Chapter 7

Representation Theory

Recall that a *representation* of a ring R is a ring homomorphism $R \to \mathrm{End}_{\mathbb{Z}}(M)$, where M is an abelian group. Now Proposition 6.14 shows that R-modules are just another way to view representations: every representation $R \to \mathrm{End}_{\mathbb{Z}}(M)$ equips M with the structure of a left R-module, and conversely. In this chapter, we focus on $R = kG$, the group algebra of a finite group G over a field k, and representations $kG \to \mathrm{End}_k(V)$, where V is a finite-dimensional vector space over k. A key tool in this study is the notion of *character*, and we will use it to prove group-theoretic theorems of Burnside and of Frobenius. The chapter ends with a discussion of division rings as well as a theorem characterizing categories of modules which explains why matrix rings arise in the study of semisimple rings.

Section 7.1. Chain Conditions

This chapter begins with rapid rephrasing of some earlier results about groups and rings into the language of modules. We have already proved the Jordan–Hölder Theorem for groups (Theorem 4.55); here is the version of this theorem for modules. [Both of these versions are special cases of a theorem about *operator groups* (Robinson, *A Course in the Theory of Groups*, p. 65).]

Theorem 7.1 (Zassenhaus Lemma). *Given submodules $A \subseteq A^*$ and $B \subseteq B^*$ of a left R-module M over a ring R, there is an isomorphism*

$$\frac{A + (A^* \cap B^*)}{A + (A^* \cap B)} \cong \frac{B + (B^* \cap A^*)}{B + (B^* \cap A)}.$$

Proof. A straightforward adaptation of the proof of Lemma 4.52. •

Definition. A ***series*** (or ***filtration***) of a left R-module M over a ring R is a sequence of submodules, $M = M_0, M_1, \ldots, M_n = \{0\}$, such that

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n = \{0\}.$$

The quotients $M_0/M_1, M_1/M_2, \ldots, M_{n-1}/M_n = M_{n-1}$ are called the ***factor modules*** of this series, and the number of strict inclusions is called the ***length*** of the series; equivalently, the length is the number of nonzero factor modules.

A ***refinement*** of a series is a series $M = M'_0, M'_1, \ldots, M'_t = \{0\}$ having the original series as a subsequence. Two series of a module M are ***equivalent*** if there is a bijection between the lists of nonzero factor modules of each so that corresponding factor modules are isomorphic.

Theorem 7.2 (Schreier Refinement Theorem). *Any two series*

$$M = M_0 \supseteq M_1 \supseteq \cdots \supseteq M_n = \{0\} \quad \textit{and} \quad M = N_0 \supseteq N_1 \supseteq \cdots \supseteq N_t = \{0\}$$

of a left R-module M have equivalent refinements.

Proof. A straightforward adaptation, using the Zassenhaus Lemma, of the proof of Theorem 4.54. •

Recall that a left R-module M is *simple* (or *irreducible*) if $M \neq \{0\}$ and M has no submodules other than $\{0\}$ and M itself. The Correspondence Theorem shows that a submodule N of a left R-module M is a maximal submodule if and only if M/N is simple; indeed, the proof of Corollary 6.25 (a left R-module M is cyclic if and only if $M \cong R/I$ for some left ideal I) can be adapted to show that a left R-module is simple if and only if it is isomorphic to R/I for some maximal left ideal I.

Definition. A ***composition series*** of a module is a series all of whose nonzero factor modules are simple.

A module need not have a composition series; for example, the abelian group $\mathbb{Z}$, considered as a $\mathbb{Z}$-module, has no composition series (Proposition 7.11). Notice that a composition series admits only insignificant refinements; we can only repeat terms (if M_i/M_{i+1} is simple, then it has no proper nonzero submodules and, hence, there is no submodule L with $M_i \supsetneq L \supsetneq M_{i+1}$). More precisely, any refinement of a composition series is equivalent to the original composition series.

Theorem 7.3 (Jordan–Hölder Theorem). *Any two composition series of a left R-module M over a ring R are equivalent. In particular, the length of a composition series, if one exists, is an invariant of M, called the* ***length*** *of M.*

Proof. As we have just remarked, any refinement of a composition series is equivalent to the original composition series. It now follows from the Schreier Refinement Theorem that any two composition series are equivalent; in particular, they have the same length. •

Corollary 7.4. *If a left R-module M has length n, then every ascending or descending chain of submodules of M has length $\leq n$.*

Proof. There is a refinement of the given chain that is a composition series, and so the length of the given chain is at most n. •

The Jordan–Hölder Theorem can be regarded as a kind of unique factorization theorem; for example, we used it in Corollary 4.56, to prove the Fundamental Theorem of Arithmetic. We now use it to prove Invariance of Dimension. If V is an n-dimensional vector space over a field k, then V has length n, for if $v_1, \ldots, v_n$ is a basis of V, then a composition series of V is

$$V = \langle v_1, \ldots, v_n \rangle \supsetneq \langle v_2, \ldots, v_n \rangle \supsetneq \cdots \supsetneq \langle v_n \rangle \supsetneq \{0\}$$

(the factor modules are one-dimensional, hence they are simple k-modules).

In Chapter 5, we considered chain conditions on a ring and its ideals; we now consider chain conditions on modules and submodules.

Definition. A left R-module M over a ring R has **ACC**, the ***ascending chain condition***, if every ascending chain of submodules ***stops***; that is, if

$$S_1 \subseteq S_2 \subseteq S_3 \subseteq \cdots$$

is a chain of submodules, then there is some $t \geq 1$ with

$$S_t = S_{t+1} = S_{t+2} = \cdots .$$

A left R-module M over a ring R has **DCC**, the ***descending chain condition***, if every descending chain of submodules ***stops***; that is, if

$$S_1 \supseteq S_2 \supseteq S_3 \supseteq \cdots$$

is a chain of submodules, then there is some $t \geq 1$ with

$$S_t = S_{t+1} = S_{t+2} = \cdots .$$

We specialize these definitions to R considered as a left R-module.

Definition. A ring R is ***left noetherian*** if it has ACC on left ideals: every ascending chain of left ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ stops; that is, there is some $t \geq 1$ with $I_t = I_{t+1} = I_{t+2} = \cdots$.

If k is a field, then every finite-dimensional k-algebra A is both left and right noetherian, for if $\dim_k(A) = n$, then there are at most n strict inclusions in any ascending chain of left ideals or of right ideals. In particular, if G is a finite group, then kG is finite-dimensional, and so it is left and right noetherian.

Definition. A ring R is ***left artinian*** if it has DCC: every descending chain of left ideals $I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$ stops; that is, there is some $t \geq 1$ with $I_t = I_{t+1} = I_{t+2} = \cdots$.

We define right artinian rings similarly, and there are examples of left artinian rings that are not right artinian (Exercise 7.10 on page 533). If k is a field, then every finite-dimensional k-algebra A is both left and right artinian, for if $\dim_k(A) = n$, then there are at most n strict inclusions in any descending chain of left ideals or of right ideals. In particular, if G is a finite group, then kG is finite-dimensional, and so it is left and right artinian. We conclude that kG has both chain conditions (on the left and on the right) when k is a field and G is a finite group.

The ring $\mathbb{Z}$ is (left) noetherian, but it is not (left) artinian, because the chain

$$\mathbb{Z} \supseteq (2) \supseteq (2^2) \supseteq (2^3) \supseteq \cdots$$

does not stop. In the next section, we will prove that left artinian implies left noetherian.

Proposition 7.5. *Let R be a ring. The following conditions on a left R-module M are equivalent.*

(i) *M has* ACC *on submodules.*

(ii) *Every nonempty family of submodules of M contains a maximal element.*

(iii) *Every submodule of M is finitely generated.*

Proof. Adapt the proof of Proposition 5.33. •

Proposition 5.33 is a special case of Theorem 7.5.

Corollary 7.6 (= Proposition 5.33). *The following conditions on a ring R are equivalent.*

(i) *R is left noetherian; that is, R has* ACC *on left ideals.*

(ii) *Every nonempty family of left ideals of R contains a maximal element.*

(iii) *Every left ideal is finitely generated.*

Proof. Consider R as a left module over itself. •

Here is the analog of Proposition 7.5.

Proposition 7.7. *Let R be a ring. A left R-module M has* DCC *on submodules if and only if every nonempty family of submodules of M contains a minimal element.*

Proof. Adapt the proof of Proposition 5.33, replacing $\subseteq$ by $\supseteq$. •

Corollary 7.8. *A ring R has the* DCC *on left ideals if and only if every nonempty family of left ideals of R contains a minimal element.*

Proof. Consider R as a left module over itself. •

Definition. A left ideal L in a ring R is a ***minimal left ideal*** if $L \neq (0)$ and there is no left ideal J with $(0) \subsetneq J \subsetneq L$.

A ring need not contain minimal left ideals. For example, $\mathbb{Z}$ has no minimal ideals: every nonzero ideal I in $\mathbb{Z}$ has the form $I = (n)$ for some nonzero integer n, and $I = (n) \supsetneq (2n) \neq (0)$.

Example 7.9. Let $R = \mathrm{Mat}_n(k)$, where k is a field. For any ℓ between 1 and n, let $\mathrm{COL}(\ell)$ denote the ℓth columns; that is,

$$\mathrm{COL}(\ell) = \big\{A = [a_{ij}] \in \mathrm{Mat}_n(k) : a_{ij} = 0 \text{ for all } j \neq \ell\big\}.$$

Let $e_1, \dots, e_n$ be the standard basis of k^n. We identify $R = \mathrm{Mat}_n(k)$ with $\mathrm{End}_k(k^n)$, and so $\mathrm{COL}(\ell)$ is identified with

$$\mathrm{COL}(\ell) = \{T\colon k^n \to k^n : T(e_j) = 0 \text{ for } j \neq \ell\}.$$

We claim that $\mathrm{COL}(\ell)$ is a minimal left ideal in R. If I is a nonzero left ideal with $I \subseteq \mathrm{COL}(\ell)$, choose a nonzero $F \in I$; now $F(e_\ell) = u \neq 0$; otherwise F would kill every basis element and, hence, would be 0. To see that $\mathrm{COL}(\ell) \subseteq I$, take $T \in \mathrm{COL}(\ell)$, and write $T(e_\ell) = w$. Since $u \neq 0$, there is $S \in \mathrm{End}_k(k^n)$ with $S(u) = w$. Observe that

$$SF(e_j) = \begin{cases} 0 & \text{if } j \neq \ell; \\ S(u) = w & \text{if } j = \ell. \end{cases}$$

Therefore, $T = SF$, because they agree on a basis; since I is a left ideal, $T \in I$. Therefore, $\mathrm{COL}(\ell) = I$, and $\mathrm{COL}(\ell)$ is a minimal left ideal. ◀

Proposition 7.10.

(i) *Every minimal left ideal L in a ring R is a simple left R-module.*

(ii) *If R is left artinian, then every nonzero left ideal I contains a minimal left ideal.*

Proof.

(i) If L contained a submodule S with $\{0\} \subsetneq S \subsetneq L$, then S would be a left ideal of R, contradicting the minimality of L.

(ii) If $\mathcal{F}$ is the family of all nonzero left ideals contained in I, then $\mathcal{F} \neq \varnothing$ because I is nonzero. By Proposition 7.8, $\mathcal{F}$ has a minimal element, and any such is a minimal left ideal. •

Proposition 7.11. *A left R-module M over a ring R has a composition series if and only if M has both chain conditions on submodules.*

Proof. If M has a composition series of length n, then no sequence of submodules can have length $> n$, lest we violate the Schreier Refinement Theorem (refining a series cannot shorten it). Therefore, M has both chain conditions.

Conversely, let $\mathcal{F}_1$ be the family of all the proper submodules of M. By Proposition 7.8, the maximum condition gives a maximal submodule $M_1 \in \mathcal{F}_1$. Let $\mathcal{F}_2$ be the family of all proper submodules of M_1, and let M_2 be maximal such. Iterating, we have a descending sequence

$$M \supsetneq M_1 \supsetneq M_2 \supsetneq \cdots.$$

If M_n occurs in this sequence, the only obstruction to constructing M_{n+1} is if $M_n = \{0\}$. Since M has both chain conditions, this chain must stop, and so $M_t = \{0\}$ for some t. This chain is a composition series of M, for each M_i is a maximal submodule of its predecessor. •

If Δ is a division ring, then a left Δ-module V is called a ***left vector space*** over Δ. The following definition from Linear Algebra still makes sense here.

Definition. Let V be a left vector space over a division ring Δ. A list $X = x_1, \dots, x_m$ in V is ***linearly dependent*** if

$$x_i \in \langle x_1, \dots, \widehat{x}_i, \dots, x_m \rangle$$

for some i; otherwise, X is called ***linearly independent***.

As for vector spaces over fields, linear independence of $x_1, \dots, x_m$ implies that

$$\langle x_1, \dots, x_m \rangle = \langle x_1 \rangle \oplus \cdots \oplus \langle x_m \rangle.$$

The proper attitude is that theorems about vector spaces over fields have true analogs for left vector spaces over division rings, but the reader should not merely accept the word of a gentleman and scholar that this is so. Here is a proof of Invariance of Dimension similar to the proof (using the Jordan–Hölder Theorem) that we gave on page 527 for vector spaces over fields.

Proposition 7.12. *Let V be a finitely generated*[1] *left vector space over a division ring Δ.*

(i) *V is a direct sum of copies of Δ; that is, every finitely generated left vector space over Δ has a basis.*

(ii) *Any two bases of V have the same number of elements.*

Proof.

(i) Let $V = \langle v_1, \dots, v_n \rangle$, and consider the series

$$V = \langle v_1, \dots, v_n \rangle \supseteq \langle v_2, \dots, v_n \rangle \supseteq \langle v_3, \dots, v_n \rangle \supseteq \cdots \supseteq \langle v_n \rangle \supseteq \{0\}.$$

Denote $\langle v_{i+1}, \dots, v_n \rangle$ by U_i, so that $\langle v_i, \dots, v_n \rangle = \langle v_i \rangle + U_i$. By the Second Isomorphism Theorem,

$$\langle v_i, \dots, v_n \rangle / \langle v_{i+1}, \dots, v_n \rangle = (\langle v_i \rangle + U_i)/U_i \cong \langle v_i \rangle / (\langle v_i \rangle \cap U_i).$$

Therefore, the ith factor module is isomorphic to a quotient of $\langle v_i \rangle \cong \Delta$ if $v_i \neq 0$. Since Δ is a division ring, its only quotients are Δ and $\{0\}$. After throwing away those v_i corresponding to trivial factor modules $\{0\}$, we claim that the remaining v's, denote them by $v_1, \dots, v_m$, form a basis. For all j, we have $v_j \notin \langle v_{j+1}, \dots, v_n \rangle$. The reader may now show, by induction on m, that $\langle v_1 \rangle, \dots, \langle v_m \rangle$ generate their direct sum.

(ii) As in the proof of (i), a basis $v_1, v_2, \dots, v_n$ of V gives a series

$$V = \langle v_1, v_2, \dots, v_n \rangle \supsetneq \langle v_2, \dots, v_n \rangle \supsetneq \langle v_3, \dots, v_n \rangle \supsetneq \cdots \supsetneq \langle v_n \rangle \supsetneq \{0\}.$$

This is a composition series, for every factor module is isomorphic to Δ and, hence, is simple, by Exercise 7.1 on page 532. By the Jordan–Hölder Theorem, the composition series arising from any other basis of V must have the same length. •

[1] This finiteness hypothesis will be removed on page 543.

Another proof of this proposition is sketched in Exercise 7.2 on page 532.

It now follows that every finitely generated left vector space V over a division ring Δ has a left dimension; it will be denoted by $\dim(V)$.

If an abelian group V is a left vector space and a right vector space over a division ring Δ, must its left dimension equal its right dimension? There is an example (Jacobson, *Structure of Rings*, p. 158) of a division ring Δ and an abelian group V, which is a vector space over Δ on both sides, with left dimension 2 and right dimension 3.

We have just seen that dimension is well-defined for left vector spaces over division rings. On the other hand, recall our discussion of IBN: there are noncommutative rings R with $R \cong R \oplus R$ as left R-modules; that is, bases of free modules may not have the same size.

Here is a surprising result.

Theorem 7.13 (Wedderburn). *Every finite division ring Δ is a field; that is, multiplication in Δ is commutative.*

Proof. (Witt)[2] If Z denotes the center of Δ, then Z is a finite field, and so it has q elements (where q is a power of some prime). It follows that Δ is a vector space over Z, and so $|\Delta| = q^n$ for some $n \geq 1$; that is, if we define

$$[\Delta : Z] = \dim_Z(\Delta),$$

then $[\Delta : Z] = n$. The proof will be complete if we can show that $n > 1$ leads to a contradiction.

If $a \in \Delta$, define $C(a) = \{u \in \Delta : ua = au\}$. It is routine to check that $C(a)$ is a subdivision ring of Δ that contains Z: if $u, v \in \Delta$ commute with a, then so do $u + v, uv$, and u^{-1} (when $u \neq 0$). Consequently, $|C(a)| = q^{d(a)}$ for some integer $d(a)$; that is, $[C(a) : Z] = d(a)$. We do not know whether $C(a)$ is commutative, but Exercise 7.5 on page 533 gives

$$[\Delta : Z] = [\Delta : C(a)][C(a) : Z],$$

where $[\Delta : C(a)]$ denotes the dimension of Δ as a left vector space over $C(a)$. That is, $n = [\Delta : C(a)]d(a)$, and so $d(a)$ is a divisor of n.

Since Δ is a division ring, its nonzero elements $\Delta^\times$ form a multiplicative group of order $q^n - 1$. By Exercise 7.4 on page 532, the center of the group $\Delta^\times$ is $Z^\times$ and, if $a \in \Delta^\times$, then its centralizer $C_{\Delta^\times}(a) = C(a)^\times$. Hence, $|Z(\Delta^\times)| = q - 1$ and $|C_{\Delta^\times}(a)| = q^{d(a)} - 1$, where $d(a) \mid n$.

The class equation for $\Delta^\times$ is

$$|\Delta^\times| = |Z^\times| + \sum_i [\Delta^\times : C_{\Delta^\times}(a_i)],$$

where one a_i is chosen from each noncentral conjugacy class. But

$$[\Delta^\times : C_{\Delta^\times}(a_i)] = |\Delta^\times|/|C_{\Delta^\times}(a_i)| = (q^n - 1)/(q^{d(a_i)} - 1),$$

[2] We shall give another proof of this in Theorem 7.127.

so that the class equation becomes

$$q^n - 1 = q - 1 + \sum_i \frac{q^n - 1}{q^{d(a_i)} - 1}. \tag{1}$$

We have already noted that each $d(a_i)$ is a divisor of n, while the condition that a_i is not central says that $d(a_i) < n$.

Recall that the nth cyclotomic polynomial is $\Phi_n(x) = \prod(x - \zeta)$, where ζ ranges over all the primitive nth roots of unity. In Corollary 2.72, we proved that $\Phi_n(q)$ is a common divisor of $q^n - 1$ and $(q^n - 1)/(q^{d(a_i)} - 1)$ for all i, and so Equation (1) gives

$$\Phi_n(q) \mid (q - 1).$$

If $n > 1$ and ζ is a primitive nth root of unity, then $\zeta \neq 1$, and hence ζ is a point on the unit circle to the left of the vertical line through $(1, 0)$. Since q is a prime power, it is a point on the x-axis with $q \geq 2$, and so the distance $|q - \zeta| > q - 1$. Therefore,

$$|\Phi_n(q)| = \prod |q - \zeta| > q - 1,$$

and this contradicts $\Phi_n(q) \mid (q - 1)$. We conclude that $n = 1$; that is, $\Delta = Z$, and so Δ is commutative. •

Exercises

∗ **7.1.** Prove that a division ring Δ is a simple left Δ-module.

∗ **7.2.** Let Δ be a division ring.

(i) Generalize the proof of Lemma 5.68 to prove that $\alpha \preceq S$, defined by $\alpha \in \langle S \rangle$, is a dependency relation from Δ to $\mathcal{P}(\Delta)$ (*dependency relation* is defined on page 337).

(ii) Use Theorem 5.70 to prove that every left vector space over Δ has a basis.

(iii) Use Theorem 5.72 to prove that any two bases of a left vector space over Δ have the same cardinality.

∗ **7.3.** If k is a field and A is a finite-dimensional k-algebra, define

$$L = \{\lambda_a \in \mathrm{End}_k(A) : \lambda_a \colon x \mapsto ax\} \text{ and } R = \{\rho_a \in \mathrm{End}_k(A) : \rho_a \colon x \mapsto xa\}.$$

Prove that L and R are k-algebras, and that there are k-algebra isomorphisms

$$L \cong A \text{ and } R \cong A^{\mathrm{op}}.$$

Hint. Show that the function $A \to L$, defined by $a \mapsto \lambda_a$, is an injective k-algebra map which is surjective because A is finite-dimensional.

∗ **7.4.** Let Δ be a division ring.

(i) Prove that the center $Z(\Delta)$ is a field.

(ii) If $\Delta^\times$ is the multiplicative group of nonzero elements of Δ, prove that $Z(\Delta^\times) = Z(\Delta)^\times$; that is, the center of the multiplicative group $\Delta^\times$ consists of the nonzero elements of $Z(\Delta)$.

∗ **7.5.** (i) Let C be a subdivision ring of a division ring Δ. Prove that Δ is a left vector space over C, and conclude that $[\Delta : C] = \dim_C(\Delta)$ is defined (if Δ is an infinite-dimensional vector space over C, we merely say $\dim_C(\Delta) = \infty$).

(ii) If $Z \subseteq C \subseteq D$ is a tower of division rings with $[\Delta : C]$ and $[C : Z]$ finite, prove that $[\Delta : Z]$ is finite and

$$[\Delta : Z] = [\Delta : C][C : Z].$$

Hint. If $u_1, \ldots, u_m$ is a basis of Δ as a left vector space over C and $c_1, \ldots, c_d$ is a basis of C as a left vector space over Z, show that the set of all $c_i u_j$ (in this order) is a basis of Δ over Z.

∗ **7.6. (Modular Law)** Let A, B, and A' be submodules of a module M. If $A' \subseteq A$, prove that $A \cap (B + A') = (A \cap B) + A'$.

∗ **7.7.** Recall that a ring R has *zero-divisors* if there exist nonzero $a, b \in R$ with $ab = 0$. More precisely, an element a in a ring R is called a ***left zero-divisor*** if $a \neq 0$ and there exists a nonzero $b \in R$ with $ab = 0$; the element b is called a ***right zero-divisor***. Prove that a left artinian ring R having no left zero-divisors must be a division ring.

∗ **7.8.** Let $0 \to A \to B \to C \to 0$ be an exact sequence of left R-modules over a ring R.

(i) Prove that if both A and C have DCC, then B has DCC. Conclude, in this case, that $A \oplus B$ has DCC.

(ii) Prove that if both A and C have ACC, then B has ACC. Conclude, in this case, that $A \oplus B$ has ACC.

(iii) Prove that every ring R that is a direct sum of minimal left ideals is left artinian.

7.9. If R is a (not necessarily commutative) ring, define the polynomial ring $R[x]$ as usual but with the indeterminate x commuting with coefficients in R; thus, $x \in Z(R[x])$. Generalize the Hilbert Basis Theorem to such polynomial rings: if R is left noetherian, then $R[x]$ is left noetherian.

∗ **7.10.** Let R be the ring of all 2×2 upper triangular matrices $\left[\begin{smallmatrix} a & b \\ 0 & c \end{smallmatrix}\right]$, where $a \in \mathbb{Q}$ and $b, c \in \mathbb{R}$. Prove that R is right artinian but not left artinian.

Hint. The ring R is not left artinian because, for every $V \subseteq \mathbb{R}$ that is a vector space over $\mathbb{Q}$,

$$\begin{bmatrix} 0 & V \\ 0 & 0 \end{bmatrix} = \left\{ \begin{bmatrix} 0 & v \\ 0 & 0 \end{bmatrix} : v \in V \right\}$$

is a left ideal.

∗ **7.11.** If k is a field of characteristic 0, then $\mathrm{End}_k(k[t])$ contains the operators

$$x\colon f(t) \mapsto \tfrac{d}{dt} f(t) \quad \text{and} \quad y\colon f(t) \mapsto t f(t).$$

(i) If $A_1(k)$ is the subalgebra of $\mathrm{End}_k(k[t])$ generated by x and y, prove that

$$yx = xy + 1.$$

(ii) Prove that $A_1(k)$ is a left noetherian ring that satisfies the left and right cancellation laws (if $a \neq 0$, then either equation $ab = ac$ or $ba = ca$ implies $b = c$).

(iii) Prove that $A_1(k)$ has no proper nontrivial two-sided ideals.

Remark. This exercise can be generalized by replacing $k[t]$ with $k[t_1, \ldots, t_n]$ and the operators x and y with

$$x_i\colon f(t_1, \ldots, t_n) \mapsto \tfrac{d}{dt_i} f(t_1, \ldots, t_n) \quad \text{and} \quad y_i\colon f(t_1, \ldots, t_n) \mapsto t_i f(t_1, \ldots, t_n).$$

The subalgebra $A_n(k)$ of $\mathrm{End}_k(k[t_1,\dots,t_n])$ generated by $x_1,\dots,x_n,y_1,\dots,y_n$ is called the nth ***Weyl algebra*** over k. Weyl introduced this algebra to model momentum and position operators in Quantum Mechanics. It can be shown that $A_n(k)$ is a left noetherian simple domain for all $n \geq 1$ (McConnell–Robson, *Noncommutative Noetherian Rings*, p. 19). ◀

7.12. Recall that an ***idempotent*** in a ring A is an element $e \in A$ with $e \neq 0$ and $e^2 = e$. If M is a left R-module over a ring R, prove that every direct summand $S \subseteq M$ determines an idempotent in $\mathrm{End}_R(M)$.

Hint. See Corollary 6.28.

∗ **7.13.** (i) **(Peirce Decomposition)** Prove that if e is an idempotent in a ring R, then

$$R = Re \oplus R(1-e).$$

(ii) Let R be a ring having left ideals I and J such that $R = I \oplus J$. Prove that there are idempotents $e \in I$ and $f \in J$ with $1 = e + f$; moreover, $I = Ie$ and $J = Jf$.
Hint. Decompose $1 = e + f$, and show that $ef = 0 = fe$.

Section 7.2. Jacobson Radical

The Jacobson radical, $J(R)$, of a ring R is the analog of the Frattini subgroup in Group Theory; it is a two-sided ideal whose behavior has an impact on R. For example, *semisimple rings* (introduced in the next section) are rings generalizing the group algebra $\mathbb{C}G$ of a finite group G, and they will be characterized in terms of their Jacobson radical and chain conditions.

Definition. If R is a ring, then its ***Jacobson radical*** $J(R)$ is defined to be the intersection of all the maximal left ideals in R. A ring R is called ***Jacobson semisimple*** if $J(R) = (0)$.

Clearly, we can define another Jacobson radical: the intersection of all the maximal *right* ideals. In Proposition 7.20, we shall see that these coincide.

Example 7.14.

(i) The ring $\mathbb{Z}$ is Jacobson semisimple. The maximal ideals in $\mathbb{Z}$ are the nonzero prime ideals (p), and so $J(\mathbb{Z}) = \bigcap_{p \text{ prime}}(p) = (0)$.

(ii) If R is a local ring with unique maximal left ideal P, then $J(R) = P$. For example, $R = \{a/b \in \mathbb{Q} : b \text{ is odd}\}$ is such a ring; its unique maximal ideal is

$$R2 = (2) = \{2a/b : b \text{ is odd}\}.$$

(iii) In Example 7.9, we saw that if $R = \mathrm{Mat}_n(k)$, where k is a field, then $\mathrm{COL}(\ell)$ is a minimal left ideal, where $1 \leq \ell \leq n$ and

$$\mathrm{COL}(\ell) = \big\{A = [a_{ij}] \in \mathrm{Mat}_n(k) : a_{ij} = 0 \text{ for all } j \neq \ell\big\}.$$

We use these minimal left ideals to construct some maximal left ideals. The reader can show that that example generalizes to $R = \mathrm{Mat}_n(\Delta)$, where Δ is

a division ring. Define

$$\text{COL}^*(\ell) = \bigoplus_{j \neq \ell} \text{COL}(j);$$

$\text{COL}^*(\ell)$ is a left ideal with

$$R/\text{COL}^*(\ell) \cong \text{COL}(\ell)$$

as left R-modules. Since $\text{COL}(\ell)$ is a minimal left ideal, it is a simple left R-module, and hence $\text{COL}^*(\ell)$ is a maximal left ideal. Therefore,

$$J(R) \subseteq \bigcap_{\ell} \text{COL}^*(\ell) = (0),$$

so that $R = \text{Mat}_n(\Delta)$ is Jacobson semisimple. ◀

Proposition 7.15. *Given a ring R, the following conditions are equivalent for $x \in R$:*

(i) $x \in J(R)$;

(ii) *for every $r \in R$, the element $1 - rx$ has a left inverse*; *that is, there is $u \in R$ with $u(1 - rx) = 1$;*

(iii) $x(R/I) = (0)$ *for every maximal left ideal I (equivalently, $xM = (0)$ for every simple left R-module M).*

Proof.

(i) $\Rightarrow$ (ii) If there is $r \in R$ with $1 - rx$ not having a left inverse, then $R(1 - rx)$ is a proper left ideal, for it does not contain 1. By Exercise on page 414, there is a maximal left ideal I with $1 - rx \in R(1 - rx) \subseteq I$. Now $rx \in J(R) \subseteq I$, because $J(R)$ is a left ideal, and so $1 = (1 - rx) + rx \in I$, a contradiction.

(ii) $\Rightarrow$ (iii) As we mentioned on page 526, a left R-module M is simple if and only if $M \cong R/I$, where I is a maximal left ideal. Suppose there is a simple module M for which $xM \neq (0)$; hence, there is $m \in M$ with $xm \neq 0$ (of course, $m \neq 0$). It follows that the submodule $Rxm \neq (0)$, for it contains $1xm$. Since M is simple, it has only one nonzero submodule, namely, M itself, and so $Rxm = M$. Therefore, there is $r \in R$ with $rxm = m$; that is, $(1 - rx)m = 0$. By hypothesis, $1 - rx$ has a left inverse, say, $u(1 - rx) = 1$. Hence, $0 = u(1 - rx)m = m$, a contradiction.

(iii) $\Rightarrow$ (i) If $x(R/I) = (0)$, then $x(1 + I) = x + I = I$; that is, $x \in I$. Therefore, if $x(R/I) = (0)$ for every maximal left ideal I, then $x \in \bigcap_I I = J(R)$. •

Notice that condition (ii) in Proposition 7.15 can be restated: $x \in J(R)$ if and only if $1 - z$ has a left inverse for every $z \in Rx$.

The following result is most frequently used in Commutative Algebra.

Corollary 7.16 (Nakayama's Lemma). *If A is a finitely generated left R-module and $JA = A$, where $J = J(R)$ is the Jacobson radical, then $A = \{0\}$.*

In particular, if R is a commutative local ring with unique maximal ideal P and A is a finitely generated R-module with $PA = A$, then $A = \{0\}$.

Proof. Let $a_1, \ldots, a_n$ be a generating set of A that is minimal in the sense that no proper subset generates A. Since $JA = A$, we have $a_1 = \sum_{i=1}^n r_i a_i$, where $r_i \in J$. It follows that

$$(1 - r_1)a_1 = \sum_{i=2}^{n} r_i a_i.$$

Since $r_1 \in J$, Proposition 7.15 says that $1 - r_1$ has a left inverse, say, u, and so $a_1 = \sum_{i=2}^n u r_i a_i$. This is a contradiction, for now A can be generated by the proper subset $\{a_2, \ldots, a_n\}$. The second statement follows at once because $J(R) = P$ when R is a local ring with maximal ideal P. •

Remark. The hypothesis in Nakayama's Lemma that the module A be finitely generated is necessary. For example, it is easy to check that $R = \{a/b \in \mathbb{Q} : b \text{ is odd}\}$ is a local ring with maximal ideal $P = (2)$, while $\mathbb{Q}$ is an R-module with $P\mathbb{Q} = 2\mathbb{Q} = \mathbb{Q}$. ◀

Remark. There are other characterizations of $J(R)$. One such will be given in Proposition 7.20, in terms of elements having two-sided inverses. Another characterization is in terms of *left quasi-regular* elements: those $x \in R$ for which there exist $y \in R$ with $y \circ x = 0$ (here, $y \circ x = x + y - yx$ is the *circle operation*); a left ideal is called ***left quasi-regular*** if each of its elements is left quasi-regular. It can be proved that $J(R)$ is the unique maximal left quasi-regular ideal in R (Lam, *A First Course in Noncommutative Rings*, pp. 67–68). ◀

Recall that an *element* a in a ring R is *nilpotent* if $a^m = 0$ for some $m \geq 1$.

Definition. A left ideal A in a ring R is ***nilpotent*** if there is some integer $m \geq 1$ with $A^m = (0)$.

The left ideal A^m is the set of all sums of products of the form $a_1 \cdots a_m$, where $a_j \in A$ for all j; that is, $A^m = \{\sum_i a_{i1} \cdots a_{im} : a_{ij} \in A\}$. It follows that if A is nilpotent, then every element $a \in A$ is nilpotent; that is, $a^m = 0$. On the other hand, if $a \in R$ is a nilpotent element, it does not follow that Ra, the left ideal generated by a, is a nilpotent ideal. For example, let $R = \mathrm{Mat}_2(k)$, for some commutative ring k, and let $a = \left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right]$. Now $a^2 = \left[\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right]$, but Ra contains $e = \left[\begin{smallmatrix} 0 & 0 \\ 1 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, which is idempotent: $e^2 = e$. Hence, $e^m = e \neq 0$ for all m, and so $(Re)^m \neq (0)$.

Corollary 7.17. *If R is a ring, then $I \subseteq J(R)$ for every nilpotent left ideal I in R.*

Proof. Let $I^n = (0)$, and let $x \in I$. For every $r \in R$, we have $rx \in I$, and so $(rx)^n = 0$. The equation

$$(1 + rx + (rx)^2 + \cdots + (rx)^{n-1})(1 - rx) = 1$$

shows that $1 - rx$ is left invertible, and so $x \in J(R)$, by Proposition 7.15. •

Proposition 7.18. *If R is a left artinian ring, then $J(R)$ is a nilpotent ideal.*

Proof. Denote $J(R)$ by J in this proof. The descending chain of left ideals,

$$J \supseteq J^2 \supseteq J^3 \supseteq \cdots,$$

stops, because R is left artinian; say, $J^m = J^{m+1} = \cdots$. Define $I = J^m$; it follows that $I^2 = I$. We will assume that $I \neq (0)$ and reach a contradiction.

Let $\mathcal{F}$ be the family of all nonzero left ideals B with $IB \neq (0)$; note that $\mathcal{F} \neq \varnothing$ because $I \in \mathcal{F}$. By Proposition 7.8, there is a minimal element $B_0 \in \mathcal{F}$. Choose $b \in B_0$ with $Ib \neq (0)$. Now

$$I(Ib) = I^2 b = Ib \neq (0),$$

so that $Ib \subseteq B_0 \in \mathcal{F}$, and minimality gives $B_0 = Ib$. Since $b \in B_0$, there is $x \in I \subseteq J = J(R)$ with $b = xb$. Hence, $0 = (1 - x)b$. But $1 - x$ has a left inverse, say, u, by Proposition 7.15, so that $0 = u(1 - x)b = b$, a contradiction. •

The Jacobson radical is obviously a left ideal (for it is an intersection of left ideals), but it turns out to be a right ideal as well; that is, $J(R)$ is a two-sided ideal. We begin by giving another source of two-sided ideals (aside from kernels of ring maps).

