Algebraic Number Theory II: Valuations, Local Fields and Adeles

Pete L. Clark

Thanks to Tom Church, Rankeya Datta, John Doyle, Tyler Genao, Ernest Guico, David Krumm and Todd Trimble for pointing out typos. Thanks to Makoto Suwama for contributing Exercise 1.50d), which gives a counterexample to a previously stated version of the exercise. Thanks to Qun Li and Haiyang Wang for contributing Exercise 4.28.

Contents

CHAPTER 1

Normed Fields and Valuation Theory

1. Absolute values and valuations

1.1. Basic definitions.

All rings are commutative with unity unless explicit mention is made otherwise.

A **norm** on a field k is a map $|\cdot| : k \to \mathbb{R}^{\geq 0}$ satisfying:

(V1) $|x| = 0 \iff x = 0$.
(V2) $\forall x, y \in k,\ |xy| = |x||y|$.
(V3) $\forall x, y \in k,\ |x + y| \leq |x| + |y|$.

EXAMPLE 1.1. *On any field k, define $|\ |_0 : k \to \mathbb{R}^{\geq 0}$ by $0 \mapsto 0,\ x \in k \setminus \{0\} \mapsto 1$. This is immediately seen to be a norm on k, called the **trivial norm**. In many respects it functions as an exception in the general theory.*

EXAMPLE 1.2. *The standard norm on the complex numbers: $|a+bi| = \sqrt{a^2 + b^2}$. The restriction of this to $\mathbb{Q}$ or to $\mathbb{R}$ will also be called "standard".*

EXAMPLE 1.3. *The p-adic norm on $\mathbb{Q}$: write $\frac{a}{b} = p^n \frac{c}{d}$ with $\gcd(p, cd) = 1$ and put $|\frac{a}{b}|_p = p^{-n}$.*

It is straightforward to check that $|\cdot|_p$ is a norm on $\mathbb{Q}$. It will be more rewarding to give a conceptual explanation. Later we will see that we we can associate a norm $|\cdot|_{\mathfrak{p}}$ to any nonzero prime ideal $\mathfrak{p}$ in a Dedekind domain. This hints that norms are both plentiful and intimately related to classical algebraic number theory.

EXERCISE 1.1. *Let $|\cdot|$ be a norm on the field k.*
a) Show that the function $d : k \times k \to \mathbb{R}$ by $d(x, y) \coloneqq |x - y|$ is a metric.
b) (Reverse Triangle Inequality) Show: for all $a, b \in k$, $||a| - |b|| \leq |a - b|$.[1]

EXERCISE 1.2. *Let R be a ring in which $1 \neq 0$. Let $|\cdot| : R \to \mathbb{R}^{\geq 0}$ be a map which satisfies (V1) and (V2) (with k replaced by R) above.*
a) Show that $|1| = 1$.
b) Show that R is an integral domain, hence has a field of fractions k.
c) Show that there is a unique extension of $|\cdot|$ to k, the fraction field of R, satisfying (V1) and (V2).
d) Suppose that moreover R satisfies (V3). Show that the extension of part b) to k satisfies (V3) and hence defines a norm on k.

[1]This is the first of many points in the course where basic metric topology intervenes. Because students may be rusty on such things, we prefer to err on the side of assuming too little rather than too much familiarity with such topics.

e) Conversely, show that every integral domain admits a mapping $|\cdot|$ satisfying (V1), (V2), (V3).

EXERCISE 1.3.
a) Let $|\ |$ be a norm on k, and let $x \in k$ be a root of unity: we have $x^n = 1$ for some $n \in \mathbb{Z}^+$. Show: $|x| = 1$.
b) Show that for a field k, the following are equivalent:
(i) Every nonzero element of k is a root of unity.
(ii) The characteristic of k is $p > 0$, and $k/\mathbb{F}_p$ is algebraic.
c) If $k/\mathbb{F}_p$ is algebraic, show that the only norm on k is $|\cdot|_0$.

In Chapter 2 we will see that the converse of Exercise 1.3c) is also true: a field that is not algebraic over a finite field admits a nontrivial norm.

EXERCISE 1.4. *Let $(k, |\cdot|$ be a normed field, and let $\sigma : k \to k$ be a field automorphism. Define $\sigma^*|\ | : k \to \mathbb{R}$ by $x \mapsto |\sigma(x)|$.*
a) Show that $\sigma^*|\cdot|$ is a norm on k.
b) Show that this defines a left action of $\mathrm{Aut}(k)$ on the set of all norms on k which preserves equivalence.
c) Let d be a squarefree integer, not equal to 0 or 1. Let $k = \mathbb{Q}(\sqrt{d})$ viewed as a subfield of $\mathbb{C}$ (for specificity, when $d < 0$, we choose $\sqrt{d}$ to lie in the upper half plane, as usual), and let $|\cdot|$ be the restriction of the standard valuation on $\mathbb{C}$ to k. Let $\sigma : \sqrt{d} \mapsto -\sqrt{d}$ be the nontrivial automorphism of k. Is $\sigma^*|\ | = |\cdot|$? (Hint: the answer depends on d.)

1.2. Absolute values and the Artin constant.

For technical reasons soon to be seen, it is convenient to also entertain the following slightly weaker version of (V3): for $C \in \mathbb{R}^{>0}$, let (V3C) be the statement

(V3C) $\forall x \in k$, $|x| \leq 1 \implies |x+1| \leq C$.

A mapping $|\cdot| : k \to \mathbb{R}^{\geq 0}$ satisfying (V1), (V2) and (V3C) for some C will be called an **absolute value**.

For an absolute value $|\ |$ on a field k, we define the **Artin constant** C_k to be the infimum of all $C \in \mathbb{R}^{>0}$ such that $|\cdot|$ satisfies (V3C).

EXERCISE 1.5. *Let $|\cdot|$ be an absolute value on k.*
a) Show that $|\cdot|$ satisfies (V3C) for some C, then $C \geq 1$.
b) Let C_k be the Artin constant. Show that $|\cdot|$ satisfies (V3C_k).
c) Compute C_k for the standard norm on $\mathbb{C}$ and the p-adic norms on $\mathbb{Q}$.

LEMMA 1.4. *Let k be a field and $|\cdot|$ an absolute value, and $C \in [1, \infty)$. Then the following are equivalent:*
(i) $\forall x \in k$, $|x| \leq 1 \implies |x+1| \leq C$.
(ii) $\forall x, y \in k$, $|x+y| \leq C \max(|x|, |y|)$.

PROOF. Assume (i) and let $x, y \in k$. Without loss of generality we may assume that $0 < |x| \leq |y|$. Then $|\frac{x}{y}| \leq 1$, so $|\frac{x}{y} + 1| \leq C$. Multiplying through by $|y|$ gives

$$|x+y| \leq C|y| = C \max(|x|, |y|).$$

Now assume (ii) and let $x \in k$ be such that$|x| \leq 1$. Then

$$|x+1| \leq C\max(|x|,|1|) = C\max(|x|,1) = C. \qquad \square$$

LEMMA 1.5. *Let k be a field and $|\cdot|$ an absolute value with Artin constant C. Then $|\cdot|$ is a norm iff $C \leq 2$.*

PROOF. ($\Longrightarrow$) Let $|\cdot|$ be a norm on k, and let $x \in k$ be such that $|x| \leq 1$. Then

$$|x+1| \leq |x| + |1| = |x| + 1 \leq 1 + 1 = 2.$$

($\Longleftarrow$) Suppose $C \leq 2$. Let $x, y \in k$. Without loss of generality, we may assume that $0 < |x| \leq |y|$. Then $|\frac{x}{y}| \leq 1$, so $|1 + \frac{x}{y}| \leq C \leq 2$. Multiplying through by y, we get $|x+y| \leq 2|y| = 2\max(|x|,|y|)$. Applying this reasoning inductively, we get that for any $x_1, \ldots, x_{2^n} \in k$ with $0 < |x_1| \leq \ldots \leq |x_{2^n}|$, we have

$$|x_1 + \ldots + x_{2^n}| \leq 2^n \max_i |x_i|.$$

Let r be an integer such that $n \leq 2^r < 2n$. Then

$$|x_1 + \ldots + x_n| = |x_1 + \ldots + x_n + 0 + \ldots + 0| \leq 2^r \max_i |x_i| \leq 2n \max_i |x_i|. \tag{1}$$

Applying this with $x_1 = \ldots = x_n = 1$ gives that $|n| \leq 2n$. Moreover, by replacing the max by a sum, we get the following weakened version of (17):

$$|x_1 + \ldots + x_n| \leq 2n \sum_{i=1}^n |x_i|.$$

Finally, let $x, y \in k$ be such that $0 < |x| \leq |y|$. Then for all $n \in \mathbb{Z}^+$,

$$|x+y|^n = |\sum_{i=0}^n \binom{n}{i} x^i y^{n-i}| \leq 2(n+1) \sum_{i=0}^n |\binom{n}{i}||x|^i |y|^{n-i}$$

$$\leq 4(n+1) \sum_{i=0}^n \binom{n}{i} |x|^i |y|^{n-i} = 4(n+1)(|x| + |y|)^n.$$

Taking nth roots and the limit as $n \to \infty$ gives $|x+y| \leq |x| + |y|$. $\square$

Why absolute values and not just norms?

LEMMA 1.6. *Let $|\cdot| : k \to \mathbb{R}^{\geq 0}$ be an absolute value with Artin constant C. Put*

$$|\cdot|^\alpha : k \to \mathbb{R}^{\geq 0},\ x \mapsto |x|^\alpha.$$

a) The map $|\cdot|^\alpha$ is an absolute value with Artin constant C^α.
b) If $|\cdot|$ is a norm, $|\cdot|^\alpha$ need not *be a norm.*

EXERCISE 1.6. *Prove Lemma 1.6.*

This is the point of absolute values: the set of such things is closed under the operation of raising to a power, whereas the set of norms need not be.

Moreover, Lemma 1.6 suggests a dichotomy for absolute values. We say an absolute value is **non-Archimedean** if the Artin constant is equal to 1 (the smallest possible value). Conversely, if the Artin constant is greater than one, we say that the norm is **Archimedean**.

For example, on $k = \mathbb{Q}$, the p-adic norm $|\cdot|_p$ is non-Archimedean, whereas the standard absolute value $|\cdot|_\infty$ is Archimedean with Artin constant 2.

EXERCISE 1.7. *Let $|\ |$ be an absolute value on l, and let k be a subfield of l.*
a) Show that the restriction of $|\cdot|$ to k is an absolute value on k.
b) If $|\cdot|$ is a norm on l, then the restriction to k is a norm on k.

1.3. Equivalence of absolute values.

Two absolute values $|\cdot|_1,\ |\cdot|_2$ on a field k are **equivalent** if there exists $\alpha \in \mathbb{R}^{>0}$ such that $|\cdot|_2 = |\cdot|_1^\alpha$. When convenient, we write this as $|\cdot|_1 \sim |\cdot|_2$.

By a **place** on a field k, we mean an equivalence class of absolute values.[2] It is easy to check that this is indeed an equivalence relation on the set of absolute values on a field k. Moreover, immediately from Lemma 1.6 we get:

COROLLARY 1.7. *Each absolute value on a field is equivalent to a norm.*

THEOREM 1.8. *Let $|\cdot|_1$, $|\ |_2$ be two nontrivial absolute values on a field k. The following are equivalent:*
(i) There exists $\alpha \in \mathbb{R}^{>0}$ such that $|\cdot|_1^\alpha = |\cdot|_2$.
(ii) $\forall x \in k$, $|x|_1 < 1 \implies |x|_2 < 1$.
(iii) $\forall x \in k$, $|x|_1 \leq 1 \implies |x|_2 \leq 1$.
(iv) $\forall x \in k$, all of the following hold:

$$|x|_1 < 1 \iff |x|_2 < 1,$$
$$|x|_1 > 1 \iff |x|_2 > 1,$$
$$|x|_1 = 1 \iff |x|_2 = 1.$$

Remark: This may seem like a strange way to organize the equivalences, but it will be seen to be helpful in the proof, which we give following [**Ws**, Thm. 1-1-4].

PROOF. We shall show (i) $\implies$ (ii) $\implies$ (iii) $\implies$ (iv) $\implies$ (i). That (i) $\implies$ (ii) (and, in fact, all the other properties) is clear.
(ii) $\implies$ (iii): let $x \in k$ be such that $|x|_1 = 1$. We must show that $|x|_2 = 1$. Since $|\cdot|_1$ is nontrivial, there exists $a \in k$ with $0 < |a|_1 < 1$, and then by (ii) we have $0 < |a|_2 < 1$. Then, for all $n \in \mathbb{Z}^+$, $|x^n a|_1 < 1$, so $|x^n a|_2 < 1$, so $|x|_2 < |a|_2^{-\frac{1}{n}}$. Taking n to infinity gives $|x|_2 \leq 1$. We may apply the same argument to x^{-1}, getting $|x|_2 \geq 1$.
(iii) $\implies$ (iv): Choose $c \in k$ such that $0 < |c|_2 < 1$. Then for sufficiently large n,

$$|x|_1 < 1 \implies |x|_1^n \leq |c|_1 \implies |\frac{x^n}{c}|_1 \leq 1 \implies |x|_2^n \leq |c|_2 < 1 \implies |x|_2 < 1.$$

So far we have shown (iii) $\implies$ (ii). As in the proof of (ii) $\implies$ (iii) we have $|x|_1 = 1 \implies |x|_2 = 1$. Moreover

$$|x|_1 > 1 \implies |\frac{1}{x}|_1 < 1 \implies |\frac{1}{x}|_2 < 1 \implies |x|_2 > 1.$$

[2]Warning: in more advanced valuation theory, one has the notion of a K-place of a field k, a related but distinct concept. In these notes we shall always use place in the sense just defined.

This establishes (iv).
(iv) $\implies$ (i): Fix $a \in k$ such that $|a|_1 < 1$. Then $|a|_2 < 1$, so

$$\alpha = \frac{\log |a|_2}{\log |a|_1} > 0.$$

We will show that $|\cdot|_2 = |\cdot|_1^{\alpha}$. For this, let $x \in k$, and put, for $i = 1, 2$,

$$\gamma_i = \frac{\log |x|_i}{\log |a|_i}.$$

It suffices to show $\gamma_1 = \gamma_2$. Let $r = \frac{p}{q}$ be a rational number (with $q > 0$). Then

$$r = \frac{p}{q} \geq \gamma_1 \iff p \log |a|_1 \leq q \log |x|_1$$

$$\iff |a^p|_1 \geq |x^q|_1 \iff |\frac{x^q}{a^p}|_1 \leq 1 \iff |\frac{x^q}{a^p}|_2 \leq 1$$

$$\iff p \log |a|_2 \geq q \log |x|_2 \iff \frac{p}{q} \geq \gamma_2. \qquad \square$$

EXERCISE 1.8. *Let $|\cdot|$ be an absolute value on a field k. Show that $|\cdot|$ is Archimedean (resp. non-Archimedean) iff every equivalent absolute value is Archimedean (resp. non-Archimedean).*

1.4. Artin-Whaples Approximation Theorem.

THEOREM 1.9. *(Artin-Whaples) Let k be a field and $|\ |_1, \ldots, |\ |_n$ be inequivalent nontrivial norms on k. Then for any $x_1, \ldots, x_n \in k$ and any $\epsilon > 0$, there exists $x \in k$ such that*

$$\forall\ i,\ 1 \leq i \leq n,\ |x - x_i|_i < \epsilon.$$

PROOF. Our proof closely follows [**A**, §1.4].
Step 1: We establish the following special case: there exists $a \in k$ such that $|a|_1 > 1$, $|a|_i < 1$ for $1 < i \leq n$.
Proof: We go by induction on n. First suppose $n = 2$. Then, since $|\cdot|_1$ and $|\cdot|_2$ are inequivalent and nontrivial, by Theorem 1.8 there exist $b, c \in k$ such that $|b|_1 < 1$, $|b|_2 \geq 1$, $|c|_1 \geq 1$, $|c_2| < 1$. Put $a = \frac{c}{b}$.

Now suppose the result holds for any $n - 1$ norms, so that there exists $b \in k$ with $|b|_1 > 1$ and $|b|_i < 1$ for $1 < i \leq n - 1$. Using the $n = 2$ case, there is $c \in k$ such that $|c|_1 > 1$ and $|c|_n < 1$.
Case 1: $|b|_n \leq 1$. Consider the sequence $a_r = cb^r$. Then for all $r \in \mathbb{Z}^+$ we have $|a_r|_1 > 1$ while $|a_r|_n < 1$. For sufficiently large r, $|a_r|_i < 1$ for all $2 \leq i \leq n$, so we may take $a = a_r$.
Case 2: $|b|_n > 1$. This time, for $r \in \mathbb{Z}^+$, we put

$$a_r = \frac{cb^r}{1 + b^r}.$$

Then for $i = 1$ and $i = n$,

$$\lim_{r\to\infty} |a_r - c|_i = \lim_{r\to\infty} |c|_i \frac{|b^r - (1 + b^r)|_i}{|1 + b^r|_i} = \lim_{r\to\infty} \frac{|c|_i}{|1 + b^r|_i} = 0,$$

so for sufficiently large r we have

$$|a_r|_1 = |c|_1 > 1 \text{ and } |a_r|_n = |c|_n < 1.$$

On the other hand, for $1 < i < n$,

$$|a_r|_i = \frac{|c|_i |b|_i^r}{|1+b^r|_i} \leq |c|_i |b_i|^r < 1.$$

Therefore we may take $a = a_r$ for sufficiently large r.
Step 2: We claim that for any $\delta > 0$, there exists $a \in k$ such that $||a|_1 - 1| < \delta$ and $|a|_i < \delta$ for $1 < i \leq n$.
Proof: If b is such that $|b|_1 > 1$ and $|b|_i < 1$ for $1 < i \leq n$, then the computations of Step 1 show that we may take $a_r = \frac{b^r}{1+b^r}$ for sufficiently large r.
Step 3: Fix $\delta > 0$. By Step 2, for each $1 \leq i \leq n$, there exists $a_i \in k$ such that $||a|_i - 1| < \delta$ and for all $j \neq i$, $|a_i|_j < \delta$. Put $A = \max_{i,j} |x_i|_j$. Take

$$x = a_1 x_1 + \ldots + a_n x_n.$$

Then

$$|x - x_i|_i \leq |a_i x_i - x_i|_i + \sum_{j \neq i} |a_j x_j|_i \leq A\delta + (n-1)A\delta = nA\delta.$$

Thus taking $\delta < \frac{\epsilon}{nA}$ does the job. □

Remark: Theorem 1.9 also goes by the name **weak approximation**. By any name, it is the most important elementary result in valuation theory, playing a role highly analogous to that of the Chinese Remainder Theorem in commutative algebra. On other hand, when both apply the Chinese Remainder Theorem is subtly stronger, in a way that we will attempt to clarify at little later on.

1.5. Archimedean absolute values.

In the land of Archimedean absolute values, there is one theorem to rule them all. It is as follows.

THEOREM 1.10. *(Big Ostrowski Theorem) Let k be a field and $|\cdot|$ an Archimedean absolute value on k. Then there exists a constant $\alpha \in \mathbb{R}^{>0}$ and an embedding $\iota : k \hookrightarrow \mathbb{C}$ such that for all $x \in k$, $|x| = |\iota(x)|_\infty^\alpha$. In other words, up to equivalence, every Archimedean absolute value arises by embedding k into the complex numbers and restricting the standard norm.*

Theorem 1.10 is a deep result: every known proof from first principles takes several pages. It immediately implies *all* of the other results in this section, and conversely these results – and more! – are used in its proof. Indeed, to prove Big Ostrowski it is convenient to use aspects of the theory of completions, so the proof is deferred until Chapter 2.

For a field k, let $\mathbb{Z} \cdot 1$ be the additive subgroup generated by 1. Recall that if k has characteristic 0, then $\mathbb{Z} \cdot 1$ is isomorphic to the integers, whereas if k has characteristic $p > 0$, $\mathbb{Z} \cdot 1 \cong \mathbb{F}_p$.[3]

PROPOSITION 1.11. *Let $|\cdot|$ be an absolute value on a field k. The following are equivalent:*
(i) $|\cdot|$ is non-Archimedean.
(ii) $|\mathbb{Z} \cdot 1|$ is bounded.

[3]Thus either way $\mathbb{Z} \cdot 1$ is a subring of k, often called the **prime subring**.

PROOF. Since both conditions (i) and (ii) are unaffected by changing the absolute value within its equivalence class, we may and shall assume that $|\cdot|$ is a norm.

The implication (i) $\implies$ (ii) follows from the remark preceding the statement of Proposition 1.11. Now suppose (ii): for specificity, suppose that there exists $M > 0$ such that $|n \cdot 1| \leq M$ for all $n \in \mathbb{Z}$. Let $a,\ b \in k$ and $n \in \mathbb{Z}^+$. Then

$$|a+b|^n = |(a+b)^n| = |\sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}| \leq M \sum_{i=0}^{n} |a|^i |b|^{n-i} \leq M(n+1)\max(|a|,|b|)^n.$$

Taking nth roots of both sides and letting n approach infinity gives the result. □

COROLLARY 1.12. *An absolute value on a field of positive characteristic is non-Archimedean.*

LEMMA 1.13. *(Ostrowski Lemma) Every Archimedean absolute value on $\mathbb{Q}$ is equivalent to the standard Archimedean norm $|\cdot|_\infty$.*

PROOF. Let $|\cdot|$ be an Archimedean absolute value on $\mathbb{Q}$. Once again we may, and shall, assume that $|\cdot|$ is a norm. By Proposition 1.11, $|\cdot|$ is unbounded on the integers, so we may define N to be the least positive integer such that $|N| > 1$. Let $\alpha \in \mathbb{R}^{>0}$ be such that $|N| = N^\alpha$. Our task is to show that $|n| = n^\alpha$ for all $n \in \mathbb{Z}$. We show separately that $|n| \leq n^\alpha$ and $|n| \geq n^\alpha$.

Step 1: For any $n \in \mathbb{Z}^+$, consider its base N expansion:

$$n = \sum_{i=0}^{\ell} a_i N^i$$

with $0 \leq a_i < N$, $a_\ell \neq 0$. (Of course ℓ depends on n and N.) Then

$$|n| \leq \sum_{i=0}^{\ell} |a_i| N^{\alpha i}.$$

Note that $n \geq N^\ell$. Also, by definition of N, we have $|a_i| \leq 1$ for all i. So

$$|n| \leq \sum_{i=0}^{\ell} N^{\alpha i} = N^{\alpha\ell} \sum_{i=0}^{\ell} (N^{-\alpha})^i \leq n^\alpha \sum_{i=0}^{\infty} N^{-\alpha i} = C_1 n^\alpha,$$

where $C_1 = \sum_{i=0}^{\infty} N^{-\alpha i}$, a constant. Now let A be a positive integer. Applying the above inequality with n^A in place of n, we get

$$|n|^A \leq C_1 n^{\alpha A}.$$

Taking Ath roots and the limit as A approaches infinity gives

$$|n| \leq n^\alpha.$$

Step 2: Keeping N and $\ell = \ell(n)$ as above, we have $N^\ell \leq n < N^{\ell+1}$. Then

$$|N^{\ell+1}| = |N^{\ell+1} - n + n| \leq |N^{\ell+1} - n| + |n|,$$

so

$$|n| \geq |N^{\ell+1}| - |N^{\ell+1} - n| \geq N^{\alpha(\ell+1)} - (N^{\ell+1} - n)^\alpha$$

$$\geq N^{\alpha(\ell+1)} - (N^{\ell+1} - N^\ell)^\alpha = N^{\alpha(\ell+1)} \left(1 - (1 - \frac{1}{N})^\alpha\right) \geq C_2 n^\alpha,$$

where $C_2 = 1 - (1 - \frac{1}{N})^\alpha$, a constant. Arguing as above, we get $|n| \geq n^\alpha$. □

THEOREM 1.14. *(Computation of the Artin constant) Let k be a field and $|\cdot|$ an absolute value on k.*
a) The Artin constant C_k of k is $\max(|1|,|2|) = \max(1,|2|)$.
b) For any subfield l of k, the Artin constant of the restriction of $|\cdot|$ to l is C_k.

PROOF. (E. Artin) a) The absolute value $|\cdot|$ is non-Archimedean iff $C_k = 1$ iff $\max(1,|2|) = 1$, so we may assume that it is Archimedean. By Corollary 1.12 the field k has characteristic 0 and thus contains $\mathbb{Q}$. Moreover by Proposition 1.11 the restriction of $|\cdot|$ to $\mathbb{Q}$ is Archimedean. If $|\ |_\infty$ denotes the standard Archimedean norm on $\mathbb{Q}$, then by the Ostrowski Lemma (Lemma 1.13), there is $\beta > 0$ such that the restriction of $|\cdot|_{\mathbb{Q}}$ is $|\cdot|_\infty^\beta$. On the other hand, let $\alpha > 0$ be such that $C_k = 2^\alpha$. Thus the conclusion of part a) is equivalent to $\alpha = \beta$.

Let $a, b, a_1, \ldots, a_m \in k$. Assuming without loss of generality that $0 < |a| \leq |b|$, we get $|\frac{a}{b}| \leq 1$ so $|\frac{a}{b} + 1| \leq 2^\alpha$, hence

$$|a+b| \leq 2^\alpha \max(|a|,|b|).$$

This argument is familiar from the proof of Lemma 1.1. A similar adaptation gives

$$|a_1 + \ldots + a_m| \leq (2m)^\alpha \max_i |a_i|.$$

In particular, we have

$$|a+b|^m = |(a+b)^m| \leq (2(m+1))^\alpha \max_i |\binom{m}{i}||a|^i|b|^{m-i}.$$

Since $\sum_{i=0}^n \binom{m}{i} = 2^m$, we have

$$|\binom{m}{i}| = \binom{m}{i}^\beta \leq 2^{m\beta}.$$

Thus

$$|a+b|^m \leq (2(m+1))^\alpha 2^{m\beta} (\max(|a|,|b|))^m.$$

Taking mth roots and the limit as $m \to \infty$, we get

$$|a+b| \leq 2^\beta \max(|a|,|b|),$$

so that $C_k = 2^\alpha \leq 2^\beta$. Since

$$|1+1| = 2^\beta = 2^\beta \max(|1|,|1|),$$

we also have $2^\beta \leq 2^\alpha$, so $\alpha = \beta$.
b) This follows immediately from part a), as the computation of the Artin constant depends only on the restriction of the absolute value to its prime subring. □

1.6. Non-archimedean norms and valuations.

EXERCISE 1.9. *Let $(k, |\cdot|)$ be a normed field.*
a) Show: for all $a, b \in k$, we have $||a| - |b|| \leq |a - b|$.
For the remainder of the exercise, we suppose that the norm is non-Archimedean.
b) Suppose $|a| > |b|$. Show that $|a + b| = |a|$.
c) Show: for all $n \in \mathbb{Z}^+$ and $x_1, \ldots, x_n \in k$, $|x_1 + \ldots + x_n| \leq \max_i |x_i|$.
*d) (**Principle of Domination**) Suppose $x_1, \ldots, x_n \in k$ and $|x_i| < |x_1|$ for all $i > 1$. Show that $|x_1 + \ldots + x_n| = |x_1|$.*

Exercise 1.9d) can be restated as: if in a finite collection of elements, there is a unique element of maximal norm, then that element "dominates" in the sense that the norm of it is the norm of the sum. Although this result does not lie any deeper than the non-Archimedean triangle inequality, its usefulness cannot be overstated: if you are trying to prove estimates on the norm of a sum of terms in a non-Archimedean field, *always* expect to use the principle of domination.

Until further notice, we let $(k, |\cdot|)$ be a non-Archimedean normed field.

EXERCISE 1.10. *Define*

$$R = \{x \in k \mid |\cdot| |x| \leq 1\}$$

and

$$\mathfrak{m} = \{x \in k \mid |\cdot| |x| < 1\}.$$

Show that R is a ring and that $\mathfrak{m}$ is the unique maximal ideal of $\mathfrak{m}$.

Thus R is a **local ring**, called the **valuation ring** of $(k, |\cdot|)$.

Remark: More generally, an integral domain R is called a **valuation ring** if for every $x \in k^\times$, at least one of $x,\ x^{-1}$ lies in R.

EXERCISE 1.11. *Show that two non-Archimedean norms on a field k are equivalent iff their valuation rings are equal.*

EXERCISE 1.12. *Let R be a valuation ring.*
a) Show that $R^\times$ is the set of elements $x \in k^\times$ such that both *x and x^{-1} lie in R.*
b) Show that $R \setminus R^\times$ is an ideal of R and hence is the unique maximal ideal of R: R is a local ring.

In the non-Archimedean case it is often fruitful to consider, in place of the norm $|\cdot|$ itself, its logarithm. This goes as follows:

A **(rank one) valuation** on a field k is a map $v : k \to \mathbb{R} \cup \{\infty\}$ such that:
(V1) $v(x) = \infty \iff x = 0$.
(V2) For all $x, y \in k$, $v(xy) = v(x) + v(y)$.
(V3) For all $x, y \in k$, $v(x + y) \geq \min(v(x), v(y))$.

EXERCISE 1.13. *Show that $v : 0 \mapsto -\infty,\ k^\times \mapsto 0$ is a valuation on k, called **trivial**.*

Two valuations v and v' on k are **equivalent** if there exists $c > 0$ such that $v' = cv$.

EXERCISE 1.14. *Let k be a field and v a valuation on k.*
*a) Show that $\Gamma := v(k^\times)$ is a subgroup of $(\mathbb{R}, +)$. It is called the **value group**.*
b) Show that a valuation is trivial iff its value group is $\{0\}$.
*A valuation is called **discrete** if Γ is a nontrivial discrete subgroup of $(\mathbb{R}, +)$.*
c) Show that every discrete subgroup of $(\mathbb{R}, +)$ is infinite cyclic.
*d) Deduce that every discrete valuation is equivalent to one with value group $\mathbb{Z}$. Such a discrete valuation is said to be **normalized**.*

EXERCISE 1.15. *Let k be a field and $c \in (1, \infty)$.*
a) If $|\cdot|$ is a non-Archimedean norm on k, show $v = -\log_c |\ |$ is a valuation on k.
b) If v is a valuation on k, then $|\cdot| = c^{-v}$ is a non-Archimedean norm on k, with

valuation ring $R = \{x \in k \mid v(x) \geq 0\}$.
c) Show that different choices of c yield equivalent norms.

THEOREM 1.15. *Let v be a nontrivial valuation on a field k with valuation ring R and maximal ideal $\mathfrak{m}$. The following are equivalent:*
(i) v is discrete.
(ii) There is an element $\pi \in R$ such that $\mathfrak{m} = (\pi)$.
(iii) The valuation ring R is a PID.
(iv) R is a Noetherian.
A valuation ring satisfying the equivalent conditions (ii) - (iv) is called a ***discrete valuation ring*** *or a* ***DVR****.*

PROOF. (i) $\implies$ (ii): If v is discrete, then by Exercise 1.14 we may as well assume that the value group is $\mathbb{Z}$. Let $\pi \in k$ be such that $v(\pi) = 1$. Then it is easily seen that $\mathfrak{m} = (\pi)$.
(ii) $\implies$ (i): If $\mathfrak{m} = (\pi)$, then necessarily π is an element of minimal positive valuation, so v is discrete.
(ii) $\implies$ (iii): This is similar to – but easier than! – the proof that $\mathbb{Z}$ is a PID. Namely, since (ii) $\implies$ (i), every ideal contains an element of minimal positive valuation, and one readily shows such an element is a generator.
(iii) $\implies$ (iv): a ring is Noetherian iff every ideal is finitely generated, so of course a PID is Noetherian.
(iv) $\implies$ (ii): we may assume that $\mathfrak{m} = \langle x_1, \ldots, x_n \rangle$ with $v(x_1) \leq \ldots \leq v(x_n)$. Then for all $i \geq 2$, $v(\frac{x_i}{x_1}) \geq 0$, so $\frac{x_i}{x_1} \in R$, so $x_1 \mid x_i$, so $\mathfrak{m} = \langle x_1 \rangle$. □

The moral here is that the *discrete* valuations are by far the easiest to understand. Thus it is natural to wonder whether we really need to bother with non-discrete valuations. The answer is yes, at least in certain circumstances. The following exercise gives an indication of this.

EXERCISE 1.16. *Let $(A, +)$ be a commutative group. Recall that A is* ***divisible*** *if for all $x \in A$ and $n \in \mathbb{Z}^+$, there exists $y \in A$ such that $ny = x$. (Equivalently, the multiplication by n map $[n] : A \to A$ is surjective.)*
a) Show: no nontrivial discrete subgroup of $\mathbb{R}$ is divisible.
b) Show: a quotient of a divisible group is divisible.
c) Show: if k is algebraically closed, then $k^\times$ is a divisible group.
d) Deduce: an algebraically closed field admits no discrete valuation.

EXERCISE 1.17. *For any field k, let $R = k[[t]]$ be the ring of formal power series with k-coefficients and $k((t))$ its fraction field, the field of formal Laurent series $\sum_{n=N}^{\infty} a_n t^n$.*
a) Show that for any ring S, the units of $S[[t]]$ are precisely the formal power series whose constant term is a unit in S.
b) Show that a nonzero $f \in k[[t]]$ may be uniquely written as $f = t^N u$ with $u \in R^\times$.
c) Show that $f \mapsto N$ is a discrete valuation on $k[[t]]$.

EXERCISE 1.18. *Let f be a field, $F = f((t))$, and $\overline{F}$ an algebraic closure of F. Let $R = F[\{t^{\frac{1}{n}}\}_{n \in \mathbb{Z}^+}]$ and let k be the fraction field of R.*
a) Show that every element in R (resp. k) can be written as a formal power series (resp. formal Laurent series) in $t^{\frac{1}{n}}$ for some $n \in \mathbb{Z}^+$ which depends on k.[4]

[4]Either type of series is called a **Puiseux series**.

b) Show that the units in R are the Puiseux series with nonzero coefficient of t^0. Deduce that R is a local ring.
c) Show that any nonzero $f \in k$ may be uniquely written as $t^{\frac{p}{q}} \cdot u$ with $u \in R^\times$. Deduce that R is a valuation ring. Show that R is not *Noetherian, so is not a DVR.*
d) Define $|||: k \to \mathbb{R}^{>0}$ by $0 \mapsto 0$, $f = t^{\frac{p}{q}} \cdot u \mapsto 2^{-\frac{p}{q}}$. Show that $|||$ is a norm on k.

1.7. R-regular valuations; valuations on Dedekind domains.

Let R be an integral domain with fraction field k. We say that a valuation v of k is **R-regular** if $v(x) \geq 0$ for all $x \in R$, i.e., if R is contained in the valuation ring R_v of v.

THEOREM 1.16. *(Classification of R-regular valuations on a Dedekind domain) Let R be a Dedekind domain with fraction field K, and let $\mathfrak{p}$ a nonzero prime ideal of R. We define a map $v_\mathfrak{p}: K \to \mathbb{Z} \cup -\infty$ as follows: $v_\mathfrak{p}(0) = -\infty$. Let $\alpha \in K^\times$. Write $\alpha = \frac{x}{y}$ with $x, y \in R \setminus \{0\}$. Let*

$$(x) = \mathfrak{p}^a \mathfrak{q}, \ (y) = \mathfrak{p}^b \mathfrak{q}'$$

with $\gcd(\mathfrak{p}, \mathfrak{q}\mathfrak{q}') = 1$. Put $v_\mathfrak{p} = a - b$.
a) The map $v_\mathfrak{p}: K \to \mathbb{Z} \bigcup \{\infty\}$ is a normalized discrete valuation.
b) Conversely, let v be a nontrivial valuation on K. If v is R-regular – i.e., $v(R) \subset [0, \infty]$ – then $v \sim v_\mathfrak{p}$ for a unique nonzero prime ideal $\mathfrak{p}$ of R. In particular, any nontrivial R-regular valuation on K is discrete.

PROOF. The proof of part a) is straightforward and left to the reader as Exercise 1.19 below. As for part b), let v be a nontrivial R-regular valuation on K. Let us call its valuation ring A_v and its maximal ideal $\mathfrak{m}_v$, so by hypothesis $R \subset A_v$. Put $\mathfrak{p} := R \cap \mathfrak{m}_v$. Since $\mathfrak{p}$ is nothing else than the pullback of the prime ideal $\mathfrak{m}_v$ under the homomorphism of rings $R \hookrightarrow A_v$, certainly $\mathfrak{p}$ is a prime ideal of R. We claim that it is nonzero. Indeed, $\mathfrak{p} = \{0\}$ would mean that every nonzero element of R is a unit in A_v. Since every nonzero element of K is a quotient of two nonzero elements of R, this would give $A_v = K$, contradicting the nontriviality of v. Thus $\mathfrak{p}$ is a nonzero prime ideal in the Dedekind domain R, hence maximal. Let $R_\mathfrak{p}$ be the localization of R at $\mathfrak{p}$, a discrete valuation ring. Since every element of $R \setminus \mathfrak{p}$ is a unit in A_v, we have an inclusion of nontrivial valuation rings $R_\mathfrak{p} \subset A_v$. By Theorem 1.8, this implies that $v_\mathfrak{p} \sim v$. □

EXERCISE 1.19. *Prove Theorem 1.16a).*

PROPOSITION 1.17 (Dedekind Approximation). *Let R be a Dedekind domain with fraction field K. Let $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ be a finite set of nonzero prime ideals of R, let $n_1, \ldots, n_r \in \mathbb{Z}$ and $x_1, \ldots, x_r \in K$. Then there is $x \in K$ such that:*
(i) For all $1 \leq i \leq r$, $v_{\mathfrak{p}_i}(x - x_i) = n_i$ and
(ii) $v_\mathfrak{q}(x) \geq 0$ for all nonzero prime ideals $\mathfrak{q}$ different from the $\mathfrak{p}_i$'s.

PROOF. Step 1: For $1 \leq i \leq r$, choose $y_i \in K$ such that $v_{\mathfrak{p}_i}(x_i - y_i) = n_i$. By Artin-Whaples approximation there is $a \in K$ such that $v_{\mathfrak{p}_i}(a - y_i) > n_i$ for all $1 \leq i \leq r$, and the principle of domination gives $v_{\mathfrak{p}_i}(a - x_i) = n_i$ for all $1 \leq i \leq r$. Step 2: Let $\{\mathfrak{q}_1, \ldots, \mathfrak{q}_m\}$ be the set of prime ideals disjoint from S at which a has negative valuation. If $m = 0$, we're done. Otherwise, let $N = -\min_{1 \leq j \leq m} v_{\mathfrak{q}_j}(a)$, and let $M \in \mathbb{N}$ be such that

$$M > n_i - v_{\mathfrak{p}_i}(a) \ \forall 1 \leq i \leq r.$$

By the Chinese Remainder Theorem there is $c \in R$ such that $c \equiv 1 \pmod{\mathfrak{p}_i^M}$ for all $1 \leq i \leq r$ and $c \equiv 0 \pmod{\mathfrak{q}_j^N}$ for all $1 \leq j \leq m$. Thus $v_{\mathfrak{p}}(ac) \geq 0$ for all $\mathfrak{p} \notin S$, and for all $1 \leq i \leq r$ we have

$$v_{\mathfrak{p}_i}(ac - x_i) = v_{\mathfrak{p}_i}((a - x_i) - (ac - a)) = n_i,$$

so we may take $x = ac$. □

Proposition 1.17 is not an immediate consequence of Artin-Whaples approximation because of the extra integrality conditions. In the case where K is a gloal field, this result is also related to the related to the **Strong Approximation Theorem**, one of the fundamental results of Chapter 6.

EXERCISE 1.20. *The special case of Proposition 1.17 in which $x_1 = \ldots = x_r = 0$ is already a useful fact. Give a proof of this case that does not use Artin-Whaples approximation. Can you prove the general case without it?*

EXERCISE 1.21.
Let R be a Dedekind domain with fraction field K. Let $S \subset \operatorname{MaxSpec} R$ be finite.
a) (Moving Lemma) Let I be a fractional ideal of R. Show: there is $\alpha \in K^\times$ such that $(\alpha)I$ is coprime to S – i.e., $(\alpha)I = \prod_{i=1}^n \mathfrak{q}_i^{a_i}$ with $a_i \in \mathbb{Z}$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_n \in \operatorname{MaxSpec} R \setminus S$.
*b) Show: if R is **semilocal** – i.e., $\operatorname{MaxSpec} R$ is finite – then R is a PID.*
c) More generally, suppose R is semilocal, let L/K be a finite degree field extension, and let S be the integral closure of R in L. Show: S is a PID. (If you like, you may assume that L/K is separable or that S is finitely generated as an R-module. The result is still true without these assumptions, but you may not wish to worry about the commutative algebraic technicalities.)
d) Let $R = \mathbb{Z}$ and $L = \mathbb{Q}(\sqrt{-5})$, so $S = \mathbb{Z}[\sqrt{-5}]$. Use

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

to show that S is not a PID. Deduce: there are infinitely many prime numbers![5]
*e) What about the converse of part c)? More precisely: is there R with $\operatorname{MaxSpec} R$ infinite and such that for all finite degree field extensions L/K, the integral closure S of R in L is a PID? (See [**Cl67**].)*

1.8. Some Classification Theorems.

In this section we give some cases of fields k over which we can classify all norms. The first, and most famous, case is $k = \mathbb{Q}$:

THEOREM 1.18. *(Norms on $\mathbb{Q}$) Up to equivalence, the nontrivial norms on $\mathbb{Q}$ are precisely the Archimedean norm $|\cdot|_\infty$ and the p-adic norms.*

PROOF. Let $|\cdot|$ be a nontrivial norm on $\mathbb{Q}$. If $|\cdot|$ is Archimedean, then by Lemma 1.13 it is equivalent to $|\cdot|_\infty$. Otherwise $|\cdot|$ is non-Archimedean. Then by Proposition 1.11, it is $\mathbb{Z}$-regular on the Dedekind domain $\mathbb{Z}$, so its valuation ring is the localization at a prime ideal of $\mathbb{Z}$, i.e., it is a p-adic norm.

To show how little is up our sleeves, let's rephrase the non-Archimedean argument in more concrete terms:

Let $|\cdot|$ be a nontrivial non-Archimedean norm on $\mathbb{Q}$. By Proposition 1.11, $|\mathbb{Z}| \subset [0, 1]$. If $|n| = 1$ for every nonzero integer, then by multiplicativity $|\cdot|$ would

[5]This ridiculous – but amusing – proof of the infinitude of $\operatorname{Spec} \mathbb{Z}$ is due to Larry Washington.

be the trivial norm on $\mathbb{Q}$, so there exists a positive integer n with $|n| < 1$. Let p be the least such positive integer; it follows easily that p is prime. By adjusting the norm in its equivalence class, we may assume that $|p| = \frac{1}{p}$, and our task is now to prove that $|\ | = |\cdot|_p$. As a multiplicative group, $\mathbb{Q}^\times$ is generated by -1 and the primes numbers ℓ. Certainly $|-1| = |-1|_p = 1$, so it suffices to show that for all primes $\ell \neq p$, $|\ell| = |\ell|_p = 1$. So suppose not, i.e., there exists $\ell > p$ such that $|\ell| < 1$. Then there exist integers x, y such that $xp + y\ell = 1$, and hence

$$1 = |1| = |xp + y\ell| \leq \max(|xp|, |y\ell|) \leq \max(|p|, |\ell|) < 1,$$

contradiction! □

Next we give the "function field analogue" of Theorem 1.18: namely, we will classify all norms on $\mathbb{F}_q(t)$. Recall that by Exercise 1.3, every norm on $\mathbb{F}_q(t)$ restricts to the trivial norm on $\mathbb{F}_q$. So the following is a more general result:

THEOREM 1.19. *(Norms on $k(t)$) Let k be any field and let $K = k(t)$, the field of rational functions over k. Then every nontrivial norm on K that is trivial on k is equivalent to exactly one of the following norms:*
(i) $|\ |_P$ for $P \in k[t]$ a monic irreducible polynomial, or
(ii) the norm $|\cdot|_\infty$ defined by $\frac{p(t)}{q(t)} \mapsto 2^{\deg(p(t)) - \deg(q(t))}$.

PROOF. Let $|\cdot|$ be a norm on K which is trivial on k. Note that since $|\cdot|$ is trivial on k, in particular $|\mathbb{Z} \cdot 1| \subset [0, 1]$ so by Proposition 1.11 $|\cdot|$ is non-Archimedean. Let $R = \mathbb{F}_q[t]$ – a Dedekind domain with fraction field K.
Case 1: If $|\cdot|$ is R-regular, then by Theorem 1.16 the associated valuation is $v_\mathfrak{p}$ for a unique prime ideal $\mathfrak{p}$ of R. This is equivalent to what is stated in (i).
Case 2: Suppose $|R| \not\subset [0, 1]$. Since by hypothesis $|k| \subset [0, 1]$, we must have $|t| > 1$. Adjusting $|\cdot|$ in its equivalence class we may assume that $|t| = \frac{1}{2}$, and our task is now to show that $|\cdot| = |\cdot|_\infty$, for which it is sufficient to show that $|P| = 2^{\deg P}$ for each polynomial $P(t) = a_n t^n + \ldots + a_1 t + a_0$. But we know that $|a_i t^i| = 2^i$ for all i, so by the Principle of Domination (Exercise 1.9d)) we get $|P| = 2^{\deg P}$. □

Note the following remarkable similarity between Theorems 1.18 and 1.19: in both cases, most of the valuations come from the prime ideals of a particularly nice Dedekind domain (in fact, a PID) with fraction field k, but there is one exception, a valuation "at infinity". This seems strange: in the case of $\mathbb{Q}$ this exceptional valuation is Archimedean, whereas in the case of $k(t)$ it is non-Archimedean.

EXERCISE 1.22. *Suppose k is algebraically closed.*
a) Show that the group $G = PGL_2(k)$ acts faithfully on $k(t)$. (Hint: linear fractional transformation).
b) Show that the orbit of $|\cdot|_\infty$ under G consists of $|\cdot|_\infty$ together with all the norms $|\cdot|_{P_c}$ where $P_c(t) = t - c$ for $c \in k$.
c) Show that G acts transitively on the set of norms of $k(t)$ which are trivial on k iff k is algebraically closed.

The proof of Theorem 1.19 pulls the norm $|\cdot|_\infty$ on $k(t)$ out of a hat and then shows that it is up to equivalence the unique norm on $k(t)$ that is trivial on k and not regular on $k[t]$. The following explanation is perhaps more conceptual: a norm on $k(t)$ that is trivial on k and not regular on $k[t]$ corresponds to a valuation v_∞ which is non-negative on k but negative at t. One can obtain such a valuation by

pulling back the valuation v_t via the automorphism $\iota \in \mathrm{Aut}(k(t)/k)$ determined by $\iota(t) = \frac{1}{t}$. If $f = \frac{p(t)}{q(t)} = \frac{a_m t^m + \ldots + a_1 t + a_0}{b_n t^n + \ldots + b_1 t + b_0}$ with $a_m, b_n \neq 0$, then

$$v_\infty\left(\frac{p}{q}\right) = v_t\left(\frac{a_m t^{-m} + \ldots + a_1 t^{-1} + a_0}{b_n t^{-n} + \ldots + b_1 t^{-1} + b_0}\right) = v_t\left(\frac{a_m t^n + \ldots + a_0 t^{m+n}}{b_n t^m + \ldots + b_0 t^{m+n}}\right)$$
$$= n - m = \deg(q) - \deg(p).$$

And here is another take on the uniqueness: let v be any rank one valuation on $k(t)$ that is trivial on k. Then the valuation ring R_v contains t or $\frac{1}{t}$ and thus contains either $R[t]$ or $R[\frac{1}{t}]$. The latter ring is equally well a Dedekind domain (of course it is the isomorphic image of $R[t]$ under the field automorphism ι) so the $k[\frac{1}{t}]$-regular valuations on $k(t)$ correspond to maximal ideals in $k[\frac{1}{t}]$. The maximal ideals of $k[t]$ other than t are the maximal ideals of $k[t, \frac{1}{t}]$, which are also the maximal ideals of $k[\frac{1}{t}]$ other than $\frac{1}{t}$.

Let us now try to extend the above work to finite extension fields. This brings us to some key definitions: a **number field** is a field k that is a finite extension of $\mathbb{Q}$. A **function field** is a field that is a finite extension of $\mathbb{F}_p(t)$ for some prime p. (As a small remark, we would not change the definition of a function field by requiring the extension to be separable: because $\mathbb{F}_p$ is perfect, a field that is a finite, nonseparable extension of $\mathbb{F}_p(t)$ can also be realized as a finite separable extension of $\mathbb{F}_p(t)$.) A **global field** is a field k that is a finite extension either of $\mathbb{Q}$ or of $\mathbb{F}_p(t)$.

The side-by-side treatment of number fields and function fields is one of the hallmarks of modern number theory. We must quote André Weil, who eloquently cast it in the language of his day (May, 1967):

"Once the presence of the real field, albeit at infinite distance, ceases to be regarded as a necessary ingredient in the arithmetician's brew, it goes without saying that the function-fields over finite fields must be granted a fully simultaneous treatment with number-fields instead of the segregated status, and at best the separate but equal facilities, which hitherto have been their lot. That, far from losing by such treatment, both races stand to gain by it, is one fact which will, I hope, clearly emerge from this book."

We turn next to the classification of norms on an algebraic number field k. Much of what we have said before carries over verbatim. There is a subtlety concerning the inequivalent Archimedean norms that will not completely resolve at this point but rather return to in Chapter 2 after developing further tools. Moreover, unlike the case of $R = \mathbb{Z},\ k = \mathbb{Q}$, it is not immediately obvious that every valuation on K is regular on the ring of integers. For this, we use the following result:

PROPOSITION 1.20. *Let L/K be a finite degree field extension. Let R be a Dedekind domain with fraction field K, and let S be the integral closure of R in L.*
a) The ring S is a Dedekind domain with fraction field L.
b) Let v be a valuation on L. Then v is S-regular iff its restriction to K is R-regular.

PROOF. a) It is straightforward to see that S is an integrally closed domain in which every nonzero prime ideal is maximal (equivalently, of Krull dimension at most one): integral closures are integrally closed [**C:CA**, Cor. 14.11], and integral

extensions preserve the Krull dimension [**C:CA**, Cor. 14.17], and neither of these results lies very deep. So the matter of it is to show that S is Noetherian. Though this may seem like an unlikely worry, actually for all $d \geq 2$ there is an integrally closed Noetherian domain R of Krull dimension d with fraction field K and a finite degree field extension L/K such that the integral closure of R in L is not Noetherian! It turns out that things are much nicer in Krull dimension one: it is a consequence of the celebrated **Krull-Akizuki Theorem** [**C:CA**, Cor. 18.8] that if R is a Noetherian domain of Krull dimension 1 with fraction field K and L/K is a finite degree field extension, then the integral closure S of R in L is Noetherian, hence a Dedekind domain. This is a rather deep theorem. However, under the additional assumption that L/K is separable it becomes much easier, because then one can show that S is finitely generated as an R-module. Since R is Noetherian, S is then a Noetherian R-module: i.e., all R-submodules of S are finitely generated, and thus *a fortiori* all S-submodules of S – i.e., all ideals of S are finitely generated. The proof of this is not essentially different from the special case that the ring of integers of a number field is finitely generated as a $\mathbb{Z}$-module: see [**C:CA**, Thm. 18.1]. (In fact, when L/K is not assumed to be separable, S need not be finitely generated as an R-module, so the Krull-Akizuki Theorem really does lie deeper.)

b) Since $R \subset S$, certainly the R-regularity of $v|_K$ is necessary for the S-regularity of v. Conversely, let x be an element of S. By definition of integral closure, there exists $n \in \mathbb{Z}^+$ and $a_0, \ldots, a_{n-1} \in R$ such that

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

Seeking a contradiction, we suppose $v(x) = N < 0$. Since each a_i is in R, by hypothesis we have $v(a_i) \geq 0$ for all $0 \leq i < n$, so $v(a_i x^i) = iN + v(a_i) \geq iN$, whereas $v(x^n) = nN$. Thus in the sum $x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ we have a unique term of smallest valuation; by Exercise 1.9c), we get

$$\infty = v(0) = v(x^n + a_{n-1}x^{n-1} + \ldots + a_1 x_1 + a_0) = nN,$$

a contradiction. So $v(x) \geq 0$. □

THEOREM 1.21. *(Norms on a number field)*
Let $k \cong \mathbb{Q}[t]/(P(t))$ be a number field, with ring of integers $\mathbb{Z}_k$. Then:
a) For every non-Archimedean norm, the corresponding valuation is equivalent to the valuation $v_{\mathfrak{p}}$ attached to a nonzero prime ideal of $\mathbb{Z}_k$. Moreover, the valuations $v_{\mathfrak{p}}$ are pairwise inequivalent.
b) Every Archimedean embeddding, up to equivalence, is of the form $x \mapsto |\iota(x)|$, where $\iota : k \to \mathbb{C}$ is a field embedding and $|\cdot|$ is the standard absolute value on $\mathbb{C}$.
c) Let r_1 be the number of real roots of $P(t)$, and let r_2 be half the number of complex roots of $P(t)$. Let r be the number of Archimedean places. Then $1 \leq r \leq r_1 + r_2$.

PROOF. a) Since $\mathbb{Z}_k$ is a Dedekind domain, this follows from Theorem 1.16 and Proposition 1.20.
b) By the Big Ostrowski Theorem, every Archimedean absolute value, up to equivalence, arises from an embedding $\iota : k \hookrightarrow \mathbb{C}$. Since $k/\mathbb{Q}$ is finite separable, there are $[k : \mathbb{Q}]$ embeddings of k into $\mathbb{C}$, obtained by sending $t \pmod{P(t)}$ to each of the $[k : \mathbb{Q}]$ complex roots of $P(t)$.
c) The subtlety is that distinct embeddings $\iota : k \hookrightarrow \mathbb{C}$ may give rise to the same norm: cf. Exercise 1.4c). Indeed, because complex conjugation on $\mathbb{C}$ preserves the

standard norm $|\cdot|_\infty$, the number r of Archimedean places of k is at most the number of orbits of the set of embeddings under complex conjugation, namely $r_1 + r_2$. $\square$

Remark: Indeed we always have equality in part c): the number of Archimedean places is precisely $r_1 + r_2$. I looked long and hard to find a proof of this fact using only the tools we have developed so far. I found it in exactly one place: [**Lor**]. But the proof given there is not easy! We will come back to this point in the context of a more general discussion on extension of valuations.

EXERCISE 1.23. *Let k be a field, $R = k[t]$, $K = k(t)$, and L/K be a finite degree field extension. Let $|\cdot|$ be an absolute value on L that is trivial on k.*
a) Let S be the integral closure of $k[t]$ in L.[6] *Show that $|\ | = |\cdot|_{\mathcal{P}}$ for some prime ideal $\mathcal{P}$ of S iff the restriction of $|\cdot|$ to k* is not *$|\cdot|_\infty$.*
b) Let $|\cdot|_{\mathfrak{p}}$ be an R-regular norm on K, with corresponding prime ideal $\mathfrak{p}$ of R. Express the number of places of L which restrict to $|\cdot|$ in terms of the factorization of $\mathfrak{p}$ in S.
c) Suppose $L \cong K[t]/P(t)$ for an irreducible polynomial $P(t)$.[7] *Can you give a more concrete description of the number of places of L which restrict to $|\cdot|_{\mathfrak{p}}$?*
d) Show that the number of places of L that extend the infinite place $|\cdot|_\infty$ of K is positive and at most $[L : K]$. Can you say more?

EXERCISE 1.24. *(For those with some knowledge of algebraic geometry.) Let $C_{/k}$ be a smooth, projective geometrically integral curve. Let v be a rank one valuation on the function field $k(C)$ that is trivial on k. Show: there is a unique closed point P such that for all $f \in k(C)^\times$, $v(f)$ is the order of vanishing of f at P.*

Let L/K be a finite degree field extension and $|\cdot|$ a place on K. As we can see from the above results and exercises, with our current vocabulary it is slightly awkward to describe the number of places of L which extend the place $|\cdot|$ of K. To elaborate: suppose for simplicity that $|\cdot|$ is a non-Archimedean place whose corresponding valuation is discrete and that L/K is separable. Then the valuation ring R of $|\cdot|$ is a DVR with fraction field K. Let S be the integral closure of R in L, so that S is again a Dedekind domain with finitely many maximal ideals (so, in fact, a PID). What we want is precisely to count the number of maximal ideals of S. In classical number theory, we do this via the criterion of Kummer-Dedekind: namely, we write $L = K[x] \cong K[t]/(P)$, where $x \in S$ has minimal polynomial $P(t)$, and then we factor P modulo the maximal ideal $\mathfrak{p}$ of R. Unfortunately this only works when $S = R[x]$. In the number field case, it is easy to see that this condition holds at least for all but the primes dividing the discriminant of the minimal polynomial P, which is usually enough for applications. But now we are in the local case, and as we shall see it is simply not true that S need be monogenic as an R-module.

In summary, the fact that ring extensions are more complicated than field extensions is doing us in. What would be fantastic is if the number of maximal ideals of S could be expressed in terms of the factorization of the polynomial P in some **field extension**. This is exactly what the theory of completions will give us, so we turn to that next.

[6]Recall that S is a Dedekind domain: cf. the proof of Proposition 1.20a).
[7]By the **Primitive Element Corollary**, this occurs if L/K is separable.

2. Completions

2.1. Introduction.

The key idea is that of the **completion** $\hat{K}$ of a normed field $(K, |\cdot|)$. This is a special case of the completion of a metric space – a concept which we will review – but bears further scrutiny in this case because we wish $\hat{K}$ to itself have the structure of a normed field.

THEOREM 1.22. *Let $(K, |\cdot|)$ be a normed field.*
a) There is a complete normed field $(\hat{K}, |\cdot|)$ and a homomorphism of normed fields $\iota : (K, |\cdot|) \to (\hat{K}, |\cdot|)$ such that $\iota(K)$ is dense in $\hat{K}$.
b) The homomorphism ι is universal for norm-preserving homomorphisms of K into complete normed fields.
c) In particular, $\hat{K}$ is unique up to canonical isomorphism.
d) It follows that any homomorphism of normed fields extends uniquely to a homomorphism on the completions.

Remark: In categorical language, these results amount to the following: completion is a functor from the category of normed fields to the category of complete normed fields which is left adjoint to the forgetful functor from the category of complete normed fields to the category of normed fields. We stress that, for our purposes here, it is absolutely not necessary to understand what the previous sentence means.

2.2. Reminders on metric spaces.

Let X be a set. A **metric** on X is a function $\rho : X \times X \to [0, \infty)$ satisfying:
(M1) (positive definiteness) $\forall x, y \in X,\ \rho(x, y) = 0 \iff x = y$.
(M2) (symmetry) $\forall x, y \in X,\ \rho(x, y) = \rho(y, x)$.
(M3) (triangle inequality) $\forall x, y, z \in X,\ \rho(x, z) \leq \rho(x, y) + \rho(y, z)$.

A **metric space** is a pair (X, ρ) where ρ is a metric on X.

For x an element of a metric space X and $r \in \mathbb{R}^{>0}$, we define the **open ball**

$$B_{<r}(x) = \{y \in X \mid \rho(y, x) < r\}.$$

The open balls form the base for a topology on X, the **metric topology**. With your indulgence, let's check this. What we must show is that if $z \in B_{<r_1}(x) \cap B_{<r_2}(y)$, then there exists $r_3 > 0$ such that $B_{<r_2}(z) \subset B_{<r_1}(x) \cap B_{<r_2}(y)$. Let $r_3 = \min(r_1 - \rho(x, z), r_2 - \rho(y, z))$, and let $w \in B_{<r_3}(z)$. Then by the triangle inequality $\rho(x, w) \leq \rho(x, z) + \rho(z, w) < \rho(x, z) + (r_1 - \rho(x, z)) = r_1$, and similarly $\rho(y, w) < r_2$.

Given a finite collection of metric spaces $\{(X_i, \rho_i)\}_{1 \leq i \leq n}$, we define the **product metric** on $X = \prod_{i=1}^n X_i$ to be $\rho(x, y) = \max_i \rho_i(x_i, y_i)$.[8]

Remark: As is typical, instead of referring to "the metric space (X, ρ)", we will often say instead "the metric space X", i.e., we allow X to stand both for the set and for the pair (X, ρ).

[8]This is just one of many possible choices of a product metric. The non-canonicity in the choice of the product is a clue that our setup is not optimal. But the remedy for this, namely **uniform spaces**, is not worth our time to develop.

EXERCISE 1.25. *Let X be a set. A function $\rho : X \times X \to \mathbb{R}^{\geq 0}$ satisfying (M2) and (M3) is called a* ***pseudometric****, and a set X endowed with a pseudometric is called a* ***pseudometric space****.*
a) Show that all of the above holds for pseudometric spaces – in particular, the open balls form the base for a topology on X, the ***pseudometric topology****.*
b) Show that for a pseudometric space (X, ρ), the following are equivalent:
(i) ρ is a metric.
(ii) The topological space X is Hausdorff.
(iii) The topological space X is separated (i.e., T_1: points are closed).
(iv) The topological space X is Kolmogorov (i.e., T_0: no two distinct points have exactly the same open neighborhoods).
c) Define an equivalence relation $\sim$ on X by $x \sim y \iff \rho(x, y) = 0$. Let $\overline{X} = X/\sim$ be the set of equivalence classes. Show that ρ factors through a function $\overline{\rho} : \overline{X} \times \overline{X} \to \mathbb{R}^{\geq 0}$ and that $\overline{\rho}$ is a metric on $\overline{X}$. Show that the map $q : X \to \overline{X}$ is the ***Kolmogorov completion*** *of the topological space X, i.e., it is the universal continuous map from X into a T_0-space.*

A **Cauchy sequence** in a metric space (X, ρ) is a sequence $\{x_n\}$ in X such that for all $\epsilon > 0$, there exists $N \in \mathbb{Z}^+$ such that $m, n \geq N \implies \rho(x_m, x_n) < \epsilon$. Every convergent sequence is convergent. Conversely, we say that a metric space X is **complete** if every Cauchy sequence converges.

Let X and Y be metric spaces. A function $f : X \to Y$ is **uniformly continuous** if for all $\epsilon > 0$, there exists $\delta > 0$ such that $\forall x, y \in X, \rho_X(x, y) < \delta \implies \rho_Y(f(x), f(y)) < \epsilon$.

EXERCISE 1.26. *Let (X, ρ) be a metric space. Show that $\rho : X \times X \to \mathbb{R}$ is a uniformly continuous function: here $\mathbb{R}$ is endowed with the standard Euclidean metric $\rho(x, y) = |x - y|$.*

EXERCISE 1.27. *Let $f : X \to Y$ be a continuous function between metric spaces.*
a) If f is uniformly continuous and $\{x_n\}$ is a Cauchy sequence in X, show that $\{f(x_n)\}$ is a Cauchy sequence in Y.
b) Give an example to show that a merely continuous function need not map Cauchy sequences to Cauchy sequences.

A topological space is **compact** if it is Hausdorff and every open covering has a finite subcovering. A topological space is **locally compact** if it is Hausdorff and every point admits a compact neighborhood. This is equivalent (thanks to the Hausdorff condition!) to the apparently stronger condition that every point has a local base of compact neighborhoods.

A metric space (X, ρ) is **ball compact**[9] if every closed bounded ball is compact.

EXERCISE 1.28. *Consider the following properties of a metric space (X, ρ):*
(i) X is compact.
(ii) X is ball compact.
(iii) X is locally compact.
(iv) X is complete.

[9] I made up the term.

Show that (i) $\implies$ (ii) $\implies$ (iii) and (ii) $\implies$ (iv), but none of the other implications hold.

2.3. Ultrametric spaces.

An **ultrametric space** is a metric space (X, ρ) in which the following stronger version of the triangle inequality holds:

$$\forall x, y, z \in X,\ \rho(x, z) \leq \max(\rho(x, y), \rho(y, z)).$$

PROPOSITION 1.23. *(Isosceles Law)*
Let x, y, z be points in an ultrametric space (X, ρ).
a) If $\rho(x, y) < \rho(x, z)$, then $\rho(x, z) = \rho(y, z)$.
b) In particular, at least two of $\rho(x, y)$, $\rho(x, z)$, $\rho(y, z)$ must be equal: "Every triangle in an ultrametric space is isosceles."

PROOF. a) We have

$$\rho(y, z) \leq \max \rho(y, x), \rho(x, z) = \rho(x, z).$$

If we had $\rho(y, z) < \rho(x, z)$, then

$$\rho(x, z) \leq \max \rho(x, y), \rho(y, z) < \rho(x, z),$$

a contradiction.
b) This follows immediately. □

LEMMA 1.24. *Let (X, ρ) be an ultrametric space, let $x_n \to x$ be a convergent sequence in X, and let $y \in X \setminus \{x\}$. Then for all sufficently large n, $\rho(x_n, y) = \rho(x, y)$.*

PROOF. Choose $N \in \mathbb{Z}^+$ such that for all $n \geq N$, $\rho(x, x_n) < \rho(x, y)$, and apply the Isosceles Law to x, x_n, y. □

LEMMA 1.25. *Let (X, ρ) be a compact metric space, and let $f : X \to \mathbb{R}$ be **locally constant**: for all $x \in X$, there is $r > 0$ such that $f|_{B_{<r}(x)}$ is constant. Then:*
a) The image $f(X)$ is finite.
*b) f is **uniformly locally constant**: there is $\delta > 0$ such that for all $x, y \in X$, if $\rho(x, y) < \delta$ then $f(x) = f(y)$.*

PROOF. a) By the very definition of a locally constant function, for all $x \in X$, $U_x = f^{-1}(f(x))$ is open in X. This gives an open covering of X; since X is compact we may extract a finite subcovering. This shows that $f(X)$ is finite. (Note that we did not use the metric yet: this holds for any continuous function on a quasi-compact topological space.)
b) A direct proof of this is similar to the argument that any continuous function on a compact metric space is uniformly continuous. We leave this to the reader as an (informal exercise). To show something a little different, we recall that every open covering $\{U_i\}_{i \in I}$ of a compact metric space (X, ρ) has a **Lebesgue number**: i.e., there is some $\delta > 0$ such that any subset $Y \subset X$ with diameter at most δ lies in some U_i. Applying this fact to the finite covering given by the fibers of the map f as in part a), we deduce the result. □

PROPOSITION 1.26. *Let (X, ρ) be an ultrametric space, and let $\Omega \subset X$ be a compact subset.*
a) Let $y \in X \setminus \Omega$. Then the set $\{d(x, a) \mid x \in \Omega\}$ is finite.
b) Let $y \in \Omega$. Then the set $\{d(x, y) \mid x \in \Omega\}$ is bounded and has no positive real number as an accumulation point.

