NONCOMMUTATIVE ALGEBRA

PETE L. CLARK

Contents

1. Basics

Throughout this document R denotes a ring, not necessarily commutative, but associative and with a multiplicative identity. A homomorphism of rings $f : R \to S$ must, by definition, map 1_R to 1_S.

1.1. **Commutants.**

Let R be a ring and $X \subset R$ a subset. We define the **commutant of X in R** as
$$Z_R(X) = \{y \in R \mid xy = yx \forall x \in X\},$$
the set of all elements of R which commute with every element of X. We also define
$$Z(R) = Z_R(R),$$
the **center** of R.

Exercise 1.1:
a) Show that for any subset $X \subset R$, $Z_R(X)$ is subring of R.
b) For a subset $X \subset R$, let S_X be the subring generated by X (i.e., the intersection of all subrings of R containing X). Show that $Z_R(X) = Z_R(S_X)$.

c) (Double commutants) Show that for every subset $S \subset R$, $S \subset Z_R(Z_R(S))$.
d) Deduce from part b) that $Z(R)$ is a commutative ring.

Exercise 1.2:[1] Show that taking commutants gives a Galois connection from the lattice of subrings of a ring R to itself. In fact, it is the Galois connection associated to the relation $x \sim y$ iff $xy = yx$ on R.

The preceding exercise is a good demonstration of the increased richness of non-commutative rings: for many non-commutative rings, taking commutants gives a rich and useful structure. However, for commutative rings we get the *trivial* Galois connection, i.e., the one for which the closure of each subset of R is simply R itself.

1.2. Opposite Rings.

Exercise 1.3: For any ring R, we define the **opposite ring** R^{op} to have the same underlying set as R and the same addition operation, but with "reversed" multiplication operation $x \bullet y = yx$.
a) Show that R^{op} is a ring, which is commutative iff R is.
b) If R is commutative, show that R is canonically isomorphic to R^{op}.
c) Left (resp. right) ideals in R correspond to right (resp. left) ideals in R^{op}.
d) Give an example of a ring which is not isomorphic to its opposite ring.
e) Show that the unit group of R is isomorphic to the unit group of R^{op}.
f) Show that R is a division ring iff R^{op} is a division ring.

Exercise 1.4: An **involution** on a ring R is a map $\iota : R \to R$ satisfying
(I1) ι induces an isomorphism on additive groups.
(I2) For all $x, y \in R$, $\iota(xy) = \iota(y)\iota(x)$.
(I3) For all $x \in R$, $\iota(\iota(x)) = x$.
a) Show that if R admits an involution, then $R \cong R^{\mathrm{op}}$. Does the converse hold?
b) Let R be any commutative ring. Exhibit an involution on $M_n(R)$, the ring of $n \times n$ matrices with R-coefficients.
c) For any ring R and $n \in \mathbb{Z}^+$, exhibit an isomorphism $M_n(R^{\mathrm{op}}) \to M_n(R)^{\mathrm{op}}$.

1.3. Units.

The set of nonzero elements of R will be denoted $R^\bullet$. A ring R is a **domain** if $(R^\bullet, \cdot)$ is a monoid: equivalently, $x \neq 0, y \neq 0 \implies xy \neq 0$.

An element $x \in R$ is a **unit** if there exists $y \in R$ such that $xy = yx = 1$. The collection of all units in R is denoted $R^\times$.

Exercise 1.5: We say that $x \in R$ is **left-invertible** (resp. **right-invertible**) if there exists $y_l \in R$ such that $y_l x = 1$ (resp. $y_r \in R$ such that $xy_r = 1$.
a) Show that $x \in R^\times$ iff x is both left-invertible and right-invertible.
b) Exhibit a ring R and an element $x \in R$ which is left-invertible and not right-invertible. (Suggestion: think about differentiation and integration with zero constant term as operators on the $\mathbb{R}$-vector space of all polynomials.)

---

[1]You need only attempt this exercise if you know about Galois connections. Moreover, don't worry if you don't: just move along.

c) Exhibit a ring R and an element $x \in R$ which is right-invertible but not left-invertible.

Exercise 1.6: A ring R is **Dedekind finite** if for all $x, y \in R$, $xy = 1 \implies yx = 1$.
a) Research the origins of this terminology. Does it have anything to do with Dedekind finite sets?[2]
b) Show that a finite ring is Dedekind finite.

1.4. Ideals.

A **left ideal** I is a subset of R which is a subgroup under addition satisfying
(LI) $RI \subset I$: for all $x \in R$ and all $y \in I$, $xy \in I$.

A **right ideal** I is a subset of R which is a subgroup under addition satisfying

(RI) $IR \subset I$: for all $x \in R$ and all $y \in I$, $yx \in I$.

A subset I of R is an **ideal** if it is both a left ideal and a right ideal.

The presence of three different notions of ideal is a basic phenomenon giving non-commutative algebra an increased intricacy over commutative algebra. If one wishes to generalize a definition or theorem of commutative algebra to the non-commutative case, one of the first things to ask is whether the ideals should be left, right or two-sided. There is no uniform answer, but some first steps in this direction are given later on in this section.

1.5. Modules.

Let R be a ring and M an abelian group. Then the structure of a **left R-module** on M is given by a function $R \times M \to M$ such that for all $x, y \in R$ and $m_1, m_2 \in M$, $x \bullet (m_1 + m_2) = x \bullet m_1 + x \bullet m_2$, $x \bullet (y \bullet m_1) = (xy) \bullet m_1$ and $1 \bullet m_1 = m_1$. On the other hand – literally! – we have the notion of a right R-module.

In commutative ring theory, one generally deals once and for all either with left R-modules or right R-modules. In noncommutative ring theory the situation is different: one regularly encounters modules of both types simultaneously. Moreover, if R and S are rings we have the notion of an **R-S bimodule**. This is given by a left R-module structure on M and a right S-module structure on M which are compatible in the following sense: for all $x \in R$, $m \in M$, $y \in S$

$$(xm)y = x(my).$$

When $R = S$ we speak of R-bimodules.

Example: If R is commutative, then any left R-module can also be given the structure of an R-bimodule simply by taking the same action on the right. This seems to explain why one sees fewer bimodules in commutative algebra, however the reader should beware that not all R-bimodules arise in this way.

---

[2]Things will become somewhat more clear later when we study **stably finite** rings.

Example: Any ring R is an R-bimodule in the obvious way. Moreover, a two-sided ideal of R is precisely an R-subbimodule of R.

Example: For any ring R and $m, n \in \mathbb{Z}^+$, the matrices $M_{m,n}(R)$ are a $M_m(R)$-$M_n(R)$ bimodule.

One of the most important uses of bimodules is to define a tensor product. Namely, if M is an $R - S$ bimodule and N is an $S - T$ bimodule, then one may define $M \otimes N$, an $R - T$ bimodule. However we are not going to use tensor products of modules over non-commutative rings in these notes so we do not enter into the formal definition here.

Exercise 1.7: Show that any $R - S$-bimodule can be given the canonical structure of an $S^{\mathrm{op}} - R^{\mathrm{op}}$-bimodule.

1.6. Division rings.

A **division ring** is a nonzero ring R with $R^\bullet = R^\times$. One of the major branches of non-commutative algebra is the study and classification of division rings. Of course a commutative ring is a division ring iff it is a field and the study of fields is a whole branch of algebra unto itself. So by the study of division rings one tends to mean the study of non-commutative division rings, or even the study of division rings "modulo the study of fields" (this does not have a precise meaning but seems accurate in spirit).

Exercise 1.8: In this problem we assume the reader has some basic familiarity with the ring $\mathbb{H}$ of Hamiltonian quaternions, a four dimensional division algebra over $\mathbb{R}$.
a) Let $P(t)$ be any nonconstant polynomial with $\mathbb{R}$-coefficients. Show that there exists $w \in \mathbb{H}$ such that $P(w) = 0$.
b) Show that in any division ring R, the equation $x^2 - 1 = 0$ has at most two solutions: ± 1.
c) Show that in $\mathbb{H}$, there are infinitely many elements w such that $w^2 = -1$. Show in fact that the set of such forms a single conjugacy class in $\mathbb{H}^\times$ and as a topological space is homeomorphic to S^3.
d) Give a necessary and sufficient condition on a polynomial $P(t) \in \mathbb{R}[t]$ such that there are infinitely many $w \in \mathbb{H}$ with $P(w) = 0$.

Lemma 1.1. *For a ring R, the following are equivalent:*
(i) R is a division ring.
(ii) Every $x \in R^\bullet$ is left-invertible.
(iii) Every $x \in R^\bullet$ is right-invertible.

Proof. Since a unit is both left-invertible and right-invertible, clearly (i) implies both (ii) and (iii).
(ii) $\implies$ (i): Let $x \in R^\bullet$; by hypothesis there exists $y \in R$ such that $yx = 1$. Also by hypothsis there exists $z \in R$ such that $zy = 1$. Then

$$z = z(yx) = (zy)x = x,$$

so that in fact y is the inverse of x.
(iii) $\implies$ (i): Of course we can argue similarly to the previous case. But actually

we do not have to: (iii) implies that every element of R^{op} is left-invertible, so by (ii) $\implies$ (i) R^{op} is a division ring, and by Exercise X.X this implies that R is a division ring. $\qquad\square$

Remark: In general, such considerations of R^{op} allow us to deduce right-handed analogues of left-handed results.

Proposition 1.2. *For a ring R, TFAE:*
(i) R is a division ring.
(ii) The only left ideals of R are 0 and R.
(iii) The only right ideals of R are 0 and R.

Proof. (i) $\implies$ (ii): let I be a nonzero left ideal, and let $x \in I^{\bullet}$. If y is the left inverse of x, then $1 = yx \in I$, so for any $z \in R$, $z = z \cdot 1 \in I$ and $I = R$.
(i) $\implies$ (iii): apply the previous argument in the division ring R^{op}.
(ii) $\implies$ (i): Let $x \in R^{\bullet}$. The left ideal Rx is nonzero, so by assumption it is all of R. In particular there exists $y \in R$ such that $yx = 1$. That is, every $x \in R^{\bullet}$ is left-invertible, so by Lemma 1.1, R is a division ring. $\qquad\square$

Proposition 1.3. *The center of a division ring is a field.*

Proof. Let R be a division ring $F = Z(R)$, and let $x \in F^{\bullet}$. Since R is division, x has a unique multiplicative inverse $y \in R$, and what we need to show is that $y \in F$, i.e., that y commutes with every element of R. So, let $z \in R$. Then

$$xzy = zxy = z = xyz,$$

and left-multiplying by x^{-1} gives $zy = yz$. $\qquad\square$

Thus every division ring D is a vector space over its center, a field F. The classification of division rings begins with the following basic dichotomy: either D is finite-dimensional over F, or it is infinite-dimensional over F. As we shall see, the former case leads to the Brauer group; the latter has a quite different flavor.

Modules over a division ring: much of linear algebra can be generalized from vector spaces over a field to (either left or right) modules over a division ring D. Indeed, one often speaks of left (or right) D-vector spaces just as if D were a field. We single out especially the following important fact: any left D-module V has a basis, and any two bases of V have the same cardinality, the **dimension** of D. This may be proved by the usual arguments of linear algebra.

Theorem 1.4. *For a ring R, TFAE:*
(i) R is a division ring.
(ii) Every left R-module is free.

Proof. (i) $\implies$ (ii) is by linear algebra, as indicated above.
(ii) $\implies$ (i):[3] let I be a maximal left ideal of R and put $M = R/I$. Then M is a simple left R-module: it has no nonzero proper submodules. By assumption M is free: choose a basis $\{x_i\}_{i \in I}$ and any one basis element, say x_1. By simplicity $Rx_1 = M$. Moreover, since x_1 is a basis element, we have $Rx_1 \cong R$ as R-modules. We conclude that as left R-modules $R \cong M$, so R is a simple left R-module. This means it has no nonzero proper left ideals and is thus a division ring. $\qquad\square$

---

[3]We follow an argument given by Manny Reyes on MathOverflow.

1.7. Endomorphism rings.

One of the main sources of noncommutative rings is endomorphism rings of modules. Let R be a ring and let M and N be left R-modules. Then $\operatorname{Hom}(M, N)$ denotes the set of all R-module maps $f : M \to N$. We note that $\operatorname{Hom}(M, N)$ naturally has the structure of an abelian group (one could try to push this further, but we will not need to do so here).

Lemma 1.5. *Let N be any left R-module. Then $\operatorname{Hom}(R, N)$ is naturally isomorphic to N, the map being given by $f \mapsto f(1)$.*

Exercise 1.9: Prove Lemma 1.5.

Lemma 1.6. *Let $\{M_i\}_{i \in I}$ be an indexed family of left R-modules. Then there is a natural isomorphism $\operatorname{Hom}(\bigoplus_{i \in I} M_i, N) = \bigoplus_{i \in I} \operatorname{Hom}(M_i, N)$.*

Exercise 1.10: Prove Lemma 1.6.

For an R-module M, we write $\operatorname{End} M$ for $\operatorname{Hom}(M, M)$. Not only may endomorphisms of M be added; they may also be composed, giving $\operatorname{End} M$ the structure of a ring. Moreover $\operatorname{End} M$ naturally acts on M, but there is some choice about exactly how to do this. Here we follow the convention of (e.g.) [L-FC]: if M is a left R-module, then $\operatorname{End} M$ will act *on the right*. When it may not be clear from the context whether the action of R on M is on the left or the right, we may indicate this by writing $\operatorname{End}(_R M)$ for the endomorphism ring of M as a left R-module or $\operatorname{End}(M_R)$ for the endomorphism ring of M as a right R-module.

Proposition 1.7. *Let R be a ring. Viewing R as a left R-module, we have a natural isomorphism $\operatorname{End}(_R R) = R$.*

Proof. This is the special case of Lemma 1.5 obtained by taking $N = R$. $\qquad\square$

Exercise 1.11 (Cayley's theorem for rings): Show that for any ring R, there exists a commutative group G such that $R \hookrightarrow \operatorname{End}_{\mathbb{Z}}(G)$. (Hint: take $G = (R, +)$.)

A module M is simple if it has exactly two R-submodules: 0 and M.[4]

Proposition 1.8. *(Schur's Lemma) Let M and N be simple R-modules. Then:*
a) If M and N are not isomorphic, then $\operatorname{Hom}(M, N) = 0$.
b) $\operatorname{Hom}(M, M) = \operatorname{End}(_R M)$ is a division ring.

Proof. a) By contraposition: suppose that $f : M \to N$ is a nonzero R-module homomorphism. Then the image of f is a nonzero submodule of the simple module N, so it must be all of N: f is surjective. Similarly the kernel of f is a proper submodule of the simple module M, so is 0. Therefore f is an isomorphism.
b) Let $f : M \to M$. Then $\ker f$ is an R-submodule of the simple R-module M. Therefore either $\ker f = 0$ – in which case $f = 0$ – or $\ker f = 0$ – in which case f is bijective, hence has an inverse. $\qquad\square$

Exercise 1.12: Prove the converse of Schur's Lemma: for any division ring D, there exists a ring R and a simple left R-module M such that $\operatorname{End}(_R M) \cong D$.

---

[4]In particular the zero module is *not* simple.

Proposition 1.9. *Let A be a left R-module. For $n \in \mathbb{Z}^+$, write M^n for the direct sum of n copies of M. There is a natural isomorphism of rings*

$$\mathrm{End}(M^n) = M_n(\mathrm{End}\, M).$$

Exercise 1.13: Prove Proposition 1.9. (Hint: suppose first that $R = A = k$ is a field. Then the statement is the familiar one that the endomorphism ring of k^n is $M_n(k)$. Recall how this goes – the general case can be proved in the same way.)

Proposition 1.9 explains the ubiquity of matrix rings in noncommutative algebra.

1.8. **Monoid Rings.**

Let R be a ring and M be a monoid. We suppose first that M is finite. Denote by $R[M]$ the set of all functions $f : M \to R$.

For $f, g \in R[M]$, we define the **convolution product** $f * g$ as follows:

$$(f * g)(m) := \sum_{(a,b) \in M^2 \ \mid \ ab=m} f(a)g(b).$$

In other words, the sum extends over all ordered pairs (a, b) of elements of M whose product (in M, of course), is m.

Proposition 1.10. *Let R be a ring and M a finite monoid. The structure $(R[M], +, *)$ whose underlying set is the set of all functions from M to R, and endowed with the binary operations of pointwise addittition and convolution product, is a ring.*

Proof. First, suppose that R is a ring and M is a monoid, then for any $f \in R[M]$ and $m \in M$, we have

$$(f*I)(m) = \sum_{(a,b) \in M^2 \ \mid \ ab=m} f(a)I(b) = f(m)I(1) = f(m) = I(1)f(m) = \ldots = (I*f)(m).$$

We still need to check the associativity of the convolution product and the distributivity of convolution over addition. We leave the latter to the reader but check the former: if $f, g, h \in R[M]$, then

$$((f * g) * h)(m) = \sum_{xc=m} (f * g)(x)h(c) = \sum_{xc=m} \sum_{ab=x} f(a)g(b)h(c)$$

$$= \sum_{abc=m} f(a)g(b)h(c)$$

$$= \sum_{ay=m} \sum_{bc=y} f(a)g(b)h(c) = \sum_{ay=m} f(a)(g * h)(y) = (f * (g * h))(m).$$

$\square$

A special case of this construction which is important in the representation theory of finite groups is the ring $k[G]$, where k is a field and G is a finite group.

Now suppose that M is an infinite monoid. Unless we have some sort of extra structure on R which allows us to deal with convergence of sums – and, in this level of generality, we do not – the above definition of the convolution product $f * g$ is problematic because the sum might be infinite. For instance, if $M = G$ is any group, then our previous definition of $(f*g)(m)$ would come out to be $\sum_{x \in G} f(x)g(x^{-1}m)$, which is, if G is infinite, an infinite sum.

Our task therefore is to modify the construction of the convolution product so as to give a meaningful answer when the monoid M is infinite, but in such a way that agrees with the previous definition for finite M.

Taking our cue from the infinite direct sum, we restrict our domain: define $R[M]$ to be subset of all functions $f : M \to R$ such that $f(m) = 0$ except for finitely many m (or, for short, **finitely nonzero functions**). Restricting to such functions,

$$(f * g)(m) := \sum_{ab=m} f(a)g(b)$$

makes sense: although the sum is apparently infinite, all but finitely terms are zero.

Proposition 1.11. *Let R be a ring and M a monoid. The structure $(R[M], +, *)$ whose underlying set is the set of all finitely nonzero functions from M to R, and endowed with the binary operations of pointwise addidition and convolution product, is a ring.*

Exercise 1.13: Prove Proposition 1.11.

Note that as an abelian group, $R[M]$ is naturally isomorphic to the direct sum $\bigoplus_{m \in M} R$, i.e., of copies of R indexed by M. One can therefore equally well view an element $R[M]$ as a formal finite expressions of the form $\sum_{m \in M} a_m m$, where $a_m \in R$ and all but finitely many are 0. Written in this form, there is a natural way to define the product

$$\left(\sum_{m \in M} a_m m \right) \left(\sum_{m \in M} b_m m \right)$$

of two elements f and g of $R[M]$: namely we apply distributivity, use the multiplication law in R to multiply the a_m's and the b_m's, use the operation in M to multiply the elements of M, and then finally use the addition law in R to rewrite the expression in the form $\sum_m c_m m$. But a moment's thought shows that c_m is nothing else than $(f * g)(m)$. On the one hand, this makes the convolution product look very natural. Conversely, it makes clear:

The polynomial ring $R[t]$ is canonically isomorphic to the monoid ring $R[\mathbb{N}]$. Indeed, the explict isomorphism is given by sending a polynomial $\sum_n a_n t^n$ to the function $n \mapsto a_n$.

The semigroup algebra construction can be used to define several generalizations of the polynomial ring $R[t]$.

Exercise 1.14: For any ring R, identify the monoid ring $R[\mathbb{Z}]$ with the ring $R[t, t^{-1}]$ of Laurent polynomials.

First, let $T = \{t_i\}$ be a set. Let $FA(T) := \bigoplus_{i \in T}(\mathbb{N}, +)$ be the direct sum of a number of copies of $(\mathbb{N}, +)$ indexed by T. Let R be a ring, and consider the monoid ring $R[FA(T)]$. Let us write the composition law in $FA(T)$ multiplicatively; moreover, viewing an arbitrary element I of $FA(T)$ as a finitely nonzero function from T to $\mathbb{N}$, we use the notation t^I for $\prod_{t \in T} t^{I(t)}$. Then an arbitrary element of $R[FA(T)]$

is a finite sum of the form $\sum_{k=1}^{n} r_k t^{I_k}$, where $I_1, \ldots, I_k$ are elements of $FA(t)$. This representation of the elements should make clear that we can view $R[FA(T)]$ as a polynomial ring in the indeterminates $t \in T$: we use the alternate notation $R[\{t_i\}]$.

For a set $T = \{t_i\}$, let $FM(T)$ be the free monoid on T. The elements of $FM(T)$ are often called **words** in T and the monoid operation is simply concatenation. For any ring R, the monoid ring $R[FM(T)]$ is called the ring of **noncommuting polynomials** with coefficients in R. Note that even though the indeterminates t_i need not commute with each other and the elements of R need not commute with each other, the elements $R \cdot 1$ do commute with each indeterminate t_i. (It is possible to consider "twisted" versions of these rings for which this is not the case.) When $T = \{t_1, \ldots, t_n\}$ is finite, we often use the notation $R\langle t_1, \ldots, t_n \rangle$.

Exercise 1.15: When R is a field, give a description of $R\langle t_1, \ldots, t_n \rangle$ in terms of tensor algebras.

The use of noncommutative polynomial rings allows us to define noncommutative rings by "generators and relations". Namely, given a set of elements $R_i \in R\langle t_1, \ldots, t_n \rangle$, we may consider the two-sided ideal I generated by the R_i's and form the quotient
$$S = R\langle t_1, \ldots, t_n \rangle / I.$$
This may be viewed as the R-algebra with generators $t_1, \ldots, t_n$ subject to the relations $R_i = 0$ for all i.

Example: Let k be a field of characteristic zero, and let I be the two-sided ideal of $k\langle x, y \rangle$ generated by $xy - yx - 1$. The quotient $k\langle x, y \rangle$ admits a natural map to the **Weyl ring** $W(k)$, namely the subring of k-vector space endomorphisms of $k[t]$ generated by multiplication by t and differentiation $\frac{d}{dt}$. To see this it is enough to observe that for any polynomial $p(t) \in k[t]$ one has $t\frac{dp}{dt} - \frac{d}{dt}(tp) = p$ (and to check that it is enough to show it on basis elements, e.g. monomials t^n: we leave this to the reader). One can in fact show that the natural map $k\langle x, y \rangle \to W(k)$ is an isomorphism, although we omit the verification here.

The universal property of monoid rings: Fix a ring R. Let B be an R-algebra and M a monoid. Let $f : R[M] \to B$ be an R-algebra homomorphism. Consider f restricted to M; it is a homomorphism of monoids $M \to (B, \cdot)$. Thus we have defined a mapping
$$\operatorname{Hom}_{\text{R-alg}}(R[M], B) \to \operatorname{Hom}_{\text{Monoid}}(M, (B, \cdot)).$$

Interestingly, this map has an inverse. If $g : M \to B$ is any homomorphism satisfying $g(0) = 0$, $g(m_1 + m_2) = g(m_1) + g(m_2)$, then g extends to a unique R-algebra homomorphism $R[M] \to B$: $\sum_{m \in M} r_m m \mapsto \sum_m r_m g(m)$. The uniqueness of the extension is immediate, and that the extended map is indeed an R-algebra homomorphism can be checked directly (please do so).

In more categorical language, this canonical bijection shows that the functor $M \mapsto R[M]$ is the **left adjoint** to the forgetful functor $(S, +, \cdot) \mapsto (S, \cdot)$ from R-algebras to commutative monoids. Yet further terminology would express this by saying

that $R[M]$ is a "free object" of a certain type.

Exercise 1.16: Formulate an explicit universal property for noncommutative polynomial rings.

Exercise 1.17: Let G be a group, and consider the group ring $R[G]$. Let V be a left R-module. Show that to give an $R[G]$-module structure on V extending the R-module structure is equivalent to giving a homomorphism $\rho : G \to \text{Aut}_R(V)$. When $R = k$ is a field, this gives a correspondence between $k[G]$-modules and **representations** of G on k-vector spaces.

1.9. **Noetherian and Artinian Rings.**

Let M be a ring. A left R-module M is **Noetherian** if the partially ordered set of submodules of M satisfies the ascending chain condition (ACC): that is, any infinite sequence

$$N_1 \subset N_2 \subset \ldots \subset N_n \subset \ldots$$

of submodules of M is eventually constant: there exists $n_0 \in \mathbb{Z}^+$ such that $N_{n_0+k} = N_{n_0}$ for all $k \in \mathbb{N}$.

A left R-module M is **Artinian** if the partially ordered set of submodules of M satisfies the descending chain condition (DCC): that is, any infinite sequence

$$N_1 \supset N_2 \supset \ldots \supset N_n \supset \ldots$$

of submodules of M is eventually constant.

The study of Noetherian and Artinian modules is one important part of noncommutative algebra which plays out virtually identically to the commutative case. Therefore I refer the interested reader to §8 of my commutative algebra notes for a more careful treatment of chain conditions on modules. We will in particular make use of the following facts:

Theorem 1.12. *Let M be a left R-module.*
a) If M is Noetherian, it is finitely generated.
b) M is both Noetherian and Artinian iff it admits a composition series. Moreover, the multiset of isomorphism classes of successive qoutients of a composition series is invariant of the choice of composition series.
c) Let

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

be a short exact sequence of R-modules. Then M_2 is Noetherian iff both M_1 and M_3 are Noetherian, and M_2 is Artinian iff both M_1 and M_3 are Artinian.

A ring R is **left Noetherian** (resp. **left Artinian**) if it is Noetherian (resp. Artinian) as a left R-module over itself. In a similar way we define right Noetherian and right Artinian rings.

Remark: There are rings which are left Noetherian but not right Noetherian, and also rings which are left Artinian but not right Artinian. We refer to [L-FC, Ch. 1] for examples.

1.9.1. *Dedekind-finiteness and stable finiteness.*

Proposition 1.13. *Let R be a ring and $n \in \mathbb{Z}^+$. Then:*
a) If R is left Noetherian, so is $M_n(R)$.
b) If R is left Artinian, so is $M_n(R)$.

Proof. For any $1 \le i, j \le n$, let $\pi_{ij} : M_n(R) \to R$ be projection onto the (i,j)-component. One checks immediately that if $S \subset M_n(R)$ is a left R-module, then $\pi_{ij}(S)$ is a left ideal of R.

a) Let $\{I_n\}_{n=1}^{\infty}$ be an infinite ascending chain of left $M_n(R)$-ideals. For all (i, j), the sequence of left ideals $\pi_{i,j}(I_n)$ eventually stabilizes in R, so every component of the sequence of ideals stabilizes and thus the sequence itself stabilizes.
b) The argument for descending chains is almost identical. $\square$

Proposition 1.14. *For a ring R, TFAE:*
(i) For all $n \in \mathbb{Z}^+$, the matrix ring $M_n(R)$ is Dedekind-finite.
(ii) For all $n \in \mathbb{Z}^+$, if $R^n \cong R^n \oplus K$, then $K = 0$.
(iii) For all $n \in \mathbb{Z}^+$, R^n is a Hopfian module: a surjective endomorphism of R^n is an isomorphism.
*A ring satisfying these equivalent conditions is said to be **stably finite**.*

Proof. (i) $\implies$ (ii): Let $\varphi : R^n \to R^n \oplus K$ be an R-module isomorphism. Let $\pi_1 : R^n \oplus K \to R^n$ be projection onto the first factor and let $\iota_1 : R^n \to R^n \oplus K$ be the map $x \mapsto (x, 0)$. Finally, define

$$A = \pi_1 \circ \varphi : R^n \to R^n, \; B = \varphi^{-1} \circ \iota_1 : R^n \to R^n.$$

Then

$$AB = \pi_1 \circ \varphi \circ \varphi^{-1} \circ \iota_1 = \pi_1 \circ \, iota_1 = 1_{R^n}.$$

Our assumption on Dedekind finiteness of $M_n(R) = \text{End} \, R^n$ gives us that A and B are isomorphisms. Since $A = \varphi \circ \pi_1$ and A and φ are isomorphisms, so is π_1. Since $\ker \pi_1 = K$, it follows that $K = 0$.
(ii) $\implies$ (iii): Let $\alpha : R^n \to R^n$ be a surjective endomorphism, and put $K = \ker \alpha$. Since R^n is free we have $R^n \cong R^n \oplus K$, and applying (ii) we get $K = 0$ and thus α is an isomorphism.
(iii) $\implies$ (i): Suppose that we have $A, B \in M_n(R)$ such that $AB = I_n$. Let $\alpha : R^n \to R^n$ be the linear map corresponding to the matrix A: the given condition implies that it is surjective. Since R^n is assumed to be Hopfian, α is in fact an isomorphism, i.e., A is invertible. Therefore $AB = I_n \implies BA = A^{-1}(AB)A = A^{-1}A = I_n$. $\square$

Theorem 1.15. *A ring is stably finite if it is either*
a) right Noetherian or
b) commutative.

Proof. CLAIM A Noetherian module is Hopfian.
Proof of claim: Let $\alpha : M \to M$ be a surjective endomorphism of M. Suppose that α is not injective and let $0 \ne x \in \ker \alpha$. For any $n \in \mathbb{Z}^+$, since α is surjective, so is α^n and thus there exists $y \in M$ such that $\varphi^n(y) = x$. It follows that $\varphi^{n+1}(y) = 0$ and $\varphi^n(y) \ne 0$ Therefore $K_n = \ker \alpha^n$ is an infinite strictly ascending chain of submodules of M, so M is not Noetherian.
a) So if R is right Noetherian, R^n is Noetherian hence Hopfian, and therefore R is stably finite by Proposition 1.14.

b) If R is commutative we may use determinants! Indeed, let $A, B \in M_n(R)$ be such that $AB = I_n$. Then $(\det A)(\det B) = 1$, so $\det B \in R^\times$. From the adjugate equation

$$B \operatorname{adj}(B) = (\det B)I_n$$

we deduce that $\frac{1}{\det B} \operatorname{adj}(B)$ is a right inverse of B. Thus B is both left invertible and right invertible, so it is invertible with left inverse equal to its right inverse: $BA = I_n$. $\qquad\square$

1.9.2. *IBN, the rank condition and the strong rank condition.*

A ring R satisfies the **Invariant Basis Number** property (IBN) for right modules if for all $m, n \in \mathbb{Z}^+$, R^m and R^n are isomorphic right R-modules iff $m = n$. A ring satisfies the **rank condition** if for all $m, n \in \mathbb{Z}^+$, there exists an R-module epimorphism $\alpha : R^m \to R^n$ iff $m \geq n$. A ring satisfies the **strong rank condition** if for all $m, n \in \mathbb{Z}^+$, there exists an R-module epimorphism $\beta : R^m \to R^n$ iff $m \leq n$.

Exercise 1.18: Let $m, n \in \mathbb{Z}^+$. For a ring R, the following are equivalent:
(i) $R^m \cong R^n$ as right R-modules.
(ii) There exist matrices $A \in M_{mn}(R)$, $B \in M_{nm}(R)$ such that $AB = I_m$, $BA = I_n$.

Exercise 1.19: a) Show that for a ring R, TFAE:
(i) R *does not* satisfy the rank condition.
(ii) There are $n > m \geq 1$, $A \in M_{nm}(R)$ and $B \in M_{mn}(R)$ such that $AB = I_n$.
b) Deduce that R satisfies the rank condition on right modules iff it satisfies the rank condition on left modules.

Exercise 1.20: Show that a ring R satisfies the strong rank condition iff for any homogeneous system of n linear equations over R in $m > n$ unknowns has a non-trivial solution in R.

Proposition 1.16. *a) In any ring R, the strong rank condition implies the rank condition, which implies IBN.*
b) In any ring R, stable finiteness implies the rank condition.

Proof. Let $\alpha : R^m \to R^n$ be an epimorphism of R-modules. Put $K = \ker \alpha$. Since R^n is free hence projective, the sequence

$$0 \to K \to R^m \to R^n \to 0$$

splits, giving

$$R^m \cong R^n \oplus K.$$

a) Suppose R satisfies the strong rank condition, and consider an epimorphism α as above. The splitting of the sequence gives an R-module monomorphism $\beta : R^n \to R^m$, so by the strong rank condition $n \leq m$. Now spupose R satisfies the rank condition: an isomorphism $R^m \cong R^n$ yields surjections $\alpha : R^m \to R^n$ and $\alpha' : R^n \to R^m$ and the rank condition yields $m \geq n$ and $n \geq m$ and thus $m = n$.
b) By contraposition: suppose R does not satisfy the rank condition, so there is a surjection $\alpha : R^m \to R^n$ with $m < n$. The splitting of the sequence gives

$$R^m \cong K \oplus R^n \cong R^m \oplus (K \oplus R^{n-m}),$$

contradicting condition (ii) for stable finiteness in Proposition 1.14.