Definition. If R is a ring and M is a left R-module, the ***annihilator*** of M is

$$\operatorname{ann}(M) = \{a \in R : am = 0 \text{ for all } m \in M\}.$$

Let us show that $\operatorname{ann}(M)$ is a two-sided ideal in R. Now $\operatorname{ann}(M)$ is a left ideal, for if $am = 0$, then $(ra)m = r(am) = 0$; let us prove that it is a right ideal. Let $a \in \operatorname{ann}(M)$, $r \in R$, and $m \in M$. Since M is a left R-module, we have $rm \in M$; since a annihilates every element of M, we have $a(rm) = 0$. Finally, associativity gives $(ar)m = 0$ for all m, and so $ar \in \operatorname{ann}(M)$.

Corollary 7.19.

(i) $J(R) = \bigcap_{\substack{I = \text{maximal} \\ \text{left ideal}}} \operatorname{ann}(R/I)$, *and so* $J(R)$ *is a two-sided ideal in* R.

(ii) $R/J(R)$ *is a Jacobson semisimple ring.*

Proof.

(i) If $x \in J(R)$, then $xM = \{0\}$ for every simple left R-module M, by Proposition 7.15(iii). But $M \cong R/I$ for some maximal left ideal I; that is, $x \in \operatorname{ann}(R/I)$. Thus, $x \in \bigcap_{\substack{I = \text{maximal} \\ \text{left ideal}}} \operatorname{ann}(R/I)$.

For the reverse inclusion, if $x \in \bigcap_{\substack{I = \text{maximal} \\ \text{left ideal}}} \operatorname{ann}(R/I)$, then $xM = \{0\}$ for every left R-module M of the form $M \cong R/I$ for some maximal left ideal I. But every simple left R-module has this form. Therefore, $x \in J(R)$.

(ii) First, $R/J(R)$ is a ring, because $J(R)$ is a two-sided ideal. The Correspondence Theorem for rings shows that if I is any two-sided ideal of R contained in $J(R)$, then $J(R/I) = J(R)/I$; the result follows if $I = J(R)$. •

Let us now show that we could have defined the Jacobson radical using right ideals instead of left ideals.

Definition. A ***unit*** in a ring R is an element $u \in R$ having a two-sided inverse; that is, there is $v \in R$ with

$$uv = 1 = vu.$$

Proposition 7.20.

(i) *If R is a ring, then*

$$J(R) = \{x \in R : 1 + rxs \text{ is a unit in } R \text{ for all } r, s \in R\}.$$

(ii) *If R is a ring and $J'(R)$ is the intersection of all the maximal right ideals of R, then $J'(R) = J(R)$.*

Proof.

(i) Let W be the set of all $x \in R$ such that $1 + rxs$ is a unit for all $r, s \in R$. If $x \in W$, then setting $s = -1$ gives $1 - rx$ a unit for all $r \in R$. Hence, $1 - rx$ has a left inverse, and so $x \in J(R)$, by Proposition 7.15. Therefore, $W \subseteq J(R)$. For the reverse inclusion, let $x \in J(R)$. Since $J(R)$ is a two-sided ideal, by Corollary 7.19, we have $xs \in J(R)$ for all $s \in R$. Proposition 7.15 says that $1 - rxs$ is left invertible for all $r \in R$; that is, there is $u \in R$ with $u(1 - rxs) = 1$. Thus, $u = 1 + urxs$. Now $(-ur)xs \in J(R)$, since $J(R)$ is a two-sided ideal, and so u has a left inverse (Proposition 7.15 once again). On the other hand, u also has a right inverse, namely, $1 - rxs$. By Exercise 6.13, u is a unit in R. Therefore, $1 - rxs$ is a unit in R for all $r, s \in R$. Finally, replacing r by $-r$, we have $1 + rxs$ a unit, and so $J(R) \subseteq W$.

(ii) The description of $J(R)$ in part (i) is left-right symmetric. After proving right-sided versions of Proposition 7.15 and Corollary 7.19, one can see that $J'(R)$ is also described as in part (i). We conclude that $J'(R) = J(R)$. •

Exercises

7.14. (i) If R is a commutative ring with $J(R) = (0)$, prove that R has no nilpotent elements.

(ii) Give an example of a commutative ring R having no nilpotent elements and for which $J(R) \neq (0)$.

7.15. Let k be a field and $R = \mathrm{Mat}_2(k)$. Prove that $a = \left[\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right]$ is left quasi-regular, but that the principal left ideal Ra is not a left quasi-regular ideal.

7.16. Prove that R is Jacobson semisimple if and only if R^{op} is.

7.17. Let I be a two-sided ideal in a ring R. Prove that if $I \subseteq J(R)$, then

$$J(R/I) = J(R)/I.$$

Section 7.3. Semisimple Rings

A group is an abstract object; it is a "cloud," a capital letter G. Of course, there are familiar concrete groups, such as the symmetric group S_n and the general linear group $\mathrm{GL}(V)$ of all nonsingular linear transformations on a vector space V over a field k. The idea underlying Representation Theory is that comparing an abstract group G with familiar groups via homomorphisms can yield concrete information about G.

We begin by showing the connection between group representations and group algebras.

Definition. A ***k-representation*** of a group G is a homomorphism

$$\sigma\colon G \to \mathrm{GL}(V),$$

where V is a vector space over a field k.

Note that if $\dim(V) = n$, then $\mathrm{GL}(V)$ contains an isomorphic copy of S_n [if $v_1, \ldots, v_n$ is a basis of V and $\alpha \in S_n$, then there is a nonsingular linear transformation $T\colon V \to V$ with $T(v_i) = v_{\alpha(i)}$ for all i]; therefore, permutation representations (homomorphisms into S_n) are special cases of k-representations. Representations of groups can be translated into the language of kG-modules (compare the next proof with that of Proposition 6.14).

Proposition 7.21. *Every k-representation $\sigma\colon G \to \mathrm{GL}(V)$ equips V with the structure of a left kG-module*; *denote this module by*

$$V^\sigma.$$

Conversely, every left kG-module V determines a k-representation $\sigma\colon G \to \mathrm{GL}(V)$.

Proof. Given a homomorphism $\sigma\colon G \to \mathrm{GL}(V)$, denote $\sigma(g)\colon V \to V$ by σ_g, and define an action $kG \times V \to V$ by

$$\Big(\sum_{g\in G} a_g g\Big)v = \sum_{g\in G} a_g \sigma_g(v).$$

A routine calculation shows that V, equipped with this scalar multiplication, is a left kG-module.

Conversely, assume that V is a left kG-module. If $g \in G$, then $v \mapsto gv$ defines a linear transformation $T_g\colon V \to V$; moreover, T_g is nonsingular, for its inverse is $T_{g^{-1}}$. It is easily checked that the function $\sigma\colon G \to \mathrm{GL}(V)$, given by $\sigma\colon g \mapsto T_g$, is a k-representation. •

If $\sigma, \tau\colon G \to \mathrm{GL}(V)$ are k-representations, and V^σ, V^τ are the kG-modules determined by σ, τ in Proposition 7.21, when is $V^\tau \cong V^\sigma$? Recall that if $T\colon V \to V$ is a linear transformation, then we made V into a $k[x]$-module V^T by defining $x^i v = T^i(v)$, and we saw, in Proposition 6.11, that if $S\colon V \to V$ is another linear transformation, then $V^S \cong V^T$ if and only if there is a nonsingular $\varphi\colon V \to V$ with $S = \varphi T \varphi^{-1}$.

Proposition 7.22. *Let G be a group and let $\sigma, \tau\colon G \to \mathrm{GL}(V)$ be k-representations, where k is a field. If V^σ and V^τ are the corresponding kG-modules defined in* Proposition 7.21*, then $V^\sigma \cong V^\tau$ as kG-modules if and only if there exists a nonsingular k-linear transformation $\varphi\colon V \to V$ with*

$$\varphi\tau(g) = \sigma(g)\varphi$$

for every $g \in G$.

Remark. We often say that φ ***intertwines*** σ and τ. ◀

Proof. If $\varphi\colon V^\tau \to V^\sigma$ is a kG-isomorphism, then $\varphi\colon V \to V$ is an isomorphism of vector spaces with

$$\varphi\left(\sum a_g g v\right) = \left(\sum a_g g\right)\varphi(v)$$

for all $v \in V$ and all $g \in G$. But the definition of scalar multiplication in V^τ is $gv = \tau(g)(v)$, while the definition of scalar multiplication in V^σ is $gv = \sigma(g)(v)$. Hence, for all $g \in G$ and $v \in V$, we have $\varphi(\tau(g)(v)) = \sigma(g)(\varphi(v))$. Therefore,

$$\varphi\tau(g) = \sigma(g)\varphi$$

for all $g \in G$.

Conversely, the hypothesis gives $\varphi\tau(g) = \sigma(g)\varphi$ for all $g \in G$, where φ is a nonsingular k-linear transformation, and so $\varphi(\tau(g)v) = \sigma(g)\varphi(v)$ for all $g \in G$ and $v \in V$. It now follows easily that φ is a kG-isomorphism; that is, φ preserves scalar multiplication by $\sum_{g\in G} a_g g$. •

We restate the last proposition in terms of matrices.

Corollary 7.23. *Let G be a group and let $\sigma, \tau\colon G \to \mathrm{Mat}_n(k)$ be k-representations. Then $(k^n)^\sigma \cong (k^n)^\tau$ as kG-modules if and only if there is a nonsingular $n \times n$ matrix P with*

$$P\tau(x)P^{-1} = \sigma(x)$$

for every $x \in G$.

Example 7.24. If G is a finite group and V is a vector space over a field k, then the ***trivial homomorphism*** $\sigma\colon G \to \mathrm{GL}(V)$ is defined by $\sigma(x) = 1_V$ for all $x \in G$. The corresponding kG-module V^σ is called the ***trivial*** kG-module: if $v \in V$, then $xv = v$ for all $x \in G$. The trivial module k (also called the ***principal*** kG***-module***) is denoted by

$$V_0(k). \quad ◀$$

We are going to study an important class of rings, *semisimple rings*, which contains most group algebras kG, but we first consider semisimple modules over any ring.

Definition. A left R-module is ***semisimple*** if it is a direct sum of (possibly infinitely many) simple modules.

We now characterize semisimple modules.

Proposition 7.25. *A left R-module M over a ring R is semisimple if and only if every submodule of M is a direct summand.*

Proof. Suppose that M is semisimple; hence, $M = \bigoplus_{j\in J} S_j$, where each S_j is simple. For any subset $I \subseteq J$, define

$$S_I = \bigoplus_{j\in I} S_j.$$

If B is a submodule of M, Zorn's Lemma provides a subset $K \subseteq J$ maximal with the property that $S_K \cap B = \{0\}$. We claim that $M = B \oplus S_K$. We must show that $M = B + S_K$, for their intersection is $\{0\}$ by hypothesis; it suffices to prove that $S_j \subseteq B + S_K$ for all $j \in J$. If $j \in K$, then $S_j \subseteq S_K \subseteq B + S_K$. If $j \notin K$, then maximality gives $(S_K + S_j) \cap B \neq \{0\}$. Thus,

$$s_K + s_j = b \neq 0,$$

where $s_K \in S_K$, $s_j \in S_j$, and $b \in B$. Note that $s_j \neq 0$, lest $s_K = b \in S_K \cap B = \{0\}$. Hence,

$$s_j = b - s_K \in S_j \cap (B + S_K),$$

and so $S_j \cap (B + S_K) \neq \{0\}$. But S_j is simple, so that $S_j = S_j \cap (B + S_K)$, and so $S_j \subseteq B + S_K$, as desired. Therefore, $M = B \oplus S_K$.

Conversely, assume that every submodule of M is a direct summand.

(i) Every nonzero submodule B contains a simple summand.

Let $b \in B$ be nonzero. By Zorn's Lemma, there exists a submodule C of B maximal with $b \notin C$. By Corollary 6.29, C is a direct summand of B: there is some submodule D with $B = C \oplus D$. We claim that D is simple. If D is not simple, we may repeat the argument just given to show that $D = D' \oplus D''$ for nonzero submodules D' and D''. Thus,

$$B = C \oplus D = C \oplus D' \oplus D''.$$

We claim that at least one of $C \oplus D'$ or $C \oplus D''$ does not contain the original element b. Otherwise, $b = c' + d' = c'' + d''$, where $c', c'' \in C$, $d' \in D'$, and $d'' \in D''$. But $c' - c'' = d'' - d' \in C \cap D = \{0\}$ gives $d' = d'' \in D' \cap D'' = \{0\}$. Hence, $d' = d'' = 0$, and so $b = c' \in C$, contradicting the definition of C. If, say, $b \notin C \oplus D'$, then this contradicts the maximality of C.

(ii) M is semisimple.

By Zorn's Lemma, there is a family $(S_j)_{j\in I}$ of simple submodules of M maximal such that the submodule U they generate is their direct sum: $U = \bigoplus_{j\in I} S_j$. By hypothesis, U is a direct summand: $M = U \oplus V$ for some submodule V of M. If $V = \{0\}$, we are done. Otherwise, by part (i), there is some simple submodule S contained in V that is a summand: $V = S \oplus V'$ for some $V' \subseteq V$. The family $\{S\} \cup (S_j)_{j\in I}$ violates the maximality of the first family of simple submodules, for this larger family also generates its direct sum. Therefore, $V = \{0\}$ and M is left semisimple. •

Corollary 7.26. *Every submodule and every quotient module of a semisimple left module M is itself semisimple.*

Proof. Let B be a submodule of M. Every submodule C of B is, clearly, a submodule of M. Since M is semisimple, C is a direct summand of M and so, by Corollary 6.29, C is a direct summand of B. Hence, B is semisimple, by Proposition 7.25.

Let M/H be a quotient of M. Now H is a direct summand of M, so that $M = H \oplus H'$ for some submodule H' of M. But H' is semisimple, by the first paragraph, and $M/H \cong H'$. •

Recall that if a ring R is viewed as a left R-module, then its submodules are its left ideals; moreover, a left ideal is minimal if and only if it is a simple left R-module.

Definition. A *ring* R is ***left semisimple***[3] if it is a direct sum of minimal left ideals.

The next proposition generalizes Example 7.14(iii).

Proposition 7.27. *Let R be a left semisimple ring.*

(i) *R is a direct sum of finitely many minimal left ideals.*

(ii) *R has both chain conditions on left ideals.*

Proof.

(i) Since R is left semisimple, it is a direct sum of minimal left ideals: $R = \bigoplus_i L_i$. Let $1 = \sum_i e_i$, where $e_i \in L_i$. If $r = \sum_i r_i \in \bigoplus_i L_i$, then $r = 1r$ and so $r_i = e_i r_i$. Hence, if $e_i = 0$, then $L_i = 0$. We conclude that there are only finitely many nonzero L_i; that is, $R = L_1 \oplus \cdots \oplus L_n$.

(ii) The series

$$R = L_1 \oplus \cdots \oplus L_n \supseteq L_2 \oplus \cdots \oplus L_n \supseteq \cdots \supseteq L_n \supseteq (0)$$

is a composition series, for the factor modules are $L_1, \ldots, L_n$, which are simple. It follows from Proposition 7.11 that R (as a left R-module over itself) has both chain conditions. •

Corollary 7.28. *The direct product $R = R_1 \times \cdots \times R_m$ of left semisimple rings $R_1, \ldots, R_m$ is also a left semisimple ring.*

Proof. Since each R_i is left semisimple, it is a direct sum of minimal left ideals, say, $R_i = J_{i1} \oplus \cdots \oplus J_{i\,t(i)}$. Each J_{ik} is a left ideal in R, not merely in R_i, as we saw in Example 6.5. It follows that J_{ik} is a minimal left ideal in R. Hence, R is a direct sum of minimal left ideals, and so it is a left semisimple ring. •

Corollary 7.29.

(i) *If R is a left semisimple ring, then every left R-module M is a semisimple module.*

[3] We can define a ring to be ***right semisimple*** if it is a direct sum of minimal right ideals, but we shall see, in Corollary 7.45, that a ring is a left semisimple ring if and only if it is right semisimple.

(ii) *If I is a two-sided ideal in a left semisimple ring R, then the quotient ring R/I is also a semisimple ring.*

Proof.

(i) There is a free left R-module F and a surjective R-map $\varphi\colon F \to M$. Now R is a semisimple module over itself (this is the definition of semisimple ring), and so F is a semisimple module (for F is a direct sum of copies of R). Thus, M is a quotient of the semisimple module F, and so it is itself semisimple, by Corollary 7.26.

(ii) First, R/I is a ring, because I is a two-sided ideal. The left R-module R/I is semisimple, by (i), and so it is a direct sum $R/I \cong \bigoplus S_j$, where the S_j are simple left R-modules. But each S_j is also simple as a left (R/I)-module, for any (R/I)-submodule of S_j is also an R-submodule of S_j. Therefore, R/I is semisimple. •

It follows that a finite direct product of fields is a commutative semisimple ring (we will prove the converse later). For example, if $n = p_1 \cdots p_t$ is a squarefree integer, then $\mathbb{I}_n \cong \mathbb{I}_{p_1} \times \cdots \times \mathbb{I}_{p_t}$ is a semisimple ring. Similarly, if k is a field and $f(x) \in k[x]$ is a product of distinct irreducible polynomials, then $k[x]/(f(x))$ is a semisimple ring.

We can now generalize Proposition 7.12: every (not necessarily finitely generated) left vector space over a division ring Δ has a basis. Every division ring is a left semisimple ring, and Δ itself is the only minimal left ideal. Therefore, every left Δ-module M is a direct sum of copies of Δ; say, $M = \bigoplus_{i\in I} \Delta_i$. If $x_i \in \Delta_i$ is nonzero, then $X = (x_i)_{i\in I}$ is a basis of M. This observation explains the presence of Zorn's Lemma in the proof of Proposition 7.25.

The next result shows that left semisimple rings can be characterized in terms of the Jacobson radical.

Theorem 7.30. *A ring R is left semisimple if and only if it is left artinian and Jacobson semisimple*; *that is, $J(R) = (0)$.*

Proof. If R is left semisimple, then there is a left ideal I with $R = J(R) \oplus I$, by Proposition 7.25. It follows from Exercise 7.13 on page 534 that there are idempotents $e \in J(R)$ and $f \in I$ with $1 = e + f$. Since $e \in J(R)$, Proposition 7.15 says that $f = 1 - e$ has a left inverse; there is $u \in R$ with $uf = 1$. But f is an idempotent, so that $f = f^2$. Hence, $1 = uf = uf^2 = (uf)f = f$, so that $e = 1 - f = 0$. Since $J(R)e = J(R)$, by Exercise 7.13 on page 534, we have $J(R) = (0)$. Finally, Proposition 7.27(ii) shows that R is left artinian.

Conversely, assume that R is left artinian and $J(R) = (0)$. We show first that if I is a minimal left ideal of R, then I is a direct summand of R. Now $I \neq (0)$, and so $I \not\subseteq J(R)$; therefore, there is a maximal left ideal A not containing I. Since I is minimal, it is simple, so that $I \cap A$ is either I or (0). But $I \cap A = I$ implies $I \subseteq A$, a contradiction, and so $I \cap A = (0)$. Maximality of A gives $I + A = R$, and so $R = I \oplus A$.

Choose a minimal left ideal I_1, which exists because R is left artinian. As we have just seen, $R = I_1 \oplus B_1$ for some left ideal B_1. Now B_1 contains a minimal left ideal, say, I_2, by Proposition 7.10, and so there is a left ideal B_2 with $B_1 = I_2 \oplus B_2$. This construction can be iterated to produce a strictly decreasing chain of left ideals $B_1 \supsetneq B_2 \supsetneq \cdots \supsetneq B_r$ as long as $B_r \neq (0)$. If $B_r \neq (0)$ for all r, then DCC is violated. Therefore, $B_r = (0)$ for some r, so that $R = I_1 \oplus \cdots \oplus I_r$ and R is semisimple. •

Note that the chain condition is needed. For example, $\mathbb{Z}$ is Jacobson semisimple, but $\mathbb{Z}$ is not a semisimple ring.

We can now prove the following remarkable result.

Theorem 7.31 (Hopkins–Levitzki). *If a ring R is left artinian, then it is left noetherian.*

Proof. It suffices to prove that R, regarded as a left module over itself, has a composition series, for then Proposition 7.11 applies at once to show that R has the ACC on left ideals (its submodules).

If $J = J(R)$ denotes the Jacobson radical, then $J^m = (0)$ for some $m \geq 1$, by Proposition 7.18, and so there is a descending chain

$$R = J^0 \supseteq J \supseteq J^2 \supseteq J^3 \supseteq \cdots \supseteq J^m = (0).$$

Since each J^q is an ideal in R, it has DCC, as does its quotient J^q/J^{q+1}. Now R/J is a semisimple ring, by Theorem 7.30 [it is left artinian, being a quotient of a left artinian ring, and Jacobson semisimple, by Corollary 7.19(ii)]. The factor module J^q/J^{q+1} is an (R/J)-module; hence, by Corollary 7.26, J^q/J^{q+1} is a semisimple module, and so it can be decomposed into a direct sum of (perhaps infinitely many) simple (R/J)-modules. But there can be only finitely many summands, for every (R/J)-submodule of J^q/J^{q+1} is necessarily an R-submodule, and J^q/J^{q+1} has DCC on R-submodules. Hence, there are simple (R/J)-modules S_i with

$$J^q/J^{q+1} = S_1 \oplus S_2 \oplus \cdots \oplus S_p.$$

Throwing away one simple summand at a time yields a series of J^q/J^{q+1} whose ith factor module is

$$(S_i \oplus S_{i+1} \oplus \cdots \oplus S_p)/(S_{i+1} \oplus \cdots \oplus S_p) \cong S_i.$$

Now the simple (R/J)-module S_i is also a simple R-module, for it is an R-module annihilated by J, so that we have constructed a composition series for J^q/J^{q+1} as a left R-module. Finally, refine the original series for R in this way, for every q, to obtain a composition series for R. •

The converse of Theorem 7.31 is false: $\mathbb{Z}$ is noetherian but not artinian.

The next result is fundamental.

Theorem 7.32 (Maschke's Theorem). *If G is a finite group and k is a field whose characteristic does not divide $|G|$, then kG is a left semisimple ring.*

Remark. The hypothesis holds if k has characteristic 0. ◀

Proof. By Proposition 7.25, it suffices to prove that every left ideal I of kG is a direct summand. Since k is a field, kG is a vector space over k and I is a subspace. By Corollary 5.48, I is a (vector space) direct summand: there is a subspace V (which may not be a left ideal in kG) with $kG = I \oplus V$. There is a k-linear transformation $d\colon kG \to I$ with $d(b) = b$ for all $b \in I$ and with $\ker d = V$ [each $u \in kG$ has a unique expression of the form $u = b + v$, where $b \in I$ and $v \in V$, and $d(u) = b$]. Were d a kG-map, not merely a k-map, then we would be done, by the criterion of Corollary 6.28 [I is a summand of kG if and only if it is a retract: there is a kG-map $D\colon kG \to I$ with $D(u) = u$ for all $u \in I$]. We now force d to be a kG-map by an "averaging process."

Define $D : kG \to kG$ by

$$D(u) = \frac{1}{|G|} \sum_{x \in G} xd(x^{-1}u)$$

for all $u \in kG$. Note that $|G| \neq 0$ in k, by the hypothesis on the characteristic of k, and so $1/|G|$ is defined. It is obvious that D is a k-map.

(i) $\operatorname{im} D \subseteq I$.

If $u \in kG$ and $x \in G$, then $d(x^{-1}u) \in I$ (because $\operatorname{im} d \subseteq I$), and $xd(x^{-1}u) \in I$ because I is a left ideal. Therefore, $D(u) \in I$, for each term in the sum defining $D(u)$ lies in I.

(ii) If $b \in I$, then $D(b) = b$.

Since $b \in I$, so is $x^{-1}b$, and so $d(x^{-1}b) = x^{-1}b$. Hence, $xd(x^{-1}b) = xx^{-1}b = b$. Therefore, $\sum_{x \in G} xd(x^{-1}b) = |G|b$, and so $D(b) = b$.

(iii) D is a kG-map.

It suffices to prove that $D(gu) = gD(u)$ for all $g \in G$ and all $u \in kG$:

$$\begin{aligned} gD(u) &= \frac{1}{|G|} \sum_{x \in G} gxd(x^{-1}u) = \frac{1}{|G|} \sum_{x \in G} gxd(x^{-1}g^{-1}gu) \\ &= \frac{1}{|G|} \sum_{y = gx \in G} yd(y^{-1}gu) = D(gu) \end{aligned}$$

(as x ranges over all of G, so does $y = gx$). •

The converse of Maschke's Theorem is true: if G is a finite group and k is a field whose characteristic p divides $|G|$, then kG is not left semisimple; a proof is outlined in Exercise 7.20 on page 549.

Before analyzing left semisimple rings further, let us give several characterizations of them.

Proposition 7.33. *The following conditions on a ring R are equivalent.*

(i) *R is left semisimple.*

(ii) *Every left R-module is a semisimple module.*

(iii) *Every left R-module is injective.*

(iv) *Every short exact sequence of left R-modules splits.*

(v) *Every left R-module is projective.*

Proof.

(i) $\Rightarrow$ (ii). This follows at once from Corollary 7.26, which says that if R is a semisimple ring, then every left R-module is a semisimple module.

(ii) $\Rightarrow$ (iii). Let E be a left R-module; Proposition 6.84 says that E is injective if every exact sequence $0 \to E \to B \to C \to 0$ splits. By hypothesis, B is a semisimple module, and so Proposition 7.25 implies that the sequence splits; thus, E is injective.

(iii) $\Rightarrow$ (iv). If $0 \to A \to B \to C \to 0$ is an exact sequence, then it must split because, as every module, A is injective, by Proposition 6.84.

(iv) $\Rightarrow$ (v). Given a module M, there is an exact sequence

$$0 \to F' \to F \to M \to 0,$$

where F is free. This sequence splits, by hypothesis, and so $F \cong M \oplus F'$. Therefore, M is a direct summand of a free module, and hence it is projective, by Theorem 6.76.

(v) $\Rightarrow$ (i). If I is a left ideal of R, then

$$0 \to I \to R \to R/I \to 0$$

is an exact sequence. By hypothesis, R/I is projective, and so this sequence splits, by Proposition 6.73; thus, I is a direct summand of R. By Proposition 7.25, R is a semisimple left R-module; that is, R is a left semisimple ring. •

Modules over semisimple rings are so nice that there is a notion of *global dimension* of a ring R that measures how far removed R is from being semisimple. We will discuss global dimension in Chapter 10.

In order to give more examples of left semisimple rings, we look at endomorphism rings of direct sums. Consider $\mathrm{Hom}_R(A, B)$, where both A and B are left R-modules that are finite direct sums: say, $A = \bigoplus_{i=1}^{n} A_i$ and $B = \bigoplus_{j=1}^{m} B_j$. Since a direct product of a finite family of modules is their direct sum, Theorem 6.45 gives

$$\mathrm{Hom}_R(A, B) \cong \bigoplus_{i,j} \mathrm{Hom}_R(A_i, B_j).$$

More precisely, if $\alpha_i \colon A_i \to A$ is the ith injection and $p_j \colon B \to B_j$ is the jth projection, then each $f \in \mathrm{Hom}_R(A, B)$ gives maps

$$f_{ji} = p_j f \alpha_i \in \mathrm{Hom}_R(A_i, B_j).$$

Thus, f defines a ***generalized*** $m \times n$ ***matrix*** $[f_{ji}]$ (we call $[f_{ji}]$ a *generalized* matrix because entries in different positions need not lie in the same algebraic system). The map $f \mapsto [f_{ji}]$ is an isomorphism $\mathrm{Hom}_R(A, B) \to \bigoplus_{ij} \mathrm{Hom}_R(A_i, B_j)$. Similarly, if $g \colon B \to C$, where $C = \bigoplus_{k=1}^{\ell} C_k$, then g defines a generalized $\ell \times m$ matrix $[g_{kj}]$, where $g_{kj} = q_k g \beta_j \colon B_j \to C_k$, $\beta_j \colon B_j \to B$ are the injections, and $q_k \colon C \to C_k$ are the projections.

The composite $gf\colon A \to C$ defines a generalized $\ell \times n$ matrix, and we claim that it is given by matrix multiplication: $(gf)_{ki} = \sum_j g_{kj} f_{ji}$:

$$\sum_j g_{kj} f_{ji} = \sum_j q_k g \beta_j p_j f \alpha_i = q_k g (\sum_j \beta_j p_j) f \alpha_i = q_k g f \alpha_i = (gf)_{ki},$$

because $\sum_j \beta_j p_j = 1_B$.

By adding some hypotheses, we can pass from generalized matrices to honest matrices.

Proposition 7.34. *Let $V = \bigoplus_{i=1}^n V_i$ be a left R-module. If there is a left R-module L and, for each i, an isomorphism $\varphi_i\colon V_i \to L$, then there is a ring isomorphism*

$$\mathrm{End}_R(V) \cong \mathrm{Mat}_n(\mathrm{End}_R(L)).$$

Proof. Define $\theta\colon \mathrm{End}_R(V) \to \mathrm{Mat}_n(\mathrm{End}_R(L))$ by

$$\theta\colon f \mapsto [\varphi_j p_j f \alpha_i \varphi_i^{-1}],$$

where $\alpha_i\colon V_i \to V$ and $p_j\colon V \to V_j$ are injections and projections, respectively. That θ is an additive isomorphism is just the identity

$$\mathrm{Hom}\Big(\bigoplus_i V_i, \bigoplus_i V_i\Big) \cong \bigoplus_{i,j} \mathrm{Hom}(V_i, V_j),$$

which holds when the index sets are finite. In the paragraph above defining generalized matrices, the home of the ij entry is $\mathrm{Hom}_R(V_i, V_j)$, whereas the present home of this entry is the isomorphic replica $\mathrm{Hom}_R(L, L) = \mathrm{End}_R(L)$.

We now show that θ preserves multiplication. If $g, f \in \mathrm{End}_R(V)$, then $\theta(gf) = [\varphi_j p_j g f \alpha_i \varphi_i^{-1}]$, while the matrix product is

$$\begin{aligned}
\theta(g)\theta(f) &= \Big[\sum_k (\varphi_j p_j g \alpha_k \varphi_k^{-1})(\varphi_k p_k f \alpha_i \varphi_i^{-1})\Big] \\
&= \Big[\sum_k \varphi_j p_j g \alpha_k p_k f \alpha_i \varphi_i^{-1}\Big] \\
&= \Big[\varphi_j p_j g \Big(\sum_k \alpha_k p_k\Big) f \alpha_i \varphi_i^{-1}\Big] \\
&= \Big[\varphi_j p_j g f \alpha_i \varphi_i^{-1}\Big]. \quad \bullet
\end{aligned}$$

Corollary 7.35. *If V is an n-dimensional left vector space over a division ring Δ, then there is an isomorphism of rings*

$$\mathrm{End}_\Delta(V) \cong \mathrm{Mat}_n(\Delta)^{\mathrm{op}}.$$

Proof. The isomorphism $\mathrm{End}_k(V) \cong \mathrm{Mat}_n(\Delta^{\mathrm{op}})$ is the special case of Proposition 7.34 for $V = V_1 \oplus \cdots \oplus V_n$, where each V_i is one-dimensional, and hence is isomorphic to Δ. Note that $\mathrm{End}_\Delta(\Delta) \cong \Delta^{\mathrm{op}}$, by Proposition 6.16. Now apply Proposition 6.17, which says that $\mathrm{Mat}_n(\Delta^{\mathrm{op}}) \cong \mathrm{Mat}_n(\Delta)^{\mathrm{op}}$. $\bullet$

The next result involves a direct sum decomposition at the opposite extreme of that in Proposition 7.34.

Corollary 7.36. *Let an R-module M be a direct sum $M = B_1 \oplus \cdots \oplus B_m$ in which $\mathrm{Hom}_R(B_i, B_j) = \{0\}$ for all $i \neq j$. Then there is a ring isomorphism*

$$\mathrm{End}_R(M) \cong \mathrm{End}_R(B_1) \times \cdots \times \mathrm{End}_R(B_m).$$

Proof. If $f, g \in \mathrm{End}_R(M)$, let $[f_{ij}]$ and $[g_{ij}]$ be their generalized matrices. It suffices to show that $[g_{ij}][f_{ij}]$ is the diagonal matrix

$$\mathrm{diag}(g_{11}f_{11}, \ldots, g_{mm}f_{mm}).$$

But if $i \neq j$, then $g_{ik}f_{kj} \in \mathrm{Hom}_R(B_i, B_j) = 0$; hence, $(gf)_{ij} = \sum_k g_{ik}f_{kj} = 0$. •

We can now give more examples of semisimple rings. The Wedderburn–Artin Theorems will say that there are no others.

Proposition 7.37.

(i) *If Δ is a division ring and V is a left vector space over Δ with $\dim(V) = n$, then $\mathrm{End}_\Delta(V) \cong \mathrm{Mat}_n(\Delta^{\mathrm{op}})$ is a left semisimple ring.*

(ii) *If $\Delta_1, \ldots, \Delta_m$ are division rings, then*

$$\mathrm{Mat}_{n_1}(\Delta_1) \times \cdots \times \mathrm{Mat}_{n_m}(\Delta_m)$$

is a left semisimple ring.

Proof.

(i) By Proposition 7.34, we have

$$\mathrm{End}_\Delta(V) \cong \mathrm{Mat}_n(\mathrm{End}_\Delta(\Delta));$$

by Proposition 6.16, $\mathrm{End}_\Delta(\Delta) \cong \Delta^{\mathrm{op}}$. Therefore, $\mathrm{End}_\Delta(V) \cong \mathrm{Mat}_n(\Delta^{\mathrm{op}})$.

Let us now show that $\mathrm{End}_\Delta(V)$ is semisimple. If $v_1, \ldots, v_n$ is a basis of V, define

$$\mathrm{COL}(j) = \{T \in \mathrm{End}_\Delta(V) : T(v_i) = 0 \text{ for all } i \neq j\}.$$

It is easy to see that $\mathrm{COL}(j)$ is a left ideal in $\mathrm{End}_\Delta(V)$: if $S \in \mathrm{End}_\Delta(V)$, then $S(Tv_i) = 0$ for all $i \neq j$. Recall Example 7.9: if we look in $\mathrm{Mat}_n(\Delta^{\mathrm{op}}) \cong \mathrm{End}_\Delta(V)$, then $\mathrm{COL}(j)$ corresponds to $\mathrm{COL}(j)$, all those matrices whose entries off the jth column are 0. It is obvious that

$$\mathrm{Mat}_n(\Delta^{\mathrm{op}}) = \mathrm{COL}(1) \oplus \cdots \oplus \mathrm{COL}(n).$$

Hence, $\mathrm{End}_\Delta(V)$ is also such a direct sum. We saw, in Example 7.14(iii), that each $\mathrm{COL}(\ell)$ is a minimal left ideal, and so $\mathrm{End}_\Delta(V)$ is a left semisimple ring.

