, w_n)$ is a well-defined

element of $A[[t_1, \ldots, t_n]]$, and the map

$$\varphi : f \in A[[t_1, \ldots, t_n]] \mapsto f(w_1, \ldots, w_n)$$

is a A-algebra endomorphism of $A[[t_1, \ldots, t_n]]$ that for $1 \leqslant i \leqslant n$ maps t_i to w_i. We claim moreover that φ is the *unique* such A-algebra endomorphism. Indeed, any such A-algebra endomorphism is uniquely determined on the subalgebra $A[t_1, \ldots, t_n]$ by the universal property of polynomial rings. The subalgebra $A[t_1, \ldots, t_n]$ is dense in the $A[[t_1, \ldots, t_n]]$ in the $\mathcal{T}$-adic topology. Because $A[[t_1, \ldots, t_n]]$ is $\mathcal{T}$-adically separated – that is, is a Hausdorff space – it suffices to show that any A-algebra endomorphism φ of $A[[t_1, \ldots, t_n]]$ mapping each t_i to w_i is continuous for the $\mathcal{T}$-adic topology. Like any homomorphism of topological groups, it suffices to check continuity at 0, which means that for all $k \in \mathbb{N}$ there is $K = K(k)$ such that $\varphi(\mathcal{T}^K) \subseteq \mathcal{T}^k$. Indeed we may take $K(k) = k$ for all k: a set of generators for $\mathcal{T}^k$ is $\{t_1^{a_1} \cdots t_n^{a_n} \mid a_1 + \ldots + a_n \geqslant k\}$ and $\varphi(t_1^{a_1} \cdots t_n^{a_n}) = w_1^{a_1} \cdots w_n^{a_n} \in \mathcal{T}^k$, so any finite $A[[t_1, \ldots, t_n]]$-linear combination of these generators gets mapped to a finite $A[[t_1, \ldots, t_n]]$-linear combination of elements of $\mathcal{T}^k$, which is of course an element of $\mathcal{T}^k$.

Step 3: Let $f \in k[[t_1, \ldots, t_n]]$ be a nonzero nonuit. By Step 1, there are $u_1, \ldots, u_{n-1} \in \mathbb{Z}^+$ such that $f(t_1^{u_1}, \ldots, t_{n-1}^{u_{n-1}}, t) \neq 0$. By Step 2, there are unique k-algebra endomorphisms φ and ψ of $k[[t_1, \ldots, t_n]]$ such that:

$$\forall 1 \leqslant i \leqslant n-1, \varphi(t_i) = t_i + t_n^{u_i} \text{ and } \varphi(t_n) = t_n$$

and

$$\forall 1 \leqslant i \leqslant n-1, \psi(t_i) = t_i - t_n^{u_i} \text{ and } \psi(t_n) = t_n.$$

Then $\psi \circ \varphi$ is a k-algebra endomorphism of $k[[t_1, \ldots, t_n]]$ that maps each t_i to itself, so by the uniqueness part of Step 2, $\psi \circ \varphi = 1$, so φ is a k-algebra automorphism of $k[[t_1, \ldots, t_n]]$. Let $g \coloneqq \varphi(f)$. Then we have

$$g(0, \ldots, 0, t_n) = f(t_n^{u_1}, \ldots, t_n^{u_{n-1}}, t_n) \neq 0.$$

Finally, we observe that evaluating $g \in k[[t_1, \ldots, t_n]]$ at $t_1 = \ldots = t_{n-1} = 0$ is equivalent to reducing modulo the maximal ideal $\mathfrak{m} = \langle t_1, \ldots, t_{n-1} \rangle$ of $R = k[[t_1, \ldots, t_{n-1}]]$, so $g(0, \ldots, t_n) \neq 0$ means precisely that g is regular. This completes the proof. □

EXERCISE 15.23. *Let R be a complete discrete valuation ring, and let $n \in \mathbb{Z}^+$. Adapt the above proof to show that the ring $R[[t_1, \ldots, t_n]]$ is a UFD.*

The same method can be used to show that if R is any PID, then for all $n \in \mathbb{Z}^+$ the ring $R[[t_1, \ldots, t_n]]$ is a UFD [**B**, Exercise §7.3.9].

However, it turns out not to be true in general that if R is a UFD then $R[[t]]$ must also be a UFD. The first counterexamples were found by Samuel:

THEOREM 15.48. *(Samuel, 1961) Let k be a perfect field of characteristic 2, let*

$$R \coloneqq k[x, y, z]/\langle z^2 - x^3 - y^7 \rangle$$

and let $\mathfrak{m} \coloneqq \langle x, y, z \rangle + \langle z^2 - x^3 - y^2 \rangle$, a maximal ideal of R. Then:

a) *The ring R is a UFD, hence so is its localization $R_{\mathfrak{m}}$.*
b) *Neither $R[[t]]$ nor $R_{\mathfrak{m}}[[t]]$ is a UFD.*

PROOF. See [**Sa61**, Thm. 4.1 and Thm. 4.3]. □

The most penetrating results of this kind come from making use of the following imporatnt definition: a Noetherian ring R is **regular** if for all $\mathfrak{m} \in \operatorname{MaxSpec} R$, the height of $\mathfrak{m}$ is $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$. This is a local property: a Noetherian ring R is regular if and only if $R_{\mathfrak{m}}$ is regular for all $\mathfrak{m} \in \operatorname{MaxSpec} R$ (this follows almost immediately from the definition) if and only if $R_{\mathfrak{p}}$ is regular for all $\mathfrak{p} \in \operatorname{Spec} R$ (this does not, but se e.g. [**Ei**, Cor. 19.14]). So it suffices to understand the concept of regularity for a Noetherian *local* ring $(R, \mathfrak{m})$. In this case, the height of $\mathfrak{m}$ is just the Krull dimension $\dim R$, by Nakayama's Lemma $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2$ is the least number of generators for M, so the Generalized Principal Ideal Theorem gives

$$\operatorname{ht}(\mathfrak{m}) \leqslant \dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2. \tag{47}$$

Thus $(R, \mathfrak{m})$ is regular if and only if equality holds in (47). It is then immediate that a PID is a regular ring. Soon we will study PIDs, discrete valuation rings and Dedekind domains in detail. Our results will imply that a one-dimensional local Noetherian domain is regular if and only if it is a discrete valuation ring and a one-dimensional Noetherian domain is regular if and only if it is a Dedekind domain. The 2-dimensional Noetherian domain $R_{\mathfrak{m}}$ of Theorem 15.48 is not regular: indeed, $R_{\mathfrak{m}}/\mathfrak{m}^2 = k[x,y,z]/\langle x^2, y^2, z^2, xy, xz, yz, z^2 - x^3 - y^2\rangle$. But since $z^2 - x^3 - y^7 \in \langle x, y, z\rangle^2$, we have $R_{\mathfrak{m}}/(\mathfrak{m}R_{\mathfrak{m}})^2 = k[x,y,z]/\langle x, y, z\rangle^2$, which is a local ring for which a k-vector space basis is $1, x, y, z$. It follows that (the images of) x, y, z are k-basis for $\mathfrak{m}/\mathfrak{m}^2$, so $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = 3 > \dim R_{\mathfrak{m}}$. (Notice that the same conclusion holds for $k[x,y,z]/(f)$ for any polynomial f each of whose monomials has degree at least 2.)

The following breakthrough result was proved independently by Buchsbaum [**Bu61**] and Samuel [**Sa61**].

THEOREM 15.49 (Buchsbaum-Samuel). *If R is a regular UFD, then so is $R[[t]]$.*

The local case of Theorem 15.49 was known slightly earlier, as we will now explain. The following is a quick consequence of Theorems 8.40b) and Theorem 8.60b):

EXERCISE 15.24. *Show: if R is a regular local ring, so is $R[[t]]$.*

The following result of Auslander-Buchsbaum [**AB59**], building on earlier work of Nagata [**Na58**], is probably the most important theorem about UFDs.

THEOREM 15.50 (Auslander-Buchsbaum). *A regular local ring is a UFD.*

If R is a regular local ring, then by Exercise 15.24 also $R[[t]]$ is a regular local ring, hence a UFD by Theorem 15.50. In particular Theorem 15.47 is essentially a consequence of Theorem 15.50.

The proof of Theorem 15.50 uses homological methods that we will unfortunately not discuss here. However, it is (to say the least!) covered in many other commutative algebra texts: see e.g. [**M**, Thm. 20.3] or [**Ei**, Thm. 19.19]. Notice that it is not even obvious that a regular local ring is a domain.

We now return to the case of power series in infniitely many indeterminates.

LEMMA 15.51. *Let R be a domain, and let α be an infinite limit ordinal. Suppose that for all ordinals $\beta < \alpha$, the formal power series ring $R[[\mathbf{t}]]_\beta$ is a UFD. For $\beta < \alpha$, let $r_\beta : R[[\mathbf{t}]]_\alpha \to R[[\mathbf{t}]]_\beta$ be the quotient by the ideal generated by t_i for*

$i \in \alpha \backslash \beta$. Let f be irreducible. Then the set of $\beta < \alpha$ such that $r_\beta(f)$ is irreducible is cofinal in α.

PROOF. We observe that since f is not a unit and r_β is unit-faithful, no $r_\beta(f)$ is a unit. Since f is nonzero and α is a limit ordinal, there is some $\delta_0 < \alpha$ such that $r_{\delta_0}(f) \neq 0$ and thus $r_\delta \neq 0$ for all $\delta \geqslant \delta_0$. Since the set of all ordinals less than α that are greater or equal to any fixed ordinal is cofinal in α, it suffices to work with $\delta_0 \leqslant \beta < \alpha$.
Step 1: Suppose that for all $\delta_0 \leqslant \beta < \alpha$, the element $r_\beta(f)$ is reducible: that is a product of at least two irreducible elements. We will show that f is reducible.

We define an inverse system $\{\mathcal{S}_\beta\}_{\delta_0 \leqslant \beta < \alpha}$ of sets. For $\beta < \alpha$, $\mathcal{S}_\beta$ is the set of all principal ideals I_β of $R[[\mathbf{t}]]_\beta$ such that

$$fR[[\mathbf{t}]]_\beta \subsetneq I_\beta \subsetneq R[[\mathbf{t}]]_\beta,$$

so each $\mathcal{S}_\beta$ is nonempty. Because $R[[\mathbf{t}]]_\beta$ is a UFD, the element $r_\beta(f)$ is a product of n_β prime elements for some $n_\beta \in \mathbb{Z}^{\geqslant 2}$. Then $\#\mathcal{S}_\beta \leqslant 2^{n_\beta} - 2$ (with equality if and only if the prime elements are pairwise nonassociate), so each $\mathcal{S}_\beta$ is finite. For $\delta_0 \leqslant \beta_1 \leqslant \beta_2 < \alpha$, we define the transition map $\varphi_{\beta_2,\beta_1} : \mathcal{S}_{\beta_2} \to \mathcal{S}_{\beta_1}$ just by pushing forward I_{β_2} via the map $r_{\beta_2,\beta_1} : R[[\mathbf{t}]]_{\beta_2} \to R[[\mathbf{t}]]_{\beta_1}$: by unit-faithfulness, this principal ideal is still proper and properly contains the ideal generated by f.

It is a corollary of Tychonoff's Theorem that an inverse limit of compact (= quasicompact Hausdorfff) spaces with continuous transition maps is a nonempty compact, Hausdorff space [**ES**, p. 217]. It follows that any inverse limit of finite sets is nonempty: just endow each set with the discrete topology.

An element $\mathcal{P} = \{\mathcal{P}_\beta\} \in \varprojlim \mathcal{S}_\beta$ is *almost* a compatible choice of a nontrivial proper factor of f in each $R[[\mathbf{t}]]_\beta$: it remains to resolve the issue of choosing compatible generators for the principal ideals $\mathcal{P}_\beta$, which we will do by transfinite recursion. If $\beta = \gamma + 1$ is a successor ordinal, then having chosen a generator g_γ of $\mathcal{P}_\gamma$, we can certainly choose a generator g_β of $\mathcal{P}_\beta$ such that $r_{\beta,\gamma}(g_\beta) = g_\gamma$. And if β is a lmit ordinal then $\beta = \{\gamma \mid \gamma < \beta\}$ and $R[[\mathbf{t}]]_\beta = \varprojlim R[[\mathbf{t}]]_\gamma$, so there is a unique such choice in this case. We get an element $g \in R[[\mathbf{t}]]_\alpha$ such that for all $\delta_0 \leqslant \beta < \alpha$ we have $r_\beta(g) = g_\beta$. For all $\delta_0 \leqslant \beta < \alpha$ there is a unique element h_β of $R[[\mathbf{t}]]_\beta$, not a unit, such that $g_\beta h_\beta = r_\beta(f)$, so this uniquely determines $h \in R[[\mathbf{t}]]_\alpha$ such that $f = gh$. By unit-faithfulness, neither g nor h is a unit, completing Step 1.
Step 2: After Step 1, since f is irreducible, we know there is some $\delta_0 \leqslant \beta_0 < \alpha$ such that $r_{\beta_0}(f)$ is irreducible. We claim that for all $\beta_0 \leqslant \beta < \alpha$, also $r_\beta(f)$ is irreducible, which suffices to prove the result, since this set of β is certainly cofinal in α. This is easy: using unit-fatihfulness several more times we see that $r_{\beta_0}(f)$ must have at least as many prime factors as $r_\beta(f)$. □

THEOREM 15.52 (Cashwell-Everett). *For a domain R, the following are equivalent:*

(i) *For all $n \in \mathbb{N}$, the ring $R[[t_1, \ldots, t_n]]$ is a UFD.*
(ii) *For all sets I, the ring $R[[\mathbf{t}]]_I$ is a UFD.*

PROOF. (i) $\implies$ (ii): Suppose that $R[[t_1, \ldots, t_n]]$ is a UFD for all $n \in \mathbb{N}$, and let I be any set. We want to show that $R[[\mathbf{t}]]_I$ is a UFD. We may assume that I is infinite and then replace I by its cardinal number κ, i.e., the least ordinal of cardinality $\#I$. Inductively, we may assume that $R[[\mathbf{t}]]_\beta$ is a UFD for all $\beta < \kappa$.

By Proposition 15.43 we have that $R[[\mathbf{t}]]_\kappa$ is an ACCP-domain, so it suffices to let $f \in R[[\mathbf{t}]]_\kappa$ be any irreducible element and show that f is prime. For this, let $g, h \in R[[\mathbf{t}]]_\kappa$ be such that $f \mid gh$. By Lemma 15.51, the set of $\beta < \kappa$ such that $r_\beta(f)$ is a prime element of $R[[\mathbf{t}]]_\beta$ is cofinal in α. For each such β, we have that $r_\beta(f) \mid r_\beta(g)r_\beta(h)$, so $r_\beta(f)$ divides at least one of $r_\beta(g)$ and $r_\beta(h)$. In any directed set, if we write a cofinal subset as a finite union of subsubsets, then at least one of those subsubsets is cofinal, so without loss of generality we may assume that the set of $\beta < \alpha$ such that $r_\beta(f)$ divides $r_\beta(g)$ is cofinal. For each such β there is therefore a unique $q_\beta \in R[[\mathbf{t}]]_\beta$ such that $r_\beta(f)q_\beta = r_\beta(g)$, and by uniqueness we must have $r_{\beta_2,\beta_1}(q_{\beta_2}) = q_{\beta_1}$ for all such $\beta_1 \leqslant \beta_2$. It follows that there is $q \in R[[\mathbf{t}]]_\kappa$ such that $fq = g$, so f is a prime element of $R[[\mathbf{t}]]_\kappa$. Thus $R[[\mathbf{t}]]_\kappa$ is a UFD.
(ii) $\implies$ (i): It suffices to show: for any set I, if $R[[\mathbf{t}]]_I$ is a UFD, then so is R. Suppose $R[[\mathbf{t}]]_I$ is a UFD. Then R is an ACCP-domain by Proposition 15.43; in particular it is an atomic domain. By Lemma 15.44, we know that for all $a \in R$, if a is irreducible, then a is irreducible as an element of $R[[\mathbf{t}]]_I$, and if a is prime as an element of $R[[\mathbf{t}]]_I$ then a is prime as an element of R. We claim that for any extension $R \hookrightarrow S$ fo domains in which R is atomic, S is a UFD, every irreducible element of R remains irreducible in S and every element of R that is prime in S is also prime in R, it follows that R is a UFD. Indeed, let $a \in R$ be a nonzero nonunit. By atomicity there are irreducibles $f_1, \ldots, f_r$ such that $a = f_1 \cdots f_r$. By assumption eaech f_i is also irreducible in the UFD S, so each f_i is prime in f, so by assumption each f_i is prime in R. □

In [**CE59**], Cashwell-Everett gave a striking consequence of Theorem 15.52, which indeed seems to have been there original motivation. For a ring R, we define the **Dirichlet ring** $\mathcal{D}_R$ as follows: the underlying set is $R^{\mathbb{Z}^+}$, the set of all functions $f : \mathbb{Z}^+ \to R$. We give it the evident R-module structrure: i.e., addition and scalar multiplication is componentwise. The product is however the convolution product:

$$f * g : n \in \mathbb{Z}^+ \mapsto \sum_{d_1 d_2 = n} f(d_1)g(d_2).$$

The case of $\mathcal{D} := \mathcal{D}_{\mathbb{C}}$ appears in elementary number theory, at which point one may solve the following exercises (but you, the reader, may want to read on a little bit to learn why these are not new results for us).

EXERCISE 15.25. *Let R be a ring.*

a) *Show that for all $f, g, h \in \mathcal{D}_R$ and all $n \in \mathbb{Z}^+$ we have*

$$((f * g) * h)(n) = \sum_{d_1 d_2 d_3 = n} f(d_1)g(d_2)h(d_3) = (f * (g * h))(n).$$

b) *Define $\iota : R \to \mathcal{D}_R$ by $\iota(r)(n) := \begin{cases} r & n = 1 \\ 0 & n \geqslant 2 \end{cases}$. Show: $\mathcal{D}_R$ is an R-algebra, and if $\mathcal{D}_R$ is a domain then R is a domain.*

EXERCISE 15.26. *Let R be a domain.For $f \in \mathcal{D}_R^\bullet$, define $N(f)$ to be the least $n \in \mathbb{Z}^+$ such that $f(n) \neq 0$; and put $N(0) := 0$.*

a) *Show: For all $f, g \in \mathcal{D}_R^\bullet$, we have $N(fg) = N(f)N(g)$. Deduce: R is a domain.*

b) *Show: if $f \in \mathcal{D}_R^\times$ if and only if $f(1) \in R^\times$.*

c) *Show: if $f \in \mathcal{D}_R^\times$ then $N(f) = 1$. Show that the converse holds for all f if and only if R is a field.*
d) *Let k be a field. Show: $\mathcal{D}_k$ is an ACCP-domain.*

The point of all this is the following simple but crucial observation:

PROPOSITION 15.53 (Cashwell-Everett). *For a ring R, the Dirichlet ring D_R is isomorphic to the ring $R[[t_1, \ldots, t_n, \ldots]]$ of formal power series in a countably infinite set of indeterminates.*

PROOF. The ring D_R is the big monoid ring $R[[(\mathbb{Z}^+, \cdot)]]$, while the formal power series ring $R[[t_1, \ldots, t_n, \ldots]]$ is the big monoid ring $\bigoplus_{n \in \mathbb{Z}^+}(\mathbb{N}, +)$. To complete the proof it suffices to show that the monoid $(\mathbb{Z}^+, \cdot)$ is isomorphic to $\bigoplus_{n \in \mathbb{Z}^+}(\mathbb{N}, +)$, i.e., that $(\mathbb{Z}^+, \cdot)$ is a free commutative monoid on a countably infinite set of generators. Indeed it is, and the (unique!) generators are the prime numbers. □

Combining Proposition 15.53 and Theorem 15.52 we get:

COROLLARY 15.54. *Let R be a domain.*
a) *For a domain R, the Dirichlet ring $\mathcal{D}_R$ is a UFD if and only if for all $n \in \mathbb{N}$, the formal power series ring $R[[t_1, \ldots, t_n]]$ is a UFD.*
b) *If R is a regular UFD, then $\mathcal{D}_R$ is a UFD. Thus $\mathcal{D}_R$ is a UFD if R is a field or a PID. In particular, $\mathcal{D} = \mathcal{D}_{\mathbb{C}}$ is UFD.*

Let us say a little bit about how $\mathcal{D}$ is used in number theory. A function $f : \mathbb{Z}^+ \to \mathbb{C}$ is called **multiplicative** $f(1) \neq 0$ and for all n_1, n_2 with $\gcd(n_1, n_2) = 1$ we have $f(n_1 n_2) = f(n_1) f(n_2)$. One then gets immediately that $f(1) = 1$.

From an abstract algebraic perspective, this definition would look more natural without the coprimality condition on n_1 and n_2: such functions are called **strongly multiplicative** and are indeed just the monoid maps from $(\mathbb{Z}^+, \cdot)$ to $(\mathbb{C}, \cdot)$. However some of the most important arithmetic functions are multiplicative but not strongly multiplicative.

PROPOSITION 15.55. *Let $\mathcal{M}$ be the subset of $\mathcal{D}$ consisting of multiplicative functions. Then $(\mathcal{M}, *)$ is a commutative group.*

PROOF. Step 1: Let $f, g \in \mathcal{M}$ and let $n_1, n_2 \in \mathbb{Z}^+$ have $\gcd(n_1, n_2) = 1$. The basic observation here is that (by unique factorization!), the divisors of $n_1 n_2$ are precisely $d_1 d_2$ with $d_1 \mid n_1$ and $d_2 \mid n_2$. So:

$$(f * g)(n_1 n_2) = \sum_{d \mid n_1 n_2} f(d) g(n/d) = \sum_{d_1 \mid n_1, d_2 \mid n_2} f(d_1 d_2) g(\frac{n_1}{d_1} \frac{n_2}{d_2})$$

$$= \sum_{d_1 \mid n_1, d_2 \mid n_2} f(d_1) f(d_2) g(\frac{n_1}{d_1}) g(\frac{n_2}{d_2}) = \left(\sum_{d_1 \mid n_1} f(d_1) g(\frac{n_1}{d_1}) \right) \left(\sum_{d_2 \mid n_2} f(d_2) g(\frac{n_2}{d_2}) \right)$$

$$= (f * g)(n_1)(f * g)(n_2)$$

and thus $f * g \in \mathcal{M}$.
Step 2: Let $f \in \mathcal{M}$. Then $f(1) = 1 \neq 0$, so there is a unique function $g : \mathbb{Z}^+ \to \mathbb{C}$ such that $f * g = 1$. Indeed we have $g(1) = 1$, while for all $n \geqslant 2$ we have

$$g(n) = - \sum_{d \mid n,\ d \neq n} f(\frac{n}{d}) g(d). \tag{48}$$

From this recursive formula, it is easy to prove by induction that g is multiplicative, similarly to Step 1. □

An important multiplicative function is the constant function 1, which we denote as $\mathbf{1}$. (Note that this is *not* the multiplicative identity, 1, which evaluates to 1 at 0 and to 0 at all $n \geqslant 2$.) For $f \in \mathcal{D}$, we put

$$F := f * \mathbf{1} : n \mapsto \sum_{d|n} f(d).$$

By Proposition 15.55, if f is multiplicative, then so is F. The function $\mathbf{1}$ is certainly completely multiplicative, so if f is completely multiplicative, then F is the convolution of two completely multiplicative functions...but need not be completely multiplicative. Indeed,

$$\sigma_0 := \mathbf{1} * \mathbf{1} : n \mapsto \sum_{d|n} 1$$

is the number of (positive) divisors of n. For any prime number p we have

$$3 = \sigma_0(p^2) \neq \sigma_0(p)\sigma_0(p) = 2^2.$$

EXERCISE 15.27. *Let $f \in \mathcal{D}$ be a compltely multiplicative function. Then f^{-1} is completely multiplicative if and only if $f = 1$.*

T. MacHenry showed [**Ma99**, Cor. 1.3.2] that the subgroup $\mathcal{M}^{\blacksquare}$ of $\mathcal{M}$ generated by the completely multiplicative functions is a free commutative group on the set of completely multiplicative functions and a proper subgroup of $\mathcal{M}$.

Let $\mu := \mathbf{1}^{-1}$. By Proposition 15.55, the function μ is also multiplicative, so to evaluate it, it suffices to know its values at $n = p^a$ for a prime number p and $a \in \mathbb{Z}^+$. By (48) we have

$$\mu(p^a) = -\sum_{d|p^a, d \neq p^a} \mathbf{1}(\frac{p^a}{d})\mu(d) = -\sum_{i=0}^{a-1} \mu(p^i).$$

By induction on a, we find that $\mu(p) = -1$ and $\mu(p^a) = 0$ for all $a \geqslant 2$. This function is called the **Möbius function**, and it appears in the following result:

PROPOSITION 15.56 (Möbius Inversion Formula). *Let $f \in \mathcal{D}$, and let $F := f * \mathbf{1} : n \mapsto \sum_{d|n} f(d)$. Then*

$$f = \sum_{d|n} F(d)\mu(n/d).$$

PROOF. By our definition of μ we have $\mathbf{1} * \mu = 1$. This is the entire content of the formula:

$$f = f * 1 = f * (\mathbf{1} * \mu) = (f * \mathbf{1}) * \mu = F * \mu.$$ □

The name Dirichlet ring comes from the following observation: to $f \in \mathcal{D}$ we can associate the formal Dirichlet series

$$D(f, s) := \sum_{n=1}^{\infty} \frac{f(n)}{n^s}.$$

We then have

$$D(f, s) + D(g, s) = D(f + g, s) \text{ and } D(f, s)D(g, s) = D(f * g, s),$$

so we may view $D_{\mathbb{C}}$ as the ring of formal Dirichlet series. For instance, we have

$$D(\mathbf{1}, s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

is the Riemann zeta function, so its inverse is

$$D(\mathbf{1}^{-1}, s) = D(\mu, s) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}.$$

EXERCISE 15.28. *Let $f \in \mathcal{M} \subset \mathcal{D}$ be a multiplicative function. Show:*

$$D(f, s) = \prod_{p \ prime} \sum_{n \geq 0} \frac{f(p^n)}{p^{ns}}.$$

To sum up: unique factorization plays a crucial role in the study of individual arithmetic functions, as seen for instance in Exercise 15.28. The fact that the ring $\mathcal{D}$ of all arithmetic functions also has unique factorization is one of the more striking mathematical results that I know. The literature contains some interesting refinements and generalizations, of which we now briefly mention just a few.

For a ring R and an infinite set I, there are many proper subrings S of $R[[\mathbf{t}]]_I$ with the property that for all finite subsets J of I we have $R[[\mathbf{t}]]_J \subseteq S \subseteq R[[\mathbf{t}]]_I$, and we can ask whether the Cashwell-Everett Theorem continues to hold for them: i.e., is S a UFD if and only if each $R[\mathbf{t}]_J$ is a UFD? There is a unique smallest such S, namely $S_1 := \bigcup_J R[[\mathbf{t}]]_I$. This is the ring of formal power series in which only finitely many indeterminates appear in any one series. Another such ring is S_2, the ring of formal power series $f \in R[[\mathbf{t}]]_I$ in which for each $n \in \mathbb{N}$, only finitely many monomials of degree n appear in f. We have $S_1 \subsetneq S_2 \subsetneq R[[\mathbf{t}]]_I$: e.g. when $I = \mathbb{Z}^+$ we have

$$t_1 + t_2^2 + \ldots + t_n^n + \ldots \in S_2 \backslash S_1 \text{ and } t_1 + t_2 + \ldots + t_n + \ldots \in R[[\mathbf{t}]]_I \backslash S_2.$$

It is known that both S_1 and S_2 are UFDs if and only if $R[[\mathbf{t}]]_J$ is a UFD for each finite set. For S_1, this is easy: we have $S_1 = \varinjlim R[[\mathbf{t}]]_J$. The proof that if each $R[\mathbf{t}]_J$ is a UFD then also $R[\mathbf{t}]_I$ is a UFD outlined in Exercise 15.14 also works to show that S_1 is a UFD. As for S_2, if we again define $\mathcal{T} := \langle t_i \mid i \in I \rangle$, then we observe that – like $R[[\mathbf{t}]]_I$ – the ring S_2 is $\mathcal{T}$-adically complete, but – unlike $R[[\mathbf{t}]]_I$ – the ring S_2 is the $\mathcal{T}$-adic completion of the polynomial ring $R[\mathbf{t}]_I$. In this text we have not given a ring-theoretic definition of completion with respect to an ideal, but we have a $\mathcal{T}$-adic metric on $R[[\mathbf{t}]]_I$ hence also on S_2 whose restriction to $R[\mathbf{t}]_I$ is the $(\mathcal{T} \cap R[\mathbf{t}]_I)$-adic metric on $R[\mathbf{t}]_I$, so both $R[\mathbf{t}]_I \hookrightarrow R[[\mathbf{t}]]_I$ and $R[[\mathbf{t}]]_I \hookrightarrow S_2$ are isometric embeddings from a metric space int oa complete metric space. However $R[\mathbf{t}]_I$ is dense in S_2 but not in $R[[\mathbf{t}]]_I$: again $t_1 + t_2 + \ldots + t_n + \ldots$ is not the limit of a sequence from $R[\mathbf{t}]_I$. That S_2 is a UFD if and only if $R[[\mathbf{t}]]_J$ is a UFD for each finite J is a result of Nishimura [**Ni73**].

Next recall that the Dirichlet ring $\mathcal{D}$ be may be viewed as the ring of formal Dirichlet series $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ with $a_n \in \mathbb{C}$. We call such a formal Dirichlet series **convergent** if the series converges in $\mathbb{C}$ for at least one $s \in \mathbb{C}$. It is known that then either the series converges for all $s \in \mathbb{C}$ or there is a smallest real number σ (the "abscissa of absolute convergence") such that the series converges absolutely in the half-plane $\Re(s) > \sigma$. From this it follows that the convergent Dirichlet series form

a subring, say $\mathcal{D}^{\mathfrak{c}}$, of the Dirichlet ring $\mathcal{D}$. It is a theorem of Bayart-Mouze [**BM03**] that $\mathcal{D}^{\mathfrak{c}}$ is also a UFD.

11. Nagata's Criterion

PROPOSITION 15.57. *Let R be a domain, S a saturated multiplicative subset, and $f \in R \backslash S$. If $f \in R$ is a prime element, then f is a prime element of R_S.*

PROOF. Since $f \in R \backslash S$, f is not a unit in R_S. Let $\alpha, \beta \in R_S$ be such that $f \mid \alpha\beta$ in R_S. So there exists $\gamma \in R_S$ such that $\gamma f = \alpha\beta$; putting $\alpha = \frac{x_1}{s_1}$, $\beta = \frac{x_2}{s_2}$, $\gamma = \frac{x_3}{s_3}$ and clearing denominators, we get $s_1 s_2 x_3 f = s_3 x_1 x_2$, so $f \mid r_3 x_1 x_2$. If $f \mid s_3$, then since S is saturated, $f \in S$, contradiction. So, being prime, f divides x_1 or x_2 in R, hence *a fortiori* in R_S and therefore it also divides either $\frac{x_1}{s_1}$ or $\frac{x_2}{s_2}$ in R_S, since these are associates to x_1 and x_2. □

THEOREM 15.58. *Every localization of a UFD is again a UFD.*

EXERCISE 15.29. *Prove Theorem 15.58.*
(Suggestions: one gets an easy proof by combining Theorem 15.1 with Proposition 15.57. But the result is also rather straightforward to prove directly.)

Certainly the converse of Theorem 15.58 is false: indeed, for *any* domain R with fraction field F, then F is a localization of R that is a UFD. However, in [**Na57**] M. Nagata gave an elegant and useful partial converse that is the subject of this section. It turns out that with some mild conditions on R, if for *the right kind* of multiplicative subset S of R we have that $S^{-1}R$ is a UFD, then we can indeed conclude that R itself is a UFD.

Roughly speaking, the condition on S that we want is that it be generated as a commutative monoid by prime elements. However, we will want to be just a bit more careful than this: for instance in the PID $\mathbb{Z}$, take $S = \{6^a \mid a \in \mathbb{N}\}$. Then S does not contain any primes at all, so certainly does not satisfy this condition. However, the saturation $\mathbf{S}$ of S is the submonoid of $\mathbb{Z}^+$ generated by the prime elements 2 and 3, and recall from Exercise 7.8 that the localizations $S^{-1}R$ and $\mathbf{S}^{-1}R$ are canonically isomorphic. This should serve to motivate the following definition:

A multiplicative subset S of a domain R is **primal** if its saturation $\mathbf{S}$ is generated as a monoid by units and prime elements of R.

EXERCISE 15.30. *Let S be a multiplicative subset of a domain R. Suppose that S is generated as a monoid by units and prime elements of R. Show: S is primal.*

LEMMA 15.59. *An irreducible element of a primal subset is prime.*

PROOF. If S is a primal multiplicative subset of R, $f \in S$ is irreducible and $\mathbf{S}$ is the saturation of S, then also f is an irreducible element of the primal multiplicative subset $\mathbf{S}$, so we may assume that S is saturated. By definition of primal, there is $u \in R^\times$ and prime elements $\pi_1, \ldots, \pi_n$ of R such that $f = u\pi_1 \cdots \pi_n$, and the irreducibility of f forces $n = 1$, so $f = u\pi_1$ is a prime element. □

THEOREM 15.60. *For an atomic domain R, the following are equivalent:*

(i) *Every multiplicative subset of R is primal.*
(ii) *R is a UFD.*

PROOF. (i) $\implies$ (ii): Since R is atomic, by Theorem 15.8 we have that R is a UFD if and only if irreducible elements of R are prime. By hypothesis, the saturated multiplicative set $R^\bullet$ is primal and f lies in $R^\bullet$, so f is a product of units and prime elements, hence (being irreducible) is a prime element.
(ii) $\implies$ (i): Suppose R is a UFD. Let S be a multiplicative subset of R, and let $\mathbf{S}$ be its saturation. Since R is a UFD, every $x \in \mathbf{S}$ is either a unit u or a product $\pi_1 \cdots \pi_n$ of prime elements, and since $\mathbf{S}$ is saturated, this means either $u \in \mathbf{S}$ or $\pi_1, \ldots, \pi_n \in \mathbf{S}$, so $\mathbf{S}$ is primal. □

There is not much content to Theorem 15.60, but it allows us to restate Theorem 15.58 as: the localization of a UFD at a primal subset is again a UFD. It is this formulation to which we can get a partial converse:

THEOREM 15.61. *(Nagata [**Na57**]) Let R be a domain, and let S be a primal subset of R such that $S^{-1}R$ is a UFD. If either of the following conditions holds, then R is a UFD:*

(i) *R is an atomic domain.*
(ii) *S is finitely generated as a commutative monoid.*

PROOF. First suppose that R is an atomic domain. We may, and shall, assume that S is saturated. By Theorem 15.8 it's enough to show: for all $f \in R$, if f is irreducible, then f is prime.
Case 1: $f \in S$. Since S is primal, Lemma 15.59 gives that f is prime.
Case 2: $f \notin S$, so by Exercise 7.9, we have that f is not a unit in $S^{-1}R$.
Step 1: We show that f is irreducible in $S^{-1}R$. If not, we may write $f = \frac{x_1}{s_1} \cdot \frac{x_2}{s_2}$ with $x_1, x_2 \in R \backslash S$ and $s_1, s_2 \in S$. Then $s_1 s_2 f = x_1 x_2$. By assumption, we may write

$$s_1 = u p_1 \cdots p_m \text{ and } s_2 = v q_1 \cdots q_n,$$

where $u, v \in R^\times$ and p_i, q_j are all prime elements of R. So $p_1 \mid x_1 x_2$; since p_1 is a prime, we must have either $\frac{x_1}{p_1} \in R$ or $\frac{x_2}{q_2} \in R$. Similarly for all the other p_i's and q_j's, so that we can at each stage divide either the first or the second factor on the right hand side by each prime element on the left hand side, without leaving the ring R. Therefore we may write $f = (\frac{1}{uv}) \frac{x_1}{t_1} \frac{x_2}{t_2}$ where t_1, t_2 are each products of the primes p_i and q_j, hence elements of S, and also such that $t_1 \mid x_1$, $t_2 \mid x_2$, i.e., the factorization takes place in R. Moreover $\frac{x_i}{t_i}$ is not a unit in $S^{-1}R$, hence *a fortiori* not a unit in R. Therefore we have exhibited a nontrivial factorization of f in R, contradiction.
Step 2: Since $S^{-1}R$ is a UFD, Step 1 implies that f is a prime element of $S^{-1}R$. Let $x, y \in R^\bullet$ be such that $f \mid xy$ in R. Then also $f \mid xy$ in $S^{-1}R$, so without loss of generality there is $s \in S$ such that $f \mid sx$. If s is a unit, we're done. If not, since S is primal there are prime elements $\pi_1, \ldots, \pi_n$ of S and $g \in S$ such that $fg = \pi_1 \cdots \pi_n x$. Since f is irreducible and does not lie in S, we cannot have $\pi_1 \mid f$; thus $\pi_1 \mid g$, and we may write $f g_1 = \pi_2 \cdots \pi_n x$. Continuing in this way, we get $g_n \in R$ such that $f g_n = x$, so $f \mid x$. Thus f is a prime element of R.

Now suppose that S is finitely generated as a monoid by $x_1, \ldots, x_n$. Since S is primal, each x_i is either a unit or product of prime elements. It follows that there is a finite set $\pi_1, \ldots, \pi_n$ of prime elements of R such that if S' is the multiplicative subset generated by $\pi_1, \ldots, \pi_n$, then the saturation of S is equal to the saturation of S', so $(S')^{-1}R \cong S^{-1}R$ is a UFD. Thus we may replace S with S'

and thereby assume that S is generated by finitely many prime elements $\pi_1, \ldots, \pi_n$. Since $S^{-1}R$ is obtained from R by iteratively localizing at the multiplicative subset generated by a single prime element, an easy inductive argument reduces us to the case $n = 1$: that is, we assume that R is a domain, π is a priime element of R, and for $S := \{1, \pi, \pi^2, \ldots, \pi^n, \ldots\}$ we have that $S^{-1}R$ is a UFD, and we must prove that R is a UFD. Step 1: Let p' be a prime element of $S^{-1}R$. Let $n \in \mathbb{N}$ be minimal so that

$$p := \pi^n p'$$

is an element of R. Let $x, y \in R$ be such that $p \mid xy$. Since in $S^{-1}R$ p is associate to the prime element p', then without loss of generality we have $p \mid x$ in $S^{-1}R$, so there is $a \in R$ and $N \in \mathbb{Z}^+$ such that $\pi^N x = ap$. The minimality of n in the definition of p ensures that $\pi \nmid p$; since moreover π is a prime element, we conclude that $\pi^N \mid a$ and thus

$$(\frac{a}{\pi^N})p = x,$$

so $p \mid x$. Thus p is a prime element of R that is associate to p' in $S^{-1}R$; it follows that p is not associate to π.
Step 2: Let $x \in R^\bullet \backslash R^\times$. If $x \in (S^{-1}R)^\times$, then by Exercise 7.9 we have that x divides π^n for some $n \in \mathbb{Z}^+$, which implies that x is associate to some power of π and thus is a product of prime elements. Otherwise there are prime elements $p_1', \ldots, p_n'$ of $S^{-1}R$ such that in $S^{-1}R$ we have

$$x = p_1' \cdots p_n'.$$

By Step 1, this means that there are prime elements $p_1, \ldots, p_n$ of R, none associate to π and $n \in \mathbb{Z}^+$ such that

$$\pi^n x = p_1 \cdots p_n.$$

But if $n \geqslant 1$ we have $\pi \mid p_1 \cdots p_n$ and thus $\pi \mid p_i$ for some i, a contradiction. So

$$x = p_1 \cdots p_n$$

is a product of prime elements. Thus R is a UFD. □

Let A be a UFD and consider $R = A[t]$. Put $S = A\backslash\{0\}$. As for any multiplicative subset of a UFD, S is generated by prime elements. But moreover, since $A[t]/(\pi A[t]) \cong (A/\pi A)[t]$, every prime element π of A remains prime in $A[t]$, so viewing S as the multiplicative subset of $A[t]$ consisting of nonzero constant polynomials, it too is generated by prime elements. But if F is the fraction field of A, $R_S = (A[t])_S = F[t]$ which is a PID and hence a UFD. Nagata's theorem applied to R and S now tells us – for the third time! – that $R = A[t]$ is a UFD.

Nagata used Theorem 15.61 to study the coordinate rings of affine quadric cones.

Let k be a field of characteristic different from 2, and let $f(x) = f(x_1, \ldots, x_n) \in k[x_1, \ldots, x_n]$ be a **quadratic form**, i.e., a homogeneous polynomial of degree 2 with k coefficients. We assume that f the associated bilinear form $(x, y) \mapsto \frac{1}{2}(f(x+y) - f(x) - f(y))$ is nonsingular. Equivalently, by making an invertible linear change of variables every quadratic form can be diagonalized, and a quadratic form is nonsingular if and only if it admits a diagonalization

$$f(x) = a_1 x_1^2 + \ldots + a_n x_n^2 \text{ with } a_1, \ldots, a_n \in k^\times. \tag{49}$$

We wish to study the **affine quadric cone** associated to f, namely $R_f = k[x]/(f)$. If quadratic forms f and g are isometric – i.e., differ by an invertible linear change

of variables – then $R_f \cong R_g$, so we assume if we like that f is in diagonal form as in (49) above. If $n \geqslant 3$ then every nonsingular diagonal quadratic polynomial is irreducible, so R_f is a domain.

THEOREM 15.62. *Let $f = f(x_1, \ldots, x_n) \in \mathbb{C}[x_1, \ldots, x_n]$ be a nondegenerate quadratic form. Then $R_f := \mathbb{C}[x_1, \ldots, x_n]/(f)$ is a UFD if and only if $n \geqslant 5$.*

PROOF. By the remarks above, R_f is a domain if and only if $n \geqslant 3$, so we may certainly restrict to this case. Because $\mathbb{C}$ is algebraically closed, every quadratic form in $n \geqslant 2$ variables is **isotropic**, i.e., there exists $0 \neq a \in k^n$ such that $f(a) = 0$: indeed, the first $n-1$ coordinates of a may be chosen arbitrarily. By an elementary theorem in the algebraic theory of quadratic forms [**La06**, Thm. I.3.4], we may make a change of variables to bring f into the form:

$$f(x) = x_1x_2 + g(x_3, \ldots, x_n).$$

Case 1: Suppose $n = 3$, so that

$$f(x) = x_1x_2 - ax_3^2$$

for some $a \in k^\times$. In this case, to show that R_f is not a UFD it suffices to show that the images $\overline{x_1}, \overline{x_2}, \overline{x_3}$ of x_1, x_2, x_3 in R_f are nonassociate irreducibles, for then $\overline{x_1x_2} = a\overline{x_3}^2$ exhibits a non-unique factorization! To establish this, regard $k[x_1, x_2, x_3]$ as a graded $\mathbb{C}$-algebra in the usual way – with x_1, x_2, x_3 each of degree 1 – so that the quotient R_f by the homogeneous ideal (f) inherits a grading. Since $\overline{x_1}$ has degree 1, if it were reducible, it would factor as the product of a degree one element $c_1x_1 + c_2x_2 + x_3x_3 + (f)$ and a degree zero element $r + (f)$, and thus

$$(rc_1 - 1)x_1 + rc_2x_2 + rc_3x_3 \in (f).$$

But the left hand side has degree 1, whereas all nonzero elements in (f) have degree 2 or higher, so $r \in \mathbb{C}[x]^\times$ and therefore the factorization is trivial. The irreducibility of $\overline{x_2}$ and $\overline{x_3}$ is proved in the same way. If $\overline{x_1} \sim \overline{x_3}$ in R_f, then we may divide both sides of $\overline{x_1x_2} - a\overline{x_3}^2$ by $\overline{x_1}$ and deduce that also $\overline{x_2} \sim \overline{x_3}$. But in the quotient ring $R_f/(\overline{x_3})$, $\overline{x_3}$ maps to 0 and $\overline{x_1}$ and $\overline{x_2}$ do not, contradiction. So R_f is not a UFD.
Case 2: Suppose $n = 4$, so $f(x) = x_1x_2 + g(x_3, x_4)$, where $g(x_3, x_4)$ is a nonsingular binary form. Here for the first time we use the full strength of the quadratic closure of k: since $k^\times = k^{\times 2}$, any two nonsingular quadratic forms in the same number of variables are isometric, so we may assume WLOG that

$$f(x) = x_1x_2 - x_3x_4.$$

Now we argue exactly as in Case 1 above: in R_f, the images $\overline{x_1}, \overline{x_2}, \overline{x_3}, \overline{x_4}$ are all non-associate irredcuble elements, so $\overline{x_1x_2} = \overline{x_3x_4}$ is a non-unique factorization.
Case 3: $n \geqslant 5$. Then $n-2 \geqslant 3$, so g is irreducible in the UFD $\mathbb{C}[x_3, \ldots, x_n]$, hence also in $\mathbb{C}[x_2, x_3, \ldots, x_n]$. Therefore $R_f/(\overline{x_1}) = \mathbb{C}[x_1, \ldots, x_n]/(x_1, f) = \mathbb{C}[x_2, \ldots, x_n]/(g)$ is a domain, i.e., $\overline{x}_1$ is a prime element. Moreover,

$$R[\overline{x_1}^{-1}] = \mathbb{C}[x_1, \ldots, x_n, x_1^{-1}]/(x_1x_2 - g)$$

$$\cong \mathbb{C}[x_1, \ldots, x_n, x_1^{-1}]/(x_2 - \frac{g}{x_1}) \cong \mathbb{C}[x_1, x_3, \ldots, x_n, x_1^{-1}]$$

is a localization of the UFD $\mathbb{C}[x_1, x_3, \ldots, x_n]$ hence a UFD. By Nagata's Criterion (Theorem 15.61), R_f itself is a UFD. □

Now let k be a field of characteristic not 2 and $f \in k[x_1, \ldots, x_n]$ a nondegenerate quadratic form. Without changing the isomorphism class of R_q we may diagonalize f; moreover without changing the ideal (f) we may scale by any element of $k^\times$, so without loss of generality we need only consider forms $x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2$.

THEOREM 15.63. *Let k be a field of characteristic different from 2, let $a_2, \ldots, a_n \in k^\times$, and let*

$$f = x_1^2 + a_2x_2^2 + \ldots + a_nx_n^2,$$

so f is a nonsingular form over k. Put $R_f := k[x_1, \ldots, x_n]/(f)$.

a) *If $n \leqslant 2$ then R_f is not a UFD.*
b) *If $n = 3$, then R_f is a UFD if and only if f is aniostropic: for all $a \in k^n$, if $f(a) = 0$ then $a = 0$.*
c) *Suppose $f = x_1^2 - ax_2^2 - bx_3^2 - cx_4^2$.*
   (i) *If a is a square in k, then R_f is a UFD if and only if $-bc$ is not a square in k.*
   (ii) *If none of a, b, c, $-ab$, $-ac$, $-bc$ is a square in k, then R_f is a UFD if and only if $-abc$ is not a square.*
d) *If $n \geqslant 5$, then R_f is a UFD.*

PROOF. a) If $n \leqslant 2$, R_f is never an integrally closed domain. Indeed, if $n = 1$, then $R_f = k[x_1]/(x_1^2)$ is not a domain. If $n = 2$, then $R_f = k[x_1, x_2]/(x_1^2 + a_2x_2^2)$ is a domain if and only if $x_1^2 + a_2x_2^2$ is irreducible if and only if $x_1^2 + a_2$ is irreducible if and only if $-a_2$ is not a square in k. If $-a_2$ is not a square in k, then $R_f \cong k[x_2][\sqrt{-a_2x_2^2}] = k[x_2][x_2\sqrt{-a}]$. Thus $\sqrt{-a}$ lies in the fraction field of R_f and is integral over R_f but does not lie in R_f.
b) The proof of Theorem 15.62 goes through to show that if f is isotropic (i.e., not anisotropic), R_f is not a UFD. The anisotropic case is due to Samuel [**Sa64**].
Part c) is due to T. Ogoma [**O74**].
Part d) goes back at least to van der Waerden [**vdW39**]. In [**Na57**], M. Nagata gives a short proof using Theorem 15.61. □

It is also interesting to consider affine rings of inhomogeneous quadric hypersurfaces. For instance, we state without proof the following result.

THEOREM 15.64. *For $n \geqslant 1$, let $R_n := \mathbb{R}[t_1, \ldots, t_{n+1}]/(t_1^2 + \ldots + t_{n+1}^2 - 1)$ be the ring of polynomial functions on the n-sphere S^n.*

a) *(Bouvier [**Bo78**]) If $n \geqslant 2$, then R_n is a UFD.*
b) *(Trotter [**Tr88**]) R_1 is isomorphic to the ring $\mathbb{R}[\cos\theta, \sin\theta]$ of real trigonometric polynomials, in which $(\sin\theta)(\sin\theta) = (1 + \cos\theta)(1 - \cos\theta))$ is an explicit non-unique factorization into irreducible elements. Hence R_1 is not a UFD.*

12. The Euclidean Criterion

In this section we give a commutative algebraic generalization of Euclid's proof that there are infinitely many prime numbers, following [**Cl17a**]. Euclid's result on the face of it pertains to irreducible elements. It happens that in $\mathbb{Z}$ every irreducible element is prime, but that is a different (and deeper) result of Euclid.

It will be helpful to slightly adjust our terminology: here an **atom** will be the

principal ideal generated by an irreducible element, so two irreducible elements determine the same atom if and only if they are associate. It seems more interesting to count atoms than irreducible elements, since in particular whenever an atomic domain that is not a field has infinite unit group it necessarily has infinitely many irreducible elements but not necessarily infinitely many atoms.

In fact our generalization works in some domains in which not all nonzero nonunits factor into irreducibles. A **Furstenberg domain** is a domain R in which every nonzero nonunit has an irreducible divisor.

We call a ring **semiprimitive** if it has zero Jacobson radical: i.e., if the only element lying in every maximal ideal is zero.

EXERCISE 15.31. a) *Show: every atomic domain is a Furstenberg domain.*
b) *Show: the ring* $\mathrm{Hol}(\mathbb{C})$ *of holomorphic functions on the complex plane is a semiprimitive Furstenberg domain that is not an atomic domain.*

EXERCISE 15.32. a) *Show that for a ring R the following conditions are equivalent:*
(i) *There is an infinite sequence $\{I_n\}_{n=1}^{\infty}$ of pairwise comaximal, proper ideals of R.*
(ii) *The set* $\mathrm{MaxSpec}\, R$ *is infinite.*
b) *Let R be a semiprimitive domain that is not a field. Show:* $\mathrm{MaxSpec}\, R$ *is infinite.*

THEOREM 15.65. *(Euclidean Criterion* [**Cl17a**, Thm. 2.3]*) Let R be a semiprimitive domain that is not a field.*
a) *There is a sequence $\{a_n\}_{n=1}^{\infty}$ of pairwise comaximal nonunits.*
b) *Suppose moreover that R is a Furstenberg domain. Then there is a sequence $\{p_n\}_{n=1}^{\infty}$ of pairwise comaximal irreducible elements. In particular R has infinitely many atoms.*

PROOF. a) We go by induction on n. Since R is not a field there is $a_1 \in R^\bullet \backslash R^\times$. Having chosen $a_1, \ldots, a_n$ that are pairwise comaximal nonunits, because $J(R) = (0)$ and R is a domain, there is $y \in R$ such that

$$a_{n+1} := ya_1 \cdots a_n + 1 \in R^\bullet \backslash R^\times.$$

(Because $a_1 \notin R^\times$ we cannot have $a_{n+1} = 0$.) Evidently we have $\langle a_i, a_{n+1} \rangle = R$ for all $1 \leqslant i \leqslant n$.
b) Again we go by induction on n. Since R is a Furstenberg domain and not a field there is some irreducible element p_1. Having chosen pairwise comaximal irreducible elements $p_1, \ldots, p_n$, because $J(R) = 0$ there is $y \in R$ such that

$$x := yp_1 \cdots p_n + 1 \in R^\bullet \backslash R^\times.$$

Because we are in a Furstenberg domain, the element x has an irreducible divisor p_{n+1}. Then for all $1 \leqslant i \leqslant n$ we have

$$1 = \left(\frac{x}{p_{n+1}}\right) p_{n+1} - y \left(\prod_{j \neq i} p_j\right) p_i,$$

which shows that $\langle p_i, p_{n+1} \rangle = 1$. Comaximal irreducible elements are nonassociate, so R has infinitely many atoms. □

COROLLARY 15.66. *For any domain R, the domain $R[t]$ has infinitely many atoms.*

EXERCISE 15.33. *Prove Corollary 15.66. (Hint: the most interesting case is when R is finite!)*

COROLLARY 15.67. *Let R be a Furstenberg domain, not a field, such that $\#R > \#R^\times$. Show: R has infinitely many atoms.*

EXERCISE 15.34. a) *Prove Corollary 15.67. (Suggestion: make use of the fact that $\#I = \#R$ for every nonzero ideal of R.)*
b) *Deduce that if $R = \mathbb{Z}$ or if $R = \mathbb{Z}[\sqrt{-1}]$ then R has infinitely many atoms.*

EXERCISE 15.35. *Let K be a number field – i.e., a finite degree extension of $\mathbb{Q}$ – and let $\mathbb{Z}_K$ be the integral closure of $\mathbb{Z}$ in K. Can you use Theorem 15.65 to show that $\mathbb{Z}_K$ has infinitely many atoms?*[3]

EXERCISE 15.36. *Let $\overline{\mathbb{Z}}$ be the ring of all algebraic integers – i.e., the integral closure of $\mathbb{Z}$ in $\mathbb{C}$. Show: $\overline{\mathbb{Z}}$ is a semiprimitive domain that is not a field that has no irreducible elements. Thus in Theorem 15.65b) the hypothesis that R is a Furstenberg domain cannot be omitted.*

EXERCISE 15.37. *Let R be an integrally closed, Noetherian domain of Krull dimension one. (In other words, R is a Dedekind domain that is not a field. See Chapter 20 for more on Dedekind domains. Results from this chapter may be helpful in solving this exercise.) Show that the following are equivalent:*

(i) *R is semiprimitive.*
(ii) *R has infinitely many maximal ideals.*
(iii) *R has inifnitely many atoms.*

PROPOSITION 15.68. *Let R be a Noetherian domain of Krull dimension one. Then R is semiprimitive if and only if* $\operatorname{MaxSpec} R$ *is infinite. When these conditions hold, R has infinitely many atoms.*

PROOF. For any domain R, if $\operatorname{MaxSpec} R = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_n\}$ is finite, then

$$J(R) = \bigcap_{i=1}^n \mathfrak{m}_i \supset \prod_{i=1}^n \mathfrak{m}_i \supsetneq (0),$$

so R is not semiprimitive. Conversely, if $J(R) \supsetneq (0)$, then maximal ideals of R are minimal prime ideals of the Noetherian ring $R/J(R)$ hence are finite in nubmer by Theorem 10.14. Since Noetherian domains are atomic and atomic domains are Furstenberg, when $\operatorname{MaxSpec} R$ is infinite the Euclidean Criterion applies to show that R has infinitely many atoms. □

LEMMA 15.69. *In an atomic domain, every prime ideal is generated by irreducible elements.*

[3]In fact $\mathbb{Z}_K$ has infinitely many principal prime ideals, but this is a rather deep theorem in algebraic number theory.

PROOF. Let $\mathfrak{p}$ be a prime ideal of the atomic domain R, and let $\{x_s\}_{s\in S}$ be a set of nonzero generators for $\mathfrak{p}$. Since R is atomic, we may factor $x_s = f_{s,1}\cdots f_{s,n_s}$ into irreducibles. Since $f_{s,1}\cdots f_{s,n_s}$ lies in the prime ideal $\mathfrak{p}$, some f_{s,j_s} does. By replacing $\{x_s\}_{s\in S}$ by $\{f_{s,j_s}\}_{s\in S}$ we get a set of irreducible generators for $\mathfrak{p}$. □

THEOREM 15.70. *Let R be an atomic domain with finitely atoms. Then R is semilocal Noetherian and* $\dim R \leqslant 1$.

PROOF. By Lemma 15.69, every prime ideal of R is generated by irreducibles. Since replacing a generator by an associate element does not change the ideal generated, we conclude that every prime ideal is finitely generated – so R is Noetherian by Cohen's Theorem (Theorem 4.32) – and that there are only finitely many prime ideals. If the Noetherian domain R had a nonzero, nonmaximal prime ideal $\mathfrak{p}$, then let $\mathfrak{m}$ be a maximal ideal strictly containing $\mathfrak{p}$. By Corollary 8.53, there are infinitely many prime ideals $\mathfrak{q}$ with $(0) \subsetneq \mathfrak{q} \subsetneq \mathfrak{m}$, contradiction. □

Here is what we have shown so far: if R is an atomic domain, not a field, with finitely many atoms, then R must be semilocal, Noetherian and of Krull dimension 1. Conversely, if R is semilocal, Noetherian of Krull dimension 1 and integrally closed, then R has finitely many atoms. It's natural to attempt to remove the integral closure hypothesis and thereby get a characterization of atomic domains with finitely many atoms. However, things are not so simple:

EXAMPLE 15.71. *Let k be a field, and consider the subring*

$$R = k[[t^2, t^3]] = k + t^2 k[[t]]$$

of the formal power series ring $k[[t]]$. For $0 \neq f = \sum_{n=0}^{\infty} a_n t^n \in k[[t]]$, we define $v(f)$ to be the least n such that $a_n \neq 0$. Then v is a discrete valuation on $k[[t]]$, and the only nonzero prime ideal of $k[[t]]$ is $(t) = \{f \in R \mid v(f) > 0\} \cup \{0\}$. The element t is integral over R – it satisfies the monic polynomial $x^2 - t^2$ – and from this it follows that the only nonzero prime ideal of R is

$$\mathfrak{m} = (tk[[t]]) \cap R = t^2 k[[t]] = \{f \in R \mid v(f) \geqslant 2\} \cup \{0\} = \langle t^2, t^3 \rangle.$$

and $R^\times = \{a_0 + \sum_{n\geqslant 2} a_n t^n \mid a_0 \neq 0\}$. We will give a complete description of the irreducibles of R. First we claim that $f \in R$ is irreducible if and only if $v(f) \in \{2, 3\}$. Indeed a nontrivial factorization $f = xy$ involves $v(x), v(y) \geqslant 2$ hence $v(f) \geqslant 4$; conversely, if $v(f) \geqslant 4$ then $f = t^2 \frac{f}{t^2}$ is a nontrivial factorization. Since $k^\times \subset R^\times$, every irreducible is associate to one of the form

$$t^2 + \sum_{n\geqslant 3} a_n t^n, \ (v(f) = 2 \text{ case})$$

or one of the form

$$t^3 + \sum_{n\geqslant 4} a_n t^n, \ (v(f) = 3 \text{ case}).$$

Associate elements have the same valuation, so certainly no irreducible of the first type is associate to an irreducible of the second type. We claim that $t^2 + \sum_{n\geqslant 3} a_n t^n$ is associate to $t^2 + \sum_{n\geqslant 3} b_n t^n$ if and only if $a_3 = b_3$ and $t^3 + \sum_{n\geqslant 3} a_n t^n$ is associate to $t^3 + \sum_{n\geqslant 3} b_n t^n$ if and only if $a_4 = b_4$. This can be done by direct computation:

$$\begin{aligned}&(t^2 + a_3 t^3 + a_1 4t^4 + a_5 t^5 + \ldots)(1 + u_2 t^2 + u_3 t^3 + \ldots)\\ &= t^2 + a_3 t^3 + (a_4 + u_2) t^4 + (a_5 + a_3 u_2 + u_3) t^5 + \ldots,\end{aligned}$$

so $a_3 = b_3$ and there is a unique choice of $u_2, u_3, \ldots$ leading to $a_n = b_n$ for all $n \geqslant 4$. The $v(f) = 3$ case is similar. Thus there are precisely $2\#k$ atoms, and hence a finite number if and only if k is finite.