PROOF. a) The function $f : \Omega \to \mathbb{R}$ given by $x \mapsto \rho(x, y)$ is continuous; it follows easily from Lemma 1.24 that it is locally constant. By Lemma 1.25, $f(\Omega) = \{d(x, y) \mid x \in \Omega\}$ is finite. b) As above we define $f : \Omega \to \mathbb{R}$ by $x \mapsto \rho(x, y)$. Fix $\epsilon > 0$. We may apply part a) with Ω replaced by $\Omega \setminus B_{<\epsilon}(y)$ to get that $f(\Omega) \cap [\epsilon, \infty)$ is finite. This shows both the boundedness and the nonexistence of any positive real number as an accumulation point. □

EXERCISE 1.29. *Let $B = B_{<r}(x)$ be an open ball in an ultrametric space (X, ρ) and let $y \in B_{<r}(x)$. Show that y is also a center for B: $B = B_{<r}(y)$. Does the same hold for closed balls?*

EXERCISE 1.30. *Let B_1, B_2 be two balls (each may be either open or closed) in an ultrametric space (X, ρ). Show that B_1 and B_2 are either disjoint or concentric: i.e., there exists $x \in X$ and $r_1, r_2 \in (0, \infty)$ such that $B_i = B(x, r_i)$ or $B_c(x, r_i)$.*

EXERCISE 1.31. *Let (X, ρ) be an ultrametric space.*
a) Let $r \in (0, \infty)$. Show that the set of open (resp. closed) balls with radius r forms a partition of X.
b) Deduce from part a) that every open ball is also a closed subset of X and that every closed ball of positive radius is also an open subset of X.
*c) A topological space is **zero-dimensional** if there exists a base for the topology consisting of clopen (= closed and open) sets. Thus part b) shows that an ultrametric space is zero-dimensional. Show that a zero-dimensional Hausdorff space is totally disconnected. In particular, an ultrametric space is totally disconnected.*

EXERCISE 1.32. *Prove or disprove: it is possible for the same topological space (X, τ) to have two compatible metrics ρ_1 and ρ_2 (i.e., each inducing the given topology τ on X) such that ρ_1 is an ultrametric and ρ_2 is not.*

EXERCISE 1.33. *Let Ω be a nonempty set, and let $\mathcal{S} = \prod_{i=1}^{\infty} \Omega$, i.e., the space of infinite sequences of elements in Ω, endowed with the metric $\rho(x, y) = 2^{-N}$ if $x_n = y_n$ for all $n < N$ and $x_N \neq y_N$. (If $x_n = y_n$ for all n, then we take $N = \infty$.)*
a) Show that $(\mathcal{S}, \rho)$ is an ultrametric space, and that the induced topology coincides with the product topology on $\mathcal{S}$, each copy of Ω being given the discrete topology.
b) Show that $\mathcal{S}$ is a complete[10] metric space without isolated points.
c) Without using Tychonoff's theorem, show that $\mathcal{S}$ is compact iff Ω is finite. (Hint: since $\mathcal{S}$ is metrizable, compact is equivalent to sequentially compact. Show this via a diagonalization argument.)
d) Suppose Ω_1 and Ω_2 are two finite sets, each containing more than one element. Show that the spaces $\mathcal{S}(\Omega_1)$ and $\mathcal{S}(\Omega_2)$ are homeomorphic.

2.4. Normed commutative groups.

Let G be a commutative group, written additively. By a **norm** on G we mean a map $| \ | : G \to \mathbb{R}^{\geq 0}$ such that:

[10]Completeness is formally defined in the next section.

(NAG1) $|g| = 0 \iff g = 0$.
(NAG2) $\forall g \in G,\ |-g| = |g|$.
(NAG3) $\forall g, h \in G,\ |g + h| \leq |g| + |h|$.

For example, an absolute value on a field k is (in particular) a norm on $(k, +)$. By analogy to the case of fields, we will say that a norm is **non-Archimedean** if $\forall g, h \in G,\ |g + h| \leq |g| + |h|$.

EXERCISE 1.34. *For a normed commutative group $(G, |\cdot|)$, define $\rho : G^2 \to \mathbb{R}^{\geq 0}$ by $\rho(x, y) = |x - y|$.*
*a) Show that ρ defines a **metric** on G. Show that the norm is non-Archimedean iff ρ is an ultrametric.*
b) Show that the norm $|\cdot| : G \to \mathbb{R}$ is uniformly continuous.

The metric topology on G is Hausdorff and first countable, so convergence can be described in terms of sequences: a sequence $\{x_n\}$ in X **converges** to $x \in G$ if for all $\epsilon > 0$, there exists $N = N(\epsilon)$ such that for all $n \geq N$, $\rho(x_n, x) < \epsilon$. A sequence is said to be **convergent** if it converges to some x. Since G is Hausdorff, a sequence converges to at most one point.

A **semi-norm** on a commutative group is a map $|\cdot| : G \to \mathbb{R}^{\geq 0}$ which satisfies (NAG2) and (NAG3). Show that a semi-norm induces a pseudometric on G.

EXERCISE 1.35. *Suppose G is an arbitrary (i.e., not necessarily abelian) group – with identity element e and group law written multiplicatively – endowed with a function $|\cdot| : G \to \mathbb{R}^{\geq 0}$ satisfying:*
(NAG1) $|g| = 0 \iff g = e$.
(NAG2) $\forall g \in G,\ |g^{-1}| = |g|$.
(NAG3) $\forall g, h \in G, |gh| \leq |g| + |h|$.
a) Show that $d : G \times G \to \mathbb{R},\ (g, h) \mapsto |gh^{-1}|$ defines a metric on G.
b) If $|\cdot|$ is a norm on G and $C \in R^{>0}$, show that $C|\cdot|$ is again a norm on G. Let us write $|\cdot|_1 \approx |\cdot|_2$ for two norms which differ by a constant in this way.
c) Define on any group G a trivial norm; show that it induces the discrete metric.

In any topological commutative group, it makes sense to discuss the convergence of infinite series $\sum_{n=1}^{\infty} a_n$ in G: as usual, we say $\sum_{n=1}^{\infty} a_n = S$ if the sequence $\{\sum_{k=1}^{n} a_k\}$ of partial sums converges to S.

A series $\sum_{n=1}^{\infty} a_n$ is **unconditionally convergent** if there exists $S \in G$ such that for every permutation σ of the positive integers, the series $\sum_{n=1}^{\infty} a_{\sigma(n)}$ converges to S.

In a normed commutative group G we may speak of **absolute convergence**: we say that $\sum_{n=1}^{\infty} a_n$ is **absolutely convergent** if the real series $\sum_{n=1}^{\infty} |a_n|$ converges.

EXERCISE 1.36. *For a normed group G, show that the following are equivalent:*
(i) Every absolutely convergent series is unconditionally convergent.
(ii) G is complete.

Whether unconditional convergence implies absolute convergence is more delicate. If $G = \mathbb{R}^n$ with the standard Euclidean norm, then by the **Riemann Rearrangement Theorem** unconditional convergence implies absolute convergence. On the

other hand, it is a famous theorem of Dvoretzky-Rogers [**DR50**] that in any infinite dimensional real Banach space (i.e., a complete, normed $\mathbb{R}$-vector space) there exists a series which is unconditionally convergent but not absolutely convergent.

Convergence in complete non-Archimedean normed groups is much simpler:

PROPOSITION 1.27. *Let G be a complete, non-Archimedean normed group, and let $\{a_n\}_{n=1}^{\infty}$ be a sequence in G. The following are equivalent:*
(i) The series $\sum_{n=1}^{\infty} a_n$ is unconditionally convergent.
(ii) The series $\sum_{n=1}^{\infty} a_n$ is convergent.
(iii) $\lim_{n\to\infty} a_n = 0$.

EXERCISE 1.37. *Prove Proposition 1.27.*

PROPOSITION 1.28. *Let X be a topological space.*
a) Let (M, ρ) is a complete metric space, and let $f_n : X \to M$ be a sequence of continuous functions such that for all $\epsilon > 0$, there is $N \in \mathbb{Z}^+$ such that for all $m, n \geq N$,

$$\rho(f_m, f_n) = \sup_{x \in X} \rho(f_m(x), f_n(x)) < \epsilon.$$

There is a continuous function $f : X \to M$ such that f_n converges uniformly to f.
*b) (**Ultrametric Weierstrass M-Test**) Let $(G, |\cdot|)$ be a complete ultrametric normed commutative group, and let $f_n : X \to G$ be a sequence of continuous functions such that*

$$||f_n|| = \sup_{x \in X} |f_n(x)| \to 0.$$

Then the series $\sum_n f_n$ converges uniformly on X to a continuous function.

PROOF. a) For each $x \in X$, $f_m(x)$ is a Cauchy sequence in the complete metric space M, so it converges; we define $f(x)$ to be the limit. It is immediate to see that the convergence of f_n to f is uniform on X, and the usual argument from advanced calculus / undergraduate real analysis that the limit of a uniformly convergent sequence of continuous functions is continuous applies here.
b) Because G is ultrametric, the hypothesis of part a) applies to the sequence of partial sums $\sum_{k=1}^{n} f_k$. □

EXERCISE 1.38. *Use Proposition 1.27 to give an explicit example of a series in $\mathbb{Q}_p$ which is unconditionally convergent but not absolutely convergent.*

EXERCISE 1.39. *Let $(G, |\cdot|)$ be a normed commutative group. Suppose that G is locally compact in the norm topology.*
a) Show that G is complete.
b) Must G be ball compact?

2.5. The topology on a normed field.

Let k be a field and $|\cdot|$ an Artin absolute value on k. We claim that there is a unique metrizable topology on k such that a sequence $\{x_n\}$ in k converges to $x \in k$ iff $|x_n - x| \to 0$. To see this, first note that the condition $|x_n - x| \to 0$ depends only on the equivalence class of the Artin absolute value, since certainly $|x_n - x| \to 0 \iff |x_n - x|^{\alpha} \to 0$ for any positive real number α. So without changing the convergence of any sequence, we may adjust $|\cdot|$ in its equivalence class to get an absolute value (i.e., with Artin constant $C \leq 2$) and then we define

the topology to be the metric topology with respect to $\rho(x,y) = |x-y|$ as above. Of course this recovers the given notion of convergence of sequences. Finally, we recall that a metrizable topological space is first countable and that there exists at most one first countable topology on a set with a given set of convergent sequences. We call this topology the **valuation topology**.

EXERCISE 1.40. *Show that the trivial valuation induces the discrete topology.*

EXERCISE 1.41. *Let $(k, |\cdot|)$ be a valued field, and let $\{x_n\}$ be a sequence in k. Show that $x_n \to 0$ iff $|x_n| \to 0$.*

PROPOSITION 1.29. *Let $|\cdot|_1$ and $|\cdot|_2$ be norms on a field k. The following are equivalent:*
(i) $|\cdot|_1 \sim |\cdot|_2$ in the sense of Theorem 1.4.
(ii) The topologies induced by $|\cdot|_1$ and $|\cdot|_2$ coincide.

PROOF. The direction (i) $\implies$ (ii) follows from the discussion given above. Assume (ii). Let $x \in k$. Then $|x|_1 < 1 \iff x^n \to 0$ in the $|\cdot|_1$-topology iff $x^n \to 0$ in the $|\cdot|_2$-metric topology $\iff |x|_2 < 1 \iff |\cdot|_1 \sim |\cdot|_2$. □

An equivalent topological statement of Artin-Whaples approximation is:

THEOREM 1.30. *(Artin-Whaples Restated) Let k be a field and, for $1 \leq i \leq n$, let $|\cdot|_i$ be inequivalent nontrivial norms on k. Let (k, τ_i) denote k endowed with the $|\cdot|_i$-norm topology, and let $k^n = \prod_{i=1}^n (k, \tau_i)$. Then the diagonal map $\Delta : k \hookrightarrow k^n,\ x \mapsto (x, \ldots, x)$ has dense image.*

EXERCISE 1.42. *Convince yourself that this is equivalent to Theorem 1.5.*

EXERCISE 1.43. *Show that any two closed balls of finite radius in a normed field are homeomorphic. Deduce that a locally compact normed field is ball compact.*

2.6. Completion of a metric space.

LEMMA 1.31. *Let (X, ρ_X) be a metric space, (Y, ρ_Y) be a complete metric space, $Z \subset X$ a dense subset and $f : Z \to Y$ a continuous function.*
a) There exists at most one extension of f to a continuous function $F : X \to Y$. (N.B.: This holds for for any topological space X and any Hausdorff space Y.)
b) f is uniformly continuous $\implies$ f extends to a uniformly continuous $F : X \to Y$.
c) If f is an isometric embedding, then its extension F is an isometric embedding.

EXERCISE 1.44. *Prove Lemma 1.31.*

Let us say that a map $f : X \to Y$ of topological spaces is **dense** if $f(X)$ is dense in Y. An **isometric embedding** is a map $f : (X, \rho_X) \to (Y, \rho_Y)$ such that for all $x_1,\ x_2 \in X$, $\rho_Y(f(x_1), f(x_2)) = \rho_X(x_1, x_2)$. An **isometry** is a surjective isometric embedding.

EXERCISE 1.45. *Let f be an isometric embedding of metric spaces.*
a) Show that f is uniformly continuous with $\delta = \epsilon$.
b) Show that f is injective. Therefore an isometry is bijective. Show that if f is an isometry, then f^{-1} is also an isometry.

THEOREM 1.32. *let (X, ρ) be a metric space.*
a) There is a complete metric space $\hat{X}$ and a dense isometric embedding $\iota : X \to \hat{X}$.
b) The completion ι satisfies the following universal mapping property: if (Y, ρ) is

a complete metric space and $f : X \to Y$ is a uniformly continuous map, then there exists a unique uniformly continuous map $F : \hat{X} \to Y$ such that $f = F \circ \iota$.
c) If $\iota' : X \hookrightarrow \hat{X}'$ is another isometric embedding into a complete metric space with dense image, then there exists a unique isometry $\Phi : \hat{X} \to \hat{X}'$ such that $\iota' = \Phi \circ \iota$.

PROOF. a) Let $X^\infty = \prod_{i=1}^\infty X$ be the set of all sequences in X. Inside X, we define $\mathcal{X}$ to be the set of all Cauchy sequences. We introduce an equivalence relation on $\mathcal{X}$ by $x_\bullet \sim y_\bullet$ if $\rho(x_n, y_n) \to 0$. Put $\hat{X} = \mathcal{X}/\sim$. For any $x \in X$, define $\iota(x) = (x, x, \ldots)$, the constant sequence based on x. This of course converges to x, so is Cauchy and hence lies in $\mathcal{X}$. The composite map $X \stackrel{\iota}{\to} \mathcal{X} \stackrel{\sim}{\to} \hat{X}$ (which we continue to denote by ι) is injective, since $\rho(x_n, y_n) = \rho(x, y)$ does not approach zero. We define a map $\hat{\rho} : \mathcal{X} \times \mathcal{X} \to \mathbb{R}$ by

$$\hat{\rho}(x_\bullet, y_\bullet) = \lim_{n\to\infty} \rho(x_n, y_n).$$

To see that this limit exists, we may reason (for instance) as follows: the sequence $x_\bullet \times y_\bullet$ is Cauchy in $X \times X$, hence its image under the uniformly continuous function ρ is Cauchy in the complete metric space $\mathbb{R}$, so it is convergent. It is easy to see that $\hat{\rho}$ factors through to a map $\hat{\rho} : \hat{X} \to \hat{X} \to \mathbb{R}$. The verification that $\hat{\rho}$ is a metric on $\hat{X}$ and that $\iota : X \to \hat{X}$ is an isometric embedding is straightforward and left to the reader. Moreover, if $x_\bullet = \{x_n\}$ is a Cauchy sequence in X, then the sequence of constant sequences $\{\iota(x_n)\}$ is easily seen to converge to $x_\bullet$ in $\hat{X}$.
b) Let $x_\bullet \in \mathcal{X}$ be a Cauchy sequence in X. As above, since f is uniformly continuous and Y is complete, $f(x_\bullet)$ is convergent in Y to a unique point, say y, and we put $y = F(x_\bullet)$. Since X is dense in $\hat{X}$ this is the only possible choice, and by Lemma 1.31 it does indeed give a well-defined uniformly continuous function $F : X \to Y$.
c) Isometric embeddings are uniformly continuous, so we may apply the universal mapping property of part b) to the map $\iota' : X \hookrightarrow \hat{X}'$ to get a map $\Phi : \hat{X} \to \hat{X}'$. Similarly, we get a map $\Phi' : \hat{X}' \to \hat{X}$. The compositions $\Phi' \circ \Phi$ and $\Phi' \circ \Phi$ are uniformly continuous maps which restrict to the identity on the dense subspace X, so they must each by the identity map, i.e., Φ and Φ' are mutually inverse bijections. By Lemma 1.31c), Φ is an isometric embedding, so it is an isometry. □

We refer to $\hat{X}$ as the **completion** of X.[11]

COROLLARY 1.33. *(Functoriality of completion)*
a) Let $f : X \to Y$ be a uniformly continuous map between metric spaces. Then there exists a unique map $F : \hat{X} \to \hat{Y}$ making the following diagram commute:

$$\begin{array}{ccc} X & \stackrel{f}{\to} & Y \\ \hat{X} & \stackrel{F}{\to} & \hat{Y}. \end{array}$$

b) If f is an isometric embedding, so is F.
c) If f is an isometry, so is F.

PROOF. a) The map $f' : X \to Y \hookrightarrow \hat{Y}$, being a composition of uniformly continuous maps, is uniformly continuous. Applying the universal property of completion to f' gives a unique extension $\hat{X} \to \hat{Y}$.
Part b) follows immediate from Lemma 1.31b). As for part c), if f is an isometry,

[11]Really we should refer to the *map* $\iota : X \hookrightarrow \hat{X}$ as the completion, but one rarely does so.

so is its inverse f^{-1}. The extension of f^{-1} to a mapping from $\hat{Y}$ to $\hat{X}$ is easily seen to be the inverse function of F. □

EXERCISE 1.46. *For a metric space (X, ρ), define the* ***distance set*** $\mathcal{D}(X) = \rho(X \times X)$*, i.e., the set real numbers which arise distances between points in X.*
a) Prove or disprove: if $\mathcal{D}$ is a discrete subset of $\mathbb{R}$, then ρ is ultrametric.
b) Prove or disprove: if ρ is an ultrametric, then $\mathcal{D}$ is discrete.
c) Let $\tilde{X}$ be the completion of X. Show that $\mathcal{D}(\tilde{X}) = \overline{\mathcal{D}(X)}$ (closure in $\mathbb{R}$).
d)(U) Determine which subsets of $\mathbb{R}^{\geq 0}$ arise as distance sets of some metric space.

EXERCISE 1.47. *The notion of a metric space and a completion seems to presuppose knowledge of $\mathbb{R}$, the set of real numbers. In particular, it is* a priori *logically unacceptable to* define $\mathbb{R}$ *to be the completion of $\mathbb{Q}$ with respect to the Archimedean norm $|\cdot|_\infty$. (Apparently for such reasons, Bourbaki's influential text* General Topology *avoids mention of the real numbers until page* 329*, long after a general discussion of uniform spaces and topological groups.) Show that this is in fact not necessary and that the completion of a metric space* can *be used to construct the real numbers. (Hint: first define a $\mathbb{Q}$-valued metric and its completion.)*

2.7. Completions of normed commutative groups and normed fields.

When G is a normed commutative group (or a field with an absolute value) we wish to show that the completion $\tilde{G}$ is, in a natural way, again a normed commutative group (or a field with an absolute value). This follows readily from the results in the previous section, but we take the opportunity to point out a simplification in the construction of $\hat{G}$ in this case.

As above, we put $G^\infty = \prod_{i=1}^\infty$ and $\mathcal{G}$ the subset of Cauchy sequences. But this time G^∞ is a commutative group and $\mathcal{G}$ is a subgroup of G^∞ (easy exercise). Furthermore, we may define $\mathfrak{g}$ to be the set of sequences converging to 0, and then $\mathfrak{g}$ is a subgroup of $\mathcal{G}$. Thus in this case we may define $\hat{G}$ simply to be the quotient group $\mathcal{G}/\mathfrak{g}$, so by its provenance it has the structure of a commutative group. Moreover, if $x_\bullet$ is a Cauchy sequence in G, then by Exercise 1.34 the sequence $|x_\bullet|$ is Cauchy in $\mathbb{R}$, hence convergent, and we may define

$$|x_\bullet| \coloneqq \lim_{n\to\infty} |x_n|.$$

We leave it to the reader to carry through the verifications that this factors to give a norm on $\hat{G}$ whose associated metric is the same one that we constructed in the proof of Theorem 1.32.

Now suppose that $(k, |\cdot|)$ is a normed field. Then the additive group $(k, +)$ is a normed commutative group, so the completion $\hat{k}$ exists at least as a normed commutative group. Again though we want more, namely we want to define a multiplication on $\hat{k}$ in such a way that it becomes a field and that the norm satisfies $|xy| = |x||y|$. Again the product map on k is uniformly continuous, so that it extends to $\hat{k}$, but to see that $\hat{k}$ is a field the algebraic construction is more useful. Indeed, it is not hard to show that k^∞ is a ring, the Cauchy sequences $\mathcal{K}$ form a subring. But more is true:

LEMMA 1.34. *The set $\mathfrak{k}$ of sequences converging to 0 is a maximal ideal of the ring $\mathcal{K}$ of Cauchy sequences. Therefore the quotient $\mathcal{K}/\mathfrak{k} = \hat{k}$ is a field.*

PROOF. Since a Cauchy sequence is bounded, and a sequence which converges to 0 multiplied by a bounded sequence again converges to 0, it follows that $\mathfrak{k}$ is an ideal of $\mathcal{K}$. To show that the quotient is a field, let $x_\bullet$ be a Cauchy sequence which does not converge to 0. Then we need to show that $x_\bullet$ differs by a sequence converging to 0 from a unit in $\mathcal{K}$. But since $x_\bullet$ is Cauchy and not convergent to 0, then (e.g. since it converges to a nonzero element in the commutative group $\hat{k}$) we have $x_n \neq 0$ for all sufficiently large n. Since changing any finite number of coordinates of $x_\bullet$ amounts to adding a sequence which is ultimately zero hence convergent to 0, this is permissible as above, so after adding an element of $\mathfrak{k}$ we may assume that for all $n \in \mathbb{Z}^+$, $x_n \neq 0$, and then the inverse of $x_\bullet$ in $\mathcal{K}$ is $\{\frac{1}{x_n}\}$. □

EXERCISE 1.48. *(This is challenging.) Find all maximal ideals in the ring $\mathcal{K}$.*

EXERCISE 1.49. *Let $(k, |\cdot|)$ be a nontrivially normed field.*
a) Show that $\#\{x \in k \mid 0 < |x| < 1\} = \#k$.
b) Show that the cardinality of the set of all convergent sequences in k is $(\#k)^{\aleph_0}$. Deduce that the same holds for the set of all Cauchy seqeunces of k.
c) Show that the cardinality of the completion of k is $(\#k)^{\aleph_0}$. (Hint: consider separately the cases in which $\#k = (\#k)^{\aleph_0}$ and $\#k < (\#k)^{\aleph_0}$.

Thus for a field k to be complete with respect to a nontrivial norm, it must satisfy a rather delicate cardinality requirement: $(\#k)^{\aleph_0} = \#k$. This certainly implies $\#k \geq 2^{\aleph_0} = \#\mathbb{R}$, i.e., k has at least continuum cardinality. Conversely, there are certainly complete fields of continuum cardinality, and indeed have $(2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \times \aleph_0} = 2^{\aleph_0}$. However, there are sets S with $2^{\aleph_0} < \#S < (\#S)^{\aleph_0}$.

Let $(k, |\cdot|)$ be a normed field, and let $\sigma : k \to k$ be a field automorphism. We say that σ is an automorphism of the normed field $(k, |\cdot|)$ if $\sigma^*|\cdot| = |\cdot|$.

EXERCISE 1.50. *Let $(K, |\cdot|)$ be a normed field and σ an automorphism of K.*
a) Show: if $\sigma^*|\cdot| \sim |\cdot|$, then σ is continuous for the norm topology on K.
b) Suppose σ is continuous for the norm topology on K. Show: $\sigma^*|\cdot| \sim |\cdot|$.
c) Suppose σ is continuous for the norm topology on K. Show that σ is an automorphism of $(K, |\cdot|)$ if any one *of the following holds:*
(i) The norm $|\cdot|$ is Archimedean.
(ii) The norm $|\cdot|$ is non-Archimedean and the corresponding rank one valuation is discrete.
(iii) The automorphism σ has finite order.
d) (M. Suwama) Let $(K, |\cdot|)$ be the field of Puiseux series over a field k (see Exercise 1.18). Construct an automorphism σ of K that is continuous for the norm topology on K but $\sigma^*|\cdot| = |\cdot|^2$.

EXERCISE 1.51. *Let $(k, |\cdot|)$ be a complete normed field, and let σ be an automorphism of k. Put $|\cdot|' = \sigma^*|\cdot|$. Show: k is complete with respect to $|\cdot|'$.*

EXERCISE 1.52. *A field K is* ***rigid*** *if it has no automorphism other than the identity.*
a) Let $\sigma \in \operatorname{Aut}\mathbb{R}$. Show that σ is continuous for the topology induced by $|\cdot|_\infty$.
(Suggestion: for $x, y \in \mathbb{R}$ we have $x < y \iff y - x \in \mathbb{R}^{\times 2} \iff \sigma(y - x) \in$

$\mathbb{R}^{\times 2} \iff \sigma(x) < \sigma(y)$. *Thus* $|x| < 1 \iff |\sigma(x)| < 1$.
b) Show: the only continuous automorphism of $\mathbb{R}$ *is the identity, and deduce* $\mathbb{R}$ *is rigid.*
c) Show: the only continuous automorphism of $\mathbb{Q}_p$ *is the identity.*
d) Thus, to show that $\mathbb{Q}_p$ *is rigid, it suffices to show that every automorphism of* $\mathbb{Q}_p$ *is continuous. Later we will deduce this from a result of Schmidt: Theorem 2.47. Can you show this using only the material we've developed so far?*

EXERCISE 1.53. *Let* $k/\mathbb{Q}$ *be a number field of degree* n. *Let* l *be its Galois closure, and let* $G \coloneqq \mathrm{Aut}(l/\mathbb{Q})$. *There is a monic irreducible polynomial* $p \in \mathbb{Q}[t]$ *such that* $k \cong \mathbb{Q}[t]/(f)$, *and then* l *is the splitting field of* k. *There is a natural faithful action of* G *on the roots of* p *in* l, *which gives* G *as a subgroup of* S_n.
a) Suppose that $n \geq 3$ *and* $G = S_n$. *Show that* k *is rigid.*
b) Can you give other sufficient criteria on G *as a subgroup of* S_n *that make* k *rigid?*

EXERCISE 1.54. *Let* k *be a field complete with respect to a discrete, nontrivial valuation. Let* R *be its valuation ring.*
a) Show that k *is homeomorphic to the infinite disjoint union* $\coprod_{i=1}^{\infty} R$.
b) Let k_1, k_2 *be two fields complete with respect to discrete, nontrivial valuations, with valuation rings* R_1, R_2. *Suppose that* R_1 *and* R_2 *are compact. Show that* k_1 *and* k_2 *are homeomorphic, locally compact topological spaces.*

We now give an algebraic construction of the completion in the special case of a discretely valued, non-Archimedean norm on k. Namely, the norm is equivalent to a $\mathbb{Z}$-valued valuation v, with valuation ring

$$R = \{x \in k \mid v(x) \geq 0\}$$

and maximal ideal

$$\mathfrak{m} = \{x \in k \mid v(x) > 0\} = \{x \in k \mid v(x) \geq 1\}.$$

LEMMA 1.35. *With notation above, suppose that* k *is moreover complete. Then the ring* R *is* $\mathfrak{m}$*-adically complete. Explicitly, this means that the natural map*

$$R \to \lim_n R/\mathfrak{m}^n$$

is an isomorphism of rings.

PROOF. This is straightforward once we unpack the definitions.
Injectivity: this amounts to the claim that $\bigcap_{n \in \mathbb{Z}^+} \mathfrak{m}^n = 0$. In fact this holds for any nontrivial ideal in a Noetherian domain (Krull Intersection Theorem), but it is obvious here, because $\mathfrak{m}^n = (\pi^n) = \{x \in R \mid v(x) \geq n$, and the only element of R which has valuation at least n for all positive integers n is 0.
Surjectivity: Take any element $\mathbf{x}$ of the inverse limit, and lift each coordinate arbitrarily to an element $x_n \in R$. It is easy to see that $\{x_n\}$ is a Cauchy sequence, hence convergent in R – since k is assumed to be complete and R is closed in k, R is complete). Let x be the limit of the sequence x_n. Then $x \mapsto \mathbf{x}$. □

EXERCISE 1.55. *Let* v *be a discrete valuation on a field* k. *Let* $\hat{R} = \lim_n R/\mathfrak{m}^n$.
a) Show that $\hat{R}$ *is again a discrete valuation ring – say with valuation* $\hat{v}$ *– whose maximal ideal* $\hat{m}$ *is generated by any uniformizer* π *of* R.
b) Let $\mathbb{K}$ *be the fraction field of* $\hat{R}$. *Show that* $\mathbb{K}$ *is canonically isomorphic to* $\hat{k}$, *the*

completion of k in the above topological sense.
c) Let $n \in \mathbb{Z}^+$. Explain why the natural topology on the quotient $R/\mathfrak{m}^n$ is the discrete topology.
d) Show that the following topologies on $\hat{R}$ all coincide: (i) the topology induced from the valuation $\hat{v}$; (ii) the topology $\hat{R}$ gets as a subset of $\prod_n R/\mathfrak{m}^n$ (the product of discrete topological spaces); (iii) the topology it inherits as a subset of $\hat{k}$ under the isomorphism of part b).

2.8. Non-Archimedean Functional Analysis: page 1.

K-Banach spaces: Let $(K, |\cdot|)$ be a complete (and not discrete) normed field. In this context we can define the notion of a normed linear space in a way which directly generalizes the more familiar cases $K = \mathbb{R}$, $K = \mathbb{C}$. Namely:

A normed K-linear space is is a K-vector space V and a map $||\cdot|| : V \to \mathbb{R}^{\geq 0}$ such that:

(NLS1) $\forall x \in V$, $x = 0 \iff ||x|| = 0$.
(NLS2) $\forall \alpha \in K,\ x \in V$, $||\alpha x|| = |\alpha|||x||$.
(NLS3A) If $(K, |\cdot|)$ is Archimedean, then $\forall x, y \in V$, $||x + y|| \leq ||x|| + ||y||$.
(NLS3NA) If $(K, |\cdot|)$ is non-Archimedean, then $\forall x, y \in V$, $||x+y|| \leq \max ||x||, ||y||$.
Weakening (NLS1) to $\implies$, we get the notion of a **seminormed space**.

A normed linear space is a normed commutative group under addition. In particular it has a metric. A **K-Banach space** is a complete normed K-linear space.

The study of K-Banach spaces (and more general topological vector spaces) for a non-Archimedean field K is called **non-Archimedean functional analysis**. This exists as a mathematical field which has real applications, e.g., to modern number theory (via spaces of p-adic modular forms). The theory is similar but not identical to that of functional analysis over $\mathbb{R}$ or $\mathbb{C}$. (Explain that the weak Hahn-Banach theorem only holds for spherically complete fields...)

Two norms $||\cdot||_1,\ ||\cdot||_2$ on a K-vector space V are **equivalent** if there exists $\alpha \in \mathbb{R}^{>0}$ such that for all $v \in V$,

$$\frac{1}{\alpha}||v||_1 \leq ||v||_2 \leq \alpha||v||_1.$$

LEMMA 1.36. *Let $||\cdot||_1$ and $||\cdot||_2$ be two norms on the K-linear space V. The following are equivalent:*
(i) The norms $||\cdot||_1$ and $||\cdot||_2$ are equivalent.
(ii) The identity map $1_V : (V, ||\cdot||_1) \to (V, ||\cdot||_2)$ is uniformly continous with uniformly continuous inverse.
(iii) The topology induced by $||\cdot||_1$ is the same as the topology induced by $||\cdot||_2$.

PROOF. a) (i) $\implies$ (ii): If $||x||_2 \leq C||x||_1$ for all x, then 1_V is uniformly continuous with $\delta = \frac{\epsilon}{C}$. Similarly the other way around.
(ii) $\implies$ (iii): In particular 1_V is a homeomorphism, so the topoloies are the same.
(iii) $\implies$ (i): We show the contrapositive. Suppose the norms are *not* equivalent; then, after interchanging them if necessary, we have that $\frac{||x||_2}{||x||_1}$ is unbounded above

as x ranges over nonzero elements of V. Choose $\alpha \in K$ such that $|\alpha| > 1$. Then for all $n \in \mathbb{Z}^+$, there is $x_n \in V$ such that

$$||x_n||_1 \leq \frac{1}{|\alpha|2^n}||x_n||_2.$$

Multiplying x_n by a suitable power of α we may assume that $||x_n||_2 \in (1, \alpha]$. Since for all nonzero $x \in V$ and nonzero $\alpha \in K$ we have $\frac{||\alpha x||_2}{||\alpha x||_1} = \frac{||x||_2}{||x||_1}$, we get

$$||x_n||_1 \leq \frac{1}{|\alpha|2^n}||x_n||_2 \leq 2^{-n}.$$

Thus x_n converges to zero respect to $||\cdot||_1$ but not with respect to $||\cdot||_2$, so the norms determine different topologies. □

EXAMPLE 1.37. *Let $n \in \mathbb{Z}^+$. We define a map $|\cdot|_\infty : K^n \to \mathbb{R}$ by*

$$|(x_1, \ldots, x_n)|_\infty = \max_i |x_i|.$$

It is easy to check that this gives a norm on K^n. Indeed this is a special case of the maximum norm on any finite product of metric spaces; it gives a metric and the induced topology is the product topology.

THEOREM 1.38. *Let $(K, |\cdot|)$ be a* complete *normed field, and let $(V, ||\cdot||)$ be a finite dimensional normed K-vector space.*
a) Any two norms on V are equivalent.
b) It follows that any norm on V is complete and the induced topology coincides with the topology obtained by pulling back the product topology on K^n via any isomorphism $V \xrightarrow{\sim} K^n$.

PROOF. a) [**Cd1**] We go by induction on $n = \dim_K V$. The case $n = 0$ is absolutely trivial. When $n = 1$ the norm $||\cdot||$ is uniquely determined by its value on any nonzero element $e_1 \in V$ because of the scaling relation $||ae_1|| = |a|||e_1||$, and thus any two norms on V are nonzero scalar multiples of each other. Since multiplication by a nonzero element of K is a homeomorphism of K, this shows that any two norms on K are equivalent.

Now suppose that $n = \dim_K V \geq 2$ and that the result holds for all normed K-vector spaces of dimension $n - 1$. Fix a K-basis $e_1, \ldots, e_n$ for V, and for $(a_1, \ldots, a_n) \in K^n$ we put

$$||a_1e_1 + \ldots + a_ne_n||_\infty \coloneqq \max_i |a_i|.$$

By Example 1.37, $||\cdot||_\infty$ is a norm on V. It suffices to show there are $0 < A \leq B$ such that

$$\forall v \in V,\ A||v||_\infty \leq ||v|| \leq B||v||_\infty, \tag{2}$$

for this shows that the arbitrary norm $||\cdot||$ is equivalent to $||\cdot||_\infty$. One direction is easy: put $B \coloneqq \sum_{i=1}^n ||e_i||$. Then for all $v = a_1e_1 + \ldots + a_ne_n \in V$, we have

$$||v|| = ||a_1e_1 + \ldots + a_ne_n|| \leq \sum_{i=1}^n ||a_ie_i|| = \sum_{i=1}^n |a_i|||e_i|| \leq B \max |a_i| = B||v||_\infty.$$

To show the other direction, we argue much less directly: seeking a contradiction, we suppose that there is no $A > 0$ so that (2) holds. This means: for all $k \in \mathbb{Z}^+$ there is $v_k \in V$ such that $||v_k|| < \frac{1}{k}||v_k||_\infty$.

For $v \in V$ and $1 \leq i \leq n$, write $v = \sum_{i=1}^n a_i(v)e_i$. By definition of $||\cdot||_\infty$ and the

Pigeonhole Principle, there is some $1 \leq i \leq n$ such that $\{k \in \mathbb{Z}^+ \mid ||v_k|| = |a_i(v_k)|\}$ is infinite. We may assume without loss of generality that $i = n$. Scaling a vector v_k by an element of $K^\times$ does not change the inequality $||v_k|| < \frac{1}{k}||v_k||_\infty$, so after rescaling and passing to a subsequence $\{v_{k_j}\}_{j=1}^\infty$ we may assume that for all $j \in \mathbb{Z}^+$ we have:

(1) $||v_{k_j}||_\infty = 1$,
(2) $a_n(v_{k_j}) = 1$,
(3) $||v_{k_j}|| < \frac{1}{k_j}||v_{k_j}||_\infty = \frac{1}{k_j}$.
Let $W = \langle e_1, \ldots, e_{n-1}\rangle_K$, and put

$$\forall j \in \mathbb{Z}^+, w_j \coloneqq v_{k_j} - e_n.$$

Then $w_j \in W$ and $||w_j + e_n|| = ||v_{k_j}|| < \frac{1}{k_j} \to 0$. Thus for all $j, j' \in \mathbb{Z}^+$ we have

$$||w_j - w_{j'}|| = ||(w_j + e_n) - (w_j + e_n)|| \leq ||w_j + e_n|| + ||w_{j'} + e_n|| \to 0$$

as $\min(j, j') \to \infty$. Thus $\{w_j\}$ is a Cauchy sequence in $(W, ||\cdot||_W)$. Since $\dim_W = n - 1$, by induction there are $C, C' > 0$ such that

$$\forall w \in W,\ ||w||_\infty \leq C||w||,\ ||w|| \leq C'||w||_\infty.$$

Thus $\{w_j\}$ is Cauchy in $(W, (||\cdot||_\infty)|_W)$. This latter space is complete – a finite product of complete metric spaces with the maximum metric – so there is $w \in W$ such that $||w_j - w||_\infty \to 0$. Again, the equivalence gives that $||w_j - w|| \to 0$. But then as $j \to \infty$ we have

$$||w + e_n|| = ||(w - w_j) + (w_j + e_n)|| \leq ||w - w_j|| + ||w_j + e_n|| \to 0,$$

so $e_n = -w \in W$, a contradiction.
b) Since $(K^n, |\cdot|_\infty)$ is complete – a finite product of complete metric spaces endowed with the maximum metric is always complete – so is $(V, |\cdot|)$. Since the product topology on K^n is the one induced by the $||\cdot||_\infty$-norm and (as used above) pulling back $||\cdot||_\infty$ via a K-vector space isomorphism gives a norm on V, the last assertion follows from part a): all norms on V induce the same topology. □

EXERCISE 1.56. *In particular Theorem 1.38 applies to the complete Archimedean normed fields $(\mathbb{R}, ||\cdot||_\infty)$ and $(\mathbb{C}, ||\cdot||_\infty)$. This case is indeed found in most basic treatments of functional analysis.*
a) Consult such a text and read the proof of Theorem 1.38 given there. It is (or should be!) easier than the one given above.
b) Show that the above proof adapts to the case in which $(K, |\cdot|)$ is locally compact. (This is in fact the case of most interest to us later on.)

THEOREM 1.39. *Let $(K, |\cdot|)$ be a complete normed field and $(V, ||\cdot||)$ a normed K-linear space. Let W be a finite-dimensional K-subspace of V. Then W is closed.*

PROOF. Choose a K-basis $w_1, \ldots, w_n$ of W. By Theorem 1.38 and Lemma 1.36, the metric induced by the norm $||\cdot||_W$ is Lipschitz equivalent to the metric induced by $||a_1w_1 + \ldots + a_nw_n|| \coloneqq \max_i |a_i|$. The latter metric is complete since K is complete, and hence so is the former metric. A complete subspace of any metric space is closed. □

We shall give alternate proof of Theorems 1.38 and 1.39 that is taken from Neukirch [**N**, p. 133]. Let $(V, ||\cdot||)$ be a finite-dimensional normed space over the complete

field $(K, |\cdot|)$. As in the above proof, choosing a basis $e_1, \ldots, e_n$ of V allows us to define a norm $||a_1e_1 + \ldots + a_ne_n||_\infty := \max_i |a_i|$. We must show that as v ranges over nonzero elements of V, the ratio $\frac{||v||}{||v||_\infty}$ is bounded above and below. As we saw, being bounded above is almost immediate. For the other direction, we again work by induction on $\dim V = n$. In particular we may assume that all $n-1$-dimensional subspaces of V are complete with the restricted norm, hence closed. Since translation by $v \in V$ is a homeomorphism, it follows that all translates $W + v$ of $n-1$-dimensional subspaces (a.k.a. all affine hyperplanes in V) are closed. In particular, for $1 \leq i \leq n$, let

$$W_i := \langle e_j \mid j \neq i \rangle_K,$$

i.e., the K-span of all standard basis vectors *except* e_i. Then $X := \bigcup_{i=1}^n W_i + e_i$ is closed and does not contain 0, so there is some $\rho > 0$ such that the open ball of radius ρ centered at 0 is disjoint from X, or in other words

$$\forall 1 \leq i \leq n,\ \forall w_i \in W_i,\ ||w_i + e_i|| \geq \rho.$$

Now let $v = a_1e_1| \ldots + a_ne_n$ be a nonzero vector of V, and let I be such that $\max |a_i| = |a_I| > 0$. Then

$$||\frac{1}{a_i}v|| = ||\frac{a_1}{a_i}v_1 + \ldots + e_I + \ldots + \frac{a_n}{a_I}e_n|| \geq \rho,$$

so

$$||v|| \geq \rho|a_n| = \rho||v||_\infty.$$

One one thinks of "Archimedean functional analysis," Theorems 1.38 and 1.39 are probably not the first two which come to mind, perhaps because they are not very interesting! On the other hand, for our purposes these results are crucially useful. Indeed, they are precisely what is needed to prove the uniqueness in Theorem 1.43, a topic to which we soon turn.

2.9. Big Ostrowski Revisited.

The goal of this section is to prove the Big Ostrowski Theorem. Our proof follows an approach taken by David Krumm who was in turn following [**N**], but with some modifications. We will prove the following result.

THEOREM 1.40. *Let $(K, |\cdot|)$ be a complete Archimedean field with Artin contant 2 (i.e., $|2| = 2$). Then $(K, |\cdot|)$ is isomorphic either to $\mathbb{R}$ with its standard absolute value or to $\mathbb{C}$ with its standard absolute value.*

Let us first establish that Theorem 1.40 is *equivalent* to the Big Ostrowski theorem. First assume Theorem 1.10, and let $(K, |\cdot|_1)$ be an Archimedean normed field with Artin constant 2. Then we have an embedding $\iota : K \hookrightarrow \mathbb{C}$ such that for all $x \in K$, $|x|_1 = |\iota(x)|$. There is an induced map on completions

$$\hat{\iota} : (\hat{K}, |\cdot|_1) \to (\hat{\mathbb{C}}, |\cdot|) = (\mathbb{C}, |\cdot|).$$

Thus $\iota(\hat{K})$ is an isometrically embedded complete subfield of $\mathbb{C}$. Since $\iota(\hat{K})$ contains $\mathbb{Q}$, it contains the topological closure of $\mathbb{Q}$ in $\mathbb{C}$, namely $\mathbb{R}$: $\mathbb{R} \subset \iota(\hat{K}) \subset \mathbb{C}$. Since $[\mathbb{C} : \mathbb{R}] = 2$, we have little choice: either

$$(\hat{K}, |\cdot_1|) \cong (\iota(\hat{K}), |\cdot|) = (\mathbb{R}, |\cdot|)$$

or

$$(\hat{K}, |\cdot_1|) \cong (\iota(\hat{K})), |\cdot|) = (\mathbb{C}, |\cdot|.$$

Conversely, assume Theorem 1.40, and let $(K, |\cdot|)$ be an Archimedean normed field with Artin constant 2. Then $(K, |\cdot|)$ is a normed subfield of its completion $\hat{K}$, which is isomorphic to either $(\mathbb{R}, |\cdot|)$ or to $(\mathbb{C}, |\cdot|)$. Either way, $(K, |\cdot|)$ can be isometrically embedded in $(\mathbb{C}, |\cdot|)$.

Now we turn to the proof of Theorem 1.40. First, since $(K, |\cdot|)$ is a complete Archimedean normed field, it has characteristic zero (Corollary 1.9) and thus contains $\mathbb{Q}$. By Ostrowski's Lemma (Lemma 1.10) and the computation of the Artin constant (Theorem 1.11), the restriction of $|\cdot|$ to $\mathbb{Q}$ must be the standard absolute value $|\cdot|_\infty$. So $(\mathbb{Q}, |\cdot|_\infty) \hookrightarrow (K, |\cdot|)$ is an isometric embedding of normed fields. Taking completions, we get an isometric embedding $(\mathbb{R}, |\cdot|_\infty) \hookrightarrow (K, |\cdot|)$. The crux of the matter is the following claim.

CLAIM The field extension $K/\mathbb{R}$ is algebraic.

SUFFICIENCY OF THE CLAIM If $K/\mathbb{R}$ is algebraic, then either $K = \mathbb{R}$ – and we're done – or $[K : \mathbb{R}] = 2$ and K is isomorphic as an $\mathbb{R}$-algebra to $\mathbb{C}$. In this case there is still something to show,, namely that $(K, |\cdot|)$ is isomorphic to $(\mathbb{C}, |\cdot|_\infty)$ *as a normed field*. Happily, the tools needed to show this were developed in the previous section. Indeed, $(K, |\cdot|)$ is a finite-dimensional normed space over the complete field $\mathbb{R}$, so the topology induced by the norm is the product topology on $\mathbb{R}^2$. We may use the $\mathbb{R}$-isomorphism of K with $\mathbb{C}$ to transport the norm $|\cdot|$ to $\mathbb{C}$. On $\mathbb{C}$ we also have the standard Archimedean norm $|\cdot|_\infty$. By the above considerations, these two norms induce the same topology on $\mathbb{C}$ so are equivalent. Moreover they both have Artin constant 2, so they are equal, whence an isomorphism of normed fields $(K, |\cdot|) \xrightarrow{\sim} (\mathbb{C}, |\cdot|_\infty)$.

PROOF OF THE CLAIM We will show that every element of K is the root of a quadratic polynomial with $\mathbb{R}$-coefficients.

Let $\alpha \in K \setminus \mathbb{R}$. For $z \in \mathbb{C}$, put

$$P_z(t) = t^2 - (z + \overline{z})t + z\overline{z}.$$

Thus $P_z(t)$ is a quadratic polynomial with $\mathbb{R}$-coefficients whose roots in $\mathbb{C}$ are z and $\overline{z}$ (a double root, if $z \in \mathbb{R}$). Moreover, define a map $f : \mathbb{C} \to \mathbb{R}^{\geq 0}$ by

$$f(z) = |P_z(\alpha)|.$$

To say that α is quadratic over $\mathbb{R}$ is to say that there is some $z \in \mathbb{C}$ such that $f(z) = 0$. We will prove this by a somewhat sneaky argument mixing algebra and topology. First, it is easy to see to see that f is continuous and that $f(z)$ tends to ∞ with $|z|_\infty$. Indeed, for $|z|_\infty$ sufficiently large, the constant term of $P_z(\alpha)$ dominates. Thus f attains a minimum value $m \in \mathbb{R}^{\geq 0}$.

Seeking a contradiction, we assume $m > 0$. Since f is continuous, the level set $Z = f^{-1}(m)$ is closed; since f tends to infinity Z is also bounded, hence compact. So there is $z_1 \in \mathbb{C}$ such that $f(z_1) = m$ and $|z_1|_\infty$ is maximal among all $z \in Z$. If we can produce $w_1 \in \mathbb{C}$ such that $|w_1|_\infty > |z_1|_\infty$, we will have attained our contradiction.

To do so, choose $\epsilon \in \mathbb{R}$ with $0 < \epsilon < m$,, and let $w_1 \in \mathbb{C}$ be a root of the "perturbed polynomial" $P_{z_1}(t) + \epsilon$. Since $P_{z_1}(t)$ is a quadratic polynomial with at most one real root, its discriminant is nonpositive; further, the discriminant of $P_{z_1}(t)$ is strictly smaller than the discriminant of $P_{z_1}(t)$, hence negative: that is, $w_1 \in \mathbb{C} \setminus \mathbb{R}$. Hence

$$P_{z_1}(t) + \epsilon = (t - z_1)(t - \overline{z_1}) + \epsilon = (t - w_1)(t - \overline{w_1}) = t^2 - (w_1 + \overline{w_1})t + w_1\overline{w_1}.$$

Comparing constant coefficients gives

$$|z_1|_\infty = \sqrt{|w_1|_\infty^2 - \epsilon} < |w_1|_{infty}.$$

By definition of z_1, we must have $f(w_1) > m$. But we claim that also $f(w_1) \leq m$. We establish this as follows: let n be an odd positive integer, and define

$$g(t) = P_{z_1}(t)^n + \epsilon^n.$$

Factor $g(t)$ over $\mathbb{C}$ as

$$g(t) = \prod_{i=1}^{2n}(t - w_i).$$

Note that since n is odd, $P_{z_1}(t) + \epsilon$ divides $g(t)$, so indeed w_1 is one of the roots of g. Also $g(t) \in \mathbb{R}[t]$, so

$$g(t) = \prod_{i=1}^{2n}(t - \overline{w_i}),$$

and thus

$$g(t)^2 = \prod_{i=1}^{2n}(t - w_i)(t - \overline{w_i}) = \prod_{i=1}^{2n}(t^2 - (w_i + \overline{w_i})t + w_i\overline{w_i}).$$

It follows that

$$|g(\alpha)|^2 = \prod_{i=1}^{2n}|\alpha^2 - (w_i + \overline{w_i})\alpha + w_i\overline{w_i}| = \prod_{i=1}^{2n} f(w_i) \geq f(w_1)m^{2n-1}.$$

On the other hand,

$$|g(\alpha)| \leq |P_{z_1}(\alpha)|^n + \epsilon^n = f(z_1)^n + \epsilon^n = m^n + \epsilon^n,$$

and thus

$$f(w_1) \leq \frac{|g(\alpha)|^2}{m^{2n-1}} \leq \frac{(m^n + \epsilon^n)^2}{m^{2n-1}} = m\left(1 + \left(\frac{\epsilon}{m}\right)^n\right)^2.$$

Since $0 < \epsilon < m$, sending n to infinity gives $f(w_1) \leq m$, contradiction! This completes the proof of Theorem 1.40.

3. Extending norms

3.1. Introduction and Reorientation.

In this chapter we will study more explicitly the topology on a field induced by a norm. Especially interesting from this perspective are the (nontrivially) normed fields which are **locally compact** with respect to the norm topology.

But we have been studying normed fields for a little while now. Where are we going? What problems are we trying to solve?

Problem 1: Local/Global Compatibility. Arguably the most interesting results in Chapter 1 were the complete classification of all norms on a **global field** K, i.e., a finite extension of either $\mathbb{Q}$ (a number field) or $\mathbb{F}_q(t)$ for some prime power q (a function field).

We interrupt for two remarks:

Remark 1: Often when dealing with function fields, we will say "Let $K/\mathbb{F}_q(t)$ be a finite *separable* field extension". It is not true that every finite degree field extension of $\mathbb{F}_q(t)$ is separable: e.g. $\mathbb{F}_q(t^{\frac{1}{q}})/\mathbb{F}_q(t)$ is an inseparable field extension. However, the following is true: if $\iota : \mathbb{F}_q(t) \hookrightarrow K$ is a finite degree field homomorphism – don't forget that this wordier description is the true state of affairs which is being elided when we speak of "a field extension K/F" – then there is always another finite degree field homomorphism $\iota' : \mathbb{F}_q(t) \hookrightarrow K$ which makes $K/\iota'(\mathbb{F}_q(t))$ into a **separable** field extension: e.g. [**Ei**, Cor. 16.18].

Remark 2: In the above passage we could of course have replaced $\mathbb{F}_q(t)$ by $\mathbb{F}_p(t)$. But the idea here is that for an arbitrary prime power q, the rational function field $\mathbb{F}_q(t)$ is still highly analogous to $\mathbb{Q}$ rather than to a more general number field. For instance, if K is any number field, then at least one prime ramifies in the extension of Dedekind domains $\mathbb{Z}_K/\mathbb{Z}$. However, the extension $\mathbb{F}_q[t]/\mathbb{F}_p[t]$ is everywhere unramified. Moreover, $\mathbb{F}_q[t]$ is always a PID.[12]

For a global field K, we saw that there is always a Dedekind ring R with K as its fraction field with "sufficiently large spectrum" in the sense that all but finitely many valuations on K are just the $\mathfrak{p}$-adic valuations associated to the nonzero prime ideals of R. This suggests – correctly!– that much of the arithmetic of K and R can be expressed in terms of the valuations on K.

A **homomorphism of normed fields** $\iota : (K, |\cdot|) \to (L, |\cdot|)$ is a field homomorphism ι such that for all $x \in K$, $|x| = |\iota(x)|$. We say that the norm on L **extends** the norm on K. When the normed is non-Archimedean, this has an entirely equivalent expression in the language of valuations: a **homomorphism of valued fields** $\iota : (K, v) \to (L, w)$ is a field homomorphism $\iota : K \hookrightarrow L$ such that for all $x \in K$, $v(x) = w(\iota(x))$. We say that w **extends** v or that $w|_K = v$. (Later we will abbreviate this further to $w \mid v$.)

Problem 2: The Extension Problem. Let $(K, |\cdot|)$ be a normed field, and let L/K be a field extension. In how many ways does v extend to a norm on L?

THEOREM 1.41. *Let $(K, |\cdot|)$ be a normed field and L/K an extension field. If* either *of the following holds, then there is a norm on L extending $|\cdot|$:*
(i) L/K is algebraic.
(ii) $(K, |\cdot|)$ is non-Archimedean.

EXAMPLE 1.42. *Let $K = \mathbb{Q}$, $|\cdot| = |\cdot|_2$ and $L = \mathbb{R}$. Then there exists a norm on $\mathbb{R}$ which extends the 2-adic norm on $\mathbb{Q}$. This may seem like a bizarre and artifical*

[12]Somewhat embarrassingly, the question of whether there exist infinitely many number fields of class number one remains open!

example, but it isn't: this is the technical heart of the proof of a beautiful theorem of Paul Monsky [**Mo70**]*: it is not possible to dissect a square into an odd number of triangles such that all triangles have the same area. In fact, after* 40 *years of further work on this and similar problems, to the best of my knowledge no proof of Monsky's theorem is known that* does not *use this valuation-theoretic fact.*

EXERCISE 1.57. *Let $(K, |\cdot|)$ be an Archimedean norm.*
a) Suppose that L/K is algebraic. Show that $|\cdot|$ extends to a norm on L.
b) Give an example where L/K is transcendental and the norm on K does extend to a norm on L.
c) Give an example where L/K is transcendental and the norm on K does not extend to a norm on L.
Hint for all three parts: use the Big Ostrowski Theorem.

In view of Exercise 1.57, we could restrict our attention to non-Archimedean norms and thus to valuations. Nevertheless it is interesting and useful to see that the coming results hold equally well in the Archimedean and non-Archimedean cases.

Theorem 1.41 addresses the existence of an extended norm but not the number of extensions. We have already seen examples to show that if L/K is transcendental, the number of extensions of a norm on K to L may well be infinite. The same can happen for algebraic extensions of infinite degree: e.g., as we will see later, for any prime p, there are uncountably many extensions of the p-adic norm to $\overline{\mathbb{Q}}$.

EXERCISE 1.58. *Let K be a field and $\{K_i\}_{i \in I}$ be a family of subfields of K such that: (i) for all $i, j \in I$ there exists $k \in I$ such that $K_i \cup K_j \subset K_k$ and (ii) $\bigcup_i K_i = K$. (Thus the family of subfields is a directed set under set inclusion, whose direct limit is simply K.) Suppose that for each i we have a norm $|\cdot|_i$ on K_i, compatibly in the following sense: whenever $K_i \subset K_j$, $|\cdot|_j$ extends $|\cdot|_i$. Show that there is aunique norm $|\cdot|$ on K extending each norm $|\cdot|$ on K_i.*

EXERCISE 1.59. *Let $(k, |\cdot|)$ be a non-Archimedean normed field. Let $R = k[t]$ and $K = k(t)$. For $P(t) = a_n t^n + \ldots + a_1 t + a_0 \in R$, define the* ***Gauss norm*** *$|P| = \max_i |a_i|$. Show that this is indeed a norm on $k[t]$ and thus induces a norm on the fraction field $K = k(t)$ extending the given norm on k. Otherwise put, this shows that every valuation on a field k extends to a valuation on $k(t)$.*

EXERCISE 1.60. *Let (K, v) be a valued field, and let L/K be a purely transcendental extension, i.e., the fraction field of a polynomial ring over K (in any number of indeterminates, possibly infinite or uncountable). Use the previous Exercise to show that v extends to a valuation on L. (Suggestion: this is a case where a transfinite induction argument is very clean.)*

Exercise 1.60 and basic field theory reduces Theorem 1.41 to the case of an algebraic extension L/K. As we will see, this can be further reduced to the case of finite extensions. Moreover, when (K, v) is a valued field and L/K is a finite extension, we wish not only to show that an extension w of v to L exists but to classify (in particular, to count!) all such extensions. We saw in §1 that this recovers one of the core problems of algebraic number theory. Somewhat more generally, if v is discrete, then the valuation ring R is a DVR – in particular a Dedekind domain – and then its integral closure S in L is again a Dedekind domain, and we are asking how the

unique nonzero prime ideal $\mathfrak{p}$ of R splits in S: i.e., $\mathfrak{p}S = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}$. With suitable separability hypotheses, we get the fundamental relation $\sum_{i=1}^r e_i f_i = [L : K]$.

THEOREM 1.43. *Let $(K, |\cdot|)$ be a complete normed field and let L/K be algebraic.*
*a) There exists a **unique** norm $|\cdot|_L$ on L such that $(K, |\cdot|) \to (L, |\cdot|_L)$ is a homomorphism of normed fields.*
b) If L/K is finite, then $(L, |\cdot|_L)$ is again complete.

COROLLARY 1.44. *If $(K, |\cdot|)$ is a normed field and L/K is an algebraic extension, then there is at least one norm on L extending the given norm on K.*

PROOF. We may as well assume that $L = \overline{K}$. The key step is to **choose** a field embedding $\Phi : \overline{K} \hookrightarrow \widehat{K}$. This is always possible by basic field theory: any homomorphism from a field K into an algebraically closed field F can be extended to any algebraic extension L/K. Since this really is the point, we recall the proof. Consider the set of all embeddings $\iota_i : L_i \hookrightarrow F$, where L_i is a subextension of L/K. This set is partially ordered by inclusion. Moreover the union of any chain of elements in this poset is another element in the poset, so by Zorn's Lemma we are entitled to a maximal embedding $\iota_i : L_i \hookrightarrow F$. If $L_i = L$, we're done. If not, there exists an element $\alpha \in L \setminus L_i$, but then we could extend ι_i to $L_i[\alpha]$ by sending α to any root of its $\iota_i(L_i)$-minimal polynomial in F. By Theorem 1.43, there is a unique norm on $\widehat{K}$ extending the given norm on K. Therefore we may define a norm on L by $x \mapsto |\Phi(x)|$. □

EXERCISE 1.61. *Use Corollary 1.44 and some previous exercises to prove Theorem 1.41.*

THEOREM 1.45. *Let $(K, |\cdot|)$ be a normed field and L/K a finite extension. Then there is a bijective correspondence between norms on L extending the given norm on K and prime ideals in the $\hat{K}$-algebra $L \otimes_K \hat{K}$.*

There is a beautiful succinctness to the expression of the answer in terms of tensor products, but let us be sure that we understand what it means in more down-to-earth terms. Suppose that there exists a primitive element $\alpha \in L$ i.e., such that $L = K(\alpha)$. Recall that this is always the case when L/K is separable or $[L : K]$ is prime. In fact, the existence of primitive elements is often of mostly psychological usefulness: in the general case we can of course write $L = K(\alpha_1, \ldots, \alpha_n)$ and decompose L/K into a finite tower of extensions, each of which has a primitive element.

Now let $P(t) \in K[t]$ be the minimal polynomial of α over K, so $P(t)$ is irreducible and $L \cong K[t]/(P(t))$. In this case, for any field extension F/K, we have isomorphisms

$$L \otimes_K F \cong K[t]/(P(t)) \otimes_K F \cong F[t]/(P(t)).$$

Thus, $L \otimes_K F$ is an F-algebra of dimension $d = \deg P = [L : K]$. It need not be a field, but its structure is easy to analyze using the Chinese Remainder Theorem in the Dedekind ring $F[t]$. Namely, we factor $P(t)$ into irreducibles: say $P(t) = P_1^{e_1} \cdots P_r^{e_r}$. Then CRT gives an isomorphism

$$L \otimes_K F \cong F[t]/(P(t)) \cong \bigoplus_{i=1}^r F[t]/(P_i^{e_i}).$$

Let us put $A_i = F[t]/(P_i^{e_i})$. This is a local Artinian F-algebra with unique prime ideal $P_i/P_i^{e_i}$. Thus the number of prime ideals in $L \otimes_K F$ is r, the number of distinct irreducible factors of F. Moreover, suppose that L/K is separable. Then $P(t)$ splits into distinct linear factors in the algebraic closure of K, which implies that when factored over the extension field F (algebraic or otherwise), it will have no multiple factors. In particular, if L/K is separable (which it most often will be for us, in fact, but there seems to be no harm in briefly entertaining the general case), then all the e_i's are equal to 1 and $A_i = F[t]/(P_i)$ is a finite, separable field extension of F.

Example: We apply this in the case $(K, |\cdot|)$ is the rational numbers equipped with the standard Archimedean norm. Then the number of extensions of $|\ |$ to $L \cong K[t]/(P(t))$ is equal to the number of (necessarily distinct) irreducible factors of $P(t)$ in $\mathbb{R} = \hat{\mathbb{Q}}$. How does a polynomial factor over the real numbers? Every irreducible factor has degree either 1 – corresponding to a real root – or 2 – corresponding to a conjugate pair of complex roots. Thus $L \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^{r_1} \oplus \mathbb{C}^{r_2}$ and the number of extensions is $r_1 + r_2$, as advertised – but not proved! – in the Remark following Theorem 1.16.

It remains to prove Theorems 1.22, 1.43 and 1.45. Before proving Theorem 1, we give several short sections of "review" on topics which are probably somewhat familiar from previous courses but are important enough to revisit from a slightly more sophisticated perspective. In §2.7 we give the proof of Theorem 1.22.

3.2. Proof of Theorem 1.43 Part I: Uniqueness.

THEOREM 1.46. *Let $(K, |\cdot|)$ be a complete normed field, let L/K be an extension of finite degree d, and let $|\cdot|_L$ be a norm on L extending $|\cdot|$. Then for all $x \in L$,*

$$|x|_L = |N_{L/K}(x)|^{\frac{1}{d}}. \tag{3}$$

PROOF. Let $G = \mathrm{Aut}(L/K)$.
Step 1: We may assume L/K is normal. This reduction is left as an exercise.
Step 2: We suppose moreover that L/K is separable, hence Galois. For $\sigma \in G$, the map $\sigma : L \to L$ is a K-linear automorphism of L, which is a finite-dimensional vector space over the complete field K, so by Theorem 1.38 it is continuous, and thus is an automorphism *of the normed field* $(L, |\cdot|_L)$: for all $x \in L$, $|\sigma(x)|_L = |x|_L$. This is the key observation, for now

$$|N_{L/K}(x)| = |\prod_{\sigma \in G} \sigma(x)| = \prod_{\sigma \in G} |x| = |x|^d.$$

Step 3: Now suppose (only) that L/K is normal. Let d_s be the **separable degree** of L/K, i.e., the number of K-embeddings of L into an algebraic closure of K, and let $d_i = \frac{d}{d_s}$ be the **inseparable degree**. Then for all $x \in L$, we have

$$N_{L/K}(x) = \left(\prod_{\sigma \in G} \sigma(x) \right)^{d_i}.$$

The proof now proceeds as in Step 2 above. □

EXERCISE 1.62. *Work out the details of Step 1 of the proof of Theorem 3.*

COROLLARY 1.47. *Let $(K, |\cdot|)$ be complete, and let L/K be an algebraic extension.*
a) There is at most one norm one L extending $|\cdot|$ on K.
b) Suppose that for every finite subextension M of L/K the mapping $x \in M \mapsto |N_{M/K}(x)|^{\frac{1}{[M:K]}}$ of (3) is indeed a norm on M. Then the mapping

$$x \in L \mapsto |N_{K[x]/K}(x)|^{\frac{1}{[K[x]:K]}} \tag{4}$$

is a norm on L.

EXERCISE 1.63. *Prove Corollary 1.47. (Hint: use Exercise 2.2.)*

3.3. Theorems of Mazur, Gelfand and Tornheim.

In this section we give a second proof of Big Ostrowski – or rather, the equivalent Theorem 1.40. Let $(K, |\cdot|)$ be a field which is complete with respect to a norm with Artin constant 2. We want to show that $(K, |\cdot|)$ is isomorphic to $(\mathbb{R}, |\cdot|_\infty)$ or $(\mathbb{C}, |\cdot|_\infty)$. As in the previous section, Little Ostrowski gives that $(K, |\cdot|)$ has a normed subfield isomorphic to $(\mathbb{R}, ||\cdot|)$. The new idea we wish to pursue here is that this implies that $(K, |\cdot|)$ is a **real Banach algebra**: that is, an $\mathbb{R}$-vector spcae A complete with respect to a norm $||\cdot||$ with $|1| = 1$ and which is (at least) **sub-multiplicative**: for all $x, y \in A$, $||xy|| \leq ||x||||y||$.

We will prove the following generalization of Theorem 1.40.

THEOREM 1.48. *(Gelfand-Tornheim* [**To52**]*) Let $(K, ||\cdot||)$ be a real Banach algebra which is also a field. Then $(K, ||\cdot||)$ is isomorphic to $(\mathbb{R}, ||\cdot||_\infty)$ or $(\mathbb{C}, ||\cdot||_\infty)$.*

There is an evident corresponding notion of a *complex* Banach algebra, and in fact the theory of complex Banach algebras is much better developed than the theory of real Banach algebras, so our first step is to reduce to the complex case. This is done as follows: if K contains a square root of -1, then it contains a subfield isomorphic to $\mathbb{C}$ (even as a normed field, by the uniqueness of the norm on a finite extension of a complete field): great. If K does not contain a square root of -1, we would like to replace K by $K(\sqrt{-1})$.

It is natural to try to prove the following result.

THEOREM 1.49. *Let K be a field of characteristic different from 2 which is complete with respect to a norm $|\cdot|$. Let L/K be a quadratic extension. Then*

$$x \in L \mapsto |N_{L/K}(x)|^{\frac{1}{2}}$$

is a norm on L extending $|\cdot|$.

Observe that Theorem 1.49 is a very special case of Theorem 3. In particular, the Archimedean case follows from Big Ostrowski and the non-Archimedean case will be proved (rather sooner than) later by other methods. In fact there is a direct proof of Theorem 1.49, but I find it somewhat lengthy and unpleasant. The reader who wants to see it may consult [**BAII**, §9.5].