(ii) This follows at once from part (i) and Corollary 7.28, for if Δ is a division ring, then so is Δ^{op}, by Exercise 6.12 on page 416. •

Corollary 7.38. *If V is an n-dimensional left vector space over a division ring Δ, then the minimal left ideals $\mathrm{COL}(\ell)$, for $1 \leq \ell \leq n$, in $\mathrm{End}_\Delta(V)$ are all isomorphic.*

Proof. Let $v_1, \ldots, v_n$ be a basis of V. For each ℓ, define $p_\ell \colon V \to V$ to be the linear transformation that interchanges v_ℓ and v_1 and that fixes all the other v_j. It is easy to see that $T \mapsto Tp_\ell$ is an isomorphism $\mathrm{COL}(1) \to \mathrm{COL}(\ell)$. •

There may be minimal left ideals other than $\text{COL}(\ell)$ for some ℓ. However, we will see [in Lemma 7.49(ii)] that all the minimal left ideals in $\text{End}_\Delta(V)$ are isomorphic to one of these.

Definition. A ring R is ***simple*** if it is not the zero ring and it has no proper nonzero two-sided ideals.

Our language is a little deceptive. It is true that left artinian simple rings are semisimple (Proposition 7.47), but there are simple rings that are not semisimple.

Proposition 7.39. *If Δ is a division ring, then $R = \text{Mat}_n(\Delta)$ is a simple ring.*

Proof. A ***matrix unit*** E_{pq} is the $n \times n$ matrix whose p, q entry is 1 and all of whose other entries are 0. The matrix units form a basis for $\text{Mat}_n(\Delta)$ viewed as a left vector space over Δ, for each matrix $A = [a_{ij}]$ has a unique expression

$$A = \sum_{i,j} a_{ij} E_{ij}.$$

[Of course, this says that $\dim_\Delta(\text{Mat}_n(\Delta)) = n^2$.] A routine calculation shows that matrix units multiply according to the following rule:

$$E_{ij}E_{k\ell} = \begin{cases} 0 & \text{if } j \neq k \\ E_{i\ell} & \text{if } j = k. \end{cases}$$

Suppose that N is a nonzero two-sided ideal in $\text{Mat}_n(\Delta)$. If A is a nonzero matrix in N, it has a nonzero entry; say, $a_{ij} \neq 0$. Since N is a two-sided ideal, N contains $E_{pi}AE_{jq}$ for all p, q. But

$$E_{pi}AE_{jq} = E_{pi}\sum_{k,\ell} a_{k\ell}E_{k\ell}E_{jq} = E_{pi}\sum_{k} a_{kj}E_{kq} = \sum_{k} a_{kj}E_{pi}E_{kq} = a_{ij}E_{pq}.$$

Since $a_{ij} \neq 0$ and Δ is a division ring, $a_{ij}^{-1} \in \Delta$, and so $E_{pq} \in N$ for all p, q. But the collection of all E_{pq} span the left vector space $\text{Mat}_n(\Delta)$ over Δ, and so $N = \text{Mat}_n(\Delta)$. •

Exercises

7.18. Prove that a finitely generated left semisimple R-module M over a ring R is a direct sum of a finite number of simple left modules.

7.19. Let A be an n-dimensional k-algebra over a field k. Prove that A can be imbedded as a k-subalgebra of $\text{Mat}_n(k)$.

Hint. If $a \in A$, define $L_a\colon A \to A$ by $L_a\colon x \mapsto ax$.

∗ **7.20.** Let G be a finite group, and let k be a commutative ring. Define $\varepsilon\colon kG \to k$ by

$$\varepsilon\Big(\sum_{g\in G} a_g g\Big) = \sum_{g\in G} a_g$$

(this map is called the ***augmentation***, and its kernel, denoted by $\mathcal{G}$, is called the ***augmentation ideal***).

(i) Prove that ε is a kG-map and that $kG/\mathcal{G} \cong k$ as k-algebras. Conclude that $\mathcal{G}$ is a two-sided ideal in kG.

(ii) Prove that $kG/\mathcal{G} \cong V_0(k)$, where $V_0(k)$ is k viewed as a trivial kG-module.
Hint. $\mathcal{G}$ is a two-sided ideal containing $xu - u = (x-1)u$.

(iii) Use part (ii) to prove that if $kG = \mathcal{G} \oplus V$, then $V = \langle v \rangle$, where $v = \sum_{g \in G} g$.
Hint. Argue as in Example 7.43.

(iv) Assume that k is a field whose characteristic p does divide $|G|$. Prove that kG is not left semisimple.
Hint. First show that $\varepsilon(v) = 0$, and then show that the short exact sequence

$$0 \to \mathcal{G} \to kG \xrightarrow{\varepsilon} k \to 0$$

does not split. (If G is a finite p-group and k is a field of characteristic p, then the Jacobson radical $J(kG)$ is the augmentation ideal; see Lam, *A First Course in Noncommutative Rings*, p. 131).

$*$ **7.21.** Let M be a left R-module over a semisimple ring R. Prove that M is indecomposable if and only if M is simple.

7.22. If Δ is a division ring, prove that every two minimal left ideals in $\mathrm{Mat}_n(\Delta)$ are isomorphic. (Compare Corollary 7.38.)

7.23. Let $T\colon V \to V$ be a linear transformation, where V is a vector space over a field k, and let $k[T]$ be defined by

$$k[T] = k[x]/(m(x)),$$

where $m(x)$ is the minimum polynomial of T.

(i) If $m(x) = \prod_p p(x)^{e_p}$, where the $p(x) \in k[x]$ are distinct irreducible polynomials and $e_p \geq 1$, prove that $k[T] \cong \prod_p k[x]/(p(x)^{e_p})$.

(ii) Prove that $k[T]$ is a semisimple ring if and only if $m(x)$ is a product of distinct linear factors. (In Linear Algebra, we show that this last condition is equivalent to T being *diagonalizable*; that is, any matrix of T [arising from some choice of basis of T] is similar to a diagonal matrix.)

7.24. (i) If $\mathbb{H}$ is the division ring of real quaternions, prove that its multiplicative group $\mathbb{H}^\times$ has a finite subgroup that is not cyclic. Compare with Theorem 2.46.

(ii) If Δ is a division ring whose center is a field of characteristic $p > 0$, prove that every finite subgroup G of $\Delta^\times$ is cyclic.
Hint. Consider $\mathbb{F}_p G$, and use Theorem 7.13.

Section 7.4. Wedderburn–Artin Theorems

We are now going to prove the converse of Proposition 7.37(ii): every left semisimple ring is isomorphic to a direct product of matrix rings over division rings. The first step shows how division rings arise.

Theorem 7.40 (Schur's Lemma). *Let M and M' be simple left R-modules over a ring R.*

(i) *Every nonzero R-map $f\colon M \to M'$ is an isomorphism.*

(ii) $\mathrm{End}_R(M)$ *is a division ring. In particular, if* L *is a minimal left ideal in a ring* R*, then* $\mathrm{End}_R(L)$ *is a division ring.*

Proof.

(i) Since M is simple, it has only two submodules: M itself and $\{0\}$. Now the submodule $\ker f \neq M$ because $f \neq 0$, so that $\ker f = \{0\}$ and f is an injection. Similarly, the submodule $\operatorname{im} f \neq \{0\}$, so that $\operatorname{im} f = M'$ and f is a surjection.

(ii) If $f\colon M \to M$ and $f \neq 0$, then f is an isomorphism, by part (i), and hence it has an inverse $f^{-1} \in \mathrm{End}_R(M)$. Thus, $\mathrm{End}_R(M)$ is a division ring. •

The second step investigates minimal left ideals.

Lemma 7.41. *If* L *and* L' *are minimal left ideals in a ring* R*, then each of the following statements implies the one below it:*

(i) $LL' \neq (0)$.

(ii) $\mathrm{Hom}_R(L, L') \neq \{0\}$ *and there exists* $b' \in L'$ *with* $L' = Lb'$.

(iii) $L \cong L'$ *as left* R*-modules.*

If also $L^2 \neq (0)$*, then* (iii) *implies* (i) *and the three statements are equivalent.*

Proof.

(i) $\Rightarrow$ (ii) If $LL' \neq (0)$, then there exists $b \in L$ and $b' \in L'$ with $bb' \neq 0$. Thus, the function $f\colon L \to L'$, defined by $x \mapsto xb'$, is a nonzero R-map, and so $\mathrm{Hom}_R(L, L') \neq \{0\}$. Moreover, $Lb' = L'$, for it is a nonzero submodule of the minimal left ideal L'.

(ii) $\Rightarrow$ (iii) If $\mathrm{Hom}_R(L, L') \neq \{0\}$, then there is a nonzero $f\colon L \to L'$, and f is an isomorphism, by Schur's Lemma; that is, $L \cong L'$.

(iii) and $L^2 \neq (0) \Rightarrow$ (i) Assume now that $L^2 \neq (0)$, so there are $x, y \in L$ with $xy \neq 0$. If $g\colon L \to L'$ is an isomorphism, then $0 \neq g(xy) = xg(y) \in LL'$, and so $LL' \neq (0)$. •

Note that if $J(R) = (0)$, then $L^2 \neq (0)$; otherwise, L is a nilpotent left ideal and Corollary 7.17 gives $L \subseteq J(R) = (0)$, a contradiction.

Proposition 7.42. *If* $R = \bigoplus_j L_j$ *is a left semisimple ring, where the* L_j *are minimal left ideals, then every simple* R*-module* S *is isomorphic to some* L_j.

Proof. Now $S \cong \mathrm{Hom}_R(R, S) \neq \{0\}$, by Corollary 6.64. But, if $\mathrm{Hom}_R(L_j, S) = \{0\}$ for all j, then $\mathrm{Hom}_R(R, S) = \{0\}$ (for $R = L_1 \oplus \cdots \oplus L_m$). Hence, $\mathrm{Hom}_R(L_j, S) \neq \{0\}$ for some j. Since both L_j and S are simple, Theorem 7.40(i) gives $L_j \cong S$. •

Here is a fancier proof of Proposition 7.42.

Proof. By Corollary 6.25, there is a left ideal I with $S \cong R/I$, and so there is a series

$$R \supseteq I \supseteq (0).$$

In Proposition 7.27, we saw that

$$R = L_1 \oplus \cdots \oplus L_n \supseteq L_2 \oplus \cdots \oplus L_n \supseteq \cdots \supseteq L_n \supseteq (0)$$

is a composition series with factor modules $L_1, \ldots, L_n$. The Schreier Refinement Theorem (Theorem 7.2) now says that these two series have equivalent refinements. Since a composition series admits only refinements that repeat a term, the factor module S occurring in the refinement of the first series must be isomorphic to one of the factor modules in the second series; that is, $S \cong L_i$ for some i. •

Example 7.43. The trivial kG-module $V_0(k)$ (Example 7.24) is a simple kG-module (for it is one-dimensional, hence has no subspaces other than $\{0\}$ and itself). By Proposition 7.42, $V_0(k)$ is isomorphic to some minimal left ideal L of kG. We shall find L by searching for elements $u = \sum_{g\in G} a_g g$ in kG with $hu = u$ for all $h \in G$. For such elements u,

$$hu = \sum_{g\in G} a_g hg = \sum_{g\in G} a_g g = u.$$

Since the elements in G form a basis for the vector space kG, we may equate coefficients, and so $a_g = a_{hg}$ for all $g \in G$; in particular, $a_1 = a_h$. As this holds for every $h \in G$, all the coefficients a_g are equal. Therefore, if we define $\gamma \in kG$ by

$$\gamma = \sum_{g\in G} g,$$

then u is a scalar multiple of γ. It follows that $L = \langle\gamma\rangle$ is a left ideal isomorphic to the trivial module $V_0(k)$; moreover, $\langle\gamma\rangle$ is the unique such left ideal. ◀

An abstract left semisimple ring R is a direct sum of finitely many minimal left ideals: $R = \bigoplus_j L_j$, and we now know that $\mathrm{End}_R(L_j)$ is a division ring for every j. The next step is to find the direct summands of R that will ultimately turn out to be matrix rings; they arise from a decomposition of R into minimal left ideals by collecting isomorphic terms.

Definition. Let R be a left semisimple ring, and let

$$R = L_1 \oplus \cdots \oplus L_n,$$

where the L_j are minimal left ideals. Reindex the summands so that no two of the first m ideals $L_1, \ldots, L_m$ are isomorphic, while every L_j in the given decomposition is isomorphic to some L_i for $1 \le i \le m$. The left ideals

$$B_i = \bigoplus_{L_j \cong L_i} L_j$$

are called the ***simple components*** of R relative to the decomposition $R = \bigoplus_j L_j$.

We shall see, in Corollary 7.50, that the simple components do not depend on the particular decomposition of R as a direct sum of minimal left ideals.

We divide Theorem 7.44, the Wedderburn–Artin[4] Theorem, into two parts: an existence theorem and a uniqueness theorem.

[4]Wedderburn proved Theorem 7.44 for semisimple k-algebras, where k is a field; E. Artin generalized the theorem as it is stated here. This theorem is why *artinian* rings are so called.

Theorem 7.44 (Wedderburn–Artin I). *A ring R is left semisimple if and only if R is isomorphic to a direct product of matrix rings over division rings.*

Proof. Sufficiency is Proposition 7.37(ii).

For necessity, if R is left semisimple, then it is the direct sum of its simple components:

$$R = B_1 \oplus \cdots \oplus B_m,$$

where each B_i is a direct sum of isomorphic minimal left ideals. Proposition 6.16 says that there is a ring isomorphism

$$R^{\mathrm{op}} \cong \mathrm{End}_R(R),$$

where R is regarded as a left module over itself. Now $\mathrm{Hom}_R(B_i, B_j) = \{0\}$ for all $i \neq j$, by Lemma 7.41, so that Corollary 7.36 applies to give a ring isomorphism

$$R^{\mathrm{op}} \cong \mathrm{End}_R(R) \cong \mathrm{End}_R(B_1) \times \cdots \times \mathrm{End}_R(B_m).$$

By Proposition 7.34, there are isomorphisms of rings

$$\mathrm{End}_R(B_i) \cong \mathrm{Mat}_{n_i}(\mathrm{End}_R(L_i)),$$

because B_i is a direct sum of isomorphic copies of L_i. By Schur's Lemma, $\mathrm{End}_R(L_i)$ is a division ring, say, Δ_i, and so

$$R^{\mathrm{op}} \cong \mathrm{Mat}_{n_1}(\Delta_1) \times \cdots \times \mathrm{Mat}_{n_m}(\Delta_m).$$

Hence,

$$R \cong [\mathrm{Mat}_{n_1}(\Delta_1)]^{\mathrm{op}} \times \cdots \times [\mathrm{Mat}_{n_m}(\Delta_m)]^{\mathrm{op}}.$$

Finally, Proposition 6.17 gives

$$R \cong \mathrm{Mat}_{n_1}(\Delta_1^{\mathrm{op}}) \times \cdots \times \mathrm{Mat}_{n_m}(\Delta_m^{\mathrm{op}}).$$

This completes the proof, for Δ_i^{op} is also a division ring for all i, by Exercise 6.12 on page 416. •

Corollary 7.45. *A ring R is left semisimple if and only if it is right semisimple.*

Proof. It is easy to see that a ring R is right semisimple if and only if its opposite ring R^{op} is left semisimple. But we saw, in the middle of the proof of Theorem 7.44, that

$$R^{\mathrm{op}} \cong \mathrm{Mat}_{n_1}(\Delta_1) \times \cdots \times \mathrm{Mat}_{n_m}(\Delta_m),$$

where $\Delta_i = \mathrm{End}_R(L_i)$. •

As a consequence of this corollary, we say that a ring is ***semisimple*** without the adjectives left or right.

Corollary 7.46. *A commutative ring R is semisimple if and only if it is isomorphic to a direct product of finitely many fields.*

Proof. A field is a semisimple ring, and so a direct product of finitely many fields is also semisimple, by Corollary 7.28. Conversely, if R is semisimple, it is a direct product of matrix rings over division rings. Since R is commutative, all the matrix rings must be of size 1×1 and all the division rings must be fields. •

Even though the name suggests it, it is not clear that simple rings are semisimple. Indeed, we must assume a chain condition: if V is an infinite-dimensional vector space over a field k, then $R = \mathrm{End}_k(V)$ is a simple ring which is not semisimple (Lam, *A First Course in Noncommutative Rings*, pp. 43–44).

Proposition 7.47. *A simple left artinian ring R is semisimple.*

Proof. (Janusz) Since R is left artinian, it contains a minimal left ideal, say, L; of course, L is a simple left R-module. For each $a \in R$, the function $f_a\colon L \to R$, defined by $f_a(x) = xa$, is a map of left R-modules: if $r \in R$, then

$$f_a(rx) = (rx)a = r(xa) = rf_a(x).$$

Now $\operatorname{im} f_a = La$, while L being a simple module forces $\ker f_a = L$ or $\ker f_a = (0)$. In the first case, we have $La = (0)$; in the second case, we have $L \cong La$. Thus, La is either (0) or a minimal left ideal.

Consider the sum $I = \big\langle \bigcup_{a\in R} La \big\rangle \subseteq R$. Plainly, I is a left ideal; it is a right ideal as well, for if $b \in R$ and $La \subseteq I$, then $(La)b = L(ab) \subseteq I$. Since R is a simple ring, the nonzero two-sided ideal I must equal R. We claim that R is a sum of only finitely many La's. As any element of R, the unit 1 lies in some finite sum of La's; say, $1 \in Le_1 + \cdots + Le_n$. If $b \in R$, then $b = b1 \in b(Le_1 + \cdots + Le_n) \subseteq Le_1 + \cdots + Le_n$ (because $Le_1 + \cdots + Le_n$ is a left ideal). Hence, $R = Le_1 + \cdots + Le_n$.

To prove that R is semisimple, it remains to show that it is a *direct sum* of simple submodules. Choose n minimal such that $R = Le_1 + \cdots + Le_n$; we claim that $R = Le_1 \oplus \cdots \oplus Le_n$. By Proposition 6.30, it suffices to show, for all i, that

$$Le_i \cap \Big(\bigoplus_{j\neq i} Le_j\Big) = (0).$$

If this intersection is not (0), then simplicity of Le_i says that $Le_i \cap (\bigoplus_{j\neq i} Le_j) = Le_i$; that is, $Le_i \subseteq \bigoplus_{j\neq i} Le_j$, and this contradicts the minimal choice of n. Therefore, R is a semisimple ring. •

The following corollary follows at once from Proposition 7.47 and Theorem 7.44, the Wedderburn–Artin Theorem.

Corollary 7.48. *If A is a simple left artinian ring, then $A \cong \mathrm{Mat}_n(\Delta)$ for some $n \geq 1$ and some division ring Δ.*

The next lemma gives some interesting properties enjoyed by semi-simple rings; it will be used to complete the Wedderburn–Artin Theorem by proving uniqueness of the constituent parts. In particular, it will say that the integer n and the division ring Δ in Corollary 7.48 are uniquely determined by A.

Lemma 7.49. *Let R be a semisimple ring, and let*

$$R = L_1 \oplus \cdots \oplus L_n = B_1 \oplus \cdots \oplus B_m,$$

where the L_j are minimal left ideals and the B_i are the corresponding simple components of R.

(i) *Each B_i is a ring that is also a two-sided ideal in R, and $B_iB_j = (0)$ if $j \neq i$.*

(ii) *If L is any minimal left ideal in R, not necessarily occurring in the given decomposition of R, then $L \cong L_i$ for some i and $L \subseteq B_i$.*

(iii) *Every two-sided ideal D in R is a direct sum of simple components.*

(iv) *Each B_i is a simple ring.*

Proof.

(i) Each B_i is a left ideal. To see that it is also a right ideal, consider

$$B_iR = B_i(B_1 \oplus \cdots \oplus B_m) \subseteq B_iB_1 + \cdots + B_iB_m.$$

Recall, for each i, that B_i is a direct sum of left ideals L isomorphic to L_i. If $L \cong L_i$ and $L' \cong L_j$, then the contrapositive, 'not (iii)' $\Rightarrow$ 'not (i)' in Lemma 7.41, applies to give $LL' = (0)$ if $j \neq i$. Hence, if $j \neq i$,

$$B_iB_j = \Big(\bigoplus_{L \cong L_i} L\Big)\Big(\bigoplus_{L' \cong L_j} L'\Big) \subseteq \bigoplus LL' = (0).$$

Thus, $B_iB_1 + \cdots + B_iB_m \subseteq B_iB_i$. Since B_i is a left ideal, $B_iB_i \subseteq RB_i \subseteq B_i$. Therefore, $B_iR \subseteq B_i$, so that B_i is a right ideal and, hence, is a two-sided ideal.

In the last step, proving that B_i is a right ideal, we saw that $B_iB_i \subseteq B_i$; that is, B_i is closed under multiplication. Therefore, to prove that B_i is a ring, it now suffices to prove that it contains a unit element. If 1 is the unit element in R, then $1 = e_1 + \cdots + e_m$, where $e_i \in B_i$ for all i. If $b_i \in B_i$, then

$$b_i = 1b_i = (e_1 + \cdots + e_m)b_i = e_ib_i,$$

for $B_jB_i = (0)$ whenever $j \neq i$, by part (i). Similarly, the equation $b_i = b_i1$ gives $b_ie_i = b_i$, and so e_i is a unit in B_i. Thus, B_i is a ring.[5]

(ii) By Proposition 7.42, a minimal left ideal L is isomorphic to L_i for some i. Now

$$L = RL = (B_1 \oplus \cdots \oplus B_m)L \subseteq B_1L + \cdots + B_mL.$$

If $j \neq i$, then $B_jL = (0)$, by Lemma 7.41, so that

$$L \subseteq B_iL \subseteq B_i,$$

because B_i is a right ideal.

(iii) A nonzero two-sided ideal D in R is a left ideal, and so it contains some minimal left ideal L, by Proposition 7.10. Now $L \cong L_i$ for some i, by Proposition 7.42; we claim that $B_i \subseteq D$. By Lemma 7.41, if L' is any minimal left ideal in B_i, then $L' = Lb'$ for some $b' \in L'$. Since $L \subseteq D$ and D is a right ideal, we have $L' = Lb' \subseteq LL' \subseteq DR \subseteq D$. We have shown that D contains every left ideal isomorphic to L_i; as B_i is generated by such ideals, $B_i \subseteq D$. Write $R = B_I \oplus B_J$, where $B_I = \bigoplus_i B_i$ with $B_i \subseteq D$ and $B_J = \bigoplus_j B_j$ with $B_j \not\subseteq D$. By Corollary 6.29 (which holds for modules over noncommutative rings), $D = B_I \oplus (D \cap B_J)$. But $D \cap B_J = (0)$; otherwise, it would contain a minimal left ideal $L \cong L_j$ for some $j \in J$ and, as above, this would force $B_j \subseteq D$. Therefore, $D = B_I$.

[5] B_i is not a subring of R because its unit e_i is not the unit 1 in R.

(iv) A left ideal in B_i is also a left ideal in R: if $a \in R$, then $a = \sum_j a_j$, where $a_j \in B_j$; if $b_i \in B_i$, then

$$ab_i = (a_1 + \cdots + a_m)b_i = a_i b_i \in B_i,$$

because $B_j B_i = (0)$ for $j \neq i$. Similarly, a right ideal in B_i is a right ideal in R, and so a two-sided ideal D in B_i is a two-sided ideal in R. By part (iii), the only two-sided ideals in R are direct sums of simple components, and so $D \subseteq B_i$ implies $D = (0)$ or $D = B_i$. Therefore, B_i is a simple ring. •

Corollary 7.50. *If R is a semisimple ring, then the simple component B_i containing a minimal left ideal L_i is the left ideal generated by all the minimal left ideals that are isomorphic to L_i. Therefore, the simple components $B_1, \ldots, B_m$ of a semisimple ring do not depend on a decomposition of R as a direct sum of minimal left ideals.*

Proof. This follows from Lemma 7.49(ii). •

Corollary 7.51. *Let A be a simple artinian ring.*

(i) *$A \cong \mathrm{Mat}_n(\Delta)$ for some division ring Δ. If L is a minimal left ideal in A, then every simple left A-module is isomorphic to L; moreover, $\Delta^{\mathrm{op}} \cong \mathrm{End}_A(L)$.*

(ii) *Two finitely generated left A-modules M and N are isomorphic if and only if $\dim_\Delta(M) = \dim_\Delta(N)$.*

Proof.

(i) Since A is a semisimple ring, by Proposition 7.47, every left module M is isomorphic to a direct sum of minimal left ideals. By Lemma 7.49(ii), all minimal left ideals are isomorphic, say, to L.

We now prove that $\Delta^{\mathrm{op}} \cong \mathrm{End}_A(L)$. We may assume that $A = \mathrm{Mat}_n(\Delta)$ and that $L = \mathrm{COL}(1)$, the minimal left ideal consisting of all the $n \times n$ matrices whose last $n-1$ columns are 0 (Proposition 7.37). Define $\varphi\colon \Delta \to \mathrm{End}_A(L)$ as follows: if $d \in \Delta$ and $\ell \in L$, then $\varphi_d\colon \ell \mapsto \ell d$. Note that φ_d is an A-map: it is additive and, if $a \in A$ and $\ell \in L$, then $\varphi_d(a\ell) = (a\ell)d = a(\ell d) = a\varphi_d(\ell)$. Next, φ is a ring antihomomorphism: $\varphi_1 = 1_L$, it is additive, and $\varphi_{dd'} = \varphi_{d'}\varphi_d$: if $\ell \in L$, then $\varphi_{d'}\varphi_d(\ell) = \varphi_d(\ell d') = \ell d' d = \varphi_{dd'}(\ell)$; that is, φ is a ring homomorphism $\Delta^{\mathrm{op}} \to \mathrm{End}_A(L)$. To see that φ is injective, note that each $\ell \in L \subseteq \mathrm{Mat}_n(\Delta)$ is a matrix with entries in Δ; hence, $\ell d = 0$ implies $\ell = 0$. Finally, we show that φ is surjective. Let $f \in \mathrm{End}_A(L)$. Now $L = AE_{11}$, where E_{11} is the matrix unit (every simple module is generated by any nonzero element in it). If $u_i \in \Delta$, let $[u_1, \ldots, u_n]$ denote the $n \times n$ matrix in L whose first column is $(u_1, \ldots, u_n)^\top$ and whose other entries are all 0. Write $f(E_{11}) = [d_1, \ldots, d_n]$. If $\ell \in L$, then ℓ has the form $[u_1, \ldots, u_n]$, and using only the definition of matrix multiplication, it is easy to see that

$[u_1, \dots, u_n] = [u_1, \dots, u_n]E_{11}$. Since f is an A-map,

$$\begin{aligned} f([u_1, \dots, u_n]) &= f([u_1, \dots, u_n]E_{11}) \\ &= [u_1, \dots, u_n]f(E_{11}) \\ &= [u_1, \dots, u_n][d_1, \dots, d_n] \\ &= [u_1, \dots, u_n]d_1 = \varphi_{d_1}([u_1, \dots, u_n]). \end{aligned}$$

Therefore, $f = \varphi_{d_1} \in \operatorname{im} \varphi$, as desired.

(ii) All minimal left ideals in A are isomorphic to L, and so M is a direct sum of $\dim_\Delta(M)/n$ copies of L. If $M \cong N$ as left $\operatorname{Mat}_n(\Delta)$-modules, then $M \cong N$ as left Δ-modules, and so $\dim_\Delta(M) = \dim_\Delta(N)$. Conversely, if $\dim_\Delta(M) = nd = \dim_\Delta(N)$, then both M and N are direct sums of d copies of L, and hence $M \cong N$ as left A-modules. •

The number m of simple components of R is an invariant, for it is the number of nonisomorphic simple left R-modules (even better, we will see, in Theorem 7.58, that if $R = \mathbb{C}G$, then m is the number of conjugacy classes in G). However, there is a much stronger uniqueness result.

Theorem 7.52 (Wedderburn–Artin II). *Every semisimple ring R is a direct product,*

$$R \cong \operatorname{Mat}_{n_1}(\Delta_1) \times \cdots \times \operatorname{Mat}_{n_m}(\Delta_m),$$

where $n_i \geq 1$ and Δ_i is a division ring, and the numbers m and n_i, as well as the division rings Δ_i, are uniquely determined by R.

Proof. Let R be a semisimple ring, and let $R = B_1 \oplus \cdots \oplus B_m$ be a decomposition into simple components arising from some decomposition of R as a direct sum of minimal left ideals. Suppose that $R = B'_1 \times \cdots \times B'_t$, where each B'_ℓ is a two-sided ideal that is also a simple ring. By Lemma 7.49, each two-sided ideal B'_ℓ is a direct sum of B_i's. But B'_ℓ cannot have more than one summand B_i, lest the simple ring B'_ℓ contain a proper nonzero two-sided ideal. Therefore, $t = m$ and, after reindexing, $B'_i = B_i$ for all i.

Dropping subscripts, it remains to prove that if $B = \operatorname{Mat}_n(\Delta) \cong \operatorname{Mat}_{n'}(\Delta') = B'$, then $n = n'$ and $\Delta \cong \Delta'$. In Proposition 7.37, we proved that $\operatorname{COL}(\ell)$, consisting of the matrices with jth columns 0 for all $j \neq \ell$, is a minimal left ideal in B, so that $\operatorname{COL}(\ell)$ is a simple B-module. Therefore,

$$(0) \subseteq \operatorname{COL}(1) \subseteq [\operatorname{COL}(1) \oplus \operatorname{COL}(2)] \subseteq \cdots \subseteq [\operatorname{COL}(1) \oplus \cdots \oplus \operatorname{COL}(n)] = B$$

is a composition series of B as a module over itself. By the Jordan–Hölder Theorem (Theorem 7.3), n and the factor modules $\operatorname{COL}(\ell)$ are invariants of B. Now $\operatorname{COL}(\ell) \cong \operatorname{COL}(1)$ for all ℓ, by Corollary 7.51, and so it suffices to prove that Δ can be recaptured from $\operatorname{COL}(1)$. But this has been done in Corollary 7.51(i): $\Delta \cong \operatorname{End}_B(\operatorname{COL}(1))^{\mathrm{op}}$. •

The description of the group algebra kG simplifies when the field k is algebraically closed. Here is the most useful version of Maschke's Theorem.

Corollary 7.53 (Molien). *If G is a finite group and k is an algebraically closed field whose characteristic does not divide $|G|$, then*

$$kG \cong \mathrm{Mat}_{n_1}(k) \times \cdots \times \mathrm{Mat}_{n_m}(k).$$

Proof. By Maschke's Theorem, kG is a semisimple ring, and its simple components are isomorphic to matrix rings of the form $\mathrm{Mat}_n(\Delta)$, where Δ arises as $\mathrm{End}_{kG}(L)^{\mathrm{op}}$ for some minimal left ideal L in kG. Therefore, it suffices to show that $\mathrm{End}_{kG}(L)^{\mathrm{op}} = \Delta = k$.

Now $\mathrm{End}_{kG}(L)^{\mathrm{op}} \subseteq \mathrm{End}_k(L)^{\mathrm{op}}$, which is finite-dimensional over k because L is; hence, $\Delta = \mathrm{End}_{kG}(L)^{\mathrm{op}}$ is finite-dimensional over k. Each $f \in \mathrm{End}_{kG}(L)$ is a kG-map, hence is a k-map; that is, $f(au) = af(u)$ for all $a \in k$ and $u \in L$. Therefore, the map $\varphi_a \colon L \to L$, given by $u \mapsto au$, commutes with f; that is, k (identified with all φ_a) is contained in $Z(\Delta)$, the center of Δ. If $\delta \in \Delta$, then δ commutes with every element in k, and so $k(\delta)$, the subdivision ring generated by k and δ, is a (commutative) field. As Δ is finite-dimensional over k, so is $k(\delta)$; that is, $k(\delta)$ is a finite extension of the field k, and so δ is algebraic over k, by Proposition 2.141. But k is algebraically closed, so that $\delta \in k$ and $\Delta = k$. •

The next corollary makes explicit a detail from the Wedderburn–Artin II, using Molien's simplification.

Corollary 7.54. *If G is a finite group and L_i is a minimal left ideal in $\mathbb{C}G$, then $\mathbb{C}G = B_1 \oplus \cdots \oplus B_m$, where B_i is the ideal generated by all the minimal left ideals isomorphic to L_i. If $\dim_{\mathbb{C}}(L_i) = n_i$, then*

$$B_i = \mathrm{Mat}_{n_i}(\mathbb{C}).$$

Example 7.55. There are nonisomorphic finite groups G and H having isomorphic complex group algebras. If G is an abelian group of order d, then $\mathbb{C}G$ is a direct product of matrix rings over $\mathbb{C}$, because $\mathbb{C}$ is algebraically closed. But G abelian implies $\mathbb{C}G$ commutative. Hence, $\mathbb{C}G$ is the direct product of d copies of $\mathbb{C}$ (for $\mathrm{Mat}_n(\mathbb{C})$ is commutative only when $n = 1$). It follows that if H is any abelian group of order d, then $\mathbb{C}G \cong \mathbb{C}H$. In particular, $\mathbb{I}_4$ and $\mathbb{I}_2 \oplus \mathbb{I}_2$ are nonisomorphic groups having isomorphic complex group algebras. It follows from this example that certain properties of a group G get lost in the group algebra $\mathbb{C}G$. ◀

Corollary 7.56. *If G is a finite group and k is an algebraically closed field whose characteristic does not divide $|G|$, then $|G| = n_1^2 + n_2^2 + \cdots + n_m^2$, where the ith simple component B_i of kG consists of $n_i \times n_i$ matrices. Moreover, we may assume that $n_1 = 1$.*[6]

Remark. Theorem 7.98 says that all the n_i are divisors of $|G|$. ◀

Proof. As vector spaces over k, both kG and $\mathrm{Mat}_{n_1}(k) \times \cdots \times \mathrm{Mat}_{n_m}(k)$ have the same dimension, for they are isomorphic, by Corollary 7.53. But $\dim(kG) = |G|$, and the dimension of the right side is $\sum_i \dim(\mathrm{Mat}_{n_i}(k)) = \sum_i n_i^2$.

[6] By Example 7.43, the group algebra kG always has a unique minimal left ideal isomorphic to $V_0(k)$, even when k is not algebraically closed.

Finally, Example 7.43 shows that there is a unique minimal left ideal isomorphic to the trivial module $V_0(k)$; the corresponding simple component, say, B_1, is one-dimensional, and so $n_1 = 1$. •

The number m of simple components in $\mathbb{C}G$ has a group-theoretic interpretation; we begin by finding the center of the group algebra.

Definition. Let $C_1, \ldots, C_r$ be the conjugacy classes in a finite group G. For each C_j, define the ***class sum*** to be the element $z_j \in \mathbb{C}G$ given by

$$z_j = \sum_{g \in C_j} g.$$

Here is a ring-theoretic interpretation of the number r of conjugacy classes.

Lemma 7.57. *If r is the number of conjugacy classes in a finite group G, then*

$$r = \dim_{\mathbb{C}}(Z(\mathbb{C}G)),$$

where $Z(\mathbb{C}G))$ is the center of the group algebra. In fact, a basis of $Z(\mathbb{C}G)$ consists of all the class sums.