CHAPTER 16

Principal Rings and Bézout Domains

A ring R in which every ideal is principal is called a **principal ring**. If R is moreover a domain, it is called a **principal ideal domain** (PID).

1. Principal ideal domains

PROPOSITION 16.1. *Let R be a UFD.*

a) *If every maximal ideal of R is principal, then R is a PID.*

b) *The ring R is a PID if and only if* $\dim R \leqslant 1$.

PROOF. a) Let R be a UFD in which every maximal ideal is principal. By Theorem 4.31 it is enough to show that every prime ideal in R is principal. Let $\mathfrak{p} \in \operatorname{Spec} R$ be a nonzero prime ideal. By Theorem 15.1, $\mathfrak{p}$ contains a prime element p. But also $\mathfrak{p}$ lies in a maximal ideal $\mathfrak{m} = (\ell)$, so

$$(p) \subset \mathfrak{p} \subset \mathfrak{m} = (\ell).$$

Thus $\ell \mid p$; since p is a prime element we get $(p) = (\ell)$, so $\mathfrak{p} = \mathfrak{m} = (\ell)$ is principal. b) The proof of part a) shows that in no domain can one have a proper containment of nonzero principal prime ideals. From this it follows that a PID has dimension at most 1. Conversely, Theorem 15.1 implies that every height one prime ideal in a UFD is prinicpal, so if $\dim R \leqslant 1$ then every prime ideal in R is principal, so – again by Theorem 4.31 – we get that R is a PID. □

EXERCISE 16.1. *We develop an alternate proof of Proposition 16.1a) following W. Dubuque.*

a) *Let R be a UFD, and let $S \subset R^\bullet$ be any subset. Show:* $\gcd(S)$ *exists.*

b) *Let R be a UFD in which all maximal ideals are principal, let I be a nonzero ideal in R. Show that we may write $I = \gcd(I)J$ for an ideal J which is not contained in any proper principal ideal, and conclude that $I = \gcd(I)$ is principal.*

We now follow with some very familiar examples.

PROPOSITION 16.2. *The integer ring $\mathbb{Z}$ is a principal ideal domain.*

PROPOSITION 16.3. *For any field k, the univariate polynomial ring $k[t]$ is a principal ideal domain.*

Surely the most reasonable way to prove Propositions 16.2 and 16.3 is by exploiting the division algorithms that both rings are well known to possess. We will consider Euclidean rings later in this chapter, so for now we take it as a challenge to bring the theory we have developed so far to bear to give other, less reasonable, proofs! For a property P of rings, a ring R is **residually P** if for all nonzero ideals I of R, the quotient R/I has property P.

LEMMA 16.4.

a) *The ring $\mathbb{Z}$ is residually Artinian.*
b) *For any field k, the ring $k[t]$ is residually Artinian.*
c) *If a ring R is residually Artinian, then* $\dim R \leqslant 1$.

PROOF. a) For any nonzero $n \in \mathbb{Z}$, the ring $\mathbb{Z}/n\mathbb{Z}$ is finite and thus Artinian.
b) For any nonzero $n(t) \in k[t]$, the ring $k[t]/(n(t))$ is a k-vector space of dimension equal to the degree of $n(t)$. So $k[t]/(n(t))$ is Artinian as a k-module hence *a fortiori* is Artinian as a ring.
c) By contraposition: if $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subset \mathfrak{p}_2$ are prime ideals, then the chain $\mathfrak{p}_1 \subset \mathfrak{p}_2$ shows that $\dim R/\mathfrak{p}_1 \geqslant 1$, so $R/\mathfrak{p}_1$ is not Artinian. □

Combining Proposition 16.1 and Lemma 16.4 we find that it suffices to show that the rings $\mathbb{Z}$ and $k[t]$ are PIDs it suffices to show that they are UFDs. Indeed we have already seen that $k[t]$ is a UFD, a special case of Theorem 15.27. As for showing that $\mathbb{Z}$ is a UFD, here are two proofs the reader may not have seen before:

First proof: Indeed a decomposition $n = p_1 \cdots p_r$ corresponds to a composition series for the $\mathbb{Z}$-module $\mathbb{Z}/n\mathbb{Z}$. Since $\mathbb{Z}/n\mathbb{Z}$ is finite, it is certainly Noetherian and Artinian, so composition series exist. Moreover the Jordan-Hölder theorem implies that any two composition series have the same number of terms – i.e., $r = s = \ell(\mathbb{Z}/n\mathbb{Z})$ – and that after a permutation the sequences of isomorphism classes of composition factors become identical.

Second proof (Lindemann [**Li33**], Zermelo [**Ze34**]): We prove both the existence and uniqueness of the factorization by an inductive argument, specifically by appeal to the well-ordering of the positive integers under $\leqslant$.

Existence: let S be the set of integers $n > 1$ which *do not* have at least one prime factorization. We wish to show that S is empty so, seeking a contradiction, suppose not. Then by well-ordering S has a least element, say N. If N is prime, then we have found a prime factorization, so suppose it is not prime: that is, we may write $N = N_1N_2$ with $1 < N_1, N_2 < N$. Thus N_1 and N_2 are too small to lie in S so each have prime factorizations, say $N_1 = p_1 \cdots p_r,\ N_2 = q_1 \cdots q_s$, and then $N = p_1 \cdots p_r q_1 \cdots q_s$ gives a prime factorization of N, contradiction!

Uniqueness: we claim that the factorization of a positive integer is unique. Assume not; then the set of positive integers which have at least two different standard form factorizations is nonempty, so has a least element, say N, where:

$$N = p_1 \cdots p_r = q_1 \cdots q_s. \tag{50}$$

Here the p_i's and q_j's are prime numbers, not necessarily distinct from each other. However, we must have $p_1 \neq q_j$ for any j. Indeed, if we had such an equality, then we could cancel and, by an inductive argument we have already rehearsed, reduce to a situation in which the factorization must be unique. In particular $p_1 \neq q_1$. Without loss of generality, assume $p_1 < q_1$. Then, if we subtract $p_1q_2 \cdots q_s$ from both sides of (50), we get

$$M := N - p_1q_2 \cdots q_s = p_1(p_2 \cdots p_r - q_2 \cdots q_s) = (q_1 - p_1)(q_2 \cdots q_s). \tag{51}$$

By the assumed minimality of N, the prime factorization of M must be unique. However, (51) gives two different factorizations of M, and we can use these to get a contradiction. Specifically, $M = p_1(p_2 \cdots p_r - q_2 \cdots q_s)$ shows that $p_1 \mid M$.

Therefore, when we factor $M = (q_1 - p_1)(q_2 \cdots q_s)$ into primes, at least one of the prime factors must be p_1. But $q_2, \ldots, q_j$ are already primes which are different from p_1, so the only way we could get a p_1 factor is if $p_1 \mid (q_1 - p_1)$. But this implies $p_1 \mid q_1$, and since q_1 is also prime this implies $p_1 = q_1$. Contradiction!

EXERCISE 16.2. *Let R be a ring, and suppose that the univariate polynomial ring $R[t]$ is a PID. Show: R is a field.*

PROPOSITION 16.5. *Let R be a Noetherian local ring with a principal maximal ideal $\mathfrak{m} = (a)$. Then every nonzero ideal of R is of the form (a^i) for some $i \in \mathbb{N}$. In particular, R is a principal ring.*

PROOF. The Krull Intersection Theorem gives $\bigcap_i \mathfrak{m}^i = \bigcap_i (a^i) = 0$. It follows that for any nonzero $r \in R$, there exists a largest $i \in \mathbb{N}$ such that $r \in (a^i)$, i.e., there exists $s \in R$ such that $r = sa^i$. But if s were not a unit then it would lie in $\mathfrak{m}$ and thus r would lie in $\mathfrak{m}^{i+1}$, contradiction. So s is a unit and $(r) = \mathfrak{m}^i$. Thus to every nonzero element r of I we attach a non-negative integer i_r. Now if I is any nonzero ideal of R, choose a nonzero element r of I with i_r minimal among elements of I. Then $I \supset (r) = \mathfrak{m}^i$, and the other containment follows by minimality of i_r. □

PROPOSITION 16.6. *For any field k, the formal power series ring $k[[t]]$ is a PID.*

EXERCISE 16.3. *Give several proofs of Proposition 16.6.*
(Suggestions: (i) Use Theorem 8.40a). (ii) Use Theorem 8.40b) and Proposition 16.5.) (iii) Let I be a nonzero ideal in $k[[t]]$ and let $f \in I$ be an element whose "order of vanishing" – i..e., the index of the least nonzero Laurent series coefficient – is minimal among elements of I. Show: $I = \langle f \rangle$.)

1.1. Dedekind-Hasse Norms. Let R be a domain. A map

$$|\cdot| : R \to \mathbb{N}$$

is a **norm** if all of the following hold:
(N0) For all $x, y \in R$, we have $|xy| = |x||y|$.
(N1) For all $x \in R$, we have $|x| = 0 \iff x = 0$.
(N2) For all $x \in R$, we have $|x| = 1 \iff x \in R^\times$.

A field k admits a unique norm: we must have $|0| = 0$ and $|x| = 1$ for all $x \in k^\bullet$. In general, a norm $|\cdot|$ on a domain R extends to its fraction field K as a map

$$|\cdot| : K \to \mathbb{Q}^{\geqslant 0}, \ \frac{x}{y} \mapsto \frac{|x|}{|y|}.$$

This is the unique such extension that retains property (N0): for all $x, y \in K$ we have $|xy| = |x||y|$. This extension retains property (N1) but property (N2) may be lost: for $x \in K^\times$, we may have $|x| = 1$ without having $x \in R$.

EXAMPLE 16.7.

a) *The standard absolute value defines a norm $|\cdot| : \mathbb{Z} \to \mathbb{N}$.*
b) *Let k be a field. We define a map $|\cdot| : k[t] \to \mathbb{N}$ by $|0| := 0$ and, for $f \in k[t]^\bullet$, $|f| := 2^{\deg f}$. This is a norm on $k[t]$.*
c) *Let R be a UFD, and let $\{\pi_i\}_{i \in I}$ be a family of prime elements of R such that for every prime element π there is exactly one $i \in I$ such that $(\pi) = (\pi_i)$. (Such a family always exists.) If $|\cdot| : R \to \mathbb{N}$ is a norm on R,*

then for all $i \in I$ there is an integer $n_i \geqslant 2$ such that $|\pi_i| = n_i$. This data determines the norm: any $x \in R^\bullet$ may be written as $u\pi_{i_1} \cdots u\pi_{i_r}$ and we have $|x| = \prod_{i=1}^r n_i$. Conversely, for each $i \in I$ let $n_i \in \mathbb{Z}^{\geqslant 2}$. Then

$$|u\pi_{i_1} \cdots \pi_{i_r}| := \prod_{i=1}^r n_i$$

is a norm on R.

Let R be a domain with fraction field K. A **Dedekind-Hasse norm** on a domain R is a norm $|\cdot| : R \to \mathbb{N}$ satisfying the following additional property: for all $x \in K\backslash R$ there are $a, b \in R$ such that $0 < |ax - b| < 1$.

PROPOSITION 16.8. *Let R be a domain with fraction field K.*

a) *R is a PID if and only if it admits a Dedekind-Hasse norm.*
b) *If R is a PID, then every norm is Dedekind-Hasse norm.*

PROOF. Step 1: Suppose that R admits a Dedekind-Hasse norm $|\cdot|$. Let I be a nonzero ideal of R, and let $d \in I^\bullet$ be an element on which $|d|$ is minimal among nonzero elements of I. We claim that $I = (d)$: if not, there is $x \in I$ such that $\frac{x}{d} \in K\backslash R$, and since $|\cdot|$ is a Dedekind-Hasse norm there are $a, b \in R$ such that $0 < |\frac{ax}{d} - b| < 1$. Thus $ax - bd \in I$ and $0 < |ax - bd| < |d|$, so $ax - bd \in I^\bullet$ has smaller norm than the norm of d: contradiction.
Step 2: If R is a PID, then it is a UFD, so by Example 16.7c) it admits a norm $|\cdot|$. To complete the proof it suffices to show that the (arbitrary) norm $|\cdot|$ is Dedekind-Hasse. Let $x \in K\backslash R$. We may write $x = \frac{p}{q}$ with $p, q \in R^\bullet$, $q \notin R^\times$ and $\gcd(p, q) = 1$; since R is a PID there are $a, b \in R$ such that $ap - bq = q$. Thus

$$|ax - b| = \left|\frac{ap}{q} - b\right| = \left|\frac{1}{q}\right| \in (0, 1). \qquad \square$$

2. Structure theory of principal rings

PROPOSITION 16.9. *Let R be a principal ring.*

a) *For any multiplicative subset S, the localization R_S is principal.*
b) *For any ideal I of R, the quotient R/I is principal.*

EXERCISE 16.4. *Prove Proposition 16.9.*

PROPOSITION 16.10. *For rings $R_1, \ldots, R_n$, the following are equivalent:*

(i) *Each R_i is a principal ring.*
(ii) *The direct product $\prod_{i=1}^n R_i$ is a principal ring.*

EXERCISE 16.5.

a) *Prove Proposition 16.10.*
b) *Show: no infinite product of nonzero principal rings is a principal ring.*

A principal ring $(R, \mathfrak{m})$ is **special** if it is a local Artinian ring, i.e., if it is local and the maximal ideal is principal and nilpotent. The complete structure of ideals in special principal rings can be deduced from Proposition 16.5: if n is the least positive integer such that $\mathfrak{m}^n = 0$, then the ideals of R are precisely the powers $\mathfrak{m}^i = (\pi^i)$ for $0 \leqslant i \leqslant n$.

We now give a structure theorem for principal rings, due originally to Krull [**Kr24**], as a byproduct of a striking result of Kaplansky [**Ka49**].

THEOREM 16.11.

a) *(Kaplansky) Let R be a Noetherian ring in which each maximal ideal is principal. Then R is the direct product of a finite number of PIDs and special principal rings.*

b) *(Krull) A ring is principal if and only if it is a finite direct product of rings, each of which is either a PID or a special principal ring.*

PROOF. It suffices to prove part a), for then part b) follows immediately.

Step 1: Since R is Noetherian of dimension at most 1, it has finitely many minimal primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$, and all other primes are maximal. The irreducible components of $\operatorname{Spec} R$ are $V(\mathfrak{p}_1), \ldots, V(\mathfrak{p}_r)$. We claim that the irreducible components are pairwise disjoint: if not there is $\mathcal{P} \in \operatorname{MaxSpec} R$ containing two distinct minimal primes, and then $R_{\mathcal{P}}$ is a Noetherian local ring with principal maximal ideal and more than one minimal prime. In particular its ideals are not totally ordered under inclusion, which contradicts Proposition 16.5.

In other words, the minimal primes are pairwise comaximal. By Exercise 10.13 there is $N \in \mathbb{Z}^+$ such that $\bigcap_{i=1}^r \mathfrak{p}_i^N = (0)$. Taking $R_i := R/\mathfrak{p}_i^N$, the Chinese Remainder Theorem gives

$$R = \prod_{i=1}^r R_i.$$

The maximal ideals of R_i are precisely the pushforwards under the quotient map of the maximal ideals of R containing $\mathfrak{p}_i$, so each R_i is a Noetherian ring in which each maximal ideal is principal and having a unique minimal prime. So it suffices to show that a Noetherian ring R having a unique minimal prime in which each maximal ideal is principal is either a PID or a special principal ring.

Step 2: If $\dim R = 0$ then R is Artinian local with principal maximal ideal, so Proposition 16.5 implies that R is a special principal ring. So suppose $\dim R = 1$. If $\operatorname{nil} R = (0)$ then we are assuming that all the prime ideals of R are principal, so R is a PID by Theorem 4.31. If $\operatorname{nil} R \supsetneq (0)$, let x be a nonzero nilpotent element, and let $\mathcal{P}$ be a maximal ideal containing $\operatorname{ann}(x)$. Then the image of x in $R_{\mathcal{P}}$ is a nonzero nilpotent. The ring $R_{\mathcal{P}}$ is one-dimensional local with principal maximal ideal $\mathcal{P}R_{\mathcal{P}} = \langle a \rangle$, say, so by Proposition 16.5 every nonzero ideal of $R_{\mathcal{P}}$ is of the form $\langle a^i \rangle$ for some $i \in \mathbb{N}$. In such a ring the only nonzero prime ideal is $\langle a \rangle$, so since $R_{\mathcal{P}}$ has dimension 1, the zero ideal must be prime and $R_{\mathcal{P}}$ must be a domain, contradicting the existence of nonzero nilpotent elements. □

Having studied PIDs, let us now turn to the case of special principal rings and principal Artinian rings: to be sure a ring is principal Artinian if and only if it is a finite product of special principal rings.. The most familiar examples of principal Artinian rings (resp. of special principal rings) are $\mathbb{Z}/n\mathbb{Z}$ (resp. $\mathbb{Z}/p^a\mathbb{Z}$ for a prime number p). Any quotient of a PID by a nonzero ideal is a principal Artinian ring (Exercise 16.9a)) and any quotient of a PID by a prime power ideal is a special principal ring.

A ring R is **self-injective** if R is an injective R-module. By Exercise 3.51d), a domain is self-injective if and only if it is a field.

EXERCISE 16.6. *Let $\{R_i\}_{i \in I}$ be a family of nonzero rings, and put $R := \prod_{i \in I} R_i$. Show: R is self-injective if and only if R_i is self-injective for all $i \in I$.*

PROPOSITION 16.12. *A principal Artinian ring is self-injective.*

PROOF. Every special principal ring is a finite product of local special principal rings, so by Exercise 16.6 we reduce to the case of a local special principal ring $(R, (\pi))$. By Proposition 16.5 if N is the least positive integer such that $\pi^N = 0$ then the ideals of R are precisely (π^a) for $0 \leqslant a \leqslant N$. By Baer's Criterion it is enough to extend every R-module homomorphism $\varphi : (\pi^a) \to R$ to all of R. The R-module (π^a) is cyclic with annihilator (π^{N-a}), hence $(\pi^a) \cong_R R/(\pi^{N-a})$, so each such homomorphism is uniquely specified by mapping π^a to any element of R killed by π^{N-a}, i.e., to any element of (π^a). Thus φ maps π^a to $x\pi^a$ for some $x \in R$, and we can extend it to $[x] : R \to R$, i.e., $y \in R \mapsto xy$. □

Proposition 16.12 implies that for $N > 1$ the ring $\mathbb{Z}/N\mathbb{Z}$ is self-injective. It follows that if A is an N-torsion commutative group and $x \in A$ has order N, then there is a subgroup B of A such that $A = \langle x \rangle \oplus B$. This is precisely what is needed in order to write a finite commutative group as a direct sum of cyclic subgroups. More generally, we can recover the following well known structure theorem.

THEOREM 16.13. *Every finitely generated module over a PID is a finite direct sum of cyclic modules.*

PROOF. Let R be a PID, and let M be a finitely generated R-module. As usual, we have the short exact sequence

$$0 \to M[\text{tors}] \to M \to M/M[\text{tors}] \to 0.$$

The module $M/M[\text{tors}]$ is finitely generated and torsionfree, hence by Theorem 3.64 is free, i.e., is isomorphic to a finite direct sum of copies of R itself. Since R is Noetherian and M is finitely generated, the torsion submodule $T := M[\text{tors}]$ is also finitely generated, hence it has nonzero annihilator $I = (a)$. Thus T is a finitely generated module over the special principal ring $R/(a)$. We claim that it has an element x with annihilator (a), so that the R-submodule $\langle x \rangle$ is isomorphic to $R/(a)$. Assuming the claim for the moment, we have an R-submodule T_2 of T such that $T = \langle x \rangle \oplus T'$. The submodule T', also being a quotient of T, is again a finitely generated torsion submodule, so we can argue as above splitting off direct summands. Since $\langle x_1 \rangle \subsetneq \langle x_1 \rangle \oplus \langle x_2 \rangle \subsetneq$ an ascending chain of submodules in the Noetherian module T, it must terminate, showing that T is a finite direct sum of cyclic modules.

To see that T has an element annihilated by a: we can easily reduce – e.g. using the CRT for modules; we leave the details to the reader – to the case of $a = \pi^k$ a prime power, and then the result is clear, since the annihilator of T is the ideal generated by the annihilators of the elements of T, so if the annihilator of each element of T were contained in (π^{k+1}) then the annihilator of T would be contained in (π^{k+1}), a contradiction. □

EXERCISE 16.7. *Let R be a PID, and let M be an R-module.*

a) *Show: M has finite length if and only if it is a finitely generated torsion R-module.*
b) *Suppose M is finitely generated. Show: M is indecomposable if and only if M is free of rank 1 or M is cyclic with prime power annihilator.*
c) *Let T be a finitely generated torsion R-module. Use the Krull-Schmidt Theorem to show that T admits a decomposition as a finite direct sum of cyclic modules with prime power annihilator. Explain the sense in which this decomposition is unique. Check the fine print of the structure theorem*

for finitely generated modules over a PID in a standard algebra text, and confirm that Theorem 16.13 and this exercise recover that full result.

Earlier we said that quotients of PIDs are the main examples of special principal rings. In fact they are the only examples:

THEOREM 16.14. *(Hungerford* [**Hu68**]*) Every special principal ring is the quotient of a PID.*

Hungerford's Theorem relies on Cohen's structure theorem for complete Noetherian local rings, a topic which we unfortunately do not treat in this text, so the proof must be omitted.

EXERCISE 16.8. *Show: for a commutative ring R, the following are equivalent:*

(i) *R is a special principal ring.*
(ii) *R is the quotient of a discrete valuation ring by a nonzero ideal.*

EXERCISE 16.9.

a) *Show that a PID is residually Artinian principal: i.e., every quotient of a PID by a nonzero ideal is an Artinian principal ring.*
b) *Hungerford's Theorem says that the quotients of PIDs by prime power ideals are precisely the local Artinian principal ring. Show: not every Artinian principal ring is a quotient of a PID.*
(Suggestion: use Exercise 8.45.)

EXERCISE 16.10. *Let k be a field. Let $R = k[x,y]$, and $\mathfrak{m}$ be the maximal ideal $\langle x, y\rangle$ in R. Show that the quotient ring $S = R/\mathfrak{m}^2$ is nonprincipal. In particular, if k is finite, then S is a finite nonprincipal local ring.*

EXERCISE 16.11. *For $n \in \mathbb{Z}^+$, show that the following are equivalent:*

(i) *Every finite ring of order n is principal.*
(ii) *The integer n is* ***cubefree****, i.e., it is not divisible by the cube of any prime number.*

EXERCISE 16.12. *It follows from the previous exercise that the least cardinality of a nonprincipal ring is 8.*

a) *Show that up to isomorphism there are 10 rings of order 8, of which two are nonprincipal: $\mathbb{Z}/2\mathbb{Z}[x,y]/\langle x^2, xy, y^2\rangle$ and $\mathbb{Z}/4\mathbb{Z}[x]/\langle 2x, x^2\rangle$.*
b) *Show that there is up to isomorphism a unique noncommutative ring of order 8.*
c) *Show that for any prime $p \geq 3$ there are up to isomorphism 11 rings of order p^3 and one noncommutative ring of order p^3. How many of these rings are principal?*

EXERCISE 16.13. *(Inspired by* `http://math.stackexchange.com/questions/361258`*) Show: for a ring R the following are equivalent:*

(i) *The polynomial ring $R[t]$ is principal.*
(ii) *R is a finite product of fields.*

(Suggestions: (ii) $\implies$ (i) is easy. For (i) $\implies$ (ii), show: if $R[t]$ is principal, then R is principal Artinian; then reduce to showing that if R is a local principal Artinian ring with nonzero maximal ideal $\mathfrak{p} = \langle \pi \rangle$, then $R[t]$ is not principal. For this let $\mathfrak{m} := \langle \pi, t\rangle \in \operatorname{MaxSpec} R[t]$ and show: $\dim_{R[t]/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = \dim_{R/\pi R} \mathfrak{m}/\mathfrak{m}^2 = 2$.)

3. Euclidean functions and Euclidean rings

3.1. Euclidean functions. If R is a domain, then a **Euclidean function** is a function $\varphi : R^\bullet \to \mathbb{N}$ such that: for all $a \in R$ and $b \in R\backslash\{0\}$, there are $q,\ r \in R$ such that $a = qb + r$ with $r = 0$ or $\varphi(r) < \varphi(b)$.

PROPOSITION 16.15. *Let R be a domain that admits a Euclidean function φ. Then R is a PID.*

PROOF. Let I be a nonzero ideal of R, and let $x \in I^\bullet$ be an element such that $\varphi(x)$ is minimal among elements of $I^\bullet$. Let $y \in I$. We may write

$$y = qx + r$$

with either $r = 0$ or $\varphi(r) < \varphi(x)$. Since $x, y \in I$, we have $r = y - qx \in I$, so because x has minimal norm among nonzero elements we must have $r = 0$ and $y \in (x)$. Thus $I = (x)$. □

EXERCISE 16.14. *Let R be a domain.*

a) *Suppose R is a field. Show:* every *function $\varphi : R^\bullet \to \mathbb{N}$ is a Euclidean function.*
b) *Suppose that $\varphi : R^\bullet \to \mathbb{N}$ is a classical Euclidean function that is constant: there is $n \in \mathbb{N}$ such that $\varphi(x) = n$ for all $x \in R^\bullet$. Show: R is a field.*

EXERCISE 16.15. *For each of the following rings R, we give a function $\varphi : R\backslash\{0\} \to \mathbb{N}$. Verify that $\varphi : R^\bullet \to \mathbb{N}$ is a Euclidean function.*

a) $R = \mathbb{Z}$, $\varphi(x) := |x|$.
b) $R = k[t]$, $\varphi(p(t)) := \deg(p(t))$.
c) $R = k[[t]]$, $\varphi(\sum_{n=0}^{\infty} a_n t^n) :=$ *the least n such that $a_n \neq 0$.*

EXERCISE 16.16. *Let $(R, \mathfrak{m})$ be a local PID and let π be a generator of the maximal ideal $\mathfrak{m}$. For $x \in R^\bullet$, there is a unique $n \in \mathbb{N}$ such that $x \in \mathfrak{m}^n\backslash\mathfrak{m}^{n+1}$, and we put $\varphi(x) := n$. Show: φ is a Euclidean function on R.*

The following result of Samuel [**Sa71**, Prop. 5] generalizes Exercise 16.14:

EXAMPLE 16.16. *Let R be a semilocal PID that is not a field, and let $\pi_1, \ldots, \pi_r$ be the mutually nonassociate prime elements of R. Then every $x \in R^\bullet$ may be uniquely expresse as*

$$x = u\pi_1^{e_1} \cdots \pi_r^{e_r} \text{ with } u \in R^\times,\ e_1, \ldots, e_r \in \mathbb{N}.$$

We claim that $\varphi : R^\bullet \to \mathbb{N}$ by $x \mapsto \sum_{i=1}^r e_i$ is a Euclidean function on R. Indeed: let $a \in R$ and $b = u_b\pi_1^{b_1} \cdots \pi_r^{b_r} \in R^\times$ with $b \nmid a$. In particular $a \neq 0$, so we may write $a = u_a\pi_1^{a_1} \cdots \pi_r^{a_r}$ and the set

$$I := \{1 \leqslant i \leqslant r \mid a_i < b_i\}$$

is nonempty. By CRT, there is $r \in R$ with

$$r \equiv \begin{cases} a \pmod{\pi_i^{b_i}} & \text{if } i \in I \\ b \pmod{\pi_i^{b_i+1}} & \text{if } i \in \{1, \ldots, r\}\backslash I \end{cases}.$$

Then

$$\varphi(r) = \sum_{i \in I} a_i + \sum_{i \notin I} b_i < \sum_{i=1}^r b_i = \varphi(b).$$

Moreover for all $1 \leqslant i \leqslant r$ *we have that* $\pi_i^{b_i} \mid a - r$*, so there is* $q \in R$ *such that* $a - r = qb$*.*

A **Euclidean domain** is a domain that admits a Euclidean function. The Euclidean function is *not* part of the structure of a Euclidean domain. The Euclidean function is most certainly *not* unique:

EXERCISE 16.17. *Let* R *be a domain, let* $\varphi : R^\bullet \to \mathbb{N}$ *be a Euclidean function, and let* $\iota : \mathbb{N} \to \mathbb{N}$ *be strictly increasing. Show:* $\iota \circ \varphi : R^\bullet \to \mathbb{N}$ *is a Euclidean function.*

If R is a finite domain, then it is a finite field, so by Exercise 16.14, every function from $R^\times$ to $\mathbb{N}$ is a Euclidean function, so the set $\mathrm{Euc}(R)$ of Euclidean functions on R is countably infinite. If R is an infinite field, then the same considerations show that $\#\,\mathrm{Euc}(R) \geqslant \mathfrak{c} = 2^{\aleph_0}$. We will see shortly that if R is a domain that is not a field, then for any Euclidean function $\varphi : R \to \mathbb{N}$ we have $\varphi(R)$ is infinite, which together with Exercise 16.17 implies that $\#\,\mathrm{Euc}(R) \geqslant \mathfrak{c}$.

Exercise 16.15 shows that Euclidean functions are bound up in the history of PIDs: indeed the Euclidean algorithm predates (by thousands of years) the concept of a principal ideal domain, so when trying to decide whether a domain R is a PID it seems only natural to ask whether it admits a Euclidean function. From the modern perspective though, this is half correct and half incorrect. The correct half is: if we know that a domain admits a Euclidean function, we should certainly use it: the Euclidean algorithm can be used to compute gcd's, generators of ideals and so forth. Though we do not discuss Smith and Hermite normal forms in this text, they exist over any PID but over a general PID are not guaranteed to be algorithmic. However, the existence of a Euclidean function yields algorithms. The incorrect half is: the specific PIDs we've considered thus far in this section are misleadingly simple. For most domains R – e.g. for the ring of integers $\mathbb{Z}_K$ of a number field K – it is *much* easier to determine whether R is a PID than to determine whether R is Euclidean. We will see some examples later on.

3.2. Euclidean norms and strictly isotone Euclidean functions. A **Euclidean norm** is a Euclidean function $|\cdot| : R^\bullet \to \mathbb{Z}^+$ such that if we extend it to 0 by $|0| := 0$, then $|\cdot|$ becomes a norm in the senseof §16.1.

EXERCISE 16.18. *In each case, show that the given norm is a Euclidean norm.*

a) $R = \mathbb{Z}$*,* $|\cdot|$ *the usual absolute value.*
b) k *a field,* $R = k[t]$*,* $|f| := 2^{\deg f}$*. (By convention, we put* $\deg(0) = -\infty$ *and* $2^{-\infty} = 0$*.)*
c) R *a local PID with maximal ideal* $\mathfrak{m} = (\pi)$*. For* $x \in R^\bullet$*, let* $n(x) \in \mathbb{N}$ *be such that* $x \in \mathfrak{m}^n \backslash \mathfrak{m}^{n+1}$*, and put* $n(0) := -\infty$*. For* $x \in R$*, put* $|x| := 2^{n(x)}$*.*
d) *Let* $d \in \{-2, -1, 2, 3\}$*,* $R = \mathbb{Z}[\sqrt{d}]$ *and* $|a + b\sqrt{d}| := |a^2 - db^2|$*.*

PROPOSITION 16.17 (Samuel). *Let* R *be a domain, and let* $\varphi : R^\bullet \to \mathbb{N}$ *be a Euclidean function. We define*

$$\varphi_1 : R^\bullet \to N,\ x \mapsto \min_{y \in (x)^\bullet} \varphi(y).$$

Then φ_1 *is a Euclidean function satisfying:*

(i) *For all* $x \in R^\bullet$*,* $\varphi_1(x) \leqslant \varphi(x)$*.*

(ii) *For all $x, y \in R^\bullet$, $\varphi_1(x) \leqslant \varphi_1(xy)$, with equality if and only if $y \in R^\times$.*

PROOF. The function φ_1 is well-defined since $\mathbb{N}$ is well-ordered. Let us check that φ_1 is a Euclidean function: let $x \in R$ and $y \in R^\bullet$ be such that $y \nmid x$. There is $z \in R^\bullet$ such that $\varphi_1(y) = \varphi(yz)$, and since φ is Euclidean, we may write

$$x = qyz + r = (qz)y + r$$

with $r \in R^\bullet$ and $\varphi(r) < \varphi(yz)$. We have

$$\varphi_1(r) \leqslant \varphi(r) < \varphi(yz) = \varphi_1(y),$$

which shows that φ_1 is a Euclidean function. That it satisfies (i) is immediate from the definition, as is the fact that for all $x, y \in R^\bullet$ we have $\varphi_1(x) \leqslant \varphi_1(xy)$. If also $y \in R^\times$ then $\varphi_1(xy) \leqslant \varphi_1(xyy^{-1}) = \varphi_1(x)$, so $\varphi_1(x) = \varphi_1(y)$. Finally, if $\varphi_1(x) = \varphi_1(xy)$, we may write $xy = qx + r$ with $r = 0$ or $\varphi_1(r) < \varphi_1(x)$. Since $r = x(y - q)$, we have $\varphi_1(x) \leqslant \varphi_1(r)$, so $r = 0$ and thus $y \in R^\times$. □

EXERCISE 16.19. *Let R be a domain that is not a field, and let $\varphi : R^\bullet \to \mathbb{N}$ be a Euclidean function on R. For each $\mathfrak{p} \in \operatorname{MaxSpec} R$, choose $\pi_\mathfrak{p}$ such that $\mathfrak{p} = (\pi_\mathfrak{p})$. Let $x \in R^\bullet$. We may write*

$$x = u \prod_{\mathfrak{p} \in \operatorname{MaxSpec} R} \pi_\mathfrak{p}^{v_\mathfrak{p}(x)}$$

for a unique $v_\mathfrak{p}(x) \in \mathbb{N}$ and such that $v_\mathfrak{p}(x) = 0$ for all but finitely many $\mathfrak{p}$ (for each fixed x). Show:

$$\varphi(x) \geqslant 1 + \sum_{\mathfrak{p} \in \operatorname{MaxSpec} R} v_\mathfrak{p}(x).$$

For a domain R and elements $x, y \in R^\bullet$, we say that **x strictly divides y** if $(x) \supsetneq (y)$. We call a Euclidean function $\varphi : R^\bullet \to \mathbb{N}$ **strictly isotone** if whenever x strictly divides y we have $\varphi(x) < \varphi(y)$.

Let R be a domain that is not a field, so there is $x \in R^\bullet \backslash R^\times$. If $\psi : R^\bullet \to \mathbb{N}$ is a strictly isotone Euclidean function, then

$$\psi(x) < \psi(x^2) < \ldots < \psi(x^n) < \ldots,$$

so $\psi(R^\bullet)$ is infinite. If now $\varphi : R^\bullet \to \mathbb{N}$ is any Euclidean function, then the Euclidean function φ_1 of Proposition 16.17 is strictly isotone, so $\varphi_1(N)$ is infinite. Since $\varphi_1(x) \leqslant \varphi(x)$ for all $x \in R^\bullet$, it follows that $\varphi(R^\bullet)$ is infinite. As mentioned above, it now follows from Exercise 16.17 that the set $\operatorname{Euc}(R)$ of Euclidean functions on R has at least continuum cardinality.

Thus on a Euclidean domain that is not a field, Euclidean functions fail spectacularly to be unique. This motivates us to search for a canonical Euclidean function on a Euclidean domain. To motivate this, consider the set $\mathbb{N}^{R^\bullet}$ of all functions $f : R^\bullet \to N$. We give this set the pointwise (or product) partial ordering: for $f, g : R^\bullet \to N$, we put $f \leqslant g$ if $f(x) \leqslant g(x)$ for all $x \in R^\bullet$. We observe that any nonempty subset $\{f_x\}_{x \in X}$ of $\mathbb{N}^{R^\bullet}$ has an infimum in

Then the partially ordered set $\mathbb{N}^{R^\bullet}$ is Artinian: to see this, let $\{f_x\}_{x \in X}$ be any nonempty subset of $\mathbb{N}^{R^\bullet}$. Then

3.3. Transfinite Euclidean Functions. In another direction, P. Samuel considered the notion of a **W-Euclidean function** on a domain R. Here W is a well-ordered set and $N : R \to W$ is a function such that for all $a \in R, b \in R\backslash\{0\}$ such that $b \nmid a$, $\exists\ q, r \in R$ with $a = qb + r$ and $N(r) < N(b)$. If R admits, for some W, a W-Euclidean function, then R is a PID.

EXERCISE 16.20. *Show: a domain is W-Euclidean for some finite W if and only if it is a field.*

Say that a domain is **Samuel-Euclidean** if it is W-Euclidean for some well-ordered set W. Samuel remarks that the an imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ has a Samuel-Euclidean ring of integers R_d if and only if $d = 1, 2, 3, 7, 11$. On the other hand, it goes back at least to Gauss that for each of $d = 19, 43, 67, 163$ the ring R_d is a PID. Thus there are PIDs which are not Samuel-Euclidean. Samuel further showed that any Samuel-Euclidean ring is W-Euclidean for a unique minimal well-ordered set (up to canonical order isomorphism) W_R and asked the question of whether one has $W_R \leqslant \mathbb{N}$ for all domains R. This was answered in the negative by Hiblot [**Hi75**], [**Hi77**].

4. Bézout domains

PROPOSITION 16.18. *Let a, b be elements of a domain R. If the ideal $\langle a, b\rangle$ is principal, then its generator is a greatest common divisor of a and b.*

PROOF. In other words, we are assuming the existence of some $d \in R$ such that $dR = aR + bR$. Then $a, b \in dR$, so d is a common divisor of a and b. If $e \mid a$ and $e \mid b$ then since there are $x, y \in R$ such that $d = xa + yb$, we have $e \mid d$. □

COROLLARY 16.19. *For a domain R, the following are equivalent:*

(i) *Every finitely generated ideal is principal.*
(ii) *For any two elements a and b of R, their gcd exists and is an R-linear combination of a and b.*

PROOF. (i) $\implies$ (ii) is immediate from Proposition 16.18: $\gcd(a, b)$ will be a generator of the ideal $\langle a, b\rangle$. Conversely, if $d = \gcd(a, b)$ exists and is of the form $d = xa + yb$ for some $x, y \in R$, then clearly $(d) = \langle a, b\rangle$, so that every ideal with two generators is principal. By an obvious induction argument, we conclude that any finitely generated ideal is principal. □

At least according to some, it was Étienne Bézout who first explicitly noted that for polynomials $P, Q \in k[t]$, $\gcd(a, b)$ exists and is a linear combination of a and b: this fact is called **Bézout's identity** or **Bézout's Lemma**. For this (somewhat tenuous) reason, a possibly non-Noetherian domain satisfying the equivalent conditions of Corollary 16.19 is called a **Bézout domain**.

EXERCISE 16.21. *Show: a localization of a Bézout domain is again a Bézout domain.*

THEOREM 16.20. *For a Bézout domain R, the following are equivalent:*

(i) *R is a PID.*
(ii) *R is Noetherian.*
(iii) *R is a UFD.*
(iv) *R is an ACCP domain.*

(v) *R is an atomic domain.*

PROOF. (i) $\iff$ (ii) immediately from the definitions.
(i) $\implies$ (iii): this is Corollary 15.2.
(iii) $\implies$ (iv) $\implies$ (v) holds for all domains.
(v) $\implies$ (iii): A Bézout domain is a GCD-domain (Corollary 16.19), a GCD-domain is an EL-domain (Proposition 15.11), and an atomic EL-domain is a UFD (Theorem 15.8), so a Bézout atomic domain is a UFD.
(iv) $\implies$ (ii): assume that R is *not* Noetherian. Then it admits an infinitely generated ideal I, which we can use to build an infinite strictly ascending chain of finitely generated ideals $I_1 \subsetneq I_2 \subsetneq \ldots \subsetneq I$. Since R is Bézout, each I_i is principal, contradicting ACCP. □

Let us say that a domain is **properly Bézout** if it is Bézout but not a PID.

We have already seen some examples of properly Bézout domains: the ring of entire functions (Theorem 5.23) and the ring of all algebraic integers (Theorem 5.1). To get further examples we move on to the next topic: valuation rings.

CHAPTER 17

Valuation Rings

1. Basic theory

Consider the divisibility relation – i.e., $a \mid b$ – on a domain R. Evidently it is reflexive and transitive, so is a **quasi-ordering**.[1] Divisibility need *not* be a partial ordering because $a \mid b$ and $b \mid a$ does not imply that $a = b$ but only that a and b are associates: $(a) = (b)$. However, one of the first ideas of ideal theory is to view associate elements as being somehow "equivalent." This motivates us to consider the equivalence relation on R in which $a \sim b$ if and only if $(a) = (b)$. This is easily seen to be a **monoidal equivalence relation**. In plainer language, if $(a_1) = (a_2)$ and $(b_1) = (b_2)$, then $(a_1 b_1) = (a_2 b_2)$. We can therefore consider the commutative monoid of principal ideals of R under multiplication, on which the divisibility relation is a partial ordering.

Having made a quasi-ordering into a partial ordering, it is natural to ask for conditions under which the divisibility relation induces a **total ordering**. Equivalently, for any $a, b \in R$ either $a \mid b$ or $b \mid a$.

PROPOSITION 17.1. *Let R be a domain with fraction field K. the following are equivalent:*

(i) *For every $a, b \in R$, $a \mid b$ or $b \mid a$.*
(ii) *For every $0 \neq x \in K$, $x \in R$ or $x^{-1} \in R$.*

EXERCISE 17.1. *Prove Proposition 17.1.*

A domain R satisfying the conditions of Proposition 17.1 is called a **valuation domain** or **valuation ring**.

Note that any field is a valuation ring. This is a trivial example which is often implicitly excluded from consideration (we will try our best to be explicit in our exclusion of trivial cases). Apart from this, in a first algebra course one may not see examples of valuation rings. But we have: if p is a prime number, then the ring $\mathbb{Z}_{(p)}$ of integers localized at p is such an example. Define $x \mid_p y$ if $\mathrm{ord}_p(\frac{y}{x}) \geqslant 0$. Then p-divisibility is immediately seen to be a total quasi-ordering: given two integers, at least one p-divides the other. The fundamental theorem of arithmetic implies

$$x \mid y \iff \forall \text{ primes } p,\ x \mid_p y.$$

However, in $\mathbb{Z}_{(p)}$, we have $x \mid y \iff x \mid_p y$, i.e., we have localized the divisibility relation to get a total quasi-order: $\mathbb{Z}_{(p)}$ is a valuation domain.

[1] By definition, a quasi-ordering is a reflexive, transitive binary relation on a set.

This argument generalizes as follows: let R be a PID[2] and $\mathfrak{p} = (\pi)$ be a prime ideal of R. We define $\mathrm{ord}_{\mathfrak{p}}(x)$ to be the least n such that $(x) \supset \mathfrak{p}^n$, and extend it to a map on $K^\times$ by $\mathrm{ord}_{\mathfrak{p}}(\frac{x}{y}) = \mathrm{ord}_{\mathfrak{p}}(x) - \mathrm{ord}_{\mathfrak{p}}(y)$. (One should check that this is well-defined; this is easy.) Finally, we define $x \mid_{\mathfrak{p}} y$ to mean $\mathrm{ord}_{\mathfrak{p}}(\frac{y}{x}) \geqslant 0$. Arguing as above, we see that the localization $R_{\mathfrak{p}}$ is a valuation ring.

In showing that $R_{\mathfrak{p}}$ was a valuation domain we proceeded by constructing a map $\mathrm{ord}_{\mathfrak{p}}$ on the nonzero elements of the fraction field K. This can be generalized, as follows: if R is a domain with quotient field K, we can extend the divisibility relation to $K^\times$ by saying that $x \mid y$ if and only if $\frac{y}{x} \in R$. Clearly $x \mid y$ and $y \mid x$ if and only if $\frac{y}{x}$ is a unit in R. Therefore the quotient of $(K^\times, \cdot)$ on which divisibility (from R!) becomes a partial ordering is precisely the quotient group $K^\times/R^\times$.

For $[x], [y] \in K^\times/R^\times$, let us write $[x] \leqslant [y]$ if $[\frac{y}{x}] \in R$. (Take a second and check that this is well-defined.)

Exercise 17.2. *Show: the divisibility quasi-ordering on R is a total quasi-ordering if and only if the ordering on $K^\times/R^\times$ is a total ordering.*

In other words, if R is a valuation ring, then the canonical map $v : K^\times \to K^\times/R^\times$ is a homomorphism onto a totally ordered commutative group. Let us relabel the quotient group by G and denote the group law by addition, so that the homomorphism property gets recorded as

(VRK1) $\forall x, y \in K^\times\ v(ab) = v(a) + v(b)$.

We recover R as

$$R = \{x \in K^\times \mid v(x) \geqslant 0\} \cup \{0\}.$$

Everything that has been said so far takes into account only the multiplicative structure on R. So the following additional property is very important:

(VRK2) $\forall x, y \in K^\times \mid x + y \neq 0,\ v(x+y) \geqslant \min(v(x), v(y))$.

Indeed, suppose without loss of generality that $v(x) \leqslant v(y)$, i.e., $\frac{y}{x} \in R$. Then $\frac{x+y}{x} = 1 + \frac{y}{x} \in R$ so $v(x) \leqslant v(x+y)$.

Exercise 17.3. *Suppose $v(x) \neq v(y)$. Show that $v(x+y) = \min(v(x), v(y))$.*

Exercise 17.4. *Show: a valuation ring is integrally closed.*

Let $(G, +, \leqslant)$ be a totally ordered commutative group. We write $G^+ = \{g \in G \mid g \geqslant 0\}$, so G^+ is a totally ordered submonoid of G. A **(G-valued) valuation** on a field K is a surjective map $v : K^\times \to G$ satisfying (VRK1) and (VRK2) above.

Exercise 17.5. *Let $v : K^\times \to G$ be a valuation. Let R be the set of elements of $K^\times$ with non-negative valuation, together with 0. Show: R is a valuation ring with fraction field K.*

[2]In fact we can take R to be any Dedekind domain, as soon as we know what such a thing is. See §18.

EXERCISE 17.6. *Let R be a domain, G a totally ordered group and $v : R\backslash\{0\} \to G^+$ be a map which satisfies both of the following properties:*
(VRR1) For all $x, y \in R^\bullet$, $v(xy) = v(x) + v(y)$.
(VRR2) For all $x, y \in R^\bullet$, if $x + y \neq 0$ then $v(x + y) \geqslant \min(v(x), v(y))$.
Show: there is a unique extension of v to a valuation $v : K^\times \to G$, namely $v(x/y) = v(x) - v(y)$.

The ideal theory of a valuation ring can be entirely understood in terms of its value group, as we now explain. Recall that in a partially ordered set $(X, \leqslant)$ an **upset** is a subset Y of X such that for all $y \in Y$ and $x \in X$, if $y \leqslant x$ then $x \in Y$. For any subset Y of X, there is an upset generated by Y, which we denote by $Y^\uparrow$: this is the intersection of all upsets of X containing Y. For $x \in X$ we write $x^\uparrow$ in place of $\{x\}^\uparrow$.An upset is called **principal** if it is generated by a single element.

Things simplify if X is totally ordered. Then an upset is principal if and only if it has a minimum, and since every nonempty finite subset of X has a minimum, every finitely generated upset is principal. Infinitely generated upsets need not be principal: indeed, $(X, \leqslant)$ is well-ordered if and only if every nonempty upset is principal. Recall that a partially ordered set *Noetherian* if the ascending chain condition holds and *Artinian* if the descending chain condition holds. A totally ordered set is well-ordered if and only if it is Artinian.

LEMMA 17.2. *Let $(X, \leqslant)$ be a partially ordered set. Let $\mathrm{Up}(X)$ be the set of all upsets of X and let $\mathrm{PrinUp}(X)$ be the set of all principal upsets of X, each partially ordered by inclusion.*

a) *The map $x \mapsto x^\uparrow$ is an antitone bijection from X to $\mathrm{PrinUp}(X)$.*
b) *The following are equivalent:*
   (i) *X is totally ordered.*
   (ii) *$\mathrm{PrinUp}(X)$ is totally ordered.*
   (iii) *$\mathrm{Up}(X)$ is totally ordered.*
c) *The following are equivalent:*
   (i) *X is well-ordered.*
   (ii) *$\mathrm{PrinUp}(X)$ is totally ordered and Noetherian.*
   (iii) *$\mathrm{Up}(X)$ is totally ordered and Noetherian.*

PROOF. a) The map $x \mapsto x^\uparrow$ is by definition a surjection from X to $\mathrm{PrinUp}(X)$. If $x_1^\uparrow = x_2^\uparrow$ then $x_1 \leqslant x_2$ and $x_2 \leqslant x_1$, so $x_1 = x_2$. Thus the map is a bijection. Moreover we have $x_1 \leqslant x_2$ if and only if $x_2 \in x_1^\uparrow$ if and only if $x_2^\uparrow \subseteq x_1^\uparrow$.
b) By part a) we know that X and $\mathrm{PrinUp}(X)$ are order-anti-isomorphic, so (i) $\iff$ (ii) is clear. (iii) $\implies$ (ii) because $\mathrm{PrinUp}(X)$ is a subset of $\mathrm{Up}(X)$. (i) $\implies$ (iii): Seeking a contradiction, suppose that X is totally ordered but $\mathrm{Up}(X)$ is not. Then there are upsets U_1 and U_2 of X and $x_1 \in U_1\backslash U_2$, $x_2 \in U_2\backslash U_1$. Since X is totally ordered, we have either $x_1 \leqslant x_2$ or $x_2 \leqslant x_1$. If $x_1 \leqslant x_2$, then since $x_1 \in U_1$, also $x_2 \in U_1$, a contradiction. Similarly, if $x_2 \leqslant x_1$, we get $x_1 \in U_2$, a contradiction.
c) Again, (i) $\iff$ (ii) because X and $\mathrm{PrinUp}(X)$ are order-anti-isomorphic, and (ii) $\implies$ (ii) because a subset of a totally ordered Noetherian set is also totally ordered Noetherian.
(i) $\implies$ (iii): If X is well-ordered then every nonempty upset is principal, so

$$\mathrm{Up}(X) = \mathrm{Prin}(X) \coprod \{\varnothing\}.$$

Thus $\mathrm{Up}(X)$ is obtained from a totally ordered Noetherian set by adjoining a bottom element. This preserves the condition of being totally ordered Noetherian. □

PROPOSITION 17.3. *Let R be a valuation ring, with value group G. Let*

$$G^+ := \{g \in G \mid g \geqslant 0\}.$$

To an ideal I of R, we put

$$\mathcal{U}(I) := v(I^\bullet).$$

To an upset U of G^+, we put

$$\mathcal{I}(U) := v^{-1}(U) \cup \{0\}.$$

Then $\mathcal{U}$ and $\mathcal{I}$ are mutually inverse isotone bijections from the set of ideals of I (ordered under inclusion) to the set of upsets of G^+ (ordered under inclusion).

PROOF. Let us first check that if I is an ideal then $v(I^\bullet)$ is an upset, and if U is an upset then $v^{-1}(U) \cup \{0\}$ is an ideal. Let $g, h \in G^+$ with $g \leqslant h$ and $g = v(x)$ for some $x \in I^\bullet$. By definition of G we have $h = v(y)$ for some $y \in R^\bullet$. We have $v(\frac{y}{x}) = v(y) - v(x) = h - g \geqslant 0$, so $\frac{y}{x} \in R$; since $y = x \cdot \frac{y}{x}$, we get $x \in I^\bullet$. Thus $v(I^\bullet)$ is an upset. Let $x, y \in v^{-1}(U) \cup \{0\}$. To see that $x + y \in v^{-1}(U) \cup \{0\}$, we may assume that $x, y \in v^{-1}(U)$ and $x + y \neq 0$. Then $v(x + y) \geqslant \min(v(x), v(y))$, so $v(x + y) \in U$, so $x + y \in v^{-1}(U)$. Now let $x \in v^{-1}(U) \cup \{0\}$ and $y \in R$. Again, we may assume that $x, y \neq 0$. Then $v(xy) = v(x) + v(y) \geqslant v(x)$, so $xy \in v^{-1}(U)$.

Consider the quotient map $v : R^\bullet \to R^\bullet/R^\times = G^{\geqslant 0}$. Since v is surjective, for any subset Y of $G^{\geqslant 0}$ we have $Y = v(v^{-1}(Y))$, while for a subset X of $R^\bullet$ we have $v^{-1}(v(X)) = X$ if and only if for all $x \in X$ and $u \in R^\times$ we have $ux \in X$. The latter condition holds for $I^\bullet$ for any ideal I of R. Up to removing the zero element, the map $I \mapsto \mathcal{U}(I)$ is just $v(I)$, and up to adding back the zero element, the map $U \mapsto \mathcal{I}(U)$ is just $v^{-1}(U)$, so these are mutally inverse isotone maps. □

A **chain ring** is a ring R in which the set of ideals of R is totally ordered under inclusion.

THEOREM 17.4. *For a domain R with fraction field K, the following are equivalent:*

(i) *R is a chain ring.*
(ii) *The set of principal ideals of R is totally ordered under inclusion.*
(iii) *R is a valuation ring.*

PROOF. (i) $\implies$ (ii): a subset of a a totally ordered set is totally ordered.
(ii) $\iff$ (iii): The principal ideals of a domain R are totally ordered under inclusion if and only if for any $x, y \in R^\bullet$ we have either $x \mid y$ or $y \mid x$ if and only if for any $x \in K^\times$ we have either $x \in R$ or $x^{-1} \in R$.
(iii) $\implies$ (i): Applying Lemma 17.2 with $X = G^+$ we get that the set of upsets of G^+ is totally ordered under inclusion. By Proposition 17.3 this implies that the set of ideals of R is totally ordered under inclusion. □

EXERCISE 17.7. *Let R be a ring.*

a) *Show: if R is a chain ring, then so is every quotient and localization.*
b) *Deduce: if R is a valuation ring and $\mathfrak{p} \in \operatorname{Spec} R$, then $R/\mathfrak{p}$ is a valuation ring.*
c) *Suppose that R is a principal ring. Show: R is a chain ring if and only if R is a quotient of a DVR.*

Let R be a valuation ring. Of course the smallest and largest ideals of R are $\{0\}$ and R; correspondingly, the smallest and largest upsets of G^+ are $\varnothing$ and G^+. There is a unique maximal proper upset of G^+, namely

$$G^{>0} := \{g \in G \mid g > 0\}.$$

It follows that

$$\mathfrak{m} := \{x \in R \mid v(x) > 0\}$$

is the unique maximal ideal of R. Thus a valuation ring is a local ring.

EXERCISE 17.8. *Let R be a valuation ring with value group G.*

a) *Let S be a set of generators for an ideal I of R. Show: $\{v(x) \mid x \in S^\bullet\}$ is a set of generators for the upset $\mathcal{U}(I) = v(I^\bullet)$.*
b) *Let T be a set of generators for an upset U of $G^{\geqslant 0}$. For each $g \in U$, choose any $x_g \in R^\bullet$ with $v(x_g) = g$. Show: $\{x_g \mid g \in U\}$ is a set of generators for the ideal $\mathcal{I}(U) = v^{-1}(U) \cup \{0\}$.*

PROPOSITION 17.5. *Let R be a local domain. The following are equivalent:*

(i) *R is a valuation ring.*
(ii) *R is a Bézout domain.*

PROOF. (i) $\implies$ (ii): Let R be a valuation ring, and let I be an ideal of R that is generated by finitely many elements $x_1, \ldots, x_n \in R^\bullet$. By Theorem 17.4 there is some $1 \leqslant i \leqslant n$ such that $(x_i) \supseteq (x_j)$ for all $1 \leqslant j \leqslant n$, and then $I = (x_i)$.
(ii) $\implies$ (i): Suppose R is a local Bézout domain. To show that R is a valuation ring, by Theorem 17.4 it is enough to show that for $x, y \in R^\bullet$ either $x \mid y$ or $y \mid x$. Let $d := \gcd(x, y)$. Then $\langle \frac{x}{d}, \frac{y}{d} \rangle = R$; since R is local, one of $\frac{x}{d}$, $\frac{y}{d}$ must be a unit. If $\frac{x}{d} \in R^\times$ then $(x) = (d) \supseteq (y)$, and if $\frac{y}{d} \in R^\times$, then $(y) = (d) \supseteq (x)$. □

2. Discrete Valuation Rings

2.1. Characterizing DVRs. The next question is when a valuation ring is Noetherian. Again we must be able to extract this information from the value group G: more precisely, Lemma 17.2 and Proposition 17.3 tell us that R is Noetherian if and only if G^+ is well-ordered. Although there are of course *many* well-ordered sets, a little thought shows that it is much harder for the positive cone G^+ of an ordered commutative group to be well-ordered, other than the trivial case $G = \{e\}$ (i.e., when R is a field), there is just one obvious example: when $G = \mathbb{Z}$ endowed with its standard ordering (in fact $\mathbb{Z}$ can be endowed with the structure of an ordered commutative group is a unique way, up to isomorphism) we have $G^+ = \mathbb{N}$ which is indeed well-ordered. A valuation ring R with value group $G \cong \mathbb{Z}$ is called a **discrete valuation ring** or **DVR**. In a DVR, the maximal ideal of all elements of positive valuation is generated by any element π of valuation 1; such an element is called a **uniformizer**. Since every nonempty upset of $\mathbb{N}$ is principal, every ideal of a DVR is principal, and every nonzero ideal is of the form (π^n) for a unique $n \in \mathbb{N}$.