$\square$

Example: As we have seen above, by a modest extension of the usual methods of linear algebra, any division ring satisfies IBN.

Exercise 1.21: Let $f : R \to S$ be a homomorphism of rings. Suppose that S satisfies IBN. Show that R satisfies IBN.

From these exercises we can show that many rings satisfy IBN, in particula every ring which admits a homomorphism to a division ring. This certainly includes any nonzero commutative ring: let $\mathfrak{m}$ be a maximal ideal of R: then $R \to R/\mathfrak{m}$ is a homomorphism to a field. In particular, a ring R which does not satisfy IBN must not admit any homomorphism to either a commutative ring or a division ring. Do such rings exist?

Indeed yes.

Proposition 1.17. *Let k be any field, and let $V = \bigoplus_{n=1}^{\infty} k$ be a k-vector space of countably infinite dimension. Then for $R = \operatorname{End}_k V$ and all $m, n \in \mathbb{Z}^+$, $R^m \cong R^n$ as right R-modules. In particular, R does not satisfy IBN.*

Proof. It will be enough to show that $R \cong R^2$. For this we use Exercise 1.18 (it is not necessary nor even especially easier to formulate the proof in this way, but it provides a nice illustration of that result). For $n \in \mathbb{Z}^+$, let e_n denote the nth standard basis vector of V. Define $f_1, f_2, g_1, g_2 : V \to V$ as follows: for all $n \in \mathbb{Z}^+$,

$$f_1 : e_n \mapsto e_{2n},$$
$$f_2 : e_n \mapsto e_{2n-1},$$
$$g_1 : e_{2n} \mapsto e_n, \ e_{2n-1} \mapsto 0,$$
$$g_2 : e_{2n-1} \mapsto e_n, \ e_{2n} \mapsto 0.$$

We have

$$g_1 f_1 = g_2 f_2 = f_1 g_1 + f_2 g_2 = 1_V, \ g_1 f_2 = g_2 f_1 = 0.$$

Equivalently, if we put $A = [f_1 f_2]$ and $B = [g_1 g_2]^t$, then

$$AB = I_1, \ BAI_2.$$

$\square$

Theorem 1.18. *Let R be a nonzero ring and suppose that R is* either
a) right Noetherian or
b) commutative.
Then R satisfies the strong rank condition.

Proof. CLAIM If A and B are right modules over a ring R with $B \neq 0$ and there exists an R-module embedding $A \oplus B \hookrightarrow A$, then A is not a Noetherian module.
Proof of claim: By hypothesis, A has an R-submodule of the form $A_1 \oplus B_1$ with $A_1 \cong A$ and $B_1 \cong B$. Applying the hypothesis again, $A \oplus B$ may be embedded in A_1, so A_1 contains a submodule $A_2 \oplus B_2$ with $A_2 \cong A$, $B_2 \cong B$. Continuing in this way we construct an infinite direct sum $\bigoplus_{i=1}^{\infty} B_i$ of nonzero submodules as a submodule of A. Thus A is not Noetherian.
a) Now let R be a nonzero right Noetherian ring, so for all $n \in \mathbb{Z}^+$, R^n is a Noetherian right R-module. Let $m > n \geq 1$ and let $A = R^n$, $B = R^{m-n}$. Then by

the claim there is no R-module embedding of $A \oplus B = R^m$ into $A = R^n$.

b) Suppose first that R is commutative, and let $A \in M_{nm}(R)$ be a matrix, with $m > n$. Let $x = (x_1, \ldots, x_m)^t$ be a column vector in R, so that $Ax = 0$ is a homogeneous linear sysem of n equations with m unknowns. The subring R_0 of R generated over the prime subring by the elements a_{ij} is finitely generated over the prime subring hence is Noetherian by the Hilbert Basis Theorem. By part a), the system $Ax = 0$ has a nontrivial solution in R_0 so it certainly has a nontrivial solution in R. $\square$

1.9.3. *Left Artinian implies left Noetherian.*

Theorem 1.19. *(Akizuki-Hopkins-Levitzki) A left-Artinian ring is left-Noetherian.*

Theorem 1.19 is a reuslt on Artinian rings that Emil Artin himself missed. It was first proved in the commutative case by Akizuki and then shortly thereafter for all rings by Hopkins [Ho39] and Levitzki [Le39].

We will prove Theorem 1.19 in §3 by making use of the Jacobson radical.

1.10. **Simple rings.**

A ring R is **simple** if it has exactly two ideals: 0 and R.

Proposition 1.20. *Let R be a ring and J a proper ideal of R.*
a) There exists a maximal ideal I containing J.
b) An ideal I of R is maximal iff R/I is simple.

Exercise 1.22: Prove Proposition 1.20.

Proposition 1.21. *Let A be a simple k-algebra. Then the center Z of A is a field.*

Proof. Since Z is certainly a commutative ring, it will be enough to show that any $x \in Z^\bullet$ is a unit in Z. But since x is central in A and A is simple, $Ax = AxA = xA = A$ so x is both left- and right-invertible and thus there exists $y \in A$ such that $xy = yx = 1$. The same argument as in Proposition 1.3 now shows that $y \in Z$ and finishes the proof. $\square$

An important class of simple rings comes from matrices. Let R be a ring, and let $M_n(R)$ denote the ring of all $n \times n$ matrices over R.

Exercise 1.23:
a) Show that $M_n(R)$ is commutative iff $n = 1$ and R is commutative.
b) Show that $M_m(M_n(R)) \cong M_{mn}(R)$.
c) Let J be an ideal of R. Let $M_n(J)$ be the set of all elements $m \in M_n(R)$ such that $m_{i,j} \in J$ for all $1 \leq i, j \leq n$. Show that $M_n(J)$ is an ideal of $M_n(R)$.

Theorem 1.22. *Let R be a ring and $n \in \mathbb{Z}^+$. Then every ideal $\mathcal{J}$ of the matrix ring $M_n(R)$ is of the form $M_n(J)$ for a unique ideal J of R.*

Proof. It is clear that for ideals J_1 and J_2 of R, $M_n(J_1) = M_n(J_2)$ iff $J_1 = J_2$, whence the uniqueness.

For an ideal $\mathcal{J}$ of $M_n(R)$, let $J(i, j)$ be the set of all $x \in R$ which appear as the (i, j)-entry of some element $m \in \mathcal{J}$. Since for any $x \in \mathcal{J}$, we may apply permutation matrices on the left and the right and still get an element of $\mathcal{J}$, it follows that in fact the sets $J(i, j)$ are independent of i and j, and from this is it follows easily

that this common subset is an ideal of R, say J. We claim that $\mathcal{J} = M_n(J)$. To see this, for any i, j, denote by $E(i, j)$ the matrix with (i, j) entry 1 and all other entries 0. Then for any matrix $m \in M_n(R)$ and any $1 \le i, j, k, l \le n$, we have

$$(1) \qquad\qquad E(i, j)mE(k, l) = m_{jk}E(i, l).$$

Now suppose $m \in \mathcal{J}$. Taking $i = l = 1$ in (1) above, we get $m_{jk}E(1, 1) \in \mathcal{J}$, so $m_{jk} \in J$. Thus $\mathcal{J} \subset M_n(J)$.

Conversely, let $a \in M_n(J)$. For any $1 \le i, l \le n$, by definition of J, there exists $m \in \mathcal{J}$ with $m_{1,1} = a_{i,l}$. Taking $j = k = 1$ in (1) we get

$$a_{il}E(i, l) = m_{11}E(i, l) = E(i, 1)mE(1, l) \in \mathcal{J}.$$

Therefore $a = \sum_{i,l} a_{i,l}E(i, l) \in \mathcal{J}$. $\qquad\qquad\qquad\qquad\qquad\qquad \square$

Corollary 1.23. *a) If R is a simple ring, then so is $M_n(R)$ for any $n \in \mathbb{Z}^+$.*
b) For any division ring D, $M_n(D)$ is a simple Artinian (and Noetherian) ring.

Proof. Part a) follows immediately from Theorem 1.22: since R is simple, its only ideals are 0 and R and thus the only ideals of $M_n(R)$ are $M_n(0) = 0$ and $M_n(R)$. Since a division ring is simple, certainly $M_n(D)$ is a simple ring. Moreover, we may view $M_n(D)$ as a left D-module, of finite dimension n^2. Since any left ideal of $M_n(D)$ is also a left D-module, it is clear that the maximum possible length of any chain of ideals in $M_n(D)$ is at most n^2, so there are no infinite ascending or descending chains. The same argument works for right ideals. $\qquad \square$

We wish now to give some further examples of simple rings.

Lemma 1.24. *Let $R_1 \subset R_2 \subset \ldots \subset R_n \subset \ldots$ be an ascending chain of simple rings. Then $R = \bigcup_{n \ge 1} R_n$ is a simple ring.*

Exercise 1.24: Prove Lemma 1.24.

Example: Let D be a division ring. Put $R_i = M_{2^i}(D)$, and embed $R_i \hookrightarrow R_{i+1}$ by mapping the $2^n \times 2^n$ matrix M to the $2^{n+1} \times 2^{n+1}$ matrix $\begin{bmatrix} M & 0 \\ 0 & M \end{bmatrix}$. The resulting ring $R = \bigcup_{n=1}^{\infty}$ is neither left-Noetherian, right-Noetherian, left-Artinian or right-Artinian.

Example: Let D be a division ring, and V a right D-vector space of countably infinite dimension. Let $E = \operatorname{End} V_D$ be its endomorphism ring and let I be the subring of endomorphisms φ such that $\varphi(V)$ is finite-dimensional. The quotient ring E/I is a simple ring which is not left/right Artinian/Noetherian.

Example: Let R be a simple ring of characteristic zero. Then the Weyl ring $W(R)$ is a non-Artinian simple ring. It is Noetherian iff R is Noetherian and is a domain iff R is a domain.

These examples are meant to show that the class of simple rings is very rich, going far beyond matrix rings over division rings. Notice however that none of these more exotic examples are Artinian. This serves as a segue to the Wedderburn-Artin structure theory discussed in the next section.

1.11. **Prime ideals and prime rings.**

An ideal $\mathfrak{p}$ of R is **prime** if for all ideals I, J of R, $IJ \subset \mathfrak{p}$ implies $I \subset \mathfrak{p}$ or $J \subset \mathfrak{p}$.

A ring R is a **prime ring** if for all $a, b \in R$, $aRb = (0) \implies a = 0$ or $b = 0$.

Proposition 1.25. *Let R be any ring and $\mathfrak{p}$ an ideal of R.*
a) I is maximal iff R/I is simple.
b) I is prime iff R/I is a prime ring.
c) If I is maximal, then I is prime.
d) Any domain is a prime ring.
e) In particular, a noncommutative prime ring need not *be a domain.*

Proof. a) We have seen this before: it follows from the basic correspondence theorem for quotient rings. It is included here for comparison.
b) Suppose first that I is a prime ideal, and let $a, b \in R/I$ be such that for all $x \in R/I$, $axb = 0$. Lift a and b to elements in R (for simplicity, we continue to call them a and b): then $axb = 0$ in the quotient is equivalent to $(RaR)(RbR) \subset I$. If I is a prime ideal, we conclude $RaR \subset I$ or $RbR \subset I$, so $a = 0$ in R/I or $b = 0$ in R/I.
Inversely suppose that I is not prime: so there exist ideals A, B of R with $AB \subset I$ and elements $a \in A \setminus I$, $b \in B \setminus I$. Then $aRb = (0)$ in R/I and $a, b \neq 0$ in R/I, so R/I is not a prime ring.
c) In light of the first two parts, to show that maximal ideals are prime ideals, it is equivalent to show that simple rings are prime rings. Let's show this instead: suppose R is a simple ring, let $a, b \in R$ such that $aRb = (0)$, and suppose for a contradiction that a and b are both nonzero. Then the principal ideals $(a) = RaR$ and $(b) = RbR$ are nonzero in the simple ring R, so $RaR = R = RbR$ and thus $R = RR = (a)(b) = (RaR)(RbR) = RaRbR$. But if $aRb = (0)$, then $RaRbR = R(0)R = 0$, a contradiction.
d) This is immediate from the definition.
e) By Theorem 1.22, for any field k and any $n \geq 2$, $M_n(k)$ is a simple, hence prime, ring which is not a domain. $\square$

An ideal I in a ring R is **nilpotent** if $I^N = (0)$ for some $N \in \mathbb{Z}^+$.

Corollary 1.26. *Let R be a ring, I a nilpotent ideal of R and $\mathfrak{p}$ a prime ideal of R. Then $I \subset \mathfrak{p}$.*

Exercise 1.25: Prove Corollary 1.26.

1.12. **Notes.**

Much of the material from this section is taken from [L-FC, §1], but most of the material of §1.9 is taken from [L-MR, §1]. We included treatment of topics like the strong rank condition because of their inherent interest and because it showcases an (apparently rare) opportunity to deduce something about commutative rings from something about not necessarily commutative Noetherian rings. (Coverage of the strong rank condition for commutative rings is thus far missing from my commutative algebra notes.) With the exception of §1.9, we have given just about the briefest overview of noncommutative rings that we could get away with.

2. Wedderburn-Artin Theory

2.1. Semisimple modules and rings.

Throughout this section all modules are *left* R-modules.

Theorem 2.1. *For an R-module M, TFAE:*
(i) M is a direct sum of simple submodules.
(ii) Every submodule of M is a direct summand.
(iii) M is a sum of simple submodules.
*A module satisfying these equivalent conditions is called **semisimple**.*

Proof. (i) $\implies$ (ii): Suppose $M = \bigoplus_{i \in I} S_i$, with each S_i a simple submodule. For each $J \subset I$, put $M_J = \bigoplus_{i \in J} S_i$. Now let N be an R-submodule of M. An easy Zorn's Lemma argument gives us a maximal subset $J \subset I$ such that $N \cap M_J = 0$. For $i \notin J$ we have $(M_J \oplus S_i) \cap N \neq 0$, so choose $0 \neq x = y + z$, $x \in N$, $y \in M_J$, $z \in S_i$. Then $z = x - y \in (M_j + N) \cap S_i$, and if $z = 0$, then $x = y \in N \cap M_j = 0$, contradiction. So $(M_J \oplus N) \cap S_i \neq 0$. Since S_i is simple, this forces $S_i \subset M_J \oplus N$. It follows that $M = M_J \oplus N$.

(ii) $\implies$ (i): First observe that the hypothesis on M necessarily passes to all submodules of M. Next we CLAIM that every nonzero submodule $C \subset M$ contains a simple module.

PROOF OF CLAIM: Choose $0 \neq c \in C$, and let D be a submodule of C which is maximal with respect to not containing c. By the observation of the previous paragraph, we may write $C = D \oplus E$. Then E is simple. Indeed, suppose not and let $0 \subsetneq F \subsetneq E$. Then $E = F \oplus G$ so $C = D \oplus F \oplus G$. If both $D \oplus F$ and $D \oplus G$ contained c, then $c \in (D \oplus F) \cap (D \oplus G) = D$, contradiction. So either $D \oplus F$ or $D \oplus G$ is a strictly larger submodule of C than D which does not contain c, contradiction. So E is simple, establishing our claim.

Now let $N \subset M$ be maximal with respect to being a direct sum of simple submodules, and write $M = N \oplus C$. If $C \neq 0$, then by the claim C contains a nonzero simple submodule, contradicting the maximality of N. Thus $C = 0$ and M is a direct sum of simple submodules.

(i) $\implies$ (iii) is immediate.

(iii) $\implies$ (i): as above, by Zorn's Lemma there exists a submodule N of M which is maximal with respect to being a direct sum of simple submodules. We must show $N = M$. If not, since M is assumed to be generated by its simple submodules, there exists a simple submodule $S \subset M$ which is not contained in N. But since S is simple, it follows that $S \cap N = 0$ and thus $N \oplus S$ is a strictly larger direct sum of simple submodules: contradiction. $\square$

Remark: By convention, the zero module is viewed as the direct sum of an empty family of simple modules, so does count as semisimple.

Exercise 2.1: Show that all submodules and quotient modules of a semisimple module are semisimple.

Corollary 2.2. *An R-module M has a unique maximal semisimple submodule, called the **socle of M** and written $\operatorname{Soc} M$. Thus M is semisimple iff $M = \operatorname{Soc} M$.*

Exercise 2.2: Prove Corollary 2.2.

Exercise 2.3: Let $N \in \mathbb{Z}^+$. Compute the socle of the $\mathbb{Z}$-module $\mathbb{Z}/N\mathbb{Z}$. Show in particular that $\mathbb{Z}/N\mathbb{Z}$ is semisimple iff N is squarefree.

Lemma 2.3. *Let R be a ring, I an infinite index set and for all $i \in I$ let M_i be a nonzero left R-module. Then the direct sum $M = \bigoplus_{i \in I} M_i$ is not finitely generated.*

Proof. Let $x_1, \ldots, x_n$ be any finite subset of M. By definition of the direct sum, the subset J of I consisting of indices of nonzero components of some x_i is finite. The left R-submodule generated by $x_1, \ldots, x_n$ is then contained in $\bigoplus_{i \in J} M_i$ and thus is certainly proper in M. $\qquad\square$

Proposition 2.4. *Let R be a ring and M a semisimple left R-module. TFAE:*
(i) M is finitely generated.
(ii) M is Noetherian.
(iii) M is Artinian.
(iv) M is a direct sum of finitely many simple modules.

Proof. Let $M = \bigoplus_{i \in I} S_i$ be a direct sum of nonzero simple submodules. Each S_i is monogenic, so if I is finite, then M is clearly finitely generated. Moreover M then has a composition series so is both Noetherian and Artinian. Therefore (iv) implies (i), (ii) and (iii).
(ii) $\implies$ (iv): M is Noetherian then I must be finite, since otherwise we could well order I and get an infinite ascending chain

$$S_0 \subset S_0 \oplus S_1 \subset \ldots \subset S_0 \oplus \ldots \oplus S_n \subset \ldots .$$

(iii) $\implies$ (iv): Similarly if M is Artinian then I must be finite, or

$$\bigoplus_{i \geq 0} S_i \supsetneq \bigoplus_{i \geq 1} S_i \supsetneq \ldots$$

is an infinite descending chain.
(i) $\implies$ (iv): This follows immediately from Lemma 2.3. $\qquad\square$

Theorem 2.5. *For a ring R, TFAE:*
(i) R is semisimple as a left R-module.
(ii) All monogenic left R-modules are semisimple.
(iii) All left R-modules are semisimple.
(iv) All short exact sequences of left R-modules split.
(v) All left R-modules are projective.
(vi) All left R-modules are injective.

Proof. (i) $\implies$ (ii): A left R-module is monogenic iff it is a quotient of the left R-module R. Now recall that quotients of semisimple modules are semisimple.
(ii) $\implies$ (iii): Let M be a left R-module. By Theorem 2.1 it is enough to show that M is a sum of simple submodules. But every module is a sum of monogenic submodules – $M = \sum_{x \in M} Rx$ – so if every monogenic R-module is semisimple then every monogenic R-module is the sum of simple submodules and thus so is M.
(iii) $\implies$ (i) is immediate.
(iii) $\implies$ (iv): A short exact sequence of R-modules

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

splits iff the submodule M_1 is a direct summand, and by Theorem 2.1 this holds when M_2 is semisimple.

(iv) $\implies$ (iii): Let $N \subset M$ be a left R-submodule. By hypothesis,

$$0 \to N \to M \to M/N \to 0$$

splits, so N is a direct summand of M.

(iv) $\iff$ (v): A left R-module P is projective iff every short exact sequence

$$0 \to M_1 \to M_2 \to P \to 0$$

splits. This holds for all P iff every short exact sequence of R-modules splits.

(iv) $\iff$ (vi): A left R-module I is injective iff every short exact sequence

$$0 \to I \to M_2 \to M_2 \to 0$$

splits. This holds for all I iff every short exact sequence of R-modules splits. $\quad\square$

Corollary 2.6. *A left semisimple ring is both left-Noetherian and left-Artinian.*

Proof. By definition we have a direct sum decomposition $R = \bigoplus_{i \in I} U_i$, where each U_i is a minimal left ideal. The same argument that proved (i) $\implies$ (iv) in Proposition 2.4 shows that the index set I is finite, and now Proposition 2.4 implies that as a left R-module R is Noetherian and Artinian. $\quad\square$

Lemma 2.7. *Let $R_1, \ldots, R_r$ be finitely many rings and put $R = \prod_{i=1}^{r} R_i$. TFAE:*
(i) Each R_i is left semisimple.
(ii) R is left semisimple.

Proof. (i) $\implies$ (ii) For each i, we may write $R_i = \bigoplus_{j=1}^{n_i} \mathcal{I}_{ij}$, a direct sum into minimal left-ideals. In turn each R_i is a two-sided ideal of R, and thus each $\mathcal{I}_{ij}$ becomes a minimal left-ideal of R. Thus $R = \bigoplus_{i,j} \mathcal{I}_{i,j}$ is a decomposition of R as a direct sum of minimal left ideals.

(ii) $\implies$ (i) Each R_i is, as a left R-module, a quotient of R, and quotients of semisimple modules are semisimple, so R_i is a semisimple left R-module. But the R_i-module structure on R_i is induced from the R-module structure – in particular, a subgroup of R_i is an R_i-submodule iff it is an R-submodule – so being semisimple as an R-module is equivalent to being semisimple as an R_i-module. $\quad\square$

2.2. Wedderburn-Artin I: Semisimplicity of $M_n(D)$.

Let D be a division ring, $n \in \mathbb{Z}^+$, and put $R = M_n(D)$. In this section we want to show that R is a left semisimple ring and explicitly decompose R into a sum of simple left R-modules.

Theorem 2.8. *(Wedderburn-Artin, Part I) Let $R = M_n(D)$ be a matrix ring over a division ring. Then:*
a) R is simple, left Artinian and left Noetherian.
b) There is a unique simple left R-module V, up to isomorphism. Moreover R acts faithfully on V and as left R-modules we have

$$_R R \cong V^n.$$

In particular R is a left semisimple ring.

Proof. a) The two-sided ideals in all matrix rings have been classified in Theorem 1.22 above; in particular, since D has no nontrivial two-sided ideals, neither does R. Moreover R is an n^2-dimensional left D-vector space and any left ideal is in particular a left D-subspace, so the length of any ascending or descending chain of

left ideals in R is bounded by n^2. Thus R is left-Noetherian and left-Artinian.

b) Let $V = D^n$ viewed as a right D-vector space. Viewing V as a space of $n \times 1$ column vectors with entries in D endows it with the structure of a left $R = M_n(D)$-module. Indeed, by Proposition 1.9 we have $R = \mathrm{End}(V_D)$. The action of the endomorphism ring of a module on the module is always faithful. Moreover, by standard linear algebra techniques one can show that for any $0 \neq v \in V$, $Rv = V$, so V is a simple left R-module.

Now, for $1 \leq i \leq n$, let U_i be the subset of R consisting of all matrices whose entries are zero outside of the ith column. One sees immediately that each U_i is a left ideal of R and

$$(2) \qquad R = \bigoplus_{i=1}^{n} U_i.$$

Moreover, each U_i is isomorphic as a left R-module to V, which shows that $_R R$ is a semisimple module and thus that R is a left semisimple ring. Morover every simple left R-module is monogenic hence of the form R/I for some left ideal I of R, hence by Jordan-Hölder is isomorphic to some U_i, i.e., is isomorphic to V. $\qquad \square$

Exercise 2.4: Show that $\mathrm{End}(_R V) \cong D$. (Suggestion: define a map $\Delta : D \to \mathrm{End}(_R V)$ by $d \in D \mapsto (v \in V \mapsto v \cdot d)$ and show that Δ is a ring isomorphism.)

2.3. Wedderburn-Artin II: Isotypic Decomposition.

A semisimple R-module M is **isotypic** if all of its simple submodules are isomorphic. That is, a module is isotypic iff there exists a simple module S such that M is isomorphic to a direct sum of copies of S. For instance a finite abelian group is isotypic as a $\mathbb{Z}$-module iff it is an elementary abelian p-group.

Lemma 2.9. *Let S_1 and S_2 be simple modules, let M_1 be an S_1-isotypic module and M_2 be an S_2-isotypic module. Suppose there exists a nonzero R-module map $f : M_1 \to M_2$. Then $S_1 \cong S_2$.*

Proof. Suppose $M_1 = \bigoplus_{i \in I_1} S_1$ and $M_2 = \bigoplus_{j \in I_2} S_2$. Then a homomorphism f from M_1 into any module is determined by its restrictions f_i to the ith direct summand: if $x = (x_i)$, then $f(x) = \sum_{i \in I_1} f_i(x_i)$. (This is the universal property of the direct sum.) Since f is not the zero map, there exists $i \in I_1$ such that $f_i : S_i \to M_2$ is nonzero. Similarly, for all $j \in I_2$, let $\pi_j : M_2 \to S_2$ be projection onto the jth copy of S_2. Choose $x \in M_1$ such that $f_i(x) \neq 0$. Then there exists $j \in I_2$ such that $\pi_j(f_i(x)) \neq 0$, so $\pi_j \circ f_i : S_1 \to S_2$ is a nonzero homomorphism between simple modules. By Proposition 2.4, this implies $S_1 \cong S_2$. $\qquad \square$

Thus every isotypic module is S-isotypic for a unique (up to isomorphism) simple module S. (It turns out to be convenient here to be sloppy in distinguishing between a simple module and its isomorphism class.)

Lemma 2.10. *Let S be a simple module and I and J be index sets. Suppose $U = \bigoplus_{i \in I} U_i$ and $V = \bigoplus_{j \in J} V_j$ and that for all i, j we have $U_i \cong V_j \cong S$. Then TFAE:*
(i) $\#I = \#J$.
(ii) $U \cong V$.

Proof. (i) $\implies$ (ii): This is almost obvious. We leave it to the reader. (ii) $\implies$ (i): Let $\varphi : U \to V$ be an isomorphism of R-modules.

Case 1: If I and J are both finite, this is a special case of Jordan-Hölder.

Case 2: Suppose that exactly one of I and J is finite. Then by Lemma 2.3 exactly one of U and V is finitely generated, so they cannot be isomorphic modules.

Case 3:[5] Finally, suppose that I and J are both infinite. For each $i \in I$, choose $0 \neq x_i \in U_i$. Then there exists a finite subset F_i of J such that

$$\varphi(x_i) \in \sum_{j \in F_i} V_j.$$

Since φ is an isomorphism, $\varphi(U_i) \cap \sum_{j \in F_i} V_j \neq 0$ and since $\varphi(U_i) \cong S$ is simple, we deduce $\varphi(U_i) \subset \sum_{j \in F_i} V_j$. Let $K = \bigcup_{i \in I} F_i$. Note that since K is a union of finite sets indexed by the infinite set I, $\#K \leq \#I$. For all $i \in I$ we have

$$\varphi(U_i) \subset \sum_{j \in K} V_j,$$

hence

$$V = \varphi(U) = \sum_{i \in I} \varphi(U_i) \subset \sum_{j \in K} V_j.$$

Since the last sum is direct, we conclude $K = J$ and thus $\#J = \#K \leq \#I$. The same argument with U and V reversed gives $\#I \leq \#J$ and thus $\#I = \#J$. $\qquad\square$

An **isotypic decomposition** of a semisimple module M is a decomposition

$$M = \bigoplus_{i \in I} U_i,$$

where each U_i is S_i-isotypic and for all $i \neq j$, S_i and S_j are nonisomorphic simple modules. This sounds rather fancy, but it handles like a dream. In particular, note that every semisimple module has an isotypic decomposition: to get one, we start with a decomposition as a direct sum of simple modules and collect together all mutually isomorphic simple modules. In fact the isotypic decomposition of a semisimple module is *unique* up to the order of the direct summands (it will be convenient to be sloppy about that too): let I be a set indexing the isomorphism classes S_i of simple modules: then we must have $M = \bigoplus_{i \in I} U_i$, where U_i is the direct sum of all simple submodules isomorphic to S_i, i.e., there is no choice in the matter. Combined with Lemma 2.10, we see that to any semisimple module and any isomorphism class S_i of simple modules we may associate a cardinal number κ_i, the number of copies of S_i appearing in any direct sum decomposition of M.

Theorem 2.11. *Let M be a nonzero finitely generated semisimple left R-module. a) Then there exists: a positive integer r, pairwise nonisomorphic simple left R-modules $S_1, \ldots, S_r$ and positive integers $n_1, \ldots, n_r$ such that the isotypic decomposition of M is*

$$M = \bigoplus_{i=1}^{r} U_i = \bigoplus_{i=1}^{r} S_i^{n_i}.$$

The integer r is uniquely determined, as are the isomorphism classes of the S_i and the integers n_i, up to permutation.

---

[5]We follow the proof of [Ch56, Thm. III.24].

b) For each i, put $D_i = \text{End}(S_i)$, which is, by Schur's Lemma, a division ring. Then

(3) $$\text{End}(_R M) \cong M_{n_1}(D_1) \times \ldots \times M_{n_r}(D_r).$$

Proof. The only thing that remains to be proven is (3). Let $f \in \text{End}(_R M)$. By Lemma 2.9, $f(U_i) \subset U_i$ for all i and thus

$$\text{End}(_R M) = \bigoplus_{i=1}^{r} \text{End}(_R U_i) = \bigoplus_{i=1}^{r} \text{End}(_R S_i^{n_i}) = \bigoplus_{i=1}^{r} M_{n_i}(D_i).$$

$\square$

Now suppose that R is a left semisimple ring, and let

$$R = B_1 \times \ldots \times B_r$$

be its isotypic decomposition. Since simple left R-submodules of R are precisely the minimal left ideals I_i of R, each B_i is precisely the left ideal generated by all minimal left ideals isomorphic as modules to I_i.

Lemma 2.12. *Let R be any ring, and for each minimal left ideal U of R, let B_U be the left R-submodule of R generated by all ideals isomorphic to U.*
a) Then B_U is a two-sided ideal.
b) If R is left semisimple, then B_U is generated as a two-sided ideal by any one minimal left ideal isomorphic to U. In particular, B_U is a minimal ideal.

Proof. a) Certainly B_U is a left ideal of R, so to show that it is an ideal, it's enough to show that for any minimal left ideal J with $J \cong U$, then $JR \subset B_U$. To see this: let $r \in R$. Then the left R-module Jr is a homomorphic image of the simple module J, so either $Jr = 0$ or $Jr \cong J \cong U$. Either way, $Jr \subset B_U$.
b) Let J be a minimal left ideal isomorphic as to I as a left R-module. Since R is semisimple, there exist left ideals J' and I such that $R = I \oplus I' = J \oplus J'$. By Jordan-Hölder, we have $J \cong J'$, and therefore any isomorphism $f : I \to J$ extends to an isomorphism $F : R \to R$. But all R-module endomorphisms of R are of the form right multiplication by a, so $J = Ia$ for some $a \in R^\times$. $\square$

Exercise 2.5: Let R be a ring and let U and U' be minimal left ideals which are *not* isomorphic as R-modules. Show that $B_U B_{U'} = 0$.

Lemma 2.13. *Let R be a left semisimple ring. Then every simple left R-module appears with positive multiplicity in the isotypic decomposition of R.*

Proof. Indeed, a simple module over any ring is monogenic, hence a quotient of R. Since R is semisimple, quotients are also direct summands. $\square$

Now let R be a left semisimple ring. By Proposition 2.4 and Lemma 2.13 there are finitely many isomorphism classes of minimal left R-ideals, say $I_1, \ldots, I_r$, and the isotypic decomposition of R as a left R-module is

$$R = B_1 \times \ldots B_r,$$

where $B_i = B_{I_i}$ is a two-sided ideal – the sum of all left ideals isomorphic to I_i.

Lemma 2.14. *Let R be any ring and suppose that we have a decomposition*

$$R = J_1 \times \ldots \times J_r$$

into a direct product of two-sided ideals. Let $1 = (e_1, \ldots, e_r)$ be the decomposition of the identity. Then for all $1 \leq i \leq r$ and all $x_i \in J_i$, $e_i x_i = x_i e_i = x_i$, i.e., each J_i is a ring in its own right with identity element e_i.

Exercise 2.6: Prove it.

Applying Theorem 2.11, we get

$$R = \mathrm{End}(_R R) \cong M_{n_1}(D_1) \times \ldots \times M_{n_r}(D_r),$$

so every left semisimple ring is a direct product of finitely many matrix rings over division rings.

Since each $M_{n_i}(D_i)$ is a simple ring, as an ideal in R it is minimal. We also have our isotypic decomposition into minimal ideals B_i, so of course it is natural to suspect that we must have, up to permutation of the factors, $B_i = M_{n_i}(D_i)$ for all i. The following simple result allows us to see that this is the case.