However, in order to prove Theorem 1.48 we can make do with less: it is enough to endow $K(\sqrt{-1})$ with an $\mathbb{R}$-algebra norm which is *sub*multiplicative: for all $x, y \in K(\sqrt{-1})$, $|xy| \leq |x||y|$. But this is easy: for $x, y \in K$, put

$$|x + \sqrt{-1}y| = |x| + |y|.$$

Certainly this endows $K(\sqrt{-1})$ with the structure of a real Banach space. Moreover, for $z = x + \sqrt{-1}y$, $z' = x' + \sqrt{-1}y'$ in $K(\sqrt{-1})$,

$$|zz'| = |xx' - y''| + |xy' + x'y| \leq |xx'| + |yy'| + |xy'| + |x'y|$$

$$\leq |x||x'| + |y||y'| + |x||y'| + |x'||y| = (|x| + |y|)(|x'| + |y'|) = |z||z'|.$$

Putting $L = K(\sqrt{-1})$, we have endowed L with the structure of a complex Banach algebra. To complete the proof of Theorem 1.48, it is enough to show that the only field which is a complex Banach algebra is $\mathbb{C}$ itself. Again we will prove rather more than this. First a few preliminaries.

LEMMA 1.50. *(Neumann) Let $(A, ||\cdot||)$ be a complex Banach algebra, and let $x \in A$ be such that $||x|| < 1$. Then $1 - x \in A^\times$. Explicitly,*

$$\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n.$$

PROOF. Since $||x|| < 1$, $\sum_{n=0}^{\infty} ||x^n|| \leq \sum_{n=0}^{\infty} ||x||^n < \infty$. That is, $\sum_{n=0}^{\infty} x^n$ is absolutely convergent and thus, by completeness, convergent. Denote the sum by b. It is then easily seen that $(1-a)b = b(1-a) = 1$. □

Let $(A, ||\cdot||)$ be a complex Banach algebra, and let $x \in A$. We define the **spectrum** $\sigma(x)$ to be the set of all complex numbers z such that $z - x \in A \setminus A^\times$. (Note that when $A = M_N(\mathbb{C})$, the spectrum of x is its set of eigenvalues. One may think of the spectrum as being a generalization of this linear algebra concept.) The comlementary set $\mathbb{C} \setminus \sigma(x)$ is the **resolvent set** of x.

Lemma 1.50 shows $A^\times$ contains a neighborhood of 1 and is thus open. It follows that the resolvent set of x is open and thus the spectrum $\sigma(x)$ is closed. Moreover, if $z \in \mathbb{C}$ is such that $|z| > ||x||$, then $||z^{-1}x|| < 1$ and $1 - z^{-1}x \in A^\times$. Since $z \in A^\times$, $z - x \in A^\times$. Thus the spectrum is bounded and the resolvent set is nonempty.

LEMMA 1.51. *Let $(A, ||\cdot||)$ be a complex Banach algebra, and let $x \in A$. Let U be the resolvent set of x. Let $\varphi : A \to \mathbb{C}$ be a bounded (equivalently, continuous) linear functional. Then the map*

$$f : U \to C,\ z \mapsto \varphi\left(\frac{1}{z-x}\right)$$

is holomorphic.

PROOF. Let $z \in U$. Then

$$\lim_{h\to 0} \frac{1}{h}\left(\varphi\left(\frac{1}{z+h-x}\right) - \varphi\left(\frac{1}{z-x}\right)\right) = \lim_{h\to 0} \frac{1}{h}\varphi\left(\frac{1}{z+h-x} - \frac{1}{z-x}\right)$$

$$= \lim_{h\to 0} \frac{1}{h}\varphi\left(\frac{h}{(z+h-x)(z-x)}\right) = \lim_{h\to 0} \varphi\left(\frac{1}{(z+h-x)(z-x)}\right)$$

$$= \varphi\left(\lim_{h\to 0} \frac{1}{(z+h-x)(z-x)}\right).$$

Lemma 1.50 implies that $x \mapsto \frac{1}{z-x}$ is continuous on U, so this last limit exists. □

THEOREM 1.52. *(Gelfand-Mazur) Let $(A, ||\cdot||)$ be a complex Banach division algebra. Then $A = \mathbb{C}$.*

PROOF. CLAIM For all $x \in A$, the spectrum $\sigma(x)$ is nonempty.
SUFFICIENCY OF CLAIM Let A be a complex Banach division algebra, and suppose there exists $x \in A \setminus \mathbb{C}$. For all $z \in \mathbb{C}$, $z - x \notin \mathbb{C}$, hence $z - x \neq 0$, hence $z - x \in A^\times$: thus $\sigma(x) = \varnothing$.
PROOF OF CLAIM Seeking a contradiction, suppose $\sigma(x) = \varnothing$, so the resolvent set U is all of $\mathbb{C}$. Let $\varphi : A \to \mathbb{C}$ be a bounded linear functional such that $\varphi(\frac{-1}{x}) \neq 0$. (To see that such a thing exists, choose a $\mathbb{C}$-basis for A in which $\frac{-1}{x}$ is the first element, and define φ by $\varphi(\frac{-1}{x}) = 1$ and for every other basis element e_i, $\varphi(e_i) = 0$. Alternatively, this is a special case of the Hahn-Banach Theorem.) Let $f : \mathbb{C} \to \mathbb{C}$ be the function $z \mapsto \varphi\left(\frac{1}{z-x}\right)$. By Lemma 1.51, f is holomorphic on $\mathbb{C}$. Let $C = ||\varphi||$, i.e., the least number such that for all $a \in A$, $|\varphi(a)| \leq C||a||$. For $|z| > 2||x||$,

$$|f(z)| = |\varphi\left(\frac{1}{z-x}\right)| = \frac{1}{|z|}|\varphi\left(\frac{1}{1-z^{-1}x}\right)|$$

$$= \frac{1}{|z|}|\varphi\left(\sum_{n=0}^{\infty}(z^{-1}x)^n\right)| \leq \frac{1}{|z|}\sum_{n=0}^{\infty}|\varphi((z^{-1}x)^n)|$$

$$\leq \frac{C}{|z|}\sum_{n=0}^{\infty}||z^{-1}x||^n < \frac{C}{|z|}\sum_{n=0}^{\infty}\frac{1}{2^n} = \frac{2C}{|z|}.$$

Thus f is a bounded entire function, hence constant by Liouville's Theorem. Moreover $\lim_{|z|\to\infty} f(z) = 0$, so $f \equiv 0$. But $f(0) = \varphi(\frac{-1}{x}) = 1$: contradiction. □

Remark: More generally, the only real Banach division algebras are $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$ (the quaternions). For a proof of this, see e.g. [**Bou**, § VI.6.4].

3.4. Proof of Theorem 1.22: Existence Modulo Hensel-Kürschák.

Let $(K, |\cdot|)$ be a complete normed field and L/K an extension of degree $d < \infty$. We have seen that if $|\cdot|$ extends to a norm on L, the extended norm *must be*

$$x \in L \mapsto |x|_L = |N_{L/K}(x)|^{\frac{1}{d}}.$$

In the Archimedean case, Big Ostrowski reduces us to checking that this is indeed the correct recipe for the norm $|\cdot|_\infty$ on $\mathbb{C}$ as a quadratic extension of $|\cdot|_\infty$ on $\mathbb{R}$, which is almost immediate. Thus we are left to deal with the non-Archimedean case. It is no problem to see that $|\cdot|_L$ satisfies properties (V1) and (V2) for a norm. The crux of the matter is to check that it satisfies the non-Archimedean triangle inequality.

From our study of absolute values in §1, we know that we do not change whether a mapping is a non-Archimedean norm by raising it to any positive power, so we may as well look at the mapping $x \mapsto |N_{L/K}(x)|$ instead. Moreover, we also know that the non-Archimedean triangle inequality is equivalent to: for all $x \in L$, $|x|_L \leq 1 \implies |x+1|_L \leq 1$ and thus also to:

$$\forall x \in L, |N_{L/K}(x)| \leq 1 \implies |N_{L/K}(x+1)| \leq 1. \tag{5}$$

LEMMA 1.53. *(Hensel-Kürschák) Let $(K, |\cdot|)$ be a complete, non-Archimedean normed field. Let*

$$P(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0 \in K[t]$$

be an irreducible polynomial with $|a_0| \leq 1$. *Then* $|a_i| \leq 1$ *for all* $0 \leq i \leq n-1$.

We will prove Lemma 1.53 later on (Theorem 1.78). For now we use it to show (5). Here goes: suppose $[L : K] = d$ and $[K[x] : K] = d$. Then (see e.g. [**C:FT**, Prop. 6.2]) we have

$$N_{L/K}(x) = N_{K[x]/K}(x)^{\frac{d}{m}}.$$

Let $P(t)$ be the minimal polynomial of x over K, so P is monic irreducible of degree m and has constant coefficient $a_0 = (-1)^m N_{K[\alpha]/K}(x)$. By assumption

$$1 \geq |N_{L/K}(x)| = |N_{K[x]/K}(x)^{n/m}| = |a_0|^{n/m},$$

so $|a_0| \leq 1$. Thus Lemma 1.53 applies to give that $|a_i| \leq 1$ for all $0 \leq i \leq n-1$.

Observe that $K[x+1] = K[x]$ and the minimal polynomial for $x+1$ is $P(t-1)$. Plugging in $t = 0$ gives

$$(-1)^m N_{K[x]/K}(x+1) = P(-1) = (-1)^m + a_{m-1}(-1)^{m-1} + \ldots + (-1)a_1 + a_0.$$

Thus

$$|N_{L/K}(x+1)| = |N_{K[x]/K}(x+1)|^{d/m} = |(-1)^m + a_{m-1}(-1)^{m-1} + \ldots + (-1)a_1 + a_0|^{d/m} \leq 1.$$

3.5. Proof of Theorem 1.43 Part III: Krull Valuations.

In this optional section we give a proof of the existence statement in Theorem 1.43 using the concept of a Krull valuation and an important (but not terribly difficult) result from commutative algebra.

Recall that a valuation ring is a domain R such that for every nonzero x in the fraction field K, at least one of x, x^{-1} lies in R. A valuation ring is necessarily local, say with maximal ideal $\mathfrak{m}$. Moreover:

LEMMA 1.54. *A valuation ring is integrally closed.*

PROOF. Let R be a valuation ring with maximal ideal $\mathfrak{m}$ and fraction field K. Let $a_0, \ldots, a_{n-1} \in R$ and let $x \in K$ such that $x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$. By definition of a valuation ring, if $x \notin R$, then $x^{-1} \in \mathfrak{m}$, so $1 = -(a_{n-1}x^{-1} + \ldots + a_0 x^{-n})) \in \mathfrak{m}$, contradiction. □

Remark: A domain R is called a **Bézout domain** if every finitely generated ideal is principal. In a valuation domain, every finitely generated ideal is generated by any element of minimal valuation, so valuation domains are Bézout. For a non-Noetherian domain, Bézout domains are very nice: e.g. they are integrally closed. See e.g. [**C:CA**, §16.4] for more details.

Valuation rings have naturally arisen in our study of normed fields: if $(K, |\cdot|)$ is a normed field, then $R = \{x \in K \mid |\cdot|x| \leq 1\}$ is a valuation ring. Equivalently, if $v = -\log|\cdot| : K^\times \to \mathbb{R}$ is an associated valuation, then $R = \{x \in K \mid v(x) \geq 0\}$. However, not every valuation ring comes from a valuation $v : K^\times \to \mathbb{R}$. We can however get a bijective correspondence by generalizing our concept of valuation to a map $v : K^\times \to \Gamma$, where Γ is an ordered commutative group.

This may sound abstruse, but it is easily motivated, as follows: let R be a domain with fraction field K. Consider the relation $\leq$ on $K^\times$ of R-divisibility: that is $x \leq y \iff \frac{y}{x} \in R$. The relation of R-divisibility is immediately seen to be

reflexive and transitive. Even when $R = \mathbb{Z}$, it is not anti-symmetric: an integer and its additive inverse divide each other. However, any relation $\leq$ on a set X which is reflexive and transitive induces a partial ordering $\leq$ on the quotient $X/\sim$, where we decree $x \sim y$ iff $x \leq y$ and $y \leq x$. In the case of $R = \mathbb{Z}$, this amounts essentially to restricting to positive integers. For R-divisibility in general, it means that we are identifying associate elements, so the quotient is precisely the group $\Gamma = K^\times/R^\times$ of principal fractional R-ideals of K.

PROPOSITION 1.55. *For an integral domain R with fraction field K and $\Gamma = K^\times/R^\times$, the following are equivalent:*
(i) The induced partial ordering $\leq$ on Γ is a total ordering.
(ii) R is a valuation ring.

PROOF. (i) $\implies$ (ii): For any $x \in K^\times$, take $y = 1$: then either $\frac{y}{x} = x^{-1}$ or $\frac{x}{y} = x$ lies in R, so that R is a valuation ring.
(ii) $\implies$ (i): If R is a valuation ring, let $x, y \in K^\times$. Then either $\frac{x}{y} \in R$ – i.e., $y \leq x$ – or $\frac{y}{x} \in R$ – i.e., $x \leq y$. □

This motivates the following definition.

Let $(\Gamma, \leq)$ be an ordered commutative group. A Γ-valued valuation on a field K is a map $v : K^\times \to \Gamma$ such that for all $x, y \in K$, $v(xy) = v(x) + v(y)$ and $v(x+y) \geq \min v(x), v(y)$. As usual, we may formally extend v to 0 by $v(0) = +\infty$. A **Krull valuation** on K is a Γ-valued valuation for some ordered commutative group Γ.

PROPOSITION 1.56. *Let $(\Gamma, \leq)$ be an ordered commutative group and $v : K \to \Gamma$ a Krull valuation. Then $R_v = \{x \in K \mid v(x) \geq 0\}$ is a valuation ring.*

Thus to a valuation ring R we can associated the Krull valuation $v : K^\times \to K^\times/R^\times$ and conversely to a Krull valuation we can associate a valuation ring. These are essentially inverse constructions. To be more precise, let $(K, v : K \to \Gamma_1)$ and $(L, w : L \to \Gamma_2)$ be two fields endowed with Krull valuations.

LEMMA 1.57. *Let $(\Gamma_1, \leq)$ and $(\Gamma_2, \leq)$ be ordered commutative groups, and let $g : \Gamma_1 \to \Gamma_2$ be a homomorphism of commutative groups.*
a) The following conditions on γ are equivalent:
(i) $x_1 < x_2 \implies g(x_1) < g(x_2)$.
(ii) $x_1 \leq x_2 \iff g(x_1) \leq g(x_2)$.
b) If the equivalent conditions of part a) hold, then g is injective.
A homomorphism satisfying the equivalent conditions of part a) is said to be a ***homomorphism of ordered commutative groups****.*

PROOF. a) Suppose g satisfies (i). Certainly $x_1 = x_2 \implies g(x_1) = g(x_2)$, so we have $x_1 \leq x_2 \implies g(x_1) \leq g(x_2)$. Now suppose that $g(x_1) \leq g(x_2)$ and that we do not have $x_1 \leq x_2$. Since the ordering is total, we then have $x_1 > x_2$, and then our assumption gives $g(x_1) > g(x_2)$, contradiction. Now suppose g satisfies (ii), and let $x_1 < x_2$. If $g(x_1) = g(x_2)$, then $g(x_1) \leq g(x_2)$ and $g(x_2) \leq g(x_1)$, so (ii) implies that $x_1 = x_2$, contradiction. Similarly, we cannot have $g(x_1) \geq g(x_2)$, so we must have $g(x_1) < g(x_2)$.
b) Assume (i) and let $x \in \Gamma_1$ be such that $g(x) = 0$. If $0 < x$, then $0 = g(0) < g(x) = 0$, contradiction. Similarly, if $x < 0$, then $0 = g(x) < g(0) = 0$, contradiction. So $x = 0$ and thus g is injective. □

A homomorphism of Krull-valued fields is a pair (ι, g), where $\iota : K \hookrightarrow L$ is a homomorphism of fields and $g : \Gamma_1 \hookrightarrow \Gamma_2$ is an injective homomorphism of ordered commutative groups such that for all $x \in K$, $w(\iota(x)) = g(v(x))$. Then the correspondences described above take isomorphic valuation rings to isomorphic Krull-valued fields and isomorphic Krull-valued fields to isomorphic valuation rings.

The **value group** of a Krull valuation is the image $v(K^\times)$. A Krull valuation is said to be trivial if its value group is the trivial group (which has a unique ordering).

In this more general context, a nontrivial Krull valuation $v : K \to \Gamma$ is said to be **rank one** if there exists a homomorphism of ordered commutative groups $g : \Gamma \to \mathbb{R}$.[13]

EXERCISE 1.64. *Show that any ordered commutative group Γ can serve as the value group of a Krull-valued field.*
Suggestion: let k be any field, and let R be the group ring $k[\Gamma]$, i.e., the set of formal sums $x = \sum_{\gamma \in \Gamma} x_\gamma [\gamma]$ where $x_\gamma \in k$ for all γ and for a fixed x, all but finitely many x_γ's are zero. Define $v : R \setminus \{0\} \to \Gamma$ by letting $v(x)$ be the least γ such that $x_\gamma \neq 0$. Show that R is an integral domain, that v extends uniquely to its fraction field K and defines a valuation on K with value group Γ.

EXERCISE 1.65. *Let Γ be a nontrivial ordered commutative group. Show that the following are equivalent:*
(i) There is a homomorphism of ordered commutative groups $g : \Gamma \to \mathbb{R}$ (Γ has rank one).
(ii) For all positive elements $x, y \in \Gamma$, there exists $n \in \mathbb{Z}^+$ such that $nx > y$ (Γ is Archimedean).

Combining the previous two exercises one gets many examples of Krull valuations not of rank one, e.g. with value group $\Gamma = \mathbb{Z} \times \mathbb{Z}$ ordered **lexicographically**.

LEMMA 1.58. *Let Γ be an ordered commutative group and $H \subset \Gamma$ be a finite index divisible subgroup. Then $H = \Gamma$.*

PROOF. Suppose not, i.e., $[\Gamma : H] = n < \infty$. Let $x \in \Gamma$. Then $nx = h \in H$. By definition of divisibility, there exists $y \in H$ such that $ny = h$. Therefore $0 = h - h = n(x - y)$, i.e., $x - y \in \Gamma[n]$. But an ordered commutative group must be torsionfree, so $x = y \in H$. □

LEMMA 1.59. *Let L be a field, $v : L^\times \to \Gamma$ a Krull valuation on L, and let K be a subfield of L with $[L : K] = n < \infty$. Then Γ is order isomorphic to a subgroup of $\Gamma_K = v(K^\times)$.*

PROOF. ([**BAII**, 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 $[L : K] = n \geq n_1 > n_2 > \ldots > n_k \geq 0$. 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

$$v(x)^{n_i - n_j} = v(\alpha_j \alpha_i^{-1}) \in \Gamma_K.$$

[13]There is a notion of rank of an ordered commutative group: see e.g. [**C:CA**, §17.2]. We will not need this here.

Thus, for $x \in L^\times$, $(n!)v(x) \in \Gamma_K$. Since Γ is torsionfree, the endomorphism $[n!] : \Gamma \to \Gamma$ (i.e., multiplication by $n!$) is injective, and thus $[n!] : \Gamma \hookrightarrow [n!]\Gamma \subset \Gamma_K$. □

COROLLARY 1.60. *Let (K, v) be a rank one valued field, L/K be a finite degree extension, and w a Krull valuation on L such that there exists a homomorphsim of Krull-valued fields $(\iota, g) : (K, v) \to (L, w)$. Then w has rank one.*

PROOF. This is immediate from Lemma 1.59 and the definition of a rank one valuation as one whose value group is order isomorphic to a subgroup of $(\mathbb{R}, +)$. □

Why would one want to use Krull valuations? One might equally well ask what is the use of general valuation rings, and the latter has a very satisfying answer:

THEOREM 1.61. *Let R be an integral domain which is not a field, and let L be a field such that $R \subset L$. Let S be the integral closure of R in L. Then S is equal to the intersection of all nontrivial valuation rings of L containing R.*

PROOF. See e.g. [**C:CA**, Thm. 17.17]. □

Now let $(K, |\cdot|)$ be a complete non-Archimedean normed field and L/K a finite degree field extension. We know that there is at most one norm on L which extends $|\cdot|$ on K. We will now give a proof of the **existence** of this extended norm. Namely, let v be any rank one valuation corresponding to $|\cdot|$, and let R be the valuation ring of K. Let S be the integral closure of R in K. It suffices to show that S is itself a valuation ring and the corresponding valuation has rank one.

Let $\mathcal{S} = \{R_w\}$ be the set of all nontrivial valuation rings of L which contain R. By Theorem 1.61, $S = \bigcap_{R_w \in \mathcal{S}} R_w$. For any valuation ring $R_w \in \mathcal{S}$, let $w : L \to \Gamma$ be the corresponding Krull valuation. By Corollary 1.60, w is a rank one valuation, hence corresponds to an non-Archimedean norm on L which (certainly after rescaling in its equivalence class) restricts to $|\cdot|$ on K. By the uniqueness of extended norms, it follows that $\#\mathcal{S} = 1$, so that $S = R_w$ is a rank one valuation ring.

3.6. Proof of Theorem 5.

We come now to the most technically complicated of the basic extension theorems, Theorem 1.45. The reader will surely have noticed that we have taken some time building up suitable tools and basic facts. Now our hard work comes to fruition: given what we already know, the proof of Theorem 1.45 is rather straightforward and elegant.

LEMMA 1.62. *Let $(L, |\cdot|)$ be a normed field, and let K be a subfield of K such that $[L : K]$ is finite. Let $\hat{K}$ and $\hat{L}$ be the corresponding completions. Then*

$$[\hat{L} : \hat{K}] \leq [L : K].$$

PROOF. Let $n = [L : K]$ and let $e_1, \ldots, e_n$ be a K-basis of L. Let W be the $\hat{K}$-subspace of $\hat{L}$ spanned by $e_1, \ldots, e_n$. Then W is a finite-dimensional normed $\hat{K}$-linear space, so it is complete and thus closed in $\hat{L}$. Moreover W contains the K-span of $e_1, \ldots, e_n$, which is L, so W id dense in $\hat{L}$. Thus $W = \hat{L}$, so $\dim_{\hat{K}} \hat{L} \leq n = [L : K]$. □

LEMMA 1.63. *Let $(K, |\cdot|)$ be a normed field, and let L/K be a finite degree field extension. Let $|\cdot|_L$ be a norm on L that extends $|\cdot|$ on K. Let C_K be the algebraic closure of $\hat{K}$, with its canonical norm $|\cdot|$. Then there is a K-algebra homomorphism $\sigma : L \hookrightarrow C_K$ such that $|\cdot|_L = \sigma^*|\cdot|$: i.e., for all $x \in L$ we have $|x|_L = |\sigma(x)|$.*

PROOF. Let $\hat{L}$ be the completion of L with respect to $|\cdot|_L$. Let C_L be the algebraic closure of $\hat{L}$. The norm on $\hat{L}$ extends to a unique norm on C_L that we continue to denote by $|\cdot||_L$. By Lemma 1.62 the extension $\hat{L}/\hat{K}$ is finite and thus C_L is also an algebraic closure of $\hat{K}$, so there is a $\hat{K}$-algebra isomorphism $\psi : C_L \to C_K$. Consider the two norms $|\cdot|_L$ and $\psi^*|\cdot|$ on C_L; both restrict to $|\cdot|$ on $\hat{K}$, so by uniqueness of norms in algebraic extensions of complete fields we must have $|\cdot|_L = \psi^*|\cdot|$. Let σ be the restriction of Ψ to L. Then $\sigma : L \to C_K$ is a K-algebra homomorphism and $|\cdot|_L = \sigma^*|\cdot|$. □

Let g be the number of norms on L extending $|\cdot|$ on K. The preceding lemma implies that

$$1 \leq g \leq n = [L : K]$$

and the problem is to compute g exactly in terms of L/K and $|\cdot|$.

For $1 \leq i \leq g$, let $|\cdot|_i$ be the ith norm on L extending $|\cdot|$ on K. Let $\hat{L}_i$ be the completion of $(L, |\cdot|_i)$.

I claim there is a canonical ring homomorphism

$$\Phi : L \otimes_K \hat{K} \to \prod_{i=1}^{g} \hat{L}_i.$$

Let's use the universal properties of the direct and tensor products to reduce to a situation where we can easily guess what the definition shuld be. First, by writing out Φ in coordinates we have $\Phi = (\Phi_i)_{i=1}^g$ for $\Phi : L \otimes_K \hat{K} \to \hat{L}_i$, and thus it suffices to define each Φ. Moreover, by the universal property ofthe sentor product, to define Φ_i we need a K-bilinear map $\varphi_i : L \times \hat{K} \to \hat{L}_i$. What is the "obvious" map here? OBserve that $\iota_i(L)$ and $\hat{K}$ are both subfields of $\hat{L}_i$, so given $x \in L$ and $y \in \hat{K}$, we may use $\iota_i 1$ to map L into $\hat{L}_i$ and then multiply them in $\hat{L}_i$. Explicitly,

$$\varphi_i(x, y) = \iota_i(x) \cdot y.$$

Thus we define Φ on "simple tensors" as

$$\Phi(x \otimes y) = (\iota_i(x)y)_{i=1}^g$$

and uniquely extend by linearity to a map on $L \otimes_K \hat{K}$.

Here is another perspective on the map $\Phi : L \otimes_K \hat{K} \to \prod_{i=1}^g \hat{L}_i$. Both its source and target are finite-dimensional $\hat{K}$-algebras, and Φ is a $\hat{K}$-linear map. Consider the diagonal map

$$\Delta : L \hookrightarrow \prod_{i=1}^{g} \hat{L}_i, \ x \mapsto (\iota_i(x)).$$

Note that Δ is K-linear and Φ is the map corresponding to Δ under the canonical **adjunction isomorphism**

$$\mathrm{Hom}_K(L, \prod_i \hat{L}_i) = \mathrm{Hom}_{\hat{K}}(L \otimes_K \hat{K}, \prod_i \hat{L}_i).$$

Moreover, like any two finite-dimensional $\hat{K}$-vector spaces, $L \otimes_K \hat{K}$ and $\prod_{i=1}^g \hat{L}_i$ come with canonical topologies, such that any $\hat{K}$-linear map between them (like Φ, for instance!) is continuous.

We are now ready to prove the following important result.

THEOREM 1.64. *Let $\Phi : L \otimes_K \hat{K} \to \prod_{i=1}^g \hat{L}_i$ be the above homomorphism.*
a) The map Φ is surjective.
b) The kernel of Φ is the Jacobson radical of the Artinian ring $L \otimes_K \hat{K}$, i.e., the intersection of all maximal ideals. More precisely, there are g maximal ideals in $L \otimes_K \hat{K}$; suitably labelled as $\mathfrak{m}_1, \ldots, \mathfrak{m}_g$, the map Φ can be identified with the Chinese Remainder Theorem homomorphism

$$L \otimes_K \hat{K} \to \prod_{i=1}^g (L \otimes_K \hat{K})/\mathfrak{m}_i.$$

c) If L/K is separable, Φ is an isomorphism.

PROOF. We put $A = L \otimes_K \hat{K}$ and $W = \Phi(A)$.
a) We wish to show that $W = \prod_{i=1}^g \hat{L}_i$. Since Φ is $\hat{K}$-linear, W is a $\hat{K}$-subspace of the finite-dimensinal $\hat{K}$-vector space $\prod_{i=1}^g \hat{L}_i$. By Theorem 2.15, W is closed. On the other hand, by Artin-Whaples the image of L under $\Delta : L \hookrightarrow \prod_{i=1}^g \hat{L}_i$ is dense. The relation "is dense in" on subspaces of a topological space is transitive, so $\Phi(L) = \Phi(L \otimes 1)$ is dense in $\prod_{i=1}^g \hat{L}_i$ and Φ is surjective.
b) Since A is a finite-dimensional $\hat{K}$-algebra, it is an Artinian ring and thus has finitely many maximal (= prime) ideals, say $\mathfrak{m}_1, \ldots, \mathfrak{m}_N$. Let J be the Jacobson (=nil) radical $\cap_{i=1}^N \mathfrak{m}_i$. We have a finite set of pairwise comaximal ideals in a commutative ring, so the Chinese Remainder Theorem gives an isomorphism

$$\Psi : A/J \xrightarrow{\sim} \prod_{j=1}^N A/\mathfrak{m}_j.$$

For each i, put $L(\mathfrak{m}_i) = A/\mathfrak{m}_i$, and notice that $L(\mathfrak{m}_i)$ is a finite field extension of $\hat{K}$. Since J is nilpotent and $\prod_{i=1}^g \hat{L}_i$ is reduced, Φ factors through Ψ:

$$A \to A/J \xrightarrow{\sim} \prod_{j=1}^N L(m_j) \xrightarrow{q} \prod_{i=1}^g \hat{L}_i.$$

By part a), what we have is one finite product of finite degree field extensions of $\hat{K}$ surjecting onto another. A little thought shows that we must have $N \geq g$ and that we can relabel the j's such that for all $1 \leq j \geq g$, $\mathfrak{m}_j = \mathrm{Ker}\, \Phi_j$ and thus

$$q : \prod_{j=1}^g \hat{L}_j \oplus \prod_{j>g} L(\mathfrak{m}_j) \to \prod_{j=1}^g \hat{L}_j$$

is projection onto the first factor. Now the result of part b) is equivalent to $g = N$, i.e., that the second summand $\prod_{j>g} L(\mathfrak{m}_j)$ does not in fact appear.

Each $L(\mathfrak{m}_j)$ is a finite extension of the complete field $\hat{K}$, so has a unique norm $|\cdot|_j$ extending the norm on $\hat{K}$, and which restricts to a norm on L. Thus if $N > g$ thre exists $j_1 \leq g$ and $j_2 > g$ such that $|\cdot|_{j_1} = |\cdot|_{j_2}$ as norms on L. Consider the projection of Ψ onto just these two factors:

$$\Psi_{j_1,j_2} : L \otimes_K \hat{K} \to \widehat{L, |\cdot|_{j_1}} \times \widehat{L, |\cdot|_{j_2}}.$$

We claim that Ψ_{j_1,j_2} is not surjective, which will give a contradiction. But this map is hardly mysterious: it is determined by the images of L and of $\hat{K}$. In particular, the restriction of Ψ_{j_1,j_2} to L is just the diagonal map. Since the two norms are equivalent on L, their topologies are the same, and thus the image of L is *closed* in $(L, |\cdot|_{j_1}) \times (L, |\cdot|_{j_2})$. Moreover, tensoring this diagonal map with $\hat{K}$ has the effect of completing these normed spaces. We have the same topology on both factors, so the closure of the diagonal is the diagonal of the closure, and thus the image of A unde Ψ_{j_1,j_2} has $\hat{K}$-dimension $\dim L(\mathfrak{m}_{j_1}) = \dim L(\mathfrak{m}_{j_2})$ and hence not equal to $\dim L(\mathfrak{m}_{j_1} \times L(\mathfrak{m}_{j_2}) = 2 \dim L(m_{j_1})$, contradiction.

c) If L/K is separable, then $A = L \otimes_K \hat{K}$ is a separable $\hat{K}$-algebra, i.e., a finite product of finite separable field extensions. To see this, write $L = K[t]/(P(t))$ with $P(t)$ an irreducible separable polynomial (this is possible by the Primitive Element Corollary). Separability of a polynomial is unaffected by extension of the ground field. Thus over $\hat{K}$, we have a factorization $P = p_1 \cdots P_g$ of P into *distinct* irreducible polynomials. Thus the ideals $\{(P_i)\}_{i=1}^g$ are pairwise comaximal, and CRT gives an isomorphism

$$A = \hat{K}[t]/(P) = \hat{K}[t]/(P_1 \cdots P_g) \cong \prod_{i=1}^g \hat{K}[t]/(P_i) \cong \prod_{i=1}^g \hat{L}_i. \qquad \square$$

4. The Degree in/equality

Let (K, v) be a valued field, with valuation ring R and maximal ideal $\mathfrak{m}$. As with any maximal ideal, the quotient ring $R/\mathfrak{m}$ is a field, called the **residue field** of K and denoted k. (Note that we have switched from k to K for our normed/valued field so as to allow the introduction of the residue field.) We have a canonical surjective map $R \to k$ called the **reduction map**.

EXAMPLE 1.65. *Suppose K is any field and v is the trivial (i.e., identically zero) valuation. Then $R = K$, $\mathfrak{m} = 0$, so $k = K$ and the reduction map is an isomorphism. Conversely, if the reduction map is injective, the valuation is trivial.*

EXAMPLE 1.66. *Let ord_p be the p-adic norm on $\mathbb{Q}$. Then the valuation ring is the local ring R of all rational numbers of the form $\frac{a}{b}$ with b not divisible by p. This is of course the localization of $\mathbb{Z}$ at the maximal ideal (p). It follows that $R/\mathfrak{m} \cong \mathbb{Z}/(p) \cong \mathbb{F}_p$.*

EXAMPLE 1.67. *Let k be a field and $R = k[[t]]$ and $K = k((t))$. Then the maximal ideal consists of all formal power series with 0 constant term, and it is easily seen that $R/\mathfrak{m} \cong k$ in such a way that the composite map $k \hookrightarrow R \to R/\mathfrak{m} \cong k$ is the identity. Thus in this case the residue field is also realized as a subfield of K.*

EXAMPLE 1.68. *Let k be a field, $R = k[t]$, $K = k(t)$. Let ord_t be the valuation corresponding to the prime element (t). Then again the residue field is isomorphic to $R/(t) \cong k$.*

More generally:

PROPOSITION 1.69. *Let R be a Dedekind domain with fraction field K. Let $\mathfrak{p}$ be a nonzero prime ideal of R, and let $v = \mathrm{ord}_{\mathfrak{p}}$ be the $\mathfrak{p}$-adic valuation. Then the residue field is naturally isomorphic to $R/\mathfrak{p}$.*

EXERCISE 1.66. *Prove Proposition 1.69.*

Now let $(L, w)/(K, v)$ be an extension of valued fields. Recall that this means that we have a field homomorphism $\iota : K \hookrightarrow L$ such that $w \circ \iota = v$. In such a situation, ι induces an embedding of valuation rings $R \hookrightarrow S$ and of maximal ideals $\mathfrak{m}_R \hookrightarrow \mathfrak{m}_S$. We may therefore pass to the quotient and get a homomorphism

$$\bar{\iota} : k = R/\mathfrak{m}_R \hookrightarrow S/\mathfrak{m}_S = l,$$

called the **residual extension**. The degree $[l : k]$ is called the **residual degree** and is also denoted $f(L/K)$.

Again let $(K, v) \hookrightarrow (L, w)$ be a homomorphism of valued fields. Then we have $v(K) \subset w(L)$. We define the **ramification index** $e(L/K)$ to be $[w(L) : v(K)]$. In terms of the associated norms, we have $e(L/K) = \frac{|L^\times|}{|K^\times|}$.

EXERCISE 1.67. *Suppose L/K is algebraic. Show $w(L)/v(K)$ is a torsion group.*

EXAMPLE 1.70. *Consider $L = \mathbb{Q}_p(p^{\frac{1}{n}})$ with the unique valuation w extending v_p on $\mathbb{Q}_p$. Of course $v_p(\mathbb{Q}_p) = \mathbb{Z}$ with uniformizing element p, so*

$$1 = w(p) = w((p^{\frac{1}{n}})^n) = nw(p^{\frac{1}{n}}),$$

so that $w(p^{\frac{1}{n}}) = \frac{1}{n}$. It follows that $e(L/\mathbb{Q}_p) \geq n$. In fact we have $e(L/\mathbb{Q}_p) = n$, a consequence of the following result.

THEOREM 1.71 (Degree Inequality I). *Let $(K, |\cdot|) \hookrightarrow (L, |\cdot|)$ be an extension of non-Archimedean normed fields, with $[L : K] = n$. Then*

$$e(L/K)f(L/K) \leq n.$$

PROOF. As usual, we let $(R, \mathfrak{m}_R)$ be the valuation ring of $(K, |\cdot|)$ and $(S, \mathfrak{m}_S)$ the valuation ring of $(L, |\cdot|)$. Let $u_1, \ldots, u_{f_1}$ be elements of S whose reductions modulo $\mathfrak{m}_S$ are linearly independent over $k = R/\mathfrak{m}_R$. (In particular, we have $u_i \in S^\times$ for all i.) Thus given elements $a_1, \ldots, a_{f_i} \in R$ such that $\sum_i a_i u_i \in \mathfrak{m}_S$, we have $a_i \in \mathfrak{m}_S$ for all i. Let $b_1, \ldots, b_{e_1}$ be elements of $L^\times$ whose images in $|L^\times|/|K^\times|$ are distinct. It suffices to show that the $e_1 f_1$ elements $u_i b_j$ of L are linearly independent over K. Scaling by elements of $K^\times$ does not disturb this conclusion, so we may assume WLOG that $b_j \in \mathfrak{m}_S$ for all j.
Step 1: Suppose that $a_i \in K$. Then $|\sum_i a_i u_i| \in |K|$.

Proof: Indeed, if $\sum_i a_i u_i \neq 0$, then some $a_i \neq 0$; by reordering we may assume that $0 = |a_1| \geq |a_i$ for all i. Then

$$|\sum_i a_i u_i| = |a_1||\sum_i \frac{a_i}{a_1} u_i|.$$

Moreover $|\sum_i \frac{a_i}{a_1} u_i| \leq 1$. If we had $|\sum_i \frac{a_i}{a_1} u_i| < 1$, then $\sum_i \frac{a_i}{a_1} u_i \in \mathfrak{m}_S$, and since $|\frac{a_i}{a_1}| \leq 1$, we have $\frac{a_i}{a_1} \in R$ for all i. The relation $\sum_i \frac{a_i}{a_1} u_i \in \mathfrak{m}_S$ contradicts the definition of the u_i. Hence $|\sum_i \frac{a_i}{a_1} u_i| = 1$, so $|\sum_i a_i u_1| = |a_1| \in |K|$.

Step 2: Now suppose that there exist $a_{ij} \in K$ such that $\sum_{i,j} a_{ij} u_i b_j = 0$. If there exists j such that $\sum_i a_{ij} u_i \neq 0$, then $\sum_{i,j} a_{ij} u_i b_j = 0$ implies the existence of distinct j, say $j = 1$ and $j = 2$, such that $|\sum_i a_{i1} u_i b_1| = |\sum_i a_{i2} u_i b_2| \neq 0$. Then $\sum_i a_{i1} u_i \neq 0$ and $\sum_i a_{i2} u_i \neq 0$, so $|\sum_i a_{i1} u_i|, |\sum_i a_{i2} u_i| \in |K^\times|$. Then $|b_1||K^\times| = |b_2||K^\times|$, contrary to the choice of the b_j's. Thus the relation $\sum a_{ij} u_i b_j = 0$ implies $\sum_i a_{ij} u_i = 0$ for all j. Scaling by a suitable nonzero element of F, we get relations of the form $\sum_i a'_{ij} u_i = 0$ with $a'_{ij} \in R$, and unless all a_{ij}'s are 0, we may assume that one of them does not lie in $\mathfrak{m}_S$, contradicting the definition of the u_i's. Therefore the $e_1 f_1$ elements $u_i b_j$ are linearly independent over K, qed. □

Must we have equality in Theorem 1.71? Of course not! Consider the familiar case in which R is a Dedekind domain, K is its fraction field, L/K is a finite separable field extension of degree n, S is the integral closure of R in L, and $v = \mathrm{ord}_{\mathfrak{p}}$ is the valuation associated to a nonzero prime ideal $\mathfrak{p}$ of R. Then if $\mathfrak{p}S = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_g}$, we have $\sum_{i=1}^g e_i f_i = n$. On the other hand, for any $1 \leq i \leq g$, if we take w_i to be the $\mathcal{P}_\rangle$-adic valuation (renormalized so as to extend $\mathrm{ord}_{\mathfrak{p}}$), then we have $e(L/K)f(L/K) = e_i f_i$. So we cannot have equality when there is more than one prime of S lying over $\mathfrak{p}$.

By now it should be clear what to do: pass to the completion. For one thing, the invariants $e(L/K)$ and $f(L/K)$ are "local" in the sense that they are unchanged upon passage to the completion:

PROPOSITION 1.72. *Let $(K, v) \hookrightarrow (L, w)$ be a finite degree extension of valued fields, with $[L : K] = n$. By functoriality of completion, we get a homomorphism $(\hat{K}, \hat{v}) \hookrightarrow (\hat{L}, \hat{w})$. Then:*
a) $[\hat{L} : \hat{K}] \leq n$.
b) $v(K) = \hat{v}(\hat{K})$ and $w(L) = \hat{w}(\hat{L})$ (completion does not change the value group).
c) The homomorphism of residue extensions $k \hookrightarrow \hat{k}$ induced by $K \hookrightarrow \hat{K}$ is an isomorphism.
d) We have $f(L/K) = f(\hat{L}/\hat{K})$ and $e(L/K) = e(\hat{L}/\hat{K})$.

EXERCISE 1.68. *Prove Proposition 1.72.*

THEOREM 1.73 (Degree In/Equality II). *Let (K, v) be a nontrivial valued field with valuation ring R, and L/K an extension of degree n. Let $w_1, \ldots, w_g$ be the valuations on L extending v on K. For $1 \leq i \leq g$, put $e_i(L/K) = e((L, w_i)/(K, v))$. Then:*
a) We have

$$\sum_{i=1}^g e(L_i/K) f(L_i/K) \leq [L : K]. \tag{6}$$

b) If v is discrete and the integral closure of R in L is finitely generated as an R-module, then we have equality in 6.
*c) In particular, if v is discrete and L/K is finite and **separable**, then equality holds in (6).*

PROOF. a) Let $\hat{L}_i$ be the completion of L with respect to w_i, and let $n_i = [\hat{L}_i : \hat{K}]$. By Theorem 1.71 and Propostion 1.72 we have, for all $1 \leq i \leq g$, that

$e_i f_i \leq n_i$. On the other hand, by Theorem 2.19 we have $\sum_i n_i = \dim_{\hat{K}} \prod_{i=1}^g \hat{L}_i \leq \dim_{\hat{K}} L \otimes_K \hat{K} = [L : K]$. Thus

$$\sum_{i=1}^g e(L_i/K) f(L_i/K) = \sum_{i=1}^g e(\hat{L}_i/\hat{K}) f(\hat{L}_i/\hat{K}) \leq \sum_{i=1}^g n_i \leq [L : K].$$

b) Suppose S is a finitely generated R-module. Since R and S are both domains, S is a torsionfree R-module. Then, since R is a DVR and hence a PID, it follows from the structure theory of finitely generated modules over a PID that $S \cong R^m$ for some $m \in \mathbb{N}$. Since $K^n \cong L = S \otimes_R K \cong K^m$, we must have $m = n = [L : K]$. Moreover S is a Dedekind domain [**C:CA**, §17]. Therefore we may take $\mathfrak{p}$, the unique nonzero prime ideal of R, and factor the pushforward into prime powers:

$$\mathfrak{p}S = \prod_{i=1}^g \mathcal{P}_i^{e_i}.$$

Applying the Chinese Remainder Theorem, we get $(R/\mathfrak{p})$-module isomorphisms

$$(R/\mathfrak{p})^n \cong R^n/\mathfrak{p}R^n \cong S/\mathfrak{p}S = S/(\prod_{i=1}^g \mathcal{P}_i^{e_i}) \cong \prod_{i=1}^g S/\mathcal{P}_i^{e_i}.$$

Since $\mathfrak{p}$ is a maximal ideal of R, $R/\mathfrak{p}$ is a vector space, and we may equate $R/\mathfrak{p}$-dimensions of both sides. Clearly $\dim(R/\mathfrak{p})^n = n$. On the other hand, since each $\mathcal{P}_i$ is a principal ideal (if it weren't, no problem: since localization commutes with passage to the quotient, we could make it so by passing the localization), multiplication by the kth power of a uniformizer of $\mathcal{P}_i$ gives an $S/\mathcal{P}_i$-isomorphism from $S/\mathcal{P}_i$ to $\mathcal{P}_i^k/\mathcal{P}_i^{k+1}$. Therefore

$$\dim_{R/\mathfrak{p}} S/\mathcal{P}_i^{e_i} = e_i \dim_{R/\mathfrak{p}} S/\mathcal{P}_i = e_i f_i \dim_{S/\mathcal{P}_i} S/\mathcal{P}_i = e_i f_i,$$

and we conclude $n = \sum_{i=1}^g e_i f_i$.

c) We recall (again!) that if R is an integrally closed Noetherian domain with fraction field K and L/K is a finite degree separable field extension, then the integral closure S of R in L is finitely generated as an R-module [**C:CA**, Thm. 18.1]. □

We will not need them, but here are two further sufficient conditions for equality in Theorem 1.73:

THEOREM 1.74. *Maintain the same setup as in Theorem 3.4. Suppose that* either *K is complete and discretely valued* or *the residue field of K has characteristic* 0. *Then equality holds in (6).*

PROOF. See [**En**]. □

If $(K, |\cdot|)$ is a non-Archimedean normed field, a finite degree extension L/K is called **defectless** if equality holds in (6). The field K itself is called **defectless** if every finite extension is defectless.

It turns out that a field is defectless iff its Henselization is defectless. If K is Henselian of residual characteristic $p > 0$, then it is a result of Ostrowski that for any finite degree extension L/K there is $\nu \geq 0$ such that

$$e(L/K) f(L/K) p^\nu = [L : K].$$

The quantity ν is called the **defect**. It turns out to be related to some key issues in positive characteristic algebraic geometry.f

5. Hensel's Lemmas

Throughout this section $(K, |\cdot|)$ is a non-Archimedean normed field with corresponding rank one valuation v, valuation ring R, maximal ideal $\mathfrak{m}$ and residue field k. We equip $K[t]$ with the Gauss norm:

$$|a_n t^n + \ldots + a_1 t + a_0| \coloneqq \max_i |a_i|.$$

A polynomial $f \in K[t]$ is **primitive** if $|f| = 1$: notice this means that each coefficient a_i lies in R and at least one coefficient does not lie in $\mathfrak{m}$.

5.1. Hensel Lifting.

THEOREM 1.75 (Hensel Lifting). *Suppose K is complete. Let $f \in R[t]$ be a primitive polynomial, and let $\overline{f} \in k[t]$ be its reduction modulo $\mathfrak{m}$. Suppose that $\overline{f} = \overline{g}\overline{h} \in k[t]$ with $\gcd(\overline{g}, \overline{h}) = 1$. Then there are $g, h \in R[t]$ such that $f = gh$, $\deg g = \deg \overline{g}$, $g \equiv \overline{g} \pmod{\mathfrak{m}}$, $h \equiv \overline{h} \pmod{\mathfrak{m}}$.*

PROOF. □

REMARK 1.76. *In Theorem 1.75, the leading coefficient of f is a unit iff $\deg \overline{f} = \deg f$ iff $\deg \overline{h} = \deg h$. In particular this holds if f is monic, and Theorem 1.75 is often stated in this special case.*

COROLLARY 1.77 (My First Hensel's Lemma).
Suppose K is complete, let $f \in R[t]$ and let $\overline{f} \in k[t]$ be its reduction modulo $\mathfrak{m}$. If $\overline{\alpha} \in k$ is a simple root of $\overline{f}$ (i.e., $\overline{f}(\alpha) = 0$ and $\overline{f}'(\alpha) \neq 0$), then there is $\alpha \in R$ such that $f(\alpha) = 0$ and $\alpha \equiv \overline{\alpha} \pmod{\mathfrak{m}}$.

PROOF. The polynomial f must be primitive, for otherwise $\overline{f}$ is the zero polynomial and there are no simple roots. Having a simple root $\overline{\alpha}$ is equivalent to a factorization

$$\overline{f} = (t - \overline{\alpha})\overline{h}$$

with $\gcd(t - \overline{\alpha}, \overline{h}) = 1$. Appying Theorem 1.75 there are $g, h \in R[t]$ such that $f = gh$, $g \equiv t - \overline{\alpha} \pmod{\mathfrak{m}}$, $h \equiv \overline{h} \pmod{\mathfrak{m}}$ and $\deg g = \deg(t - \overline{\alpha}) = 1$. Thus $g = at - b$ for $a, b \in R$ with $a \equiv 1 \pmod{\mathfrak{m}}$, so in particular $a \in R^\times$. Put $\alpha \coloneqq \frac{b}{a}$. Then $\alpha = \frac{b}{a} \equiv b \equiv \overline{\alpha} \pmod{\mathfrak{m}}$. □

5.2. Hensel-Kürschak.

THEOREM 1.78 (Hensel-Kürschák). *Suppose K is complete. Let $f = a_n t^n + \ldots + a_1 t + a_0 \in K[t]$ be irreducible such that $a_0 a_n \neq 0$. Then*

$$|f| = \max |a_0|, |a_n|.$$

PROOF. It is harmless to scale f by an element of $K^\times$, and after doing so we may assume $|f| = 1$, hence in particular that $f \in R[t]$. Let $0 \leq r \leq n$ be the least index such that $|a_r| = 1$. Thus

$$f \equiv t^r(a_r + a_{r+1}t + \ldots + a_n t^{n-r}) \pmod{\mathfrak{m}}.$$

If $|a_0|, |a_n|$ were both less than 1 then $0 < r < n$, and Hensel's Lemma applies to show that f is reducible, a contradiction. □

5.3. Hensel-Newton.

THEOREM 1.79 (Hensel-Newton). *Suppose K is complete. Let $f \in R[t]$ be a polynomial, and let $\alpha \in R$ be such that*

$$|f(\alpha)| < |f'(\alpha)|^2.$$

a) There is a unique $\beta \in R$ such that $f(\beta) = 0$ and $|\beta - \alpha| < |f'(\alpha)|$.
b) We have

$$|\beta - \alpha| = \left|\frac{f(\alpha)}{f'(\alpha)}\right| \text{ and } |f'(\beta)| = |f'(\alpha)|.$$

5.4. Multivariate Hensel-Newton.

THEOREM 1.80 (Multivariate Hensel-Newton).

THEOREM 1.81 (Hensel Smooth Lifting).

5.5. An Application: Selmer's Equation. For a place v of $\mathbb{Q}$, we denote the corresponding completion by $\mathbb{Q}_v$: thus $\mathbb{Q}_p$ is as usual and $\mathbb{Q}_\infty = \mathbb{R}$.

THEOREM 1.82. *Let $f(X,Y,Z) = 3X^3 + 4Y^3 - 5Z^3$. Then for every place v of $\mathbb{Q}$ there is a nonzero $\alpha \in \mathbb{Q}_v^3$ such that $f(\alpha) = 0$.*

We will need a result from arithmetic geometry. For now we will state it in a concrete form, then we will come back and deduce it from more general results.

PROPOSITION 1.83. *Let $f(X,Y,Z)$ be a homogeneous cubic polynomial defined over the finite field $\mathbb{F}_q$. If f is **smooth** – i.e., if there is no $\alpha \in \overline{\mathbb{F}_q}^3$ such that $\frac{\partial f}{\partial x}(\alpha) = \frac{\partial f}{\partial y}(\alpha) = \frac{\partial f}{\partial z}(\alpha) = 0$ – then there is a nonzero $\alpha \in \mathbb{F}_q^3$ such that $f(\alpha) = 0$.*

First we dispose of the infinite place of $\mathbb{Q}$: like any polynomial equation of odd degree, there are nonzero $\mathbb{R}$-points: plugging in arbitrary nonzero values for X and Y we get a cubic equation in Z that we can solve over $\mathbb{R}$.

Now suppose that $p \neq 2, 3, 5$ is a prime number. Then f is smooth over $\mathbb{F}_p$: if $\frac{\partial f}{\partial x} = \frac{\partial f}{\partial y} = \frac{\partial f}{\partial z} = 0$ then $9X^2 = 12Y^2 = -15Z^3 = 0$ in $\mathbb{F}_p$, so $(X,Y,Z) = 0$. By Proposition 1.83, there is $\overline{\alpha} \in \mathbb{F}_p^3 \setminus \{(0,0,0)\}$ such that $\overline{f}(\overline{\alpha}) \equiv 0 \pmod p$, and thus by Theorem 1.81 there is $\alpha \in \mathbb{Z}_p^3$ such that $f(\alpha) = 0$ and $\alpha \equiv \overline{\alpha} \pmod p$, so $\alpha \neq 0$.

Suppose $p = 5$. In this case the cubic is not smooth over $\mathbb{F}_5$: all partial derivatives of f vanish at $(0,0,1)$, so this point cannot be lifted using Hensel's Lemma. If we can find $\overline{\alpha} = (X_0, Y_0, Z_0)$ with $X_0 \neq 0 \pmod 5$, then we can apply My First Hensel's Lemma to $f(X, Y_0, Z_0)$, with $\alpha = X_0$, since $f'(\alpha) = 9X_0^2 \not\equiv 0 \pmod 5$. To find such a point: well, brute force will work. Here is one idea though: the map $x \mapsto x^3$ is a bijection on $\mathbb{F}_5$, so we can take $Z_0 = 0$, $Y_0 = 1$ and uniquely solve for X_0, getting $(X_0, Y_0, Z_0) = (3, 1, 0)$.

Suppose $p = 2$. In this case the cubic is not smooth over $\mathbb{F}_2$: all partial derivatives of f vanish at $(0,1,0)$, s othis point cannot be lifted using Hensel's Lemma. As above we look for an $\overline{\alpha} = (X_0, Y_0, Z_0)$ with $f(\overline{\alpha}) = 0$ in $\mathbb{F}_2$ and $X_0 \neq 0$, for then $\frac{\partial f}{\partial X}(\overline{\alpha}) \neq 0$. Again the map $x \mapsto x^3$ is a bijection on $\mathbb{F}_2$, so we can take $Y_0 = 0$, $Z_0 = 1$ and solve for X, getting $(X_0, Y_0, Z_0) = (1, 0, 1)$.

Finally we suppose $p = 3$. This case is different: at every point $(X_0, Y_0, Z_0) \in \mathbb{F}_3^3$, all partial derivatives of f vanish. In other words, for any $\overline{\alpha}$ we have $||(\nabla f)(\overline{\alpha})|| \leq \frac{1}{3}$. Thus in order to apply Hensel-Newton we need to go mod 3^3. It suffices to find $(X_0, Y_0, Z_0) \in \mathbb{Z}_3^3$ with $Z_0 \not\equiv 0 \pmod 3$ and $f(X_0, Y_0, Z_0) \equiv 0 \pmod{3^3}$, for then Newton-Hensel applies to $f(X_0, Y_0, Z)$ with $\alpha = Z_0$:

$$|f(X_0, Y_0, \alpha)| = |f(X_0, Y_0, Z_0)| \leq \frac{1}{27} < \frac{1}{9} = |-15Z_0^2|^2 = |f'(X_0, Y_0, \alpha)|^2.$$

For this: reduced residues modulo 27 that are cubes are $1, 8, 10, 17, 19, 26$. We may as well try taking $X_0 = 0$ and $Y_0 = 1$. Then we have $5Z^3 \equiv 4 \pmod{27}$ or $Z^3 \equiv 17 \pmod{27}$. So we may take $(X_0, Y_0, Z_0) = (0, 1, 5)$.

Let us now return to Proposition 1.83. I know several proofs, but all use some ideas from arithmetic geometry that are beyond the scope of these notes to properly develop. In particular, we use that a smooth homogeneous cubic polynomial over a field defines a nice (smooth, projective, geometrically integral) curve of genus one. Then one can use the following celebrated result.

THEOREM 1.84 (Weil). *Let $C_{/\mathbb{F}_q}$ be a nice curve of genus g defined over a finite field of order q. Let $C(\mathbb{F}_q)$ be the number of $\mathbb{F}_q$-rational points on C. Then we have*

$$|\#C(\mathbb{F}_q) - (q+1)| \leq 2g\sqrt{q}.$$

EXERCISE 1.69. *Maintain the notation of Theorem 1.84.*
a) Show that if $g = 0$ then $\#C(\mathbb{F}_q) = q+1$. If you know and care about such things, deduce that C is $\mathbb{F}_q$-rationally isomorphic to $\mathbb{P}^1$.
b) Show that if $g = 1$ then $\#C(\mathbb{F}_q) \geq (\sqrt{q} - 1)^2 \geq 1$. If you know and care about such things, deduce that C is an elliptic curve.
c) Suppose that g is fixed. Show that for all sufficiently large q, we have $\#C(\mathbb{F}_q) \geq 1$.

In fact one has the following result.

THEOREM 1.85. *Let K be a number field, and let $X_{/K}$ be a nice variety of dimension $d \geq 1$. For a non-Archimedean place v of K, let K_v be the corresponding completion. Then, for all but (possibly) finitely many places v, we have $X(K_v) \neq \varnothing$.*

PROOF. By the Bertini Theorem, admits a nice curve $C_{/K}$ as a K-rational subvariety. (It is intuitively obvious and easy to prove that a variety of dimension d contains varieties of all smaller dimensions. The problem is to nail down the nonsingularity condition, and the Bertini Theorem assures this.) Let $\mathcal{C}$ be any model over the ring of integers $\mathbb{Z}_K$: in other words, we give C by homogeneous equations with coefficients in $\mathbb{Z}_K$. The non-Archimedean places v correspond to maximal ideals $\mathfrak{p}_v$ of $\mathbb{Z}_K$, and the corresponding residue field is $\mathbb{Z}_K/\mathfrak{p}_v \cong \mathbb{F}_{q_v}$. It is a fact (openness of the smooth locus) that since $C_{/K}$ is smooth, any given model $\mathcal{C}$ over $\mathbb{Z}_K$ will be smooth over R_v – equivalently, the variety defined by the system of equations over the residue field $\mathbb{F}_{q_v}$ is smooth – for all but (possibly) finitely many v. Moreover, $\mathbb{Z}_K$ has only finitely many residue fields of a given characteristic hence only finitely many residue fields of bounded size. It follows from Exercise 1.69c) that for all but finitely many v there is a smooth point over k_v, so by Theorem 1.81 there is a K_v-rational point. □

5.6. Henselian Normed Fields. A non-Archimedean normed field $(K, |\cdot|)$ is **Henselian** if the norm extends uniquely to any algebraic exetension L/K. As we have seen above, complete implies Henselian. Remarkably, it turns out that the class of fields satisfying each of the versions of Hensel's Lemma stated above is precisely the Henselian fields.

THEOREM 1.86.
For a non-Archimedean normed field $(K, |\cdot|)$, the following are equivalent:
(i) K is Henselian.
(ii) (Hensel-Kürschak) An irreducible polynomial $f = a_n^n + \ldots + a_1 t + a_0 \in K[t]$ with $a_n a_0 \neq 0$ has

$$|f| \coloneqq \max_i |a_i| = \max |a_0|, |a_n|.$$

(iii) (Hensel Lifting) Let $f \in R[t]$ be a primitive polynomial. If f factors modulo $\mathfrak{m}$ as $\overline{g}\overline{h}$ with $\gcd(\overline{g}, \overline{h}) = 1$, then there are $g, h \in R[t]$ such that $f = gh$, $g \mod \mathfrak{m} = \overline{g}$, $h \mod \mathfrak{m} = \overline{h}$ and $\deg g = \deg \overline{g}$.
(iv) (My First Hensel's Lemma) Let $f \in R[t]$, and let $\overline{f} \in k[t]$ be its reduction modulo $\mathfrak{m}$. If there is $\overline{\alpha} \in k$ such that $\overline{f}(\overline{\alpha}) = 0$ and $\overline{f}'(\overline{\alpha}) \neq 0$, then there is $\alpha \in R$ such that $f(\alpha) = 0$ and $\alpha \pmod{\mathfrak{m}} = \overline{\alpha}$.
(vi) (Hensel-Newton)
(vii) (Multivariate Hensel-Newton)
(viii) (Hensel Smooth Lifting)

5.7. Henselian Local Rings.

CHAPTER 2

Local Fields

1. Remedial number theory I: Dedekind-Kummer

The material of this section comes from [**Se:CL**, Ch. III].

PROPOSITION 2.1. *Let R be a DVR with maximal ideal $\mathfrak{m}$ and residue field k. Let $f \in R[t]$ be monic of positive degree, and put*

$$S \coloneqq R[t]/(f).$$

Then S is a semi-local ring, and its maximal ideals are obtained as follows: let $\overline{f}$ be the image of f in $k[t]$, and factor it: $\overline{f} = p_1^{e_1} \cdots p_r^{e_r}$ with $p_1, \ldots, p_r \in k[t]$ distinct monic irreducible polynomials. For each $1 \leq i \leq r$, choose $g_i \in R[t]$ that lifts p_i (i.e., so that the reduction of g_i modulo $\mathfrak{m}$ is p_i). For $1 \leq i \leq r$, put

$$\mathcal{P}_i \coloneqq \langle \mathfrak{m}, g_i \rangle.$$

Then $\operatorname{MaxSpec} S = \{\mathcal{P}_1, \ldots, \mathcal{P}_r\}$.

PROOF. For $1 \leq i \leq r$, we have

$$S/\mathcal{P}_i = R[t]/\langle \mathfrak{m}, f, g_i \rangle = k[t]/(p_i)$$

is a (finite degree) field extension of k, so $\mathcal{P}_i$ is a maximal ideal of S. The ideals $\mathcal{P}_1, \ldots, \mathcal{P}_g$ are precisely the maximal ideals of S that contain $\mathfrak{m}S$. We claim that these are all the maximal ideals of S. To see this, let $\mathcal{P}$ be any maximal ideal of S. If $\mathcal{P}$ did not contain $\mathfrak{m}S$, then we would have $\mathcal{P} + \mathfrak{m}S = S$; since S is finitely generated as a module over the local ring $(R, \mathfrak{m})$, Nakayama's Lemma implies $\mathcal{P} = S$, a contradiction. □

LEMMA 2.2. *Let R be a commutative ring, let $f \in R[t]$, and let $a \in R$. There is a unique $g \in R[t]$ such that*

$$f(t) = f(a) + f'(a)(t-a) + (t-a)^2 g(t).$$

PROOF. By the universal property of polynomial rings, there is a unique R-algebra homomorphism $\Psi : R[t] \to R[t]$ that maps t to $t - a$. Clearly the unique homomorphism that maps t to $t + a$ is its inverse, so Ψ is an isomorphism. In particular, it is an R-module isomorphism, so it carries the R-basis $\{t^n \mid n \in \mathbb{N}\}$ to the R-basis $\{(t-a)^n \mid n \in \mathbb{N}\}$. Thus there unique $\{b_n\}_{n=0}^{\infty}$ in R, all but finitely of which are zero, such that

$$f = \sum_{n=0}^{\infty} b_n (t-a)^n = b_0 + b_1(t-a) + (t-a)^2 \sum_{n=2}^{\infty} b_n (t-a)^{n-2}.$$

Evaluating at a we find $b_0 = f(a)$. Differentiating and then evaluating at a we find that $b_1 = f'(a)$. Taking $g \coloneqq \sum_{n=2}^{\infty} b_n (t-a)^{n-2}$, we get

$$f(t) = f(a) + f'(a)(t-a) + (t-a)^2 g(t).$$

The polynomial g has to be unique, for if another polynomial h worked in its place we would have $(t-a)^2(g(t)-h(t))=0$, but the monic polynomial $(t-a)^2$ is not a zero divisor in $R[t]$. □

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. We say that S/R is **monogenic** if there is $\alpha \in S$ such that $S = R[\alpha]$. (In particular this implies that S is finitely generated as an R-module, which is always true if L/K is separable but need not hold in general.) In a "global" context, monogenicity is a sensitive issue: it is far from guaranteed that e.g. the ring of integers of a number field is monogenic over $\mathbb{Z}$. (In this classical context, instead of monogenicty one often speaks in terms of the existence of a **power basis**.) However, in the local context monogenicity is much easier: the following result shows in particular that if R is a complete discrete valuation ring with perfect residue field then S/R is monogenic for every finite degree separable field extension L/K. In particular, the ring of integers of every p-adic field is monogenic over $\mathbb{Z}_p$.

THEOREM 2.3. *Let R be a DVR with fraction field K. Let L/K be a separable finite degree field extension, and let S be the integral closure of R in L. We assume:*
(i) S is a DVR; and
(ii) the residual extension l/k is separable.
Then S is monogenic over R.

PROOF. Let $\mathfrak{p}$ be the maximal ideal of R and $\mathcal{P}$ be the maximal ideal of S, and let π be a uniformizer of S. Let $e = e(L/K)$, so $\mathfrak{p}S = (\pi^e)$. Let $k := R/\mathfrak{p}$ and $l := S/\mathcal{P}$, so $f = [l:k]$. By Theorem 1.73 we have $ef = [L:K]$. Since l/k is assumed separable, by the Primitive Element Corollary there is $\overline{x} \in l$ such that $l = k[\overline{x}]$. Let x be a lift of $\overline{x}$ to S.
Step 1: We claim that $\{x^i\pi^j\}_{0\le i<f,\ 0\le j<e}$ span S as an R-module.[1] By Nakayama's Lemma it is enough to show that their images in $S/\mathfrak{p}S$ span it as an R-module. Since $\mathfrak{p}S = \pi^e S$, it is enough to show that for all $0 \le m < e$, if the elements span $S/\pi^m S$ then they span $S/\pi^{m+1}S$. For $m = 0$, we have $S/\pi S = l$, so certainly the elements $1, x, \ldots, x^{f-1}$ span. Inductively we assume that for $1 \le m < e$ the elements $x^i\pi^j$ with $0 \le j < m$ span $S/\pi^m S$, and let $x \in S$. Then by assumption there are $r_{i,j} \in R$ and $y \in S$ such that

$$x - \sum_{i,j} r_{i,j} x^i \pi^j = \pi^m y.$$

There are $a_0, \ldots, a_{f-1} \in R$ such that $y - \sum_i a_i x^i \in \pi S$. Thus

$$x - \sum_{i,j} r_{i,j} x^i \pi^i - \sum_{i=0}^{f-1} a_i x^i \pi^m \in \pi^{m+1} S.$$

Step 2: We claim that we may choose x such that there is $g \in R[t]$ monic of degree f such that $g(x)$ is a uniformizer of S.
Proof: Start first with $g \in R[t]$ monic that reduces to the minimal polynomial of $\overline{x}$ over k. Let w be the normalized valuation on L, so $w(g(x)) \ge 1$. If $w(g(x)) = 1$,

[1] Since L/K is separable, S is free of rank n as an R-module. By [**C:CA**, Thm. 3.44], the claim implies that $\{x^i\pi^j\} - 0 \le i < f,\ 0 \le j < e$ in fact form an R-basis of S.

we have found our g. Otherwise $w(g(x)) \geq 2$. Let π be a uniformizer for L. By Lemma 2.2 there is $s \in S$ such that

$$g(x+\pi) = g(x) + \pi g'(x) + \pi^2 s.$$

Since l/k is separable, we have $\overline{g}'(\overline{x}) \neq 0$, so $w(\pi g'(x)) = 1$ and thus $w(g(x+\pi)) = 1$. Thus $x + \pi$ is an acceptable choice of x.
Step 3: Choose x as in Step 2 and put $\pi := g(x)$. By Step 1, the elements $\{x^i g(x)^j\}_{0 \leq i < f,\ 0 \leq j < e}$ span S over R. Thus $S = R[x]$. □

2. Unramified extensions

2.1. Distinguished classes of fields. Following Lang [**L-Alg**, p. 227], a class of field extensions $\mathcal{C} = \{L/K\}$ is said to be **distinguished** if it satisfies the following two conditions:

(DE1) (Tower condition): if K/F and L/K are both in $\mathcal{C}$, then L/F is in $\mathcal{C}$.
(DE2) (Base change condition): suppose E, F, K are subfields of a common field, and $F \subset K$, $F \subset E$ and $K/F \in \mathcal{C}$. Then $EK/E \in \mathcal{C}$.