Proof. If $z_j = \sum_{g \in C_j} g$ is a class sum, then we claim that $z_j \in Z(\mathbb{C}G)$. If $h \in G$, then $hz_jh^{-1} = z_j$, because conjugation by any element of G merely permutes the elements in a conjugacy class. Note that if $j \neq \ell$, then z_j and z_ℓ have no nonzero components in common, and so $z_1, \ldots, z_r$ is a linearly independent list. It remains to prove that the z_j span the center.

Let $u = \sum_{g \in G} a_g g \in Z(\mathbb{C}G)$. If $h \in G$, then $huh^{-1} = u$, and so $a_{hgh^{-1}} = a_g$ for all $g \in G$. Thus, if g and g' lie in the same conjugacy class of G, then their coefficients in u are the same. But this says that u is a linear combination of the class sums z_j. •

Theorem 7.58. *If G is a finite group, then the number m of simple components in $\mathbb{C}G$ is equal to the number r of conjugacy classes in G.*

Proof. We have just seen, in Lemma 7.57, that $r = \dim_{\mathbb{C}}(Z(\mathbb{C}G))$. On the other hand, $Z(\mathrm{Mat}_{n_i}(\mathbb{C}))$, the center of a matrix ring, is the subspace of all scalar matrices, so that $m = \dim_{\mathbb{C}}(Z(\mathbb{C}G))$, by Lemma 7.57. •

We began this section by seeing that k-representations of a group G correspond to kG-modules. Let us now return to representations.

Definition. A k-representation of a group G is ***irreducible*** if the corresponding kG-module is simple.

For example, a one-dimensional (necessarily irreducible) k-representation is a group homomorphism $\lambda\colon G \to k^\times$, where $k^\times$ is the multiplicative group of nonzero elements of k. The trivial kG-module $V_0(k)$ corresponds to the representation $\lambda_g = 1$ for all $g \in G$.

The next result is basic to the construction of the character table of a finite group.

Theorem 7.59. *If G is a finite group, then the number of its irreducible complex representations is equal to the number r of its conjugacy classes.*

Proof. By Proposition 7.42, every simple $\mathbb{C}G$-module is isomorphic to a minimal left ideal. Since the number of minimal left ideals is m [the number of simple components of $\mathbb{C}G$], we see that m is the number of irreducible $\mathbb{C}$-representations of G. But Theorem 7.58 equates m with the number r of conjugacy classes in G. •

Example 7.60.

(i) If $G = S_3$, then $\mathbb{C}G$ is six-dimensional. There are three simple components, for S_3 has three conjugacy classes (by Theorem 1.9, the number of conjugacy classes in S_n is equal to the number of different cycle structures) having dimensions 1, 1, and 4, respectively. (We could have seen this without Theorem 7.58, for this is the only way to write 6 as a sum of squares aside from a sum of six 1's.) Therefore,

$$\mathbb{C}S_3 \cong \mathbb{C} \times \mathbb{C} \times \mathrm{Mat}_2(\mathbb{C}).$$

One of the one-dimensional irreducible representations is the trivial one; the other is sgn (signum).

(ii) We now analyze kG for $G = \mathbf{Q}$, the quaternion group of order 8. If $k = \mathbb{C}$, then Corollary 7.53 gives

$$\mathbb{C}\mathbf{Q} \cong \mathrm{Mat}_{n_1}(\mathbb{C}) \times \cdots \times \mathrm{Mat}_{n_r}(\mathbb{C}),$$

while Corollary 7.56 gives

$$|\mathbf{Q}| = 8 = 1 + n_2^2 + \cdots + n_r^2.$$

It follows that either all $n_i = 1$ or four $n_i = 1$ and one $n_i = 2$. The first case cannot occur, for it would imply that $\mathbb{C}\mathbf{Q}$ is a commutative ring, whereas the group $\mathbf{Q}$ of quaternions is not abelian. Therefore,

$$\mathbb{C}\mathbf{Q} \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathrm{Mat}_2(\mathbb{C}).$$

We could also have used Theorem 7.58, for $\mathbf{Q}$ has exactly five conjugacy classes, namely, $\{1\}$, $\{\overline{1}\}$, $\{i, \overline{i}\}$, $\{j, \overline{j}\}$, $\{k, \overline{k}\}$.

The group algebra $\mathbb{R}\mathbf{Q}$ is more complicated because $\mathbb{R}$ is not algebraically closed. Exercise 6.14 on page 416 shows that $\mathbb{H}$ is a quotient of $\mathbb{R}\mathbf{Q}$, hence $\mathbb{H}$ is isomorphic to a direct summand of $\mathbb{R}\mathbf{Q}$ because $\mathbb{R}\mathbf{Q}$ is semisimple. It turns out that

$$\mathbb{R}\mathbf{Q} \cong \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{H}. \quad \blacktriangleleft$$

Here is an amusing application of the Wedderburn–Artin Theorems.

Proposition 7.61. *Let R be a ring whose group of units $U = U(R)$ is finite and of odd order. Then U is abelian and there are positive integers m_i with*

$$|U| = \prod_{i=1}^{t} (2^{m_i} - 1).$$

Proof. First, we note that $1 = -1$ in R, lest -1 be a unit of even order. Consider the group algebra kU, where $k = \mathbb{F}_2$. Since k has characteristic 2 and $|U|$ is odd, Maschke's Theorem says that kU is semisimple. There is a ring map $\varphi\colon kU \to R$ carrying every k-linear combination of elements of U to "itself." Now $R' = \operatorname{im}\varphi$ is a finite subring of R containing U (for kU is finite); since dropping to a subring cannot create any new units, we have $U = U(R')$. By Corollary 7.29, the ring R' is semisimple, so that Wedderburn–Artin Theorem I gives

$$R' \cong \prod_{i=1}^{t} \operatorname{Mat}_{n_i}(\Delta_i),$$

where each Δ_i is a division ring.

Now Δ_i is finite, because R' is finite, and so Δ_i is a finite division ring. By the "other" theorem of Wedderburn, Theorem 7.13, each Δ_i is a field. But $-1 = 1$ in R implies that $-1 = 1$ in Δ_i (for $\Delta_i \subseteq R'$), and so each field Δ_i has characteristic 2; hence,

$$|\Delta_i| = 2^{m_i}$$

for integers $m_i \geq 1$. All the matrix rings must be 1×1, for any matrix ring of larger size must contain an element of order 2, namely, $I + K$, where K has entry 1 in the first position in the bottom row, and all other entries 0. For example,

$$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix} = I.$$

Therefore, R' is a direct product of finite fields of characteristic 2, and so $U = U(R')$ is an abelian group whose order is described in the statement. •

It follows, for example, that there is no ring having exactly five units.

The ***Jacobson–Chevalley Density Theorem***, an important generalization of the Wedderburn–Artin Theorems for certain nonartinian rings, was proved in the 1930s. Call a ring R ***left primitive*** if there exists a faithful simple left R-module S; that is, S is simple and, if $r \in R$ and $rS = \{0\}$, then $r = 0$. It can be proved that commutative primitive rings are fields, while left artinian left primitive rings are simple. Assume now that R is a left primitive ring, that S is a faithful simple left R-module, and that Δ denotes the division ring $\operatorname{End}_R(S)$. The Density Theorem says that if R is left artinian, then $R \cong \operatorname{Mat}_n(\Delta)$, while if R is not left artinian, then for every integer $n > 0$, there exists a subring R_n of R with $R_n \cong \operatorname{Mat}_n(\Delta)$. We refer the reader to Lam, *A First Course in Noncommutative Rings*, pp. 191–193.

The Wedderburn–Artin Theorems led to several areas of research, two of which are descriptions of division rings and of finite-dimensional algebras. Division rings will be considered in the context of central simple algebras in Chapter 8 and crossed product algebras in Chapter 9. Let us discuss finite-dimensional algebras now.

Thanks to the theorems of Maschke and Molien, the Wedderburn–Artin Theorems apply to ***ordinary*** representations of a finite group G; that is, to kG-modules, where k is a field whose characteristic does not divide $|G|$. We know kG is semisimple in this case. However, ***modular*** representations, that is, kG-modules for which the characteristic of k does divide $|G|$, arise naturally. For example, if G is a finite

p-group, for some prime p, then a minimal normal subgroup N is a vector space over $\mathbb{F}_p$ (Rotman, *An Introduction to the Theory of Groups*, p. 106). Now G acts on N (by conjugation), and so N is an $\mathbb{F}_pG$-module. Modular representations are used extensively in the classification of the finite simple groups. In his study of modular representations, Brauer observed that the important modules M are *indecomposable* rather than irreducible. Recall that a module M is indecomposable if $M \neq \{0\}$ and there are no nonzero modules A and B with $M = A \oplus B$ (in the ordinary case, a module is indecomposable if and only if it is irreducible [i.e., simple], but this is no longer true in the modular case). When kG is semisimple, Proposition 7.42 says that there are only finitely many simple modules (corresponding to the minimal left ideals), which implies that there are only finitely many indecomposables. This is not true in the modular case, however. For example, if k is an algebraically closed field of characteristic 2, $k\mathbf{V}$ and kA_4 have infinitely many nonisomorphic indecomposable modules.

A finite-dimensional k-algebra R over a field k is said to have ***finite representation type*** if there are only finitely many nonisomorphic finite-dimensional indecomposable R-modules. D. G. Higman proved, for a finite group G, that kG has finite representation type for every field k if and only if all its Sylow subgroups G are cyclic (Curtis–Reiner, *Representation Theory of Finite Groups and Associative Algebras*, p. 431). In the 1950s, the following two problems, known as the ***Brauer–Thrall conjectures***, were posed. Let R be a ring not of finite representation type.

(I) Are the dimensions of the indecomposable R-modules unbounded?

(II) Is there a strictly increasing sequence $n_1, n_2, \ldots$ with infinitely many nonisomorphic indecomposable R-modules of dimension n_i for every i?

The positive solution of the first conjecture, by Roiter in 1968, had a great impact. Shortly thereafter, Gabriel introduced graph-theoretic methods, associating finite-dimensional algebras to certain oriented graphs, called *quivers*. He proved that a connected quiver has a finite number of nonisomorphic finite-dimensional representations if and only if the quiver is a Dynkin diagrams of type A_n, D_n, E_6, E_7, or E_8 (*Dynkin diagrams* are multigraphs that describe simple complex Lie algebras; see the discussion on page 748). Gabriel's result can be rephrased in terms of *left hereditary* k-algebras (all left ideals are projective modules). Dlab and Ringel extended Gabriel's result to Dynkin diagrams of any type, and they also extended the classification to certain left hereditary algebras.

A positive solution of Brauer–Thrall II for all finite-dimensional algebras over an algebraically closed field follows from results of Bautista, Gabriel, Roiter, and Salmerón. M. Auslander and Reiten created a theory involving *almost split sequences* and *Auslander–Reiten quivers*. As of this writing, Auslander–Reiten Theory is the most powerful tool in the study of representations of finite-dimensional algebras. For a discussion of these ideas, we refer the reader to Artin–Nesbitt–Thrall, *Rings with Minimum Condition*, Dlab–Ringel, *Indecomposable Representations of Graphs and Algebras*, Drozd–Kirichenko, *Finite-Dimensional Algebras*, Jacobson, *Structure of Rings*, and Rowen, *Ring Theory*.

Exercises

7.25. Find $\mathbb{C}G$ if $G = D_8$, the dihedral group of order 8.

7.26. Find $\mathbb{C}G$ if $G = A_4$.

Hint. A_4 has four conjugacy classes.

7.27. (i) Let k be a field, and view $\operatorname{sgn}\colon S_n \to \{\pm 1\} \subseteq k$. Define $\operatorname{Sig}(k)$ to be k made into a kS_n-module (as in Proposition 7.21): if $\gamma \in S_n$ and $a \in k$, then $\gamma a = \operatorname{sgn}(\gamma)a$. Prove that if $\operatorname{Sig}(k)$ is an irreducible kS_n-module and k does not have characteristic 2, then $\operatorname{Sig}(k) \ncong V_0(k)$.

(ii) Find $\mathbb{C}S_5$.
Hint. There are five conjugacy classes in S_5.

7.28. Let G be a finite group, and let k and K be algebraically closed fields whose characteristics p and q, respectively, do not divide $|G|$.

(i) Prove that kG and KG have the same number of simple components.

(ii) Prove that the degrees of the irreducible representations of G over k are the same as the degrees of the irreducible representations of G over K.

Section 7.5. Characters

Characters will enable us to use the preceding results to produce numerical invariants whose arithmetic properties help to prove theorems about finite groups. The first important instance of this technique is the following theorem.

Theorem 7.62 (Burnside). *Every group of order $p^m q^n$, where p and q are primes, is a solvable group.*

Notice that Burnside's Theorem cannot be improved to groups having orders with only three distinct prime factors, for A_5 is a simple group of order $60 = 2^2 \cdot 3 \cdot 5$.

Using representations, we will prove the following theorem.

Theorem 7.63. *If G is a nonabelian finite simple group, then $\{1\}$ is the only conjugacy class whose size is a prime power.*

Proposition 7.64. Theorem 7.63 *implies Burnside's Theorem.*

Proof. Assume that Burnside's Theorem is false, and let G be a "least criminal;" that is, G is a counterexample of smallest order. If G has a proper normal subgroup H with $H \neq \{1\}$, then both H and G/H are solvable, for their orders are smaller than $|G|$ and are of the form $p^i q^j$. By Proposition 3.25, G is solvable, and this is a contradiction. We may assume, therefore, that G is a nonabelian simple group.

Let Q be a Sylow q-subgroup of G. If $Q = \{1\}$, then G is a p-group, contradicting G being a nonabelian simple group; hence, $Q \neq \{1\}$. Since the center of Q

is nontrivial, by Theorem 1.113, there exists a nontrivial element $x \in Z(Q)$. Now $Q \subseteq C_G(x)$, for every element in Q commutes with x, and so

$$[G : Q] = [G : C_G(x)][C_G(x) : Q];$$

that is, $[G : C_G(x)]$ is a divisor of $[G : Q] = p^m$. Of course, $[G : C_G(x)]$ is the number of elements in the conjugacy class x^G of x (Corollary 1.109), and so the hypothesis says that $|x^G| = 1$; hence, $x \in Z(G)$, contradicting G being simple. •

We now specialize the definition of k-representation on page 539 from arbitrary fields k of scalars to the complex numbers $\mathbb{C}$.

Definition. A ***representation*** of a group G is a homomorphism

$$\sigma\colon G \to \mathrm{GL}(V),$$

where V is a vector space over $\mathbb{C}$. The ***degree*** of σ is $\dim_{\mathbb{C}}(V)$.

For the rest of this section, all groups are finite and all representations are finite-dimensional over $\mathbb{C}$***.***

If $\sigma\colon G \to \mathrm{GL}(V)$ is a representation of degree n, then a choice of basis of V allows each $\sigma(g)$ to be regarded as an $n \times n$ nonsingular complex matrix.

Representations can be translated into the language of modules. In Proposition 7.21, we proved that every representation $\sigma\colon G \to \mathrm{GL}(V)$ equips V with the structure of a left $\mathbb{C}G$-module (and conversely): for each $g \in G$, we have $\sigma(g)\colon V \to V$ and, if $v \in V$, we define scalar multiplication gv by

$$gv = \sigma(g)(v).$$

We denote V made into a $\mathbb{C}G$-module in this way by V^σ, and we call it the ***corresponding module***.

Example 7.65. Let L be a left ideal in $\mathbb{C}G$ and let $\dim_{\mathbb{C}}(L) = d$. Then $\sigma\colon G \to \mathrm{GL}(L)$, defined by $\sigma(g)\colon u \mapsto gu$ for all $u \in L$, is a representation of degree d. The corresponding $\mathbb{C}G$-module V^σ is just L itself, for the original scalar multiplication on the left ideal L coincides with the scalar multiplication given by σ. ◀

Example 7.66. We now show that permutation representations, that is, G-sets,[7] give a special kind of representation. A G-set X corresponds to a homomorphism $\pi\colon G \to S_X$, where S_X is the symmetric group of all permutations of X. If V is the complex vector space having X as a basis, then we may regard $S_X \subseteq \mathrm{GL}(V)$ in the following way. Each permutation $\pi(g)$ of X, where $g \in G$, is now a permutation of a basis of V and, hence, it determines a nonsingular linear transformation on V. With respect to the basis X, the matrix of $\pi(g)$ is a ***permutation matrix***: it arises by permuting the columns of the identity matrix I by $\pi(g)$; thus, it has exactly one entry equal to 1 in each row and column while all its other entries are 0. ◀

One of the most important representations is the *regular representation*.

[7]Recall that if a group G acts on a set X, then X is called a *G-set*.

Definition. If G is a group, then the representation $\rho\colon G \to \mathrm{GL}(\mathbb{C}G)$ defined, for all $g, h \in G$, by

$$\rho(g)\colon h \mapsto gh,$$

is called the ***regular representation***.

By Example 7.65, the module corresponding to the regular representation is just $\mathbb{C}G$ considered as a left module over itself.

Two representations $\sigma\colon G \to \mathrm{GL}(V)$ and $\tau\colon G \to \mathrm{GL}(W)$ can be added.

Definition. If $\sigma\colon G \to \mathrm{GL}(V)$ and $\tau\colon G \to \mathrm{GL}(W)$ are representations, then their ***sum*** $\sigma + \tau\colon G \to \mathrm{GL}(V \oplus W)$ is defined by

$$(\sigma + \tau)(g)\colon (v, w) \mapsto (\sigma(g)v, \tau(g)w)$$

for all $g \in G$, $v \in V$, and $w \in W$.

In matrix terms, if $\sigma\colon G \to \mathrm{GL}(n, \mathbb{C})$ and $\tau\colon G \to \mathrm{GL}(m, \mathbb{C})$, then

$$\sigma + \tau\colon G \to \mathrm{GL}(n + m, \mathbb{C}),$$

and if $g \in G$, then $(\sigma + \tau)(g)$ is the direct sum of blocks $\sigma(g) \oplus \tau(g)$; that is,

$$(\sigma + \tau)(g) = \begin{bmatrix} \sigma(g) & 0 \\ 0 & \tau(g) \end{bmatrix}.$$

The following terminology is the common one used in Group Representations.

Definition. A representation σ of a group G is ***irreducible*** if the corresponding $\mathbb{C}G$-module is simple. A representation σ is ***completely reducible*** if it is a direct sum of irreducible representations; that is, the corresponding $\mathbb{C}G$-module is semisimple.

Example 7.67. A representation σ is ***linear*** if $\mathrm{degree}(\sigma) = 1$. The trivial representation of any group G is linear, for the principal module $V_0(\mathbb{C})$ is one-dimensional. If $G = S_n$, then $\mathrm{sgn}\colon G \to \{\pm 1\}$ is also a linear representation.

Every linear representation is irreducible, for the corresponding $\mathbb{C}G$-module must be simple; after all, every submodule is a subspace, and $\{0\}$ and V are the only subspaces of a one-dimensional vector space V. It follows that the trivial representation of any group G is irreducible, as is the representation sgn of S_n. ◀

Recall the proof of the Wedderburn–Artin Theorem: there are pairwise nonisomorphic minimal left ideals $L_1, \ldots, L_r$ in $\mathbb{C}G$ and $\mathbb{C}G = B_1 \oplus \cdots \oplus B_r$, where B_i is generated by all minimal left ideals isomorphic to L_i. By Corollary 7.53, $B_i \cong \mathrm{Mat}_{n_i}(\mathbb{C})$, where $n_i = \dim_{\mathbb{C}}(L_i)$. But all minimal left ideals in $\mathrm{Mat}_{n_i}(\mathbb{C})$ are isomorphic, by Lemma 7.49(ii), so that $L_i \cong \mathrm{COL}(1) \cong \mathbb{C}^{n_i}$ [see Example 7.14(iii)]. Therefore,

$$B_i \cong \mathrm{End}_{\mathbb{C}}(L_i).$$

Proposition 7.68.

(i) *For each minimal left ideal L_i in $\mathbb{C}G$, there is an irreducible representation $\lambda_i\colon G \to \mathrm{GL}(L_i)$, given by left multiplication*:

$$\lambda_i(g)\colon u_i \mapsto gu_i,$$

where $g \in G$ and $u_i \in L_i$; moreover, $\text{degree}(\lambda_i) = n_i = \dim_{\mathbb{C}}(L_i)$.

(ii) *The representation λ_i extends to a $\mathbb{C}$-algebra map $\widetilde{\lambda}_i\colon \mathbb{C}G \to \text{End}_{\mathbb{C}}(L_i)$ if we define*

$$\widetilde{\lambda}_i(g)u_j = \begin{cases} gu_i & \text{if } j = i \\ 0 & \text{if } j \neq i \end{cases}$$

for $g \in G$ and $u_j \in B_j$.

Proof.

(i) Since L_i is a left ideal in $\mathbb{C}G$, each $g \in G$ acts on L_i by left multiplication, and so the representation λ_i of G is as stated. By Example 7.65, the corresponding module L_i^{σ} is L_i, and so λ_i is an irreducible representation because L_i, being a minimal left ideal, is a simple module.

(ii) If we regard $\mathbb{C}G$ and $\text{End}_{\mathbb{C}}(L_i)$ as vector spaces over $\mathbb{C}$, then λ_i extends to a linear transformation $\widetilde{\lambda}_i\colon \mathbb{C}G \to \text{End}_{\mathbb{C}}(L_i)$ (because the elements of G are a basis of $\mathbb{C}G$):

$$\widetilde{\lambda}_i\colon \sum_{g\in G} c_g g \mapsto \sum_{g\in G} c_g \lambda_i(g)$$

[remember that $\lambda_i(g) \in \text{GL}(L_i) \subseteq \text{End}_{\mathbb{C}}(L_i)$]. Let us show that $\widetilde{\lambda}_i\colon \mathbb{C}G \to \text{End}_{\mathbb{C}}(L_i)$ is an algebra map. Now $\mathbb{C}G = B_1 \oplus \cdots \oplus B_r$, where the B_j are two-sided ideals. To prove that $\widetilde{\lambda}_i$ is multiplicative, it suffices to check its values on products of basis elements. If $u_j \in B_j$ and $g, h \in G$, then

$$\widetilde{\lambda}_i(gh)\colon u_j \mapsto (gh)u_j,$$

while

$$\widetilde{\lambda}_i(g)\widetilde{\lambda}_i(h)\colon u_j \mapsto hu_j \mapsto g(hu_j);$$

these are the same, by associativity. Thus,

$$\widetilde{\lambda}_i(gh) = \widetilde{\lambda}_i(g)\widetilde{\lambda}_i.$$

Finally, $\widetilde{\lambda}_i(1) = \lambda_i(1) = 1_{L_i}$, and so $\widetilde{\lambda}_i$ is an algebra map. •

It is natural to call two representations *equivalent* if their corresponding modules are isomorphic. The following definition arises from Corollary 7.23, which gives a criterion that $\mathbb{C}G$-modules $(\mathbb{C}^n)^{\sigma}$ and $(\mathbb{C}^n)^{\tau}$ are isomorphic as $\mathbb{C}G$-modules.

Definition. Let $\sigma, \tau\colon G \to \text{GL}(n, \mathbb{C})$ be representations of a group G. Then σ and τ are ***equivalent***, denoted by $\sigma \sim \tau$, if there is a nonsingular $n \times n$ matrix P that intertwines them; that is, for every $g \in G$,

$$P\sigma(g)P^{-1} = \tau(g).$$

Corollary 7.69.

(i) *Every irreducible representation of a finite group G is equivalent to one of the representations λ_i given in* Proposition 7.68(i).

(ii) *Every irreducible representation of a finite abelian group is linear.*

(iii) *If $\sigma\colon G \to \text{GL}(V)$ is a representation of a finite group G, then $\sigma(g)$ is similar to a diagonal matrix for each $g \in G$.*

Proof.

(i) If $\sigma\colon G \to \mathrm{GL}(V)$ is an irreducible representation σ, then the corresponding $\mathbb{C}G$-module V^σ is a simple module. Therefore, $V^\sigma \cong L_i$, for some i, by Proposition 7.42. But $L_i \cong V^{\lambda_i}$, so that $V^\sigma \cong V^{\lambda_i}$ and $\sigma \sim \lambda_i$.

(ii) Since G is abelian, $\mathbb{C}G = \bigoplus_i B_i$ is commutative, and so all $n_i = 1$ [we know that $B_i \cong \mathrm{Mat}_{n_i}(\mathbb{C})$, and the matrix ring is not commutative if $n_i \geq 2$]. But $\mathrm{degree}(\lambda_i) = n_i$, by Proposition 7.68(i).

(iii) If $\tau = \sigma|\langle g\rangle$, then $\tau(g) = \sigma(g)$. Now τ is a representation of the abelian group $\langle g\rangle$, and so part (ii) implies that the module V^τ is a direct sum of one-dimensional submodules. If $V^\tau = \langle v_1\rangle \oplus \cdots \oplus \langle v_m\rangle$, then the matrix of $\sigma(g)$ with respect to the basis $v_1, \ldots, v_m$ is diagonal. •

Example 7.70.

(i) The Wedderburn–Artin Theorems can be restated to say that every representation $\tau\colon G \to \mathrm{GL}(V)$ is completely reducible: $\tau = \sigma_1 + \cdots + \sigma_k$, where each σ_j is irreducible; moreover, the multiplicity of each σ_j is uniquely determined by τ. Since each σ_j is equivalent to the irreducible representation λ_i arising from a minimal left ideal L_i, we usually collect terms and write $\tau \sim \sum_i m_i\lambda_i$, where the multiplicities m_i are nonnegative integers.

(ii) The regular representation $\rho\colon G \to \mathrm{GL}(\mathbb{C}G)$ is important because every irreducible representation is a summand of it. Now ρ is equivalent to the sum

$$\rho \sim n_1\lambda_1 + \cdots + n_r\lambda_r,$$

where n_i is the degree of λ_i [recall that $\mathbb{C}G = \bigoplus_i B_i$, where $B_i \cong \mathrm{End}_{\mathbb{C}}(L_i) \cong \mathrm{Mat}_{n_i}(\mathbb{C})$; as a $\mathbb{C}G$-module, the simple module L_i can be viewed as the first columns of $n_i \times n_i$ matrices, and so B_i is a direct sum of n_i copies of L_i]. ◀

Recall that the *trace* of an $n \times n$ matrix $A = [a_{ij}]$ with entries in a commutative ring k is the sum of the diagonal entries: $\mathrm{tr}(A) = \sum_{i=1}^n a_{ii}$.

When k is a field, then $\mathrm{tr}(A)$ turns out to be the sum of the eigenvalues of A (we will assume this result now, but it is more convenient for us to prove it in the next chapter). Here are several other elementary facts about the trace that we will prove now.

Proposition 7.71.

(i) *If I is the $n \times n$ identity matrix and k is a field of characteristic 0, then* $\mathrm{tr}(I) = n$.

(ii) *If $A = [a_{ij}]$ and $B = [b_{ij}]$ are $n \times n$ matrices with entries in a commutative ring k, then*

$$\mathrm{tr}(A + B) = \mathrm{tr}(A) + \mathrm{tr}(B) \quad \textit{and} \quad \mathrm{tr}(AB) = \mathrm{tr}(BA).$$

(iii) *If $B = PAP^{-1}$, then* $\mathrm{tr}(B) = \mathrm{tr}(A)$.

Proof.

(i) The sum of the diagonal entries is n, which in not 0 because k has characteristic 0.

(ii) The additivity of trace follows from the diagonal entries of $A + B$ being $a_{ii} + b_{ii}$. If $(AB)_{ii}$ denotes the ii entry of AB, then

$$(AB)_{ii} = \sum_j a_{ij} b_{ji},$$

and so

$$\operatorname{tr}(AB) = \sum_i (AB)_{ii} = \sum_{i,j} a_{ij} b_{ji}.$$

Similarly,

$$\operatorname{tr}(BA) = \sum_{j,i} b_{ji} a_{ij}.$$

The entries commute because they lie in the commutative ring k, and so $a_{ij} b_{ji} = b_{ji} a_{ij}$ for all i, j. It follows that $\operatorname{tr}(AB) = \operatorname{tr}(BA)$, as desired.

(iii)
$$\operatorname{tr}(B) = \operatorname{tr}\big((PA)P^{-1}\big) = \operatorname{tr}\big(P^{-1}(PA)\big) = \operatorname{tr}(A). \quad \bullet$$

It follows from Proposition 7.71(iii) that we can define the trace of a linear transformation $T\colon V \to V$, where V is a vector space over a field k, as the trace of any matrix arising from it: if A and B are matrices of T, determined by two choices of bases of V, then $B = PAP^{-1}$ for some nonsingular matrix P, and so $\operatorname{tr}(B) = \operatorname{tr}(A)$.

Definition. If $\sigma\colon G \to \mathrm{GL}(V)$ is a representation, then its ***character*** is the function $\chi_\sigma\colon G \to \mathbb{C}$ defined by

$$\chi_\sigma(g) = \operatorname{tr}(\sigma(g)).$$

We call χ_σ the character ***afforded*** by σ. An ***irreducible character*** is a character afforded by an irreducible representation. The ***degree*** of χ_σ is defined to be the degree of σ; that is,

$$\operatorname{degree}(\chi_\sigma) = \operatorname{degree}(\sigma) = \dim(V).$$

Example 7.72.

(i) The character θ afforded by a linear representation (Example 7.67) is called a ***linear character***; that is, $\theta = \chi_\sigma$, where $\operatorname{degree}(\sigma) = 1$. Since every linear representation is simple, every linear character is irreducible.

(ii) The representation $\lambda_i\colon G \to \mathrm{GL}(L_i)$, given by $\lambda_i\colon u_i \mapsto g u_i$ if $u_i \in L_i$, is irreducible [see Proposition 7.68(i)]. Thus, the character χ_i afforded by λ_i, defined by

$$\chi_i = \chi_{\lambda_i},$$

is irreducible.

(iii) In light of Proposition 7.68(ii), it makes sense to speak of $\chi_i(u)$ for every $u \in \mathbb{C}G$. If we write $u = u_1 + \cdots + u_r \in B_1 \oplus \cdots \oplus B_r$, where $u_j \in B_j$, define $\chi_i(u) = \widetilde{\lambda}_i(u_i)$. In particular, $\chi_i(u_i) = \operatorname{tr}(\widetilde{\lambda}_i(u_i))$ and $\chi_i(u_j) = 0$ if $j \neq i$.

(iv) If $\sigma\colon G \to \mathrm{GL}(V)$ is a representation, then $\sigma(1)$ is the identity matrix. Hence, Proposition 7.71(i) gives $\chi_\sigma(1) = n$, where n is the degree of σ.

(v) Let $\sigma\colon G \to S_X$ be a homomorphism; as in Example 7.66, we may regard σ as a representation on V, where V is the vector space over $\mathbb{C}$ with basis X. For every $g \in G$, the matrix $\sigma(g)$ is a permutation matrix, and its xth diagonal entry is 1 if $\sigma(g)x = x$; otherwise, it is 0. Thus,

$$\chi_\sigma(g) = \mathrm{tr}(\sigma(g)) = \mathrm{Fix}(\sigma(g)),$$

the number of $x \in X$ fixed by $\sigma(g)$. In other words, if X is a G-set, then each $g \in G$ acts on X, and the number of ***fixed points*** of the action of g is a character value (see Example 7.92 for a related discussion). ◀

Characters are compatible with addition of representations. If $\sigma\colon G \to \mathrm{GL}(V)$ and $\tau\colon G \to \mathrm{GL}(W)$, then $\sigma + \tau\colon G \to \mathrm{GL}(V \oplus W)$, and

$$\mathrm{tr}((\sigma+\tau)(g)) = \mathrm{tr}\left(\begin{bmatrix}\sigma(g) & 0\\ 0 & \tau(g)\end{bmatrix}\right) = \mathrm{tr}(\sigma(g)) + \mathrm{tr}(\tau(g)).$$

Therefore,

$$\chi_{\sigma+\tau} = \chi_\sigma + \chi_\tau.$$

If σ and τ are equivalent representations, then

$$\mathrm{tr}(\sigma(g)) = \mathrm{tr}(P\sigma(g)P^{-1}) = \mathrm{tr}(\tau(g))$$

for all $g \in G$; that is, they have the same characters: $\chi_\sigma = \chi_\tau$. It follows that if $\sigma\colon G \to \mathrm{GL}(V)$ is a representation, then its character χ_σ can be computed relative to any convenient basis of V.

Proposition 7.73.

(i) *Every character χ_σ is a linear combination $\chi_\sigma = \sum_i m_i\chi_i$, where $m_i \geq 0$ are nonnegative integers and*

$$\chi_i = \chi_{\lambda_i}$$

is the irreducible character afforded by the irreducible representation λ_i arising from the minimal left ideal L_i.

(ii) *Equivalent representations have the same character.*

(iii) *The only irreducible characters of G are $\chi_1, \ldots, \chi_r$, the characters afforded by the irreducible representations λ_i.*

Proof.

(i) The character χ_σ arises from a representation σ of G, which, in turn, arises from a $\mathbb{C}G$-module V. But V is a semisimple module (because $\mathbb{C}G$ is a semisimple ring), and so V is a direct sum of simple modules: $V = \bigoplus_j S_j$. By Proposition 7.42, each $S_j \cong L_i$ for some minimal left ideal L_i. If, for each i, we let $m_i \geq 0$ be the number of S_j isomorphic to L_i, then $\chi_\sigma = \sum_i m_i\chi_i$.

(ii) This follows from part (ii) of Proposition 7.71 and Corollary 7.69(i).

(iii) This follows from part (ii) and Corollary 7.69(i). •

As a consequence of the proposition, we call $\chi_1, \dots, \chi_r$ ***the irreducible characters*** of G.

Example 7.74.

(i) The (linear) character χ_1 afforded by the trivial representation $\sigma\colon G \to \mathbb{C}$ with $\sigma(g) = 1$ for all $g \in G$ is called the ***trivial character***. Thus, $\chi_1(g) = 1$ for all $g \in G$.

(ii) Let us compute the ***regular character*** $\psi = \chi_\rho$ afforded by the regular representation $\rho\colon G \to \mathrm{GL}(\mathbb{C}G)$, where $\rho(g)\colon u \mapsto gu$ for all $g \in G$ and $u \in \mathbb{C}G$. Any basis of $\mathbb{C}G$ can be used for this computation; we choose the usual basis comprised of the elements of G. If $g = 1$, then Example 7.72(iv) shows that $\psi(1) = \dim(\mathbb{C}G) = |G|$. On the other hand, if $g \neq 1$, then for all $h \in G$, we have gh a basis element distinct from h. Therefore, the matrix of $\rho(g)$ has 0's on the diagonal, and so its trace is 0. Thus,

$$\psi(g) = \begin{cases} 0 & \text{if } g \neq 1 \\ |G| & \text{if } g = 1. \end{cases} \qquad \blacktriangleleft$$

We have already proved that equivalent representations have the same character. The coming discussion will give the converse: if two representations have the same character, then they are equivalent.

Definition. A function $\varphi\colon G \to \mathbb{C}$ is a ***class function*** if it is constant on conjugacy classes; that is, if $h = xgx^{-1}$, then $\varphi(h) = \varphi(g)$.