Say an ideal I in a ring R is **indecomposable** if it cannot be written in the form $I_1 \times I_2$ where I_1 and I_2 are two nonzero ideals. Clearly a minimal ideal is indecomposable.

Lemma 2.15. *Let R be a ring with nonzero ideals $B_1, \ldots, B_r, C_1, \ldots, C_s$ such that*

$$R = B_1 \oplus \ldots \oplus B_r = C_1 \oplus \ldots \oplus C_s$$

and all ideals B_i, C_j indecomposable. Then $r = s$ and after a permutation of indices we have $B_i = C_i$ for all i.

Proof. As in Lemma 2.14, we may view each B_i as a ring in its own right and then $R = B_1 \times \ldots \times B_r$. Under such a decomposition every ideal of R is of the form $I_1 \times \ldots I_r$ with each I_i an ideal of R_i. Applying this in particular to C_1 and using its indecomposability, we find that $C_1 \subset B_i$ for some i; after reindexing we may assume $C_1 \subset B_1$. A symmetrical argument shows that $B_1 \subset C_j$ for some j and thus $C_1 \subset B_1 \subset C_j$. Evidently then we must have $j = 1$ and $B_1 = C_1$. We are done by induction. $\square$

Theorem 2.16. *(Wedderburn-Artin, Part II) Let R be a left semisimple ring. Let*

$$(4) \hspace{4cm} R = V_1^{n_1} \oplus \ldots V_r^{n_r}$$

be its isotypic decomposition, i.e., $V_1, \ldots, V_r$ are pairwise non-isomorphic simple left R-modules and $n_i \in \mathbb{Z}^+$. For all $1 \leq i \leq r$, let $D_i = \mathrm{End}(_R V_i)$. Then:
a) Each D_i is a division algebra.
*b) We have a **Wedderburn Decomposition***

$$(5) \hspace{4cm} R = M_{n_1}(D_1) \times \ldots \times M_{n_r}(D_r),$$

where $M_{n_i}(D_i)$ is the V_i-isotypic ideal of R.
c) The integer r, the multiset $\{n_1, \ldots, n_r\}$ and the multiset of isomorphism classes $\{[D_1], \ldots, [D_r]\}$ are invariants of R.
d) Conversely, a finite product of matrix rings over division rings is left semisimple.

Proof. Part a) has already been established. As for part b), the only new statement is that $M_{n_i}(D_i) = V_i^{n_i}$. But we know that $V_i^{n_i}$ is the isotypic ideal B_{V_i}, so both (4) and (5) are decompositions of R into products of indecomposable ideals, so by Lemma 2.15 these ideals are equal after a permutation. But by Theorem 2.8,

$M_{n_i}(D_i)$ is isomorphic as a left R-module to $V_i^{n_i}$ and (by the theory of isotypic decompositions) *not* to any other $V_j^{n_j}$, so we must have equality. As for part c): we have gone to some trouble to show that the Wedderburn decomposition (5) *is* the isotypic decomposition (4) which is *unique*, so everything is an invariant of R. d) By Theorem 2.8 we know that every matrix ring over a division ring is semisimple, and by Lemma 2.7 we know that a finite product of semisimple rings is semisimple. $\square$

Corollary 2.17. *A ring R is left semisimple iff it is right semisimple.*

Proof. First recall that a ring D is division iff D^{op} is division. Now apply Wedderburn-Artin: R is left semisimple iff

$$R \cong \prod_{i=1}^{r} M_{n_i}(D_i)$$

iff

$$R^{\mathrm{op}} \cong \prod_{i=1}^{r} M_{n_i}(D_i^{\mathrm{op}}) = \prod_{i=1}^{r} M_{n_i}(D_i')$$

iff R^{op} is left semisimple iff R is right semisimple. $\square$

Note that in light of Corollary 2.17, we need no longer say "left semisimple ring" or "right semisimple ring" but merely "semisimple ring". What a relief!

2.4. **Wedderburn-Artin III: When Simple Implies Semisimple.**

It is perhaps time to state Wedderburn's version of the Wedderburn-Artin Theorem. Wedderburn was interested in rings R whose center contains a field k and such that R is finite-dimensional as a k-vector space: in short, finite-dimensional k-algebras. (In fact for much of the course this is the class of rings we shall be interested in as well.)

Theorem 2.18. *(Classical Wedderburn Theorem) A finite dimensional k-algebra is simple if and only if it is isomorphic to $M_n(D)$, where D/k is a finite degree division algebra.*

Comparing Theorems 2.16 and 2.18, we see that to show the latter we must show that a finite dimensional simple k-algebra is semisimple. In terms of pure terminology, it is somewhat unfortunate that simple does not imply semisimple for all rings, but this is indeed not the case since we have seen simple rings which are Noetherian and not Artinian and also simple rings which are not Noetherian, whereas any semisimple ring is Artinian. Indeed this turns out to be the key condition:

Theorem 2.19. *(Wedderburn-Artin, Part III) For a simple ring R, TFAE:*
(i) R is left Artinian.
(ii) R has a minimal left ideal.
(iii) R is left semisimple.
(iv) $R \cong M_n(D)$ for some division ring D and some $n \in \mathbb{Z}^+$.

Proof. (i) $\implies$ (ii) is immediate: if DCC holds for ideals, choose a nonzero ideal I_1; it is not minimal among nonzero ideals, choose a smaller nonzero ideal I_2. If I_2 is not minimal among nonzero ideals, choose a smaller nonzero ideal I_3. And so forth: if we never arrived at a minimal nonzero ideal then we would have an infinite

descending chain of ideals: contradiction.

(ii) $\implies$ (iii): Let I be a minimal nonzero ideal, and let B_I be the associated isotypic ideal. Thus B_I is a nonzero ideal in the simple ring R, so $B_I = R$. This exhibits R as a sum of simple left R-modules, so R is semisimple.

(iii) $\implies$ (iv) is part of Wedderburn-Artin, Part II (Theorem 2.16).

(iv) $\implies$ (i): By Wedderburn-Artin, Part I (Theorem 2.8, matrix rings over division rings are left semisimple and left Artinian. $\square$

Exercise 2.7: Show that Theorem 2.19 implies Theorem 2.18.

2.5. **Maschke's Theorem.**

The following classic result of Maschke[6] provides a link between the theory of semisimple algebras and the representation theory of finite groups.

Theorem 2.20. *(Maschke* [Ma99]*) For k a field and G a group, TFAE:*
(i) G is finite, and the characteristic of k does not divide $\#G$.
(ii) The group ring $k[G]$ is semisimple.

Proof. (i) $\implies$ (ii): Let $N = \#G$. Let U be a $k[G]$-module and V a $k[G]$-submodule. We must show that V is a direct summand of U. Certainly we may choose a k-subspace W of U such that $U = V \oplus W$. There is the minor problem that W need not be a $k[G]$-submodule, but we can fix this by an *averaging process*: let $\pi : U = V \oplus W \to V$ be projection onto the first factor. Define $\pi' : U \to U$ by

$$\pi'(u) = \frac{1}{N} \sum_{g \in G} g\pi(g^{-1}u);$$

note that $\frac{1}{N} \in k$ since the characteristic of k does not divide N.

CLAIM π' is a $k[G]$-module map.

Proof of claim: let $x \in G$ and $u \in U$. Then:

$$\pi'(xu) = \frac{1}{N} \sum_{g \in G} g\pi(g^{-1}xu) = \frac{1}{N} \sum_{g \in G} xx^{-1}g\pi(g^{-1}xu)$$

$$= \frac{1}{N}x\left(\sum_{g \in G} x^{-1}g\pi(g^{-1}xu) \right) = x\pi'(u).$$

Since V is a $k[G]$-submodule of U, for all $g \in G$ and $v \in V$ we have $gv \in V$, and thus $\pi'(U) \subset V$. Moreover, since π is the identity on V, for all $g \in G$ and $v \in V$,

$$g\pi(g^{-1}v) = gg^{-1}v = v,$$

so $\pi'|_V = 1_V$. The endomorphism π' is therfore a projection operator – i.e., $\pi'^2 = \pi'$ – and thus

$$U = \ker(\pi') \oplus \mathrm{im}(\pi') = \ker(\pi') \oplus V.$$

Since π' is a $k[G]$-module map, $\ker(\pi')$ is a $k[G]$-submodule of U.

(ii) $\implies$ (i): For any field k and group G, we denote by k the $k[G]$-module with underlying k-vector space k and *trivial G-action*: for all $\alpha \in k$, $g\alpha = \alpha$. There is a surjective $k[G]$-module map $\epsilon : k[G] \to k$ defined by $\epsilon(g) = 1$ for all $g \in G$, the

---

[6]Heinrich Maschke, 1853-1908

augmentation map. Let $\Delta = \ker \epsilon$, the **augmentation ideal**, so we have a short exact sequence of $k[G]$-modules

$$0 \to \Delta \to k[G] \overset{\epsilon}{\to} k \to 0.$$

If $k[G]$ is semisimple, this sequence splits, i.e., there exists a one-dimensional k-subspace V of $k[G]$ with trivial G-action such that $k[G] = \Delta \oplus V$.

Case 1: Suppose G is finite, $\#G = N$, and $N = 0$ in k. We may compute the submodule $k[G]^G$ of elements on which G acts trivially: it consists of elements of the form αv_0 for $\alpha \in k$, where $v_0 = \sum_{g \in G} g$. Then $\epsilon(\alpha v_0) = \alpha N = 0$, so these elements lie in Δ. Thus when the characteristic of k divides N Δ is not a direct summand of $k[G]$.

Case 2: Suppose G is infinite. Then $v_0 = \sum_{g \in G} g$ is *not* an element of $k[G]$: it has infinitely many nonzero coefficients. From this it follows that $k[G]^G = (0)$, which in turn implies that the augmentation ideal Δ of $k[G]$ is not a direct summand. $\quad\square$

Exercise 2.8: For a group G consider the **integral group ring** $\mathbb{Z}[G]$.
a) Show that we still have a surjective augmentation map $\epsilon : \mathbb{Z}[G] \to \mathbb{Z}$ and an augmentation ideal $\Delta = \ker \epsilon$.
b) Show that $\mathbb{Z}[G]$ is not a semisimple ring. (Hint: show that $\mathbb{Z}$ is not semisimple and apply part a).)
c) Show that if G is nontrivial, the short exact sequence of $\mathbb{Z}[G]$-modules

$$1 \to \Delta \to \mathbb{Z}[G] \to \mathbb{Z} \to 1$$

does not split, and thus $\mathbb{Z}$ is not a projective $\mathbb{Z}[G]$-module.[7]

Exercise 2.9: Let G be a group and k a field.
a) For any $k[G]$-module V, recall that $V^G = \{x \in V \mid gx = x \; \forall g \in G\}$. Show that the functor $V \mapsto V^G$ is left exact: i.e., if

$$0 \to V_1 \to V_2 \to V_3 \to 0,$$

is a short exact sequence of $k[G]$-modules, then

$$0 \to V_1^G \to V_2^G \to V_3^G$$

is exact.
b) Give an example of k and G such that there exists a surjection $V \to W$ of $k[G]$-modules such that $V^G \to W^G$ is not surjective.
c) Show that for any $k[G]$-module V, $V^G = \text{Hom}_{k[G]}(k, V)$.
d) Deduce that the functor $V \mapsto V^G$ is exact iff k is a projective $k[G]$-module.
e) Give necessary and sufficient conditions on k and G for $V \mapsto V^G$ to be exact.

Theorem 2.21. *Let G be a finite group, and let*

$$(6) \qquad \mathbb{C}[G] = \prod_{i=1}^{r} M_{n_i}(\mathbb{C})$$

be the Wedderburn decomposition of the complex group ring.
a) The number r of simple factors is equal to the number of conjugacy classes of G.

---

[7]This is an important early result in group cohomology: the **cohomological dimension** of a group G is the minimal length of a projective resolution of $\mathbb{Z}$ as a $\mathbb{Z}[G]$-module (or ∞ if there is no finite projective resolution), and this shows that the cohomological dimension of a group is zero iff the group is trivial.

b) Also r is equal to the number of inequivalent irreducible $\mathbb{C}$-representations of G.
c) The numbers $n_1, \ldots, n_r$ are the dimensions of the irreducible representations.
d) We have $\sum_{i=1}^{r} n_i^2 = \#G$.

Proof. a) Step 1: Take centers in the Wedderburn decomposition:

$$Z = Z(\mathbb{C}[G]) = Z(\prod_{i=1}^{r} M_{n_i}(\mathbb{C})) = \prod_{i=1}^{r} Z(M_{n_i}(\mathbb{C})) = \prod_{i=1}^{r} \mathbb{C}.$$

Therefore $r = \dim_{\mathbb{C}} Z$, so it suffices to show that the latter quantity is equal to the number of conjugacy classes in G.
Step 2: We define a **class function** $f : G \to \mathbb{C}$ to be a function which is constant on conjugacy classes: for all $x, g \in G$, $f(xgx^{-1}) = f(g)$. The class functions form a $\mathbb{C}$-subspace of $\mathbb{C}[G]$ of dimension equal to the number of conjugacy classes. So it suffices to show that the $\mathbb{C}$-dimension of the center of the group ring is equal to the $\mathbb{C}$-dimension of the space of class functions.
Step 3: We claim that in fact these two spaces are identical: that is, the class functions, as a subset of $\mathbb{C}[G]$, are precisely the center Z. We leave the verification of this to the reader as a pleasant exercise.
b),c) By definition an irreducible representation is a homomorphism $\rho : G \to \mathrm{GL}(V)$, where V is a finite-dimensional $\mathbb{C}$-vector space which does not admit any nonzero, proper G-invariant subspace. Representations correspond precisely to $\mathbb{C}[G]$-modules, and under this correspondence the irreducible representations correspond to simple $\mathbb{C}[G]$-modules. We now appeal to Wedderburn-Artin theory: the isomorphism classes of the simple $\mathbb{C}[G]$ modules are determined by the Wedderburn decomposition of $\mathbb{C}[G]$: there are precisely r of them, say $V_1, \ldots, V_r$ occuring with multiplicities $n_1, \ldots, n_r$. Moreover, as a right $D_i = \mathrm{End}\, V_i = \mathbb{C}$-module, $V_i \cong D_i^{n_i} \cong \mathbb{C}^{n_i}$, and thus the dimension of the underlying $\mathbb{C}$-vector space is n_i.
d) This follows by taking $\mathbb{C}$-dimensions of the left and right hand sides of (6). $\square$

Exercise 2.10: Show that there is no group of order 8 with exactly four conjugacy classes. (Hint: there are up to isomorphism five groups of order 8, but this is *not* the easy way to solve this problem.)

Exercise 2.11: a) In the notation of Theorem 2.21, let a be the number of indices i such that $n_i = 1$. Show: a is equal to the order of the abelianization of G.
b) Deduce that the dimensions of the irreducible $\mathbb{C}$-representations of S_3 are $(1, 1, 2)$.

If we work over a field k, of characteristic not dividing the order of G so that $k[G]$ is semisimple, but *not* algebraically closed, then the division algebras appearing in the Wedderburn decomposition need not be k itself, which makes things more interesting (and more complicated). The following exercises explore this.

Exercise 2.12: Let G be a finite cyclic group of order n.
a) Show that for any field k the group ring $k[G]$ is isomorphic to $k[t]/(t^n - 1)$.
b) Use part a) to directly verify that $k[G]$ is semisimple iff the characteristic of k does not divide n.
c) If k is algebraically closed of characteristic not dividing n (e.g. $k = \mathbb{C}$), show that $k[G] \cong k^n$.

d) If n is prime, show that $\mathbb{Q}[G] \cong \mathbb{Q} \times \mathbb{Q}(\zeta_n)$. Conclude that there is a $(p-)1$-dimensional $\mathbb{Q}$-irreducible representation which "splits" into $p - 1$ inequivalent 1-dimensional $\mathbb{C}$-representations.
e) What is the structure of $\mathbb{Q}[G]$ for not necessarily prime n?

Exercise 2.13: Let G be the quaternion group of order 8. It can be constructed (conveniently for this exercise) as the subgroup $\{\pm 1, \pm i, \pm j, \pm ij\}$ of the multiplicative group $B^\times$ of the quaternion algebra $B = \left(\frac{-1,-1}{\mathbb{Q}}\right)$.
a) Show that
$$\mathbb{Q}[G] \cong \mathbb{Q}^4 \oplus B.$$
b) Deduce that
$$\mathbb{C}[G] \cong \mathbb{C}^4 \oplus M_2(\mathbb{C}).$$
c) Explain why it's reasonable to say: the $\mathbb{Q}[G]$-module B **ramifies** in $\mathbb{Q}(i)/\mathbb{Q}$.

Theorem 2.22. *Let p be a prime number, G a finite p-group (i.e., $\#G = p^a$ for some $a \in \mathbb{Z}^+$) and k a field of characteristic p.*
a) Let $0 \neq V$ be a $k[G]$-module which is finite-dimensional over k. Then $V^G \neq 0$.
b) Up to isomorphism the only irreducible finite-dimensional k-representation of G is the one-dimensional trivial representation k.

Proof. a) It is no loss of generality to assume that G acts faithfully on V (otherwise we are proving the result for some proper quotient of G) and thus without loss of generality $G \subset \mathrm{GL}_n(k)$. For all $g \in G$ we have $g^{p^a} = 1$ and therefore the eigenvalues of g are p-power roots of unity. Since k has characteristic p, all the eigenvalues of g are equal to 1: g is a **unipotent matrix**. We work by induction on $a = \log_p \#G$. Base Case: When $a = 1$, $G = \langle g \rangle$ for a single unipotent matrix g. Since the eigenvalues of G lie in the ground field, g may be put in Jordan canonical form over k, which indeed means that g is conjugate to an element of T_n and thus acts trivially on a nonzero vector as above.
Induction Step: Now assume $a > 1$ and the result holds for all p-groups of order less than p^a. Recall that a p-group is nilpotent hence solvable, so there exists a normal subgroup H of G of index p. Let $W = V^H$ be the maximal subspace on which H acts trivially. By induction $W \neq 0$. We claim that W is a G-invariant subspace. Indeed, for any $g \in G$, the group $H = gHg^{-1}$ acts trivially on gW, so $gW \subset W$. Since G acts on W and H acts trivially, the action factors through G/H, which has order p. By the Base Case, there is $0 \neq v \in V$ such that every element of G/H acts trivially on v and thus G acts trivially on v.
b) This follows immediately from part a). $\qquad\square$

2.6. **Notes.**

The treatment of semisimple modules and rings from §2.1 is partially taken from my commutative algebra notes, but here I have taken a slightly more elementary approach (formerly the proof invoked Baer's Criterion at a critical juncture; this is not necessary!). The treatment of this section as well as §2.2 through §2.4 follows [L-FC, §3] quite closely. §2.5 on the radical follows [AB, §13] and §2.6 on Maschke's Theorem follows [AB, §12]. (To be historically accurate: Maschke in [Ma99] proves the implication (i) $\implies$ (ii) of Theorem 2.20 only. This is the less trivial direction; we have added the converse implication for perspective.) The text of Alperin and

Bell was used in a course I took as an undergraduate at the University of Chicago, taught by J.L. Alperin. I found it to be a thoroughly reliable guide then and I still do now. The exercises are especially well thought out and lead the reader deftly through several additional results.

3. RADICALS

3.1. Radical of a module.

Let M be a left R-module. We define $\mathcal{S}(M)$ to be the set of left R-submodules N of M such that M/N is a simple R-module.

Example: Let $R = k$. Then $\mathcal{S}(M)$ is the family of codimension one subspaces in the k-vector space M.

Example: Let $R = \mathbb{Z}$ and let M be any divisible abelian group, e.g. $\mathbb{Q}/\mathbb{Z}$. Then every quotient of M is divisible, whereas the simple $\mathbb{Z}$-modules $\mathbb{Z}/p\mathbb{Z}$ are all finite. Therefore $\mathcal{S}(M) = \varnothing$.

We define the **radical of M**

$$\operatorname{rad} M = \bigcap_{N \in \mathcal{S}(M)} N.$$

As above, we may have $\mathcal{S}(M) = \varnothing$: in this case, our (reasonable) convention is that an empty intersection over submodules of M is equal to M itself.

Exercise 3.1: Let M be a left R-module.
a) Show that $\operatorname{rad} M$ is an R-submodule of M.
b) Show that $\operatorname{rad}(M/\operatorname{rad} M) = 0$.

Proposition 3.1. *If M is a semisimple R-module then $\operatorname{rad} M = 0$.*

Proof. Write $M = \bigoplus_{i \in I} S_i$ as a direct sum of simple modules. For each $i \in I$, put $T_i = \bigoplus_{j \neq i} S_i$. Then $M/T_i \cong S_i$ is simple and $\bigcap_{i \in I} T_i = 0$, so $\operatorname{rad} M = 0$. $\square$

Theorem 3.2. *For a left R-module M, TFAE:*
(i) M is finitely generated semisimple (i.e., a finite direct sum of simple modules).
(ii) M is Artinian and $\operatorname{rad} M = 0$.

Proof. (i) $\implies$ (ii) is immediate from Propositions 2.4 and 3.1.
(ii) $\implies$ (i): Let $\{N_i\}_{i \in I}$ be a family of submodules of M such that M/N_i is simple and $\bigcap_{i \in I} N_i = 0$. Since M is Artinian, the family of all intersections of finitely many elements of I has a minimal element which, since the infinite intersection is 0, clearly must be zero: that is, there are $i_1, \ldots, i_k$ such that $N_{i_1} \cap \ldots \cap N_{i_k} = 0$. Then we get an embedding

$$M \to \bigoplus_{j=1}^{k} M/N_{i_j}$$

which shows that M is a submodule of a finitely generated semisimple (hence Noetherian) module and thus is itself finitely generated semisimple. $\square$

Lemma 3.3. *Let $f : M_1 \to M_2$ be an R-module map. Then $\varphi(\operatorname{rad} M_1) \subset \operatorname{rad} M_2$.*

Proof. For any submodule N of M_2, φ induces an injection $M_1/\varphi^{-1}(N) \hookrightarrow M_2/N$. So if M_2/N is simple, then either $\varphi^{-1}(N) = M_1$ or $M_1/\varphi^{-1}(N) \cong M_2/N$ is simple. Either way we have $M_1/\varphi^{-1}(N) \supset \operatorname{rad} M_1$. Thus $\varphi^{-1}(\operatorname{rad} M_2) \subset \operatorname{rad} M_1$. $\qquad\square$

Let R be a ring. We write $\operatorname{rad}_l(R)$ for the radical of R viewed as a left R-module and $\operatorname{rad}_r(R)$ for the radical of R viewed as a right R-module.

Corollary 3.4. *For a left R-module M we have*

$$\operatorname{rad}_l(R)M \subset \operatorname{rad} M.$$

Proof. Fix $m \in M$. Then the map $x \in R \mapsto xm \in M$ gives an R-module map from R to M, and the result now follows from Lemma 3.3. $\qquad\square$

Lemma 3.5. *Let M be a left R-module. We define the **annihilator of M** as*

$$\operatorname{ann}(M) = \{x \in R \mid xm = 0 \forall m \in M\}.$$

a) The annihilator $\operatorname{ann}(M)$ is an ideal of R.
b) If $\{M_i\}_{i\in I}$ is a family of left R-modules, then

$$\operatorname{ann}(\bigoplus_{i\in I} M_i) = \bigcap_{i\in I} \operatorname{ann}(M_i).$$

*We say that $\bigcap_{i\in I} \operatorname{ann}(M_i)$ is the **common annihilator** of the modules M_i.*

Exercise 3.2: Prove Lemma 3.5.

Proposition 3.6. *a) For $x \in R$, TFAE:*
(i) For every semisimple left R-module M, $xM = 0$.
(ii) For every simple left R-module m, $xM = 0$.
(iii) $x \in \operatorname{rad}_l R$.
That is, $\operatorname{rad}_l R$ is the common annihilator of all simple R-modules.
b) For any nonzero ring R, $\operatorname{rad}_l R$ is an ideal of R.

Proof. a) (i) $\iff$ (ii): First note for $x \in R$ and an R-module M, $xM = 0 \iff x \in \operatorname{ann} M$. For any family $\{M_i\}_{i\in I}$ of R-modules,

$$\operatorname{ann} \bigoplus_i M_i = \bigcap_{i\in I} \operatorname{ann} M_i.$$

Thus any x which annihilates every simple module also annihilates every semisimple module, and the converse is obvious.
(ii) $\implies$ (iii): Suppose x kills every simple left R-module, and let I be a maximal left ideal of R. Then R/I is simple so $x(R/I) = 0$, i.e., $x \in I$.
(iii) $\implies$ (ii): Every simple left R-module M is monogenic and thus isomorphic to R/I for some maximal left ideal of R. So if $x \in \operatorname{rad}_l R$, $x \in I$ hence $x(R/I) = 0$.
b) Let $\{S_i\}_{i\in I}$ be a set of representatives for the simple left R-modules, i.e., such that every simple left R-module is isomorphic to a unique S_i. (Since every simple R-module is a quotient of R, $\#I \leq 2^{\#R}$; in particular I is a set!) By part a), $\operatorname{rad}_l R = \operatorname{ann} \bigoplus_{i\in I} S_i$, hence by Lemma 3.5 $\operatorname{rad}_l R$ is an ideal of R. If R is a nonzero ring it has a maximal ideal and hence a simple module, which $1 \in R$ does not annihilate. Therefore $\operatorname{rad}_l R$ is a proper ideal of R. $\qquad\square$

Exercise 3.3: Let M be a left R-module of finite length r. Show: $(\operatorname{rad}_l R)^r M = 0$.

Of course the results of this section apply equally well to $\mathrm{rad}_r(R)$. In particular $\mathrm{rad}_r R$ is also a two-sided ideal of R. Our next major goal is to show

$$\mathrm{rad}_l(R) = \mathrm{rad}_r(R),$$

after which we will write simply $\mathrm{rad}\, R$ and call it the **Jacobson radical** of R. The next section develops some machinery for this.

3.2. Nakayama's Lemma.

Lemma 3.7. *For an element x of a left R-module M, TFAE:*
(i) $x \in \mathrm{rad}\, M$.
(ii) If N is a submodule of M such that $Rx + N = M$, then $N = M$.

Proof. $\neg$ (i) $\implies$ $\neg$ (ii): Suppose that $x \notin \mathrm{rad}\, M$, so there is a submodule $N \subset M$ with M/N semisimple and $x \notin N$. In this case $Rx + N = M$ and $N \subsetneq M$.
$\neg$ (ii) $\implies$ $\neg$ (i): Suppose that $N \subsetneq M$ is such that $Rx + N = M$. Note that this implies $x \notin N$. By Zorn's Lemma there exists such a submodule N which is maximal with respect to the property $x \notin N$, so without loss of generality we may assume N has this property. It follows that N is in fact a maximal left R-submodule of N, because any strictly larger submodule would contain N and x and thus M. Therefore M/N is simple, $\mathrm{rad}\, M \subset N$ and $x \notin \mathrm{rad}\, M$. $\qquad\square$

Theorem 3.8. *(Nakayama's Lemma For Modules)*
Let P be a submodule of the left R-module M.
a) Suppose that for all submodules N of M, if $P + N = M \implies N = M$. Then $P \subset \mathrm{rad}\, M$.
b) Conversely, suppose P that either P or M is a finitely generated and $P \subset \mathrm{rad}\, M$. Then for all submodules N of M, $P + N = M \implies N = M$.

Proof. a) Seeking a contradiction, we suppose that there exists $x \in P \setminus \mathrm{rad}\, M$. By Lemma 3.7 there exists a proper submodule N of M such that $M = Rx + N \subset P + N$. Thus $P + N = M$ and $N = M$, contradiction.
b) Suppose that N is a submodule of M such that $P + N = M$. If M is finitely generated, then there exists some finitely generated submodule Q of P such that $Q + N = M$. Thus either way we may assume that P is finitely generated as a left R-module, say by $x_1, \ldots, x_n$. We may now apply Lemma 3.7 to the submodule $Rx_2 + \ldots + Rx_n + N$ to get $Rx_2 + \ldots + Rx_n + N = M$. Next we apply Lemma 3.7 to $Rx_3 + \ldots + Rx_n + N$ to get $Rx_3 + \ldots + Rx_n + N = M$. Continuing in this way, we eventually get that $N = M$. $\qquad\square$

The following theorem is due to Azumaya[8] [Az51] and Nakayama[9] [Na51]. (See the notes at the end of this section for further commentary.)

Theorem 3.9. *(Nakayama's Lemma For Rings)*
For a left ideal P of a ring R, TFAE:
(i) $P \subset \mathrm{rad}_l R$.
(ii) If M is a finitely generated left R-module, and N is a submodule of M such that $N + PM = M$, then $N = M$.
(iiii) $1 + P \subset R^\times$.

---

[8]Goro Azumaya, 1920-2010
[9]Tadasi Nakayama, 1912-1964

Proof. (i) $\implies$ (ii): By Corollary 3.4, $(\mathrm{rad}_l R)M \subset \mathrm{rad}\, M$. The implication now follows immediately from Lemma 3.8.

(ii) $\implies$ (iii): Put $G = 1+P$. Let $x \in P$ and put $y = 1+x$. Then $1 = y-x \in Ry+P$, so $Ry + PR = R$. Since R is a finitely generated left R-module, by our assumption it follows that $Ry = R$, i.e., there exists $z \in R$ such that $1 = zy = z + zx$, so $z = 1 + (-z)x \in G$. We have shown that every element of G has a right inverse in G which (together with the fact that $1 \in G$) shows that G is a subgroup of $(R, \cdot)$ and thus is contained in $R^{\times}$.

(iii) $\implies$ (i): Suppose $G = 1 + P \subset R^{\times}$. By Lemma 3.7, it is enough to show that for any left ideal N of R such that $Rx + N = R$ we have $N =$. But the hypothesis $Rx + N = R$ implies $1 = zy + y$ for some $z \in R$ and $y \in N$. It follows that $y = 1 + (-z)x$ with $(-z)x \in P$, and thus $y \in R^{\times} \cap N$ and $N = R$. $\qquad\square$

Corollary 3.10. *Let M be a finitely generated left R-module such that $(\mathrm{rad}_l R)M = M$. Then $M = 0$.*

Proof. Apply Theorem 3.9 with $P = \mathrm{rad}_l R$ and $N = 0$. $\qquad\square$

Corollary 3.11. *For any ring R we have an equality of ideals $\mathrm{rad}_l R = \mathrm{rad}_r R$.*

Proof. There is of course a right-handed analogue of Theorem 3.9. In particular, a right ideal P is contained in $\mathrm{rad}_r R$ iff $1 + P \subset R^{\times}$. But this latter condition is ambidextrous! So let P be $\mathrm{rad}_r R$ viewed as a left ideal (by Proposition 3.6, it is a two-sided ideal, so this is permissible): since $1 + \mathrm{rad}_r R \subset R^{\times}$ we deduce $\mathrm{rad}_r R \subset \mathrm{rad}_l R$. Similarly, we deduce $\mathrm{rad}_l R \subset \mathrm{rad}_r R$ and thus $\mathrm{rad}_l R = \mathrm{rad}_r R$. $\qquad\square$

The ideal $\mathrm{rad}_l R = \mathrm{rad}_r R$ will simply be denoted $\mathrm{rad}\, R$ and called the **Jacobson radical** of R. To rephrase things in ideal-theoretic language, Corollary 3.11 shows that in any ring R, the intersection of all maximal left ideals is equal to the intersection of all maximal right ideals, a beautiful, unexpected and useful ambidexterity!

Corollary 3.12. *The Jaocobson radical $\mathrm{rad}\, R$ of a ring is equal to all of the following:*
(i) The intersection of all maximal left ideals of R.
(ii) The intersection of all maximal right ideals of R.
(iii) The set of all $x \in R$ such that $1 + Rx \subset R^{\times}$.
(iv) The set of all $x \in R$ such that $1 + xR \subset R^{\times}$.

Exercise 3.4: Prove Corollary 3.12.

Corollary 3.13. *An Artinian ring R is semisimple iff $\mathrm{rad}\, R = 0$.*

Exercise 3.5: Prove Corollary 3.13.

Exercise 3.6: Let $f : R \to S$ be a surjective ring map. Show that $f(\mathrm{rad}\, R) \subset \mathrm{rad}\, S$.

Exercise 3.7: Show that $\mathrm{rad}(R_1 \times \ldots R_n) = \mathrm{rad}\, R_1 \times \ldots \times \mathrm{rad}\, R_n$.

3.3. **Nilpotents and the radical.**

Recall that an element $x \in R$ is **nilpotent** if $x^n = 0$ for some $n \in \mathbb{Z}^+$. A left, right or two-sided ideal I of R is called **nil** if every element is a nilpotent. A two-sided ideal I is **nilpotent** if $I^n = 0$ for some $n \in \mathbb{Z}^+$.

