Modules and Wedderburn Theory

Alexander Duncan

April 13, 2023

Modern representation theory is usually phrased in the language of non-commutative rings/algebras and their modules. Until now I've avoided this language so I could focus on the basics. However, the module-theoretic perspective is much more versatile — even for finite groups over $\mathbb{C}$. It is much more urgently needed to discuss representation theory over other fields.

The main object is the *group ring* $\mathbb{Z}G$ or *group algebra* kG. We will see that most of the language of representation theory of finite groups can be efficiently expressed as special cases of module theory over kG. Then we will use the language to go even further.

Since module theory is part of the standard algebra qual sequence, I will frequently omit proofs and even many definitions under the assumption that you should have seen them before. However, the emphasis in qual courses is usually on *commutative* rings so some reminders are in order. I recommend finding a graduate algebra textbook with a good treatment of modules, such as [DF04, §10] or [Lan02, §III], to refer to if something is unfamiliar.

The "basics" of module-theoretic representation theory is in almost every text I've referenced, often at a very early stage; see [DF04], [EGH$^+$11], [FH91], [Lan02] etc. Serre's book [Ser77], does not use the module-theoretic perspective at first, but then abruptly changes gears in chapter 6 and assumes you've seen Wedderburn theory (developed below). I will also draw heavily from [AB95, §12,13], [Alp86], and [CR06].

Conventions

Throughout, we assume that all rings and algebras are unital (have an identity element) but are *not necessarily* commutative. We will reserve k for a commutative ring, which will usually be a field or $\mathbb{Z}$. When a ring R is

commutative, we will typically ignore the distinction between left and right R-modules and simply call them R-modules.

1 Warm up: Matrix Algebra over a Field

In this section, we consider the particular case of the non-commutative k-algebra $\mathrm{M}_n(k)$ where k is a field. Many of the quirks of non-commutative rings will show themselves even in this setting.

Example 1.1. The space k^n of column vectors is a left $\mathrm{M}_n(k)$-module. The space $(k^n)^T$ of row vectors is a right $\mathrm{M}_n(k)$-module. More generally, for an integer m, the space of $n \times m$-matrices $\mathrm{M}_{n\times m}(k)$ is a left $\mathrm{M}_n(k)$-module and the space of $m \times n$-matrices $\mathrm{M}_{m\times n}(k)$ is a right $\mathrm{M}_n(k)$-module.

We will see shortly that the above example has exhibited all isomorphism classes of finitely-generated left and right $\mathrm{M}_{m\times n}(k)$-modules.

Definition 1.2. Let R be a ring and M a (left or right) R-module. We say M is *simple* if $M \neq 0$ has no submodules except for 0 and M itself. We say M is *indecomposable* if M cannot be written as a direct sum of non-zero submodules. We say M is *semisimple* if M is a direct sum of simple submodules.

From the above example, we see that k^n is both simple and indecomposable as a left $\mathrm{M}_n(k)$-module. We have a decomposition

$$\mathrm{M}_{n\times m}(k) \cong (k^n)^{\oplus m}$$

as left $\mathrm{M}_n(k)$-modules, so $\mathrm{M}_{n\times m}(k)$ is not simple or indecomposable; however, it is semisimple.

1.1 Ideals

Given a subspace $V \subseteq k^n$, let I be the subset of $\mathrm{M}_n(k)$ where every row is taken from V, and let J be the subset of $\mathrm{M}_n(k)$ where every column is taken from V. Observe that multiplication of I on the left takes each row to a linear combination of elements of V, so we conclude I is a left ideal. Similarly, J is a right ideal.

This procedure is invertible. Given a left ideal I of $\mathrm{M}_n(k)$, we can reconstruct the subspace V as the set of rows occurring among the elements of I. Similarly, for right ideals. We conclude:

Proposition 1.3. *The left (resp. right) ideals of* $\mathrm{M}_n(k)$ *are in canonical bijective correspondence with the vector subspaces of* k^n*.*

Example 1.4. I find the correspondences are somehow easier to understand via specific examples. Let V be the subspace, I the corresponding left ideal, and J the corresponding right ideal. The values a, b, c, d, e, f represent arbitrary elements of k. In $\mathrm{M}_2(k)$, we have the example:

$$V = \mathrm{span}_k \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix} \right\} \quad I = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \right\} \quad J = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \right\}$$

In $\mathrm{M}_3(k)$, we have

$$V = \mathrm{span}_k \left\{ \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} \right\} \quad J = \left\{ \begin{pmatrix} a & b & c \\ a+d & b+e & c+f \\ d & e & f \end{pmatrix} \right\}$$

and I is just the transpose.

Remark 1.5. For those who know some algebraic geometry, the set of subspaces of fixed dimension r in k^n is the *Grassmannian* $\mathrm{Gr}(n, r)$. In particular, the set of subspaces of dimension 1 is the projective space $\mathbb{P}^{n-1}$. The correspondence above allows us to define Grassmannians and projective spaces as sets of left ideals of $\mathrm{M}_n(k)$. This shift of perspective is useful when we define more general objects such as Severi-Brauer varieties when the algebra is not a matrix algebra.

Choosing a basis $v_1, \ldots v_m$ for a subspace V, consider the matrix

$$M_V := \begin{pmatrix} \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \\ v_1 & \cdots & v_n & 0 & \cdots & 0 \\ \vdots & \cdots & \vdots & \vdots & \cdots & \vdots \end{pmatrix}$$

whose first m columns are the basis vectors $v_1, \ldots, v_m$ and the remaining columns are 0. We observe that the corresponding right ideal J is generated by M_V. Similarly, I is generated by M_V^T.

Recall that an ideal is *principal* if it is generated by one element. Thus we have the following:

Corollary 1.6. *Every left (resp. right) ideal of* $\mathrm{M}_n(k)$ *is principal.*

Definition 1.7. We say a ring R is *simple* if its only two-sided ideals are 0 and R itself. We say a ring R is *semisimple* if it is a product of simple rings.

From the explicit description of left and right ideals of $\mathrm{M}_n(k)$, we see that:

Proposition 1.8. $\mathrm{M}_n(k)$ *is a simple ring.*

Be careful about a possible ambiguity with regard to the word "simple." Recall that $\mathrm{M}_n(k)$ can also be viewed a left (or right) module over itself. As a left module, $\mathrm{M}_n(k)$ is usually *not* simple since it has many submodules (left ideals).

We will see later that a finite-dimensional algebra is semisimple as a ring if and only if it is semisimple as a (left or right) module, but this is not obvious: the simple summands are not the same in each context!

1.2 Idempotents

Definition 1.9. Let R be a ring. An element e is an *idempotent* if $e^2 = e$. Two idempotents e_1, e_2 are *orthogonal* if $e_1e_2 = e_2e_1 = 0$. A *primitive idempotent* is a non-zero idempotent that is not a sum of two non-zero orthogonal idempotents.

The idempotents of $\mathrm{M}_n(k)$ are exactly the (matrices representing) the projections $\pi : k^n \to k^n$. Given an idempotent $e \in \mathrm{M}_n(k)$ with corresponding projection π_e, we obtain a direct sum decomposition

$$k^n = \ker(\pi_e) \oplus \mathrm{im}(\pi_e) \ .$$

Observe that idempotent $1 - e$ is orthogonal to e and that

$$\ker(\pi_{1-e}) = \mathrm{im}(\pi_e) \text{ and } \mathrm{im}(\pi_{1-e}) = \ker(\pi_e).$$

Thus, we have a decomposition of vector spaces

$$k^n = e(k^n) + (1 - e)(k^n)$$

where we warn that $e(k^n)$ and $(1 - e)(k^n)$ are *not* $\mathrm{M}_n(k)$-modules.

More generally, a set of orthogonal idempotents $e_1, \ldots, e_r$ such that $1 = e_1 + \ldots + e_r$ gives a decomposition

$$k^n = V_1 \oplus V_2 \oplus \cdots \oplus V_r$$

where $V_i = \mathrm{im}(\pi_i) = e_i(k^n)$ for $1 \leq i \leq r$.

We see that the primitive idempotents of $\mathrm{M}_n(k)$ correspond to the rank 1 projections. Moreover, a maximal set $e_1, \ldots, e_r$ of orthogonal primitive idempotents amounts to a choice of basis for k^n.