We will study ordered commutative groups more systematically in the next section. If we borrow one result from the next section, we can prove now that a Noetherian valuation ring is (a field or) a DVR. Namely, what we need is the following (Theorem 17.17): in any ordered commutative group $(G, \leqslant)$, exactly one of the following holds: I. G is isomorphic as an ordered commutative group to a

subgroup of $\mathbb{R}$; or II. there are elements $0 < g < h$ in G such that $ng < h$ for all $n \in \mathbb{Z}^+$. We will also make use of:

EXERCISE 17.9. *Let G be a nontrivial subgroup of $\mathbb{R}$. Show: exactly one of the following holds:*

a) *G has a least positive element x, and then G is infinite cyclic with generator x.*
b) *G is dense in $\mathbb{R}$ in the order topology: for all $x < y$ in $\mathbb{R}$ there is $g \in G$ with $x < g < y$.*

THEOREM 17.6. *Let R be a valuation ring with nontrivial value group G and maximum ideal $\mathfrak{m}$. The following are equivalent:*

(i) *R is a discrete valuation ring: that is $G \cong \mathbb{Z}$.*
(ii) *R is a PID.*
(iii) *R is Noetherian.*
(iv) *R satisfies (ACCP), the ascending chain condition on principal ideals.*
(v) *The positive cone G^+ of G is well-ordered.*
(vi) *We have $\bigcap_{n=1}^{\infty} \mathfrak{m}^n = (0)$.*

PROOF. (i) $\implies$ (ii): If $G \cong \mathbb{Z}$, then because $G^+ = \mathbb{N}$ is well-ordered, every nonempty upset in $\mathbb{N}$ is principal. By Exercise 17.14 this implies that every ideal of R is principal.
(ii) $\implies$ (iii) $\implies$ (iv) is immediate for all rings.
(iv) $\iff$ (v): By Theorem 17.4 and Proposition 17.3, the set of principal ideals of R is totally ordered and order-isomorphic to the set $\mathrm{PrinUp}(G^+)$ of principal upsets of G^+. Thus R satisfies (ACCP) if and only if $\mathrm{PrinUp}(G^+)$ is Noetherian, which by Lemma 17.2c) holds if and only if G^+ is well-ordered.
(v) $\implies$ (i): We go by contraposition: suppose that G is not isomorphic to $\mathbb{Z}$. By our "borrowed fact" (Theorem 17.17 from the following section), then exactly one of the following holds: I. G is isomorphic (as an ordered group) to a subgroup of $\mathbb{R}$ or II. has elements $0 < x < y$ such that $nx < y$ for all $n \in \mathbb{Z}^+$. If (i) holds, then since G is not cyclic, by Exercise 17.14 we have that G is order-dense in $\mathbb{R}$. In particular G^+ contains a strictly decreasing sequence converging to 0, so G^+ is not well-ordered. If (ii) holds, then

$$h > h - g > h - 2g > \ldots > h - nh > \ldots > 0$$

is an infinite descending chain in G^+, again showing that G^+ is not well-ordered.
(i) $\implies$ (vi): As we saw, if R is a discrete valuation ring then R is a local PID, so $\mathfrak{m} = (\pi)$ for some $\pi \in R$. The nonempty upsets of $G^+ = \mathbb{N}$ are $\mathbb{Z}^{\geq n}$ for $n \in \mathbb{N}$, so every nonzero ideal of R is of the form $\mathfrak{m}^n = (\pi^n)$ for a unique $n \in \mathbb{N}$. So $\bigcap_{n=1}^{\infty} \mathfrak{m}^n$ is strictly contained in every nonzero ideal of R, so it is the zero ideal.
(vi) $\implies$ (i): Let $n \in \mathbb{Z}^+$. The ideal $\mathfrak{m}^n$ is generated by elements of the form $x_1 \cdots x_n$ where $x_1, \ldots, x_n \in \mathfrak{m}^\bullet$. The corresponding upset $\mathcal{U}(\mathfrak{m}^n)$ of G^+ is the upset generated by elements $g_1 + \ldots + g_n$ for $g_1, \ldots, g_n \in G^{>0}$. We again go by contraposition: suppose G is not isomorphic to $\mathbb{Z}$.

First suppose that I. above holds: then G is isomorphic to an order-dense subgroup of $\mathbb{R}$. In this case, for any $g \in G^{>0}$ there are $h_1, \ldots, h_n \in G^{>0}$ such that $h_1 + \ldots + h_n < g$, so it follows that $\mathcal{U}(\mathfrak{m}^n) = G^{>0}$ and thus $\mathfrak{m}^n = \mathfrak{m}$ for all $n \in \mathbb{Z}^+$. In this case we have $\bigcap_{n=1}^{\infty} \mathfrak{m}^n = \mathfrak{m} \supsetneq (0)$.

Now suppose that II. above holds: there are $0 < g < h$ in G such that $ng < h$

for all $n \in \mathbb{Z}^+$. Let $n \in \mathbb{Z}^+$. Then $ng \in \mathcal{U}(\mathfrak{m}^n)$, so $h \in \mathcal{U}(\mathfrak{m}^n)$. Let $x \in R^\bullet$ be an element with $v(x) = h$. Then $x \in \bigcap_{n=1}^{\infty} \mathfrak{m}^n$, so $\bigcap_{n=1}^{\infty} \mathfrak{m}^n \neq (0)$. □

EXERCISE 17.10. *Show directly: a local PID is a valuation ring with value group* $\mathbb{Z}$.

2.2. Further characterizations of DVRs. In many ways, discrete valuation rings are – excepting only fields – the simplest class of rings. Nevertheless they have an important role to play in algebra and arithmetic and algebraic geometry. One reason for this is as follows: every DVR is a one-dimensional Noetherian local ring. The converse does not hold.

EXAMPLE 17.7. *Let k be a field, and let $R := k[t^2, t^3] \subset k[t]$. Then $\mathfrak{m} = \langle t^2, t^3 \rangle$ and even after localizing at $\mathfrak{m}$, the ideal $\mathfrak{m}_\mathfrak{m}$ of $R_\mathfrak{m}$ is not principal, as we have seen before. Here is another argument: there is a discrete valuation ord_t on the fraction field $k(t)$: $\mathrm{ord}_t(f/g)$ is the multiplicity of 0 as a root of f minus the multiplicity of 0 as a root of g. The valuation ring T of this valuation contains $R_\mathfrak{m}$ and if $\mathcal{M}$ is the maximal ideal of T, then $\mathcal{M} \cap R_\mathfrak{m} = \mathfrak{m}_\mathfrak{m}$. Since $\mathfrak{m}_\mathfrak{m}$ contains elements t^2 and t^3 with $\mathrm{ord}_t(t^2) = 2$ and $\mathrm{ord}_t(t^3) = 3$, if $\mathfrak{m}_m m$ had a single generator π then we would have $\mathrm{ord}_t(\pi) = 1$. But there is no such element in $R_\mathfrak{m}$.*

Thus, whereas in the previous section we gave conditions for a valuation ring to be a DVR, now we want conditions for a one-dimensional Noetherian local domain to be a DVR. Remarkably, it turns out if a local, one-dimensional Noetherian domain has any one of a large number of good properties, it will necessarily be a DVR:

THEOREM 17.8. *(Recognition Theorem for DVRs) Let R be a one-dimensional Noetherian local domain, with maximal ideal $\mathfrak{m}$. the following are equivalent:*

(i) *R is **regular**: the dimension of $\frac{\mathfrak{m}}{\mathfrak{m}^2}$ as an $R/\mathfrak{m}$-vector space is 1.*
(ii) *$\mathfrak{m}$ is principal.*
(iii) *R is a PID.*
(iv) *R is a UFD.*
(v) *R is integrally closed.*
(vi) *Every nonzero ideal is of the form $\mathfrak{m}^n$ for some $n \in \mathbb{N}$.*

PROOF. (i) $\iff$ (ii): Choose $t \in \pi \backslash \pi^2$. By assumption, t generates $\mathfrak{m}/\mathfrak{m}^2$, so by Nakayama's Lemma t generates $\mathfrak{m}$. Conversely, if $\mathfrak{m}$ is monogenic as an R-module, certainly $\mathfrak{m}/\mathfrak{m}^2$ is monogenic as an $R/\mathfrak{m}$-module.
Evidently (iii) $\implies$ (ii). Proposition 16.5 gives (ii) $\implies$ (iii) and also (ii) $\implies$ (vi). Moreover (iii) $\iff$ (iv) by Proposition 16.1 and (iv) $\implies$ (v) by 15.14. Next, for all $n \in \mathbb{N}$ we have $(\pi)^n/(\pi)^{n+1} \cong R/\mathfrak{m}$, thus R is regular.

(vi) $\implies$ (i): Assume that $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 > 1$. Choose $u \in \mathfrak{m} \backslash \mathfrak{m}^2$. Then

$$\mathfrak{m} \subsetneq \langle u, \mathfrak{m}^2 \rangle \subsetneq \mathfrak{m}^2.$$

So we have (i) $\iff$ (ii) $\iff$ (iii) $\iff$ (iv) $\iff$ (vi) $\implies$ (v).

Finally, we show (v) $\implies$ (ii): Let $0 \neq x \in \mathfrak{m}$. Since $\mathfrak{m}$ is the only prime ideal containing (x) we must have $r((x)) = \mathfrak{m}$. Since $R/(x)$ is Noetherian, its radical, $\mathfrak{m}/(x)$, is nilpotent, so there is a unique *least* $n \in \mathbb{Z}^+$ such that $\mathfrak{m}^n \subset (x)$. Let $y \in \mathfrak{m}^{n-1} \backslash (x)$ and consider the element $q = \frac{x}{y}$ of the fraction field K of R. Since $y \notin (x)$, $q^{-1} = \frac{y}{x} \notin R$; since R is integrally closed in K, q^{-1} is not integral over R. Then $\mathfrak{q}^{-1}\mathfrak{m}$ is not contained in $\mathfrak{m}$, for otherwise $\mathfrak{m}$ would be a faithful $R[q^{-1}]$-module

which is finitely generated as an R-module, contradicting Theorem 14.1. But by construction, $q^{-1}\mathfrak{m} = \frac{y}{x}\mathfrak{m} \subset R$, hence $q^{-1}\mathfrak{m} = R$ and then $\mathfrak{m} = Rx = (x)$. □

2.3. Extensions of Discrete Valuations. Let L/K be a field extension. If G is a totally ordered commutative group and $w : L^\times \twoheadrightarrow G$ is a G-valued valuation, then $v := w|_K^\times : K^\times \to G$ is a valuation on K with value group $w(K^\times)$, which may be a proper subgroup of G (indeed, it may even be trivial). We also say that the valuation w on L is an **extension** of the valuation v on K.

There is a whole theory of extensions of valuations, of which we need only a small piece here. First:

LEMMA 17.9. *Let L/K be a field extension of finite degree n, let G be a totally ordered commutative group, and let $v : L^\times \twoheadrightarrow G$ be a G-valued valuation on L. Let $H := v(K^\times)$. Then G is, as an ordered commutative group, isomorphic to a subgroup of H.*

PROOF. ([**J2**, p. 582]) For any nonzero $x \in L$, we have a relation of the form $\sum_{i=1}^k \alpha_i x^{n_i}$, where $\alpha_i \in K$ and the n_i are integers such that $[L : K] = n \geqslant n_1 > n_2 > \ldots > n_k \geqslant 0$. If there existed any index j such that for all $i \neq j$ we had $v(\alpha_i x^{n_i}) > v(\alpha_j x^{n_j})$, then $\infty = v(\sum_{i=1}^k \alpha_i x^{n_i}) = v(\alpha_j x^{x_j})$ and thus $\alpha_j x^{n_j} = 0$, a contradiction. Thus there exist $i > j$ such that $v(\alpha_i x^{n_i}) = v(\alpha_j x^{n_j})$, so

$$(n_i - n_j)v(x) = v(\alpha_j \alpha_i^{-1}) \in H.$$

Thus, for $x \in L^\times$, we have $(n!)v(x) \in H$. Since G is torsionfree, the endomorphism $[n!] : G \to G$ given by $g \mapsto n!g$ is injective, and thus $[n!] : G \hookrightarrow [n!]G \subset H$. □

In consequence:

COROLLARY 17.10. *Let L/K be a finite field extension, let v be a valuation on K, and let w be an extension of v to a valuation on L. Then v is discrete if and only if w is discrete.*

EXERCISE 17.11. *Prove Corollary 17.10.*

For the rest of this section we will be working exclusively with rank 1 valuations, so we take all of our value groups to be subgroups of $\mathbb{R}$. With this very slightly different viewpoint, a **discrete valuation** on a field is a map $v : K^\times \to \mathbb{R}$ satisfying (VRK1) and (VRK2) such that $v(K^\times)$ is infinite cyclic. We say that two valuations on K are **equivalent** if they have the same valuation ring. We say that a discrete valuation v is **normalized** if $v(K^\times) = \mathbb{Z}$.

EXERCISE 17.12. *Let K be a field.*

a) *Let $v, w : K^\times \to \mathbb{R}$ be discrete valuations on K. Show: v and w are equivalent if and only if there is $\alpha \in \mathbb{R}^{>0}$ such that for all $x \in K^\times$, $w(x) = \alpha v(x)$.*
b) *Let $v : K^\times \to \mathbb{R}$ be a discrete valuation on K. Show: there is a unique normalized discrete valuation w on K that is equivalent to v.*

Now let L/K be a field extension of finite degree n, and $w : L^\times \to \mathbb{R}$ a rank 1 valuation on L, and let v be the restriction of w to K. As we just saw, v is discrete if and only if w is. Now the point is: we may replace either v or w by an equivalent normalized discrete valuation, but we cannot necessarily do both while keeping the condition that v is the restriction of w to K. Indeed, let $\mathfrak{m}$ be the maximal ideal of

the valuation ring R of K and let $\mathcal{M}$ be the maximal ideal of the valuation ring T of L. Then $\mathfrak{m}T$ is a nonzero ideal generated by elements of positive valuation, so it is proper in T. Thus there is a unique $e \in \mathbb{Z}^+$ such that

$$\mathfrak{m}T = \mathcal{M}^e.$$

The positive integer e is called the **ramification index** of w over v. We say that $w|v$ is **unramified** if $e = 1$. If v is normalized – so $v(K^\times) = \mathbb{Z}$ – then $w(K^\times) = \frac{1}{e}\mathbb{Z}$, so w is normalized if and only if $w|v$ is unramified. Similarly, if w is normalized – so $w(L^\times) = \mathbb{Z}$ – then $v(K^\times) = e\mathbb{Z}$, so v is normalized if and only if $w|v$ is unramified. Thus for a ramified extension we need to choose whether to normalize v or to normalize w: both conventions are in common use.

THEOREM 17.11. *Let $v : K^\times \to \mathbb{R}$ be a discrete valuation on a field K, and let L/K be a finite degree field extension. Then the set of valuations w on L that extend v is finite and nonempty.*

We will defer the proof of Theorem 17.11 until §21.3 (and will not use the result until Chapter 22). Let us also remark that this is a very special case of the truth: in fact, given any valuation $v : K^\times \twoheadrightarrow G$ on a field and any field extension L/K, the valuation v extends to L in the sense that there is a valuation $w : L^\times \twoheadrightarrow \tilde{G}$ and an embedding $\iota : G \hookrightarrow \tilde{G}$ of ordered commutative groups such that $w|_{K^\times} = \iota \circ v$. We however do not need this result.

2.4. Modules over DVRs.

LEMMA 17.12. *Let R be a DVR with uniformizing element π, and let $a \in \mathbb{Z}^+$. Then the ring $R_a = R/(\pi^a)$ is **self-injective** – i.e., R_a is an injective R_a-module.*

EXERCISE 17.13. *Prove Lemma 17.12. (Hint: Baer's Criterion!)*

THEOREM 17.13. *Let R be a DVR with uniformizing element π, and let M be a nonzero finitely generated R-module.*

a) *There is $N \in \mathbb{N}$ and positive integers $n, a_1 \geqslant a_2 \geqslant \ldots \geqslant a_n$ such that*

$$M \cong R^N \oplus \bigoplus_{i=1}^{n} R/(\pi^{a_i}). \tag{52}$$

b) *The numbers $N, n, a_1, \ldots, a_n$ are invariants of the isomorphism class of the module M: i.e., they are the same for any two decompositions of M as in (52) above.*

PROOF.
Step 0: Consider the canonical short exact sequence

$$0 \to M[\text{tors}] \to M \to M/M[\text{tors}] \to 0.$$

Since M is a finitely generated module over a Noetherian ring, $M[\text{tors}]$ is finitely generated. Moreover, $M/M[\text{tors}]$ is a finitely generated torsionfree module over a PID, hence is free (Proposition 3.64). Moreover, we know that the rank of a free module over any (commutative!) ring is well-defined (when R is a domain with fraction field K, the proof is especially easy: the rank of a free module M is $\dim_K M \otimes_R K$), so the invariant N in the statement of the theorem is precisely the rank of $M/M[\text{tors}]$. Moreover, since $M/M[\text{tors}]$ is free – hence projective – the sequence splits, so

$$M = R^N \oplus M[\text{tors}].$$

We are reduced to the case of a nonzero finitely generated torsion module M.
Step 1: The annihilator of M is an ideal of R, of which there aren't so many: it must be (π^{a_1}) for some $a_1 \in \mathbb{Z}^+$. Thus M may be viewed as a faithful $R_{a_1} = R/(\pi^{a_1})$-module. Moreover, choosing an element x of M which is not annihilated by π^{a_1-1}, the unique R_{a_1}-module map $R_{a_1} \to M$ which sends 1 to m is an injection. Taking $M' = M/R_{a_1}$, we get a short exact sequence

$$0 \to R_{a_1} \to M \to M' \to 0.$$

By Lemma 17.12, R_{a_1} is an injective R_{a_1}-module, so the sequence splits:

$$M \cong R_{a_1} \oplus M'.$$

Step 2: Since M is finitely generated over R_{a_1}, it is a quotient of some Artinian R_{a_1}-module $R_{a_1}^M$, hence by Theorem 8.4 M is Artinian. Moreover M is a finitely generated module over the Noetherian ring, so M is also Noetherian. By Theorem 8.14, this means that M has finite length as an R-module. Hence so does its direct summand M' and indeed clearly the length of M' is less than the length of M. This completes the proof of part a) by induction.
Step 3: So far we have that a finitely generated torsion R-module is of the form $\bigoplus_{i=1}^n R/(\pi^{a_i})$ with positive integers $a_1 \geqslant a_2 \geqslant \ldots \geqslant a_n$, and with $\operatorname{ann}(M) = (\pi^{a_1})$. In order to prove the uniqueness statement of part b), it suffices to prove that for all $0 < b \leqslant a$, $R/(\pi^b)$ is an indecomposable $R/(\pi^a)$-module. If so, then

$$M \cong \bigoplus_{i=1}^n R/(\pi^{a_i})$$

is simply the decomposition of the finite length module M into indecomposables described in the Krull-Schmidt Theorem: in particular, since clearly $R/(\pi^a) \cong R/(\pi^b)$ implies $a = b$ (consider annihilators), it is unique up to permutation of the factors. So suppose that $R/(\pi^a) = M_1 \oplus M_2$ with M_1, M_2 nonzero. If π^a does not annihilate M_1, then as above we can find a split embedding $R/(\pi^a) \hookrightarrow M_1$, which contradicts the fact that the length of M_1 must be smaller than the length of $R/(\pi^a)$. So M_1 – and similarly M_2 – is annihilated by π^{a-1} and thus $R/(\pi^a)$ would be annihilated by π^{a-1}, a contradiction. □

3. Ordered commutative groups

Let $(G, +)$ be an commutative group, written additively. In particular the identity element of G will be denoted by 0. As for rings, we write $G^\bullet$ for $G \backslash \{0\}$.

By an **ordering** on G we mean a total (a.k.a. linear) ordering $\leqslant$ on G which is compatible with the addition law in the following sense:

(OAG) For all $x_1, x_2, y_1, y_2 \in G$, $x_1 \leqslant x_2$ and $y_1 \leqslant y_2$ implies $x_1 + y_1 \leqslant x_2 + y_2$.

One has the evident notions of a homomorphism of ordered commutative groups, namely an isotone group homomorphism.

EXERCISE 17.14. *Let $(G, \leqslant)$ be an ordered commutative group.*
a) *Let $x \in G^\bullet$. Show: either $x > 0$ or $-x > 0$ but not both.*
b) *Show: for all $x, y \in G$, $x \leqslant y \iff -y \leqslant -x$.*

EXERCISE 17.15. *Let $(G, \leqslant)$ be an ordered commutative group, and let H be a subgroup of G. Show: the induced order on H makes H into an ordered commutative group.*

EXAMPLE 17.14. *For an ordered field $(F, \leqslant)$, the additive group $(F, +)$ is an ordered commutative group. In particular, the additive group $(\mathbb{R}, +)$ of the real numbers is an ordered commutative group, as is any subgroup. In particular, $(\mathbb{Z}, +)$ and $(\mathbb{Q}, +)$ are ordered commutative groups.*

EXERCISE 17.16. *Exhibit an commutative group which admits two nonisomorphic orderings.*

EXAMPLE 17.15. *(Lexicographic ordering): Let $\{G_i\}_{i \in I}$ be a nonempty indexed family of ordered commutative groups. Suppose that we are given a well-ordering on the index set I. We may then endow the direct product $G = \prod_{i \in I} G_i$ with the structure of an ordered commutative group, as follows: for $(g_i), (h_i) \in G$, we decree $(g_i) < (h_i)$ if for the least index i such that $g_i \neq h_i$, $g_i < h_i$.*

EXERCISE 17.17. *Check that the lexicographic ordering on the product $\prod_{i \in I} G_i$ is indeed a total ordering on G.*

THEOREM 17.16. *(Levi [**Le43**]) For an commutative group G, the following are equivalent:*

(i) *The group G admits at least one ordering.*
(ii) *The group G is torsionfree.*

PROOF. (i) $\implies$ (ii) Suppose $<$ is an ordering on G and let $x \in G^\bullet$. Then exactly one of $x, -x$ is positive; without loss of generality say it is x. Then for all $n \in \mathbb{Z}^+$, $nx = x + \ldots x$ (n times) must be positive, so x has infinite order in G.
(ii) $\implies$ (i): Let G be a torsionfree commutative group. By Corollary 3.98, G is a flat $\mathbb{Z}$-module. Tensoring the injection $\mathbb{Z} \hookrightarrow \mathbb{Q}$ gives us an injection $G \hookrightarrow G \otimes \mathbb{Q}$. Since $\mathbb{Q}$ is a field, the $\mathbb{Q}$-module $G \otimes \mathbb{Q}$ is free, i.e., it is isomorphic to $\bigoplus_{i \in I} \mathbb{Q}$. Choose a well-ordering on I. Give each copy of $\mathbb{Q}$ its standard ordering as a subfield of $\mathbb{R}$ and put the lexicographic ordering on $\bigoplus_{i \in I} \mathbb{Q} \cong G \otimes \mathbb{Q}$. Via the injection $G \hookrightarrow G \otimes \mathbb{Q}$ this induces an ordering on G. □

EXERCISE 17.18.

a) *Show: the commutative group $\mathbb{Z}$ admits exactly one ordering (here when we say "ordering", we always mean "ordering compatible with the group structure in the sense of (OAG).*
b) *Give an example of an commutative group which admits two distinct – even nonisomorphic – orderings.*

An ordered commutative group $(G, +)$ is **Archimedean** if for all $x, y \in G$ with $x > 0$, there exists $n \in \mathbb{Z}^+$ with $nx > y$.

EXERCISE 17.19.

a) *Suppose H is a subgroup of the Archimedean ordered group $(G, +)$. Show: the induced ordering on G is Archimedean.*
b) *Let $(G, +)$ be an ordered commutative group such that there exists an embedding $(G, +) \hookrightarrow (\mathbb{R}, +)$ into the additive group of the real numbers. Deduce: G is Archimedean.*

Conversely:

THEOREM 17.17. *(Hölder [**Hö01**]) Let $(G,+)$ be an ordered commutative group. If G is Archimedean, there is an embedding $(G,+) \hookrightarrow (\mathbb{R},+)$.*

PROOF. We may assume G is nontrivial. Fix any positive element x of G. We will construct an order embedding of G into $\mathbb{R}$ mapping x to 1.

Namely, let $y \in G$. Then the set of integers n such that $nx \leqslant y$ has a maximal element n_0. Put $y_1 = y - n_0 x$. Now let n_1 be the largest integer n such that $nx \leqslant 10y_1$: observe that $0 \leqslant n_1 < 10$. Continuing in this way we get a set of integers $n_1, n_2, \ldots \in \{0, \ldots, 9\}$. We define $\varphi(y)$ to be the real number $n_0 + \sum_{k=1}^{\infty} \frac{n_k}{10^k}$. It is not hard to show that φ is isotone – $y \leqslant y' \implies \varphi(y) \leqslant \varphi(y')$ – and also that φ is injective: we leave these tasks to the reader.

But let us check that φ is a homomorphism of groups. For $y \in G$, and $r \in \mathbb{Z}^+$, let $\frac{n}{10^r}$ be the rational number obtained by truncating $\varphi(y)$ at r decimal places. The numerator n is characterized by $nx \leqslant 10^r y < (n+1)x$. For $y' \in G$, if $n'x \leqslant 10^r y' \leqslant (n'+1)x$, then

$$(n+n')x \leqslant 10^r(y+y') < (n+n'+2)x,$$

so

$$\varphi(y+y') - (n+n')10^{-r} < \frac{2}{10^r}$$

and thus

$$|\varphi(y+y') - \varphi(y) - \varphi(y')| < \frac{4}{10^r}.$$

Since r is arbitrary, we conclude $\varphi(y+y') = \varphi(y) + \varphi(y')$. □

A nontrivial ordered commutative group which can be embedded in $\mathbb{R}$ is said to have **rank one**. For many applications this is by far the most important case. Later we will give the general definition of the rank of an ordered commutative group.

LEMMA 17.18. *Let R be a domain, $(G,\leqslant)$ a totally ordered commutative group, and let $G^+ = \{g \in G \mid g \geqslant 0\}$. Then:*

a) *G^+ is an ordered commutative monoid.*
b) *The monoid ring $R[G^+]$ is a domain.*
c) *The group ring $R[G]$ is naturally isomorphic to the localization of $R[G^+]$ at the multiplicative subset G^+. In particular, $R[G]$ is a domain.*

EXERCISE 17.20.

a) *Write out the statements of Lemma 17.18 when $G = \mathbb{Z}$.*
b) *Prove Lemma 17.18.*

THEOREM 17.19. *(Malcev, Neumann) For any ordered commutative group G, there exists a valuation domain with value group isomorphic to G.*

PROOF. It suffices to construct a field K and a surjective map $v : K^\times \to G$ satisfying (VD1K) and (VD2K). Let k be any field and put $A := k[G^+]$. By Lemma 17.18, A is a domain; let K be its fraction field. Define a map $v : A^\bullet \to G$ by sending a nonzero element $\sum_{g \in G} a_g g$ to the least g for which $a_g \neq 0$. Then v satisfies the properties of Exercise 17.5 and therefore extends uniquely to a valuation $v : K^\times \to G$, where K is the fraction field of R. □

Recall from §5.5 the notion of a "big monoid ring" $k[[\Gamma]]$, the collection of *all* functions $f : \Gamma \to k$ under pointwise addition and convolution product. As we saw though, in order for the convolution product to be defined "purely algebraically" – i.e., without recourse to some limiting process – we need to impose the condition of *divisor finiteness* on Γ. It follows easily from Proposition **??** that for $\Gamma = G^{\geqslant 0}$ the monoid of non-negative elements in a totally ordered commutative group, divisor finiteness holds if and only if $G = \mathbb{Z}$, i.e., if and only if the valuation is discrete.

However, Malcev [**Ma48**] and Neumann [**Ne49**] independently found a way around this by considering a set in between $k[G^{\geqslant 0}]$ and $k[[G^{\geqslant 0}]]$. Namely, define $k_{\mathrm{MN}}[G^{\geqslant 0}]$ to be the set of all functions $f : G^{\geqslant 0} \to k$ such that the *support* of f – i.e., the set of $g \in G^{\geqslant 0}$ such that $f(g) \neq 0$ – is well-ordered. It turns out that on such functions the convolution product can be defined and endows $k_{\mathrm{MN}}[G^{\geqslant 0}]$ with a domain. The fraction field $k_{\mathrm{MN}}(G)$ is simply the collection of all functions $f : G \to k$ with well-ordered support. Moreover, mapping each such nonzero function to the least element of G in its support gives a G-valued valuation. The elements of such rings are called **Malcev-Neumann series**.

3.1. Convex Subgroups.

A subset S of a totally ordered set $(X, \leqslant)$ is **convex** if for all $x < y < z \in X$, if $x, z \in S$, then $y \in S$.

Exercise 17.21. *Let H be a subgroup of an ordered commutative group $(G, \leqslant)$. Show: H is convex if and only if for all $x, y \in G$ with $0 \leqslant x \leqslant y$, if $y \in H$ then also $x \in H$.*

Proposition 17.20. *Let $(G, \leqslant)$ be an ordered commutative group, and let $\mathcal{C}(G)$ be the set of convex subgroups of G. Then $\mathcal{C}(G)$ is totally ordered under inclusion.*

Proof. Let H_1 and H_2 be convex subgroups. Seeking a contradiction, we suppose there is $h_1 \in H_1 \backslash H_2$ and $h_2 \in H_2 \backslash H_1$. Subgroups are closed under inversion, so we may assume that $h_1, h_2 \geqslant 0$ and then, without loss of generality, that $0 \leqslant h_1 \leqslant h_2$. Since H_2 is a convex subgroup, we get $h_1 \in H_2$, contradiction. □

For an ordered commutative group G, we define $r(G)$ to be the order isomorphism type of the linearly ordered set $\mathcal{C}(G)^\bullet = \mathcal{C}(G) \backslash \{\{0\}\}$ of nontrivial convex subgroups of G. When this set is finite we may view $r(G)$ as a natural number, and when $r(G)$ is infinite, we write $r(G) > n$ for all $n \in \mathbb{N}$. In particular, $r(G) = 1$ if and only if G is nontrivial and has no proper, nontrivial convex subgroups.

Exercise 17.22.

a) *Let G_1 and G_2 be ordered commutative groups, and let $G = G_1 \times G_2$ be lexicographically ordered. Show: $r(G) = r(G_1) + r(G_2)$, where on the right hand side we have the ordered sum: every element of the first linearly ordered set is less than every element of the second linearly ordered set.*

b) *Let $n \in \mathbb{Z}^+$. Show: $r(\mathbb{Z}^n) = n$.*

Proposition 17.21. *For a nontrivial ordered commutative group G, the following are equivalent:*

(i) *G is Archimedean.*

(ii) *G has rank one.*

PROOF. (i) $\implies$ (ii): We go by contraposition: let $\{0\} \subsetneq H \subsetneq G$ be a convex subgroup of G, let $y \in G^+ \backslash H$ and let $x \in H^+$. If for some $n \in \mathbb{Z}^+$ we had $nx > y$ then by convexity of H we would have $y \in H$: contradiction.
(ii) $\implies$ (i): Again we go by contraposition: suppose G is not Archimedean, so there are $x, y \in G$ such that $0 < nx < y$ for all $n \in \mathbb{Z}^+$. Let H be the set of elements of G such that there is $n \in \mathbb{Z}^+$ such that $-nx \leqslant z \leqslant nx$. Then $\{0\} \subsetneq H \subsetneq G$ is a convex subgroup of G. □

EXERCISE 17.23. *Let R be a valuation ring with nontrivial value group G. Show: R is completely integrally closed if and only if G has rank one.*

EXERCISE 17.24. *Let R be a valuation ring containing a field of rank greater than one. (Notice that our proof of Theorem 17.19 shows that for any totally ordered group G and any field k, there is a valuation ring containing k and with value group G.) Use Theorem 14.14 to show that $R[[t]]$ is* not *integrally closed.*

In view of Proposition 17.21 it makes sense to call $r(G)$ the **rank** of the linearly ordered group G: indeed we have already defined a group to have rank one if it is nontrivial and can be order embedded in $(\mathbb{R}, +)$. By Theorem 17.17, G is Archimedean if and only if it can be order embedded in $(\mathbb{R}, +)$, so by Proposition 17.21 our new notion of rank coincides with our old notion of rank one.

THEOREM 17.22. *Let $v : K^\times \to (G, \leqslant)$ be a valuation on a field K, with valuation ring R. There is an inclusion reversing bijection $\Phi : \operatorname{Spec} R \to \mathcal{C}(G)$ given by*

$$\mathfrak{p} \mapsto G \backslash \pm v(\mathfrak{p}^\bullet).$$

PROOF. Step 1: We claim that for $\mathfrak{p} \in \operatorname{Spec} R$, $\Phi(\mathfrak{p})$ is a convex subgroup. Clearly $\Phi(\mathfrak{p})$ contains 0 and is closed under inversion, so suppose $\sigma_1, \sigma_2 \in \Phi(\mathfrak{p})$. Since $\Phi(\mathfrak{p})$ is closed under inversion, we may assume that either $\sigma_1, \sigma_2 > 0$ or $\sigma_1 > 0$, $\sigma_2 < 0$ and $\sigma_1 + \sigma_2 > 0$.
Case 1: Suppose $\sigma_1, \sigma_2 > 0$. Choose $x_1, x_2 \in R$ with $v(x_i) = \sigma_i$ for $i = 1, 2$. If $\sigma_1 + \sigma_2 \notin \Phi(\mathfrak{p})$, then there is $x \in \mathfrak{p}$ with $v(x) = \sigma_1 + \sigma_2 = v(x_1 x_2)$. Thus $ux = x_1 x_2$ for some $u \in R^\times$, so $x_1 x_2 \in \mathfrak{p}$. Since $\mathfrak{p}$ is prime this implies that at least one of x_1, x_2 lies in $\mathfrak{p}$, hence at least one of σ_1, σ_2 does not lie in $\Phi(\mathfrak{p})$, contradiction.
Case 2: Suppose $\sigma_1 > 0$, $\sigma_2 < 0$, $\sigma_1 + \sigma_2 > 0$. If $\sigma_1 + \sigma_2 \notin \Phi(\mathfrak{p})$, then there is $x \in \mathfrak{p}$ with $v(x) = \sigma_1 + \sigma_2$. Choose $y \in R$ with $v(y) = -\sigma_2$. Then $yx \in \mathfrak{p}$ and $v(yx) = \sigma_1$, so $\sigma_1 \in v(\mathfrak{p})$, contradiction.

To show convexity: let $0 \leqslant \sigma_1 \leqslant \sigma_2 \in G$, and suppose $\sigma_2 \in \Phi(\mathfrak{p})$. If $\sigma_1 \in v(\mathfrak{p}^\bullet)$, then there exists $x \in \mathfrak{p}$ with $v(x) = \sigma_1$. There is $y \in R$ such that $v(y) = \sigma_2 - \sigma_1$, and thus $v(yx) = \sigma_2$, so $\sigma_2 \notin \Phi(\mathfrak{p})$, contradiction.
Step 2: To a convex subgroup H of G, we associate

$$\Psi(H) = \{x \in R^\bullet \mid v(x) \notin H\} \cup \{0\}.$$

By similar – but easier – reasoning to the above, one checks that $\Psi(H) \in \operatorname{Spec} R$.
Step 3: One checks that Φ and Ψ are mutually inverse maps, hence Φ is a bijection. □

EXERCISE 17.25. *Supply the details of Steps 2 and 3 in the proof of Theorem 17.22.*

EXERCISE 17.26. *Show: the maps Φ and Ψ are obtained by restricting the Galois connection associated to a relation on $R \times G$.*

COROLLARY 17.23. *For a valuation ring R t, the following are equivalent:*

(i) *R has rank one, i.e., the value group is Archimedean and nontrivial.*

(ii) *R has Krull dimension one.*

Let R be a domain with fraction field K. Recall that an overring of R is a ring T with $R \subseteq T \subseteq K$. Every localization of R is an overring; depending upon R, it may or may not be the case that every overring is a localization (later we will see many counterexamples). Clearly an overring T of R is a localization if and only if it is the subring of T generated by R and by the inverses of elements lying in some subset of $R^\bullet$. This simple remark is certainly not the full answer to the question of when overrings are localizations, but it can be helpful: earlier we used it to see that every overring of a PID is a localization.

Now let R be a valuation ring. We will determine all the overrings of R. First, we claim that every overring T of R is a localization: indeed, every element of $T \setminus R$ is the inverse of an element of R. Also T is again a valuation ring, hence local. By Exercise 7.13, this means that $T = R_{\mathfrak{p}}$ for a unique $\mathfrak{p} \in \operatorname{Spec} R$. This gives us an inclusion-reversing bijection between $\operatorname{Spec} R$ and the set of overings of R. Combining with Theorem 17.22 we get an inclusion-preserving bijection between the set of convex subgroups H of the value group G and the set of overrings of T: the saturated multiplicative subset corresponding to H is

$$S_H := \{x \in R^\bullet \mid v(x) \in H\}.$$

We have

$$(S_H^{-1}R)^\times = \{x \in K^\times \mid v(x) \in H\},$$

so

$$K^\times/(S_H^{-1}R)^\times = G/H.$$

Since $S_H^{-1}R$ is a valuation ring, the group G/H is ordered and the quotient $q : G \to G/H$ is a homomorphism of ordered groups. We have discovered that the quotient group G/H can be given an ordering such that $q : G \to G/H$ is an isotone map, necessarily in a unique way: if $(X, \leqslant)$ is an ordered set, Y is a set and $f : X \to Y$ is a surjection, then the only possible total ordering on Y making f an isotone map is $y_1 < y_2$ if and only if for all $x_1 \in f^{-1}(y_1)$ and $x_2 \in f^{-1}(y_2)$ we have $x_1 < x_2$. However this need not be well-defined. We are seeing here that it is, but let us also show this directly:

PROPOSITION 17.24. *Let $(G, +, \leqslant)$ be an ordered commutative group, and let H be a convex subgroup. On the quotient G/H, we define $x + H < y + H$ if $H < y - x$. This defines a total ordering on G/H and $q_H : G \to G/H$ is an isotone map.*

EXERCISE 17.27. *Prove Proposition 17.24.*

In fact, now that we know Proposition 17.24, we can just as easily run things in reverse: given a G-valued valuation $v : K^\times \to G$ on a field K and a convex subgroup H of G with quotient map $q_H : G \to G/H$, then

$$v_H := q_H \circ v : K^\times \to G/H$$

is a G/H-valued valuation on K whose valuation ring R_H contains the valuation ring R of v.

EXERCISE 17.28. *Let G be an ordered commutative group, and let H be a nontrivial convex subgroup of G.*

a) *Show: the set of convex subgroups of G/H is the set of convex subgroups of G containing H. In other words, the possible ranks of quotients of G by convex subgroups are the principal upsets $[H, \infty)$ of $r(G)$.*
b) *Suppose that $r(G) = n$ is finite. Show: $r(G) = r(H) + r(G/H)$.*

4. Connections with integral closure

Let $(R, \mathfrak{m}_R)$ and $(T, \mathfrak{m}_T)$ be local rings with $R \subset T$. We say that **T dominates R**, and write $R \leqslant T$, if $\mathfrak{m}_T \cap R = \mathfrak{m}_R$.

LEMMA 17.25. *Let R be a subring of a field K, and let $\mathfrak{p} \in \operatorname{Spec} R$. Then there exists a valuation ring T of K such that $R \subset T$ and $\mathfrak{m}_T \cap R = \mathfrak{p}$.*

PROOF. (Matsumura)
Step 0: We may replace R by $R_{\mathfrak{p}}$ and thus asume that $(R, \mathfrak{p})$ is a local ring. In this case, what we are trying to show is precisely that there exists a valuation ring of K dominating R.
Step 1: Let $\mathcal{F}$ be the set of all rings R' with $R \subset R' \subset K$ such that $\mathfrak{p}R' \subsetneq R'$, partially ordered by inclusion. We have $R \in \mathcal{F}$, so $\mathcal{F} \neq \varnothing$. Moreover the union of a chain in $\mathcal{F}$ is again an element of $\mathcal{F}$, so Zorn's Lemma gives us a maximal element T of $\mathcal{F}$. Since $\mathfrak{p}T \subsetneq T$, there exists a maximal ideal $\mathfrak{m}$ of T containing $\mathfrak{p}T$. Since $T \subset T_{\mathfrak{m}}$ and $T_{\mathfrak{m}} \in \mathcal{F}$, by maximality of T we have $T = T_{\mathfrak{m}}$, so $(T, \mathfrak{m})$ is a local ring dominating $(R_{\mathfrak{p}}, \mathfrak{p})$.
Step 2: We CLAIM that T is a valuation ring.
PROOF OF CLAIM: Let $x \in K^\times$. We wish to show that at least one of x, x^{-1} lies in T. Seeking a contradiction, assume neither is the case. Then $T[x]$ properly contains T, so by maximality of T we have $1 \in \mathfrak{p}T[x]$, i.e., we get a relation of the form

$$1 = a_0 + a_1 x + \ldots + a_n x^n, a_i \in \mathfrak{p}T.$$

Since T is local, $1 - a_0 \in T^\times$, and the relation may be rewritten in the form

$$1 = b_1 x + \ldots + b_n x^n, b_i \in \mathfrak{m}. \tag{53}$$

Among all such relations, we may choose one with minimal exponent n. In exactly the same way, $T[x^{-1}]$ properly contains T and thus there exists a relation

$$1 = c_1 x^{-1} + \ldots + c_n x^{-m}, c_i \in \mathfrak{m}, \tag{54}$$

and among all such relations we may choose one with minimal m. Without loss of generality $m \leqslant n$: otherwise interchange x and x^{-1}. Then multiplying (54) by $b_n x^n$ and subtracting from (53) gives another relation of the form (53) but with exponent smaller than n, contradiction. □

A subring R of a field K is a **maximal subring** if $R \subsetneq K$ and there is no ring intermediate between R and K.

EXERCISE 17.29. *Let K be the algebraic closure of a finite field.*
a) *Show: every subring of K is a field.*
b) *Show: K has no maximal subring. (Hint: use Galois theory.)*

EXERCISE 17.30. *Let R be a valuation ring, with value group G and fraction field K.*
a) *Show: the following are equivalent:*
(i) *R is a maximal subring of K.*

(ii) $r(G) = 1$.

b) *Show: the following are equivalent:*
   (i) *There is a maximal subring of K containing R.*
   (ii) *The set of proper convex subgroups of G has a maximal element.*

c) *Show: the following are equivalent:*
   (i) *R is the intersection of its proper overrings.*
   (ii) *The set of nontrivial convex subgroups of G* does not *have a minimal element.*

THEOREM 17.26. *Let K be a field and $R \subset K$ a subring. Then the integral closure $\overline{R}$ of R in K is the intersection of all valuation rings of K containing R.*

PROOF. Let $\mathcal{R}$ be the intersection of all valuation rings of K containing R. Since each such ring is integrally closed in K and the intersection of a family of rings each integrally closed in K is again integrally closed in K, $\mathcal{R}$ is integrally closed in K, whence $\overline{R} \subset \mathcal{R}$.
Conversely, let $x \in K \backslash \overline{R}$. It suffices to find a valuation ring of K containing R but not x. Let $y = x^{-1}$. The ideal $yR[y]$ of $R[y]$ is proper: for if $1 = a_1 y + \ldots + a_n y^n$ with $a_i \in R$, then x would be integral over R. Let $\mathfrak{p}$ be a maximal ideal of R containing y. By Lemma 17.25, there exists a valuation ring T of K such that $R[y] \subset K$ and $\mathfrak{m}_T \cap R[y] = \mathfrak{p}$. Then $y = x^{-1} \in \mathfrak{m}_T$, so $x \notin T$. □

In Theorem 17.1 it is natural to ask when a domain R is the intersection of the *discrete* valuation rings containing it. Such an R must be integrally closed. This is however not sufficient: if R is a valuation ring with value group G, then R a rank one overring if and only if G admits a maximal proper convex subgroup H, in which case $S_H^{-1}R$ is the unique rank one overring of R. So a valuation ring is never the intersection of rank 1 overrings that properly contain it and thus is not an intersection of DVRs unless it is itself a DVR.

This raises the question of whether any Noetherian integrally closed domain is the intersection of DVRs. The answer to this is a resounding **yes**, as we will show later on. On the other hand:

EXERCISE 17.31. *Let R be a UFD, and let $\mathrm{Spec}_1 R$ denote the set of height one primes of R.*

a) *Show: for each height one $\mathfrak{p} \in SpecR$, the localization $R_\mathfrak{p}$ is a DVR.*
b) *Show: $R = \bigcap_{\mathfrak{p} \in \mathrm{Spec}_1 R} R_\mathfrak{p} = R$.*

Thus every UFD is the intersection of its DVR overrings, so there are many non-Noetherian rings with this property.

5. Another proof of Zariski's Lemma

The following result is a close relative of Lemma 17.25.

LEMMA 17.27. *Let K be a field and Ω an algebraically closed field. Let $\mathcal{S}$ be the set of all pairs (A, f) with A is a subring of K and $f : A \hookrightarrow \Omega$, partially ordered by*

$$(A, f) \leqslant (A', f') \iff A \subset A' \text{ and } f'|_A = f.$$

Then $\mathcal{S}$ contains maximal elements, and for any maximal element (B, g), B is a valuation ring of K.

PROOF. An easy Zorn's Lemma argument shows that $\mathcal{S}$ has maximal elements. Let (B, g) be a maximal element. Put $\mathfrak{p} = \mathrm{Ker}(g)$; since $g(B)$ is a subring of the field Ω, it is a domain and thus $\mathfrak{p}$ is a prime ideal of B. By functoriality of localization, G extends to a homomorphism $B_{\mathfrak{p}} \to \Omega$. By maximality of (B, g) we have $B_{\mathfrak{p}} = B$, so that B is a local ring with maximal ideal $\mathfrak{p}$. If there existed an element $x \in K$ which is transcendental over the fraction field of B, then $B[x]$ is a polynomial ring and certainly g extends to $B[x]$. So K is algebraic over the fraction field of B.

Next let $x \in K^\times$. We claim that either the ideal $\mathfrak{p}B[x]$ or $\mathfrak{p}B[x^{-1}]$ is proper. Indeed this is proved exactly as in Lemma 17.25 above.

Finally, we show that B is a valuation ring of K. Let $x \in K^\bullet$. Without loss of generality, we may assume that $\mathfrak{p}B[x]$ is a proper ideal of B (otherwise replace x by x^{-1}). Put $B' = B[x]$. By assumption, $\mathfrak{p}B[x]$ is contained in a maximal ideal $\mathfrak{m}$ of B' and $\mathfrak{m} \cap B = \mathfrak{p}$. Hence the embedding of domains $B \to B'$ induces an embedding of fields $k := B/\mathfrak{p} \hookrightarrow B'/\mathfrak{m} = k'$. Moreover k' is generated over k by the image of the algebraic element x, so k'/k is a finite degree field extension. So g induces an embedding $k \hookrightarrow \Omega$, and since Ω is algebraically closed, this extends to an embedding $k' = B'/\mathfrak{m} \hookrightarrow \Omega$. By maximality of B, this implies $x \in B$. □

PROPOSITION 17.28. *Let $A \subset B$ be domains with B finitely generated as an A-algebra. Let $\beta \in B^\bullet$. There exists $\alpha \in A^\bullet$ satisfying the following property: any homomorphism f of A into an algebraically closed field Ω with $f(\alpha) \neq 0$ extends to a homomorphism $f : B \to \Omega$ with $f(\beta) \neq 0$.*

PROOF.
Step 0: Induction on the number of generators reduces us to the case $B = A[x]$.
Step 1: Suppose that x is transcendental over A, i.e., B is a univariate polynomial ring over A. Write

$$\beta = a_n x^n + \ldots + a_1 x + a_0, a_i \in A$$

and put $\alpha = a_0$. If $f : A \to \Omega$ is such that $f(\alpha) \neq 0$, then since Ω is infinite, there exists $\zeta \in \Omega$ such that $f(a_n)\zeta^n + \ldots + f(a_1)\zeta + f(a_0) \neq 0$. Using the universal polynomial of polynomial rings, we may uniquely extend f to a homomorphism from B to Ω by putting $f(x) = \zeta$, and then $f(\beta) \neq 0$.
Step 2: Suppose that x is algebraic over the fraction field of A. Then so is β^{-1}. Hence we have equations of the form

$$a_n x^m + \ldots + a_1 x + a_0, \ a_i \in A$$
$$a'_m \beta^{-m} + \ldots + a'_1 \beta^{-1} + a'_0, a'_i \in A.$$

Put $\alpha = a_n a'_m$. Suppose $f : A \to \Omega$ is any homomorphism with $f(\alpha) \neq 0$. We may extend f to a homomorphism from $A[\alpha^{-1}] \to \Omega$ by mapping α^{-1} to $f(\alpha)^{-1}$ and then, by Lemma 17.27, to a homomorphism $f : C \to \Omega$ for some valuation ring C containing $A[\alpha^{-1}]$. By construction x is integral over $A[\alpha^{-1}]$. Since C is integrally closed, $x \in C$. Thus C contains B and in particular $\beta \in C$. Similarly, β^{-1} is integral over $A[\alpha^{-1}]$ so $\beta^{-1} \in C$. Thus $\beta \in C^\times$, so $f(\beta) \neq 0$. Restricting to B gives the desired homomorphism. □

Proof of Zariski's Lemma: Let k be a field and B a field that is finitely generated as a k-algebra. We want to show that the field extension B/k has finite degree. For this it is enough to show that B/k is algebraic. In Proposition 17.28 take $A = k$, $\beta = 1$ and Ω to be an algebraic closure of k. □

CHAPTER 18

Normalization Theorems

We work in the following situation: R is an integrally closed domain with fraction field K, L/K is a field extension, and $S = I_L(R)$ is the integral closure of R in L. In more geometric language, S is the **normalization** of R in the extension L/K.

As above, we may as well assume that L/K is algebraic, since in the general case, if we let $L' = I_K(L)$ be the algebraic closure of K in L, then S is contained in L' anyway. So let us assume this. Then we know that S is integrally closed with fraction field L. We also know that the Krull dimensions of S and R coincide.

The major questions are the following:

(Q1) Is S finitely generated as an R-module?
(Q2) Is S Noetherian?
(Q3) If not, then can anything nice be said about S?

Note that if R is Noetherian, then an affirmative solution to (Q1) implies an affirmative answer to (Q2). Also, the example $R = \mathbb{Z}$, $K = \mathbb{Q}$, $L = \overline{\mathbb{Q}}$ shows that both (Q1) and (Q2) may have a negative answer if $\big[L : K\big]$ is infinite.

1. The First Normalization Theorem

The first, and easiest, result is the following:

THEOREM 18.1. *(First Normalization Theorem) Let R be an integrally closed domain with fraction field K, L/K a finite **separable** field extension, and $S = I_L(R)$.*

a) *There is a K-basis $x_1, \ldots, x_n$ of L such that S is contained in the R-submodule generated by $x_1, \ldots, x_n$.*
b) *If R is Noetherian, S is a finitely generated R-module.*
c) *If R is a PID, then S is a free R-module of rank $\big[L : K\big]$.*

PROOF. a) By the proof of Proposition 14.10, for any $x \in L$, there exists $0 \neq r \in R$ such that $rx \in S$. Therefore there exists a K-basis $u_1, \ldots, u_n$ of L such that $u_i \in S$ for all i.[1] Now take $x \in S$ and write $x = \sum_i b_i u_i$ with $b_i \in K$. Since L/K is separable there are $n = \big[L : K\big]$ distinct K-embeddings of L into $\overline{K}$, say $\sigma_1, \ldots, \sigma_n$, and the discriminant $\Delta = \Delta(u_1, \ldots, u_n) = (\det(\sigma_j(u_i)))^2$ is nonzero. We may put $\sqrt{\Delta}) = \det(\sigma_j(u_i))$. For all $1 \leqslant j \leqslant n$ we have

$$\sigma_j(x) = \sum_i b_i \sigma_j(u_i).$$

[1]We have not yet used the separability hypothesis, so this much is true in the case of an arbitrary finite extension.

Using Cramer's rule, we may solve for the b_i to get

$$\sqrt{\Delta}b_i = \sum_j d_{ij}\sigma_j(x),\ db_i = \sum_j \sqrt{d}d_{ij}\sigma_j(x),$$

where the d_{ij}'s are polynomials in the $\sigma_j(u_i)$ with coefficients in $\mathbb{Z}$. Thus Δb_i and $\sqrt{\Delta}b_i$ are integral over R. Since $\Delta \in K$ and R is integrally closed, we have $\Delta b_i \in A$. Therefore S is contained in the R-span $\langle \frac{u_1}{\Delta}, \ldots, \frac{u_n}{\Delta}\rangle_R$, establishing part a).
b) By part a), S is a submodule of a finitely generated R-module, hence if R is Noetherian S is finitely generated.
c) We know that S is a submodule of a free rank n R-module; if R is a PID, then S is a free R-module of rank at most n. Since $S \otimes_R K = L$, the rank must be n. □

This has the following important result, which is the first of three fundamental **finiteness theorems** in algebraic number theory, the existence of a finite integral basis for the ring of integers of any algebraic number field:

COROLLARY 18.2. *Let $R = \mathbb{Z}$, $K = \mathbb{Q}$, L a number field of degree n. Then the ring $\mathbb{Z}_L = \overline{\mathbb{Z}} \cap K$ of all algebraic integers lying in L, is an integrally closed, Noetherian domain of Krull dimension one which is, as a $\mathbb{Z}$-module, free of rank n.*

PROOF. Indeed $\mathbb{Z}_L = I_L(\mathbb{Z})$, so by Proposition 14.12, it is integrally closed in its fraction field L. Since $\mathbb{Z}$ is a PID and $L/\mathbb{Q}$ is finite separable, Theorem 18.1 applies to show that $\mathbb{Z}_L \cong \mathbb{Z}^n$ as a $\mathbb{Z}$-module. Being a finitely generated $\mathbb{Z}$-module, still more is it a finitely generated *algebra* over the Noetherian ring $\mathbb{Z}$, so it is itself Noetherian. Since $\mathbb{Z}$, like any PID, has Krull dimension one and $\mathbb{Z}_L$ is an integral extension of $\mathbb{Z}$, by Corollary 14.20 $\mathbb{Z}_L$ also has Krull dimension one. □

A **Dedekind domain** is a domain which is Noetherian, integrally closed and of Krull dimension at most one. We will systematically study Dedekind domains in §20, but for now observe that Corollary 18.2 implies that the ring of integers of an algebraic number field is a Dedekind domain. In fact, the argument establishes that the normalization S of any Dedekind domain R in a finite separable field extension L/K is again a Dedekind domain that is finitely generated as an R-module.

2. The Second Normalization Theorem

THEOREM 18.3. *(Second Normalization Theorem) Let R be a domain with fraction field K. Suppose that at least one of the following holds:*
- *R is absolutely finitely generated – i.e., finitely generated as a $\mathbb{Z}$-algebra – or*
- *R contains a field k and is finitely generated as a k-algebra.*

Let L/K be a finite degree field extension. Then $S = I_L(R)$ is a finitely generated R-module.

PROOF. First suppose that R is a finitely generated algebra over a field k.
Step 0: We may assume that L/K is normal. Indeed, let M be the normal closure of L/K, so M/K is a finite normal extension. Let T be the integral closure of R in M. If we can show that T is finitely generated over R, then, since R is Noetherian, the finitely submodule S is also finitely generated over R.
Step 1: We will make use of the field-theoretic fact that if M/K is normal and L is the maximal purely inseparable subextension of M/K, then M/L is separable [**FT**, §6.3]. Let S be the integral closure of R in L and T the integral closure of R in T. Then T is a finitely generated R-module if and only if T is a finitely generated

S-module and S is a finitely generated R-module. Suppose we can show that S is a finitely generated R-module. Then S is a finitely generated R-algebra so S is a Noetherian integreally closed domain, and the module finiteness of T over S follows from Theorem 18.1. Thus we are redueced to the case in which L/K is purely inseparable, say $[L:K] = q = p^a$.
Step 2: By Noether Normalization, R is finitely generated as a module over a polynomial ring $k[t_1, \ldots, t_d]$. If S is a finitely generated $k[t_1, \ldots, t_d]$-module, then certainly it is a finitely generated R-module. Thus we may assume without loss of generality that $R = k[t_1, \ldots, t_d]$ and $K = k(t_1, \ldots, t_d)$. In particular we may assume that R is integrally closed (in K). For all $a \in L$, $N_{L/K}(a) = a^q \in K$. Let k'/k be the extension obtained by adjoining the qth roots of the coefficients of the minimal polynomials of a finite set of generators of L/K, so k'/k is finite, so $L \subset k'(t_1^{1/q}, \ldots, t_d^{1/q})$. So it is enough to show that the integral closure of $k[t_1, \ldots, t_d]$ in $k'(t_1^{1/q}, \ldots, t_d^{1/q})$ is finite over $k[t_1, \ldots, t_d]$. But in this case the integral closure can be computed exactly: it is $k'[t_1^{1/q}, \ldots, t_d^{1/q}]$ (indeed it is at least this large, and this ring is a UFD, hence integrally closed), which is finite over $k[t_1, \ldots, t_d]$. □

3. The Krull-Akizuki Theorem

In this section we come to one of the most beautiful and useful results in the subject, the Krull-Akizuki Theorem. Its content is essentially that normalization works magnificently well in dimension one. Our treatment follows [**M**, §11].