Warning: In a commutative ring, the ideal generated by a set of nilpotent elements consists entirely of nilpotent elements, i.e., is a nil ideal. This need not hold in a noncommutative ring!

Exercise 3.8: Give an example of a ring R and a nilpotent element $x \in R$ such that neither Rx nor xR is a nil ideal.

Proposition 3.14. *Let I be a (left, right or two-sided) nil ideal. Then $I \subset \operatorname{rad} R$.*

Proof. It is enough to treat the case of a left ideal. For note that for any $x \in R$, if $x^n = 0$ then

$$(1+x)(\sum_{i=0}^{n-1}(-x)^i) = (\sum_{i=0}^{n-1}(-x)^i)(1+x) = 1,$$

so $1 + x \in R^\times$. Since this hold for all $x \in R$, we have $1 + I = 1 + RI \subset R^\times$. Applying Corollary 3.12, we conclude $I \subset \operatorname{rad} R$. $\square$

Theorem 3.15. *Let R be a left Artinian ring.*
a) The Jacobson radical $\operatorname{rad} R$ is nilpotent.
b) For a left ideal I of R, TFAE:
(i) I is nilpotent.
(ii) I is nil.
(iii) $I \subset \operatorname{rad} R$.

Proof. a) Step 1: The sequence $\operatorname{rad} A \supset (\operatorname{rad} A)^2 \supset \ldots$ is a descending chain of left ideals, so in the Artinian ring R there must exist $k \in \mathbb{Z}^+$ such that $(\operatorname{rad} A)^k = (\operatorname{rad} A)^{k+1}$.
Step 2: We assume that $(\operatorname{rad} A)^k \neq 0$ and derive a contradiction. Indeed the set of nonzero left ideals I of R such that $(\operatorname{rad} R)I = I$ then includes $(\operatorname{rad} R)^k$. By the Artinian condition, there is a minimal such ideal I. Since $I = (\operatorname{rad} R)I = (\operatorname{rad} R)^2 I = \ldots = (\operatorname{rad} R)^k I$, there exists $x \in I$ such that $(\operatorname{rad} R)^k x \neq 0$. Then $J = (\operatorname{rad} A)^k x$ is a left ideal contained in I and satisfying $(\operatorname{rad} R)J = J$, so by minimality we have $I = (\operatorname{rad} A)^k x \subset Rx \subset I$. Therefore $I = Rx$ is a finitely generated left R-module such that $(\operatorname{rad} R)I = I \neq 0$, contradicting Nakayama's Lemma (specifically, Corollary 3.10).
b) (i) $\implies$ (ii) is immediate and (ii) $\implies$ (iii) is Proposition 3.14. (In fact each of these implications hold in any ring.)
(iii) $\implies$ (i): By part a), since R is left Artinian $\operatorname{rad} R$ is nilpotent, and in any ring an ideal contained in a nilpotent ideal is nilpotent. $\square$

Exercise 3.9: This exercise sketches an alternate proof of the semisimplicity of $k[G]$ for G finite such that $N = \#G \in k^\times$ (i.e., the greater part of Maschke's Theorem).
a) Show that if $k[G]$ is not semisimple, there exists $0 \neq a \in k[G]$ such that for every element $x \in k[G]$, ax is nilpotent.
b) For $x \in G$, define $T(x)$ to be the trace of $x\bullet$ viewed as a k-linear map on $k[G]$. Show that

$$T(\sum_{g \in G} x_g[g]) = Nx_g \in k.$$

c) Show that if $x \in k[G]$ is nilpotent, then $T(x) = 0$.
d) Using the previous parts, show that $k[G]$ is semisimple.

3.4. **The Brown-McCoy radical.**

For any ring R, we define the **Brown-McCoy radical** $\mathfrak{r}R$ to be the intersection of all maximal (two-sided!) ideals of R.

Lemma 3.16. *For any ring R,* $\operatorname{rad} R \subset \mathfrak{r}R$.

Proof. Let $x \in \operatorname{rad} R$, and let $\mathfrak{m}$ be a maximal ideal of R. Seeking a contradiction, suppose $x \in R \setminus \mathfrak{m}$: then $(x) + \mathfrak{m} = R$, i.e., there exist $a, b \in R$ and $m \in \mathfrak{m}$ such that $m = 1 + axb$. Since $\operatorname{rad} R$ is an ideal, $x \in \operatorname{rad} R$ implies $x' = xb \in \operatorname{rad} R$ and then $1 + ax' \in \mathfrak{m}$ implies $1 + Rx'$ is not contained in $R^{\times}$, contradicting Corollary 3.12. So x lies in every maximal ideal of R and thus in the Brown-McCoy radical $\mathfrak{r}R$. $\square$

Theorem 3.17. *In a left Artinian ring R,* $\operatorname{rad} R = \mathfrak{r}R$.

Proof. For any ring R, by Lemma 3.16 we have $\operatorname{rad} R \subset \mathfrak{r}R$. So it suffices to show the reverse inclusion. To see this, put $\overline{R} = R/\operatorname{rad} R$. Then $\overline{R}$ is a finite product of simple rings, so $\mathfrak{r}\overline{R} = 0$. By correspondence, this gives us that the intersection of all maximal ideals of R containing $\operatorname{rad} R$ is equal to $\operatorname{rad} R$ and thus $\mathfrak{r}R \subset \operatorname{rad} R$. $\square$

3.5. **Theorems of Wedderburn and Kolchin.**

Theorem 3.18. *(Wedderburn's Nilpotence Theorem [We37]) Let A be a ring which is finite-dimensional as a k-algebra, and let B be a k-subspace which is closed under multiplication. Suppose that B is spanned as a k-vector space by nilpotent elements. Then B is a nilpotent algebra: there exists $N \in \mathbb{Z}^{+}$ such that $B^{N} = (0)$.*

Proof. Let $u_1, \ldots, u_n$ be a k-spanning set of B consisting of nilpotent elements. Let C be the k-subspace generated by 1 and B, so that C is subring of A. We claim that B is contained in every maximal ideal $\mathfrak{m}$ of C, for then by Theorem 3.17 $B \subset \operatorname{rad} C$ and by Theorem 3.15 $C^{N} = (0)$ for some N.

So let $\mathfrak{m}$ be a maximal ideal of C and, seeking a contradiction, suppose that $\mathfrak{m}$ does not contain B. Since B is a codimension one subspace in C, we must therefore have $\mathfrak{m} + B = C$, so $\overline{C} = C/\mathfrak{m} \cong B/(B \cap \mathfrak{m})$. Thus the simple algebra $\overline{C}$ is spanned over k by the nilpotent elements $\overline{u}_1, \ldots, \overline{u}_n$. Let l be the center of $\overline{C}$, so that by Proposition 1.21 l is a field extension of k. By Wedderburn's (other) Theorem, $\overline{C}$ is isomorphic as an l-algebra to $M_m(D)$, where D is a division algebra with center l. Let $\overline{l}$ be an algebraic closure of l. We need to assume a result which will be proved later on in these notes (Proposition 4.2): if R is a finite dimensional simple l-algebra with center l and m/l is any field extension, then the base extension $R_m = R \otimes_l m$ is a simple m-algebra. Applying this to the l-algebra $\overline{C}$ with $m = \overline{l}$, we find that $\overline{C}_{\overline{l}} = \overline{C} \otimes_l \overline{l}$ is a finite dimensional simple algebra over an algebraically closed field and thus is isomorphic to $M_n(\overline{l})$. Once again the elements $\overline{u}_i \otimes 1$ are nilpotent and span $\overline{C}_{\overline{l}}$ over $\overline{l}$. But for any field K and any $n \in \mathbb{Z}^{+}$, the matrix ring $M_n(K)$ cannot be spanned by nilpotent matrices: indeed, any nilpotent matrix has trace zero and therefore the trace, being a K-linear map from $M_n(K) \to K$, would be the zero map. But it is not, of course: the trace of the matrix unit E_{11} is equal to 1. $\square$

Theorem 3.19. *(Kolchin) Let k be a field, and let $M \subset \operatorname{GL}_n(k)$ be a submonoid conisting entirely of unipotent matrices – i.e., for all $m \in M$, every eigenvalue of m is 1. Then M is conjugate to a submonoid of the standard unipotent group T_n.*

Proof. (Herstein [He86]) Note that a matrix g is unipotent iff $1 - g$ is nilpotent (has every eigenvalue 0). Let $S \subset M_n(k)$ be the k-subspace generated by all elements $1 - g$ for $g \in S$. For any $g, h \in M$ we have

$$(1 - g)(1 - h) = (1 - g) + (1 - h) - (1 - gh),$$

so the k-subspace S is closed under multiplication. Moreover, a matrix $g \in M_n(k)$ is unipotent iff $1 - g$ is nilpotent, so S satisfies the hypotheses of Theorem 3.18 and is therefore a nilpotent algebra: there exists $N \in \mathbb{Z}^+$ such that $S^N = (0)$. We may assume that $S \neq (0)$ – this occurs iff $M = \{1\}$, a trivial case – and then there exists $N \in \mathbb{Z}^+$ such that $S^{N-1} \neq 0$ and $S^N = (0)$. Choose $u \in S^{N-1} \setminus (0)$: then for all $g \in M$ we have $u(1 - g) \in S^N$ so $u(1 - g) = 0$. That is, for all $g \in M$, $gu = u$: every element of M fixes the nonzero vector u. Let $V_1 = k^n$ and choose a basis $e_1, \dots, e_n$ for k^n with first element u: with respect to this new basis, the matrix g is of the form

$$\begin{bmatrix} 1 & * \\ 0 & g' \end{bmatrix}, * \in k, \ g' \in GL_{n-1}(k).$$

If we let V_2 be the vector space spanned by $e_2, \dots, e_n$, then $g' \in \mathrm{GL}(V_2)$ is a unipotent matrix, and we are done by induction. $\qquad \square$

Exercise 3.10: Show that Theorem 2.22 follows immediately from Kolchin's Theorem.

3.6. **Akizuki-Levitzki-Hopkins.**

Theorem 3.20. *Let R be a left Artinian ring.*
a) Every Artinian left R-module is Noetherian.
b) In particular R itself is left Noetherian.

Proof. Let us write J for the Jacobson radical $\operatorname{rad} R$ of R. Since R is Artinian, by Theorem 3.15 there exists $k \in \mathbb{Z}^+$ with $J^k = 0$. Let M be an Artinian left R-module; by the above, there exists a *least* $n \in \mathbb{Z}^+$ such that $J^n M = 0$. We go by induction on this n. Note that $n = 0 \iff M = 0$: this is a trivial case.
Base Case ($n = 1$): Suppose $JM = 0$. Then M may be considered as a module over the semisimple ring R/J. It is therefore a semsimple module, so by Proposition 2.4 being Artinian it is also Noetherian.
Induction Step: let $n > 1$ and assume that any Artinian module N with $J^{n-1}N = 0$ is Noetherian. Let M be an Artinian module with $J^n M = 0$, so by induction JM is Noetherian. Therefore M fits into a short exact sequence

$$0 \to JM \to M \to M/JM \to 0.$$

Now M/JM is a quotient of the Artinian module M so is Artinian. But as above it is a module over the semisimple ring R/J, so it is semisimple and thus Noetherian. Therefore M is an extension of one Noetherian module by another so is Noetherian. $\qquad \square$

Corollary 3.21. *For a left module M over a left Artinian ring, TFAE:*
(i) M is Artinian.
(ii) M is Noetherian.
(iii) M is finitely generated.

Exercise 3.11: Prove Corollary 3.21.

3.7. **Functoriality of the Jacobson radical.**

Let R be a semisimple k-algebra. As for any k-algebra, it is natural and useful to *extend the base* and see what happens. Namely, let l/k be a field extension and consider the l-algebra $R_l = R \otimes_k l$.

Exercise 3.12: Let I be a left (resp. right, two-sided) ideal of R.
a) Show that $I_l = I \otimes_k l$ is a left (resp. right, two-sided) ideal of R_l.
b) Show that $I \subset J \iff I_l \subset J_l$ and $I \subsetneq J \iff I_l \subsetneq J_l$. (Hint: this holds even for vector spaces.)
c) Show that if R_l is Noetherian (resp. Artinian), then R is Noetherian (resp. Artinian). Does the converse hold?

Exercise 3.13: Let I be a nil ideal of R.
a) Show that if I is nilpotent than I_l is nilpotent.
b) If $[R : k]$ is finite, show that I_l is nil.
c) Must I_l be nil in general?

In this section we explore the relationship between the semisimplicity of R and the semisimplicity of R_l.

Exercise 3.14:
a) Suppose $[R : k]$ is finite. Show that if R_l is semisimple, then R is semisimple.
b) Show that the conclusion of part b) still holds if instead of assuming $[R : k]$ is finite we assume that R_l is Artinian. Is it enough to assume that R is Artinian?

To a certain extent, it helps to study a more general problem: let $\iota : R \hookrightarrow S$ be an inclusion of rings. Then what is the relationship between $R \cap \operatorname{rad} S$ and $\operatorname{rad} R$? The next two results are in this context, but we quickly return to the case of scalar extension of k-algebras.

Proposition 3.22. *Let $R \subset S$ be an inclusion of rings. Suppose that either*
(i) As left R-modules, R is a direct summand of S, or
(ii) There exists a group G of ring automorphisms of S such that

$$R = S^G = \{x \in S \mid gx = x \ \forall g \in G\}.$$

Then $R \cap \operatorname{rad} S \subset \operatorname{rad} R$.

Proof. Assume (i), and write $S = R \oplus T$ as left R-modules. It suffices to show that for $x \in R \cap \operatorname{rad} S$, $1 - x \in R^\times$. Since $x \in \operatorname{rad} S$, $1 - x \in S^\times$, so there exist $y \in R, t \in T$ such that

$$1 = (1 - x)(y + t) = (1 - x)y + (1 - x)t.$$

Therefore we have $1 - (1 - x)y = (1 - x)t$ with $1 - (1 - x)y \in R$ and $(1 - x)t \in T$. Since $R \cap T = 0$, we conclude $1 = (1 - x)y$ and $1 - x \in R^\times$.
Assume (ii). As above, let $x \in R \cap \operatorname{rad} S$, so that there exists $s \in S$ such that $1 = (1 - x)s$. Therefore for any $\sigma \in G$, $1 = (1 - x)\sigma(s)$, and by the uniqueness of inverses we conclude that $s \in S^G = R$. $\qquad\square$

Proposition 3.23. *Let $\iota : R \to S$ be a ring homomorphism. Suppose that there exists a finite set $x_1, \ldots, x_n$ of left R-module generators of S such that each x_i lies in the commutant $C_S(\iota(R))$. Then $\iota(\operatorname{rad} R) \subset \operatorname{rad} S$.*

Proof. Put $J = \operatorname{rad} R$. To show $\iota(J) \subset \operatorname{rad} S$, it suffices to show that J annihilates every simple left R-module M. We may write $M = Sa$. Then

$$M = (Rx_1 + \ldots + Rx_n)a = Rx_1 a + \ldots + Rx_n a,$$

so M is finitely generated as a left R-module. Observe that JM is an S-submodule of M since

$$\forall 1 \le i \le n, \ x_j(JM) = (x_j J)M = (J x_j)M \subset JM.$$

Viewing M as a nonzero R-module and applying Nakayama's Lemma, we get $JM \subsetneq M$, and since JM is an S-submodule of the simple S-module M we must have $JM = 0$. $\qquad\square$

Theorem 3.24. *Let R be a k-algebra and l/k a field extension.*
a) We have $R \cap (\operatorname{rad} R_l) \subset \operatorname{rad} R$.
b) If l/k is algebraic or $[R : k] < \infty$, then

(7) $$R \cap (\operatorname{rad} R_l) = \operatorname{rad} R.$$

c) If $[l : k] = n < \infty$, then

$$(\operatorname{rad} R_l)^n \subset (\operatorname{rad} R)_l.$$

Proof. a) Let $\{e_i\}_{i \in I}$ be a k-basis for l with $e_{i_0} = 1$, say. Then

$$R_l = R \oplus \bigoplus_{i \neq i_0} Re_i$$

is a direct sum decomposition of R_l as a left R-module. Therefore condition (i) of Proposition 3.22 is satisfied, so the conclusion applies: $\operatorname{rad} R_l \cap R \subset \operatorname{rad} R$.
b) If $[R : k]$ is finite, then $\operatorname{rad} R$ is nilpotent, hence so is $(\operatorname{rad} R)_l$. It follows that $(\operatorname{rad} R)_l \subset \operatorname{rad} R_l$, so $\operatorname{rad} R \subset R \cap \operatorname{rad} R_l$. In view of part a), this gives the desired equality (7). Next assume that $[l : k]$ is finite. Then $\{e_1, \ldots, e_n\}$ is a spanning set for R_l as an R-module such that each e_i commutes with every element of R, so by Proposition 3.23 we get $R \cap \operatorname{rad} R_l \subset \operatorname{rad} R$, and again by part a) we conclude $R \cap \operatorname{rad} R_l = \operatorname{rad} R$. If l/k is any algebraic extension, then any (using part a)) any element of $\operatorname{rad} R_l$ lies in $\operatorname{rad} R_{l'}$ for some finite subextension l' of l/k, so the conclusion for any algebraic extension l/k follows immediately.
c) Let V be a simple right R-module. Then V_l is a right R_l-module which, as an R-module, is isomorphic to $\bigoplus_{i=1}^{n} V \otimes e_i$ and thus has length n. It follows that as a right R_l-module V_l has length at most n. Therefore for any $z \in (\operatorname{rad} R_l)^n$, $V_l z = 0$. Writing $z = \sum_i r_i \otimes e_i$ with $r_i \in R$, for any $v \in V$ we have

$$0 = (v \otimes 1)(\sum_i r_i \otimes e_i) = \sum_i v r_i \otimes e_i \implies v r_i = 0 \forall 1 \le i \le n.$$

So $V r_i = 0$ for all i, hence $r_i \in \operatorname{rad} R$ for all i and $z = \sum_i r_i \otimes e_i \in (\operatorname{rad} R)_l$. $\qquad\square$

Theorem 3.25. *Let R be a k-algebra and l/k a separable algebraic extension. Then*

$$\operatorname{rad} R_l = (\operatorname{rad} R)_l.$$

Proof. Step 1: We prove that $\operatorname{rad} R = 0 \implies \operatorname{rad} R_l = 0$.

Proof: As in the proof of Theorem 3.24 it is enough to assume that $[l : k]$ is finite. Let m be the normal closure of l/k, so m/k is a finite Galois extension, and put $G = \operatorname{Aut}(m/k)$. Applying Theorem 3.24 to the extension m/l, we get $\operatorname{rad} R_l \subset \operatorname{rad} R_m$, so it's enough to show that $\operatorname{rad} R_m = 0$.

Let $e_1, \ldots, e_n$ be a basis for m/k, and extend the action of G on m to $R_m = R \otimes_k m$ via $\sigma(x \otimes y) = x \otimes \sigma y$. Let $z = \sum_i r_i \otimes e_i \in \operatorname{rad} R_m$. Then for all $\sigma \in G$ and $1 \le j \le n$, we have

$$(8) \qquad \sigma(z e_j) = \sigma(\sum_i r_i \otimes e_i e_j) = \sum_i r_i \otimes \sigma(e_i e_j).$$

It is clear from the definition of the radical that it is invariant under all ring automorphisms; therefore $z \in \operatorname{rad} R_m \implies \sigma(z) \in \operatorname{rad} R_m$ and thus also $\sigma(z e_j) = \sigma(z)\sigma(e_j) \in \operatorname{rad} R_m$ since $\operatorname{rad} R_m$ is an ideal. Summing (8) over all $\sigma \in G$, we get

$$\sum_i r_i \otimes \sum_{\sigma \in G} \sigma(e_i e_j) = \sum_i \otimes \operatorname{Tr}_{m/k}(e_i e_j)$$

$$= \sum_i r_i \operatorname{Tr}_{m/k}(e_i e_j) \otimes 1 \in R \cap \operatorname{rad} R_m \subset \operatorname{rad} R = 0.$$

therefore $\sum_i r_i \operatorname{Tr}_{m/k}(e_i e_j) = 0$ for all j. Since m/k is separable, the trace form is nondegenerate and thus $r_i = 0$ for all i, so $z = 0$.

. Step 2: By Theorem 3.24 we have $(\operatorname{rad} R)_l \subset (\operatorname{rad} R_l)$. Moreover, $R_l/(\operatorname{rad} R)_l \cong (R/\operatorname{rad} R)_l$ (this is true for all k-subspaces of R_l). By Step 1, since $\operatorname{rad}(R/\operatorname{rad} R) = 0$, $\operatorname{rad}(R/\operatorname{rad} R)_l = 0$ and thus $\operatorname{rad}(R_l/(\operatorname{rad} R)_l) = 0$, i.e., $\operatorname{rad} R_l = (\operatorname{rad} R)_l$. $\qquad\square$

For later use, we single out the following special case.

Corollary 3.26. *Let $R_{/k}$ be a finite-dimensional semisimple k-algebra and l/k a separable algebraic field extension. Then R_l is a semisimple l-algebra.*

What about inseparable algebraic field extensions? Here are some examples.

Exercise 3.15: For any field extension l/k, show that $M_n(k) \otimes l \cong M_n(l)$. In particular, matrix algebras remain semsimple (indeed simple) upon arbitrary scalar extension.

Exercise 3.16: Let l/k be an inseparable algebraic field extension. Let m be the normal closure of l/k. Show that $l_m = l \otimes_k m$ is not semisimple.

Exercise 3.17: Let D be a finite-dimensional division k-algebra with center l, an inseparable algebraic extension of k. Show that D_l is not semisimple. (Hint: show that D_l contains a nonzero nilpotent ideal.)

3.8. **Notes.**

"The" radical was first studied in finite dimensional algebras by Wedderburn. A very efficient, readable treatment of the radical in this special case is given in [AB]. The reader who is more interested in getting quickly to central simple algebras might do well do skip the details of our treatment and consult their text instead. In retrospect, what Wedderburn developed was a good theory of the radical for

Artinian rings. The extension of the radical to all rings was done by Jacobson[10], who was a student of Wedderburn at Princeton University.

The Jacobson radical is now embedded so seamlessly into the larger theory of (both commutative and non-commutative) rings that it seems surprising that it emerged relatively late: the fundamental paper on the subject is [Ja45]. With the benefit of hindsight one can see the Jacobson radical of a ring as a close analogue of the **Frattini subgroup** $\Phi(G)$ of a group G, i.e., the intersection of all maximal subgroups of G. The fact that for finite G, $\Phi(G)$ is a nilpotent group seems in spirit quite close to the fact that the radical of an Artinian (e.g. finite!) ring is a nilpotent ideal (Theorem 3.15). Frattini's work was however done in 1885!

The Brown-McCoy radical of a ring first appears in [BM47] and [BM48] and has been the object of much further study (including in non-unital rings, non-associative algebras...). In fact many other types of radicals have been defined: see e.g. [Sz81].

"Nakayama's Lemma" is a name which is freely given to any member of a family of related results.[11] See [CA, §3.8] for some other formulations of Nakayama's Lemma in commutative algebra. With regard to the history: it seems that Nakayama's Lemma for Rings (Theorem 3.9) was independently proved by Azumaya [Az51] and Nakayama [Na51]. In his text on commutative algebra [M], Matsumura makes the following "Remark. This theorem [what is essentially Theorem 3.9 in the commutative case] is usually referred to as Nakayama's Lemma, but the late Professor Nakayama maintained that it should be referred to as a theorem of Krull and Azumaya; it is in fact difficult to determine which of the three first had the result in the case of commutative rings, so we refer to it as NAK in this book." Nevertheless the most common practice seems to be to refer to such results – equally for commutative rings or arbitrary rings – as Nakayama's Lemma.

The 1937 theorem of Wedderburn discussed in §3.5 is apparently not very well known: for instance on MathSciNet it is cited only twice. It is in spirit very close to an 1890 theorem of Friedrich Engel: a finite dimensional Lie algebra L is nilpotent as an algebra iff it is "ad-nilpotent": for all $x \in L$, the operator $\mathrm{ad}(x) : L \to L, y \mapsto [x, y]$ is nilpotent. (Note though that in Engel's theorem the ad-nilpotence holdsfor *every* element of L, not merely a spanning set of elements.) As above, "Kolchin's Theorem" is used for any of several cognate results. A more standard incarnation is the statement that a connected solvable algebraic subgroup of GL_n over an algebraically closed field k leaves invariant (but not necessarily pointwise fixed) a one-dimensional subspace of k. By induction, this shows that every connected solvable subgroup is conjugate to a subgroup of the **standard Borel subgroup** B_n of upper triangular matrices (with arbitrary nonzero entries on the main diagonal). This is a 1948 theorem of Kolchin[12], whose Lie algebra analogue is indeed an 1876 theorem of Lie[13]. Our route to Kolchin's Theorem via Wedderburn's Theorem was first given by Herstein [He86]; it is not the standard one. See for instance [K, Thm. C, p. 100], [L-FC, §9] for other approaches.

---

[10]Nathan Jacobson, 1910-1999

[11]This same useful practice is applied elsewhere in mathematics, e.g. to Hensel's Lemma.

[12]Ellis Robert Kolchin, 1916-1991

[13]Sophus Lie, 1842-1899

Textbook References: A very thorough treatment of the Jacobson radical is the subject of Chapter 2 of [L-FC]. Here we have chosen to follow the more stream-lined presentation of [P, Ch. 4].

4. Central Simple Algebras I: The Brauer Group

4.1. **First properties of CSAs.**

In general we wish to hedge our bets between finite-dimensional and infinite- dimensional k-algebras with the following device: we say that a k-algebra A (which is also an associative ring, as always) is a **CSA** over k if:
(CSA1) $\dim_k A < \infty$,
(CSA2) A is a simple ring, and
(CSA3) $Z(A) = k$.

Thus a central simple k-algebra is a CSA iff it is finite-dimensional over k. We denote the collection of all CSAs over k by CSA_k.

Lemma 4.1. *Let B be a central simple k-algebra and C any k-algebra. The ideals of the k-algebra $B \otimes C$ are precisely those of the form $B \otimes J$ for an ideal J of C.*

Proof. [S-QF, Lemma 19.4] Step 1: For any k-algebras B and C and ideals I_1 of B, I_2 of C, $I_1 \otimes I_2$ is an ideal of $B \otimes C$. This is straightforward and left to the reader. Step 2: Let $\mathcal{J}$ be a nonzero ideal of $B \otimes C$, and put $J = \mathcal{J} \cap C$: then J is an ideal of C and $B \otimes J \subset \mathcal{J}$. We may choose a k-basis $\{x_i\}_{i \in I}$ of C such that there exists $I' \subset I$ with $\{x_i\}_{i \in I'}$ a k-basis of J. Put $I'' = I \setminus I'$. Then

$$B \otimes C = \bigoplus_{i \in I} B \otimes x_i$$

and

$$B \otimes J = \bigoplus_{i \in I'} B \otimes x_i.$$

Seeking a contradiction, we suppose there exists $w \in \mathcal{J} setminus B \otimes J$. Write $w = \sum_{i \in I} b_i \otimes x_i$. By adding to w an element of $B \otimes J$, we may assume that $w = \sum_{i \in I''} b_i \otimes x_i$. Put $I_w = \{i \in I \mid b_i \neq 0\}$; then I_w is finite and nonempty (since $w \notin B \otimes J$). Out of all $w \in \mathcal{J} \setminus B \otimes J$, we may choose one with $\#I_w$ minimal. Fix $i_0 \in I_w$ and put

$$H = \{c_{i_0} \mid \sum_{i \in I_w} c_i \otimes x_i \in \mathcal{J}\},$$

so H is an ideal of B. Moreover $0 \neq b_{i_0} \in H$, so since B is simple, $H = B$. In particular $1 \in H$: there exists $z \in \mathcal{J}$, $z = \sum_{i \in I_w} c_i \otimes x_i$ with $c_{i_0} = 1$. Let $d \in B$. Then $\mathcal{J}$ contains $dz - zd = \sum_{i \in I_w} (dc_i - c_i d) \otimes x_i$. Since the i_0-coefficient of this expression is $d - d = 0$, by minimality of w we must have $dz - zd = 0$ and thus for all $i \in I_w$, $dc_i = c_i d$. Since $d \in B$ was arbitrary, for all $i \in I_w$, $c_i \in ZB = k$ and thus $z \in \mathcal{J} \cap (k \otimes C) = \mathcal{J} \cap C = J$. But since $c_{i_0} = 1$ and $i_0 \notin I'$, this is a contradiction. Therefore $\mathcal{J} = B \otimes J$. $\square$

Exercise 4.1: Explain why Lemma 4.1 is almost a generalization of Theorem 1.22.

Proposition 4.2. *Let B and C be k-algebras.*
a) If $B \otimes C$ is simple, then so are B and C.
b) If B is central simple and C is simple, then $B \otimes C$ is simple.

Proof. a) If B is not simple, there is a k-algebra B' and a non-injective homomorphism $\varphi : B \to B'$. Then $\varphi \otimes 1_C : B \otimes C \to B' \otimes C$ is a non-injective homomorphism to the k-algebra $B' \otimes C$, so $B \otimes C$ is not simple. Similarly for C.
b) This follows immediately from Lemma 4.1. $\square$

Exercise 4.2:
a) Show that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \times \mathbb{C}$.
b) Let l/k be a field extension of (finite) degree $n > 1$. Show that $l \otimes_k l$ is never a simple l-algebra. Show also that it is isomorphic to l^n iff l/k is Galois.
c) Does there exist a nontrivial field extension l/k such that $l \otimes_k l$ is a simple k-algebra?

Proposition 4.3. *Let B and C be k-algebras, and put $A = B \otimes C$. Then:*
a) $C_A(B \otimes k) = Z(B) \otimes C$.
b) $Z(A) = Z(B) \otimes Z(C)$.
c) If l/k is a field extension, then $Z(B)_l = Z(B_l)$.

Proof. a) Since $A = B \otimes C$, $B \otimes k$ and $k \otimes C$ are commuting subalgebras of A and thus $Z(B) \otimes C$ commutes with $B \otimes k$. Conversely, let $\{y_j\}_{j \in J}$ be a k-vector space basis for C. Then every element of A has the form $w = \sum_j x_j \otimes y_j$ for some $x_j \in B$. If $w \in C_A(B \otimes_k)$, then for all $x \in B$,

$$0 = (x \otimes 1)w - w(x \otimes 1) = \sum_{j \in J}(xx_j - x_j x) \otimes y_j,$$

which implies $x_j x = x x_j$ for all j and thus that $x_j \in Z(B)$, so that $w \in Z(B) \otimes C$.
b) Applying part a) with the roles of B and C reversed, we get

$$C_A(k \otimes C) = B \otimes Z(C).$$

Since $A = B \otimes C$, we have

$$Z(A) = C_A(B \otimes k) \cap C_A(k \otimes C) = (Z(B) \otimes C) \cap (B \otimes Z(C)) = Z(B) \otimes Z(C).$$

c) In part b) take $C = l$. Then

$$Z(B_l) = Z(B) \otimes_k Z(l) = Z(B) \otimes_l = Z(B)_l.$$

$\square$

Theorem 4.4. *Let B, C be central simple k-algebras, and let l/k be a field extension.*
a) Then $B \otimes C$ is a central simple k-algebra, and is a CSA iff B and C are CSAs.
b) B_l is a central simple l-algebra and is a CSA over l iff B is a CSA over k.
c) B^{op} is a central simple k-algebra and is a CSA iff B is.
d) If $B \in \mathrm{CSA}_k$ then $B \otimes B^{\mathrm{op}} \cong \mathrm{End}_k(B) \cong M_n(k)$.

Proof. a) By Proposition 4.2 $B \otimes C$ is simple, and by Proposition 4.3 $Z(B \otimes C) = Z(B) \otimes Z(C) = k \otimes_k k = k$. Thus $B \otimes C$ is a central simple k-algebra. Clearly it is finite-dimensional over k iff both B and C are finite-dimensional over k.
b) If B is central simple over k, then by Proposition 4.2 B_l is simple over l and by Proposition 4.3c) B_l is central over l, so B_l is central simple over l. Conversely if B_l is simple then by Proposition 4.2 B is simple and if B_l is l-central then B is

k-central. Evidently $[B : k] = [B_l : l]$, so the result follows. c) This is clear and merely recorded for reference.

d) We define an explicit map $\Phi : B \otimes B^{\mathrm{op}} \to \mathrm{End}_k(B)$, namely, $(x, y) \mapsto (z \mapsto xzy)$. It is immediate to see that it is a k-algebra homomorphism. By parts a) and c), $B \otimes B^{\mathrm{op}} \in \mathrm{CSA}_k$: in particular it is simple, hence injective. Since both source and target are k-vector spaces of finite dimension $(\dim_k B)^2$, Φ must be an isomorphism. $\qquad\square$

4.2. The Brauer group.

One of the many important consequences of Theorem 4.4 is that it shows that the set of isomorphism classes of CSAs over a field k forms a monoid under tensor product. In fact once we pass to isomorphism classes this monoid is commutative, since for all k-algebras $A \otimes B \cong B \otimes A$, the isomorphism being the evident one which switches the order of the factors.