Example 1.10. Consider the matrix algebra $\mathrm{M}_2(\mathbb{C})$ and set

$$a = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, b = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, c = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}, \text{ and } d = \begin{pmatrix} \frac{1}{2} & -\frac{1}{2} \\ -\frac{1}{2} & \frac{1}{2} \end{pmatrix}.$$

Each of a, b, c, d are primitive idempotents. We see that a, b are orthogonal and c, d are orthogonal. However, a, c are not orthogonal.

Idempotents are a handy language for understanding decompositions of ideals. If V is the subspace corresponding to a left ideal I, then $I = \mathrm{M}_n(k)e$ where e is the idempotent corresponding to a projection $k^n \to V$.

More generally, if $e_1, \ldots, e_r$ is a set of orthogonal idempotents satisfying $e_1 + \cdots + e_r = 1$, then

$$\mathrm{M}_n(k) = \mathrm{M}_n(k)e_1 \oplus \cdots \oplus \mathrm{M}_n(k)e_r$$

as left $\mathrm{M}_n(k)$-modules and

$$\mathrm{M}_n(k) = e_1 \,\mathrm{M}_n(k) \oplus \cdots \oplus e_r \,\mathrm{M}_n(k)$$

as right $\mathrm{M}_n(k)$-modules. Moreover, we have the decomposition

$$\mathrm{M}_n(k) = \bigoplus_{1 \leq i,j \leq r} e_i \,\mathrm{M}_n(k) e_j$$

as k-vector spaces, which can be thought of as a kind of block matrix decomposition.

Definition 1.11. Let R be a ring. The *center* of R is the subset

$$Z(R) := \{z \in R \mid rz = zr \text{ for all } r \in R\},$$

which is a commutative subring of R.

Note that $Z(\mathrm{M}_n(k)) \cong k$ is just the set of scalar matrices.

Definition 1.12. An idempotent e is *central* if e is contained in the center $Z(R)$ of R. A *primitive central idempotent* is a non-zero central idempotent that is not a sum of two non-zero orthogonal central idempotents.

Warning: a primitive central idempotent is always central but not necessarily primitive! Sometimes the term "centrally primitive" is used instead of "primitive central," which is either more or less confusing depending on which side of the bed you rolled out of that morning.

The matrix algebra $\mathrm{M}_n(k)$ has exactly two central idempotents: the zero matrix and the identity matrix. Only the identity matrix is a primitive central idempotent. (The identity is *not* a primitive idempotent unless $n = 1$.)

Central idempotents are not so interesting for the matrix ring, but they are interesting for products of rings.

Exercise 1.13. *Let R be a ring and suppose e is a central idempotent. Then eRe is a ring under the same addition and multiplication where e is the identity. (Note eRe is a subring only eRe when it contains the identity, which only happens if $e = 1$.)*

Exercise 1.14. *Let R be a ring. A decomposition*

$$R = R_1 \times \cdots \times R_n$$

where $R_1, \ldots, R_n$ are rings corresponds to a set of orthogonal central idempotents $e_1, \ldots, e_n$ such that $R_i \cong e_i R e_i$ for each $1 \leq i \leq n$.

Exercise 1.15. *Let R be a ring and suppose e is a primitive central idempotent. Then eRe cannot be written as a product of two non-zero rings.*

2 The Group Ring

Definition 2.1. Suppose G is a finite group. The *group ring* $\mathbb{Z}G$ is the free abelian group on G with multiplication given by

$$\left(\sum_{g \in G} a_g g\right) \cdot \left(\sum_{g \in G} b_g g\right) := \sum_{g \in G} \sum_{h \in G} a_g b_h gh$$

for integers $\{a_g\}_{g \in G}$ and $\{b_g\}_{g \in G}$. More generally, given a commutative ring k, the *group algebra* kG is the free k-module on G with multiplication as above.

One checks immediately that $\mathbb{Z}G$ is a non-commutative ring with identity 1 corresponding to the basis element of the identity in G. Similarly, kG is a k-algebra with identity 1. Since $1 \in G$ corresponds to $1 \in \mathbb{Z}G$, the identification of the basis of $\mathbb{Z}G$ with the elements of G is mostly harmless if G is written multiplicatively.

Example 2.2. Suppose $G = D_6 = \langle s, r \mid s^2, r^3, (sr)^2 \rangle$ is the dihedral group of order 6. We have the following computation in $\mathbb{Z}G$:

$$\begin{aligned}&(3 + 2s + 5r)(r - sr + 5r^2)\\ =&3r - 3sr + 15r^2 + 2sr - 2r + 10sr^2 + 5r^2 - 5s + 25\\ =&25 - 5s + r + 20r^2 - sr + 10sr^2\end{aligned}$$

Example 2.3. Let $G = \langle r \mid r^n \rangle$ be a cyclic group of order n. Thus G has basis $\{1, r, r^2, \ldots, r^{n-1}\}$ where $r^i \cdot r^j = r^{i+j}$ subject to the relation $r^n = 1$. In other words, $\mathbb{Z}G$ is isomorphic to the ring $\mathbb{Z}[x]/(x^n - 1)$.

Note that using additive notation $\mathbb{Z}/n\mathbb{Z}$ for the cyclic group of order n would be dangerously ambiguous in the example above. For this reason, we usually use "exponential notation" for group rings of additive groups. If $a + b = c$ in an additive group, then we write $x^a x^b = x^{a+b} = x^c$ in the group ring.

Exercise 2.4. *Prove that $\mathbb{Z}G$ is commutative if and only G is abelian.*

It is useful to write the coefficients of the product as a formula of the multiplicands. Specifically, if

$$\left(\sum_{g \in G} a_g g\right) \cdot \left(\sum_{g \in G} b_g g\right) = \sum_{g \in G} c_g g$$

then

$$c_g = \sum_{h \in G} a_h b_{h^{-1}g}$$

for every $g \in G$.

Since G is finite, an equivalent description of $\mathbb{Z}G$ is as the set $\mathrm{Hom}_{\mathrm{Set}}(G, \mathbb{Z})$ of functions from G to $\mathbb{Z}$. However, the ring structure is *not* the "obvious one." The additive structure is indeed pointwise addition, but we use the *convolution product* of two functions f_1, f_2 defined via

$$(f_1 * f_2)(g) = \sum_{ij=g} f_1(i) f_2(j)$$

for $g \in G$ and the indices in the sum i, j vary over all pairs of elements of G such that $ij = g$. The isomorphism with $\mathbb{Z}G$ is by identifying each basis element $g \in \mathbb{Z}G$ with the characteristic function χ_g in $\mathrm{Hom}_{\mathrm{Set}}(G, \mathbb{Z})$ satisfying $\chi_g(h) = \delta_{gh}$ for all $h \in G$.

2.1 Modules of the Group Ring

The relevance of the group ring to group theory is evident from the following proposition:

Proposition 2.5. *Let G be a finite group and k a field. The structure of a representation of G over the field k is equivalent to the structure of a left kG-module. Finite-dimensional representations correspond to finitely generated modules. Moreover, G-equivariant linear transformations are exactly the kG-module homomorphisms.*

Proof. Let M be a left kG-module. In particular, M is a k-vector space. We construct a linear representation $\rho : G \to \mathrm{GL}(M)$ via $\rho_g(m) = gm$ for $g \in G$ and $m \in M$. Conversely, given a linear representation $\sigma : G \to \mathrm{GL}(V)$, we endow V with a left kG-module structure via

$$\left(\sum_{g \in G} a_g g\right) v := \sum_{g \in G} a_g \sigma_g(v)$$

for $\{a_g\}$ from k and $v \in V$. These are mutually inverse operations.

If M is a finitely-generated left kG-module, say by $\{s_1, \ldots, s_n\}$, then M is spanned as a k-vector space by $\{gs_i \mid g \in G, 1 \leq i \leq n\}$. Thus ρ is a finite-dimensional representation. Conversely, if V is finite-dimensional, then a basis for V as a k-vector space is a fortiori a generating set for V as a kG-module.

Finally, we observe that a G-equivariant linear transformation $f : (V, \rho) \to (W, \sigma)$ of representations are exactly the kG-module homomorphisms under

the above correspondence. Indeed,

$$\begin{aligned} & f\left(\left(\sum_{g\in G} c_g g\right) v\right) \\ =& f\left(\sum_{g\in G} c_g \rho_g(v)\right) \\ =& \sum_{g\in G} c_g f\left(\rho_g(v)\right) \\ =& \sum_{g\in G} c_g \sigma_g\left(f(v)\right) \\ =& \left(\sum_{g\in G} c_g g\right) f(v) \end{aligned}$$

where we used the fact that f is linear and G-equivariant. □

Immediately, we see that subrepresentations correspond to submodules, quotient representations correspond to quotient modules, and direct sums correspond to direct sums. However, while $V \otimes_k W$ and $\mathrm{Hom}_k(V, W)$ have induced kG-module structures, they are *not* the same as the module-theoretic constructions $V \otimes_{kG} W$ and $\mathrm{Hom}_{kG}(V, W)$ discussed below. Moreover, the "trivial module" is the zero representation, *not* the "trivial representation".