LEMMA 18.4. *For a Noetherian domain R, the following are equivalent:*
(i) *R has dimension at most one.*
(ii) *For every nonzero ideal I of R, the ring R/I is Artinian.*
(iii) *For every nonzero ideal I of R, we have $\ell_R(R/I) < \infty$.*

PROOF. (i) $\implies$ (ii): R/I is Noetherian, and prime ideals of R/I correspond to prime ideals of R containing the nonzero ideal I, so are all maximal. By Theorem 8.36, R/I is Artinian.
(ii) $\implies$ (iii): Every finitely generated module over an Artinian ring is also Noetherian hence has finite length.
$\neg$ (i) $\implies$ $\neg$ (iii): If R has dimension greater than one, there is a nonzero, nonmaximal prime ideal $\mathfrak{p}$ of R. The R-module $R/\mathfrak{p}$ is a domain which is not a field, hence not Artinian, hence of infinite length. □

LEMMA 18.5. *Let R be a one-dimensional Noetherian domain with fraction field K. Let M be a torsionfree R-module with $r = \dim_K M \otimes_R K < \infty$. Then for all $x \in R^\bullet$, $\ell(M/xM) \leqslant r\ell(R/xR)$.*

PROOF. Step 1: First suppose that M is finitely generated. Let $\eta_1, \ldots, \eta_r \in M$ be R-linearly independent and put $E = \langle \eta_1, \ldots, \eta_r \rangle_M$. Since $r = \dim_K M \otimes_R K$, for $\eta \in M$, there is $t \in R$ with $t\eta \in E$. Put $C = M/E$. Then C is finitely generated, so there is $t \in R^\bullet$ such that $tC = 0$. By Lemma 18.4, the ring R/tR is Artinian. Since C is a finitely generated R/tR-module, it has finite length, and thus it also has finite length, say m, as an R-module. For $x \in R^\bullet$ and $n \in \mathbb{Z}^+$, the exact sequence

$$E/x^nE \longrightarrow M/x^nM \to C/x^nC$$

yields

$$\ell(M/x^nM) \leqslant \ell(E/x^nE) + \ell(C). \tag{55}$$

Since E and M are torsionfree, we have $x^iM/x^{i+1}M \cong M/xM$ for all $i \in \mathbb{N}$ and similarly $x^iE/x^{i+1}E \cong E/xE$; it follows that

$$n\ell(M/xM) \leqslant n\ell(E/xE) + \ell(C) \ \forall n \in \mathbb{Z}^+,$$

and thus

$$\ell(M/xM) \leqslant \ell(E/xE).$$

Since $E \cong R^r$, $E/xE \cong (R/xR)^r$, so

$$\ell(M/xM) \leqslant \ell((R/xR)^r) = r\ell(R/xR).$$

Step 2: In the general case, put $\overline{M} = M/xM$ and let $\overline{N} = \langle \overline{\omega_1}, \ldots, \overline{\omega_s} \rangle$ be a finitely generated submodule of $\overline{M}$. Lift each $\overline{\omega_i}$ to $\omega_i \in M$ and put $M_1 = \langle \omega_1, \ldots, \omega_s \rangle$. We get

$$\ell(\overline{N}) \leqslant \ell(M_1/M_1 \cap xM) \leqslant \ell(M_1/xM_1) \leqslant r\ell(R/xR),$$

the last inequality by Step 1. Because the right hand side of this inequality is independent of $\overline{N}$, by Exercise 8.13 $\ell(\overline{M}) \leqslant r\ell(R/xR)$.
Step 3: We have $\ell(R/xR) < \infty$ by Lemma 18.4. □

THEOREM 18.6. *(Krull-Akizuki) Let R be a one-dimensional Noetherian domain with fraction field K, let L/K be a finite degree field extension of K, and let S be a ring with $R \subset S \subset L$. Then:*

a) *S is Noetherian of dimension at most 1.*
b) *If J is a nonzero ideal of S, then S/J is a finite length R-module.*

PROOF. b) It is no loss of generality to replace L by the fraction field of S. Let $r = [L : K]$, so that S is a torsionfree R-module of rank r. By Lemma 18.5, for any $x \in R^\bullet$ we have $\ell_R(S/aS) < \infty$. Let J be a nonzero ideal of S and $b \in J^\bullet$. Since b is algebraic over R it satisfies a relation

$$a_m b^m + \ldots + a_1 b + a_0 = 0, \ a_i \in R$$

of minimal degree. Since S is a domain, $a_0 \in (J \cap R)^\bullet$, so

$$\ell_R(S/J) \leqslant \ell_R(S/a_0S) < \infty.$$

a) Since

$$\ell_S(J/a_0S) \leqslant \ell_R(J/a_0S) \leqslant \ell_R(S/a_0S) < \infty,$$

J/a_0S is a finitely generated S-module. Being an extension of a finitely generated S-module by a finitely generated S-module, J is itself a finitely generated: S is Noetherian. If $\mathcal{P}$ is a nonzero prime ideal of S then $S/\mathcal{P}$ has finite length so is an Artinian domain, hence a field: S has dimension at most one. □

We remark that S need not be finitely generated as an R-module. Thus Step 2 in the proof of Lemma 18.5 is actually used in the proof of the Krull-Akizuki Theorem.

Comparing the following exercise with Exercise 8.34 gives a good illustration of how much simpler things are in dimension 1.

EXERCISE 18.1. *Let k be a field, and let A be a k-subalgebra of $k[t]$. Show: either $A = k$ or A is a one-dimensional Noetherian domain that is finitely generated as a k-algebra.*

COROLLARY 18.7. *Let R be a one-dimensional Noetherian domain with fraction field K, let L/K be a finite degree field extension, and let S be the integral closure of R in L. Then S is a Dedekind domain, and for every maximal ideal $\mathfrak{p}$ of R there are only finitely many prime ideals of S lying over $\mathfrak{p}$.*

EXERCISE 18.2. *Prove Corollary 18.7.*

CHAPTER 19

The Picard Group and the Divisor Class Group

1. Fractional ideals

Let R be a domain with fraction field K. A **fractional ideal** of R is a nonzero R-submodule I of K for which there exists $0 \neq a \in R$ such that $aI \subset R$ – or equivalently, if $I \subset \frac{1}{a}R$.

When one is talking about fractional R-ideals, one inevitably wants to compare them to ideals of R in the usual sense, and for this it is convenient to speak of an **integral R-ideal**, i.e., an R-submodule of R.

EXERCISE 19.1. *Show: a finitely generated R-submodule of K is a fractional ideal.*

Some texts *define* a fractional R-ideal to be a finitely generated R-submodule of K, but this seems wrong because we certainly want every nonzero integral ideal of R to be a fractional ideal, but if R is not Noetherian then not every integral ideal will be finitely generated. (It is not such a big deal because most of these references are interested only in *invertible* fractional ideals – to be studied shortly – and one of the first things we will see is that an invertible fractional ideal is necessarily finitely generated as an R-module.)

We denote the set of all fractional ideals of R by $\mathrm{Frac}(R)$.

THEOREM 19.1. *Let I, J, M be fractional ideals in a domain R.*

a) *All of*
$$I \cap J = \{x \in K \mid x \in I \text{ and } x \in J\},$$
$$I + J = \{x + y \mid x \in I,\ y \in J\},$$
$$IJ = \{\sum_{i=1}^{n} x_i y_i,\ \mid x_i \in I,\ y_i \in J\},$$
$$(I : J) = \{x \in K \mid xJ \subset I\}$$
are fractional ideals.

b) *We may partially order* $\mathrm{Frac}(R)$ *under inclusion. Then the greatest lower bound of I and J is $I \cap J$ and the least upper bound of I and J is $I + J$.*

c) *If $I \subset J$, then $IM \subset JM$.*

d) *R itself is a fractional ideal, and $R \cdot I = R$. Thus the fractional ideals form a commutative monoid under multiplication.*

PROOF. a) It is immediate that $I \cap J$, $I + J$, IJ and $(I : J)$ are all R-submodules of K. It remains to be seen that they are nonzero and can be scaled to lie inside R. Suppose $I \subset \frac{1}{a}R$ and $J \subset \frac{1}{b}R$. Then:

$0 \subsetneq I \subset I + J \subset \frac{1}{ab}R$, so $I + J$ is a fractional ideal.
$0 \subsetneq IJ \subset I \cap J \subset \frac{1}{ab}R$, so IJ and $I \cap J$ are fractional ideals.
Since $I \cap R$ is a fractional ideal, there exists a nonzero $c \in R$ lying in I. Then for $y \in J$, $\frac{c}{b}y \in cR \subset I$, so $\frac{c}{b} \in (I : J)$. Similarly, if $0 \neq d \in J$, then $\frac{1}{ad}(I : J) \subset R$.
Parts b), c) and d) can be easily verified by the reader. □

PROPOSITION 19.2. *Let I, J be fractional ideals for a domain R. The map*

$$(I : J) \to \mathrm{Hom}_R(J, I),\ x \mapsto (y \mapsto xy)$$

is an isomorphism of R-modules.

EXERCISE 19.2. *Prove Proposition 19.2.*

The following result is the analogue for fractional ideals of Exercise 7.11:

PROPOSITION 19.3. *Let I and J be fractional ideals for a domain R, and let $S \subseteq R$ be a multiplicative subset.*

a) *We have $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$.*
b) *We have $S^{-1}(I + J) = S^{-1}I + S^{-1}J$.*
c) *We have $S^{-1}(IJ) = (S^{-1}I)(S^{-1}(J)$.*
d) *If J is finitely generated, then we have $S^{-1}(I : J) = (S^{-1}I : S^{-1}J)$.*

EXERCISE 19.3. *Prove Proposition 19.3.*

A fractional ideal is **principal** if it is of the form xR for some $x = \frac{a}{b} \in K^\bullet$.

PROPOSITION 19.4. *For a fractional ideal I of R, the following are equivalent:*

(i) *I is principal.*
(ii) *I is monogenic as an R-module.*
(iii) *$I \cong_R R$.*
(iv) *I is free as an R-module.*

PROOF. (i) $\iff$ (ii): By definition, a monogenic R-module M is one of the form Rx for some $x \in M$.
(i) $\implies$ (iii): For $x \in K^\times$ multiplication by x^{-1} is an R-module isomorphism from xR to R.
(iii) $\implies$ (ii) and (iii) $\implies$ (iv) are immediate.
(iv) $\implies$ (iii): It is no loss of generality to assume that $I \subset R$. Since any two elements $x, y \in I$ are R-linearly dependent – indeed $(y)x + (-x)y = 0$ – if I is free, it must have rank 1. □

If xR is a principal fractional ideal, so is $x^{-1}R$, and we have

$$(xR)(x^{-1}R) = R.$$

Thus, in $\mathrm{Frac}(R)$, every principal fractional ideal xR is a unit, with inverse $x^{-1}R$.

Let $\mathrm{Prin}(R)$ denote the set of all principal fractional ideals of the domain R.

EXERCISE 19.4. *Show: $\mathrm{Prin}(R)$ is a subgroup of $\mathrm{Frac}(R)$, and we have a short exact sequence $1 \to R^\times \to K^\times \to \mathrm{Prin}(R) \to 1$.*

EXERCISE 19.5. *Define the **ideal class monoid** $C(R) = \mathrm{Frac}(R)/\mathrm{Prin}(R)$.*

a) *Show: $C(R)$ is well-defined as a commutative monoid.*
b) *Show: $C(R)$ is trivial if and only if R is a PID.*

c) *Show:* $C(\mathbb{Z}[\sqrt{-3}])$ *is a finite commutative monoid which is not a group.*

For a general domain, $C(R)$ need only be a commutative monoid. In the next section we "repair" this by defining the **Picard group** $\mathrm{Pic}(R)$.

2. The Ideal Closure

For a nonempty subset S of K, put

$$S^* = (R : S) = \{x \in K \mid xS \subseteq R\}.$$

EXERCISE 19.6. *For nonempty subsets S_1 and S_2 of K, show $S_1 \subseteq S_2 \implies S_1^* \supseteq S_2^*$.*

Usually we are interested in I^* for a fractional R-ideal I, and in general it is not so easy to compute. But it is in the following case let $a \in K^\times$. Then

$$(aR)^* = \{x \in K \mid xaR \subseteq R\} = \{x \in K \mid xa \subseteq R\} = (1/aR).$$

EXERCISE 19.7. *Let R be a domain. Show: for any fractional R-ideal I, we have that I^* is a fractional R-ideal.*
(Hint: sandwich I between two principal fractional ideals.)

The fractional ideal I^* is called[1] the **quasi-inverse** of I. As we shall see later in this section, if the ideal I has an inverse in the monoid $\mathrm{Frac}\, R$, then its inverse must be I^*: i.e. $II^* = R$. In general though all we get from the definition of I^* is the relation $II^* \subset R$. This observation motivates the following one.

PROPOSITION 19.5. *Let R be a domain, and let $\mathcal{R} \subset K \times K$ given by $x\mathcal{R}y$ if and only if $xy \in R$. Let (Φ, Ψ) be the induced Galois connection from 2^K to itself. Then, for any fractional ideal I of R, $\Phi(I) = \Psi(I) = I^*$. In other words, $I \mapsto I^*$ is a self-dual antitone Galois connection on* $\mathrm{Frac}\, R$.

EXERCISE 19.8. *Prove Proposition 19.5.*

As usual, we denote the associated closure operator by $I \mapsto \overline{I}$. Now the machinery of Galois connections gives us many facts for free that we would otherwise have to spend a little time deriving:

COROLLARY 19.6. *Let R be a domain and let $I, J \in \mathrm{Frac}\, R$.*

a) *If $I \subset J$, then $J^* \subset I^*$.*
b) *We have $I^* \subset J^* \iff \overline{I} \supset \overline{J}$.*
c) *We have $\overline{\overline{I}} = \overline{I}$ and $\overline{I^*} = I^*$.*
d) *We have $(I + J)^* = I^* \cap J^*$. In fact, if $\{I_i\}_{i \in S}$ is any family of fractional ideals, then*

$$(\langle I_i \mid i \in S\rangle)^* = \bigcap_{i \in S} I_i^*.$$

EXERCISE 19.9. *Prove Corollary 19.6.*

PROPOSITION 19.7. *Let R be a domain. Let S be a nonempty set and $\{I_i\}_{i \in S}$ a family of fractional R-ideals.*

a) *If $\langle I_i \mid i \in S\rangle$ is a fractional R-ideal, then so is $\langle \overline{I_i} \mid i \in S\rangle$ and*

$$\overline{\langle I_i\rangle} = \overline{\langle \overline{I_i}\rangle}.$$

[1] Unfortunately?

b) *Suppose that each I_i is divisorial and $\bigcap_{i\in I} I_i \neq (0)$. Then $\bigcap_{i\in I} I_i$ is divisorial.*

PROOF. a) Put $I := \langle I_i \mid i \in S\rangle$ and $J := \langle \overline{I_i} \mid i \in S\rangle$. For all $i \in S$ we have $I_i \subseteq I$ hence $\overline{I_i} \subseteq \overline{I}$ and thus $J \subseteq \overline{I}$ is a fractional ideal and $\overline{J} \subseteq \overline{\overline{I}} = \overline{I}$. Since $I \subseteq J$ we have $\overline{I} \subseteq \overline{J}$.
b) Let $x \in \overline{\bigcap_{i\in S} I_i}$. Then for all $i \in S$ we have $x \in \overline{I_i} = I_i$, so $x \in \bigcap_{i\in S} I_i$. □

EXERCISE 19.10. *Give an example of $I, J \in \operatorname{Frac} R$ with $J^* \subset I^*$ but $I \not\subset J$.*

PROPOSITION 19.8. *For a domain R and $I \in \operatorname{Frac} R$, we have*

$$\overline{I} = \bigcap_{d\in K^\times \mid I\subset d^{-1}R} d^{-1}R.$$

PROOF.

$$\overline{I} = (I^*)^* = \{x \in K \mid xI^* \subset R\} = \{x \in K \mid \forall d \in K^\times, dI \subset R \implies xd \in R\}$$

$$= \bigcap_{d\in K^\times \mid I\subset d^{-1}R} d^{-1}R.$$ □

3. Invertible fractional ideals and the Picard group

Like any monoid, $\operatorname{Frac}(R)$ has a group of units, i.e., the subset of invertible elements. Explicitly, a fractional ideal I is **invertible** if there exists another fractional ideal J such that $IJ = R$. We denote the group $\operatorname{Frac}(R)^\times$ of invertible fractional ideals by $\operatorname{Inv}(R)$.

EXERCISE 19.11. *Let $I_1, \ldots, I_n$ be fractional ideals of R. Show: the product $I_1 \cdots I_n$ is invertible if and only if each I_i is invertible.*

LEMMA 19.9.

a) *For a fractional ideal I, the following are equivalent:*
   (i) *I is invertible.*
   (ii) *$II^* = R$.*

b) *(**To contain is to divide**) If $I \subset J$ are fractional ideals with J invertible, then*

$$I = J(I : J).$$

PROOF. a) (i) $\implies$ (ii): As above, for any fractional ideal I we have $II^* \subset R$. Now suppose there exists some fractional ideal J such that $IJ = R$, then

$$J \subset (R : I) = I^*,$$

so

$$R = IJ \subset II^*.$$

(ii) $\implies$ (i) is obvious.
b) By definition of $(I : K)$ we have $J(I : J) \subset I$. Conversely, since $I \subset J$, $J^{-1}I \subset R$. Since $(J^{-1}I)J = I$, it follows that $J^{-1}I \subset (I : J)$ and thus $I \subset J(I : J)$. □

PROPOSITION 19.10. *Let I be an invertible fractional ideal. Then I is a finitely generated projective rank one module.*

PROOF. Step 1: We show an invertible fractional ideal I is a finitely generated projective module. Since $II^* = R$, we may write $1 = \sum_{i=1}^n x_i y_i$ with $x_i \in I$ and $y_i \in I^*$. For $1 \leqslant i \leqslant n$, define $f_i \in \mathrm{Hom}(I, R)$ be $f_i(x) = xy_i$. Then for all $x \in I$,

$$x = \sum_i x x_i y_i = \sum_i x_i f_i(x).$$

By the Dual Basis Lemma, I is a projective R-module generated by $x_1, \ldots, x_n$.
Step 2: To show that I has rank one, it suffices to show that for all $\mathfrak{p} \in \mathrm{Spec}\, R$, $I_{\mathfrak{p}}$ is free of rank one over $R_{\mathfrak{p}}$. But since projective implies locally free, we know that $I_{\mathfrak{p}}$ is a free $R_{\mathfrak{p}}$-module of some rank, and for any ring R and any ideal I, I cannot be free of rank greater than one over R. Indeed, if so I would have two R-linearly independent elements x and y, which is absurd, since $yx + (-x)y = 0$. □

Conversely:

PROPOSITION 19.11. *Let I be a nonzero fractional ideal of R which is, as an R-module, projective. Then I is invertible.*

PROOF. We have the inclusion $\iota : II^* \subset R$ which we wish to show is an equality. This can be checked locally: i.e., it is enough to show that for all $\mathfrak{p} \in \mathrm{Spec}\, R$, $\iota_{\mathfrak{p}} : I_{\mathfrak{p}} I_{\mathfrak{p}}^* \to R_{\mathfrak{p}}$ is an isomorphism. By Proposition 19.3, it is equivalent to show that $I_{\mathfrak{p}}(I_{\mathfrak{p}})^* \to R_{\mathfrak{p}}$ is an isomorphism, but since I is projective, by Kaplansky's Theorem $I_{\mathfrak{p}}$ is free. As above, being a nonzero ideal, it is then necessarily free of rank one, i.e., a principal fractional ideal $xR_{\mathfrak{p}}$. It follows immediately that $(I_{\mathfrak{p}})^* = x^{-1}R_{\mathfrak{p}}$ and thus that the map is an isomorphism. □

To sum up:

THEOREM 19.12. *Let R be a domain, and let I be a fractional R-ideal. Then I is invertible if and only if it is projective, in which case it is projective of rank one.*

For any R-module M, the R-dual is defined to be $M^\vee = \mathrm{Hom}(M, R)$. There is a canonical R-bilinear map $T : M^\vee \times M \to R$ obtained by mapping $(f, x) \mapsto f(x)$. This induces an R-linear map $T : M^\vee \otimes_R M \to R$. We say that an R-module M is **invertible** if T is an isomorphism.

PROPOSITION 19.13. *Consider the following conditions on an R-module M:*

(i) *M is rank one projective.*
(ii) *M is invertible.*
(iii) *There is an R-module N and an isomorphism $T : M \otimes_R N \cong R$.*

Then (i) $\implies$ (ii) $\implies$ (iii) always, and (iii) $\implies$ (i) if M is finitely generated.

PROOF. (i) $\implies$ (ii): We have a map $T : M^\vee \otimes M \to R$ so that it suffices to check locally that is an isomorphism, but M is locally free so this is easy.
(ii) $\implies$ (iii) is immediate.
(iii) $\implies$ (i): Since M is finitely generated, by Theorem 13.37 to show that M is projective it is enough to show that for all $\mathfrak{p} \in \mathrm{Spec}\, R$ $M_{\mathfrak{p}}$ is free of rank one. Thus we may as well assume that $(R, \mathfrak{m})$ is a local ring with residue field $R/\mathfrak{m} = k$. The base change of the isomorphism T to $R/\mathfrak{m}$ is an isomorphism (recall that tensor product commutes with base change)

$$T_k : M/\mathfrak{m}M \otimes_k N/\mathfrak{m}N \to k.$$

This shows that $\dim_k M/\mathfrak{m}M = \dim_k N/\mathfrak{m}N = 1$, so in particular $M/\mathfrak{m}M$ is monogenic as an $R/\mathfrak{m}$-module. By Nakayama's Lemma the lift to R of any generator x of $M/\mathfrak{m}M$ is a generator of M, so M is a monogenic R-module and is thus isomorphic to R/I for some ideal I. But indeed $I = \operatorname{ann}(M) \subset \operatorname{ann}(M \otimes_R N) = \operatorname{ann}(R) = 0$, so $M \cong R/(0) = R$ is free of rank one. □

THEOREM 19.14. *(Cohen) Let R be a domain.*

a) *The set of invertible ideals of R is an Oka family in the sense of § 4.5.*
b) *If every nonzero prime ideal of R is invertible, then every nonzero fractional ideal of R is invertible.*

PROOF. a) Let $I \subset J$ be ideals of R with J and $(I : J)$ invertible (this implies $I \neq 0$). By Lemma 19.9, $I = J(I : J)$ and thus, as the product of two invertible ideals, I is invertible. Since for any ideals I, J of R we have $(I : J) = (I : I + J)$, by taking $J = \langle I, x\rangle$ for any $x \in R$ we recover the Oka condition.
b) Seeking a contradiction, suppose I is a nonzero ideal of R which is not invertible. Consider the partially ordered set $\mathcal{S}$ of ideals containing I which are not invertible. Then the union of any chain in $\mathcal{S}$ is a non-invertible ideal: indeed, if it were invertible then by Proposition 19.10 it would be finitely generated and thus equal to some element in the chain: contradiction. Thus by Zorn's Lemma there is a nonzero ideal J which is maximal element in the family of ideals which are not invertible. By part a) and the Prime Ideal Principle, J is prime: contradiction. □

THEOREM 19.15. *Let I and J be invertible fractional ideals. Then there is a canonical isomorphism of R-modules*

$$I \otimes_R J \xrightarrow{\sim} IJ.$$

PROOF. The natural multiplication map $I \times J \to IJ$ is R-bilinear so factors through an R-module map $m : I \otimes_R J \to IJ$. Once we have a globally defined map, to see that it is an isomorphism it is enough to check it locally: for all $\mathfrak{p} \in \operatorname{Spec} R$,

$$m_{\mathfrak{p}} : I_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} J_{\mathfrak{p}} \xrightarrow{\sim} I_{\mathfrak{p}} J_{\mathfrak{p}}$$

and we are thus allowed to assume that I and J are principal fractional ideals. This makes things very easy, and we leave the endgame to the reader. □

COROLLARY 19.16. *Let I and J be invertible fractional R-ideals. the following are equivalent:*

(i) *There is $x \in K^\times$ such that $xI = J$.*
(ii) *We have $I \cong_R J$, i.e., I and J are isomorphic R-modules.*

PROOF. (i) $\implies$ (ii): If $J = xI$, then multiplication by x gives an R-module isomorphism from I to J.
(ii) $\implies$ (i): Since $I \cong_R J$ we have

$$I^{-1}J \cong I^{-1} \otimes_R J \cong I^{-1} \otimes_R I \cong II^{-1} = R.$$

By Proposition 19.4, $I^{-1}J$ is a principal fractional ideal, i.e., there exists $x \in K^\times$ such that $I^{-1}J = xR$. Multiplying through by I, we get $xI = J$. □

PROPOSITION 19.17. *Let M be a rank one projective module over a domain R with fraction field K. Then there is a fractional R-ideal I such that $M \cong_R I$.*

PROOF. Since M is projective, it is flat, and so tensoring the injection $R \hookrightarrow K$ with M we get an injection $f : M = R \otimes_R M \hookrightarrow M \otimes_R K \cong K$, the last isomorphism since M is locally free of rank 1. Thus $f : M \xrightarrow{\sim} f(M)$, and $f(M)$ is a finitely generated R- submodule of K and thus a fractional R-ideal. □

Putting together all the pieces we get the following important result.

THEOREM 19.18. *Let R be a domain. The following two commutative groups are canonically isomorphic:*

(i) $\mathrm{Inv}(R)/\mathrm{Prin}(R)$ *with* $[I][J] := [IJ]$.
(ii) *Isomorphism classes of rank one projective R-modules under tensor product.*

We may therefore define the ***Picard group*** $\mathrm{Pic}\, R$ *to be* either *the group of invertible fractional ideals modulo principal fractional ideals under multiplication or the group of isomorphism classes of rank one projective modules under tensor product.*

LEMMA 19.19. *In any domain R, let $\mathcal{P}_1, \ldots, \mathcal{P}_k$ be a set of invertible prime ideals and let $\mathcal{Q}_1, \ldots, \mathcal{Q}_l$ be any set of prime ideals. Suppose that*

$$\prod_{i=1}^{k} \mathcal{P}_i = \prod_{j=1}^{l} \mathcal{Q}_j.$$

Then $i = j$ and there exists some permutation σ of the set $\{1, \ldots, k\}$ such that for all $1 \leqslant i \leqslant k$ we have $\mathcal{P}_i = \mathcal{Q}_{\sigma(i)}$.

In other words, prime factorization is unique for products of invertible primes.

PROOF. Assume without loss of generality that $\mathcal{P}_1$ does not strictly contain any $\mathcal{P}_i$. Since $\prod_j \mathcal{Q}_j \subset \mathcal{P}_1$, some $\mathcal{Q}_j$, say $\mathcal{Q}_1$, is contained in $\mathcal{P}_1$. Similarly, since $\prod_i \mathcal{P}_i \subset \mathcal{Q}_1$, there exists i such that $\mathcal{P}_i \subset \mathcal{Q}_1$. Thus $\mathcal{P}_i \subset \mathcal{Q}_1 \subset \mathcal{P}_1$. By our assumption on the minimality of $\mathcal{P}_1$, we have $\mathcal{P}_1 = \mathcal{P}_i = \mathcal{Q}_1$. We can thus cancel $\mathcal{P}_1 = \mathcal{Q}_1$ by multiplying by $\mathcal{P}_1^{-1}$ and obtain the result by induction. □

LEMMA 19.20. *Let R be an integrally closed Noetherian domain with fraction field K, and let I be a fractional R-ideal. Then $(I : I) := \{x \in K \mid xI \subset I\} = R$.*

PROOF. Clearly $R \subset (I : I)$. Conversely, let $x \in (I : I)$. Then I is a faithful $R[x]$-module that is finitely generated over R, so x is integral over R. □

LEMMA 19.21. *Let R be a domain with fraction field K, $S \subset R \backslash \{0\}$ a multiplicative subset, and I, J fractional R-ideals.*

a) *We have $(I + J)_S = I_S + J_S$.*
b) *We have $(IJ)_S = I_S J_S$.*
c) *We have $(I \cap J)_S = I_S \cap J_S$.*
d) *If I is finitely generated, then $(I^*)_S = (I_S)^*$.*

PROOF. Parts a) and b) are immediate and are just recorded for future reference. For part c), we evidently have $(I \cap J)_S \subset I_S \cap J_S$. Conversely, let $x \in I_S \cap J_S$, so $x = \frac{i}{s_1} = \frac{j}{s_2}$ with $i \in I$, $j \in J$, $s_1, s_2 \in S$. Put $b = a_1 s_2 = a_2 s_1 \in I \cap J$; then $x = \frac{b}{s_1 s_2} \in (I \cap J)_S$, establishing part c). For part d), note first that $(I + J)^* = I^* \cap J^*$. Also if $0 \neq x \in K$, then $(Rx)_S = R_S x$. Hence if $I = Rx_1 + \ldots + Rx_n$, then

$I_S = R_S x_1 + \ldots + R_S x_n$, so $(I_S)^* = \bigcap_{i=1}^n \frac{1}{x_i} R_S$. On the other hand, $I^* = \bigcap_{i=1}^n \frac{1}{x_i} R$, and thus part c) we have

$$(I^*)_S = \bigcap_{i=1}^n \frac{1}{x_i} R_S = (I_S)^*. \qquad \square$$

LEMMA 19.22. *A nonzero ideal in a Noetherian domain contains a product of nonzero prime ideals.*

PROOF. Assume not: let I be a nonzero ideal which is maximal with respect to the property of not containing a product of nonzero prime ideals. Then I is not prime: there are $x_1,\ x_2 \in R \backslash I$ such that $x_1 x_2 \in I$. For $i = 1, 2$ put $I_i := \langle I, x_i \rangle$, so that $I \subsetneq I_i$ and $I \supset I_1 I_2$. By maximality of I, $I_1 \supset \mathfrak{p}_1 \cdots \mathfrak{p}_\mathfrak{r}$ and $I_2 \supset \mathfrak{q}_1 \cdots \mathfrak{q}_s$ (with $\mathfrak{p}_i$, $\mathfrak{q}_j$ prime for all i, j), and then $I \supset \mathfrak{p}_1 \cdots \mathfrak{p}_\mathfrak{r} \mathfrak{q}_1 \supset \mathfrak{q}_s$, contradiction. $\square$

LEMMA 19.23. *(Jacobson) Let R be a Noetherian domain of Krull dimension at most one. Let I be a proper, nonzero ideal of R. Then $(R : I) \supsetneq R$.*

PROOF. Let $0 \neq a \in I$, so $aR \subset I \subset R$. By Lemma 19.22, there are nonzero prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ such that $aR \supset \mathfrak{p}_1 \cdots \mathfrak{p}_m$; we may assume m is minimal. Let $\mathfrak{m}$ be a maximal ideal containing I. Then $\mathfrak{m} \supset I \supset aR \supset \mathfrak{p}_1 \cdots \mathfrak{p}_m$; since nonzero prime ideals are maximal, this implies $\mathfrak{m} = \mathfrak{p}_i$ for some i, say for $i = 1$. If $m = 1$ then $I = aR$ so $(R : I) = a^{-1}R \supsetneq R$. Now suppose $m > 1$; by minimality of m, aR does *not* contain $\mathfrak{p}_2 \cdots \mathfrak{p}_m$ so we may choose $b \in \mathfrak{p}_2 \cdots \mathfrak{p}_m \backslash aR$. Put $c = a^{-1}b$. Then $c \notin R$ and $cI \subset c\mathfrak{m} = a^{-1}b\mathfrak{m} \subset a\mathfrak{m}\mathfrak{p}_2 \cdots \mathfrak{p}_m \subset a^{-1}(aR) = R$, so $c \in (R : I)$. $\square$

The following result gives information about when a prime ideal is invertible.

PROPOSITION 19.24. *Let R be a Noetherian domain, and $\mathfrak{p}$ a nonzero prime ideal of R. If $\mathfrak{p}$ is invertible, then it has height one and $R_\mathfrak{p}$ is a DVR.*

PROOF. Since $\mathfrak{p}$ is invertible, $R_\mathfrak{p}$ is a Noetherian local domain with a principal maximal ideal $\mathfrak{p}R_\mathfrak{p}$. By Theorem 17.8, $R_\mathfrak{p}$ is a DVR, and thus $\mathfrak{p}$ has height one. $\square$

4. Divisorial ideals and the Divisor Class Group

For $I, J \in \mathrm{Frac}(R)$, we write $I \leqslant J$ if every principal fractional ideal that contains I also contains J. The ideal $\overline{I}$ is the intersection of the principal fractional ideals containing I and it is the largest fractional ideal that is contained in the same principal fractional ideals as I, so we have $I \leqslant J \iff \overline{J} \subseteq \overline{I}$, which by Corollary 19.6b) holds if and only if $I^* \subseteq J^*$. Thus upon restriction to divisorial fractional ideals, our ordering $\leqslant$ becomes *the reverse* of the usual ordering of fractional ideals by inclusion. This is designed for the following purpose: we will soon see that under a certain condition on R (namely, complete integral closure) we will define the structure of an ordered commutative group on the set of divisorial fractional ideals of R. R itself will be the identity element, and then *with the order reversal* the positive cone in this group will be the set of divisorial integral ideals. This is also a generalization of the fact that for $a, b \in R^\bullet$ we have $a \mid b$ if and only if $(a) \supseteq (b)$, so we are in some sense taking the "divibility ordering" rather than the "ideal containment ordering."

We write $I \sim J$ if $I \leqslant J$ and $J \leqslant I$; this holds if and only if $\overline{I} = \overline{J}$ if and only

if $I^* = J^*$. The relation $\sim$ is an equivalence relation on the set of fractional ideals of R. We put

$$D(R) := \mathrm{Frac}(R)/\sim$$

be the set of equivalence classes. Elements of $D(R)$ are called **divisors** on R. For $I \in \mathrm{Frac}(R)$ we denote its image in $D(R)$ by $\mathrm{div}(I)$. The class $\mathrm{div}(I)$ has a canonical representative, namely $\overline{I}$: for every $J \in \mathrm{div}(I)$ we have $J \subseteq \overline{I}$. We call a fractional ideal **divisorial** if $I = \overline{I}$.

Let $a \in K^\times$. We saw above that $(aR)^* = (\frac{1}{a}R)^*$, hence $\overline{aR} = (\frac{1}{a}R)^* = aR$. Thus invertible fractional ideals are divisorial. A divisor $\mathrm{div}(I)$ is **principal** if it contains a principal fractional ideal, in which case its canonical representative $\overline{I}$ is a principal fractional ideal.

PROPOSITION 19.25. *Every invertible fractional ideal is divisorial.*

PROOF. Let I be an invertible fractional ideal. By Lemma 19.9 we have $I^* = I^{-1}$, which is also invertible, so

$$\overline{I} = (I^*)^* = (I^{-1})^* = (I^{-1})^{-1} = I. \qquad \square$$

PROPOSITION 19.26. *Let $I \in \mathrm{Frac}\, R$. Then I is divisorial if and only if it is the intersection of a nonempty family of principal fractional ideals.*

PROOF. If I is divisorial, then $I = \overline{I}$ and by Proposition 19.8, $\overline{I}$ is the intersection of the principal fractional ideals in which it is contained. Moreover, by definition, a fractional ideal is contained in $a^{-1}R$ for some $a \in R^\bullet$.

Conversely, let $\{I_i\}_{i\in I}$ be a nonempty family of principal fractional ideals such that $\bigcap_{i\in S} I_i$ is a fractional ideal (i.e., is nonzero). Then each I_i is divisorial, so Proposition 19.7b) tells us that $\bigcap_{i\in I}$ is divisorial. $\square$

EXAMPLE 19.27. *Let k be a field, and let R be the subring $k[x^2, x^3]$ of $k[X]$: otherwise put, it is the ring of polynomials in which the monomial t does not appear. (This however makes one wonder a little why it is a ring, possibly even after calulating that it is closed under multiplication. In fact it is the monoid ring $k[M]$, where M is the submonoid $\{0\} \cup \mathbb{Z}^{\geq 2}$ of $\mathbb{N}$.) The ring R is not integrally closed: indeed $x = \frac{x^3}{x^2}$ lies in the fraction field of R and satisfies the monic polynomial $t^2 - x^2 \in R[t]$, but x does not lie in R.*

We claim that the maximal ideal $\mathfrak{m} := \langle \mathfrak{m}, \mathfrak{m}^2\rangle$ of R is divisorial but not invertible. Indeed we have

$$\mathfrak{m} = R \cap \frac{1}{x}R$$

is an intersection of principal fractional ideals hence divisorial. The elements t^2 and t^3 are nonassociate irreducibles, so if $\mathfrak{m} = \langle a\rangle$, then $a \mid t^2$ and $a \mid t^3$, which implies $a \in R^\times$, contradicting the properness of $\mathfrak{m}$.

The ring R is isomorphic to $k[x,y]/(x^3 - y^2)$, and under that isomorphism the maximal ideal $\mathfrak{m}$ corresponds to $\mathfrak{m} = \langle x, y\rangle$. Similarly to the dscussion following Theorem 15.48, we see that $\dim_{R/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = \dim_k \mathfrak{m}/\mathfrak{m}^2 = 2$, which means that even the pushforward $\mathfrak{m}_\mathfrak{m}$ of $\mathfrak{m}$ to the local ring $R_\mathfrak{m}$ is not prinicpal. Therefore $\mathfrak{m}$ is a divisorial ideal that is not invertible.

EXERCISE 19.12. *Let $I \in \mathrm{Frac}\, R$ and $x \in K^\bullet$. Show: I is divisorial if and only if xI is divisorial.*

PROPOSITION 19.28. *For $I, J, M \in \operatorname{Frac} R$, we have:*

$$\operatorname{div} I \leqslant \operatorname{div} J \implies \operatorname{div} IM \leqslant \operatorname{div} JM.$$

PROOF. By hypothesis $\overline{J} \subset \overline{I}$; equivalently $(R : I) = I^* \subset J^* = (R : J)$. Then $(IM)^* = (R : IM) = ((R : I) : M) \subset ((R : J) : M) = (R : JM) = (JM)^*$. It follows that $\overline{JM} \subset \overline{IM}$, so $\operatorname{div} IM \leqslant \operatorname{div} JM$. □

PROPOSITION 19.29. *Let R be a domain.*

a) *For $\operatorname{div} I, \operatorname{div} J \in D(R)$, the operation*

$$\operatorname{div} I + \operatorname{div} J := \operatorname{div} IJ$$

is well-defined and endows $D(R)$ with the structure of a commutative monoid.

b) *The monoid $(D(R), +, \leqslant)$ is lattice-ordered.*

PROOF. We have

$$(R : IJ) = ((R : I) : J) = (R : \overline{I}) : J) = ((R : J) : \overline{I})$$
$$= ((R : \overline{J}) : \overline{I}) = (R : \overline{I} \cdot \overline{J}),$$

so $(IJ)^* = (\overline{I} \cdot \overline{J})^*$, which implies

$$\overline{IJ} = \overline{\overline{I} \cdot \overline{J}},$$

showing that $\operatorname{div}(IJ)$ depends only on $\operatorname{div}(I)$ and $\operatorname{div}(J)$.
b) For $I, J, M \in \operatorname{Frac} R$ with $\operatorname{div} I \leqslant \operatorname{div} J$, by Proposition 19.28 and part a),

$$\operatorname{div} I + \operatorname{div} M = \operatorname{div} IM \leqslant \operatorname{div} JM = \operatorname{div} J + \operatorname{div} M,$$

and thus the partial ordering is compatible with the monoid structure. To show that we have a lattice, for any $I, J \in \operatorname{Frac} R$, we need to find the supremum and infimum of $\operatorname{div} I$ and $\operatorname{div} J$. We claim that in fact we have

$$\operatorname{div}(I \cap J) = \sup \operatorname{div} I, \operatorname{div} J$$
$$\operatorname{div}(I + J) = \inf \operatorname{div} I, \operatorname{div} J.$$

To see this we may assume I and J are divisorial. By Exercise 19.12, $I \cap J$ is divisorial, so it is clear that for any divisorial ideal M,

$$(\operatorname{div} I \leqslant M,\ \operatorname{div} J \leqslant M) \iff (M \subset I,\ M \subset J)$$
$$\iff (M \subset I \cap J) \iff \operatorname{div} I \cap J \leqslant \operatorname{div} M.$$

Next, observe that since $I, J \subset I + J$, $\operatorname{div} I + J \leqslant \operatorname{div} I, \operatorname{div} J$, i.e., $\operatorname{div} I + J$ is a lower bound for $\{\operatorname{div} I, \operatorname{div} J\}$. Conversely, if $M \in \operatorname{Frac} R$ is such that $\operatorname{div} M \leqslant \operatorname{div} I,\ \operatorname{div} J$, then $I, J \subset \overline{M}$ so $I + J \subset \overline{M}$ and $\overline{I + J} \subset \overline{\overline{M}} = \overline{M}$ and $\operatorname{div} M = \operatorname{div} \overline{M} \leqslant \operatorname{div} \overline{I + J} = \operatorname{div} I + J$. □

Notice that in Proposition 19.29 we *did not* prove that $\overline{IJ} = \overline{I} \cdot \overline{J}$. This is not true in general: that is, unlike principal fraction ideals and invertible fractional ideals, the product of two divisorial ideals need not be divisor. We will see why shortly.

THEOREM 19.30. *For a domain R, the following are equivalent:*

(i) *$D(R)$ is a group.*

(ii) *R is completely integrally closed.*

PROOF. (i) $\implies$ (ii): Let $x \in K^\times$. Suppose there is $d \in R^\bullet$ such that $dx^n \in R$ for all $n \in \mathbb{Z}^+$. Then $I = \langle R, a \rangle_R \in \operatorname{Frac} R$ and $aI \subset I$. Then

$$\operatorname{div} I \leqslant \operatorname{div} aI = \operatorname{div} a + \operatorname{div} I.$$

Since $D(R)$ is a group, $\operatorname{div} R = 0 \leqslant \operatorname{div} a$, and since aR and R are divisorial, $a \in R$.
(ii) $\implies$ (i): We'll show: for all divisorial fractional ideals I, $(II^*)^* = R^* = R$, hence $\operatorname{div} I + \operatorname{div} I^* = \operatorname{div} R = 0$. By Proposition 19.8, it's enough to show that II^* and R are contained in the same principal fractional ideals. Since $II^* \subset R$, any principal fractional ideal which contains R contains II^*. Thus, let $x \in K^\times$ be such that $II^* \subset xR$; we want to show $R \subset xR$, i.e., $x^{-1} \in R$. Suppose that for $y \in K^\times$ we have $I \subset yR$, so $y^{-1} \in I^*$ and thus $Iy^{-1} \subset xR$; equivalently, $x^{-1}I \subset yR$. Thus $x^{-1}I$ is contained in every principal fractional ideal containing I, so $x^{-1}I \subset \overline{I} = I$. It follows that $x^{-n}I \subset I$ for all $n \in \mathbb{Z}^+$. Let $w \in R^\bullet$ be such that $wI \subset R$. Then $dx^{-n}I \subset R$, and if $z \in I^\bullet$ then $(wz)x^{-n} \in R$ for all $n \in \mathbb{Z}^+$. Since $dc \in R^\bullet$ and R is completely integrally closed, by Theorem 14.43 $x^{-1} \in R$. □

If $I \in \operatorname{Frac} R$ is divisorial, then in the proof of Theorem 19.30 we showed that $(II^*)^* = R$. It follows that $\overline{II^*} = R$. Thus if I is not invertible then the product of the two divisorial ideals I and I^* is not divisorial...and this is more good than bad, since it allows $D(R)$ to be a group for e.g. any Noetherian integrally closed domain.

If R is completely integrally closed (e.g. Noetherian and integrally closed), the divisors form a group $D(R)$. The principal divisors $P(R)$ always form a group, so we may form the quotient

$$\operatorname{Cl} R := D(R)/P(R),$$

the **divisor class group** of R. Because invertible fractional ideals are divisorial and form a group (with no conditions on the domain R), we get an injection

$$\operatorname{Pic} R \hookrightarrow \operatorname{Cl} R.$$

This gives us two competing class groups. The Picard group $\operatorname{Pic} R$ is also often called the **Cartier divisor class group** or the **locally principal divisor class group**. The divisor class group $\operatorname{Cl} R$ is often called the **Weil divisor class group**. Unfortunately the way we have defined it does not make the relationship to Weil divisors as seen in algebraic geometry very clear. We will come back to this when we discuss Krull domains.

THEOREM 19.31. *Let $R = \mathbb{C}[x, y, z]/(xy - z^2)$. Then R is a Noetherian integrally closed domain with $\operatorname{Pic} R = 0$ and $\operatorname{Cl} R \cong \mathbb{Z}/2\mathbb{Z}$.*

CHAPTER 20

Dedekind Domains and Prüfer Domains

A **Dedekind domain** is a domain that is Noetherian, integrally closed, and of dimension at most one. A Dedekind domain has dimension zero if and only if it is a field. The case of fields will be ignored whenever possible (although we try to state our results so as to be correct in this trivial case).

EXERCISE 20.1. *Show: a PID is a Dedekind domain.*

Let R be a Dedekind domain with fraction field K, let L/K be a finite degree field extension, and let S be the integral closure of R in L. It follows from the Krull-Akizuki Theorem that S is also a Dedekind domain. Two special cases of this are of the highest level of importance:

• The ring $\mathbb{Z}$ is a PID, with fraction field $\mathbb{Q}$. Let K be a number field — i.e., a finite degree field extension of $\mathbb{Q}$. Let $\mathbb{Z}_K$ be the integral closure of $\mathbb{Z}$ in K. Then $\mathbb{Z}_K$ is a Dedekind domain. Algebraic number theory begins by applying the general theory of Dedekind domains that we will develop here to this class of examples and goes on to explore properties that are particular to this class of Dedekind domains, e.g. the finiteness of the class group.

• Let k be a field. The ring $k[t]$ is a PID, with fraction field k. Let $L/k(t)$ be a finite degree field extension, and let S be the integral closure of $k[t]$ in L. Then S is a Dedekind domain. There is a geometric interpretation here: $k(t)$ if the field of rational functions on the projective line $\mathcal{P}^1_{/k}$, the field L is the field of rational functions of a (unique, up to isomorphism) projective, regular, connected algebraic curve $C_{/k}$, and the field extension $L/k(t)$ corresponds to a finite morphism of curves $\pi : C \to \mathcal{P}^1_{/k}$. The preimage of the affine line $\mathbb{A}^1_{/k}$ under π is an affine, regular, connected algebraic curve C°/k, and the ring S is $k[C^\circ]$, the ring of rational functions on C that are regular on C°. There is a close connection between the class group of the Dedekind domain S and the Picard group of the complete curve C. Exploiting this connection is one way to see that when k is finite, the class group of S is finite.

We will give several characterizations of Dedekind domains: the first one is that a domain R is Dedekind if and only if each nonzero fractional R-ideal is invertible (equivalently, if each nonzero R-ideal is invertible). A **Prüfer domain** is a domain in which each nonzero finitely generated ideal is invertible. It follows that a Dedekind domain is precisely a Noetherian Prüfer domain. Thus conversely we may think of Prüfer domains as a class of domains that are like Dedekind domains except that they need not be Noetherian, in close analogy to the way that Beźout domains are like PIDs except that they need not be Noetherian. Indeed:

EXERCISE 20.2. *Show: a Bézout domain is a Prüfer domain.*

1. Invertibility of Ideals

THEOREM 20.1. *For a domain R, the following are equivalent:*

(i) *R is Dedekind: Noetherian, integrally closed of dimension at most one.*
(ii) *Every fractional R-ideal is invertible.*
(iii) *Every nonzero prime ideal of R is invertible.*

PROOF. (i) $\implies$ (ii): Let R be a Noetherian, integrally closed domain of dimension at most one, and let I be a fractional R-ideal. Then $II^* \subset R$ and hence also $II^*(II^*)^* \subset R$, so $I^*(II)^* \subset I^*$. It follows from Lemma 19.20 that $(II^*)^* \subset R$; moreover, since $II^* \subset R$, Lemma 19.23 implies $II^* = R$, i.e., I is invertible.
(ii) $\implies$ (i): Since invertible ideals are finitely generated, if every nonzero ideal is invertible, then R is Noetherian. Let $\mathfrak{p}$ be a nonzero, nonmaximal prime ideal of R, so that there exists a maximal ideal $\mathfrak{m}$ which $0 \subsetneq \mathfrak{p} \subsetneq \mathfrak{m}$. By the mantra "to contain is to divide" for invertible fractional ideals, there exists some invertible integral ideal I such that $\mathfrak{p} = \mathfrak{m}I$. Suppose that $I \subset \mathfrak{p}$. Then $I = RI \supset \mathfrak{m}I = \mathfrak{p}$, so we would have $\mathfrak{p} = I$ and then $\mathfrak{m} = R$, contradiction. Then there are $x \in \mathfrak{m}\backslash\mathfrak{p}$ and $y \in I\backslash\mathfrak{p}$ such that $xy \in \mathfrak{p}$, contradicting the primality of $\mathfrak{p}$.

Finally, we check that R is integrally closed: let $x = \frac{b}{c}$ be a nonzero element of K which is integral over R, so there exist $a_0, \ldots, a_{n-1} \in R$ such that

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0.$$

Let M be the R-submodule of K generated by $1, x, \ldots, x^{n-1}$; since M is finitely generated, it is a fractional R-ideal. We have $M^2 = M$, and thus – since M is invertible – $M = R$. It follows that $x \in R$.
(ii) $\implies$ (iii) is immediate.
(iii) $\implies$ (ii) by Theorem 19.14. □

Recall that a ring R is **hereditary** if every ideal of R is a projective R-module.

COROLLARY 20.2. *A domain R is hereditary if and only if it is a Dedekind domain.*

PROOF. By Theorem 20.1 a domain R is a Dedekind domain if and only if every fractional ideal of R is invertible, and clearly the latter condition holds if and only if every nonzero integral ideal of R is invertible. Moreover, by Theorem 19.12, a nonzero ideal of a ring is invertible if and only if it is projective as an R-module. □

2. Ideal Factorization in Dedekind Domains

Here we will show that in a Dedekind domain every nonzero integral ideal factors uniquely into a product of primes and derive consequences for the group of invertible ideals and the Picard group. (The fact that factorization – unique or otherwise! – into products of primes implies invertibility of all fractional ideals – is more delicate and will be pursued later.)

LEMMA 20.3. *Let I be an ideal in a ring R. If there exist J_1, J_2 ideals of R, each strictly containing I, such that $I = J_1J_2$, then I is not prime.*

PROOF. Choose, for $i = 1, 2$, $x_i \in J_i\backslash I$; then $x_1x_2 \in I$, so I is not prime. □

THEOREM 20.4. *Every proper integral ideal in a Dedekind domain has a unique factorization into a product of of prime ideals.*

PROOF. After Lemma 19.19 it suffices to show that a nonzero proper integral ideal I in a Dedekind domain R factors into a product of primes. Suppose not, so the set of ideals which do not so factor is nonempty, and (as usual!) let I be a maximal element of this set. Then I is not prime, so in particular is not maximal: let $\mathfrak{p}$ be a maximal ideal strictly containing I, so $I = \mathfrak{p}J$. Then $J = \mathfrak{p}^{-1}I$ strictly contains I so factors into a product of primes, hence I does. □

If I is any nonzero integral ideal of I and $\mathfrak{p}$ is any nonzero prime ideal of a Dedekind domain R, then we may define $\mathrm{ord}_{\mathfrak{p}}(I)$ via the prime factorization

$$I = \prod_{\mathfrak{p}} \mathfrak{p}^{\mathrm{ord}_{\mathfrak{p}}(I)}.$$

The product extends formally over all primes, but as I is divisible by only finitely many primes, all but finitely many exponents are zero, so it is really a finite product.

COROLLARY 20.5. *Let R be a Dedekind domain.*

a) *The monoid $\mathcal{M}(R)$ of nonzero integral ideals is a free commutative monoid on the maximal ideals.*
b) *The fractional ideals form a free commutative group on the maximal ideals:*

$$\mathrm{Frac}(R) = \bigoplus_{0 \neq \mathfrak{p} \in \mathrm{Spec}\, R} \mathbb{Z}.$$

PROOF. Part a) is simply the statement of unique factorization into prime elements in any commutative monoid. In the group $\mathcal{I}(R)$ of all fractional ideals, the subgroup G generated by the nonzero primes is a free commutative group on the primes: this just asserts that for primes $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ and integers $n_1, \ldots, n_r$, the equation $\mathfrak{p}_1^{n_1} \cdots \mathfrak{p}_r^{n_r} = R$ implies $n_1 = \ldots = n_r = 0$, which is easily seen – e.g. by localizing. Since any fractional ideal J is of the form $\frac{1}{x}I$ with I an integral ideal, decomposing I and (x) into their prime factorizations expresses J as a $\mathbb{Z}$-linear combination of prime ideals, so $\mathrm{Frac}(R) = G$. □

Corollary 20.5 allows us to extend the definition of $\mathrm{ord}_{\mathfrak{p}}$ to any fractional R-ideal.

Since for a Dedekind domain there is no distinction between invertible fractional ideals and all fractional ideals, the Picard group takes an especially simple form: it is the quotient of the free commutative group $\mathrm{Frac}(R)$ of all fractional ideals modulo the subgroup $\mathrm{Prin}(R) = K^\times/R^\times$ of principal fractional ideals. We therefore have a short exact sequence

$$0 \to \mathrm{Prin}(R) \to \mathrm{Frac}(R) \to \mathrm{Pic}(R) \to 0,$$

and also a slightly longer exact sequence

$$0 \to R^\times \to K^\times \to \mathrm{Frac}(R) \to \mathrm{Pic}(R) \to 0.$$

THEOREM 20.6. *For a Dedekind domain R, the following are equivalent:*

(i) *We have* $\mathrm{Pic}(R) = 0$.
(ii) *The ring R is a PID.*
(iii) *The ring R is a UFD.*
(iv) *The ring R has only finitely many nonprincipal prime ideals.*

PROOF. Evidently each fractional ideal is principal if and only if each integral ideal is principal: $(i) \equiv (ii)$. Since R has dimension at most one, (ii) $\iff$ (iii) by Proposition 16.1. Evidently (ii) $\implies$ (iv), so the interesting implication is that (iv) implies the other conditions. So assume that the set of (nonzero) nonprincipal prime ideals is nonempty but finite, and enumerate them: $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. Let I be an integral ideal, and suppose that

$$I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n} \mathfrak{q}_1^{b_1} \cdots \mathfrak{q}_m^{b_m}.$$

(As usual, we allow zero exponents.) By the Chinese Remainder Theorem we may choose an $\alpha \in R$ such that $\operatorname{ord}_{\mathfrak{p}_i}(\alpha) = a_i$ for all i.[1] Now consider the fractional ideal $(\alpha^{-1})I$; it factors as

$$(\alpha^{-1})I = \mathfrak{q}_1^{b_1} \cdots \mathfrak{q}_m^{b_m} \mathfrak{r}_1^{c_1} \cdots \mathfrak{r}_l^{c_l},$$

where the $\mathfrak{r}_i$'s are some other prime ideals, i.e., disjoint from the $\mathfrak{p}_i$'s. But all of the (fractional) ideals in the factorization of $(\alpha^{-1})I$ are principal, so $(\alpha^{-1})I = (\beta)$ for some $\beta \in K^\times$ and then $I = (\alpha\beta)$ is principal! □

EXERCISE 20.3.

a) *Consider the ring*

$$R_1 = \mathbb{Z}[\sqrt{-3}] = \mathbb{Z}[t]/(t^2 + 3).$$

Show: R_1 is a one-dimensional Noetherian domain with exactly one nonprincipal prime ideal, namely $\mathfrak{p}_2 = \langle 1 + \sqrt{-3}, 1 - \sqrt{-3} \rangle$.

b) *For any $n \in \mathbb{Z}^+$, exhibit a ring R_n which is one-dimensional Noetherian and has exactly n nonprincipal prime ideals.*

3. Local Characterization of Dedekind domains

THEOREM 20.7. *Let R be a domain.*

a) *If R is Dedekind and S is a multiplicative subset, then $S^{-1}R$ is Dedekind.*
b) *If R is a Dedekind domain and $0 \neq \mathfrak{p}$ is a prime ideal of R, then $R_{\mathfrak{p}}$ is a DVR.*

PROOF. Being Noetherian, dimension at most one and integrally closed are all preserved under localization, so part a) is immediate. Similarly, if $0 \neq \mathfrak{p}$ is a prime ideal, then the localization $R_{\mathfrak{p}}$ is a local, one-dimensional integrally closed Noetherian domain, hence by Theorem 17.8 a DVR, establishing b). □

EXERCISE 20.4. *Let R be Dedekind with fraction field K; let $0 \neq \mathfrak{p} \in \operatorname{Spec} R$.*

a) *Show: the map $\operatorname{ord}_{\mathfrak{p}} : K^\times \to \mathbb{Z}$ defined above is nothing else than the discrete valuation corresponding to the localization $R_{\mathfrak{p}}$.*
b) *Conversely, let $v : K^\times \to \mathbb{Z}$ be a discrete valuation. Show that the valuation ring $R_v = v^{-1}(\mathbb{N})$ is the localization of R at some maximal ideal $\mathfrak{p}$.*

[1] Note that we want equality, not just $\operatorname{ord}_{P_i}(\alpha) \geqslant a_i$, so you should definitely think about how to get this from CRT if you've never seen such an argument before.

4. Factorization Into Primes Implies Dedekind

THEOREM 20.8. *(Matusita* [**Ma44**]*) Let R be a domain with the property that every nonzero proper integral ideal is a product of prime ideals. Then R is Dedekind.*

PROOF. Step 1: Let $\mathfrak{p}$ be an invertible prime of R. We show that $\mathfrak{p}$ is maximal. Let $a \in R \backslash \mathfrak{p}$, and suppose that $\langle a, \mathfrak{p} \rangle \subsetneq R$. Let us then write

$$I_1 := \langle a, \mathfrak{p} \rangle = \mathfrak{p}_1 \cdots \mathfrak{p}_m,$$

$$I_2 := \langle a^2, \mathfrak{p} \rangle = \mathfrak{q}_1 \cdots \mathfrak{q}_n,$$

where the $\mathfrak{p}_i$ and $\mathfrak{q}_j$ are prime ideals. By assumption, $I_1 \supsetneq \mathfrak{p}$, and, since $\mathfrak{p}$ is prime, we have also $I_2 \supsetneq \mathfrak{p}$. Therefore each $\mathfrak{p}_i$ and $\mathfrak{q}_j$ strictly contains $\mathfrak{p}$. In the quotient $\overline{R} = R/\mathfrak{p}$ we have

$$(\overline{a}) = a\overline{R} = \overline{\mathfrak{p}}_1 \cdots \overline{\mathfrak{p}}_m$$

and

$$(\overline{a^2}) = a^2\overline{R} = \overline{\mathfrak{q}}_1 \cdots \overline{\mathfrak{q}}_n.$$

The principal ideals $(\overline{a})$ and $(\overline{a^2})$ are invertible, and the $\overline{\mathfrak{p}}_i$ and $\overline{\mathfrak{q}}_j$ remain prime in the quotient. Therefore, we have

$$\overline{\mathfrak{q}}_1 \cdots \overline{\mathfrak{q}}_n = \overline{\mathfrak{p}}_1^2 \cdots \overline{\mathfrak{p}_m}^2.$$

Thus the multisets $\{\{\overline{\mathfrak{q}}_1, \ldots, \overline{\mathfrak{q}}_n\}$ and $\{\overline{\mathfrak{p}}_1,\ \overline{\mathfrak{p}}_1, \ldots, \overline{\mathfrak{p}}_m, \overline{\mathfrak{p}}_m\}\}$ coincide, and pulling back to R the same holds without the bars. Thus

$$I_1^2 = \langle a, \mathfrak{p} \rangle^2 = \mathfrak{p}_1^2 \cdots \mathfrak{p}_m^2 = \mathfrak{q}_1 \cdots \mathfrak{q}_n = \langle a^2, \mathfrak{p} \rangle,$$

so

$$\mathfrak{p} \subset \langle a, \mathfrak{p} \rangle^2 = a^2R + a\mathfrak{p} + \mathfrak{p}^2 \subset aR + \mathfrak{p}^2.$$

So if $p \in \mathfrak{p}$, $p = ax + y$ with $x \in R,\ y \in \mathfrak{p}^2$, so $ax \in \mathfrak{p}$, and since $a \in R \backslash \mathfrak{p}$, $x \in \mathfrak{p}$. Thus $\mathfrak{p} \subset a\mathfrak{p} + \mathfrak{p}^2 \subset \mathfrak{p}$, so $\mathfrak{p} = a\mathfrak{p} + \mathfrak{p}^2$. Multiplication by $\mathfrak{p}^{-1}$ gives $R = a + \mathfrak{p}$, contrary to hypothesis. So $\mathfrak{p}$ is maximal.