By Wedderburn's theorem every $A \in \mathrm{CSA}_k$ is isomorphic to $M_n(D)$ for a unique $n \in \mathbb{Z}^+$ and a unique (up to isomorphism) division algebra D. One may well ask why we deal with CSAs then and not directly with division algebras. The answer is that both part a) and part b) of Theorem 4.4 fail for division algebras: the base extension of a division algebra is always a CSA but need not be a division algebra. To see this we need only take l to be algebraically closed, since there are no finite dimensional division algebra over an algebraically closed field. Let us now see that part a) fails as well: suppose D/k is a nontrivial k-central division algebra. Choose any $\alpha \in D \setminus k$. Then the k-subalgebra of D generated by α is a proper, finite degree field extension, say l. It follows that inside $D \otimes D$ we have $l \otimes_k l$. This l-algebra either has nontrivial idempotents (if l/k is separable) or nontrivial nilpotents (if l/k is not separable), neither of which can exist inside a division algebra!

The fruitful perspective turns out to be to regard two CSAs as equivalent if they have isomorphic "underlying" division algebras. The following results analyze this relation.

Lemma 4.5. *For any central simple k-algebras A and B and any $m, n \in \mathbb{Z}^+$ we have a canonical isomorphism of algebras*

$$M_m(A) \otimes M_n(B) = M_{mn}(A \otimes B).$$

Exercise 4.3: Prove Lemma 4.5.

Lemma 4.6. *For $A, B \in \mathrm{CSA}_k$, TFAE:*
(i) $A \cong M_{n_1}(D_1)$ and $B \cong M_{n_2}(D_2)$ with $D_1 \cong D_2$.
(ii) There exists a division algebra $D \in \mathrm{CSA}_k$ and $m, n \in \mathbb{Z}^+$ such that $A \cong M_n(D)$ and $B \cong M_m(D)$.
(iii) There exist $r, s \in \mathbb{Z}^+$ such that $A \otimes M_r(k) \cong B \otimes M_s(k)$.

Exercise 4.4: Prove Lemma 4.6.

If A and B satisfy the equivalent conditions of Lemma 4.6 we say A and B are **Brauer equivalent** and write $A \sim B$. We also write $\mathrm{Br}(k)$ for the set $\mathrm{CSA}_k / \sim$, i.e., Brauer equivalence classes of CSAs over k.

This has the following simple but useful consequence: to show that two CSAs are isomorphic, it suffices to show that they are Brauer equivalent and have the same dimension.

Corollary 4.7. *For $A, B \in \mathrm{CSA}_k$, TFAE:*
(i) $A \cong B$.
b) $A \sim B$ and $[A : k] = [B : k]$.

Exercise 4.5: Prove Corollary 4.7.

We claim that the tensor product of CSAs induces a well-defined binary operation on Brauer equivalence classes. That is, for $A, B \in \mathrm{CSA}_k$ we wish to define

$$[A] \cdot [B] = [A \otimes B],$$

but we need to check that this is well-defined independent of the choice of the representative. To see this, suppose that $A' \sim A$ and $B' \sim B$. Then we may write $A \cong M_m(D_1)$, $A' \cong M_{m'}(D_1)$, $B \cong M_n(D_2)$, $B' \cong M_{n'}(D_2)$ and compute

$$[A \otimes B] = [M_m(D_1) \otimes M_n(D_2)] = [M_{mn}(D_1 \otimes D_2)] = [D_1 \otimes D_2],$$

$$[A' \otimes B'] = [M_{m'}(D_1) \otimes M_{n'}(D_2)] = [M_{m'n'}(D_1 \otimes D_2)] = [D_1 \otimes D_2] = [A \otimes B],$$

which shows that the product of Brauer classes is well defined. It follows immediately that $\mathrm{Br}(k)$ is a commutative monoid, since indeed $[k]$ is an identity. More precisely, a CSA A represents the identity element of $\mathrm{Br}(k)$ iff it is of the form $M_n(k)$ for some $n \in \mathbb{Z}^+$. Indeed, Lemma 4.6 makes clear that the elements of $\mathrm{Br}(k)$ may be identified as a set with the division CSA's over k (the subtlety comes in when we try to compute the group law: since $D_1 \otimes D_2$ need not itself be a division algebra, in order to identify $[D_1] \cdot [D_2]$ with a division algebra, we need to appeal to Wedderburn's Theorem that any CSA is a matrix algebra over a unique division algebra). Finally, upon passing to Brauer classes the relation $A \otimes A^{\mathrm{op}} \cong \mathrm{End}_k(A)$ of Theorem 4.4 becomes

$$[A] \cdot [A^{\mathrm{op}}] = [\mathrm{End}_k(A)] = [M_n(k)] = 1,$$

i.e., in $\mathrm{Br}(k)$ the classes $[A]$ and $[A^{\mathrm{op}}]$ are mutually inverse. To sum up:

Theorem 4.8. *For any field k, the set of finite dimensional central simple algebras modulo Brauer equivalence form a commutative group $\mathrm{Br}(k)$, called the **Brauer group of k**, the group law being induced by the tensor product of algebras. The elements of the Brauer group are also naturally in bijection with the finite dimensional k-central division algebras over k.*

Exercise 4.6: Let l/k be an arbitrary field extension. Show that mapping $A \in \mathrm{CSA}_k$ to $A_l = A \otimes_k l \in \mathrm{CSA}_l$ induces a homomorphism of groups $\mathrm{Br}\, k \to \mathrm{Br}\, l$. Conclude that the set of isomorphism classes of k-central division algebras D such that $D_l \cong M_n(l)$ forms a subgroup of $\mathrm{Br}(k)$, the **relative Brauer group** $\mathrm{Br}(l/k)$.

4.3. The Skolem-Noether Theorem.

Lemma 4.9. *Let B be a finite-dimensional simple k-algebra, and let M be a k-vector space. Suppose $\varphi, \psi : B \to \mathrm{End}_k(M)$ are k-algebra homomorphisms. then there exists $\alpha \in \mathrm{Aut}_k(M)$ such that $\varphi(x) = \alpha^{-1}\psi(x)\alpha$ for all $x \in B$.*

Proof. The homomorphisms φ and ψ naturally endow M with the structure of a right B-module. But a finite-dimensional simple k-algebra is semisimple with a unique isomorphism class of simple modules, from which it follows that two finite-dimensional B-modules are isomorphic iff they have the same k-dimension. Therefore the two B-module structures, say M_φ and M_ψ are isomorphic, and we may take α to be an isomorphism between them. $\square$

Theorem 4.10. *(Skolem-Noether) Let A be a finite-dimensional central simple k-algebra and B a simple k-algebra. Then any two k-algebra maps $\chi_1, \chi_2 : B \to A$ are conjugate by an element of $A^\times$.*

Proof. Let $\Phi : A \otimes A^{\mathrm{op}} \to \mathrm{End}_k(A)$ be the isomorphism of Theorem 4.4. We define

$$\varphi = \Phi(\chi_1 \otimes 1) : B \otimes A^{\mathrm{op}} \to \mathrm{End}_k(A)$$

and

$$\psi = \Phi(\chi_2 \otimes 1) : B \otimes A^{\mathrm{op}} \to \mathrm{End}_k(A).$$

By Proposition 4.2, $B \otimes A^{\mathrm{op}}$ is simple, so Lemma 4.9 applies to show that there exists $\alpha \in \mathrm{Aut}_k(A)$ such that for all $x \in B, y \in A^{\mathrm{op}}$

$$\varphi(x \otimes y) = \alpha^{-1}\psi(x \otimes y)\alpha.$$

Let $z = \Phi^{-1}(\alpha) \in (A \otimes A^{\mathrm{op}})^\times$. Then

$$\Phi(z(\chi_2(x) \otimes y))) = \Phi(z)\Phi(\chi_2(x) \otimes y)) = \alpha\varphi(x \otimes y)$$

$$= \psi(x \otimes y)\alpha = \Phi(\chi_2(x) \otimes y)\Phi(z) = \Phi((\chi_2(x) \otimes y)z).$$

Since Φ is injective, it follows that for all $x \in B, y \in A^{\mathrm{op}}$,

(9) $$\chi_1(x) \otimes y = \alpha^{-1}(\chi_2(x) \otimes y)\alpha.$$

Taking $x = 1$ in (9), we get $z(1 \otimes y) = (1 \otimes y)z$, i.e., $z \in C_{A \otimes A^{\mathrm{op}}}(k \otimes A^{\mathrm{op}}) = A \otimes k$. Similarly $z^{-1} \in A \otimes k$. We may therefore write $z = u \otimes 1$, $z^{-1} = v \otimes 1$ with $u, v \in A$. Indeed $uv = vu = 1$ so $u \in A^\times$ and $v = u^{-1}$. Taking $y = 1$ in (9), we get $\chi_1(x) \otimes 1 = u^{-1}\chi_2(x)u \otimes 1$ for all $x \in B$: that is, $\chi_1(x) = u^{-1}\chi_2(x)u$, qed. $\square$

Corollary 4.11. *For any field k and any $n \in \mathbb{Z}^+$, the group of k-algebra automorphisms of $M_n(k)$ is the projective general linear group $\mathrm{PGL}_n(k)$.*

Proof. Applying Skolem-Noether with $A = B = M_n(k)$, we deduce that every automorphism of $M_n(k)$ is *inner*, i.e., obtained as conjugation by an element $\alpha \in M_n(k)^\times = \mathrm{GL}_n(k)$. The kernel of the conjugation action of $\mathrm{GL}_n(k)$ on $M_n(k)$ is the center of $\mathrm{GL}_n(k)$, which is the subgroup Z of nonzero scalar matrices. By definition, $\mathrm{PGL}_n(k) = \mathrm{GL}_n(k)/Z$. $\square$

4.4. **The Double Centralizer Theorem.**

In this section we will establish the mighty Double Centralizer Theorem.

Let A and B be finite dimensional k-algebras which are simple but not necessarily central simple. We define $A \sim B$ to mean that there exist $m, n \in \mathbb{Z}^+$ such that $M_m(A) \cong M_n(B)$.

Exercise 4.7: Show that $A \sim B$ iff $Z(A) \cong Z(B)$ and, after identifying these two fields with a fixed k-algebra l, A and B are Brauer-equivalent in CSA_l.

Lemma 4.12. *Let A be a k-algebra and B a k-subalgebra of A.*
a) The k-linear map $\Phi : A \otimes_k B^{\mathrm{op}} \to \mathrm{End}_k(A)$ given by $a \otimes b \mapsto (x \in A \mapsto axb)$
endows A with the structure of a left $A \otimes_k B^{\mathrm{op}}$-module.
b) With respect to the above module structure on A, we have

$$\mathrm{End}_{A \otimes B^{\mathrm{op}}} A = C_A(B) = \{x \in A \mid xy = yx \; \forall y \in B\}.$$

Exercise 4.8: Prove Lemma 4.12.

Lemma 4.13. *Let $\mathcal{A}$ be a finite dimensional simple k-algebra, and let S be the (unique, up to isomorphism) simple left $\mathcal{A}$-module. Put $D = \mathrm{End}_{\mathcal{A}} S$. Let M be a finitely generated left $\mathcal{A}$-module.*
a) As a right D-module, $S \cong D^r$ for some $r \in \mathbb{Z}^+$.
b) We have $\mathcal{A} \cong M_r(D)$.
c) $M \cong S^n$ for some $n \in \mathbb{Z}^+$ and thus $\mathcal{B} := \mathrm{End}_{\mathcal{A}} M \cong M_n(D)$.
d) We have

$$[M : k]^2 = [\mathcal{A} : k][\mathcal{B} : k].$$

Proof. Parts a) through c) are all parts or immediate consequences of the Wedderburn-Artin theory of §2 and are reproduced here for the convenience of the reader. As for part d), we simply compute:

$$[M : k] = [S^n : k] = n[S : k] = n[D^r : k] = nr[D : k],$$

$$[\mathcal{A} : k] = [M_r(D) : k] = r^2[D : k],$$

$$[\mathcal{B} : k] = [M_n(D) : k] = n^2[D : k],$$

so $[M : K]^2 = [\mathcal{A} : k][\mathcal{B} : k]$. $\square$

Theorem 4.14. *(Double Centralizer Theorem) Let $A \in \mathrm{CSA}_k$, let B be a simple subalgebra of A. Let $l = Z(B)$ be the center of B, and let $C = C_A(B)$ be the commutant of B in A. Then:*

 a) *C is simple.*
 b) *$[B : k][C : k] = [A : k]$.*
 c) *$C_A(C) = C_A(C_A(B)) = B$.*
 d) *$C \sim A \otimes B^{\mathrm{op}}$. In particular, $Z(C) = l$.*
 e) *$A_l \sim B \otimes_l C$.*
 f) *If B is central simple, so is $C_A(B)$, and then $A = B \otimes C_A(B)$.*

Proof. Put $\mathcal{A} = A \otimes B^{\mathrm{op}}$ and $M = A$. By Proposition 4.2b), $A \otimes B^{\mathrm{op}}$ is a finite-dimensional simple k-algebra, and by Lemma 4.12a) M is a finite-dimensional left $\mathcal{A}$-module. Therefore Lemma 4.13 applies: in the notation of that result, we have

$$C = \mathrm{End}_{A \otimes B^{\mathrm{op}}} A = \mathrm{End}_{\mathcal{A}} M \cong M_n(D)$$

and

$$A \otimes B^{\mathrm{op}} = \mathcal{A} \cong M_r(D).$$

Thus C is a simple algebra which is Brauer equivalent to $A \otimes B^{\mathrm{op}}$, which establishes parts a) and d). Moreover, applying Lemma 4.13d) gives

$$[A : k]^2 = [A \otimes B^{\mathrm{op}} : k][C : k] = [A : k][B : k][C : k],$$

and dividing through by $[A : k]$ we get part b). Next,

$$B \otimes_l C \sim B \otimes_l (A \otimes_k B^{\mathrm{op}}) \cong (B \otimes_l B^{\mathrm{op}}) \otimes_k A \sim l \otimes_k A = A_l,$$

establishing part e).

Put $B' = C_A(C)$. By part a), C is simple so we may apply part b) to $C \subset A$, giving $[B : k] = [B' : k]$. But any ring is contained in its own second commutant, i.e., $B \subset C_A(C_A(B)) = B'$ and thus $B = B'$, establishing c).

Finally, we assume that $B \in \text{CSA}_k$. Then the subalgebras B and C commute with each other, the universal property of the tensor product of algebras gives us a map $B \otimes C \to A$ which, since $B \otimes C$ is simple, is an injection. By part b) the two sides have equal k-dimension, so this map is an isomorphism. $\qquad\square$

Remark: The terminology "Double Centralizer Theorem" is traditional (and rather snappy), so we have preserved it even though it does not quite fit in our framework. For one thing, we speak of "commutants" rather than "centralizers", and for another there is much more to the theorem than the assertion that taking two commutants gets us back to where we stated.

Against our better judgment, we will sometimes use the abbreviation **DCT** for the Double Centralizer Theorem.

4.5. **Notes.**

The material in this section is extremely classical and, up to isomorphism, can be found in many texts.

The Skolem-Noether theorem was first proved by Skolem[14], a powerful and prolific Norwegian mathematician. Nowadays Skolem is best known as one of the founders of model theory (e.g. the Skolem-Löwenheim Theorem) but he was also a leading researcher in number theory and algebra. It seems that many of his papers were published in Norwegian journals which were not well read by the international mathematical community, so that some of his results were duplicated by others. This holds for the Skolem-Noether theorem, which was independently proven by Noether[15] a few years after Skolem.

Unfortunately I do not know anything about the history of the Double Centralizer Theorem. (Please contact me if you do!) Both the Skolem-Noether and Double Centralizer Theorems hold with weaker finiteness conditions on the ambient central simple algebra A: see [P, Ex. 1, p. 231] for an outline of a proof of a more general Skolem-Noether theorem.

The Brauer group is named after the great algebraist R. Brauer[16] stemming from his work on central simple algebras from the 1920's to the 1940's. It would be hard to overstate its importance: for instance, Brauer groups were woven into the foundations of class field theory by Artin and Tate, were brought into algebraic geometry by Grothendieck and into the study of Diophantine equations by Manin.

Textbook references: in the large we have followed the exposition of [P] for the

---

[14]Thoralf Albert Skolem, 1887-1963

[15]Amalie Emmy Noether, 1882-1935. Emmy Noether is often credited with the title "greatest female mathematician." This is probably true, but one should say more: she was easily one of the greatest mathematicians of the 20th century, and she had a greater hand in crafting algebra into the subject it is today than any other single person.

[16]Richard Brauer, 1901-1977

results of this section (and for many of the sections to come). At this point in the course we were already short of time, and I tried to find the shortest, simplest statements and proofs of theorems that I could. So for instance we replaced several other technical results with Lemma 4.1 taken from [S-QF, Lemma 19.4]. (This result is also of interest in itself as a natural generalization of Theorem 1.22.) Our statement and proof of the Double Centralizer Theorem follow [Lo08, Thm. 29.14].

5. Quaternion algebras

5.1. Definition and first properties.

In this section we let k denote a field of characteristic different from 2. For $a, b \in k^\times$, we define a k-algebra $\left(\frac{a,b}{k}\right)$ by generators and relations, as follows: it has two generators i and j and is subject to the relations $i^2 = a$, $j^2 = b$, $ij = -ji$. A k-algebra which is isomorphic to $\left(\frac{a,b}{k}\right)$ for some $a, b \in k^\times$ is called a **quaternion algebra**.

Our first order of business is to show that $\left(\frac{a,b}{k}\right)$ is a 4-dimensional k-algebra with k-basis given by $1, i, j, ij$. It is easy to see that $1, i, j, ij$ is a spanning set for $\left(\frac{a,b}{k}\right)$ (try it). To show that these elements are k-linearly independent it is enough to show that the k-algebra with basis $1, i, j, ij$ and multiplication law

$$(a_1 + b_1 i + c_1 j + d_1 ij)(a_2 + b_2 i + c_2 j + d_2 ij) = \ldots$$

is actually associative. This can be done brute force: it is enough to check that for any three basis elements e_i, e_j, e_k, the **associator** $[e_i, e_j, e_k] = (e_i e_j) e_k - e_i (e_j e_k)$ is zero. This computation is actually carried out in [NA, pp. 6-7].

Exercise 5.1: Show that the center of $\left(\frac{a,b}{k}\right)$ is k.

Exercise 5.2: Show directly that $\left(\frac{a,b}{k}\right)$ is a simple k-algebra.
(For instance, this is done in the proof of [Ch, Thm. 1.5].)

Proposition 5.1. *Let k be a field of characteristic different from* 2.
  a) *For any $a, b \in k^\times$, the algebra $\left(\frac{a,b}{k}\right)$ is a 4-dimensional CSA over k.*
  b) *Therefore $\left(\frac{a,b}{k}\right)$ is either a division algebra or isomorphic to $M_2(k)$.*

Proof. Part a) follows from all the brute force we applied above. As for part b), by Wedderburn's Theorem, $\left(\frac{a,b}{k}\right) \cong M_n(D)$. Since it has dimension 4, the only possibilities for n are $n = 1$, in which case the algebra is isomorphic to D and $n = 2$, in which case the algebra is isomorphic to $M_2(k)$. $\square$

A quaternion algebra B is called **split** if it is isomorphic to $M_2(k)$ an otherwise **nonsplit**.

Exercise 5.3: Show that for all $a, b \in k^\times$, $\left(\frac{a,b}{k}\right)^{\mathrm{op}} \cong \left(\frac{b,a}{k}\right)$.

Exercise 5.4: Let $a, b, c \in k^\times$.

a) Show that the indicated quaternion algebras are isomorphic by constructing explicit isomorphisms:

(i) $\left(\frac{a,b}{k}\right) \cong \left(\frac{b,a}{k}\right)$.

(ii) $\left(\frac{ac^2,b}{k}\right) \cong \left(\frac{a,b}{k}\right) \cong \left(\frac{a,bc^2}{k}\right)$.

b) Deduce: every quaternion algebra is isomorphic to its opposite algebra.

5.2. Quaternion algebras by Descent.

There are better ways to show that quaternion algebas are CSAs. One begins with the key observation that $M_2(k)$ is a quaternion algebra. Indeed:

Proposition 5.2. *For any $a, b \in k^\times$, we have $\left(\frac{a^2,b}{k}\right) \cong M_2(k)$.*

Proof. We define explicit matrices

$$I = \begin{bmatrix} a & 0 \\ 0 & -a \end{bmatrix}, \ J = \begin{bmatrix} 0 & b \\ 1 & 0 \end{bmatrix}.$$

They satisfy the relations $I^2 = a$, $J^2 = b$, $IJ = -IJ$. Moreover, the four matrices $1, I, J, IJ$ are k-linearly independent, so generate $M_2(k)$ as an algebra. Therefore sending $i \mapsto I, j \mapsto J$ gives a surjective k-algebra map $\left(\frac{a^2,b}{k}\right) \to M_2(k)$. Since both algebras have dimension 4, this map is an isomorphism. $\square$

Now consider a quaternion algebra $B = \left(\frac{a,b}{k}\right)$ over k. If a is a square, then we know $B \cong M_2(k)$. Otherwise $l = k(\sqrt{a})$ is a quadratic field extension, and consider the base extension of B to l:

$$B_l = B \otimes_k l = \left(\frac{a,b}{l}\right) = \left(\frac{(\sqrt{a})^2, b}{l}\right) \cong M_2(l).$$

Now the sneaky part: since $B_l \cong M_2(l)$ is a CSA over l, by Theorem 4.4 B itself is a CSA over k. This gives a new proof of Proposition 5.1.

5.3. The involution, the trace and the norm.

Let $B = \left(\frac{a,b}{k}\right)$ be a quaternion algebra over k. We define the **canonical involution** on B explicitly as follows: if

$$w = x_1 \cdot 1 + x_2 \cdot i + x_3 \cdot j + x_4 \cdot ij,$$

then

$$\overline{w} = x_1 \cdot 1 - x_2 \cdot i - x_3 \cdot j - x_4 \cdot ij.$$

Note that this is reminiscent of complex conjugation in that we are negating the three "imaginary components" of w.

Exercise 5.5: a) Show that w is indeed an involution on B, namely:
(i) For all $w_1, w_2 \in B$, $\overline{w_1 w_2} = \overline{w_2} \ \overline{w_1}$ and
(ii) For all $w \in B$, $\overline{\overline{w}} = w$.
b) Show (again) that every quaternion algebra is isomorphic to its opposite algebra.

We define a k-linear map $t : B \to k$, the **reduced trace**, by $w \in B \mapsto w + \overline{w}$. In coordinates

$$t(x_1 \cdot 1 + x_2 \cdot i + x_3 \cdot j + x_4 \cdot ij) = 2x_1.$$

Thus the reduced trace is a *linear form* on B.

We define $n : B \to k$, the **reduced norm**, by $w \in B \mapsto w\overline{w}$. In coordinates,

$$n(x_1 \cdot 1 + x_2 \cdot i + x_3 \cdot j + x_4 \cdot ij) = x_1^2 - ax_2^2 - bx_3^2 + abx_4^2.$$

Thus the reduced norm is a nondegenerate *quadratic form* on B.

Exercise 5.6: Show that the reduced norm n is multiplicative: that is, for all $w_1, w_2 \in B$, $n(w_1 w_2) = n(w_1)n(w_2)$.

Remark: A **composition algebra** is a unital but not necessarily associative k-algebra C together with a nondegenerate quadratic form $N : C \to k$ which is multiplicative in the sense that for all $x, y \in C$, $N(xy) = N(x)N(y)$. Thus any quaternion algebra endowed with its reduced norm is a composition algebra.

Exercise 5.7:[17] Consider the left regular representation of B: for each $w \in B$, consider $w\bullet$ as a linear endomorphism of the 4-dimensional k-vector space B. By choosing a basis, this gives an embedding $\iota : B \hookrightarrow M_4(k)$.
a) Show that for all $w \in B$, the trace of $\iota(w)$ is $2t(w)$.
b) Show that for all $w \in B$, the determinant of $\iota(w)$ is $n(w)^2$.

Exercise 5.8: Let φ be a k-algebra automorphism of B. Show that for all $w \in B$ we have $t(\varphi(w)) = t(w)$ and $n(\varphi(w)) = n(w)$. That is, the reduced trace and reduced norm are "intrinsic" to B rather than depending upon the chosen quaternionic basis. Since $\overline{w} = t(w) - w$, the same holds for the canonical involution – it is indeed canonical. (Hint: apply the Skolem-Noether Theorem and the previous exercise.)

Recall that for a quadratic form $q(x)$, there is an associated bilinear form, given by

$$\langle x, y \rangle = \frac{1}{2} \left(q(x + y) - q(x) - q(y) \right).$$

Proposition 5.3. *The bilinear form associated to the norm form $n(x)$ is*

$$\langle x, y \rangle = t(x\overline{y}).$$

Exercise 5.9: Prove Proposition 5.3.

Recall that a quadratic form $q(x) = q(x_1, \ldots, x_n)$ over a field k is **anistropic** if for every $0 \neq x \in k^n$, $q(x) \neq 0$. A nondegenerate quadratic form which is not anisotropic is **isotropic**.

Theorem 5.4. *For a quaternion algebra B, the following are equivalent:*
  (i) *B is nonsplit, i.e., a division algebra.*
  (ii) *The norm form n is anisotropic.*

---

[17]This exercise serves to explain the names "reduced trace" and "reduced norm".

Proof. (i) $\implies$ (ii): For any $w \in B$, we have $n(w) = w\overline{w} \in k$. Clearly $w \neq 0 \iff$ $\overline{w} \neq 0$, so if B is a division algebra it is in particular a domain and for nonzero w, $n(w) = w\overline{w} \neq 0$.

(ii) $\implies$ (i): Suppose that n is anisotropic, and let $0 \neq w \in B$. Then $n(w) \in k^{\times}$; multiplying the equation $w\overline{w} = n(w)$ by $n(w)^{-1}$ gives

$$w \left(\frac{\overline{w}}{n(w)} \right) = 1,$$

so $w \in B^{\times}$. $\qquad\square$

Remark: The proof of Theorem 5.4 has the ring of the familiar. It is for instance how one shows that $\mathbb{C}$ is a field. In fact it holds for all composition algebras.

Example: The reduced norm on $B = \left(\frac{1,b}{k} \right)$ is $n = x_1^2 - x_2^2 - bx_3 + bx_4^2$. This form is visibly isotropic: take for instance $w = (1, 1, 0, 0)$. Using Theorem 5.4 we see (again) that $B \cong M_2(k)$.

Example: We can now give everyone's first example of a noncommuative division algebra, namely the **Hamiltonians** $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}} \right)$. The norm form is

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2,$$

which is clearly anisotropic over $\mathbb{R}$ since a sum of squares, not all of which are zero, is strictly positive and thus nonszero. Note that the same argument works just as well for $B = \left(\frac{a,b}{k} \right)$ for any field k which admits an **ordering** with respect to which a and b are both negative: again $n(w)$ is strictly positive for all nonzero w. So this gives for instance many examples of quaternion algebras over $\mathbb{Q}$.

Exercise 5.10: Show that $\mathbb{H}$ is, up to isomorphism, the *unique* division quaternion algebra over $\mathbb{R}$. (Hint: the isomorphism class of $\left(\frac{a,b}{k} \right)$ depends only on the **square classes** of a and b, i.e., their images in $k^{\times}/k^{\times 2}$.)

5.4. **Every** 4**-dimensional CSA is a quaternion algebra.**

Theorem 5.5. *Let k be a field of characteristic different from 2, and let B/k be a 4-dimensional CSA. Then there are $a, b \in k^{\times}$ such that $B \cong \left(\frac{a,b}{k} \right)$.*

Proof. Let B/k be a 4-dimensional CSA. By Classical Wedderburn (Theorem 2.18), we have that either $B \cong M_2(k)$ or B/k is a division algebra. Proposition 5.2 gives $M_2(k) \cong \left(\frac{1,1}{k} \right)$, so we may assume that B/k is a division algebra.

Step 1: Let $x \in B \setminus k$, and let l be the k-subalgebra of B generated by x. Then l/k is a field extension with $k \subsetneq l \subsetneq B$. Applying the Double Centralizer Theorem to the simple subalgebra l of B, we find that $[l : k] = 2$ and $Z_B(l) = l$.

Step 2: Since k does not have characteristic 2, every quadratic extension of k is obtained by adjoining a square root, so there exists $I \in l$ such that $I^2 = a \in k^{\times}$. Let $\sigma : l \to l$ be the unique nontrivial k-algebra automorphism of l. By Skolem-Noether, σ can be expresed as conjugation by some $J \in B^{\times}$: that is, for all $y \in l$,

$$\sigma(y) = J^{-1}yJ.$$

Since for all $y \in l$, $y = \sigma^2(y) = J^{-2}yJ^2$, $J^2 \in Z_B(l) = l$. Clearly $J \notin l$, so

$$k \subset k[J^2] \cap l \subset k[J] \cap l = k.$$

Therefore $J^2 = b \in k^\times$. Finally, we have

$$J^{-1}IJ = \sigma(I) = -I.$$

So $i \mapsto I$, $j \mapsto J$ gives a homomorphism from the 4-dimensional simple algebra $\left(\frac{a,b}{k}\right)$ to the 4-dimensional algebra B; any such homomorphism is an isomorphism.

$\square$

5.5. The ternary norm form and associated conic.

In addition to the quaternary norm form, it turns out to be useful to consider two associated ternary quadratic forms

$$n_0(x, y, z) = -ax^2 + -by^2 + abz^2$$

and

$$C(x, y, z) = ax^2 + by^2 - z^2.$$

Thus $n_0(x, y, z)$ is the norm form restricted to the trace zero subspace of B, the so-called **pure quaternions**, so n is the orthogonal direct sum of the one-dimensional form w^2 with n_0. We will call n_0 the **ternary norm form** or the **pure norm form**. Moreover, n_0 is up to isomorphism a rescaling of C: that is, if we multiply every coefficient of C by $-ab$ we get

$$(-ab)C : -b(ax)^2 - a(by)^2 + abz^2,$$

and then the linear change of variables

$$x \mapsto by, \ y \mapsto bx$$

shows that abC is isomorphic to n_0: the quadratic forms n_0 and C are **similar**.

Remark: geometrically speaking C defines a **plane conic curve**, i.e., a degree 2 curve in the projective plane $\mathbb{P}^2_{/k}$. Conversely, every plane conic is given by a quadratic form, and it is not hard to show (see e.g. paper on eevip...) that two plane conics are are isomorphic as algebraic curves iff the corresponding ternary quadratic forms are similar: that is, one can be obtained from the other by a linear change of variables followed by a rescaling. Thus n_0 and C give rise to "the same" conic curve, and that turns out to be paramount.

Theorem 5.6. *For $a, b \in k^\times$, the following are equivalent:*
   (i) *The ternary norm form n_0 is isotropic.*
   (i′) *The quadratic form C is isotropic.*
   (ii) *The norm form n is isotropic.*
   (iii) *The element a is a norm from $k(\sqrt{b})/k$.*
   (iii′) *The element b is a norm from $k(\sqrt{a})/k$.*

Proof. To abbreviate the proof, we ask the reader to verify for herself that all of the equivalences hold rather vacuously if either a or b is a square in k. Henceforth we assume that this is not the case.
(i) $\iff$ (i′): As above, the quadratic forms n_0 and C are similar: up to isomorphism, one is just a rescaling of the other. It is immediate to show that two similar

forms are both isotropic or both anisotropic.

(i) $\implies$ (ii): The form n_0 is a subform of n, so if n_0 is isotropic n is as well. In less formy language, n_0 is isotropic iff some nonzero pure quaternion has reduced norm zero, which certainly implies that some nonzero quaternion has reduced norm zero.

(i$'$) $\implies$ (iii), (iii$'$): Since C is isotropic, there are $x, y, z \in k$, not all 0 such that

$$z^2 = ax^2 + by^2.$$

If $x = 0$, then $y = 0 \iff z = 0 \iff x = y = z = 0$, so $y, z \neq 0$ and then $b \in k^{\times 2}$, contradiction. So $x \neq 0$ and

$$a = \left(\frac{z}{x}\right)^2 - b\left(\frac{y}{x}\right)^2 = N(\frac{z}{x} + \sqrt{b}\frac{y}{x}).$$

Similarly, if $y = 0$, then $x = 0 \iff z = 0 \iff x = y = z = 0$, so $x, z \neq 0$ and $a \in k^{\times}$, contradiction. So $y \neq 0$ and

$$b = \left(\frac{z}{y}\right)^2 - a\left(\frac{x}{y}\right)^2 = N(\frac{z}{y} + \sqrt{a}\frac{x}{y}).$$

(iii) $\implies$ (i$'$): If b is a norm from $k(\sqrt{a})$, then there exist $z, x \in k$ such that

$$N(z + \sqrt{a}x) = z^2 - ax^2 = b,$$

so $ax^2 + b(1)^2 = z^2$. Thus C is isotropic.