Exercise 2.1. *Show that (DE1) and (DE2) imply the following:*
(DE3) Suppose K, L_1, L_2 are subfields of a common field, with K contained in both L_1 and L_2 and that $L_1/K,\ L_2/K \in \mathcal{C}$. Then $L_1L_2/K \in \mathcal{C}$.

Example 2.4. *a) The following classes of field extensions are distinguished: finite extensions, separable extensions; purely inseparable extensions; finitely generated extensions; purely transcendental extensions.*
b) The following classes of field extensions are not distinguished: normal extensions; Galois extensions: they satisfy (DE2) but not (DE1).

2.2. Unramified extensions.

Suppose K is a complete discretely valued field and L/K is a finite degree extension with separable residue extension l/k. By the Primitive Element Corollary, we may write $l = k[t]/(\overline{f})$ for a monic irreducible polynomial $\overline{f}$. Now lift $\overline{f}$ to a monic polynomial $f \in R[t]$. The polynomial f is irreducible in $R[t]$, so by Gauss's Lemma it is also irreducible in $K[t]$. Therefore we may form an extension $L' = K[t]/(f)$. It follows from Hensel's Lemma that L' is a subextension of L/K. What we would like to show is that the residual extension l'/k is simply l/k: it follows that L' is unramified and is the maximal unramified subextension of L/K. The following consequence of Proposition 2.1 gives this and a bit more.

Proposition 2.5. *With the setup of Proposition 2.1, assume that $\overline{f}$ is irreducible and put $L = K[t]/(f)$, so L is a field extension. Then $S := R[t]/(f)$ is the integral closure of R in L. It has maximal ideal $\mathfrak{m}S$ and residual extension $k[t]/(\overline{f})$. In particular, L/K is unramified.*

Proof. By Proposition 2.1, the ring S is local with maximal ideal $\mathfrak{m}S$ and residue field $k[t]/(\overline{f})$. Let π be a generator for $\mathfrak{m}$. Since $\mathfrak{m}$ is principal, so is $\mathfrak{m}S$, so S is a one-dimensional Noetherian local domain with principal maximal ideal, hence a DVR. In particular (in fact, this is equivalent among one-dimensional Noetherian local domains) S is integrally closed, so it is the integral closure S of R in L. The rest follows from Proposition 2.1. □

Conversely, to every finite degree separable extension $l = k[t]/(\overline{f})$ of k, we may lift to a monic $f \in R[t]$ and then the previous proposition shows that $L = K[t]/(f)$ is an unramified extension of K with residual extension l/k. Thus we get a bijective correspondence between unramified finite degree extensions of K and separable finite degree extensions of k. We can therefore also replace both instances of "finite degree' by "algebraic."

COROLLARY 2.6. *The unramified algebraic extensions of a CDVF form a distinguished class.*

PROOF. It is immediate that if M/L and L/K are unramified, so is M/K. Conversely, suppose K is a CDVF field, L/K is unramified and E/K is any algebraic extension. Then we must show that LE/E is unramified. By the classification of unramified extensions, an algebraic extension is unramified iff it is generated by the lifts to the valuation ring of roots of separable polynomials over k. This property is preserved by base change, so the proof is complete. □

3. Remedial Number Theory II: Schönemann-Eisenstein

COROLLARY 2.7 (Corollary to Gauss's Lemma). *Let R be a UFD with fraction field K, and let $f \in R[t]$ be a polynomial.*
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 exist $g, h \in R[t]$ such that $\deg(g), \deg(h) < \deg(f)$ and $f = gh$.

PROOF. See e.g. [**C:CA**, Cor. 15.25]. □

THEOREM 2.8. *(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 $0 \leq i < d$ 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 $0 < k \leq n$. 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) If R is a GCD-domain, and suppose for a contradiction that f is reducible over $K[t]$, then by Corollary 2.7b), 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 through to give a contradiction. □

Remark: For our purposes we wish to apply this to the valuation ring R attached to a (as always rank one, unless otherwise specified) valuation v on the fraction field K, with $\mathfrak{p}$ the unique maximal ideal of R. Notice that in this case we may pass to the completion $\hat{K}$ and its valuation ring $\hat{R}$ without disturbing any of the

hypotheses, so we get an automatic strengthening of Eisenstein's Criterion: f is irreducible not merely over $K[t]$ but also over $\hat{K}[t]$.

Remark: In particular, if (R, v) is a DVR with uniformizing element π, then Eisenstein's criterion applied to $P_n(t) = t^n - \pi$ gives rise to a totally ramified extension of degree n for all $n > 1$, as we have seen before.

EXERCISE 2.2. *Let (K, v) be a nontrivial rank one valued field, with valuation ring R and maximal ideal $\mathfrak{m}$. Show that the following are equivalent:*
(i) $\mathfrak{m}^2 \subsetneq \mathfrak{m}$.
(ii) $\bigcap_{i=1}^{\infty} \mathfrak{m}^i = \{0\}$.
(iii) R is Noetherian.
(iv) Γ *is discrete.*

In particular, for a (rank one) valuation ring, Eisenstein's criterion can only be successfully applied if the valuation is discrete.

EXERCISE 2.3. *Give an example of a non-Noetherian valuation ring R to which Eisenstein's Criterion can be nontrivially applied.*

4. Totally ramified extensions

PROPOSITION 2.9. *Let R be a DVR with maximal ideal $\mathfrak{m}$ and residue field k. $f = t^n + a_{n-1} + \ldots + a_1 t + a_0 \in R[t]$, $a_i \in \mathfrak{m}$, $a_0 \notin \mathfrak{m}^2$. Then $S_f \coloneqq R[t]/(f)$ is a DVR with maximal ideal generated by the image of t and with residue field k. Thus, if L is the fraction field of S_f, then L/K is totally ramified.*

PROOF. Upon reducing modulo $\mathfrak{m}$, we have $\overline{f} = t^n$. Proposition 2.1 gives that S_f is a local ring with maximal ideal $\langle \mathfrak{m}, t \rangle$. Moreover, the hypotheses give us that a_0 is a uniformizer of R. Let us write $\bar{t}$ for the image of t in the quotient ring $S_f = R[t]/(f)$. Then we have

$$-a_0 = \bar{t}^n + a_{n-1}\bar{t}^{n-1} + \ldots + a_1\bar{t},$$

so $a_0 \in (\bar{t})$. Therefore $\langle \mathfrak{m}, \bar{t} \rangle = \langle a_0, \bar{t} \rangle = \langle \bar{t} \rangle$. That is, S_f is a local ring with a principal maximal ideal. Since a_0 is not nilpotent, neither is $\bar{t}$, so S_f is a DVR. The rest follows immediately. □

We deduce:

COROLLARY 2.10. *An Eisenstein polynomial $f(t)$ is irreducible in $K[t]$, and if $L \coloneqq K[t]/(f)$, then $S_f \coloneqq R[t]/(f)$ is the integral closure of R in L.*

EXERCISE 2.4. *Prove Corollary 2.10.*

Conversely:

THEOREM 2.11. *Let R be a DVR with fraction field K, let L/K a degree n field extension, and let S be the integral closure of R in L. Suppose that S is a DVR and $e(L/K) = n = [L : K]$. Let π be a uniformizer of S and let $f \in K[t]$ be the minimal polynomial of π. Then $f \in R[t]$ is Eisenstein and the homomorphism $R[t] \to S$ mapping $t \mapsto \pi$ induces an isomorphism $S_f \xrightarrow{\sim} S$.*

PROOF. Since R is integally closed, by [**C:CA**, Thm. 14.18], we have $f \in R[t]$. Let us write

$$f = a_n t^n + a_{n-1} t^{n-1} + \ldots + a_1 t + a_0,\ a_i, a_n = 1 \in R.$$

(The reason for writing out a_n when it is equal to 1 will become clear shortly.) Evaluating at π, we get

$$a_n \pi^n + a_{n-1} \pi^{n-1} + \ldots + a_0 = 0.$$

Let w be the normalized discrete valuation assocated to S, i.e., such that $w(\pi) = 1$. Then because of total ramification, we have $w(a) \equiv 0 \pmod{n}$ for all $a \in R \setminus \{0\}$.

Put

$$r \coloneqq \min_{0 \leq i \leq n} w(a_i \pi^i).$$

By the Domination Principle, there must be $0 \leq i < j \leq n$ such that

$$r = w(a_i) + i = w(a_i \pi^i) = w(a_j \pi^j) = w(a_j) + j.$$

Then

$$j - i = w(a_i) - w(a_j) \equiv 0 \pmod{n}.$$

This forces $i = 0$, $j = n$ and

$$n = w(\pi^n) = w(a_n \pi^n) = w(a_0).$$

Let v be the discrete valuation on K, and let $\mathfrak{p}$ be the maximal ideal of R. Since $e(L/K) = n$ and w is normalized, we have $w|_K = nv$, so $v(a_0) = 1$ and $a_0 \in \mathfrak{p} \setminus \mathfrak{p}^2$. Moreover, for all $1 \leq i \leq n-1$ we have

$$w(a_i) + i = w(a_i \pi^i) \geq r = n,$$

so $w(a_i) \geq n - i$ and thus $v(a_i) > 0$, i.e., $a_i \in \mathfrak{p}$. Thus f is indeed Eisenstein. □

5. Higher unit groups

Let K be a field, and let $v : K^\times \to \mathbb{Z}$ be a normalized discrete valuation on K. Let R be the valuation ring, $\mathfrak{m}$ the maximal ideal, π a uniformizing element, and $k = R/\mathfrak{m}$ the residue field.

In this section we will define a natural descending filtration on the group of units of R. Here it comes: put

$$U_0 \coloneqq R^\times,$$
$$\forall n \in \mathbb{Z}^+,\ U_n \coloneqq 1 + \mathfrak{m}^n,$$

so as advertised, we have

$$R^\times = U_0 \supset U_1 \supset U_2 \supset \ldots \supset U_n \supset \ldots$$

Let $r_n : R \to R/\mathfrak{m}^n$ be the usual reduction map. Then by definition we have

$$U_n = \operatorname{Ker} r_n.$$

Since R is local, the induced map on unit groups $r_n^\times : R^\times \to (R/\mathfrak{m}^n)^\times$ is surjective, so $r_1^\times$ induces an isomorphism

$$U_0/U_1 \xrightarrow{\sim} k^\times.$$

EXERCISE 2.5. *Show* $\bigcap_{n \geq 0} U_n = \{1\}$.

PROPOSITION 2.12. *For all $n \in \mathbb{Z}^+$, we have a canonical isomorphism*

$$U^n/U^{n+1} \cong (k, +).$$

PROOF. Indeed, consider the map $\Phi : \mathfrak{m}^n \to U^n/U^{n+1}$ given by $x \mapsto 1 + x + U^{n+1}$. Since $U^n = 1 + \mathfrak{m}^n$, this map is visibly a surjection. On the other hand, there is some multiplicative to additive funny business going on here, so that it is not immediately clear that Φ is a homomorphism! Let's check it:

$$\Phi(x)\Phi(y)\Phi(x+y)^{-1} = \frac{(1+x)(1+y)}{1+x+y} = \frac{1+x+y+xy}{1+x+y} = 1 + \frac{xy}{1+x+y}.$$

Since $v(x+y) \geq \min v(x), v(y) \geq n$, $v(1+x+y) = 0$, so $v(xy/(1+x+y)) \geq 2n \geq n+1$, so $1 + \frac{xy}{1+x+y} \in U^{n+1}$. Thus Φ is a homomorphism. The kernel of Φ is $\mathfrak{m}^{n+1}$, so we get $U^n/U^{n+1} \cong \mathfrak{m}^n/\mathfrak{m}^{n+1} \cong (k, +)$. □

THEOREM 2.13. *Let $K/\mathbb{Q}_p$ be a finite extension with ramification index e. Then for all sufficiently large positive integers n, there is an isomorphism of topological groups $\Phi : (U_n, \cdot) \xrightarrow{\sim} (\mathfrak{m}^n, +)$.*

The proof of Theorem 2.13 will be developed in the following exercise.

EXERCISE 2.6. *Consider the following formal power series:*

$$L(t) = \sum_{n=1}^{\infty} (-1)^{n+1} \frac{(t-1)^n}{n} \in \mathbb{C}_p[[t]],$$

$$E(t) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \in \mathbb{C}_p[[t]].$$

Note that $L(t)$ and $E(t)$ are precisely the usual Taylor series expansions of $\log(t)$ at $t = 1$ and e^t at $= 0$ encountered in real/complex analysis.
a) Consider $L(x)$ and $E(x)$ as functions on, say, $\mathbb{C}_p$. Show that the radius of convergence of $L(x)$ is 1 and the radius of convergence of $E(x)$ is $R_p := p^{\frac{-1}{p-1}}$.
b) Show that $|x-1| < R_p \implies E(L(x)) = x$ and $L(E(x)-1) = x-1$.
c) Show that for all x, y with $|x|, |y| \leq 1$ we have $L(xy) = L(x) + L(y)$ and that for all x, y with $|x|, |y| \leq R_p$ we have $E(x+y) = E(x)E(y)$.
d) Now let K be a p-adic field. Show that there exists a constant $C = C([K : \mathbb{Q}_p], p)$ such that for all $n \geq \max(1, C)$, the map $x \mapsto L(x)$ induces an isomorphism of topological groups $(U_n, \cdot) \to (\mathfrak{m}^n, +)$. Show in particular that when $K = \mathbb{Q}_p$ with $p > 2$, the isomorphism holds for all $n \geq 1$ and that for $\mathbb{Q}_2$ it holds for all $n \geq 2$.

In positive characteristic, $L(x)$ and $E(x)$ are not even defined as formal power series, as some of the terms have denominators divisble by p. And indeed the structure of the unit group is much different in this case:

EXERCISE 2.7. *Let $K = \mathbb{F}_q((t))$. Show that there is no nontrivial group homomorphism from $(\mathbb{F}_q[[t]], +)$ to $U = \mathbb{F}_q[[t]]^\times$. (Hint: consider p-torsion.)*

6. Locally compact fields

6.1. The classification of nondiscrete locally compact topological fields. Some of the most important theorems in mathematics give complete classifications of certain fundamental structures. Examples: the classification of (topological!) surfaces, the classificaiton of simple Lie algebras, the classification of finite simple

groups. In this section we discuss a classification theorem which belongs somewhere in the above pantheon.

LEMMA 2.14 (Cohen [**Co48**]). *Let $(K, |\cdot||)$ be a complete nontrivially normed field. For a normed K-linear space $(V, ||\cdot||)$ the following are equivalent:*
(i) V is locally compact.
(ii) If $C > 0$ and $A \in (1, \infty) \cap |K^\times|$, there does not *exist an ininite sequence $\{x_n\}$ in V such that*

$$\forall n \in \mathbb{Z}^+,\ C \leq ||x_n|| \leq CA^2;\ \forall m \neq n \in \mathbb{Z}^+,\ C \leq ||x_m - x_n|| \leq CA^2. \tag{7}$$

(iii) K is locally compact and $\dim_K V$ is finite. Moreover, if K is non-Archimedean, then it is discretely valued with finite residue field.

PROOF. (i) $\implies$ (ii): We first claim that since V is locally compact, it is ball compact. Indeed, local compactness gives $\epsilon > 0$ such that the closed ball $B_{\leq \epsilon}(0)$ is compact. Since for all $\alpha \in K^\times$ the map $x \mapsto \alpha x$ is a homeomorphism of V, also the closed balls $B_{\leq |\alpha| \epsilon}(0)$ are compact. Since the norm is nontrivial, $|\alpha|$ can be arbitrarily large, so we get that all closed bounded subsets of V are compact. It follows that there is no sequence in V satisfying (7), since any such sequence cannot have a convergent subsequence.
(ii) $\implies$ (iii): Let $x \in V \setminus \{0\}$ and put $r \coloneqq ||x||$. Then there is no sequence $\{a_n\}$ in K such that

$$\forall n,\ C/r \leq |a_n| \leq C/rA^2; \forall m \neq n,\ C/r \leq |a_m - a_n| \leq C/rA^2.$$

In the non-Archimedean case, the valuation on K must therefore be discrete: otherwise the value group is dense in $\mathbb{R}$, so there is a sequence $\{a_n\}$ such that $|a_n|$ takes distinct values in $[C/r, C/rA^2]$, and then

$$|a_m - a_n| = \max |a_m|, |a_n| \leq [C/r, C/rA^2].$$

Moreover, in the non-Archimedean case the residue field must be finite, for otherwise there is a sequence $\{b_n\}$ in K with $|b_n| = 1$ for all n and $|b_m - b_n| = 1$ for all $m, n \in \mathbb{Z}^+$; there is $a \in K$ such that $C/r \leq |a| \leq C/rA^2$ and then taking $a_n = ab_n$ gives a contradiction as above.

In the Archimedean case, K must be either $\mathbb{R}$ or $\mathbb{C}$ by Ostrowski, hence is locally compact. In the non-Archimedean case, a complete discretely valued field with finite residue field is locally compact because the valuation ring R is the inverse limit of finite discrete spaces $R/\mathfrak{m}^n$, hence is compact.

It remains to show that V is finite-dimensional. Assuming it isn't, we will build a sequence $\{x_n\}$ in V satisfying (7). Suppose we have constructed $x_1, \ldots, x_n$ satisfying (7), and let W be the K-subspace of V spanned by $x_1, \ldots, x_n$. Then W is closed. Let $y \in V \setminus W$, and put

$$d \coloneqq \inf_{x \in W} ||y - x||.$$

We must have $d > 0$: otherwise there is a sequence of points in W converging to y, contradicting the closure of W. There is $x' \in W$ such that

$$d \leq ||y - x'|| \leq dA.$$

Replacing y with $y - x'$, we get

$$d \leq ||y|| \leq dA;\ \forall x \in W,\ ||y - x|| \geq d.$$

Choose $a \in K$ such that $C/d \leq |a| \leq C/dA$. Then we may take $x_{n+1} \coloneqq ay$.
(iii) $\implies$ (i): We know that V is homeomorphic to K^n, and a finite product of locally compact spaces is locally compact. □

THEOREM 2.15. *Let $(K, |\cdot|)$ be a nontrivially normed non-Archimedean field, with valuation ring R and residue field k. The following are equivalent:*
(i) K is locally compact.
(ii) K is ball compact.
(iii) R is compact.
(iv) K is complete, discretely valued, and k is finite.
(v) K is a finite extension of $\mathbb{Q}_p$ or of $\mathbb{F}_p((t))$, for a suitable prime number p.

PROOF. Since in a normed field any two closed balls are homeomorphic, such a field is locally compact iff any closed ball is compact iff every closed ball is compact. This gives (i) $\iff$ (ii) $\iff$ (iii).
(i) $\implies$ (iv): If K is locally compact, then as above it is ball compact and thus complete. It follows from Lemma 2.14 that K is discretely valued. Moreover, R is compact and $\mathfrak{m}$ is an open subgroup, so $k = R/\mathfrak{m}$ is on the one hand discrete and on the other hand compact, being the continuous image of the compact space R. So k is finite.
(iv) $\implies$ (iii): Let $\hat{R}$ be the completion of the discrete valuation ring R with respect to the maximal ideal $\mathfrak{m}$. By definition this is, as a topological ring, $\varprojlim_n R/\mathfrak{m}^n$. Here, as above, each quotient $R/\mathfrak{m}^n$ has the discrete topology, and $\hat{R}$ is given the natural topology it inherits as a closed subspace of the direct product $X = \prod_{n=1}^{\infty} R/\mathfrak{m}^n$. As we have seen before, the finiteness of $k = R/\mathfrak{m}$ implies the finiteness of $R/\mathfrak{m}^k$ for all k. Therefore X is a product of finite discrete spaces, so is compact (by Tychonoff's theorem, or alternately by Exercise 2.X.), and $\hat{R}$ is a closed subspace of X so is also compact. We have a natural map $\Phi : R \to \hat{R}$ in which we send each $x \in R$ to the compatible sequence of cosets $(x + \mathfrak{m}^n)$. The fundamental result, from which our claim follows immediately, is that Φ is an isomorphism of topological rings. Happily, this is easy to check: $\ker(\Phi) = \bigcap \mathfrak{m}^n = 0$, so Φ is injective. To see surjectivity, let $(x_n + \mathfrak{m}^n)$ be any element of the inverse limit, i.e., we require that $x_{n+1} \equiv x_n \pmod{}m^n$. Let us choose a system of coset representatives $\mathcal{S} = r_1, \ldots, r_q$ for $R/\mathfrak{m}$ in R. Then (by definition) there exists a unique $a_1 \in \mathcal{S}$ such that $x_1 + \mathfrak{m} = a_1 + \mathfrak{m}$. Moreover, there exists a unique $a_2 \in \mathcal{S}$ such that $x_2 + \mathfrak{m}^2 = a_1 + a_2\pi + \mathfrak{m}^2$. Continuing in this way, we get a unique sequence of elements $a_1, \ldots, a_n \in \mathcal{S}$ such that for all n, we have that $x_n + \mathfrak{m}^n = \sum_{i=0}^{n-1} a_i \pi^{n-1}$. But since $a_n \pi^n \to 0$, the series $\sum_{i=1}^{\infty} a_i \pi^{i-1}$ converges to a unique element, say x, of R, which has the property that for all $n \geq 0$, $x + \mathfrak{m}^n = x_n + \mathfrak{m}^n$. Thus $\Phi(x) = (x_n + \mathfrak{m}^n)$ and Φ is surjective, thus an isomorphism of rings. In each of these topological rings, a neighborhood basis of 0 is given by powers of the maximal ideal $\mathfrak{m}^n$, so Φ is certainly a homeomorphism as well. Thus $\Phi : R \xrightarrow{\sim} \hat{R}$ (we say that R is an $\mathfrak{m}$-adically complete local ring).
(v) $\implies$ (i) is immediate: a finite degree extension of a locally compact field is a locally compact field.
(i) $\implies$ (v): Let $(K, |\cdot|)$ be a discretely valued locally compact field. First suppose that K has characteristic 0. Thus $\mathbb{Q} \hookrightarrow K$ and the norm on K restricts to a non-Archimedean norm on $\mathbb{Q}$. But we have classified all such and know that they are (up to equivalence, which is harmless here) all of the form $|\cdot|_p$ for a unique prime number p. Therefore the closure of $\mathbb{Q}$ inside K is the completion of $\mathbb{Q}$ with respect

to $|\cdot|_p$, i.e., is $\mathbb{Q}_p$, so we have embeddings of normed fields

$$\mathbb{Q} \hookrightarrow \mathbb{Q}_p \hookrightarrow K.$$

Now we apply Lemma 2.14: since K is a locally compact, normed $\mathbb{Q}_p$-vector space, it is finite dimensional over $\mathbb{Q}_p$, which is what we wanted to show.

Now suppose that K has characteristic $p > 0$, so that we have $\mathbb{F}_p \subset K$. Recall that an algebraic extension of a finite field carries only trivial norms, so in particular $\mathbb{F}_p$ is already complete in K. So we need to introduce a little more: since (i) $\iff$ (iv), K is discretely valued. Let $t \in K$ be a uniformizing element, i.e., $v(t) = 1$. Then, by the above remarks, t is *not* algebraic over $\mathbb{F}_p$ for otherwise we would have $v(t) = 0$. Thus the least extension of K containing t is $\mathbb{F}_p(t)$, the rational function field over $\mathbb{F}_p$. Now we are homefree as before: the restriction of v to $\mathbb{F}_p(t)$ is a discrete valuation such that $v(t) = 1$. There is a unique such valuation, namely the valuation ord_t coming from the irreducible element t in the polynomial ring $\mathbb{F}_p[t]$, so that the closure in K of $\mathbb{F}_p(t)$ is nothing else than the Laurent series field $\mathbb{F}_p((t))$. Arguing as above, we get that K is finite-dimensional over $\mathbb{F}_p((t))$, done. □

Since Ostrowski's Theorem tells us that the only locally compact Archimedean fields are $\mathbb{R}$ and $\mathbb{C}$, we get the following result.

COROLLARY 2.16. *Every locally compact, nondiscrete, normed field is isomorphic to $\mathbb{R}$, $\mathbb{C}$ or to a finite extension of $\mathbb{Q}_p$ or of $\mathbb{F}_p((t))$.*

In the latter case, it turns out that one can say much more:

COROLLARY 2.17. *A locally compact normed field of positive characteristic is isomorphic to $\mathbb{F}_q((t))$ for some prime power q.*

PROOF. Let K be a locally compact normed field of positive characteristic, so by Corollary 2.16 K is a finite degree extension of $\mathbb{F}_p((t))$. As the proof of Theorem 2.15 shows, K is discretely valued, and we can choose t to be a uniformizing element of K. Let K' be the maximal unramified subextension of $K/\mathbb{F}_p((t))$, so that $K' = \mathbb{F}_q((t))$, where $q = \#k$, the residue field of K. But then the extension $K/\mathbb{F}_q((t))$ is totally ramified with ramification index 1, since the uniformizer t of K is also an element (necessarily then a uniformizing element) of $\mathbb{F}_q((t))$. Since the residue field, $\mathbb{F}_q$, is perfect, it follows that $K = \mathbb{F}_q((t))$. □

Nevertheless $K = \mathbb{F}_q((t))$ has totally ramified extensions of every degree: e.g. $K(t^{\frac{1}{n}})$. The point is that every totally ramified extension of $\mathbb{F}_q((t))$ is, as an abstract field, isomorphic to $\mathbb{F}_q((t))$. This leads to the following definitions.

Let (K, v) be a locally compact non-Archimedean field, with residue field $k = \mathbb{F}_q = \mathbb{F}_{p^f}$. Then its **absolute residual degree** is f, and its **absolute ramification index** is $v(p)$.

Despite the fact that these definitions are uniform across the two cases of p-adic fields and Laurent series fields, their implications are quite different:
Let K be a locally compact field of characteristic 0 and residue characteristic p. Then K is canonically an extension of $\mathbb{Q}_p$: indeed, this follows from the proof above, because $\mathbb{Q}_p$ is constructed inside K as the closure of $\mathbb{Q}$. Moreover the degree $[K : \mathbb{Q}_p]$ is ef. On the other hand, let K be a locally compact field of characteristic p. Then its absolute ramification index is $e = v(p) = v(0) = \infty$. This may seem like

a strange definition, but it's a suggestive one, since for any n, K admits a subfield F such that $e(K/F) = n$. In particular, there is no canonical copy of $\mathbb{F}_p((t))$ inside K, and certainly no minimal copy.

We remark in passing that one can consider topological fields where the topology is not necessarily induced by a norm. It turns out that requiring the topology to come from a norm does not restrict the class of locally compact fields:

THEOREM 2.18. *Let L be a locally compact, nondiscrete topological field.*
a) Then L is a finite extension of one of the following fields:
(i) $K = \mathbb{R}$.
(ii) $K = \mathbb{Q}_p$.
(iii) $K = \mathbb{F}_p((t))$.
b) In case (i) $L = \mathbb{R}$ or $L = \mathbb{C}$.
c) In case (ii) the ramification index $e(L/\mathbb{Q}_p)$ and residual degree $f(L/\mathbb{Q}_p)$ are uniquely determined by the abstract field L, and for any given $e, f \in \mathbb{Z}^+$, the number of finite extensions $L/\mathbb{Q}_p$ of ramification index e and residual degree f is finite and nonempty.
d) In case (iii) the residual degree f is determined by the abstract field L, but the ramification index is not. Moreover, every totally ramified extension of $\mathbb{F}_q((t))$ is isomorphic to $\mathbb{F}_q((t))$.

Theorem 2.18 is perhaps most gracefully proved using the Haar measure on a locally compact topological group. We refer to [**Wl**] for details.

6.2. An application of compactness. How do you describe $\mathbb{Z}_p$ to your colleagues in other areas of mathematics? Depending upon their background, a discussion of valuations, inverse limits, completions etc. may not be called for. Rather, one often says that $\mathbb{Z}_p$ is a domain containing $\mathbb{Z}$ such that a system of polynomial equations over $\mathbb{Z}$ has a solution over $\mathbb{Z}_p$ iff it has congruential solutions modulo p^a for all positive integers a. Or possibly some special case of this: e.g. that an integer x is a square in $\mathbb{Z}_2$ iff it is a square in $\mathbb{Z}/2^a\mathbb{Z}$ for all $a \in \mathbb{Z}^+$. Is this obvious?

One direction is: if R is a ring and $f_1(t_1, \ldots, t_n), \ldots, f_m(t_1, \ldots, t_n) \in R[t_1, \ldots, t_n]$ are polynomials, and $x = (x_1, \ldots, x_n) \in R^n$ is such that $f_1(x) = \ldots = f_m(x) = 0$, then if $\varphi : R \to R'$ is any ring homomorphism, then $\varphi(x) = (\varphi(x_1), \ldots, \varphi(x_n)) \in (R')^n$ is a solution to the equations $\varphi(f_1), \ldots, \varphi(f_m) \in R'[t_1, \ldots, t_n]$. Applying this with $\varphi : \mathbb{Z}_p \to \mathbb{Z}_p/(p^a) = \mathbb{Z}/p^a\mathbb{Z}$ shows that having solutions in $\mathbb{Z}_p$ necessitates solutions in $\mathbb{Z}/p^a\mathbb{Z}$ for all a.

The other direction really is not obvious, nor is it a version of Hensel's Lemma. However it is true!

THEOREM 2.19. *Let $(K, |\cdot|)$ be a locally compact nondiscrete non-Archimedean normed field, with valuation ring R and maximal ideal $\mathfrak{m}$. Let $f_1(t), \ldots, f_m(t) \in R[t] = R[t_1, \ldots, t_n]$ be polynomials. The following are equivalent:*
(i) There is $x \in R^n$ such that $f_1(x) = \ldots = f_m(x) = 0$.
(ii) For all $a \in \mathbb{Z}^+$ there is $x \in R^n$ such that $f_1(x) \equiv \ldots \equiv 0 \pmod{\mathfrak{m}^a}$.

PROOF. Let $||\cdot||$ be our favorite norm on K^m: $||(y_1, \ldots, y_m)|| := \max_j |y_j|$. Consider the following function

$$F : R^n \to \mathbb{R},\ x = (x_1, \ldots, x_n) \in R^n \mapsto ||(f_1(x), \ldots, f_m(x))||.$$

Now here is the key observation: the function F is continuous, and the hypotheses on K imply that R is compact, and thus F assumes a minimum value $m \geq 0$.
Case 1: Suppose $m = 0$. Then there is $x \in R^n$ such that $F(x) = 0$, i.e., $f_1(x) = \ldots = f_m(x) = 0$. Thus (i) holds.
Case 2: Suppose $m > 0$. Then there is no $x \in R^n$ such that $f_1(x) = \ldots = f_m(x) = 0$, i.e., (i) fails. Let π be a generator for $\mathfrak{m}$. Then $|\pi| < 1$, so there is $A \in \mathbb{Z}^+$ such that $|\pi^A| < m$. Thus for all $x \in R^n$ we have

$$F(x) = \max_j |f_j(x)| > |\pi^A|,$$

so there is $1 \leq j \leq m$ such that $f_j(x) \notin \mathfrak{m}^A$. Thus (ii) fails. □

7. Squares in local fields

PROPOSITION 2.20. *Let (K, v) be a discretely valued field. Then a choice of uniformizing element $\pi \in K$ gives rise to an isomorphism of groups $(K^\times, \cdot) \cong (R^\times, \cdot) \times (\mathbb{Z}, +)$.*

PROOF. We have the short exact sequence

$$1 \to R^\times \to K^\times \stackrel{v}{\to} \mathbb{Z} \to 0.$$

Because $\mathbb{Z}$ is a free – hence projective! – $\mathbb{Z}$-module, the sequence splits. To choose a splitting it is necessary and sufficient to lift the generator $1 \in \mathbb{Z}$ to an element in $K^\times$. This is precisely the choice of a uniformizing element. □

Thus for instance the group-theoretic study of $K^\times$ is reduced to that of $R^\times$. In these kind of considerations, it is traditional to change notation and terminology: put $U := R^\times$ and call U the **unit group** of K. (This is, strictly speaking, an abuse of terminology, since the unit group of K should just be $K^\times$. However, it is traditional and not very confusing. Anyway, by the previous result, the two groups are very closely related!)

PROPOSITION 2.21. *Let p be an odd prime number, and let $u \in \mathbb{Z}$ be a quadratic nonresidue modulo p. Then $[\mathbb{Q}_p^\times : \mathbb{Q}_p^{\times 2}] = 4$, and a set of coset representatives is $1, p, u, pu$.*

EXERCISE 2.8. *Prove Proposition 2.21.*

PROPOSITION 2.22. *We have $[\mathbb{Q}_2^\times : \mathbb{Q}_2^{\times 2}] = 8$. A set of coset representatives is $\pm 1, \pm 2, \pm 5, \pm 10$.*

EXERCISE 2.9. *Prove Proposition 2.22.*

PROPOSITION 2.23. *Let q be an odd prime power and let $K = \mathbb{F}_q((t))$. Then $[K^\times : K^{\times 2}] = 4$. A set of coset representatives is $1, u, t, ut$, where $u \in \mathbb{F}_q^\times \setminus \mathbb{F}_q^{\times 2}$.*

EXERCISE 2.10. *Prove Proposition 2.23.*

Note that for for any field K, $K^\times / K^{\times 2}$ is an elementary abelian 2-group, called the group of **square classes** of K. In particular, it is a $\mathbb{Z}/2\mathbb{Z}$-vector space. Thus, instead of listing all of its elements, it would be equivalent but more efficient to give a basis. In the case of $\mathbb{Q}_p$ with p odd, a basis is given by p, u. In the case of $\mathbb{Q}_2$, a basis is given by $-1, 2, 5$.

EXERCISE 2.11. *a) Let K be a Henselian discrete valuation field with residue field k of characteristic different from 2. Show that* $\dim_{\mathbb{F}_2} K^\times/K^{\times 2} = \dim_{\mathbb{F}_2} k^\times/k^{\times 2} + 1$.
b) Suppose further that $K = k((t))$. Let $\{b_i\}_{i\in I}$ be an $\mathbb{F}_2$-basis for $k^\times/k^{\times 2}$. Show that an $\mathbb{F}_2$-basis for $k((t))^\times/k((t))^{\times 2}$ is $\{b_i\} \cup \{t\}$.

EXERCISE 2.12. *What can you say about the set of square classes in $\mathbb{F}_2((t))$?*

THEOREM 2.24. *(Local Square Theorem) Let K be a Henselian discretely valued field of characteristic different from 2, with valuation ring R and uniformizer π. For any $\alpha \in R$, $1 + 4\pi\alpha \in R^{\times 2}$.*

PROOF. [**G**, Thm. 3.39] Let $f(t) = \pi t^2 + t - \alpha$. Then

$$v(f(\alpha)) = v(\pi\alpha^2) = 1 + 2v(\alpha) \geq 1 > 0 - v(2\pi\alpha + 1) = v(f'(\alpha)),$$

so by Hensel's Lemma there exists $\beta \in R$ such that $f(\beta) = 0$. Therefore the discriminant $1 + 4\pi\alpha$ of f is a square in K, so $1 + 4\pi\alpha \in K^{\times 2} \cap R = R^{\bullet 2}$. □

8. Quadratic forms over local fields

We begin with a very brief review of the notion of a quadratic form over a field and some associated invariants. For more information, the reader may consult [**C:QF**] or the classic texts of Cassels [**Ca:QF**] or Lam [**Lam**].

Let K be a field of characteristic different from 2 but otherwise arbitrary.[2] A **quadratic form** q over K is a polynomial $q(x_1, \ldots, x_n) = \sum_{1\leq i\leq j\leq n} a_{ij}x_ix_j$, i.e., homogeneous of degree 2. (We say that n is the **dimension** of q.) We define the **Gram matrix** M_q whose (i,i) entry is $a_{i,i}$ and whose (i,j) entry, for $i \neq j$, is $\frac{a_{ij}}{2}$ (note that we are using $2 \in K^\times$ here!). Then if we let x denote the column vector $(x_1, \ldots, x_n)$, we have the identity

$$q(x_1, \ldots, x_n) = x^T M_q x.$$

We wish to regard two quadratic forms over K as "equivalent" if one can be obtained from the other by an invertible linear change of variables. More explicitly, for any $P \in \mathrm{GL}_n(K)$, we define $(P \bullet q)(x) = q(Px)$. Here is one slightly tricky point for beginners: for any vector $x \in K^n$, we have

$$(P \cdot q)(x) = x^T M_{P\cdot q} x = (Px)^T M_q Px = x^T P^T M_q Px,$$

and it follows that the matrix representative of $P \bullet q$ is $P^T M_q P$. In other words, the induced relation on symmetric matrices is not similarity but the above relation, classically called **congruence** of matrices.

Recall that any symmetric matrix M over the real numbers can be not only diagonalized but orthogonally diagonalized, i.e., there exists a matrix P with $PP^T = 1_n$ such that $P^{-1}MP$ is diagonal. By orthogonality of P, we have $P^{-1}MP = P^TMP$, so the result implies that any quadratic form over the real numbers can be **diagonalized**, i.e., after a linear change of variables is given in the diagonal form

$$\langle a_1, \ldots, a_n \rangle = a_1x_1^2 + \ldots + a_nx_n^2.$$

[2]The case of characteristic 2 comes up in at least one exercise, but only as an example of what can go wrong!

One of the classical theorems of the subject is a generalization of this: over any field K of characteristic different from 2 is diagonalizable.

EXERCISE 2.13. *A very special and important quadratic form is $q_{\mathbb{H}}(x_1, x_2) = x_1x_2$, the so-called* ***hyperbolic plane****.*
a) Let K be any field of characteristic different from 2. Give an explicit change of variables that diagonalizes $q_{\mathbb{H}}$.
b) Show by brute force that $q_{\mathbb{H}}$ cannot be diagonalized over $\mathbb{F}_2$.
c) Show that $q_{\mathbb{H}}$ cannot be diagonalized over any field of characteristic 2.

A quadratic form is said to be **nondegenerate** if any of its defining symmetric matrices are invertible, and otherwise degenerate. It can be shown that any nondegenerate quadratic form in n variables is $\mathrm{GL}_n(K)$-equivalent to a quadratic form in fewer variables. Applying this observation repeatedly, we may view any degenerate quadratic form simply as a strangely presented nondegenerate quadratic form in fewer (possibly 0) variables, so it is harmless to restrict attention to nondegenerate forms.

A quadratic form q is **anisotropic** if for all $a = (a_1, \ldots, a_n) \in K^n$, $q(a) = 0$ implies $a = (0, \ldots, 0)$. In other words, the quadratic hypersurface $q(x) = 0$ has no K-rational points. A nondegenerate quadratic form which is not anisotropic is called **isotropic**.

Let $n \in \mathbb{Z}^+$. A field K is said to have **u-invariant** n – written $u(K) = n$ – if every quadratic form over K in more than n variables is isotropic and there exists at least one n-dimensional anisotropic quadratic form over K. If no such positive integer exists, we say that $u(K) = \infty$.

Over any field K, the quadratic form $q(x) = x^2$ is anisotropic. Over the complex numbers, any quadratic form in at least 2-variables is isotropic, so $u(\mathbb{C}) = 1$. Indeed this holds for any algebraically closed field. Moreover, we say a field is **quadratically closed** if it admits no nontrivial quadratic extension – equivalently, $K^\times = K^{\times 2}$. Then:

EXERCISE 2.14. *Let L/K be a degree n field extension. Let $b_1, \ldots, b_n$ be a K-basis for L. Define a polynomial $N(x)$ by $N_{L/K}(x_1b_1 + \ldots + x_nb_n)$ (i.e., the norm from L down to K).*
a) Show that for all $0 \neq x \in K^n$, $N(x) \neq 0$.
b) Suppose $n = 2$. Show that the equivalence class of the quadratic form $N(x)$ is well-defined independent of the chosen basis of L/K.

EXERCISE 2.15. *Let K be any field of characteristic different from 2. Show: $u(K) = 1$ iff K is quadratically closed.*

EXAMPLE 2.25. *For any $n \in \mathbb{Z}^+$, the quadratic form $q(x) = x_1^2 + \ldots + x_n^2$ is anisotropic over $\mathbb{R}$, since it is always strictly positive when evaluated at any nonzero vector. Thus $u(\mathbb{R}) = \infty$. The same holds for any* ***formally real*** *field. (However the converse is not true, e.g. a rational function field in infinitely many indeterminates over $\mathbb{C}$ has u-invariant ∞.)*

PROPOSITION 2.26. *The u-invariant of any finite field is 2.*

PROOF. Since every finite field admits a quadratic extension, it follows from Exercise 2.14 that the u-invariant is at least 2. The fact that any quadratic form in at least 3-variables over a finite field has a nontrivial zero is a special case of the Chevalley-Warning theorem. □

LEMMA 2.27. *Let K be a Henselian, discretely valued field with valuation ring R, uniformizer π, and residue field k of characteristic different from 2. Let $n \in \mathbb{Z}^+$ and $a_1, \ldots, a_n \in R^\times$, and let $0 \leq r \leq n$. Consider the quadratic forms*

$$q_1(x_1, \ldots, x_r) = a_1 x_1^2 + \ldots + a_r x_r^2$$
$$q_2(x_{r+1}, \ldots, x_n) = a_{r+1} x_{r+1}^2 + \ldots + a_n x_n^2$$
$$q(x) = q_1(x_1, \ldots, x_r) + \pi q_2(x_{r+1}, \ldots, x_n).$$

Then q is isotropic over K iff at least one of q_1, q_2 is isotropic over K.

PROOF. Clearly q_2 is isotropic iff πq_2 is isotropic. Just as clearly, if a subform of a quadratic form is isotropic, then so is the quadratic form. Thus certainly the isotropy of either q_1 or q_2 implies the isotropy of q, so it suffices to show the converse: assume q is isotropic. Then by the usual rescaling arguments there exists a *primitive vector* x such that $q(x) = 0$: that is, each coordinate of x lies in R and at least one coordinate of x is not divisible by π.
Case 1: Suppose there is $1 \leq i \leq r$ with $x_i \neq 0$. Then reducing mod p gives $q_1 \equiv 0 \pmod{p}$ and $\frac{\partial q_0}{\partial x_i} = 2a_i x_i \neq 0 \pmod{p}$, so by Hensel's Lemma q_1 is isotropic.
Case 2: Then we have that $p \mid x_i$ for $1 \leq i \leq r$, so $q_1(x_1, \ldots, x_r) \equiv 0 \pmod{p}^2$. Therefore reducing modulo p^2 and dividing by p, we see that $q_1(x_{r+1}, \ldots, x_n) \equiv 0 \pmod{p}$. Applying Hensel's Lemma as in Case 1, we see q_2 is isotropic over $\mathbb{Q}_p$. □

THEOREM 2.28. *Let K be a Henselian discretely valued field with residue field k. We suppose that the characteristic of k is different from 2. Then*

$$u(K) = 2u(k).$$

In particular, for an odd prime p, $u(\mathbb{Q}_p) = 4$.

PROOF. Let $q = q(x_1, \ldots, x_n)$ be a nonsingular quadratic form over K with $n > 2u(k)$. Then q is equivalent (under a linear change of variables) to a form $q = q_1 + \pi q_2$ as in the statement of Lemma 2.27. By our hypothesis on n, at least one of q_1, q_2 has more than $u(k)$ variables, so the reduction modulo (π) is isotropic by assumption and then the form itself is isotropic by Hensel's Lemma. Thus $u(K) \leq 2u(k)$.

Conversely, if $u(k) = r$, let $\overline{q}(x_1, \ldots, x_r)$ be an anisotropic form over k. We may lift each coefficient of $\overline{q}$ to an element of $R^\times$ and thus get a quadratic form $q(x_1, \ldots, x_r)$. Now q itself is anisotropic over K: indeed, if not, there would exist a primitive vector x such that $q(x) = 0$ and then reduction modulo (π) would show that $\overline{q}$ is isotropic. It then follows from Lemma 2.27 that the quadratic form $q(x_1, \ldots, x_n) + \pi q(x_{n+1}, \ldots, x_{2n})$ is isotropic over K. □

EXAMPLE 2.29. *Suppose that $p \equiv 3 \pmod{4}$. Then $(\frac{-1}{p}) = -1$, so $x^2 + y^2$ is anisotropic mod p. The above proof shows that $x_1^2 + x_2^2 + px_3^2 + px_4^2$ is anisotropic over $\mathbb{Q}_p$.*

EXERCISE 2.16. *Show that for every $a \in \mathbb{N}$, there exists a field K with $u(K) = 2^a$.*

EXERCISE 2.17. *a) Show that $q(x,y,z) = x^2 + y^2 + z^2$ is anistropic over $\mathbb{Q}_2$. b) For a prime p, find $a, b, c \in \mathbb{Z}$ such that $q = ax^2 + by^2 + cz^2$ is anisotropic over $\mathbb{Q}_p$.*

EXERCISE 2.18. *Show that $u(\mathbb{Q}_2) = 4$. (See* [**Lam**] *for one approach.)*

9. Roots of unity in local fields

For any field F, we denote by $\mu(F)$ the torsion subgroup of $F^\times$ – or, more colloquially, the **roots of unity** in F.

We are interested in the roots of unity of a valued field (K, v). Note that we certainly have $\mu(K) \subset R^\times$: all roots of unity have valuation 0. As usual, we can say something in this level of generality, but to get definitive results we will restrict to p-adic fields and/or Laurent series fields.

We define $\mu'(K)$ as follows: if the residue field k has characteristic 0, then $\mu'(K) = \mu(K)$. However, if the residue field k has characteristic $p > 0$, then $\mu'(K)$ is, by definition, the group of all roots of unity of K of order coprime to p.

This somewhat curious definition is justified by the following result.

PROPOSITION 2.30. *Let (K, v) be a Henselian valued field. Then the mod $\mathfrak{m}$ reduction map induces an isomorphism of groups $r' : \mu'(K) \xrightarrow{\sim} \mu(k)$.*

PROOF. As observed above, every root of unity of K lies in the valuation ring. Moreover, certainly the image of an element of finite order under a group homomorphism has finite order, so there is no doubt that there is a homomorphism $r : \mu(K) \to \mu(k)$. Note though that because – when $\mathrm{char}(k) = p > 0$ – k has no p-power roots of unity, the reduction map restricted to $\mu[p^\infty](K)$ is trivial, so we may as well restrict our attention to the complementary subgroup $\mu'(K)$.
Let $x \in \mu(k) = \mu'(k)$ have order n. Put $P(t) = t^n - 1$; then $P'(x) = nx^{n-1} \neq 0$. By Hensel's Lemma, there exists $\tilde{x} \in K$ reducing to x and such that $x^n = 1$. Since $\tilde{x}^n = 1$, the order of $\tilde{x}$ divides n; since $q(\tilde{x}) = x$, n divides the order of $\tilde{x}$, thus $\tilde{x}$ has exact order n. The surjectivity of r' follows. But moreover, suppose that the kernel of ρ' is nontrivial. Then, being a nontrivial torsion group with no elements of order p, the kernel contains an element of prime order $\ell \neq p$, i.e., there exists a primitive ℓth root of unity $\tilde{x}$ such that $r(\tilde{x}) = 1$ and therefore $r(\tilde{x}^k) = 1$ for all k. But by virtue of being a primitive ℓth root of unity, we have $\tilde{x}^{\ell-1} + \ldots + \tilde{x} + 1 = 0$ and reducing this equation modulo the maximal ideal gives $\ell = 0$, a contradiction. Therefore r' is an isomorphism. □

In particular, this shows that the group of roots of unity in $\mathbb{Q}_p$ of order prime to p is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$, hence cyclic of order $p-1$. Next we wonder whether there are any p-power roots of unity in $\mathbb{Q}_p$. If there are any such, there are primitive pth roots of unity, so that the pth cyclotomic polynomial $\Phi_p(t)$ would have a root over $\mathbb{Q}_p$. It is well-known from basic algebraic number theory that $\Phi_p(t)$ is irreducible over $\mathbb{Q}$, a textbook application of Eisenstein's criterion. As we now explain, the same application of Eisenstein's criterion in fact gives the irreducibility over $\mathbb{Q}_p$ as well. Recall: Coming back down to earth, we apply the Eisenstein Criterion to $\mathbb{Q}_p$

and $f(t) = \Phi_p(t+1)$. We have

$$f(t) = \frac{(t+1)^p - 1}{t+1-1} = t^{p-1} + \binom{p}{1} t^{p-2} + \ldots + \binom{p}{p-2} t + p.$$

Applying the Eisenstein criterion to $\mathbb{Z}_p$ and $\mathfrak{p} = (p)$, we conclude that $f(t)$ is irreducible in $\mathbb{Q}_p[t]$ hence also $\Phi_p(t) = f(t-1)$ is irreducible in $\mathbb{Q}_p$. Therefore $\mathbb{Q}_p$ does not contain a primitive pth root of unity. In conclusion:

THEOREM 2.31. *For any prime p, $\mu(\mathbb{Q}_p) \cong (\mathbb{Z}/p\mathbb{Z})^\times$.*

THEOREM 2.32. *Let K be a locally compact non-Archimedean field. Then the group $\mu(K)$ of roots of unity in K is finite.*

PROOF. Let R be the valuation ring, $\mathfrak{m}$ the maximal ideal, and $k \cong \mathbb{F}_q$ be the residue field of k, of characteristic p. By Proposition 2.30, reduction modulo $\mathfrak{m}$ induces an isomorphism

$$\mu'(K) \xrightarrow{\sim} \mu(\mathbb{F}_q) \cong (\mathbb{Z}/(q-1)\mathbb{Z}, +).$$

Thus it suffices to show that the group $\mu_{p^\infty}(K)$ of p-power roots of unity is finite. Step 1: Suppose $K = \mathbb{Q}_p$. For $a \in \mathbb{Z}^+$, let

$$\Phi_{p^a}(t) = \frac{t^{p^a} - 1}{t^{p^{a-1}} - 1} = \Phi_p(t^{p^{a-1}}).$$

Thus Φ_{p^a} is the unique monic polynomial with roots the primitive p^ath roots of unity. polynomial whose roots are the primitive p^ath roots of unity. As we did when $a = 1$ above, we put

$$g \coloneqq \Phi_{p^a}(t+1).$$

Then $g(0) = \Phi_{p^a}(1) = \Phi_p(1^{p^{a-1}}) = p$. Moreover,

$$\left((t+1)^{p^{a-1}} - 1\right) g = \left((t+1)^{p^a} - 1\right),$$

and reducing modulo p gives

$$t^{p^{a-1}} g = t^{p^a} \in \mathbb{F}_p[t]$$

or

$$g = t^{p^a - p^{a-1}} \in \mathbb{F}_p[t].$$

Thus all the terms of g except for the leading coefficient are divisible by p, so g is Eisenstein with respect to the prime ideal (p) in the UFD $\mathbb{Z}_p$. It follows that g and hence also Φ_{p^a} is irreducible over $\mathbb{Q}_p$. Thus if ζ_{p^a} is a primitive p^ath root of unity in $\overline{\mathbb{Q}_p}$ we get that

$$[\mathbb{Q}_p(\zeta_{p^a}) : \mathbb{Q}_p] = \varphi(p^a) = p^a - p^{a-1}.$$

Step 2: Let K be a p-adic field. By Step 1, if K contains a primitive p^ath root of unity then

$$[K : \mathbb{Q}_p] \geq [\mathbb{Q}_p(\zeta_{p^a}) : \mathbb{Q}_p] = \varphi(p^a).$$

Since $\varphi(p^a) \geq p^{a-1}$, certainly $\lim_{a\to\infty} \varphi(p^a) = \infty$ and thus K contains only finitely many p-power roots of unity. Step 3: Suppose $K \cong \mathbb{F}_q((t))$. In this case we have, as for every field of characteristic $p > 0$, no nontrivial p-power roots of unity. □

COROLLARY 2.33. *Let $K/\mathbb{Q}_p$ be a p-adic field, with $[K : \mathbb{Q}_p] = e(K/\mathbb{Q}_p) f(K/\mathbb{Q}_p)$.*
a) The group of roots of unity of order relatively prime to p is cyclic of order $p^f - 1$.
b) If $(p-1) \nmid e(K/\mathbb{Q}_p)$, then $\mu_{p^\infty}(K) = 1$.
c) In general $\#\mu_{p^\infty}(K) \leq p^{\mathrm{ord}_p(e)+1}$.

EXERCISE 2.19. *Prove Corollary 2.33.*

10. Nth power classes

Let $N \in \mathbb{Z}^+$. In this section we will compute $[K^\times : K^{\times N}]$ for any locally compact field of characteristic not dividing N. The Archimedean case is immediately disposed of.

EXERCISE 2.20. *Let $N \in \mathbb{Z}^+$.*
a) Show: $[\mathbb{C}^\times : \mathbb{C}^{\times N}] = 1$.
b) Show: $[\mathbb{R}^\times : \mathbb{R}^{\times N}] = \begin{cases} 1 & N \text{ odd} \\ 2 & N \text{ even} \end{cases}$.

To state the following result we will use some notation borrowed from the arithmetic of elliptic curves. Let $f : A \to Z$ be a homomorphism of commutative groups. We will denote the kernel of f by $A[f]$. (In particular, if we consider the multiplication by n homomorphism from A to itself, then $A[n]$ is the n-torsion subgroup of A.)

LEMMA 2.34. *Let $f : A \to Z$ be a homomorphism of commutative groups. Let B be a subgroup of A. Then*

$$[A : B] = [f(A) : f(B)] \cdot [A[f] : B[f]].$$

PROOF. Let g be the composite homomorphism $A \to f(A) \to f(A)/f(B)$. Then g is surjective and has kernel $B + A[f]$, so

$$A/(B + A[f]) \cong f(A)/f(B).$$

Moreover $A \supset B + A[f] \supset B$ and hence

$$(B + A[f])/B \cong A[f]/(A[f] \cap B) = A[f]/B[f].$$

Therefore

$$[A[f] : B[f]][f(A) : f(B)] = [A : B + A[f]][B + A[f] : B] = [A : B]. \qquad \square$$

LEMMA 2.35. *Let (K, v) be a discretely valued field, with valuation ring R and uniformizing element π. Let $x \in R$. Then for any $N, r \in \mathbb{Z}^+$ such that $\mathrm{char}(K) \nmid N$ and $v(N\pi^{r+1}) \geq \pi^{2r}$, we have*

$$(1 + x\pi^r)^N \equiv 1 + Nx\pi^r \pmod{N\pi^{r+1}}. \tag{8}$$

PROOF. Let p be the residue characteristic, and write $N = N'p^a$ with $\gcd(N', p) = 1$, so $N' \in R^\times$. Put $e = v(p)$. Thus $v(N) = ae$, so our assumption is that

$$ae + r + 1 = v(N\pi^{r+1}) \leq \pi^{2r} = 2r,$$

i.e., that

$$ae + 1 \leq r.$$

Now the desired conclusion is a congruence modulo $(N\pi^{r+1})$, i.e., modulo π^{ae+r+1}. Thus, by our assumption, it is enough to show that the two sides of (8) are congruent modulo π^{2r}. And this is easy:

$$(1 + x\pi^r)^N = 1 + \binom{N}{1} x\pi^r + \sum_{j=2}^{N} \binom{N}{j} x^j \pi^{rj}.$$

Since $j \geq 2$, each term in the sum is divisible by π^{2r}, qed. $\square$

THEOREM 2.36. *Let K be a field that is Henselian with respect to a normalized discrete valuation v and with finite residue field $k \cong \mathbb{F}_q$. Let R be the valuation ring, $\mathfrak{m}$ the maximal ideal, $U := R^\times$ the unit group. Let N be a positive integer not divisible by* $\mathrm{char}(K)$. *Let $\mu_N(K)$ denote the group of Nth roots of unity in K. Then:*
a) We have

$$[U : U^N] = q^{v(N)} \# \mu_N(K).$$

b) We have

$$[K^\times : K^{\times N}] = N q^{v(N)} \# \mu_N(K).$$

PROOF. a) Put $s := v(N)$, and let π be a uniformizer of K. Let r be a positive integer that is sufficiently large so that $r \geq s+1$ and so that the higher unit group U_r contains no nontrivial Nth roots of unity (cf. Exercise 2.5). The crux of the matter is the following claim:

$$U_r^N = U_{r+s}. \tag{9}$$

Step 1: We assume (9) and complete the proof.

Applying Lemma 2.34 with $A = U$, $B = U_r$, $f(x) = x^N$. Thus

$$[U : U_r] = [U^N : U_r^N] \# \mu_N(K) = [U^N : U_{r+s}] \# \mu_N(K) = \frac{[U : U_{r+s}]}{[U : U^N]} \# \mu_N(K)$$

so

$$[U : U^N] = \frac{[U : U_{r+s}]}{[U : U_r]} \# \mu_N(K) = [U_r : U_{r+s}] \# \mu_N(K).$$

By Proposition 2.12 we have

$$[U_r : U_{r+s}] = \# \mathfrak{m}^r / \mathfrak{m}^{r+s} = q^s = q^{v(N)},$$

so

$$[U : U^N] = q^{v(N)} \# \mu_N(K).$$

Step 2: By Lemma 2.35 for all $x \in R$ we have

$$(1 + x\pi^r)^N \equiv 1 + Nx\pi^r \pmod{N\pi^{r+1}}. \tag{10}$$

Putting $s = v(N)$, this gives

$$U_r^N \subset U_{r+s}.$$

Step 3: Fix $x \in R$, and put

$$P(t) := t^N - (1 + x\pi^{r+s}) \in R[t].$$

We have

$$v(P(1)) = v(x\pi^{r+s}) \geq r + s$$

and

$$v(P'(1)) = v(N \cdot 1^{N-1}) = s.$$

Since $r > s$ we have

$$v(P(1)) > v(P'(1))^2.$$

So we may apply Hensel-Newton (Theorem 1.79) with $\alpha = 1$ to get:

$$\exists \beta \in R \text{ such that } P(\beta) = 0 \text{ and } v(\beta - 1) = v(P(1)) - v(P'(1)) = r.$$

Thus $\beta^N = 1 + x\pi^{r+s}$ and $\beta \in U_r$. This shows that $U_{r+s} \subset U_r^N$.

b) Since the choice of uniformizer yields a decomposition $K^\times = U \times \mathbb{Z}$, this follows immediately from part a). □

In particular, if K is locally compact, the group $[K^\times : K^{\times N}]$ is finite for all N not divisible by $\operatorname{char} K$. In [**A**, p. 209, Thm. 5], Artin proves this result under the assumption that K contains the Nth roots of unity. In [**L-ANT**, p. 47, Prop. 6], Lang gives this result when K is a p-adic field. He says he is following [**A**]. On the one hand, his proof does not use that K has characteristic 0 but only that $\operatorname{char} K \nmid N$. On the other hand, it seems to me that his proof is incomplete: he only argues for $U_r^N \subset U_{r+s}$. Artin himself gives the other direction via a further argument using (10) and relying on the completness of K. Since earlier we proved special cases of this result using Hensel's Lemma, it is natural to try to use Hensel's Lemma, and an interesting aspect of the proof if that it uses the evaluation of $|\alpha - \beta|$ that is not a traditional part of the statement of Hensel-Newton but is present in Conrad's treatment. Using this argument instead of Artin's allows us to weaken "complete" to "Henselian."

EXERCISE 2.21. *One might wonder where the finiteness of the residue field is used: e.g. perhaps in the context of Theorem 2.36, if we drop the assumption that $k \cong \mathbb{F}_q$ we could have*

$$[K^\times : K^{\times N}] = N(\#k)^{v(N)}\#\mu_N(K)?$$

a) Show that for all $N \in \mathbb{Z}^+$ we have $[\mathbb{C}((t))^\times : \mathbb{C}((t))^{\times N}] = N$. Deduce that the answer to the above question is "no."
b) Exactly where was the finiteness of k used in the proof?

COROLLARY 2.37.
Let $(K, v, \pi, k = \mathbb{F}_q)$ be a locally compact field of characteristic different from 2.
a) If $\operatorname{char}(k) > 2$, there are exactly three quadratic extensions of K.
b) If $\operatorname{char}(k) = 2$, there are exactly $2^{[K:\mathbb{Q}_p]+2} - 1$ quadratic extensions of K.

EXERCISE 2.22. *Prove Corollary 5.11.*

Things are truly different when $K = \mathbb{F}_{p^f}((t))$ and $p \mid m$.

EXERCISE 2.23. *Let $K = \mathbb{F}_{p^f}((t))$. Show that if $p \mid m$, then $[K^\times : K^{\times m}] = \infty$.*

11. Krasner's Lemma and applications

11.1. Krasner's Lemma.

THEOREM 2.38. *(Krasner's Lemma) Let $(K, |\cdot|)$ be a Henselian non-Archimedean normed field with algebraic closure $\overline{K}$. Let $\alpha, \beta \in \overline{K}$. Write out the distinct K-conjugates of α as $\alpha = \alpha_1, \ldots, \alpha_n$. Suppose that for all $i > 1$ we have*

$$|\alpha - \beta| < |\alpha - \alpha_i|.$$

a) Then $K(\alpha, \beta)/K(\beta)$ is purely inseparable.
b) If α is separable over K, $K(\alpha) \subset K(\beta)$.

PROOF. Part b) immediately follows from part a). As for part a), it suffices to show the following: for every $K(\beta)$-algebra embedding τ of $K(\alpha, \beta)$ into an algebraic closure $\overline{K}$, $\tau(\alpha) = \alpha$. As we have seen before, the uniqueness of extended norms implies that we have, for all $i > 1$,

$$|\tau(\alpha) - \beta| = |\tau(\alpha) - \tau(\beta)| = |\alpha - \beta| < |\alpha - \alpha_i|$$

and hence

$$|\tau(\alpha) - \alpha| \leq \max|\tau(\alpha) - \beta|, |\beta - \alpha| < |\alpha - \alpha_i|.$$

Since this holds for all $i > 1$ and $\tau(\alpha)$ is a conjugate of α, we get $\tau(\alpha) = \alpha$. □

REMARK 2.39. *In fact a non-Archimedean normed field is "Krasnerian" – i.e., satisfies the conclusions of Theorem 2.38 – iff it is Henselian* [**Ri**, p. 141].

11.2. Krasner's Corollary.

EXERCISE 2.24. *Let $(K, |\cdot|)$ be an algebraically closed normed field.*
a) Let $n \in \mathbb{Z}^+$. Let $D(n)$ be the set of all degree n polynomials with coefficients in K which have n distinct roots, viewed as a subset of K^{n+1} in the evident way. Show that $D(n)$ is open in (the product topology on) K^{n+1}.
b) Suppose that K is any algebraically closed field. Show that $D(n)$ is open in K^{n+1} in the Zariski topology.
c) Show that the roots are continuous functions of the coefficients in the following sense: for all $\epsilon > 0$, there exists $\delta > 0$ such that: for any two polynomials $f(t) = \sum_n a_n t^n$ and $g(t) = \sum_n b_n t^n$ with $|a_i - b_i| < \delta$ for all i, there exist orderings of the roots $\alpha_1, ..., \alpha_n$ of f and $\beta_1, ..., \beta_n$ of g such that $|\alpha_i - \beta_i| < \epsilon$ for all i.
d) Suppose that you restrict to degree n polynomials in $D(n)$. State and prove a version of part b) which does not involve permuting the roots. (Suggestion: consider disjoint open disks about each of the roots and argue that under sufficiently small changes of the coefficients, the roots stay inside the disjoint disks.)