Step 2: Let $\mathfrak{p}$ be a nonzero prime ideal in R, and $0 \neq b \in \mathfrak{p}$. Then $\mathfrak{p} \supset bR$ and

$$bR = \mathfrak{p}_1 \cdots \mathfrak{p}_m,$$

with each $\mathfrak{p}_i$ invertible and prime. Thus by Step 1 the $\mathfrak{p}_i$'s are maximal. Since $\mathfrak{p}$ is prime we have $\mathfrak{p} \supset \mathfrak{p}_i$ for some i and then by maximality $\mathfrak{p} = \mathfrak{p}_i$, hence $\mathfrak{p}$ is invertible. Since by assumption every proper integral ideal is a product of primes, we conclude that every integral ideal is invertible, which, by Theorem 20.1 implies that R is Dedekind. □

Let $\mathfrak{a}$ and $\mathfrak{b}$ be ideals of a domain R. We say that $\mathfrak{b}$ **divides** $\mathfrak{a}$ if there is an ideal $\mathfrak{c}$ such that $\mathfrak{bc} = \mathfrak{a}$.

EXERCISE 20.5. *Suppose $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ are ideals of a domain R such that $\mathfrak{b}\ c = \mathfrak{a}$.*

a) *Show: $\mathfrak{b} \supset \mathfrak{a}$.*
b) *Show: $\mathfrak{c} \subset (\mathfrak{a} : \mathfrak{b})$.*
c) *Can we have $\mathfrak{c} \subsetneq (\mathfrak{a} : \mathfrak{b})$?*

PROPOSITION 20.9. *For a Noetherian domain R, the following are equivalent:*

(i) *R is a Dedekind domain.*
(ii) ***To contain is to divide**: For all ideals $\mathfrak{a}$, $\mathfrak{b}$ of R, $\mathfrak{b} \supset \mathfrak{a} \iff \mathfrak{b}$ divides $\mathfrak{a}$.*

PROOF. (i) $\implies$ (ii): The statement is trivial if $\mathfrak{b} = (0)$. Otherwise, $\mathfrak{b}$ is invertible so $\mathfrak{a} = \mathfrak{b}(\mathfrak{a} : \mathfrak{b})$ by Lemma 19.9.
(ii) $\implies$ (i): We claim that every proper nonzero ideal of R is a product of prime ideals. Since R is Noetherian, if this is not the case there is an ideal $\mathfrak{a}$ which is maximal with respect to not having this property. Let $\mathfrak{p}$ be a maximal ideal with $\mathfrak{a} \subset \mathfrak{p}$. By hypothesis, there is an ideal $\mathfrak{c}$ with $\mathfrak{a} = \mathfrak{p}_1\mathfrak{c}$. Then $\mathfrak{c} \supset \mathfrak{a}$. Suppose we had equality; then repeatedly substituting $\mathfrak{a} = \mathfrak{p}_1\mathfrak{a}$ gives $\mathfrak{a} = \mathfrak{p}_1^k\mathfrak{a}$ for all $k \in \mathbb{Z}^+$, and then by the Krull Intersection Theorem, $\mathfrak{a} \subset \bigcap_{k=1}^{\infty} \mathfrak{p}_1^k = (0)$, contradiction. So $\mathfrak{c}$ properly contains $\mathfrak{a}$, so we may write $\mathfrak{c} = \mathfrak{p}_2 \cdots \mathfrak{p}_r$ and thus $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r$: contradiction. □

THEOREM 20.10. *For a domain R which is not a field, the following are equivalent:*

(i) *R is Noetherian, integrally closed, and of Krull dimension one.*
(ii) *Every fractional (equivalently, every integral) R-ideal is invertible.*
(iii) *R is Noetherian, and the localization at every maximal ideal is a DVR.*
(iv) *Every nonzero proper integral ideal factors into a product of prime ideals.*
(iv′) *Every nonzero proper integral ideal factors* uniquely *into a product of primes.*
(v) *R is Noetherian, and to contain is to divide for all ideals of R.*

5. Generation of Ideals in Dedekind Domains

THEOREM 20.11. *Let R be a Dedekind domain and I a nonzero ideal of R. Then the quotient ring R/I is a principal Artinian ring.*

PROOF. Write $I = \prod_{i=1}^r \mathfrak{p}_i^{a_i}$. By the Chinese Remainder Theorem,

$$R/I \cong \prod_{i=1}^r R/\mathfrak{p}_i^{a_i}.$$

Each factor $R/\mathfrak{p}_i^{a_i}$ is also a quotient of the localized ring $R_{\mathfrak{p}}/\mathfrak{p}_i^{a_i}$, which shows that it is Artinian and principal. Finally, a finite product of Artinian (resp. principal ideal rings) remains Artinian (resp. a principal ideal ring). □

This has the following striking consequence:

THEOREM 20.12. *(Asano-Jensen) For a domain R, the following are equivalent:*

(i) *R is a Dedekind domain.*
(ii) *For every nonzero ideal I of R and every element $a \in I^\bullet$, there is $b \in I$ such that $I = \langle a, b \rangle$.*

PROOF. The direction (i) $\implies$ (ii) follows immediately from Theorem 20.11. Conversely, assume condition (ii) holds. By Theorem 20.10 it suffices to show that R is Noetherian and that its localization at each nonzero prime ideal $\mathfrak{p}$ is a DVR. Certainly condition (ii) implies Noetherianity; moreover it continues to hold for nonzero ideals in any localization. So let I be a nonzero ideal in the Noetherian local domain $(R_{\mathfrak{p}}, \mathfrak{p})$. It follows that there exists $b \in \mathfrak{p}$ such that $\mathfrak{p} = I\mathfrak{p} + bR_{\mathfrak{p}}$. By Nakayama's Lemma, $I = bR_{\mathfrak{p}}$, so $R_{\mathfrak{p}}$ is a local PID, hence a DVR. □

PROPOSITION 20.13. *([**J2**, Ex. 10.2.11]) Let R be a Dedekind domain, I a fractional ideal of R and J a nonzero integral ideal of R. Then there is $a \in I$ such that $aI^{-1} + J = R$.*

PROOF. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ be the prime ideals of R dividing J. For each $1 \leqslant i \leqslant r$, choose $a_i \in I\mathfrak{p}_1 \cdots \mathfrak{p}_r\mathfrak{p}_i^{-1} \backslash I\mathfrak{p}_1 \cdots \mathfrak{p}_r$. Put $a = a_1 + \ldots + a_r$. We claim that $aI^{-1} + J = R$. It is enough to check this locally. For every prime $\mathfrak{q} \neq \mathfrak{p}_i$, we have $JR_{\mathfrak{q}} = R_{\mathfrak{q}}$. On the other hand, for all $1 \leqslant i \leqslant r$, aI^{-1} is not contained in $\mathfrak{p}_i$, so its pushforward to $R_{\mathfrak{p}_i}$ is all of $R_{\mathfrak{p}_i}$. □

6. Finitely Generated Modules Over a Dedekind Domain

The main aim of this section is to prove the following important result.

THEOREM 20.14. *Let M be a finitely generated module over a Dedekind domain.*

a) *$P := M/M[\text{tors}]$ is finitely generated projective, say of rank r.*
b) *If $r = 0$, then $M = M[\text{tors}]$. If $r \geqslant 1$ then*

$$M \cong M[\text{tors}] \oplus P \cong M[\text{tors}] \oplus R^{r-1} \oplus I,$$

with I a nonzero ideal of R.
c) *The class $[I]$ of I in $\operatorname{Pic} R$ is an invariant of M.*
d) *There is $N \in \mathbb{Z}^+$, maximal ideals $\mathfrak{p}_i$ and positive integers n_i such that*

$$M[\text{tors}] \cong \bigoplus_{i=1}^{N} R/\mathfrak{p}_i^{n_i}.$$

Much of the content of the main theorem of this section lies in the following converse of Proposition 3.8b) for finitely generated modules over a Dedekind domain.

THEOREM 20.15. *For a finitely generated module M over a Dedekind domain, the following are equivalent:*

(i) *M is projective.*
(ii) *M is flat.*
(iii) *M is torsionfree.*

PROOF. Of course (i) $\implies$ (ii) $\implies$ (iii) for modules over any domain, and we have seen that (i) $\equiv$ (ii) for finitely generated modules over a Noetherian ring. So it suffices to show (iii) $\implies$ (i).

Suppose R is a Dedekind domain and M is a finitely generated nonzero torsionfree R-module. By Proposition 3.8c), we may assume that $M \subset R^n$ for some $n \geqslant 1$. We prove the result by induction on n. If $n = 1$, then M is nothing else than a nonzero ideal of R, hence invertible by Theorem 20.10 and thus a rank one projective module by Theorem 19.12. So we may assume that $n > 1$ and that every finitely generated torsionfree submodule of R^{n-1} is projective. Let $R^{n-1} \subset R^n$ be the span of the first $n-1$ standard basis elements. Let $\pi_n : R^n \to R$ be projection onto the nth factor, and consider the restriction of π_n to M:

$$0 \to M \cap R^{n-1} \to M \xrightarrow{\pi_n} \pi_n(M) \to 0.$$

Put $I = \pi_n(M)$. Then I is an ideal of R, hence projective, so the sequence splits:

$$M \to (M \cap R^{n-1}) \oplus I.$$

Now $M \cap R^{n-1}$ is a torsionfree, finitely generated (since M is finitely generated and R is Noetherian) submodule of R^{n-1}, hence is projective by induction. Certainly a direct sum of projective modules is projective, so we're done. $\square$

For any module M over a domain R, we have that $M/M[\text{tors}]$ is torsionfree, so if M is a finitely generated module over a Dedekind domain, then Theorem 20.15 implies that $P := M/M[\text{tors}]$ is projective, which is Theorem 20.14a). Because P is projective, we get

$$M \cong M[\text{tors}] \oplus P,$$

which is the first part of Theorem 20.14b).

Moreover, the method of proof of Theorem 20.15 yields the following important corollary:

COROLLARY 20.16. *Let P be a finitely generated rank r projective module over a Dedekind domain R. Then we have a direct sum decomposition $P \cong \bigoplus_{i=1}^{r} I_i$, where each I_i is a nonzero rank one projective R-module.*

LEMMA 20.17. *$I_1, \ldots, I_n$ be fractional ideals in the Dedekind domain R. Then the R-modules $\bigoplus_{i=1}^{n} I_i$ and $R^{n-1} \oplus I_1 \cdots I_n$ are isomorphic.*

PROOF. We will prove the result when $n = 2$. The general case follows by an easy induction argument left to the reader.
Choose $0 \neq a_1 \in I_1$. Applying Proposition 20.13 with $I = I_2$ and $J = a_1 I_1^{-1} \subset R$, that there exists $a_2 \in I_2$ such that $a_1 I_1^{-1} + a_2 I_2^{-1} = R$. That is there exist $b_i \in I_i^{-1}$ such that $a_1 b_1 + a_2 b_2 = 1$. The matrix

$$\begin{bmatrix} b_1 & -a_2 \\ b_2 & a_1 \end{bmatrix}$$

is invertible with inverse

$$A^{-1} = \begin{bmatrix} a_1 & a_2 \\ -b_2 & b_1 \end{bmatrix}.$$

For $(x_1, x_2) \in I_1 \oplus I_2$, we have

$$y_1 = x_1 b_1 + x_2 \in R,\ y_2 = -x_1 a_2 + x_2 a_1 \in I_1 I_2.$$

On the other hand, if $y_1 \in R$ and $y_2 = c_1 c_2 \in I_1 I_2$, then

$$x_1 = a_1 y_1 - b_2 c_1 c_2 \in I_1,\ x_2 = a_2 y_1 + b_1 c_1 c_2 \in I_2.$$

Thus $[x_1 x_2] \mapsto [x_1 x_2]A$ gives an R-module isomorphism from $I_1 \oplus I_2$ to $R \oplus I_1 I_2$. $\square$

Thus for our finitely generated module M over a Dedekind domain R with $P := M/M[\text{tors}]$ projective of rank r, Corollary 20.16 and Lemma 20.17 give

$$M = M[\text{tors}] \oplus P \cong M[\text{tors}] \oplus \bigoplus_{i=1}^{r} I_i = M[\text{tors}] \oplus R^{r-1} \oplus (I_1 \cdots I_r),$$

completing the proof of Theorem 20.14b).

To prove Theorem 20.14c), we need to show that if I and J are fractional ideals of the Dedekind domain R and there is $n \in \mathbb{N}$ such that $R^n \oplus I \cong_R R^n \oplus J$, then $[I] = [J]$ in $\operatorname{Pic} R$. To see this we apply Lemma 20.17:

$$R^{n+1} \oplus R = R^{n+2} \cong (R^n \oplus I) \oplus I^{-1} \cong (R^n \oplus J) \oplus I^{-1} \cong R^{n+1} \oplus JI^{-1}.$$

Thus the rank 1 projective module JI^{-1} is stably free, so by Proposition 7.18 JI^{-1} is a free R-module, i.e., a principal ideal, so $[J][I^{-1}] = 1$ and thus $[I] = [J]$.

Finally, we prove Theorem 20.14d): let T be a finitely generated torsion R-module. We notice that the statement of the classification is identical to that of finitely generated torsion modules over a PID. This is no accident, as we can easily reduce to the case of a PID – and indeed to that of a DVR, which we have already proven (Theorem 17.13). Namely, let I be the annihilator of T, and (assuming $T \neq 0$, as we certainly may) write $I = \prod_{i=1}^r \mathfrak{p}_i^{a_i}$. Then T is a module over $R/I \cong R/\prod_{i=1}^r \mathfrak{p}_i^{r_i} \cong \bigoplus_{i=1}^r R/\mathfrak{p}_i^{a_i}$. T naturally decomposes as $T = \bigoplus_{i=1}^r T_i$, where T_i is a module over $R/\mathfrak{p}_i^{a_i}$. This gives the primary decomposition of T. Moreover, each T_i is a module over the DVR $R_{\mathfrak{p}}$, so Theorem 17.13 applies.

COROLLARY 20.18. *For any Dedekind domain R, the Picard group* $\operatorname{Pic} R$ *is canonically isomorphic to the reduced K_0-group $\widetilde{K_0(R)}$.*

PROOF. Let P be a finitely generated projective R-module of rank $r \geqslant 1$. According to Theorem 20.14c) the monoid of isomorphism classes of finitely generated projective R-modules is *cancellative*: this means that the canonical map $\varphi : \operatorname{Pic}(R) \to K_0(R)$ is injective. It follows easily that the composite map $\Phi : \operatorname{Pic}(R) \xrightarrow{\varphi} K_0(R) \to \widetilde{K_0(R)}$ is an injection: indeed, for $\varphi(I)$ to be killed in $\widetilde{K_0(R)}$ but not $K_0(R)$ it would have to be a fractional ideal which has rank zero as an R-module, and there are no such things. Now an arbitrary nonzero finitely generated projective R-module is isomorphic to $R^{r-1} \oplus I$, hence becomes equal to the class of the rank one module I in $\widetilde{K_0(R)}$, so Φ is surjective. To check that it is a homomorphism of groups we may look on a set of generators – namely, the classes of rank one projective modules. Let us use $[P]$ for the class of the projective module P in $K_0(R)$ and $[[P]]$ for its image in $\widetilde{K_0(R)}$. Then by Lemma 20.17 we have

$$\Phi([I_1 \otimes I_2]) = [[I_1 \otimes I_2]] = [[I_1 I_2]] = [[R \oplus I_1 I_2]] = [[I_1 \oplus I_2]] = [[I_1]] + [[I_2]]. \quad \square$$

EXERCISE 20.6. *State and prove an appropriate analogue of Proposition 6.13 for finitely generated projective modules over a Dedekind domain R.*

COROLLARY 20.19. *For a module M over a Dedekind domain, the following are equivalent:*

(i) *The module M is torsionfree.*
(ii) *The module M is flat.*

PROOF. (i) $\implies$ (ii): If M is finitely generated and torsionfree, then M is flat by Theorem 20.15. By Corollary 3.96, every torsionfree R-module is flat.
(ii) $\implies$ (i): This holds for modules over any domain: Proposition 3.38. $\square$

COROLLARY 20.20. *For a Noetherian domain R, the following are equivalent:*

(i) *Every torsionfree R-module is flat.*
(ii) *Every finitely generated torsionfree R-module is flat.*
(iii) *The ring R is a Dedekind domain.*

PROOF. (i) $\implies$ (ii) is immediate. (ii) $\implies$ (iii): Let I be an ideal of R. Since R is Noetherian, I is a finitely generated torsionfree R-module, hence flat by assumption, and then I is projective by Corollary 7.32. By Theorem 19.12, I is invertible. In particular every nonzero prime ideal of R is invertible, so R is

Dedekind by Theorem 20.1.
(iii) $\implies$ (i) by Corollary 20.19. □

The full characterization of domains in which every torsionfree module is flat is coming up soon: Theorem 20.31.

7. Injective Modules Over a Dedekind Domain

THEOREM 20.21. *For a domain R with fraction field K, the following are equivalent:*

(i) *R is Dedekind.*
(ii) *Every divisible R-module is injective.*

PROOF. (i) $\implies$ (ii): Let D be a divisible R-module. We will show D is injective using Baer's Criterion: let I be an ideal of R and $f : I \to D$ a module map. We may assume that I is nonzero and thus, since R is a Dedekind domain, invertible: if $I = \langle a_1, \ldots, a_n \rangle$, there are $b_1, \ldots, b_n \in K$ such that $b_i I \subset R$ for all i and $1 = \sum_{i=1}^n a_i b_i$. Since D is divisible, there are $d_1, \ldots, d_n \in D$ with $f(a_i) = a_i d_i$ for all i. Then for $x \in I$,

$$f(x) = f(\sum_i b_i a_i x) = \sum (b_i x) f(a_i) = \sum_i (b_i x) a_i d_i = x \sum_i (b_i a_i) e_i.$$

Put $d = \sum_{i=1}^n (b_i a_i) d_i$. Thus $F : R \to D$ by $x \mapsto dx$ lifts f.
(ii) $\implies$ (i): Let I be injective. Then I is divisible and a quotient of a divisible module is divisible, so every quotient of I is divisible, and thus by assumption every quotient of I is injective. By Corollaries 3.61 and 20.2, R is Dedekind. □

As an application, we will prove a generalization to Dedekind domains of a nontrivial result in commutative group theory. Given an commutative group A, it is natural to ask when its torsion subgroup $A[\text{tors}]$ is a direct summand of A, so that A is the direct sum of a torsion group and a torsionfree group. It is easy to see that this happens when A is finitely generated, because then $A/A[\text{tors}]$ is a finitely generated torsionfree module over a PID, hence projective. The following exercise shows that some condition is necessary.

EXERCISE 20.7. *Let $A = \prod_p \mathbb{Z}/p\mathbb{Z}$, where the product extends over all prime numbers. Show that $A[\text{tors}]$ is not a direct summand of A.*

These considerations should serve to motivate the following result.

THEOREM 20.22. *Let M be a module over a Dedekind domain R. If $M[\text{tors}] = M[r]$ for some $r \in R$, then $M[\text{tors}]$ is a direct summand of M.*

PROOF. Step 1: We CLAIM that if A is a torsionfree R-module, then for every R-module B, $\text{Ext}^1_R(A, B)$ is divisible.
PROOF OF CLAIM Let $V = A \otimes_R K$. Since A is torsionfree, we have an exact sequence

$$0 \to A \to V \to V/A \to 0.$$

Applying the cofunctor $\text{Hom}(\cdot, B)$, a portion of the long exact Ext sequence is

$$\text{Ext}^1_R(V, B) \to \text{Ext}^1_R(A, B) \to \text{Ext}^2_R(V/A, B).$$

Since R is hereditary, Theorem 3.101a) gives $\text{Ext}^2_R(V/A, B) = 0$, so $\text{Ext}^1_R(A, B)$ is a quotient of $\text{Ext}^1_R(V, B)$. Since V is a K-module, so is $\text{Ext}^1_R(V, B)$ and thus

$\mathrm{Ext}^1_R(V,B)$ and its quotient $\mathrm{Ext}^1_R(A,B)$ is a divisible module, hence injective by Theorem 20.21.
Step 2: Let $T = M[\mathrm{tors}] = M[r]$. We will show that the sequence

$$0 \to T \to M \to M/T \to 0$$

splits by computing $\mathrm{Ext}^1_R(M/T,T) = 0$. Since M/T is torsionfree, by Step 1 $\mathrm{Ext}^1_R(M/T,T)$ is divisible. On the other hand, since $T = T[r]$, $\mathrm{Ext}^1_R(M/T,T) = \mathrm{Ext}^1_R(M/T,T)[r]$. Thus multiplication by r on $\mathrm{Ext}^1_R(M/T,T)$ is on the one hand surjective and on the other hand identically zero, so $\mathrm{Ext}^1_R(M/T,T) = 0$. By Theorem 3.92 the sequence splits. □

8. Characterizations of Prüfer Domains

Now we return to discuss Prüfer domains: recall that a Prüfer domain is a domain in which each nonzero finitely generated ideal is invertible. At first this condition ma look a bit abstruse. The following result shows that, on the contrary, this determines a very natural class of domains.

THEOREM 20.23. *(Characterization of Prüfer Domains)*
For a domain R, the following are equivalent:

(i) *R is a Prüfer domain: every nonzero finitely generated ideal is invertible.*
(i′) *Every nonzero ideal of R generated by two elements is invertible.*
(ii) *Nonzero finitely generated ideals are cancellable: if $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ are ideals of R and $\mathfrak{a}$ is finitely generated and nonzero, then $\mathfrak{ab} = \mathfrak{ac} \implies \mathfrak{b} = \mathfrak{c}$.*
(iii) *For every $\mathfrak{p} \in \operatorname{Spec} R$, the ring $R_{\mathfrak{p}}$ is a valuation ring.*
(iii′) *For every $\mathfrak{m} \in \operatorname{MaxSpec} R$, the ring $R_{\mathfrak{m}}$ is a valuation ring.*
(iv) *For all ideals A, B, C of R, we have $A(B \cap C) = AB \cap AC$.*
(v) *For all ideals A, B of R, we have $(A+B)(A \cap B) = AB$.*
(vi) *If A and C are ideals of R with C finitely generated and $A \subseteq C$, then there is an ideal B of R such that $A = BC$.*
(vii) *For all ideals A, B, C of R with C finitely generated, we have*

$$(A + B :_R C) = (A :_R C) + (B :_R C).$$

(viii) *For all ideals A, B, C of R with C finitely generated, we have*

$$(C :_R A \cap B) = (C :_R A) + (C :_R B).$$

(ix) *For all ideals A, B, C of R, we have $A \cap (B + C) = (A \cap B) + (A \cap C)$.*

PROOF. We will first show:
(i′) $\implies$ (i) $\implies$ (ii) $\implies$ (iii) $\implies$ (iii′) $\implies$ (iv) $\implies$ (v) $\implies$ (i′).
Then we will show:
(i) $\implies$ (vi) $\implies$ (iii),
(iii′) $\implies$ (vii) $\implies$ (i′),
(iii′) $\implies$ (viii) $\implies$ (i′), and
(iii′) $\iff$ (ix).
This suffices!
(i′) $\implies$ (i): We go by induction on the number of generators. A nonzero ideal with a single generator is principal, hence invertible. By assumption, every nonzero ideal generated by two elements is invertible. Hence we may assume that $n \geqslant 3$

and that every nonzero ideal of R generated by $n-1$ elements is invertible, and let $\mathfrak{c} = \langle c_1, \ldots, c_n \rangle$. We may assume $c_i \neq 0$ for all i. Put

$$\mathfrak{a} := \langle c_1, \ldots, c_{n-1} \rangle, \ \mathfrak{b} := \langle c_2, \ldots, c_n \rangle,$$
$$\mathfrak{d} := \langle c_1, c_n \rangle, \ \mathfrak{e} := c_1 \mathfrak{a}^{-1} \mathfrak{d}^{-1} + c_n \mathfrak{b}^{-1} \mathfrak{d}^{-1}.$$

Then

$$\mathfrak{c}\mathfrak{e} = (\mathfrak{a} + \langle c_n \rangle) c_1 \mathfrak{a}^{-1} \mathfrak{d}^{-1} + (\langle c_1 \rangle + \mathfrak{b}) c_n \mathfrak{b}^{-1} \mathfrak{d}^{-1}$$
$$= c_1 \mathfrak{d}^{-1} + c_1 c_n \mathfrak{a}^{-1} \mathfrak{d}^{-1} + c_1 c_n \mathfrak{b}^{-1} \mathfrak{d}^{-1} + c_n \mathfrak{d}^{-1}$$
$$= c_1 \mathfrak{d}^{-1}(R + c_n \mathfrak{b}^{-1}) + c_n \mathfrak{d}^{-1}(R + c_1 \mathfrak{a}^{-1}).$$

Since $c_n \mathfrak{b}^{-1}, \ c_1 \mathfrak{a}^{-1} \subset R$, we get

$$\mathfrak{c}\mathfrak{e} = c_1 \mathfrak{d}^{-1} + c_n \mathfrak{d}^{-1} = \langle c_1, c_n \rangle \mathfrak{d}^{-1} = R.$$

(iii) $\implies$ (iii′) is immediate. (iii′) $\implies$ (iii): if $\mathfrak{p} \in \operatorname{Spec} R$, let $\mathfrak{m}$ be a maximal ideal containing $\mathfrak{p}$. Then $R_{\mathfrak{p}}$ is an overring of $R_{\mathfrak{m}}$, and every overring of a valuation ring is a valuation ring.
(i) $\implies$ (ii) is immediate, since invertible ideals are cancellable.
(ii) $\implies$ (iii): Step 1: Suppose $\mathfrak{a}$ is a nonzero finitely generated ideal and $\mathfrak{b}, \mathfrak{c}$ are ideals of R with $\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a}\mathfrak{c}$. Then

$$\mathfrak{a}\mathfrak{c} = \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c} = \mathfrak{a}(\mathfrak{b} + \mathfrak{c}).$$

By our assumption, we may cancel $\mathfrak{a}$ to get $\mathfrak{c} = \mathfrak{b} + \mathfrak{c}$, so $\mathfrak{b} \subseteq \mathfrak{c}$.
Step 2: Now let $\mathfrak{p} \in \operatorname{Spec} R$. By Proposition 17.4, to show that $R_{\mathfrak{p}}$ is a valuation ring it is enough to show that given any two principal ideals of $R_{\mathfrak{p}}$, one contains the other. Since every principal ideal of a localization $S^{-1}R$ is generated by an element of R, it suffices to show: for any $a, b \in R^{\bullet}$, we have either $aR_{\mathfrak{p}} \subseteq bR_{\mathfrak{p}}$ or $bR_{\mathfrak{p}} \subseteq aR_{\mathfrak{p}}$. Since

$$(ab)\langle a, b \rangle \subseteq \langle a^2, b^2 \rangle \langle a, b \rangle,$$

by Step 1 we have $(ab) \subseteq \langle a^2, b^2 \rangle$, so

$$ab = xa^2 + yb^2 \text{ for some } x, y \in R.$$

This implies $(yb)\langle a, b \rangle \subseteq (a)\langle a, b \rangle$ and thus $(yb) \subseteq (a)$, so thre is $u \in R$ such that $yb = au$. Then $ab = xa^2 + uab$ or

$$xa^2 = ab(1 - u).$$

If $u \notin \mathfrak{p}$, then $a = b(\frac{y}{u}) \in bR_{\mathfrak{p}}$. If $u \in \mathfrak{p}$ then $1 - u \notin \mathfrak{p}$ and $b = a(\frac{x}{1-u}) \in aR_{\mathfrak{p}}$.
(iii) $\implies$ (iii′) is immediate: maximal ideals are prime.
(iii′) $\implies$ (iv): First suppose that R is a valuation ring, and let A, B, C be ideals of R. Since R is a chain ring, after interchanging B and C if necessary we may assume that $B \subseteq C$, and then

$$A(B \cap C) = AB = AB \cap AC.$$

Now suppose that $R_{\mathfrak{m}}$ is a valuation ring for all $\mathfrak{m} \in \operatorname{MaxSpec} R$. For an ideal I of R, we put $I_{\mathfrak{m}} := IR_{\mathfrak{m}}$. Using Exercise 7.11, we get

$$A(B \cap C)R_{\mathfrak{m}} = A_{\mathfrak{m}}(B_{\mathfrak{m}} \cap C_{\mathfrak{m}})$$
$$= A_{\mathfrak{m}}B_{\mathfrak{m}} \cap A_{\mathfrak{m}}C_{\mathfrak{m}} = (AB)_{\mathfrak{m}} \cap (AC)_{\mathfrak{m}} = (AB \cap AC)R_{\mathfrak{m}}.$$

By Exercise 7.22, we deduce: $A(B \cap C) = AB \cap AC$.
(iv) $\implies$ (v): Suppose (iv) holds, and let A and B be ideals of R. Then

$$(A + B)(A \cap B) = ((A + B)A) \cap ((A + B)B) \supseteq AB.$$

Conversely if $x \in A$, $y \in B$ and $z \in A \cap B$, then $(x+y)z = xz+yz \in AB+AB = AB$.
(v) $\implies$ (i′): Suppose (v) holds, and let $I := \langle x_1, x_2 \rangle$ be a nonzero ideal of R. If either $x_1 x_2 = 0$, then I is principal, hence invertible, so we may assume that $x_1, x_2 \in R^\bullet$, and then $A := (x_1)$ and $B := (x_2)$ are invertible, and

$$C(A \cap B)B^{-1}A^{-1} = (A+B)(A \cap B)B^{-1}A^{-1} = ABB^{-1}A^{-1} = R,$$

so C is invertible.
(i) $\implies$ (vi): Suppose (i) holds, and let $A \subseteq C$ be ideals of R with C finitely generated. We may assume that C is nonzero, hence invertible, so AC^{-1} is an ideal of R and $A = (AC^{-1}C)$.
(vi) $\implies$ (iii): Suppose that (vi) holds, and let $\mathfrak{p} \in \operatorname{Spec} R$. We will show that $R_\mathfrak{p}$ is a chain ring: thus for $a, b \in R^\bullet$ we must show that either $aR_\mathfrak{p} \subseteq bR_\mathfrak{p}$ or $bR_\mathfrak{p} \subseteq aR_\mathfrak{p}$. Since $(a) \subseteq \langle a, b \rangle$, so there is an ideal B of R such that $(a) = \langle a, b \rangle B$, and thus there are $x, y \in B$ such that

$$a = ax + by.$$

Suppose $x \in \mathfrak{p}$. Then $1 - x \notin \mathfrak{p}$, so $a = \frac{by}{1-x} \in bR_\mathfrak{p}$. Now suppose $x \notin \mathfrak{p}$. Since $bB \subseteq (a)$, we have $bx \in (a)$ and thus $b \in aR_\mathfrak{p}$.
(iii′) $\implies$ (vii): First we observe that for all ideals A, B, C in a chain ring, we have

$$((A+B) :_R C) = (A :_R C) + (B :_R C).$$

Indeed, after interchanging A and B we may assume that $A \subseteq B$ and then both sides are $(A :_R C)$. Now suppose that (iii′) holds,let A, B, C be ideals of R with C finitely generated, and let $\mathfrak{m} \in \operatorname{MaxSpec} R$. By Exercise **??**, we have

$$(A+B) :_R C)R_\mathfrak{m} = (A_\mathfrak{m} + B_\mathfrak{m}) :_{R_\mathfrak{m}} C_\mathfrak{m})$$

$$= (A_\mathfrak{m} :_{R_\mathfrak{m}} C_\mathfrak{m}) + (B_\mathfrak{m} :_{R_\mathfrak{m}} C_\mathfrak{m})$$

$$= (A :_R C)_\mathfrak{m} + (B :_R C)_\mathfrak{m} = ((A :_R C) + (B :_R C))R_\mathfrak{m}.$$

By Exercise 7.22, we deduce: $(A+B) :_R C = (A :_R C) + (B :_R C)$.
(vii) $\implies$ (i′): Suppose (vii) holds, and let $a, b \in R^\bullet$. Then

$$R = \langle a, b \rangle :_R \langle a, b \rangle = (a) :_R \langle a, b \rangle + (b) :_R \langle a, b \rangle$$

$$= (a) :_R (b) + (b) :_R (a).$$

Write $1 = x + y$ for $xb \in (a)$ and $ya \in (b)$. Then $xb^2, ya^2 \in (ab)$, so

$$\langle a, b \rangle \langle bx, ay \rangle \subseteq (ab) = (abx + aby) \subseteq \langle a, b \rangle \langle bx, ay \rangle.$$

Thus $\langle a, b \rangle \langle bx, ay \rangle = (ab)$, so $\langle a, b \rangle$ is invertible.
(iii′) $\implies$ (viii): Suppose (iii′) holds, let A, B, C be ideals of R with C finitely generated, and let $\mathfrak{m} \in \operatorname{MaxSpec} R$. Without loss of generality, suppose that $\min(A_\mathfrak{m}, B_\mathfrak{m}) = A_\mathfrak{m}$. Then:

$$(C :_R (A \cap B)R_\mathfrak{m}) \subseteq (C_\mathfrak{m} :_{R_\mathfrak{m}} (A \cap B)_\mathfrak{m})$$

$$(C_\mathfrak{m} :_{R_\mathfrak{m}} A_\mathfrak{m} = (C :_{R_\mathfrak{m}} A_\mathfrak{m}) + (C :_{R_\mathfrak{m}} B_\mathfrak{m})$$

$$= (C :_R A)_\mathfrak{m} + (C :_R B)_\mathfrak{m} = ((C :_R A) + C :_R B))_\mathfrak{m} \subseteq (C :_R (A \cap B))_\mathfrak{m}.$$

Thus $(C :_R (A \cap B))_\mathfrak{m} = ((C :_R A) + (C :_R B))_\mathfrak{m}$. Since this holds for all $\mathfrak{m} \in \operatorname{MaxSpec} R$, by Exercise 7.22 we deduce: $(C :_R (A \cap B)) = (C :_R A) + (C :_R B)$.
(viii) $\implies$ (i′): Suppose (viii) holds, and let $a, b \in R^\bullet$. Then

$$R = ((a) \cap (b)) :_R ((a) \cap (b)) = ((a) \cap (b) :_R (a)) + ((a) \cap (b)) :_R (b)) = (b) :_R (a) + (a) :_R (b).$$

We finish using the argument of (vii) $\implies$ (i′).
(iii′) $\implies$ (ix): For any ideals A, B, C in a chain ring, we have

$$A \cap (B + C) = A \cap \max(B, C) = (A \cap B) + (A \cap C),$$

so if (iii′) holds, then Exercise 7.22 implies that the same identity holds for ideals A, B, C of R.
(ix) $\implies$ (iii′): Suppose (ix) holds, let $\mathfrak{m} \in \operatorname{MaxSpec} R$ and let $a, b \in R$. Since $(a) \subseteq (b) + (a - b)$, we have

$$(a) = (a) \cap ((b) + (a - b)) = ((a) \cap (b)) + ((a) \cap (a - b)).$$

Thus we may write

$$a = t + c(a - b)$$

with $t \in (a) \cap (b)$, $c \in R$ and $c(a-b) \in (a)$. Then $cb \in (a)$ and $(1-c)a = t - cb \in (b)$. Suppose $c \in \mathfrak{m}$. Then $1 - c \notin \mathfrak{m}$, so $a \in bR_{\mathfrak{m}}$. Now suppose $c \notin \mathfrak{m}$. Then $b \in aR_{\mathfrak{m}}$. It follows that $R_{\mathfrak{m}}$ is a valuation ring. □

Exercise 20.8. *Let R be a Prüfer domain.*

a) *Let S be a multiplicative subset of R. Show: $S^{-1}R$ is a Prüfer domain.*
b) *Let $\mathfrak{p} \in \operatorname{Spec} R$. Show: $R/\mathfrak{p}$ is a Prüfer domain.*
(Hint: Use Lemma 7.8 and Exercise 17.7b).)

Exercise 20.9. *Let R be a Prüfer domain, and let I and J be ideals of R. Suppose there is $n \in \mathbb{Z}^+$ such that $I^n = J^n$. Show: $I = J$.*

Theorem 20.24. *Let R be a domain.*

a) *Suppose R is a GCD-domain. Then R is Prüfer if and only if it is Bézout.*
b) *A Prüfer UFD is a PID.*

Proof. a) Since principal ideals are invertible, any Bézout domain is a Prüfer domain. Conversely, suppose R is a GCD-domain and a Prüfer domain. Let $x, y \in R^\bullet$ and let d be a GCD of x, y. Certainly we have $(d) \supset \langle x, y \rangle$. Thus $\iota : \langle x, y \rangle \hookrightarrow (d)$ is a homomorphism of R-modules which we want to show is an isomorphism. By the Local-Global Principle for Module Homomorphisms it is enough to show that for all $\mathfrak{p} \in \operatorname{Spec} R$, $\iota_{\mathfrak{p}}$ is an isomorphism of $R_{\mathfrak{p}}$-modules, i.e., $\langle x, y \rangle_{R_{\mathfrak{p}}} = \langle d \rangle_{\mathbb{R}_{\mathfrak{p}}}$. By Proposition 15.16, d is again the GCD of x and y in the valuation ring $R_{\mathfrak{p}}$ (equivalently, the valuation of d is the minimum of the valuations of x and y) so that the principal ideal $\langle x, y \rangle_{R_{\mathfrak{p}}}$ is generated by $\langle d \rangle_{R_{\mathfrak{p}}}$.
b) Suppose R is a Prüfer UFD. By part a) R is Bézout, and by Theorem 16.20 a Bézout UFD is a PID. □

Proposition 20.25. *For a Prüfer domain R, the following are equivalent:*

(i) *The ring R is a Bézout domain.*
(ii) *We have* $\operatorname{Pic}(R) = 0$.

Proof. A nonzero ideal in a Prüfer domain is invertible if and only if it is finitely generated. So (i) and (ii) each assert that every nonzero finitely generated ideal is principal. □

Proposition 20.26. *A Prüfer domain is integrally closed.*

Proof. In Theorem 20.1 we showed that a domain in which all fractional R-ideals are invertible is integrally closed. In the proof we only used the invertbility of finitely generated fractional ideals, so the argument works in any Prüfer domain. □

EXERCISE 20.10. *Prove Proposition 20.26 using the local nature of integral closure.*

EXERCISE 20.11. *Let R be a Prüfer domain.*

a) *Show: if $\dim R \leq 1$, then R is completely integrally closed. (Hint: use Exercise 17.23.)*
b) *Show: the ring $\operatorname{Hol}\mathbb{C}$ of entire functions is a completely integrally closed Prüfer domain of infinite Krull dimension.*
c) *Suppose $\dim R > 1$. Show: there is $\mathfrak{m} \in \operatorname{MaxSpec} R$ such that $R_{\mathfrak{m}}$ is* not *completely integrally closed.*
d) *Deduce from parts b) and c) that the localization of a completely integrally closed domain* need not *be completely integrally closed.*

8.1. A Chinese Remainder Theorem for Prüfer domains.

Recall that we have a Chinese Remainder Theorem which is valid in any ring: Theorem 4.22. There is however another useful version of the Chinese Remainder Theorem which holds in a domain R if and only if R is a Prüfer domain.

Let R be a ring, let $I_1, \ldots, I_n$ be a finite sequence of ideals in R and let $x_1, \ldots, x_n$ be a finite sequence of elements in R. We may ask: when is there an element $x \in R$ such that $x \equiv x_i \pmod{I_i}$ for all i?

If we assume the ideals I_i are pairwise comaximal, then this holds in any ring by CRT (Theorem 4.22). But suppose we drop that condition. Then, if such an x exists, we have $x - x_i \in I_i$ for all i, hence for all i and j,

$$x_i - x_j = (x - x_j) - (x - x_i) \in I_i + I_j. \tag{56}$$

Thus we get a necessary condition (which, notice, is vacuous when the ideals are pairwise comaximal). Let us say that a ring has property **ECRT(n)** if for all ideals $I_1, \ldots, I_n$ and elements $x_1, \ldots, x_n$ satisfying (56), there exists $x \in R$ such that $x \equiv x_i \pmod{I_i}$ for all i. We say that R satisfies **ECRT** (Elementwise Chinese Remainder Theorem) if it satisfies ECRT(n) for all $n \in \mathbb{Z}^+$.

EXERCISE 20.12. *Show: a PID satisfies property ECRT.*

LEMMA 20.27. *Any ring satisfies ECRT(1) and ECRT(2).*

PROOF. ECRT(1) is trivial. For ECRT(2): let I, J be ideals of R, let $x_1, x_2 \in R$, and suppose $x_1 - x_2 \in I + J$: there are $i \in I$, $j \in J$ such that $x_1 - x_2 = i + j$. Put $x = x_1 - i = x_2 + j$. Then $x \equiv x_1 \pmod{I}$ and $x \equiv x_2 \pmod{J}$. □

THEOREM 20.28. *For a ring R, the following are equivalent:*

(i) *ECRT holds in R.*
(ii) *ECRT(3) holds in R.*
(iii) *For all ideals A, B, C in R, $A + (B \cap C) = (A + B) \cap (A + C)$.*
(iv) *For all ideals A, B, C in R, $A \cap (B + C) = (A \cap B) + (A \cap C)$.*

PROOF. (i) $\implies$ (ii) is immediate.
(ii) $\implies$ (iii): The inclusion $A + (B \cap C) \subset (A + B) \cap (A + C)$ holds for ideals in any ring. Conversely, let $t \in (A + B) \cap (A + C)$. Then by ECRT(3) there is $x \in R$ satisfying all of the congruences

$$x \equiv 0 \pmod{A},$$

$$x \equiv t \pmod{B},$$
$$x \equiv t \pmod{C},$$

and thus $x \in A$, $x - t \in B \cap C$, so $t = x - (x - t) \in A + (B \cap C)$.
(iii) $\implies$ (iv): For A, B, C ideals of R, we we have

$$(A \cap B) + (A \cap C) = ((A \cap B) + A) \cap ((A \cap B) + C) = A \cap ((A \cap B) + C)$$

and

$$(A \cap B) + (A \cap C) = (A + (A \cap C)) \cap ((A \cap C) + B) = A \cap ((A \cap C) + B),$$

and thus

$$(A \cap B) + C = (A \cap C) + B.$$

It follows that

$$(A \cap B) + C = (A \cap B) + C + (A \cap C) + B = B + C$$

and thus

$$(A \cap B) + (A \cap C) = A \cap ((A \cap B) + C) = A \cap (B + C).$$

(iv) $\implies$ (iii): Assume (iv). Then for all ideals A, B, C of R,

$$(A + B) \cap (A + C) = (A + B) \cap A \ + \ (A + B) \cap C = A \cap (A + B) \ + \ C \cap (A + B)$$
$$= (A \cap A) + (A \cap B) + (A \cap C) + (B \cap C) = A + (A \cap B) + (A \cap C) + (B \cap C) = A + (B \cap C).$$

(iii) $\implies$ (i): We go by induction on n. Having established that ECRT(1) and ECRT(2) hold in any ring, we let $n \geqslant 2$, assume ECRT(n) and show ECRT($n+1$): let $x_1, \ldots, x_{n+1} \in R$ and $I_1, \ldots, I_{n+1}$ be ideals of R such that $x_i - x_j \in I_i + I_j$ for all $1 \leqslant i, j \leqslant n$. By ECRT($n$), there is $y \in R$ with $y \equiv x_i \pmod{I}_i$ for $1 \leqslant i \leqslant n$. We CLAIM that $y - x_{n+1} \in I_{n+1} + \bigcap_{i=1}^{n} I_i$.
PROOF OF CLAIM: Since we have assumed (iii), we have by induction that

$$\mathfrak{a} + \bigcap_{i=1}^{n} \mathfrak{b}_i = \bigcap_{i=1}^{n} (\mathfrak{a} + \mathfrak{b}_i),$$

and in particular

$$I_{n+1} + \bigcap_{i=1}^{n} I_i = \bigcap_{i=1}^{n} (I_i + I_{n+1}).$$

Also, for all $1 \leqslant i \leqslant n$, we have

$$y - x_{n+1} = (y - x_i) + (x_i - x_{n+1}) \in I_i + I_i + I_{n+1} \in I_i + I_{n+1}$$

and thus indeed

$$y - x_{n+1} \in \bigcap_{i=1}^{n} (I_i + I_{n+1}) = I_{n+1} + \bigcap_{i=1}^{n} I_i.$$

Because of the claim and ECRT(2), there is $t \in R$ satisfying

$$t \equiv y \pmod{\bigcap_{i=1}^{n} I_i},$$
$$t \equiv x_{n+1} \pmod{I_{n+1}}.$$

Then for $1 \leqslant i \leqslant n$,

$$t - x_i = (t - y) + (y - x_i) \in I_i. \qquad \square$$

9. Modules over a Prüfer domain

Recall that a module is **semihereditary** if every finitely generated submodule is projective and that a ring R is **semihereditary** if the module R is semihereditary: i.e., every finitely generated ideal of R is projective.

PROPOSITION 20.29. *A domain R is a semihereditary if and only if it is a Prüfer domain.*

EXERCISE 20.13. *Prove Proposition 20.29.*

LEMMA 20.30. *Let R be a domain, and let M be a finitely generated torsionfree R-module. Then M is a submodule of a finitely generated free module.*

PROOF. Since M is torsionfree, $M \hookrightarrow M \otimes_R K$, and $\iota : M \otimes_R K \cong K^n$ for some $n \in \mathbb{N}$. Since M is finitely generated, there exists $x \in R^\bullet$ such that the image of xM in $M \otimes_R K$ is contained in R^n, and thus $\iota \circ (x\bullet) : M \hookrightarrow R^n$. □

THEOREM 20.31. *For a domain R, the following are equivalent:*

(i) *Every torsionfree R-module is flat.*
(ii) *Every finitely generated torsionfree R-module is projective.*
(iii) *R is a Prüfer domain.*

PROOF. (i) $\implies$ (ii): Let M be a finitely generated torsionfree R-module. By assumption M is flat, and since R is a domain, by Corollary 13.38 M is projective.
(ii) $\implies$ (iii): Finitely generated ideals are assumed projective, hence invertible.
(iii) $\implies$ (i): Let R be a Prüfer domain and M a torsionfree R-module. Then $M = \varinjlim_i M_i$ is the direct limit of its finitely generated submodules, hence a direct limit of finitely generated torsionfree modules M_i. By Lemma 20.30, each M_i is a finitely generated submodule of a free R-module. By Theorems 20.29 and 3.69, each M_i is projective, hence flat. Thus M is a direct limit of flat modules, hence is itself a flat module by Corollary 3.95. □

EXERCISE 20.14. *Let R be a domain. Show: the following are equivalent:*

(i) *R is a Beźout domain.*
(ii) *Every finitely generated torsionfree R-module is free.*

(Suggestion: Consult §3.9.2.)

10. Almost Dedekind Domains

A domain R is **almost Dedekind** if $R_\mathfrak{m}$ is a DVR for all $\mathfrak{m} \in \operatorname{MaxSpec} R$. Thus a field is an almost Dedekind domain, and any almost Dedekind domain that is not a field is a one-dimensional Prüfer domain. The converse is not true: for instance, if R is a valuation domain with value group $(\mathbb{Q}, +)$ then R is a one-dimensional Prüfer domain that is not almost Dedekind. Clearly a Dedekind domain is almost Dedekind, and since a Noetherian Prüfer domain is a Dedekind domain, also a Noetherian almost Dedekind domain is Dedekind.

PROPOSITION 20.32. *For a one-dimensional domain R, the following are equivalent:*

(i) *R is almost Dedekind.*
(ii) *An ideal of R is primary if and only if it is a prime power.*

PROOF. Let R be a one-dimensional domain. Since nonzero prime ideals are maximal, a nonzero ideal I of R is primary if and only if its radical is prime if and only if it is contained in a unique prime ideal. Let $\mathfrak{p} \in \operatorname{MaxSpec} R$, and let $\iota : R \to R_{\mathfrak{p}}$ be the localization map. By Exercise 7.10, the pushforward ι_* gives a bijection between the $\mathfrak{p}$-primary ideals of R and the $\mathfrak{p}_{\mathfrak{p}}$-primary ideals of $R_{\mathfrak{p}}$; moreover the latter is the set of all nonzero, proper ideals of $R_{\mathfrak{p}}$.

Suppose R is almost Dedekind. Then ι_* gives a bijection from the $\mathfrak{p}$-primary ideals of R to the set $\{\mathfrak{p}_{\mathfrak{p}}^n \mid n \in \mathbb{Z}^+\}$. Of course, for all $n \in \mathbb{Z}^+$ we have $\iota_*(\mathfrak{p}^n) = \mathfrak{p}_{\mathfrak{p}}^n$, so it follows that every $\mathfrak{p}$-primary ideal of R is of the form $\mathfrak{p}^n$ for a unique $n \in \mathbb{Z}^+$.

Suppose every $\mathfrak{p}$-primary ideal of R is of the form $\mathfrak{p}^n$ for some $n \in \mathbb{Z}^+$. Then every nonzero ideal of $R_{\mathfrak{p}}$ is of the form $\mathfrak{p}_{\mathfrak{p}}^n$ for some $n \in \mathcal{B}$. Thus ideals of $R_{\mathfrak{p}}$ satisfy ACC: $R_{\mathfrak{p}}$ is Noetherian. Moreover the set of ideals of $R_{\mathfrak{p}}$ is linearly ordered, so $R_{\mathfrak{p}}$ is a valuation ring. Thus $R_{\mathfrak{p}}$ is a DVR, so R is almost Dedekind. □

LEMMA 20.33. *Let $(R, \mathfrak{m})$ be a valuation ring, and let I be a nonzero ideal of R. The following are equivalent:*

(i) *We have $I\mathfrak{m} = I$.*
(ii) *The ideal I is* not *principal.*

PROOF. (i) $\implies$ (ii): We go by contraposition. If I is principal, then in $\operatorname{Frac} R$ it is invertible, so multiplying both sides of $I\mathfrak{m} = I$ by I^{-1} gives $\mathfrak{m} = R$, a contradiction.
(ii) $\implies$ (i): Suppose I is not principal; we will show that the upset $\mathcal{U}(I)$ is contained in the upset $\mathcal{U}(I\mathfrak{m})$. Let $h \in \mathcal{U}(I)$. Since I is not principal, neither is $\mathcal{U}(I)$, and thus there is $g \in \mathcal{U}(I)$ with $g < h$. Then $h = g + (h - g)$ with $g \in \mathcal{U}(I)$ and $h - g > 0$, so $h \in \mathcal{U}(I) + \mathcal{U}(\mathfrak{m}) \subseteq \mathcal{U}(I\mathfrak{m})$. □

THEOREM 20.34. *Let R be a domain that is not a field. The following are equivalent:*

(i) *R is almost Dedekind.*
(ii) *R is Prüfer and for each proper ideal I of R we have $\bigcap_{n \geqslant 1} I^n = (0)$.*
(iii) *R is Prüfer of dimension one, and for each $\mathfrak{m} \in \operatorname{MaxSpec} R$ we have $\mathfrak{m}^2 \subsetneq \mathfrak{m}$.*
(iv) *The monoid of nonzero ideals of R under multiplication is cancellative.*

PROOF. We begin with the following simple observation: let I be an ideal of a domain R, and let $S \subseteq R^\bullet$ be a multiplicative subset. Let $I_S := I(S^{-1}R)$ be the pushforward of I to $S^{-1}R$. Then $\bigcap_{n \in \mathbb{Z}^+} I^n = (0)$ if and only if $\bigcap_{n \in \mathbb{Z}^+} I_S^n = (0)$. Indeed, since $\bigcap_{n \in \mathbb{Z}^+} I^n \subseteq \bigcap_{n \in \mathbb{Z}^+} I_S^n$, if $\bigcap_{n \in \mathbb{Z}^+} I_S^n = (0)$ then $\bigcap_{n \in \mathbb{Z}^+} I^n = 0$. Conversely, if $x \in (\bigcap_{n \in \mathbb{Z}^+} I_S^n)^\bullet$ then we may write $x = \frac{a}{s}$ with $a \in R^\bullet$ and $s \in S$, and then $x \in (\bigcap_{n \in \mathbb{Z}^+} I^n)^\bullet$.
(i) $\implies$ (ii): Suppose R is almost Dedekind. Then R is Prüfer. For a proper ideal I of R, choose $\mathfrak{m} \in \operatorname{MaxSpec} R$ such that $I \subseteq \mathfrak{m}$. Then $R_{\mathfrak{m}}$ is a DVR with maximal ideal $\mathfrak{m}_{\mathfrak{m}}$, so $\bigcap_{n \in \mathbb{Z}^+} \mathfrak{m}_{\mathfrak{m}}^n = (0)$, so $\bigcap_{n \in \mathbb{Z}^+} I^n \subseteq \bigcap_{n \in \mathbb{Z}^+} \mathfrak{m}^n = (0)$.
(ii) $\implies$ (i): Suppose R is Prüfer. Then for all $\mathfrak{m} \in \operatorname{MaxSpec} R$, the local ring $R_{\mathfrak{m}}$ is a valuation ring. By Theorem 17.16 and the above observation, for $\mathfrak{m} \in \operatorname{MaxSpec} R$, since $\bigcap_{n \in \mathbb{Z}^+} \mathfrak{m}^n = (0)$, also $\bigcap_{n \in \mathbb{Z}^+} \mathfrak{m}_{\mathfrak{m}}^n = (0)$, so the ring $R_{\mathfrak{m}}$ is a DVR.
(i) $\implies$ (iii): This follows from the same argument used to show (ii) $\implies$ (i).
(iii) $\implies$ (i): Suppose R is Prüfer of dimension 1, and let $\mathfrak{m} \in \operatorname{MaxSpec} R$. Then $R_{\mathfrak{m}}$ is a rank one valuation ring, so the value group G is Archimedean. The proof of

Theorem 17.16 shows that in this case if the valuation is not discrete then $\mathfrak{m}^2 = \mathfrak{m}$, so the valuation must be discrete.
(i) $\implies$ (iv): Suppose R is almost Dedekind, and let $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$ be nonzero ideals of R such that $\mathfrak{ac} = \mathfrak{bc}$. Then for all $\mathfrak{m} \in \operatorname{MaxSpec} R$ we have $\mathfrak{a}_\mathfrak{m}\mathfrak{c}_\mathfrak{m} = \mathfrak{b}_\mathfrak{m}\mathfrak{c}_\mathfrak{m}$. Since $R_\mathfrak{m}$ is Dedekind, $c_\mathfrak{m}$ is invertible, and thus $a_\mathfrak{m} = \mathfrak{b}_\mathfrak{m}$. By Exercise 7.22b), we get $\mathfrak{a} = \mathfrak{b}$.
(iv) $\implies$ (i): Let S be a multiplicative subset of a ring R, and let $\iota : R \to S^{-1}R$ be the localization map. Then ι^* is an injective homomorphism from the monoid of nonzero ideals of $S^{-1}R$ to the monoid of nonzero ideals of R, so if the monoid of nonzero ideals of R is cancellative, so is the monoid of nonzero ideals of $S^{-1}R$.

Now suppose that the monoid of nonzero ideals of R is cancellative. In particular, nonzero *finitely generated* ideals of R are cancellable, so by Theorem 20.23 we know that R is Prüfer. Let $\mathfrak{m} \in \operatorname{MaxSpec} R$, so $R_\mathfrak{m}$ is a valuation ring in which every nonzero ideal is cancellable. By Lemma 20.33, every ideal of $R_\mathfrak{m}$ is principal, i.e., $R_\mathfrak{m}$ is a DVR. Thus R is almost Dedekind. □

THEOREM 20.35. *For an almost Dedekind domain R, the following are equivalent:*

(i) *R is a Dedekind domain.*
(i) *For every nonzero ideal I of R, the set of maximal ideals containing I is finite.*

PROOF. (i) $\implies$ (ii): For a nonzero ideal I in a Dedekind domain, the maximal ideals $\mathfrak{p}$ containing I are the ones appearing to a positive power in the factorization of I into prime ideals, so they are certainly finite in number.
(ii) $\implies$ (i): Let R be almost Dedekind, and let I be a nonzero ideal that is contained in finitely many maximal ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. By Theorem 20.34, for each $1 \leqslant i \leqslant n$ there is $n_i \in \mathbb{Z}^+$ such that I is contained in $\mathfrak{p}_i^{n_i}$ and is *not* contained in $\mathfrak{p}_i^{n_i+1}$. We claim that $I = \prod_{i=1}^n \mathfrak{p}_i^{n_i}$. If so, Theorem 20.8 implies that R is Dedekind.

By Exercise 7.22b), it suffices to the equality $I = \prod_{i=1}^n \mathfrak{p}_i^{n_i}$ locally. Let $\mathfrak{m} \in \operatorname{MaxSpec} R$. If $\mathfrak{m}$ does not equal $\mathfrak{p}_i$ for some I, then $\mathfrak{m}$ contains neither I nor $\prod_{i=1}^n \mathfrak{p}_i^{n_i}$, so

$$I_\mathfrak{m} = R_\mathfrak{m} = (\prod_{i=1}^n \mathfrak{p}_i^{n_i})_\mathfrak{m}.$$

Now suppose that $\mathfrak{m} = \mathfrak{p}_i$ for some $1 \leqslant i \leqslant n$. Then $(\prod_{i=1}^n \mathfrak{p}_i^{n_i})_\mathfrak{m} = \mathfrak{m}_\mathfrak{m}^{n_i}$. Since $I \subseteq \mathfrak{m}^{n_i}$ we have $I_\mathfrak{m} \subseteq \mathfrak{m}_\mathfrak{m}^{n_i}$. On the other hand, since I is *not* contained in $\mathfrak{m}^{n_i+1}$, by Exercise 7.23a) this containment must fail after localizing at some maximal ideal $\mathfrak{m}'$. For any $\mathfrak{m}' \neq \mathfrak{m}$ we have $\mathfrak{m}_{\mathfrak{m}'}^{n_i+1} = R_{\mathfrak{m}'} \supseteq I_{\mathfrak{m}'}$, so we must have that $I_\mathfrak{m}$ is not contained in $\mathfrak{m}_\mathfrak{m}^{n_i+1}$. Thus $I_\mathfrak{m} = \mathfrak{m}_\mathfrak{m}^{n_i}$, completing the proof. □

EXERCISE 20.15. *Let R be an almost Dedekind domain with fraction field K. Let L/K be a finite degree field extension, and let T be the integral closure of R in L.*

a) *Show: T is almost Dedekind.*
b) *Let $\mathfrak{p} \in \operatorname{MaxSpec} R$. Show: the set $\{\mathcal{P} \in \operatorname{MaxSpec} T \mid \mathcal{P} \cap R = \mathfrak{p}\}$ is finite and nonempty.*

11. Infinite Integral Closure

LEMMA 20.36. *Let $(R, \mathfrak{m})$ be an integrally closed local domain with fraction field K. Let $f \in R[t]^\bullet$ be a polynomial that has at least one coefficient in $R^\times$, and let $x \in K^\times$ be a root of f. Then one of x and x^{-1} lies in R.*

PROOF. We go by induction on the degree n of f. For the base case: suppose $f = a_1 t - a_0$, so $x = \frac{a_0}{a_1}$. Since one of $a_0, a_1 \in R^\times$, at least one of x and x^{-1} lies in R.