Example 2.6. Every ring is a both a left and right module over itself. The group algebra kG viewed as a left kG-module corresponds to the regular representation of G.

Another important subtlety in the above is that the dimension of a representation is *not* in general the same as the minimal number of generators of the corresponding kG-module.

A left kG-module is indecomposable if it is indecomposable as a representation. A left kG-module is simple if and only if it is irreducible as a representation of G. In particular, irreducible representations can be generated by one element as a left kG-module (though the converse may not be true).

Theorem 2.7 (Maschke's Theorem restated)**.** *If G is finite of order coprime to the characteristic of a field k, then every finitely-generated left kG-module is semisimple.*

2.2 Center of the Group Ring

The center of a group ring is of special importance. Note that we also have the notion of the center $Z(G)$ of a group G. Indeed, the group ring of the center of a group is contained in the center of the group ring; in other words

$$kZ(G) \subseteq Z(kG).$$

However, equality holds only when $G = Z(G)$, which is a consequence of the following result.

Proposition 2.8. *The center $Z(kG)$ of the group algebra kG has basis*

$$\left\{ \sum_{g \in K} g \;\middle|\; K \in \mathcal{K} \right\}$$

where $\mathcal{K}$ is the set of conjugacy classes of G.

Proof. Let K be a conjugacy class in $\mathcal{K}$. Note that $g \in K$ implies $hgh^{-1} \in K$. Thus we observe that

$$h \left(\sum_{g \in K} g \right) = \left(\sum_{g \in K} g \right) h$$

for all $h \in H$. Conversely, any element x of the group algebra satisfying the property $hx = xh$ must have the same coefficient on basis elements belonging to the same conjugacy class. □

Example 2.9. Suppose $G = D_6 = \langle s, r \mid s^2, r^3, (sr)^2 \rangle$ is the dihedral group of order 6. We determine that $Z(\mathbb{Z}G)$ has basis

$$\{1, a = s + sr + sr^2, b = r + r^2\}.$$

The multiplication table is determined by a few calculations:

$$\begin{aligned} a^2 &= 3 + 3b \\ ab = ba &= 2a \\ b^2 &= 2 + b. \end{aligned}$$

Thus, the structure of the center is a bit obscure in this basis.

When $k = \mathbb{C}$ the center is especially easy to describe. We will see in Corollary 2.12 below that $Z(\mathbb{C}G) \cong \mathbb{C}^{|K|}$ as $\mathbb{C}$-algebras. However, this is not at all obvious in the basis described above!

2.3 Decomposition of the Complex Group Algebra

Let G be a finite group. Let $W_1, \ldots, W_r$ be the distinct complex irreducible representations of G and let $n_1, \ldots, n_r$ be their dimensions.

Theorem 2.10. *There is a canonical isomorphism*

$$\mathbb{C}G \cong \bigoplus_{i=1}^{r} \mathrm{End}_{\mathbb{C}}(W_i)$$

of $\mathbb{C}$-algebras.

Proof. If V is a left $\mathbb{C}G$-module and x is an element of kG, then the multiplication map $v \mapsto xv$ is an endomorphism of V. This gives a map from $\mathbb{C}G$ to each $\mathrm{End}_C(W_i)$ and we obtain a map to the direct sum. The map is injective since the action on the regular representation is faithful. Since both algebras have dimension $n_1^2 + \cdots + n_r^2$, this must be an isomorphism. □

Note that for any complex vector space V of dimension n, we have a (non-canonical) isomorphism $\mathrm{End}(V) \cong \mathrm{M}_n(\mathbb{C})$. Thus, we can rewrite the theorem above as:

Corollary 2.11. $\mathbb{C}G \cong \bigoplus_{i=1}^{r} \mathrm{M}_{n_i}(\mathbb{C})$

Recall that the center of a matrix algebra $\mathrm{M}_n(\mathbb{C})$ is just the subalgebra of scalar matrices, which is isomorphic to $\mathbb{C}$. In view of Corollary 2.11, therefore have:

Corollary 2.12. *$Z(\mathbb{C}G) \cong \mathbb{C}^r$ as $\mathbb{C}$-algebras.*

Thus we have two bases of $Z(\mathbb{C}G)$: one indexed by conjugacy classes and one indexed by irreducible representations. The character table of G is exactly the change of basis matrix between these two bases.

Example 2.13. Let $G = \mathbb{Z}/3\mathbb{Z}$ be the cyclic group of order 3. Note $kG \cong k[x]/(x^3 - 1)$ for any field k. We find that $\mathbb{R}G \cong \mathbb{R} \oplus \mathbb{C}$, so the corollary is more subtle over non-closed fields. Moreover, the element $x - 1$ in $\mathbb{F}_3 G$ is nilpotent, so things are potentially much worse when Maschke's theorem does not hold.

2.4 Idempotents of the Group Ring

Earlier in the course, we have seen several examples of projections in $\mathrm{End}_k^G(V)$ for various representations (V, ρ). For example, the projection $\pi : V \to V^G$ onto the invariant subspace has the formula

$$\pi(v) = \frac{1}{|G|} \sum_{g \in G} \rho_g(v)$$

for $v \in V$. Other examples include the Young projectors, Young symmetrizers, and the projections onto isotypic components. These are all more naturally considered as coming from elements of the group algebra.

Given a representation $\rho : G \to \mathrm{GL}(V)$ and an element

$$f = \sum_{g \in G} c_g g$$

in the group algebra kG, define $\widehat{f}(\rho) \in \mathrm{End}(V)$ via

$$\widehat{f}(\rho)(v) = \sum_{g \in G} c_g \rho_g(v)$$

for all $v \in V$. Thus, the projection π above is simply the endomorphism $\widehat{f}(\rho)$ where $f = |G|^{-1} \sum_{g \in G} g$. In practice, we will simply write f instead of $\widehat{f}(\rho)$ since there is rarely danger of confusion.

First, observe that if $p \in kG$ is an idempotent, then $\widehat{p}(\rho)$ is a projection for any representation ρ. (The converse is not true, consider the direct sum of two copies the regular representation and the projection onto a summand.) Second, if p is a primitive idempotent, then the corresponding projection π on the regular representation has image an indecomposable subrepresentation.

For the complex group ring, we can even say more.

Proposition 2.14. *Let $\chi_1, \ldots \chi_r$ be the irreducible complex characters of G. The primitive central idempotents of $\mathbb{C}G$ are precisely the elements*

$$e_i := \frac{\chi_i(1)}{|G|} \sum_{g \in G} \overline{\chi_i(g)} g$$

for each $i = 1, \ldots, r$. If (V, ρ) is a representation of G, then $\widehat{e_i}(\rho) : V \to V$ is the projection onto the isotypic component of V corresponding to χ_i.

Proof. From the isomorphism

$$\mathbb{C}G \cong \bigoplus_{i=1}^{r} \mathrm{End}(W_i)$$

we recall that the center is $\mathbb{C}^r$, corresponding to scalar multiplication in each $\mathrm{End}(W_i)$. The central idempotents of $\mathbb{C}G$ correspond to the case where each scalar multiplication is 1 or 0. The primitive central idempotents are those which are the identity in exactly one $\mathrm{End}(W_i)$ and trivial elsewhere. The explicit formulas for the primitive central idempotents now follow from the explicit formula for the projection onto the isotypic components of a representation. □

3 Bimodules and Tensor Products

Recall R is a commutative ring, we will often just say R-module without specifying whether it is left or right.

Definition 3.1. If k is a *commutative* ring, then we define an *k-algebra* as a (not-necessarily commutative) ring R along with a ring homomorphism $\pi : k \to R$ such that $\pi(k) \subseteq Z(R)$. An *k-algebra homomorphism* $f : R \to S$ is simply a ring homomorphism such that $\pi_S = f \circ \pi_R$.

Equivalently, an k-algebra is both a k-module and a ring such that the structures are compatible. Observe that this alternative characterization breaks down if k is not in the center of the overring R, since it is not clear whether R should be a left or right R-module. Thus, the restriction to commutative base rings in the center of the overring is fairly reasonable.