COROLLARY 2.40 (Krasner's Corollary). *Let K be a Henselian non-Archimedean normed field. Let $f(t) = a_n t^n + \ldots + a_1 t + a_0$ be an irreducible separable degree n polynomial, and let α be one of its roots in a fixed algebraic closure $\overline{K}$. Then there exists $\delta > 0$ such that: for all $b_0, \ldots, b_n \in K$ with $|a_i - b_i| < \delta$ for all $0 \leq i \leq n$, the polynomial $g(t) := b_n t^n + \ldots + b_1 t + b_0$ is irreducible, separable, and has a root β such that $K(\alpha) = K(\beta)$.*

PROOF. We apply Exercise 2.24 on continuity of roots of a polynomial with coefficients in a normed field in terms of the coefficients: for any $\epsilon > 0$, by taking δ sufficiently small we can ensure that the polynomial g is also separable and that its roots $\beta_1, \ldots, \beta_n$, in some ordering, each lie within ϵ of the corresponding roots $\alpha_1, \ldots, \alpha_n$ of f. Taking $\epsilon = \min_{i>1} |\alpha_1 - \alpha_i|$ and applying part b) of Krasner's Lemma to β_1, we get that $K(\alpha_1) \subset K(\beta_1)$. However, since β_1 satisfies g, a polynomial of degree n, we have

$$n \geq [K(\beta_1) : K] \geq [K(\alpha_1) : K] = n.$$

Thus $[K(\beta_1) : K] = [K(\alpha_1) : K] = n$, so $g(t)$ is irreducible and $K(\alpha_1) = K(\beta_1)$. □

THEOREM 2.41 (Generalized Krasner's Corollary). *Let K be a Henselian non-Archimedean normed field. Let $f = a_n t^n + \ldots + a_1 t + a_0 \in K[t]$ be a separable polynomial. Then there is $\delta > 0$ such that: for all $g = b_n t^n + \ldots + b_1 t + b_0 \in K[t]$ such that $|a_i - b_i| < \delta$ for all $0 \leq i \leq n$, we have an isomorphism of K-algebras*

$$K[t]/(f) \cong K[t]/(g).$$

PROOF. Let $f = \prod_{i=1}^r f_i$ with each $f_i \in K[t]$ irreducible separable, and such that $(f_i) \neq (f_j)$ for $i \neq j$. Write $f_i(t) = \prod_{i=1}^{d_i}(t - \alpha_{ij})$ for $\alpha_{ij} \in \overline{K}$. By Exercise 2.24, if δ is small enough, then g is separable and can be factored as $\prod_{i=1}^r g_i$ with each $g_i \in \overline{K}[t]$ and $g_i(t) = \prod_{i=1}^{d_i}(t - \beta_{ij})$. Again by taking δ small enough we can ensure that for all i, j, the root β_{ij} is closer to α_{ij} than to any other root of f and, symmetrically, that the root α_{ij} is closer to β_{ij} than to any other root of

g. Applying Krasner's Lemma to f, α_{ij} and β_{ij} we get that $K(\alpha_{ij}) \subset K(\beta_{ij})$. Similarly, applying it to g, β_{ij} and α_{ij} we get that $K(\beta_{ij}) \subset K(\alpha_{ij})$. Thus for all i, j we have $K(\alpha_{ij}) = K(\beta_{ij})$. Moreover, since K is Henselian, every element of $\mathfrak{g}_K = \mathrm{Aut}(\overline{K}/K)$ acts continuously on $\overline{K}$, so – after shrinking δ, if necessary – if $\sigma \in \mathfrak{g}_K$ carries α_{i1} to α_{ij}, then it must carry β_{i1} to β_{ij}. It follows that for all i, the full set of conjugates of β_{i1} is $\beta_{i1}, \ldots, \beta_{id_i}$, where $d_i = \deg f_i = \deg g_i$. Thus $g_i \in K[t]$ and for all i we have $K[t]/(f_i) \cong K[t]/(g_i)$. The Chinese Remainder Theorem gives

$$K[t]/(f) = K[t]/(f_1 \cdots f_r) \cong \prod_{i=1}^{r} K[t]/(f_i) \cong \prod_{i=1}^{r} K[t]/(g_i) \cong K[t]/(g_1 \cdots g_r) = K[t]/(g).$$

□

REMARK 2.42. *The above proof was suggested to me by M. Suwama.*

11.3. Local extensions come from global extensions.

COROLLARY 2.43. *Let $(K, |\ |)$ be a non-Archimedean normed field with completion $\hat{K}$, and let $\mathcal{L}/\hat{K}$ be a finite separable field extension of degree d. Then there exists a degree d separable field extension L/K such that $\mathcal{L} = L\hat{K}$.*

PROOF. By the Primitive Element Corollary, $\mathcal{L} \cong \hat{K}[t]/f(t)$, where $f(t) \in \hat{K}[t]$ is monic, separable of degree d. Since K is dense in $\hat{K}$, there exists a degree d polynomial $g(t) \in K[t]$ whose coefficients are all δ-close to the corresponding coefficients of $f(t)$, for any preassigned $\delta > 0$. By Corollary 2.40, for sufficiently small δ, $g(t)$ is irreducible separable of degree d and there exist roots α_1 of f, β_1 of g such that $\hat{K}(\alpha_1) = \hat{K}(\beta_1)$. It follows that $\mathcal{L} = L\hat{K}$. □

THEOREM 2.44. *(Finite Local-Global Compatibility for Extensions) Let K be a field, and let $|\cdot|_1, \ldots, |\cdot|_g$ be inequivalent norms on K. For each $1 \leq i \leq g$, let $\hat{K}_i$ be the completion of K with respect to $|\cdot|_i$. Fix a positive integer d, and for each $1 \leq i \leq g$, let A_i be a degree d separable $\hat{K}_i$-algebra (i.e., a finite product of finite degree separable field extensions of K, with $\dim_{\hat{K}_i} A_i = d$). Then there is a separable extension L/K of degree d and, for all $1 \leq i \leq g$, $\hat{K}_i$-algebra isomorphisms*

$$\Phi_i : L \otimes_K \hat{K}_i \xrightarrow{\sim} A_i.$$

EXERCISE 2.25. *Prove Theorem 2.44.*

Here is an application of Theorem 2.44 to number fields. For a field F, we denote by F^{ab} the maximal extension of F (within a fixed algebraic closure) that is algebraic and Galois with commutative Galois group.

EXERCISE 2.26. *Let $K \supsetneq \mathbb{Q}$ be a number field, and let $d \geq 2$.*
a) Show that there is a degree d extension L/K such that $L/\mathbb{Q}$ is not *Galois.*
(Suggestion: you may use that there are infinitely many prime numbers p that split completely in K. This is a consequence of the Chebotarev Density Theorem, although there are much more elementary proofs. Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be two primes of K that lie over the same rational prime p. Use Theorem 2.44 to construct L/K such that the splitting behavior over $\mathfrak{p}_1$ differs from the splitting behavior over $\mathfrak{p}_2$.)
b) Show: $K^{\mathrm{ab}} \supsetneq \mathbb{Q}^{\mathrm{ab}}$.

11.4. $\mathbb{C}_p$.

LEMMA 2.45. *Let $(K, |\cdot|)$ be a separably closed, complete (nontrivially!) normed field. Then K is algebraically closed.*

PROOF. In characteristic 0 the notions of separable closure and algebraic closure coincide, so assume that K has positive characteristic p. It is enough to show that K is perfect: let $a \in K$, and let $\alpha \in \overline{K}$ be the unique element such that $\alpha^p = a$. We must show that $\alpha \in K$. Fix $c \in K^\times$ with $v(c) > 0$. For $n \in \mathbb{Z}^+$ we consider

$$P_n(t) \coloneqq t^p - c^n t - a \in K[t].$$

Evidently we have

$$\lim_{n\to\infty} P_n = t^p - a,$$

which has α as its unique root. By continuity of the roots of a polynomial as functions of the coefficients, if for each $n \in \mathbb{Z}^+$ we choose a root α_n of P_n in $\overline{K}$, then we have $\alpha_n \to \alpha$. Since each P_n is separable and K is separably closed, we have that $\alpha_n \in K$ for all n. Since the sequence $\{\alpha_n\}_{n=1}^\infty$ is convergent in $\overline{K}$, it is Cauchy in k, but K is complete, so $\alpha = \lim_{n\to\infty} \alpha_n$ lies in K. □

COROLLARY 2.46. *Suppose $(K, |\cdot|)$ is a separably closed normed field. Then its completion $(\hat{K}, |\cdot|)$ is algebraically closed.*

PROOF. By Corollary 2.43, the field $\hat{K}$ is complete and separably closed, so by Lemma 2.45 it is algebraically closed. □

In particular, defining $\mathbb{C}_p$ to be the completion of the algebraic closure of $\mathbb{Q}_p$, the field $\mathbb{C}_p$ is complete and algebraically closed.

Corollary 2.43 can be viewed as saying that any one inert local extension of a NA normed field may be realized as the completion of a global extension. This result can be generalized in several ways: we can take work with several (but finitely many!) local extensions at once, each local extension need not be a field but only a separable algebra, and finally Archimedean places can be admitted. We get the following result, which has been of use to me in my own work (cf. [**Cl09a**, Thm. 6] and [**CGP17**, Thm. 3.2]).

11.5. Multi-complete and multi-Henselian fields.

Define a field K to be **multi-complete** if it is complete with respect to (at least) two inequivalent nontrivial norms. This seems like a strong property, and we seek to classify multi-complete fields.

Example: the complex field $\mathbb{C}$ is multi-complete. On the one hand $\mathbb{C}$ is complete with respect to the standard Archimedean norm. On the other hand, for any prime p, let $\mathbb{C}_p$ be the completion of the algebraic closure of $\mathbb{Q}_p$ with the p-adic norm. By Corollary 2.46, $\mathbb{C}_p$ is complete and algebraically closed. It is easy to see that $\#\mathbb{C}_p = \#\mathbb{C}$. By pure field theory – e.g. [**C:FT**, Cor. 78] – it follows that we have an isomorphism of abstract fields $\mathbb{C} \cong \mathbb{C}_p$.

EXERCISE 2.27. *What is the cardinality of the set of pairwise inequivalent norms on $\mathbb{C}$ with respect to which $\mathbb{C}$ is complete?*

EXERCISE 2.28. *Suppose that K is a field which is complete with respect to an Archimedean norm $||\cdot||_1$ and also an inequivalent norm $||\cdot||_2$. Show that $K \cong \mathbb{C}$.*

Thus in our study of multi-complete fields we may, and shall, restrict to non-Archimedean norms, or equivalently, to valuations.

Here is the main theorem for multi-complete fields.

THEOREM 2.47. *(Schmidt [**Sc33**]) A multi-complete field is algebraically closed.*

From this we can deduce a classification result for multi-complete fields.

COROLLARY 2.48. *(Schmidt) For a field K, the following are equivalent:*
(i) K is multi-complete.
(ii) K is algebraically closed and complete with respect to a nontrivial valuation.
(iii) K is algebraically closed and $(\#K) = (\#K)^{\aleph_0}$.

PROOF. By Theorem 2.47, (i) $\implies$ (ii). Recall from Exercise 2.30.5 that a field which is complete with respect to a nontrivial norm satisfies $\#K = (\#K)^{\aleph_0}$, so (ii) $\implies$ (iii). Conversely, if K is algebraically closed and satisfies the cardinality condition, then K_v is complete, algebraically closed (cf. Proposition 3.22 below) and of uncountably cardinality equal to that of K, so $K_v \cong K$. Thus (iii) $\equiv$ (ii). Finally, assume that K is algebraically closed and complete with respect to a nontrivial valuation v. Let $t \in K$ have negative valuation and which is transcendental over the prime subfield of K. (If every transcendental element t had non-negative valuation, then for any element of a of K, $v(a) = v(t+a-t) \geq \min v(t+a, -t) \geq 0$, so every element of K has non-negative valuation, and thus v is trivial.) By standard field theory – cf. e.g. the proof of [**C:FT**, Thm. 80], the automorphim group of the algebraically closed field K acts transitively on the set of all transcendence bases for K over its prime subfield. In particular, there exists an automorphism σ such that $\sigma(t) = \frac{1}{t}$, and such an automorphism is evidently discontinuous for the valuation topology. Thus $\sigma^* v : x \mapsto v(\sigma(x))$ is an inequivalent complete valuation, i.e., K is multi-complete. □

It remains to prove Theorem 2.47. We will introduce a variant which we claim is more natural and more penetrating (in particular, it will imply Theorem 2.47). Namely, we define a field K to be **multi-Henselian** if it is Henselian with respect to two inequivalent nontrivial valuations. Here is the main theorem of this section.

THEOREM 2.49. *(Kaplansky-Schilling [**KS**]) A multi-Henselian field is separably closed.*

PROOF. Let K be a field that is Henselian with respect to inequivalent, nontrivial valuations v_1 and v_2. Let L/K be a finite degree separable field extension. By the Primitive Element Corollary we have $L \cong K[t]/(P_1(t))$ for a monic, irreducible seaprable $P_1 \in K[t]$, say of degree d. Our task is to show that $d = 1$.

By weak approximation the diagonal image of K in $K_{v_1} \times K_{v_2}$ is dense.

On the one hand, by Krasner's Lemma, there exists $\epsilon > 0$ such that any monic polynomial $Q \in K_{v_1}[t]$ each of whose coefficients is ϵ-close to the corresponding coefficients of P is also irreducible of degree d.

On the other hand, let $P_2(t) = t(t+1)^{d-1}$. Then $P_2(t)$ is monic of degree d, and its reduction modulo v_2 is (of course) $t(t+1)^{d-1} \in k_{v_2}[t]$. We may therefore apply Hensel's Lemma to P_2 to see that it has a root in K. Well, that's silly – of course it

has a root: $P_2(0) = 0$. But moreover, if $Q(t) \in K[t]$ is any polynomial sufficiently close to P_2 such that the coefficients of $P_2 - Q$ all have positive valuation, then the reduction of Q modulo the maximal ideal is also equal to $t(t+1)^{d-1}$. Therefore Hensel's Lemma applies equally well to show that Q has a rational root.

The endgame is thus: by weak approximation, we may choose a monic degree d polynomial Q which is, at the same time, sufficiently v_1-adically close to P_1 to be irreducible and sufficiently v_2-adically close to P_2 so as to have a rational root. Of course an irreducible polynomial with a rational root must have degree 1. □

EXERCISE 2.29. *(Kaplansky-Schilling* [**KS**]*) Deduce the following strengthening of Schmidt's theorem: Let v_1 and v_2 be inequivalent nontrivial valuations on a field K. Suppose that K is complete with respect to v_1 and Henselian with respect to v_2. Then K is algebraically closed of at least continuum cardinality.*

Similarly, we may classify all multi-Henselian fields, and this is simpler in that no conditions on the cardinality intervene.

PROPOSITION 2.50. *Let K be a separably closed field, and let v be a valuation on K. Then K is Henselian with respect to v.*

PROOF. By definition of Henselian, we must show that if L/K is a finite degree field extension, then there is a unique valuation on L extending v. If $L = L_n \supset L_{n-1} \supset \ldots \supset L_0 = K$ is a tower of finite degree purely inseparable extensions, then if every valuation v_i on L_i extends uniquely to a valuation on L_{i+1}, then certainly the valuation $v = v_0$ on K extends uniquely to L. Therefore we may assume that L/K is purely inseparable and *primitive*, i.e., generated by a single root of a purely inseparable polynomial, i.e., $L = K[t]/(P)$, where P has only one distinct root in an algebraic closure $\overline{K}$ of K.

Now recall Theorem 2.5: if (K, v) is a valued field and L/K is a finite degree field extension, there is a bijective correspondence betweeen valuations on L extending v and prime ideals in the Artinian K_v-algebra $L \otimes_K K_v$. With our choice of $L = K[t]/(P(t))$, with P purely inseparable, we have $L \otimes_K K_v \cong K_v[t]/(P(t))$. But since P is purely inseparable, it has only one root in an algebraic closure, hence also in any field extension. Therefore over $K_v(t)$ we have a factorization $P = Q^e$, where Q is again irreducible, so $L \otimes_K K_v \cong K_v[t]/(Q^e)$, which is a local algebra with unique maximal ideal (Q). Therefore the extension of v to L is unique. □

PROPOSITION 2.51. *Let K be a separably closed field that is* not *the algebraic closure of a finite field. Then K is multi-Henselian: indeed it is Henselian with respect to infinitely many pairwise inequivalent distinct valuations.*

PROOF. By Proposition 2.45, K is Henselian with respect to all of its valuations. The remainder is just a rehash of some already proved valuation theory: if K is an algebraic extension of a finite field, then it admits only the trivial valuation. Otherwise, K admits at least one nontrivial valuation. Indeed, if K has characteristic 0 then it contains $\mathbb{Q}$ and hence has p-adic valuations for all p, each of which extends, by Theorem 2.1, to a valuation of K; this gives infinitely many inequivalent valuations. Otherwise K has characteristic $p > 0$ and thus contains $\mathbb{F}_p(t)$, a field which has infinitely many inequivalent valuations by Theorem 1.14. □

Remark: This is [**KS**, Theorem 2], except that the need to exclude the algebraic closure of a finite field is overlooked there.

EXERCISE 2.30. *Show that a multi-Henselian field is Henselian for* uncountably many *pairwise inequivalent valuations!*

EXERCISE 2.31. *Give an example of a multi-Henselian field that is not multi-complete.*

Finally, we give an application of these results.

THEOREM 2.52. *(Continuity of Automorphisms) Let (K, v) be a field which is Henselian for a nontrivial valuation v. Suppose that* either
(i) K is not *separably closed, or*
(ii) K is complete with respect to v and is not *algebraically closed.*
Then every automorphism of K is continuous with respect to the valuation topology.

PROOF. Let σ be an automorphism of K. By Exercise 2.31, σ is continuous with respect to the valuation topology iff σ is an automorphism of the valued field (K, v), i.e., for all $x \in K$, we have $\sigma^* v = v$, where $\sigma^* v$ is the valuation $x \mapsto v(\sigma(x))$. It is easy to see that since v is Henselian, so is $\sigma^* v$ and that v is complete iff $\sigma^* v$ is complete (cf. Exercise 2.32). Therefore if σ were *not* continuous with respect to the valuation topology, then v and $\sigma^* v$ would be inequivalent nontrivial valuations on K, i.e., K is multi-Henselian. Thus by Kaplansky-Schilling, K is separably closed. Similarly, if K is complete with respect to v, then it is multi-complete and thus, by Schmidt's theorem, algebraically closed, qed. □

This immediately implies the following result.

COROLLARY 2.53. *Let $K/\mathbb{Q}_p$ be a degree d field extension. Then $\#\operatorname{Aut}(K) \leq d$. In particular, $\mathbb{Q}_p$ is* rigid*, i.e., has no nontrivial field automorphisms.*

11.6. The number of degree m extensions of a locally compact field.

THEOREM 2.54. *Let K be a locally compact field, and let $m \in \mathbb{Z}^+$ be such that* $\operatorname{char}(K)$ *does not divide m. Then the set of degree m extensions of K inside a fixed algebraic closure of K is finite.*

PROOF. We know that there is a unique unramified extension of each degree, so by an easy dévissage argument we are reduced to proving the result for totally ramified extensions. For this we use Theorem 2.11: every totally ramified extension L/K of degree m is separable and of the form $K[t]/(P(t))$ for an Eisenstein polynomial $P(t) \in R[t]$: that is,

$$P(t) = t^m + a_{m-1}t^{m-1} + \ldots = a_1 t + a_0 \in R[t],\ a_i \in \mathfrak{m}\ \forall 0 \leq i \leq n-1,\ a_0 \notin \mathfrak{m}^2.$$

The mapping $P \mapsto (a_0, \ldots, a_{m-1})$ gives a bijection from the set of all degree m polynomials with R coefficients to the compact space R^m. Define the **Eisenstein locus** $\mathcal{E}_m \subset R^m$ to be the set of all Eisenstein polynomials. Then $\mathcal{E}_m$ is closed (in fact also open) in R^m and is thus compact. Moreover, every point of $\mathcal{E}_m$ corresponds to an irreducible, separable polynomial of degree n. By Corollary 2.40, to each point $P \in \mathcal{E}_m$ there is an open disk D_P such that for any two roots α and β of any two polynomials in D_P, the field extensions $K(\alpha)$ and $K(\beta)$ are conjugate. (With more care, we could choose roots so that they are the same, but since finiteness of the number of field extensions up to conjugacy certainly implies finiteness of the number of field extensions, it seems simplest not to worry about this.) Now, by compactness, $\mathcal{E}_m$ can be covered by finitely many such disks $D_{P_1}, \ldots, D_{P_N}$, such that on each disk we get a field extension (up to conjugacy) $K(\alpha_1), \ldots, K(\alpha_N)$. It follows that

every Eisenstein polynomial of degree m generates a field extension conjugate to $K(\alpha_i)$ for some $1 \leq i \leq N$, so that there are only finitely many degree m totally ramified extensions of K up to conjugacy, hence only finitely many overall. □

Exercise 2.23 above shows that if $q = p^a$, then $K = \mathbb{F}_q((t))$ has infinitely many extensions of degree p. Probably you solved this exercise by constructing extensions of the form $K(x^{\frac{1}{p}})$, i.e., purely inseparable extensions. More surprisingly there are also infinitely many separable degree p extensions of $\mathbb{F}_q((t))$.

Indeed, let K be any field of characteristic p. Define the Artin-Schreier isogeny $\wp_p : K \to K$, $x \mapsto x^p - x$. The point is that this is a homomorphism $(K, +) \to (K, +)$ whose kernel is $\mathbb{F}_p$. By Artin-Schreier theory [**C:FT**, §9], every separable degree p extension in characteristic p comes from adjoining the root of an Artin-Schreier polynomial $t^p - t - a = 0$. The irreducibility of the polynomial is equivalent to its having a root, i.e., to a being in the image of the Artin-Schreier isogeny. Moreover, there are infinitely many separable p-extensions iff the quotient $K/\wp_p(K)$ is infinite. But this is true for $K = k((t))$ and any field k of positive characteristic. Indeed, for $n \in \mathbb{Z}^+$ and prime to p, the elements $\frac{1}{t^n}$ give rise to distinct cosets of $\wp_p(K)$. Explicitly, if $n \neq n'$, there does not exist $f \in k((t))$ such that $\frac{1}{t^n} - \frac{1}{t^{n'}} = f^p - f$: exercise!

What about the number of totally ramified degree m extensions of a local field?

Exercise 2.32. *Let K be a non-Archimedean local field, and let $m \in \mathbb{Z}^+$ be prime to the residue characteristic of K. Show: there are precisely m totally ramified extensions of K of degree m.*

Theorem 2.55 (Serre). *Let K be non-Archimedean and locally compact, with residual cardinality q. For $m \in \mathbb{Z}^+$, let Σ_m be the set of all totally ramified extensions of degree n of K contained in a fixed separable closure. For $L \in \Sigma_m$, put*

$$c(L) = d(L) - m + 1,$$

where $d(L)$ is the valuation of the discriminant of L/K. Then

$$\sum_{K \in \Sigma_m} \frac{1}{q^{c(L)}} = n.$$

Proof. See [**Se78**]. □

Note that this sum is infinite when $n = p = \mathrm{char}(K) > 0$!

For more recent work on this topic, see [**Ke07**] and [**Bh07**].

12. Autoduality of locally compact fields

Let G be a locally compact commutative group. We define its **character group** $G^\vee = \mathrm{Hom}_c(G, S^1)$, i.e., the group of all *continuous* homomorphisms from G to the unit circle S^1 (viewed as a subgroup of $(C^\times, \cdot)$). However, we wish $G^\vee$ to itself have the structure of a topological group. Given topological spaces X and Y, there is a ubiquitous reasonable topology to put on the space $\mathcal{C}(X, Y)$ of all continuous maps from X to Y. It is defined as follows: for K a compact subset of X and U an open subset of Y, let $[K, U) := \{f \in \mathcal{C}(X, Y) \mid f(K) \subset U\}$.

EXERCISE 2.33. *For $x \in \mathbb{Q}_p$, let n be the least non-negative integer such that $p^n x \in \mathbb{Z}_p$. Let r be such that $r \equiv p^n x \pmod{p^n}$. Put $\Psi(x) = e^{2\pi i r/p^n}$.*
a) Show: $\Psi : (\mathbb{Q}_p, +) \to (S^1, \cdot)$ is a continuous homomorphism, i.e., $\Psi \in \mathbb{Q}_p^\vee$.
b) Show that $\ker(\Psi) = \mathbb{Z}_p$. In particular, Ψ is nontrivial.

EXERCISE 2.34. *Write $x \in \mathbb{F}_p((t))$ as $x = \sum_{n=r}^\infty a_n t^n$. Define $\Psi(x) = e^{(2\pi i)a_{-1}/p}$.*
a) Show that $\Psi \in \mathbb{F}_p((t))^\vee$.
b) Compute the kernel of Ψ and thereby show that it is nontrivial.

EXERCISE 2.35. *Let L/K be a finite separable extension of non-Archimedean local fields. Suppose that Ψ_K is a nontrivial character of K. Show that $x \in L \mapsto \Psi_K(\mathrm{Tr}_{L/K}(x))$ defines a nontrivial character of L, say Ψ_L.*

PROPOSITION 2.56. *(Classification of characters) Let K be a nondiscrete locally compact field, and let Ψ be any nontrivial element of $K^\vee$, i.e., Ψ is an additive to multiplicative homomorphism $\Psi : (K, +) \to (S^1, \cdot)$ such that $\Psi(x) \neq 1$ for at least one $x \in K$.*
a) For any $a \in K$, the map $\chi_a : K \to S^1$ by $x \mapsto \Psi(ax)$ gives a character of K.
b) The character χ_a is trivial iff $a = 0$.
c) The mapping $a \mapsto \chi_a$ defines a continuous injection $\Phi : K \hookrightarrow K^\vee$.
d) For all $b \in K$, $\chi_a(b) = 1$ for all $a \in K \iff b = 0$. It follows that $\Phi(K)$ is dense.
e) $\Phi(K)$ is a complete, hence closed, subgroup of K.
f) It follows that $\Phi : K \to K^\vee$ is an isomorphism of topological groups.

EXERCISE 2.36. *Prove Proposition 2.56.*

13. Structure theory of CDVFs

We now specialize to the following situation: let $(K, |\cdot|)$ be a complete, non-Archimedean field whose valuation ring R is a DVR and whose residue field k is perfect. Under these hypotheses we can give a much more penetrating analysis of the structure of the absolute Galois group $\mathfrak{g}_K = \mathrm{Gal}(K^{\mathrm{sep}}/K)$ and also of the multiplicative group $K^\times$.

Recall that a finite extension L/K is **unramified** if $e(L/K) = 1$; equivalently, $f(L/K) = [L : K]$. (Note that we are using our assumption of the perfection of k here, for otherwise we would need to add the condition that the residual extension l/k is unramified.) An algebraic extension L/K is unramified if all of its finite subextensions are unramified.

A finite extension L/K is **totally ramified** if $e(L/K) = [L : K]$; equivalently, $l = k$. An algebraic extension L/K is totally ramified if each finite subextension if totally ramified; equivalently, $l = k$.

Let p be the characteristic exponent of the residue field k. (In other words, when k has positive characteristic, we take p to be the characteristic; when k has characteristic 0, we take $p = 1$.)

Here is a new definition: a finite extension L/K is **tamely ramified** if $e(L/K)$ is prime to p. An algebraic extension is tamely ramified if every finite subextension is

tamely ramified. Note that in particular every unramified extension is tamely ramified, so perhaps more accurate terminology would be "at worst tamely ramified", but the terminology we have given is standard. Note also that if $\mathrm{char}(k) = 0$ then *every algebraic extension* of K is tamely ramified.

An extension L/K is **totally tamely ramified**, or **TTR**, if it is both totally ramified and tamely ramified.

Both unramified and tamely ramified extensions are **distinguished** classes of field extensions in the sense of Lang, as we now explain. A class of field extensions $\mathcal{C} = \{L/K\}$ is said to be distinguished if it satisfies the following two conditions:

(DE1) (Tower condition): if K/F and L/K are both in $\mathcal{C}$, then L/F is in $\mathcal{C}$.
(DE2) (Base change condition): suppose E, F, K are subfields of a common field, and $F \subset K$, $F \subset E$ and $K/F \in \mathcal{C}$. Then $EK/E \in \mathcal{C}$.

Exercise 2.37. *Show that (DE1) and (DE2) imply the following:*
(DE3) Suppose K, L_1, L_2 are subfields of a common field, with K contained in both L_1 and L_2 and that $L_1/K,\ L_2/K \in \mathcal{C}$. Then $L_1L_2/K \in \mathcal{C}$.

Examples: finite extensions; separable extensions; purely inseparable extensions; finitely generated extensions; purely transcendental extensions.

Important non-examples: normal extensions, Galois extensions: they satisfy (DE2) but not (DE1).

Now we state some of the main results we will prove later in this chapter.

Theorem 2.57. *Let K be a CDVF with perfect residue field k. Inside the class of all algebraic extensions of K, we have*
a) The class of unramified extensions is a distinguished class.
b) The class of tamely ramified extensions is a distinguished class.

Note that the tower property of unramified and tamely ramified extensions follows directly from the definition, since ramification indices multiply in towers. The base change property is less obvious, and for this we will need more explicit information about the structure of unramified and tamely ramified extensions, coming up soon!

Example: Totally ramified and totally tamely ramified extensions need *not* form a distinguished class. For instance, let $K = \mathbb{Q}((x))$, let $n \geq 3$, and consider the Eisenstein polynomial $f(t) = t^n - x$. The extension $L = K[t]/(f)$ is totally tamely ramified. It is (of course) separable, but it is not normal: rather, the normal closure is $M = K(x^{\frac{1}{n}}, \zeta_n)$, which contains the nontrivial unramified extension $K(\zeta_n)/K$.

Because the unramified extensions form a distinguished class, there is a unique maximal unramified extension – namely, the compositum of all finite degree totally unramified extensions, K^{unr}. The residue field of K^{unr} is $\overline{k}$. The extension $K^{\mathrm{sep}}/K^{\mathrm{unr}}$ is (necessarily) Galois and totally ramified. The extension K^{unr}/K is also Galois. Moreover, we have a short exact sequence of Galois groups

$$1 \to \mathfrak{g}_{K^{\mathrm{unr}}} \to \mathfrak{g}_K \xrightarrow{\rho} \mathrm{Gal}(\overline{k}/k) \to 1.$$

The map ρ is defined as follows: since every element $\sigma \in \mathfrak{g}_K$ is continuous, it preserves the valuation ring R and also the maximal ideal $\mathfrak{m}$ and therefore induces an automorphism $\rho(\sigma)$ of $R/\mathfrak{m}$. This short exact sequence follows from passage to the limit of the special case of the inertia group / decomposition group / residual extension short exact sequence that we get from a finite Galois extension S/R of Dedekind domains and primes $\mathcal{P}|\mathfrak{p}$.

Similarly, because the tamely ramified extensions form a distinguished class, there is a unique maximal tamely ramified extension, K^{tame} of K, which is Galois over K. This gives rise to a short exact sequence of Galois groups

$$1 \to \mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}}) \to \mathrm{Gal}(K^{\mathrm{tame}}/K) \to \mathrm{Gal}(K^{\mathrm{unr}}/K) = \mathfrak{g}_K \to 1.$$

In fact, the group $\mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}})$ is the easiest to understand.

THEOREM 2.58. *We have* $\mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}}) \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$.

This will also follow from the structure theory of tamely ramified extensions.

An extension is called **wildly ramified** if it is not tamely ramified. The remaining piece of the Galois group $\mathrm{Gal}(K^{\mathrm{sep}}/K^{\mathrm{tame}})$ describes the "purely wildly ramified" extensions. In general, this is the most complicated and scariest part of the absolute Galois group of a CDVF, but there is one important fact which comes for free:

13.1. Tamely ramified extensions. Let K be a Henselian discretely valued field with valuation ring R, normalized valuation v and residue field k of characteristic $p \geq 0$. We extend the valuation v to $\overline{K}$. A finite degree extension L/K is **tamely ramified** if $p \nmid e(L/K)$. We say that L/K is **totally tamely ramified** if it is tamely ramified and $e(L/K) = [L : K]$.

PROPOSITION 2.59. *Let e be a positive integer not divisible by p. Let $a \in R\backslash\{0\}$, and let $\alpha \in \overline{K}$ be a root of $t^e - a$. Then:*
a) The extension $K(\alpha)/K$ is tamely ramified.
b) If $\gcd(e, v(a)) = 1$, then the exension $K(\alpha)/K$ is totally ramified.

PROOF. a) Write $a = \pi^v u$ with π a uniformizer of K and $u \in R^\times$. Let $\zeta_e \in \overline{K}$ be a primitive eth root of unity, and let $u^{\frac{1}{e}}$, $\pi^{\frac{1}{e}}$ be eth roots of u and π in $\overline{K}$. Then

$$K(\alpha) \subset K(\zeta_e, u^{\frac{1}{e}}, \pi^{\frac{1}{e}}).$$

Since $p \nmid e$, the extension $F \coloneqq K(\zeta_e, u^{\frac{1}{e}})$ is unramified over K, so π is still a uniformizer of F. So the polynomial $t^e - \pi$ is Eisenstein at the maximal ideal of the valuation ring of F and thus the exension $F(\pi^{\frac{1}{e}})/F$ is totally ramified of degree d and thus totally tamely ramified. It follows that

$$e(K(\alpha)/K) \mid e(K(\zeta_e, u^{\frac{1}{e}}, \pi^{\frac{1}{e}})/K) = e,$$

so $K(\alpha)/K$ is tamely ramified.
b) Since $\alpha^e = a$, we have $v(\alpha) = \frac{v(a)}{e}$. Thus if $\gcd(e, v(a)) = 1$ then the subgroup of $v(\overline{K}^\times) = (\mathbb{Q}, +)$ generated by $v(\alpha)$ is $\frac{1}{e}\mathbb{Z}$. Since $[K(\alpha) : K] \leq e$, we must have that $K(\alpha)/K$ has degree e and is totally ramified. □

THEOREM 2.60. *Let L/K be totally tamely ramified, with $[L : K] = e(L/K) = e$. Then there is a uniformizer π of K and a uniformizer Π of L such that $\Pi^e = \pi$. In particular, $L \cong K[t]/(t^e - \pi)$.*

PROOF. Let S be the valuation ring of L and let $\mathcal{P}$ be the maximal ideal of S. Fix a uniformizing element ϖ of K. Let β a uniformizing elment of L, i.e., $v(\beta) = \frac{1}{e}$. We may write

$$\beta^e = \varpi u$$

with $u \in S^\times$. Because L/K is totally ramified, the residual extension is trivial, and thus there is $u_0 \in R^\times$ such that $u \equiv u_0 \pmod{\mathcal{P}}$. Put

$$\pi \coloneqq \varpi u_0.$$

Then $x \coloneqq \frac{u-u_0}{u_0} \in \mathcal{P}$ is such that

$$\beta^e = \varpi u = \varpi u_0 + (\varpi u_0)\frac{u-u_0}{u_0} = \pi + \pi x,$$

and thus we have

$$v(\beta^e - \pi) > v(\pi) = 1.$$

Put $f \coloneqq t^e - \pi \in K[t]$, and let $\alpha_1, \dots, \alpha_e$ be its roots. Then

$$\sum_{i=1}^{e} v(\beta - \alpha_i) = v(f(\beta)) = v(\beta^e - \pi) > v(\pi) = 1.$$

On the other hand, for all $1 \le i \le e$ we have $v(\alpha_i) = \frac{1}{e}$. Hence, after relabelling the roots if necessary we get

$$v(\beta - \alpha_1) > \frac{1}{e}.$$

On the other hand we have

$$\forall 2 \le j \le n,\ v(\alpha_1 - \alpha_j) \ge \min v(\alpha_1), v(\alpha_j) = \frac{1}{e}$$

and

$$\frac{e-1}{e} = (e-1)v(\alpha_1) = v(f'(\alpha_1)) = \sum_{i=2}^{e} v(\alpha_1 - \alpha_i) \ge \frac{e-1}{e},$$

and thus

$$\forall 2 \le j \le n,\ v(\alpha_1 - \alpha_j) = v(\alpha_1).$$

Krasner's Lemma now applies to give $K[t]/(t^e - \pi) \cong K(\alpha_1) \subset K(\beta)$. Since both $K(\alpha_1)$ and $K(\beta)$ have degree e over K, we have $K(\alpha_1) = K(\beta)$. □

COROLLARY 2.61. *The tamely ramified extensions of a CDVF form a distinguished class.*

PROOF. Since both unramified extensions and totally tamely ramified extensions have the tower property, so do tamely ramified extensions. It remains to see that the base change of a tamely ramified extension is tamely ramified. Again, by splitting a tamely ramified extension into an unramified extension followed by a totally tamely ramified extension, it suffices to show that the base change of a totally tamely ramified extension is tamely ramified. In view of Theorem 1, we must show that if E/K is any algebraic extension and π is any uniformizer of K, then for any e prime to the residue characteristic p (which we may assume to be positive, otherwise there is nothing to show), the extension $E(\pi^{\frac{1}{e}})/E$ is tamely ramified. Here we need to be a bit careful: by $\pi^{\frac{1}{e}}$ we mean *any root* of the separable polynomial $t^e - \pi$ in $\overline{K}$. In fact it is easier (and sufficient!) to see that the extension $E(\pi^{\frac{1}{e}}, \zeta_e)/E$ is tamely ramified, for this is a Galois extension, namely the splitting field of $t^e - \pi$. As we have seen, adjoining the eth roots of unity gives an unramified extension,

and then once we have the eth roots of unity in the ground field, Kummer theory applies to show that $[E(\pi^{\frac{1}{e}}, \zeta_e) : E(\zeta_e)]$ is the order of π in $E^\times/E^{\times e}$, hence divisible by e and therefore prime to p. □

THEOREM 2.62. *Suppose that K is a Henselian DVF with **algebraically closed** residue field k of characteristic exponent p. Then there exists, for each positive integer e prime to p, a unique degree e tamely ramified extension L_e/K, obtained by taking the eth root of any uniformizing element of K. Moreover, we have $K^{\mathrm{tame}} = \bigcup_e L_e$ and $\mathrm{Gal}(K^{\mathrm{tame}}/K) \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$.*

PROOF. Our assumption $k = \overline{k}$ implies that K contains all roots of unity of order prime to p and also that all extensions are totally ramified, so any tamely ramified extension is totally tamely ramified. Thus Theorem 2.60 applies to show that every degree e tamely ramified extension L/K is of the form $K[\pi^{\frac{1}{e}}]$ for some uniformizer π of K. Conversely, for any uniformizer π we certainly do get a degree e (hence tamely ramified) extension in this way. So what we wish to show is that for any two uniformizers π and π' we have $K[\pi^{\frac{1}{e}}] = K[\pi'^{\frac{1}{e}}]$. By Kummer theory, this occurs iff $\pi \equiv \pi' \pmod{K^{\times e}}$. However, since k is algebraically closed, every element of $k^\times$ is an eth power. The usual Hensel's Lemma argument now shows that every unit in the valuation ring of K is an eth power, in particular π/π' is an eth power. Now let $L_e = K[\pi^{\frac{1}{e}}]$ be the unique degree e extension of K. Again by basic Kummer theory, we have $\mathrm{Gal}(L_e/K) \cong \mathbb{Z}/e\mathbb{Z}$. If $e \mid e'$ then we have natural surjections $\mathrm{Gal}(L_{e'}/K) \to \mathrm{Gal}(L_e/K)$, and one easily checks that the following diagram commutes,

$$\mathrm{Gal}(L_{e'}/K) \xrightarrow{\sim} \mathbb{Z}/e'\mathbb{Z}$$

$$\mathrm{Gal}(L_e/K) \xrightarrow{\sim} \mathbb{Z}/e\mathbb{Z},$$

where the second vertical map is the usual quotient. It follows that $\mathrm{Gal}(K^{\mathrm{tame}}/K) \cong \varprojlim \mathbb{Z}/e\mathbb{Z} = \prod_{\ell \neq p} \mathbb{Z}_\ell$. □

COROLLARY 2.63. *Supose that K is a Henselian DVF with perfect residue field k of characteristic exponent p. Then for each positive integer e that is prime to p, there is a unique degree e tamely ramified extension L_e/K^{unr}, obtained by taking the eth root of any uniformizing element of K^{unr}. Moreover we have $K^{\mathrm{tame}} = \bigcup_e L_e$ and $\mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}}) \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$.*

EXERCISE 2.38. *Prove Corollary 2.63. (This is just a check on your understanding of unramified extensions.)*

13.2. Wildly ramified extensions.

THEOREM 2.64. *The wild ramification group $\mathrm{Gal}(K^{\mathrm{sep}}/K^{\mathrm{tame}})$ is a pro-p-group.*

Indeed, every finite quotient is purely wildly ramified, therefore has p-power order.

13.3. A Filtration on the absolute Galois group.

To summarize, let K be a Henselian, discretely valued field. Then we have split up the Galois extension K^{sep}/K into three pieces by introducing K^{unr}/K, the maximal unramified extension and $K^{\mathrm{tame}}/K^{\mathrm{unr}}$, the maximal totally tamely ramified

extension. Corresponding to the tower $K^{\mathrm{sep}}/K^{\mathrm{tame}}/K^{\mathrm{unr}}/K$ we get a **filtration** by normal subgroups

$$1 \subset \mathrm{Gal}(K^{\mathrm{sep}}/K^{\mathrm{tame}}) \subset \mathrm{Gal}(K^{\mathrm{sep}}/K^{\mathrm{unr}}) \to\subset \mathrm{Gal}(K^{\mathrm{sep}}/K).$$

There are useful things to say about each of the successive quotients of this filtration.

The bottom piece of the filtration is $\mathrm{Gal}(K^{\mathrm{unr}}/K)$. As we showed in §X.X, reduction modulo the maximal ideal gives a canonical isomorphism from this group to the absolute Galois group $\mathfrak{g}_k = \mathrm{Gal}(k^{\mathrm{sep}}/k)$ of the residue field k. In particular, if k is finite, then via the Frobenius automorphism we have canonically $\mathrm{Gal}(K^{\mathrm{unr}}/K) = \hat{\mathbb{Z}}$, a very well understood group.

The middle piece of the filtration is $\mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}})$, which is the maximal tamely ramified extension *of* K^{unr}. As we discussed, we have a noncanonical isomorphism $\mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}}) \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$.

The top piece $\mathrm{Gal}(K^{\mathrm{sep}}/K^{\mathrm{tame}})$ is trivial if $\mathrm{char}(k) = 0$ and is an infinite pro-p-group if $p > 0$: indeed for any uniformizer π of K and all $n \in \mathbb{Z}^+$, the polynomial $t^{p^n} - \pi$ is Eisenstein and hence the corresponding extension has ramification index p^n, so the polynomial remains irreducible over K^{tame}.

We list some immediate consequences of this analysis of the filtration.

THEOREM 2.65. *The absolute Galois group $\mathfrak{g}_K$ is pro-solvable iff the absolute Galois group $\mathfrak{g}_k$ of the residue field is pro-solvable. In particular, this occurs when the residue field k is finite.*

THEOREM 2.66. *Let $K = \mathbb{C}((t))$. Then the algebraic closure of K is the Puiseux series field $\bigcup_{n \in \mathbb{Z}^+} K(t^{\frac{1}{n}})$ and $\mathfrak{g}_K \cong \hat{\mathbb{Z}}$.*

PROOF. Indeed, since the residue field is algebraically closed, $K^{\mathrm{unr}} = K$. Moreover, since the residue characteristic is zero, there are no wildly ramified extensions: $K^{\mathrm{sep}} = \overline{K} = K^{\mathrm{tame}}$. Therefore $\mathrm{Gal}(\overline{K}/K) = \mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}}) = \prod_\ell \mathbb{Z}_\ell = \hat{\mathbb{Z}}$. □

Now let us go a little deeper and determine the action of $\mathfrak{g}_k$ on $\prod_{\ell \neq p} \mathbb{Z}_\ell$. First we recall the general procedure for obtaining such an action: let A be a commutative normal subgroup of a group G, with quotient Q:

$$1 \to A \to G \xrightarrow{q} H \to 1.$$

Then we can define a homomorphism $\rho : H \to \mathrm{Aut}(A)$ as follows: take $h \in H$, lift to any $\tilde{h}$ in G, and define $\rho(h)(a) = \tilde{h}a\tilde{h}^{-1}$. First note that the given element maps under the quotient map q to $hq(a)h^{-1} = h \cdot 1 \cdot h^{-1} = 1$, so indeed $\rho(h)(a) \in A$. Second note that it is well-defined indepedent of the choice of lift $\tilde{h}$: indeed, any other lift would differ by an element of A, and since A is abelian, conjugation by an element of A is trivial.

Now we identify the $\mathfrak{g}_k$ action on $\prod_{\ell \neq p} \mathbb{Z}_\ell$. First we recall that for any n prime to p, the reduction map identifies the nth roots of unity in K^{unr} with the nth roots of unity in k^{sep}, of which there will be precisely n (since n is prime to p). In other words, the groups $\mu_n(K^{\mathrm{unr}})$ and $\mu_n(k^{\mathrm{sep}})$ are isomorphic as Galois modules. For any $\ell \neq p$, let $\mathbb{Z}_\ell(1) = \lim_{n \to \infty} \mu_{\ell^n}(K^{\mathrm{unr}})$. As a group, this is isomorphic to $\mathbb{Z}_\ell$, but

it has a generally nontrivial $\mathrm{Gal}(K^{\mathrm{unr}}/K) = \mathfrak{g}_k$-module structure. We may also form the Galois module $\prod_{\ell \neq p} \mathbb{Z}_\ell$ which is the inverse limit over all finite prime to p roots of unity.

We pause for some important terminology. For any field K of characteristic different from p, the Galois action on the inverse limit of ℓ-power roots of unity gives a homomorphism

$$\mathfrak{g}_K \to \mathrm{Aut}(\mathbb{Z}_\ell) \cong \mathbb{Z}_\ell^\times.$$

This homomorphism is called the (ℓ-adic) **cyclotomic character** and often denoted χ_ℓ. It is the first nontrivial example of a Galois representation. When K has characteristic 0, it is traditional to compile all the ℓ-adic characters together to get one representation

$$\chi : \mathfrak{g}_K \to \mathrm{Aut}(\prod_\ell \mathbb{Z}_\ell) = \mathrm{Aut}(\hat{\mathbb{Z}}) = \hat{\mathbb{Z}}^\times,$$

again called the cyclotomic character. A more down to earth description of this character is as follows: for any $n \in \mathbb{Z}^+$, its image in $(\mathbb{Z}/n\mathbb{Z})^\times$ may be calculated by choosing a primitive nth root of unity ζ_n and writing

$$\sigma(\zeta_n) = \zeta_n^{\chi(\sigma)}.$$

THEOREM 2.67. *In the extension*

$$1 \to \mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}}) \to \mathrm{Gal}(K^{\mathrm{tame}}/K) \to \mathfrak{g}_k \to 1,$$

the action of $\mathfrak{g}_k$ on $\mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{unr}}) \cong \prod_{\ell \neq p} \mathbb{Z}_\ell$ is precisely as the prime to p cyclotomic character. We indicate this by writing $\mathrm{Gal}(K^{\mathrm{tame}}/K^{\mathrm{sep}}) = \prod_{\ell \neq p} \mathbb{Z}_\ell(1)$. Moreover, this extension splits (noncanonically) as a semidirect product:

$$K^{\mathrm{tame}} = \prod_{\ell \neq p} \mathbb{Z}_\ell(1) \rtimes_\chi \mathfrak{g}_k.$$

EXERCISE 2.39. *Prove Theorem 2.67.*
(Hint for the splitting:[3] choose a uniformizer π and a compatible system of eth roots of π.)

Here is an application of these ideas.

THEOREM 2.68. *Let $K = \mathbb{C}((t_1))((t_2))$. Then $\mathfrak{g}_K \cong \hat{\mathbb{Z}} \times \hat{\mathbb{Z}}$.*

PROOF. Since the residue characteristic is 0, we have $K^{\mathrm{sep}} = K^{\mathrm{tame}}$ hence a short exact sequence

$$1 \to \prod_\ell \mathbb{Z}_\ell(1) \to \mathfrak{g}_K \to \hat{\mathbb{Z}} \to 1.$$

By Corollary X.X, the sequence splits and $\mathfrak{g}_K = \hat{\mathbb{Z}} \ltimes \hat{\mathbb{Z}}$. But moreover the semidirect product is given by a homomorphism $\rho : \hat{Z} \to \mathrm{Aut}(\hat{\mathbb{Z}})$ which is nothing else than the cyclotomic character on the Galois group of the residue field $\mathbb{C}((t_1))$. But the residue field contains $\mathbb{C}$ and hence all roots of unity, and therefore the cyclotomic character is trivial, ρ is trivial, and the product is direct. □

Remark: An easy induction argument gives that the absolute Galois group of an iterated Laurent series field in n variables over $\mathbb{C}$ (or any algebraically closed field of characteristic 0) is isomorphic to $\hat{\mathbb{Z}}^n$.

[3] Thanks to Brian Conrad.

COROLLARY 2.69. *When $K = \mathbb{Q}_p$, the Galois group $\mathrm{Gal}(K^{\mathrm{tame}}/K$ is isomorphic to the profinite completion of the discrete group*

$$\mathcal{T} = \langle \sigma, \tau \mid \varphi, \tau \mid \varphi\tau\varphi^{-1} = \tau^p \rangle.$$

EXERCISE 2.40. *Prove Corollary 2.69.*

COROLLARY 2.70. *Suppose that $\mathfrak{g}_K \cong \hat{\mathbb{Z}}$. Then the extension*

$$1 \to \mathfrak{g}_{K^{\mathrm{unr}}} \to \mathfrak{g}_K \to \mathfrak{g}_k \to 1$$

splits (noncanonically) as a semidirect product. Equivalently, there exists a (nonunique!) extension L/K such that (i) L/K is totally ramified and (ii) K^{sep}/L is unramified.

PROOF. This is the profinite analogue of the fact that a short exact sequence

$$1 \to A \to G \to \mathbb{Z} \to 1$$

splits, because to get a splitting we need a section $\iota : \mathbb{Z} \to G$, and since $\mathbb{Z}$ is a free group, there are no relations to satisfy: a section ι is determined simply by choosing any lift of $1 \in \mathbb{Z}$ to G. In the profinite case, we lift any topological generator of $\hat{\mathbb{Z}}$ to get a map $\iota : \mathbb{Z} \to \mathrm{Gal}(K^{\mathrm{sep}}/K)$ and then ι extends uniquely to a continuous homomorphism on $\hat{\mathbb{Z}}$. We leave to the reader the task of checking this carefully and also verifying that the splitting of the sequence is equivalent to the existence of a totally ramified extension L/K such that K^{sep}/L is unramified. □

Remark: More generally, a profinite group H for which any short exact sequence

$$1 \to N \to G \to H \to 1$$

of profinite groups splits as a semidirect product is called **projective**. A profinite group is projective iff its Sylow p-subgroups are free pro-p-groups. Most profinite groups are *not* projective. So far as I know, in general the short exact sequence

$$1 \to \mathfrak{g}_{K^{\mathrm{unr}}} \to \mathfrak{g}_K \to \mathfrak{g}_k \to 1$$

need not split. It would be nice to know a specific example!

EXERCISE 2.41. *This exercise requires background in arithmetic geometry.*

*Suppose that K is a Henselian discrete valuation field with residue field k, and **assume** that the short exact sequence*

$$1 \to \mathfrak{g}_{K^{\mathrm{unr}}} \to \mathfrak{g}_K \to \mathfrak{g}_k \to 1$$

splits: there is a totally ramified extension L/K such that K^{sep}/L is unramified.
*a) (Serre-Tate [**ST68**]) Let $A_{/K}$ be an abelian variety with potentially good reduction. Show: there is a totally ramified extension L/K such that $A_{/L}$ has good reduction.*
*b) (Clark-Xarles [**CX08**]) Deduce that there exists an injection $A(K)[\mathrm{tors}'] \hookrightarrow A(k)[\mathrm{tors}']$, where for a commutative group G, $G[\mathrm{tors}']$ means the subgroup of elements of order prime to the residue characteristic.*

CHAPTER 3

Adeles

1. Introducing the Adeles

1.1. What should the adeles do?

We have now come to what is probably the most important topic in our course: the systematic study of global fields using their locally compact completions.

Let K be a global field – we call that this means that K is either a finite extension of $\mathbb{Q}$ (a number field) or a finite separable extension of $\mathbb{F}_q(t)$ (a function field).

In the case of a locally compact field K, the additive group $(K, +)$ and the multiplicative group $(K^\times, \cdot)$ play key roles in the theory. Each is a locally compact commutative group, hence amenable to the methods of Fourier analysis. Moreover, the additive group is self-Pontrjagin dual, and the multiplicative group $K^\times$ is a target group for class field theory on K: that is, there is a bijective correspondence between the finite abelian extensions L/K and the finite index open subgroups H_L of $K^\times$ such that $K^\times/H_L \cong \mathrm{Gal}(L/K)$.

We seek global analogues of all of these facts. That is, for K a global field, we will define a commutative topological ring $\mathbb{A}_K$, the **adele ring**, which is locally compact and self-Pontrjagin dual. (This allows us to do harmonic analysis on global fields, as was first done in John Tate's 1950 Princeton thesis. We will not actually do this in our course, but it is an all-important topic in modern number theory, and I wish to be aware of it and be prepared to learn it!) Moreover, the group of units, suitably topologized, is called the **idele group** $\mathbb{I}_K$. It is again a locally compact commutative group.

There are further important topological properties that we do not see in the local case: namely, we will have canonical embeddings $K \hookrightarrow \mathbb{A}_K$ and $K^\times \hookrightarrow \mathbb{I}_K$. In the additive case, K is discrete (hence closed) as a subgroup of the adele ring, and the quotient $\mathbb{A}_K$ is compact. In the multiplicative case, $K^\times$ is again a discrete subgroup of $\mathbb{I}_K$; the quotient group is denoted $C(K)$. $C(K)$ need not be compact, but it is again a target group for class field theory on K.

1.2. The adele ring.

For each place v of K, the completion K_v is a locally compact field, so it seems natural not to proceed merely by analogy but actually to use the fields K_v in the construction of our putative $\mathbb{A}_K$. The first idea is simply to take the product of all the completions: $\prod_v K_v$. However, this will not work:

EXERCISE 3.1. *Let $\{X_i\}_{i\in I}$ be an indexed family of nonempty topological spaces. Show that the following are equivalent:*
(i) $X = \prod_{i\in I} X_i$ is locally compact.
(ii) Each X_i is locally compact, and $\{i \in I \mid X_i$ is not compact$\}$ is finite.

So the next try is cut down by taking only compact groups except in finitely many places. In our case this makes sense: all but finitely many places v (all of them in the function field case!) are non-Archimedean, so that we have the valuation ring R_v of K_v, a compact subgroup (subring, even) of K_v. Thus the product $\prod_{vArch} K_v \times \prod_{vNA} R_v$ is a locally compact commutative group having something to do with the global field K. But not enough: we would like to have an embedding $K \hookrightarrow \mathbb{A}_K$ and this is clearly not the case with the above product. For instance, taking $K = \mathbb{Q}$ we see that an element $x \in K$ lies in the direct product iff $\mathrm{ord}_p(x) \geq 0$ for all primes p, i.e., iff $x \in \mathbb{Z}$. So this is a reasonable "global completion" of $\mathbb{Z}$: indeed it is precisely $\hat{\mathbb{Z}} \times \mathbb{R}$, i.e., the direct product of the usual profinite completion of $\mathbb{Z}$ with $\mathbb{R}$.

Suppose we wanted to make an analogous construction that included the nonzero rational number $\frac{x}{y}$. Then y is divisible only by a finite set of primes, say S. Thus $\frac{x}{y}$ naturally lives in $\mathbb{R} \times \prod_{\ell\in S} \mathbb{Q}_\ell \times \prod_{\ell\notin S} \mathbb{Z}_\ell$, which is still a locally compact group since it has only finitely many noncompact factors. Of course the finite set S that we need to take depends on $\frac{x}{y}$: indeed, to get all possible denominators we will need to use all the groups

$$\mathbb{A}_{\mathbb{Q}}(S) = \mathbb{R} \times \prod_{\ell\in S} \mathbb{Q}_\ell \times \prod_{\ell\notin S} \mathbb{Z}_\ell.$$

But can we get one locally compact commutative group out of this family of locally compact groups indexed by the finite subsets S of non-Archimedean places of $\mathbb{Q}$? Indeed yes! Observe that these locally compact groups naturally form a directed system: if $S \subset S'$, then $\mathbb{A}_{\mathbb{Q}}(S) \hookrightarrow \mathbb{A}_{\mathbb{Q}}(S')$ embeds as an open subgroup. Therefore we may define

$$\mathbb{A}_{\mathbb{Q}} = \lim_S \mathbb{A}_{\mathbb{Q}}(S).$$

Thus, as a set, $\mathbb{A}_{\mathbb{Q}}$ is the subset of $\mathbb{R} \times \prod_\ell \mathbb{Q}_\ell$ consisting of sequences (r, x_ℓ) such that $x_\ell \in \mathbb{Z}_\ell$ for all but finitely many primes ℓ. (Note that this is strongly reminiscent of a direct sum, except that instead of requiring all but finitely many components to be zero, we require that they lie in a fixed compact subgroup.)

How do we topologize $\mathbb{A}_{\mathbb{Q}}$? Well, how do we topologize a direct limit of topological spaces? There is a standard recipe for this. More generally, suppose we have a directed system of topological spaces $\{X_i\}_{i\in I}$ – i.e., I is a directed set and for each pair of indices with $i \leq j$ we have continuous maps $\varphi(i,j) : X_i \to X_j$ such that $\varphi(i,k) = \varphi(j,k) \circ \varphi(i,j)$ when $i \leq j \leq k$ – a set X, and maps $f_i : X_i \to X$ which are compatible in the sense that $i \leq j$ implies $f_i = f_j \circ \varphi(i,j)$. Then the canonical topology to put on X is the **final topology**, i.e., the finest topology which makes all the maps f_i continuous. (To see that such a topology exists, note that the trivial topology on X makes all the maps continuous and given any family of topologies which makes all the maps continuous, their union is such a topology.) This topology can also be characterized by a universal mapping property. To make use of this, the following exercise is critical.

EXERCISE 3.2. *a) Show that the final topology can be characterized as follows: a subset $U \subset X$ is open in the final topology iff for all $i \in I$, $f_i^{-1}(U)$ is open in U. b) Deduce that for each finite subset S of prime numbers, $\mathbb{A}_{\mathbb{Q}}(S)$ is an open, locally compact subring of $\mathbb{A}_{\mathbb{Q}}$, and therefore that $\mathbb{A}_{\mathbb{Q}}$ is a locally compact topological ring.*

We want the same sort of construction with $\mathbb{Q}$ replaced by an arbitrary global field K. In fact, we may as well develop things in "proper generality" (it costs nothing extra): the key concept is that of the **restricted direct product**.

Suppose we are given the following data: (i) a nonempty index set I, (ii) for all $i \in I$, a topological group G_i, (iii) for all $i \in I$ an subgroup H_i of G_i. Then we define the **restricted direct product** $G = \prod' G_i$ to be the subset of $\prod G_i$ consisting of tuples (x_i) such that $x_i \in H_i$ for all but finitely many i's. For each finite subset $J \subset I$, let $G^J = \prod_{i \in J} G_i \times \prod_{i \notin J} H_i$. Then $G = \lim_J G^J$, and we give it the final topology.

EXERCISE 3.3. *Is it true that the direct limit topology on G is the same topology as it inherits as a subset of the direct product $\prod_{i \in I} G_i$?*

EXERCISE 3.4. *Show: G is compact iff each G_i is compact.*

EXERCISE 3.5. *Show that G is locally compact iff: each G_i is locally compact and all but finitely many H_i's are compact.*

We now give a more technical discussion of the relation of Haar measure on each of a family $\{G_i\}$ of locally compact commutative groups and the Haar measure on the restricted direct product. This will be used (only) in the proof of the Adelic Blichfeldt-Minkowski Lemma.

We place ourselves in the following situation: we are given a family $\{G_i\}_{i \in I}$ of commutative topological groups together with, on the complement of some finite subset I_∞ of I, a compact open subgroup H_i of G_i. Let $G = \prod' G_i$ be the restricted direct product of the G_i's with respect to the H_i's. Then, for each $i \in I$, there is a Haar measure mu_i on G_i. Moreover, for each $i \in I \setminus I_\infty$, we can normalize μ_i by decreeing $\mu_i(H_i) = 1$. We define a **product measure** on G to be a measure whose σ-algebra is generated by cylindrical sets $\prod_i M_i$ such that each $M_i \subset G_i$ is μ_i measurable and has $\mu_i(M_i) < \infty$ and such that $M_i = G_i$ for all but finitely many i. There is a unique measure μ on G such that $\mu(\prod_i M_i) = \prod_i \mu_i(M_i)$. Note that the restriction of μ to any subgroup $G_S = \prod_{i \in S} G_i \times \prod_{i \in I \setminus S} H_i$ is the usual product measure, a Haar measure.

Definition: Let K be any global field. We define the **adele ring** $\mathbb{A}_K$ as the restricted direct product of the topological fields $G_v := K_v$ as v ranges over all places of K and with the following chosen subgroups: if v is Archimedean, we put $H_v = K_v$ (no restriction), and if v is non-Archimedean, we put $H_v = R_v$, the valuation ring, a compact subring. Thus $\mathbb{A}_K$ is a locally compact ring.

Notation: Despite some misgivings, we introduce the following notation. For a global field K, we let Σ_K denote the set of all places of K, i.e., equivalence classes of nontrivial norms on K. (Recall that at this point we have associated a canonical normalized Artin absolute value to each place in K.) Further we write Σ_K^{NA} for the subset of non-Archimeden places of K, and let Σ_K^{Arch} denote the subset of

Archimedean places of K, which is nonempty iff K is a number field.

For each finite S with $\Sigma_K^{\mathrm{Arch}} \subset S \subset \Sigma_K$, let $\mathbb{A}_K(S) = \prod_{v \in S} K_v \times \prod_{v \notin S} R_v$ be the ring of **S-adeles**.

EXERCISE 3.6. *a) Show that $\mathbb{A}_K(S)$ is both open and closed in $\mathbb{A}_K$.*
b) Let $\iota : K \to \prod_v K_v$ be the natural embedding. Show that $\iota(K) \subset \mathbb{A}_K$.

EXERCISE 3.7. *a) Show that the adele ring $\mathbb{A}_K$ is* not *an integral domain.*
b) Compute $\operatorname{Spec} \mathbb{A}_K$.[1]

1.3. Basic results on the topology of the adeles.

LEMMA 3.1. *Let L/K be a finite separable extension of global fields. Then we have a canonical isomorphism of topological rings $\mathbb{A}_L = \mathbb{A}_K \otimes_K L$.*

PROOF. The main idea of the proof is the following familiar fact: for every place v of K we have an isomorphism of topological K_v-algebras $L \otimes_K K_v \cong \prod_{w \mid v} L_w$. Compiling these local isomorphisms gives the global isomorphism. For the topological isomorphism, we check that both sides are topologized by the same restricted direct product topology. Details are left to the reader as a good exercise. □

COROLLARY 3.2. *Maintain the notation of the previous lemma. Then, as additive groups, $(\mathbb{A}_L, +) \cong (\mathbb{A}_K, +)^{[L:K]}$.*

PROOF. We use the topological group isomorphism $\mathbb{A}_K \otimes_K L \cong \mathbb{A}_K^{[L:K]}$. □

THEOREM 3.3. *Let K be a global field. As a subspace of $\mathbb{A}_K$, K is discrete. Moreover, the quotient $\mathbb{A}_K/K$ is compact.*

PROOF. By Corollary 3.2, we may assume that $K = \mathbb{Q}$ or $K = \mathbb{F}_q(t)$. In the number field case, we let ∞ denote the Archimedean place, whereas in the function field case, we let (as usual) ∞ denote the place at infinity, for which $\frac{1}{t}$ is a uniformizer. Let $R = \mathbb{Z}$ or $\mathbb{F}_q[t]$, accordingly.
Let us show the discreteness of K in $\mathbb{A}_K$. Because we are in a topological group, it is enough to find a neighborhood of zero $U \subset \mathbb{A}_K$ such that $U \cap K = \{0\}$. Let U be the set of adeles x with $|x_\infty|_\infty < 1$ and $|x_p|_p \leq 1$ for all finite places p. Certainly U is an open set. When $K = \mathbb{Q}$ the intersection $U \cap K$ consists of rational numbers which are integral at all places – i.e., integers – and have standard absolute value strictly less than 1. Clearly this intersection is 0. Similarly, in the function field case, the integrality conditions force $x \in K \cap U \implies x \in R$, i.e., x is a polynomial, whereas $|x|_\infty < 1$ means that x is, if not zero, a rational function of negative degree. So $x = 0$. This proves the discreteness in both cases.

Let $W \subset \mathbb{A}_K$ be the compact subset defined by $|x_\infty|_\infty \leq 1$, $|x_v|_v \leq 1$ for all finite places v. We claim that every adele y can be written in the form $b + x$, with $b \in K$, $x \in W$. When $K = \mathbb{Q}$ this is an easy but enlightening exercise using the Chinese Remainder Theorem that we leave to the reader. For the sake of variety let's do the $K = \mathbb{F}_q(t)$ case instead. Let $x \in \mathbb{A}_K$, and let S be the finite set of finite places v for which $|x_v|_v > 1$. We realize each such v as a monic irreducible

[1]Hint/Warning: This involves ultrafilters and such.

polynomial $v(t) \in \mathbb{F}_q[t]$, and let $n(v) \in \mathbb{Z}^+$ be such that $|v^{n(v)}x_v|_v = 1$. For $v \in S$, put

$$u_v \coloneqq \prod_{w \in S \setminus \{v\}} w^{n(w)},$$

so $|u_v|_v = 1$. By the Chinese Remainder Theorem, there is $y' \in \mathbb{F}_q[t]$ such that for all $v \in S$, $y' \equiv u_v v^{n(v)} x_v \pmod{v^{n(v)}}$. We put

$$y = \frac{y'}{\prod_{v \in S} v^{n(v)}}.$$

Thus for all $v \in S$ we have $|x_v - y|_v \leq 1$, and for all finite $v \notin S$ we have $|x_v|_v \leq 1$ and $|y|_v \leq 1$, so certainly $|x_v - y|_v \leq 1$.

Finally we must deal with the place $v = \infty$. If we add to y any polynomial $f(t) \in \mathbb{F}_q[t]$ we do not disturb anything that we have already done. If $\deg(x-y) \leq 0$, then $|x - y|_\infty \leq 1$ and we need not do anything. If $\deg(x - y) \geq 1$, then by polynomial long division we may write $x - y = f + \frac{r}{s}$ with $f, r, s \in \mathbb{F}_q[t]$ and $\deg r < \deg s$. Thus replacing y by $y - f$ preseserves all our finite integrality conditions and attains integrality at the infinite place.

So the quotient map $\mathbb{A} \to \mathbb{A}/K$ restricted to W is surjective: we're done. □

LEMMA 3.4. *(Adelic Blichfeldt-Minkowski Lemma) Let K be a global field. There is a constant $C = C(K)$ such that: if $x = \{x_v\} \in \mathbb{A}_K$ is such that $|x_v|_v = 1$ for almost every v and $\prod_v |x_v|_v > C$, then there is a nonzero $y \in K$ such that for all $v \in \Sigma_K$, we have $|y|_v \leq |x_v|_v$.*

PROOF. This proof uses the product measure μ on $\mathbb{A}_K$ defined above. Moreover, since K is countable and $\mathbb{A}_K/K$ is compact, it has a finite, positive, total measure c_0 with respect to the Haar measure – in other words, this is the measure of a fundamental region for the coset space $\mathbb{A}_K/K$ in K. Let c_1 be the measure of the subset of $\mathbb{A}_K$ defined by the inequalities $|x_v|_v \leq \frac{1}{10}$ at the Archimedean places and $|x_v|_v \leq 1$ at the non-Archimedean places. It is easy to see that $0 < c_1 < \infty$. We show that we may take $C = \frac{c_0}{c_1}$.

Now fix an adele $\alpha = (\alpha_v)$ such that $|\alpha_v|_v = 1$ for almost every v and $\prod_v |\alpha_v|_v > C$. Let T be the set of adeles (x_v) with $|x_v|_v \leq \frac{1}{10}|\alpha_v|_v$ at Archimedean places and $|x_v|_v \leq |\alpha_v|_v$ at non-Archimedean places. The set T has measure $c_1 \prod_v |\alpha_v| > c_1 C = c_0$, hence there must exist distinct elements of T with the same image in the quotient $\mathbb{A}_K/K$, say τ' and τ'' so that $\beta := \tau' - \tau''$ is a nonzero element of K such that $|\beta|_v = |\tau'_v - \tau''_v| \leq |\alpha_v|_v$, qed. □

EXERCISE 3.8. *What was the point of inserting the factor $\frac{1}{10}$ at the Archimedean places?*

Remark: For a statement of the classical Blichfeldt Lemma, see e.g. Theorem 5 of `http://math.uga.edu/~pete/4400Minkowski.pdf`.

For future reference, a constant C as in the statement of Lemma 3.4 will be called an **adelic Blichfeldt constant**.