Now let $n \geqslant 2$, suppose that the result holds for all polynomials of degree $n-1$, and conisder

$$f \coloneqq \sum_{i=0}^{n} a_i t^i \in R[t]$$

of degree n. If $a_n \in R^\times$ then x is integral over R, hence $x \in R$ since R is integrally closed. So we may suppose that $a_n \notin R^\times$. Multiplying through by $a_n^{n_1}$ we get that $a_n x$ is integral over R, hence $a_n x \in R$. If $a_n x \in R^\times$ then $x^{-1} \in R$, so we may assume that $a_n x \in \mathfrak{m}$. Consider the equation

$$(a_n x + a_{n-1})x^{n-1} + \sum_{i=0}^{n-2} a_i x^i = 0.$$

If $a_{n-1} \in R^\times$ then $a_n x + a_{n-1} \in R^\times$ and again x is integral over R hence lies in R. Otherwise we have $a_i \in R^\times$ for some $0 \leqslant i \leqslant n-2$, and applying the induction hypothesis to the polynomial $g(t) \coloneqq (a_n x + a_{n-1})t^{n-1} + \sum_{i=0}^{n-1} a_i t^i$ shows that one of x and x^{-1} lies in R. □

THEOREM 20.37. *Let R be a Prüfer domain with fraction field K, et L/K be an algebraic field extension, and let T be the integral closure of R in L. Then T is a Prüfer domain.*

PROOF. It suffices to show that for all $\mathcal{P} \in \operatorname{MaxSpec} T$, the localization $T_{\mathcal{P}}$ is a valuation ring. Put $\mathfrak{p} \coloneqq \mathcal{P} \cap R$, and let $x \in L^\times$. Because L/F is algebraic, there is a polynomial $p \in R_{\mathfrak{p}}[t]^\bullet] \subseteq T_{\mathcal{P}}^\bullet$ such that $p(x) = 0$. By Theorem 20.23, the ring $R_{\mathfrak{p}}$ is a valuation ring, so we may recale p so that one of its coefficients lies in $R_{\mathfrak{p}}^\times \subseteq T_{\mathcal{P}}^\times$. Applying Lemma 20.36, we find that one of x and x^{-1} lies in $T_{\mathcal{P}}$, so $T_{\mathcal{P}}$ is a valuation ring. □

PROPOSITION 20.38. *Let $(X, \leqslant)$ be a directed set, and elt $\{R_i, \varphi_{ij}\}$ be an X-indexed directed system of Prüfer domains with injective transition maps $\varphi_{ij} : R_i \hookrightarrow R_j$. Then the direct limit $R = \varinjlim R_i$ is a Prüfer domain.*

PROOF. We may regard R as the union of its subrings R_i, and the directedness is precisely buying us that for any finite subset J of I, there is $i \in I$ such that $R_i \supseteq \bigcup_{j \in J} R_j$. In particular, any finite subset of R lies in R_i for some i. Thus R is a domain, and if $I = \langle x_1, \ldots, x_n \rangle$ is a finitely generated ideal of R, then there is some $i \in I$ such that $x_1, \ldots, x_n \in R_i$ and then $I = (\varphi_i)_* I_i$, where $I_i = \langle x_1, \ldots, x_n \rangle_{R_i}$ and $\varphi_i : R_i \hookrightarrow R$ is the natural map. Since R_i is Prüfer, the ideal I_i is invertible and thus so is its pushforward I. □

Let R be a Dedekind domain with fraction field K, let L/K be a finite degree field extension, and let T be the integral closure of R in L. By the Krull-Akizuki Theorem, we know that L is also a Dedekind domain. Similarly, if R is almost Dedekind

then its integral closure in a finite degree field extension is also almost Dedekind by Exercise 20.15. On the other hand, suppose R is Dedekind with fraction field K, L/K is an algebraic field extension of infinite degree and T is the integral closure of R in L. Let $\{L_i\}_{i \in X}$ be the set of all finite degree subextensions of L/K, and for each $i \in X$ let T_i be the integral closure of R in L_i. Thus T_i is Dedekind, hence Prüfer, and $T = \varinjlim T_i$ (since every element of an algebraic field extension lies in some finite degree subextension), so by Proposition 20.38 we have at least that T is Prüfer. But when is T Dedekind or almost Dedekind?

We have already seen an example in which T need not be Dedekind. Namely, take $R = \mathbb{Z}$ (a PID), so $K = \mathbb{Q}$ and take $L = \overline{\mathbb{Q}}$ to be an algebraic closure of $\mathbb{Q}$, and let $\overline{\mathbb{Z}}$ be the integral closure of R in L, the ring of all algebraic integers. Then $\overline{\mathbb{Z}}$ is a one-dimensional Prüfer domain that is not Noetherian: in fact, if x is an algebraic integer, then so is $\sqrt{x}$, so $\overline{\mathbb{Z}}$ is not only not atomic but has no irreducible elements whatsoever.

EXAMPLE 20.39. *We give two examples in which the "infinite integral closure" of a Dedekind domain remains Dedekind. The first is quite elementary, while the second requires some number-theoretic background.*

a) *Let l/k be any infinite degree algebraic extension of fields. Put $R := k[t]$, a PID with fraction field $k(t)$. Let $L := l(t)$. Then the integral closure of R in L is $l[t]$, which is not only a Dedekind domain but again a PID.*
b) *Let $R = \mathbb{Z}_p$ be the ring of p-adic integers, with fraction field $\mathbb{Q}_p$. This is a complete DVR with residue field $\mathbb{F}_p$. Let $L := \mathbb{Q}_{p^\infty}$ be the maximal unramified extension of $\mathbb{Q}_p$ (inside some algebraic closure). Then the integral closure T of $\mathbb{Z}_p$ in $\mathbb{Q}_{p^\infty}$ is $\mathbb{Z}_{p^\infty}$, which is a (not complete) DVR with residue field $\overline{\mathbb{F}_p}$, the algebraic closure of $\mathbb{F}_p$. More generally, if R is any complete or even Henselian DVR with a perfect residue field that is neither algebraically closed nor real-closed, then the pasage from R to R^{unr} is an instance of integral closure of a DVR in an infinite degree algebraic field extension that remains a DVR.*

We would now like to give some conditions under which the integral closure of a Dedekind domain in an infinite degree algebraic extension remains a Dedekind domain and also conditions under which it becomes an almost Dedekind domain that is not Dedekind. The latter is perhaps even more interesting to us, because not withstanding our study of almost Dedekind domains in the previous section, we have not yet seen any examples of almost Dedekind domains that are not Dedekind!

We begin with some simple facts about direct and inverse limits. Rather than speaking of a directed system of sets with injective transition maps and its direct limit, it is a bit simpler to speak of a set S that is a **directed union** of a family of subsets $\{S_i\}_{i \in X}$: that is, $S = \bigcup_{i \in X} S_i$ and the family $\{S_i\}$ is, when partially ordered under inclusion, directed: for any S_1, S_2, there is S_3 such that $S_1 \cup S_2 \subseteq S_3$. For a set S, let 2^S denote the set of subsets of S. We claim that when S is the directed union of its subsets $\{S_i\}_{i \in X}$, then we have a natural bijection

$$\Phi : 2^S \to \varprojlim 2^{S_i}.$$

First of all, $\{2^{S_i}\}_{i \in X}$ forms an X-indexed inverse system: if $S_i \subseteq S_j$ then we define

$$\psi_{j,j} : 2^{S_j} \to 2^{S_i}, A_j \subseteq S_j \mapsto A_j \cap S_i.$$

If A is a subset of S, then $\Phi(A) := \{A \cap S_i\}_{i \in X}$ is an element of $\varprojlim 2^{S_i}$. Conversely, given an element $\{A_i\}_{i \in X}$ of $\varprojlim 2^{S_i}$, we may put

$$\Psi(\{A_i\}) := \bigcup_{i \in X} A_i \in 2^S.$$

It is nearly immedidate that Φ and Ψ are mutually inverse bijections, which we may use to identify $2^{\varinjlim S_i}$ with $\varprojlim 2^{S_i}$.

Now suppose that we have a ring R that is the directed union of subrings $\{R_i\}_{i \in X}$. For any ring A, let $\widetilde{\mathcal{I}}(A)$ denote the monoid of ideals of A (including the zero ideal) under multiplication. If we denote the inclusion map $R_i \hookrightarrow R$ by φ_i, then for an ideal I of R, we have $I \cap R_i = \iota_i^*(I)$ is an ideal of R_i. Thus the map Φ above restricted to $\widetilde{\mathcal{I}}(R)$ has image in $\varprojlim \widetilde{\mathcal{I}}(R_i)$.

EXERCISE 20.16. *Let R be a ring that is the directed union of a family of subrings $\{R_i\}_{i \in X}$.*

a) *Show that the restriction of the map $\Phi : 2^R \to \varprojlim 2^{R_i}$ defined above restricts to a bijection*

$$\widetilde{\mathcal{I}}(R) \to \varprojlim \widetilde{\mathcal{I}}(R_i).$$

b) *Let I be an ideal of R. Show: I is prime if and only if $I \cap R_i$ is a prime ideal of R_i for all $i \in X$. Deduce that Φ restricts to a bijection*

$$\operatorname{Spec} R \to \varprojlim \operatorname{Spec} R_i.$$

c) *Suppose that for all $i \in X$ and $\mathfrak{m} \in \operatorname{MaxSpec} R$ we have $\mathfrak{m} \cap R_i \in \operatorname{MaxSpec} R_i$ and that for all i, j with $R_i \subseteq R_j$ and $\mathfrak{m}_j \in \operatorname{MaxSpec} R_j$ we have $\mathfrak{m}_j \cap R_i \in \operatorname{MaxSpec} R_i$. (This holds if each $R_i \subseteq R_j$ is an integral extension of rings: then also each $R_i \subseteq R$ is an integral extension.) Let I be an ideal of R. Show: Φ restricts to a bijection*

$$\operatorname{MaxSpec} R \to \varprojlim \operatorname{MaxSpec} R_i.$$

Now back to work: let R be an almost Dedekind domain with fraction field K, let L/K be an algebraic field extension, and let T be the integral closure of R in L, so T is a one-dimensional Prüfer domain. Let X be the set of finite degree subextensions L_i of L/K and for each $i \in I$, let T_i be the integral closure of R in L_i, so T_i is an almost Dedekind domain by Exercise 20.15, and we have

$$T = \varinjlim T_i$$

and thus

$$\operatorname{MaxSpec} T = \varprojlim \operatorname{MaxSpec} T_i.$$

We want to give conditions for T to be almost Dedekind and conditions for T to be Dedekind. A good starting point is Theorem 20.25, which characterizes Dedekind domains among almost Dedekind domains. We will restate this using a new piece of terminology: a ring R has **finite character** if for any infinite subset S of $\operatorname{MaxSpec} R$ we have $\bigcap_{\mathfrak{m} \in S} \mathfrak{m} = (0)$, or in other words, if for all $x \in R^\bullet$, the set of maximal ideals containing x is finite. (In yet other words, a ring R has finite character if and only if it is residually semilocal: for all nonzero ideals I of R, $\operatorname{MaxSpec} R/I$ is finite.)

Then Theorem 20.25 says that an almost Dedekind domain is Dedekind if and only if it has finite character.

EXERCISE 20.17. *Let $\{S_i\}_{i \in X}$ be an inverse system of nonempty finite sets with surjective transition maps. Show: for all $i \in I$, the natural map $\varprojlim S_i \to S_i$ is surjective.*
(Hint: in the proof of Lemma 15.51 we recalled why the inverse limit of an inverse system of nonempty finite sets is nonempty. Deduce the result from this.)

THEOREM 20.40. *Let R be an almost Dedekind domain with fraction field $K \supsetneq R$, let L/K be an algebraic field extension, and let T be the integral closure of R in L. Let $\{L_i\}_{i \in X}$ be the set of finite degree subextensions L_i of L/K; for $i \in I$, let let T_i be the integral closure of R in L_i. The following are equivalent:*

(i) *The domain T has finite character.*
(ii) *R is Dedekind and for every $\mathfrak{p} \in \operatorname{MaxSpec} R$ there is $N(\mathfrak{p}) \in \mathbb{Z}^+$ such that for all $i \in X$, we have*

$$\#\{\mathcal{P} \in \operatorname{MaxSpec} T_i \mid \mathcal{P} \cap R = \mathfrak{p}\} \leqslant N(\mathfrak{p}).$$

PROOF. Fix $\mathfrak{m} \in \operatorname{MaxSpec} R$. By Exercise 20.15b), for all $i \in X$, the set $M_i(\mathfrak{p})$ of maximal ideals $\mathfrak{P}$ of T_i that contract to $\mathfrak{m}$ is finite and nonempty, and by Exercise 20.16 we have that the set of maximal ideals of T that contract to $\mathfrak{p}$ may be identified with $\varprojlim M_i(\mathfrak{p})$. Here the $M_i(\mathfrak{p})$'s form an X-indexed inverse system of nonempty finite sets with surjective transition maps (the surjectivity is because an integral extension induces a surjection on MaxSpec's), so by Exercise 20.17, for any $\mathfrak{P} \in M_i(\mathfrak{p})$ there is a maximal ideal $\mathcal{P}$ of T that contracts to $\mathfrak{P}$.
(i) $\implies$ (ii): We go by contraposition. First suppose that R is not Dedekind: thus there is an infinite sequence $\{\mathfrak{p}_n\}$ of distinct maximal ideals of R such that $\bigcap_{n \geqslant 1} \mathfrak{p}_n \supsetneq (0)$. By the first paragraph, for each $n \in \mathbb{Z}^+$ we may choose a maximal ideal $\mathcal{P}_n$ of T that contracts to $\mathfrak{p}_n$. Then $\{\mathcal{P}_n\}$ is an infinite sequence of distinct maximal ideals of T such that

$$\bigcap_{n \geqslant 1} \mathcal{P}_n \supseteq \bigcap_{n \geqslant 1} \mathfrak{p}_n \supsetneq (0),$$

so T does not have finite character. Next suppose that there is some $\mathfrak{p} \in \operatorname{MaxSpec} R$ such that for all $N \in \mathbb{Z}^+$ there is $i \in I$ such that the fiber $M_i(\mathfrak{p})$ of $\operatorname{Spec} T_i$ over $\mathfrak{p}$ has at least N elements. By the first paragraph, this means there are at least N elements of $\operatorname{MaxSpec} T$ contracting to $\mathfrak{p}$, and since this holds for all $N \in \mathbb{Z}^+$, the fiber of $\operatorname{MaxSpec} T \to \operatorname{MaxSpec} R$ over $\mathfrak{p}$ is infinite. Then if we intersect all of the maximal ideals in the fiber over $\mathfrak{p}$ we get an ideal containing $\mathfrak{p}$, hence nonzero, so again T does not have finite character.
(ii) $\implies$ (i): Suppose the conditions of (ii) hold. In particular, since R is Dedekind, for all $i \in I$, the ring T_i is the integral closure of a Dedekind domain in a finite degree field extension, so T_i is Dedekind and thus has finite character. Let $\{\mathcal{P}_n\}$ be a countable set of maximal ideals of T with nonzero intersection. Then there is some $i \in X$ and $x \in T_i^\bullet$ such that $x \in \bigcap_n \mathcal{P}_n$. Then $x \in \bigcap_n (\mathcal{P}_n \cap T_i)$, and since T_i has finite character there can be only finitely many distinct maximal ideals $\mathcal{P}_n \cap T_i$, say $\mathfrak{P}_1, \ldots, \mathfrak{P}_N$. For each $1 \leqslant j \leqslant N$, the fibers $M_{i'}(\mathfrak{P}_j)$ with $i' \geqslant i$ form an inverse system of nonempty finite sets of uniformly bounded size with surjective transition maps. Such an inverse system must stabilize: along a cofinal subset, all the transition maps are bijections between finite sets of fixed cardinality, and then

the inverse limit is a finite set of that same cardinality. Thus the pullback map $\operatorname{MaxSpec} T \to \operatorname{MaxSpec} T_i$ restricted to $\{\mathcal{P}_n\}$ has finite image and finite fibers, so the set $\{\mathcal{P}_n\}$ is finite. Thus T has finite character. □

Next we will give a criterion for T to be almost Dedekind. Because T is one-dimensional Prüfer, for $\mathfrak{m} \in \operatorname{MaxSpec} R$ the local ring $R_{\mathfrak{m}}$ is a rank one valuation ring, and we need to know when each $R_{\mathfrak{m}}$ is a DVR.

Let $\mathfrak{P}$ be a maximal ideal of T_i that contracts to the maximal ideal $\mathfrak{p}$ of R. Then $(T_i)_{\mathfrak{P}}$ is a DVR. Let $v_i : L_i^\times \to G_i$ be its valuation, so $\mathcal{P}$ is the set of $x \in T_i$ such that $v(x) > 0$. Let $H := v(K^\times)$. Then

$$(v_i)|_{K^\times} : K^\times \to H$$

is a valuation on K, and the elements of R for which this valuation are positive are precisely $\mathfrak{P} \cap R = \mathfrak{p}$. Thus we get an embedding of DVRs $R_{\mathfrak{p}} \hookrightarrow (T_i)_{\mathfrak{P}}$. Both G and G_i are infinite cyclic groups and G is a subgroup of G_i, so if g_i is a generator for G_i there is a unique $e_i \in \mathbb{Z}^+$ such that $e_i g_i$ is a generator for H. This e_i is called the **ramification index** of $\mathfrak{P}$ over $\mathfrak{p}$, and we say that $\mathfrak{P}|\mathfrak{p}$ **ramifies** if $e_i > 1$. Equivalently, if $\mathfrak{p}_{\mathfrak{p}}$ is the maximal ideal of $R_{\mathfrak{p}}$, then

$$\mathfrak{p}_{\mathfrak{p}}(T_i)_{\mathfrak{P}} = \mathfrak{P}_{\mathfrak{P}}^{e_i}.$$

Now let $\mathcal{P} \in \operatorname{MaxSpec} T$. Then $T_{\mathcal{P}}$ is a rank one valuation ring, so up to isomorphism of ordered groups there is a subgroup G of $(\mathbb{R}, +)$ such that the valuation v on $T_{\mathcal{P}}$ is

$$v : L^\times \to G.$$

Similarly to the above, for $i \in X$, upon restricting v to L_i we get a valuation on L_i whose valuation ring is $(T_i)_{\mathcal{P} \cap T_i}$, and thus the value group G_i is a subgroup of G. Since every element of T lies in some T_i, we have

$$G = \varinjlim G_i.$$

Thus G is a subgroup of $\mathbb{R}$ that is a directed union of infinite cyclic subgroups G_i such that if $G_i \subseteq G_j$ then $[G_j : G_i]$ is finite. It follows that $G \subset H \otimes_{\mathbb{Q}} \cong \mathbb{Q}$. If g_1 is the positive generator for H, then the map $\mathbb{R} \to \mathbb{R}$ by $x \mapsto \frac{x}{g_1}$ is an automorphism of ordered groups under which g_1 maps to 1; after making this rescaling, we have $\mathbb{Z} \subseteq G \subseteq \mathbb{Q}$.

Thus:
• Suppose that the sequence $\{G_i\}_{i \in I}$ stabilizes: there is $i \in I$ such that $G_j = G_i$ for all $j \geqslant i$. Then $G = G_i \cong \mathbb{Z}$ and $T_{\mathcal{P}}$ is a DVR.
• Otherwise, for all $i \in I$ there is $j > i$ such that $G_j \supsetneq G_i$. Then $\mathbb{Z}$ has infinite index in G, so G has no smallest positive element. In this situation we say that $\mathcal{P}|\mathfrak{p}$ is **infinitely ramified**. We say that $\mathfrak{p} \in \operatorname{Spec} R$ is infinitely ramified if some prime $\mathcal{P}$ of T lying over $\mathfrak{p}$ is infinitely ramified. This holds if and only if there is a sequence $i_0 < i_1 < i_2 < \ldots < i_n < \ldots$ in X with $L_{i_0} = K$ and a sequence $\{\mathfrak{p}_n\}_{n=0}^{\infty}$ with $\mathfrak{p}_0 = \mathfrak{p}$ and $\mathfrak{p}_n$ a maximal ideal of T_{i_n} such that for all $n \geqslant 0$, $\mathfrak{p}_{n+1} \cap T_{i_n} = \mathfrak{p}_n$ and $\mathfrak{p}_{n+1}/\mathfrak{p}_n$ is ramified. (Such a sequence defines a maximal ideal $\mathfrak{P}$ of the Prüfer domain $\bigcup_{n \geqslant 0} T_{i_n}$ lying over $\mathfrak{p}$ and such that $\mathfrak{P}/\mathfrak{p}$ is infinitely ramified, and then for any prime $\mathcal{P}$ of T lying over $\mathfrak{P}$ we have that $\mathcal{P}/\mathfrak{p}$ is infinitely ramified.)

We have shown:

PROPOSITION 20.41. *Let R be an almost Dedekind domain with fraction field K, let L/K be an algebraic extension, and let T be the algebraic closure of R in L. Then T is a Prüfer domain if and only if no $\mathfrak{p} \in \operatorname{MaxSpec} R$ is infinitely ramified in T.*

EXERCISE 20.18. *Let R be an almost Dedekind domain with fraction field K, let L/K be an algebraic extension, and let T be the algebraic closure of R in L. Let $\mathcal{P} \in \operatorname{MaxSpec} T$. Show: $\mathcal{P}^2 = \mathcal{P}$ if and only if $\mathcal{P}|(\mathcal{P} \cap R)$ is infinitely ramified.*

EXAMPLE 20.42. *We will show that the ring $R := \overline{\mathbb{Z}}$ of all algebraic integers is* not *an almost Dedekind domain. In fact the ramification is the most extreme possible: let p be any prime number, and let $\mathcal{P}$ be any prime of $\overline{\mathbb{Z}}$ lying over (p). As above, the we may normalize the valuation $v : \overline{\mathbb{Q}}^\times \to G$ such that G is a subgroup of $\mathbb{Q}$ and $v(p) = 1$. Then for all $n \in \mathbb{Z}^+$ the ring R contains the element $p^{\frac{1}{n}}$; since*

$$1 = v(p) = v((p^{\frac{1}{n}})^n) = nv(p^{\frac{1}{n}}),$$

we have $v(p^{\frac{1}{n}}) = \frac{1}{n}$. Thus $G = \mathbb{Q}$. In particular every *maximal ideal $\mathcal{P}$ of R is idempotent: $\mathcal{P}^2 = \mathcal{P}$.*

To go further we need to make use of some algebraic number theory.

PROPOSITION 20.43. *Let R be a Dedekind domain with fraction field K. Suppose that we have a set $\{L_i\}_{i \in X}$ of finite degree separable field extensions of K all lying inside a common algebraic closure $\overline{K}$ such that for every maximal ideal $\mathfrak{p}$ of R, there is at most one $i \in X$ such that $\mathfrak{p}$ ramifies in the integral closure T_i of R in L_i. Let L be the subfield of $\overline{K}$ generated by all the L_i's, and let T be the integral closure of R in L. Then T is an almost Dedekind domain.*

PROOF. Let $\mathfrak{p} \in \operatorname{MaxSpec} R$. If $\mathfrak{p}$ does not ramify in any T_i, then it does not ramify in the integral closure of R in any finite degree subextension of L/K, so the value group at any prime of T lying over $\mathfrak{p}$ is $\mathbb{Z}$. If $\mathfrak{p}$ ramifies in T_i, then every prime $\mathfrak{p}$ of T_i lying over $\mathfrak{p}$ is unramified in T, so every prime of T lying over $\mathfrak{p}$ is finitely ramified. □

For a finite group G, we write $\exp G$ for the least common multiple of all orders of elements of G. When G is commutative, there is always an element of order $\exp G$; in general, this need not be the case: e.g. S_4 has exponent 12 but the largest order of any element of S_4 is 4.

For an algebraic field extension $L/\mathbb{Q}$, we will denote the integral closure of $\mathbb{Z}$ in L by $\mathbb{Z}_L$.

PROPOSITION 20.44. *For each $n \in \mathbb{Z}^+$, let $K_n/\mathbb{Q}$ be a finite Galois extension with Galois group G_n. Suppose that:*

(i) *We have $\frac{\#G_n}{\exp G_n} \geqslant n$; and*

(ii) *There is a prime number p such that for all $n \in \mathbb{Z}^+$, (p) does not ramify in $\mathbb{Z}_{K_n}$.*

Let L be any algebraic extension of $\mathbb{Q}$ containing L_n for all $n \in \mathbb{Z}^+$. Then there are infinitely many maximal ideals of $\mathbb{Z}_L$ lying over (p), so $\mathbb{Z}_L$ is not *Dedekind.*

PROOF. We need the following result from algebraic number theory. Let R be a Dedekind domain with fraction field K, let L/K be a finite Galois extension of degree n, let S be the integral closure of R in L, and let $\mathfrak{p} \in \operatorname{MaxSpec} R$. There are unique $e, f, g \in \mathbb{Z}^+$ such that:
I. $\mathfrak{p}S = \mathfrak{P}_1^e \cdots \mathfrak{P}_g^e$ for distinct maximal ideals $\mathfrak{P}_1, \ldots, \mathfrak{P}_g$;
II. For all $1 \leqslant i \leqslant g$, we have $[S/\mathfrak{P}_i : R/\mathfrak{p}] = f$; and
III. We have $efg = [L : K] = \#G$.
Thus $\mathfrak{p}$ is unramified in S if and only if $e = 1$. Suppose $R = \mathbb{Z}$ and that $\mathfrak{p} = (p)$ is unramified in $S = \mathbb{Z}_K$, so $fg = \#G$. Then there is an element $\sigma_p \in G$, well-determined up to conjugacy, such that f is equal to the order of the element σ_p in the finite group G. (This element σ_p is called a *Frobenius element*, but we don't need to know anything else about it than what we've just said.) Therefore $f \mid \exp(G)$, so $g = \frac{\#G}{f}$ is diviisble by $\frac{\#G}{\exp G}$. Our hypotheses therefore for all $n \in \mathbb{Z}^+$ there are at least $\frac{\#G_n}{\exp G_n} \geqslant n$ maximal ideals of $\mathbb{Z}_{K_n}$ lying over (p). Since $\mathbb{Z}_{K_n} \hookrightarrow \mathbb{Z}_L$ is an integral extension, the map $\operatorname{MaxSpec} \mathbb{Z}_L \to \operatorname{MaxSpec} \mathbb{Z}_{K_n}$ is surjective, for all $n \in \mathbb{Z}^+$ there are at least n maximal ideals of $\mathbb{Z}_L$ lying over (p), or in other words there are infintiely many maximal ideals of $\mathbb{Z}_L$ lying over (p), so $\mathbb{Z}_L$ does not have finite character and therefore is not Dedekind. □

For a student of algebraic number theory it is not a particularly difficult exercise to find an infinite degree algebraic extension $L/\mathbb{Q}$ such that Proposition 20.29 applies to show that $\mathbb{Z}_T$ is almost Dedekind and Proposition 20.30 applies to show that $\mathbb{Z}_T$ is not Dedekind. In fact the most natural example is the one given already by N. Nakano in [**Na53**], which was the first construction of an almost Dedekind domain that is not Dedekind.

THEOREM 20.45 (Nakano). *For a prime number p, let $\zeta_p \in \overline{\mathbb{Q}}$ be a primitive pth root of unity. Let L be the field extension of $\mathbb{Q}$ generated by ζ_p for all primes p. Then $\mathbb{Z}_L$ is an almost Dedekind domain that is not Dedekind.*

PROOF. Note that $\zeta_2 = -1$, so $\mathbb{Q}(\zeta_2) = \mathbb{Q}$. For $p > 3$, the number field $\mathbb{Q}(\zeta_p)$ has degree $p - 1$, and p is the unique prime of $\mathbb{Z}$ that ramifies in $\mathbb{Z}_{\mathbb{Q}(\zeta_p)}$. Thus no prime ℓ ramifies in $\mathbb{Z}_{\mathbb{Q}(\zeta_p)}$ for more than one prime p and the prime 2 does not ramify in any $\mathbb{Z}_{\mathbb{Q}(\zeta_p)}$. So Proposition 20.29 implies that $\mathbb{Z}_L$ is almost Dedekind.

Order the primes $2 = p_1 < p_2 < p_3 < \ldots < p_n < \ldots$. For $n \geqslant 2$, put

$$K_n := \mathbb{Q}(\zeta_{p_2}, \ldots, \zeta_{p_{n+1}}) = \mathbb{Q}(\zeta_{p_2 \cdots p_{n+1}}).$$

Then $K_n/\mathbb{Q}$ is Galois with group $G_n := (\mathbb{Z}/(p_2 \cdots p_{n+1})\mathbb{Z})^\times \cong \prod_{i=2}^{n+1} (\mathbb{Z}/p_i\mathbb{Z})^\times$. So

$$\#G_n = \prod_{i=2}^{n+1} (p_i - 1).$$

Each group $(\mathbb{Z}/p_i\mathbb{Z})^\times$ is cyclic of order $p - 1$, so

$$\exp G_n = \operatorname{lcm}(p_2 - 1, \ldots, p_{n+1} - 1).$$

Because for all $2 \leqslant i \leqslant n + 1$ the number $p_i - 1$ is even, we get

$$\frac{\#G_n}{\exp G_n} \geqslant 2^n \geqslant n.$$

Moreover (2) does not ramify in any K_n. So Proposition 20.30 implies that $\mathbb{Z}_L$ is not Dedekind. □

EXERCISE 20.19. *Let L be the field of Theorem 20.30. Show: for evey prime number p, there are infinitely many maximal ideals of $\mathbb{Z}_L$ lying over (p).*

THEOREM 20.46. *(Kaplansky [**K**]) Let R be a Dedekind domain with fraction field K, and let $\overline{K}$ be an algebraic closure of K. Suppose that for every finite extension L/K, the Picard group of the integral closure R_L of R in L is a torsion commutative group. Then the integral closure S of R in $\overline{K}$ is a Bézout domain.*

PROOF. Let $I = \langle a_1, \ldots, a_n \rangle$ be a finitely generated ideal of S. Then $L = K[a_1, \ldots, a_n]$ is a finite extension of K. Let R_L be the integral closure of R in L, and let $I_L = \langle a_1, \ldots, a_n \rangle_{R_L}$. By hypothesis, there exists $k \in \mathbb{Z}^+$ and $b \in R_L$ such that $I_L^k = bR_L$. Let c be a kth root of b in S and let $M = L[c]$. Thus in the Dedekind domain R_M we have $(I_L R_M)^k = (c^k)$, and from unique factorization of ideals we deduce $I_L R_M = cR_M$. Thus $I = I_L R_M S = cR_M S = cS$ is principal. □

Recall the basic fact of algebraic number theory that for any number field K, the Picard group of $\mathbb{Z}_K$ is finite. This shows that the ring $R = \mathbb{Z}$ satisfies the hypotheses of Theorem 20.46. We deduce that the ring of all algebraic integers $\overline{\mathbb{Z}}$ is a Bézout domain: Theorem 5.1.

EXERCISE 20.20. *Adapt the proof of Theorem 20.46 to show that the Picard group of the ring of integers of the maximal solvable extension $\mathbb{Q}^{\mathrm{solv}}$ of $\mathbb{Q}$ is trivial.*

EXERCISE 20.21. *State a function field analogue of Theorem 5.1 and deduce it as a special case of Theorem 20.46.*

We quote without proof two more results on Picard groups of integer rings of infinite algebraic extensions of $\mathbb{Q}$.

THEOREM 20.47. *(Brumer [**Br81**]) Let $\mathbb{Q}^{\mathrm{cyc}} = \bigcup_{n \in \mathbb{Z}^+} \mathbb{Q}(\zeta_n)$ be the field obtained by adjoining to $\mathbb{Q}$ all roots of unity, and let $\mathbb{Z}^{\mathrm{cyc}}$ be its ring of integers, i.e., the integral closure of $\mathbb{Z}$ in $\mathbb{Q}^{\mathrm{cyc}}$. Then*

$$\operatorname{Pic} \mathbb{Z}^{\mathrm{cyc}} \cong \bigoplus_{i=1}^{\infty} \mathbb{Q}/\mathbb{Z}.$$

THEOREM 20.48. *(Kurihara [**Ku99**]) Let $\mathbb{Q}^{\mathrm{cyc}\,+} = \bigcup_{n \in \mathbb{Z}^+} \mathbb{Q}(\zeta_n + \zeta_n^{-1})$ be the maximal real subfield of $\mathbb{Q}^{\mathrm{cyc}}$, and let $\mathbb{Z}^{\mathrm{cyc}\,+}$ be its ring of integers, i.e., the integral closure of $\mathbb{Z}$ in $\mathbb{Q}^{\mathrm{cyc}\,+}$. Then*

$$\operatorname{Pic} \mathbb{Z}^{\mathrm{cyc}\,+} = 0.$$

CHAPTER 21

Structure of Overrings

Let R be a domain with fraction field K. . By an **overring** of R we mean a subring of K containing R, i.e., a ring T with $R \subset T \subset K$. (We allow equality.) This is standard terminology among commutative algebraists, but we warn that someone who has not heard it before will probably guess incorrectly at its meaning: one might well think that "T is an overring of R" would simply mean that "R is a subring of T".

We are interested in particular in the following:

QUESTION 5. *Let R be a domain.*

a) *Can we (in some sense) classify the overrings of R?*
b) *Under what conditions is every overring of R a localization?*
c) *Let T be an overring of R. What is the relationship between* $\operatorname{Pic} T$ *and* $\operatorname{Pic} R$*?*

As a warmup, suppose R is a PID. In this case every overring is indeed a localization: to see this it is enough to show that for all coprime $x, y \in R^\bullet$, $\frac{1}{y} \in R[\frac{x}{y}]$. But since x and y are coprime in the PID R, there are $a, b \in R$ such that $ax + by = 1$, and then $\frac{1}{y} = \frac{ax+by}{y} = a\left(\frac{x}{y}\right) + b \in R[\frac{x}{y}]$. It follows that every overring of a PID is obtained by localizing at a multiplicative subset $S \subset R^\bullet$. Further, by uniqueness of factorization the saturated multiplicatively closed subsets of $R^\bullet$ are in bijection with subsets of $\operatorname{MaxSpec} R$: in other words, an overring is entirely determined by the set of prime elements we invert, and inverting different sets of prime elements leads to distinct overrings. Further, since a localization of a PID is a again a PID, in this case we have $\operatorname{Pic} T = 0$ for all overrings.

We will give satisfactory answers to Question 5 for any Dedekind domain. Some of the theory of overrings of Dedekind domains seems most naturally to be deduced from the structure of overring of Prüfer domains. Indeed, we will give two more characteristic properties of Prüfer domains in terms of Dedekind domains: a domain R is Prüfer if and only if every overring T is a flat R-module if and only if every overring T is integrally closed.

Our discussion of Picard groups of overrings of Dedekind domains includes the notion of **elasticity**, which is an active topic in recent and contemporary factorization theory. We will also use our study of Picard groups of overrings to prove a celebrated theorem of Claborn: every commutative group whatseover is (up to isomorphism) the ideal class group of some Dedekind. Claborn's original proof involves Krull domains, which we have not yet discussed, so we will give a more recent proof due to the present author.

1. Flatness of Overrings

Let T be an overring of R. Whether T is flat (as an R-module) turns out be a key question in the structure and classification of overrings, so we begin with some characterizations of this. For ideals I and J of R, we put

$$(I :_J J) := \{x \in R \mid xJ \subseteq I\}.$$

Here the subscripted R is meant to differentiate from the colon ideal construction for *fractional ideals*, as considered e.g. in Chapter 19.

EXERCISE 21.1. *Let $\iota : R \to T$ be a ring homomorphism, and let $I_1, \ldots, I_n$ be ideals of R. Show: if $\iota_*(I_i) = T$ for all $1 \leqslant i \leqslant n$, then $\iota_*(\bigcap_{i=1}^n I_i) = T$.*
(Hint: for each $1 \leqslant j \leqslant n$, write $1 = C_j$, where C_j is a finite I_j-linear combination of elements of T; then $1 = \prod_{j=1}^n C_j$.)

THEOREM 21.1. *For an overring T of a domain R, the following are equivalent:*

(i) *For all $\mathfrak{p} \in \operatorname{Spec} R$, we have either $\mathfrak{p}T = T$ or $T \subseteq R_{\mathfrak{p}}$.*
(ii) *For all $x, y \in R^\bullet$ such that $\frac{x}{y} \in T$, we have $((y) :_R (x))T = T$.*
(iii) *T is a flat R-module.*

PROOF. (i) $\implies$ (ii): We go by contraposition: suppose there are $x, y \in R^\bullet$ such that $\frac{x}{y} \in T$ and $((y) :_R (x))T \neq T$. There is a maximal ideal $\mathcal{M}$ of T containing $((y) :_R (x))$, and then $\mathfrak{p} := \mathcal{M} \cap R$ is a prime ideal containing $((y)_R : (x))$ such that $\mathfrak{p}T \subsetneq T$. Thus if (i) were to hold we would have $T \subseteq R_{\mathfrak{p}}$, so $\frac{x}{y} \in R_{\mathfrak{p}}$. This gives $\frac{x}{y} = \frac{a}{s}$ for $a \in R$ and $s \in R \backslash \mathfrak{p}$ so $xs = ya$ and thus $s \in ((y) :_R (x)) \subseteq \mathfrak{p}$: contradiction. So condition (i) does not hold.
(ii) $\implies$ (i): Suppose (ii) holds, and let $\mathfrak{p} \in \operatorname{Spec} R$ be such that $\mathfrak{p}T \subsetneq T$. Let $x, y \in R^\bullet$ be such that $\frac{x}{y} \in T$. Then $((y) :_R (x))T = T$, so $((y)) :_R (x))$ is not contained in $\mathfrak{p}$. Let $s \in ((y) :_R (x)) \backslash \mathfrak{p}$, so there is $a \in R$ such that $sx = ay$ and then $\frac{x}{y} = \frac{a}{s} \in R_{\mathfrak{p}}$. It follows that $T \subseteq R_{\mathfrak{p}}$.
(ii) $\implies$ (iii): Suppose (ii) holds. By the Tensorial Criterion for Flatness, it suffices to show that for an ideal I of R, the homomorphism $\varphi : I \otimes_R T \to T$ given by $a \otimes b \mapsto ab$ is injective. Let $c \in I \otimes_R T$; we may write $c = \sum_{i=1}^n a_i \otimes b_i$ with $a_i \in I$ and $b_i \in T$. There are $b, c_1, \ldots, c_s \in R$ such that for $1 \leqslant i \leqslant s$ we have $b_i = \frac{c_i}{b}$, so

$$c = \sum_{i=1}^n a_i \otimes \frac{c_i}{b}.$$

By our assumption, for all $1 \leqslant i \leqslant n$ we have $((b) :_R (c_i))T = T$, so if

$$C := \bigcap_{i=1}^n ((b) :_R (c_i)).$$

then Exercise 21.1 gives $CT = T$. Suppose now that $\varphi(c) = 0$, i.e., $\sum_{I=1}^n a_i \frac{c_i}{b} = 0$. For $d \in C$ we have $d\frac{c_i}{b} \in R$ for all $1 \leqslant i \leqslant n$, so

$$dc = \sum_{i=1}^s a_i \otimes d\frac{c_i}{b} = \sum_{I=1}^n da_i \frac{c_i}{b} \otimes 1 = \left(d \sum_{i=1}^n a_i \frac{c_i}{b} \right) \otimes 1 = 0.$$

It follows that $Cc = 0$. Write $1 = \sum_{i=1}^N a_i t_i$ with $a_i \in C$ and $t_i \in T$. Then

$$c = c \cdot 1 = c \cdot (\sum_i a_i t_i) = \sum_i (a_i c) t_i = \sum_i 0 \cdot t_i = 0.$$

(iii) $\implies$ (i): Suppose T is a flat R-module. Let $x, y \in R^\bullet$ be such that $\frac{x}{y} \in T$. Applying the Equational Criterion for Flatness to the linear equation $y(\frac{x}{y}) - x(1) = 0$, there are elements $\{b_{jk}\}_{1 \leqslant j \leqslant r, 1 \leqslant k \leqslant 2}$ and $y_1, \ldots, y_r \in T$ such that

$$\frac{x}{y} = \sum_{j=1}^{r} y_j z_{j,1}$$

$$1 = \sum_{j=1}^{r} y_j b_{j,2}$$

and

$$\forall 1 \leqslant j \leqslant r,\ b_{j,1} y - b_{j,2} x = 0.$$

Let $\mathfrak{p} \in \operatorname{Spec} R$. If for all $1 \leqslant j \leqslant r$ we have $b_{j,2} \in \mathfrak{p}$, then $\mathfrak{p}T = T$ and we're done. Otherwise, for all $\frac{x}{y} \in T$, there is some j such that $b_{j,2} \notin \mathfrak{p}$, and then $b_{j,2} \in ((y) :_R (x))$, so $((y) :_R (x))$ is not contained in $\mathfrak{p}$, so there is $s \in R \backslash \mathfrak{p}$ and $a \in R$ such that $sx = ay$, so $\frac{x}{y} = \frac{a}{s} \in R_\mathfrak{p}$ and thus $T \subseteq R_\mathfrak{p}$. □

Proposition 21.2. *Let R be a domain with fraction field K and consider rings $R \subset T \subset T' \subset K$.*

a) *If T' is flat over R, then T' is flat over T.*
b) *If T' is flat over T and T is flat over R, then T' is flat over R.*

Proof. a) Suppose T' is flat over R. Let $a, b \in T$ be such that $\frac{a}{b} \in T'$. Write $a = \frac{c}{s}$, $b = \frac{d}{s}$ with $c, d, s \in R$. Then $\frac{c}{d} \in T'$, so by Theorem 21.1, $((d) : (c))T' = T'$. Hence $1 = t_1 u_1 + \ldots + t_k u_k$ for some $t_i \in T'$ and $u_i \in R$ with $u_i c \in (d)$ for all i. Then there is $z_i \in R$ such that $u_i c = d z_i$, so $u_i a = z_i \frac{d}{s} = z_i b \in Tb$ for all i. So $(Tb : Ta)T' = T'$. Applying Theorem 21.1 again, we get that T' is flat over T.
b) This holds for any $R_1 \subset R_2 \subset R_3$, since $M \otimes_{R_1} R_3 \cong (M \otimes_{R_1} R_2) \otimes_{R_2} R_3$. □

Theorem 21.3. *(Richman [**Ri65**]) For an overring T of a domain R, the following are equivalent:*

(i) *The ring T is flat over R.*
(ii) *For all $\mathcal{P} \in \operatorname{MaxSpec} T$, we have $T_\mathcal{P} = R_{\mathcal{P} \cap R}$.*
(iii) *$T = \bigcap_{\mathcal{P} \in \operatorname{MaxSpec} T} R_{\mathcal{P} \cap R}$.*

Proof. (i) $\implies$ (ii): Suppose that T is flat over R, let $\mathcal{P} \in \operatorname{MaxSpec} T$ and let $\mathfrak{p} := \mathcal{P} \cap R$. Clearly $R_\mathfrak{p} \subseteq T_\mathcal{P}$. Let $\frac{x}{y} \in T_\mathcal{P}$ with $x, y \in T^\bullet$ and $y \in T \backslash \mathcal{P}$. Then there are $u, v, s \in R^\bullet$ such that $x = \frac{u}{s}$ and $y = \frac{v}{s}$. Put

$$C := ((s) :_R (u)) \cap ((s) :_R (v)).$$

By Theorem 21.1 and Exercise 21.1 we have $CT = T$, so C is *not* contained in $\mathfrak{p}$. Let $z \in C \backslash \mathfrak{p}$. Then $zx, zy \in R$ and $zy \notin \mathcal{P}$, so $zy \notin \mathfrak{p}$. Thus $\frac{x}{} = \frac{zx}{zy} \in R_\mathfrak{p}$, so $T_\mathcal{P} \subseteq R_\mathfrak{p}$.
(ii) $\implies$ (iii): Suppose (ii) holds. By Corollary 7.16 we have

$$T = \bigcap_{\mathcal{P} \in \operatorname{MaxSpec} T} T_\mathcal{P} = \bigcap_{\mathcal{P} \in \operatorname{MaxSpec} T} R_{\mathcal{P} \cap R}.$$

(iii) $\implies$ (i): Suppose (iii) holds, and let $\mathfrak{p} \in \operatorname{Spec} R$ be such that $\mathfrak{p}T \subsetneq T$. Then there is $\mathcal{P} \in \operatorname{MaxSpec} T$ such that $\mathfrak{p}T \subseteq \mathcal{P}T$ and $\mathfrak{p} \subseteq \mathcal{P} \cap R$, so $R_{\mathcal{P} \cap R} \subseteq R_\mathfrak{p}$. But by our assumption we also have $T \subseteq R_{\mathcal{P} \cap R}$, so $T \subseteq R_\mathfrak{p}$. By Theorem 21.1, T is flat over R. □

For a domain R and a multiplicative subset S of R, we know that $S^{-1}R$ is a flat overring of R. We will see later on that the converse is false: there are even Dedekind domains in which not every overring is a localization. Richman's Theorem however gives a kind of weak converse: every flat overring of a domain is obtained by intersecting localizations of R of the form $R_{\mathfrak{p}}$ for $\mathfrak{p} \in \operatorname{Spec} R$. According to [**Ri65**, p. 796], the converse of *this* is false: namely, for a domain R and a subset $X \subseteq \operatorname{Spec} R$, the overring $\bigcap_{\mathfrak{p} \in X} R_{\mathfrak{p}}$ need not be flat. In truth we will not see this: for most of the remainder of this chapter we will palce ourselves in a situation in which *all* overrings are flat.

PROPOSITION 21.4. *Let T be an overring of a domain R that is both integral and flat over R. Then $R = T$.*

PROOF. Let $x, y \in R^\bullet$ be such that $\frac{x}{y} \in T$. Then by Theorem 21.1, we have $((y) :_R (x))T = T$. Let $\mathfrak{p} \in \operatorname{MaxSpec} R$. By Theorem 14.16, there exists a prime (in fact maximal by Corollary 14.19, but this is not needed here) ideal $\mathcal{P}$ of T lying over $\mathfrak{p}$. Since $\mathfrak{p}T \subset \mathcal{P}$, we have $\mathfrak{p}T \subsetneq T$. Therefore $((y) : (x))$ is not contained in any maximal ideal of R, so $((y) : (x)) = R$. It follows that $x \in (y)$, i.e., $x = ay$ for some $a \in R$, so that $\frac{x}{y} \in R$. Thus $R = T$. □

2. Overrings of Prüfer Domains

THEOREM 21.5. *For a domain R, the following are equivalent:*

(i) *Every overring of R is a Prüfer domain.*
(ii) *R is a Prüfer domain.*
(iii) *Every overring of R is flat.*
(iv) *Every overring of R is integrally closed.*

PROOF. (i) $\implies$ Since R itself is an overring of R, this is immediate.
(ii) $\implies$ (iii): Suppose R is Prüfer, and let T be an overring of R. Then T is a torsionfree R-module, so by Theorem 20.31, T is a flat R-module.
(iii) $\implies$ (i): Suppose every overring of R is flat over R, and let T be an overring of R. By Proposition 22.3a), every overring of T is flat over T. So it is enough to show that R is Prüfer, for then T is Prüfer for the same reason. For this it suffices to show that for $\mathfrak{m} \in \operatorname{MaxSpec} R$, the ring $R_{\mathfrak{m}}$ is a valuation ring. By Proposition 21.2, every overring of $R_{\mathfrak{m}}$ is flat. Suppose that $x, y \in R_{\mathfrak{m}}^\bullet$ are such that $\frac{x}{y} \notin R$. We want to show that $\frac{y}{x} \in R$.

By Proposition 21.4, it is enough to show that $\frac{y}{x}$ is integral over R. Because $\frac{x}{y} \notin R$ we have that $1 \notin ((y) :_R (x))$ and thus $((y) :_R ((x)) \subseteq \mathfrak{m}$. Since $R[\frac{x}{y}]$ is flat over R, by Theorem 21.1 we have $((y) :_R ((x))R[\frac{x}{y}] = R[\frac{x}{y}]$ and thus that $\mathfrak{m}R[\frac{x}{y}] = R[\frac{x}{y}]$. This means that there is $n \in \mathbb{Z}^+$ and $a_0, \ldots, a_n \in \mathfrak{m}$ such that

$$a_n \frac{x^n}{y^n} + \ldots + a_1 \frac{x}{y} + a_0 = 1,$$

so

$$(a_0 - 1)(\frac{y}{x})^n + a_1(\frac{y}{x})^{n-1} + \ldots + a_{n-1}\frac{y}{x} + a_n = 0.$$

Because $a_0 \in \mathfrak{m}$ and $(R, \mathfrak{m})$ is a local ring, we have $a_0 - 1 \in \mathfrak{m}^\times$, and dividing by $a_0 - 1$ shows that $\frac{y}{x}$ is integral over R, as desired.
(i) $\implies$ (iv): This is immediate from Proposition 20.38: Prüfer domains are integrally closed.

(iv) $\implies$ (ii): Suppose that every overring of R is integrally closed. To show that R is Prüfer, it suffices to show that for all $\mathfrak{m} \in \operatorname{MaxSpec} R$, the local ring $R_{\mathfrak{m}}$ is a valuation ring. Let K be the fraction field of $R_{\mathfrak{m}}$, and let $x \in K^\bullet$. Then $R_{\mathfrak{m}}[x^2]$ must be integrally closed and x is integral over $R_{\mathfrak{m}}[x^2]$, so $x \in R_{\mathfrak{m}}[x^2]$: that is, there are $a_0, \ldots, a_n \in R_{\mathfrak{m}}$ such that $x = \sum_{i=0}^n a_i x^{2i}$. Lemma 20.36 now applies to show that one of x and x^{-1} lies in $R_{\mathfrak{m}}$, so $R_{\mathfrak{m}}$ is a valuation ring. □

COROLLARY 21.6. *Let R be a domain that is not a field.*

a) *If R is almost Dedekind, then so is every overring of R.*

b) *If R is Dedekind, then so is every overring of R.*

PROOF. a) A Prüfer domain is almost Dedekind if and only if the localization at every maximal ideal is a DVR, so suppose that R is almost Dedekind and let T be an overring of R, which we may of course assume is not a field. Since R is Prüfer, T is flat and thus by Theorem 21.3 for every $\mathcal{P} \in \operatorname{MaxSpec} T$ we have $T_{\mathcal{P}} = R_{\mathcal{P} \cap R}$ is (not a field hence) a DVR.

b) Let T be an overring of the Dedekind domain R. By part b), T is almost Dedekind. By Krull-Akizuki, T is Noetherian, so T is Dedekind. □

THEOREM 21.7. *Let R be a Prüfer domain, let T be an overring of R, and put*

$$W = \{\mathfrak{p} \in \operatorname{Spec}(R) \mid \mathfrak{p}T \subsetneq T\}.$$

Then $T = \bigcap_{\mathfrak{p} \in W} R_{\mathfrak{p}}$.

PROOF. For $\mathcal{P} \in \operatorname{MaxSpec} T$, let us put $\mathfrak{p}_{\mathcal{P}} := \mathcal{P} \cap R$. By Theorems 22.6 and 22.4, we have

$$T = \bigcap_{\mathcal{P} \in \operatorname{MaxSpec} T} R_{\mathfrak{p}_{\mathcal{P}}}.$$

Every prime ideal $\mathfrak{p}_{\mathcal{P}}$ lies in W, so

$$\bigcap_{\mathfrak{p} \in W} R_{\mathfrak{p}} \subseteq \bigcap_{\mathcal{P} \in \operatorname{MaxSpec} T} R_{\mathfrak{p}_{\mathcal{P}}} = T.$$

Conversely, if $\mathfrak{p} \in W$, then there is $\mathcal{P} \in \operatorname{MaxSpec} T$ such that $\mathfrak{p} \subseteq \mathfrak{p}_{\mathcal{P}}$, and then

$$R_{\mathfrak{p}_{\mathcal{P}}} \subseteq R_{\mathfrak{p}},$$

so

$$T = \bigcap_{\mathcal{P} \in \operatorname{MaxSpec} T} R_{\mathfrak{p}_{\mathcal{P}}} \subseteq \bigcap_{\mathfrak{p} \in W} R_{\mathfrak{p}}.$$ □

For a Prüfer domain R with fraction field K and a subset W of $\operatorname{Spec} R$, let us put

$$R_W := \bigcap_{\mathfrak{p} \in W} R_{\mathfrak{p}} \text{ and } R^W := \bigcap_{\mathfrak{p} \in \operatorname{Spec} R \setminus W} R_{\mathfrak{p}}.$$

Notice that for $\mathfrak{p} \in \operatorname{Spec} R$, we have $R_{\{\mathfrak{p}\}} = R_{\mathfrak{p}}$; we will also put

$$R^{\mathfrak{p}} := R^{\{\mathfrak{p}\}} = \bigcap_{\mathfrak{q} \in \operatorname{Spec} R \mid \mathfrak{q} \neq \mathfrak{p}} R_{\mathfrak{q}}.$$

Then Theorem 22.8 asserts that $W \mapsto R_W$ is a surjective map from $2^{\operatorname{Spec} R}$ to the set $\operatorname{Over}(R)$ of overrings of R. It is natural to ask whether this map must be injective as well. There is a silly reason why it cannot be: the reasonable interpretation of $R_\varnothing$ is K, but also $R_{\{(0)\}} = K$. So we should avoid the zero ideal. More generally, if $\dim R \geqslant 2$ injectivity will still fail: if to any subset W_1 of $\operatorname{MaxSpec} R$ we adjoin

any subset W_2 of prime ideals such that each element of W_2 is contained in some element of W_1, then we have $R_{W_1} = R_{W_1 \cup W_2}$. So a more meaningful version of this question concerns maximal ideals only.

LEMMA 21.8. *For a Prüfer domain R, the following are equivalent:*

(i) *The map $W \mapsto R_W$ gives an injection $2^{\operatorname{MaxSpec} R} \to \operatorname{Over}(R)$.*

(ii) *For all $\mathfrak{p} \in \operatorname{MaxSpec}$ we have $R^{\mathfrak{p}} \supsetneq R$.*

PROOF. (i) $\implies$ (ii): Suppose that (i) holds. Since $R^{\mathfrak{p}} = R_{\operatorname{MaxSpec} R \setminus \mathfrak{p}}$ and $R = R_{\operatorname{MaxSpec} R}$, this is immediate.
(ii) $\implies$ (i): Suppose that (ii) holds. Let W_1 and W_2 be distinct subsets of $\operatorname{MaxSpec} R$. After interchanging W_1 and W_2 if necessary, we may choose $\mathfrak{p} \in W_1 \setminus W_2$, and then

$$R^{\mathfrak{p}} \subseteq R_{W_2},$$

but since $R_{W_1} \subseteq R_{\mathfrak{p}}$, if we had $R^{\mathfrak{p}} \subseteq R_{W_1}$ then we would have $R^{\mathfrak{p}} \subseteq R_{\mathfrak{p}}$ and thus $R^{\mathfrak{p}} \subseteq R^{\mathfrak{p}} \cap R_{\mathfrak{p}} = R$, contradicting (ii). So $R^{\mathfrak{p}}$ is *not* contained in R_{W_1} and thus $R_{W_1} \neq R_{W_2}$. □

3. Overrings of Dedekind Domains

3.1. Classification of Overrings. The equivalent conditions of Lemma 21.8 *do not* hold in all Prüfer domains. In [**Gi66**], Gilmer analyzes these conditions. He shows in particular: (i) they do not hold in any almost Dedekind domain that is not a Dedekind domain, and (ii) they hold in a one-dimensional Prüfer domain if and only if every maximal ideal is the radical of a finitely generated ideal. The latter certainly implies that these conditions hold in any Dedekind domain, which we will now show. Indeed we may just as easily prove a slightly stronger result. Recall that for a maximal ideal $\mathfrak{p}$ of a Dedekind domain R with fraction field $K \supsetneq R$, we have a discrete valuation $v_{\mathfrak{p}} : K^\times \to \mathbb{Z}$: for $x \in K^\times$, we define $v_{\mathfrak{p}}(x)$ to be the power to which $\mathfrak{p}$ appears in the prime factorization of the fractional ideal (x).