Every character χ_σ afforded by a representation σ is a class function: if $h = xgx^{-1}$, then

$$\sigma(h) = \sigma(xgx^{-1}) = \sigma(x)\sigma(g)\sigma(x)^{-1},$$

and so $\mathrm{tr}(\sigma(h)) = \mathrm{tr}(\sigma(g))$; that is,

$$\chi_\sigma(h) = \chi_\sigma(g).$$

Not every class function is a character. For example, if χ is a character, then $-\chi$ is a class function; it is not a character because $-\chi(1)$ is negative, and so it cannot be a degree.

Definition. We denote the set of all class functions $G \to \mathbb{C}$ by $\mathrm{cf}(G)$:

$$\mathrm{cf}(G) = \{\varphi\colon G \to \mathbb{C} : \varphi(g) = \varphi(xgx^{-1}) \text{ for all } x, g \in G\}.$$

It is easy to see that $\mathrm{cf}(G)$ is a vector space over $\mathbb{C}$.

An element $u = \sum_{g\in G} c_g g \in \mathbb{C}G$ is an n-tuple (c_g) of complex numbers; that is, u is a function $u\colon G \to \mathbb{C}$ with $u(g) = c_g$ for all $g \in G$. From this viewpoint, we see that $\mathrm{cf}(G)$ is a subring of $\mathbb{C}G$. Note that a class function is a scalar multiple of a class sum; therefore, Lemma 7.57 says that $\mathrm{cf}(G)$ is the center $Z(\mathbb{C}G)$, and so

$$\dim(\mathrm{cf}(G)) = r,$$

where r is the number of conjugacy classes in G (Theorem 7.58).

Definition. Write $\mathbb{C}G = B_1 \oplus \cdots \oplus B_r$, where $B_i \cong \mathrm{End}_{\mathbb{C}}(L_i)$, and let e_i denote the identity element of B_i; hence,

$$1 = e_1 + \cdots + e_r,$$

where 1 is the identity element of $\mathbb{C}G$. The elements e_i are called the ***idempotents*** in $\mathbb{C}G$.

Not only is each e_i an idempotent, that is, $e_i^2 = e_i$, but it is easy to see that

$$e_i e_j = \delta_{ij} e_i,$$

where δ_{ij} is the Kronecker delta.

Lemma 7.75. *The irreducible characters $\chi_1, \ldots, \chi_r$ form a basis of* $\mathrm{cf}(G)$.

Proof. We have just seen that $\dim(\mathrm{cf}(G)) = r$, and so it suffices to prove that $\chi_1, \ldots, \chi_r$ is a linearly independent list, by Corollary 2.112(ii). We have already noted that $\chi_i(u_j) = 0$ for all $j \neq i$; in particular, $\chi_i(e_j) = 0$. On the other hand, $\chi_i(e_i) = n_i$, where n_i is the degree of χ_i, for it is the trace of the $n_i \times n_i$ identity matrix.

Suppose now that $\sum_i c_i \chi_i = 0$. It follows, for all j, that

$$0 = \Big(\sum_i c_i \chi_i\Big)(e_j) = c_j \chi_j(e_j) = c_j n_j.$$

Therefore, all $c_j = 0$, as desired. •

Since $\chi_i(1)$ is the trace of the $n_i \times n_i$ identity matrix, we have

$$n_i = \chi_i(1) = \sum_j \chi_i(e_j) = \chi_i(e_i), \tag{1}$$

where e_i is the identity element of B_i.

Theorem 7.76. *Two representations σ, τ of a finite group G are equivalent if and only if they afford the same character*: $\chi_\sigma = \chi_\tau$.

Proof. We have already proved necessity, in Proposition 7.73(ii). For sufficiency, Proposition 7.73(i) says that every representation is completely reducible: there are nonnegative integers m_i and ℓ_i with $\sigma \sim \sum_i m_i \lambda_i$ and $\tau \sim \sum_i \ell_i \lambda_i$. By hypothesis, the corresponding characters coincide:

$$\sum_i m_i \chi_i = \chi_\sigma = \chi_\tau = \sum_i \ell_i \chi_i.$$

As the irreducible characters $\chi_1, \ldots, \chi_r$ are a basis of $\mathrm{cf}(G)$, $m_i = \ell_i$ for all i, and so $\sigma \sim \tau$. •

There are relations between the irreducible characters that facilitate their calculation. We begin by finding the expression of the idempotents e_i in terms of the basis G of $\mathbb{C}G$. Observe, for all $y \in G$, that

$$\chi_i(e_i y) = \chi_i(y), \tag{2}$$

for $y = \sum_j e_j y$, and so $\chi_i(y) = \sum_j \chi_i(e_j y) = \chi_i(e_i y)$, because $e_j y \in B_j$.

Proposition 7.77. *If* $e_i = \sum_{g\in G} a_{ig}g$, *where* $a_{ig} \in \mathbb{C}$, *then*

$$a_{ig} = \frac{n_i\chi_i(g^{-1})}{|G|}.$$

Proof. Let ψ be the regular character; that is, ψ is the character afforded by the regular representation. Now $e_ig^{-1} = \sum_h a_{ih}hg^{-1}$, so that

$$\psi(e_ig^{-1}) = \sum_{h\in G} a_{ih}\psi(hg^{-1}).$$

By Example 7.74(ii), $\psi(1) = |G|$ when $h = g$ and $\psi(hg^{-1}) = 0$ when $h \neq g$. Therefore,

$$a_{ig} = \frac{\psi(e_ig^{-1})}{|G|}.$$

On the other hand, since $\psi = \sum_j n_j\chi_j$, we have

$$\psi(e_ig^{-1}) = \sum_j n_j\chi_j(e_ig^{-1}) = n_i\chi_i(e_ig^{-1}),$$

by Proposition 7.68(ii). But $\chi_i(e_ig^{-1}) = \chi_i(g^{-1})$, by Equation (1). Therefore, $a_{ig} = n_i\chi_i(g^{-1})/|G|$. •

It is now convenient to equip $\mathrm{cf}(G)$ with an inner product.

Definition. If $\alpha, \beta \in \mathrm{cf}(G)$, define

$$(\alpha, \beta) = \frac{1}{|G|}\sum_{g\in G} \alpha(g)\overline{\beta(g)},$$

where $\overline{c}$ denotes the complex conjugate of a complex number c.

It is easy to see that we have defined an inner product;[8] that is, for all $c_1, c_2 \in \mathbb{C}$,

(i) $(c_1\alpha_1 + c_2\alpha_2, \beta) = c_1(\alpha_1, \beta) + c_2(\alpha_2, \beta)$;

(ii) $(\beta, \alpha) = \overline{(\alpha, \beta)}$.

Note that (α, α) is real, by (ii), and the inner product is *definite*; that is, $(\alpha, \alpha) > 0$ if $\alpha \neq 0$.

Theorem 7.78. *With respect to the inner product just defined, the irreducible characters* $\chi_1, \ldots, \chi_r$ *form an orthonormal basis*; *that is,*

$$(\chi_i, \chi_j) = \delta_{ij}.$$

Proof. By Proposition 7.77, we have

$$e_j = \frac{1}{|G|}\sum_g n_j\chi_j(g^{-1})g.$$

[8]This inner product is *not* symmetric because we have $(\beta, \alpha) = \overline{(\alpha, \beta)}$, not $(\beta, \alpha) = (\alpha, \beta)$. Such a function is often called a *Hermitian form* or a *sesquilinear form* (*sesqui* means "one and a half").

Hence,

$$\chi_i(e_j)/n_j = \frac{1}{|G|}\sum_g \chi_j(g^{-1})\chi_i(g) = \frac{1}{|G|}\sum_g \chi_i(g)\overline{\chi_j(g)} = (\chi_i, \chi_j);$$

the next to last equation follows from Exercise 7.30 on page 588, for χ_j is a character (not merely a class function), and so $\chi_j(g^{-1}) = \overline{\chi_j(g)}$. The result now follows, for $\chi_i(e_j)/n_j = \delta_{ij}$, by Equations (1) and (2). •

The inner product on $\mathrm{cf}(G)$ can be used to check irreducibility.

Definition. A ***generalized character*** φ on a finite group G is a $\mathbb{Z}$-linear combination

$$\varphi = \sum_i m_i\chi_i,$$

where $\chi_1, \ldots, \chi_r$ are the irreducible characters of G and all $m_i \in \mathbb{Z}$.

If θ is a character, then $\theta = \sum_i m_i\chi_i$, where all the coefficients are *nonnegative* integers, by Proposition 7.73.

Corollary 7.79. *A generalized character θ of a group G is an irreducible character if and only if $\theta(1) > 0$ and $(\theta, \theta) = 1$.*

Proof. If θ is an irreducible character, then $\theta = \chi_i$ for some i, and so $(\theta, \theta) = (\chi_i, \chi_i) = 1$. Moreover, $\theta(1) = \deg(\chi_i) > 0$.

Conversely, let $\theta = \sum_j m_j\chi_j$, where $m_j \in \mathbb{Z}$, and suppose that $(\theta, \theta) = 1$. Then $1 = \sum_j m_j^2$; hence, some $m_i^2 = 1$ and all other $m_j = 0$. Therefore, $\theta = \pm\chi_i$, and so $\theta(1) = \pm\chi_i(1)$. Since $\chi_i(1) = \deg(\chi_i) > 0$, the hypothesis $\theta(1) > 0$ gives $m_i = 1$. Therefore, $\theta = \chi_i$, and so θ is an irreducible character. •

Let us assemble the notation we will use from now on.

Notation. If G is a finite group, we denote its conjugacy classes by

$$C_1, \ldots, C_r,$$

a choice of elements, one from each conjugacy class, by

$$g_1 \in C_1, \ldots, g_r \in C_r,$$

its irreducible characters by

$$\chi_1, \ldots, \chi_r,$$

their degrees by

$$n_1 = \chi_1(1), \ldots, n_r = \chi_r(1),$$

and the sizes of the conjugacy classes by

$$h_1 = |C_1|, \ldots, h_r = |C_r|.$$

The matrix $[\chi_i(g_j)]$ is a useful way to display information.

Definition. The ***character table*** of G is the $r \times r$ complex matrix whose ij entry is $\chi_i(g_j)$.

We always assume that $C_1 = \{1\}$ and that χ_1 is the trivial character. Thus, the first row consists of all 1's, while the first column consists of the degrees of the characters: $\chi_i(1) = n_i$ for all i, by Example 7.72(iv). The ith row of the character table consists of the values

$$\chi_i(1), \chi_i(g_2), \ldots, \chi_i(g_r).$$

There is no obvious way of labeling the other conjugacy classes (or the other irreducible characters), so that a finite group G has many character tables. Nevertheless, we usually speak of "the" character table of G.

Since the inner product on $\mathrm{cf}(G)$ is summed over all $g \in G$, not just the chosen g_i (one from each conjugacy class), it can be rewritten as a "weighted" inner product:

$$(\chi_i, \chi_j) = \frac{1}{|G|} \sum_{k=1}^{r} h_k \chi_i(g_k) \overline{\chi_j(g_k)}.$$

Theorem 7.78 says that the weighted inner product of distinct rows in the character table is 0, while the weighted inner product of any row with itself is 1.

Example 7.80. A character table can have complex entries. For example, it is easy to see that the character table for a cyclic group $G = \langle x \rangle$ of order 3 is given in Table 1, where $\omega = e^{2\pi i/3}$ is a primitive cube root of unity. ◀

g_i	1	x	x^2
h_i	1	1	1
χ_1	1	1	1
χ_2	1	ω	ω^2
χ_3	1	ω^2	ω

Table 1. Character table of $\mathbb{I}_3$.

Example 7.81. Write the four-group in additive notation:

$$\mathbf{V} = \{0, a, b, a + b\}.$$

As a vector space over $\mathbb{F}_2$, $\mathbf{V}$ has basis a, b, and the "coordinate functions" on $\mathbf{V}$, which take values in $\{1, -1\} \subseteq \mathbb{C}$, are linear; hence, they are irreducible representations. For example, the character χ_2 arising from the function that is nontrivial on a and trivial on b is

$$\chi_2(v) = \begin{cases} -1 & \text{if } v = a \quad \text{or} \quad v = a + b \\ 1 & \text{if } v = 0 \quad \text{or} \quad v = b. \end{cases}$$

Table 2 is the character table for $\mathbf{V}$.

Table 3 is the character table for the symmetric group $G = S_3$. Since two permutations in S_n are conjugate if and only if they have the same cycle structure, there are three conjugacy classes, and we choose elements 1, (1 2), and (1 2 3) from each. In Example 7.60(i), we saw that there are three irreducible representations: $\lambda_1 =$ the trivial representation, $\lambda_2 = \mathrm{sgn}$, and a third representation λ_3 of degree 2. We now give the character table, after which we discuss its entries.

g_i	0	a	b	$a+b$
h_i	1	1	1	1
χ_1	1	1	1	1
χ_2	1	-1	1	-1
χ_3	1	1	-1	-1
χ_4	1	-1	-1	1

Table 2. Character table of $\mathbf{V}$.

g_i	1	(1 2)	(1 2 3)
h_i	1	3	2
χ_1	1	1	1
χ_2	1	-1	1
χ_3	2	0	-1

Table 3. Character table of S_3.

We have already discussed the first row and column of any character table. Since $\chi_2 = \text{sgn}$, the second row records the fact that 1 and (1 2 3) are even while (1 2) is odd. The third row has entries

$$2 \quad a \quad b,$$

where a and b are to be found. The weighted inner products of row 3 with the other two rows give the equations

$$2 + 3a + 2b = 0$$
$$2 - 3a + 2b = 0.$$

It follows easily that $a = 0$ and $b = -1$. ◀

The following lemma will be used to describe the inner products of the columns of the character table.

Lemma 7.82. *If A is the character table of a finite group G, then A is nonsingular and its inverse A^{-1} has ij entry*

$$(A^{-1})_{ij} = \frac{h_i \overline{\chi_j(g_i)}}{|G|}.$$

Proof. If B is the matrix whose ij entry is displayed in the statement, then

$$(AB)_{ij} = \frac{1}{|G|} \sum_k \chi_i(g_k) h_k \overline{\chi_j(g_k)} = \frac{1}{|G|} \sum_g \chi_i(g) \overline{\chi_j(g)} = (\chi_i, \chi_j) = \delta_{ij},$$

because $h_k \overline{\chi_j(g_k)} = \sum_{y \in C_k} \overline{\chi_j(y)}$. Therefore, $AB = I$. •

The next result is fundamental.

Theorem 7.83 (Orthogonality Relations). *Let G be a finite group of order n with conjugacy classes $C_1, \ldots, C_r$ of cardinalities $h_1, \ldots, h_r$, respectively, and choose elements $g_i \in C_i$. Let the irreducible characters of G be $\chi_1, \ldots, \chi_r$, and let χ_i have degree n_i. Then the following relations hold:*

(i)

$$\sum_{k=1}^{r} h_k \chi_i(g_k) \overline{\chi_j(g_k)} = \begin{cases} 0 & \text{if } i \neq j; \\ |G| & \text{if } i = j. \end{cases}$$

(ii)
$$\sum_{i=1}^{r} \chi_i(g_k)\overline{\chi_i(g_\ell)} = \begin{cases} 0 & \text{if } k \neq \ell; \\ |G|/h_k & \text{if } k = \ell. \end{cases}$$

Proof.

(i) This is just a restatement of Theorem 7.78.

(ii) If A is the character table of G and $B = [h_i\overline{\chi_j(g_i)}/|G|]$, we proved, in Lemma 7.82, that $AB = I$. It follows that $BA = I$; that is, $(BA)_{k\ell} = \delta_{k\ell}$. Therefore,
$$\frac{1}{|G|}\sum_i h_k\overline{\chi_i(g_k)}\chi_i(g_\ell) = \delta_{k\ell},$$
and this is the second orthogonality relation. •

In terms of the character table, the second orthogonality relation says that the usual (unweighted, but with complex conjugation) inner product of distinct columns is 0 while, for every k, the usual inner product of column k with itself is $|G|/h_k$.

The orthogonality relations yield the following special cases.

Corollary 7.84.

(i) $|G| = \sum_{i=1}^{r} n_i^2$.
(ii) $\sum_{i=1}^{r} n_i\chi_i(g_k) = 0 \quad \text{if } k > 1$.
(iii) $\sum_{k=1}^{r} h_k\chi_i(g_k) = 0 \quad \text{if } i > 1$.
(iv) $\sum_{k=1}^{r} h_k|\chi_i(g_k)|^2 = |G|$.

Proof.

(i) This equation records the inner product of column 1 with itself: it is Theorem 7.83(ii) when $k = \ell = 1$.

(ii) This is the special case of Theorem 7.83(ii) with $\ell = 1$, for $\chi_i(1) = n_i$.

(iii) This is the special case of Theorem 7.83(i) in which $j = 1$.

(iv) This is the special case of Theorem 7.83(i) in which $j = i$. •

We can now give another proof of Burnside's Lemma, Theorem 1.124, which counts the number of orbits of a G-set.

Theorem 7.85 (Burnside's Lemma). *Let G be a finite group and let X be a finite G-set. If N is the number of orbits of X, then*
$$N = \frac{1}{|G|}\sum_{g\in G} \mathrm{Fix}(g),$$
where $\mathrm{Fix}(g)$ *is the number of $x \in X$ with $gx = x$.*

Proof. Let V be the complex vector space having X as a basis. As in Example 7.66, the G-set X gives a representation $\sigma\colon G \to \mathrm{GL}(V)$ by $\sigma(g)(x) = gx$ for all $g \in G$ and $x \in X$; moreover, if χ_σ is the character afforded by σ, then Example 7.72(v) shows that $\chi_\sigma(g) = \mathrm{Fix}(g)$.

Let $\mathcal{O}_1, \ldots, \mathcal{O}_N$ be the orbits of X. We begin by showing that $N = \dim(V^G)$, where V^G is the space of *fixed points*:

$$V^G = \{v \in V : gv = v \text{ for all } g \in G\}.$$

For each i, define s_i to be the sum of all the x in $\mathcal{O}_i$; it suffices to prove that these elements form a basis of V^G. It is plain that $s_1, \ldots, s_N$ is a linearly independent list in V^G, and it remains to prove that they span V^G. If $u \in V^G$, then $u = \sum_{x\in X} c_x x$, so that $gu = \sum_{x\in X} c_x(gx)$. Since $gu = u$, however, $c_x = c_{gx}$. Thus, given $x \in X$ with $x \in \mathcal{O}_j$, each coefficient of gx, where $g \in G$, is equal to c_x; that is, all the x lying in the orbit $\mathcal{O}_j$ have the same coefficient, say, c_j, and so $u = \sum_j c_j s_j$. Therefore,

$$N = \dim(V^G).$$

Now define a linear transformation $T\colon V \to V$ by

$$T = \frac{1}{|G|}\sum_{g\in G} \sigma(g).$$

It is routine to check that T is a $\mathbb{C}G$-map, that $T|(V^G) = \text{identity}$, and that $\operatorname{im} T = V^G$. Since $\mathbb{C}G$ is semisimple, $V = V^G \oplus W$ for some submodule W. We claim that $T|W = 0$. If $w \in W$, then $\sigma(g)(w) \in W$ for all $g \in G$, because W is a submodule, and so $T(w) \in W$. On the other hand, $T(w) \in \operatorname{im} T = V^G$, and so $T(w) \in V^G \cap W = \{0\}$, as claimed.

If $w_1, \ldots, w_\ell$ is a basis of W, then $s_1, \ldots, s_N, w_1, \ldots, w_\ell$ is a basis of $V = V^G \oplus W$. Note that T fixes each s_i and annihilates each w_j. Since trace preserves sums,

$$\mathrm{tr}(T) = \frac{1}{|G|}\sum_{g\in G} \mathrm{tr}(\sigma(g)) = \frac{1}{|G|}\sum_{g\in G} \chi_\sigma(g) = \frac{1}{|G|}\sum_{g\in G} \mathrm{Fix}(g).$$

It follows that

$$\mathrm{tr}(T) = \dim(V^G),$$

for the matrix of T with respect to the chosen basis is the direct sum of an identity block and a zero block, and so $\mathrm{tr}(T)$ is the size of the identity block, namely, $\dim(V^G) = N$. Therefore,

$$N = \frac{1}{|G|}\sum_{g\in G} \mathrm{Fix}(g). \quad \bullet$$

Character tables can be used to detect normal subgroups.

Definition. If χ_τ is the character afforded by a representation $\tau\colon G \to \mathrm{GL}(V)$, then

$$\ker \chi_\tau = \ker \tau.$$

Proposition 7.86. *Let $\theta = \chi_\tau$ be the character of a finite group G afforded by a representation $\tau\colon G \to \mathrm{GL}(V)$.*

(i) *For each $g \in G$, we have*

$$|\theta(g)| \le \theta(1).$$

(ii)

$$\ker\theta = \{g \in G : \theta(g) = \theta(1)\}.$$

(iii) *If $\theta = \sum_j m_j\chi_j$, where m_j are positive integers, then*

$$\ker\theta = \bigcap_j \ker\chi_j.$$

(iv) *If N is a normal subgroup of G, there are irreducible characters $\chi_{i_1}, \ldots, \chi_{i_s}$ with $N = \bigcap_{j=1}^{s} \ker\chi_{i_j}$.*

Proof.

(i) By Lagrange's Theorem, $g^{|G|} = 1$ for every $g \in G$; it follows that the eigenvalues $\varepsilon_1, \ldots, \varepsilon_d$ of $\tau(g)$, where $d = \theta(1)$, are $|G|$th roots of unity, and so $|\varepsilon_j| = 1$ for all j. By the triangle inequality in $\mathbb{C}$,

$$\big|\theta(g)\big| = \Big|\sum_{j=1}^{d} \varepsilon_j\Big| \le d = \theta(1).$$

(ii) If $g \in \ker\theta = \ker\tau$, then $\tau(g) = I$, the identity matrix, and $\theta(g) = \mathrm{tr}(I) = \theta(1)$. Conversely, suppose that $\theta(g) = \theta(1) = d$; that is, $\sum_{j=1}^{d} \varepsilon_j = d$. By Proposition 2.73, all the eigenvalues ε_j are equal, say, $\varepsilon_j = \omega$ for all j. Therefore, $\tau(g) = \omega I$, by Corollary 7.69(iii), and so

$$\theta(g) = \theta(1)\omega.$$

But $\theta(g) = \theta(1)$, by hypothesis, and so $\omega = 1$; that is, $\tau(g) = I$ and $g \in \ker\tau$.

(iii) For all $g \in G$, we have

$$\theta(g) = \sum_j m_j\chi_j(g);$$

in particular,

$$\theta(1) = \sum_j m_j\chi_j(1).$$

If $g \in \ker\theta$, then $\theta(g) = \theta(1)$. Suppose that $\chi_{j'}(g) \ne \chi_{j'}(1)$ for some j'. Since $\chi_{j'}(g)$ is a sum of roots of unity, Proposition 2.73 applies to force $|\chi_{j'}(g)| < \chi_{j'}(1)$, and so $|\theta(g)| \le \sum_j m_j|\chi_j(g)| < \sum_j \chi_j(1) = 1$, which implies that $\theta(g) \ne \theta(1)$, a contradiction. Therefore, $g \in \bigcap_j \ker\chi_j$. For the reverse inclusion, if $g \in \ker\chi_j$, then $\chi_j(g) = \chi_j(1)$, and so

$$\theta(g) = \sum_j m_j\chi_j(g) = \sum_j m_j\chi_j(1) = \theta(1);$$

hence, $g \in \ker\theta$.

(iv) It suffices to find a representation of G whose kernel is N. By part (ii) and Example 7.74(ii), the regular representation ρ of G/N is faithful (i.e., is an injection), and so its kernel is $\{1\}$. If $\pi\colon G \to G/N$ is the natural map, then $\rho\pi$ is a representation of G having kernel N. If θ is the character afforded by $\rho\pi$, then $\theta = \sum_j m_j\chi_j$, where the m_j are positive integers, by Lemma 7.75, and so part (iii) applies. •

Example 7.87. We will construct the character table of S_4 in Example 7.97. We can see there that $\ker\chi_2 = A_4$ and $\ker\chi_3 = \mathbf{V}$ are the only two normal subgroups of S_4 (other than $\{1\}$ and S_4). Moreover, we can see that $\mathbf{V} \subseteq A_4$.

In Example 7.88, we can see that $\ker\chi_2 = \{1\} \cup z^G \cup y^G$ (where z^G denotes the conjugacy class of z in G) and $\ker\chi_3 = \{1\} \cup z^G \cup x^G$. Another normal subgroup occurs as $\ker\chi_2 \cap \ker\chi_3 = \{1\} \cup z^G$. ◀

A normal subgroup described by characters is given as a union of conjugacy classes; this viewpoint can give another proof of the simplicity of A_5. In Exercise 1.97 on page 74, we saw that A_5 has five conjugacy classes, of sizes 1, 12, 12, 15, and 20. Since every subgroup contains the identity element, the order of a normal subgroup of A_5 is the sum of some of these numbers, including 1. But it is easy to see that 1 and 60 are the only such sums that are divisors of 60, and so the only normal subgroups are $\{1\}$ and A_5 itself.

There is a way to "lift" a representation of a quotient group to a representation of the group.

Definition. Let $H \lhd G$ and let $\sigma\colon G/H \to \mathrm{GL}(V)$ be a representation. If $\pi\colon G \to G/H$ is the natural map, then the representation $\sigma\pi\colon G \to \mathrm{GL}(V)$ is called a ***lifting*** of σ.

Scalar multiplication of G on a $\mathbb{C}(G/H)$-module V is given, for $v \in V$, by

$$gv = (gH)v.$$

Thus, every $\mathbb{C}(G/H)$-submodule of V is also a $\mathbb{C}G$-submodule; hence, if V is a simple $\mathbb{C}(G/H)$-module, then it is also a simple $\mathbb{C}G$-module. It follows that if $\sigma\colon G/H \to \mathrm{GL}(V)$ is an irreducible representation of G/H, then its lifting $\sigma\pi$ is also an irreducible representation of G.

Example 7.88. We know that D_8 and $\mathbf{Q}$ are nonisomorphic nonabelian groups of order 8; we now show that they have the same character tables.

If G is a nonabelian group of order 8, then its center has order 2, say, $Z(G) = \langle z\rangle$. Now $G/Z(G)$ is not cyclic, by Exercise 1.77 on page 59, and so $G/Z(G) \cong \mathbf{V}$. Therefore, if $\sigma\colon \mathbf{V} \to \mathbb{C}$ is an irreducible representation of $\mathbf{V}$, then its lifting $\sigma\pi$ is an irreducible representation of G. This gives four (necessarily irreducible) linear characters of G, each of which takes value 1 on z. As G is not abelian, there must be an irreducible character χ_5 of degree $n_5 > 1$ (if all $n_i = 1$, then $\mathbb{C}G$ is commutative and G is abelian). Since $\sum_i n_i^2 = 8$, we see that $n_5 = 2$. Thus, there are five irreducible representations and, hence, five conjugacy classes; choose representatives g_i to be $1, z, x, y, w$. Table 4 on page 580 is the character table.

g_i	1	z	x	y	w
h_i	1	1	2	2	2
χ_1	1	1	1	1	1
χ_2	1	1	-1	1	-1
χ_3	1	1	1	-1	-1
χ_4	1	1	-1	-1	1
χ_5	2	-2	0	0	0

Table 4. Character table of D_8 and of $\mathbf{Q}$.

The values for χ_5 are computed from the orthogonality relations of the columns. For example, if the last row of the character table is

$$2 \quad a \quad b \quad c \quad d,$$

then the inner product of columns 1 and 2 gives the equation $4 + 2a = 0$, so that $a = -2$. The reader may verify that $0 = b = c = d$. ◀

The orthogonality relations help to complete a character table but, obviously, it would also be useful to have a supply of characters. One important class of characters consists of those afforded by *induced representations*; that is, representations of a group G determined by representations of a subgroup H of G.

The original construction of induced representations, due to Frobenius, is rather complicated. Tensor products make this construction more natural. The ring $\mathbb{C}G$ is a $(\mathbb{C}G, \mathbb{C}H)$-bimodule (for $\mathbb{C}H$ is a subring of $\mathbb{C}G$), so that if V is a left $\mathbb{C}H$-module, then the tensor product $\mathbb{C}G \otimes_{\mathbb{C}H} V$ is defined; Proposition 6.106 says that this tensor product is, in fact, a left $\mathbb{C}G$-module.

Definition. Let H be a subgroup of a group G. If V is a left $\mathbb{C}H$-module, then the ***induced module*** is the left $\mathbb{C}G$-module

$$V\uparrow^G = \mathbb{C}G \otimes_{\mathbb{C}H} V.$$

The corresponding representation $\rho\uparrow^G : G \to V^G$ is called the ***induced representation***. The character of G afforded by $\rho\uparrow^G$ is called the ***induced character***, and it is denoted by $\chi_\rho\uparrow^G$.

Let us recognize at the outset that the character of an induced representation need not restrict to the original representation of the subgroup. For example, we have seen that there is an irreducible character χ of $A_3 \cong \mathbb{I}_3$ having complex values, whereas every irreducible character of S_3 has (real) integer values. A related observation is that two elements may be conjugate in a group but not conjugate in a subgroup (for example, 3-cycles are conjugate in S_3, for they have the same cycle structure, but they are not conjugate in the abelian group A_3).

The next lemma will help us compute the character afforded by an induced representation.

Lemma 7.89.

(i) *If $H \subseteq G$, then $\mathbb{C}G$ is a free right $\mathbb{C}H$-module on $[G:H]$ generators.*

(ii) *If a left $\mathbb{C}H$-module V has a (vector space) basis $e_1, \ldots, e_m$, then a (vector space) basis of the induced module $V\uparrow^G = \mathbb{C}G \otimes_{\mathbb{C}H} V$ is the family of all $t_i \otimes e_j$, where $t_1, \ldots, t_n$ is a transversal of H in G.*

Proof.

(i) Since $t_1, \ldots, t_n$ is a transversal of H in G (of course, $n = [G:H]$), we see that G is the disjoint union

$$G = \bigcup_i t_i H;$$

thus, for every $g \in G$, there is a unique i and a unique $h \in H$ with $g = t_i h$. We claim that $t_1, \ldots, t_n$ is a basis of $\mathbb{C}G$ viewed as a right $\mathbb{C}H$-module.

If $u \in \mathbb{C}G$, then $u = \sum_g a_g g$, where $a_g \in \mathbb{C}$. Rewrite each term

$$a_g g = a_g t_i h = t_i a_g h$$

(scalars in $\mathbb{C}$ commute with everything), collect terms involving the same t_i, and obtain $u = \sum_i t_i \eta_i$, where $\eta_i \in \mathbb{C}H$.

To prove uniqueness of this expression, suppose that $0 = \sum_i t_i \eta_i$, where $\eta_i \in \mathbb{C}H$. Now $\eta_i = \sum_{h \in H} a_{ih} h$, where $a_{ih} \in \mathbb{C}$. Substituting,

$$0 = \sum_{i,h} a_{ih} t_i h.$$

But $t_i h = t_j h'$ if and only if $i = j$ and $h = h'$, so that $0 = \sum_{i,h} a_{ih} t_i h = \sum_{g \in G} a_{ih} g$, where $g = t_i h$. Since the elements of G form a basis of $\mathbb{C}G$ (viewed as a vector space over $\mathbb{C}$), we have $a_{ih} = 0$ for all i, h, and so $\eta_i = 0$ for all i.

(ii) By Theorem 6.110,

$$\mathbb{C}G \otimes_{\mathbb{C}H} V \cong \bigoplus_i t_i \mathbb{C}H \otimes_{\mathbb{C}H} V.$$

It follows that every $u \in \mathbb{C}G \otimes_{\mathbb{C}H} V$ has a unique expression as a $\mathbb{C}$-linear combination of $t_i \otimes e_j$, and so these elements comprise a basis. •

Notation. If $H \subseteq G$ and $\chi\colon H \to \mathbb{C}$ is a function, then $\dot{\chi}\colon G \to \mathbb{C}$ is given by

$$\dot{\chi}(g) = \begin{cases} 0 & \text{if } g \notin H \\ \chi(g) & \text{if } g \in H. \end{cases}$$

Theorem 7.90. *If χ_σ is the character afforded by a representation $\sigma\colon H \to \mathrm{GL}(V)$ of a subgroup H of a group G, then the induced character $\chi_\sigma\uparrow^G$ is given by*

$$\chi_\sigma\uparrow^G(g) = \frac{1}{|H|} \sum_{a \in G} \dot{\chi}_\sigma(a^{-1} g a).$$

Proof. Let $t_1, \ldots, t_n$ be a transversal of H in G, so that G is the disjoint union $G = \bigcup_i t_i H$, and let $e_1, \ldots, e_m$ be a (vector space) basis of V. By Lemma 7.89, a basis for the vector space $V^G = \mathbb{C}G \otimes_{\mathbb{C}H} V$ consists of all $t_i \otimes e_j$. If $g \in G$, we compute the matrix of left multiplication by g relative to this basis. Note that

$$gt_i = t_{k(i)} h_i,$$

where $h_i \in H$, and so

$$g(t_i \otimes e_j) = (gt_i) \otimes e_j = t_{k(i)} h_i \otimes e_j = t_{k(i)} \otimes \sigma(h_i) e_j$$

(the last equation holds because we can slide any element of H across the tensor sign). Now $g(t_i \otimes e_j)$ is written as a $\mathbb{C}$-linear combination of *all* the basis elements of $V\uparrow^G$, for the coefficients $t_p \otimes e_j$ for $p \neq k(i)$ are all 0. Hence, $\sigma\uparrow^G(g)$ gives the $nm \times nm$ matrix whose m columns labeled by $t_i \otimes e_j$, for fixed i, are all zero except for an $m \times m$ block equal to

$$[a_{pq}(h_i)] = [a_{pq}(t_{k(i)}^{-1} g t_i)].$$

Thus, the big matrix is partitioned into $m \times m$ blocks, most of which are 0, and a nonzero block is on the diagonal of the big matrix if and only if $k(i) = i$; that is,

$$t_{k(i)}^{-1} g t_i = t_i^{-1} g t_i = h_i \in H.$$

The induced character is the trace of the big matrix, which is the sum of the traces of these blocks on the diagonal. Therefore,

$$\chi_\sigma\uparrow^G(g) = \sum_{t_i^{-1} g t_i \in H} \operatorname{tr}([a_{pq}(t_i^{-1} g t_i)]) = \sum_i \dot{\chi}_\sigma(t_i^{-1} g t_i)$$

(remember that $\dot{\chi}_\sigma$ is 0 outside of H). We now rewrite the summands (to get a formula that does not depend on the choice of the transversal): if $t_i^{-1} g t_i \in H$, then $(t_i h)^{-1} g (t_i h) = h^{-1}(t_i^{-1} g t_i) h$ in H, so that, for fixed i,

$$\sum_{h \in H} \dot{\chi}_\sigma\big((t_i h)^{-1} g (t_i h)\big) = |H| \dot{\chi}_\sigma(t_i^{-1} g t_i),$$

because χ_σ is a class function on H. Therefore,

$$\chi_\sigma\uparrow^G(g) = \sum_i \dot{\chi}_\sigma(t_i^{-1} g t_i) = \frac{1}{|H|} \sum_{i,h} \dot{\chi}_\sigma\big((t_i h)^{-1} g (t_i h)\big) = \frac{1}{|H|} \sum_{a \in G} \dot{\chi}_\sigma(a^{-1} g a). \quad \bullet$$

Remark. We have been considering induced characters, but it is easy to generalize the discussion to ***induced class functions***. If $H \subseteq G$, then a class function θ on H has a unique expression as a $\mathbb{C}$-linear combination of irreducible characters of H, say, $\theta = \sum c_i \chi_i$, and so we can define

$$\theta\uparrow^G = \sum c_i \chi_i\uparrow^G.$$

It is plain that $\theta\uparrow^G$ is a class function on G, and that the formula in Theorem 7.90 extends to induced class functions. ◀

If, for $h \in H$, the matrix of $\sigma(h)$ (with respect to the basis $e_1, \ldots, e_m$ of V) is $B(h)$, then define $m \times m$ matrices $\dot{B}(g)$, for all $g \in G$, by

$$\dot{B}(g) = \begin{cases} 0 & \text{if } g \notin H; \\ B(g) & \text{if } g \in H. \end{cases}$$

The proof of Theorem 7.90 allows us to picture the matrix of the induced representation in block form

$$\sigma\uparrow^G(g) = \begin{bmatrix} \dot{B}(t_1^{-1}gt_1) & \dot{B}(t_1^{-1}gt_2) & \cdots & \dot{B}(t_1^{-1}gt_n) \\ \dot{B}(t_2^{-1}gt_1) & \dot{B}(t_2^{-1}gt_2) & \cdots & \dot{B}(t_2^{-1}gt_n) \\ \vdots & \vdots & \vdots & \vdots \\ \dot{B}(t_n^{-1}gt_1) & \dot{B}(t_n^{-1}gt_2) & \cdots & \dot{B}(t_n^{-1}gt_n) \end{bmatrix}.$$

Corollary 7.91. *Let H be a subgroup of a finite group G and let χ be a character on H.*

(i) $\chi\uparrow^G(1) = [G : H]\chi(1)$.