COROLLARY 3.5. *Let v_0 be a normalized valuation on K. Choose a sequence $\{\delta_v\}_{v \neq v_0}$ such that $\delta_v > 0$ for all v and $\delta_v = 1$ for all but finitely many v. Then there exists $x \in K^\times$ such that $|x|_v \leq \delta_v$ for all $v \neq v_0$.*

PROOF. Choose $\alpha_v \in K_v$ with $0 < |\alpha_v| \leq \delta_v$ and $|\alpha_v|_v = 1$ if $\delta_v = 1$. Choose $\alpha_{v_0} \in K_{v_0}$ such that $\prod_v |\alpha_v|_v > C$. Apply the Lemma. □

THEOREM 3.6. *(Strong Approximation) Fix any valuation v_0 of the global field K. Define $\mathbb{A}_K^{v_0}$ to be the restricted direct product of the K_v's (with $v \neq v_0$) with respect to the subrings R_v for the non-Archimedean places. Then the natural embedding $K \hookrightarrow \mathbb{A}_K^{v_0}$ has dense image.*

PROOF. The theorem is equivalent to the following statement: suppose we are given (i) a finite set S of valuations $v \neq v_0$, (ii) elements $\alpha_v \in K_v$ for all $v \in S$ and (iii) $\epsilon > 0$. Then there exists $\beta \in K$ such that $|\beta - \alpha_v|_v \leq \epsilon$ for all $v \in S$ and $|\beta|_v \leq 1$ for all $v \neq v_0$. By the proof of Theorem 3.3, there exists $W \subset \mathbb{A}_K$ defined by inequalities $|\alpha_v|_v \leq \delta_v$ for all v, $\delta_v = 1$ for all but finitely many v, such that every adele $\alpha \in \mathbb{A}_K$ is of the form $\alpha = y + w$, $y \in K$, $w \in W$. By Corollary 3.5, there exists $x \in K^\times$ such that $|x|_v < \delta_v^{-1}\epsilon$ for all $v \in S$ and $|x|_v \leq \delta_v^{-1}$ for all $v \neq v_0$. Let α be any adele. Write $x^{-1}\alpha = y + w$ with $y \in K$, $w \in W$, and multiply by x to get $\alpha = xy + xw$. Finally, choose α to be the adele with v component the given α_v for all $v \in S$ and 0 elsewhere. Then we may take $\beta = xy$. □

EXERCISE 3.9. *Give a hands-on proof of Theorem 3.6 when $K = \mathbb{Q}$, $v_0 = \infty$.*

1.4. Ideles.

Let R be a topological ring. Then the group of units $R^\times$ need not be a topological group under the induced topology: the problem is that inversion need not be continuous.

It will be helpful to use the following snippet from the theory of topological groups: a **paratopological group** is a group G endowed with a topology with respect to which the group law is "jointly continuous", i.e., $\cdot : G \times G \to G$ is continuous. A **semitopological group** is a group endowed with a topology with respect to which the group law is "separately continuous": for all $y \in G$, the maps $y\bullet : G \to G,\ x \mapsto yx$ and $\bullet y : G \to G,\ x \mapsto xy$ are continuous. Thus a topological group is precisely paratopological group in which the inversion map $x \mapsto x^{-1}$ is continuous, and every paratopological group is a semitopological group but not necessarily conversely.

THEOREM 3.7. *(Ellis)*
a) Every locally compact paratopological group is a topological group [**El57a**].
b) Every locally compact semitopological group is a topological group [**El57b**].

EXERCISE 3.10. *a) Suppose R is a locally compact topological ring in which $R^\times$ is open. Show that $R^\times$ is a topological group: i.e., $x \mapsto x^{-1}$ is a homeomorphism of $R^\times$ under the subspace topology.*
b)[2] *Take on $\mathbb{Q}$ the topology τ_T for which a neighborhood base at $x \in \mathbb{Q}$ is given by $\{x + n\mathbb{Z}\}_{n=1}^\infty$. Show that τ_T is Hausdorff, so in particular $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ is open. Show that inversion on $\mathbb{Q}^\times$ is not continuous.*

There is a general method for endowing $R^\times$ with the structure of a topological group. Namely, we think of $R^\times$ as a subset of $R \times R$ via the injection $x \mapsto (x, x^{-1})$. Let us call this the **multiplicative topology**.

[2] I received this example from T. Trimble, who took it from [**Wa**, p. 113].

PROPOSITION 3.8. *Let R be a Hausdorff topological ring.*
a) Show that the multiplicative topology on $R^\times$ is at least as fine as the subspace topology.
b) Show that if we endow $R^\times$ with the multiplicative topology, it is a Hausdorff topological group.

EXERCISE 3.11. *Prove Proposition 3.8.*

Of course the case we have in mind is $R = \mathbb{A}_K$, the adele ring of a global field K. We define the **idele group** $\mathbb{I}_K$ to be the unit group of the adele ring.

PROPOSITION 3.9. *Let $\mathbb{I}_K = \mathbb{A}_K^\times$ be the idele group.*
a) $\mathbb{I}_K$ is the set of all adeles $(x_v)_v$ with $x_v \neq 0$ for all v and $x_v \in R_v^\times$ for almost all v.
b) The idele group $\mathbb{I}_K$ is not *an open subgroup of $\mathbb{A}_K$.*
c) The multiplicative topology on $\mathbb{I}_K$ is strictly finer than the subspace topology.
d) The multiplicative topology on $\mathbb{I}_K$ makes it into a locally compact (Hausdorff) topological group. In fact, it is nothing else than the restricted direct product of the spaces $K_v^\times$ with respect to the compact subgroups $R_v^\times$ (and the locally compact subgroups $K_v^\times$ at the Archimedean places, if any).

EXERCISE 3.12. *Prove Proposition 3.9.*

EXERCISE 3.13. *For finite S, $\Sigma_K^{\mathrm{Arch}} \subset S \subset \Sigma_K$, define the group of S-ideles*

$$\mathbb{I}_K(S) = \prod_{v \in S} K_v^\times \times \prod_{v \notin S} R_v^\times.$$

a) Show that each $\mathbb{I}_K(S)$ is open and closed as a subgroup of $\mathbb{I}_K$.
b) Show that the natural (diagonal) map from $K^\times$ to $\mathbb{I}_K(S)$ is an injection. Henceforth we identify $K^\times$ with its image in $\mathbb{I}_K$ or $\mathbb{I}_K(S)$ for some S.

LEMMA 3.10. *$K^\times$ is discrete in $\mathbb{I}_K$.*

PROOF. By the definition of the topology on the adeles, it is enough to show that discreteness of $K^\times$ as embedded in $\mathbb{A}_K \times \mathbb{A}_K$ via $x \mapsto (x, x^{-1})$. But this follows immediately from the discreteness of K in $\mathbb{A}_K$ and the easy fact that a product of two discrete spaces is discrete. □

EXERCISE 3.14. *a) Give a direct proof of Lemma 3.10 when $K = \mathbb{Q}$ or $\mathbb{F}_p(t)$: i.e., exhibit a compact neighborhood U of 1 in $\mathbb{I}_K$ such that $U \cap K^\times = \{1\}$.*
b) Let K/K_0 be a separable extension of global fields. Can you deduce the discreteness of $K^\times$ in $\mathbb{I}_K$ from the discreteness of $K_0^\times$ in $\mathbb{A}_K$ as we did in the additive case?

Stop for a moment and think what should be coming next. The natural question is – isn't it? – whether $K^\times$ is cocompact in $\mathbb{I}_K$ as was the case for K and $\mathbb{A}_K$. The answer is no, and this is a fundamental difference between the ideles and the adeles. To see this, we will construct a continuous map from the **idele class group** $C(K) = \mathbb{I}_K/K^\times$ to a noncompact subgroup of $R^\times$, a kind of "norm map".

Normalized valuations: let K_0 be $\mathbb{Q}$ or $\mathbb{F}_p(t)$, the prime global field. For v a place of K, we choose a particular norm as follows: say $v \mid v_0$ a place of K_0, let $|\cdot|_{v_0}$ be the standard norm on the $(K_0)_{v_0}$– i.e. which gives a uniformizer norm $\frac{1}{p}$ –

and define $|| \cdot ||_v$ by $||x||_v = |N_{K/K_0}(x)|$. (This coincides with the canonical norm given by the Haar measure.)

THEOREM 3.11. *(Product formula) Let $x \in K^\times$. Then*

$$\prod_v ||x||_v = 1.$$

PROOF. Step 1: Suppose $K = \mathbb{Q}$ or $\mathbb{F}_p(t)$. In this case it is straightforward to verify the product formula directly. Indeed, in both cases it takes the special form that the norm at the infinite place is exactly the reciprocal of the product of the norms at all the finite places. This verification was done in class with the help of the students, and we leave it to you, the reader, now.
Step 2: Let L/K be a finite degree separable field extension. We wish to reduce the product formula for L to the product formula for K, a task which involves little more than careful bookkeeping. First we recall the following appealing formula for the normalized Artin absolute values. Let L_w/K_v be a finite exension of locally compact fields. Then for all $x \in L_w$, we have

$$||x||_{L_w} = |N_{L/K}(x)|_{K_v}.$$

Thus, for $x \in L$, we have

$$||x|| = \prod_{v \in \Sigma_K} \prod_{w \mid v} ||x||_w = \prod_{v \in \Sigma_K} \prod_{w \mid v} |N_{L_w/K_v} x|_v.$$

On the other hand, we have

$$L \otimes_K K_v \cong \prod_{w \mid v} L_w,$$

and thus

$$\prod_{w \mid v} N_{L_w/K_v}(x) = N_{L/K}(x).$$

Using this identity, we get

$$||x|| = \prod_{v \in \Sigma_K} |N_{L/K}(x)| = 1$$

by Step 1. □

We define a norm map $|\cdot| : \mathbb{I}_K \to \mathbb{R}^{>0}$ by $x \in \mathbb{I}_K \mapsto |x| = \prod_v |x_v|_v$. It is immediate that this is a group homomorphism.

EXERCISE 3.15. *Show that the norm map $|| \cdot || : \mathbb{I}_K \to \mathbb{R}^{>0}$ is continuous.*

Since our normalized Artin absolute values on $\mathbb{R}$ and $\mathbb{C}$ are both surjective onto $\mathbb{R}^{>0}$, if K is a number field, looking only at ideles which have component 1 except at one fixed Archimedean place shows that the norm map is surjective. If K has characteristic $p > 0$, then the image of the norm map lies somewhere in between $p^{\mathbb{Z}}$ and $p^{\mathbb{Q}}$: i.e., it is not surjective, but its image is an unbounded – hence noncompact – subset of $\mathbb{R}^\times$. Thus we have shown:

LEMMA 3.12. *The idele class group $C(K) = \mathbb{I}_K/K^\times$ is* not *compact.*

We also include, for future use, the following result to the effect that the disparity between the subspace and multiplicative topologies is eliminated by passage to norm one ideles:

LEMMA 3.13. *The norm one ideles $\mathbb{I}_K^1$ are closed as a subset of the adele ring $\mathbb{A}_K$. Moreover, the topology that $\mathbb{I}_K^1$ inherits from $\mathbb{A}_K$ is the same as the topology it inherits from $\mathbb{I}_K$.*

PROOF. First we show that $\mathbb{I}_K^1$ is closed in $\mathbb{A}_K$. So let $\alpha \in \mathbb{A}_K \setminus \mathbb{I}_K^1$. We must, of course, find a neighborhood W of α that does not meet $\mathbb{I}_K^1$.
Case 1: $\prod_v |\alpha_v|_v < 1$. Let $S \subset \sigma_K$ be a finite set containing all places v with $|\alpha_v|_v > 1$ and such that $\prod_{v \in S} |\alpha_v|_v < 1$. Let W_ϵ be the set of all $\beta \in \mathbb{A}_K$ such that $|\beta_v - \alpha_v|_v < \epsilon$ for all $v \in S$ and $|\beta_v|_v \leq 1$ for all other v. Then W_ϵ does the job for all sufficiently small ϵ.
Case 2: $\prod_v |\alpha_v|_v = C > 1$. Then there is a finite set S of places v containing each place v with $|\alpha_v|_v > 1$ and if $v \notin S$ then $|\beta_v|_v < 1 \implies \frac{C}{2}$. (For instance, in the number field case we may take S to contain all Archimedean places and all finite places of residue characteristic $p \leq 2C$. Similarly, in the function field case we may take S to contain all places extending places of $K_0 = \mathbb{F}_p(t)$ with residue cardinality at most $2C$.) Then defining W_ϵ as above does the job for all sufficiently small ϵ.

Now we show that the adelic and idelic topologies on $\mathbb{I}_K^1$ coincide. Fix $\alpha \in \mathbb{I}_K^1$. Let $W \subset \mathbb{I}_K^1$ be an adelic neighborhood of α. Then it contains an adelic neighborhood of type $W_\epsilon(S)$ above, for some finite subset S. The corresponding set $W'_\epsilon(S)$ defined by β such that $|\beta_v - \alpha_v|_v < \epsilon$ for all $v \in S$ and $|\beta_v|_v = 1$ for all other v, is an idelic neighborhood of α and $W'_\epsilon(S) \subset W_\epsilon(S)$. Conversely, let $H \subset \mathbb{I}_K^1$ be an idelic neighborhood. Then it contains a neighborhood of type $W_\epsilon(S)$ where S contains all Archimedean places and all v such that $|\alpha_v|_v \neq 1$. Since by assumption $\prod_v |\alpha_v|_v = 1$, by taking ϵ sufficiently small we get $\prod_v |\beta_v|_v < 2$. Then $W_\epsilon(S) \cap \mathbb{I}_K^1 = W'_\epsilon(S) \cap \mathbb{I}_K^1$, qed. □

It is natural to try to "fix" the noncompactness of $C(K)$ by passing to the kernel of the norm map. So we make another key definition: put $C^1(K) = \ker(|\cdot| : \mathbb{I}_K/K^\times \to \mathbb{R}^{>0})$, the **norm one idele class group**.

THEOREM 3.14. *The norm one idele class group $C^1(K)$ is compact.*

PROOF. Using Lemma 3.13, it suffices to find a compact subset $W \subset \mathbb{A}_K$ such that the map $W \cap \mathbb{I}_K^1 \to \mathbb{I}_K^1/K^\times$ is surjective. Let C be an adelic Blichfeldt constant for K; let $\alpha = (\alpha_v)$ be an idele with $||\alpha|| > C$, and let W be the set of adeles β such that for all places v of K, $|\beta_v|_v \leq |\alpha_v|_v$. W is easily seen to be compact. Now let $\beta \in \mathbb{I}_K^1$. Then, by the adelic Blichfeldt-Minkowski Lemma, there is $x \in K^\times$ such that for all places v, $|x|_v \leq |\beta_v^{-1}\alpha_v|_v$. Then $x\beta \in W$. □

2. The Adelic Approach to Class Groups and Unit Groups

2.1. Rings of S-integers.

Despite some misgivings, we introduce the following notation. For a global field K, we let Σ_K denote the set of all places of K, i.e., equivalence classes of nontrivial norms on K. (Recall that at this point we have associated a canonical normalized Artin absolute value to each place in K.) Further we write Σ_K^{NA} for the subset of non-Archimedean places of K, and let Σ_K^{Arch} denote the subset of Archimedean places of K, which is nonempty iff K is a number field.

Now let $S \subset \Sigma_K$ be a finite set such that $S \supset \Sigma_K^{\mathrm{Arch}}$. We define the ring R_S of **S-integers** of K to be the set of $x \in K$ such that $v(x) \geq 0$ for all $v \in \Sigma_K^{\mathrm{NA}} \setminus S$.

EXAMPLE 3.15. *a) Let K be a number field, and let $S = \Sigma_K^{\mathrm{Arch}}$. Then*

$$R_S = \{x \in K \mid v_{\mathfrak{p}}(x) \geq 0 \ \forall \mathfrak{p} \in \mathrm{MaxSpec}\, \mathbb{Z}_K\} = \mathbb{Z}_K.$$

b) Let $K = \mathbb{Q}$ and let $S = \{\infty, p_1, \ldots, p_r\}$ be any finite subset containing the infinite place. Then

$$R_S = \mathbb{Z}[\frac{1}{p_1 \cdots p_r}].$$

c) Let $K = \mathbb{F}_q(t)$, and let $S = \{\infty\}$. Then $R_S = \mathbb{F}_q[t]$.

EXERCISE 3.16.
a) If K is a function field and $S = \emptyset$, show: R_S is the maximal finite subfield of K (or, in other words, the "algebraic closure of $\mathbb{F}_p$ in K".)
b) Show: if $S \neq \emptyset$, then R_S is a Dedekind domain that is not a field.

EXERCISE 3.17. *Suppose that $S \subset T$ are finite subsets of Σ_K with $\Sigma_K^{\mathrm{Arch}} \subset S$.*
a) Show: $R_S \subset R_T$.
b) Suppose R_S is a PID. Show: there are prime elements $p_1, \ldots, p_r$ of R_S such that

$$R_T = R_S[\frac{1}{p_1 \cdots p_r}].$$

c) Show: in general R_T is a localization of R_S.*[3]

2.2. Finiteness of the S-class groups.

Like any Dedekind domain, R_S has an interesting invariant: its ideal class group. Let us review the construction in more generality.

Let R be a domain with fraction field K. A **fractional R-ideal** is a nonzero R-submodule $I \subset K$ for which there is $a \in R \setminus \{0\}$ such that $aI \subset R$. Let $\mathrm{Frac}\, R$ denote the set of all fractional R-ideals. For $I, J \in \mathrm{Frac}\, R$ we define the product IJ to be the R-submodule of K generated by all the pairwise products xy for $x \in I$, $y \in J$. Then IJ is again a fractional ideal, and this operation endows $\mathrm{Frac}\, R$ with the structure of a commutative monoid (that is, the operation is associative and has a multiplicative identity – the fractional ideal R – but elements need not have multiplicative inverses). A fractional ideal I is **invertible** if there is a fractional ideal J such that $IJ = R$. We denote the set of invertible fractional ideals of R by $\mathrm{Inv}\, R$: this is indeed nothing else than the group of units of the monoid $\mathrm{Frac}\, R$.

A fractional ideal I is **principal** if it is monogenic as an R-module: in other words, there is $x \in K^\times$ such that

$$I = (x) \coloneqq \{rx \mid r \in R\}.$$

The inverse of the principal fractional ideal (x) is the principal fractional ideal (x^{-1}), so the set $\mathrm{Prin}\, R$ of principal fractional ideals forms a subgroup of $\mathrm{Inv}\, R$. We define the **Picard group** of R to be the quotient

$$\mathrm{Pic}\, R \coloneqq \mathrm{Frac}(R)/\,\mathrm{Prin}(R).$$

This is a rather general definition. The generality is indeed useful in number theory – e.g. for the case of a non-maximal order in a number field. However, for Dedekind domains things simplify:

[3] I don't see how to do this without using the finiteness of the class group of R_S, coming up soon.

THEOREM 3.16. *For a domain R, the following are equivalent:*
(i) R is a Dedekind domain.
(ii) Every fractional R-ideal is invertible: $\operatorname{Frac} R = \operatorname{Inv} R$.

PROOF. See [**C:CA**, Thm. 20.1]. □

Thus in a Dedekind domain, $\operatorname{Pic} R$ is simply the group of all fractional ideals modulo principal ideals. It is a basic fact that for a Dedekind domain R we have

$$\operatorname{Pic} R \text{ is trivial} \iff R \text{ is a UFD} \iff \text{ is a PID},$$

and thus the nontriviality of $\operatorname{Pic} R$ is the obstruction to unique factorization of elements in R. When R is understood to be a Dedekind domain, we will write $\operatorname{Cl} R$ in place of $\operatorname{Pic} R$ and call it the **class group**.[4]

EXERCISE 3.18. *a) Let k be a field, and let $(E, O)_{/k}$ be an elliptic curve. Let $k[E^\circ]$ be the standard affine coordinate ring of E: this is the ring of all rational functions $f \in k(E)$ that are regular away from the neutral point O. Let $k(E)$ be the group of k-rational points of E. Show that there is a canonical isomorphism*

$$\operatorname{Cl} k[E^\circ] \xrightarrow{\sim} E(k),$$

where $E(k)$ is the group of k-rational points of E.
b) By taking $k = \mathbb{C}$, deduce that there is a Dedekind domain whose class group is uncountably finite and not a torsion group.

The preceding exercise suggests there are no obvious restrictions on the class group of a Dedekind domain other than commutativity. Indeed there are none!

THEOREM 3.17. *(Claborn [**Cl66**]) For every commutative group A, there is a Dedekind domain R such that* $\operatorname{Cl} R \cong A$.

THEOREM 3.18. *Let K be a global field and $S \subset \Sigma_K$ a finite set containing all the Archimedean places. Then the ideal class group* $\operatorname{Cl}(R_S) = \operatorname{Frac}(K)/\operatorname{Prin}(K)$ *is a finite commutative group.*

Especially in the number field case, the group $\operatorname{Cl} R_S$ is sometimes called the **S-class group** of K. It is closely related to the general concept of overrings of a Dedekind domain, which again we explain briefly in somewhat more generality.

If R is a domain with fraction field K, then by an **overring** of R we mean a ring T with $R \subset T \subset K$. In particular every localization is an overring, but in general this does not yield all possible overrings. Suppose now that R is a Dedekind domain, and let T be an overring of R. For each $\mathfrak{p} \in \operatorname{MaxSpec} R$, the localization $R_{\mathfrak{p}}$ is a DVR with fraction field K – these are precisely the maximal overrings of R, and we have

$$R = \bigcap_{\mathfrak{p} \in \operatorname{MaxSpec} R} R_{\mathfrak{p}}.$$

The following result completely classifies the overrings of a Dedekind domain as "generalized S-integer rings."

[4]For a general domain R one can also define a **divisor class group** $\operatorname{Cl} R$: see e.g. [**C:CA**, §19.4]. The class of domains on which the divisor class group and the Picard group coincides includes all Dedekind domains, so with Dedekind domains there is no need to be so fastidious.

THEOREM 3.19. *Let R be a Dedekind domain. For every subset $W \subset \operatorname{MaxSpec} R$, let*

$$R_W = \bigcap_{\mathfrak{p} \in \operatorname{MaxSpec} R \setminus W} R_{\mathfrak{p}}.$$

a) Then R_W is a Dedekind domain.
b) Let T be an overring of R, and put

$$W(T) \coloneqq \{\mathfrak{p} \in \operatorname{MaxSpec} R \mid \mathfrak{p}T = \mathfrak{p}\}.$$

Then $T = R_{W(T)}$.

PROOF. See [**C:CA**, Thm. 23.3]. □

An **elliptic Dedekind domain** is an overring of a Dedekind domain of the form $k[E^\circ]$ for an elliptic curve (E, O) defined over a field k. The following result gives a new proof of Theorem 3.17 that builds on earlier work of Rosen [**Ro76**].

THEOREM 3.20. *(Clark [**Cl09b**]) Let A be a commutative group. Then there is an elliptic Dedekind domain R with $\operatorname{Cl} R \cong A$.*

EXERCISE 3.19. *Let R be a Dedekind domain and let $T = R_W$ be an overring of R. The map $\iota : R \hookrightarrow T$ induces a map on ideal class groups, $\iota_* : \operatorname{Cl}(R) \to \operatorname{Cl}(T)$, simply by pushing forward ideals: $I \mapsto IT$. Show that ι_* is surjective with kernel the subgroup of $\operatorname{Pic} R$ generated by W, i.e., by the classes of prime ideals $\mathfrak{p}$ of R with $\mathfrak{p}T = T$. In particular, if $\operatorname{Cl}(R)$ is finite, then so is $\operatorname{Cl}(S)$.*

Now we give the **proof** of Theorem 3.18 in the number field case, so let K be a number field and S a finite set of places of K containing all Archimedean places. Note that we may naturally view $\operatorname{MaxSpec} R_S$ as $\Sigma_K \setminus S$. We define a group homomorphism

$$V : \mathbb{I}_K \to \operatorname{Frac}(R_S)$$

by associating to the idele (x_v) the sequence of valuations $v(x_v)$ as v ranges over elements of $\Sigma_K \setminus S$ (here we are identifying a non-Archimedean place on K with its corresponding $\mathbb{Z}$-valued valuation) and then putting

$$V((x_v)) \coloneqq \prod_{\mathfrak{p} \in \operatorname{MaxSpec} R_S} \mathfrak{p}_v^{v(x_v)}.$$

This map is well-defined because $v(x_v) = 0$ for almost every v. It is plainly surjective. If $x \in K^\times$, then $V(x) = (x)$, so V descends to a surjective homomorphism

$$V : C(K) \to \operatorname{Cl}(R_S).$$

We claim that V remains surjective when restricted to $C^1(K)$: indeed, as K is a number field we have at least one Archimedean place, and at each Archimedean place the local norm map surjects onto $\mathbb{R}^{>0}$, so by modifying the idele at a single Archimedean place we can make the norm one without changing V. Now we observe that the kernel of V contains the open subgroup $\prod_v R_v^\times$, so the image is discrete in the natural (quotient space) topology. Thus in the quotient topology, $\operatorname{Cl}(R_S)$ is both discrete and compact, and therefore finite!

What about the function field case? The setup, including the definition of the map $V : \mathbb{I}_K \to \operatorname{Frac} R_S$, is identical to the above. There is just one change: S no longer contains any Archimedean places. If $S = \varnothing$, then R_S is a finite field so $\operatorname{Cl} R_S$ is trivial. Otherwise what we can assume about S is that it contains a

non-Archimedean place v, and then if K has characteristic $p > 0$, there is some positive integer power q of p such that $|K_v^\times|_v = q^{\mathbb{Z}}$. Since this is true for every $v \in \Sigma_K$, the norm of any idele lies in $p^{\mathbb{Z}}$. Thus we *cannot* necessarily adjust the vth component of an idele in order to make the norm be 1, so V restricted to $C^1(K)$ need not be surjective. But if $q = p^f$, this shows that $\mathrm{Cl}\, R_S$ is the image of the elements of $C(K)$ with norm lying in $[1, q]$, and this is still a compact space. This completes the proof in the function field case.

2.3. Structure of the S-unit groups.

With K and S as above, we now wish to study the structure of the unit group $U_S = R_S^\times$. Again, in the number field case this is often called the **S-unit group**. We will give a generalization of the celebrated Dirichlet unit theorem to S-class groups of either number fields or function fields.

LEMMA 3.21. *Let $0 < c < C$. Then the set $\mathcal{S} = \mathcal{S}(S, c, C)$ of S-units x with $c \leq |x|_v \leq C$ for all $v \in S$ is finite.*

PROOF. The set W of ideles $x = (x_v)$ with $|x_v|_v = 1$ for all $v \notin S$ and $c \leq |x_v|_v \leq C$ for all $s \in S$ is visibly compact. We have $\mathcal{S} = W \cap K^\times$, so $\mathcal{S}$ is compact and discrete, thus finite. □

LEMMA 3.22. *The set of elements $x \in K$ such that $|x|_v = 1$ for all places v of K is precisely the group of roots of unity of K, which is a finite commutative group.*

PROOF. Let $\mu(K)$ be the group of roots of unity of K and let $\mathcal{T}$ be the subgroup of elements of $K^\times$ which have norm one at every place v of K. By Exercise 1.3a), $\mu(K) \subset \mathcal{T}$. Applying Lemma 3.21 (with any fnite set S containing Σ_K^{Arch}) and $c = C = 1$ shows that $\mathcal{T}$ is finite. In particular, each element of $\mathcal{T}$ has finite order, so $\mathcal{T} \subset \mu(K)$. Thus $\mathcal{T} = \mu(K)$ is finite. □

Remark: In fact, it follows from our work on locally compact fields that in any locally compact field except $\mathbb{C}$, the group of roots of unity is finite. This is obvious for $\mathbb{R}$. For a non-Archimedean locally compact field, this is Theorem 2.32.

LEMMA 3.23. *Let $r, s \in \mathbb{Z}$ with $s \geq r \geq 0$, and let $G = \mathbb{R}^r \times \mathbb{Z}^{s+1-r}$. Let $\lambda : G \to (\mathbb{R}, +)$ be a nontrivial homomorphism of topological groups. Moreover:*
• *When $r = 0$, we assume that $\lambda(\mathbb{Z}^{s+1-r}) \cong (\mathbb{Z}, +)$*
•, *When $r > 0$, we assume that $\lambda|_{\mathbb{R}^r} \cong (\mathbb{R}, +)$.*
Let $\mathcal{K} = \mathrm{Ker}(\lambda)$ and let Γ be any discrete, cocompact subgroup of $\mathcal{K}$. Then $\Gamma \cong \mathbb{Z}^s$.

PROOF. Write $\lambda = \lambda_1 + \lambda_2$, where $\lambda_1 = \lambda|_{\mathbb{R}^r}$ and $\lambda_2 = \lambda|_{\mathbb{Z}^{s+1-r}}$.
Case 1: $r = 0$. Then $\lambda_1 = 0$, so (by assumption!) $\mathbb{Z}^{s+1}/\mathcal{K} \cong \mathbb{Z}$ and thus $\mathcal{K} \cong \mathbb{Z}^s$. In this case every subgroup of $\mathcal{K}$ is discrete and is cocompact iff it has maximal rank, so indeed $\Gamma \cong \mathbb{Z}^s$.
Case 2: $\lambda_2 = 0$. Then $\mathcal{K} = \ker(\lambda_1) \oplus \mathbb{Z}^{s+1-r} \cong \mathbb{R}^{r-1} \oplus \mathbb{Z}^{s+1-r}$. A discrete cocompact subgroup of this is obtained by choosing a rank $r-1$ lattice of $\mathbb{R}^{r-1}$ together with $\mathbb{Z}^{s+1-r}$, hence is isomorphic to $\mathbb{Z}^s$.
Case 3: Finally, we assume that λ_1 and λ_2 are both nontrivial. Then the image of λ_2 is isomorphic to $\mathbb{Z}^t$ for some $1 \leq t \leq s + 1 - r$. Then

$$K_0 := \{(x, y) \in G \mid \lambda_1(x) = \lambda_2(x) = 0\}$$

is a subgroup of $\mathcal{K}$ and $\mathcal{K}/K_0 \cong \mathbb{Z}^t$. Explicitly, $K_0 \cong \mathbb{R}^{r-1} \times \mathbb{Z}^{s+1-r-t}$, and thus $\mathcal{K} \cong \mathbb{R}^{r-1} \times \mathbb{Z}^{s-r+1}$, so again a discrete cocompact subgroup must have rank s. □

We now give the following attractive generalization of Dirichlet's Unit Theorem, the third basic finiteness theorem in algebraic number theory.

THEOREM 3.24. *Let K be a global field, S a finite nonempty set of places of K containing all Archimedean places (if any). Let U_S be the group of S-units. Then U_S is a finitely generated commutative group. More precisely, its torsion subgroup is the finite group of roots of unity in K, and its rank is $\#S - 1$.*

PROOF. (Ramakrishnan-Valenza [**RV**]) Step 1: For $v \in \Sigma_K$, let $C_v = \{x \in K_v \mid \cdot |x|_v = 1\}$. This is a compact subgroup of $K_v^\times$. Therefore, by Tychonoff, $C := \prod_v C_v$ is a compact subgroup of $I_K(S)$, the "adelic circle group". We have a short exact sequence of topological groups

$$1 \to C \to \mathbb{I}_K(S) \to \prod_{v \in S} K_v^\times / C_v \to 1.$$

Now $K_v^\times / C_v$ is isomorphic to $\mathbb{R}^{>0} \cong (\mathbb{R}, +)$ if v is Archimedean and isomorphic to $\mathbb{Z}$ if v is non-Archimedean. If we put $s = \#S - 1$, $r = \#\Sigma_K^{\mathrm{Arch}}$, then we may rewrite the exact sequence as

$$1 \to C \to \mathbb{I}_K(S) \to \mathbb{R}^r \oplus \mathbb{Z}^{s+1-r} \to 0.$$

We wish to first restrict this sequence of norm one S-ideles and then further to elements of $K^\times \cap \mathbb{I}_K^1(S)$.

Step 2: Consider the norm map restricted to the subgroup of S-ideles: $|| \cdot || : \mathbb{I}_K(S) \to \mathbb{R}^{>0}$. The circle group C lies in the kernel of λ, so the norm map factors through a homomorphism $\mathbb{R}^{r_1} \oplus \mathbb{Z}^{r_2} \to \mathbb{R}^{>0} \stackrel{\log}{\to} (\mathbb{R}, +)$, which we will call λ. We claim that λ satisfies the hypotheses of Lemma 3.23. Indeed, if $r = 0$ then we are in the function field case, so the image of the norm map is an infinite cyclic subgroup of $\mathbb{R}^{>0}$, whereas if $r > 0$ then we are in the number field case and the norm map is surjective. It follows that any discrete, cocompact subgroup of $\mathcal{K} = \ker(\lambda)$ is isomorphic to $\mathbb{Z}^s \cong \mathbb{Z}^{\#S-1}$.

Step 3: Now consider the S-unit group $R_S^\times = K \cap \mathbb{I}_S(K)$. By Lemma 3.22, $R_S^\times \cap C = \mu(K)$, the finite group of roots of unity in K. Therefore we may define Γ to be the image of $R_S^\times$ in $G \cong \mathbb{R}^{r_1} \oplus \mathbb{Z}^{r_2}$; note that $\Gamma \cong R_S^\times / \mu(K)$. Moreover, since $K^\times$ is discrete and cocompact in $\mathbb{I}_K^1$ and $\mathbb{I}_K(S)$ is closed in $\mathbb{I}_K$, $R_S^\times = K^\times \cap \mathbb{I}_K(S)$ is discrete and cocompact in $\mathbb{I}_K^1(S) = \mathbb{I}_K^1 \cap \mathbb{I}_K(S)$. Therefore we may apply Lemma 3.23 to $\Gamma := R_S^\times / \mu(K)$, getting the desired result. □

Let us now admit that in the number field case, it is easy to deduce the S-Unit Theorem from the Dirchlet Unit Theorem.

EXERCISE 3.20. *Let K be a number field, and let S be a finite set of finite places of K (here we can ignore the infinite places). The injection $\mathbb{Z}_K \to \mathbb{Z}_{K,S}$ induces an injection on unit groups $\mathbb{Z}_K^\times \to \mathbb{Z}_{K,S}^\times$, and to prove the S-Unit Theorem modulo the Dirichlet Unit Theorem it suffices to show that $\mathbb{Z}_{K,S}^\times / \mathbb{Z}_K^\times$ is free commutative*

of rank $\#S$.
a) Write $S = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$. Consider the map

$$V : \mathbb{Z}_{K,S}^\times \to \mathbb{Z}^s,\ x \mapsto (\mathrm{ord}_{\mathfrak{p}_1}(x), \ldots, \mathrm{ord}_{\mathfrak{p}_s}(x)).$$

Show:

$$\mathbb{Z}_{K,S}^\times \cong \mathbb{Z}_K^\times \times V(\mathbb{Z}_{K,S}^\times),$$

so it suffices to show that $V(\mathbb{Z}_{K,S}^\times) \cong \mathbb{Z}^s$; equivalently, that $\mathbb{Z}^s/V(\mathbb{Z}_{K,S}^\times)$ is finite.
b) Let $h = \#\operatorname{Cl} K$ be the class number of K. Show: $V(\mathbb{Z}_{K,S}^\times) \supset h\mathbb{Z}^s$ and thus $[\mathbb{Z}^s : V(\mathbb{Z}_{K,S}^\times)] \leq h^s$.

2.4. A geometric approach.

In this section we discuss a less elementary, but more penetrating, approach to the S-class groups and S-unit groups in the function field case. For some of what we do we can work in more generality, namely for one variable function fields over an arbitrary ground field. Let k be any field. A field extension K/k is called a **function field in one variable** over k if K/k is finitely generated, of transcendence degree 1, and inside a fixed algebraic closure $\overline{K}$ of k we have that K and $\overline{k}$ are linearly disjoint over k. This latter condition implies that if l is a subextension of K/k such that l/k is algebraic then $l = k$ – "k is algebraically closed in K" – and in characteristic 0 these conditions are equivalent. It also implies that the ring $K \otimes_k \overline{k}$ is a domain: the latter condition is called "geometric integrality."

We define the **divisor group** $\mathrm{Div}(K)$ to be the free commutative group on the places of K. Again, we have a notion of principal divisors: for any $f \in K^\times$, we send f to its valuation vector $(v(f))$. And we may define the class group $\mathrm{Cl}(K) = \mathrm{Div}(K)/\operatorname{Prin}(K)$ exactly as above. However, this class group $\mathrm{Cl}(K)$ will in fact be *infinite* in all cases for a rather shallow reason: every divisor $D \in \mathrm{Div}(K)$ has a **degree** $D \in \mathbb{Z}$, the set of all degrees of divisors is a nontrivial subgroup $I\mathbb{Z}$ of $\mathbb{Z}$, and every principal divisor has degree 0.

For example, consider $K = \mathbb{F}_p(t)$. For each $n \in \mathbb{Z}^+$ let $D_n = n[\infty]$, where $[\infty]$ is the point at infinity. I claim that the D_n's are all distinct elements of $\mathrm{Cl}(K)$, which is therefore infinite. To see this, suppose not. Then there exist $m < n$ and a nonzero rational function $f \in \mathbb{F}_p(t)$ such that $f = (n-m)[\infty]$. But a rational function which is integral away from the place at ∞ is a polynomial, whereas the fact that $v_\infty(f) = n - m > 0$ means that f has negative degree: contradiction!

Those who have studied even a little algebraic geometry or Riemann surface theory will know a more convincing explanation: for any $f \in K^\times$, the principal divisor (f) has, in a natural sense, exactly as many zeros as it has poles. More precisely it has **degree zero**, whereas there are divisors on $\mathbb{F}_p(t)$ of any integer degree, so $\mathrm{Cl}(\mathbb{F}_p(t))$ must contain a copy of $\mathbb{Z}$.

Our task now is to define the degree map. To preserve the analogy with Riemann surface theory, we might as well work in a little more generality: in place of $\mathbb{F}_p$ we will take an arbitary field k as our constant field, and we will let K be a finite, separable extension of $k(t)$. For each place v of K which is trivial on k, the

residue field $k_v = R_v/\mathfrak{m}_v$ is a finite extension of k; let f_v be the residual degree. Then for an element $D = \sum n_v[v]$ of the divisor group, we define its degree

$$\deg(D) = \sum_v n_v f_v \in \mathbb{Z}.$$

As usual, we note that this sum is a finite sum because by definition $n_v = 0$ for all but finitely many places v.

PROPOSITION 3.25. *For any $f \in K^\times$, $\deg(f) = 0$.*

PROOF. First we address the case of a general ground field k. For a complete proof, see e.g. [**St**, Th. 1.4.11]. We will however give a sketch (that is less elementary than Stichtenoth's). A nonconstant function $f \in K$ is equivalent to finite map of algebraic curves $\pi : C \to \mathbb{P}^1$. For any closed point $x \in \mathbb{P}^1$, one can define the preimage of $\pi^*(x)$: as a divisor it is $\sum_{y \to x} e(y)[y]$, where valuation theoretically y runs through the places of K lying over the place corresponding to x on $\mathbb{P}^1$ and $e(y)$ and $f(y)$ are the usual ramification index. Theorem 1.71 implies that $\deg \pi^*(x) \leq [k(C) : k(t)]$. We claim that in fact equality holds using Theorem 1.73b): here R is the discrete valuation ring of functions on $\mathbb{P}^1$ that are regular at x. For this we need to know that the integral closure of R in $k(C)$ is finitely generated as an R-module (even if $k(C)/k(t)$ is not separable, which it need not be), and this follows from [**C:CA**, Thm. 18.4]. Now the divisor of f is equal to $\pi^*(0) - \pi^*(\infty)$, so it has degree 0.

Second we restrict our attention to the case in which $k = \mathbb{F}_q$. In this case we leave it to the reader to check that $\deg(f) = 0$ is manifestly equivalent to the product formula. □

Let I be the gcd of all degrees of divisors on K. Let $\mathrm{Div}^0(K)$ be the subgroup of degree zero divisors and $\mathrm{Prin}\, K$ be the principal divisors, so $\mathrm{Prin}\, K \subset \mathrm{Div}^0(K)$, and we put $\mathrm{Cl}^0(K) = \mathrm{Div}^0(K)/\mathrm{Prin}\, K$. Then we get an induced map

$$\deg : \mathrm{Cl}(K)/\mathrm{Cl}^0(K) \xrightarrow{\sim} I\mathbb{Z} \cong \mathbb{Z},$$

so $\mathrm{Cl}(K)$ is infinite.

Remark: In fact, if k is a finite field, we have $I(K) = 1$ always, i.e., the degree map is surjective. This was first proved by F.K. Schmidt around 1915 using (what would later be called!) the Hasse-Weil zeta function. For those who know some algebraic geometry, it should not be hard to use the Riemann hypothesis for curves over finite fields (proven by Weil) to show that for any smooth, projective curve $X_{/\mathbb{F}_q}$, for all sufficiently large n, X has degree n rational points. In particular, for some n it has a degree n rational point and also a degree $n+1$ rational point, and hence it has a divisor of degree 1. (But we will not use this result in the sequel.)

Because of Proposition 3.25, we may define $\mathrm{Div}^0(K) = \mathrm{Ker}(\deg)$, the kernel of the degree map and then $\mathrm{Prin}(K) \subset \mathrm{Div}^0(K)$. Thus finally we may define $\mathrm{Cl}^0(K) = \mathrm{Div}^0(K)/\mathrm{Prin}(K)$, the degree 0 divisor class group.

THEOREM 3.26. *For any finite separable extension $K/\mathbb{F}_p(t)$, the degree zero divisor class group $\mathrm{Cl}^0(K)$ is a finite commutative group.*

PROOF. If we look back at the proof of the number field case, we see immediately what needs to be modified: because we do not have Archimedean places,

it is not clear that the norm one idele class group surjects onto $\mathrm{Cl}(K)$. However, let $D = \sum_v n_v[v] \in \mathrm{Div}(K)$. We define an idele x_D as follows: for each v with $n_v \neq 0$, let $x_v \in K_v^\times$ be such that $v(x_v) = n_v$; as above, for every place v with $n_v = 0$, we define $x_v = 1$. Then $|x| = p^{\sum f_v n_v}$, whereas $\deg D = \sum f_v n_v$. Thus $\deg(D) = 0 \iff |x_D| = 1$. It follows that $C^1(K)$ surjects onto $\mathrm{Cl}^0(K)$, and the remainder of the proof proceeds as above. □

THEOREM 3.27. *(Rosen [**Ro73**]) Let $C^S := C \setminus S$ be a nonsingular, geometrically integral affine curve over a field k, and let $R_S = k[C^S]$ be the affine coordinate ring. Let $D^0(S)$ be the subgroup of $\mathrm{Div}^0 K$ of degree 0 divisors supported on S, and let $P(S) = \mathrm{Prin}(K) \cap D^0(S)$ be the principal divisors supported on S. Let d be the least positive degree of a divisor supported on S (so $d = 1$ if S contains a k-rational point), and let i be the least positive degree of a divisor on C. Then there are exact sequences*

$$1 \to k^\times \to R_S^\times \to P(S) \to 0 \tag{11}$$

and

$$0 \to D^0(S)/P(S) \xrightarrow{\iota} \mathrm{Cl}^0(K) \xrightarrow{\alpha} \mathrm{Cl}\, R_S \xrightarrow{\beta} C(d/i) \to 0, \tag{12}$$

, where $C(d/i)$ is a finite cyclic group of order d/i.

PROOF. The homomorphism $R_S^\times \to P(S)$ is the restriction to $R_S^\times$ of the map that associates to a nonzero rational function its associated divisor. That is is well-defined and surjective follows immediately from the definitions, and its kernel is the set of rational functions without zeros or poles, i.e., $k^\times$. This establishes (11).

The map ι is induced by mapping a degree zero divisor supported on S to its class in $\mathrm{Cl}^0 K = \mathrm{Div}^0 / \mathrm{Prin}(K)$; the kernel of this map is $\mathrm{Prin}\, K \cap D^0(S)$, so ι is injective. The map α is induced by the map $\mathrm{Div}^0 K \to \mathrm{Frac}\, R_S$ in which we simply remove the components of the divisor at places corresponding to S. Under this map, the divisor of a rational function f gets sent to the principal fractional ideal generated by f, hence we get a well-defined map $\mathrm{Cl}^0 K \to \mathrm{Cl}\, R_S$. Under this map, a degree zero divisor class represented by D maps to 0 iff there is a rational function f such that $D - (f)$ is supported on S, so the kernel of α is the image of ι.

The map β is the most interesting. We claim that an element of $\mathrm{Cl}\, R_S$ has a degree that is well-defined up to a multiple of d. Indeed, let I represent an element of $\mathrm{Cl}\, R_S$. Then if $D \in \mathrm{Div}\, K$ is any divisor that maps to I and X is any divisor supported on S, then also $D + X$ is a divisor that maps to I. (Modifying I within its equivalence class does not change the degree, since the degree of any principal divisor is 0.) Since the degree of every divisor supported on S is a multiple of d, there is a well-defined homomorphism $\mathrm{Cl}\, R_S \to \mathbb{Z}/d\mathbb{Z}$. The kernel of this homomorphism consists of divisors whose degree is a multiple of d, and thus the divisor X supported on S can be suitable chosen so that $\deg(X + S) = 0$ and thus I lies in the image of α. Conversely, any divisor lying in the image of α has degree a multiple of d, so the kernel of β is the image of α. The image of β is the set of all multiples of the least positive degree of a divisor on C, i.e., i. Thus the map β may be viewed as a surjection onto a finite cyclic group of order $\frac{d}{i}$, completing the proof. □

EXERCISE 3.21. *Suppose $S = P$ for some $P \in C(k)$. Show that the exact sequence reduces to an isomorphism $\mathrm{Pic}^0(C) \to \mathrm{Pic}(C^\circ)$. Now prove this directly.*

Let K be a function field over k, and let $S \subset \Sigma_K$ be a finite set of places. It is natural to ask about the structure of the unit group

$$R_S^\times = \{f \in K \mid v_P(f) = 0 \ \forall P \in \Sigma_K \setminus S\}$$

but unreasonable to expect it to be finitely generated: indeed we always have $k^\times \subset R_S^\times$ (with equality if $S = \varnothing$) and the unit group of a field is rarely finitely generated – indeed it could have any infinite cardinality. So it is natural to consider the "relative unit group" $R_S^\times/k^\times$. Let us say that the function field K is **Dirichlet** if for all finite subsets $S \subset \Sigma_K$, we have

$$R_S^\times/k^\times \cong \mathbb{Z}^{\#S-1}.$$

When k is finite, we have $k^\times = \mu(K)$, and thus the assertion that K is Dirichlet is precisely the S-Unit Theorem in the function field case.

THEOREM 3.28. *(Rosen* [**Ro73**]*) For a function field K/k, the following are equivalent:*
(i) The field K is Dirichlet.
(ii) The degree zero divisor class group $\mathrm{Cl}^0 K$ is torsion.

PROOF. Let S be a nonempty finite set of places of K containing the Archimedean places, and let $s = \#S$. By (11) we have

$$R_S^\times/k^\times = P(S),$$

the group of principal divisors supported on S. Since the group of divisors supported on S is free commutative of rank s and $D^0(S)$ is the kernel of a surjective homomorphism to $\mathbb{Z}$, we have $D^0(S) \cong \mathbb{Z}^{s-1}$. Since $P(S)$ is a subgroup of $D^0(S)$ we have $P(S) \cong \mathbb{Z}^r$ for some $r \leq s-1$, with equality iff $D^0(S)/P(S)$ is torsion.

By (12), if $\mathrm{Cl}^0(K)$ is torsion then so is $D^0(S)/P(S)$, so K is Dirichlet. Now suppose that K is Dirichlet, and let $D \in \mathrm{Div}^0 K$. Then $D \in D^0(S)$ for some finite S and the class of D in $\mathrm{Cl}^0 K$ lies in the image of $D^0(S)/P(S)$, so has finite order. □

Notice that when k is finite, this deduces the S-Unit Theorem from the finiteness of the class number.

2.5. An algebraic approach. In this section we offer a commutative algebraic variant of Theorems 3.24 and 3.28. We need the following result on the class group of an overring of a Dedekind domain.

THEOREM 3.29. *Let R be a Dedekind domain, and let $W \subset \mathrm{MaxSpec}\, R$. As above, we put*

$$R_W := \bigcap_{\mathfrak{p} \in \mathrm{MaxSpec}\, R \setminus W} R_{\mathfrak{p}}.$$

Also let $\mathrm{Frac}_W R := \bigoplus_{\mathfrak{p} \in W} \mathbb{Z}$ be the subgroup of fractional R-ideals supported on W. There is an exact sequence

$$1 \to R^\times \to R_W^\times \to \mathrm{Frac}_W R \to \mathrm{Pic}\, R \to \mathrm{Pic}\, R_W \to 1.$$

PROOF. See e.g. [**C:CA**, Thm. 23.7]. □

COROLLARY 3.30. *Let R be a Dedekind domain, and let $W \subset \operatorname{MaxSpec} R$.*
a) The relative unit group $R_W^\times/R^\times$ is free commutative of rank at most $\#W$.
b) Suppose $\operatorname{Cl} R$ is a torsion group. Then

$$R_W^\times \cong R^\times \times \bigoplus_{\mathfrak{p} \in W} \mathbb{Z}.$$

c) Let K be a global field. Then

$$K^\times \cong \mu(K) \times \bigoplus_{n=1}^{\infty} \mathbb{Z},$$

where $\mu(K)$ is the group of roots of unity in K, which is finite.

EXERCISE 3.22. *Prove Corollary 3.30.*

In fact the class of fields K such that $K^\times/\mu(K)$ is free commutative is much larger, containing for instance every field that is finitely generated over its prime subfield. See e.g. [**Ma80**].

3. Ray Class Groups and Ray Class Fields

3.1. Intro.

We wish to explain our earlier claim that the idele class group $C(K)$ is, as a topological group, a "target group" for global class field theory: i.e., its profinite completion is canonically isomorphic to the Galois group $\operatorname{Gal}(K^{\mathrm{ab}}/K)$.

Note first that the statement that $C(K)$ is such a target group is equivalent to the statement that $C^1(K)$ is such a target group: namely, we have in the number field case a short exact sequence

$$1 \to C^1(K) \to C(K) \to \mathbb{R}^{>0} \to 1$$

which shows that the inclusion $C^1(K) \hookrightarrow C(K)$ induces an isomorphism on the profinite completions.

EXERCISE 3.23. *What happens in the function field case?*

It may therefore be worth mentioning that the object $C(K)$ is for many purposes "more fundamental", whereas the subgroup $C^1(K)$ was – by virtue of being compact – technically more convenient to establish the two finiteness theorems of the previous section.

3.2. Moduli and ray class fields.

N.B.: On a first reading, I suggest that the reader make her task a little easier by: (i) restricting to the number field case, and (ii) ignoring – or mostly ignoring – the infinite part of the modulus.

What we can do is define a certain **family** $\{K(\mathfrak{m})\}$ of abelian extensions which are parameterized solely by some arithmetic data $\mathfrak{m}$ from K (you are not yet supposed to know what this means; don't worry). These field $K(\mathfrak{m})$ are called **ray class fields** of K. It is too much to hope for that every finite abelian extension of K is a ray class field, but what turns out to be true is that every abelian extension

L is **contained** in some ray class field – in fact, in infinitely many ray class fields, but there will be a unique **smallest** ray class field containing L. The Galois theory of subextensions of abelian extensions behaves beautifully – in particular every subextension is Galois – so that if we know all the ray class fields, we have a good chance at understanding all the finite abelian extensions.

Let me now describe the objects $\mathfrak{m}$ by which ray class fields are parameterized.

Recall that if $K/\mathbb{Q}$ is a number field of degree d, say given as $\mathbb{Q}[t]/(P(t))$, then the embeddings of K into $\mathbb{R}$ correspond precisely to the real roots of $P(t)$: in particular there is somewhere between 0 and $[K : \mathbb{Q}]$ such embeddings. Let us label these embeddings $\infty_1, \infty_2, \ldots, \infty_r$. We call such embeddings "real places."

The function field case is simpler: there are no real embeddings to worry about.

Now a **modulus** $\mathfrak{m}$ is a formal product of two different quantities: the first, **finite** part $\mathfrak{m}_0$, is precisely a nonzero integral ideal of R, which we further view as a formal product $\prod_v v^{\mathfrak{m}_{\mathfrak{o}} v}$. Note that in the number field case, this is simply a nonzero ideal of the ring of integers $\mathbb{Z}_K$. In the function field case, this is viewed purely formally, as an element of the divisor group $\operatorname{Div} K$.

In the function field case we put $\mathfrak{m} = \mathfrak{m}_0$. If K is a number field which has real places, then there is also an **infinite part** $\mathfrak{m}_\infty$, which you can think of as a subset of the real places but which we write formally as a product.

For a prime $\mathfrak{p}$ of R and a modulus $\mathfrak{m}$, define $\operatorname{ord}_{\mathfrak{p}} \mathfrak{m}$ just to be $\operatorname{ord}_{\mathfrak{p}}(\mathfrak{m}_0)$.

Example: When $K = \mathbb{Q}$, a modulus is either the ideal generated by a positive integer (n), or $(n) \cdot \infty$.

By $\operatorname{Frac}(K)$, we mean the free commutative group generated by the non-Archimedean places of K. Note that when K is a number field, this is the usual group of fractional $\mathbb{Z}_K$-ideals, where $\mathbb{Z}_K$ is the ring of integers of K. In the function field case, this is the commutative group that we formerly called $\operatorname{Div} K$, the divisor group of K.

Let $\mathfrak{m}$ be a modulus. We define two groups, $I(\mathfrak{m})$ and $P(\mathfrak{m})$, as follows:

Let $I(\mathfrak{m})$ be the free commutative group generated by finite places of K which do not divide $\mathfrak{m}$. Note that $I(\mathfrak{m}) = I(\mathfrak{m}_{\mathfrak{o}})$, i.e., this definition depends only on the finite part of the modulus. In particular $I(1) = \operatorname{Frac}(K)$. Moroever, if $\mathfrak{m}$ divides $\mathfrak{m}'$, then viewing both as subgroups of $\operatorname{Frac}(K)$ gives a natural inclusion $I(\mathfrak{m}) \to I(\mathfrak{m}')$.

Next, we define $P(\mathfrak{m})$ to be the subgroup generated by principal fractional ideals (α) with a generator α satisfying:

(i) for all finite places $v \mid \mathfrak{m}$, $\operatorname{ord}_{\mathfrak{p}}(x - 1) \geq \mathfrak{m}_v$, and
(ii) For all $\infty_i \in \mathfrak{m}_\infty$, $\infty_i(\alpha) > 0$.

It is easy to see that $P(\mathfrak{m})$ is a subgroup of $I(\mathfrak{m})$, so we may form the quotient: $\mathrm{Cl}_{\mathfrak{m}}(K) = I(\mathfrak{m})/P(\mathfrak{m})$, the **$\mathfrak{m}$-ray class group**. In the function field case, we also define $\mathrm{Cl}^0_{\mathfrak{m}}(K) = I^0(\mathfrak{m})/P(\mathfrak{m})$: then we have a short exact sequence

$$0 \to \mathrm{Cl}^0_{\mathfrak{m}}(K) \to \mathrm{Cl}_{\mathfrak{m}}(K) \to \mathbb{Z} \to 0,$$

so, unlike $\mathrm{Cl}_{\mathfrak{m}}(K)$, the group $\mathrm{Cl}^0_{\mathfrak{m}}(K)$ has a fighting chance of being finite.

EXAMPLE 3.31. *Again let $K = \mathbb{Q}$. If $\mathfrak{m} = (n)$, then $P(\mathfrak{m})$ just consists of principal ideals I which can be expressed in the form (x) with $x \equiv 1 \pmod{n}$. Note that the "expressed" is important here; since every nonzero ideal of $\mathbb{Z}$ has precisely two generators – x and $-x$ – what this really says is that I is generated by something which is $\pm 1 \pmod{n}$.*

EXERCISE 3.24. *Show: $I(n)/P(n) \cong (\mathbb{Z}/n\mathbb{Z})^\times/(\pm 1)$.*

The other kind of modulus is $\mathfrak{m} = (n)\infty$. Then $P(\mathfrak{m})$ consists of principal ideals I which can be expressed in the form (x) with $x > 0$ and $x \equiv 1 \pmod{n}$.

EXERCISE 3.25. *a) Show that for $n > 2$, $[P((n)) : P((n)\infty)] = 2$.*
b) Show that $I((n)\infty)/P((n)\infty) \cong (\mathbb{Z}/n\mathbb{Z})^\times$.

EXERCISE 3.26. *Let K be a global function field, and let $\mathfrak{m}$ be a modulus on K.*
a) Define a natural degree map (e.g. use the injection $I(\mathfrak{m}) \to \mathrm{Div}(K)$) to $\mathbb{Z}$.
b) Show that the degree map is surjective. (Hint: feel free to use the Weil bounds for curves over finite fields.)*
c) Define $I^0(\mathfrak{m})$ to be the kernel of the degree map. Show that $P(\mathfrak{m}) \subset I^0(\mathfrak{m})$.
d) Suppose that $K = \mathbb{F}_q(t)$ is a rational function field. Show that $I^0(1) = P(1)$.
e) Suppose that $K = \mathbb{F}_q(t)$, and let v be any one place of K, viewed as a modulus on K. Compute $I^0(v)/P(v)$.

There is a fairly evident notion of divisibility of moduli: we say that $\mathfrak{m} \mid \mathfrak{m}'$ if the finite part of $\mathfrak{m}$ divides the finite part of $\mathfrak{m}'$ in the usual sense of ideal division and if the set of real places in $\mathfrak{m}$ is a subset of the set of real places in $\mathfrak{m}'$. So e.g. for $K = \mathbb{Q}$ we have $(2) \mid (12) \mid (60\infty)$.

EXERCISE 3.27. *Let K be a global field and $\mathfrak{m}$, $\mathfrak{m}'$ be two moduli on K, with $\mathfrak{m} \mid \mathfrak{m}'$. In this case there is a natural inclusion map $\iota : I(\mathfrak{m}') \to I(\mathfrak{m})$: note well that ι is* injective *and not* surjective. *The map ι sends principal ideals congruent to 1 modulo $\mathfrak{m}'$ to principal ideals congruent to 1 modulo $\mathfrak{m}$. Thus there is an induced homomorphism of ray class groups $\bar{\iota} : \mathrm{Cl}_{\mathfrak{m}'}(K) \to \mathrm{Cl}_{\mathfrak{m}}(K)$.*
*a) Show that $\bar{\iota}$ is **surjective**. (Hint: weak approximation).*
b) Show that in the function field case we also have a surjective map on degree 0 ray class groups.

If L/K is a finite extension and ∞_i is a real place of K, we say that it is **unramified** in L if every extension of ∞_i to an embedding $\iota : L \hookrightarrow \mathbb{C}$ has $\iota(L) \subset \mathbb{R}$. Otherwise we say that it ramifies. For example, the place ∞ of $\mathbb{Q}$ ramifies in an imaginary quadratic field but not in a real quadratic field. More generally, if K is a number field, then $K/\mathbb{Q}$ is unramified at ∞ if for every embedding $\iota : K \hookrightarrow \mathbb{C}$ we have $\iota(K) \subset \mathbb{R}$. Such number fields are called **totally real**. (When $[K : \mathbb{Q}] > 2$ this is a stronger condition than just saying that K can be embedded into $\mathbb{R}$.)

At last we can describe the ray class fields $K(\mathfrak{m})$, at least indirectly.

For each modulus $\mathfrak{m}$, there exists an abelian extension $K(\mathfrak{m})/K$, called the $\mathfrak{m}$-**ray class field** of K, with the following properties:

(RC0) In the number field case, $K(\mathfrak{m})/K$ is finite. In the function field case, $K(\mathfrak{m})$ contains the maximal constant extension $\overline{\mathbb{F}_q}$, so is certainly infinite. But it is "otherwise finite", i.e., $K(\mathfrak{m})/K\overline{\mathbb{F}_q}$ is finite.

(RC1) $\mathfrak{p} \mid \Delta(K(\mathfrak{m})/K) \implies \mathfrak{p} \mid \mathfrak{m}$; also if an infinite place ∞_i of K ramifies in $K(\mathfrak{m})$ then $\infty_i \mid \mathfrak{m}$.

In other words, the extension is only ramified at primes (including "infinite primes") dividing the modulus.

In view of (RC1), we may restrict the Artin map to have domain $I(\mathfrak{m})$:

$$\mathfrak{r} : I(\mathfrak{m}) \to \mathrm{Gal}(K(\mathfrak{m})/K).$$

(Chebotarev tells us that this restricted map is still surjective.)

(RC2) The kernel of the restricted Artin map is precisely the subgroup $P(\mathfrak{m})$.

Therefore there is a canonical isomorphism

$$r : I(\mathfrak{m})/P(\mathfrak{m}) \xrightarrow{\sim} \mathrm{Gal}(K(\mathfrak{m})/K).$$

(RC3) If $\mathfrak{m} \mid \mathfrak{m}'$, $K(\mathfrak{m}) \subseteq K(\mathfrak{m}')$.

The divisbility relation endows the moduli with the structure of a directed set (a partially ordered set in which any pair of elements is less than or equal to some third element). Therefore by (RC3) the ray class fields form a directed system of fields.

(RC4) $\varinjlim_{\mathfrak{m}} K(\mathfrak{m}) = K^{\mathrm{ab}}$, the maximal abelian extension of K.

Passing to Galois groups, the immediate consequence is:

COROLLARY 3.32. *In the number field case, we have an isomorphism* $\mathrm{Gal}(K^{\mathrm{ab}}/K) \cong \varprojlim_{\mathfrak{m}} \mathrm{Cl}_{\mathfrak{m}}(K)$.

In the function field case, the extension $K\overline{\mathbb{F}_q}/K$ has Galois group $\hat{\mathbb{Z}}$, so the correct analogue is that we have a (necessarily split) short exact sequence

$$0 \to \varprojlim_{\mathfrak{m}} \mathrm{Cl}^0_{\mathfrak{m}}(K) \to \mathrm{Gal}(K^{\mathrm{ab}}/K) \to \hat{\mathbb{Z}} \to 0.$$

(RC4) itself is a slightly fancy way of saying that every finite abelian extension is contained in some ray class field. In fact we can be much more precise than this:

For a finite abelian extension L/K, put

$$\Gamma(L) = \mathrm{Ker}(r : I(\Delta(L/K)) \to \mathrm{Gal}(L/K)).$$

(RC5) There exists a unique smallest modulus $\mathfrak{c}$ such that $L \subset K(\mathfrak{m})$. Moreover, for this minimal $\mathfrak{c}$: the finite part of $\mathfrak{c}$ is divisible only by primes dividing $\Delta(L/K)$; the infinite part of $\mathfrak{c}$ includes no unramified inifnite places; and $P(\mathfrak{c}) \subset \Gamma(L)$, so that we have a short exact sequence

$$1 \to \Gamma(L)/P(\mathfrak{c}) \to I(\mathfrak{c})/P(\mathfrak{c}) \to \mathrm{Gal}(L/K) \to 1$$

exhibiting the Galois group of an arbitrary finite abelian extension L/K as a quotient of a certain ray class group.

The minimal modulus $\mathbf{c}$ for L/K of (RC5) is called the **conductor** of L/K.

The main result of global class field theory is that there is indeed a unique family of fields satisfying all of these properties. In the number field case, this was first shown by Artin, drawing partly on Chebotarev's proof of his density theorem.[5] There is no way we are going to discuss the proof here. All known proofs extremely long and difficult. What is worse, they are not really enlightening. The essential point is that although the proof of the theorem involves "constructing" the ray class fields in the sense of showing their existence, this construction is in general very far from being constructive or explicit. One of the great open problems in algebraic number theory is to give a reasonable explicit construction of the class fields of a given number field K. There are only two cases which are completely understood: the case of $\mathbb{Q}$, which we will give as an example below, and the case of an imaginary quadratic field, for which see Cox's book [**Cox**] and the notes for the 8430 course.

3.3. The Hilbert Class Field.

In this section we assume that K is a number field. (Again, there is a function field analogue which is not too hard to work out; we leave the correct statement to the interested reader.) Let us note the following extremely important special case: take $\mathfrak{m} = 1$, i.e., the "empty modulus."

THEOREM 3.33. *Concerning the ray class field $K(1)/K$:*
a) It is the maximal everywhere unramified abelian extension of K.
b) The map r induces a canonical isomorphism $I(1)/P(1) = \mathrm{Pic}(R) \xrightarrow{\sim} \mathrm{Gal}(K(1)/K)$.
c) A prime ideal $\mathfrak{p}$ of R splits completely in $K(1)$ iff it is a principal ideal of R.

PROOF. (RC1) says that $K(1)$ cannot be ramified anywhere (not even at the real places, if any). Moreover, (RC5) implies that any finite everywhere unramified abelian extension L is contained in $K(1)$, establishing a). By definition the Picard group of the Dedekind ring R is the fractional ideals modulo the principal fractional ideals, i.e., $I(1)/P(1)$, so b) follows from (RC2). Similarly part c) follows because a prime splits completely iff its Frobenius element is trivial iff it lies in the kernel $P(1)$ of the Artin map, i.e., is principal. □

Definition: The extension $K(1)/K$ is called the **Hilbert class field** of K.

[5]Unfortunately I do not know who first showed it in the function field case – it is even conceivable to me that this was also due to Artin, who certainly thought deeply about function fields.

As Theorem 3.33 shows, the Hilbert class field has some remarkable (and useful!) properties. In particular, the theorem implies that the maximal everywhere unramified abelian extension of K is finite, which is certainly not obvious.

3.4. An exact sequence for $\mathrm{Cl}_{\mathfrak{m}}(K)$. In this section we assume (for now?) that K is a number field. For a modulus $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$ of K, we know that there is a surjective group homomorphism $\mathrm{Cl}_{\mathfrak{m}}(K) \to \mathrm{Cl}\, K$. In this section we explicitly determine the kernel, following [**Coh**, Ch. 3].

We define

$$(\mathbb{Z}_K/\mathfrak{m})^\times := (\mathbb{Z}_K/\mathfrak{m}_0)^\times \oplus (\mathbb{Z}/2\mathbb{Z})^{\#\mathfrak{m}_\infty}.$$

That is, $(\mathbb{Z}_K/\mathfrak{m})^\times$ is the direct product of the usual unit group of the residue ring modulo the ideal $\mathfrak{m}_0$ with an elementary 2-group whose $\mathbb{F}_2$-rank is equal to the number of real places in $\mathfrak{m}_\infty$. We put

$$\varphi(\mathfrak{m}) := \#(\mathbb{Z}_K/\mathfrak{m})^\times = 2^{\#\mathfrak{m}_\infty}\varphi(\mathfrak{m}_0).$$

EXERCISE 3.28. *Let $\mathfrak{m}_0 = \mathfrak{p}_1^{a_1}\cdots\mathfrak{p}_r^{a_r}$ be the prime power factorization, and suppose that $N(\mathfrak{p}_i) = \#\mathbb{Z}_K/\mathfrak{p}_i = p_i^{f_i}$ for (not necessarily distinct) prime numbers p_i and positive integers f_i. Show:*

$$\varphi(\mathfrak{m}_0) = \prod_{i=1}^{r} N(\mathfrak{p}_i)^{a_i-1}(N(\mathfrak{p}_i)-1).$$

We put

$$K_{\mathfrak{m}}^\times := \{x \in K^\times \mid x \equiv 1 \pmod{\mathfrak{m}}\},$$
$$U(K) = \mathbb{Z}_K^\times,\ U_{\mathfrak{m}}(K) = U(K) \cap K_{\mathfrak{m}}^\times.$$

THEOREM 3.34. *We have an exact sequence*

$$1 \to U_{\mathfrak{m}}(K) \to U(K) \xrightarrow{\rho} (\mathbb{Z}_K/\mathfrak{m})^\times \xrightarrow{\psi} \mathrm{Cl}_{\mathfrak{m}}(K) \xrightarrow{\phi} \mathrm{Cl}\, K \to 1.$$

PROOF. The map $U_{\mathfrak{m}}(K) \to U(K)$ is inclusion and the map $\mathrm{Cl}_{\mathfrak{m}}(K) \to \mathrm{Cl}(K)$ is the aforementioned quotient map. Also the quotient map $\mathbb{Z}_K \to \mathbb{Z}_K/\mathfrak{m}_0$ induces a homomorphism on unit groups $\rho_1 : U(K) \to (\mathbb{Z}_K/\mathfrak{m}_0)^\times$. The map $\rho_2 : U(K) \to (\mathbb{Z}/2\mathbb{Z})^{\#\mathfrak{m}_\infty}$ maps a unit u to its "signature," i.e., for each real place $\infty_i \in \mathfrak{m}_\infty$, the ith component of $\rho_2(u)$ is 1 if $\infty_i(u)$ is positive and -1 if $\infty_i(u)$ is negative. Then we put $\rho = \rho_1 \times \rho_2$.