Over non-commutative rings, there are some subtleties to homomorphisms and tensor products that can be ignored in the commutative setting. Here we discuss some of these subtleties.

Definition 3.2. Given a ring R, the *opposite ring* R^{op} has the same underlying abelian group, but the multiplication is in the reverse order; in other words, $a \cdot_{\mathrm{op}} b := ba$.

Note that commutative rings are canonically isomorphic to their opposite rings by the identity map. Since the base ring k of a k-algebra is always

commutative, the opposite ring of a (possibly non-commutative) k-algebra is still a k-algebra.

The transpose map $A \mapsto A^T$ gives a canonical isomorphism of the matrix ring $\mathrm{M}_n(k)$ with its opposite $\mathrm{M}_n(k)^{\mathrm{op}}$. The transpose map $g \to g^{-1}$ gives a canonical isomorphism of the group ring $\mathbb{Z}G$ with its opposite $\mathbb{Z}G^{\mathrm{op}}$.

An important example for our purposes shows that we cannot expect canonical isomorphisms in general:

Example 3.3. Let V be a finite-dimensional vector space with dual $V^\vee$ and consider the ring $\mathrm{End}(V)$. We have a canonical isomorphism

$$\psi : \mathrm{End}(V)^{\mathrm{op}} \to \mathrm{End}(V^\vee)$$

via $\psi(f)(g) := g \circ f$ for $f \in \mathrm{End}(V)^{\mathrm{op}}$ and $g \in V^\vee$. We obtain a (non-canonical) isomorphism between $\mathrm{End}(V)^{\mathrm{op}}$ and $\mathrm{End}(V)$ by way of a choice of isomorphism $V \cong V^\vee$.

Despite these example, rings are not necessarily isomorphic to their opposite. We will see later that this does not even hold for *division rings*, which are important for representation theory. Here is a small, somewhat contrived, example for the impatient:

Exercise 3.4. *Consider the subring $R \subseteq \mathrm{M}_2(\mathbb{Q})$ given by*

$$R = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \;\middle|\; a \in \mathbb{Z}, b \in \mathbb{Q}, c \in \mathbb{Q} \right\}.$$

Prove that R is not isomorphic to R^{op}.

Observe that every left R-module is a right R^{op}-module via the scalar multiplication $m \cdot_{\mathrm{op}} r := rm$. Similarly, every right R-module is a left R^{op}-module. In particular, as we have already observer, the distinction between left and right R-modules is inconsequential precisely when R is commutative.

Definition 3.5. Let R and S be rings. An (R, S)-*bimodule* M is a left R-module that is also a right S-module such that $(rm)s = r(ms)$ for all r.

Exercise 3.6. *Show that being an (R, S)-bimodule is equivalent to being a left $R \times S^{\mathrm{op}}$-module, and also to being a right $R^{\mathrm{op}} \times S$-module.*

Bimodules are a quite natural object:

Example 3.7. The ring R is in particular an (R, R)-bimodule.

Example 3.8. Let V and W be k-modules. The set of homomorphisms $\mathrm{Hom}_k(V, W)$ is a $(\mathrm{End}_k(W), \mathrm{End}_k(V))$-bimodule via $fgh := f \circ g \circ h$.

Every left R-module has a canonical structure of a $(R, \mathbb{Z})$-bimodule; indeed even a $(R, Z(R))$-bimodule where $Z(R)$ is the center of R. Similarly, every right R-module has a canonical structure of a $(Z(R), R)$-bimodule. As a consequence, if R is a k-algebra, then every left or right R-module is canonically both a left and right k-module.

Definition 3.9. If M and N are left R-modules, then

$$\mathrm{Hom}_R(M, N) = \mathrm{Hom}_{R-\mathrm{mod}}(M, N)$$

is the set of left R-module homomorphisms $f : M \to N$. If M and N are right R-modules, then

$$\mathrm{Hom}_{\mathrm{mod}-R}(M, N)$$

is the set of right R-module homomorphisms $f : M \to N$.

Suppose that S and T are rings, M is an (R, S)-bimodule, and N is an (R, T)-bimodule. Then $\mathrm{Hom}_R(M, N)$ has a (S, T)-bimodule structure via $(s\phi t)(m) := \phi(ms)t$ for $s \in S, m \in M, t \in T$. Similarly, if M is an (S, R)-bimodule and N is a (T, R)-bimodule, then $\mathrm{Hom}_{\mathrm{mod}-R}(M, N)$ has a (T, S)-bimodule structure.

Thus, when R is commutative, $\mathrm{Hom}_R(M, N)$ has a canonical R-module structure due to the canonical (R, R)-bimodule structure on M (and N). More generally, $\mathrm{Hom}_R(M, N)$ has only a $Z(R)$-module structure. If R is a k-algebra, then $\mathrm{Hom}_R(M, N)$ is canonically a k-module. At the very least $\mathrm{Hom}_R(M, N)$ is always an abelian group due to the canonical $\mathbb{Z}$-module structure.

Example 3.10. Suppose V and W are representations of a finite group G over a field k. Then

$$\mathrm{Hom}_{kG}(V, W) = \mathrm{Hom}_k^G(V, W)$$

is the k-vector space of G-equivariant linear transformations $f : V \to W$.

Definition 3.11. Suppose M is right R-module, N is a left R-module, and A is an abelian group. A group homomorphism $f : M \times N \to A$ is *R-balanced* if $f(mr, n) = f(m, rn)$ for all $r \in R$, $m \in M$, and $n \in N$. A *tensor product* $M \otimes_R N$ is an abelian group together with a R-balanced group homomorphism $\pi : M \times N \to M \otimes_R N$ such that for any R-balanced group homomorphism $\phi : M \times N \to A$ there exists a unique group homomorphism $\psi : M \otimes_R N \to A$ such that $\phi = \psi \circ \pi$.

Once again, we have:

Proposition 3.12. *Tensor products exist and are unique up to unique isomorphism.*

Just like with hom-sets, the tensor product carries additional structures when the ingredients are bimodules. If M is an (S, R)-bimodule and N is an (R, U)-bimodule, then $M \otimes_R N$ is an (S, U)-bimodule via the multiplication $s(m \otimes n)r := (sm) \otimes (nr)$ extended by linearity.

Many constructions use the various canonical bimodule structures implicitly. For example, if R is commutative, and M and N are both *left* R-modules, then we can use the canonical *right* R-module structure on M to make sense of $M \otimes_R N$. Then $M \otimes_R N$ has an R-module structure using either the left R-module structure on M or the right R-module structure on N (which agree). For annother example, if R is a k-algebra, then $M \otimes_R N$ has a canonical k-module structure.

We are now in a position to state an important result:

Theorem 3.13 (Tensor-Hom Adjunction)**.** *Let R, S, U, V be rings. Let M be an (R, S)-bimodule, N be an (S, U)-bimodule, and P be an (R, V)-bimodule. Then there is a natural isomorphism*

$$\mathrm{Hom}_R(M \otimes_S N, P) \cong \mathrm{Hom}_S(N, \mathrm{Hom}_R(M, P))$$

of (U, V)-bimodules.

Exercise 3.14. *The hom-sets in the statement of the Tensor-Hom Adjunction use the* left *module structures on M, N, P etc. Determine the analogous statement where the hom-sets refer to the* right *module structures.*

Rarely are all bimodule structures needed at once! The most important special case is when M is an (R, S)-bimodule, N is a left S-module and P is left R-module; the resulting isomorphism is then just of abelian groups.

One of the main applications of the Tensor-Hom Adjunction is understanding restriction and extension of scalars.

Definition 3.15. Let $f : R \to S$ be a ring homomorphism. If N is a left S-module, then the *restriction of scalars of* N is the left R-module structure on N given by $r \cdot_R n := f(r)n$ for $r \in R$ and $n \in N$. We often denote the restriction of scalars by ${}_RN$ or ${}_fN$ to emphasize the distinction with the original N viewed as a left S-module.

When f is the inclusion of a subring, one can think of the restriction of scalars as "forgetting" some of the structure of N. For example, a complex vector space $\mathbb{C}^n$ becomes the real vector space $\mathbb{R}^{2n}$ under restriction by the inclusion $\mathbb{R} \to \mathbb{C}$.

Example 3.16. If H is a subgroup of a group G, the we have an inclusion $kH \to kG$ of group algebras. Let V be a representation of a finite group G over a field k. Then V has the structure of a left kG-module. The restriction of scalars ${}_{kH}V$ is the left kH-module corresponding to $\operatorname{Res}^G_H V$.

Somewhat trickier is going in the other direction.