(iii$'$) $\implies$ (i$'$): If a is a norm from $k(\sqrt{b})$, then there exist $z, y \in k$ such that

$$N(z + \sqrt{b}y) = z^2 - by^2 = a,$$

so $a(1)^2 + by^2 = z^2$. Thus C is isotropic.

(ii) $\implies$ (iii$'$): Suppose there exist $x, y, z, w \in k$, not all zero, such that

$$x^2 - ay^2 - bz^2 + abw^2 = 0.$$

We claim $z \pm w\sqrt{a} \neq 0$. Indeed, if not $0 = (z + w\sqrt{a})(z - w\sqrt{a}) = z^2 - aw^2$, and since a is not a square, this implies $z = w = 0$. Also $x^2 - ay^2 = b(z^2 - aw^2) = 0$, so $x = y = 0$, a contradiction. So we have

$$N\left(\frac{x + y\sqrt{a}}{z + w\sqrt{a}}\right) = \frac{x^2 - ay^2}{x^2 - aw^2} = b. \qquad \square$$

Corollary 5.7. *Let $q(x, y, z)$ be a ternary quadratic form over k. Suppose that q represents $-\operatorname{disc}(q)$. Then q is isotropic.*

Proof. Step 1: Suppose $\operatorname{disc}(q) = 1$, so $q = n_0$ is a ternary norm form. Since q represents $-\operatorname{disc}(q) = -1$, by the First Representation Theorem ([QF1, Thm. 18]) the form $n = q \oplus \langle 1 \rangle$ is isotropic. By Theorem 5.6, q itself is isotropic.

Step 2: Now suppose $\operatorname{disc}(q) = d \in K^{\times}$. Let $q' = dq$; since the number of variables is odd, $\operatorname{disc}(q') = 1$ (recall that the discriminant of a quadratic form over a field is a square-class in the field). Since q represents $-\operatorname{disc}(q) = -d$, q' represents $d \cdot (-d)$ and thus $-1 = -\operatorname{disc}(q')$. By Step 1, q' is isotropic, and hence so is q. $\qquad \square$

Theorem 5.6 reduces the determination of the splitness of a quaternion algebra to a problem in field theory. Moreover, when the ground field is of the sort that number theorists care about – e.g. a p-adic field or a number field – then this field-theoretic problem can be solved using very standard (which is not to say trivial) number-theoretic techniques. For instance, recall the following classical theorem.

Theorem 5.8. *(Legendre) Let a, b, c be squarefree positive integers which are pair-wise coprime. Then the equation $ax^2 + by^2 - cz^2$ has a nontrivial integral solution iff there exist $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{Z}$ such that all of the following hold:*

(i) $-ab \equiv \lambda_1^2 \pmod{c}$.
(ii) $-bc \equiv \lambda_2^2 \pmod{a}$.
(iii) $-ac \equiv \lambda_3^2 \pmod{b}$.

Proof. See e.g. [Cl-NT, Thm. 18.4]. $\qquad\square$

Corollary 5.9. *Let a and b be two coprime squarefree integers, not both negative. Then the quaternion algebra $B = \left(\frac{a,b}{\mathbb{Q}}\right)$ is nonsplit iff $|a|$ is a square modulo $|b|$ and $|b|$ is a square modulo $|a|$.*

Proof. By Theorem 5.6, B is split iff the conic $C = ax^2 + by^2 - z^2$ has a nontrivial $\mathbb{Q}$-rational solution. Since the equation is homogeneous, it has a nontrivial $\mathbb{Q}$-solution iff it has a nontrivial $\mathbb{Z}$-solution.
Case 1: Suppose that a and b are both positive. Then Legendgre's Theorem applies to show that $ax^2 + by^2 - z^2 = 0$ has a nontrivial $\mathbb{Z}$-solution iff a is a square modulo b and b is a square modulo a.
Case 2: Suppose a is positive and b is negative. Then multiplying by -1 shows that the equation $ax^2 + by^2 - z^2 = 0$ has a nontrivial $\mathbb{Z}$-solution iff the equation $x^2 + |b|y^2 - az^2 = 0$ has a nontrivial $\mathbb{Z}$-solution. Legendre's Theorem applies to show that this occurs iff a is a square modulo $|b|$ and $|b|$ is a square modulo a.
Case 3: Of course the case in which a is negative and b is positive can be reduced to Case 2, e.g. by interchanging a and b. $\qquad\square$

Exercise 5.11: a) Apply Corollary 5.9 to show that for a prime number p, the quaternion algebra $\left(\frac{-1,p}{\mathbb{Q}}\right)$ is split iff $p \equiv 1, 2 \pmod{4}$.
b) Show $B_1 = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ and $B_2 = \left(\frac{-1,3}{\mathbb{Q}}\right)$ are nonisomorphic division algebras.

Exercise 5.12: Show that Legendre's Theorem gives a criterion for any quaternion algebra $\left(\frac{a,b}{\mathbb{Q}}\right)$ to be split in terms of certain sign conditions and certain positive integers being squares modulo certain other positive integers. (Hint: let a, b, c be nonzero integers such that a and b are both divisible by p and c is not divisible by p. Then the equation $ax^2 + by^2 - cz^2 = 0$ has a nontrivial $\mathbb{Z}$-solution iff the equation $\frac{a}{p}x^2 + \frac{b}{p}y^2 - pcz^2$ has a nontrivial $\mathbb{Z}$-solution.)

Exercise 5.13: For $a, b \in \mathbb{Q}^\times$, put $B = \left(\frac{a,b}{\mathbb{Q}}\right)$. Show that TFAE:
(i) $B \cong M_2(\mathbb{Q})$.
(ii) For all primes p, $B \otimes \mathbb{Q}_p \cong M_2(\mathbb{Q}_p)$ and $B \otimes \mathbb{R} \cong M_2(\mathbb{R})$.
(Suggestion: use Legendre's Theorem.)

Exercise 5.14: Let p be an odd prime number, let a, b be nonzero integers and consider $B = \left(\frac{a,b}{\mathbb{Q}_p}\right)$.
a) Suppose that a and b are both prime to p. Show that B is split.
b) Suppose a is prime to p and $b = p$. Show B is split iff a is a square modulo p.
c) Suppose $a = b = p$. Show that B is split iff $p \equiv 1 \pmod{4}$.
d) Suppose a is prime to p and $b = vp$ with $\gcd(v, p) = 1$. Show that B is split iff

a is a square modulo p.

e) Suppose $a = up$ and $b = vp$ with $\gcd(uv, p) = 1$. Show that B is split iff $-uv$ is a square modulo p.

f) Explain why the computations of parts a) through e) are sufficient to determine whether any quaternion algebra over $\mathbb{Q}_p$ is split. (Hint: $\mathbb{Q}_p^\times$ has four square classes. If u is any integer which is a quadratic nonresidue modulo p, they are represented by $1, u, p, pu$.)

g) Show that parts a) through f) still hold for any p-adic field with p odd.

Exercise 5.15: By a similar analysis, determine exactly when a quaternion algebra over $\mathbb{Q}_2$ is split. Do these calculations work in any 2-adic field? (No!)

5.6. Isomorphism of Quaternion Algebras.

Theorem 5.10. *Let* $B = \left(\frac{a,b}{k}\right)$ *and* $B' = \left(\frac{a',b'}{k}\right)$ *be two quaternion algebras over* k, *with respective quaternary norm forms* n *and* n', *ternary norm forms* n_0 *and* n_0' *and conic curves* C *and* C'. *The following are equivalent:*

   (i) *We have* $B \cong B'$ *(as k-algebras).*
   (ii) *We have* $n \cong n'$ *(as quadratic forms).*
   (iii) *We have* $n_0 \cong n_0'$ *(as quadratic forms).*
   (iv) *We have* $C \cong C'$ *(as algebraic curves).*

Proof. (i) $\implies$ (ii): The quaternary norm form n_0 of a quaternion algebra B is defined in terms of the intrinsic structure of B and therefore its isomorphism class depends only on the isomorphism class of B.

(ii) $\implies$ (iii): apply the Witt Cancellation Theorem.

(iii) $\implies$ (i): Consider the associated bilinear form of n_0: by Proposition 5.3 it is

$$\langle x, y \rangle = t(x\overline{y}) = x\overline{y} + y\overline{x} = -(xy + yx).$$

Therefore two elements x, y in the trace zero subspace B_0 anticommute iff they are orthogonal for this bilinear form: $\langle x, y \rangle = 0$. Now let

$$f : (B_0, \langle, \rangle) \to (B_0', \langle, \rangle)$$

be an isometry of quadratic spaces. Then $i, j \in B_0$ and

$$-2f(i)^2 = \langle f(i), f(i) \rangle = \langle i, i \rangle = -2i^2 = -2a,$$

so $f(i)^2 = a$. Similarly $f(j)^2 = b$. Also i and j anticommute in B_0, so $\langle i, j \rangle = 0$, so $\langle f(i), f(j) \rangle = 0$, so $f(i)$ and $f(j)$ anticommute. It follows that $B \cong B'$.

(ii) $\iff$ (iv): as mentioned above, two ternary quadratic forms determine isomorphic conic curves iff the forms are *similar*: but since n_0 and n_0' both have determinant $-1 \in k^\times/k^{\times 2}$, they are similar iff they are isomorphic. $\qquad\square$

Remark: The equivalence of (i) through (iv) (with (iv) reinterpreted as saying that the corresponding quadric hypersurfaces are isomorphic algebraic varieties) continues to hold for all composition algebras: see e.g. [NA].

Theorem 5.11. *Assigning to each quaternion algebra its conic curve gives a bijection between isomorphism classes of quaternion algebras over k and isomorphism classes of conic curves over k.*

Proof. It remains only to check that, up to isomorphism, every conic curve is the conic curve of some quaternion algebra. Since the characteristic of k is not 2, any quadratic form can be diagonalized so any plane conic is isomorphic to $Ax^2 + By^2 + Cz^2 = 0$ for some $A, B, C \in k^\times$. Recalling that isomorphism of conics corresponds to similarity of quadratic forms, we may divide by $-C$ to get the isomorphic conic $\frac{-A}{C}x^2 + \frac{-B}{C}y^2 - z^2 = 0$, which is the conic associated to $\left(\frac{\frac{-A}{C}, \frac{-B}{C}}{k}\right)$. $\square$

Remark: We sketch a higher brow proof, using the following facts about conics:
• A plane conic C is isomorphic to $\mathbb{P}^1$ iff it has a k-rational point: $C(k) \neq \varnothing$. (Indeed, having a rational point is clearly necessary to be isomorphic to $\mathbb{P}^1$. If one has a k-rational point P_0 then considering for each $P \in C(k)$ unique line joining P_0 and P – when $P_0 = P$ we take the tangent line at P_0 – gives a natural bijection from $C(k)$ to the set of lines in the plane, i.e., to $\mathbb{P}^1(k)$.)
• If k^{sep} is a separable closure of k, then every plane conic has a k^{sep}-rational point. (A plane conic is a geometrically integral algebraic variety and every geometrically integral algebraic variety over a separably closed field has a rational point.)
• The automorphism group of $\mathbb{P}^1$ is $\mathrm{PGL}_2(k)$.

Therefore by the principle of Galois descent, the pointed set of plane conic curves is given by the nonabelian Galois cohomology set $H^1(k, \mathrm{PGL}_2)$.

On the quaternion algebra side, we know that every quaternion algebra over k becomes isomorphic over $\overline{k}$ to $M_2(k)$ and also by Skolem-Noether that $\mathrm{Aut}(M_2(k)) = \mathrm{PGL}_2(k)$. Therefore by Galois descent the pointed set of quaternion algebras over k is given by the nonabelian Galois cohomology set $H^1(k, \mathrm{PGL}_2)$.

Thus we have parameterized both isomorphism classes of plane conics and isomorphism classes of quaternion algebras by the same set $H^1(k, \mathrm{PGL}_2)$, whence another proof of Theorem 5.11.

5.7. The generic quaternion algebra is a division algebra.

Let K be any field of characteristic different from 2. By the **generic quaternion algebra** over K we mean the quaternion algebra $\left(\frac{s,t}{k}\right)$ where a and b are independent indeterminates and $k = K(s,t)$. Thus "the generic quaternion algebra over K" is not in fact a quaternion algebra over K but rather is a quaternion algebra over k such that any quaternion algebra $\left(\frac{a,b}{k}\right)$ is obtained by *specializing* the values of s and t to $s = a$ and $s = t$ respectively. (This has a precise meaning in algebraic geometric terms, which is however beyond the scope of these notes.)

Theorem 5.12. *For any field K, the generic quaternion algebra over K is a division algebra.*

Proof. By Theorem 5.6 it suffices to show that the associated quadratic form

$$(10) \qquad\qquad \mathcal{C} : ax_1^2 + bx_2^2 - x_3^2 = 0$$

is anisotropic over $k = K(a,b)$. Seeking a contradiction, we suppose that there exists $x = (x_1, x_2, x_2) \in k^3 \setminus \{0\}$ such that $\mathcal{C}(x) = 0$. Let R be the UFD $K[a,b]$. By rescaling x_1, x_2, x_3, we may assume that $(x_1, x_2, x_3) \in R^3$ is a **primitive** solution, i.e., not all coordinates are simultaneously divisible by any nonunit in R. It follows

that a does not divide x_2: for if not then also $a \mid x_3$, so $a^2 \mid bx_2^2 - x_3^2 = ax_1^2$, and thus, since a is a prime element of R, $a \mid x_1$, contradicting primitivity. So consider the equation in the quotient ring $R/(a) = K[b]$:

$$bx_2^2 - x_3^2 = 0$$

with $x_1, x_2 \neq 0$. It follows that b is a square in $K(b)$, a contradiction. $\qquad \square$

5.8. Notes.

Once again the material of this section can be found in many places: this time I used my own 2003 PhD thesis (on the arithmetic of abelian surfaces with potential quaternionic multiplication) as a first outline. That the treatment in my thesis is rather reminiscent of [P, Ch. 1] is presumably not accidental.

6. Central Simple Algebras II: Subfields and Splitting Fields

6.1. Dimensions of subfields.

We begin with a few easy comments about the subfields in division algebras. Throughout this section we fix a field k and all rings are k-algebras. In particular "subfield" really means "k-subalgebra which is a field". Let D be a division k-algebra and $x \in D$. We claim that there is a unique minimal subfield of D containing k. There are two cases:

Case 1: There is no nonzero polynomial $f \in k[t]$ such that $f(x) = 0$. We say that x is **transcendental** over k. Then it is clear that the k-subalgebra $k[x]$ of D generated by x is a polynomial ring and its field $k(x)$ of rational functions is the minimal subfield of D containing x.

Case 2: There is a nonzero polynomial $f \in k[t]$ such that $f(x) = 0$. We say that x is **algebraic** over k. In this case the set of all $f \in k[t]$ such that $f(x) = 0$ in D forms a nonzero prime ideal in $k[t]$. Any nonzero ideal in the PID $k[t]$ has a unique monic generator $P(t)$ which we call (is it a surprise?) the **minimal polynomial** of x. Then the k-subalgebra of D generated by x is isomorphism to $k[t]/(P(t))$ a field extension of k of degree equal to the degree of P.

Exercise 6.1: Let A be any finite dimensional k-algebra, and let $x \in A$.
a) Show that x has a well-defined minimal polynomial $P(t)$.
b) Show that (as claimed above) if A is a division algebra, then the minimal polynomial of any element of x is a nonzero irreducible polynomial. (Hint: it is enough for A to be a domain – although in fact, for finite dimensional k-algebras, this is equivalent to being a division algebra.)
c) By contrast, $A = M_n(k)$ show that every monic degree n polynomial $P \in k[t]$ is the minimal polynomial of some $x \in A$.

Exercise 6.2: A k-algebra A is **algebraic** if every $x \in A$ is algebraic over k.
a) Show that any finite dimensional k-algebra is algebraic.
b) Show that if k is algebraically closed, then the only algebraic division algebra over k is k itself.
c) Exhibit a field k and a k-central algebraic division algebra D which is *not* finite-dimensional over k.

Let $A \in \mathrm{CSA}_{/k}$. Recall $\dim_k A$ is a perfect square. Therefore we may define

$$\deg A = \sqrt{\dim_k A} \in \mathbb{Z}^+,$$

the **reduced degree** of A.[18] For a finite dimensional k-algebra A, we will sometimes write $[A : k]$ for the k-dimension of A.

Theorem 6.1. *Let l be a subfield of $A \in \mathrm{CSA}_k$, and let $C = C_A(l)$. Then $l \subset C$, $C \in \mathrm{CSA}_l$ and*

(11) $$[l : k] \deg C = \deg A.$$

In particular $[l : k] \mid \deg A$.

Proof. By DCTd), $Z(C) = l$ and $C \in \mathrm{CSA}_l$. Since l is commutative, $l \subset C$. Thus

$$(\deg A)^2 = [A : k] \overset{*}{=} [l : k][C : k] = [l : k]^2[C : l] = ([l : k] \deg C)^2,$$

where in the starred equality we have used DCTb). The result follows. $\square$

A subfield l of the CSA A is called **maximal** if (what else?) it is not properly contained in any othe subfield of A. On the other hand, Theorem 6.1 gives us an upper bound of $\deg A$ for the degree of a maximal subfield and hence a target. Let us say that a subfield l of $A \in \mathrm{CSA}_k$ is **strictly maximal** if $[l : k] = \deg A$.

Theorem 6.2. *Let l be a subfield of $A \in \mathrm{CSA}_k$, and let $C = C_A(l)$. Then*
a) The field l is strictly maximal iff $l = C$.
b) If A is a division algebra then every maximal subfield is strictly maximal.

Proof. a) This follows immediately from (11).
b) If A is a division algebra, then by DCTa), C is a simple subalgebra of the division algebra A, so C is also a division algebra. If $x \in C \setminus l$, then $l[x]$ is a strictly larger subfield of A than l, contradicting maximality. So $C = l$ and part a) applies. $\square$

In general a maximal subfield l of $A \in \mathrm{CSA}_k$ need not be strictly maximal. One apparently rather drastic way for this to occur is that k need not admit a field extension of degree $\deg A$. For instance, if k is algebraically closed then evidently k is a maximal subfield of $M_n(k)$ for all n.

In fact this is essentially the only obstruction. For $n \in \mathbb{Z}^+$, we say a field k is **n-closed** if there is no proper field extension l/k with $[l : k] \mid n$.

Proposition 6.3. *Let l be a subfield of $A \in \mathrm{CSA}_k$, and let $C = C_A(l)$.*
a) [P, §13]) Then l is maximal iff $C \cong M_n(l)$ and l is n-closed.
b) If every finite extension l/k itself admits finite extensions of all possible degrees, then l is maximal iff it is strictly maximal.

Exercise 6.3: Prove Proposition 6.3.

Exercise 6.4: Suppose that a field k admits a nontrivial discrete valuation. Show that k satisfies the hypothesis of Proposition 6.3b) and thus every maximal subfield l of a $A \in \mathrm{CSA}_k$ has $[l : k] = \deg A$.[19]

---

[18]It is common to elide this merely to "degree", and we will probably do so ourselves.

[19]Most fields "of number-theoretic interest" admit a nontrivial discrete valuation – e.g. a local field, a global field, a field which is finitely generated and nonalgebraic over some other field, and so forth – so in practice the distinction between maximal subfields and strictly maximal subfields is not to be worried about.

6.2. **Introduction to splitting fields.**

Let $A \in CSA_k$, and let l/k be a field extension. We say that l is a **splitting field** for A if $A_l = A \otimes_k l \cong M_{\deg A}(l)$.

Exercise 6.5: l is a splitting field for A iff $[A] \in \mathrm{Br}(l/k)$ iff $A_l \sim l$.

Exercise 6.6: If l is a splitting field for k and m is an extension of l then m is a splitting field for k.

Exercise 6.7: If l is algebraically closed, it is a splitting field for every $A \in \mathrm{CSA}_k$.

Exercise 6.8:
a) Show that if l is a splitting field for A, then there exists a subextension m of l/k which is finitely generated over k and which splits A.
b) Deduce that every $A \in \mathrm{CSA}_k$ admits a finite degree splitting field.

Example: For a quaternion algebra $B = \left(\frac{a,b}{k} \right)$, the maximal subfields are precisely the quadratic subfields l, and every such field is a splitting field for B, since B_l contains $l \otimes l \cong l^2$. The next result generalizes this to all CSAs.

Theorem 6.4. *For $A \in \mathrm{CSA}_k$ and l a subfield of A, TFAE:*
(i) l is strictly maximal: $[l:k] = \deg A$.
(ii) l is a splitting field for A.

Proof. Let $C = C_A(l)$, so that by Theorem 6.1 we have $C \in \mathrm{CSA}_l$ and $[l:k] \deg C = \deg A$. DCTe) gives $C \sim A \otimes l^{\mathrm{op}} = A \otimes l = A_l$. Therefore l is maximal iff $[l:k] = \deg A$ iff $\deg C = 1$ iff $C = l$ iff $A_l \sim l$ iff l is a splitting field for A. $\qquad\square$

Moreover, for a $A \in \mathrm{CSA}_k$, if we look at all field extensions l/k of degree equal to that of A, we find that the two concepts we have been studying coincide: l is a splitting field for A iff l is (up to k-algebra isomorphism) a subfield of A.

Theorem 6.5. *For $E \in \mathrm{CSA}_k$ and l/k such that $[l:k] = \deg E$, TFAE:*
(i) There exists a k-algebra map $\iota : l \to E$.
(ii) l is a splitting field for E.

Proof. Put $n = [l:k] = \deg E$.
(i) $\implies$ (ii): $\iota(l)$ is a maximal subfield of E, hence by Theorem 6.4,

$$E \otimes_k l \cong E \otimes_k \iota(l) \cong M_n(\iota(l)).$$

(ii) $\implies$ (i): Let $A = E \otimes M_n(k)$. Let $\rho : l \to M_n(k)$ be the left regular representation, so that $x \in l \mapsto 1 \otimes x$ embeds l as a subfield of A. By DCTb),

$$n[C_A(l):k] = [A:k] = n^4,$$

so $[C_A(l):k] = n^3$. By DCTe), $C_A(l) \sim M_n(E) \otimes l^{\mathrm{op}} \cong M_{n^2}(l) \sim l$. It follows that $C_A(l) \cong M_n(l)$, so we may write $C_a(l) = l \otimes C$ with $C \cong M_n(k)$. Let $B = C_A(C)$. Then $l \subset B$, and since $C \in \mathrm{CSA}_k$, by DCT also $B \in \mathrm{CSA}_k$. Since also $C = C_A(B)$, by DCTe) we find $k \sim C \sim A \otimes B^{\mathrm{op}}$ and thus $B \sim A \sim E$. Moreover, DCTb) shows $[B:k] = [A:k]/[C:k] = [E:k]$ and thus by Corollary 4.7, $B \cong E$. $\qquad\square$

Lemma 6.6. *Let $A \in \mathrm{CSA}_k$ with $\deg A = n$, and let l be a subfield of k with $[l : k] = d$. Put $C = C_A(l)$ and $a = \deg C$. TFAE:*
(i) l is a splitting field for A.
(ii) $C \cong M_a(l)$.
(iii) $A = X \otimes Y$ with $X \in \mathrm{CSA}_k$, $Y \cong M_a(k)$ and l strictly maximal in X.

Proof. (i) $\iff$ (ii): By DCTe), $A_l \sim C_l$, so l is a splitting field for A iff $C \sim l$. One checks easily that $[C : k] = [M_a(l)]$, so by Corollary 4.7, $C \sim l \iff C \cong M_a(l)$.
(ii) $\implies$ (iii): We have $C \cong M_a(l) \cong l \otimes M_a(k)$, with corresponding tensor product decomposition $C = l \otimes_k Y$, say (i.e., Y is the preimage of $1 \otimes M_a(k)$ under the above isomorphism). Let $X = C_A(Y)$. By DCT, $X \in \mathrm{CSA}_k$ and $A = X \otimes Y$. Since l commutes with Y, $l \subset X$, and DCTb) implies

$$[X : k] = \frac{(\deg A)^2}{a^2} = d^2,$$

so $\deg X = d$ and l is a maximal subfield of X.
(iii) $\implies$ (i): If (iii) holds l is a splitting field for X, and $A \cong X \otimes M_a(k) \sim X$, so l is also a splitting field for A. $\qquad\square$

Theorem 6.7. *For $A \in \mathrm{CSA}_k$ and l/k any finite degree extension field, TFAE:*
(i) l is a splitting field for A.
(ii) There exists $B \sim A$ such that l is a strictly maximal subfield of B.

Proof. (i) $\implies$ (ii) is immediate from Lemma 6.6" if l splits A then we may write $A = X \otimes Y$ with $X \sim A$ and l a strictly maximal subfield of X.
(ii) $\implies$ (i): By Theorem 6.4, every strictly maximal subfield of a CSA is a splitting field. $\qquad\square$

For $A \in \mathrm{CSA}_k$, we define the **cohomological index** $I_c(A)$ to be the greatest common divisor of all degrees $[l : k]$ as l ranges over finite degree field extensions of k which are splitting fields for A.

Theorem 6.8. *For any $A \in \mathrm{CSA}_k$, the Schur index $\mathrm{Ind}\, A$ is equal to the cohomological index $I_c(A)$. Moreover the cohomological index is* attained *in the sense that there is a splitting field l with $[l : k] = I_c(A)$.*

Proof. Step 1: We show that $\mathrm{Ind}\, A \mid I_c(A)$. Equivalently, we must show that for any finite degree splitting field l/k of A, we have $\mathrm{Ind}\, A \mid [l : k]$. By Theorem 6.7, there exists a CSA B with $B \sim A$ and such that l is a strictly maximal subfield of B. Suppose $A \cong M_a(D)$ and $B \cong M_b(A)$ with D a division algebra. Then $[l : k] = \deg B = ab \deg D = ab \, \mathrm{Ind}\, A$.
Step 2: Supposing again that $A \cong M_a(D)$, let l be a strictly maximal subfield of D. Thus l is a splitting field of D hence also of the Brauer equivalent algebra A and $[l : k] = \deg D = \mathrm{Ind}\, A$. Thus $I_c A \mid \mathrm{Ind}\, A$, and in view of Step 1 $I_c A = \mathrm{Ind}\, A$. Finally, l is therefore a splitting field of degree $I_c(A)$, showing that the cohomological index is attained. $\qquad\square$

Remark: The name "cohomological index" alludes to the identification of $\mathrm{Br}\, K$ with the Galois cohomology group $H^2(K, \mathbb{G}_m)$. For any commutative Galois module M and any Galois cohomology class $\eta \in H^i(K, M)$ with $i > 0$, we may define the **period** of η to be the order of η in this abelian group and the **index** of η to be the gcd of all finite degrees l/k of field extensions l/k such that restriction to L kills η. Then for $A \in \mathrm{CSA}_k$, the index of the corresponding cohomology class

$\eta_A \in H^2(K, \mathbb{G}_m)$ is precisely the cohomological index $I_c A$ as defined above. The fact that the cohomological index is "attained" is a special property of Brauer groups: it need not hold for arbitrary Galois cohomology groups. On the other hand, for all Galois cohomology classes η, we have that the period of eta divides the index of η and in particular the period of η is finite: $H^i(K, M)$ is a torsion abelian group. In the context of CSA's this translates to the following result, which unfortunately we will not be able to prove via our non-cohomological methods.

Theorem 6.9. *For any $A \in \mathrm{CSA}_k$, $A^{\otimes \mathrm{Ind}\, A} = A \otimes A \otimes \ldots \otimes A \sim k$. In particular the Brauer group of any field is a torsion abelian group.*

6.3. Existence of separable splitting fields.

In this section we will prove the key result that over any field k, any CSA admits a separable splitting field. Recall that we have already had need of this in our characterization of separable algebras over a field.

Lemma 6.10. *Let $D \in \mathrm{CSA}_k$ be a division algebra with $D \neq k$. Then there exists a subfield l of k such that l/k is separable and $l \neq k$.*

Proof. ([S-QF, Lemma 19.16])
Step 0: Choose any $\alpha \in D \setminus k$. Then the k-subalgebra $k[\alpha]$ is a proper algebraic field extension of k. We are done already unless k has characteristic $p > 0$, so let us assume this is the case.
Step 1: Consider the nontrivial extension $k[\alpha]/k$. As with any algebraic field extension, there exists a subextension l such that l/k is separable and $k[\alpha]/l$ is purely inseparable [FT, §6.4]. If $l \supsetneq k$ we are done, so we may assume that $k[x]/k$ is purely inseparable. Therefore $q = [k[\alpha] : k] = p^a$ for some $a \in \mathbb{Z}^+$ and $\alpha^q \in k$. Let $u = \alpha^{p^{a-1}}$, so $u^p \in k$ and $[k[u] : k] = p$. Consider conjugation by u as a k-algebra automorphism σ of D: $\sigma : x \in D \mapsto uxu^{-1}$. Clearly u has order p; in particular, since we are in characteristic p we have $u - 1 \neq 0$ and $(u-1)^p = 0$. Let r be the largest integer such that $(u-1)^r \neq 0$, so $1 \leq r < p$. Let $y \in D$ be such that $(\sigma - 1)^r y \neq 0$ and put

$$a = (\sigma - 1)^{r-1} y, \ b = (\sigma - 1)^r y.$$

Then

$$0 \neq b = \sigma(a) - a$$

and

$$\sigma(b) - b = (\sigma - 1)^{r+1} y = 0.$$

Let $c = b^{-1}a$. Then

$$\sigma(c) = \sigma(b)^{-1}\sigma(a) = b^{-1}(b + a) = c + 1,$$

Thus σ induces a nontrivial k-algebra automorphism on the (necessarily proper) field extension $k[c]/k$. It follows that $k[c]/k$ is not purely inseparable, so it contains a nontrivial separable subextension, qed. $\square$

Theorem 6.11. *Let $D \in \mathrm{CSA}_k$ be a division algebra.*
a) There exists a separable subfield l of D with $[l : k] = \deg D$.
b) For every $A \in \mathrm{CSA}_k$ there exists a finite degree Galois extension m/k such that m is a splitting field for A.

Proof. a) Let $m = \deg D$. Clearly we may assume $m > 1$. By Lemma 6.10, there exists a nontrivial separable subfield l of k. Of all separable subfields, choose one of maximal degree, say $[l : k] = a$. We wish to show that $a = m$, so seeking a contradiction we asume otherwise: $1 < a < m$. Let D' be the commuting algebra of l in A. By Theorem 6.1 we have $D' \in \mathrm{CSA}_l$ and

$$m = \deg D = [l : k] \deg D' = a \deg D'.$$

Since D is a finite-dimensional division algebra, so is its k-subalgebra D'. Since $a < m$, D' is a nontrivial central division algebra over l. Applying Lemma 6.10 again, there exists a nontrivial separable field extension m/l such that m is a subfield of D'. But then m is a separable subfield of D with $[m : k] = [m : l][l : k] > a$, contradicting the maximality of a).

b) Any $A \in \mathrm{CSA}_k$ if of the form $M_n(D)$ for a k-central division algebra D and a field extension l/k is a splitting field for A iff it's a splitting field for D, so we may assume without loss of generality that A is itself a division algebra. By part a) there exists a separable subfield l of D with $[l : k] = \deg D$, and by Theorem 6.4 any such subfield is a splitting field for D. Thus we have found a finite degree separable splitting field l for A. Since any field containing a splitting field is also a splitting field, to get a finite degree Galois splitting field m for A we need only take m to be the normal closure of l/k. $\qquad\qquad\square$

6.4. **Higher brow approaches to separable splitting fields.**

The argument that we gave for the existence of separable splitting fields is elementary but not overly conceptual. It would be nice to have a deeper understanding of this basic and important fact. In this section we briefly sketch several higher brow approaches.

6.4.1. *Severi-Brauer varieties.* It turns out that to every degree n CSA $A_{/k}$ one can naturally associate an $n - 1$-dimensional algebraic k-variety V_A such that:

(SB1) If $A_1 \cong A_2$ then $V_{A_1} \cong V_{A_2}$.
(SB2) $A \cong M_n(k) \iff V_A \cong \mathbb{P}^{n-1} \iff V_A(k) \neq \emptyset$.
(SB3) For any field extension l/k, $V_A \otimes_k l \cong V_{A_l}$.
(SB4) For any algebraically closed field k, $V_A \cong \mathbb{P}^{n-1}$.
(SB5) For any K-variety V such that $V \otimes_k \overline{k} \cong \mathbb{P}^{n-1}$, there exists a degree n CSA A/k such that $V \cong V_A$.