(ii) *If $H \lhd G$, then $\chi\uparrow^G(g) = 0$ for all $g \notin H$.*

Proof.

(i) For all $a \in G$, we have $a^{-1}1a = 1$, so that there are $|G|$ terms in the sum $\chi\uparrow^G(1) = \frac{1}{|H|}\sum_{a\in G} \dot{\chi}(a^{-1}ga)$ that are equal to $\chi(1)$; hence,

$$\chi\uparrow^G(1) = \frac{|G|}{|H|}\chi(1) = [G : H]\chi(1).$$

(ii) If $H \lhd G$, then $g \notin H$ implies that $a^{-1}ga \notin H$ for all $a \in G$. Therefore, $\dot{\chi}(a^{-1}ga) = 0$ for all $a \in G$, and so $\chi\uparrow^G(g) = 0$. •

Example 7.92. Let $H \subseteq G$ be a subgroup of index n, let $X = \{t_1H, \ldots, t_nH\}$ be the family of left cosets of H, and let $\varphi\colon G \to S_X$ be the (permutation) representation of G on the cosets of H. As in Example 7.72(v), we may regard $\varphi\colon G \to \mathrm{GL}(V)$, where V is the vector space over $\mathbb{C}$ having basis X; that is, φ is a representation in the sense of this section.

We claim that if χ_φ is the character afforded by φ, then $\chi_\varphi = \epsilon\uparrow^G$, where ϵ is the trivial character on H. On the one hand, Example 7.72(v) shows that

$$\chi_\varphi(g) = \mathrm{Fix}(\varphi(g))$$

for every $g \in G$. On the other hand, suppose $\varphi(g)$ is the permutation (in two-rowed notation)

$$\varphi(g) = \begin{pmatrix} t_1H & \ldots & t_nH \\ gt_1H & \ldots & gt_nH \end{pmatrix}.$$

Now $gt_iH = t_iH$ if and only if $t_i^{-1}gt_i \in H$. Thus, $\dot{\epsilon}(t_i^{-1}gt_i) \neq 0$ if and only if $gt_iH = t_iH$, and so

$$\epsilon\uparrow^G(g) = \mathrm{Fix}(\varphi(g)). \quad \blacktriangleleft$$

Even though a character λ of a subgroup H is irreducible, its induced character need not be irreducible. For example, let $G = S_3$ and let H be the cyclic subgroup generated by (1 2). The linear representation $\sigma = \text{sgn}\colon H \to \mathbb{C}$ is irreducible, and it affords the character χ_σ with

$$\chi_\sigma(1) = 1 \quad \text{and} \quad \chi_\sigma((1\ 2)) = -1.$$

Using the formula for the induced character, we find that

$$\chi_\sigma\uparrow^{S_3}(1) = 3, \quad \chi_\sigma\uparrow^{S_3}((1\ 2)) = -1, \quad \text{and} \quad \chi_\sigma\uparrow^{S_3}((1\ 2\ 3)) = 0.$$

Corollary 7.79 shows that $\chi_\sigma\uparrow^{S_3}$ is not irreducible, for $(\chi_\sigma\uparrow^{S_3}, \chi_\sigma\uparrow^{S_3}) = 2$. It is easy to see that $\chi_\sigma\uparrow^{S_3} = \chi_2 + \chi_3$, the latter being the nontrivial irreducible characters of S_3.

Here is an important result of Brauer (Curtis–Reiner, *Representation Theory of Finite Groups and Associative Algebras*, p. 283). Call a subgroup E of a finite group G ***elementary*** if $E = Z \times P$, where Z is cyclic and P is a p-group for some prime p.

Theorem 7.93 (Brauer). *Every complex character θ on a finite group G has the form*

$$\theta = \sum_i m_i \mu_i\uparrow^G,$$

where $m_i \in \mathbb{Z}$ and the μ_i are linear characters on elementary subgroups of G.

Proof. See Curtis–Reiner, *Representation Theory of Finite Groups and Associative Algebras*, p. 283. •

Definition. If H is a subgroup of a group G, then every representation $\sigma\colon G \to \text{GL}(V)$ gives, by restriction, a representation $\sigma|H\colon H \to \text{GL}(V)$. (In terms of modules, every left $\mathbb{C}G$-module V can be viewed as a left $\mathbb{C}H$-module.) We call $\sigma|H$ the ***restriction*** of σ, and we denote it by $\sigma\downarrow_H$. The character of H afforded by $\sigma\downarrow_H$ is denoted by $\chi_\sigma\downarrow_H$.

The next result displays an interesting relation between characters on a group and characters on a subgroup. (Formally, it resembles the Adjoint Isomorphism.)

Theorem 7.94 (Frobenius Reciprocity). *Let H be a subgroup of a group G, let χ be a class function on G, and let θ be a class function on H. Then*

$$(\theta\uparrow^G, \chi)_G = (\theta, \chi\downarrow_H)_H,$$

where $(\square, \square)_G$ denotes the inner product on $\text{cf}(G)$ and $(\square, \square)_H$ denotes the inner product on $\text{cf}(H)$.

Proof. We have

$$\begin{aligned}(\theta\uparrow^G, \chi)_G &= \frac{1}{|G|}\sum_{g\in G} \theta\uparrow^G(g)\overline{\chi(g)}\\ &= \frac{1}{|G|}\sum_{g\in G}\frac{1}{|H|}\sum_{a\in G}\dot\theta(a^{-1}ga)\overline{\chi(g)}\\ &= \frac{1}{|G|}\frac{1}{|H|}\sum_{a,g\in G}\dot\theta(a^{-1}ga)\overline{\chi(a^{-1}ga)},\end{aligned}$$

the last equation occurring because χ is a class function. For fixed $a \in G$, as g ranges over G, then so does $a^{-1}ga$. Therefore, writing $x = a^{-1}ga$, the equations continue:

$$\begin{aligned}&= \frac{1}{|G|}\frac{1}{|H|}\sum_{a,x\in G}\dot\theta(x)\overline{\chi(x)}\\ &= \frac{1}{|G|}\frac{1}{|H|}\sum_{a\in G}\Big(\sum_{x\in G}\dot\theta(x)\overline{\chi(x)}\Big)\\ &= \frac{1}{|G|}\frac{1}{|H|}|G|\sum_{x\in G}\dot\theta(x)\overline{\chi(x)}\\ &= \frac{1}{|H|}\sum_{x\in G}\dot\theta(x)\overline{\chi(x)}\\ &= (\theta, \chi\downarrow_H)_H,\end{aligned}$$

the next to last equation holding because $\dot\theta(x)$ vanishes off the subgroup H. •

The following elementary remark facilitates the computation of induced class functions.

Lemma 7.95. *Let H be a subgroup of a finite group G, and let χ be a class function on H. Then*

$$\chi\uparrow^G(g) = \frac{1}{|H|}\sum_i |C_G(g_i)|\dot\chi(g_i^{-1}gg_i).$$

Proof. Let $|C_G(g_i)| = m_i$. If $a_0^{-1}g_ia_0 = g$, we claim that there are exactly m_i elements $a \in G$ with $a^{-1}g_ia = g$. There are at least m_i elements in G conjugating g_i to g; namely, all aa_0 for $a \in C_G(g_i)$. There are at most m_i elements, for if $b^{-1}g_ib = g$, then $b^{-1}g_ib = a_0^{-1}g_ia_0$, and so $a_0b \in C_G(g_i)$. The result now follows by collecting terms involving g_is in the formula for $\chi\uparrow^G(g)$. •

Example 7.96. Table 5 is the character table of A_4, where $\omega = e^{2\pi i/3}$ is a primitive cube root of unity.

The group A_4 consists of the identity, eight 3-cycles, and three products of disjoint transpositions. In S_4, all the 3-cycles are conjugate; if $g = (1\ 2\ 3)$, then $[S_4 : C_{S_4}(g)] = 8$. It follows that $|C_{S_4}(g)| = 3$, and so $C_{S_4}(g) = \langle g\rangle$. Therefore, in A_4, the number of conjugates of g is $[A_4 : C_{A_4}(g)] = 4$ [we know that $C_{A_4}(g) = A_4 \cap C_{S_4}(g) = \langle g\rangle$]. The reader may show that g and g^{-1} are not conjugate, and so we have verified the first two rows of the character table.

g_i	(1)	(1 2 3)	(1 3 2)	(1 2)(3 4)
h_i	1	4	4	3
χ_1	1	1	1	1
χ_2	1	ω	ω^2	1
χ_3	1	ω^2	ω	1
χ_4	3	0	0	-1

Table 5. Character table of A_4.

The rows for χ_2 and χ_3 are liftings of linear characters of $A_4/\mathbf{V} \cong \mathbb{I}_3$. Note that if $h = (1\ 2)(3\ 4)$, then $\chi_2(h) = \chi_2(1) = 1$, because $\mathbf{V}$ is the kernel of the lifted representation; similarly, $\chi_3(h) = 1$. Now $\chi_4(1) = 3$, because $3 + (n_4)^2 = 12$. The bottom row arises from orthogonality of the columns. (We can check, using Corollary 7.79, that the character of degree 3 is irreducible.) ◀

Example 7.97. Table 6 is the character table of S_4.

g_i	(1)	(1 2)	(1 2 3)	(1 2 3 4)	(1 2)(3 4)
h_i	1	6	8	6	3
χ_1	1	1	1	1	1
χ_2	1	-1	1	-1	1
χ_3	2	0	-1	0	2
χ_4	3	1	0	-1	-1
χ_5	3	-1	0	1	-1

Table 6. Character table of S_4.

We know, for all n, that two permutations in S_n are conjugate if and only if they have the same cycle structure; the sizes of the conjugacy classes in S_4 were computed in Table 1 on page 10.

The rows for χ_2 and χ_3 are liftings of irreducible characters of $S_4/\mathbf{V} \cong S_3$. The entries in the fourth column of these rows arise from $(1\ 2)\mathbf{V} = (1\ 2\ 3\ 4)\mathbf{V}$; the entries in the last column of these rows arise from $\mathbf{V}$ being the kernel (in either case), so that $\chi_j((1\ 2)(3\ 4)) = \chi_j(1)$ for $j = 2, 3$.

We complete the first column using $24 = 1+1+4+n_4^2+n_5^2$; thus, $n_4 = 3 = n_5$. Let us see whether χ_4 is an induced character; if it is, then Corollary 7.91(i) shows that it arises from a linear character of a subgroup H of index 3. Such a subgroup has order 8, and so it is a Sylow 2-subgroup; that is, $H \cong D_8$. Let us choose one such subgroup:

$$H = \big\langle \mathbf{V}, (1\ 3) \big\rangle = \mathbf{V} \cup \{(1\ 3), (2\ 4), (1\ 2\ 3\ 4), (1\ 4\ 3\ 2)\}.$$

The conjugacy classes are

$$\begin{aligned} C_1 &= \{1\};\\ C_2 &= \{(1\ 3)(2\ 4)\};\\ C_3 &= \{(1\ 2)(3\ 4), (1\ 4)(2\ 3)\};\\ C_4 &= \{(1\ 3), (2\ 4)\};\\ C_5 &= \{(1\ 2\ 3\ 4), (1\ 4\ 3\ 2)\}. \end{aligned}$$

Let θ be the character on H defined by

$$\begin{array}{ccccc} C_1 & C_2 & C_3 & C_4 & C_5 \\ 1 & 1 & -1 & 1 & -1. \end{array}$$

Define $\chi_4 = \theta\uparrow^{S_4}$. Using the formula for induced characters, assisted by Lemma 7.95, we obtain the fourth row of the character table. However, before going on to row 5, we observe that Corollary 7.79 shows that χ_4 is irreducible, for $(\chi_4, \chi_4) = 1$. Finally, the orthogonality relations allow us to compute row 5. ◀

At this point in the story, we must introduce algebraic integers. Since G is a finite group, Lagrange's Theorem gives $g^{|G|} = 1$ for all $g \in G$. It follows that if $\sigma\colon G \to \mathrm{GL}(V)$ is a representation, then $\sigma(g)^{|G|} = I$ for all g; hence, all the eigenvalues of $\sigma(g)$ are $|G|$th roots of unity, and so all the eigenvalues are algebraic integers. By Proposition 2.70, the trace of $\sigma(g)$, being the sum of the eigenvalues, is also an algebraic integer.

We can now prove the following interesting result.

Theorem 7.98. *The degrees n_i of the irreducible characters of a finite group G are divisors of $|G|$.*

Proof. By Theorem 2.63, the rational number $\alpha = |G|/n_i$ is an integer if it is also an algebraic integer. Now Corollary 6.37(ii) says that α is an algebraic integer if there is a faithful $\mathbb{Z}[\alpha]$-module M that is a finitely generated abelian group, where $\mathbb{Z}[\alpha]$ is the smallest subring of $\mathbb{C}$ containing α.

By Proposition 7.77, we have

$$e_i = \sum_{g\in G} \frac{n_i}{|G|}\chi_i(g^{-1})g = \sum_{g\in G} \frac{1}{\alpha}\chi_i(g^{-1})g.$$

Hence, $\alpha e_i = \sum_{g\in G} \chi_i(g^{-1})g$. But e_i is an idempotent: $e_i^2 = e_i$, and so

$$\alpha e_i = \sum_{g\in G} \chi_i(g^{-1})ge_i.$$

Define M to be the abelian subgroup of $\mathbb{C}G$ generated by all elements of the form $\zeta g e_i$, where ζ is a $|G|$th root of unity and $g \in G$; of course, M is a finitely generated abelian group.

To see that M is a $\mathbb{Z}[\alpha]$-module, it suffices to show that $\alpha M \subseteq M$. But

$$\alpha\zeta g e_i = \zeta g \alpha e_i = \zeta g \sum_{h\in G} \chi_i(h^{-1}) h e_i = \sum_{h\in G} \chi_i(h^{-1}) \zeta g h e_i.$$

This last element lies in M, however, because $\chi_i(h^{-1})$ is a sum of $|G|$th roots of unity.

Finally, if $\beta \in \mathbb{C}$ and $u \in \mathbb{C}G$, then $\beta u = 0$ if and only if $\beta = 0$ or $u = 0$. Since $\mathbb{Z}[\alpha] \subseteq \mathbb{C}$ and $M \subseteq \mathbb{C}G$, however, it follows that M is a faithful $\mathbb{Z}[\alpha]$-module, as desired. •

We will present two important applications of Character Theory in the next section; for other applications, as well as a more serious study of representations, the interested reader should look at the books by Curtis–Reiner, Feit, Huppert, and Isaacs.

Representation Theory is used throughout the proof of the Classification Theorem of Finite Simple Groups. An account of this theorem, describing the infinite families of such groups as well as the 26 sporadic simple groups, can be found in the ATLAS, by Conway et al. This book contains the character tables of every simple group of order under 10^{25} as well as the character tables of all the sporadic groups.

Exercises

7.29. Prove that if θ is a generalized character of a finite group G, then there are characters χ and ψ with $\theta = \chi - \psi$.

∗ **7.30.** (i) Prove that if z is a complex root of unity, then $z^{-1} = \overline{z}$.

(ii) Prove that if G is a finite group and $\sigma\colon G \to \mathrm{GL}(V)$ is a representation, then

$$\chi_\sigma(g^{-1}) = \overline{\chi_\sigma(g)}$$

for all $g \in G$.

Hint. Use the fact that every eigenvalue of $\sigma(g)$ is a root of unity, as well as the fact that if A is a nonsingular matrix over a field k and if $u_1, \ldots, u_n$ are the eigenvalues of A (with multiplicities), then the eigenvalues of A^{-1} are $u_1^{-1}, \ldots, u_n^{-1}$; that is, $\overline{u_1}, \ldots, \overline{u_n}$.

7.31. If $\sigma\colon G \to \mathrm{GL}(n, \mathbb{C})$ is a representation, its ***contragredient*** $\sigma^*\colon G \to \mathrm{GL}(n, \mathbb{C})$ is the function given by

$$\sigma^*(g) = \sigma(g^{-1})^\top,$$

where $\square^\top$ denotes transpose.

(i) Prove that the contragredient of a representation σ is a representation that is irreducible when σ is irreducible.

(ii) Prove that the character χ_{σ^*} afforded by the contragredient σ^* is

$$\chi_{\sigma^*}(g) = \overline{\chi_\sigma(g)},$$

where $\overline{\chi_\sigma(g)}$ is the complex conjugate. Conclude that if χ is a character of G, then $\overline{\chi}$ is also a character.

∗ **7.32.** Construct an irreducible representation of S_3 of degree 2.

7.33. (i) Let $g \in G$, where G is a finite group. Prove that g is conjugate to g^{-1} if and only if $\chi(g)$ is real for every character χ of G.

(ii) Prove that every character of S_n is real-valued. (It is a theorem of Frobenius that every character of S_n is integer-valued.)

7.34. (i) Recall that the *character group* G^* of a finite abelian group G is

$$G^* = \mathrm{Hom}(G, \mathbb{C}^\times),$$

where $\mathbb{C}^\times$ is the multiplicative group of nonzero complex numbers ($\mathbb{C}^\times \cong \mathbb{R}/\mathbb{Z}$, by Corollary 8.30). Prove that $G^* \cong G$.

Hint. Use the Fundamental Theorem of Finite Abelian Groups.

(ii) Prove that $\mathrm{Hom}(G, \mathbb{C}^\times) \cong \mathrm{Hom}(G, \mathbb{Q}/\mathbb{Z})$ when G is a finite abelian group.

∗ **7.35.** Prove that the only linear character of a simple group is the trivial character. Conclude that if χ_i is not the trivial character, then $n_i = \chi_i(1) > 1$.

∗ **7.36.** Let $\theta = \chi_\sigma$ be the character afforded by a representation σ of a finite group G.

(i) If $g \in G$, prove that $|\theta(g)| = \theta(1)$ if and only if $\sigma(g)$ is a scalar matrix.
Hint. Use Proposition 2.73 on page 121.

(ii) If θ is an irreducible character, prove that

$$Z(G/\ker\theta) = \{g \in G : |\theta(g)| = \theta(1)\}.$$

∗ **7.37.** If G is a finite group, prove that the number of its (necessarily irreducible) linear representations is $[G : G']$.

7.38. Let G be a finite group.

(i) If $g \in G$, show that $|C_G(g)| = \sum_{i=1}^{r} |\chi_i(g)|^2$. Conclude that the character table of G gives $|C_G(g)|$.

(ii) Show how to use the character table of G to see whether G is abelian.

(iii) Show how to use the character table of G to find the lattice of normal subgroups of G and their orders.

(iv) If G is a finite group, show how to use its character table to find the commutator subgroup G'.
Hint. If $K \lhd G$, then the character table of G/K is a submatrix of the character table of G, and so we can find the abelian quotient of G having largest order.

(v) Show how to use the character table of a finite group G to determine whether G is solvable.

7.39. (i) Show how to use the character table of G to find $|Z(G)|$.

(ii) Show how to use the character table of a finite group G to determine whether G is nilpotent.

7.40. Recall that the group $\mathbf{Q}$ of quaternions has the presentation

$$\mathbf{Q} = (A, B | A^4 = 1, A^2 = B^2, BAB^{-1} = A^{-1}).$$

(i) Show that there is a representation $\sigma\colon \mathbf{Q} \to \mathrm{GL}(2,\mathbb{C})$ with

$$A \mapsto \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \text{ and } B \mapsto \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

(ii) Prove that σ is an irreducible representation.

7.41. (i) If $\sigma\colon G \to \mathrm{GL}(V)$ and $\tau\colon G \to \mathrm{GL}(W)$ are representations, prove that

$$\sigma \otimes \tau\colon G \to \mathrm{GL}(V \otimes W),$$

defined by

$$(\sigma \otimes \tau)(g) = \sigma(g) \otimes \tau(g)$$

is a representation.

(ii) Prove that the character afforded by $\sigma \otimes \tau$ is the pointwise product:

$$\chi_\sigma \chi_\tau\colon g \mapsto \mathrm{tr}(\sigma(g))\,\mathrm{tr}(\tau(g)).$$

(iii) Prove that $\mathrm{cf}(G)$ is a commutative ring (usually called the ***Burnside ring*** of G).

Section 7.6. Theorems of Burnside and of Frobenius

Character Theory will be used in this section to prove two important results in Group Theory: Burnside's $p^m q^n$ Theorem and a theorem of Frobenius. We begin with the following variation of Schur's Lemma.

Proposition 7.99 (Schur's Lemma II). *If $\sigma\colon G \to \mathrm{GL}(V)$ is an irreducible representation and a linear transformation $\varphi\colon V \to V$ satisfies*

$$\varphi\sigma(g) = \sigma(g)\varphi$$

for all $g \in G$, then φ is a scalar transformation: there exists $\omega \in \mathbb{C}$ with $\varphi = \omega 1_V$.

Proof. The vector space V is a $\mathbb{C}G$-module with scalar multiplication $gv = \sigma(g)(v)$ for all $v \in V$, and any linear transformation θ satisfying the equation $\theta\sigma(g) = \sigma(g)\theta$ for all $g \in G$ is a $\mathbb{C}G$-map $V^\sigma \to V^\sigma$. Since σ is irreducible, the $\mathbb{C}G$-module V^σ is simple. By Schur's Lemma, $\mathrm{End}(V^\sigma)$ is a division ring, and so every nonzero element in it is nonsingular. Now $\varphi - \omega 1_V \in \mathrm{End}(V^\sigma)$ for every $\omega \in \mathbb{C}$; in particular, this is so when ω is an eigenvalue of φ (which lies in $\mathbb{C}$ because $\mathbb{C}$ is algebraically closed). The definition of eigenvalue says that $\varphi - \omega 1_V$ is singular, and so it must be 0; that is, $\varphi = \omega 1_V$, as desired. •

Recall that if L_i is a minimal left ideal in $\mathbb{C}G$ and $\lambda_i\colon G \to \mathrm{End}_{\mathbb{C}}(L_i)$ is the corresponding irreducible representation, then we extended λ_i to a linear transformation $\widetilde{\lambda}_i\colon \mathbb{C}G \to \mathrm{End}_{\mathbb{C}}(L_i)$:

$$\widetilde{\lambda}_i(g)u_j = \begin{cases} gu_i & \text{if } j = i \\ 0 & \text{if } j \neq i \end{cases}$$

Thus, $\widetilde{\lambda}_i(g) = \lambda_i(g)$ for all $g \in G$. In Proposition 7.68(ii), we proved that $\widetilde{\lambda}_i$ is a $\mathbb{C}$-algebra map.

Corollary 7.100. *Let L_i be a minimal left ideal in $\mathbb{C}G$, let $\lambda_i\colon G \to \mathrm{End}_{\mathbb{C}}(L_i)$ be the corresponding irreducible representation, and let $\widetilde{\lambda}_i\colon \mathbb{C}G \to \mathrm{End}_{\mathbb{C}}(L_i)$ be the algebra map of* Proposition 7.68(ii).

(i) *If $z \in Z(\mathbb{C}G)$, then there is $\omega_i(z) \in \mathbb{C}$ with*

$$\widetilde{\lambda}_i(z) = \omega_i(z)I.$$

(ii) *The function $\omega_i\colon Z(\mathbb{C}G) \to \mathbb{C}$, given by $z \mapsto \omega_i(z)$, is an algebra map.*

Proof.

(i) Let $z \in Z(\mathbb{C}G)$. We verify the hypothesis of Schur's Lemma II in the special case $V = L_i$, $\sigma = \lambda_i$, and $\varphi = \widetilde{\lambda}_i(z)$. For all $g \in G$, we have $\widetilde{\lambda}_i(z)\lambda_i(g) = \lambda_i(zg)$ (because $\widetilde{\lambda}_i$ is a multiplicative map extending λ_i), while $\lambda_i(g)\widetilde{\lambda}_i(z) = \lambda_i(gz)$. These are equal, for $zg = gz$ because $z \in Z(\mathbb{C}G)$. Proposition 7.99 now says that $\widetilde{\lambda}_i(z) = \omega_i(z)I$ for some $\omega_i(z) \in \mathbb{C}$.

(ii) This follows from the equation $\widetilde{\lambda}_i(z) = \omega_i(z)I$ and Proposition 7.68, which says that $\widetilde{\lambda}_i$ is an algebra map. •

Recall, from Lemma 7.57, that a basis for $Z(\mathbb{C}G)$ consists of the *class sums*

$$z_i = \sum_{g \in C_i} g,$$

where the conjugacy classes of G are $C_1, \ldots, C_r$.

Proposition 7.101. *Let $z_1, \ldots, z_r$ be the class sums of a finite group G.*

(i) *For each i, j, we have*

$$\omega_i(z_j) = \frac{h_j \chi_i(g_j)}{n_i},$$

where $g_j \in C_j$.

(ii) *There are nonnegative integers $a_{ij\nu}$ with*

$$z_i z_j = \sum_{\nu} a_{ij\nu} z_\nu.$$

(iii) *The complex numbers $\omega_i(z_j)$ are algebraic integers.*

Proof.

(i) Computing the trace of $\widetilde{\lambda}_i(z_j) = \omega_i(z_j)I$ gives

$$n_i\omega_i(z_j) = \chi_i(z_j) = \sum_{g \in C_j} \chi_i(g) = h_j\chi_i(g_j),$$

for χ_i is constant on the conjugacy class C_j. Therefore, $\omega_i(z_j) = h_j\chi_i(g_j)/n_i$.

(ii) Choose $g_\nu \in C_\nu$. The definition of multiplication in the group algebra shows that the coefficient of g_ν in $z_i z_j$ is

$$|\{(g_i, g_j) \in C_i \times C_j : g_i g_j = g_\nu\}|,$$

the cardinality of a finite set, and hence it is a nonnegative integer. As all the coefficients of z_ν are equal [for we are in $Z(\mathbb{C}G)$], it follows that this number is $a_{ij\nu}$.

(iii) Let M be the (additive) subgroup of $\mathbb{C}$ generated by all $\omega_i(z_j)$, for $j = 1, \ldots, r$. Since ω_i is an algebra map,

$$\omega_i(z_j)\omega_i(z_\ell) = \sum_\nu a_{j\ell\nu}\omega_i(z_\nu),$$

so that M is a ring that is finitely generated as an abelian group (because $a_{ij\nu} \in \mathbb{Z}$). Hence, for each j, M is a $\mathbb{Z}[\omega_i(z_j)]$-module that is a finitely generated abelian group. If M is faithful, then Corollary 6.37(ii) will give $\omega_i(z_j)$ an algebraic integer. But $M \subseteq \mathbb{C}$, so that the product of nonzero elements is nonzero, and this implies that M is a faithful $\mathbb{Z}[\omega_i(z_j)]$-module, as desired. •

We are almost ready to complete the proof of Burnside's Theorem.

Proposition 7.102. *If $(n_i, h_j) = 1$ for some i, j, then either $|\chi_i(g_j)| = n_i$ or $\chi_i(g_j) = 0$.*

Proof. By hypothesis, there are integers s and t in $\mathbb{Z}$ with $sn_i + th_j = 1$, so that, for $g_j \in C_j$, we have

$$\frac{\chi_i(g_j)}{n_i} = s\chi_i(g_j) + \frac{th_j\chi_i(g_j)}{n_i}.$$

Hence, Proposition 7.101 gives $\chi_i(g_j)/n_i$ an algebraic integer, and so $|\chi_i(g_j)| \le n_i$, by Proposition 7.86(i). Thus, it suffices to show that if $|\chi_i(g_j)/n_i| < 1$, then $\chi_i(g_j) = 0$.

Let $m(x) \in \mathbb{Z}[x]$ be the minimum polynomial of $\alpha = \chi_i(g_j)/n_i$; that is, $m(x)$ is the monic polynomial in $\mathbb{Z}[x]$ of least degree having α as a root. We proved, in Corollary 2.145, that $m(x)$ is irreducible in $\mathbb{Q}[x]$. If α' is a root of $m(x)$, then Proposition 3.14 shows that $\alpha' = \sigma(\alpha)$ for some $\sigma \in \mathrm{Gal}(E/\mathbb{Q})$, where $E/\mathbb{Q}$ is the splitting field of $m(x)(x^{|G|} - 1)$. But

$$\alpha = \frac{1}{n_i}\left(\varepsilon_1 + \cdots + \varepsilon_{n_i}\right),$$

where the ε's are $|G|$th roots of unity, and so $\alpha' = \sigma(\alpha)$ is also such a sum. It follows that $|\alpha'| \le 1$ [as in the proof of Proposition 7.86(i)]. Therefore, if $N(\alpha)$ is the norm of α [which is, by definition, the absolute value of the product of all the roots of $m(x)$], then $N(\alpha) < 1$ (for we are assuming that $|\alpha| < 1$). But $N(\alpha)$ is the absolute value of the constant term of $m(x)$, which is an integer. Therefore, $N(\alpha) = 0$, hence $\alpha = 0$, and so $\chi_i(g_j) = 0$, as claimed. •

At last, we can prove Theorem 7.63.

Theorem 7.103. *If G is a nonabelian finite simple group, then $\{1\}$ is the only conjugacy class whose size is a prime power. Therefore, Burnside's Theorem is true: every group of order $p^m q^n$, where p and q are primes, is solvable.*

Proof. Assume, on the contrary, that $h_j = p^e > 1$ for some j. By Exercise 7.36 on page 589, for all i, we have

$$Z(G/\ker\chi_i) = \{g \in G : |\chi_i(g)| = n_i\}.$$

Since G is simple, $\ker\chi_i = \{1\}$ for all i, and so $Z(G/\ker\chi_i) = Z(G) = \{1\}$. By Proposition 7.102, if $(n_i, h_j) = 1$, then either $|\chi_i(g_j)| = n_i$ or $\chi_i(g_j) = 0$. Of course, $\chi_1(g_j) = 1$ for all j, where χ_1 is the trivial character. If χ_i is not the trivial character, then we have just seen that the first possibility cannot occur, and so $\chi_i(g_j) = 0$. On the other hand, if $(n_i, h_j) \neq 1$, then $p \mid n_i$ (for $h_j = p^e$). Thus, for every $i \neq 1$, either $\chi_i(g_j) = 0$ or $p \mid n_i$.

Consider the orthogonality relation, Corollary 7.84(ii):

$$\sum_{i=1}^{r} n_i\chi_i(g_j) = 0.$$

Now $n_1 = 1 = \chi_1(g_j)$, while each of the other terms is either 0 or of the form $p\alpha_i$, where α_i is an algebraic integer. It follows that

$$0 = 1 + p\beta,$$

where β is an algebraic integer. This implies that the rational number $-1/p$ is an algebraic integer, hence lies in $\mathbb{Z}$, and we have the contradiction that $-1/p$ is an integer. •

Another early application of characters is a theorem of Frobenius. We begin with a discussion of doubly transitive permutation groups. Let G be a finite group and X a finite G-set. Recall that if $x \in X$, then its *orbit* is $\mathcal{O}(x) = \{gx : g \in G\}$ and its *stabilizer* is $G_x = \{g \in G : gx = x\}$. Theorem 1.107 shows that $|\mathcal{O}(x)||G_x| = |G|$. A G-set X is *transitive* if it has only one orbit: if $x, y \in X$, then there exists $g \in G$ with $y = gx$; in this case, $\mathcal{O}(x) = X$.

If X is a G-set, then there is a homomorphism $\alpha\colon G \to S_X$, namely, $g \mapsto \alpha_g$, where $\alpha_g(x) = gx$. We say that X is a ***faithful*** G-set if α is an injection; that is, if $gx = x$ for all $x \in X$, then $g = 1$. In this case, we may regard G as a subgroup of S_X acting as permutations of X.

Cayley's Theorem (Theorem 1.95) shows that every group G can be regarded as a faithful transitive G-set.

Definition. A G-set X is ***doubly transitive*** if, for every pair of 2-tuples (x_1, x_2) and (y_1, y_2) in $X \times X$ with $x_1 \neq x_2$ and $y_1 \neq y_2$, there exists $g \in G$ with $y_1 = gx_1$ and $y_2 = gx_2$.[9]

We often abuse language and call a *group* G doubly transitive if there exists a doubly transitive G-set.

[9]More generally, we call a G-set X k-transitive, where $1 \leq k \leq |X|$, if, for every pair of k-tuples $(x_1, \ldots, x_k)$ and $(y_1, \ldots, y_k)$ in $X \times \cdots \times X$ having distinct coordinates, there exists $g \in G$ with $y_i = gx_i$ for all $i \leq k$. Using the Classification Theorem of Finite Simple Groups, it can be proved that if $k > 5$, then the only faithful k-transitive groups are the symmetric groups and the alternating groups. The five ***Mathieu groups*** are interesting sporadic simple groups that are also highly transitive: M_{22} is 3-transitive, M_{11} and M_{23} are 4-transitive, and M_{12} and M_{24} are 5-transitive.

Note that every doubly transitive G-set X is transitive: if $x \neq y$, then (x, y) and (y, x) are 2-tuples as in the definition, and so there is $g \in G$ with $y = gx$ (and $x = gy$).

Example 7.104.

(i) If $n \geq 2$, the symmetric group S_n is doubly transitive; that is, $X = \{1, \ldots, n\}$ is a doubly transitive S_X-set.

(ii) The alternating group A_n is doubly transitive if $n \geq 4$.