To define the map ρ, first we observe that the map $\rho : \mathbb{Z}_K \to (\mathbb{Z}_K/\mathfrak{m}_0)^\times \times (\mathbb{Z}/2\mathbb{Z})^{\mathfrak{m}_\infty}$ is surjective by Strong Approximation (cf. [**Coh**, p. 4]). We define the map ψ by mapping $\rho(\alpha) \in (\mathbb{Z}_K/\mathfrak{m})^\times$ to the class of $\alpha\mathbb{Z}_K$ in $\mathrm{Cl}_{\mathfrak{m}}(K)$. We need to check that this is well-defined: if $\rho(\alpha) = \rho(\beta)$, then α and β are coprime to $\mathfrak{m}_0$, we have $\alpha \equiv \beta \pmod{\mathfrak{m}_0}$ and $\mathrm{sgn}(\infty_i(\alpha)) = \mathrm{sgn}(\infty_i(\beta))$ for all $\infty_i \in \mathfrak{m}_\infty$. It follows that $\frac{\alpha}{\beta} \equiv 1 \pmod{\mathfrak{m}}$, so the ideals $\alpha\mathbb{Z}_K$ and $\beta\mathbb{Z}_K$ determine the same element of $\mathrm{Cl}_{\mathfrak{m}}(K)$.

That the kernel of ρ is $U_{\mathfrak{m}}(K)$ is really the definition of $U_{\mathfrak{m}}(K)$. Moreover, we have $\psi(\rho(\alpha)) = 1$ iff $\alpha\mathbb{Z}_K \in P_{\mathfrak{m}}(K)$, i.e., there is $\beta \equiv 1 \pmod{\mathfrak{m}}$ such that $\alpha\mathbb{Z}_K = \beta\mathbb{Z}_K$, and thus $u := \frac{\alpha}{\beta} \in U(K)$. Since $\beta \equiv 1 \pmod{\mathfrak{m}}$ the images of u and α in $(\mathbb{Z}_K/\mathfrak{m})^\times$ agree and thus the kernel of ψ is contained in the image of ρ. Conversely, starting with any $u \in \mathbb{Z}_K^\times$ we get the class of the ideal $u\mathbb{Z}_K = 1\mathbb{Z}_K$ in $\mathrm{Cl}_{\mathfrak{m}}(K)$, which is certainly trivial.

If an ideal class $[\mathfrak{a}] \in \mathrm{Cl}_{\mathfrak{m}}\, K$ is mapped to the trivial element of $\mathrm{Cl}\, K$, then

$\mathfrak{a} = \alpha\mathbb{Z}_K$ is a principal fractional ideal coprime to $\mathfrak{m}_0$, hence α is coprime to $\mathfrak{m}_0$, so $[\mathfrak{a}]$ lies in the image of ψ.

The surjectivity of ϕ follows from the fact every ideal class in a Dedekind domain has a representative that is prime to $\mathfrak{m}_0$, which is itself an easy consequence of Artin-Whaples approximation. □

The following useful consequence is immediate.

COROLLARY 3.35. *We have a short exact sequence*

$$1 \to (\mathbb{Z}_K/\mathfrak{m})^\times / \operatorname{Image}(U(K)) \to \operatorname{Cl}_{\mathfrak{m}}(K) \to \operatorname{Cl}(K) \to 1,$$

and thus

$$\#\operatorname{Cl}_{\mathfrak{m}}(K) = \#\operatorname{Cl}(K)\frac{\varphi(\mathfrak{m})}{[U(K) : U_{\mathfrak{m}}(K)]}.$$

EXERCISE 3.29. *Use Corollary 3.35 to deduce that for $n \leq 2$ we have*

$$\mathbb{Q}((n)) = \mathbb{Q}((n)\infty) = \mathbb{Q}$$

and that for $n \geq 3$ we have

$$[\mathbb{Q}((n)) : \mathbb{Q}] = \frac{\varphi(n)}{2},\ [\mathbb{Q}((n)\infty) : \mathbb{Q}] = \varphi(n).$$

EXERCISE 3.30. *Let K be an imaginary quadratic field. Since we have no real places, for any modulus $\mathfrak{m}$ we have $\mathfrak{m} = \mathfrak{m}_0$.*
a) Suppose $K \neq \mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{-3})$. Show:

$$[K(\mathfrak{m}) : K] = \begin{cases} \varphi(\mathfrak{m}) & \mathfrak{m} \mid (2) \\ \frac{\varphi(\mathfrak{m})}{2} & \mathfrak{m} \nmid (2) \end{cases}.$$

b) Suppose $K = \mathbb{Q}(\sqrt{-1})$. Show:

$$[K(\mathfrak{m}) : K] = \begin{cases} \varphi(\mathfrak{m}) & \mathfrak{m} \mid (1+i) \\ \frac{\varphi(\mathfrak{m})}{2} & \mathfrak{m} \nmid (1+i) \text{ and } \mathfrak{m} \mid (2) \\ \frac{\varphi(\mathfrak{m})}{4} & \mathfrak{m} \nmid 2 \end{cases}.$$

c) Suppose $K = \mathbb{Q}(\sqrt{-3})$. Show:

$$K(\mathfrak{m}) : K] = \begin{cases} 1 & \mathfrak{m} = (1) \\ \frac{\varphi(\mathfrak{m})}{2} & \mathfrak{m} \neq (1) \text{ and } \mathfrak{m} \mid (\zeta_3 - 1) \\ \frac{\varphi(\mathfrak{m})}{3} & \mathfrak{m} = (2) \\ \frac{\varphi(\mathfrak{m})}{6} & \text{otherwise} \end{cases}.$$

3.5. Remarks on real places, narrow class groups, et cetera.

Let K be a number field, and v a real place of K, i.e., an Archimedean norm on K with completion $K_v = \mathbb{R}$. Let L be a finite extension of K. As we know, the norms on L extending v on K correspond to the maximal ideals in the algebra $L \otimes_K \mathbb{R}$, which is a finite dimensional, separable $\mathbb{R}$-algebra, hence isomorphic to $\mathbb{R}^{s_1} \oplus \mathbb{C}^{s_2}$, where $s_1 + 2s_2 = [L : K]$. If w is a norm on L extending the real norm v, we say that $w|v$ is **ramified** if $L_w \cong \mathbb{C}$ and otherwise that $w|v$ is unramified.

Now let $\mathfrak{m}$ be a modulus on K. If the real place v does not appear in $\mathfrak{m}$, then the corresponding ray class field $K(\mathfrak{m})$ is unramified over v: i.e., every place w of

$K(\mathfrak{m})$ dividing v is unramified.

Now one case worth examining explicitly is the case of ray class fields corresponding to moduli $\mathfrak{m}$ whose finite part $\mathfrak{m}_0$ is 1 but for which ramification at real places is allowed. For this, let us define the modulus ∞ simply to include all real infinite places, and to avoid trivialities we assume that K is not totally imaginary, i.e., that it has at least one real place.

Now consider the ray class group $\mathrm{Cl}_\infty(K)$: explicitly, this is the group of all fractional $R = \mathbb{Z}_K$-ideals modulo principal ideals with totally positive generators. This is often called the **narrow class group** of K. For distinction, the usual ideal class group $\mathrm{Cl}(K)$ is then sometimes called the **wide class group**.

Just for brevity, let us define $q_\infty = \frac{\#\,\mathrm{Cl}_\infty(K)}{\#\,\mathrm{Cl}(K)}$. This is a positive integer.

If K has r_1 real places, it is clear that $q_\infty \mid 2^{r_1}$.

EXERCISE 3.31. *Show that in fact $q_\infty \mid 2^{r_1-1}$ and that the kernel of the map $\mathrm{Cl}_\infty(K) \to \mathrm{Cl}(K)$ is a 2-torsion group (aka an "elementary 2-group").*

More explicitly, the discrepancy between the wide and narrow ideal class groups may be interpreted in terms of the possible signatures of units in K.

For example, let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field.

EXERCISE 3.32. *a) For K a real quadratic field, show that the following are equivalent:*
(i) The groups $\mathrm{Cl}_\infty(K)$ and $\mathrm{Cl}(K)$ coincide.
(ii) The fundamental unit of K has norm -1.
(iii) There exist units in $\mathbb{Z}_K$ of all four possible signatures $(+,+)$, $(+,-)$, $(-,+)$, $(-,-)$ with respect to the pair of real places (∞_1, ∞_2) of K.
(iv) The period length of the contiinued fraction expansion of $\sqrt{d}$ is odd.[6]
b) If the equivalent conditions of part a) do not hold, then $[\mathrm{Cl}_\infty(K) : \mathrm{Cl}(K)] = 2$.

In practice, when dealing with real quadratic fields (and more generally totally real fields), things often become simpler when we assume that the *narrow* class number is one, rather than the usual class number. Thus "narrow class number one" appears as a technical hypothesis in many theorems in algebraic number theory and arithmetic geometry.

EXERCISE 3.33. *Consider the real quadratic fields $\mathbb{Q}(\sqrt{d})$ for $d = 2, 3, 5, 6, 7, 10$.*
a) Compute the ideal class groups.
b) Compute the narrow class groups.

In particular, it is certainly possible for $\mathrm{Cl}_\infty(K) = 1$. (Thus the conductor of the ∞-ray class field can be equal to 1.) Moreover, it has been conjectured at least since Gauss's time that there are infinitely many real quadratic fields of narrow class number one. Indeed, heuristics predict that when real quadratic fields are ordered by discriminant, a positive proportion of them will have narrow class number one. This is one of the great open problems of algebraic number theory!

[6]Note that the equivalence of (ii), (iii) and (iv) is part of the classical theory of quadratic fields and is often discussed in elementary texts udner the name **Pell equation**.

3.6. A word about class field towers.

In this section we restrict to the case of number fields.

The Hilbert class field is one of the most remarkable (and also useful) constructions in all of algebraic number theory. Even the fact that the maximal everywhere unramified abelian extension of a number field is *finite* is deep and surprising. We wish to drive this point home by examining what happens when the word "abelian" is removed.

When $K = \mathbb{Q}$, one does not have to appeal to class field theory to see that the maximal everywhere unramified abelian extension of $\mathbb{Q}$ is simply $\mathbb{Q}$. Indeed, in a first course in algebraic number theory one learns the stronger fact that every proper finite extension $L/\mathbb{Q}$ is unramified at at least one finite place, which follows from Minkowski's lower bound on the discriminant of a number field: see e.g. [**Bak**, Cor. 3.14]. However, for an algebraic number field $K \neq \mathbb{Q}$, there may very well be an infinite degree everywhere unramified extension L/K. (Note that if there exists such an extension, its normal closure remains everywhere unramified, hence there exists an infinite degree everywhere unramified *Galois* extension M/K.) Indeed – quite remarkably – the Hilbert class field is an essential tool in such constructions!

The idea is this: suppose that K is a number field. Then we can take its Hilbert class field which, for reasons which will shortly become apparent, we will write in this section (only) as K^1. We know that K^1/K is finite, but we can certainly ensure – e.g. using imaginary quadratic fields, by the aid of genus theory – that $K^1 \neq K$. Now we have a new number field, and we can take *its* Hilbert class field, say K^2. Proceeding in this way, we get an increasing sequence of number fields K^n. Put $K^\infty = \bigcup_n K^n$. Note that K^∞ is everywhere unramified over K (equivalently, every finite subextension is everywhere unramified over K). Indeed, this follows immediately from the tower property of unramified extensions.

Now a basic dichotomy occurs:

Case 1: After some point, we reach a field K^N which has class number one, so that $K^N = K^{N+1} = K^{N+2} = \ldots$. Thus $K^\infty = K^N$ has finite degree over K.

Case 2: For all n, $K^n \subsetneq K^{n+1}$, and thus K^∞ has infinite degree over K.

Evidently if we are in Case 2, we get an infinite degree everywhere unramified (even solvable) extension K^∞/K.

The sequence of number fields K^N attached to K is usually called the **class field tower** of K. Thus the question is: is there a number field K whose class field tower is strictly increasing? This problem was posed by Fürtwangler and considered by Hasse in 1926. However, it was not solved until 1964, when Golod and Shafarevich gave examples in which the class field tower was infinite. Explicitly, one may take $K = \mathbb{Q}(\sqrt{-2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13}) = \mathbb{Q}(\sqrt{-30030})$.

To the best of my knowledge, if one is given a number field K, it is a difficult problem to decide whether its class field tower is infinite. Certainly class field towers remain an active topic of contemporary research. For more information, I recommend the excellent survey article by P. Roquette in [**CF**].

3.7. Class field theory over $\mathbb{Q}$.

But first let us look at the one case where it is easy to at least state what the class fields are: $K = \mathbb{Q}$. Recall that we computed above that if $\mathfrak{m} = n$, the $\mathfrak{m}$-ray class group is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times/\pm 1$, whereas if $\mathfrak{m} = n\infty$, the $\mathfrak{m}$-ray class group is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$.

So we would like to find – or at least to correctly guess – for every positive integer n an abelian extension $\mathbb{Q}(n)/\mathbb{Q}$ whose Galois group is $(\mathbb{Z}/n\mathbb{Z})^\times/\pm 1$ and another abelian extension $\mathbb{Q}(n\infty)/\mathbb{Q}$ with Galois group $(\mathbb{Z}/n\mathbb{Z})^\times$.

If we have made it this far, we would have to guess that $\mathbb{Q}(n\infty) = \mathbb{Q}(\zeta_n)$, wouldn't we? It has the right Galois group and the right ramification properties: the only finite primes at which if ramifies are those dividing $n = \mathfrak{m}$, in accordance with (RC1). In fact in a previous exercise we computed the Artin map in this case, so we can verify that these are the $(n\infty)$-ray class fields: I leave it to you to do so.

What about the moduli $\mathfrak{m} = n$? The point here is that we have not included ∞, so that by (RC1) the ray class field $\mathbb{Q}(n)$ is not allowed to ramify at ∞: in other words, it must be totally real.

Exercise 3.34. *Deduce from the axioms for ray class fields that* $\mathbb{Q}(n) = \mathbb{Q}(\zeta_n + \zeta_n^{-1})$.

Applying (RC4) we get a very important result:

Theorem 3.36. *(Kronecker-Weber) A finite extension $K/\mathbb{Q}$ is abelian iff it is a subfield of some cyclotomic field $\mathbb{Q}(\zeta_n)$. Equivalently, the maximal abelian extension $\mathbb{Q}^{ab}$ of $\mathbb{Q}$ is the (infinite algebraic) extension obtained by adjoining to $\mathbb{Q}$ all roots of unity.*

In particular, we have a single transcendental function, namely $e(t) := e^{2\pi i t}$ which maps $\mathbb{R}/\mathbb{Z}$ isomorphically to the unit circle in the complex plane. Then for all n, the $n\infty$-ray class field of $\mathbb{Q}$ is obtained by adjoining to $\mathbb{Q}$ the value of the function e at the n-torsion points of the one-dimensional torus $\mathbb{R}/\mathbb{Z}$, namely at $\frac{1}{n}, \ldots, \frac{n-1}{n}$ (or also at just $\frac{1}{n}$, of course). Wouldn't it be amazing if all (or a cofinal set) of class fields for any number field K could be obtained just by adjoining special values of a nice transcendental function? This was Kronecker's **Jugendtraum** ("youthful dream.") We will see later that this dream comes true when K is an imaginary quadratic field.[7]

Exercise 3.35. *a) Notice that $\mathbb{Q}(1) = \mathbb{Q}(\infty)$, which shows that the association of a ray class field to a modulus need not be injective.*

[7]Much of the work on automorphic functions in number theory in the last 50 years has been motivated by a desire to extend this Jugendtraum to other fields. There are indeed some results in this direction, but it is remarkable how much more complicated any other case is – even for e.g. a real quadratic field there is not to my knowledge a complete, satisfactory answer.

b) Find all moduli $\mathfrak{m}$ *such that* $\mathbb{Q}(\mathfrak{m}) = \mathbb{Q}$.
c) Show that if n *is odd, then* $\mathbb{Q}(n \cdot \infty) = \mathbb{Q}(2n \cdot \infty)$.
d) Find all pairs $\mathfrak{m} \neq \mathfrak{m}'$ *such that* $\mathbb{Q}(\mathfrak{m}) = \mathbb{Q}(\mathfrak{m}')$.

This exercise implies that the conductor of the $\mathfrak{m}$-ray class field $K(\mathfrak{m})$ may be strictly smaller than $\mathfrak{m}$, unlike what virtually everyone expects at first!

EXERCISE 3.36. *Let* p *be an odd prime. Certainly* $\mathbb{Q}(\sqrt{p})/\mathbb{Q}$ *and* $\mathbb{Q}(\sqrt{-p})$ *are an abelian extension. What are their conductors? (And what can you say about the conductor of an arbitrary quadratic extension* $\mathbb{Q}(\sqrt{D})$*?)*

EXERCISE 3.37. *Use class field theory to prove the quadratic reciprocity law.*

3.8. Idelic interpretation. The goal here is to define each ray class group $G(\mathfrak{m})$ as a discrete quotient of the idele class group C. That is, we wish to find for each $\mathfrak{m}$ an open finite-index subgroup of $C(K)$ whose quotient is $G(\mathfrak{m})$ – compatibly with inclusions – and also to see that these open subgroups are cofinal in the set of all open finite index subgroups of $C(K)$, so that the profinite completion of $C(K)$ is isomorphic to the inverse limit of the ray class groups, i.e., to the Galois group of the maximal abelian extension of K.

It seems best to begin with the ideal class group, which we wish to be attached to the modulus $\mathfrak{m} = 1$. As we saw, this can be viewed as a quotient of $C(K)$ via the valuation map $v : \mathbb{I}_K \to \mathrm{Frac}(K)$ which sends an idele $(x_v)_v$ to its sequence of valuations at finite places $(v(x_v))$. The kernel of this map is

$$U(1) := \prod_{NAv} U_v \times \prod_{v \mid \infty} K_v^\times.$$

Therefore after passage to the quotient we get an isomorphism

$$K^\times \backslash \mathbb{I}^K / U(1) \xrightarrow{\sim} \mathrm{Cl}(K).$$

Now let $\mathfrak{m}$ be a modulus on K. For all places v dividing $\mathfrak{m}$, we define $W_{\mathfrak{m}}(v)$. Namely, if v is non-Archimedean, we put $W_{\mathfrak{m}}(v) = 1 + \mathfrak{p}_v^{\mathfrak{m}_v} R_v = U_v^{\mathfrak{m}_v}$, the $\mathfrak{m}_{\mathfrak{v}}$th higher unit group, whereas if v is real Archimedean, we put $W_{\mathfrak{m}}(v) = \mathbb{R}^{>0}$.

Also put

$$\mathbb{I}_{\mathfrak{m}} = \left(\prod_{v \nmid \mathfrak{m}} K_v^\times \times \prod_{v \mid \mathfrak{m}} W_{\mathfrak{m}}(v) \right) \cap \mathbb{I}.$$

PROPOSITION 3.37. *We have:*

$$P(\mathfrak{m}) = K^\times \cap \prod_{v \mid \mathfrak{m}} W_{\mathfrak{m}}(v) = K^\times \cap \mathbb{I}_{\mathfrak{m}}.$$

EXERCISE 3.38. *Prove Proposition 3.37.*

Now we put

$$U(\mathfrak{m}) := \prod_{v \nmid \infty} U_v^{\mathfrak{m}_v} \times \prod_{v \mid \infty} K_v(\mathfrak{m}_v).$$

EXERCISE 3.39. *a) Show that* $U(\mathfrak{m})$ *is a finite index open subgroup of* $U(\mathfrak{1})$.
b) Deduce that the quotient group $K^\times \backslash \mathbb{I}^K / U(\mathfrak{m})$ *is finite.*

We define a map $v : \mathbb{I}_{\mathfrak{m}} \to I(\mathfrak{m})$ in the familiar way: we send the idele $(x_v)_v$ to its vector of valuations $v(x_v)$ for x_v lying outside $\mathfrak{m}_0$. This is evidently a surjective homomorphism.

LEMMA 3.38. *(Kernel-Cokernel Sequence) Let $A \stackrel{f}{\to} B \stackrel{g}{\to} C$ be a pair of homomorphisms of commutative groups. Then there is an exact sequence*

$$0 \to \operatorname{Ker} f \to \operatorname{Ker}(g \circ f) \stackrel{f}{\to} \operatorname{Ker} g \to \operatorname{Coker} f \to \operatorname{Coker}(g \circ f) \to \operatorname{Coker} g \to 0.$$

PROOF. See [**Mil**, Appendix A]. □

PROPOSITION 3.39. *a) The homomorphism v induces an isomorphism*

$$P(\mathfrak{m})\backslash\mathbb{I}_{\mathfrak{m}}/U(\mathfrak{m}) \stackrel{\sim}{\to} \mathrm{Cl}_{\mathfrak{m}}(K).$$

b) The inclusion $\mathbb{I}_{\mathfrak{m}} \hookrightarrow \mathbb{I}$ induces an isomorphism

$$\mathbb{I}_{\mathfrak{m}}/P(\mathfrak{m}) \stackrel{\sim}{\to} \mathbb{I}^{\times}/K^{\times}.$$

PROOF. The map $P(\mathfrak{m}) \to \mathbb{I}_{\mathfrak{m}}$ is an injection, and the map $\Phi : \mathbb{I}_{\mathfrak{m}} \to I(\mathfrak{m})$ is a surjection with kernel $U(\mathfrak{m})$. The "kernel-cokernel sequence" of this pair of maps is therefore

$$U(\mathfrak{m}) \to \mathbb{I}_{\mathfrak{m}}/P(\mathfrak{m}) \to C(\mathfrak{m}) \to 1,$$

which proves part a). As for part b), the kernel of $\mathbb{I}_{\mathfrak{m}} \to \mathbb{I}/K^{\times}$ is $K^{\times} \cap \mathbb{I}_{\mathfrak{m}}$ which, by Proposition 8.10, is equal to $P(\mathfrak{m})$. Therefore the map $\mathbb{I}_{\mathfrak{m}}/P(\mathfrak{m}) \stackrel{\sim}{\to} \mathbb{I}^{\times}/K^{\times}$ is an injection. That is a surjection follows from a weak approximation argument very similar to that of Exercise 3.27. Details are left to the reader as a useful (and not difficult) exercise. □

Putting these results together, we get:

THEOREM 3.40. *We have a canonical isomorphism*

$$K^{\times}\backslash\mathbb{I}^{K}/U(\mathfrak{m}) \stackrel{\sim}{\to} I(\mathfrak{m})/P(\mathfrak{m}).$$

EXERCISE 3.40. *a) If K is a number field, deduce that every ray class group $\mathrm{Cl}_{\mathfrak{m}}(K)$ is finite.*
b) If K is a function field, deduce that every ray class group $\mathrm{Cl}^0_{\mathfrak{m}}(K)$ is finite.

EXERCISE 3.41. *a) Let K be a number field. Show that every finite index open subgroup of $C(K) = K^{\times}\backslash\mathbb{I}_K$ contains $K^{\times}U(\mathfrak{m})$ for some modulus $\mathfrak{m}$. In particular, the profinite completion of $C(K)$ is isomorphic to the inverse limit $\varprojlim_{\mathfrak{m}} K^{\times}\backslash\mathbb{I}_K/U(\mathfrak{m})$.*
b) State and prove an appropriate analogue of part a) in the function field case.

EXERCISE 3.42. *Deduce from Exercise 8.14 and Corollary 3.32 that the idele class group $C(K)$ is a target group for global class field theory: i.e., its profinite completion is isomorphic to $\mathrm{Gal}(K^{\mathrm{ab}}/K)$.*

Please remember that Corollary 3.32 is merely a group-theoretic restatement of property (RC4) of ray class fields, i.e., that they are cofinal in all finite abelian extensions L/K and that we have by no means proved this property (or any of the four other properties of ray class fields). Conversely, it is not so hard to deduce the ideal-theoretic properties of ray class groups and fields from this idelic

description. It is indeed possible to **prove** these results (and other ones that we have not even stated) of global class field theory either using the classical ideal-theoretic approach (which involves some quite intricate counting arguments) or via the idele-theoretic formulation. Most contemporary mathematicians prefer this latter approach – among other things, it can be made to match up formally with the proofs of the main results of local class field theory. The key ingredient for the "modern" proofs both locally and globally is Galois cohomology of $K^\times$ and of $C(K)$, and specifically the formalism of **class formations**. These notions are beyond the scope of this course. In my opinion the most careful, complete and readable treatment of the local and global cases is to be found in Milne's book-length set of lecture notes on Class Field Theory [**Mil**].

CHAPTER 4

Complements and Applications

1. Mahler series

In this section we follow [**Ro**, Chapter 4].

1.1. Introduction.

One of the great theorems of classical analysis is the Weierstrass Approximation Theorem: every continuous function $f : [a, b] \to \mathbb{R}$ is a uniform limit of polynomial functions. More generally, one has the **Stone-Weierstrass Theorem**: Let X be a compact metric space, and let $\mathcal{A}$ be an algebra of continuous real-valued functions on X that **separates points** – for all $x \neq y \in X$ there is $f \in \mathcal{A}$ with $f(x) \neq f(y)$ – and **vanishes at no point**: for all $x \in X$, there is $f \in \mathcal{A}$ with $f(x) \neq 0$. Then every continuous function $f : X \to \mathbb{R}$ is a uniform limit of a sequence of functions in $\mathcal{A}$.

It is natural to inquire about p-adic analogues of these results. The p-adic analogue of $[a, b]$ is a closed ball. Just as in $\mathbb{R}$ by making an affine linear change of variables we may as well consider $[0, 1]$, in $\mathbb{Q}_p$ by an affine linear change of variables we may consider $\mathbb{Z}_p$. Notice that $\mathbb{Z}_p$ is again a compact metric space, so *Stone*-Weierstrass applies. In fact, since $\mathbb{Z}_p$ is compact, totally disconnected, metrizable, and containing more than a single point, it is isomorphic to the classical Cantor set, so there is a topological embedding $\iota : \mathbb{Z}_p \hookrightarrow \mathbb{R}$. Let $\mathbb{R}[\iota]$ be the subalgebra of real-valued functions on $\mathbb{Z}_p$ generated by $1_{\mathbb{Z}_p}$ and ι: these are precisely the polynomial functions in ι, which explains the notation. We need look no further than 1 and ι to see that $\mathbb{R}[\iota]$ separates points of $\mathbb{Z}_p$ and vanishes at no point of $\mathbb{Z}_p$, hence by Stone-Weierstrass, every continuous function $f : \mathbb{Z}_p \to \mathbb{R}$ is a uniform limit of polynomials in ι. If we want to think of $\mathbb{Z}_p$ as being embedded inside of $\mathbb{R}$ then this is a close cousin of the classical Weierstrass Theorem. The entire discussion applies verbatim with $\mathbb{Z}_p$ replaced by any compact DVR.

However this is not a very satisfying p-adic analogue of Weierstrass approximation, since the function ι does not have an intrinsic meaning in terms of $\mathbb{Z}_p$. A better p-adic analogue would consider not continuous functions $f : \mathbb{Z}_p \to \mathbb{R}$ but continuous functions $f : \mathbb{Z}_p \to \mathbb{Q}_p$, or more generally with values in some complete ultrametric field containing $\mathbb{Q}_p$. In fact, observing that polynomials $p(t) \in \mathbb{Q}_p[t]$ give continuous functions from $\mathbb{Z}_p$ to $\mathbb{Q}_p$, we can ask a better question.

QUESTION 4.1. *Is every continuous function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ a uniform limit of polynomial functions $p_n(t) \in \mathbb{Q}_p[t]$?*

Kurt Mahler gave a positive answer to this question. But in fact he did much more. In the setting of the classical Weierstrass Approximation Theorem, for a general continuous function $f : [0, 1] \to \mathbb{R}$ there are many different sequences of polynomial

functions converging uniformly to f, there is not in any useful sense a *canonical* such sequence. However, Mahler constructed a class of series of polynomials such that every continuous function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ is represented by a *unique* such series, which moreover has a useful connection to **p-adic interpolation**.

Let us motivate this last part. The standard representation of $\mathbb{Z}_p$ as a series $\sum_n a_n p^n$ with $a_n \in \{0, \ldots, p-1\}$ shows that $\mathbb{N}$ is dense in $\mathbb{Z}_p$. Thus any continuous function $f : \mathbb{Z}_p \to \mathbb{Q}_p$ is entirely determined by its restriction to $\mathbb{N}$. Conversely, suppose $f : \mathbb{N} \to \mathbb{Q}_p$. When does f extend continuously to $\mathbb{Z}_p$?

Exercise: Let X be a metric space, Z be a complete metric space, $Y \subset X$ a dense subspace, and let $f : Y \to Z$ be a function. Show:
a) There is at most one extension of f to a continuous function on X.
b) If f is uniformly continuous, then it extends continuously to X.
c) If X is compact and f extends continuously to X, then it is uniformly continuous.

Thus a function $f : \mathbb{N} \to \mathbb{Q}_p$ extends continuously to $\mathbb{Z}_p$ if and only if it is uniformly continuous for the p-adic metric. This latter condition has a pleasing natural enunciation in terms of preservation of p-adic congruences: for every $E \in \mathbb{Z}^+$ there is a $D \in \mathbb{Z}^+$ such that if $m \equiv n \pmod{p^D}$ then $f(m) \equiv f(n) \pmod{p^E}$.

In order to state Mahler's Theorem we first make the following definition. Let M be a $\mathbb{Z}$-module, and let $f : \mathbb{N} \to M$ be a function. Then we define the **discrete derivative** (or **forward difference**) $\nabla f : \mathbb{N} \to M$ as follows:

$$\nabla f : n \mapsto f(n+1) - f(n).$$

We view ∇ as a $\mathbb{Z}$-linear operator on the $\mathbb{Z}$-module $M^{\mathbb{N}}$ of functions from $\mathbb{N}$ to M.

THEOREM 4.2. *(Mahler's Theorem) Let $f : \mathbb{Z}_p \to \mathbb{C}_p$ be a continuous function. For $n \in \mathbb{N}$, put $a_n := (\nabla^n f)(0)$. Then:*
a) We have $\lim_{n\to\infty} a_n = 0$.
b) The series $\sum_{n=0}^{\infty} a_n \binom{x}{n}$ converges uniformly to f on $\mathbb{Z}_p$.
c) Let $||f|| = \sup_{x\in\mathbb{Z}_p} |f(x)|$. Then $||f|| = \sup_n |a_n|$.

Here $\binom{x}{n}$ is the usual binomial coefficient $\frac{x(x-1)\cdots(x-n+1)}{n!}$. It is a polynomial function with coefficients in $\mathbb{Q}$. Thus the equation

$$\forall x \in \mathbb{Z}_p,\ f(x) = \sum_{n=0}^{\infty} (\nabla^n f)(0) \binom{x}{n} \tag{13}$$

gives a canonical representation of every continuous function $f : \mathbb{Z}_p \to \mathbb{C}_p$ as a uniform limit of polynomials with coefficients in $\mathbb{C}_p$. Moreover, if $K \subset \mathbb{C}_p$ is any complete subfield such that $f(\mathbb{N}) \subset K$, then $f(\mathbb{Z}_p) \subset K$ and (13) exhibits f as a uniform limit of polynomials with coefficients in K.

Let us give a preliminary discussion of Mahler series. For any $x, n \in \mathbb{N}$, let $P_n \in \mathbb{Q}[t]$ be the polynomial $\binom{t}{n}$. For all $x \in \mathbb{N}$, $P_n(x)$ is the number of n element subsets of an x element set, so certainly $P_n(x) \in \mathbb{N}$. Since P_n defines a continuous function from $\mathbb{Z}_p$ to $\mathbb{C}_p$ and $\mathbb{N}$ is dense in $\mathbb{Z}_p$, it follows that

$$P_n(\mathbb{Z}_p) = P_n(\overline{\mathbb{N}}) \subset \overline{P_n(\mathbb{N})} \subset \overline{\mathbb{N}} = \mathbb{Z}_p.$$

Otherwise put, for all $x \in \mathbb{Z}_p$ and $n \in \mathbb{N}$, we have $|\binom{x}{n}| \leq 1$.

LEMMA 4.3. *Let $\{a_n\}_{n=0}^{\infty}$ be a sequence in $\mathbb{C}_p$, and consider the series of functions $\sum_{n=0}^{\infty} a_n \binom{x}{n}$. a) The following are equivalent:*
(i) The series converges uniformly on $\mathbb{Z}_p$.
(ii) The series converges pointwise on $\mathbb{Z}_p$.
(iii) We have $\lim_{n\to\infty} a_n = 0$.
*When these equivalent conditions hold, we call $\sum_{n=0}^{\infty} a_n \binom{x}{n}$ a **Mahler series**.*
b) Any Mahler series is a continuous function from $\mathbb{Z}_p$ to $\mathbb{C}_p$.

PROOF. a) (i) $\implies$ (ii) is clear. (ii) $\implies$ (iii): Suppose the series converges pointwise on $\mathbb{Z}_p$, and plug in $x = -1$. Then $\sum_n a_n \binom{-1}{n}$ converges, so $a_n \binom{-1}{n} = (-1)^n a_n \to 0$, so $a_n \to 0$.
(iii) $\implies$ (i). In a complete ultrametric normed field, a series of functions $\sum_n f_n$ converges uniformly iff $||f_n|| \to 0$. If $a_n \to 0$, then $||a_n \binom{x}{n}|| \leq |a_n| \to 0$.
b) A Mahler series has the form $\sum_n f_n$, where $f_n = a_n \binom{x}{n}$. Thus each $f_n : \mathbb{Z}_p \to \mathbb{C}_p$ is a polynomial, hence continuous. The usual "$\epsilon/3$ argument" from undergraduate analysis shows that if X and Y are metric spaces and $f_n : X \to Y$ is a sequence of continuous functions that converges uniformly to $f : X \to Y$, then the limit function f is continuous. □

In many ways the Mahler series is a close analogue of a power series, even though a function defined by a Mahler series need not be differentiable. In particular, there is a uniqueness theorem for power series: if $f = \sum_n a_n x^n$ is a power series with a positive radius of convergence, then repeated differentiation shows that $a_n = \frac{f^{(n)}(0)}{n!}$. As we will now show, there is an analogue for Mahler series.

EXERCISE 4.1.
a) Let $\{f_n : \mathbb{Z}_p \to \mathbb{C}\}$ be a sequence of functions converging uniformly to $f : \mathbb{Z}_p \to \mathbb{C}$. Show that the squence ∇f_n converges uniformly on $\mathbb{Z}_p$ to ∇f.
b) Let $n \in \mathbb{Z}^+$. Show: $\Delta \binom{x}{n} = \binom{x}{n-1}$.
c) Let $f = \sum_{n=0}^{\infty} a_n \binom{x}{n}$ be a Mahler series. Show: $\Delta f = \sum_{n=1}^{\infty} a_n \binom{x}{n-1}$.

So let $f = \sum_{n=0}^{\infty} a_n \binom{x}{n}$ be a Mahler series. Evaluating at 0 we get $a_0 = f(0)$. Applying ∇, we get $\nabla f = \sum_{n=1}^{\infty} a_n \binom{x}{n-1}$, and evaluating at 0 we get $a_1 = (\nabla f)(0)$. And so forth: repeating this procedure we find that $a_n = (\nabla^n f)(0)$ for all n.[1]

Before proving Mahler's Theorem we need some preliminaries on discrete calculus. Under the terminology "the calculus of finite differences," this material is very classical. However, it was not very fashionable and most contemporary mathematicians barely know this subject exists. As we will see, this is unfortunate, since these simple ideas have important applications in algebra and number theory.

1.2. Newton Expansions.

[1]This argument is essentially identical to the way one proves that every convergent power series is its own Taylor series. On the other hand, justifying the term-by-term discrete differentiation of Mahler series is easier than the term-by-term differentation of power series.

LEMMA 4.4. *Let M be a $\mathbb{Z}$-module and $f : \mathbb{N} \to M$ a function. Then for all $n \in \mathbb{N}$ we have*

$$(\nabla^n f)(0) = \sum_{i=0}^{n} (-1)^i \binom{n}{i} f(n-i). \tag{14}$$

EXERCISE 4.2. *a) Prove Lemma 4.4. (Suggestion: by induction on n.)*
b) Use Lemma (14) to prove the following exponential generating function identity: for all $f : N \to \mathbb{C}$, we have

$$\sum_{n=0}^{\infty} (\nabla^n f)(0) \frac{x^n}{n!} = e^{-x} \sum_{n=0}^{\infty} f(n) \frac{x^n}{n!}.$$

THEOREM 4.5. *(Newton Expansion) Let M be a $\mathbb{Z}$-module, and let $f : \mathbb{N} \to M$ be a function. Then there is a unique squence $\{a_n\}$ in M such that:*

$$\forall x \in \mathbb{N}, f(x) = \sum_{n=0}^{\infty} a_n \binom{x}{n} = \sum_{n=0}^{x} a_n \binom{x}{n}.$$

Moreover, for all $n \in \mathbb{N}$ we have $a_n = (\nabla^n f)(0)$.

PROOF. For all $i, j \in \mathbb{N}$ we have

$$\nabla^i \binom{x}{j}\Big|_{x=0} = \binom{0}{j-i} = \delta(i,j).$$

Thus successively applying ∇ and evaluating at 0 to $\sum_{n=0}^{\infty} a_n \binom{x}{n}$, we find that $a_n = (\nabla^n f)(0)$ for all $n \in \mathbb{N}$, establishing uniqueness. As for existence, let

$$\varphi : \mathbb{N} \to M,\ x \mapsto f(x) - \sum_{n=0}^{\infty} (\nabla^n f)(0).$$

By Lemma 4.4, for all $n \in \mathbb{N}$ we have

$$0 = (\nabla^n \varphi)(0) = \sum_{i=0}^{n-1} (-1)^i \binom{n}{i} \varphi(n-i).$$

Certainly we have $\varphi(0) = 0$, so the result follows by induction. □

A function $f : \mathbb{N} \to M$ is **periodic of period N** if for all $x \in \mathbb{N}$ we have $f(x) = f(x+N)$. It is **periodic** if it is periodic of period N for some $N \in \mathbb{Z}^+$. We make the same definitions for functions $f : \mathbb{Z} \to M$ and observe that a periodic function $f : N \to M$ extends uniquely to a periodic function $f : \mathbb{Z} \to M$ and this extension has the same minimial period. In turn a function $f : \mathbb{Z} \to M$ is periodic of period N iff it factors through a map $f : \mathbb{Z}/N\mathbb{Z} \to M$.

PROPOSITION 4.6. *Let p be a prime number and $t \in \mathbb{Z}^+$.*
a) For all $0 \le n < p^t$, the function $\binom{\cdot}{n} : \mathbb{N} \to \mathbb{Z}/p\mathbb{Z}$ is periodic of period p^t and accordingly may be viewed as an element of the $\mathbb{Z}/p\mathbb{Z}$-vector space $V(p,t) := (\mathbb{Z}/p\mathbb{Z})^{\mathbb{Z}/p^t\mathbb{Z}}$ of all maps from $\mathbb{Z}/p^t\mathbb{Z}$ to $\mathbb{Z}/p\mathbb{Z}$.
b) The functions $\{\binom{\cdot}{i}\}_{0 \le i < p^t}$ form an $\mathbb{F}_p$-basis for $V(p,t)$.

PROOF. a) For $x \in \mathbb{N}$, we have

$$(1+u)^x = \sum_{n=0}^{x} \binom{x}{n} u^n.$$

Thus

$$(1+u)^{x+p^t} = (1+u)^x(1+u)^{p^t} \equiv (1+u)^x \cdot (1+u^{p^t}) \pmod{p}.$$

It follows that for $n < p^t$ the coefficient of u^n in $(1+u)^{x+p^t}$ is congruent modulo p to the coefficient of u^n in $(1+u)^x$, i.e.,

$$\forall 0 \leq n < p^t, \ \binom{x+p^t}{n} \equiv \binom{x}{n} \pmod{p}.$$

We define a $\mathbb{Z}/p\mathbb{Z}$-linear map

$$\Phi : V(p,t) \to (\mathbb{Z}/p\mathbb{Z})^{p^t}, f \mapsto ((\nabla^n f)(0))_{0 \leq i < p^t}.$$

If $\Phi(f) = 0$, then by (14) we have $f(n) = 0$ for all $0 \leq n < p^t$, i.e., $f = 0$, so Φ is injective. Both the source and target of Φ are sets of size p^{p^t}, so Φ is an isomorphism. Moreover, for all $0 \leq n < p^t$, then as we've seen, $\Phi(\binom{\cdot}{n})$ is the element of $(\mathbb{Z}/p\mathbb{Z})^{p^t}$ whose nth coordinate is 1 and all other coordinates are 0, i.e., the nth standard basis element. Thus $\{\binom{\cdot}{i}\}_{0 \leq i < p^t}$ is a $\mathbb{Z}/p\mathbb{Z}$-basis for $V(p,t)$. □

THEOREM 4.7. *Let M be a vector space over $\mathbb{Z}/p\mathbb{Z}$, and let $f : \mathbb{N} \to M$ be a function that is periodic of period p^t for some $t \in \mathbb{Z}^+$. Then there are unique $m_0, \ldots, m_{p^t-1} \in M$ such that*

$$\forall x \in \mathbb{Z}, \ f(x) = \sum_{0 \leq n < p^t} \binom{x}{n} m_n. \tag{15}$$

PROOF. By Theorem 4.5, for all $0 \leq x < p^t$ we have

$$f(x) = \sum_{0 \leq n < p^t} (\nabla^n f)(0) \binom{x}{n}.$$

The function f is periodic of period p^t. By Proposition 4.6 so is $\sum_{0 \leq n < p^t} (\nabla^n f)(0) \binom{\cdot}{n}$, so (15) holds for all $x \in \mathbb{N}$. The uniqueness is by the usual argument of discretely differentiating and evaluating at 0. □

1.3. Proof of Mahler's Theorem.

Let $f : \mathbb{Z}_p \to \mathbb{C}_p$ be continuous. Certainly Theorem 4.2 holds if f is identically zero, so we may assume otherwise. We may replace f by $\frac{1}{||f||} f$ and thus assume that $||f|| = 1$. In particular the image $f(\mathbb{Z}_p)$ lies in the valuation ring R_p of $\mathbb{C}_p$. Let φ be the composition of f with the natural map $R_p \to R_p/pR_p$. Then

$$\varphi : \mathbb{Z}_p \to R_p/pR_p$$

is a continuous map from a compact space to a discrete space, so it is locally constant and finitely valued. The nonempty fibers of the map give a finite partition of $\mathbb{Z}_p$ into open subsets, and thus the map is constant on cosets of $p^t\mathbb{Z}_p$ for some $t_1 \in \mathbb{Z}^+$, i.e., the restriction to $\mathbb{N}$ is periodic with period p^{t_1}. Applying Theorem 4.7 we get that there are unique $a_0^0, \ldots, a_{p^{t_1}-1}^0 \in R_p$, unique modulo pR_p such that for all $x \in \mathbb{N}$,

$$f(x) - \sum_{0 \leq n < p^{t_1}} a_n^0 \binom{x}{n} \in pR_p.$$

Because $||f|| = 1$ and $|p| < 1$, we must have $\max |a_n^0| = 1$. Put

$$f_1 \coloneqq f - \sum_{0 \leq n < p^{t_1}} a_n^0 \binom{\cdot}{n},$$

so $r_1 \coloneqq ||f_1|| \leq |p|$. If $r_1 = 0$, we're done; otherwise we repeat the procedure with f_1 in place of f, with $t_2 > t_1$ and with pR_p/p^2R_p in place of R_p/pR_p. Defining $a_n^0 = 0$ for all $n \geq p^{t_1}$ we get

$$f_2 \coloneqq f_1 - \sum_{0 \leq n < p^{t_2}} a_n^1 \binom{\cdot}{n} = f - \sum_{0 \leq n < p^{t_2}} (a_n^0 + a_n^1) \binom{\cdot}{n} \in p^2 R_p.$$

Continuing in this manner, we produce for all $k \in \mathbb{N}$ a sequence $a_n^k \in \mathbb{C}_p$ such that $|a_n^k| \leq |p^k|$, and thus a convergent series

$$a_n = \sum_{k=0}^{\infty} a_n^k \in \mathbb{C}_p, \ |a_n^k| \leq |p^k| \to 0.$$

Since $||f - \sum_{n=0}^{\infty} (a_n^0 + \ldots + a_n^k)\binom{\cdot}{n}|| \leq |p^k|$ for all $k \in \mathbb{N}$, the series $\sum_{n=0}^{\infty} a_n \binom{\cdot}{n}$ converges uniformly to f on $\mathbb{Z}_p$. Also, $|a_n| \leq 1$ for all $0 \leq n < p^{t_1}$ and $|a_n| \leq |p^n|$ for all $p^{t_n} \leq n < p^{t_{n+1}}$. Since $|a_n^0| = 1$ for some $0 \leq n < p^{t_1}$, it follows that

$$||f|| = 1 = \max_n |a_n|,$$

attained for at least one $0 \leq n < p^{t_1}$ and for no $n > p^{t_1}$. This completes the proof of Mahler's Theorem.

COROLLARY 4.8. *Let $f : \mathbb{N} \to \mathbb{C}_p$ be a function. For $n \in \mathbb{N}$, let $a_n = (\nabla^n f)(0)$. The following are equivalent:*
(i) We have $\lim_{n\to\infty} a_n = 0$.
(ii) The function f extends continuously to $\mathbb{Z}_p$.
(iii) The function f is uniformly continuous for the p-adic topology on $\mathbb{N}$.
(iv) We have $\lim_{k\to\infty} ||\nabla^k f|| \to 0$.

PROOF. (i) $\implies$ (ii): If $a_n \to 0$, then by §4.1.1 the series $F(x) = \sum_{n=0}^{\infty} a_n \binom{\cdot}{n}$ converges uniformly on $\mathbb{Z}_p$ to a continuous function and $F(x) = f(x)$ for all $x \in \mathbb{N}$.
(ii) $\implies$ (iii): By assumption, f extends to a continuous function on $\mathbb{Z}_p$. Since $\mathbb{Z}_p$ is a compact metric space, f is uniformly continuous on $\mathbb{Z}_p$ and thus is uniformly continuous on $\mathbb{N}$.
(iii) $\implies$ (ii): A uniformly continuous function from a metric space to a complete metric space always admits a continuous extension to the completion.
(ii) $\implies$ (iv): By Mahler's Theorem, we have $f = \sum_{n=0}^{\infty} a_n \binom{\cdot}{n}$. We may discretely differentiate termwise, getting the Mahler series

$$\nabla^k f = \sum_{n \geq k} a_k \binom{\cdot}{n-k}.$$

Applying Mahler's Theorem again, we get $||\nabla^k f|| = \sup_{n \geq k} |a_n| \to 0$.
(iv) $\implies$ (i) is immediate. $\square$

1.4. Work of de Shalit. Let R be a CDVR with finite residue field $\mathbb{F}_q$, fraction field K, maximal ideal $\mathfrak{m}$, and let π be a uniformizing element. Let

$$\mathrm{Int}(R,R) = \{f \in K[t] \mid f(R) \subset R\}$$

be the ring of integer-valued polynomialsm, and let

$$\mathrm{Int}_n(R,R) = \{f \in \mathrm{Int}(R,R) \mid \deg(f) \leq n\}.$$

Let $\mathfrak{a}_n$ be the set of leading coeffiicients of elements of $\mathrm{Int}_n(R,R)$; then $\mathfrak{a}_n$ is a fractional R-ideal that is – like every fractional ideal over a DVR – principal. If $\mathfrak{a}_n = \langle f_n \rangle_R$, then

$$\mathrm{Int}_n(R,R) = \mathrm{Int}_{n-1}(R,R) \oplus Rf_n.$$

Let $\{f_n\}_{n=0}^{\infty}$ be a sequence in $\mathrm{Int}_n(R,R)$ such that for all $n \in \mathbb{N}$, f_n generates $\mathfrak{a}_n$. Then $\{f_n\}$ is a basis for $\mathrm{Int}(R,R)$ as an R-module, called a **Mahler basis**. We note that f_n is *not* unique; however, it is unique up to multiplication by an element of $R^\times$ and addition of an R-linear combination of $f_0, \ldots, f_{n-1}$.

For $n \in \mathbb{Z}^+$, put

$$w_q(n) = \sum_{i=1}^{\infty} \left\lfloor \frac{n}{q^i} \right\rfloor.$$

Exercise 4.3. *a) Show:* $w_q(q^m) = \frac{q^m-1}{q-1}$.
b) Let $n \in \mathbb{Z}^+$ *have base* q *expansion* $n = \sum_{i=0}^{m-1} b_i q^i$*; thus* $0 \leq b_i < q$ *for all* i*. Show:*

$$w_q(n) = \sum_{i=0}^{m-1} b_i w_q(q^i).$$

Proposition 4.9. *For all* $n \in \mathbb{Z}^+$*, we have*

$$\mathfrak{a}_n = \pi^{-w_q(n)} R.$$

Proof. For now, see Cahen-Chabert, "Old problems and new questions around integer-valued polynomials and factorial sequences," in *Multiplicative ideal theory in commutative algebra*, Springer, New York, 2006, 89–108. □

Exercise 4.4. *Let* $\mathcal{T}$ *be the set of Teichmüller representatives of* $\mathbb{F}_q$ *in* R *– that is,* $\mathcal{T}$ *consists of the* $(q-1)$*-st roots of unity together with* 0*. Put* $\mathcal{R}_0 \coloneqq 0$*; for* $m \in \mathbb{Z}^+$*, put*

$$\mathcal{R}_m \coloneqq \{\sum_{i=0}^{m-1} a_i \pi^i \mid a_i \in \mathcal{T}\}$$

and put

$$\mathcal{R} \coloneqq \bigcup_m \mathcal{R}_m.$$

Then $\mathcal{R}_m$ *is a system of coset representatives for* $R/\pi^m R$ *in* R*. Put* $g_0(t) \coloneqq 1$*. For* $m \in \mathbb{Z}^+$*, put*

$$g_{q^m}(t) \coloneqq \pi^{-\frac{(q^m-1)}{(q-1)}} \prod_{r \in \mathcal{R}_m} (t-r);$$

if $n = \sum_{i=0}^{m-1} b_i q^i$ *is the base* q *expansion of* n*, put*

$$g_n(t) \coloneqq \prod_{i=0}^{m-1} g_{q_i}^{b_i}.$$

EXERCISE 4.5. *a) Show that for all $n \in \mathbb{Z}^+$, $g_n(t) \in \mathrm{Int}(R,R)$.*
b) Show: $\{g_n(t)\}_{n=0}^{\infty}$ is a Mahler basis. (Hint: use Proposition 4.9.)

Let $q : R \to R/\mathfrak{m} \cong \mathbb{F}_q$ be the quotient map. For a function $f : R \to R$, let

$$\overline{q} \coloneqq q \circ f : R \to \mathbb{F}_q.$$

THEOREM 4.10. *(de Shalit) Let $\{f_n\}_{n=0}^{\infty}$ be a Mahler basis for $\mathrm{Int}(R,R)$.*
a) The sequence $\{\overline{f_n}\}_{n=0}^{\infty}$ forms an $\mathbb{F}_q$-basis for the space $C(R,\mathbb{F}_q)$ of locally constant functions $f : R \to F_q$.
b) The functions $\overline{f_0}, \ldots, \overline{f_{q^m-1}}$ forms an $\mathbb{F}_q$-basis for the space $C(R/\pi^m R, \mathbb{F}_q)$ of functions $f : R \to \mathbb{F}_q$ that are constant on cosets of $\pi^m R$.
c) For every continuous function $f : R \to K$, there is a unique sequence $\{a_n\}$ in K such that we have a uniformly convergent series

$$f = \sum_{n=0}^{\infty} a_n f_n$$

with $a_n \to 0$ and $||f|| = \max |a_n|$. Conversely, if $\{a_n\}$ is a sequence in K with $a_n \to 0$, then $\sum_{n=0}^{\infty} a_n f_n$ converges uniformly to a continuous function.

COROLLARY 4.11. *For a Mahler basis $\{f_n\}$ and $k \in \mathbb{Z}^+$, let $f_{n,k}$ be the composite of $f_n : R \to R$ with the quotient map $q_k : R \to R/\pi^k R$. Then $\{f_{n,k}\}_{n=0}^{\infty}$ is an $R/\pi^k R$-basis for the space $C(R, R/\pi^k R)$ of locally constant $R/\pi^k R$-valued functions on R.*

Let

$$\mathcal{R}'_m \setminus \mathcal{R}_m \setminus \mathcal{R}_{m-1}.$$

For $r \in \mathcal{R}$ we define its **length** $\ell(r)$ to be the unique m such that $r \in \mathcal{R}'_m$. For $r \in \mathcal{R}$, let χ_r be the characteristic function of the disk

$$D_r \coloneqq r + \pi^{\ell(r)} R.$$

Then $\{\chi_r\}_{r \in \mathcal{R}}$ is an orthonormal basis for $C(R,K)$ in the ultrametric Banach sense. On the other hand, the K-vector space $S(R,K)$ spanned by the χ_r's in the algebraic sense are precisely the locally constant function. The largest length $\ell(f)$ of a χ_r appearing in the expansion of $f \in S(R,K)$ is the smallest $\ell \geq 0$ such that f is constant on cosets of $\pi^\ell R$. We call it the **level** of f and denote it by $\ell(f)$. Thus $\ell(\chi_r) = \ell(r)$. All of the above results continue to hold if K is replaced by any commutative ring.

2. Monsky's theorem

2.1. Statement of the Theorem.

In 1970 P. Monsky gave a startling application of valuation theory to the solution of a problem in elementary plane geometry. By a **polygonal region** we mean a bounded subset $\mathcal{R}$ of the Euclidean plane $\mathbb{R}^2$ with boundary a simple polygon. If $\mathcal{R}$ and $T_1, \ldots, T_n$ are polygonal regions, we say that $\{T_i\}_{i=1}^n$ is a **dissection** of $\mathcal{R}$ if $\bigcup_{i=1}^n T_i = \mathcal{R}$ and for each $i \neq j$, $T_i \cap T_j \subset \partial T_i \cup \partial T_j$. A **triangular dissection** is a dissection in which each T_i is (the region bounded by) a triangle. A **triangulation** is a triangular dissection in which for each $i \neq j$, ∂T_i and ∂T_j are either disjoint or consists of an entire common edge.

For a polygonal region R, we denote by $\mu(R)$ its area (Lebesgue measure).

The aim of this section is to give a complete proof of the following result.

THEOREM 4.12. *(Monsky's theorem) Let $T_1, \ldots, T_n$ be a triangular dissection of the unit square $S = [0,1]^2$.*
a) There is a polynomial $f \in \mathbb{Z}[t_1, \ldots, t_n]$ such that $f(\mu(T_1), \ldots, \mu(T_n)) = \frac{1}{2}$.
b) In particular if $\mu(T_1) = \ldots = \mu(T_n)$ then n is even.

EXERCISE 4.6. *Deduce part b) of Monsky's theorem from part a).*

2.2. Sperner's Lemma.

We begin by establishing several forms of **Sperner's Lemma**, a 1928 result of E. Sperner [**Sp28**].

THEOREM 4.13. *(Polygonal Sperner Lemma) Consider a triangulation $T_1, \ldots, T_n$ of the polygonal region $\mathcal{R}$. Consider a **tricoloring** of the set of vertices of the triangles, i.e., a partition of this set into three parts $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$. Let A be the number of **complete triangles**, i.e., triangles with all vertices given different colors. Let B be the number of edges on the boundary $\partial\mathcal{R}$ of $\mathcal{R}$ which contain a vertex from $\mathcal{A}$ and a vertex from $\mathcal{B}$. Then*

$$A \equiv B \pmod 2.$$

PROOF. (M. Xu) Place a dot on each side of each $\mathcal{AB}$ segment. We will count the total number of dots in $\mathcal{R}$ in two different ways. On the one hand, each interior segment contributes either 2 or 0 dots in $\mathcal{R}$, while each boundary segment contributes either 1 or 0 dot according (in either case) to whether it is an $\mathcal{AB}$ segment or not. Thus the number of dots in $\mathcal{R}$ is congruent to B modulo 2. On the other hand, each complete triangle contributes one dot to $\mathcal{R}$ whereas each incomplete triangle contributes two dots (if its vertex set is contained in $\mathcal{A} \cup \mathcal{B}$) or 0 dots (otherwise). Thus the number of dots in $\mathcal{R}$ is congruent to A modulo 2. □

COROLLARY 4.14. *(Sperner's Lemma) Suppose we are given a triangle ABC and a triangulation T of the triangle. A **Sperner coloring** is a map from the vertex set of the triangulation to $\{0,1,2\}$ such that:*
- *A, B and C are colored 0, 1 and 2 respectively.*
- *Each vertex on an edge of ABC is colored with one of the two colors of the ends of its edge.*

Then any Sperner coloring of T contains an odd number of complete triangles.

EXERCISE 4.7. *Show that the Polygonal Sperner Lemma implies Sperner's Lemma.*

So far as I know, in most applications of Sperner's Lemma it suffices to know that under the given hypotheses there is at least one complete triangle. For this there is the following amazing proof, first shown to me by K. Nyman. We begin by observing that the number of 01-segments on the boundary must be odd: they can only occur along the full edge from A to B, and since every vertex on that edge is colored 0 or 1, to get from 0 to 1 the number of "color changes" must be odd. Now we view the triangle ABC as a house, each triangle in the triangulation as a room, and each 01-edge as a door. Note that a room has two doors if the corresponding triangle is not complete and one door if the corresponding triangle is complete. Thus if we

enter the house via a door on the boundary and never backtrack through a door we already used, then we have a unique path which either takes us through the house to exit via another boundary door, or we get stuck in a room corresponding to a complete triangle. Since each path which leaves the house uses two boundary doors and the number of boundary doors is odd, there must be at least one path which gets stuck inside the house...and thus there must be at least one complete triangle.

Perhaps you think that Sperner's Lemma is a piece of recreational mathematics. The following proof is meant to disabuse you of that idea (and is included only to illustrate the content of Sperner's Lemma; it has nothing to do with Monsky's theorem).

THEOREM 4.15. *(Brouwer's Theorem) Every continuous function $f : [0,1]^2 \to [0,1]^2$ has a fixed point.*

PROOF. We may replace f by any homeomorphic space. We choose

$$\Delta_0 = \{(x,y,z) \in \mathbb{R}^3 \mid 0 \leq x,y,z,\ x+y+z = 1\},$$

the "standard 2-simplex". Let $f : \Delta_0 \to \Delta_0$; seeking a contradiction, we suppose f has no fixed point. Then $T = \{T_1, \ldots, T_n\}$ be a triangulation of Δ. We may tricolor the vertex set of the triangulation using the ordered set $\{1,2,3\}$ as follows: for a vertex v, we give v the color i if i is the least index such that the ith coordinate of $f(v) - v$ is negative: since $f(v) \neq v$ but the sum of the coordinates of $f(v)$ and v are each equal to 1, there must be at least one such coordinate. Let $v_{0,0} = (1,0,0)$, $v_{0,1} = (0,1,0)$ and $v_{0,2} = (0,0,1)$. Then each v_i gets colored i. Further, any vertex lying on the boundary of Δ must be colored with one of the two colors of the complete edge e_ie_j on which it lies since every point on e_ie_j has k-coordinate 0. Thus we have given a Sperner coloring, so by Sperner's Lemma we must have one triangle Δ_1 which is colored with all three colors.

We may now triangulate Δ_1 and apply the argument of the previous paragraph. Since we get to pick the triangulation, in this way we can get a nested sequence $\{\Delta_n\}_{n=0}^{\infty}$ of complete triangles with diameters going to zero. By (e.g.) the Cantor Interection Theorem there is a unique point $P = (x,y,z) \in \bigcap_{n=0}^{\infty} \Delta_n$. Since $v_{n,0} \to x$ and $f(P)_0 < v_{n,0}$ for all n, $f(P)_0 \leq x$. Similarly $f(P)_1 \leq y$ and $f(P)_2 \leq z$. Since $x+y+z = 1 = f(P)_0 + f(P)_1 + f(P)_2$, we must have $f(P)_0 = x$, $f(P)_y = y$ and $f(P)_z = z$, i.e., $f(P) = P$ and P is a fixed point for f. □

EXERCISE 4.8. *Theorem 4.15 is frequently deduced as a consequence of the **No Retraction Theorem**: there is no continuous map f from the closed unit disk in $\mathbb{R}^2$ to its boundary S^1 such that $f(P) = P$ for all $P \in S^1$. Prove the No Retraction Theorem using Sperner's Lemma.*

A solution to Exercise 4.8 can be found in [**Iv09**]. This note further clarifies the relationship between these theorems and their more traditional homological proofs by recasting the combinatorial proof of Sperner's Lemma in terms of cohomology.

Since Monsky's theorem concerns triangular dissections and not merely triangulations,[2] we need another variant of Sperner's Lemma. Given a tricoloring of the

[2]Or at least, that is the way Monsky stated it. The special case involving triangulations is still interesting, and some expositions of Monsky's theorem restrict (usually without comment)

set of vertices of a triangular dissection, we say that a segment joining two vertices is **of type $\mathcal{AB}$** if one of its vertices if of type $\mathcal{A}$ and the other is of type $\mathcal{B}$. A **full edge** of $\mathcal{R}$ is a maximal line segment on the boundary of $\mathcal{R}$.

LEMMA 4.16. *(Monsky's Sperner Lemma) Consider a triangular dissection $T_1, \ldots, T_n$ of the polygonal region $\mathcal{R}$ and a partition of the vertex set into three parts $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$. We suppose moreover no full edge of $\mathcal{R}$ or any T_i contains vertices of all three types. Let A be the number of* ***complete triangles****, i.e., triangles with all vertices given different colors. Let B be the number of full edges of $\partial\mathcal{R}$ of type $\mathcal{AB}$. Then*

$$A \equiv B \pmod 2.$$

PROOF. The condition that no full edge of any triangle has vertices of all three types implies that each complete triangle T_i contributes an odd number of edges of type $\mathcal{AB}$ whereas each incomplete triangle contributes an even number of edges of type $\mathcal{AB}$. Thus summing from i equals 1 to n the number of $\mathcal{AB}$ edges in T_i gives a number which is congruent modulo 2 to A. Since this summation counts each interior edge twice and each boundary edge once, A is congruent modulo 2 to the number of edges of type $\mathcal{AB}$ on the boundary of $\mathcal{R}$. Similarly, the condition that no full edge of $\partial\mathcal{R}$ has vertices of all three types implies that each boundary full edge of type $\mathcal{AB}$ contains an odd number of $\mathcal{AB}$ edges and each boundary full edge not of type $\mathcal{AB}$ contains an even number of $\mathcal{AB}$ edges. Thus $A \equiv B \pmod 2$. □

2.3. Monsky's theorem, part b).

Although part b) of Theorem 4.12 is an immediate consequence of part a), we will (following [**Mo70**]) give the proof of part b) first.

The first step is the most dramatic. We choose an extension of the 2-adic norm $|\cdot|$ on $\mathbb{Q}$ to the real numbers $\mathbb{R}$. This exists by Theorem X.X. Thus $|\cdot| : \mathbb{R} \to \mathbb{R}^{\geq 0}$ is an ultrametric norm with $|2| < 1$. Now we tripartition $\mathbb{R}^2$ as follows:

Put

$$\begin{aligned}\mathcal{A} &= \{(x,y) \in \mathbb{R}^2 \mid |x|, |y| < 1\},\\ \mathcal{B} &= \{(x,y) \in \mathbb{R}^2 \mid |x| \geq 1,\ |x| \geq |y|\},\\ \mathcal{C} &= \{(x,y) \in \mathbb{R}^2 \mid |y| \geq 1,\ |x| < |y|\}.\end{aligned}$$

Ttwo points in $\mathbb{R}^2$ which both lie in any one of $\mathcal{A}$, $\mathcal{B}$ and $\mathcal{C}$ are **of the same type**.

LEMMA 4.17. *Let $P = (x,y),\ P' = (x',y') \in \mathbb{R}^2$.*
a) If $P \in \mathcal{B}$ and $P' \in \mathcal{C}$ then $|xy'| > |x'y|$ and $|xy' - x'y| = |xy'|$.
b) If $P' - P \in \mathcal{A}$, then P and P' are of the same type.
c) No line ℓ in $\mathbb{R}^2$ contains points of all three types.
d) If T is a complete triangle then $|\mu(T)| > 1$.

PROOF. a) Left to the reader as an easy exercise.
b) • Let $P \in \mathcal{A}$. Then $|x'| \leq \max|x|, |x'-x| < 1$ and $|y'| \leq \max|y|, |y'-x| < 1$, so $P \in \mathcal{A}$.
• Let $P \in \mathcal{B}$. Then $|x'| = |x| \geq 1$ and $|y'| \leq \max|y|, |y'-y| \leq \max|y|, 1 \leq |x'|$, so

to that special case. On a first reading, you may want to do that, in which case the Polygonal Sperner Lemma is all you need and you can skip to the next section now.