The variety V_A is called the **Severi-Brauer variety** of V. In summary, the Severi-Brauer variety of $A \in CSA_k$ is a variety which upon base extension to the algebraic closure of k becomes projective space of dimension one less than the degree of A: one says V_A is a **twisted form** of projective space. Conversely, every twisted form of projective space is the Severi-Brauer variety of some CSA. Moreover, the Brauer class of A is trivial iff V_A has a k-rational point. It follows that $\mathrm{Br}\, k = 0$ iff every twisted form of projective space has a k-rational point. But any twisted form of projective space is a smooth, projective geometrically integral variety, so certainly any field k for which $V(k) \neq \varnothing$ for every geometrically integral variety V has trivial Brauer group. Such fields are called **pseudoalgebraically closed** or **PAC** and are studied in a branch of mathematics called **Field Arithmetic**.

Thus, via the theory of Severi-Brauer varieties, the following fact implies that every CSA has a separable splitting field.

Theorem 6.12. *Any separably closed field is PAC.*

Proof. Let k be separably closed. It is enough to show that every geometrically intgral affine k-variety V has a k-rational point. To see this, we apply a strengthening of Noether's normalization theorem [E, Cor. 16.18]: since V is not just integral but geometrically integral, there is a polynomial subring $k[t_1, \ldots, t_n]$ of the affine coordinate ring $k[V]$ such that $k[V]$ is finitely generated as a $k[t_1, \ldots, t_n]$ and such that the extension of fraction fields $k(V)/k(t_1, \ldots, t_n)$ is *separable*. In more geometric language, there exists a finite, generically separable k-morphism $f : V \to \mathbb{A}^n$. From this it follows that there exists a nonempty Zariski-open subset U of $\mathbb{A}^n$ such that the restriction of f to the preimage of U is a **finite etale** morphism. Now take any k-rational point $P \in U$ (since k is separably closed, it is infinite, and thus any nonempty Zariski-open subset of affine space has infinitely many k-rational points). The previous incantations ensure that the fiber of f over P is a finite etale k-algebra, i.e., a finite product of separable field extensions of k. But since k is assumed separably closed, the fiber is isomorphic to k^d and thus the preimage consists of $\deg f$ k-rational points. $\square$

The explicit construction of the Severi-Brauer variety is relatively elementary: it is omitted here because of time limitations only. Note though that we have already seen it in an important special case: namely, if A has degree 2 – i.e., if A is a quaternion algebra, then the Severi-Brauer variety V_A is nothing else than the conic curve C given by the zero set of the ternary norm form n_0. (On the other hand, we *will* later define a norm form for any CSA, but it does not have a direct connection to the Severi-Brauer variety as in degree $d = 2$.)

6.4.2. *Cohomology.* One can similarly ask for a conceptual explanation for the connection between CSAs and twisted forms of projective space. This connection is provided by the machinery of Galois cohomology. Namely, since every CSA over k splits over k^{sep}, every CSA is a k^{sep}/k-twisted form of $M_n(k)$. By Skolem-Noether, the automorphism group of $M_n(k)$ is $\text{PGL}_n(k)$, so therefore the set of all degree n CSAs over k is parameterized by the Galois cohomology set $H^1(k, \text{PGL}_n)$. On the other hand, the Severi-Brauer varieties of CSAs over k are precisely the k^{sep}/k-twisted forms of projective space $\mathbb{P}^{n-1}$, and the automorphism group of $\mathbb{P}^{n-1}$ is indeed PGL_n. Therefore the degree n Severi-Brauer varieties are parameterized by the Galois cohomology set $H^1(k, \text{PGL}_n)$: this gives (albeit inexplicitly) the correspondence between CSAs and Severi-Brauer varieties!

To make this correspondence work, we have already used that every $\overline{k}/k$-twisted form of $M_n(k)$ becomes isomorphic to $M_n(k)$ over k^{sep} and similarly that every $\overline{k}/k$-twisted form of $\mathbb{P}^{n-1}$ becomes isomorphic to $\mathbb{P}^{n-1}$ over k^{sep}. What if we didn't know about the existence of separable splitting fields? We can still formalize this as a descent problem, but in a fancier way, using **flat cohomology**. That is, both central simple algebras of degree n and Severi-Brauer varieties of dimension $n-1$ are *a priori* are parameterized by $H^1_f(k, \text{PGL}_n)$. So the question is now why the flat cohomology group $H^1_f(k, \text{PGL}_n)$ can be replaced by the Galois cohomology group

$H^1(k, \mathrm{PGL}_n)$. It turns out that flat cohomology coincides with étale (or here, Galois) cohomology when the coefficient module is a **smooth group scheme**, which PGL_n indeed is. In other words, from a *very highbrow* standpoint, the existence of separable splitting fields comes from a property of the automorphism group scheme of the objects in question: whenever it is smooth, going up to k^{sep} is enough.

6.5. Separable algebras.

Theorem 6.13. *For a k-algebra R, TFAE:*
(i) $R \cong \prod_{i=1}^{r} M_{n_i}(D_i)$ such that for all $1 \leq i \leq r$, each D_i is a finite-dimensional division k-algebra and $l_i = Z(D_i)$ a finite separable field extension of k.
(ii) $R_{k^{\mathrm{sep}}}$ is isomorphic to a finite product of matrix algebras over k^{sep}.
(iii) $R_{\overline{k}}$ is semisimple.
(iv) For every algebraically closed extension field l/k, R_l is semisimple.
(v) For every extension field l/k, R_l is semisimple.
*An algebra satisfying these equivalent conditions is called a **separable k-algebra**.*

Proof. (i) $\implies$ (ii): Without loss of generality we may assume $r = 1$, i.e., $R \cong M_n(D)$ with $Z(D) = l$ a finite separable field extension of k. By Corollary 3.26, $R_{k^{\mathrm{sep}}}$ is a semisimple k-algebra. By Proposition 4.3, its center is $Z(R) \otimes_k k^{\mathrm{sep}} = l \otimes_k k^{\mathrm{sep}} \cong \prod_{i=1}^{[l:k]} k^{\mathrm{sep}}$. Thus $R_{k^{\mathrm{sep}}}$ is isomorphic to a product of $[l : k]$ CSA's over k^{sep}, and since the Brauer group of a separably closed field is trivial, this means $R_{k^{\mathrm{sep}}}$ is isomorphic to a product of matrix algebras over k^{sep}.
(ii) $\implies$ (iii): If $R_{k^{\mathrm{sep}}} \cong \prod_{i=1}^{s} M_{n_i}(k^{\mathrm{sep}})$ then

$$R_{\overline{k}} \cong R_{k^{\mathrm{sep}}} \otimes_{k^{\mathrm{sep}}} \overline{k} \cong \prod_{i=1}^{s} M_{n_i}(\overline{k})$$

is semisimple.
(iii) $\implies$ (iv): Indeed the above argument shows that if $R_{\overline{k}}$ is semisimple, then so is R_l for any field extension l containing $\overline{k}$, and the desired implication is a special case of this.
(iv) $\implies$ (v): Let l be an arbitrary field extension of k and $\overline{l}$ it slgebraic closure, so $R_{\overline{l}}$ is semisimple by hypothesis. Then R_l is semisimple by Theorem 3.24b).
(v) $\implies$ (i): We will prove the contrapositive. Suppose $R \cong M_n(D) \times R'$, where $Z(D) = l/k$ is an inseparable field extension. Let m/k be the normal closure of l/k. Then $Z(M_n(D)_m) = l \otimes_k m$ has nonzero nilpotent elements, and the ideal generated by a central nilpotent element is a nilpotent ideal, so $M_n(D)_m$ is not semisimple and thus neither is R_m. $\square$

Exercise 6.9: a) Let R/k be a separable algebra, and let l/k be a field extension. Shw that $R_{/l}$ is separable.
b) Let A and B be separable k-algebras. Show that $A \otimes_k B$ is a separable k-algebra.

6.6. Crossed products. A CSA $A_{/k}$ is a **crossed product** if it admits a strictly maximal subfield l such that l/k is Galois.

Exercise 6.10: Show: every CSA is Brauer equivalent to a crossed product.

The previous exercise is the key to the cohomological interpretation of the Brauer group. It is also the archetypical example of a question about CSAs which is much easier if it is asked only up to Brauer equivalence. It is another matter entirely

to tell whether a given CSA – e.g. a division algebra – is a crossed product. One of the major questions in the entire subject is for which positive integers $n \in \mathbb{Z}^+$ every degree n division algebra is a crossed-product. Here is what is known:

Theorem 6.14. *a) Every division algebra of degree dividing* 6 *is cyclic.*
b) Every division algebra of degree 4 *is a crossed product algebra.*
c) If n is divisible by 8 *or by the square of an odd prime, then there exists a field K and a degree n division algebra $D_{/K}$ which is not a crossed product algebra.*

Proof. Part a) is due to Albert, Dickson and Wedderburn: see [P, Ch. 15] for a proof. Part b) due to Albert [Al29]. Part c) is due to Amitsur [Am72]. $\square$

To the best of my knowledge, all other cases are open. In particular, for no prime number $p \geq 5$ is it known whether every division algebra of degree p is a crossed product algebra! This is a dramatic example of the theory of division algebras being harder than the theory of CSAs up to Brauer equivalence.

6.7. **The Brauer Group of a Finite Field (I).**

We now give our first proof of the following celebrated theorem of Wedderburn.

Theorem 6.15. *(Wedderburn's Little Theorem)*
a) A finite division ring is a field.
b) The Brauer group of a finite field is zero.

Proof. a) Let D be a finite division ring. Then the center of D is a finite field, say $\mathbb{F}$, and $D \in \mathrm{CSA}_{\mathbb{F}}$. Put $a = \deg D$. From our theory of subfields of division algebras, we know that D admits a subfield $l/\mathbb{F}$ with $[l : \mathbb{F}] = a = \deg D$, i.e., a maximal subfield. But the finite field $\mathbb{F}$ admits a unique (up to $\mathbb{F}$-algebra isomorphism) finite extension of any given degree, so all maximal subfields of D are isomorphic to l. By Skolem-Noether, it follows that all maximal subfields of D are conjugate. Since every element of D lies in a maximal subfield, we conclude

$$(12) \qquad D^{\times} = \bigcup_{x \in D^{\times}} x l^{\times} x^{-1}.$$

Further, if $N = \{x \in D^{\times} \mid x l^{\times} x^{-1} = l^{\times}\}$ is the normalizer of $l^{\times}$ in $D^{\times}$, by the Orbit-Stablizer Theorem the number of maximal subfields of D equals $m = [D^{\times} : N]$. From (12) we get that $D^{\times}$ is a union of m conjugates of $l^{\times}$. If $m > 1$, the union is not disjoint since each conjugate contains 1, and so $m > 1$ implies

$$\#D^{\times} < [D^{\times} : N] \# l^{\times} < [D^{\times} : l^{\times}] \# l^{\times} < \#D^{\times},$$

a contradiction. Therefore $m = 1$ so $D = l$ is commutative.
b) For any field k, every finite-dimensional division algebra over k is commutative iff for all finite extensions l/k every finite-dimensional l-central division algebra is commutative iff for all finite extensions l/k we have $\mathrm{Br}(l) = 0$. $\square$

The name "Wedderburn's Little Theorem" is informal but somewhat traditional: certainly it is of a lesser stature than the Wedderburn theory of semisimple algebras (most things are). Perhaps it also alludes to the rough restatement "A little division algebra is a field." In any case, the result is not trivial: elementary proofs are possible but are, to my taste, involved and contrived.

On the other hand it is possible to prove the theorem in many different ways.

The above proof is very much in the style of arguments in finite group theory involving the "class equation". If I may be so bold, one way to measure the value of a proof of Wedderburn's Little Theorem is by seeing what information it yields about Brauer groups of infinite fields. The above proof gives absolutely nothing, except what follows formally from the theorem itself. Later we will show that a field has vanishing Brauer group if it is quasi-algebraically closed – i.e., if any homogeneous degree d polynomial in n variables with $n > d$ has a nontrivial 0. This applies to finite fields by the Chevalley-Warning Theorem, but also to many infinite fields.

Exercise 6.11 (a mild generalization of Wedderburn's Little Theorem):
a) Let D be a division algebra with center k of positive characteristic which is *absolutely algebraic*: that is, every $x \in D$ satisfies a nonzero polynomial $f \in \mathbb{F}_p[t]$. Show that D is commutative.
b) Deduce that for any algebraic extension k of $\mathbb{F}_p$, $\mathrm{Br}(k) = 0$.
c) Show in fact that if for a field k, $\mathrm{Br}(l) = 0$ for all finite extensions of k, then $\mathrm{Br}(l) = 0$ for all algebraic extensions of k.

Exercise 6.12: Let D be a division ring with center k of characteristic $p > 0$. Let $G \subset D^\times$ be a finite subgroup. Show that G is cyclic.

Remark: It is a well-known undergraduate level result that any finite subgroup of the multiplicative group of a field is cyclic (it is especially well-known that for a finite field $\mathbb{F}$, $\mathbb{F}^\times$ is a cyclic group, and the previous exercise relies on this). However finite subgroups of division algebras in characteristic 0 need not be cyclic or even abelian: the natural counterexample is the quaternion group of order 8 inside the Hamiltonian quaternions. The full classification of finite subgroups of division rings was attained by S. Amitsur and is a significant work. As a rule of thumb, division algebras in characteristic 0 tend to be more complicated and interesting than division algebras in positive characteristic.

6.8. The Brauer Group of $\mathbb{R}$.

Theorem 6.16. *The Brauer group of $\mathbb{R}$ has order 2, the nontrivial element being given by the Hamiltonian quaternions $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}} \right)$.*

Proof. Let $D \in \mathrm{CSA}_\mathbb{R}$ be a division algebra, and put $d = \deg D$. Then there exists a subfield l of D with $[l : \mathbb{R}] = d$, and it follows that $d = 1$ or $d = 2$. Clearly $d = 1 \iff D = \mathbb{R}$, whereas by Theorem 5.5, $d = 2 \iff [D : k] = 4 \iff D \cong \left(\frac{a,b}{\mathbb{R}} \right)$ is a quaternion algebra over $\mathbb{R}$. But the isomorphism class of $\left(\frac{a,b}{\mathbb{R}} \right)$ depends only on the square classes of a and b and a quaternion algebra is split iff either a or b is a square, the only possibility for a division quaternion algebra over $\mathbb{R}$ is when a and b are both negative, hence congruent modulo squares to $a = b = -1$. $\square$

Exercise 6.13: Show: the conclusion of Theorem 6.16 holds for any real-closed field.

Remark: One might try to look for other fields k for which $[\overline{k} : k] = d < \infty$, for then the same argument as above shows that the degree of any central division algebra over k is at most d. However, there is a remarkable theorem of Artin-Schreier classifying fields k with $d < \infty$ as above: it consists precisely of the algebraically closed

fields ($d = 1$) and the fields for which $d = 2$, which are moreover uniquely orderable and have $\overline{k} = k(\sqrt{-1})$: i.e., they are real-closed. Thus we don't get anything more than we have already seen.

Remark: Sometimes one sees a classification of finite-dimensional division algebras over $\mathbb{R}$ which includes the **octonions** $\mathbb{O}$, an eight-dimensional *non-associative* $\mathbb{R}$-algebra which is a division algebra in the slightly generalized sense that for all $x \in \mathbb{O}^\bullet$, left multiplication and right multiplication by x are both $\mathbb{R}$-isomorphisms of $\mathbb{O}$. Such algebras lie outside the scope of our philosophy here, but they have a lot in common with quaternion algebras in that they are both composition algebras. Indeed, the composition algebras over a field k are precisely k itself, the separable quadratic algebras, the quaternion algebras, and the octonion algebras.

6.9. **Biquaternion Algebras.**

A **biquaternion algebra** over a field k is a CSA $A_{/k}$ which is isomorphic to the tensor product of two quaternion algebras. Division biquaternion algebras are arguably the simplest (and certainly historically the first) central simple algebras satifying certain properties, e.g. having index strictly larger than their period.

In §5 we only considered quaternion algebras away from characteristic 2, so the same hypothesis will be made on k in our study of biquaternion algebras over k. With that proviso, every biquaternion algebra is (up to isomorphism) of the form

$$A = B_1 \otimes B_2 = \left(\frac{a, b}{k} \right) \otimes \left(\frac{c, d}{k} \right)$$

for $a, b, c, d \in k^\times$. The main goal in this section is to compute the Schur index Ind A in terms of a, b, c, d. Since deg $A = 4$ the three possibilities are:

Case I. $A \cong M_2(k)$.
Case II. $A \cong M_2(B_3)$, where B_3 is a division quaternion algebra.
Case III. A is a division algebra.

It is clear that I. holds iff $B_1 \cong B_2^{\mathrm{op}} \iff B_1 \cong B_2$. We have already discussed isomorphism of quaternion algebras in §5: especially, it is necessary and sufficient that their ternary norm forms n_{0,B_1} and n_{0,B_2} be isomorphic. We consider this to be a satisfactory characterization of when Case I. occurs.

Let $A = B_1 \otimes B_2$ be a biquaternion algebra. Since $B_1 \otimes B_1^{\mathrm{op}}$ and $B_2 \cong B_2^{\mathrm{op}}$, $(B_1 \otimes B_2)^{\mathrm{op}} \cong B_1^{\mathrm{op}} \otimes B_2^{\mathrm{op}} \cong B_1 \otimes B_2$, i.e., $A \cong A^{\mathrm{op}}$. A better way to see this is to recall that a CSA A is isomorphic to its opposite algebra A^{op} iff $[A]$ has order at most 2 in the Brauer group, and in any multiplicative abelian group, the product of two elements of order at most 2 again has order at most 2. Recall also that a nice way for an algebra to be isomorphic to its opposite algebra is for it to admit an involution, and indeed A admits involutions. In fact, taking the canonical involutions on B_1 and B_2 determines an involution on A, given by

$$\iota(x \otimes y) := \overline{x} \otimes \overline{y}.$$

(This involution on A is *not* canonical: it depends upon the chosen decomposition into a tensor product of quaternion algebras. But we can still put it to good use.)

Exercise 6.14: Let V be a vector space over a field k of characteristic different from 2, and let ι be an automorphism of V such that $\iota^2 = 1_V$. Let V^+ be the **+1 eigenspace** for ι, i.e., the set of all $v \in V$ such that $\iota v = v$, and let V^- be the **-1 eigenspace** for ι, i.e., the set of all $v \in V$ such that $\iota v = -v$. Show that $V = V^+ \oplus V^-$.

Lemma 6.17. *Consider the involution ι acting on the 16-dimensional k-vector space $A = B_1 \otimes B_2$. Then*

$$A^+ = k \cdot 1 \oplus (B_1^- \otimes B_2^-), \ A^- = (B_1^- \otimes k) \oplus (k \otimes B_1^-).$$

Proof. It is immediate to see that the subspace $k \cdot 1 \oplus (B_1^- \otimes B_2^-)$, of dimension 10, is contained in A^+ and that the subspace $(B_1^- \otimes k) \oplus (k \otimes B_1^-)$, of dimension 6, is contained in A^-. We have therefore accounted for all 16-dimensions of A so we must have found the full $+1$ and -1 eigenspaces for ι. $\square$

Lemma 6.18. *Let B_1 and B_2 be two quaternion algebras over k. TFAE:*
(i) There exist $a, b, b' \in k^\times$ such that $B_1 \cong \left(\frac{a,b}{k}\right)$ and $B_2 \cong \left(\frac{a,b'}{k}\right)$.
(ii) B_1 and B_2 have a common quadratic subfield.
(iii) B_1 and B_2 have a common quadratic splitting field.
*When these conditions hold, we say that B_1 and B_2 **have a common slot**.*

We will show that $A = B_1 \otimes B_2$ is a division algebra iff B_1 and B_2 *do not have* a common slot iff the **Albert form** – a certain sextenary quadratic form built from B_1 and B_2 – is isotropic over k. It follows that when B_1 and B_2 do have a common slot, we must have $A \cong M_2(B_3)$, and we will determine the quaternion algebra B_3 in terms of B_1 and B_2.

Theorem 6.19. *a) For all $a, b, b' \in k^\times$, we have*

$$A := \left(\frac{a,b}{k}\right) \otimes \left(\frac{a,b'}{k}\right) \cong \left(\frac{a,bb'}{k}\right) \otimes M_2(k).$$

b) In particular, the tensor product of any two quaternion algebras with a common slot is Brauer equivalent to another quaternion algebra.

Proof. a) The following pleasantly lowbrow proof is taken from [GS, Lemma 1.5.2]. Let $(1, i, j, ij)$ and $(1, i', j', i'j')$ denote the standard quaternionic bases of $\left(\frac{a,b}{k}\right)$, $\left(\frac{a,b'}{k}\right)$, respectively. Consider the following explicit k-subspaces of A:

$$B_3 = k(1 \otimes 1) \oplus k(i \otimes 1) \oplus k(j \otimes j') \oplus k(ij \otimes j'),$$

$$B_4 = k(1 \otimes 1) \oplus k(1 \otimes j') \oplus k(i \otimes i'j') \oplus k((-b'i) \otimes i').$$

One checks that B_3 and B_4 are closed under multiplication and thus k-subalgebras of A. Moreover B_3 and B_4 are commuting subalgebras of A, so there is an induced k-algebra map from the 16-dimensional CSA $B_1 \otimes B_2$ to the 16-dimensional CSA A: such a map is necessarily an isomorphism.[20] Moreover, putting $I_1 = i \otimes 1$ and

---

[20]Or: one can easily check that all 16 standard basis elements of A lie in the image of the map.

$J_1 = j \otimes j'$ one finds that $I_1^2 = a$, $J_1^2 = bb'$ and $I_1 J_1 = -J_1 I_1$, so that

$$B_3 \cong \left(\frac{a, bb'}{k} \right).$$

Similarly we find

$$B_4 \cong \left(\frac{b', -a^2 b'}{k} \right) \cong \left(\frac{b', -b'}{k} \right) \cong M_2(k),$$

the last isomorphism coming from the fact that the ternary norm form of $\left(\frac{b', -b'}{k} \right)$ is $b' x^2 - b' y^2 + (b')^2 z^2 = 0$, which is visibly isotropic: take $(x, y, z) = (1, 1, 0)$. Part b) follows immediately. $\square$

Theorem 6.20. *(Albert) For $A = B_1 \otimes B_2$, TFAE:*
(i) B_1, B_2 have a common slot: $\exists a, b, b' \in k$ such that $B_1 \cong \left(\frac{a, b}{k} \right)$ and $B_2 \cong \left(\frac{a, b'}{k} \right)$.
*(ii) The **Albert form***

$$\varphi(x, y) = \varphi(x_1, x_2, x_3, y_1, y_2, y_3) = n_{0, B_1}(x) - n_{0, B_2}(y)$$

is isotropic over k.
(iii) A is not a division algebra.

Proof. (i) $\implies$ (ii): Assume (i). Then by Lemma 6.18 there exists $x \in B_1^-$ and $y \in B_2^-$ such that $-n(x) = x^2 = a = y^2 = -n(y)$ and thus $\varphi(x, y) = 0$.
(ii) $\implies$ (iii): Suppose there exists $x \in B_1^-$, $y \in B_2^-$, not both zero, such that $\varphi(x, y) = 0$. Note that x and y commute, and thus

$$0 = \varphi(x, y) = y^2 - x^2 = (y + x)(y - x).$$

If A were a division algebra we could deduce $y = \pm x$, an obvious contradiction since $B_1^- \cap B_2^- = 0$, and thus A is not a division algebra.
$\neg$ (i) $\implies$ $\neg$ (iii): we assume (c.f. Lemma 6.18) that B_1 and B_2 admit no common quadratic subfield and show that A is division.
Step 0: Notice that the hypothesis implies that both B_1 and B_2 are division: indeed, if say $B_1 \cong M_2(k)$, then every quadratic extension l/k is a subfield of B_1, so every quadratic subfield of B_2 gives a common slot for B_1 and B_2.
Step 1: Choose quadratic subfields l_1 of B_1 and l_2 of B_2. By Step 0 and our hypothesis, $(B_1)_{l_2}$ and $(B_2)_{l_1}$ are both division subalgebras of A. Our general strategy is as follows: by Lemma 1.1 it is enough to show that for all $\alpha \in A^\bullet$, α is *left*-invertible, and observe that for any element α in any ring R, if there exists $\beta \in R$ such that $\beta \alpha$ is left-invertible, so then is α. Thus it suffices to find for all $\alpha \in A^\bullet$ an element $\alpha^* \in A$ such that $\alpha^* \alpha$ is a nonzero element of either the division subalgebra $(B_1)_{l_2}$ or the division sualgebra $(B_2)_{l_1}$.
Step 2: Write $l_2 = k(j)$ and complete this to a quaternionic basis i, j for B_2. Since $A = B_1 \otimes B_2$, for all $\alpha \in A^\bullet$ there exist unique $\beta_1, \beta_2, \beta_3, \beta_4 \in B_1$ such that

$$\alpha = (\beta_1 + \beta_2)j + (\beta_3 + b_4 j)ij.$$

Put $\gamma = \beta_3 + \beta_4 j$. We may assume that $\gamma \neq 0$, for otherwise $\alpha = (\beta_1 + \beta_2)j$ lies in the division algebra $(B_1)_{l_2}$. Thus γ^{-1} exists in $(B_1)_{l_2}$. As in Step 1 it is enough to show that $\gamma^{-1}\alpha$ is left-invertible, which reduces us to the case

$$\alpha = \beta_1 + \beta_2 j + ij.$$

If β_1 and β_2 commute then $k(\beta_1, \beta_2)$ is contained in a quadratic subfield l_1 of Q_1 and thus $\alpha \in (B_2)_{l_1}$: okay. So we may assume that $\beta_1\beta_2 - \beta_2\beta_1 \neq 0$ and then we – magically? – take
$$\alpha^* = \beta_1 - \beta_2 j - ij.$$
Using the facts that $ij \in B_2$ commutes with $\beta_1, \beta_2 \in B_1$, we calculate
$$\alpha^*\alpha = (\beta_1 - \beta_2 j - ij)(\beta_1 + \beta_2 j + ij) = (\beta_1 - \beta_2 j)(\beta_1 + \beta_2 j) - (ij)^2$$
$$= \left(\beta_1^2 - \beta_2^2 j^2 - (ij)^2\right) + (\beta_1\beta_2 - \beta_2\beta_1)j.$$
The parenthesized term on the right hand side lies in B_1 and thus the entire expression lies in $(B_1)_{l_2}$. Moreover $j \notin B_1$ and by assumption the coefficient of j is nonzero, so $\alpha^*\alpha \neq 0$. Done! $\square$

A field k is said to be **linked** if any two quaternion algebras over k have a common slot. By the above results there are many equivalent ways to restate this: a field is linked iff the classes of quaternion algebras form a subgroup of the Brauer group of k iff there is no division biquaternion algebra iff every Albert form is isotropic. We immediately deduce:

Corollary 6.21. *Let k be a field of u-invariant at most 4, i.e., for which every quadratic form in more than 4 variables over k is isotropic. Then there are no division biquaternion algebras over k.*

Remark: The reader who is not very familiar with the algebraic theory of quadratic forms should be asking why Corollary 6.21 was not stated with the hypothesis that k is a field of u-invariant at most 5, since this would clearly also be sufficient to force all Albert forms to be isotropic. The answer is that that there are in fact no fields of u-invariant 5, so the extra generality is illusory.

Example: The hypothesis of Corollary 6.21 apply to any $C_2(2)$ field. Recall that for non-negative integers r and d, a field is $C_r(d)$ if every homogeneous form of degree d in more than d^r variables has a nontrivial zero, and a field is C_r if it is $C_r(d)$ for all d. By a theorem of Lang-Nagata, a field of transcendence degree at most one over a C_1 field is C_2 and thus by Tsen's theorem a field of transcendence degree at most 2 over an algebraically closed field is C_2. In particular the rational function field $\mathbb{C}(a, b)$ in two independent indeterminates is C_2, hence has u-invariant at most 4, hence is linked.

Example: If K is a Henselian discretely valued field with perfect residue field k, then $u(K) = 2u(k)$. In particular if the residue field k is a C_1-field then $u(k) \leq 2$ so $u(K) \leq 4$ and K is a linked field. By the Chevalley-Warning Theorem finite fields are C_1, and therefore any p-adic field or Laurent series field over a finite field is a linked field.

Example: We claim that any global field is a linked field. We recall the celebrated Hasse-Minkowski theorem: a quadratic form over a global field K is isotropic iff its extension to K_v is isotropic for all places v of K. If K is a global function field then all places v are finite and thus for all v the Laurent series field with finite residue field K_v has u-invariant 4, which by Hasse-Minkowski implies that K has u-invariant 4 and thus is linked. For number fields we must also consider the Archimedean places v: for every complex place v, $K_v \cong \mathbb{C}$ which has u-invariant 1.

However for a real place v, $K_v \cong \mathbb{R}$ which admits anistropic forms in any number of variables. However, a diagonal quadratic form is anisotropic over $\mathbb{R}$ iff its coefficients are either all positive or all negative. It is now time to look explicitly at the Albert form of $A = \left(\frac{a,b}{k}\right) \otimes \left(\frac{c,d}{k}\right)$:

$$\varphi(x_1, x_2, x_3, x_4, x_5, x_6) = ax_1^2 + bx_2^2 - abx_3^2 - cx_4^2 - dx_5^2 + cdx_6^2 = 0.$$

From this we see immediately that no matter how a, b, c, d are chosen in any ordered field k, there are always terms both of positive and negative sign, In particular Albert form is isotropic over K_v for all real places v of K. Let us record some of what we have shown:

Theorem 6.22. *No local or global field admits a division biquaternion algebra.*

Theorem 6.23. *Let K be any field of characteristic different from 2. Then the **generic biquaternion algebra** over K is a division algebra. That is, let a, b, c, d be independent indeterminates over K and put $k = K(a, b, c, d)$. Then*

$$A = \left(\frac{a,b}{k}\right) \otimes \left(\frac{c,d}{k}\right)$$

is a division k-algebra.

Proof. By Theorem 6.20 it suffices to show that the Albert form

$$\varphi(x) = ax_1^2 + bx_2^2 - abx_3^2 - cx_4^2 - dx_5^2 + cdx_6^2 = 0$$

is anisotropic over $k = K(a, b, c, d)$. Seeking a contradiction, we suppose there exists $x = (x_1, x_2, x_3, x_4, x_5, x_6) \in k^6 \setminus \{0\}$ such that $\varphi(x) = 0$. Let R be the UFD $K[a, b, c, d]$. By rescaling the coordinates of x we may assume $x \in R^6$ is **primitive**.
Step 1: Observe that x_1, x_2, x_3, x_4 cannot all be divisible by d, for if so $d^2 \mid (dx_5^2 - cdx_6^2)$ and thus $d \mid x_5^2 - cx_6^2$. Then consider the images $\overline{x_5}$ and $\overline{x_6}$ of x_5 and x_6 in the quotient ring $R_1 : R/(d) \cong K[a, b, c]$: by assumption, they are not both zero and satisfy the equation $\overline{x_5}^2 - c\overline{x_6}^2 = 0$, implying that c is a square in $K(a, b, c)$, which it isn't.
Step 2: Consider now the homomorphic image of the equation in the quotient ring R_1: there exists $y = (y_1, y_2, y_3, y_4) \in K[a, b, c]^4$, not all zero, such that

$$ay_1^2 + by_2^2 - aby_3^2 - cy_4^2 = 0,$$

and again we may assume that y is a primitive vector. Now y_1, y_2, y_3 cannot all be divisible by c, since then c^2 would divide $ay_1^2 + by_2^2 - aby_3^2 = cy_4^4$, which implies c divides y_4.
Step 3: Consider now the homomophic image of the equation in the quotient ring $R_2 = R_1/(c) \cong K[a, b]$: we get

$$az_1^2 + bz_2^3 - abz_3^2 = 0.$$

But this is precisely the ternary norm form associated to the generic quaternion algebra $\left(\frac{a,b}{k}\right)$ which by Theorem 5.12 is anisotropic. This gives a contradiction which shows that φ is anisotropic. $\square$

Remark: Comparing Theorems 5.12 and 6.23, it is natural to wonder whether for all n the "generic n-quaternion algebra over k" – i.e., a tensor product of n quaternion algebras all of whose entries are independent indeterminates over k – is a division algebra. This is indeed the case, but to the best of my knowledge it is not possible

to prove this using quadratic forms arguments. Indeed for a tensor product of more than 2 quaternion algebras there is – so far as I'm aware! – no associated quadratic form whose anisotropy is equivalent to the algebra being division. On the other hand for *every* CSA A over every field k there is a "norm form" which is anisotropic iff the algebra is division. But in general the norm form is a homogeneous polynomial of degree equal to $\deg A$. Thus that the Albert form exists at all seems somewhat miraculous in light of the more general theory.