Definition 3.17. Let $f : R \to S$ be a ring homomorphism and M be an R-module. Let S_R be the corresponding (S, R)-bimodule structure on S and let ${}_RS$ be the corresponding (R, S)-bimodule structure on S. The *extension of scalars of* M is the left S-module $S_R \otimes_R M$. The *coextension of scalars of* M is the left S-module $\operatorname{Hom}_R({}_RS, M)$.

Note that the notation S_R and ${}_RS$ is usually considered unnecessarily pedantic. We typically write simply $S \otimes_R M$ for extension of scalars and $\operatorname{Hom}_R(S, M)$ for coextension of scalars. This is usually unambiguous, although perhaps confusing for beginners.

The Tensor-Hom adjunction shows that extension of scalars and restriction of scalars are adjoint. Indeed, viewing S as an (S, R)-bimodule, we have $\operatorname{Hom}_S(S, M) \cong {}_RM$. Thus, the adjunction becomes

$$\operatorname{Hom}_R(S \otimes_R N, M) \cong \operatorname{Hom}_R(N, {}_RM)$$

for a left R-module N and a left S-module M.

Once again, these have immediate connections to representation theory:

Example 3.18. If H is a subgroup of a group G, the we have an inclusion $kH \to kG$ of group algebras. Let W be a representation of a finite group H over a field k. Then W has the structure of a left kH-module. The extension of scalars $kG \otimes_{kH} W$ is the left kG-module corresponding to $\operatorname{Ind}_H^G W$.

To see why extension of scalars corresponds to induction, we just need to recall that we essentially *defined* induction to be the linear representation that satisfied (a version of) Frobenius reciprocity. The Tensor-Hom adjunction gives us an isomorphism of k-vector spaces

$$\operatorname{Hom}_{kG}(kG \otimes_{kH} W, V) \cong \operatorname{Hom}_{kH}(W, {}_{kH}V))$$

which is exactly the isomorphism

$$\operatorname{Hom}_k^G(\operatorname{Ind}_H^G W, V) \cong \operatorname{Hom}_k^H(W, \operatorname{Res}_H^G V)$$

from Frobenius Reciprocity!

We leave it as an exercise to check that coextension of scalars corresponds to coinduction. Indeed, the distinction is not important (at least in our setting) in view of the following:

Exercise 3.19. *Suppose H is subgroup of finite group G and W is a kH-module. Prove that*

$$kG \otimes_{kH} W \cong \operatorname{Hom}_{kH}(kG, W)$$

as left kG-modules.

4 Wedderburn Decomposition

Throughout this section, k is a field. The main goal of this section is to prove the following:

Theorem 4.1 (Wedderburn's Theorem)**.** *A finite dimensional k-algebra A is* semisimple *if and only if*

$$A \cong \bigoplus_{i=1}^{r} \mathrm{M}_{n_i}(D_i)$$

where $D_1, \ldots, D_r$ are finite-dimensional k-algebras and $n_1, \ldots, n_r$ are positive integers.

Definition 4.2. Let A be a k-algebra and M be a left A-module. A *composition series* or *simple finite filtration* is a descending sequence of submodules

$$M = M_0 \supsetneq M_1 \supsetneq \cdots \supsetneq M_r = 0$$

such that each quotient M_i/M_{i+1} is simple. The integer r is the *length* of the filtration. The module M is of *finite length* if it possesses a simple finite filtration or $M = 0$.

Theorem 4.3 (Jordan-Hölder)**.** *Any two composition series of a left module M are* equivalent*: the isomorphism classes of the quotients M_i/M_{i+1} are unique up to reordering.*

In view of the Jordan-Hölder theorem, the following notion is well-defined:

Definition 4.4. The *length* of a module M of finite length is the length of any composition series (or 0 if $M = 0$).

Recall that a ring is Artinian (resp. Noetherian) if it satisfies the descending chain condition (resp. ascending chain condition) on ideals. Similarly, a module is Artinian (resp. Noetherian) if it satisfies the descending chain condition (resp. ascending chain condition) on submodules. Vector spaces over a field are in particular, both Artinian and Noetherian so we immediately have the following.

Proposition 4.5. *Suppose A is a finite-dimensional k-algebra, and M is a finitely generated left A-module. Then A and M are both Noetherian and Artinian. In particular, we see that M has finite length.*

If M is a semisimple left module, then there is a decomposition

$$M = M_1 \oplus \cdots \oplus M_r, \tag{4.1}$$

where each M_i is a submodule isomorphic to $S_i^{\oplus a_i}$, S_i is simple, a_i is a positive integer and $S_i \ncong S_j$ when $i \neq j$. Note that the each submodule M_i is canonical, but the isomorphism $M_i \cong S_i^{\oplus a_i}$ is not. The submodules $M_1, \ldots, M_r$ are called the *isotypic components* of M, and (4.1) is called the *isotypic decomposition* of M.

Lemma 4.6. *Let A be a finite-dimensional k-algebra and M be a finitely generated left A-module. The following are equivalent:*

(a) every submodule of M is a direct summand,

(b) M is semisimple, and

(c) M is sum of simple submodules (not a priori direct).

Proof. If $N_1 \subset N_2 \subset M$ is a chain of submodules and N_1 is a direct summand of M then N_1 is a direct summand of N_2. Thus (a) $\implies$ (b) follows by induction on the dimension of M, with simple modules as the base case. The implication (b) $\implies$ (c) is immediate. It remains to show (c) $\implies$ (a).

Let N be a submodule of M. Let N' be the maximal submodule of M such that $N \cap N' = 0$ (which exists since M is finite-dimensional). If $N + N' = M$ then we are done, so suppose $N + N' \subsetneq M$. Then there is a simple submodule S of M not contained in $N + N'$; in fact, $S \cap (N + N') = 0$ since it is simple.

In particular, $N' \subsetneq N' + S$. Consider $m \in (N' + S) \cap N$. We have $m = n + s$ where and $n \in N'$ and $s \in S$. The element $s = m - n$ is in both S and $N + N'$, so is trivial. Thus $m \in N' \cap N$ is itself trivial. We conclude that $(N' + S) \cap N$ is trivial. The module $N' + S$ is a counterexample to the assumption of maximality of N'. □

Lemma 4.7. *Submodules and quotient modules of semisimple modules are semisimple.*

Proof. Submodules are semisimple by an argument similar to (1) $\implies$ (2) from Lemma 4.6. Quotient modules are semisimple by Schur's lemma and condition (3) from Lemma 4.6. □

Recall that an algebra A is semisimple if and only if it is a direct product of simple rings. We will see that this is equivalent to A being semisimple as a left module over itself. In the interim, we prove a third equivalent restatement:

Lemma 4.8. *Let A be a finite-dimensional k-algebra. Every finitely generated left A-module is semisimple if and only if ${}_AA$ is semisimple as a left A-module over itself.*

Proof. Suppose ${}_AA$ is semisimple as a left A-module. Any A-module M can be written as a quotient of the free A-module A^n for some positive integer n. Thus any submodule M is semisimple by Lemma 4.7. The converse follows a fortiori. □

As a consequence of the previous lemma, along with Jordan-Hölder, we conclude that a semisimple algebra has only finitely many isomorphism classes of simple modules!

Lemma 4.9. *Let A be a finite-dimensional k-algebra. If A is a simple algebra, then ${}_AA$ is semisimple.*

Proof. Let M be the sum of all simple submodules in ${}_AA$. If S is a simple submodule in ${}_AA$ and $a \in A$, then the left ideal Sa is either 0 or a simple submodule of ${}_AA$. Thus $Ma \subseteq M$ for any $a \in A$. Thus M is a right ideal of A so, in fact, a two-sided ideal. Since $M \neq 0$ and A is simple as a ring, $M = A$. So ${}_AA$ is a sum of simple submodules, and thus is semisimple. □

Corollary 4.10. *Let A be a finite-dimensional k-algebra. If A is a semisimple algebra, then ${}_AA$ is semisimple.*

Proof. Let $A = A_1 \oplus \cdots \oplus A_n$ where each A_i is a simple k-algebra. Observe that the left A-module structure on ${}_AA_i$ factors through the A_i-module structure. Each A_i is, in particular, a submodule of ${}_AA$. Since they are semisimple, so is their sum. □

(The converse of the corollary will follow as a consequence of Wedderburn's theorem.)