(iii) Let V be a finite-dimensional vector space over $\mathbb{F}_2$, and let $X = V - \{0\}$. Then X is a doubly transitive $\mathrm{GL}(V)$-set, for every pair of distinct nonzero vectors x_1, x_2 in V must be linearly independent (Exercise 2.74 on page 144). Since every linearly independent list can be extended to a basis, there is a basis $x_1, x_2, \ldots, x_n$ of V. Similarly, if y_1, y_2 is another pair of distinct nonzero vectors, there is a basis $y_1, y_2, \ldots, y_n$. But $\mathrm{GL}(V)$ acts transitively on the set of all bases of V, by Exercise 2.86 on page 155. Therefore, there is $g \in \mathrm{GL}(V)$ with $y_i = gx_i$ for all i, and so X is a doubly transitive $\mathrm{GL}(V)$-set. ◀

Proposition 7.105. *A G-set X is doubly transitive if and only if, for each $x \in X$, the G_x-set $X - \{x\}$ is transitive.*

Proof. Let X be a doubly transitive G-set. If $y, z \in X - \{x\}$, then (y, x) and (z, x) are 2-tuples of distinct elements of X, and so there is $g \in G$ with $z = gy$ and $x = gx$. The latter equation shows that $g \in G_x$, and so $X - \{x\}$ is a transitive G_x-set.

To prove the converse, let (x_1, x_2) and (y_1, y_2) be 2-tuples of distinct elements of X. We must find $g \in G$ with $y_1 = gx_1$ and $y_2 = gy_2$. Let us denote (gx_1, gx_2) by $g(x_1, x_2)$. There is $h \in G_{x_2}$ with $h(x_1, x_2) = (y_1, x_2)$: if $x_1 = y_1$, we may take $h = 1_X$; if $x_1 \neq y_1$, we use the hypothesis that $X - \{x_2\}$ is a transitive G_{x_2}-set. Similarly, there is $h' \in G_{y_1}$ with $h'(y_1, x_2) = (y_1, y_2)$. Therefore, $h'h(x_1, x_2) = (y_1, y_2)$, and X is a doubly transitive G-set. •

Example 7.106. Let k be a field, let $f(x) \in k[x]$ have no repeated roots, let E/k be a splitting field, and let $G = \mathrm{Gal}(E/k)$ be the Galois group of $f(x)$. If $X = \{\alpha_1, \ldots, \alpha_n\}$ is the set of all the roots of $f(x)$, then X is a G-set (Theorem 3.3) that is transitive if and only if $f(x)$ is irreducible (Proposition 3.14). Now $f(x)$ factors in $k(\alpha_1)[x]$:

$$f(x) = (x - \alpha_1) f_1(x).$$

The reader may show that $G_1 = \mathrm{Gal}(E/k(\alpha_1)) \subseteq G$ is the stabilizer G_{α_1} and that $X - \{\alpha_1\}$ is a G_1-set. Thus, Proposition 7.105 shows that X is a doubly transitive G-set if and only if both $f(x)$ and $f_1(x)$ are irreducible (over $k[x]$ and $k(\alpha_1)[x]$, respectively). ◀

Recall Example 1.100: if H is a (not necessarily normal) subgroup of a group G and $X = G/H$ is the family of all left cosets of H in G, then G acts on G/H by $g\colon aH \mapsto gaH$. The G-set X is transitive, and the stabilizer of $aH \in G/H$ is aHa^{-1}; that is, $gaH = aH$ if and only if $a^{-1}ga \in H$ if and only if $g \in aHa^{-1}$.

Proposition 7.107. *If X is a doubly transitive G-set, then*

$$|G| = n(n-1)|G_{x,y}|,$$

where $n = |X|$ and $G_{x,y} = \{g \in G : gx = x \text{ and } gy = y\}$. Moreover, if X is a faithful G-set, then $|G_{x,y}|$ is a divisor of $(n-2)!$.

Proof. First, Theorem 1.107 gives $|G| = n|G_x|$, because X is a transitive G-set. Now $X - \{x\}$ is a transitive G_x-set, by Proposition 7.105, and so

$$|G_x| = |X - \{x\}||(G_x)_y| = (n-1)|G_{x,y}|,$$

because $(G_x)_y = G_{x,y}$. The last remark follows, in this case, from $G_{x,y}$ being a subgroup of $S_{X-\{x,y\}} \cong S_{n-2}$. •

It is now easy to give examples of groups that are not doubly transitive, for the orders of doubly transitive groups are constrained.

Definition. A transitive G-set X is called ***regular*** if only the identity element of G fixes any element of X; that is, $G_x = \{1\}$ for all $x \in X$.

For example, Cayley's Theorem shows that every group G is isomorphic to a regular subgroup of S_G. The notion of regularity extends to doubly transitive groups.

Definition. A doubly transitive G-set X is ***sharply doubly transitive*** if only the identity of G fixes two elements of X; that is, $G_{x,y} = \{1\}$ for all distinct pairs $x, y \in X$.

Proposition 7.108. *The following conditions are equivalent for a faithful doubly transitive G-set X with $|X| = n$.*

(i) *X is sharply doubly transitive.*

(ii) *If (x_1, x_2) and (y_1, y_2) are 2-tuples in $X \times X$ with $x_1 \neq x_2$ and $y_1 \neq y_2$, then there is a unique $g \in G$ with $y_1 = gx_1$ and $y_2 = gy_2$.*

(iii) *$|G| = n(n-1)$.*

(iv) *$G_{x,y} = \{1\}$ for all distinct $x, y \in X$.*

(v) *For every $x \in X$, the G_x-set $X - \{x\}$ is regular.*

Proof. All the implications are routine. •

Example 7.109.

(i) S_3 and A_4 are sharply doubly transitive groups.

(ii) The affine group $\mathrm{Aff}(1, \mathbb{R})$, defined in Exercise 1.53 on page 45, is

$$\mathrm{Aff}(1, \mathbb{R}) = \{f\colon \mathbb{R} \to \mathbb{R} : f(x) = ax + b \text{ with } a \neq 0\}$$

under composition. It is isomorphic to the subgroup of $\mathrm{GL}(2, \mathbb{R})$ consisting of all matrices of the form $\left[\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right]$. It is plain that we can define $\mathrm{Aff}(1, k)$ for any field k in a similar way. In particular, if k is the finite field $\mathbb{F}_q$, then the affine group $\mathrm{Aff}(1, \mathbb{F}_q)$ is finite, and of order $q(q-1)$. The reader may check that $\mathbb{F}_q$ is a sharply doubly transitive $\mathrm{Aff}(1, \mathbb{F}_q)$-set. ◄

Notation. If G is a group, then $G^{\#} = \{g \in G : g \neq 1\}$.

By Cayley's Theorem, every group acts regularly on itself. We now consider transitive groups G such that each $g \in G^{\#}$ has at most one fixed point. In case every $g \in G^{\#}$ has no fixed points, we say that the action of G is ***fixed-point-free***. Thompson proved that if a finite group H has a fixed-point-free automorphism α of prime order (that is, the action of the group $G = \langle \alpha \rangle$ on $H^{\#}$ is fixed-point-free), then H is nilpotent (Robinson, *A Course in the Theory of Groups*, pp. 306–307). Thus, let us consider such actions in which there is some $g \in G^{\#}$ that has a fixed point; that is, the action of G is not regular.

Definition. A finite group G is a ***Frobenius group*** if there exists a transitive G-set X such that

(i) every $g \in G^{\#}$ has at most one fixed point;

(ii) there is some $g \in G^{\#}$ that does have a fixed point.

If $x \in X$, we call G_x a ***Frobenius complement*** of G.

Note that condition (i) implies that the G-set X in the definition is necessarily faithful. Let us rephrase the two conditions: (i) if every $g \in G^{\#}$ has at most one fixed point, then $G_{x,y} = \{1\}$; (ii) if there is some $g \in G^{\#}$ that does have a fixed point, then $G_x \neq \{1\}$.

Example 7.110.

(i) The symmetric group S_3 is a Frobenius group: $X = \{1, 2, 3\}$ is a faithful transitive S_3-set; no $\alpha \in (S_3)^{\#}$ fixes two elements; each transposition $(i\ j)$ fixes one element. The cyclic subgroups $\langle (i\ j) \rangle$ are Frobenius complements (so Frobenius complements need not be unique). A permutation $\beta \in S_3$ has no fixed points if and only if β is a 3-cycle. We are going to prove, in every Frobenius group, that 1 together with all those elements having no fixed points comprise a normal subgroup.

(ii) The example of S_3 in part (i) can be generalized. Let X be a G-set, with at least three elements, which is a sharply doubly transitive G-set. Then X is transitive, $G_{x,y} = \{1\}$, and $G_x \neq \{1\}$ (for if $x, y, z \in X$ are distinct, there exists $g \in G$ with $x = gx$ and $z = gy$). Therefore, every sharply doubly transitive group G is a Frobenius group. ◀

Proposition 7.111. *A finite group G is a Frobenius group if and only if it contains a proper nontrivial subgroup H such that $H \cap gHg^{-1} = \{1\}$ for all $g \notin H$.*

Proof. Let X be a G-set as in the definition of Frobenius group. Choose $x \in X$, and define $H = G_x$. Now H is a proper subgroup of G, for transitivity does not permit $gx = x$ for all $g \in G$. To see that H is nontrivial, choose $g \in G^{\#}$ having a fixed point; say, $gy = y$. If $y = x$, then $g \in G_x = H$. If $y \neq x$, then transitivity provides $h \in G$ with $hy = x$, and Exercise 1.109 on page 76 gives $H = G_x = hG_yh^{-1} \neq \{1\}$. If $g \notin H$, then $gx \neq x$. Now $g(G_x)g^{-1} = G_{gx}$. Hence, if $h \in H \cap gHg^{-1} = G_x \cap G_{gx}$, then h fixes x and gx; that is, $h \in G_{x,y} = \{1\}$.

For the converse, we take X to be the G-set G/H of all left cosets of H in G, where $g\colon aH \mapsto gaH$ for all $g \in G$. We remarked earlier that X is a transitive G-set and that the stabilizer of $aH \in G/H$ is the subgroup aHa^{-1} of G. Since $H \neq \{1\}$, we see that $G_{aH} \neq \{1\}$. Finally, if $aH \neq bH$, then

$$G_{aH,bH} = G_{aH} \cap G_{bH} = aHa^{-1} \cap bHb^{-1} = a\big(H \cap a^{-1}bHb^{-1}a\big)a^{-1} = \{1\},$$

because $a^{-1}b \notin H$. Therefore, G is a Frobenius group. •

The significance of this last proposition is that it translates the definition of Frobenius group from the language of G-sets into the language of abstract groups.

Definition. Let X be a G-set. The ***Frobenius kernel*** of G is the subset

$$N = \{1\} \cup \{g \in G : g \text{ has no fixed points}\}.$$

When X is transitive, we can describe N in terms of a stabilizer G_x. If $a \notin N^{\#}$, then there is some $y \in X$ with $ay = y$. Since G acts transitively, there is $g \in G$ with $gx = y$, and $a \in G_y = gG_xg^{-1}$. Hence, $a \in \bigcup_{g\in G} gG_xg^{-1}$. For the reverse inclusion, if $a \in \bigcup_{g\in G} gG_xg^{-1}$, then $a \in gG_xg^{-1} = G_{gx}$ for some $g \in G$, and so a has a fixed point; that is, $a \notin N$. We have proved that

$$N = \{1\} \cup \Big(G - \Big(\bigcup_{g\in G} gG_xg^{-1}\Big)\Big).$$

Exercise 1.96 on page 74 shows that if G_x is a proper subgroup of G, then $G \neq \bigcup_{g\in G} gG_xg^{-1}$, and so $N \neq \{1\}$ in this case.

Proposition 7.112. *If G is a Frobenius group with Frobenius complement H and Frobenius kernel N, then $|N| = [G : H]$.*

Proof. By Proposition 7.111, there is a disjoint union

$$G = \{1\} \cup \Big(\bigcup_{g\in G} gH^{\#}g^{-1}\Big) \cup N^{\#}.$$

Note that $N_G(H) = H$: if $g \notin H$, then $H \cap gHg^{-1} = \{1\}$, and so $gHg^{-1} \neq H$. Hence, the number of conjugates of H is $[G : N_G(H)] = [G : H]$ (Proposition 1.110). Therefore, $|\bigcup_{g\in G} gH^{\#}g^{-1}| = [G : H](|H| - 1)$, and so

$$|N| = |N^{\#}| + 1 = |G| - ([G : H](|H| - 1)) = [G : H]. \quad \bullet$$

The Frobenius kernel may not be a subgroup of G. It is very easy to check that if $g \in N$, then $g^{-1} \in N$ and $aga^{-1} \in N$ for every $a \in G$; the difficulty is in proving that N is closed under multiplication. For example, if $V = k^n$ is the vector space of all $n \times 1$ column vectors over a field k, then $V^{\#}$, the set of nonzero vectors in V, is a faithful transitive $\mathrm{GL}(V)$-set. Now $A \in \mathrm{GL}(V)$ has a fixed point if and only if there is some $v \in V^{\#}$ with $Av = v$; that is, A has a fixed point if and only if 1 is an eigenvalue of A. Thus, the Frobenius kernel now consists of the identity matrix together with all linear transformations which do not have 1 as an eigenvalue. Let $|k| \geq 4$, and let α be a nonzero element of k with $\alpha^2 \neq 1$. Then $A = \left[\begin{smallmatrix} \alpha & 0 \\ 0 & \alpha \end{smallmatrix}\right]$ and $B = \left[\begin{smallmatrix} \alpha^{-1} & 0 \\ 0 & \alpha \end{smallmatrix}\right]$ lie in N, but their product $AB = \left[\begin{smallmatrix} 1 & 0 \\ 0 & \alpha^2 \end{smallmatrix}\right]$ does not lie in N. However,

if G is a Frobenius group, then N is a subgroup; the only known proof of this fact uses characters.

We have already remarked that if ψ is a character on a subgroup H of a group G, then the restriction $(\psi\uparrow^G)_H$ need not equal ψ. The next proof shows that irreducible characters of a Frobenius complement do extend to irreducible characters of G.

Lemma 7.113. *Let G be a Frobenius group with Frobenius complement H and Frobenius kernel N. For every irreducible character ψ on H other than the trivial character ψ_1, define the generalized character*

$$\varphi = \psi - d\psi_1,$$

where $d = \psi(1)$. Then $\psi^* = \varphi\uparrow^G + d\chi_1$ is an irreducible character on G, and $\psi^*_H = \psi$; that is, $\psi^*(h) = \psi(h)$ for all $h \in H$.

Proof. Note first that $\varphi(1) = 0$. We claim that the induced generalized character $\varphi\uparrow^G$ satisfies the equation

$$(\varphi\uparrow^G)_H = \varphi.$$

If $t_1 = 1, \ldots, t_n$ is a transversal of H in G, then for $g \in G$, the matrix of $\varphi\uparrow^G(g)$ on page 583 has the blocks $\dot{B}(t_i^{-1}gt_i)$ on its diagonal, where $\dot{B}(t_i^{-1}gt_i) = 0$ if $t_i^{-1}gt_i \notin H$ (this is just the matrix version of Theorem 7.90). If $h \in H$, then $t_i^{-1}ht_i \notin H$ for all $i \neq 1$, and so $\dot{B}(t_i^{-1}ht_i) = 0$. Therefore, there is only one nonzero diagonal block, and

$$\operatorname{tr}(\varphi\uparrow^G(h)) = \operatorname{tr}(B(h));$$

that is,

$$\varphi\uparrow^G(h) = \varphi(h).$$

We have just seen that $\varphi\uparrow^G$ is a generalized character on G such that $(\varphi\uparrow^G)_H = \varphi$. By Frobenius Reciprocity (Theorem 7.94),

$$(\varphi\uparrow^G, \varphi\uparrow^G)_G = (\varphi, (\varphi\uparrow^G)_H)_H = (\varphi, \varphi)_H.$$

But $\varphi = \psi - d\psi_1$, so that orthogonality of ψ and ψ_1 gives

$$(\varphi, \varphi)_H = 1 + d^2.$$

Similarly,

$$(\varphi\uparrow^G, \chi_1)_G = (\varphi, \psi_1)_H = -d,$$

where χ_1 is the trivial character on G. Define

$$\psi^* = \varphi\uparrow^G + d\chi_1.$$

Now ψ^* is a generalized character on G, and

$$(\psi^*, \psi^*)_G = (\varphi\uparrow^G, \varphi\uparrow^G)_G + 2d(\varphi\uparrow^G, \chi_1)_G + d^2 = 1 + d^2 - 2d^2 + d^2 = 1.$$

We have

$$(\psi^*)_H = (\varphi\uparrow^G)_H + d(\chi_1)_H = \varphi + d\psi_1 = (\psi - d\psi_1) + d\psi_1 = \psi.$$

Since $\psi^*(1) = \psi(1) > 0$, Corollary 7.79 says that ψ^* is an irreducible character on G. •

Theorem 7.114 (Frobenius). *Let G be a Frobenius group with Frobenius complement H and Frobenius kernel N. Then N is a normal subgroup of G, $N \cap H = \{1\}$, and $NH = G$.*

Remark. A group G having a subgroup Q and a normal subgroup K such that $K \cap Q = \{1\}$ and $KQ = G$ is called a *semidirect product*. We will discuss such groups in Chapter 9. ◀

Proof. For every irreducible character ψ on H other than the trivial character ψ_1, define the generalized character $\varphi = \psi - d\psi_1$, where $d = \psi(1)$. By Lemma 7.113, $\psi^* = \varphi\uparrow^G + d\chi_1$ is an irreducible character on G. Define

$$N^* = \bigcap_{\psi \neq \psi_1} \ker \psi^*.$$

Of course, N^* is a normal subgroup of G.

By Lemma 7.113, $\psi^*(h) = \psi(h)$ for all $h \in H$; in particular, if $h = 1$, we have

$$\psi^*(1) = \psi(1) = d. \tag{1}$$

If $g \in N^{\#}$, then for all $a \in G$, we have $g \notin aHa^{-1}$ (for g has no fixed points), and so $\dot{\varphi}(aga^{-1}) = 0$. The induced character formula, Theorem 7.90, now gives $\varphi\uparrow^G(g) = 0$. Hence, if $g \in N^{\#}$, then Equation (5) gives

$$\psi^*(g) = \varphi\uparrow^G(g) + d\chi_1(g) = d.$$

We conclude that if $g \in N$, then

$$\psi^*(g) = d = \psi^*(1);$$

that is, $g \in \ker \psi^*$. Therefore,

$$N \subseteq N^*.$$

The reverse inclusion will arise from a counting argument.

Let $h \in H \cap N^*$. Since $h \in H$, Lemma 7.113 gives $\psi^*(h) = \psi(h)$. On the other hand, since $h \in N^*$, we have $\psi^*(h) = \psi^*(1) = d$. Therefore, $\psi(h) = \psi^*(h) = d = \psi(1)$, so that $h \in \ker \psi$ for every irreducible character ψ on H. Consider the regular character, afforded by the regular representation ρ on H: $\chi_\rho = \sum_i n_i\psi_i$. Now $\chi_\rho(h) = \sum_i n_i\psi_i(h) \neq 0$, so that Example 7.74(ii) gives $h = 1$. Thus,

$$H \cap N^* = \{1\}.$$

Next, $|G| = |H|[G : H] = |H||N|$, by Proposition 7.112. Note that HN^* is a subgroup of G, because $N^* \lhd G$. Now $|HN^*||H \cap N^*| = |H||N^*|$, by the Second Isomorphism Theorem; since $H \cap N^* = \{1\}$, we have $|H||N| = |G| \geq |HN^*| = |H||N^*|$. Hence, $|N| \geq |N^*|$. But $|N| \leq |N^*|$, because $N \subseteq N^*$, and so $N = N^*$. Therefore, $N \lhd G$, $H \cap N = \{1\}$, and $HN = G$. •

Much more can be said about the structure of Frobenius groups. Every Sylow subgroup of a Frobenius complement is either cyclic or generalized quaternion (Huppert, *Endliche Gruppen* I, p. 502), and it is a consequence of Thompson's Theorem on fixed-point-free automorphisms that every Frobenius kernel is nilpotent (Robinson, *A Course in the Theory of Groups*, p. 306); that is, N is the direct

product of its Sylow subgroups. The reader is referred to Curtis–Reiner, *Representation Theory of Finite Groups and Associative Algebras*, pp. 242–246, or Feit, *Characters of Finite Groups*, pp. 133–139.

Exercises

7.42. Prove that the affine group $\mathrm{Aff}(1, \mathbb{F}_q)$ is sharply doubly transitive.

7.43. Assume that the family of left cosets G/H of a subgroup $H \subseteq G$ is a G-set via the representation on cosets. Prove that G/H is a faithful G-set if and only if $\bigcap_{a\in G} aHa^{-1} = \{1\}$. Give an example in which G/H is not a faithful G-set.

7.44. Prove that every Sylow subgroup of $\mathrm{SL}(2, \mathbb{F}_5)$ is either cyclic or quaternion.

7.45. A subset A of a group G is a **T.I. set** (***trivial intersection set***) if $A \subseteq N_G(A)$ and $A \cap gAg^{-1} \subseteq \{1\}$ for all $g \notin N_G(A)$.

(i) Prove that a Frobenius complement H in a Frobenius group G is a T.I. set.

(ii) Let A be a T.I. set in a finite group G, and let $N = N_G(A)$. If α is a class function vanishing on $N - A$ and β is a class function on N vanishing on $\big(\bigcup_{g\in G}(A^g \cap N)\big) - A$, prove, for all $g \in N^{\#}$, that $\alpha\!\uparrow^G(g) = \alpha(g)$ and $\beta\!\uparrow^G(g) = \beta(g)$.
Hint. See the proofs of Lemma 7.114 and Theorem 7.113.

(iii) If $\alpha(1) = 0$, prove that $(\alpha, \beta)_N = (\alpha\!\uparrow^G, \beta\!\uparrow^G)_G$.

(iv) Let H be a *self-normalizing* subgroup of a finite group G; that is, $H = N_G(H)$. If H is a T.I. set, prove that there is a normal subgroup K of G with $K \cap H = \{1\}$ and $KH = G$.
Hint. See Feit, *Characters of Finite Groups*, p. 124.

∗ **7.46.** Prove that there are no nonabelian simple groups of order n, where $60 < n \leq 100$.

Hint. By Burnside's Theorem, the only candidates for n in the given range are 66, 70, 78, 84, and 90; note that 90 was eliminated in Exercise 4.32 on page 251.

7.47. Prove that there are no nonabelian simple groups of order n, where $101 \leq n < 168$. We remark that $\mathrm{PSL}(2, \mathbb{F}_7)$ is a simple group of order 168, and it is the unique such group up to isomorphism. In view of Proposition 4.44, Corollary 4.71, and Exercise 7.46, we see that A_5 is the only nonabelian simple group of order strictly less than 168.

Hint. By Burnside's Theorem, the only candidates for n in the given range are 102, 105, 110, 120, 126, 130, 132, 138, 140, 150, 154,154, 156, and 165. Use Exercise 1.108 on page 76 and Exercise 4.33 on page 252.

Section 7.7. Division Algebras

When applying the Wedderburn–Artin Theorems to group algebras kG, where k is algebraically closed, we used Molien's Theorem (Corollary 7.53) to assume that the matrix rings have entries in k. If k is not algebraically closed, then (noncommutative) division rings can occur. At the moment, the only example we know of such a ring is the quaternions $\mathbb{H}$, and it is not at all obvious how to construct other examples.

Linear representations of a finite group over a field k are the simplest ones, for every finite subgroup of the multiplicative group $k^\times$ is cyclic (Theorem 2.46). Herstein proved that every finite subgroup of $D^\times$ is cyclic if D is a division ring whose center is a field of characteristic $p > 0$, but it is false when $Z(D)$ has characteristic 0 (obviously, the group of quaternions is a subgroup of $\mathbb{H}^\times$). All finite subgroups of multiplicative groups of division rings were found by Amitsur, Finite subgroups of division rings, *Trans. Amer. Math. Soc.* 80 (1955), 361–386.

That the tensor product of algebras is, again, an algebra, is used in the study of division rings.

Definition. A ***division algebra over a field*** k is a division ring regarded as an algebra over its center k.

Let us begin by considering the wider class of simple algebras.

Definition. A finite-dimensional[10] k-algebra A over a field k is ***central simple*** if it is simple (no two-sided ideals other than A and $\{0\}$) and its center $Z(A) = k$.

Notation. If A is an algebra over a field k, then we write

$$[A : k] = \dim_k(A).$$

Example 7.115.

(i) Every division algebra Δ that is finite-dimensional over its center k is a central simple k-algebra. The ring $\mathbb{H}$ of quaternions is a central simple $\mathbb{R}$-algebra, and every field is a central simple algebra over itself.

(ii) If k is a field, then $\mathrm{Mat}_n(k)$ is a central simple k-algebra (it is simple, by Proposition 7.39, and its center consists of all scalar matrices $\{aI : a \in k\}$, by Exercise 6.9 on page 415).

(iii) If A is a central simple k-algebra, then its opposite algebra A^{op} is also a central simple k-algebra. ◀

Theorem 7.116. *Let A be a central simple k-algebra. If B is a simple k-algebra, then $A \otimes_k B$ is a central simple $Z(B)$-algebra. In particular, if B is a central simple k-algebra, then $A \otimes_k B$ is a central simple k-algebra.*

Proof. Each $x \in A \otimes_k B$ has an expression of the form

$$x = a_1 \otimes b_1 + \cdots + a_n \otimes b_n, \tag{1}$$

where $a_i \in A$ and $b_i \in B$. For nonzero x, define the *length* of x to be n if there is no such expression having fewer than n terms. We claim that if x has length n, that is, if Equation (1) is a shortest such expression, then $b_1, \ldots, b_n$ is a linearly independent list in B (viewed as a vector space over k). Otherwise, there is some j and $u_i \in k$, not all zero, with $b_j = \sum_i u_i b_i$. Substituting and collecting terms gives

$$x = \sum_{i \neq j} (a_i + u_i a_j) \otimes b_i,$$

which is a shorter expression for x.

[10] We assume that central simple algebras are finite-dimensional, but some authors do not. Hilbert gave an example of an infinite-dimensional division algebra (Drozd–Kirichenko, *Finite-Dimensional Algebras*, p. 81).

Let $I \neq (0)$ be a two-sided ideal in $A \otimes_k B$. Choose x to be a (nonzero) element in I of smallest length, and assume that Equation (1) is a shortest expression for x. Now $a_1 \neq 0$. Since Aa_1A is a two-sided ideal in A, simplicity gives $A = Aa_1A$. Hence, there are elements a'_p and a''_p in A with $1 = \sum_p a'_p a_1 a''_p$. Since I is a two-sided ideal,

$$x' = \sum_p a'_p x a''_p = 1 \otimes b_1 + c_2 \otimes b_2 + \cdots + c_n \otimes b_n \tag{2}$$

lies in I, where, for $i \geq 2$, we have $c_i = \sum_p a'_p a_i a''_p$. At this stage, we do not know whether $x' \neq 0$, but we do know, for every $a \in A$, that $(a \otimes 1)x' - x'(a \otimes 1) \in I$. Now

$$(a \otimes 1)x' - x'(a \otimes 1) = \sum_{i \geq 2} (ac_i - c_i a) \otimes b_i. \tag{3}$$

First, this element is 0, lest it be an element in I of length smaller than the length of x. Since $b_1, \ldots, b_n$ is a linearly independent list, the k-subspace it generates is $\langle b_1, \ldots, b_n \rangle = \langle b_1 \rangle \oplus \cdots \oplus \langle b_n \rangle$, and so

$$A \otimes_k \langle b_1, \ldots, b_n \rangle = A \otimes_k \langle b_1 \rangle \oplus \cdots \oplus A \otimes_k \langle b_n \rangle.$$

It follows from Equation (3) that each term $(ac_i - c_i a) \otimes b_i$ must be 0. Hence, $ac_i = c_i a$ for all $a \in A$; that is, each $c_i \in Z(A) = k$. Equation (2) becomes

$$\begin{aligned} x' &= 1 \otimes b_1 + c_2 \otimes b_2 + \cdots + c_n \otimes b_n \\ &= 1 \otimes b_1 + 1 \otimes c_2 b_2 + \cdots + 1 \otimes c_n b_n \\ &= 1 \otimes (b_1 + c_2 b_2 + \cdots + c_n b_n). \end{aligned}$$

Now $b_1 + c_2 b_2 + \cdots + c_n b_n \neq 0$, because $b_1, \ldots, b_n$ is a linearly independent list, and so $x' \neq 0$. Therefore, I contains a nonzero element of the form $1 \otimes b$. But simplicity of B gives $BbB = B$, and so there are $b'_q, b''_q \in B$ with $\sum_q b'_q b b''_q = 1$. Hence, I contains $\sum_q (1 \otimes b'_q)(1 \otimes b)(1 \otimes b''_q) = 1 \otimes 1$, which is the unit in $A \otimes_k B$. Therefore, $I = A \otimes_k B$ and $A \otimes_k B$ is simple.

We now seek the center of $A \otimes_k B$. Clearly, $k \otimes_k Z(B) \subseteq Z(A \otimes_k B)$. For the reverse inequality, let $z \in Z(A \otimes_k B)$ be nonzero, and let

$$z = a_1 \otimes b_1 + \cdots + a_n \otimes b_n$$

be a shortest such expression for z. As in the preceding argument, $b_1, \ldots, b_n$ is a linearly independent list over k. For each $a \in A$, we have

$$0 = (a \otimes 1)z - z(a \otimes 1) = \sum_i (aa_i - a_i a) \otimes b_i.$$

It follows, as above, that $(aa_i - a_i a) \otimes b_i = 0$ for each i. Hence, $aa_i - a_i a = 0$, so that $aa_i = a_i a$ for all $a \in A$ and each $a_i \in Z(A) = k$. Thus, $z = 1 \otimes x$, where $x = a_1 b_1 + \cdots + a_n b_n \in B$. But if $b \in B$, then

$$0 = z(1 \otimes b) - (1 \otimes b)z = (1 \otimes x)(1 \otimes b) - (1 \otimes b)(1 \otimes x) = 1 \otimes (xb - bx).$$

Therefore, $xb - bx = 0$ and $x \in Z(B)$. We conclude that $z \in k \otimes_k Z(B)$. •

It is not generally true that the tensor product of simple k-algebras is again simple; we must pay attention to the centers. In Exercise 7.52 on page 612, we saw that if E/k is a field extension, then $E \otimes_k E$ need not be a field. The tensor product of division algebras need not be a division algebra, as we see in the next example.

Example 7.117. The algebra $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H}$ is an eight-dimensional $\mathbb{R}$-algebra, but it is also a four-dimensional $\mathbb{C}$-algebra: a basis is

$$1 = 1 \otimes 1,\ 1 \otimes i,\ 1 \otimes j,\ 1 \otimes k.$$

We let the reader prove that the vector space isomorphism $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H} \to \mathrm{Mat}_2(\mathbb{C})$ with

$$1 \otimes 1 \mapsto \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad 1 \otimes i \mapsto \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \quad 1 \otimes j \mapsto \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad 1 \otimes k \mapsto \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix},$$

is an isomorphism of $\mathbb{C}$-algebras. ◀

Another way to see that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H} \cong \mathrm{Mat}_2(\mathbb{C})$ arises from Example 7.60(ii). We remarked then that

$$\mathbb{R}\mathbf{Q} \cong \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{R} \times \mathbb{H};$$

tensoring by $\mathbb{C}$ gives

$$\mathbb{C}\mathbf{Q} \cong \mathbb{C} \otimes_{\mathbb{R}} \mathbb{R}\mathbf{Q} \cong \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times \mathbb{C} \times (\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H}).$$

It follows from the uniqueness in Wedderburn–Artin Theorem II that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H} \cong \mathrm{Mat}_2(\mathbb{C})$ (we give yet another proof of this in the next theorem).

The next theorem puts the existence of the isomorphism in Example 7.117 into the context of central simple algebras.

Theorem 7.118. *Let k be a field and let A be a central simple k-algebra.*

(i) *If $\overline{k}$ is the algebraic closure of k, then there is an integer n with*

$$\overline{k} \otimes_k A \cong \mathrm{Mat}_n(\overline{k}).$$

In particular, $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H} \cong \mathrm{Mat}_2(\mathbb{C})$.

(ii) *If A is a central simple k-algebra, then there is an integer n with*

$$[A : k] = n^2.$$

Proof.

(i) By Theorem 7.116, $\overline{k} \otimes_k A$ is a simple $\overline{k}$-algebra. Hence, Wedderburn's Theorem (actually, Corollary 7.51) gives $\overline{k} \otimes_k A \cong \mathrm{Mat}_n(D)$ for some $n \geq 1$ and some division ring D. Since D is a finite-dimensional division algebra over $\overline{k}$, the argument in Molien's Corollary 7.53 shows that $D = \overline{k}$. In particular, since $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$, we have $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H} \cong \mathrm{Mat}_n(\mathbb{C})$ for some n; as $\dim_{\mathbb{R}}(\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H}) = 4$, we have $n = 2$.

(ii) We claim that $[A : k] = [\overline{k} \otimes_k A : \overline{k}]$, for if $a_1, \ldots, a_m$ is a basis of A over k, then $1 \otimes a_1, \ldots, 1 \otimes a_m$ is a basis of $\overline{k} \otimes_k A$ over $\overline{k}$ (essentially because tensor product commutes with direct sum). Therefore,

$$[A : k] = [\overline{k} \otimes_k A : \overline{k}] = [\mathrm{Mat}_n(\overline{k}) : \overline{k}] = n^2. \quad \bullet$$

Definition. A ***splitting field*** for a central simple k-algebra A is a field extension E/k for which there exists an integer n such that $E \otimes_k A \cong \mathrm{Mat}_n(E)$.

Theorem 7.118 says that the algebraic closure $\overline{k}$ of a field k is a splitting field for every central simple k-algebra A. We are going to see that there always exists a splitting field that is a finite extension of k, but we first develop some tools in order to prove it.

Definition. If A is a k-algebra and $X \subseteq A$ is a subset, then its ***centralizer***, $C_A(X)$, is defined by

$$C_A(X) = \{a \in A : ax = xa \text{ for every } x \in X\}.$$

It is easy to check that centralizers are always subalgebras.

The key idea in the next proof is that a subalgebra B of A makes A into a (B, A)-bimodule, and that the centralizer of B can be described in terms of an endomorphism ring.

Theorem 7.119 (Double Centralizer). *Let A be a central simple algebra over a field k and let B be a simple subalgebra of A.*

(i) *$C_A(B)$ is a simple k-algebra.*

(ii) *$B \otimes_k A^{\mathrm{op}} \cong \mathrm{Mat}_s(\Delta)$ and $C_A(B) \cong \mathrm{Mat}_r(\Delta)$ for some division algebra Δ, where $r \mid s$.*

(iii) *$[B : k][C_A(B) : k] = [A : k]$.*

(iv) *$C_A(C_A(B)) = B$.*

Proof. Associativity of the multiplication in A shows that A can be viewed as a (B, A)-bimodule. As such, it is a left $(B \otimes_k A^{\mathrm{op}})$-module (Proposition 6.127), where $(b \otimes a)x = bxa$ for all $x \in A$; we denote this module by A^*. But $B \otimes_k A^{\mathrm{op}}$ is a simple k-algebra, by Theorem 7.116, so that Corollary 7.51 gives $B \otimes_k A^{\mathrm{op}} \cong \mathrm{Mat}_s(\Delta)$ for some integer s and some division algebra Δ over k; in fact, $B \otimes_k A^{\mathrm{op}}$ has a unique (to isomorphism) minimal left ideal L, and $\Delta^{\mathrm{op}} \cong \mathrm{End}_{B \otimes_k A^{\mathrm{op}}}(L)$. Therefore, as $(B \otimes_k A^{\mathrm{op}})$-modules, Corollary 7.28 gives $A^* \cong L^r$, the direct sum of r copies of L, and so $\mathrm{End}_{B \otimes_k A^{\mathrm{op}}}(A^*) \cong \mathrm{Mat}_r(\Delta)$.