6.10. **Notes.**

Much of this section is taken directly from [P, Ch. 13], the major exception being §6.4, where we have broken form a bit to talk about results of a more arithmetic geometric nature. The characterization of separable algebras given in §6.5 is surprisingly hard to find in the literature (though the experts know it, of course).

The basic theory of biquaternion algebras of §6.9 is due to Albert.[21] Our proof of Theorem 6.20 follows Gille and Szamuely [GS] which follows T.-Y. Lam [L-QF], which follows Albert! I believe the term "linked field" is also due to Lam, and it comes up in *loc. cit.*. There is more material on C_1 fields, including the theorems of Tsen and Chevalley-Warning, in the next section: it is slightly out of sequence to mention them here, but it was approximately at this point in the lectures that I discussed biquaternion algebras, so I decided to preserve that order.

It is very embarrassing that I forgot to mention Merkurjev's theorem that over a field of characteristic different from 2, every central simple algebra of period 2 is Brauer equivalent to a tensor product of quaternion algebras. (But I did.)

7. Central Simple Algebras III: the reduced trace and reduced norm

7.1. **The reduced characteristic polynomial of a CSA.**

Let $A \in \mathrm{CSA}_k$, and let l/k be an extension field. A k-algebra homomorphism $\rho : A \to M_n(l)$ is called an **l-representation of A of degree n**. By the universal property of the tensor product of algebras, there is a unique extension $\rho_l : A_l \to M_n(l)$. Especially, if $n = \deg A$, then ρ_l must be an isomorphism, and thus an l-representation of degree $\deg A$ exists iff l is a splitting field for A.

Let $A \in \mathrm{CSA}_k$ with $\deg A = n$. For $a \in A$, we define the **reduced characteristic polynomial** $p_a(t)$ to be the characteristic polynomial of the matrix $\rho_l(a) \in M_n(l)$ for any degree n l-representation ρ of A. This is well-defined, because as above any other l-representation ρ' induces an l-algebra embedding $\rho_l : A_l \to M_n(l)$, and by Skolem-Noether any two such embeddings are conjugate by an element of $M_n(l)^\times$, i.e., the matrices $\rho'_l(a)$ and $\rho_l(a)$ are similar and thus have the same characteristic polynomial. But actually we claim more: the coefficients of $p_a(t)$ lie in k. To see this, choose a finite Galois extension l/k which is a splitting field for A, and let $\sigma \in G = \mathrm{Aut}(l/k)$. Then $x \in A$ is identified with $x \otimes 1$ in A_l, so that the natural G-action on A_l given by $\sigma(x \otimes y) = x \otimes \sigma(y)$ is such that $A \subset A_l^G$. On the other hand, for any $a \in A_l$ and $\sigma \in G$, the characteristic polynomial of $\rho_l(\sigma a)$ is $\sigma p_a(t)$.

---

[21]Abraham Adrian Albert, 1905-1972: he is perhaps one of the greatest mathematicians that most other mathematicians have never heard of.

It follows that for all $x \in A$, $p_a(t) \in l[t]^G = k[t]$.

Remark: This argument comes down to the fact that for any Galois extension of fields l/k with automorphism group G, $l^G = k$, which is of course a characteristic property of Galois extensions. We then apply this coefficient by coefficient to get $l[t]^G = k[t]$. We also used that for *any* field extension l/k, if V is a k-vector space then $V_l = V \otimes_k l$ has a natural $G = \operatorname{Aut}(l/k)$-action given by $\sigma(x \otimes y) = x \otimes \sigma(y)$, and then $V \subset V_l^G$. Having come this far we may as well record the more general principle at work here.

Proposition 7.1. *(Galois Descent for Vector Spaces) Let l/k be a Galois extension with $G = \operatorname{Aut}(l/k)$ and let V be a k-vector space. Then G acts naturally on $V \otimes_k l$ via $\sigma(x \otimes y) = x \otimes \sigma(y)$. Moreover we have*

$$(V \otimes_k l)^G = V.$$

Proof. See e.g. [C-GD, Thm. 2.14]. $\square$

Exercise: Let $A_{/k}$ be any finite-dimensional (associative, unital) algebra. For $a \in A$, the **unreduced characteristic polynomial** $P_a(t) \in k[t]$ is the characteristic polynomial of $a\bullet \in \operatorname{End}_k A$.
a) Show: if $A \in \operatorname{CSA}_{/k}$, then for all $a \in A$,

$$P_a(t) = p_a(t)^{\deg A} = p_a(t)^{\sqrt{\dim A}}.$$

b) Explain why part a) completely determines the reduced characteristic polynomial $p_a(t)$ and also why we did not take this as the definition.

Exercise 7.0: Let $A \in \operatorname{CSA}_{/k}$, and let l/k be any field extension. Let $a \in A$. Show that the reduced characteristic polynomial of a is equal to the reduced characteirstic polynmial of $a \otimes 1 \in A_{/l}$.

Although all the coefficients of the characteristic polynomial $P(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_0$ of a matrix M are important, especially important are $-a_{n-1}$, the **trace** of M and $(-1)^n a_0$, the **determinant** of M. For $a \in A$ with reduced characteristic polynomial $P(t)$, we define the **reduced trace** $t(a)$ of $a \in A$ as $-a_{n-1}$ and the **reduced norm** $n(a)$ of $a \in A$ as $(-1)^n a_0$.

Exercise 7.1: Show that for all $a \in A$, $p_a(a) = 0$.

Exercise 7.2: Let $A \in \operatorname{CSA}_k$.
a) Show that the reduced trace $t : A \to k$ is a k-linear map.
b) Show that the reduced norm $n : A \to k$ is multiplicative: for all $x, y \in A$, $n(xy) = n(x)n(y)$.

For any finite-dimensional k-algebra $A_{/k}$, the left regular representation $A \hookrightarrow M_{[A:k]}(k)$ allows us to define a trace and norm: namely the trace and determinant of the linear operator $a\bullet$ on A. Let us call these quantities $T(a)$ and $N(a)$.

Proposition 7.2. *Let $A \in \operatorname{CSA}_k$ with $\deg A = n$. For any $a \in A$, we have*

$$T(a) = n \cdot t(a), \quad N(a) = n(a)^n.$$

Proof. If the desired identities hold after extending the base to any field extension l/k, then they also hold over k, so by taking l to be a splitting field we reduce to the case of $A_l \cong M_n(l)$. Now as we know, the unique simple left $M_n(l)$-module up to isomorphism is $V = l^n$ and $M_n(l)$ as a left $M_n(l)$-module is isomorphic to V^n. More concretely, the matrix representation of $a\bullet$ on V^n is simply a block diagonal matrix containing n copies of the matrix a. From this description it is clear that the trace of $a\bullet$ is precisely n times the trace of a and that the determinant of $a\bullet$ is precisely the nth power of $\det(a)$. $\qquad\square$

Exercise: Prove Proposition 7.2 using the unreduced characteristic polynomial.

The reduced trace and the full trace are two k-linear forms on A such that the latter is precisely $n \cdot 1$ times the former. When n is not divisible by the characteristic of k, this is a harmless difference and one could certainly use either the reduced trace or the full trace for any given purpose. However, when n is divisible by the characteristic of k the full algebra trace is identically zero, whereas the reduced trace is always surjective.

Exercise 7.3: Show that for any $A \in \mathrm{CSA}_k$, the quadratic form $x \in A \mapsto t(x^2)$ is nondegenerate. (Hint: reduce to the case of a matrix ring.)

7.2. Detecting division algebras via the reduced norm.

Theorem 7.3. *Let $A \in \mathrm{CSA}_k$ with $\deg A = n$.*
a) For $x \in A$, TFAE:
(i) $x \in A^\times$.
(ii) $n(x) \in k^\times$.
*b) A is a division algebra iff the reduced norm is **anistropic**: $n(x) = 0 \implies x = 0$.*

Proof. a) If $A \cong M_n(k)$, then we are saying a matrix is invertible iff its determinant is nonzero, a fact which is very familiar from linear algebra. We reduce to this case as follows: let l/k be a Galois splitting field for A. If $n(x) = 0$, then as an element of $A_l \cong M_n(l)$, $n(x) = n(x \otimes 1) = 0$; as above, by linear algebra $n(x)$ is not a unit in A_l, so it is certainly not a unit in the subring A. Conversely, if $n(x) \neq 0$, then by linear algebra there exists $y \in A_l$ such that $xy = 1$. We want to show that $y \in A$: since $x \in A$, for all $\sigma \in \mathrm{Aut}(l/k)$, $1 = \sigma(1) = \sigma(xy) = x\sigma(y)$ (and similarly $1 = \sigma(y)x$ if we do not want to invoke the Dedekind-finiteness of Noetherian rings), and thus by the uniqueness of inverses we have $\sigma(y) = y$. Therefore $y \in A$ and $x \in A^\times$.
b) By part a), A is division iff every nonzero x in A is a unit iff every nonzero x in A has $n(x) \neq 0$. $\qquad\square$

Proposition 7.4. *Let $A \in \mathrm{CSA}_k$ with $\deg A = n$. Choose a k-basis $e_1, \ldots, e_{n^2}$ for A, and let $x_1, \ldots, x_{n^2}$ be independent indeterminates over k. Then the **reduced norm form** $n(x) = n(x_1 e_1 + \ldots + x_{n^2} e_{n^2}) \in k[x_1, \ldots, x_{n^2}]$ is a geometrically irreducible homogeneous polynomial of degree n in n^2 variables.*

Theorem 7.5. *Let k be a field.*
*a) Suppose that k is **pseudo-algebraically closed** (or "PAC"): every geometrically irreducible k-variety admits a k-rational point. Then $\mathrm{Br}\, k = 0$.*
*b) Suppose that k is **quasi-algebraically closed** (or "C_1"): every homogeneous*

polynomial of degree d in n variables with $n > d$ has a nontrivial zero. Then Br $k = 0$.

Proof. Seeking a contradiction, suppose D is a k-central division algebra of degree $m > 1$, and consider the reduced norm form $n(x)$. The polynomial defining the determinant of a generic $n \times n$ matrix is well-known to be irreducible over any algberaically closed field, so $n(x) = 0$ is a geometrically irreducible affine variety V. Since $m > 1$, the complement of the origin in V is thus also geometrically irreducible, so if k is PAC it has a rational point and by Theorem 7.3 this means that D is not a division algebra.

Similarly, $n(x)$ is a degree m form in m^2 variables, and $m > 1 \implies m^2 > m$. So if k is a C_1-field, there must exist $0 \neq x \in D$ such that $n(x) = 0$, which once again means that D is not a division algebra. $\square$

Remark: The argument fails in both cases for the unreduced norm form $N(x) = n(x)^m$: it has degree m^2 and m^2 variables, and it is reducible.

Exercise 7.4: Suppose that k is either PAC or C_1. Show that in fact every finite dimensional division algebra over k is commutative.

Corollary 7.6. *a) Each of the following fields is PAC so has vanishing Brauer group: an algebraically closed field, a separably closed field, an infinite degree algebraic extension $\mathbb{F}_q$, a nonprincipal ultraproduct of finite fields $\mathbb{F}_q$ with $q \to \infty$.*
b) Each of the following fields is C_1 so has vanishing Brauer group: an algebraically closed field, a finite field, a Henselian valued field with algebraically closed residue field, a field of transcendence degree one over an algebraically closed field.

Proof. We have compiled various results due to various people. Let us give sketches, attributions and references.
a) It is a rather easy fact that an algebraically closed field is both PAC and C_1 (for instance it follows immediately from Hilbert's Nullstellensatz, although one can get away with much less). By Theorem 6.12, every separably closed field is PAC. Moreover, we record the fact that a field is PAC iff every geometrically integral curve over k has a k-rational point.

Suppose k is an infinite algebraic extension of a finite field $\mathbb{F}$, and let $C_{/k}$ be a geometrically integral algebraic curve. Then C is defined over some finitely generated subfield of k and thus over some finite extension field $\mathbb{F}'$ and thus over finite subfields of k of arbitrarily large order. However, it follows from the Weil bounds that for every fixed $g \in \mathbb{N}$, a curve of genus g has $\mathbb{F}$-rational points over any sufficiently large finite field $\mathbb{F}$, and thus C has a k-rational point. The argument for ultraproducts of finite fields is similar. It uses the fact that a field k is PAC iff for every d, every geometrically irreducible plane curve has a k-rational point. For each fixed d, the assertion "Every geometrically irreducible plane curve over k has a k-rational point" can be expressed as a first-order sentence in the language of fields. Moreover, by the Weil bounds, for any fixed d the statement holds for all finite fields of sufficiently large cardinality. The result now follows from Los's theorem on ultraproducts.
b) That a finite field is C_1 is a corollary of the celebrated Chevalley-Warning theorem [Ch36] [Wa36] [CW]. Note that this gives a second proof of Wedderburn's Little Theorem. That a Henselian discretely valued field with algebraically closed

residue field is C_1 is a theorem of Lang [La52]. That a function field in one variable over an algebraically closed field of C_1 is a theorem of Tsen and, later but apparently independently, Lang [Ts36] [La52]. The more general statement follows immediately since every algebraic extension of a C_1 field is C_1. $\square$

7.3. Further examples of Brauer groups.

For a field k, we define its **character group** $X(k) = \mathrm{Hom}(\mathrm{Gal}_k, \mathbb{Q}/\mathbb{Z})$. In other words, $X(k)$ is the discrete torsion group which is Pontrjagin dual to the (compact, totally disconnected) Galois group of the maximal abelian extension of k.

Theorem 7.7. *a) Let K be a Henselian valued field with perfect residue field k. Then there exists a short exact sequence*

$$0 \to \mathrm{Br}\, k \to \mathrm{Br}\, K \to X(k) \to 0.$$

b) In particular, if k is finite – e.g. if K is a p-adic field or $\mathbb{F}_q((t))$ – then the Brauer group of K is isomorphic to $\mathbb{Q}/\mathbb{Z}$.

Proof. Beyond the scope of this course, but see e.g. [S-LF, §12.3, Thm. 2]. $\square$

Example: Perhaps the most transparent example of a field with an infinite Brauer group is the iterated Laurent series field $K = \mathbb{C}((s))((t))$. By Corollary 7.6, the field $k = \mathbb{C}((s))$ has vanishing Brauer group, so by Theorem 7.7a) the Brauer group of $K = k((t))$ is isomorphic to the Galois group of the maximal abelian extension of $\mathbb{C}((s))$. In fact $\mathbb{C}((s))$ has a unique extension of every degree $n \in \mathbb{Z}^+$, namely $s^{\frac{1}{n}}$, which is cyclic of degree n. That is, $\mathrm{Gal}_{\mathbb{C}((s))} \cong \hat{\mathbb{Z}}$, so $\mathrm{Br}\, \mathbb{C}((s))((t)) \cong X(\hat{\mathbb{Z}}) = \mathbb{Q}/\mathbb{Z}$.

Now let K be a global field, i.e., a finite extension of $\mathbb{Q}$ or of $\mathbb{F}_p(t)$. For each place v of K, let K_v denote the completion. If v is complex – i.e., $K_v \cong \mathbb{C}$, then $\mathrm{Br}\, K_v = 0$. If v is real – i.e., $K_v \cong \mathbb{R}$, then by Theorem 6.16 we have $\mathrm{Br}\, K_v \cong \mathbb{Z}/2\mathbb{Z}$, but it will be useful to think of this group as the unique order two subgroup $\frac{\frac{1}{2}\mathbb{Z}}{\mathbb{Z}}$ of $\mathbb{Q}/\mathbb{Z}$. For every finite place, by Theorem 7.7b) $\mathrm{Br}\, K_v \cong \mathbb{Q}/\mathbb{Z}$. Therefore for all places $v \in K$ we have an injection $\mathrm{inv}_v : \mathrm{Br}\, K_v \hookrightarrow \mathbb{Q}/\mathbb{Z}$, the *invariant map*. There is therefore an induced map $\Sigma : \bigoplus_v \mathrm{Br}\, K_v \to \mathbb{Q}/\mathbb{Z}$, namely take the sum of the invariants, the sum extending over all places of K. (If you like, this is exactly the map determined from each of the maps inv_v by the universal property of the direct sum.)

Theorem 7.8. *(Albert-Hasse-Brauer-Noether) For any global field K, we have an exact sequence*

$$0 \to \mathrm{Br}\, K \to \bigoplus_v \mathrm{Br}\, K_v \xrightarrow{\Sigma} \mathbb{Q}/\mathbb{Z} \to 0.$$

Proof. This is beyond the scope of this course. See e.g. [P, Ch. 18]. $\square$

This is a seminal result in algebraic number theory. In particular it implies that for any CSA A over a number field K, A is *globally split* – i.e., $A \sim K$ – iff A is *everywhere locally split* – i.e., for all places v, $A_v \sim K_v$ and is therefore a critical success of the **local-global principle** or **Hasse principle**. Indeed "Hasse principle" is an especially appropriate name here because Hasse was critically involved in the proof, which involves an auxiliary result: an element in a cyclic extension of global fields is a global norm iff it is a norm everywhere locally. The rest of the theorem

says that the global Brauer group is very close to being the full direct sum of the local Brauer groups: the single constraint here is that the sum of the invariants be equal to zero. This constraint is also extremely important: for instance, applied to quaternion algebas over $\mathbb{Q}$ it can be seen to be equivalent the quadratic reciprocity law. It also shows that a CSA A over a global field K is trivial in the Brauer group if it is locally trivial at every place *except possibly one*. I have exploited this "except possibly one" business in my work on genus one curves over global fields: [Cl06].

7.4. Notes.

The material on reduced norms and reduced traces can be found in almost every text treating CSAs, e.g. [P, Ch. 16], [Lo08, Ch. 29], [S-QF, Ch. 4]. We developed only the results we needed for the applications of §7.2.

Our discussion of PAC fields is less traditional, but has in recent years become an important part of **field arithmetic**. Field arithmetic is a remarkable example of a field of mathematics which has developed around a single text (through several editions): the reader who wants to learn quite a lot about it need only consult [FJ].

8. Cyclic Algebras

Our use of Skolem-Noether to realize every 4-dimensional CSA as a quaternion algebra can be vastly generalized.

Theorem 8.1. *Let $A \in \mathrm{CSA}_k$ with $\deg A = n$. Suppose A admits a strictly maximal subfield l such that $\mathrm{Aut}(l/k)$ is cyclic of order n, with generator σ.*
a) There exists $J \in A^\times$ such that
(i) $A = \bigoplus_{0 \leq j < n} J^n l$,
(ii) For all $x \in l$, $\sigma(x) = J^{-1}xJ$ and
(iii) $J^n = b \in k^\times$.
b) Suppose moreover that k contains a primitive nth root of unity ζ_n. Then there exists $I \in l$ such that $\sigma(I) = \zeta_n I$ and $I^n = a \in k^\times$, and $\zeta_n JI = IJ$, and A is generated as a k-algebra by I and J.

Exercise 8.1: Use the Skolem-Nother theorem to prove Theorem 8.1.

A CSA A with a strictly maximal cyclic subfield l is called a **cyclic algebra**. Thus for instance every quaternion algebra is a cyclic algebra. And indeed, just as we constructed quaternion algebras "by hand" using generators and relations, Theorem 8.1b) motivates us to do the same for degree n cyclic algebras under the assumption that the ground field contains a primitive nth root of unity.

Theorem 8.1 motivates us to define a higher-degree analogue of quaternion algebras, as follows: let k be a field, and let ζ_n be a primitive nth root of unity in k. For $a, b \in k^\times$, we define a k-algebra $\left(\frac{a,b}{k}\right)_n$ as the quotient of the free k-algebra $k\langle i, j \rangle$ by the two-sided ideal generated by the relations $i^n = a$, $j^n = b, ji = \zeta_n ij$. Notice that taking $n = 2$ we recover our usual quaternion algebra.

Remark: Note well that although that the (traditional) notation does not show it, the algebra $\left(\frac{a,b}{k}\right)_n$ depends upon the choice of primitive nth root of unity.

Theorem 8.2. *a) Let ζ_n be a primitive nth root of unity in a field k. For any $a, b \in k^\times$, the **symbol algebra** $\left(\frac{a,b}{k}\right)_n$ is a central simple k-algebra of degree n.*
b) Suppose that k is a field of characteristic not dividing n, l/k is a degree n cyclic extension with generator σ, and $b \in k^\times$. Define an n^2-dimensional k-algebra (l, σ, b) as follows: it contains l as a subfield and is generated as a k-algebra by l and one additional element J, such that: the elements $1, J, \ldots, J^{n-1}$ are l-linearly independent, $J^n = b$, and for all $x \in L$, $xJ = J\sigma(x)$. Then (l, σ, b) is a central simple k-algebra of degree n.

Exercise 8.2: Prove Proposition 8.2. (Hint: prove part a) by adapting the proof of Proposition 5.2, and prove part b) by extending the base from k to $k(\zeta_n)$ and applying Kummer theory.)

Exercise 8.3: Show that if either a or b is an nth power in k, then $\left(\frac{a,b}{k}\right)_n \cong M_n(k)$.

Exercise 8.4: We say that $a \in k^\times$ is **n-primitive** if it has order n in $k^\times/k^{\times n}$. If a is n-primitive, show that the symbol algebra $\left(\frac{a,b}{k}\right)$ is a cyclic algebra.

We are now going to state some important theorems about cyclic algebras. Unfortunately we will not prove them: by far the most natural proofs involve the tool of group cohomology, which we are not introducing in these notes.

Theorem 8.3. *Let l/k be a degree n cyclic extension with generator σ, and let $a, b \in k^\times$. Then*

$$[l, \sigma, a] \otimes [l, \sigma, b] \sim [1, \sigma, ab].$$

Theorem 8.4. *Let l/k be a degree n cyclic extension with generator σ, and let $a, b \in k^\times$.*
a) We have $[l, \sigma, a] \cong [l, \sigma, b] \iff \frac{a}{b} \in N_{l/k}(l^\times)$.
b) In particular $[l, \sigma, a] \cong M_n(k) \iff a \in N_{l/k}(l^\times)$.

Corollary 8.5. *Let l/k be a degree n cyclic extension with generator σ. The map $a \in k^\times \mapsto [l, \sigma, a] \in \operatorname{Br} k$ induces an isomorphism of groups*

$$k^\times/N_{l/k}(l^\times) \cong \operatorname{Br}(l/k).$$

Proof. The map is a well-defined homomorphism by Theorem 8.3. Since l is a strictly maximal subfield of $[l, \sigma, a]$ it is a splitting field, and thus the map lands in $\operatorname{Br}(l/k)$. The computation of the kernel is Theorem 8.4b). $\square$

The following is an immediate consequence of Corollary 8.5.

Corollary 8.6. *Let l/k be cyclic of degree n with generator σ, and let $a \in k^\times$ be such that a has order n in $k^\times/N_{l/k}(l^\times)$. Then the degree n cyclic algebra $[l, \sigma, a]$ has order n in $\operatorname{Br}(k)$.*

Remark: In fact in the situation of Corollary 8.6, the algebra $[l, \sigma, a]$ has Schur index n, i.e., is a division algebra. This follows from the **period-index inequality**: for any CSA A, the order of $[A]$ in the Brauer group divides $\operatorname{Ind} A$. This is another result which we are missing out on for lack of a cohomological approach.

Nevertheless Corollary 8.6 can be used to show that for many familiar fields k,

the Brauer group of k contains elements of every order. For instance, suppose k is a p-adic field. Then for all $n \in \mathbb{Z}^+$ there exists a degree n cyclic extension l/k: for instance we may take the unique degree n unramified extension. Then by **local class field theory** the norm cokernel $k^\times/N_{l/k}(l^\times$ is cyclic of order n, so we may take $a \in k^\times$ which has order n in the norm cokernel and thus $[k, \sigma, a]$ is a CSA of order n – and again, in fact it is an n^2-dimensional group. More precisely, this shows that $\mathrm{Br}(l/k)$ is cyclic of order n. With more work, one can show that every order n element in $\mathrm{Br}\, k$ is split by the degree n unramified extension, and thus $\mathrm{Br}(k)[n] \cong \mathbb{Z}/n\mathbb{Z}$.

When k is a number field, there are infinitely many degree n cyclic extensions l/k, and for any one of them, the norm cokernel group contains infinitely many elements of order n. For instance, by Cebotarev density there are infinitely many finite places v which are inert in l/k so that the local extension $l_v = l \otimes_k k_v/k_v$ is again cyclic of degree n, and then by weak approximation any element of the norm cokernel group of l_v/k_v is attained as the image of $a \in \mathbb{Q}$. For such an a, for no $k < n$ is a^k even a norm from l_v, let alone from l. By keeping track of the splitting behavior at various primes, one can quickly see that any number field k admits *infinitely* many n^2-dimensional k-central division algebras for any $n > 1$. This provides some "corroborating evidence" of Theorem 7.8: the Brauer group of a number field is indeed rather large.

8.1. **Notes.**

The material of this sketchy final section is taken from [P, Ch. 15].

REFERENCES

[AB]   J.L. Alperin and R.B. Bell, *Groups and representations.* Graduate Texts in Mathematics, 162. Springer-Verlag, New York, 1995.

[Al29] A.A. Albert, *A determination of all normal division algebras in 16 units.* Trans. Amer. Math. Soc. 31 (1929), 253–260.

[Al32] A.A. Albert, *A construction of non-cyclic normal division algebras.* Bull. Amer. Math. Soc. 38 (1932), 449–456.

[Am72] S. Amitsur, *On central division algebras.* Israel J. of Math. 12 (1972), 408–420.

[Ar27] E. Artin, *Zur Theorie der hyperkomplexen Zahlen.* Abh. Hamburg, 5 (1927), 251-260.

[Az51] G. Azumaya, *On maximally central algebras.* Nagoya Math. Journal 2 (1951), 119–150.

[BM47] B. Brown and N.H. McCoy, *Radicals and subdirect sums.* Amer. J. Math. 69 (1947), 46–58.

[BM48] B. Brown and N.H. McCoy, *The radical of a ring.* Duke Math. J. 15 (1948), 495–499.

[CA]   P.L. Clark, *Commutative algebra.* Notes available at http://math.uga.edu/~pete/integral.pdf

[C-GD] K. Conrad, *Galois descent.* Notes available at http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/galoisdescent.pdf

[Ch36] C. Chevalley, *Démonstration d'une hypoth'ese de M. Artin.* Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg 11 (1936), 73–75.

[Ch56] C. Chevalley, *Fundamental concepts of algebra.* Academic Press Inc., New York, 1956.

[Ch]   W.K. Chan, *Arithmetic of Quaternion Algebras.* http://wkchan.web.wesleyan.edu/.

[Ch61] S.U. Chase, *A generalization of the ring of triangular matrices.* Nagoya Math. J. 18 (1961), 13–25.

[Cl06] P.L. Clark, *There are genus one curves of every index over every number field.* J. Reine Angew. Math. 594 (2006), 201–206.

[CW]   P.L. Clark, *The Chevalley-Warning Theorem.* Notes available at http://math.uga.edu/~pete/4400ChevalleyWarning.pdf

[E]   D. Eisenbud, *Commutative algebra. With a view toward algebraic geometry*. Graduate
           Texts in Mathematics, 150. Springer-Verlag, New York, 1995.

[FJ]   M.D. Fried and M. Jarden, *Field arithmetic*. Third edition. Revised by Jarden. Ergeb-
           nisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys
           in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of
           Modern Surveys in Mathematics], 11. Springer-Verlag, Berlin, 2008.

[FT]   P.L. Clark, *Field Theory*. Notes available at `http://www.math.uga.edu/~`
           `pete/FieldTheory.pdf`.

[G]   M.J. Greenberg, *Lectures on forms in many variables*. W. A. Benjamin, Inc., New
           York-Amsterdam 1969.

[GS]   P. Gille and T. Szamuely, *Central simple algebras and Galois cohomology*. Cambridge
           Studies in Advanced Mathematics, 101. Cambridge University Press, Cambridge, 2006.

[He86]   I.N. Herstein, *On Kolchin's theorem*. Rev. Mat. Iberoamericana 2 (1986), 263–265.

[Ho39]   C. Hopkins, *Rings with minimal condition for left ideals*. Ann. of Math. (2) (1939),
           712–730.

[Ja45]   N. Jacobson, *The radical and semi-simplicity for arbitrary rings*. Amer. J. Math. 67
           (1945), 300–320.

[K]   I. Kaplansky, *Fields and rings*. Second edition. Chicago Lectures in Mathematics. The
           University of Chicago Press, Chicago, Ill.-London, 1972.

[Ka58]   I. Kaplansky, *On the dimension of modules and algebras. X. A right hereditary ring
           which is not left hereditary*. Nagoya Math. J. 13 (1958), 85–88.

[La52]   S. Lang, *On quasi algebraic closure*. Ann. of Math. (2) 55 (1952), 373–390.

[Le39]   J. Levitzki, *On rings which satisfy the minimum condition for the right-hand ideals*.
           Compositio Math. (1939), 214–222.

[L-FC]   T.Y. Lam, *A first course in noncommutative rings*. Second edition. Graduate Texts in
           Mathematics, 131. Springer-Verlag, New York, 2001.

[L-MR]   T.Y. Lam, *Lectures on modules and rings*. Graduate Texts in Mathematics, 189.
           Springer-Verlag, New York, 1999.

[L-QF]   T.-Y. Lam, *Introduction to quadratic forms over fields*. Graduate Studies in Mathe-
           matics, 67. American Mathematical Society, Providence, RI, 2005.

[Lo08]   F. Lorenz, *Algebra. Vol. II. Fields with structure, algebras and advanced topics*. Trans-
           lated from the German by Silvio Levy. With the collaboration of Levy. Universitext.
           Springer, New York, 2008.

[M]   H. Matsumura, *Commutative ring theory*. Translated from the Japanese by M. Reid.
           Second edition. Cambridge Studies in Advanced Mathematics, 8. Cambridge University
           Press, Cambridge, 1989.

[Ma99]   H. Maschke, *Beweis des Satzes, dass diejenigen endlichen linearen Substitutionsgrup-
           pen, in welchen einige durchgehends verschwindende Coefficienten auftreten, intransi-
           tiv sind*. Math. Ann. 52 (1899), 363–368.

[NA]   P.L. Clark, *Non-associative algebras*. Notes available at
           `http://math.uga.edu/~pete/nonassociativealgebra.pdf`

[Na51]   T. Nakayama, *A remark on finitely generated modules*. Nagoya Math. Journal 3 (1951),
           139–140.

[Cl-NT]   Pete L. Clark *Number Theory: A Contemporary Introduction*. `http://alpha.math.`
           `uga.edu/~pete/4400FULL.pdf`

[QF1]   P.L. Clark, *Quadratic forms: Witt's Theory*. Notes available at
           `http://math.uga.edu/ pete/~pete/quadraticforms.pdf`

[QF2]   P.L. Clark, *Quadratic forms over fields II: structure of the Witt ring*. Notes available
           at `http://math.uga.edu/~pete/quadraticforms2.pdf`

[P]   R.S. Pierce, *Associative algebras*. Graduate Texts in Mathematics, 88. Studies in the
           History of Modern Science, 9. Springer-Verlag, New York-Berlin, 1982.

[R]   I. Reiner, *Maximal orders*. London Mathematical Society Monographs, No. 5. Academic
           Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1975.

[S-LF]   J.-P. Serre, *Local fields*. Translated from the French by Marvin Jay Greenberg. Graduate
           Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979.

[S-QF]   G. Shimura, *The arithmetic of quadratic forms*. Springer Monographs in Mathematics,
           2010.

[Sk27]   T. Skolem, *Zur Theorie der assoziativen Zahlensysteme* 1927.

[Sm65]   L.W. Small, *An example in Noetherian rings*. Proc. Nat. Acad. Sci. U.S.A. 54 (1965), 1035–1036.

[Sz81]   F.A. Szász, *Radicals of rings*. Translated from the German by the author. A Wiley-Interscience Publication. John Wiley & Sons, Ltd., Chichester, 1981.

[Ts36]   C. Tsen, *Zur Stufentheorie der Quasi-algebraisch-Abgeschlossenheit kommutativer Körper*. J. Chinese Math. Soc. 171 (1936), 81–92.

[Wa36]   E. Warning, *Bemerkung zur vorstehenden Arbeit von Herrn Chevalley*. Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg 11 (1936), 76–83.

[We07]   J.H.M. Wedderburn, *On Hypercomplex Numbers*. Proc. of the London Math. Soc. 6 (1907), 77–118.

[We37]   J.H.M. Wedderburn, *Note on algebras*. Ann. of Math. (2) 38 (1937), 854–856.

DEPARTMENT OF MATHEMATICS, BOYD GRADUATE STUDIES RESEARCH CENTER, UNIVERSITY OF GEORGIA, ATHENS, GA 30602-7403, USA

Email address: pete@math.uga.edu