A proof of the following is left as an exercise:

Lemma 4.11. *Let A be a ring. Let $M = M_1 \oplus \cdots \oplus M_m$ and $N = N_1 \oplus \cdots \oplus N_n$ be direct sums of A-modules. Then*

$$\mathrm{Hom}_A\left(\bigoplus_i M_i,\ \bigoplus_j N_i\right) \cong \bigoplus_{i,j} \mathrm{Hom}_A(M_i, N_j)\ .$$

Lemma 4.12. *Let A be a finite-dimensional k-algebra and let M be a semisimple left A-module. Suppose*

$$M = M_1 \oplus \cdots \oplus M_r$$

is the isotypic decomposition where $M_i = S_i^{\oplus n_i}$ for some simple A-module S_i. There is a canonical isomorphism of k-algebras

$$\mathrm{End}_A(M) \cong \mathrm{M}_{n_1}(\mathrm{End}_A(S_1)) \oplus \cdots \oplus \mathrm{M}_{n_r}(\mathrm{End}_A(S_r)).$$

Proof. By Lemma 4.11, we have $\mathrm{End}_A(N) = \mathrm{Hom}_A(N, N)$ and $\mathrm{End}_A(M^{\oplus n}) \cong M_n(\mathrm{End}_A(N))$ for any left A-module N and any positive integer n. Thus, it suffices to show that $\mathrm{Hom}_A(M_i, M_j) = 0$ whenever $i \neq j$. Note that $M_i = S_i^{\oplus n_i}$ and $M_j = S_j^{\oplus n_j}$ for integers n_i, n_j and non-isomorphic simple modules S_i and S_j. Again using the previous lemma, $\mathrm{Hom}_A(M_i, M_j)$ is a direct sum of modules of the form $\mathrm{Hom}_A(S_i, S_j)$. These are 0 by Schur's lemma. □

Lemma 4.13. *Let A be a k-algebra. There is a canonical isomorphism $A^{\mathrm{op}} \cong \mathrm{End}_A({}_AA)$ of k-algebras.*

Proof. Given an element $a \in A^{\mathrm{op}}$, there is a unique endomorphism $\phi_a \in A^{\mathrm{op}}$ such that $\phi_a(1) = a$. This gives a correspondence that commutes with addition and scalar multiplication. Thus there is an isomorphism between the underlying vector spaces. The computation

$$(\phi_a \circ \phi_b)(1) = \phi_a(b) = b\phi_a(1) = ba$$

shows that the multiplications agree. Thus the algebras are isomorphic. □

One more observation before the main theorem:

Lemma 4.14. *For a k-algebra A, there is a k-algebra isomorphism $\mathrm{M}_n(A)^{\mathrm{op}} \cong \mathrm{M}_n(A^{\mathrm{op}})$.*

Proof. Take a matrix to its transpose. This is clearly a vector space isomorphism. A short calculation shows that the multiplications are also compatible. □

We now prove Wedderburn's theorem.

Proof of Theorem 4.1. Suppose A is semisimple as a k-algebra. Then ${}_AA$ is semisimple as a left A-module by Corollary 4.10.

Since ${}_AA$ is semisimple, it has an isotypic decomposition

$${}_AA = S_1^{\oplus n_1} \oplus \cdots \oplus S_r^{\oplus n_r}$$

where S_i are pairwise non-isomorphic simple modules. Let $D_i = \mathrm{End}_A(S_i)$, which are division algebras by Schur's Lemma.

Thus

$$\begin{aligned} A^{\mathrm{op}} &\cong \mathrm{End}_A(A) \\ &\cong \mathrm{End}_A(S_1^{\oplus n_1}) \oplus \cdots \oplus \mathrm{End}_A(S_r^{\oplus n_r}) \\ &\cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_r}(D_r) \ , \end{aligned}$$

and applying the last lemma:

$$A \cong M_{n_1}(D_1^{\mathrm{op}}) \oplus \cdots \oplus M_{n_r}(D_r^{\mathrm{op}}) \ .$$

We leave the converse as an exercise. □

Note that a corollary of the above (one direction of which was used in the proof) is the following characterization of semisimplicity of an algebra.

Corollary 4.15. *Let A be a finite-dimensional k-algebra. The following are equivalent:*

- *A is semisimple as a ring (a direct sum of simple rings).*
- *A is semisimple as a left A-module (a direct sum of simple modules).*
- *Every finitely generated left A-module is semisimple.*

5 Central Simple Algebras

As in the previous section, k is a field. We denote the algebraic closure of k by $\overline{k}$. Some of the results here are elaborated in texts on central simple algebras and the Brauer group (for example, [GS17] or [Sal99]).

Since a semisimple algebra is a direct sum of simple algebras, we are now interested in studying simple algebras. The most important invariant of a simple algebra is its center, which is always a field since otherwise there is a non-trivial two-sided ideal. This motivates the following definition.

Definition 5.1. A *central simple k-algebra* is a finite-dimensional k-algebra A with center $Z(A) = k$. A *central division k-algebra* is a finite-dimensional k-algebra A with center $Z(A) = k$.

Recall the following, which we proved when we established Schur's Lemma in the complex case:

Proposition 5.2. *If k is algebraically closed, then every central division k-algebra is isomorphic to k.*

In view of Wedderburn's theorem, we have a good description of central simple algebras and how they relate to the other kinds of algebras we've seen. If A is a finite dimensional k-algebra, then:

1. If A is semisimple, then it is a product of simple k-algebras.
2. If A is simple, then it is a central simple K-algebra, where K is a finite field extension of k.
3. If A is a central simple k-algebra, then $A \cong \mathrm{M_n}(D)$ where D is a central division k-algebra.

Central simple algebras and division algebras are closely related. In one sense, the former can be totally understood in terms of the latter:

Proposition 5.3. *If A is a central simple k-algebra, then there is a unique central division k-algebra D (up to isomorphism) and positive integer n such that $A \cong \mathrm{M}_n(D)$.*

Proof. Suppose $A \cong M_n(D) \cong M_m(E)$ for central division k-algebras D and E. Let L be a minimal left ideal of A. Then $D^{\oplus n} \cong L \cong E^{\oplus m}$ since all the algebras are simple and have only isomorphism class of simple module. One may view $D^{\oplus n}$ as the set of column vectors with entries in D. Observe that an endomorphism $D^{\oplus n} \to D^{\oplus n}$ as left A-modules is wholly determined by the image of the element $(1, 0, \ldots, 0)$. One checks that the only permitted images are of the form $(a, 0, \ldots, 0)$ for $a \in A$. Thus $\mathrm{End}_A(D^{\oplus n}) \cong D$. Thus

$$D \cong \mathrm{End}_A(D^{\oplus n}) \cong L \cong \mathrm{End}_A(E^{\oplus m}) \cong E$$

and $m = n$ follows by a dimension count. □

However, central simple algebras naturally come up in constructions that are a bit awkward if restricted to division algebras alone.

Lemma 5.4. *If A and B are k-algebras, then $Z(A \otimes_k B) = Z(A) \otimes_k Z(B)$.*

Proof. Clearly, $Z(A) \otimes_k Z(B) \subseteq Z(A \otimes_k B)$. Now, suppose $z = \sum_i a_i \otimes b_i$ is an element of $Z(A \otimes_k B)$. We may assume the a_i are linearly independent. Take $x \in B$ and observe that

$$0 = z(1 \otimes x) - (1 \otimes x)z = \sum_i a_i \otimes (b_i x - x b_i),$$

implying that each $b_i x - x b_i = 0$. Thus each $b_i \in Z(B)$. Thus $z \in A \otimes_k Z(B)$. Now, we may assume (after possibly rewriting z) that the b_i are linearly independent in $Z(B)$ and conclude similarly that each a_i is in $Z(A)$. □

Lemma 5.5. *If A is a central simple k-algebra and B is a simple k-algebra, then $A \otimes_k B$ is a simple k-algebra.*

Proof. Let I be a non-trivial two-sided ideal in $A \otimes_k B$. Let r be the minimal positive integer such that there exists an element $x \in I$ that can be written

$$x = \sum_{i=1}^{r} a_i \otimes b_i.$$

Since I is A is simple, $Aa_1A = A$. Thus we have $y, z \in A \otimes 1$ such that

$$x' = yxz = 1 \otimes b_1 + \sum_{i=2}^{r} a_i' \otimes b_i$$

for $a_i' = ya_iz$, where $x' \in I$ also. For all $w \in A$, we see that

$$(w \otimes 1)x' - x'(w \otimes 1) = -\sum_{i=2}^{r} (wa_i' - a_i'w) \otimes b_i = 0$$

by minimality of r. Thus $x' \in Z(A) \otimes_k B = k \otimes_k B$. Thus $x' = 1 \otimes b \in I$ for some $b \in B$. But B is simple, so $BbB = B$. Thus $1 \otimes 1 \in I$. We conclude that $A \otimes B = I$ as desired. □

Note that the hypothesis that A is central over k is vital in Lemma 5.5 — consider $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$.