$P \in \mathcal{B}$.
• Let $P \in \mathcal{C}$. Then $|y'| = |y| \geq 1$ and $|x'| \leq \max|x|, |x' - x| < |y| = |y'|$, so $P \in \mathcal{C}$.
c) Step 1: If ℓ contains a point Q of type $\mathcal{A}$, then for all $P \in \ell$, $Q = P-(P-Q) \in \mathcal{A}$, so by part b) P and $P - Q$ have the same type. So we may assume $0 \in \ell$.
Step 2: Let $P = (x, y) \in \ell$ be of type $\mathcal{B}$ and $P' = (x', y') \in \ell$ be of type $\mathcal{C}$. Then $|x| \geq |y|$ and $|x'| < |y'|$, so $|xy'| > |x'y|$, contradicting the fact that $xy' = x'y$ since P and P' lie on the same line through the origin.
d) Again we may translate T and thus assume that $(0, 0) \in T \cap \mathcal{A}$. Let (x, y) be the vertex of type $\mathcal{B}$ and (x', y') be the vertex of type $\mathcal{C}$. Then again we have $|xy'| > |x'y|$, and since $\mu(T) = \pm\frac{1}{2}(xy' - x'y)$,

$$|\mu(T)| = |\frac{1}{2}||xy' - x'y| = |\frac{1}{2}||xy'| = 2|x||y'| \geq 2 > 1. \qquad \square$$

Consider a triangular dissection $\{T_i\}_{i=1}^n$ of the square $\mathcal{R} = [0, 1]^2$ with $\mu(T_1) = \ldots = \mu(T_n)$ and thus $\mu(T_i) = \frac{1}{n}$ for all i. Then on $\partial\mathcal{R}$ type $\mathcal{A}$ vertices occur only on the left and bottom edges of $\mathcal{R}$, type $\mathcal{B}$ vertices *cannot* occur on the left edge of $\mathcal{R}$, and type C vertices *cannot* occur on the bottom edge of $\mathcal{R}$. Thus $\mathcal{AB}$ edges can occur only on the bottom edge of $\mathcal{R}$, on this bottom edge every vertex is of type $\mathcal{A}$ or $\mathcal{B}$, the lower left corner is of type $\mathcal{A}$ and the lower right corner is of type $\mathcal{B}$. It follows that the number of $\mathcal{AB}$ edges in the triangulation of $\mathcal{R}$ is odd. By Lemma 4.17c) and Monsky's Sperner Lemma, the number of complete triangles in the dissection is odd: in particular there is at least one complete triangle T_i. By Lemma 4.17d) we have $|\mu(T_i)| = |\frac{1}{n}| > 1$. It follows that n is even!

2.4. Monsky's theorem, part a).

Let $T_1, \ldots, T_n$ be a triangular dissection of the polygonal region $\mathcal{R}$; for $1 \leq i \leq n$ put $a_i = \mu(T_i)$. Let $R = \mathbb{Z}[a_1, \ldots, a_n]$ be the subring of $\mathbb{R}$ generated by the a_i's. Every element of R is obtained from $f \in \mathbb{Z}[t_1, \ldots, t_n]$ by evaluating at $a_1, \ldots, a_n$.

Case 1: Suppose $2 \in R^\times$. Then there is an element $f(a_1, \ldots, a_n) \in R$ such that $2f(a_1, \ldots, a_n) = 1$, i.e., $f(a_1, \ldots, a_n) = \frac{1}{2}$.

Case 2: Suppose $2 \notin R^\times$. Let $\mathfrak{p}$ be a minimal prime ideal containing 2. Since $2 \neq 0 \in R$ and R is a domain, $\mathfrak{p}$ has height at least one. Since R is Noetherian (it is a quotient of $\mathbb{Z}[t_1, \ldots, t_n]$, which is Noetherian by the Hilbert Basis Theorem), by Krull's Hauptidealsatz $\mathfrak{p}$ has height at most 1: thus $\mathfrak{p}$ has height one. By the Krull-Akizuki Theorem, the integral closure $\tilde{R}$ of $R_\mathfrak{p}$ is a DVR. The valuation v yields a non-Archimedean norm $|\cdot|$ on the fraction field K of $\tilde{R}$, a subfield of $\mathbb{R}$. Since v is R-regular, $|a_i| \leq 1$ for all 1; since $2 \in \mathfrak{p}$ it lies also in the maximal ideal of $\tilde{R}$ and thus $|2| < 1$. We extend this norm to $\mathbb{R}$ and tripartition $\mathbb{R}^2$ as in the proof of part b) above. Also as in the proof of part b) above there must be a complete triangle T_i and thus $|a_i| > 1$, a contradiction. So Case 1 must hold.

Remark: Although one can find many expositions of part b) of Monsky's theorem (including some which are essentially identical to ours; we include this result because it is a striking application of valuation theory, not because we have anything new to say), most of them neglect part a). Similarly, although there there have been further results "of Monsky type" (one of which is given in the next

section) I am not aware of any further work on the polynomial relation of part a) of Monsky's Theorem...until very recently. The polynomial relation is explored in detail in the preprint [**AP14**]. The first author, A. Abrams, introduced me to Monsky's Theorem in 2006; the second author, J. Pommersheim, introduced me to number theory in 1992. I am happy to recommend their paper to you!

2.5. Mead's theorem.

It is remarkable that the first published proof of the innocuous Theorem 4.12 uses valuation theory. What is much more remarkable is that in the last forty-something years no other proof of Monsky's Theorem has been found.

On the other hand the technique behind Monsky's theorem has been used to prove several other results in "equidissection theory". We restrict ourselves to what is probably the most direct generalization, a 1979 result of D.G. Mead [**Me79**]. For other results with a similar flavor, see [**Ka89**], [**Mo90**] and [**Pr02**]. Let $\mathcal{R}$ be a polytope in $\mathbb{R}^d$. A **simplicial dissection** is a decomposition of $\mathcal{R}$ is given by a collection $S_1, \ldots, S_n$ of d-simplices such that $\mathcal{R} = \bigcup_{i=1}^n S_i$ and $S_i \cap S_j \subset \partial S_i \cup \partial S_j$. A **simplicialization** is a simplicial dissection such that if a vertex V of one simplex S_i lies on the boundary of another simplex S_j then V is a vertex of S_j.

We write μ for the d-dimensional Lebesgue measure on $\mathbb{R}^d$.

THEOREM 4.18. *(Mead) Let $\mathcal{R} = [0,1]^d \subset \mathbb{R}^d$. Let $S_1, \ldots, S_n$ be a simplicial dissection of $\mathcal{R}$ with $\mu(S_i) = \mu(S_j)$ for all j. Then $d! \mid n$.*

We begin by discussing Sperner's Lemma in d-dimensions. Again there are three versions: the classical version (still established by Sperner in [**Sp28**]), a version for simplicializations of polytopes, and a version for simplicial dissections of polytopes.

If $k \leq d$, we consider k-simplices in $\mathbb{R}^d$ and colorings from $\{0, \ldots, d\}$. Such a coloring is **complete** if it contains every element from $\{0, \ldots, k\}$.

THEOREM 4.19. *(Polytopal Sperner's Lemma) Consider a simplicialization of a polytope $\mathcal{R}$ in $\mathbb{R}^d$ in which each vertex is colored with an element of $\{0, \ldots, d\}$. Then the number of complete d-simplices is congruent modulo 2 to the number of complete $(d-1)$-simplices in $\partial\mathcal{R}$.*

EXERCISE 4.9. *Prove Lemma 4.20.*

THEOREM 4.20. *(Sperner's Lemma) Consider a simplicialization of the standard simplex Δ in $\mathbb{R}^{d+1}$. A **Sperner coloring** is a map from the vertex set into $\{0, \ldots, d\}$ such that:*
(i) The vertex $e_i = (0, \ldots, 1, \ldots, 0)$ of Δ gets colored i.
(ii) Every vertex appearing on any k-dimensional facet F of Δ is colored with the color of one of the vertices of F.
*Then the number of **complete simplices** – i.e., simplices colored with all $n+1$ colors – is odd.*

EXERCISE 4.10. *Show: Theorem 4.19 implies Theorem 4.20.*

EXERCISE 4.11. *Show: Theorem 4.20 implies the full Brouwer Fixed Point Theorem: every continuous map from the closed unit ball in $\mathbb{R}^d$ to itself has a fixed point.*

EXERCISE 4.12. *Show that Theorem 4.20 implies the d-dimensional No Retraction Theorem: there is no continuous map from the closed unit ball B in $\mathbb{R}^d$ to itself which restricts to the identity on ∂B.*

LEMMA 4.21. *(Mead's Sperner Lemma) Let $S_1, \ldots, S_n$ be a simplicialization of a polytope $\mathcal{R}$ in $\mathbb{R}^d$. Consider an $n+1$-coloring of the vertices of the simplices with "colors" $\{0, \ldots, d\}$. We suppose that every k-dimensional affine subspace which contains vertices labelled $0, \ldots, k$ contains no vertex labelled $i > k$. Then the number of d-simplices colored with every element of $\{0, \ldots, d\}$ is congruent modulo 2 to the number of $d-1$-simplices on $\partial\mathcal{R}$ colored with every element of $\{0, \ldots, d-1\}$.*

The following exercise is challenging. For help, see [**Me79**].

EXERCISE 4.13. *a) Prove Lemma 4.21.*
b) Use Lemma 4.21 to prove Theorem 4.18.

3. Linear groups over locally compact fields

The topological groups $\mathrm{GL}_n(\mathbb{R})$ and $\mathrm{GL}_n(\mathbb{C})$ have an inexhaustibly rich structure and importance in all parts of modern mathematics: analysis, geometry, topology, representation theory, number theory....The serious study of these groups was already begun in the 19th century by Lie and his contemporaries.

Somewhat more recently (say, about 1950) it has been realized that for a non-Archimedean locally compact field K, the groups $\mathrm{GL}_n(K)$ also have a rich and useful structure.

We will give some of this structure theory here: namely, we will classify the maximal compact subgroups of $\mathrm{GL}_n(K)$ for K a nondiscrete locally compact field. This has immediate applications to the structure of finite subgroups of $\mathrm{GL}_n(\mathbb{Q})$, which are of intrinsic interest and are quite useful in areas like representation theory and modular and automorphic forms. Moreover, this material (actually, a small piece of it suffices) can be combined with a beautiful embedding theorem of J.W.S. Cassels to deduce a celebrated 1960 theorem of A. Selberg: for any field K of characteristic 0, a finitely generated subgroup of $\mathrm{GL}_n(K)$ is virtually torsionfree: i.e., has a finite index subgroup without any nontrivial elements of finite order.

3.1. $\mathrm{GL}_n(K)$ is a locally compact group. Let K be a nondiscrete locally compact field, and let n be a positive integer. We consider the group $\mathrm{GL}_n(K)$ of invertible $n \times n$ matrices with coefficients in K. We wish to endow $\mathrm{GL}_n(K)$ with a natural locally compact topology. There are in fact two natural ways to do this, which, happily, lead to the same result.

For any $n \in \mathbb{Z}^+$, we endow the Cartesian product K^n with the product topology, which of course makes it a locally compact topological group. We will sometimes refer to this topology on K^n and other topologies induced from it as the **analytic topology**, to distinguish it from the Zariski topology. (However, the reader need not know what the Zariski topology is in order to read these notes.)

Let $M_n(K)$ be the ring of $n \times n$ matrices with entries in K. As a K-vector space, $M_n(K) \cong K^{n^2}$, and we give it the topology pulled back from the analytic topology

on K^{n^2} via the isomorphism. (Easy exercise: the topology we get on $M_n(K)$ is independent of the chosen basis.)

Now $\mathrm{GL}_n(K)$ is a subset of $M_n(K)$. We claim that in the induced (subspace) topology it is locally compact, and indeed this is foisted off on the reader in the form of the following straightforward exercises.

EXERCISE 4.14. *Let $P(t_1, \ldots, t_n) \in K[t_1, \ldots, t_n]$ be a polynomial, thought of as an algebraic object. Then P induces a function $P : K^n \to K$ in the usual way: $(x_1, \ldots, x_n) \mapsto P(x_1, \ldots, x_n)$. Show that P is continuous for the analytic topologies on K^n and K.*

EXERCISE 4.15. *Deduce: $\mathrm{GL}_n(K)$ is an open subset of $M_n(K)$.*

EXERCISE 4.16. *A subset A of a topological space X is **locally closed** if it can be written in the form $U \cap V$, where U is open and V is closed.*
a) Show that A is locally closed iff A is open in its closure $\overline{A}$.
b) Suppose that X is a locally compact Hausdorff space and A is a locally closed subset of X. Show that A is locally compact in the subspace topology.
c) Does the converse of part b) hold?

So $\mathrm{GL}_n(K)$, being an open subset of a locally compact space, is locally compact.

Now we give a second definition of the topology which is closely related to the "multiplicative" topology on the unit group of a topological ring. (Indeed, $\mathrm{GL}_n(K)$ is the group of units of the noncommutative topological ring $M_n(K)$, but never mind.) This definition realizes $\mathrm{GL}_n(K)$ as a closed subset of a K-vector space of one higher dimension. Namely, consider the subset of K^{n^2+1} given as the zero locus of the single polynomial $D(t_1, \ldots, t_{n^2})t_{n^2+1} - 1 = 0$, where D is the degree n polynomial giving the discriminant of an $n \times n$ matrix. There is a bijection between this locus and $\mathrm{GL}_n(K)$ as follows: write the entries of a matrix $M \in \mathrm{GL}_n(K)$ in linear order, say, $m_1, \ldots, m_{n^2}$; then to M we associate the point $(m_1, \ldots, m_{n^2}, \frac{1}{\det M}) \in K^{n^2+1}$. Then we may endow $\mathrm{GL}_n(K)$ with the subspace topology; being a closed subspace of the locally compact space K^{n^2+1}, it is locally compact.

EXERCISE 4.17. *Show: the two topologies defined on $\mathrm{GL}_n(K)$ coincide.*

3.2. The orthogonal group of a quadratic form.

We suppose that the characteristic of K is not 2 and $q(x) = a_1x_1^2 + \ldots + a_nx_n^2$ is a nonsingular quadratic form. There is an associated bilinear form $\langle x, y\rangle = \frac{1}{2}(q(x+y) - q(x) - q(y))$ and thus an associated **orthogonal group**

$$O(q) = \{M \in \mathrm{GL}_n(K) \mid \forall x, y \in K^n, \langle Mx, My\rangle = \langle x, y\rangle\}.$$

Equivalently, in terms of the natural action of $\mathrm{GL}_n(K)$ on symmetric matrices by conjugation – i.e., $P \mapsto GPG^T$ – the orthogonal group of q is precisely the stabilizer of the Gram matrix of q. Either way, $O(q)$ is clearly defined by the satisfaction of a finite system of polynomial equations, so is a linear algebraic group. Note that when $q = x_1^2 + \ldots + x_n^2$ we recover the "standard orthogonal group"

$$O(n) = \{M \in \mathrm{GL}_n(K) \mid MM^T = 1\}.$$

The structure of $O(q)$ is quite different depending upon whether the quadratic form q is isotropic or anisotropic. Indeed, there is the following general result.

THEOREM 4.22. *Let K be a nondiscrete locally compact field, and q a nonsingular quadratic form. The following are equivalent:*
(i) The orthogonal group $O(q)$ is compact.
(ii) The quadratic form q is anisotropic.

First we will prove the implication (i) $\implies$ (ii) of Theorem 4.22, assuming some quadratic form theory. In particular, let $q_{\mathbb{H}}(xy) = xy$ be the **hyperbolic plane**. We will use the following fact:

THEOREM 4.23. *(Witt Decomposition* [**Lam**, Thm. I.4.1]*)*
Let $q(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ be a quadratic form over a field K of characteristic different from 2. Then there is $h \in \mathbb{Z}^{\geq 0}$ and an orthogonal direct sum decomposition

$$q \cong q_0 \oplus \bigoplus_{i=1}^{h} q_{\mathbb{H}} \oplus q_a$$

where q_0 is totally isotropic (i.e., the assocated function is identically zero) and q_a is anisotropic. Thus q is nondegenerate iff $q_0 = 0$ and is aniostropic iff $q_0 = 0$ and $h = 0$.

EXERCISE 4.18. *Let K be a field of characteristic different from 2.*
a) Show that $K^\times$ acts effectively by isometries on $q_{\mathbb{H}}$ via $a \in K^\times \mapsto \begin{bmatrix} a & 0 \\ 0 & \frac{1}{a} \end{bmatrix}$. To be fancy, we will write $\mathbb{G}_m$ for $K^\times$.
b) Show that in fact $\mathrm{SO}(q_{\mathbb{H}}) = \mathbb{G}_m$: that is, $\mathbb{G}_m$ is the subgroup of $O(q_{\mathbb{H}})$ consisting of matrices of determinant 1.
c) Show: $\tau := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ is an element of $O(q_{\mathbb{H}})$ of determinant -1.
d) Show: $O(q_{\mathbb{H}}) = \mathbb{G}_m \rtimes \langle \tau \rangle$.
(Hint for parts b) through d): the space $(K^2, q_{\mathbb{H}})$ has exactly two isotropic lines: $e_1 = (1, 0)$ and $e_2 = (0, 1)$. An element of the orthogonal group of $q_{\mathbb{H}}$ must therefore either fix both lines or exchange them.)

EXERCISE 4.19. *Let q_1 and q_2 be quadratic forms over a field K of characteristic different from 2.*
a) Show: there is an injective group homomorphism $O(q_1) \times O(q_2) \hookrightarrow O(q_1 \oplus q_2)$.
b) Show: if $q(x_1, \ldots, x_n)$ is totally isotropic, then $O(q) = \mathrm{GL}_n(K)$.

EXERCISE 4.20. *Let K be a locally compact nondiscrete field of characteristic different from 2. Let $q(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ be a quadratic form. Show: if $O(q)$ is compact, then q is anisotropic.*

EXERCISE 4.21.
a) Let K be a field of characteristic different from 2. Show: $O(x^2) = \{\pm 1\}$.
b) Let q be an n-ary quadratic form over $\mathbb{C}$. Show: $O(q)$ is compact iff $n = 1$.

Now we will prove the implication (ii) $\implies$ (i) of Theorem 4.22, following Speyer [**Sp12**]. Let $q(x_1, \ldots, x_n)$ be an anisotropic n-ary quadratic form with coefficients

in the locally compact field K. As usual, we endow K^n with the norm

$$|(x_1, \ldots, x_n)|_\infty := \max_{1 \leq i \leq n} |x_i|.$$

Then

$$B_\infty := \{X \in K^n \mid |x|_\infty \leq 1\} \text{ and } S_\infty := \{x \in K^n \mid |x|_\infty = 1\}$$

are both compact. Since f is anisotropic, the continuous function

$$F : S_\infty \to \mathbb{R},\ x \mapsto |f(x)|$$

is strictly positive, so by compactness of S_∞ there is $\epsilon > 0$ such that $F(x) \geq \epsilon$ for all $x \in S_\infty$. Let $r \in |K^\times|$. We claim that

$$F(x) \leq r \implies |x|_\infty \leq \sqrt{\frac{r}{\epsilon}}. \tag{16}$$

Clearly we may assume $x \neq 0$. Put $s = |x|_\infty$; then $s \in |K^\times|$, so there is $\alpha \in K$ with $|\alpha| = s$. Then $|\frac{1}{\alpha}x|_\infty = 1$, so

$$\epsilon \leq F(\frac{1}{\alpha}x) = |f(\frac{1}{\alpha}x_1, \ldots, \frac{1}{\alpha}x_n)| = |\frac{1}{\alpha^2}f(x_1, \ldots, x_n)| = \frac{1}{s^2}F(x) \leq \frac{r}{s^2},$$

and thus $s \leq \sqrt{\frac{r}{\epsilon}}$.

Now let $R := \max_{1 \leq i \leq n} F(e_i)$. If $M \in O(q)$, then we have

$$F(Me_i) = |q(Me_i)| = |q(e_i)| = F(e_i) \leq R,$$

so by (16) we have $|Me_i|_\infty \leq \sqrt{\frac{R}{\epsilon}}$. Thus we have shown: if $M \in O(q)$ then every entry of M has norm at most $\sqrt{\frac{R}{\epsilon}}$, so $O(q)$ is a bounded subset of $M_n(K)$. If G is the Gram matrix for q in the standard basis, then the elements $M \in O(q)$ satisfy the equation $MGM^T = G$, which makes clear that $O(q)$ is closed in $M_n(K)$. Since $M_n(K)$ is ball compact, this implies that $O(q)$ is compact.

3.3. Maximal compact subgroups of $\mathrm{GL}_n(\mathbb{R})$: orthogonal groups. In the case of $K = \mathbb{R}$, a bilinear form $\langle , \rangle$ on $\mathbb{R}^n$ is said to be an **inner product** if it is positive-definite: for all $x \in \mathbb{R}^n$, $\langle x, x \rangle \geq 0$, with equality iff $x = 0$. Note that any two quadratic forms giving inner products are equivalent under the action of $\mathrm{GL}_n(K)$ (also called "isometric", but the formulation in terms of group actions will be convenient for us here), i.e., all inner products are conjugate to the standard inner product $\langle (x_1, \ldots, x_n), (y_1, \ldots, y_n) \rangle = x_1y_1 + \ldots + x_ny_n$ coming from the sum of squares form $q(x_1, \ldots, x_n) = x_1^2 + \ldots + x_n^2$.

EXERCISE 4.22. *a) Let G be a group acting on a set X. For $x \in X$, let $G_x = \{g \in G \mid gx = x\}$ be the stabilizer of x. Show that for any $g \in G$, $G_{gx} = gG_xg^{-1}$.*
b) Deduce from part a) that in a transitive group action, all point stabilizers are conjugate subgroups of G.

EXERCISE 4.23. *a) Let $O(n)$ be the standard real orthogonal group, i.e., the orthogonal group associated to the standard inner product. Show that it is a compact subgroup $\mathrm{GL}_n(\mathbb{R})$.*
b) Deduce from Exercise 9.5 that any orthogonal group associated to a positive definite quadratic form on $\mathbb{R}$ is conjugate to the standard orthogonal group $O(n)$.

EXERCISE 4.24. *a) If q is a quadratic form and $\alpha \in K^\times$, let αq be the quadratic form with coefficients scaled by α.*[3] *Show that $O(\alpha q) = O(q)$.*
b) Conclude that the orthogonal group of any negative definite real quadratic form is also conjugate to $O(n)$, hence also compact.

EXERCISE 4.25. *For $a, b \in \mathbb{N}$ with $a + b = n$, let $q_{a,b}$ be the diagonal quadratic form with a coefficients of $+1$ and b coefficients of -1. Let $O(a, b)$ be the orthogonal group of $q_{a,b}$.*
a) Show: the orthogonal group of any nonsingular real quadratic form is conjugate to a unique $O(a, b)$ with $a \geq b$.
b) Show: if $a \geq b > 0$, $O(a, b)$ is not compact.

PROPOSITION 4.24. *A compact subgroup of $\mathrm{GL}_n(\mathbb{R})$ admits an invariant inner product.*

PROOF. (Weyl) Start with any inner product $\langle , \rangle$, say the standard one. It need not be G-invariant, but we can make it G-invariant by "averaging" over the action of G. Namely, define a new inner product $\langle , \rangle_G$ by

$$\langle x, y \rangle_G := \int_G \langle gx, gy \rangle d\mu(g),$$

where $\mu(g)$ is the unit Haar measure on the compact group G. We leave it to the reader to check that this gives a G-invariant inner product. □

Remark: Some readers may remember this argument from courses in representation theory and/or functional analysis. It applies equally well to infinite-dimensional representations V of G and shows that they are all *orthogonalizable*. (More common is to consider complex representations and then the term *unitarizable* is more familiar. More on this coming up.) It follows from this that any G-invariant subspace W of V has a G-invariant complement, namely $W^\perp$ and thus any representation of a compact group is completely reducible. Note that in the case of a finite group this is known as Maschke's Theorem, and in this case the integral is just the usual sum over all values divided by $\#G$.

THEOREM 4.25. *(Maximal compact subgroups of $\mathrm{GL}_n(\mathbb{R})$) Every compact subgroup is contained in the orthogonal group of a definite quadratic form. It follows that the maximal compact subgroups of $\mathrm{GL}_n(\mathbb{R})$ are precisely these definite orthogonal groups, that all maximal compact subgroups are conjugate, and that every compact subgroup is contained in a maximal compact subgroup.*

PROOF. The first sentence is a restatement of Proposition 4.24. By Exercise 4.23, all definite orthogonal groups are conjugate. The rest follows immediately. □

3.4. Maximal compact subgroups of $\mathrm{GL}_n(\mathbb{C})$: unitary groups.

Consider now the case of $\mathrm{GL}_n(\mathbb{C})$. If $n \geq 2$, then by Exercise 4.21 for no quadratic form $q(x_1, \ldots, x_n) \in \mathbb{C}[x_1, \ldots, x_n]$ is the orthogonal group $O(q)$ compact.

However, from linear algebra we learn that the appropriate analogue of a bilinear form over $\mathbb{C}$ is a Hermitian form, i.e., an $\mathbb{R}$-bilinear form on $\mathbb{C}^n$ which is $\mathbb{C}$-linear

[3]Note: this not the same as acting on q by the scalar matrix αI_n: the latter gives $\alpha^2 q$, which is equivalent to q, whereas αq need not be.

in the first variables and conjugate linear in the second variable. The standard sesqulinear form is

$$\langle x, y\rangle = x_1\overline{y_1} + \ldots + x_n\overline{y_n},$$

and this is positive definite in the sense that $\langle x, x\rangle \geq 0$ for all $x \in \mathbb{C}^n$ and is zero only if $x = 0$. To a Hermitian form H we associate its **unitary group**

$$U(H) = \{g \in \mathrm{GL}_n(\mathbb{C}) \mid \forall x, y \in \mathbb{C}^n H(gx, gy) = H(x, y)\}.$$

The unitary group associated to the standard Hermitian form is denoted $U(n)$.

EXERCISE 4.26. *The unitary group of a Hermitian form is compact iff the form is positive definite.*

The analogy to the real case should now be clear. We leave to the reader the proofs of the following results.

PROPOSITION 4.26. *Any compact subgroup G of $\mathrm{GL}_n(\mathbb{C})$ admits a G-invariant positive definite Hermitian form.*

THEOREM 4.27. *(Maximal compact subgroups of $\mathrm{GL}_n(\mathbb{C})$) Every compact subgroup is contained in the unitary group of a definite Hermitian form. It follows that the maximal compact subgroups of $\mathrm{GL}_n(\mathbb{C})$ are precisely these definite unitary groups, that all maximal compact subgroups are conjugate, and that every compact subgroup is contained in a maximal compact subgroup.*

3.5. Maximal compact subgroups of $\mathrm{GL}_n(K)$: lattice stabilizers.

We now turn to the case of a non-Archimedean locally compact field K. In this case the maximal compact subgroups of $\mathrm{GL}_n(K)$ look quite different from the Archimedean case. This can be seen already in the case $n = 1$, i.e., $K^\times$.

- The maximal compact subgroup of $\mathbb{R}^\times$ is $\{\pm 1\} = O(1)$.
- The maximal compact subgroup of $\mathbb{C}^\times$ is $S^1 = U(1)$.

In each of these cases, the maximal compact subgroup is closed (of course!) but not open, and thus of smaller dimension than $\mathrm{GL}_n(K)$ itself. However, $K^\times$ admits **open** compact subgroups, namely $R^\times$. Although we have not developed a theory of non-Archimedean analytic manifolds and their dimensions, in some intuitive sense it is clear that both $K^\times$ and $R^\times$ have dimension one. (And indeed, this can be formalized.) In general, in the non-Archimedean case we have the following procedure for producing compact subgroups:

THEOREM 4.28. *Let K be a NA locally compact field with valuation ring R. For any closed subgroup G of $\mathrm{GL}_n(K)$, define $G(R) := G \cap \mathrm{GL}_n(R)$. Then $G(R)$ is compact and open in G.*

PROOF. Since G is closed in $\mathrm{GL}_n(K)$, $G(R) = G \cap \mathrm{GL}_n(R)$ is closed in $\mathrm{GL}_n(R)$. Thus it is enough to show that $\mathrm{GL}_n(R)$ is compact and open. Recall that we may view $\mathrm{GL}_n(K)$ as the closed subset of K^{n^2+1} of all pairs $(M, \alpha) \in M_n(K) \times K$ satisfying $\det(M)\alpha = 1$. Under this interpretation, clearly $\mathrm{GL}_n(R)$ is the closed subset of R^{n^2+1} of all pairs in $M_n(R) \times R$ satisfying the same relation. Since R^{n^2+1} is compact, so is $\mathrm{GL}_n(R)$. □

Now we momentarily work in a slightly more general setting: let R be a PID with fraction field K. We are interested in finding sufficient condition for a subgroup G of $\mathrm{GL}_n(K)$ to be conjugate to a subgroup of $\mathrm{GL}_n(R)$. The next few results are taken from [**Se:Lie**].

LEMMA 4.29. *Let $n \in \mathbb{Z}^+$, and let M be an R-submodule of K^n. The following are equivalent:*
(i) M is a finitely generated R-module and M generates K^n as a K-module.
(ii) $M \cong R^n$.

PROOF. (i) $\implies$ (ii). Since M is an R-submodule of K^n, it is torsion free. A finitely generated module over a PID is free, say $M \cong R^m$. There is a natural map $M \otimes_R K \to K^n$, which is surjective since M generates K^n as a K-module: thus $m \geq n$. On the other hand, a basis for M is an R-linearly independent set, hence also K-linearly independent (clear denominators), so by linear algebra $m \leq n$. (ii) $\implies$ (i): if $M \cong R^n$, then evidently M is finitely generated. If M did not generate K^n as a K-module, then the elements $e_1, \ldots, e_n$ of a basis for R form a K-linearly independent subset of K^n which does not span, contradicting linear algebra. □

An R-module M satisfying the equivalent conditions of Lemma 4.29 will be called a **lattice** in K^n. (Note that this usage is roughly analogous but not identical to that of a $\mathbb{Z}$-lattice in $\mathbb{R}^n$.)

LEMMA 4.30. *For lattices $M_1, \ldots, M_k$ in K^n, $M = \langle M_1, \ldots, M_k \rangle_R$ is also a lattice.*

PROOF. M is a finitely generated R-module whose K-span is K^n, so this follows immediately from Lemma 4.29. □

Fix $n \in \mathbb{Z}^+$, and let $\mathcal{L}$ denote the set of all R-lattices in K^n. Any element $\Lambda \in \mathcal{L}$ can be represented as $\langle v_1, \ldots, v_n \rangle_R$, where $(v_1, \ldots, v_n)$ is a K-basis for K^n. The natural (simply transitive) action of $\mathrm{GL}_n(K)$ on ordered bases of K^n induces a transitive action on $\mathcal{L}$. We claim that the stabilizer of the standard lattice $R^n \subset K^n$ is precisely the subgroup $\mathrm{GL}_n(R)$. Indeed, it is immediate that each element of $\mathrm{GL}_n(R)$ preserves R^n, and conversely, if $M \in \mathrm{GL}_n(K)$ preserves R^n then for all $1 \leq i \leq n$, $Me_1 \in R^n$, so $M \in M_n(R)$. The same holds for M^{-1}, so $M \in \mathrm{GL}_n(R)$.

Therefore:

PROPOSITION 4.31.
a) We have an isomorphism of $\mathrm{GL}_n(K)$-sets $\mathrm{GL}_n(K)/\mathrm{GL}_n(R) \cong \mathcal{L}$.
b) For every $\Lambda \in \mathcal{L}$, the stabilizer G_Λ of Λ in $\mathrm{GL}_n(K)$ is of the form $g\,\mathrm{GL}_n(R)g^{-1}$ for some $g \in \mathrm{GL}_n(K)$.

EXERCISE 4.27. *Prove Proposition 9.9.*

PROPOSITION 4.32. *Let G be a subgroup of $\mathrm{GL}_n(K)$ with the following property:*
(LF) There exists a lattice $\Lambda_1 \in \mathcal{L}$ such that the orbit $G.\Lambda_1$ is finite.
Then G is conjugate to a subgroup of $\mathrm{GL}_n(R)$.

PROOF. By hypothesis, $G.\Lambda_1$ is a finite set, say $\{\Lambda_1, \ldots, \Lambda_m\}$. Put $\Lambda = \langle \Lambda_1, \ldots, \Lambda_m \rangle_R$. By Lemma 4.30, Λ is again a lattice. By construction, for any $g \in G$ and $x \in \Lambda$, $gx \in \Lambda$, i.e., $g\Lambda \subset \Lambda$. Applying this with g^{-1} as well gives $g\Lambda = \Lambda$, Thus G stabilizes Λ, so $G \subset G_\Lambda$, which is conjugate to $\mathrm{GL}_n(R)$. □

Certainly hypothesis (LF) is satisfied if G is finite, and we conclude:

COROLLARY 4.33. *Let R be a PID with fraction field K. Then any finite subgroup of $\mathrm{GL}_n(K)$ is conjugate to a subgroup of $\mathrm{GL}_n(R)$.*

Already the case $R = \mathbb{Z}$ is interesting and useful, as we shall see shortly.

Finally, we return to the case in which K is a non-Archimedean locally compact field and R is its valuation ring. In this case, the group $\mathrm{GL}_n(R)$ is compact and open in $\mathrm{GL}_n(K)$. By Proposition 4.31, the same holds for the stabilizer G_Λ of every lattice in K^n.

THEOREM 4.34. *Let H be a compact subgroup of $\mathrm{GL}_n(K)$. Then there exists $\Lambda \in \mathcal{L}$ such that $g\Lambda = \Lambda$ for all $g \in H$. Equivalently, $H \subset G_\Lambda$.*

PROOF. By Proposition 4.32 it will suffice to show that a compact subgroup has property (LF). Begin with any lattice Λ_1. Then $H_{\Lambda_1} := H \cap G_{\Lambda_1}$ is the subgroup of H consisting of elements preserving Λ_1. Since G_{Λ_1} is open in $\mathrm{GL}_n(K)$, H_{Λ_1} is open in H. Since the cosets of H_{Λ_1} in H give an open covering of the compact group H, we must have $[H : H_{\Lambda_1}] < \infty$. It follows that the orbit $H.\Lambda_1$ is finite, qed. □

4. Cassels's embedding theorem

4.1. Statement of the Theorem.

THEOREM 4.35. *(Cassels [**Ca76**]) Let K be a finitely generated field of characteristic 0, and let $x_1, \ldots, x_n \in K^\times$. Then there exist infinitely many prime numbers p such that there is a field embedding $\iota_p : K \hookrightarrow \mathbb{Q}_p$ such that for all $1 \leq i \leq n$, $|\iota_p(x_i)|_p = 1$.*

4.2. Three Lemmas.

LEMMA 4.36. *Let R be an infinite integral domain, and let $f_1, \ldots, f_m \in R[t_1, \ldots, t_n]$ be nonzero polynomials. Then there exist $(a_1, \ldots, a_n) \in \mathbb{Z}^n$ such that for all $1 \leq i \leq m$, $f_i(a_1, \ldots, a_n) \neq 0$.*

PROOF. We go by induction on n. The case of $n = 1$ is trivial, since a nonzero univariate polynomial over a domain has only finitely many roots, so we may select any element a of R in the complement of a finite set. Assume the result holds for all polynomials in $n-1$ variables. Put $S = R[t_1]$ – an infinite integral domain – so that $R[t_1, \ldots, t_n] = S[t_2, \ldots, t_n]$. By induction, there exist $a_2(t_1), \ldots, a_m(t_1) \in S$ such that for all i, $f_i(t_1, a_2(t_1), \ldots, a_n(t_1)) \neq 0$. Now we apply the $n = 1$ case. □

LEMMA 4.37. *Let $f(t) \in \mathbb{Z}[t]$ be a nonconstant polynomial. Then there exist infinitely many prime numbers p such that the reduction mod p of f has a $\mathbb{Z}/p\mathbb{Z}$-rational root.*

PROOF. We give two proofs. First, we may plainly assume that f is irreducible over $\mathbb{Q}[t]$. Put $K = \mathbb{Q}[t]/(f)$ and let L be its normal closure. Then, by the Cebotarev Density Theorem, the set of prime numbers p which split completely in L has positive density, and for such primes the mod p reduction of f splits completely.

However, it is possible to give a completely elementary argument. Namely, write $f(t) = a_n t^n + \ldots + a_1 t + a_0$. Clearly we may assume that $a_0 \neq 0$, otherwise

0 is a root of every mod p reduction. Suppose for the sake of contradiction that there exists a finite set S of prime numbers such that if p is a prime not lying in S, then the mod p reduction of f has no $\mathbb{F}_p$-rational root. Let $c \in \mathbb{Z}$ be an integer divisible by all primes in S. Then

$$f(ca_0) = a_0 r(c) = a_0(a_n a_0^{n-1} c^n + a_{n-1} a_0^{n-2} c^{n-1} + \ldots + 1).$$

Since f is nonconstant, we may choose c such that $r(c) \neq \pm 1$; do so, and let ℓ be prime dividing $r(c)$. Since $r(c) \equiv 1 \pmod{p}$ for all $p \in S$, ℓ is a prime outside of S such that f has a rational root modulo ℓ. □

LEMMA 4.38. *For any prime p, the transcendence degree of $\mathbb{Q}_p$ over $\mathbb{Q}$ is uncountable.*

PROOF. Indeed, since $\mathbb{Q}_p$ has continuum cardinality, this is clear. (But since we are following Cassels' proof so closely, we did not want to meddle with his auspicious number of preliminary lemmas.) □

4.3. The proof of the Cassels Embedding Theorem.

Let K be a finitely generated field of characteristic zero, and let S be a finite set of nonzero elements of K. At the cost of replacing S with a larger finite set, we may assume that C is closed under inversion, i.e., $s \in S \implies s^{-1} \in S$, and then it suffices to find, for infinitely many primes p, embeddings $\iota_p : K \hookrightarrow \mathbb{Q}_p$ such that for all $s \in S$, $\iota_p(s) \in \mathbb{Z}_p$.

The case in which K is algebraic over $\mathbb{Q}$ is easy: then $K \cong \mathbb{Q}[t]/(f(t))$ is a number field, and applying Lemma 4.37 to $f(t)$, we get infinitely many primes p such that there exists a degree one prime ideal $\mathfrak{p}$ of K lying over p, and thus $K \hookrightarrow K_{\mathfrak{p}} \cong \mathbb{Q}_p$. Moreover, any element of K is a $\mathfrak{p}$-adic integer except at finitely many prime ideals of $\mathbb{Z}_K$, so we need only exclude this finite set of primes.

Therefore we may assume that the transcendence degree of K over $\mathbb{Q}$ is positive, say n, and let $x_1, \ldots, x_n$ be a transcendence basis for $K/\mathbb{Q}$, i.e., such that $K/\mathbb{Q}(x_1, \ldots, x_n)$ is finite. Since we are in characteristic 0, the primitive element theorem applies, and there exists $y \in K$ such that $K = \mathbb{Q}(x_1, \ldots, x_n, y)$. Therefore each element c of C may be written in the form

$$c = \frac{U_c(y, x_1, \ldots, x_n)}{V_c(x_1, \ldots, x_n)}$$

for nonzero polynomials $U_c \in \mathbb{Z}[t, x_1, \ldots, x_n]$, $V_c \in \mathbb{Z}[x_1, \ldots, x_n]$. Moreover, a simple denominator-clearing argument shows there is a polynomial

$$H(t) = H(t, x_1, \ldots, x_n) \in \mathbb{Z}[t, x_1, \ldots, x_n]$$

which is irreducible over $\mathbb{Q}(x_1, \ldots, x_n)$ and such that $g(y) = 0$. We write

$$H(t) = h_s(x_1, \ldots, x_n)t^s + \ldots + h_1(x_1, \ldots, x_n)t + h_0(x_1, \ldots, x_n),\ h_i \in \mathbb{Z}[x_1, \ldots, x_n],$$

with $h_s \neq 0$. Let $\Delta = \Delta(x_1, \ldots, x_n)$ be the discriminant of $H(t)$, which is a nonzero element of $\mathbb{Z}[x_1, \ldots, x_n]$.
Now we begin! By Lemma 4.36, we may choose integers $a_1, \ldots, a_n$ such that

$$\Delta(a_1, \ldots, a_n) \neq 0$$

$$h_s(a_1, \ldots, a_n) \neq 0$$

and

$$\forall c \in C,\ V_c(a_1, \ldots, a_n) \neq 0.$$

Apply Lemma 4.37 to the polynomial $H(t, a_1, \ldots, a_n) \in \mathbb{Z}[t]$: there exist infinitely many primes p and integers b_p such that

$$H(b_p, a_1, \ldots, a_n) \equiv 0 \pmod{p}. \tag{17}$$

By excluding finitely many primes, we may also assume that none of $\Delta(a_1, \ldots, a_n)$ and $V_c(a_1, \ldots, a_n)$ are congruent to 0 mod p. For each such prime number p, we will construct the desired embedding ι_p.

Now by Lemma 4.38, let $\theta_1, \ldots, \theta_n$ be elements of $\mathbb{Q}_p$ which are algebraically independent over $\mathbb{Q}$. By replacing each θ_i by $p^m\theta_i$ if necessary (this certainly does not disturb the algebraic independence), we may assume that $0 < |\theta_i|_p < 1$ for all i. For all i, put

$$\xi_i = \theta_i + a_i.$$

Thus the ξ_i's are algebraically independent over $\mathbb{Q}$ such that for all i,

$$|\xi_i - a_i|_p < 1. \tag{18}$$

By (17) and (18) we have

$$|H(b_p, \xi_1, \ldots, \xi_n)|_p < 1.$$

Since the discriminant of H is a p-adic unit, it has distinct roots modulo p, and Hensel's Lemma applies to show that there exists $\eta \in \mathbb{Z}_p$ such that

$$H(\eta, \xi_1, \ldots, \xi_n) = 0.$$

It follows that for all $c \in C$,

$$U_c(\eta, \xi_1, \ldots, \xi_n),\ V_c(\eta, \xi_1, \ldots, \xi_n) \in \mathbb{Z}_p$$

and

$$|V_c(\eta, \xi_1, \ldots, \xi_n)|_p = 1.$$

So we may define an embedding $\iota_p : K \hookrightarrow \mathbb{Q}_p$ by:

$$\forall i,\ \iota_p : x_i \mapsto \xi_i,$$

and

$$\iota_p : y \mapsto \eta.$$

Moreover, for all $c \in C$,

$$|\iota_p(c)|_p = |U_c(\eta, \xi_1, \ldots, \xi_n)/V_c(\eta, \xi_1, \ldots, \xi_n))|_p = |U_c(\eta, \xi_1, \ldots, \xi_n)|_p \leq 1,$$

QED.

See [**DSS15**] for a recent "explicit" form of Theorem 4.35.

One might hope for the positive characteristic of Cassels's Embedding Theorem.

THEOREM? 4.39. *Let K be a finitely generated field of characteristic $p > 0$, with constant subfield $\mathbb{F}_q$. (I.e., let $\mathbb{F}_q$ be the algebraic closure of $\mathbb{F}_p$ in K.) Let C be a finite set of nonzero elements of K. Then there is a field embedding $\iota : K \hookrightarrow \mathbb{F}_q((t))$ such that for all $c \in C$, we have $\iota(c) \in \mathbb{F}_q[[t]]^\times$.*

EXERCISE 4.28.
a) Show[4] *"Theorem 4.39" is false by taking* $K = \mathbb{F}_q(x)$ *and* $C = \{x, x^q - x\}$.
b) Can the result be salvaged somehow?

5. Finite matrix groups

A group G is said to be **torsionfree** if the only element of finite order is the identity. A group is **virtually torsionfree** if it has a finite index torsionfree subgroup. Some easy properties are established in the following exercise.

EXERCISE 4.29. *a) Show: every subgroup of a torsionfree group is torsionfree.*
b) Show: every finite group is virtually torsionfree.
c) Give an example of a group that is not virtually torsionfree.
d) Let G be a finitely generated virtually torsionfree group. Show: G has a finite index ***normal*** *subgroup that is torsion free. (Hint: a finitely generated groups has only finitely many subgroups of any given index.)*

One reason to be interested to be interested in whether a group is virtually torsionfree is the following simple result.

PROPOSITION 4.40. *Suppose that a group G has a torsionfree subgroup of finite index n. Then the order of any finite subgroup of G divides n.*

EXERCISE 4.30. *Prove Proposition 4.40.*

EXERCISE 4.31. *Suppose that a group G has a torsionfree subgroup of index dividing $n < \infty$. Show that the same holds for each subgroup of G.*

An important class of examples of virtually torsionfree groups are the groups $\mathrm{GL}_n(\mathbb{Z}_p)$. In view of Proposition 4.40, it is useful to have an explicit upper bound on the index of a torsionfree subgroup, and the following result achieves this.

THEOREM 4.41. *Let p be a prime number.*
a) For $p > 2$, $\mathrm{GL}_n(\mathbb{Z}_p)$ has a torsionfree normal subgroup of index $\prod_{i=1}^n (p^n - p^{i-1})$.
b) $\mathrm{GL}_n(\mathbb{Z}_2)$ has a torsionfree normal subgroup of index $2^{n^2} \prod_{i=1}^n (2^n - 2^{i-1})$.

PROOF. a) Suppose p is odd, and consider the subgroup U^1 of $\mathrm{GL}_n(\mathbb{Z}_p)$ consisting of matrices of the form $1 + pM_n(\mathbb{Z}_p)$ – i.e., the kernel of the reduction map $r : \mathrm{GL}_n(\mathbb{Z}_p) \to \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})$.[5] Evidently U^1 is normal and of finite index. We claim that U^1 has no elements of finite order. Indeed, assuming to the contrary it would have some element of prime order ℓ ($\ell = p$ is allowed). But for $B \in M_n(\mathbb{Z}_p)^\bullet$,

$$(1 + pB)^\ell = 1 + \ell pB + \binom{\ell}{2} p^2 B^2 + \ldots + p^\ell B^\ell.$$

Now apply the principle of domination: the least p-adic valuation of an entry of ℓpB is strictly smaller than the p-adic valuation of every entry of every matrix $\binom{\ell}{i} p^i B^i$ for $2 \leq i \leq n$: when $\ell = p$ we are using that $p \mid \binom{\ell}{2}$, which is valid since $p > 2$. Therefore

$$(1 + pB)^\ell - 1 = \sum_{i=1}^{\ell} \binom{\ell}{i} p^i B^i \neq 0,$$

[4]This observation is due to Qun Li and Haiyang Wang, who took the Spring 2019 version of the course on which these notes are based.

[5]Note that when $n = 1$, this is indeed the first higher unit group considered in Chapter 5.

contradiction.
b) When $p = 2$, the above argument does not go through. To remedy it, we need to use U^2 instead, the kernel of the reduction map $r : \mathrm{GL}_n(\mathbb{Z}_2) \to \mathrm{GL}_n(\mathbb{Z}/2^2\mathbb{Z})$. We leave it to the reader to check that U^2 has no nontrivial elements of finite order by modifying the above argument. Moreover, we have $[\mathrm{GL}_n(\mathbb{Z}_2) : U^2] = \#\,\mathrm{GL}_n(\mathbb{Z}/4\mathbb{Z})$. To compute the latter quantity, we use the short exact sequence

$$1 \to 1 + (2)M_n(\mathbb{Z}/4\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{Z}/4\mathbb{Z}) \to \mathrm{GL}_n(\mathbb{Z}/2\mathbb{Z}) \to 1,$$

noting that $\#(1 + (2)M_n(\mathbb{Z}/4\mathbb{Z}) = 2^{n^2}$. □

THEOREM 4.42. *(Selberg* [**Se60**]*) Let K be a field of characteristic zero, $n \in \mathbb{Z}^+$, and let G be a finitely generated subgroup of $\mathrm{GL}_n(K)$. Then G is virtually torsionfree.*

PROOF. Let S be a finite, symmetric set of generators of G, i.e., if $x \in S$, then $x^{-1} \in S$. The subfield K' obtained by adjoining to $\mathbb{Q}$ all the matrix entries of the elements of S is finitely generated, and since S is a generating set for G, we have $G \subset \mathrm{GL}_n(K')$. By Theorem 4.35, there exists a prime number p and an embedding $\iota : K' \to \mathbb{Q}_p$ such that every entry of each matrix in S gets mapped into $\mathbb{Z}_p$. Thus ι induces an embedding $\iota : M_n(K') \hookrightarrow M_n(\mathbb{Q}_p)$ such that$\iota(G) \subset M_n(\mathbb{Z}_p)$, and since $\iota(G)$ is a group we must have $\iota(G) \subset \mathrm{GL}_n(\mathbb{Z}_p)$. By Theorem 4.41, $\mathrm{GL}_n(\mathbb{Z}_p)$ is virtually torsionfree, hence by Exercise 9.14 so is $G \cong \iota(G)$. □

Theorem 4.42 is false without the hypothesis that K has characteristic 0 [**Wh**, p. 57]. However, Wehrfritz showed [**Wh70**, Prop. 3.2] that for any field K and any finitely generated subgroup G of $\mathrm{GL}_n(K)$, there is a finite index normal subgroup N of G such that every finite order element g of N is **unipotent**: i.e., the only eigenvalue over $\overline{K}$ is 1; equivalently, there is $n \in \mathbb{Z}^+$ such that $(g-1)^n = 0$. An understanding of these phenomena may be helpful to those trying to state and prove a true version of Theorem 4.39.

EXERCISE 4.32. *Show that Wehrfritz's Theorem implies Selberg's Theorem.*

Let $n \in \mathbb{Z}^+$, and let G be a finite subgroup of $\mathrm{GL}_n(\mathbb{Q})$. By Corollary 4.33, G is conjugate to a subgroup of $\mathrm{GL}_n(\mathbb{Z})$ and hence to a finite subgroup of $\mathrm{GL}_n(\mathbb{Z}_p)$ for all primes p. Combining Proposition 4.40, Exercise 9.14 and Theorem 4.41, we get:

$$\#G \mid \gcd((2^{n^2}\prod_{i=1}^{n}(2^n - 2^{i-1}), \{\prod_{i=1}^{n}(p^n - p^{i-1})\}_{p>2}).$$

In practice, this gcd is attained by looking only at very small odd primes. For example, when $n = 2$, it is easy to see that the gcd is equal to 48, which is also $\#\,\mathrm{GL}_2(\mathbb{Z}/3\mathbb{Z})$: all the other orders are proper multiplies of 48, eg. $\#\,\mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) = 96$, $\#\,\mathrm{GL}_2(\mathbb{Z}/5\mathbb{Z}) = 480$.

Is this upper bound sharp, i.e., is 48 indeed the least common multiple of all orders of finite subgroups of $\mathrm{GL}_2(\mathbb{Q})$ (or equivalently, $\mathrm{GL}_2(\mathbb{Z})$)? Close, but not quite. There are well-known matrices of order 4 and 6 in $\mathrm{SL}_2(\mathbb{Z})$, namely

$$A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \; B = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}.$$

Moreover, put

$$S = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$

so that S has determinant -1 and order 2. Then we have

$$SAS^{-1} = A^{-1}, SBS^{-1} = B^{-1},$$

so that as subgroups of $\mathrm{GL}_2(\mathbb{Z})$ we have

$$\langle A, S\rangle \cong D_4, \langle B, S\rangle \cong D_6,$$

of orders 8 and 12 respectively. Thus the lcm of all orders of finite subgroups of $\mathrm{GL}_2(\mathbb{Z})$ is a multiple of 24.

To show that 24 is sharp, we will use information coming from the Archimedean place of $\mathbb{Q}$! Namely, we can also embed $\mathrm{GL}_2(\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{R})$, so that by Theorem 4.25 every finite (hence compact) subgroup of $\mathrm{GL}_2(\mathbb{Q})$ is conjugate to a subgroup of the standard orthogonal group $O(2)$. But $O(2)$ has a very agreeable structure: the determinant map induces a short exact sequence

$$1 \to SO(2) \to O(2) \stackrel{\det}{\to} \{\pm 1\} \to 1,$$

where the special orthogonal group $SO(2)$ of all orthogonal matrices of determinant one is just the circle group:

$$SO(2) = S^1 = \{ \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \mid \theta \in \mathbb{R}\}.$$

At first sight this seems unhelpful, because of course $SO(2)$ contains finite subgroups of all orders, namely the nth roots of unity. Conversely, it is easy to see that any finite subgroup of $SO(2)$ is generated by any element of minimal argument θ, so that the cyclic groups C_n generated by the nth roots of unity are the only finite subgroups of $SO(2)$. However, very few of the groups C_n have rational entries: indeed, C_n contains the matrix

$$\begin{bmatrix} \cos(\frac{2\pi}{n}) & -\sin(\frac{2\pi}{n}) \\ \sin(\frac{2\pi}{n}) & \cos(\frac{2\pi}{n}) \end{bmatrix}$$

of trace $2\cos(\frac{2\pi}{n}) = \zeta_n + \zeta_n^{-1}$, which generates the real subfield of the nth cyclotomic field so for all $n > 2$ has degree $\frac{\varphi(n)}{2}$. Thus this is rational iff $\varphi(n) = 2$ iff $n = 3, 4, 6$. Thus, up to conjugacy, the only matrices in $\mathrm{GL}_2(\mathbb{R})$ with finite order and rational trace are ± 1, A and B. This shows that the least common multiple of all orders of finite subgroups of $\mathrm{SL}_2(\mathbb{Q})$ is 12 and thus that of $\mathrm{SL}_2(\mathbb{Q})$ is 24.

If we put $M(n)$ to be the least common multiple of all orders of finite subgroups of $\mathrm{GL}_n(\mathbb{Q})$, the above work gives an explicit upper bound on $M(n)$ for a given n. In fact, the exact value of $M(n)$ for all n was computed by Minkowski.

THEOREM 4.43. *(Minkowksi, 1887) For all $n \in \mathbb{Z}^+$,*

$$M(n) = \prod_{\ell} \ell^{\lfloor \frac{n}{\ell-1} \rfloor + \lfloor \frac{n}{\ell(\ell-1)} \rfloor + \lfloor \frac{n}{\ell^2(\ell-1)} \rfloor + \cdots},$$

where the product extends over all prime numbers ℓ.

Remarkably, the efficacy of the argument of looking at the completion at an Archimedean place and restricting to matrices with rational trace also holds for all $n \geq 2$, as the following theorem shows:

THEOREM 4.44. *(Schur, 1905) Let $G \subset \mathrm{GL}_n(\mathbb{C})$ be a finite subgroup of matrices such that $\mathrm{Tr}(g) \in \mathbb{Q}$ for all $g \in G$. Then $\#G \mid M(n)$.*

For modern (and novel) proofs of Theorems 4.42 and 4.43, we heartily recommend the recent paper of Guralnick and Lorenz [**GL06**].

For fixed n, it is also interesting to ask for the **maximum** order of a finite subgroup of $\mathrm{GL}_n(\mathbb{Q})$, say $m(n)$. Evidently $m(n) \mid M(n)$. E.g. we found that $m(2) = 12$. This is achieved by the following remarkable theorem of Walter Feit.

THEOREM 4.45. *(Feit, 1998) Let n be a positive integer, $n \neq 2, 4, 6, 7, 8, 9, 10$.*
a) Then $m(n) = 2^n n!$
b) Let $G \subset \mathrm{GL}_n(\mathbb{Q})$ be a subgroup of order $2^n n!$. Then G is conjugate to the subgroup of signed permutation matrices, i.e., the subgroup generated by all permutation matrices and all diagonal matrices with diagonal entries ± 1.

EXERCISE 4.33. *Show: for all $n \geq 1$, the group of signed permutation matrices is $O_n(\mathbb{Z}) := O_n(\mathbb{R}) \cap \mathrm{GL}_n(\mathbb{Z})$.*

Feit's theorem relies upon a 1984 manuscript of B. Weisfeiler [**We84**]. Weisfeiler's manuscript is remarkable in that it uses the classification of finite simple groups, one of the first to do so in an essential way to derive a significant theorem.

However, there is an even more remarkable, and sad, story concerning Weisfeiler himself. Boris Weisfeiler has been "missing" in Chile since January 4, 1985. In March of 1985 the local Chilean court ruled that Weisfeiler had died by accidental drowning. However, it has long been suspected that Weisfeiler was a *desaparecido*, i.e., that his death was one of the secret murders committed by the Pinochet regime.

Bibliography

[A] E. Artin, *Algebraic numbers and algebraic functions*. Gordon and Breach Science Publishers, New York-London-Paris 1967 xiii+349 pp.

[AP14] A. Abrams and J. Pommersheim, *Spaces of polygonal triangulations and Monsky polynomials*. To appear in Discrete and Computational Geometry.

[AW] E. Artin and G. Whaples, *A note on axiomatic characterization of fields*. Bull. Amer. Math. Soc. Volume 52, Number 4 (1946), 245-247.

[BAII] N. Jacobson, *Basic algebra. II*. Second edition. W. H. Freeman and Company, New York, 1989.

[Bak] M. Baker, *Algebraic Number Theory Course Notes (2006)*, available at `http://people.math.gatech.edu/~mbaker/pdf/ANTBook.pdf`

[Bh07] M. Bhargava, *Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants*. Int. Math. Res. Not. IMRN 2007, no. 17, 20 pp.

[Bou] 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.

[C:CA] P.L. Clark, *Commutative Algebra*, available at `http://math.uga.edu/~pete/integral.pdf`

[C:FT] P.L. Clark, *Field Theory*, `http://math.uga.edu/~pete/FieldTheory.pdf`.

[C:QF] P.L. Clark, *Quadratic Forms*, `http://www.math.uga.edu/~pete/quadraticforms.pdf`.

[Ca:LF] J.W.S. Cassels, *Local fields*. London Mathematical Society Student Texts, 3. Cambridge University Press, Cambridge, 1986.

[Ca:QF] J.W.S. Cassels, *Rational quadratic forms*. London Mathematical Society Monographs, 13. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978.

[Ca76] J.W.S. Cassels, *An embedding theorem for fields*. Bull. Austral. Math. Soc. 14 (1976), 193–198.

[Cd1] K. Conrad, *Equivalence of norms*. `https://kconrad.math.uconn.edu/blurbs/gradnumthy/equivnorms.pdf`

[CF] Algebraic number theory. Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the Inter national Mathematical Union. Edited by J. W. S. Cassels and A. Fröhlich Academic Press, London; Thompson Book Co., Inc., Washington, D.C. 1967.

[CGP17] P.L. Clark, S. Gosavi and P. Pollack, *The number of atoms in a primefree atomic domain*. Comm. Algebra 45 (2017), 5431–5442.

[Cl66] L. Claborn, *Every abelian group is a class group*. Pacific J. Math. 18 (1966), 219–222.

[Cl67] L. Claborn, *A generalized approximation theorem for Dedekind domains*. Proc. Amer. Math. Soc. 18 (1967). 378–380.

[Cl09a] P.L. Clark, *On the Hasse principle for Shimura curves*. Israel J. Math. 171 (2009), 349–365.

[Cl09b] P.L. Clark, *Elliptic Dedekind domains revisited*. Enseign. Math. (2) 55 (2009), 213–225.

[Co48] I.S. Cohen, *On non-Archimedean normed spaces*. Nederl. Akad. Wetensch., Proc. 51, (1948) 693–698 = Indagationes Math. 10, 244–249.

[Coh] H. Cohen, *Advanced Topics in Computational Number Theory*. Graduate Texts in Mathematics 193, Springer-Verlag, 2000.

[Cox] D.A. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory and complex multiplication*. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989.

[CX08] P.L. Clark and X. Xarles, *Local bounds for torsion points on abelian varieties*. Canad. J. Math. 60 (2008), 532–555.

[DR50] A. Dvoretzky and C.A. Rogers, *Absolute and unconditional convergence in normed linear spaces*. Proc. Nat. Acad. Sci. USA 36 (1950), 192–197.

[DSS15] A. Dubickas, M. Sha and I. Shparlinski, *Explicit form of Cassels' p-adic embedding theorem for number fields*. Canad. J. Math. 67 (2015), 1046–1064.

[Ei] D. Eisenbud, *Commutative algebra. With a view toward algebraic geometry*. Graduate Texts in Mathematics, 150. Springer-Verlag, New York, 1995.

[El57a] R. Ellis, *A note on the continuity of the inverse*. Proc. Amer. Math. Soc. 8 (1957), 372–373.

[El57b] R. Ellis, *Locally compact transformation groups*. Duke Math. J. 24 (1957), 119–125.

[En] O. Endler, *Valuation theory*. To the memory of Wolfgang Krull (26 August 1899–12 April 1971). Universitext. Springer-Verlag, New York-Heidelberg, 1972.

[Fe96] W. Feit, *Orders of finite linear groups*. Proceedings of the First Jamaican Conference on Group Theory and its Applications (Kingston, 1996), 9–11, Univ. West Indies, Kingston, 1996.

[Ge41] I.M. Gelfand, *Normierte Ringe*. Rec. Math. [Mat. Sbornik] N.S. 9 (1941), 3–24.

[G] L.J. Gerstein, *Basic Quadratic Forms*. Graduate Studies in Mathematics Volume 90, 2008.

[GL06] R.M. Guralnick and M. Lorenz, *Orders of finite groups of matrices*. (English summary) Groups, rings and algebras, 141–161, Contemp. Math., 420, Amer. Math. Soc., Providence, RI, 2006.

[Iv09] S. Ivanov, *Sperner's Theorem, the Brouwer Fixed Point Theorem, and Cohomology*. Preprint available at `http://arxiv.org/pdf/0906.5193v1.pdf`.

[Ka89] E.A. Kasimatis, *Dissections of regular polygons into triangles of equal areas*. Discrete Comput. Geom. 4 (1989), 375–381.

[KS] I. Kaplansky and O. F. G. Schilling, *Some remarks on relatively complete fields*. Bull. Amer. Math. Soc. 48, (1942). 744–747.

[Ke07] K.S. Kedlaya, *Mass formulas for local Galois representations*. With an appendix by Daniel Gulotta. Int. Math. Res. Not. IMRN 2007, 26 pp.

[Kr62] M. Krasner, *Nombre des extensions d'un degré donné d'un corps p-adique énoncé des résultats et préliminaires de la démonstration (espace des polynomes, transformation T)*. C. R. Acad. Sci. Paris 254 (1962), 3470–3472.

[Kü13] J. Kürschák, *Über Limesbildung und allgemeine Körpertheorie*. J. Reine Angew. Math. 142 (1913), 211–253.

[Lam] T.-Y. Lam, *Introduction to quadratic forms over fields*. Graduate Studies in Mathematics, 67. American Mathematical Society, Providence, RI, 2005.

[L-Alg] S. Lang, *Algebra*. Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002.

[L-ANT] S. Lang, *Algebraic number theory*. Second edition. Graduate Texts in Mathematics, 110. Springer-Verlag, New York, 1994.

[Lor] D. Lorenzini, *An invitation to arithmetic geometry*. Graduate Studies in Mathematics, 9. American Mathematical Society, Providence, RI, 1996.

[Ma58] K. Mahler, *An interpolation series for continuous functions of a p-adic variable*. J. Reine Angew. Math. 199 (1958), 23–34.

[Ma80] W. May, *Fields with free multiplicative groups modulo torsion*. Rocky Mountain J. Math. 10 (1980), 599–604.

[ML39] S. Mac Lane, *Subfields and automorphism groups of p-adic fields*. Ann. of Math. (2) 40 (1939), 423–442.

[Me79] D.G. Mead, *Dissection of the hypercube into simplexes*. Proc. Amer. Math. Soc. 76 (1979), 302–304.

[Mil] J. Milne, *Class field theory*, notes available at jmilne.org.

[Mo70] P. Monsky, *On dividing a square into triangles*. Amer. Math. Monthly 77 (1970), 161–164.

[Mo90] P. Monsky, *A conjecture of Stein on plane dissections*. Math. Z. 205 (1990), 583–592.

[N] J. Neukirch, *Algebraic number theory*. Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 322. Springer-Verlag, Berlin, 1999.

[Os18] A. Ostrowski, *Über einige Lösungen der Funktionalgleichung* $\varphi(x) \cdot \varphi(y) = \varphi(xy)$. Acta Math. 41 (1918) 271–284.

[Pr02] I. Praton, *Cutting polyominos into equal-area triangles*. Amer. Math. Monthly 109 (2002), 818–826.

[Ri] P. Ribenboim, *The theory of classical valuations*. Springer Monographs in Mathematics. Springer-Verlag, New York, 1999.

[Ri67] P. Ribenboim, *A short note on Henselian fields*. Math. Ann. 173 (1967), 83–88.

[Ri85] P. Ribenboim, *Equivalent forms of Hensel's lemma*. Exposition. Math. 3 (1985), 3–24.

[Ro] A.M. Robert, *A course in p-adic analysis*. Graduate Texts in Mathematics, 198. Springer-Verlag, New York, 2000.

[Ro73] M. Rosen, *S-units and S-class group in algebraic function fields*. J. Algebra 26 (1973), 98–108.

[Ro76] M. Rosen, *Elliptic curves and Dedekind domains*. Proc. Amer. Math. Soc. 57 (1976), 197–201.

[RV] D. Ramakrishnan and R.J. Valenza, *Fourier analysis on number fields*. Graduate Texts in Mathematics, 186. Springer-Verlag, New York, 1999.

[Sc33] F.K. Schmidt, *Mehrfach perfekte Körper*. Math. Ann. 108 (1933), no. 1, 1–25.

[Se60] A. Selberg, *On discontinuous groups in higher-dimensional symmetric spaces*. 1960 Contributions to function theory (internat. Colloq. Function Theory, Bombay, 1960) pp. 147–164 Tata Institute of Fundamental Research, Bombay

[Se:Lie] J.-P. Serre, *Lie algebras and Lie groups*. Lectures given at Harvard University, 1964 W. A. Benjamin, Inc., New York-Amsterdam 1965.

[Se:CL] J.-P. Serre, *Local fields*. Translated from the French by Marvin Jay Greenberg. Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979.

[Se78] J.-P. Serre, *Une "formule de masse" pour les extensions totalement ramifiées de degré donné d'un corps local*. C. R. Acad. Sci. Paris Sér. A-B 286 (1978), A1031–A1036.

[Sp28] E. Sperner, *Neuer Beweis für die Invarianz der Dimensionszahl und des Gebietes*. Abh. Math. Sem. Hamburg VI (1928), 265–272.

[Sp12] D.E. Speyer (https://mathoverflow.net/users/297/david-e-speyer), orthogonal group over local field, URL (version: 2012-08-18): https://mathoverflow.net/q/90122

[St] H. Stichtenoth, *Algebraic function fields and codes*. Second edition. Graduate Texts in Mathematics, 254. Springer-Verlag, Berlin, 2009.

[ST68] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*. Ann. of Math. 88 (1968), 492–517.

[To52] L. Tornheim, *Normed fields over the real and complex fields*. Michigan Math. J. 1 (1952), 61–68.

[Wa] S. Warner, *Topological fields*. North-Holland Mathematics Studies, 157. Notas de Matemática [Mathematical Notes], 126. North-Holland Publishing Co., Amsterdam, 1989.

[We84] B. Weisfeiler, *On the size and structure of finite linear groups*, unpublished 1984 manuscript, available at `http://boris.weisfeiler.com`.

[Wh] B.A.F. Wehrfritz, *Infinite linear groups*. Queen Mary College Mathematical Notes. Queen Mary College, Department of Pure Mathematics, London, 1969.

[Wh70] B.A.F. Wehrfritz, *Groups of automorphisms of soluble groups*. Proc. London Math. Soc. (3) 20 (1970), 101–122.

[Wl] A. Weil, *Basic number theory*. Reprint of the second (1973) edition. Classics in Mathematics. Springer-Verlag, Berlin, 1995.

[Ws] E. Weiss, *Algebraic number theory*. Reprint of the 1963 original. Dover Publications, Inc., Mineola, NY, 1998.