PROPOSITION 21.9. *Let R be a Dedekind domain that is not a field. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$ be distinct maximal ideals of R, and let $a_1, \ldots, a_n \in \mathbb{Z}$. Then there is $x \in K^\bullet$ such that for all $1 \leqslant i \leqslant n$ we have $v_{\mathfrak{p}_i}(x) = a_i$ and $v_{\mathfrak{q}}(x) \geqslant 0$ for all $\mathfrak{q} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$.*

PROOF. Step 1: By CRT, for any $b_1, \ldots, b_n \in \mathbb{N}$ there is $x \in R^\bullet$ such that $v_{\mathfrak{p}_i}(x) = b_i$ for all $1 \leqslant i \leqslant n$: indeed CRT implies that the natural map $R \to \prod_{i=1}^n R/\mathfrak{p}_i^{b_i+1}$ is surjective, so there is $x \in R$ that maps into $\mathfrak{p}_i^{b_i} \setminus \mathfrak{p}_i^{b_i+1}$.
Step 2: Put $a := \max_{1 \leqslant i \leqslant n} |a_i|$. By Step 1, there is $y \in R$ such that for all $1 \leqslant i \leqslant n$ we have $v_{\mathfrak{p}_i}(y) = a$, hence $v_{\mathfrak{p}_i}(\frac{1}{y}) = -a$. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_m$ be the set of maximal ideals $\mathfrak{q} \notin \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$ such that $v_{\mathfrak{q}}(\frac{1}{y}) < 0$. (The set of such maximal ideals is certainly finite, but may be empty: i.e., we can have $m = 0$.) For $1 \leqslant i \leqslant n$, put $b_i := a + a_i \in \mathbb{N}$. By Step 1 applied to the set $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_n, \mathfrak{q}_1, \ldots, \mathfrak{q}_m\}$, there is $z \in R$ such that for all $1 \leqslant i \leqslant n$ we have $v_{\mathfrak{p}_i}(z) = b_i$ and for all $1 \leqslant j \leqslant m$ we have $v_{\mathfrak{q}_j}(z) = -v_{\mathfrak{q}_j}(\frac{1}{y})$. Then $x := \frac{z}{y}$ is the desired element. □

So if R is a Dedekind domain that is not a field and $\mathfrak{p} \in \operatorname{MaxSpec} R$, by Proposition 22.9 there is $x \in K^\times$ such that $v_{\mathfrak{p}}(x) = -1$ and $v_{\mathfrak{q}}(x) \geqslant 0$ for all other maximal ideals $\mathfrak{q}$. Then $x \in R^{\mathfrak{p}} \setminus R$. We deduce the following classification of overrings of a Dedekind domain:

THEOREM 21.10. *Let R be a Dedekind domain.*

a) *The map $2^{\operatorname{MaxSpec} R} \to \operatorname{Over}(R)$ given by $W \mapsto R_W = \bigcap_{\mathfrak{p} \in W} R_{\mathfrak{p}}$ is a bijection.*

b) *Let $\iota : R \hookrightarrow T$ be an overring of R, and let*

$$W := \{\mathfrak{p} \in \operatorname{MaxSpec} R \mid \mathfrak{p}T \subsetneq T\}.$$

Then:

(i) *We have $T = R_W$.*

(ii) *For all $\mathcal{P} \in \operatorname{MaxSpec} T$ we have $\iota_* \iota^*(\mathcal{P}) = \mathcal{P}$.*

(iii) *The map $\iota^* : \operatorname{MaxSpec} T \to \operatorname{MaxSpec} R$ is injective with image W.*

PROOF. We may assume that R is not a field. Let $\iota : R \hookrightarrow T$ be an overring of R, and let W be the set of maximal ideals $\mathfrak{p}$ of R such that $\mathfrak{p}T \subsetneq T$. By Theorem 22.8, we have that $T = R_W \cap R_{(0)}$, but since $R_{(0)} = K$, we also have $T = R_W$. This shows that the map $W \mapsto R_W$ is surjective onto the set of overrings of R. By Proposition 22.9, for any $\mathfrak{p} \in \operatorname{MaxSpec} R$ there is $x \in K$ with $v_{\mathfrak{p}}(x) = -1$ and $v_{\mathfrak{q}}(x) \geqslant 0$ for all maximal ideals $\mathfrak{q} \neq \mathfrak{p}$, so by Lemma 21.8 the map $W \mapsto R_W$ is injective. If $\mathcal{P} \in \operatorname{MaxSpec} R$, then by Theorem 22.4 we have $T_{\mathcal{P}} = R_{\mathcal{P} \cap R}$. Since T is not a field, neither is $T_{\mathcal{P}}$, so $\mathcal{P} \cap R$ is a maximal ideal of R. Thus if $\mathcal{P}_1, \mathcal{P}_2 \in \operatorname{MaxSpec} R$ are such that $\mathcal{P}_1 \cap R = \mathcal{P}_2 \cap R$, then we have

$$T_{\mathcal{P}_1} = R_{\mathcal{P}_1 \cap R} = R_{\mathcal{P}_2 \cap R} = T_{\mathcal{P}_2},$$

which implies $\mathcal{P}_1 = \mathcal{P}_2$, showing that $\iota^* : \operatorname{MaxSpec} T \to \operatorname{MaxSpec} R$ is an injection with image W. Since for $\mathcal{P} \in \operatorname{MaxSpec} T$ we just showed that the only maximal ideal of T lying over $\mathcal{P} \cap R$ is $\mathcal{P}$, it follows that $\iota_* \iota^*(\mathcal{P})$ is a power of $\mathcal{P}$. Since the DVRs $R_{\mathcal{P} \cap R}$ and $T_{\mathcal{P}}$ are equal, we must have $\iota_* \iota^*(\mathcal{P}) = \mathcal{P}$. □

3.2. Proof of Theorem 17.11. We are now in a position to prove Theorem 17.11 from Chapter 17, which we restate for the reader's convenience.

THEOREM 21.11. *Let $v : K^\times \to \mathbb{R}$ be a discrete valuation on a field K, and let L/K be a finite degree field extension. Then the set of valuations w on L that extend v is finite and nonempty.*

PROOF. Let R be the valuation ring of v, and let $\mathfrak{m}$ be the maximal ideal of R. The desired result holds for v if and only if it holds for any equivalent discrete valuation, so we may asume that $v = v_{\mathfrak{m}}$ is the normalized $\mathfrak{m}$-adic valuation. Let T be the integral closure of R in L. Since T is an integral extension of R, for every $\mathcal{M} \in \operatorname{MaxSpec} T$ we have that $\mathcal{M} \cap R$ is a maximal ideal and thus $\mathcal{M} \cap R = \mathfrak{m}$. From this and Corollary **??** we get find that $\operatorname{MaxSpec} R$ is finite and nonempty. We claim that for a valuation w on L, $w|_K$ is equivalent to $v_{\mathfrak{m}}$ if and only if w is equivalent to $w_{\mathcal{M}}$, the normalized discrete valuation attached to the maximal ideal $\mathcal{M}$ of a Dedekind domain. This suffices.

Let $\mathcal{M} \in \operatorname{MaxSpec} T$, and let $w_{\mathcal{M}}$ be the normalized $\mathcal{M}$-adic valuation. If we write

$$\mathfrak{m}T = \prod_{\mathcal{M} \in M_{\mathfrak{m}}} \mathcal{M}^{e_{\mathcal{M}}},$$

then $w_{\mathcal{M}}|_K = e_{\mathcal{M}} v_{\mathfrak{m}}$, which is indeed equivalent to $v_{\mathfrak{m}}$.

Now let w be a valuation on L whose restriction to K is equivalent to $v_{\mathfrak{m}}$. Let T_w be the valuation ring of w. For $x \in T^\bullet$, there are $a_0, \ldots, a_{n-1} \in R$ such that

$$x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0. \tag{57}$$

If $w(x)$ were negative, then $w(x^n) = nw(x)$ is the unique term on the left hand side of (57) of minimal valuation, so the valuation of the left hand side is $w(x^n)$, so the left hand side cannot be 0. Thus $w(x) \geqslant 0$, so $T \subseteq T_w$. From our classification of overrings of a Dedekind domain, we know that T_w is of the form $T_{\mathcal{M}}$ for some maximal ideal $\mathcal{M}$ of T, so w is discrete and equivalent to $w_{\mathcal{M}}$. □

EXERCISE 21.2. *Let $v : K^\times \to \mathbb{R}$ be a discrete valuation on a field K, and let L/K be an algebraic field extension.*

a) *Show: there is a rank one valuation on L that extends v.*
b) *Show: there need not be a discrete valuation on L that extends v, but every valuation on L that extends v is equivalent to one with value group contained in $\mathbb{Q}$.*

3.3. When overrings are localizations.

LEMMA 21.12. *Let R be an integrally closed domain with fraction field K, and let T be an overring of R.*

a) *The relative unit group $T^\times/R^\times$ is torsionfree.*
b) *Suppose that R is a Dedekind domain, $\mathfrak{p} \in \Sigma_R$ and $T = R^{\mathfrak{p}}$. The following are equivalent:*
   (i) $T^\times/R^\times \cong \mathbb{Z}$.
   (ii) $T^\times \supsetneq R^\times$.
   (iii) $[\mathfrak{p}] \in \mathrm{Pic}(R)[\mathrm{tors}]$.
   (iv) *There is $x \in R$ that is contained in $\mathfrak{p}$ and in no maximal ideal $\mathfrak{q} \neq \mathfrak{p}$.*

PROOF. a) Since R is integrally closed, all finite order elements of $K^\times$ (i.e., roots of unity in K) lie in R and *a fortiori* in T: $R^\times[\mathrm{tors}] = T^\times[\mathrm{tors}]$. On the other hand, let $x \in T^\times$ be of infinite order such that $x^n \in R^\times$ for some $n \in \mathbb{Z}^+$. Again integral closure of R implies $x \in R$, and then $x^n \in R^\times \implies x \in R^\times$.
b) (i) $\implies$ (ii) is clear.
(ii) $\implies$ (iii): Let $x \in K^\times$. Then $x \in T^\times$ if and only if $Rx = \mathfrak{p}^a$ for some $a \in \mathbb{Z}$, and $x \in R^\times$ if and only if $a = 0$. Therefore (ii) holds if and only if some power of $\mathfrak{p}$ is principal, which is to say that the class of $\mathfrak{p} \in \mathrm{Pic}\, R$ is torsion.
(iii) $\implies$ (i): Let a be the least positive integer such that $\mathfrak{p}^a$ is principal. Thus $\mathfrak{p}^a = xR$ with x uniquely determined modulo $R^\times$. It follows that $T^\times$ is generated by $R^\times$ and x, so $T^\times/R^\times$ is a nontrivial cyclic group. By part a) it is also torsionfree so $T^\times/R^\times \cong \mathbb{Z}$.
(iii) $\implies$ (iv): If $\mathfrak{p}^a = xR$, then x lies in $\mathfrak{p}$ but in no other maximal ideal $\mathfrak{q}$.
(iv) $\implies$ (iii): If $a = v_{\mathfrak{p}}(x)$, then $a > 0$ and $xR = \mathfrak{p}^a$. □

Remark: Part (iv) of Lemma 21.12 was added following an observation of H. Knaf.

THEOREM 21.13. *(Goldman [**Gol64**])*
For a Dedekind domain R, the following are equivalent:

(i) *Every overring of R is a localization.*
(ii) *$\mathrm{Pic}\, R$ is a torsion group.*

PROOF. (i) $\implies$ (ii): Let $\mathfrak{p} \in \mathrm{MaxSpec}\, R$. We've seen that $R^{\mathfrak{p}}$ is a proper overring of R, so by assumption $R^{\mathfrak{p}}$ is a localization of R and thus has a strictly larger unit group. By Lemma 21.12 this implies that $[\mathfrak{p}] \in \mathrm{Pic}(R)[\mathrm{tors}]$. Since $\mathrm{Pic}(R)$ is generated by the classes of the nonzero prime ideals, it follows that $\mathrm{Pic}\, R$ is torsion.

(ii) $\implies$ (i): Let T be an overring of R, and put $S = R \cap T^\times$. We want to show that $T = S^{-1}R$. That $S^{-1}R \subset T$ is clear. Conversely, let $x \in T$, and write $xR = \mathfrak{a}\mathfrak{b}^{-1}$ with $\mathfrak{a}, \mathfrak{b}$ coprime integral ideals of R: $\mathfrak{a} + \mathfrak{b} = R$. Thus $\mathfrak{a}T + \mathfrak{b}T = T$ whereas $\mathfrak{a}T = x\mathfrak{b}T \subset \mathfrak{b}T$, so $\mathfrak{b}T = T$ and hence also $\mathfrak{b}^n T = T$ for all $n \in \mathbb{Z}^+$. Since $\operatorname{Pic} R$ is torsion, there exists $n \in \mathbb{Z}^+$ with $\mathfrak{b}^n = bR$. It follows that $bT = T$ and thus $b \in S$. Now $x\mathfrak{b} = \mathfrak{a} \subset R$, so $xb \in R$. Thus $x \in S^{-1}R$, and we conclude $T \subset S^{-1}R$. □

COROLLARY 21.14. *Let R be a Dedekind domain. Suppose that W is a finite subset of* $\operatorname{MaxSpec} R$ *and that every $\mathfrak{p} \in W$ has finite order in* $\operatorname{Pic} R$. *Then there is $a \in R^\bullet$ such that $R^W = R[\frac{1}{a}]$.*

EXERCISE 21.3. *Prove Corollary 21.14.*

EXERCISE 21.4. *Let $T = R^W$ be an overring of R such that $T = R[\frac{1}{a}]$ for some $a \in R^\bullet$.*

a) *Show: W is finite.*
b) *Must it be the case that every $\mathfrak{p} \in W$ has finite order in* $\operatorname{Pic} R$*?*

3.4. The Picard group of an overring.

THEOREM 21.15. *Let R be a Dedekind domain, let $W \subseteq \operatorname{MaxSpec} R$, and let $\operatorname{Frac}_W R = \bigoplus_{\mathfrak{p} \in W} \mathbb{Z}$ denote the subgroup of fractional R-ideals supported on W. There is a short exact sequence*

$$1 \to R^\times \to (R^W)^\times \xrightarrow{v} \operatorname{Frac}_W R \to \operatorname{Pic} R \xrightarrow{\iota_*} \operatorname{Pic} R^W \to 1.$$

PROOF. The map $v : (R^W)^\times \to \operatorname{Frac}_W R$ is obtained by restricting the canonical map $K^\times \to \operatorname{Frac} R$ to $(R^W)^\times$: the fractional ideals so obtained have $\mathfrak{p}$-adic valuation 0 for all $\mathfrak{p} \in \operatorname{MaxSpec} R^W = \operatorname{MaxSpec} R \backslash W$: thus the image lands in $\operatorname{Frac}_W R$.
It is easy to see most of the exactness claims: certainly $R^\times \to (R^W)^\times$ is injective; further, for $x \in (R^W)^\times$, $v(x) = 0$ iff $v_\mathfrak{p}(x) = 0$ for all $\mathfrak{p} \in W \cup \operatorname{MaxSpec} R^W = \operatorname{MaxSpec} R$ if and only if $x \in R^\times$. If $I \in \operatorname{Frac}_W R$, then I is principal if and only if it has a generator $x \in K^\times$ with $v_\mathfrak{p}(x) = 0$ for all $\mathfrak{p} \in \operatorname{MaxSpec} R \backslash W = \operatorname{MaxSpec} R^W$ if and only if $I = (x)$ for $x \in (R^W)^\times$. Exactness at $\operatorname{Pic} R$: Let $[I] \in \operatorname{Pic} R$ be such that $\iota_*([I]) = 1$: thus there is $x \in K^\times$ with $IR^W = xR^W$. Then $[I] = [x^{-1}I]$ and $x^{-1}I \in \operatorname{Frac}_W R$. Conversely, if $I \in \operatorname{Frac}_W R$, then $IR^W = R^W$. Finally, by Theorem 22.10 we have $\iota_* \circ \iota^* = 1_{\operatorname{MaxSpec}(R^W)}$, so every prime ideal of R^W is of the form $\iota_*(\mathfrak{p})$ for a prime ideal of R. This certainly implies that $\iota_* : \iota_* : \operatorname{Pic} R \to \operatorname{Pic} R^W$ is surjective. □

Let us examine the special case of Theorem 21.15 of localization: namely, let S be a multiplicative subset of R, and consider the overring $S^{-1}R$. Then if V is the set of maximal ideals $\mathfrak{p}$ of R that are disjoint from S, we have $S^{-1}R = R_V$, so if $W := \operatorname{MaxSpec} R \backslash V$ is the complementary set, of maximal ideals $\mathfrak{p}$ such that $\mathfrak{p}S^{-1}R = S^{-1}R$, then $S^{-1}R = R^W$. Theorem 21.15 asserts that the natural map $\operatorname{Pic} R \to \operatorname{Pic} S^{-1}R$ is surjective, with kernel the set of classes $[I]$ where $I \in \operatorname{Frac} R$ satisfies the condition $v_\mathfrak{p}(I) \neq 0 \implies \mathfrak{p} \in W$.

EXERCISE 21.5. *We maintain the setup of Theorem 21.15.*

a) *Use Theorem 21.15 to give a new proof of Lemma 21.12.*
b) *Show that the relative unit group $(R^W)^\times / R^\times$ is free abelian.*
(This strengthens Lemma 21.12 when R is a Dedekind domain.)

c) *Suppose* $\operatorname{Pic} R$ *is torsion. Show:*

$$(R^W)^\times \cong R^\times \oplus \bigoplus_{\mathfrak{p} \in W} \mathbb{Z}.$$

d) *Suppose that* K *is a number field. Show that* $K^\times$ *is isomorphic to the product of a finite cyclic group with a free commutative group of countable rank.*

4. Repleteness in Dedekind domains

4.1. Repleteness and Repletions. Let R be a Dedekind domain, and consider the map $\Phi : \operatorname{MaxSpec} R \to \operatorname{Pic} R$ given by $\mathfrak{p} \mapsto [\mathfrak{p}]$. We say that R is **replete** if Φ is surjective, i.e., if every element of $\operatorname{Pic} R$ is of the form $[\mathfrak{p}]$ for some *prime* ideal $\mathfrak{p}$.

EXAMPLE 21.16. *Let R be an S-integer ring in a global field. It follows from the* ***Chebotarev Density Theorem*** *that R is replete.*

For our coming applications it is useful to consider a variant: we say that a Dedekind domain R is **weakly replete** if for every subgroup $H \subset \operatorname{Pic} R$, there is a subset $W_H \subset \operatorname{MaxSpec} R$ such that $\langle \Phi(W_H) \rangle = H$. The point of this condition is that it allows a complete classification of the Picard groups of overrings of R. Indeed:

PROPOSITION 21.17. *Let R be a weakly replete Dedekind domain. Then for any subgroup H of* $\operatorname{Pic} R$*, there is an overring T of R such that* $\operatorname{Pic} T \cong (\operatorname{Pic} R)/H$.

PROOF. By definition of weakly replete, there is a subset $W \subset \operatorname{MaxSpec} R$ such that $\langle \Phi(W) \rangle = H$. By Theorem 21.15, $\operatorname{Pic} R^W \cong \operatorname{Pic} R / \langle \Phi(W) \rangle \cong (\operatorname{Pic} R)/H$. □

PROPOSITION 21.18. *Let R be a Dedekind domain and R^W an overring of R.*

a) *If R is replete, then every nontrivial element of* $\operatorname{Pic} R^W$ *is of the form* $[\mathfrak{p}]$ *for some $\mathfrak{p} \in MaxSpecR^W$.*

b) *If R is weakly replete, so is R^W.*

EXERCISE 21.6. *Prove Proposition 21.18.*

Notice that Proposition 21.18 does not quite assert that if R is replete, then so is every overring. In fact this is false, as we now show:

PROPOSITION 21.19. *Let R be a Dedekind domain that is not a field, and let S be the multiplicative subset of R generated by the set of all prime elements of R. Then:*

a) *The natural map $\iota_* : \operatorname{Pic} R \to \operatorname{Pic} S^{-1}R$ is an isomorphism.*

b) *No maximal ideal of $S^{-1}R$ is principal.*

PROOF. a) We know from Theorem 21.15 that ι_* is surjective and that its kernel consists of classes $[I]$ such that $I = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_n^{a_n}$ with each $\mathfrak{p}_i$ a maximal ideal of R that meets S. Thus each $\mathfrak{p}_i$ contains a product of prime elements and thus, being prime, contains a prime element, hence (since $\mathfrak{p}_i$ has height one) is principal. It follows that I is a principal fraction ideal, so $[I]$ is trivial and thus ι_* is an isomorphism.

b) Every maximal ideal of $S^{-1}R$ is of the form $\iota_*(\mathfrak{p})$ for a maximal ideal $\mathfrak{p}$ of R that does not meet S. If $\iota_*(\mathfrak{p})$ is principal, then it is generated by an element x of R. We have $v_{\mathfrak{p}}(x) = 1$; we may have $v_{\mathfrak{q}}(x) > 0$ for finitely many other maximal

ideals $\mathfrak{q}_1, \ldots, \mathfrak{q}_n$, but every such $\mathfrak{q}_i$ must lie in the kernel of $\iota : R \hookrightarrow S^{-1}R$, so for all $1 \leqslant i \leqslant n$ there is an element π_i of R that generates $\mathfrak{q}_i$. Then $\frac{x}{\prod_{i=1}^n \pi_i^{v_{\mathfrak{p}_i}(x)}}$ is a generator for $\mathfrak{p}$, so $\mathfrak{p}$ does meet S: contradiction. □

Thus if we apply Proposition 21.19 to a replete Dedekind domain (e.g. the ring of integers of a number field), we get a localization in which the principal class of $\operatorname{Pic} R$ is not represented by any maximal ideal.

A **repletion** of a Dedekind domain R is a replete Dedekind domain S together with an injective ring homomorphism $\iota : R \hookrightarrow S$, such that $\iota_* : \operatorname{Pic}(R) \xrightarrow{\sim} \operatorname{Pic}(S)$.

Let R be a Dedekind domain. Recall that a polynomial $f \in R[t]^\bullet$ is **naively primitive** if the coeffiicents of f generate the unit ideal of R. (In the context of Dedekind domains this definition is not actually "naive," but we will maintain the terminology.) By Proposition 15.23, if $f, g \in R[t]^\bullet$ are naively primitive, then so is fg. The following exercise gives a mild generalization.

EXERCISE 21.7. *Let R be a Dedekind domain with fraction field K. For $f \in K[t]^\bullet$, we define the **content** $c(f)$ of f to be the fractional R-ideal of K generated by the coefficients of f. Let $f, g \in K[t]^\bullet$.*

a) *Show: $c(fg) = c(f)c(g)$.*
b) *Show: $fg \in R[t] \iff g \in c(f)^{-1}R[t]$.*

THEOREM 21.20. *(Claborn) For a Dedekind domain R with fraction field $K \supsetneq R$, and let R^1 denote the localization of $R[t]$ at the multiplicative set of all monic polynomials. Then R^1 is Dedekind and the composite map $\iota : R \to R[t] \to R^1$ is a repletion.*

PROOF. Step 1: Let S be the multiplicative subset of $R[t]$ consisting of monic polynomials. We will show that $S^{-1}R[t]$ is Dedekind.

The ring $S^{-1}R[t]$ is a localization of a Noetherian, integrally closed domain, hence is Noetherian and integrally closed, so the matter of it is to show that nonzero prime ideals of $S^{-1}R[t]$ are maximal. Every nonzero prime ideal of $S^{-1}R[t]$ is pushed forward from a nonzero prime ideal $\mathcal{P}$ of $R[t]$ that is disjoint from S. Moreover, in any localization map $\iota : A \to B$, if $\mathfrak{p}$ is a prime ideal of A such that $\iota_*(\mathfrak{p}) \neq B$, then the height of $\mathfrak{p}$ is the same as the height of $\iota_*(\mathfrak{p})$. Since $\dim R[t] = 2$, what we need to check then is that for every height 2 prime $\mathcal{P}$ of $R[t]$ we have $\mathcal{P}S^{-1}R[t] = S^{-1}R[t]$. Every such $\mathcal{P}$ is a maximal ideal of $R[t]$. If $\mathcal{P} \cap R = (0)$, then by Theorem 8.57, the prime $\mathcal{P}$ pushes forward to a maximal ideal of $K[t]$; since $K[t]$ is itself a localization of $R[t]$, this shows that $\mathcal{P}$ has height 1. On the other hand, if $\mathfrak{p} := \mathcal{P} \cap R$ is nonzero, then $\mathfrak{p} \in \operatorname{MaxSpec} R$, so by Theorem 8.56a) we have $\mathcal{P} = \langle \mathfrak{p}, f \rangle$ for a monic polynomial f and thus $\mathcal{P}S^{-1}R[t] = S^{-1}R[t]$. Step 2: Let $\iota : R \hookrightarrow R^1$ be the inclusion map. We will show that $[\iota_*] : \operatorname{Pic} R \to \operatorname{Pic} R^1$ is injective.

Let I and J be nonzero integral ideals of R such that $[IR^1] = [JR^1]$. Then there are $f_1, g_1, f_2, g_2 \in R[t]^\bullet$ with g_1 and g_2 monic such that the ideals $(\frac{f_1}{g_1})I$ and $(\frac{f_2}{g_2})J$ of R^1 are equal. For $i = 1, 2$, let a_i be the leading coefficient of f_i, and let $d \in I$. Then there is $j \in J[t]^\bullet$ and a monic $g \in R[t]$ such that

$$d\frac{f_1}{g_1} = \frac{e}{g}\frac{f_2}{g_2},$$

so

$$dg_2f_1g = ef_2g_1.$$

The leading coefficient on the right hand side lies in a_2J, so $a_1I \subseteq a_2J$. Symmetrically, we get $a_2J \subseteq a_1I$, so $a_1I = a_2J$ and thus $[I] = [J]$.

Step 3: We will show that $[\iota_*]$ is surjective. For this it is enough to show that for every $\mathcal{P} \in \operatorname{MaxSpec} R^1$ there is a fraction ideal I of R such that $[\iota_*(I)] = [\mathcal{P}]$: indeed if so, then the image of $[\iota_*]$ is a subgroup of $\operatorname{Pic} R^1$ containing a set of generators for $\operatorname{Pic} R^1$. We may view $\mathcal{P}$ as a height one prime ideal of $R[t]$ containing no monic polynomial.

Case 1: Suppose $\mathcal{P} \cap R \neq (0)$. Then it follows from Theorem 8.56a) that there is $\mathfrak{p} \in \operatorname{MaxSpec} R$ such that $\iota_*(\mathfrak{p}) = \mathcal{P}$, so $[\iota_*(\mathfrak{p})] = [\mathcal{P}]$.

Case 2: Suppose $\mathcal{P} \cap R = (0)$, so by Theorem 8.57 we have that $\mathcal{P}K[t]$ is a prime ideal which is generated by some $f \in R[t]$, and we have $(\mathcal{P}K[t]) \cap R[t] = \mathcal{P}$. Exercise 21.7 gives

$$\mathcal{P} = (fK[t]) \cap R[t] = c(f)^{-1}fR[t],$$

so

$$[\mathcal{P}] = [\iota_*(c(f)^{-1})].$$

Step 4: We show that R^1 is replete. Let I be a nonzero integral ideal of R, so $I = \langle a_0, a_1 \rangle_R$. Let

$$f := a_0 + a_1t \in R[t],$$

so f is irreducible in $K[t]$ and $c(f) = I$ As we saw in Step 3,

$$\mathcal{P} := (fK[t]) \cap R[t] = c(f)^{-1}fR[t] = I^{-1}fR[t]$$

is a height one prime ideal of $R[t]$, so in $\operatorname{Pic} R[t]$ we have $[\mathcal{P}] = [I^{-1}]$. Thus

$$[\iota_*(I^{-1})] = [\mathcal{P}R^1].$$

By Step 2, if I is nonprincipal then $[\mathcal{P}R^1]$ is nontrivial, so $\mathcal{P}R^1 \in \operatorname{MaxSpec} R^1$. By Step 3, every nontrivial class in $x \in \operatorname{Pic} R^1$ is of the form $\iota_*(I^{-1})$ for some nontrivial I, so $x = [\mathcal{P}R^1]$ and thus x is represented by a maximal ideal. Finally, since R is nont a field, there is a nonzero nonunit element $a_1 \in R$. Then $(a_1t + 1)$ is a prime ideal of $R[t]$ that contains no primitive polynomial, so $a_1t + 1$ is a prime element of R^1. Thus R^1 is replete. □

EXERCISE 21.8. *Let R be a Dedekind domain that is not a PID. Show: every maximal ideal of $R[t]$ has height 2.*

4.2. Elasticity in Replete Dedekind Domains. Let R be a domain and $x \in R^\bullet \backslash R^\times$. If for $n \in \mathbb{Z}^+$ there are (not necessarily distinct) irreducible elements $\alpha_1, \ldots, \alpha_n$ of R such that $x = \alpha_1 \cdots \alpha_n$, we say that x admits an irreducible factorization of **length** n.

A **half factorial domain** (or **HFD**) is an atomic domain in which for all $x \in R^\bullet \backslash R^\times$, any two irreducible factorizations of x have the same length.

EXERCISE 21.9. *(Zaks) Show: $\mathbb{Z}[\sqrt{-3}]$ is a HFD that is not integrally closed.*

For R an atomic domain and $x \in R^\bullet \backslash R^\times$, let $L(x)$ be the supremum of all lengths of irreducible factorizations of x and let $\ell(x)$ be the minimum of all lengths of irreducible factorizations of x. We define the **elasticity of x**, $\rho(x)$, as the ratio $\frac{L(x)}{\ell(x)}$. We also make the convention that for $x \in R^\times$, $\rho(x) = 1$. Finally we define the

elasticity of R as $\rho(R) = \sup_{x \in R^\bullet} \rho(x)$.

An atomic domain is a HFD if and only if $\rho(R) = 1$. Thus $\rho(R)$ is a quantitative measure of how far an atomic domain is from being a HFD.

Let $(G, \cdot)$ be a commutative group. A finite sequence $g_1, \ldots, g_n$ of elements in G is **irreducible** if for all nonempty proper subsets $S \subset \{1, \ldots, n\}$, $\prod_{i \in S} g_i \neq 1$.

LEMMA 21.21. *Let $(G, \cdot)$ be a commutative group, let $x_1, \ldots, x_n$ be an irreducible sequence in G, and let $x_{n+1} = (\prod_{i=1}^n x_i)^{-1}$. If $x_{n+1} \neq 1$, then $x_1, \ldots, x_n, x_{n+1}$ is an irreducible sequence.*

PROOF. A nontrivial proper subsequence of $x_1, \ldots, x_{n+1}$ with trivial product must be of the form $x_{i_1}, \ldots, x_{i_k}, x_{n+1}$ for some nonempty proper subset $S = \{i_1, \ldots, i_k\}$ of $\{1, \ldots, n\}$. Put $S' = \{1, \ldots, n\} \setminus S$. Then $\prod_{i \in S'} x_i^{-1} = 1$, hence also $\prod_{i \in S'} x_i = 1$, contradicting the irreducibility of $x_1, \ldots, x_n$. □

PROPOSITION 21.22. *Let R be a Dedekind domain, let $x \in R^\bullet \setminus R^\times$, and let*

$$(x) = \prod_{i=1}^r \mathfrak{p}_i$$

be the factorization of x into prime ideals.

a) *(Carlitz-Valenza* [**Ca60**] [**Va90**]*) The following are equivalent:*
   (i) *For no nonempty proper subset $S \subset \{1, \ldots, r\}$ is $\prod_{i \in S} \mathfrak{p}_i$ is principal.*
   (ii) *The element x is irreducible.*

b) *If $\mathfrak{p}$ is a prime ideal such that $\mathfrak{p}^r = (x)$ and $\mathfrak{p}^s$ is nonprincipal for all $1 \leqslant s < r$, then x is irreducible.*

c) *If no $\mathfrak{p}_i$ is principal, the length of any irreducible factorization of x is at most $\frac{r}{2}$.*

EXERCISE 21.10. *Prove Proposition 21.22.*

For a commutative group $(G, \cdot)$ the **Davenport constant** $D(G)$ of G is the maximum length of an irreducible sequence in G, or ∞ if the lengths of irreducible sequences in G are unbounded.

PROPOSITION 21.23. *Let R be a Dedekind domain, and let $x \in R^\bullet$ be irreducible. Write $(x) = \mathfrak{p}_1 \cdots \mathfrak{p}_r$. Then $r \leqslant D(\operatorname{Pic} R)$.*

PROOF. By Proposition 21.22a), $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ is an irreducible sequence in $\operatorname{Pic} R$. □

PROPOSITION 21.24.
a) *If H is a subgroup of a commutative group G, then $D(H) \leqslant D(G)$.*
b) *If H is a quotient of a commutative group G, then $D(H) \leqslant D(G)$.*
c) *$D(G) \geqslant \exp G = \sup_{x \in G} \#\langle x \rangle$.*
d) *If G is infinite, then $D(G) = \infty$.*
e) *If G is finite, then $D(G) \leqslant \#G$.*
f) *If G is finite cyclic, then $D(G) = \#G$.*
g) *We have*

$$D(\bigoplus_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}) \geqslant 1 + \sum_{i=1}^r (n_i - 1). \tag{58}$$

PROOF. a) If H is a subgroup of G, then any irreducible sequence in H is an irreducible sequence in G.
b) If $q : G \to H$ is a surjective homomorphism and $x_1, \ldots, x_n$ is irreducible in H, then choosing any lift $\tilde{x_i}$ of x_i to G yields an irreducible sequence $\tilde{x}_1, \ldots, \tilde{x}_n$.
c) If $x \in G$ and $n \in \mathbb{Z}^+$ is less than or equal to the order of x, then $x, x, \ldots, x$ (n times) is an irreducible sequence in G of length n.
d) By part c), we may assume G is infinite and of finite exponent. Then for some prime p, $G[p]$ is infinite, and by part a) it suffices to show that $D(G[p]) = \infty$. But $G[p]$ is an infinite-dimensional vector space over the field $\mathbb{F}_p$: let $\{e_i\}_{i=1}^{\infty}$ be an infinite $\mathbb{F}_p$-linearly independent subset of $G[p]$. Then for all $n \in \mathbb{Z}^+$ the sequence $e_1, \ldots, e_n$ is irreducible.
e) Suppose $\#G = n$, and let $g_1, \ldots, g_{n+1}$ be a sequence in G. For $1 \leqslant i \leqslant n$, let $P_i = g_1 \cdots g_i$. By the Pigeonhole Principle there is $1 \leqslant i < j \leqslant n+1$ such that $P_i = P_j$, and thus $g_{i+1} \cdots g_j = 1$.
f) Since $\exp \mathbb{Z}/n\mathbb{Z} = \#\mathbb{Z}/n\mathbb{Z} = n$, this follows from parts c) and e).
g) Let $G = \bigoplus_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}$,[1] and let $d(G) = 1 + \sum_{i=1}^{k}(n_i - 1)$. There is an "obvious" irreducible sequence $x_1, \ldots, x_{d(G)-1}$: for $1 \leqslant i \leqslant k$, let e_i be the element of G with ith coordinate 1 and other coordinates 0. Take $e_1, \ldots, e_1$ ($n_1 - 1$ times), $e_2, \ldots, e_2$ ($n_2 - 1$ times),....,$e_k, \ldots, e_k$ ($n_k - 1$ times). The sum of these elements is $(n_1 - 1, \ldots, n_k - 1) \neq 0$, so by Lemma 21.21 taking $x_{d(G)} = -\sum_{i=1}^{d(G)-1} x_i$, we get an irreducible sequence of length $d(G)$. □

EXERCISE 21.11. *Let G be a commutative group.*
a) *Show:* $D(G) = 1 \iff \#G = 1$.
b) *Show:* $D(G) = 2 \iff \#G = 2$.

THEOREM 21.25. *Let R be a Dedekind domain.*
a) *We have* $\rho(R) \leqslant \max(\frac{D(\operatorname{Pic} R)}{2}, 1)$.
b) *If R is replete, then* $\rho(R) = \max(\frac{D(\operatorname{Pic} R)}{2}, 1)$.

PROOF. For $x \in R^\bullet \backslash R^\times$, let $P(x)$ be the number of prime ideals (with multiplicity) in the factorization of (x).
Step 0: Of course if $\operatorname{Pic} R$ is trivial then $D(\operatorname{Pic} R) = 1$, $\rho(R) = 1$ and the result holds in this case. Henceforth we assume $\operatorname{Pic} R$ is nontrivial and thus $D(\operatorname{Pic} R) \geqslant 2$, and our task is to show that $\rho(R) \leqslant \frac{D(\operatorname{Pic} R)}{2}$, with equality if R is replete.
Step 1: Let $x \in R^\bullet \backslash R^\times$. Consider two irreducible factorizations

$$x = \alpha_1 \cdots \alpha_m = \beta_1 \cdots \beta_n$$

of x with $m \geqslant n$. Let k be the number of principal prime ideals in the prime ideal factorization of (x). Then $k = n \iff k = m \implies \rho(x) = 1$. Henceforth we assume $k < \min(m, n)$ (since $\operatorname{Pic} R$ is nontrivial, there is at least one such x). We may further assume that $\alpha_1, \ldots, \alpha_k$ (resp. $\beta_1, \ldots, \beta_k$) are prime elements and $\alpha_{k+1}, \ldots, \alpha_m$ (resp. $\beta_{k+1}, \ldots, \beta_n$) are not; dividing through by these prime elements and correcting by a unit if necessary, we may write

$$x' = \alpha_{k+1} \cdots \alpha_m = \beta_{k+1} \cdots \beta_n.$$

Since for $k+1 \leqslant i \leqslant m$, α_i is irreducible but not prime, $P(\alpha_i) \geqslant 2$ and thus

$$2(m-k) \leqslant P(\alpha_{k+1} \cdots \alpha_m) = P(x').$$

[1]Here we are considering G as an additive group.

On the other hand, by Proposition 21.23 we have

$$P(x') = P(\beta_{k+1} \cdots \beta_n) \leqslant (n-k)D(\operatorname{Pic} R).$$

Combining these inequalities gives

$$\frac{m}{n} \leqslant \frac{m-k}{n-k} \leqslant \frac{D(\operatorname{Pic} R)}{2}.$$

It follows that $\rho(x) \leqslant \frac{D(\operatorname{Pic} R)}{2}$ and thus $\rho(R) \leqslant \frac{D(\operatorname{Pic} R)}{2}$, establishing part a).
Step 2: Suppose R is replete.
Step 2a: Suppose first that $\operatorname{Pic} R$ is finite and put $D = D(\operatorname{Pic} R)$. By repleteness, choose prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_D$ whose classes form an irreducible sequence in $\operatorname{Pic} R$. For $1 \leqslant i \leqslant D$, let $\mathfrak{q}_i$ be a prime ideal with $[\mathfrak{q}_i] = [\mathfrak{p}_i]^{-1}$. For $1 \leqslant i \leqslant D$, let c_i be such that $(c_i) = \mathfrak{p}_i\mathfrak{q}_i$; using Lemma 21.21 there are $d_1, d_2 \in R$ such that $(d_1) = \mathfrak{p}_1 \cdots \mathfrak{p}_D$ and $(d_2) = \mathfrak{q}_1 \cdots \mathfrak{q}_D$ and

$$c_1 \cdots c_D = d_1 d_2.$$

By Proposition 21.22, $c_1, \ldots, c_D, d_1, d_2$ are all irreducible, and thus $\rho(R) \geqslant \frac{D}{2}$.
Step 2b: If $\operatorname{Pic} R$ is infinite, then $D(\operatorname{Pic} R) = \infty$ and from this, repleteness and Lemma 21.21, for all $D \in \mathbb{Z}^+$ there are prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_D$ whose classes form an irreducible sequence in $\operatorname{Pic} R$ and such that $\mathfrak{p}_1 \cdots \mathfrak{p}_D$ is principal. The argument of Step 2a now shows $\rho(R) \geqslant \frac{D}{2}$. Since this holds for all $D \in \mathbb{Z}^+$, $\rho(R) = \infty$. □

When $\operatorname{Pic} R$ is finite, Theorem 21.25 is due to Steffan [**St86**] and Narkiewicz [**Na95**].

Remark: The condition that R be replete is essential in Theorem 21.25. For instance, A. Zaks has shown that for every finitely generated commutative group G, there is a half factorial Dedekind domain R with $\operatorname{Pic} R \cong G$ [**Za76**]. Whether any commutative group can occur, up to isomorphism, as the Picard group of a half factorial Dedekind domain is an open problem.

Corollary 21.26.

a) *A replete Dedekind domain R is a HFD if and only if $\#\operatorname{Pic} R \leqslant 2$.*
b) *(Carlitz [**Ca60**]) Let K be a number field. Then its ring of integers $\mathbb{Z}_K$ is a HFD if and only if the class number of K – i.e., $\#\operatorname{Pic} \mathbb{Z}_K$ – is either 1 or 2.*
c) *(Valenza [**Va90**]) Let K be a number field. Then*

$$\rho(\mathbb{Z}_K) = \max\left(\frac{D(\operatorname{Pic} \mathbb{Z}_K)}{2}, 1\right).$$

d) *A replete Dedekind domain has infinite elasticity if and only if it has infinite Picard group.*

Exercise 21.12. *Prove Corollary 21.26.*

Later we will show that every commutative group arises, up to isomorphism, as the Picard group of a Dedekind domain. Combining this with Theorems 21.20 and 21.25 we see that the possible elasticities for replete Dedekind domains are precisely $\frac{n}{2}$ for any integer $n \geqslant 2$ and ∞.

We end this section by giving a little more information on the Davenport constant: let G be a finite commutative group, so that there is a unique sequence of

positive integers $n_1, \dots, n_r$ with $n_r \mid n_{r-1} \mid \dots \mid n_1 > 1$ such that $G \cong \bigoplus_{i=1}^r \mathbb{Z}/n_i\mathbb{Z}$. We put $d(G) = 1 + \sum_{i=1}^k (n_i - 1)$, so that (58) reads more succinctly as

$$D(G) \geqslant d(G). \tag{59}$$

J.E. Olson conjectured that equality holds in (58) for all finite commutative groups G [**Ol69a**]. He proved that the conjecture holds for p-groups [**Ol69a**] and also when $r \leqslant 2$ [**Ol69b**]. However, it was shown by P. van Emde Boas and D. Kruyswijk that (for instance) $D(G) > d(G)$ for $G = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ [**EBK69**]. Whether $D(G) = d(G)$ for all groups with $r = 3$ is still an open problem. The exact value of $D(G)$ is unknown for most finite commutative groups.

5. Every commutative group is a class group

To any ring R we attached a commutative group, the Picard group $\operatorname{Pic} R$. In fact the construction is functorial: a homomorphism $\varphi : R \to R'$ of domains induces a homomorphism $\varphi_* : \operatorname{Pic} R \to \operatorname{Pic} S$ of Picard groups. Explicitly, if M is a rank one projective R-module, then $M \otimes_R R'$ is a rank one projective R'-module. In general when one is given a functor it is natural to ask about its image. Here we are asking the following

QUESTION 6. *Which commutative groups occur (up to isomorphism) as the Picard group of a commutative ring?*

It would be interesting to know at what point algebraists began serious consideration of the above questions. I am not aware of any early work on this problem: so far as I know, the first paper that addresses this in the literature came relatively late and gives a full solution:

THEOREM 21.27. *(Claborn* [**Cl66**]*) For every commutative group G, there is a Dedekind domain R with* $\operatorname{Pic} R = \operatorname{Cl} R \cong G$.

Claborn proceeds by first constructs a *Krull domain* T with divisor class group isomorphic to G and then using an approximation process, constructs a Dedekind domain R with $\operatorname{Cl} R \cong \operatorname{Cl} T$.

A more elementary – but still quite ingenious and intricate – proof was given later by C.R. Leedham-Green [**Le72**]. Leedham-Green constructs the requisite R as the integral closure of a PID in a separable quadratic field extension.

Several years after that M. Rosen took a more naturally geometric approach, inspired by the Picard groups of varieties that appear in algebraic geometry. His approach uses some elliptic curve theory.

Let k be a field of characteristic zero.[2] Fix elements $A, B \in K$ such that $4A^3 + 27B^2 \neq 0$, and let

$$k[E^\circ] := k[x, y]/(y^2 - x^3 - Ax - B).$$

Then $k[E^\circ]$ is the affine coordinate ring of the elliptic curve

$$E : y^2 = x^3 + Ax + B.$$

PROPOSITION 21.28. *The ring $k[E^\circ]$ is a Dedekind domain.*

[2]This hypothesis is by no means essential, but it is certainly sufficient for our purposes. Really we are avoiding characteristics 2 and 3 so that every elliptic curve can be expressed in short Weierstrass form (for no reason other than notational simplicity) and so that quadratic field extensions are separable.

EXERCISE 21.13. *Prove Proposition 21.28. (Suggestions: the matter of it is to show that $k[E^\circ]$ is integrally closed. For this, show (or look up in an introductory text on elliptic curves!) that the condition that $4A^3 + 27B^2 \neq 0$ means that $x^3 + Ax + B \in k[x]$ is separable – i.e., has distinct roots in an algebraic closure – and thus is squarefree. Apply Theorem 15.17.)*

We denote the fraction field of $k[E^\circ]$ by $k(E)$, also called the **function field** of $E_{/k}$. An **elliptic Dedekind domain** is a Dedekind domain R that arises as an overring of the standard affine ring $k[E^\circ]$ of some elliptic curve E defined over a field k of characteristic 0. We refer to k as the **ground field** of R.

EXERCISE 21.14. *Let k be a countable field, and let R be an elliptic Dedekind domain with ground field k.*

a) *Show:* $\operatorname{Pic} R$ *is countable.*
b) *More generally, show: if R is an elliptic Dedekind domain with ground field k, then* $\#\operatorname{Pic} R \leqslant \max(\aleph_0, \#k)$.

Conversely:

THEOREM 21.29. *(Rosen [**Ro76**]) For every countable commutative group G, there exists an elliptic Dedekind domain R with ground field an algebraic extension of $\mathbb{Q}$ and such that* $\operatorname{Pic} R \cong G$.

In 2008 I built on this work of Rosen to prove the following result [**Cl09**].

THEOREM 21.30. *For any commutative group G, there is an elliptic Dedekind domain R such that:*

(i) *R is the integral closure of a PID in a separable quadratic field extension, and*
(ii) $\operatorname{Pic} R \cong G$.

Thus Theorem 21.30 implies the results of Claborn and Leedham-Green. On the other hand, Exercise 23.12 shows that the absolute algebraicity (or even the countability!) of the ground field k achieved in Rosen's construction cannot be maintained for uncountable Picard groups. Indeed our argument goes to the other extreme: we construct the ground field k as a transfinitely iterated function field.

Our argument will require some tenets of elliptic curve theory, especially the notion of the **rational endomorphism ring** $\operatorname{End}_k E$ of an elliptic curve $E_{/k}$. A k-rational endomorphism of an elliptic curve is a morphism $\varphi : E \to E$ defined over k which carries the neutral point O of E to itself.

PROPOSITION 21.31. *Let k be a field of characteristic 0, and let $E_{/k}$ be an elliptic curve.*

a) *The additive group of* $\operatorname{End}_k(E)$ *is isomorphic to $\mathbb{Z}^{a(E)}$ for $a(E) \in \{1, 2\}$.*
b) *There is a short exact sequence*

$$0 \to E(k) \to E(k(E)) \to \operatorname{End}_k(E) \to 0.$$

Since $\operatorname{End}_k(E)$ *is free abelian, we have $E(k(E)) \cong E(k) \bigoplus \mathbb{Z}^{a(E)}$.*
c) *There is a canonical isomorphism $E(k) \cong \operatorname{Pic} k[E^\circ]$.*

PROOF. a) See [**Si86**, Cor. III.9.4].
b) $E(k(E))$ is the group of rational maps from the nonsingular curve E to the

complete variety E under pointwise addition. Every rational map from a nonsingular curve to a complete variety is everywhere defined, so $E(k(E))$ is the group of morphisms $E \to E$ under pointwise addition. The constant morphisms form a subgroup isomorphic to $E(k)$, and every map $E \to E$ differs by a unique constant from a map of elliptic curves $(E, O) \to (E, O)$, i.e., an endomorphism of E.
c) By Riemann-Roch, $\Psi_1 : E(k) \to \mathrm{Pic}^0 E$ by $P \in E(k) \mapsto [[P] - [O]]$ is an isomorphism [**Si86**, Prop. III.3.4]. Moreover, $\Psi_2 : \mathrm{Pic}^0(E) \to \mathrm{Pic}\, k[E^\circ]$ given by $\sum_P n_P[P] \mapsto \sum_{P \neq O} n_P[P]$ is an isomorphism. Thus $\Psi_2 \circ \Psi_1 : E(k) \xrightarrow{\sim} \mathrm{Pic}\, k[E^\circ]$. □

Now fix a field k, and let $(E_0)/k$ be any elliptic curve. Put $K_0 := k$, and for all $n \in \mathbb{N}$, put $K_{n+1} := K_n(E_{/K_n})$. Then Proposition 21.31 gives

$$E(K_n) \cong E(k) \oplus \bigoplus_{i=1}^{n} \mathbb{Z}^{a(E)}.$$

Lemma 21.32 (Continuity Lemma). *Let K be a field, $(K_i)_{i \in I}$ a directed system of field extensions of K, and let $E_{/K}$ an elliptic curve. There is a canonical isomorphism*

$$\varinjlim E(K_i) = E(\varinjlim K_i).$$

Exercise 21.15. *Prove Lemma 21.32.*

Now let o be an ordinal number. We define the field K_o by transfinite induction: $K_0 = k$, for an ordinal $o' < o$, $K_{o'+1} = K_{o'}(E_{/K_{o'}})$, and for a limit ordinal o, $K_o = \lim_{o' < o} K_{o'}$. By the Continuity Lemma, we have $E(K_o) = \lim_{o' \in o} E(K_{o'})$.

Lemma 21.33. *Let $a \in \mathbb{Z}^+$. For a commutative group A, the following are equivalent:*

(i) *The group A is free commutative of rank $a \cdot \kappa$ for some cardinal κ.*
(ii) *The group A has a well-ordered ascending series with all factors $A_{s+1}/A_s \cong \mathbb{Z}^a$.*

Exercise 21.16. *Prove Lemma 21.33.*
(Suggestion: use the Transfinite Dévissage Lemma.)

Corollary 21.34. *We have $E(K_o)/E(k) \cong \bigoplus_{o' \in o} \mathbb{Z}^{a(E)}$.*

Exercise 21.17. *Prove Corollary 21.34.*

One can put together the results derived so far together with Exercise 22.2 to get a proof of Theorem 21.27. However, to prove Theorem 21.30 we need to circumvent the appeal to Theorem 21.20. This is handled as follows.

Theorem 21.35. *Let $E_{/k}$ be an elliptic curve with equation $y^2 = P(x) = x^3 + Ax + B$.*

a) *The ring $k[E^\circ]$ is weakly replete.*
b) *If k is algebraically closed, then $k[E^\circ]$ is not replete.*
c) *Suppose k does not have characteristic 2 and that $k[E^\circ]$ is not replete. Then for all $x \in k$, there is $y \in k$ with $y^2 = P(x)$.*

Proof. a) Each point $P \neq O$ on $E(k)$ is a prime ideal in the standard affine ring $k[E^\circ]$; according to the isomorphism of Proposition 21.31c), every nontrivial element of $\mathrm{Pic}(k[E^\circ])$ arises in this way.

Part b) is similar: if k is algebraically closed, then by Hilbert's Nullstellensatz every prime ideal of $k[E^\circ]$ corresponds to a k-valued point $P \neq O$ on $E(k)$, which under Proposition 21.31c) corresponds to a nontrivial element of the class group. Therefore the trivial class is not represented by any prime ideal.
c) We go by contraposition: suppose there is $a \in k$ such that $P(a)$ is not a square in k. Then the divisor of the function $x - a \in k(E)$ is of the form

$$D = D_+ - 2[O],$$

where

$$D_+ := [(a, \sqrt{P(a)})] + [(a, -\sqrt{P(a)})].$$

Under the isomorphism $\mathrm{Pic}^0(E) \xrightarrow{\sim} \mathrm{Pic}\, k[E^\circ]$, the divisor D maps to D_+, which therefore represents the trivial class. Because $\sqrt{P(a)}) \notin k$, the divisor D_+ corresponds to a maximal ideal of $k[E^\circ]$. Together with the proof of part a), this shows that $k[E^\circ]$ is replete. □

Finally we prove Theorem 21.30(i). Let G be a commutative group, and write it as F/H where F is a free commutative group of infinite rank. As above let k be any field of characteristic zero and $E_{/k}$ any elliptic curve. By Corollary 21.34, for all sufficiently large ordinals o, there is a surjection $E(K_0) \to F$ and thus also a surjection $E(K_o) \to G$. By Proposition 21.31c), there is a subgroup H of $K_o[E]$ such that $(\mathrm{Pic}\, K_o[E])/H \cong G$. By Proposition **??**a) and Proposition 21.17, there is an overring T of $K_o[E]$ such that $\mathrm{Pic}\, T \cong G$, establishing Theorem 21.30(i).

As for the second part: let σ be the automorphism of the function field $k(E)$ induced by $(x, y) \mapsto (x, -y)$, and notice that σ corresponds to inversion $P \mapsto -P$ on $E(k) = \mathrm{Pic}(k[E^\circ])$. Let $S = R^\sigma$ be the subring of R consisting of all functions which are fixed by σ. Then $k[E^\circ]^\sigma = k[x]$ is a PID, and S is an overring of $k[x]$, hence also a PID. More precisely, S is the overring of all functions on the projective line which are regular away from the point at infinity and the x-coordinates of all the elements in H (since H is a subgroup, it is stable under inversion). Finally, to see that R is the integral closure of S in the separable quadratic field extension $k(E)/k(x)$, it suffices to establish the following simple result.

LEMMA 21.36. *Let L/K be a finite Galois extension of fields, and S a Dedekind domain with fraction field L. Suppose that for all $\sigma \in \mathrm{Gal}(L/K)$, $\sigma(S) = S$. Then S is the integral closure of $R := S \cap K$ in L.*

PROOF. Since S is integrally closed, it certainly contains the integral closure of R in L. Conversely, for any $x \in S$, $P(t) = \prod_{\sigma \in \mathrm{Gal}(L/K)} (t - \sigma(x))$ is a monic polynomial with coefficients in $(S \cap K)[t]$ satisfied by x. □

This completes the proof of Theorem 21.30.

CHAPTER 22

Krull Domains

1. Families of Valuations

A domain R with fraction field K is a **Krull domain** if there is a family $\{v_i\}_{i \in X}$ of discrete valuations on K such that:
(KDV1) We have $R = \bigcap_{i \in X} R_i$, where for $i \in I$, R_i is the valuation ring of v_i; and
(KDV2) For all $x \in K^\times$, we have $v_i(x) \neq 0$ for only finitely many $i \in X$.

In this definition, the family X of discrete valuations is not part of the formal structure of a Krull domain: rather, such a family is simply required to exist, and in general there is more than one such family (but later it will turn out that there is a canonical minimal such family). For now, we call such a family of valuations a **defining family**. We say the defining family is **normed** if each element has value group $\mathbb{Z}$ (rather than an ordered group isomorphic to $\mathbb{Z}$).

EXAMPLE 22.1. *Let R be a domain with fraction field K.*

a) *If $R = K$ – i.e., if R is a field – then trivially R is a Krull domain: take $X := \varnothing$. As usual, although we allow the case of fields, it is not where our interest lies.*
b) *If R is Dedekind, then it is a Krull domain. Indeed we may take $X := \operatorname{MaxSpec} R$ and for $\mathfrak{p} \in \operatorname{MaxSpec} R$, we take $v_\mathfrak{p}$ to be the standard $\mathfrak{p}$-adic valuation. Then (KDV1) holds because $R = \bigcap_{\mathfrak{m} \in \operatorname{MaxSpec} R} R_\mathfrak{m}$ for any domain, and that (KDV2) holds has been observe previously in our discussion of almost Dedekind domains: for $x \in K^\times$, the set of $\mathfrak{p} \in \operatorname{MaxSpec} R$ such that $v_\mathfrak{p}(x) \neq 0$ are the fractional ideals that appear in the prime power decomposition of (x), so they are finite in number.*
c) *If R is a UFD, then it is a Krull domain. Indeed we may take $X := \operatorname{Spec}_1 R$, the set of height one primes of R. Since R is a UFD, each $\mathfrak{p} \in \operatorname{Spec}_1 R$ is generated by a prime element π, so for $x \in K^\times$ we may write $x = \frac{a}{b}$ for $a, b \in R^\bullet$ and take $v_\mathfrak{p}(x)$ to be the number of times π appears in the (unique!) prime factorization of a minus the number of times π appears in the (unique!) prime factorization of b. Then (VDK1) and (VDK2) hold very similarly as in in part b).*

Notice that in both parts b) and c) of Example 22.1, the defining family of discrete valuations on the Krull domain R turned out to be the ones associated to height one primes of R. This suggests that we consider the class of domains R such that (i) for every height one prime $\mathfrak{p}$, the one-dimensional local ring $R_\mathfrak{p}$ is a DVR, (ii) we have $R = \bigcap_{\mathfrak{p} \in \operatorname{Spec}_1 R} R_\mathfrak{p}$ and (iii) for $x \in R^\bullet$, the set of height one primes $\mathfrak{p}$ such that $x \notin R_\mathfrak{p}^\times$ is finite. In fact this will turn out to be *precisely the same class of*

rings, but the definition we gave using families of valuations is easier to work with initially, as we will now see.

PROPOSITION 22.2. *Let R be a Krull domain with fraction field K, and let $\{v_i\}_{i \in X}$ be a defining set of valuations of R. For $i \in X$, let R_i be the valuation ring of v_i. Let $S \subseteq R^\bullet$ be a multiplicative subset, and put*

$$Y := \{i \in X \mid v_i(s) = 0 \forall s \in S\}.$$

Then:

a) *We have $S^{-1}R = \bigcap_{i \in Y} R_i$.*
b) *The ring $S^{-1}R$ is a Krull domain.*

PROOF. a) For $i \in Y$, $x \in R^\bullet$ and $s \in S$ we have $v_i(\frac{x}{s}) = v_i(x) \geqslant 0$, so $S^{-1}R \subseteq R_i$, and thus $S^{-1}R = \bigcap_{i \in Y} R_i$. Now let $x \in (\bigcap_{i \in Y} R_i)^\bullet$. If $v_i(x) \geqslant 0$ for all $i \in X$, then $x \in R \subseteq S^{-1}R$. Otherwise, let $v_{i_1}, \ldots, v_{i_n}$ be the finite set of valuations (for $i_j \in X$) with $v_{i_j}(x) < 0$. For all $1 \leqslant j \leqslant n$ we must have $v_{i_j} \in X \backslash Y$, so there is $s_i \in S$ with $v_{i_j}(s_i) > 0$. Put $s := s_1 \cdots s_n$. Then for all sufficiently large $N \in \mathbb{Z}^+$ and all $1 \leqslant j \leqslant n$ we have $v_{i_j}(s^N x) \geqslant 0$, so $s^N x \in R$, so $x \in S^{-1}R$.
b) The family $\{v_i\}_{i \in Y}$ of discrete valuations on K satisfies (KDV1) and (KDV2) with respect to $S^{-1}R$, so $S^{-1}R$ is a Krull domain. □

There is a partial converse:

EXERCISE 22.1. *Let $\{v_i\}_{iinX}$ be a defining family of valuations on a Krull domain R. For $i \in X$, let R_i be the valuation ring of v_i. Let $Y \subseteq X$, and put $R_Y := \bigcap_{i \in Y} R_i$. Show: R_Y is a Krull domain.*
(Note though that R_Y need not be a localization of R: we have seen counterexamples already when R is Dedekind.)

EXERCISE 22.2. *Let R be a Krull domain with fraction field K, and let k be a subfield of K. Show: $R \cap k$ is a Krull domain.*

Thus the class of Krull domains is "localizable." However, being a Krull domain is *not* a local property: that is, for a domain R we may have that $R_\mathfrak{p}$ is a Krull domain for all $\mathfrak{p} \in \operatorname{Spec} R$ without R being a Krull domain: later we will see that a one-dimensional Krull domain is a Dedekind domain, so any almost Dedekind domain that is not Dedekind is a domain that is locally Krull but not Krull. On the other hand, it will turn out that among Noetherian domains, being a Krull domain is a local property: indeed, it will turn out to be equivalent to a local property that we already know.

PROPOSITION 22.3. *Let R be a Krull domain with fraction field K.*

a) *R is completely integrally closed.*
b) *The monoid $D(R)$ of divisors is a lattice-ordered group.*

PROOF. a) Let $\{v_i\}_{i \in X}$ be a family of valuations on K satisfying (KDV1) and (KDV2), and for each $i \in X$ we let R_i be the valuation ring of v_i, a DVR, so $R = \bigcap_{i \in X} R_i$. Each R_i is completely integrally closed by Exercise 17.23 and it is immediate that a domain that is an intersection of a family of completely integrally closed overrings is itself compeltely integrally closed.
b) By Theorem 19.30, for a domain R, the lattice-ordered monoid $D(R)$ is a group if and only if R is completely integrally closed. □

Thus any Krull domain R has a divisor class group $\operatorname{Cl} R$. Recall that for any completely integrally closed domain R, the Picard group $\operatorname{Pic} R$ is a subgroup of the divisor class group $\operatorname{Cl} R$, with equality if and only if each divisorial ideal is invertible. So clearly in a Dedekind domain these groups coincide and we may just speak of the "class group." We know that a Dedekind domain is a PID if and only if it is a UFD if and only if its class group is trivial. We will see in this chapter that a Krull domain is a UFD if and only if its divisor class group $\operatorname{Cl} R$ is trivial, but that there are Krull domains R with trivial Picard group that are not UFDs.