Lemma 5.6. *If A is a finite-dimensional central simple k-algebra, then there is a k-algebra isomorphism $A \otimes_k A^{\mathrm{op}} \cong M_n(k)$ for $n = \dim_k(A)$.*

Proof. By extension by linearity, there is a k-algebra homorphism $\Psi : A \otimes_k A^{\mathrm{op}} \to \mathrm{End}_k(A)$ such that $\Psi(x \otimes y)(z) = xzy$ for $x, z \in A$ and $y \in A^{\mathrm{op}}$. The map is injective since $A \otimes A^{\mathrm{op}}$ is simple. Surjectivity follows by a dimension count. □

(In fact, the converse of the previous lemma is also true, but we do not need this.)

Definition 5.7. Two central simple k-algebras A and B are *Brauer equivalent* if $A \otimes_k M_n(k) \cong B \otimes_k M_m(k)$ for some positive integers m, n. The *Brauer group*, denoted $\mathrm{Br}(k)$, is the set of Brauer-equivalence classes of central simple k-algebras.

From the lemmas above, we have the following:

Proposition 5.8. *The Brauer group* $\mathrm{Br}(k)$ *is a group under tensor product of representatives, with identity the class of matrix algebras* $M_n(k)$ *and inverse given by* $[A] \mapsto [A^{\mathrm{op}}]$.

Equivalently, A and B are Brauer equivalent if A and B are both matrix rings over the same central division k-algebra. Thus $\mathrm{Br}(k)$ can also be viewed as the set of isomorphism classes of central division k-algebras; however, the group structure is more obscure with this definition.

Another reason once studies central simple algebras instead of just the underlying division algebras is that property of being a central simple algebra is invariant under field extension.

Proposition 5.9. *Let A be a finite-dimensional k-algebra. The following are equivalent:*

(a) A is a central simple k-algebra.

(b) $A \otimes_k K$ is a central simple K-algebra for a field extension K/k.

(c) $A \cong \mathrm{M}_n(D)$ for a central division k-algebra D and some n.

(d) $A \otimes_k \overline{k} \cong \mathrm{M}_n(\overline{k})$ for some n.

(e) $A \otimes_k K \cong \mathrm{M}_n(K)$ for a finite field extension K/k and some n.

(f) $A \otimes_k K \cong \mathrm{M}_n(K)$ for a finite Galois field extension K/k and some n.

Proof. The equivalence of (e) and (f) boils down to showing that one can choose a *separable* field extension. Since we're mostly working in characteristic 0, we won't consider (f) here; see [GS17, Proposition 2.2.5] for a proof.

We begin by establishing (a) $\implies$ (b). By Lemma 5.5 we conclude that $A \otimes_k K$ is simple since K is simple. The center of $A \otimes_k K$ is $k \otimes_k K = K$ by Lemma 5.4. Thus $A \otimes_k K$ is a central simple K-algebra as desired.

Let us consider (b) $\implies$ (a). If J is a two-sided ideal of A, then $J \otimes_k K$ will be a two-sided ideal of $A \otimes_k K$; thus A is simple. If z is in the center $Z(A)$, then $z \otimes 1$ is in the center of $Z(A \otimes K)$. Thus $z \in K \cap k = k$.

The implication (a) $\implies$ (c) we have already seen follows from Wedderburn theory. The implication (c) $\implies$ (d) follows from Proposition 5.2 using the fact that we have already shown (a) $\implies$ (b). The implication (d) $\implies$ (e) follows from the Lefschetz principle: the coefficients in an explicit isomorphism $A \otimes_k \overline{k} \cong \mathrm{M}_n(\overline{k})$ must be defined over some finite extension of k. The implication (e) $\implies$ (b) is immediate. □

In view of the previous proposition, we may discuss some standard concepts associated to central simple algebras.

Definition 5.10. Let A be a central simple k-algebra. The algebra A is *split* if $A \cong \mathrm{M}_n(k)$ for some integer n. A *splitting field* of A is a field extension K/k such that $A \otimes_k K \cong \mathrm{M}_n(K)$.

Note that if V is a k-vector space, then $\dim_k(V) = \dim_K(V \otimes_k K)$ for all field extensions K/k. Thus, the dimension $\dim_k(A)$ of a central simple k-algebra A is always a square since $A \otimes_k K \cong \mathrm{M}_n(K)$ for some field extension K/k.

Definition 5.11. Let A be a central simple k-algebra. The *degree* of A is the unique positive integer $\deg(A)$ such that $\dim_k(A) = \deg(A)^2$. The *(Schur) index* of A is given by $\mathrm{ind}(A) = \deg(D)$ where D is the central division k-algebra such that $A \cong \mathrm{M}_n(D)$.

Proposition 5.12. *If A is a central simple k-algebra and M is a simple left A-module, then* $\dim_k(M) = \deg(A)\,\mathrm{ind}(A)$.

Proof. Note $A \cong \mathrm{M}_r(D)$ for a central division k-algebra D. Since M is simple, we have $M \cong D^{\oplus r}$. Thus $\dim_k(M) = r\deg(D)^2 = \deg(A)\,\mathrm{ind}(A)$. □

Let A be a central simple k-algebra with splitting field K and let $\Psi : A \hookrightarrow M_n(K)$ be the embedding obtained by composition with an isomorphism $A \otimes_k K \cong M_n(K)$. Given an element $a \in A$, we define the *reduced characteristic polynomial*

$$\mathrm{Prd}_{A,a}(t) := \chi_{\Psi(a)}(t)$$

where $\chi_{\Psi(a)}(t)$ is the characteristic polynomial of $\Psi(a)$ in $M_n(K)$.

Proposition 5.13. *The reduced characteristic polynomial* $\mathrm{Prd}_{A,a}(t)$ *has coefficients in* k *and does not depend on the choice of splitting field* K *nor the choice of isomorphism* $A \otimes_k K \cong M_n(K)$.

Proof. We omit the proof since this is not fundamental to our story. □

Writing

$$\mathrm{Prd}_{A,a}(t) = t^n - e_1 t^{n-1} + \cdots + (-1)^n e_n$$

as a polynomial in $k[t]$, we define the *reduced trace* $\mathrm{Trd}_A(a) = e_1$ and *reduced norm* $\mathrm{Nrd}_A(a) = e_n$.

Proposition 5.14. *Let* A *be a central simple* k*-algebra. Let* $\chi_{A/k,a}(t)$, $\mathrm{Tr}_{A/k}(a)$, *and* $\mathrm{N}_{A/k}(a)$ *be the "usual" characteristic polynomial, trace, and norm of* a *as an element of the* k*-algebra* A*. Then we have*

$$\chi_{A,a}(t) = \mathrm{Prd}_{A,a}^n(t) \quad \mathrm{Tr}_{A/k}(a) = n\,\mathrm{Trd}_A(a) \quad \mathrm{N}_{A/k}(a) = (\mathrm{Nrd}_A(a))^n$$

where $n = \deg(A)$.

5.1 Quaternion Algebras

Let k be a field of characteristic $\neq 2$. Suppose $a, b \in k^\times$. Let $Q_{a,b}$ be k-algebra with basis $\{1, i, j, ij\}$ where the multiplication satisfies

$$i^2 = a, j^2 = b, ij = -ij.$$

The algebra $Q_{a,b}$ is a *(generalized) quaternion* k*-algebra*. Observe that $Q_{-1,-1} \cong \mathbb{H}$ when $k = \mathbb{R}$.

Let $K = k(\sqrt{a})$. We have an injective k-algebra homomorphism $\Phi : Q_{a,b} \to \mathrm{M}_2(K)$ via

$$x + yi + zj + wij \mapsto \begin{pmatrix} x + \sqrt{a}y & bz + b\sqrt{a}w \\ z - \sqrt{a}w & x - \sqrt{a}y \end{pmatrix}$$

for $x, y, z, w \in k$. This shows that $Q_{a,b}$ is a central simple k-algebra and K is a splitting field. Note that $k(\sqrt{b})$ is also a splitting field of $Q_{a,b}$.

The reduced norm is given by

$$\mathrm{Nrd}(x + yi + zj + wij) = x^2 - ay^2 - bz^2 + abw^2.$$

Observe that if $q \in Q_{a,b}$, then $\Phi(q)$ is invertible if and only if $\mathrm{Nrd}(q) \neq 0$. In this case, the inverse of q is $\overline{q}/\mathrm{Nrd}(q)$ where

$$\overline{q} = x - yi - zj - wij$$

is the *conjugate* of q. Thus the inverse of q, if it exists in $\mathrm{M}_2(K)$, is also in $Q_{a,b}$.

Proposition 5.15. *Let $Q_{a,b}$ be a quaternion k-algebra. The following are equivalent:*

(a) $Q_{a,b}$ is split.

(b) $Q_{a,b}$ is not division k-algebra.

(c) $\mathrm{Nrd} : Q_{a,b} \to k$ has a non-trivial zero.

(d) $ax^2 + by^2 = 1$ has a solution (x, y) over k.

Proof. The equivalence of (a) and (b) follow from Wedderburn's theorem since $Q_{a,b} = M_n(D)$ for a division k-algebra D and n can only be 1 or 2. The equivalence of (b) and (c) follow from the discussion of inverses above. We see that (d) implies (c) via the element $1 - xi - yj$.

Now assume (c). If a is a square, then we are already done. Thus, we may assume $k(\sqrt{a})/k$ is a non-trivial field extension. Then there exist $x, y, z, w \in k$, not all zero, such that

$$(x^2 - ay^2) = b(z^2 - aw^2).$$

Observe that $N(x + y\sqrt{a}) = x^2 - ay^2$ where $N : k(\sqrt{a}) \to k$ is the usual norm of the field extension $k(\sqrt{a})/k$. Thus $b = N(x+y\sqrt{a})N(z+w\sqrt{a})^{-1} = N(u + v\sqrt{a})$ for some $u, v \in k$ by the multiplicativity of the norm map. In other words, $b = u^2 - av^2$ and so we have $a(v/u)^2 + b(1/v)^2 = 1$. Thus $(u/v, 1/v)$ gives the desired solution establishing (d). □

5.2 Cyclic Algebras

Let L/k be a cyclic Galois extension of degree n, suppose σ is a generator of $\mathrm{Gal}(K/k)$, and suppose $b \in k$. Consider the matrices

$$Y = \begin{pmatrix} 0 & 0 & \cdots & 0 & b \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix} \quad X(\ell) = \begin{pmatrix} \ell & 0 & 0 & \cdots & 0 \\ 0 & \sigma(\ell) & 0 & \cdots & 0 \\ 0 & 0 & \sigma^2(\ell) & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \sigma^{n-1}(\ell) \end{pmatrix}$$

where $\ell \in L$. Observe that $YX(\ell) = X(\sigma(\ell))Y$, $Y^n = 1$ and $X(\ell)$ satisfies the same minimal polynomial as ℓ.

Consider the k-algebra $A = A(L, \sigma, b)$ generated by X and Y. Such algebras are called *cyclic algebras*. Observe that, at least when a is not a square in k, the quaternion algebras above are special cases with $Q_{a,b} \cong A(k(\sqrt{a}), \sqrt{a} \mapsto -\sqrt{a}, b)$.

Choose $X = X(\ell)$ where ℓ is a primitive element of L/k. Observe that X^n is in the span of the k-linearly independent set $\{1, X, X^2, \ldots, X^{n-1}\}$. We see that

$$\{X^i Y^j \mid 0 \leq i, j < n\}$$

is a basis for A as a k-vector space. Since $\dim_k A = n^2$ and we have an embedding as a k-algebra in $M_n(L)$, we see that every cyclic algebra is a central simple algebra of degree n.

5.3 Brauer groups over special fields

In general, central simple algebras over arbitrary fields can be quite challenging to understand. They are absolutely an area of active and ongoing research. However, in special cases of especial relevance to the representation theory of finite groups, we can say considerably more. We summarize some of these now.

First of all, a trivial but important observation:

Proposition 5.16. *If k is algebraically closed, then $\mathrm{Br}(k) = 0$. In other words, every central simple algebra over a finite field is split.*

Next, we have the real numbers.

Theorem 5.17 (Frobenius)**.** *The only central division $\mathbb{R}$-algebras are $\mathbb{R}$ and $\mathbb{H}$. In particular,* $\mathrm{Br}(\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$

Also finite fields:

Theorem 5.18 (Wedderburn's Little Theorem)**.** *If k is a finite field, then* $\mathrm{Br}(k) = 0$*. In other words, every central simple algebra over a finite field is split.*

Recall that a *number field* k is a finite extension of $\mathbb{Q}$. Roughly speaking, everything interesting that happens in the representation theory of finite groups occurs over number fields. Due to work of Albert-Brauer-Hasse-Noether, we have a very complete answer in this case. Namely, the construction in the previous section is general enough to capture every example:

Theorem 5.19. *Let k be a number field. Every central simple k-algebra is Brauer-equivalent to a cyclic k-algebra.*

In fact, we know even more if one knows some algebraic number theory. Recall that a number field k has *primes* which may be "finite" or "infinite." To each prime, we have a corresponding local field k_p. The prototypical example is $k = \mathbb{Q}$ where the primes p are the usual primes in $\mathbb{N}$ along with the "infinite" real prime ∞. Here $\mathbb{Q}_p$ is the p-adic field for each finite prime p, and $\mathbb{Q}_\infty = \mathbb{R}$.

Theorem 5.20. *Let k be a number field with prime p. Then*

$$\mathrm{Br}(k_p) \cong \begin{cases} \mathbb{Q}/\mathbb{Z} & \text{if } p \text{ is finite,} \\ \frac{1}{2}\mathbb{Z}/\mathbb{Z} & \text{if } p \text{ is real,} \\ 0 & \text{if } p \text{ is complex.} \end{cases}$$

In particular, the theorem above allows us to define the *Hasse invariant*:

$$\mathrm{inv}_p : \mathrm{Br}(k_p) \to \mathbb{Q}/\mathbb{Z}$$

which is an injective group homomorphism. The notation $\frac{1}{2}\mathbb{Z}/\mathbb{Z}$ for the real case is meant to emphasize that $\mathrm{inv}_\infty([\mathbb{R}]) = 1$ while $\mathrm{inv}_\infty([\mathbb{H}]) = \frac{1}{2}$.

Given a central division algebra A over a number field k and a prime p, the base extension $A \otimes_k k_p$ is a central division k_p-algebra. Thus, for each prime p we have a group homomorphism

$$\mathrm{Br}(k) \to \mathrm{Br}(k_p).$$

Now we have the following local-to-global principle which completely classifies central division algebras over a number field.

Theorem 5.21. *Let k be a number field. There is an exact sequence of abelian groups*

$$0 \to \mathrm{Br}(k) \to \bigoplus_p \mathrm{Br}(k_p) \to \mathbb{Q}/\mathbb{Z} \to 0$$

where the direct sum is over all primes p of k.

References

[AB95] J. L. Alperin and Rowen B. Bell. *Groups and representations*, volume 162 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1995.

[Alp86] J. L. Alperin. *Local representation theory*, volume 11 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1986. Modular representations as an introduction to the local representation theory of finite groups.

[CR06] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras*. AMS Chelsea Publishing, Providence, RI, 2006. Reprint of the 1962 original.

[DF04] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.

[EGH+11] Pavel Etingof, Oleg Golberg, Sebastian Hensel, Tiankai Liu, Alex Schwendner, Dmitry Vaintrob, and Elena Yudovina. *Introduction to representation theory*, volume 59 of *Student Mathematical Library*. American Mathematical Society, Providence, RI, 2011. With historical interludes by Slava Gerovitch.

[FH91] William Fulton and Joe Harris. *Representation theory*, volume 129 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. A first course, Readings in Mathematics.

[GS17] Philippe Gille and Tamás Szamuely. *Central simple algebras and Galois cohomology*, volume 165 of *Cambridge Studies in Advanced*

Mathematics. Cambridge University Press, Cambridge, 2017. Second edition of [MR2266528].

[Lan02] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[Sal99] David J. Saltman. *Lectures on division algebras*, volume 94 of *CBMS Regional Conference Series in Mathematics*. Published by American Mathematical Society, Providence, RI; on behalf of Conference Board of the Mathematical Sciences, Washington, DC, 1999.

[Ser77] Jean-Pierre Serre. *Linear representations of finite groups*. Graduate Texts in Mathematics, Vol. 42. Springer-Verlag, New York-Heidelberg, 1977. Translated from the second French edition by Leonard L. Scott.