Let R be a Krull domain, and let $\{v_i\}_{i\in X}$ be a normed defining family of discrete valuations on the fraction field K of R. For $i \in X$ and a fractional R-ideal I, let $x \in I^\bullet$ and let $a \in K^\times$ be such that $I \subseteq (a)$. Then $(x) \subseteq (a)$, so there is $y \in R$ with $x = ya$ and thus $v_i(x) = v_i(y) + v_i(a) \geqslant v_i(a)$. It follows that

$$v_i(I) \coloneqq \max\{v_i(a) \mid I \subseteq (a)\}$$

is well-defined. Moreover, we claim that for fixed I, we have $v_i(I) \neq 0$ for only finitely many $i \in X$. Indeed, let $x, a \in K^\times$ be such that

$$(x) \subseteq I \subseteq (a).$$

Then for all $i \in X$ we have $v_i(a) \leqslant v_i(I) \leqslant v_i(x)$, and by (KDV2) we have $v_i(a) = v_i(x) = 0$ for all but finitely many $i \in X$. Recall that for fractional ideals I, J we put $I \sim J$ if $\overline{I} = \overline{J}$ and that $\operatorname{div} I$ is the $\sim$-equivalence class of I. We have $I \sim J$ if and only if I and J are contained in the same principal fractional ideals, it follows that if $I \sim J$ we have $v_i(I) = v_i(J)$.

Proposition 22.4. *Let R be a Krull domain with defining family of valuations $\{v_i\}_{i\in X}$. For $I, J \in \operatorname{Frac} R$, the following are equivalent:*

(i) *We have $I \geqslant J$.*
(ii) *We have $v_i(I) \geqslant v_i(J)$ for all $i \in X$.*

Proof. We have $I \geqslant J \iff \overline{I} \subseteq \overline{J}$, so by the above remarks we may assume that I and J are divisorial and show that $I \subseteq J \iff v_i(I) \geqslant v_i(J)$ for all $i \in X$. If $I \subseteq J$ then for all $a \in K^\times$, if $J \subseteq (a)$ then also $I \subseteq (a)$, so $v_i(I) \leqslant v_i(J)$ for all $i \in X$. Conversely, suppose that $v_i(I) \geqslant v_i(J)$ for all $i \in X$. Let $x \in I$, so $v_i(x) \geqslant v_i(I)$ for all $i \in I$. If $J \subseteq (b)$, then $v_i(x) \geqslant v_i(I) \geqslant v_i(J) \geqslant v_i(b)$, so $v_i(\frac{x}{b}) \geqslant 0$ for all $i \in X$, so $x \in (b)$. Thus every element of I lies in every principal fractional ideal containing J, so $I \subseteq J$ because J is divisorial. □

Let $\mathbb{Z}^{(X)} \coloneqq \bigoplus_{i\in X} \mathbb{Z}[i]$ be the free commutative group on the set X. We may define

$$\varphi : D(R) \to \mathbb{Z}^{(X)},\ I \mapsto (v_i(I)).$$

The group $\mathbb{Z}^{(X)}$ has a natural partial ordering, the product ordering from the total ordering on each of its factors. This makes $\mathbb{Z}^{(X)}$ into an Artinian lattice-ordered group. A map $f : (X, \leqslant) \to (Y, \leqslant)$ of partially ordered sets is **strongly isotone** if for all $x_1, x_2 \in X$ we have $x_1 \leqslant x_2$ if and only if $f(x_1) \leqslant f(x_2)$. The point is that for partially ordered sets, an isotone bijection need not be an order-isomorphism, but a strongly isotone bijection must be. It is immediate from Proposition 22.4 that the map φ is a strongly isotone injection, so $D(R)$ is also Artinian. Recalling that our ordering on divisors orders divisorial ideals by *reverse* inclusion, we have shown that in a Krull domain, the ascending chain condition holds on divisorial

ideals: let us call this condition **(ACCD)**.

Thus at this point we know two purely ring-theoretic facts about Krull domains: they are completely integrally closed and they satisfy (ACCD). It turns out that these are characteristic properties:

THEOREM 22.5. *For a domain R, the following are equivalent:*

(i) *R is a Krull domain.*

(ii) *R is completely integrally closed and satisfies (ACCD).*

PROOF. Let K be the fraction field of R. We just saw that (i) $\implies$ (ii), so let R be a completely integrally closed domain that satisfies (ACCD). Again we stop to mention the order reversal: (ACCD) on divisorial ideals means that the set $D(R)$ of divisors is Artinian: every nonempty subset has a minimum. Of course we may, and shall, assume that R is not a field, so the set of proper divisorial ideals of R is nonempty, hence the set $\{\mathfrak{p}_i\}_{i \in X}$ of minimal positive elements of $D(R)$ (these the maximal elements in the set of proper, integral divisorial elements) is nonempty.

Step 1: Because R is completely integrally closed, the divisorial fractional ideals $D(R)$ form a lattice-ordered group $D(R)$ with positive cone $D^+(R)$ of divisorial integral ideals. We claim that every element of $D^+(R)$ is a finite $\mathbb{N}$-linear combination of the minimal positive elements. This is a familiar argument: if not, then because $D^+(R)$ is Artinian there must be a minimal element $I \in D^+(R)$ that cannot be expressed as such a combination. So we must have $0 < \mathfrak{p}_i < I$ for some $i \in I$ and then $0 < I - \mathfrak{p}_i < I$, so $I - \mathfrak{p}_i$ is an $\mathbb{N}$-linear combination of the minimal elements, which means that I is: contradiction. Since every element of $D(R)$ is a difference of two elements of $D^+(R)$, it follows that $\{\mathfrak{p}_i\}_{i \in X}$ is a set of generators for $D(R)$.
Step 2: We claim that $D^+(R) = \bigoplus_{i \in X} \mathbb{N}[\mathfrak{p}_i]$ as a partially ordered commutative monoid: that is, every element of $D^+(R)$ has a *unique* expression as $\sum_{i \in X} m_i \mathfrak{p}_i$ and that $\sum_{i \in X} m_i \mathfrak{p}_i \leqslant \sum_{i \in X} n_i \mathfrak{p}_i$ if and only if $m_i \leqslant n_i$ for all $i \in X$. It is clear that if $m_i \leqslant n_i$ for all $i \in X$ then $\sum_{i \in X} m_i \mathfrak{p}_i \leqslant \sum_{i \in X} n_i \mathfrak{p}$.
Step 2a): Suppose that we have $I, J \in D^+(R)$ such that $\mathfrak{p}_i \leqslant I + J$. We claim that either $\mathfrak{p}_i \leqslant I$ or $\mathfrak{p}_i \leqslant J$. Indeed, by the minimality of $\mathfrak{p}_i$, we have either $\mathfrak{p}_i \cap I = I$ or $\mathfrak{p}_i \cap I = 0$. In the former case we have $\mathfrak{p}_i \leqslant I$, so suppose that $\mathfrak{p}_i \cap I = 0$. Then certainly

$$J \leqslant (\mathfrak{p}_i + J) \cap (I + J).$$

If for $M \in D^+(R)$ we have $M \leqslant \mathfrak{p}_i + J$ and $M \leqslant I + J$, then $M - J \leqslant \mathfrak{p}_i \cap I = 0$, so $M \leqslant J$; this shows that

$$J \geqslant (\mathfrak{p}_i + J) \cap (I + J),$$

and thus

$$J = (\mathfrak{p}_i + J) \cap (I + J),$$

which implies $\mathfrak{p}_i \leqslant J$.
Step 2b): It follows by induction that if $I_1, \ldots, I_n > 0$ and $\mathfrak{p}_i \leqslant I_1 + \ldots + I_n$, then $\mathfrak{p}_i \leqslant I_j$ for some $1 \leqslant j \leqslant n$.
Step 2c): Now suppose that we have

$$\sum_{i \in X} m_i \mathfrak{p}_i \leqslant \sum_{i \in X} n_i \mathfrak{p}_i,$$

and, seeking a contradiction, that $m_i > n_i$ for some $i \in X$. Thus the set

$$Y := \{i \in X \mid m_i > n_i\}$$

is nonempty. Put

$$b_i := \begin{cases} m_i - n_i & i \in Y \\ n_i - m_i & i \notin Y \end{cases}.$$

Then

$$\sum_{i \in Y} b_i \mathfrak{p}_i \leqslant \sum_{j \in X \backslash Y} b_j \mathfrak{p}_j.$$

Since Y is nonempty, the left hand side is strictly positive, hence so is the right hand side. By Step 2b), for each $i \in Y$ there is $j \in X \backslash Y$ such that $\mathfrak{p}_i \leqslant \mathfrak{p}_j$: contradiction. Step 3: For $x \in K^\times$, after Step 2 we may uniquely write

$$\operatorname{div}(x) = \sum_{i \in X} n_i(x) \mathfrak{p}_i.$$

For $i \in X$ we may define $v_i : K^\times \to \mathbb{Z}$ by $v_i(x) := n_i(x)$. For $x, y \in K^\times$,

$$\operatorname{div}(xy) = \operatorname{div}(x) + \operatorname{div}(y) = \sum_{i \in X} (n_i(x) + n_i(y)) \mathfrak{p}_i,$$

so $v_i(xy) = v_i(x) + v_i(y)$. Moreover $\operatorname{div}(x) \wedge \operatorname{div}(y) = \operatorname{div}(\langle x, y \rangle) \leqslant div(x+y)$. Also

$$(\sum_{i \in X} m_i \mathfrak{p}_i) \wedge (\sum_{i \in X} n_i \mathfrak{p}_i) = \sum_{i \in I} \min(m_i, n_i) \mathfrak{p}_i.$$

So if $x + y \neq 0$, then

$$\operatorname{div}(x+y) = \sum_{i \in X} c_i \mathfrak{p}_i \geqslant \sum_{i \in X} \min(m_i, n_i) \mathfrak{p}_i,$$

so for all $i \in X$ we have $v_i(x+y) \geqslant \min(v_i(x), v_i(y))$. Thus each v_i is a discrete valuation on K. It is immediate that the family of valuations $\{v_i\}_{i \in X}$ satisfies (KDV2). Moreover, for $x \in K^\times$, if $v_i(x) \geqslant 0$ then $\operatorname{div}(x) \geqslant 0$, so $x \in R$, and conversely $x \in R^\bullet$ implies $v_i(x) \geqslant 0$ for all $i \in X$. Thus $\{v_i\}_{i \in X}$ shows that R is a Krull domain. □

Corollary 22.6. *A Noetherian integrally closed domain is a Krull domain.*

Proof. A Noetherian integrally closed domain is completely integrally closed and satisfies (ACCD), so this is immedaite from Theorem 22.5. □

2. Essential Valuations

Let R be a Krull domain. The proof of Theorem 22.5 gives us a canonical defining family $\{v_i\}_{i \in X}$ of discrete valuations on R, namely the ones corresponding to ideals of R that are maximal among proper divisorial ideals. We call such valuations **essential**. For $i \in X$, let $\mathcal{P}_i$ be the divisorial ideal of R such that $\operatorname{div}(\mathcal{P}_i) = \mathfrak{p}_i$.

For any divisorial fractional R-ideal I and $x \in K^\times$, we may uniquely write $\operatorname{div} I = \sum_{i \in X} n_i \mathfrak{p}_i$, and we have $x \in I$ if and only if $(x) \subseteq I$ if and only if $\operatorname{div}(x) \geqslant \operatorname{div}(I)$ if and only if $v_i(x) \geqslant n_i$ for all $i \in X$. Conversely, given any $(n_i) \in \bigoplus_{i \in X} \mathbb{Z}[\mathfrak{p}_i]$, then

$$I := \{x \in K^\times \mid v_i(x) \geqslant n_i\} \cup \{0\}$$

is the divisorial fractional ideal with divisor $\sum_{i \in X} n_i \mathfrak{p}_i$.

Now let I be a fractional R-ideal. By Proposition 22.4, for $x \in K^\times$ we have $x \in \overline{I}$ if and only if $v_i(x) \geqslant v_i(I)$ for all $i \in I$. It follows that

$$\operatorname{div}(I) = \sum_{i \in I} v_i(I) \mathfrak{p}_i. \tag{60}$$

Let Y be a set, and suppose that for each $j \in Y$ we have a divisorial fractional ideal I_j of R such that $I \coloneqq \langle I_j \mid j \in Y\rangle_R$ is a fractional R-ideal. Since $I \supseteq I_j$ for all $j \in Y$ we have $\operatorname{div}(I) \leqslant \operatorname{div}(I_j)$ for all $j \in Y$. If J is a divisorial fractional ideal such that $J \leqslant \operatorname{div}(I_j)$ for all j then $J \supseteq I_j$ for all j, so $J \supseteq I$ and thus $\operatorname{div} J \leqslant \operatorname{div}(I)$. It follows that $\operatorname{div}(I)$ is the infimum of $\{\operatorname{div}(I_j) \mid j \in Y\}$ in $D(R)$. Let $I \in \operatorname{Frac} R$. Applying this observation to the family of principal fractional ideals contained in I, we get that $\operatorname{div}(I)$ is the infimum of the set $\operatorname{div}(x)$ for $x \in I^\bullet$. It follows that

$$\operatorname{div}(I) = \sum_{i \in X} \min\{v_i(x) \mid x \in I^\bullet\}\mathfrak{p}_i. \tag{61}$$

Comparing (60) and (61), we deduce:

$$\forall I \in \operatorname{Frac}(R),\ \forall i \in X,\ v_i(I) = \min\{v_i(x) \mid x \in I^\bullet\}.$$

From this we deduce that for every $i \in X$, we have $v_i(K^\times) = \mathbb{Z}$. Indeed, certainly $v_i(K^\times)$ is a subgroup of $\mathbb{Z}$. Conversely, let I be the divisorial ideal with $\operatorname{div}(I) = 2\mathfrak{p}_i$. Since $v_i(I) = 2$, we have $I \subsetneq \mathcal{P}_i$. If $x \in \mathcal{P}_i \backslash I$, then

$$\mathfrak{p}_i \leqslant \operatorname{div}(x) < 2\mathfrak{p}_i,$$

so $v_i(x) = 1$.

Above, for any defining family $\{v_i\}_{i\in X}$ of valuations on a Krull domain R, we defined a map $\varphi : D(R) \to \mathbb{Z}^{(X)} \coloneqq \bigoplus_{i\in X} \mathbb{Z}$, $\operatorname{div}(I) \mapsto (v_i(I))$ and showed that this is a strongly isotone injection. When we restrict to the family of essential valuations, we can prove a more precise result:

THEOREM 22.7. *Let R be a Krull domain, and let $\{v_i\}_{i\in X}$ be the set of essential valuations of R. The map*

$$\varphi : D(R) \to \mathbb{Z}^{(X)},\ \operatorname{div}(I) \mapsto (v_i(I)),$$

is an isomorphism of lattice-ordered groups.

PROOF. In fact, all that remains is to show that φ is a group homomorphism. Indeed, we already know that φ is a strongly isotone injection whose image contains the elements $\mathfrak{p}_i$ for $i \in X$. But $\mathbb{Z}^{(X)}$ is generated by $\{\mathfrak{p}_i\}_{i\in X}$, so φ is then a strongly isotone group isomorphism, hence an isomorphism of lattice-ordered groups.

Let I and J be divisorial fractional ideals. We must show that for all $i \in X$, $v_i(IJ) = v_i(I)+v_i(J)$. We may choose $x \in I^\bullet$ and $y \in J^\bullet$ such that $v_i(I) = v_i(x)$ and $v_i(J) = v_i(y)$. Then $xy \in IJ \subseteq \overline{IJ}$, so $v_i(IJ) \geqslant v_i(I)+v_i(J)$. On the other hand, we may choose $a, b \in K^\times$ such that $I \subseteq (a)$, $J \subseteq (b)$ and $v_i(I) = v_i(a)$, $v_i(J) = v_i(b)$, and then $IJ \subseteq (ab)$, so $v_i(IJ) \geqslant v_i(ab) = v_i(a) + v_i(b) = v_i(I) + v_i(J)$. □

PROPOSITION 22.8. *Let R be a Krull domain, with fraction field K, and let $\{v_i\}_{i\in X}$ be the set of essential valuations of R. For $i \in X$, the ideal $\mathcal{P}_i$ is a prime ideal of R. If R_i is the valuation ring of v_i, then $R_i = R_{\mathcal{P}_i}$.*

PROOF. Let $\mathfrak{m}_i$ be the maximal ideal of the DVR R_i. For $x \in R^\bullet$ we have $v_i(x) > 0$ if and only if $x \in \mathcal{P}_\rangle$, so

$$\mathcal{P}_i = \mathfrak{m}_i \cap R$$

and thus $\mathcal{P}_i$ is a prime ideal of R. By Proposition 22.2, if

$$Y \coloneqq \{j \in X \mid v_j(s) = 0\ \forall s \in R\backslash\mathcal{P}_i\},$$

then $R_{\mathcal{P}_\setminus} = \bigcap_{j \in Y} R_j$, so it suffices to show that $S = \{i\}$. Clearly $i \in Y$; conversely, if $j \in X \backslash \{i\}$, then $\mathcal{P}_j$ and $\mathcal{P}_i$ are distinct ideals that are both maximal among proper divisorial ideals of R, so $\mathcal{P}_j \nsubseteq \mathcal{P}_i$: that is, there is $s \in R \backslash \mathcal{P}_i$ such that $v_j(s) > 0$, so $j \notin Y$. □

THEOREM 22.9. *Let R be a Krull domain, and let $\{v_i\}_{i \in X}$ be the set of essential valuations. For $\mathfrak{p} \in \operatorname{Spec} R$, the following are equivalent:*

(i) *$\mathfrak{p}$ is divisorial.*
(ii) *$\mathfrak{p} = \mathcal{P}_i$ for some $i \in X$.*
(iii) *$\operatorname{ht}(\mathfrak{p}) = 1$.*

PROOF. (i) $\implies$ (ii): Suppose $\mathfrak{p}$ is divisorial, so

$$\operatorname{div} \mathfrak{p} = \sum_{i \in X} n_i \mathfrak{p}_i = \sum_{i \in X} n_i \operatorname{div} \mathcal{P}_i = \operatorname{div} \prod_{i \in X} \mathcal{P}_i^{n_i}.$$

It follows that $\mathfrak{p} \supseteq \prod_{i \in X} \mathfrak{p}_i^{n_i}$, and since $\mathfrak{p}$ is prime we have $\mathfrak{p} \supseteq \mathfrak{p}_i$ for some i. Since $\mathfrak{p}_i$ is maximal among proper divisorial ideals of R, we have $\mathfrak{p} = \mathfrak{p}_i$.
(ii) $\implies$ (i) is immediate: the primes $\mathcal{P}_i$ are divisorial by definition.
(ii) $\implies$ (iii): By Proposition 22.8, for $i \in X$ we have $R_{\mathcal{P}_i} = R_i$ is a DVR, so $\mathcal{P}_i$ has height one.
(iii) $\implies$ (ii): Let $\mathfrak{p} \in \operatorname{Spec}_1 R$. By Propositions 22.2 and 22.8, there is a nonempty subset $Y \subseteq X$ such that $R_{\mathfrak{p}} = \bigcap_{i \in Y} R_{\mathcal{P}_i}$. Choose $i \in Y$. (It will shortly become clear that we did not really have a choice.) Then we have $R_{\mathfrak{p}} \subseteq R_{\mathcal{P}_i}$, which implies that $\mathcal{P}_i \subseteq \mathfrak{p}$. Since $\mathfrak{p}$ has height 1, we have $\mathfrak{p} = \mathcal{P}_i$. □

COROLLARY 22.10. *For a domain R, the following are equivalent:*

(i) *R is a Krull domain.*
(ii) *All of the following hold:*
  (a) *For all $\mathfrak{p} \in \operatorname{Spec}_1 R$, the local ring $R_{\mathfrak{p}}$ is a DVR.*
  (b) *We have $R = \bigcap_{\mathfrak{p} \in \operatorname{Spec}_1 R} R_{\mathfrak{p}}$.*
  (c) *Every $x \in R^\bullet$ lies in only finitely many height one primes.*

PROOF. (i) $\implies$ (ii): Immediate from Proposition 22.8 and Theorem 21.8.
(ii) $\implies$ (i): If conditions (a), (b) and (c) hold, then each height one prime defines a discrete valuation, and this family of valuations satisfies (KDV1) and (KDV2), so R is a Krull domain and this is the family of essential valuations on R. □

THEOREM 22.11. *For a Krull domain R, the following are equvialent:*

(i) *R is a UFD.*
(ii) *$\operatorname{Cl} R = 0$.*

PROOF. (i) $\implies$ (ii): If R is a UFD, then by Corollary 15.2 every $\mathfrak{p} \in \operatorname{Spec}_1 R$ is principal. But $\operatorname{Cl} R$ is generated the divisors of height one primes, so every divisor is principal: $\operatorname{Cl} R = 0$.
(ii) $\implies$ (i): Conversely, $\operatorname{Cl} R = 0$ implies that every height one prime of R is principal. Thus every essential valuation of R is of the form v_π for a prime element π, which means that for $x \in R^\bullet$, we have $v_\pi(x) = n$ if and only if $x \in (\pi^n) \backslash (\pi^{n+1})$. Let $\mathcal{P}$ be a maximal set of mutually nonassociate prime elements – i.e., we choose exactly one generator of each nonzero principal prime ideal. Then for $x \in R^\bullet$,

$$y := \prod_{\pi \in \mathcal{P}} \pi^{v_\pi(x)} \in R^\bullet$$

is well-defined, and $\operatorname{div}(x) = \operatorname{div}(y)$, so $div(x/y) = 0$, so $(x) = (y)$, and thus there is $u \in R^\times$ such that

$$x = u \prod_{\pi \in \mathcal{P}} \pi^{v_\pi(x)}.$$

So every element of $R^\bullet$ is a product of prime elements, and thus R is a UFD. □

EXERCISE 22.3. *Show: Krull domains satisfy the Krull Intersection Theorem: if I is a proper ideal in a Krull domain, then $\bigcap_{n \geqslant 1} I^n = (0)$.*

THEOREM 22.12. *For a Krull domain R that is not a field, the following are equivalent:*

(i) $\dim R = 1$.
(ii) *R is a Dedekind domain.*
(iii) *R is a Prüfer domain.*

PROOF. (i) $\implies$ (ii): the localization of a Krull domain at a height one prime is a DVR, so if $\dim R = 1$ then the localization of R at each maximal ideal is a DVR: thus, R is almost Dedekind. Moreover, (VDK2) implies that R has finite character, so R is Dedekind by Theorem 20.35.
(ii) $\implies$ (iii): Every Dedekind domain is a Prüfer domain.
(iii) $\implies$ (i): Suppose that R is both Krull and Prüfer. For every $\mathfrak{m} \in \operatorname{MaxSpec} R$, the local ring $R_\mathfrak{m}$ is a Krull domain by Proposition 22.2 and a valuation ring by Theorem 20.23 it is a valuation ring. By Exercise 22.3 we have $\bigcap_{n \geqslant 1} \mathfrak{m}_\mathfrak{m}^n = (0)$, so by Theorem 17.16 the ring $R_\mathfrak{m}$ is a DVR. Thus R has dimension 1. □

3. Integral Closure

LEMMA 22.13. *Let K be a field, and let $v : K^\times \to \mathbb{R}$ be a discrete valuation, with valuation ring R. Let L/K be an algebraic field extension. Let $x \in L$, and let $f = t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 \in K[t]$ be the minimal polynomial of x. If $w(x) \geqslant 0$ for every valuation w on L that extends v, then $f \in R[t]$.*

PROOF. Put $L' := K[x]$. Every extension of v to a valuation v' on L' is still discrete, and by Exercise 21.2 v' extends to a valuation on L. Thus the hypothesis is equivalent to assuming that $v'(x) \geqslant 0$ for every valuation v' on L extending v, so we may assume that $L = L'$, i.e., that L/K has finite degree. And we shall.

Let M be the normal closure of L/K, and let $\tilde{w}$ be an extension of v to M. For $\sigma \in \operatorname{Aut}(M/K)$, the map

$$\sigma^* \tilde{w} : M^\times \to \mathbb{R},\ x \mapsto \tilde{w}(\sigma(x))$$

is a valuation on M that extends v, hence so does its restriction to L, and thus

$$\sigma^* \tilde{w}(x) = \tilde{w}(\sigma(x)) \geqslant 0.$$

Since M/K is normal and contains the root x of f, in M the polynomial splits, say

$$f = (t - x_1) \cdots (t - x_n),\ \text{with } x_1 = x.$$

For each $1 \leqslant i \leqslant n$ there is $\sigma \in \operatorname{Aut}(M/K)$ with $\sigma(x) = x_i$, and thus $\tilde{w}(x_i) \geqslant 0$ for all $1 \leqslant i \leqslant n$. Since for $0 \leqslant i \leqslant n-1$, the coefficient a_i of t^i in f is a symmetric polynomial in the roots $x_1, \ldots, x_n$ with coefficients in $\mathbb{Z}$, it follows that $v(a_i) = \tilde{w}(a_i) \geqslant 0$, so $f \in R[t]$. □

REMARK 8. *Using the fact that every valuation extends to every algebraic field extension, Lemma 22.13 can be extended to all valuations, not just discrete ones.*

THEOREM 22.14. *Let R be a Krull domain with fraction field K, let L/K be a finite degree field extension, and let T be the integral closure of R in L. Then T is a Krull domain.*

PROOF. Let $\{v_i\}_{i \in I}$ be the set of essential valuations of R, and let $\{w_j\}_{j \in J}$ be the set of valuations on L that extend some v_i. For $j \in J$, let T_j be the valuation ring of w_j; by Corollary 17.10, each T_j is a DVR. We claim that $\{w_j\}_{j \in J}$ is a defining family of discrete valuations for T: if so, T is a Krull domain.

Step 1: Put $\tilde{T} := \bigcap_{j \in J} T_j$. We will show that $T = \tilde{T}$, establishing (KDV1).
Step 1a): As we saw in the proof of Theorem 17.11, If we have a valuation v on a field K, subring R of K such that $v(x) \geqslant 0$ for all $x \in R^\bullet$ and an element y that is integral over R, then $v(y) \geqslant 0$. It follows that $T \subseteq \tilde{T}$.

Step 1b): Let $x \in \tilde{T}$, and let $f \in K[t]$ be the minimal polynomial of x. Lemma 22.13 implies that for all $i \in I$ we have $f \in R_i[t]$, so $f \in (\bigcap_{i \in I} R_i)[t] = R[t]$. Thus x is integral over R, so $x \in T$.
Step 2: Let $x \in T^\bullet$, so there are $a_0, \ldots, a_{n-1} \in R$ with $a_0 \neq 0$ such that

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0. \tag{62}$$

For all but finitely many $i \in I$, we have $a_j \neq 0 \implies v_i(a_j) = 0$. Choose such an i. For any $j \in J$ such that w_j extends v_i, we CLAIM that $w_j(x) = 0$. If so, then Theorem 17.11 implies that there are only finitely many $j \in J$ such that w_j extends v_i, so the set of j such that $w_j(x) \neq 0$ is finite, establishing (KDV2).

To establish the claim: if $w_j(x) > 0$, the unique term of minimal valuation in the left hand side of (62) is a_0, so the valuation of the left hand side is 0, contradiction. If $w_j(x) < 0$, the unique term of minimal valuation in the left hand side of (62) is x^n, so the valuation of the left hand side is $v(x^n)$, contradiction. $\square$

Bibliography

[AB59] M. Auslander and D.A. Buchsbaum, *Unique factorization in regular local rings.* Proc. Nat. Acad. Sci. U.S.A. 45 (1959), 733–734.

[Ab73] S. Abhyankar, *On Macaulay's examples.* Notes by A. Sathaye. Lecture Notes in Math., Vol. 311, Conference on Commutative Algebra (Univ. Kansas, Lawrence, Kan., 1972), pp. 1–16, Springer, Berlin-New York, 1973.

[Ad62] J.F. Adams, *Vector fields on spheres.* Ann. of Math. (2) 75 (1962), 603–632.

[AHRT] J. Adámek, H. Herrlich, J. Rosický and W. Tholen, *Injective hulls are not natural.* Algebra Universalis 48 (2002), 379–388.

[AKP98] D.D. Anderson, B.G. Kang and M.H. Park, *Anti-Archimedean rings and power series rings.* Comm. Algebra 26 (1998), 3223—3238.

[Al63] N.L. Alling, *The valuation theory of meromorphic function fields over open Riemann surfaces.* Acta Math. 110 (1963), 79–96.

[Al99] N. Alon, *Combinatorial Nullstellensatz.* Recent trends in combinatorics (Mátraháza, 1995). Combin. Probab. Comput. 8 (1999), 7–29.

[An00] D.D. Anderson, *GCD domains, Gauss' lemma, and contents of polynomials.* Non-Noetherian commutative ring theory, 1–31, Math. Appl., 520, Kluwer Acad. Publ., Dordrecht, 2000.

[AR97] D.D. Anderson and M. Roitman, *A characterization of cancellation ideals.* Proc. Amer. Math. Soc. 125 (1997), 2853–2854.

[AZ94] D.D. Anderson and M. Zafrullah, *On a theorem of Kaplansky.* Boll. Un. Mat. Ital. A (7) 8 (1994), 397–402.

[AP82] J.K. Arason and A. Pfister, *Quadratische Formen über affinen Algebren und ein algebraischer Beweis des Satzes von Borsuk-Ulam.* (German) J. Reine Angew. Math. 331 (1982), 181–184.

[Ar27] E. Artin, *Zur Theorie der hyperkomplexen Zahlen.* Abh. Hamburg, 5 (1927), 251-260.

[Ar73] J.T. Arnold, *Krull dimension in power series rings.* Trans. Amer. Math. Soc. 177 (1973), 299–304.

[AT51] E. Artin and J.T. Tate, *A note on finite ring extensions.* J. Math. Soc. Japan 3 (1951), 74–77.

[At89] M.F. Atiyah, *K-theory.* Notes by D. W. Anderson. Second edition. Advanced Book Classics. Addison-Wesley Publishing Company, Redwood City, CA, 1989.

[AM] M.F. Atiyah and I.G. Macdonald, *Introduction to commutative algebra.* Addison-Wesley Publishing Co., Reading Mass.-London-Don Mills, Ont. 1969.

[Ba40] R. Baer, *Abelian groups that are direct summands of every containing commutative group.* Bull. Amer. Math. Soc. 46 (1940), 800–806.

[Ba59] H. Bass, *Global dimension of rings*, Ph.D. Thesis, University of Chicago, 1959.

[Ba63] H. Bass, *Big projective modules are free.* Illinois J. Math. 7 1963 24–31.

[Ba62] G. Baumslag, *On abelian hopfian groups. I.* Math. Z. 78 1962 53–54.

[Ba63] G. Baumslag, *Hopficity and commutative groups.* 1963 Topics in Abelian Groups (Proc. Sympos., New Mexico State Univ., 1962) pp. 331–335 Scott, Foresman and Co., Chicago, Ill.

[BCR] J.Bochnak, M. Coste and M.-F. Roy, *Real algebraic geometry.* Ergebnisse der Mathematik und ihrer Grenzgebiete (3) 36. Springer-Verlag, Berlin, 1998.

[Be] D.J. Benson, *Polynomial invariants of finite groups* London Mathematical Society Lecture Note Series, 190. Cambridge University Press, Cambridge, 1993.

[Bo50] S. Borofsky, *Factorization of polynomials.* Amer. Math. Monthly 57 (1950), 317–320.

[BM58] R. Bott and J. Milnor, *On the parallelizability of the spheres.* Bull. Amer. Math. Soc. 64 (1958), 87–89.

[B] N. Bourbaki, *Commutative algebra. Chapters 1–7.* Translated from the French. Reprint of the 1989 English translation. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998.

[BM03] F. Bayart and A. Mouze, *Factorialité de l'anneau des séries de Dirichlet analytiques.* C. R. Math. Acad. Sci. Paris 336 (2003), 213–218.

[Bo78] A. Bouvier, *Le groupe des classes de l'algebre affine d'une forme quadratique.* Publ. Dép. Math. (Lyon) 15 (1978), no. 3, 53–62.

[BMRH] J.W. Brewer, P.R. Montgomery, E.A. Rutter and W.J. Heinzer, *Krull dimension of polynomial rings.* Conference on Commutative Algebra (Univ. Kansas, Lawrence, Kan., 1972), pp. 26-45. Lecture Notes in Math., Vol. 311, Springer, Berlin, 1973.

[Br02] G. Brookfield, *The length of Noetherian modules.* Comm. Algebra 30 (2002), 3177–3204.

[Br81] A. Brumer, *The class group of all cyclotomic integers.* J. Pure Appl. Algebra 20 (1981), no. 2, 107–111.

[Bu61] D.A. Buchsbaum, *Some remarks on factorization in power series rings.* J. Math. Mech. 10 1961 749–753.

[Ca60] L. Carlitz, *A Characterization of Algebraic Number Fields with Class Number Two.* Proc. AMS 11 (1960), 391–392.

[Cd-SF] K. Conrad, *Stably Free Modules.* Notes available at `http://www.math.uconn.edu/~kconrad/blurbs/linmultialg/stablyfree.pdf`

[CDVM13] L.F. Cáceres Duque and J.A. Vélez-Marulanda, *On the Infinitude of Prime Elements.* Rev. Colombiana Mat. 47 (2013), 167–179.

[CE] H. Cartan and S. Eilenberg, *Homological algebra.* Princeton University Press, Princeton, N. J., 1956.

[CE59] E.D. Cashwell and C.J. Everett, *The ring of number-theoretic functions.* Pacific J. Math. 9 (1959) 975–985.

[CK51] I.S. Cohen and I. Kaplansky, *Rings for which every module is a direct sum of cyclic modules.* Math. Z. 54 (1951), 97–101.

[Cl66] L.E. Claborn, *Every commutative group is a class group.* Pacific J. Math. 18 (1966), 219–222.

[Cl-GT] P.L. Clark, *General Topology.* `http://math.uga.edu/~pete/pointset2018.pdf`.

[Cl09] P.L. Clark, *Elliptic Dedekind domains revisited.* Enseignement Math. 55 (2009), 213–225.

[Cl15] P.L. Clark, *A note on Euclidean order types.* Order 32 (2015), 157–178.

[Cl17a] P.L. Clark, *The Euclidean criterion for irreducibles.* Amer. Math. Monthly 124 (2017), 198–216.

[Cl17b] P.L. Clark, *The cardinal Krull dimension of a ring of holomorphic functions.* Expo. Math. 35 (2017), 350–356.

[Cn68] P.M. Cohn, *Bézout rings and their subrings.* Proc. Cambridge Philos. Soc. 64 (1968), 251–264.

[Cn73] P.M. Cohn, *Unique factorization domains.* Amer. Math. Monthly 80 (1973), 1–18.

[Co46] I.S. Cohen, *On the structure and ideal theory of complete local rings.* Trans. Amer. Math. Soc. 59, (1946), 54–106.

[CS46] I.S. Cohen and A. Seidenberg, *Prime ideals and integral dependence.* Bull. Amer. Math. Soc. 52 (1946), 252–261.

[Co64] A.L.S. Corner, *On a conjecture of Pierce concerning direct decompositions of Abelian groups.* 1964 Proc. Colloq. Abelian Groups (Tihany, 1963) pp. 43–48 Akadémiai Kiadó, Budapest.

[Co11] D.A. Cox, *Why Eisenstein proved the Eisenstein criterion and why Schönemann discovered it first.* Amer. Math. Monthly 118 (2011), 3–21.

[Da09] C.S. Dalawat, *Wilson's theorem.* J. Théor. Nombres Bordeaux 21 (2009), 517–521.

[DM71] F. DeMeyer and E. Ingraham, *Separable algebras over commutative rings.* Lecture Notes in Mathematics, Vol. 181 Springer-Verlag, Berlin-New York 1971.

[Ea68] P.M. Eakin, Jr. *The converse to a well known theorem on Noetherian rings.* Math. Ann. 177 (1968), 278–282.

[EBK69] P. van Emde Boas and D. Kruyswijk, *A combinatorial problem on finite commutative groups, III*, Report ZW-1969-008, Math. Centre, Amsterdam, 1969.

[Ec00] O. Echi, *A topological characterization of the Goldman prime spectrum of a commutative ring.* Comm. Algebra 28 (2000), 2329–2337.

[ES53] B. Eckmann and A. Schopf, *Über injektive Moduln.* Arch. Math. (Basel) 4 (1953), 75–78.

[Ei] D. Eisenbud, *Commutative algebra. With a view toward algebraic geometry.* Graduate Texts in Mathematics, 150. Springer-Verlag, New York, 1995.

[Ei50] F. Eisenstein, *Über die Irredicibilität une einige andere Eigenschaften der Gleichung von welche der Theilung der ganzen Lemniscate abhängt.* J. Reine Angew. Math. 39 (1950), 160–179.

[ES] S. Eilenberg and N. Steenrod, *Foundations of Algebraic Topology.* Princeton University Press, 1952.

[Fo64] O. Forster, *Über die Anzahl der Erzeugenden eines Ideals in einem Noetherschen Ring.* Math. Z. 84 (1) (1964) 80-–87.

[FR70] R.L. Finney and J.J. Rotman, *Paracompactness of locally compact Hausdorff spaces.* Michigan Math. J. 17 (1970), 359–361.

[FT] *Field Theory*, notes by P.L. Clark, available at `http://www.math.uga.edu/~pete/FieldTheory.pdf`

[FW67] C. Faith and E.A. Walker, *Direct-sum representations of injective modules.* J. Algebra 5 (1967), 203–221.

[Fl71] C.R. Fletcher, *Euclidean rings.* J. London Math. Soc. 4 (1971), 79–82.

[Fo73] E. Formanek, *Faithful Noetherian modules.* Proc. Amer. Math. Soc. 41 (1973), 381–383.

[Fs73] R.M. Fossum, *The divisor class group of a Krull domain.* Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 74. Springer-Verlag, New York-Heidelberg, 1973.

[Fu59] L. Fuchs, *The existence of indecomposable commutative groups of arbitrary power.* Acta Math. Acad. Sci. Hungar. 10 (1959) 453–457.

[Fu74] L. Fuchs, *Indecomposable commutative groups of measurable cardinalities.* Symposia Mathematica, Vol. XIII (Convegno di Gruppi Abeliani, INDAM, Rome, 1972), pp. 233-244. Academic Press, London, 1974.

[Ga64] N. Ganesan, *Properties of rings with a finite number of zero divisors.* Math. Ann. 157 (1964), 215–218.

[Ga71] T.E. Gantner, *A Regular Space on which every Continuous Real-Valued Function is Constant.* Amer. Math. Monthly 78 (1971), 52–53.

[Ge91] R. Germundsson, *Basic Results on Ideals and Varieties in Finite Fields.* Technical report, Department of Electrical Engineering, Lïnkoping University, 1991.

[Gi64] R.W. Gilmer, *Integral domains which are almost Dedekind.* Proc. Amer. Math. Soc. 15 (1964), 813–818.

[Gi66] R.W. Gilmer, *Overrings of Prüfer domains.* J. Algebra 4 (1966), 331–340.

[Gi72] R. Gilmer, *On commutative rings of finite rank.* Duke Math. J. 39 (1972), 381—383.

[Gi74] R. Gilmer, *A two-dimensional non-Noetherian factorial ring.* Proc. Amer. Math. Soc. 44 (1974), 25–30.

[GJ76] L. Gillman and M. Jerison, *Rings of continuous functions.* Reprint of the 1960 edition. Graduate Texts in Mathematics, No. 43. Springer-Verlag, New York-Heidelberg, 1976.

[Gol51] O. Goldman, *Hilbert rings and the Hilbert Nullstellensatz.* Math. Z. 54 (1951). 136–140.

[Gol64] O. Goldman, *On a special class of Dedekind domains.* Topology 3 (1964) suppl. 1, 113–118.

[GoN] P.L. Clark, *Geometry of numbers with applications to number theory.* `http://math.uga.edu/~pete/geometryofnumbers.pdf`

[Gov65] V.E. Govorov, *On flat modules.* (Russian) Sibirsk. Mat. Ž. 6 (1965), 300–304.

[GoRo] R. Gordon and J.C. Robson, *Krull dimension.* Memoirs of the American Mathematical Society, No. 133. American Mathematical Society, Providence, R.I., 1973.

[GuRo] R.C. Gunning and H. Rossi, *Analytic functions of several complex variables.* Prentice-Hall, Inc., Englewood Cliffs, N.J. 1965.

[Gr74] A. Grams, *Atomic rings and the ascending chain condition for principal ideals.* Proc. Cambridge Philos. Soc. 75 (1974), 321–329.

[Gu73] T.H. Gulliksen, *A theory of length for Noetherian modules*. J. Pure Appl. Algebra 3 (1973), 159–170.

[Ha] R. Hartshorne, *Algebraic geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[Ha94] B. Haible, *Gauss' Lemma without Primes*, preprint, 1994.

[Ha28] H. Hasse, *Über eindeutige Zerlegung in Primelemente oder in Primhauptideale in Integrit-tsbereichen*. J. reine Angew. Math. 159 (1928), 3–12.

[He40] O. Helmer, *Divisibility properties of integral functions*. Duke Math. J. 6 (1940), 345–356.

[He53] M. Henriksen, *On the prime ideals of the ring of entire functions*. Pacific J. Math. 3 (1953), 711–720.

[He70] W. Heinzer, *Quotient overrings of an integral domain*. Mathematika 17 (1970), 139–148.

[He74] R.C. Heitmann, *PID's with specified residue fields*. Duke Math. J. 41 (1974), 565–582.

[He06] G. Hessenberg, *Grundbegriffe der Mengenlehre*. Göttingen, 1906.

[HH] J. Herzog and T. Hibi, *Monomial ideals*. Graduate Texts in Mathematics, 260. Springer-Verlag London, Ltd., London, 2011.

[Hi90] D. Hilbert, *Ueber die Theorie der algebraischen Formen*. Mathl Annalen 36 (1890), 473–534.

[Hi75] J.-J. Hiblot, *Des anneaux euclidiens dont le plus petit algorithme n'est pas à valeurs finies*.

[Hi77] J.-J. Hiblot, *Correction à une note sur les anneaux euclidiens: "Des anneaux euclidiens dont le plus petit algorithme n'est pas à valeurs finies" (C. R. Acad. Sci. Paris Sér. A-B 281 (1975), no. 12, A411–A414)*. C. R. Acad. Sci. Paris S er. A-B 284 (1977), no. 15, A847–A849.

[Ho69] M. Hochster, *Prime ideal structure in commutative rings*. Trans. Amer. Math. Soc. 142 (1969), 43–60.

[Hö01] O. Hölder, *Die Axiome der Quantitat und die Lehre vom Mass*. Ber. Verh. Sachs. Ges. Wiss. Leipzig, Math.-Phys. Cl. 53 (1901), 1-64.

[Ho79] W. Hodges, *Krull implies Zorn*. J. London Math. Soc. (2) 19 (1979), 285–287.

[Hu68] T.W. Hungerford, *On the structure of principal ideal rings*. Pacific J. Math. 25 (1968), 543–547.

[Hs66] D. Husemöller, *Fibre bundles*. McGraw-Hill Book Co., New York-London-Sydney 1966.

[J1] N. Jacobson, *Basic algebra. I*. Second edition. W. H. Freeman and Company, New York, 1985.

[J2] N. Jacobson, *Basic algebra. II*. Second edition. W. H. Freeman and Company, New York, 1989.

[Jo00] P. Jothilingam, *Cohen's theorem and Eakin-Nagata theorem revisited*. Comm. Algebra 28 (2000), 4861–4866.

[JR80] M. Jarden and P. Roquette, *The Nullstellensatz over p-adically closed fields*. J. Math. Soc. Japan 32 (1980), 425–460.

[K] I. Kaplansky, *Commutative rings*. Allyn and Bacon, Inc., Boston, Mass. 1970.

[Ka] M. Karoubi, *K-theory. An introduction*. Reprint of the 1978 edition. With a new postface by the author and a list of errata. Classics in Mathematics. Springer-Verlag, Berlin, 2008.

[Ka49] I. Kaplansky, *Elementary divisors and modules*. Trans. Amer. Math. Soc. 66 (1949), 464–491.

[Ka52] I. Kaplansky, *Modules over Dedekind rings and valuation rings*. Trans. Amer. Math. Soc. 72 (1952), 327–340.

[Ka58] I. Kaplansky, *Projective modules*. Ann. of Math. 68 (1958), 372–377.

[Ka17] M. Kapovich, *Krull dimensions of rings of holomorphic functions*. Complex analysis and dynamical systems VII, 167–173, Contemp. Math., 699, Amer. Math. Soc., Providence, RI, 2017.

[KeOm10] K.A. Kearnes and G. Oman, *Cardinalities of residue fields of Noetherian integral domains*. Comm. Algebra 38 (2010), 3580–3588.

[Kh03] D. Khurana, *On GCD and LCM in domains - a conjecture of Gauss*. Resonance 8 (2003), 72–79.

[KM99] G. Kemper and G. Malle, *Invariant fields of finite irreducible reflection groups*. Math. Ann. 315 (1999), 569–586.

[Ko89] V. Kolyvagin, *On the Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves*, Math. USSR-Izv. 33 (1989), 473–499.

[Kr24] W. Krull, *Die verschiedenen Artender Hauptidealringe*. Sitzungsberichte der Heidelberg Akademie (1924) no. 6.

[Kr31] W. Krull, *Allgemeine Bewertungstheorie*. J. Reine Angew. Math. 167 (1931), 160–196.

[Kr37] W. Krull, *Beiträge zur Arithmetik kommutativer Integritätsbereiche, III, zum Dimensionsbegriff der Idealtheorie*, Mat. Zeit 42 (1937), 745–766.

[Kr51] W. Krull, *Jacobsonsche Ringe, Hilbertscher Nullstellensatz Dimensionen theorie*. Math. Z. 54 (1951), 354–387.

[Ku99] M. Kurihara, *On the ideal class groups of the maximal real subfields of number fields with all roots of unity*. J. Eur. Math. Soc. (JEMS) 1 (1999), 35–49.

[La87] D. Laksov, *Radicals and Hilbert Nullstellensatz for not necessarily algebraically closed fields*. Enseign. Math. (2) 33 (1987), 323–338.

[La99] T.Y. Lam, *Lectures on modules and rings*. Graduate Texts in Mathematics, 189. Springer-Verlag, New York, 1999.

[La05] T.Y. Lam, *Introduction to quadratic forms over fields*. Graduate Studies in Mathematics, 67. American Mathematical Society, Providence, RI, 2005.

[La06] T.Y. Lam, *Serre's problem on projective modules*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2006.

[LR08] T.Y. Lam and M.L. Reyes, *A prime ideal principle in commutative algebra*. J. Algebra 319 (2008), 3006–3027.

[Lg53] S. Lang, *The theory of real places*. Ann. of Math. (2) 57 (1953), 378–391.

[Lg02] S. Lang, *Algebra*. Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002.

[LM] M.D. Larsen and P.J. McCarthy, *Multiplicative theory of ideals*. Pure and Applied Mathematics, Vol. 43. Academic Press, New York-London, 1971.

[La05] E. Lasker, *Zur Theorie der Moduln und Ideale*. Math. Ann. 60 (1905), 19–116.

[La64] D. Lazard, *Sur les modules plats*. C. R. Acad. Sci. Paris 258 (1964), 6313–6316.

[Le72] C.R. Leedham-Green, *The class group of Dedekind domains*. Trans. Amer. Math. Soc. 163 (1972), 493–500.

[Le43] F.W. Levi, *Contributions to the theory of ordered groups*. Proc. Indian Acad. Sci., Sect. A. 17 (1943), 199–201.

[Le67] L. Lesieur, *Divers aspects de la théorie des idéaux d'un anneau commutatif*. Enseignement Math. 13 (1967), 75–87.

[Li33] F.A Lindemann, *The Unique Factorization of a Positive Integer*. Quart. J. Math. 4, 319-320, 1933.

[Ma48] A.I. Malcev, *On the embedding of group algebras in division algebras (Russian)*, Dokl. Akad. Nauk. SSSR 60 (1948), 1499–1501.

[Ma58] H.B. Mann, *On integral bases*. Proc. Amer. Math. Soc. 9 (1958), 167–172.

[M] H. Matsumura, *Commutative ring theory*. Translated from the Japanese by M. Reid. Second edition. Cambridge Studies in Advanced Mathematics, 8. Cambridge University Press, Cambridge, 1989.

[Ma44] K. Matusita, *Über ein bewertungstheoretisches Axiomensystem für die Dedekind-Noethersche Idealtheorie*. Jap. J. Math. 19 (1944), 97–110.

[Ma99] T. MacHenry, *A subgroup of the group of units in the ring of arithmetic functions*. Rocky Mt. J. Math. 29 (1999), 1055–1065.

[McC76] J. McCabe, *A Note on Zariski's Lemma*. Amer. Math. Monthly 83 (1976), 560–561.

[Mi] J.W. Milnor, *Topology from the differentiable viewpoint*. Based on notes by David W. Weaver. The University Press of Virginia, Charlottesville, Va. 1965.

[Mo49] T. Motzkin, *The Euclidean algorithm*. Bull. Amer. Math. Soc. 55 (1949), 1142–1146.

[MRSW] F.W. Moore, M. Rogers and S. Sather-Wagstaff, *Monomial ideals and their decompositions*. Universitext. Springer, Cham, 2018.

[msegc] `https://math.stackexchange.com/questions/3898391/image-of-sup-inf-under-galois-connection-between-lattices`

[Na53] N. Nakano, *Idealtheorie in einem speziellen unendlichen algebraischen Zahlkörper*. J. Sci. Hiroshima Univ. Ser. A 16 (1953), 425–439.

[Na54] M. Nagata, *Note on integral closures of Noetherian domains.* Mem. Coll. Sci. Univ. Kyoto Ser. A. Math. 28 (1954), 121–124.

[Na57] M. Nagata, *A remark on the unique factorization theorem.* J. Math. Soc. Japan 9 (1957), 143–145.

[Na58] M. Nagata, *A general theory of algebraic geometry over Dedekind domains. II. Separably generated extensions and regular local rings.* Amer. J. Math. 80 (1958), 382–420.

[Na68] M. Nagata, *A type of subrings of a noetherian ring.* J. Math. Kyoto Univ. 8 (1968), 465–467.

[Na05] A.R. Naghipour, *A simple proof of Cohen's theorem.* Amer. Math. Monthly 112 (2005), 825–826.

[Na53] N. Nakano, *Idealtheorie in einem speziellen unendlichen algebraischen Zahlkörper.* J. Sci. Hiroshima Univ. Ser. A. 16: 425–439.

[Na95] W. Narkiewicz, *A Note on Elasticity of Factorizations.* J. Number Theory 51 (1995), 46–47.

[Ne49] B.H. Neumann, *On ordered division rings.* Trans. Amer. Math. Soc. 66 (1949), 202–252.

[Ne07] M.D. Neusel, *Invariant theory.* Student Mathematical Library, 36. American Mathematical Society, Providence, RI, 2007.

[Ni73] H. Nishimura, *On the unique factorization theorem for formal power series. II.* J. Math. Kyoto Univ. 13 (1973), 149–158.

[No21] E. Noether, *Idealtheorie in Ringbereichen.* Math. Ann. 83 (1921), 24–66.

[No26] E. Noether, *Der Endlichkeitsatz der Invarianten endlicher linearer Gruppen der Charakteristik p.* Nachr. Ges. Wiss. G-ttingen: 28-35.

[NT] P.L. Clark, *Number Theory: A Contemporary Introduction.* `http://www.math.uga.edu/~pete/4400FULL.pdf`

[O74] T. Ogoma, *On a problem of Fossum.* Proc. Japan Acad. 50 (1974), 266–267.

[Ol69a] J.E. Olson, *A combinatorial problem on finite Abelian groups. I.* J. Number Theory 1 (1969), 8–10.

[Ol69b] J.E. Olson, *A combinatorial problem on finite Abelian groups. II.* J. Number Theory 1 (1969), 195–199.

[Pa59] Z. Papp, *On algebraically closed modules.* Publ. Math. Debrecen 6 (1959), 311–327.

[Pe04] H. Perdry, *An elementary proof of Krull's intersection theorem.* Amer. Math. Monthly 111 (2004), 356–357.

[P] A. Pfister, *Quadratic forms with applications to algebraic geometry and topology.* London Mathematical Society Lecture Note Series, 217. Cambridge University Press, Cambridge, 1995.

[Qu76] D. Quillen, *Projective modules over polynomial rings.* Invent. Math. 36 (1976), 167–171.

[Ra30] J.L. Rabinowitsch, *Zum Hilbertschen Nullstellensatz.* Math. Ann. 102 (1930), 520.

[R] M. Reid, *Undergraduate commutative algebra.* London Mathematical Society Student Texts, 29. Cambridge University Press, Cambridge, 1995.

[Ri65] F. Richman, *Generalized quotient rings.* Proc. Amer. Math. Soc. 16 (1965), 794–799.

[Ro67] A. Robinson, *Non-standard theory of Dedekind rings.* Nederl. Akad. Wetensch. Proc. Ser. A 70=Indag. Math. 29 (1967), 444–452.

[Ro93] M. Roitman, *Polynomial extensions of atomic domains.* J. Pure Appl. Algebra 87 (1993), 187–199.

[Ro76] M. Rosen, *Elliptic curves and Dedekind domains.* Proc. Amer. Math. Soc. 57 (1976), 197–201.

[Ro] J.J. Rotman, *An introduction to homological algebra.* Second edition. Universitext. Springer, New York, 2009.

[Rü33] W. Rückert, *Zum Eliminationsproblem der Potenzreihenideale*, Math. Ann. 107 (1933), 259–281.

[Ru87] W. Rudin, *Real and complex analysis.* Third edition. McGraw-Hill Book Co., New York, 1987.

[Sa61] P. Samuel, *On unique factorization domains.* Illinois J. Math. 5 (1961), 1–17.

[Sa64] P. Samuel, *Lectures on unique factorization domains.* Notes by M. Pavaman Murthy. Tata Institute of Fundamental Research Lectures on Mathematics, No. 30 Tata Institute of Fundamental Research, Bombay 1964.

[Sa68] P. Samuel, *Unique factorization*. Amer. Math. Monthly 75 (1968), 945–952.
[Sa71] P. Samuel, *About Euclidean rings*. J. Algebra 19 (1971), 282–301.
[Sa08] A. Sasane, *On the Krull dimension of rings of transfer functions*. Acta Appl. Math. 103 (2008), 161- -168.
[S] W. Scharlau, *Quadratic and Hermitian forms*. Grundlehren der Mathematischen Wissenschaften 270. Springer-Verlag, Berlin, 1985.
[Sc45] T. Schönemann, *Grundzüge einer allgemeinen Theorie der höhern Congruenzen, deren Modul eine reelle Primzahl ist*. J. Reine Angew. Math. 31 (1845), 269–325.
[Sc46] T. Schönemann, *Von denjenigen Moduln, welche Potenzen von Primzahlen sind*. J. Reine Angew. Math. 32 (1846), 93–105.
[Sc46b] O.F.G. Schilling, *Ideal theory on open Riemann surfaces*. Bull. Amer. Math. Soc. 52 (1946), 945–963.
[Se56] A. Seidenberg, *Some remarks on Hilbert's Nullstellensatz*. Arch. Math. (Basel) 7 (1956), 235–240.
[Se66] A. Seidenberg, *Derivations and integral closure*. Pacific J. Math. 16 (1966), 167–173.
[Si86] J. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer Verlag, 1986.
[St86] J.-L. Steffan, *Longueurs des décompositions en produits d'éléments irréductibles dans un anneau de Dedekind*. J. Algebra 102 (1986), 229–236.
[ST42] A.H. Stone and J.W. Tukey, *Generalized "sandwich" theorems*. Duke Math. J. 9 (1942), 356–359.
[Su11] B. Sury, *Uncountably Generated Ideals of Functions*. College Math. Journal 42 (2011), 404–406.
[Su76] A.A. Suslin, *Projective modules over polynomial rings are free*. Dokl. Akad. Nauk SSSR 229 (1976), 1063–1066.
[Sw62] R.G. Swan, *Vector bundles and projective modules*. Trans. Amer. Math. Soc. 105 (1962), 264–277.
[Sw67] R.G. Swan, *The number of generators of a module*. Math. Z. 102 (4) (1967) 318-–322.
[Sw69] R.G. Swan, *Invariant rational functions and a problem of Steenrod*. Invent. Math. 7 (1969), 148–158.
[Te66] G. Terjanian, *Sur les corps finis*. C. R. Acad. Sci. Paris Sér. A-B 262 (1966), A167–A169.
[Te72] G. Terjanian, *Dimension arithmétique d'un corps*. J. Algebra 22 (1972), 517–545.
[Tr88] H.F. Trotter, *An overlooked example of nonunique factorization*. Amer. Math. Monthly 95 (1988), no. 4, 339–342.
[Va90] R.J. Valenza, *Elasticity of factorizations in number fields*. J. Number Theory 36 (1990), 212–218.
[vdW39] B.L. van der Waerden, *Einftihrung in die algebraische Geometrie*, Berlin, 1939.
[Wa] R.B. Warfield, Jr., *Rings whose modules have nice decompositions*. Math. Z. 125 (1972) 187–192.
[We07] J.H.M. Wedderburn, *On Hypercomplex Numbers*. Proc. of the London Math. Soc. 6 (1907), 77-118.
[W] C.A. Weibel, *An introduction to homological algebra*. Cambridge Studies in Advanced Mathematics, 38. Cambridge University Press, Cambridge, 1994.
[We80] R.O. Wells Jr., *Differential analysis on complex manifolds*. Second edition. Graduate Texts in Mathematics, 65. Springer-Verlag, New York-Berlin, 1980.
[Za04] F. Zanello, *When are there infinitely many irreducible elements in a principal ideal domain?* Amer. Math. Monthly 111 (2004), 150–152.
[Za76] A. Zaks, *Half factorial domains*. Bull. Amer. Math. Soc. 82 (1976), 721–723.
[Za47] O. Zariski, *A new proof of Hilbert's Nullstellensatz*. Bull. Amer. Math. Soc. 53 (1947), 362–368.
[Za69] H. Zassenhaus, *On Hensel factorization. I*. J. Number Theory 1 (1969), 291–311.
[Ze34] E. Zermelo, *Elementare Betrachtungen zur Theorie der Primzahlen*. Nachr. Gesellsch. Wissensch. G-ttingen 1, 43-46, 1934.