We claim that

$$C_A(B) \cong \mathrm{End}_{B \otimes_k A^{\mathrm{op}}}(A^*) \cong \mathrm{Mat}_r(\Delta);$$

this will prove (i) and most of (ii). If $\varphi \in \mathrm{End}_{B \otimes_k A^{\mathrm{op}}}(A^*)$, then it is, in particular, an endomorphism of A as a right A-module. Hence, for all $a \in A$, we have

$$\varphi(a) = \varphi(1a) = \varphi(1)a = ua,$$

where $u = \varphi(1)$. In particular, if $b \in B$, then $\varphi(b) = ub$. On the other hand, taking the left action of B into account, we have $\varphi(b) = \varphi(b1) = b\varphi(1) = bu$. Therefore, $ub = bu$ for all $b \in B$, and so $u \in C_A(B)$. Thus, $\varphi \mapsto \varphi(1)$ is a function $\mathrm{End}_{B \otimes_k A^{\mathrm{op}}}(A^*) \to C_A(B)$. It is routine to check that this function is an injective k-algebra map; it is also surjective, for if $u \in C_A(B)$, then the map $A \to A$, defined by $a \mapsto ua$, is a $(B \otimes_k A^{\mathrm{op}})$-map.

We now compute dimensions. Define $d = [\Delta : k]$. Since L is a minimal left ideal in $\mathrm{Mat}_s(\Delta)$, we have $\mathrm{Mat}_s(\Delta) \cong L^s$ [concretely, $L = \mathrm{COL}(1)$, all the first columns of $s \times s$ matrices over Δ]. Therefore, $[\mathrm{Mat}_s(\Delta) : k] = s^2[\Delta : k]$ and $[L^s : k] = s[L : k]$, so that

$$[L : k] = sd.$$

Also,

$$[A : k] = [A^* : k] = [L^r : k] = rsd.$$

It follows that

$$[A : k][B : k] = [B \otimes_k A^{\mathrm{op}} : k] = [\mathrm{Mat}_s(\Delta) : k] = s^2 d.$$

Therefore, $[B : k] = s^2 d/rsd = s/r$, and so $r \mid s$. Hence,

$$[B : k][C_A(B) : k] = [B : k][\mathrm{Mat}_r(\Delta) : k] = \frac{s}{r} \cdot r^2 d = rsd = [A : k],$$

because we have already proved that $C_A(B) \cong \mathrm{Mat}_r(\Delta)$.

Finally, we prove (iv). It is easy to see that $B \subseteq C_A(C_A(B))$: after all, if $b \in B$ and $u \in C_A(B)$, then $bu = ub$, and so b commutes with every such u. But $C_A(B)$ is a simple subalgebra, by (i), and so the equation in (iii) holds if we replace B by $C_A(B)$:

$$[C_A(B) : k][C_A(C_A(B)) : k] = [A : k].$$

We conclude that $[B : k] = [C_A(C_A(B)) : k]$; together with $B \subseteq C_A(C_A(B))$, this equality gives $B = C_A(C_A(B))$. •

Here is a minor variant of the theorem.

Corollary 7.120. *If B is a simple subalgebra of a central simple k-algebra A, where k is a field, then there is a division algebra D with $B^{\mathrm{op}} \otimes_k A \cong \mathrm{Mat}_s(D)$.*

Proof. By Theorem 7.119(ii), we have $B \otimes_k A^{\mathrm{op}} \cong \mathrm{Mat}_s(\Delta)$ for some division algebra Δ. Hence, $(B \otimes_k A^{\mathrm{op}})^{\mathrm{op}} \cong (\mathrm{Mat}_s(\Delta))^{\mathrm{op}}$. But $(\mathrm{Mat}_s(\Delta))^{\mathrm{op}} \cong \mathrm{Mat}_s(\Delta^{\mathrm{op}})$, by Proposition 6.17, while $(B \otimes_k A^{\mathrm{op}})^{\mathrm{op}} \cong B^{\mathrm{op}} \otimes_k A$, by Exercise 7.50 on page 612. Setting $D = \Delta^{\mathrm{op}}$ completes the proof. •

If Δ is a division algebra over a field k and $\delta \in \Delta$, then the subdivision algebra generated by k and δ is a field, because elements in the center k commute with δ. We are interested in maximal subfields of Δ.

Lemma 7.121. *If Δ is a division algebra over a field k, then a subfield E of Δ is a maximal subfield if and only if $C_\Delta(E) = E$.*

Proof. If E is a maximal subfield of Δ, then $E \subseteq C_\Delta(E)$ because E is commutative. For the reverse inclusion, it is easy to see that if $\delta \in C_\Delta(E)$, then the division algebra E' generated by E and δ is a field. Hence, if $\delta \notin E$, then $E \subsetneq E'$, and the maximality of E is contradicted.

Conversely, suppose that E is a subfield with $C_\Delta(E) = E$. If E is not a maximal subfield of Δ, then there exists a subfield E' with $E \subsetneq E'$. Now $E' \subseteq C_\Delta(E)$, so that if there is some $a' \in E'$ with $a' \notin E$, then $E \neq C_\Delta(E)$. Therefore, E is a maximal subfield. •

After proving an elementary lemma about tensor products, we will extend the next result from division algebras to central simple algebras (Theorem 7.131).

Theorem 7.122. *If D is a division algebra over a field k and E is a maximal subfield of D, then E is a splitting field for D; that is, $E \otimes_k D \cong \mathrm{Mat}_s(E)$, where $s = [D : E] = [E : k]$.*

Proof. Let us specialize the algebras in Theorem 7.119. Here, $A = D$, $B = E$, and $C_A(E) = E$, by Lemma 7.121. Now the condition $C_A(B) \cong \mathrm{Mat}_r(\Delta)$ becomes $E \cong \mathrm{Mat}_r(\Delta)$; since E is commutative, $r = 1$ and $\Delta = E$. Thus, Corollary 7.120 says that $E \otimes_k D = E^{\mathrm{op}} \otimes_k D \cong \mathrm{Mat}_s(E)$.

The equality in Theorem 7.119(iii) is now $[D : k] = [E : k][E : k] = [E : k]^2$. But $[E \otimes_k D : k] = [\mathrm{Mat}_s(E) : k] = s^2[E : k]$, so that $s^2 = [D : k] = [E : k]^2$ and $s = [E : k]$. •

Corollary 7.123. *If D is a division algebra over a field k, then all maximal subfields have the same degree over k.*

Remark. It is not true that maximal subfields in arbitrary division algebras are isomorphic; see Exercise 7.62 on page 613. ◀

Proof. For every maximal subfield E, we have $[E : k] = [D : E] = \sqrt{[D : k]}$. •

This corollary can be illustrated by Example 7.117. The quaternions $\mathbb{H}$ is a four-dimensional $\mathbb{R}$-algebra, so that a maximal subfield must have degree 2 over $\mathbb{R}$; this is so, for $\mathbb{C}$ is a maximal subfield.

We now prove a technical theorem that will yield wonderful results. Recall that a *unit* in a noncommutative ring A is an element having a two-sided inverse in A.

Theorem 7.124. *Let k be a field, let B be a simple k-algebra, and let A be a central simple k-algebra. If there are algebra maps $f, g\colon B \to A$, then there exists a unit $u \in A$ with*

$$g(b) = uf(b)u^{-1}$$

for all $b \in B$.

Proof. The map f makes A into a left B-module if we define the action of $b \in B$ on an element $a \in A$ as $f(b)a$. This action makes A into a (B, A)-bimodule, for the associative law in A gives $\big(f(b)x\big)a = f(b)(xa)$ for all $x \in A$. As usual, this (B, A)-bimodule is a left $(B \otimes_k A^{\mathrm{op}})$-module, where $(b \otimes a')a = baa'$ for all $a \in A$; denote it by ${}_fA$. Similarly, g can be used to make A into a left $(B \otimes_k A^{\mathrm{op}})$-module we denote by ${}_gA$. By Theorem 7.116, $B \otimes_k A^{\mathrm{op}}$ is a simple k-algebra. Now

$$[{}_fA : \Delta] = [A : \Delta] = [{}_gA : \Delta],$$

so that ${}_fA \cong {}_gA$ as $(B \otimes_k A^{\mathrm{op}})$-modules, by Corollary 7.51. If $\varphi\colon {}_fA \to {}_gA$ is a $(B \otimes_k A^{\mathrm{op}})$-isomorphism, then

$$\varphi(f(b)aa') = g(b)\varphi(a)a' \tag{4}$$

for all $b \in B$ and $a, a' \in A$. Since φ is an automorphism of A as a right module over itself, $\varphi(a) = \varphi(1a) = ua$, where $u = \varphi(1) \in A$. To see that u is a unit, note that

$\varphi^{-1}(a) = u'a$ for all $a \in A$. Now $a = \varphi\varphi^{-1}(a) = \varphi(u'a) = uu'a$ for all $a \in A$; in particular, when $a = 1$, we have $1 = uu'$. The equation $\varphi^{-1}\varphi = 1_A$ gives $1 = u'u$, as desired. Substituting into Equation (4), we have

$$uf(b)a = \varphi(f(b)a) = g(b)\varphi(a) = g(b)ua$$

for all $a \in A$. In particular, if $a = 1$, then $uf(b) = g(b)u$ and $g(b) = uf(b)u^{-1}$. •

Corollary 7.125 (Skolem–Noether). *Let A be a central simple k-algebra over a field k, and let B and B' be isomorphic simple k-subalgebras of A. If $\psi\colon B \to B'$ is an isomorphism, then there exists a unit $u \in A$ with $\psi(b) = ubu^{-1}$ for all $b \in B$.*

Proof. In the theorem, take $f\colon B \to A$ to be the inclusion, define $B' = \operatorname{im}\psi$, and define $g = i\psi$, where $i\colon B' \to A$ is the inclusion. •

There is an analog of the Skolem–Noether Theorem in Group Theory. A theorem of G. Higman, B. H. Neumann, and H. Neumann says that if B and B' are isomorphic subgroups of a group G, say, $\varphi\colon B \to B'$ is an isomorphism, then there exists a group G^* containing G and an element $u \in G^*$ with $\varphi(b) = ubu^{-1}$ for every $b \in B$. There is a proof in Rotman, *An Introduction to the Theory of Groups*, p. 404.

Corollary 7.126. *Let k be a field. If ψ is an automorphism of $\mathrm{Mat}_n(k)$, then there exists a nonsingular matrix $P \in \mathrm{Mat}_n(k)$ with*

$$\psi(T) = PTP^{-1}$$

for every matrix T in $\mathrm{Mat}_n(k)$.

Proof. The matrix ring $A = \mathrm{Mat}_n(k)$ is a central simple k-algebra. Set $B = B' = A$ in the Skolem–Noether Theorem. •

Here is another proof of Wedderburn's Theorem 7.13 in the present spirit.

Theorem 7.127 (Wedderburn). *Every finite division ring D is a field.*

Proof. (**van der Waerden**) Let $Z = Z(D)$, and let E be a maximal subfield of D. If $d \in D$, then $Z(d)$ is a subfield of D, and hence there is a maximal subfield E_d containing $Z(d)$. By Corollary 7.123, all maximal subfields have the same degree, hence have the same order. By Corollary 2.158, all maximal subfields here are isomorphic (this is not generally true; see Exercise 7.62). For every $d \in D$, the Skolem–Noether Theorem says that there is $x_d \in D$ with $E_d = x_d E x_d^{-1}$. Therefore, $D = \bigcup_x xEx^{-1}$, and so

$$D^\times = \bigcup_x xE^\times x^{-1}.$$

If E is a proper subfield of D, then $E^\times$ is a proper subgroup of $D^\times$, and this equation contradicts Exercise 1.96 on page 74. Therefore, $D = E$ is commutative. •

Theorem 7.128 (Frobenius). *If D is a noncommutative finite-dimensional real division algebra, then $D \cong \mathbb{H}$.*

Proof. If E is a maximal subfield of D, then $[D : E] = [E : \mathbb{R}] \leq 2$. If $[E : \mathbb{R}] = 1$, then $[D : \mathbb{R}] = 1^2 = 1$ and $D = \mathbb{R}$. Hence, $[E : \mathbb{R}] = 2$ and $[D : \mathbb{R}] = 4$. Let us identify E with $\mathbb{C}$ (we know they are isomorphic). Now complex conjugation is an automorphism of E, so that the Skolem–Noether Theorem gives $x \in D$ with $\overline{z} = xzx^{-1}$ for all $z \in E$. In particular, $-i = xix^{-1}$. Hence,

$$x^2ix^{-2} = x(-i)x^{-1} = -xix^{-1} = i,$$

and so x^2 commutes with i. Therefore, $x^2 \in C_D(E) = E$, by Lemma 7.121, and so $x^2 = a + bi$ for $a, b \in \mathbb{R}$. But

$$a + bi = x^2 = xx^2x^{-1} = x(a + bi)x^{-1} = a - bi,$$

so that $b = 0$ and $x^2 \in \mathbb{R}$. If $x^2 > 0$, then there is $t \in \mathbb{R}$ with $x^2 = t^2$. Now $(x + t)(x - t) = 0$ gives $x = \pm t \in \mathbb{R}$, contradicting $-i = xix^{-1}$. Therefore, $x^2 = -r^2$ for some real r. The element j, defined by $j = x/r$, satisfies $j^2 = -1$ and $ji = -ij$. The list $1, i, j, ij$ is linearly independent over $\mathbb{R}$: if $a+bi+cj+dij = 0$, then $(-di-c)j = a+ib \in \mathbb{C}$. Since $j \notin \mathbb{C}$ (lest $x \in \mathbb{C}$), we must have $-di-c = 0 = a+bi$. Hence, $a = b = 0 = c = d$. Since $[D : \mathbb{R}] = 4$, the list $1, i, j, ij$ is a basis of D. It is now routine to see that if we define $k = ij$, then $ki = j = -ik$, $jk = i = -kj$, and $k^2 = -1$, and so $D \cong \mathbb{H}$. •

In 1929, Brauer introduced the Brauer group to study division rings. Since construction of division rings was notoriously difficult, he considered the wider class of central simple algebras. Brauer introduced the following relation on central simple k-algebras.

Definition. Two central simple k-algebras A and B are ***similar***, denoted by

$$A \sim B,$$

if there are integers n and m with $A \otimes_k \mathrm{Mat}_n(k) \cong B \otimes_k \mathrm{Mat}_m(k)$.

If A is a (finite-dimensional) central simple k-algebra, then Corollary 7.48 and Wedderburn–Artin II show that $A \cong \mathrm{Mat}_n(\Delta)$ for a unique k-division algebra Δ. We shall see that $A \sim B$ if and only if they determine the same division algebra.

Lemma 7.129. *Let A be a finite-dimensional algebra over a field k. If S and T are k-subalgebras of A such that*

(i) $st = ts$ *for all* $s \in S$ *and* $t \in T$,

(ii) $A = ST$,

(iii) $[A : k] = [S : k][T : k]$,

then $A \cong S \otimes_k T$.

Proof. There is a k-linear transformation $f\colon S \otimes_k T \to A$ with $s \otimes t \mapsto st$, because $(s, t) \mapsto st$ is a k-bilinear function $S \times T \to A$. Condition (i) implies that f is an algebra map, for

$$f\big((s \otimes t)(s' \otimes t')\big) = f(ss' \otimes tt') = ss'tt' = sts't' = f(s \otimes t)f(s' \otimes t').$$

Since $A = ST$, by condition (ii), the k-linear transformation f is a surjection; since $\dim_k(S \otimes_k T) = \dim_k(A)$, by condition (iii), f is a k-algebra isomorphism. •

Lemma 7.130. *Let k be a field.*

(i) *If A is a k-algebra, then*

$$A \otimes_k \mathrm{Mat}_n(k) \cong \mathrm{Mat}_n(A).$$

(ii) $\mathrm{Mat}_n(k) \otimes_k \mathrm{Mat}_m(k) \cong \mathrm{Mat}_{nm}(k)$.

(iii) *$A \sim B$ is an equivalence relation.*

(iv) *If A is a central simple algebra, then*

$$A \otimes_k A^{\mathrm{op}} \cong \mathrm{Mat}_n(k),$$

where $n = [A : k]$.

Proof.

(i) Define k-subalgebras of $\mathrm{Mat}_n(A)$ by

$$S = \mathrm{Mat}_n(k) \quad \text{and} \quad T = \{aI : a \in A\}.$$

If $s \in S$ and $t \in T$, then $st = ts$ (for the entries of matrices in S commute with elements $a \in A$). Now S contains every matrix unit E_{ij} (whose i, j entry is 1 and whose other entries are 0), so that ST contains all matrices of the form $a_{ij}E_{ij}$ for all i, j, where $a_{ij} \in A$; hence, $ST = \mathrm{Mat}_n(A)$. Finally, $[S : k][T : k] = n^2[A : k] = [\mathrm{Mat}_n(A) : k]$. Therefore, Lemma 7.129 gives the desired isomorphism.

(ii) If V and W are vector spaces over k of dimensions n and m, respectively, it suffices to prove that $\mathrm{End}_k(V) \otimes_k \mathrm{End}_k(W) \cong \mathrm{End}_k(V \otimes_k W)$. Define S to be all $f \otimes 1_W$, where $f \in \mathrm{End}_k(V)$, and define T to be all $1_V \otimes g$, where $g \in \mathrm{End}_k(W)$. It is routine to check that the three conditions in Lemma 7.129 hold.

(iii) Since $k = \mathrm{Mat}_1(k)$, we have $A \cong A \otimes_k k \cong A \otimes_k \mathrm{Mat}_1(k)$, so that $\sim$ is reflexive. Symmetry is obvious; for transitivity, suppose that $A \sim B$ and $B \sim C$; that is,

$$A \otimes_k \mathrm{Mat}_n(k) \cong B \otimes_k \mathrm{Mat}_m(k) \quad \text{and} \quad B \otimes_k \mathrm{Mat}_r(k) \cong C \otimes_k \mathrm{Mat}_s(k).$$

Then $A \otimes_k \mathrm{Mat}_n(k) \otimes_k \mathrm{Mat}_r(k) \cong A \otimes_k \mathrm{Mat}_{nr}(k)$, by part (ii). On the other hand,

$$\begin{aligned} A \otimes_k \mathrm{Mat}_n(k) \otimes_k \mathrm{Mat}_r(k) &\cong B \otimes_k \mathrm{Mat}_m(k) \otimes_k \mathrm{Mat}_r(k) \\ &\cong C \otimes_k \mathrm{Mat}_m(k) \otimes_k \mathrm{Mat}_s(k) \\ &\cong C \otimes_k \mathrm{Mat}_{ms}(k). \end{aligned}$$

Therefore, $A \sim C$, and so $\sim$ is an equivalence relation.

(iv) Define $f\colon A \times A^{\mathrm{op}} \to \mathrm{End}_k(A)$ by $f(a, c) = \lambda_a \circ \rho_c$, where $\lambda_a\colon x \mapsto ax$ and $\rho_c\colon x \mapsto xc$; it is routine to check that λ_a and ρ_c are k-maps (so their composite is also a k-map), and that f is k-biadditive. Hence, there is a k-map $\widehat{f}\colon A \otimes_k A^{\mathrm{op}} \to \mathrm{End}_k(A)$ with $\widehat{f}(a \otimes c) = \lambda_a \circ \rho_c$. Associativity $a(xc) = (ax)c$ in A says that $\lambda_a \circ \rho_c = \rho_c \circ \lambda_a$, from which it easily follows that $\widehat{f}$ is a k-algebra map. As $A \otimes_k A^{\mathrm{op}}$ is a simple k-algebra and $\ker \widehat{f}$ is a proper two-sided ideal, we have $\widehat{f}$ injective. Now $\dim_k(\mathrm{End}_k(A)) = \dim_k(\mathrm{Hom}_k(A, A)) = n^2$,

where $n = [A : k]$. Since $\dim_k(\operatorname{im} \widehat{f}) = \dim_k(A \otimes_k A^{\mathrm{op}}) = n^2$, it follows that $\widehat{f}$ is a k-algebra isomorphism: $A \otimes_k A^{\mathrm{op}} \cong \operatorname{End}_k(A)$. •

We now extend Theorem 7.122 from division algebras to central simple algebras.

Theorem 7.131. *Let A be a central simple k-algebra over a field k, so that $A \cong \operatorname{Mat}_r(\Delta)$, where Δ is a division algebra over k. If E is a maximal subfield of Δ, then E splits A; that is, there is an integer n and an isomorphism*

$$E \otimes_k A \cong \operatorname{Mat}_n(E).$$

More precisely, if $[\Delta : E] = s$, then $n = rs$ and $[A : k] = (rs)^2$.

Proof. By Theorem 7.122, Δ is split by a maximal subfield E (which is, of course, a finite extension of k): $E \otimes_k \Delta \cong \operatorname{Mat}_s(E)$, where $s = [\Delta : E] = [E : k]$. Hence,

$$\begin{aligned} E \otimes_k A &\cong E \otimes_k \operatorname{Mat}_r(\Delta) \cong E \otimes_k (\Delta \otimes_k \operatorname{Mat}_r(k)) \\ &\cong (E \otimes_k \Delta) \otimes_k \operatorname{Mat}_r(k) \cong \operatorname{Mat}_s(E) \otimes_k \operatorname{Mat}_r(k) \cong \operatorname{Mat}_{rs}(E). \end{aligned}$$

Therefore, $A \cong \operatorname{Mat}_r(\Delta)$ gives $[A : k] = r^2[\Delta : k] = r^2 s^2$. •

Definition. If $[A]$ denotes the equivalence class of a central simple k-algebra A under similarity, define the ***Brauer group*** $\operatorname{Br}(k)$ to be the set

$$\operatorname{Br}(k) = \big\{[A] : A \text{ is a central simple } k\text{-algebra}\big\}$$

with binary operation

$$[A][B] = [A \otimes_k B].$$

Theorem 7.132. $\operatorname{Br}(k)$ *is an abelian group for every field k. Moreover, if $A \cong \operatorname{Mat}_n(\Delta)$ for a division algebra Δ, then Δ is a central simple k-algebra and $[A] = [\Delta]$ in* $\operatorname{Br}(k)$.

Proof. We show that the operation is well-defined: if A, A', B, B' are k-algebras with $A \sim A'$ and $B \sim B'$, then $A \otimes_k B \sim A' \otimes_k B'$. The isomorphisms

$$A \otimes_k \operatorname{Mat}_n(k) \cong A' \otimes_k \operatorname{Mat}_m(k) \quad \text{and} \quad B \otimes_k \operatorname{Mat}_r(k) \cong B' \otimes_k \operatorname{Mat}_s(k)$$

give $A \otimes_k B \otimes_k \operatorname{Mat}_n(k) \otimes_k \operatorname{Mat}_r(k) \cong A' \otimes_k B' \otimes_k \operatorname{Mat}_m(k) \otimes_k \operatorname{Mat}_s(k)$ (we are using commutativity and associativity of tensor product), so that Lemma 7.130(ii) gives $A \otimes_k B \otimes_k \operatorname{Mat}_{nr}(k) \cong A' \otimes_k B' \otimes_k \operatorname{Mat}_{ms}(k)$. Therefore, $A \otimes_k B \sim A' \otimes_k B'$.

That $[k]$ is the identity follows from $k \otimes_k A \cong A$, associativity and commutativity follow from associativity and commutativity of tensor product, and Lemma 7.130(iv) shows that $[A]^{-1} = [A^{\mathrm{op}}]$. Therefore, $\operatorname{Br}(k)$ is an abelian group.

If A is a central simple k-algebra, then $A \cong \operatorname{Mat}_r(\Delta)$ for some finite-dimensional division algebra Δ over k. Hence, $k = Z(A) \cong Z(\operatorname{Mat}_r(\Delta)) \cong Z(\Delta)$, by Theorem 7.116. Thus, Δ is a central simple k-algebra, $[\Delta] \in \operatorname{Br}(k)$, and $[\Delta] = [A]$ (because $\Delta \otimes_k \operatorname{Mat}_r(k) \cong \operatorname{Mat}_r(\Delta) \cong A \cong A \otimes_k k \cong A \otimes_k \operatorname{Mat}_1(k)$). •

The next proposition shows the significance of the Brauer group.

Proposition 7.133. *If k is a field, then there is a bijection from $\mathrm{Br}(k)$ to the family $\mathcal{D}$ of all isomorphism classes of finite-dimensional division algebras over k, and so $|\mathrm{Br}(k)| = |\mathcal{D}|$. Therefore, there exists a noncommutative division ring, finite-dimensional over its center k, if and only if $\mathrm{Br}(k) \neq \{0\}$.*

Proof. Define a function $\varphi\colon \mathrm{Br}(k) \to \mathcal{D}$ by setting $\varphi([A])$ to be the isomorphism class of Δ if $A \cong \mathrm{Mat}_n(\Delta)$. Note that Theorem 7.132 shows that $[A] = [\Delta]$ in $\mathrm{Br}(k)$. Let us see that φ is well-defined. If $[\Delta] = [\Delta']$, then $\Delta \sim \Delta'$, so there are integers n and m with $\Delta \otimes_k \mathrm{Mat}_n(k) \cong \Delta' \otimes_k \mathrm{Mat}_m(k)$. Hence, $\mathrm{Mat}_n(\Delta) \cong \mathrm{Mat}_m(\Delta')$. By the uniqueness in the Wedderburn–Artin Theorems, $\Delta \cong \Delta'$ (and $n = m$). Therefore, $\varphi([\Delta]) = \varphi([\Delta'])$.

Clearly, φ is surjective, for if Δ is a finite-dimensional division algebra over k, then the isomorphism class of Δ is equal to $\varphi([\Delta])$. To see that φ is injective, suppose that $\varphi([\Delta]) = \varphi([\Delta'])$. Then, $\Delta \cong \Delta'$, which implies $\Delta \sim \Delta'$. •

Example 7.134.

(i) If k is an algebraically closed field, then $\mathrm{Br}(k) = \{0\}$, by Theorem 7.118.

(ii) If k is a finite field, then Wedderburn's Theorem 7.127 (= Theorem 7.13) shows that $\mathrm{Br}(k) = \{0\}$.

(iii) If $k = \mathbb{R}$, then Frobenius's Theorem 7.128 shows that $\mathrm{Br}(\mathbb{R}) \cong \mathbb{I}_2$.

(iv) It is proved, using Class Field Theory, that $\mathrm{Br}(\mathbb{Q}_p) \cong \mathbb{Q}/\mathbb{Z}$, where $\mathbb{Q}_p$ is the field of p-adic numbers. Moreover, there is an exact sequence

$$0 \to \mathrm{Br}(\mathbb{Q}) \to \mathrm{Br}(\mathbb{R}) \oplus \bigoplus_p \mathrm{Br}(\mathbb{Q}_p) \to \mathbb{Q}/\mathbb{Z} \to 0.$$

In a series of deep papers, $\mathrm{Br}(k)$ was computed for the most interesting fields k arising in Algebraic Number Theory (*local fields*, one of which is $\mathbb{Q}_p$, and *global fields*) by Albert, Brauer, Hasse, and Noether. ◀

Proposition 7.135. *If E/k is a field extension, then there is a homomorphism*

$$f_{E/k}\colon \mathrm{Br}(k) \to \mathrm{Br}(E)$$

given by $[A] \mapsto [E \otimes_k A]$.

Proof. If A and B are central simple k-algebras, then $E \otimes_k A$ and $E \otimes_k B$ are central simple E-algebras, by Theorem 7.116. If $A \sim B$, then $E \otimes_k A \sim E \otimes_k B$ as E-algebras, by Exercise 7.59 on page 613. It follows that the function $f_{E/k}$ is well-defined. Finally, $f_{E/k}$ is a homomorphism, because

$$(E \otimes_k A) \otimes_E (E \otimes_k B) \cong (E \otimes_E E) \otimes_k (A \otimes_k B) \cong E \otimes_k (A \otimes_k B),$$

by Proposition 6.121, associativity of tensor product. •

Definition. If E/k is a field extension, then the ***relative Brauer group***, $\mathrm{Br}(E/k)$, is the kernel of the homomorphism $f_{E/k}\colon \mathrm{Br}(k) \to \mathrm{Br}(E)$:

$$\mathrm{Br}(E/k) = \ker f_{E/k} = \big\{[A] \in \mathrm{Br}(k) : A \text{ is split by } E\big\}.$$

Corollary 7.136. *For every field k, we have*

$$\mathrm{Br}(k) = \bigcup_{E/k \text{ finite Galois}} \mathrm{Br}(E/k).$$

Proof. This follows from Theorem 7.131 after showing that we may assume that E/k is Galois. •

In a word, the Brauer group arose as a way to study division rings. It is an interesting object, but we have not really used it seriously. For example, we have not yet seen any noncommutative division rings other than the real division algebra $\mathbb{H}$ (and its variants for subfields k of $\mathbb{R}$). We will remedy this when we introduce *crossed product algebras* in Chapter 9. For example, we will see, in Corollary 9.143, that there exists a division ring whose center is a field of characteristic $p > 0$. For further developments, we refer the reader to Jacobson, *Finite-Dimensional Division Algebras over Fields*, and Reiner, *Maximal Orders*.

Exercises

7.48. (i) If k is a subfield of a field K, prove that the ring $K \otimes_k k[x]$ is isomorphic to $K[x]$.

(ii) Suppose that k is a field, $p(x) \in k[x]$ is irreducible, and $K = k(\alpha)$, where α is a root of $p(x)$. Prove that, as rings, $K \otimes_k K \cong K[x]/(p(x))$, where $(p(x))$ is the principal ideal in $K[x]$ generated by $p(x)$.

(iii) The polynomial $p(x)$, though irreducible in $k[x]$, may factor in $K[x]$. Give an example showing that the ring $K \otimes_k K$ need not be semisimple.

(iv) Prove that if K/k is a finite separable extension, then $K \otimes_k K$ is semisimple. (The converse is also true.)

7.49. If $A \cong A'$ and $B \cong B'$ are k-algebras, where k is a commutative ring, prove that $A \otimes_k B \cong A' \otimes_k B'$ as k-algebras.

∗ **7.50.** If k is a commutative ring and A and B are k-algebras, prove that

$$(A \otimes_k B)^{\mathrm{op}} \cong A^{\mathrm{op}} \otimes_k B^{\mathrm{op}}.$$

7.51. If R is a commutative k-algebra, where k is a field and G is a group, prove that $R \otimes_k kG \cong RG$.

∗ **7.52.** (i) If k is a subring of a commutative ring R, prove that $R \otimes_k k[x] \cong R[x]$ as R-algebras.

(ii) If $f(x) \in k[x]$ and (f) is the principal ideal in $k[x]$ generated by $f(x)$, prove that $R \otimes_k (f)$ is the principal ideal in $R[x]$ generated by $f(x)$. More precisely, there is a commutative diagram

$$\begin{array}{ccccc} 0 & \longrightarrow & R \otimes_k (f) & \longrightarrow & R \otimes_k k[x] \\ & & \downarrow & & \downarrow \\ 0 & \longrightarrow & (f) & \longrightarrow & R[x] \end{array}$$

(iii) Let k be a field and $E \cong k[x]/(f)$, where $f(x) \in k[x]$ is irreducible. Prove that $E \otimes_k E \cong E[x]/(f)_E$, where $(f)_E$ is the principal ideal in $E[x]$ generated by $f(x)$.

(iv) Give an example of a field extension E/k with $E \otimes_k E$ not a field.
Hint. If $f(x) \in k[x]$ factors into $g(x)h(x)$ in $E[x]$, where $(g, h) = 1$, then the Chinese Remainder Theorem applies.

7.53. Let k be a field and let $f(x) \in k[x]$ be irreducible. If K/k is a field extension, then $f(x) = p_1(x)^{e_1} \cdots p_n(x)^{e_n} \in K[x]$, where the $p_i(x)$ are distinct irreducible polynomials in $K[x]$ and $e_i \geq 1$.

(i) Prove that $f(x)$ is separable if and only if all $e_i = 1$.

(ii) Prove that a finite field extension K/k is separable if and only if $K \otimes_k K$ is a semisimple ring.
Hint. First, observe that K/k is a simple extension, so there is an exact sequence $0 \to (f) \to k[x] \to K \to 0$. Second, use the Chinese Remainder Theorem.

7.54. Prove that $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H} \cong \mathrm{Mat}_4(\mathbb{R})$ as $\mathbb{R}$-algebras.

Hint. Use Corollary 7.48 for the central simple $\mathbb{R}$-algebra $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{H}$.

7.55. We have given one isomorphism $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{H} \cong \mathrm{Mat}_2(\mathbb{C})$ in Example 7.117. Describe all possible isomorphisms between these two algebras.

Hint. Use the Skolem–Noether Theorem.

7.56. Prove that $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} \cong \mathbb{C} \times \mathbb{C}$ as $\mathbb{R}$-algebras.

7.57. (i) Let $\mathbb{C}(x)$ and $\mathbb{C}(y)$ be function fields. Prove that $R = \mathbb{C}(x) \otimes_{\mathbb{C}} \mathbb{C}(y)$ is isomorphic to a subring of $\mathbb{C}(x, y)$. Conclude that R has no zero-divisors.

(ii) Prove that $\mathbb{C}(x) \otimes_{\mathbb{C}} \mathbb{C}(y)$ is not a field.
Hint. Show that R is isomorphic to the subring of $\mathbb{C}(x, y)$ consisting of polynomials of the form $f(x, y)/g(x)h(y)$.

(iii) Use Exercise 7.7 on page 533 to prove that the tensor product of artinian algebras need not be artinian.

∗ **7.58.** Let A be a central simple k-algebra. If A is split by a field E, prove that A is split by any field extension E' of E.

∗ **7.59.** Let E/k be a field extension. If A and B are central simple k-algebras with $A \sim B$, prove that $E \otimes_k A \sim E \otimes_k B$ as central simple E-algebras.

7.60. If D is a finite-dimensional division algebra over $\mathbb{R}$, prove that D is isomorphic to either $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{H}$.

7.61. Prove that $\mathrm{Mat}_2(\mathbb{H}) \cong \mathbb{H} \otimes_{\mathbb{R}} \mathrm{Mat}_2(\mathbb{R})$ as $\mathbb{R}$-algebras.

∗ **7.62.** (i) Let A be a four-dimensional vector space over $\mathbb{Q}$, and let $1, i, j, k$ be a basis. Show that A is a division algebra if we define 1 to be the identity and

$$\begin{aligned} i^2 &= -1, & j^2 &= -2, & k^2 &= -2, \\ ij &= \ k, & jk &= \ 2i, & ki &= \ j, \\ ji &= -k, & kj &= -2i, & ik &= -j. \end{aligned}$$

Prove that A is a division algebra over $\mathbb{Q}$.

(ii) Prove that $\mathbb{Q}(i)$ and $\mathbb{Q}(j)$ are nonisomorphic maximal subfields of A.

7.63. Let D be the $\mathbb{Q}$-subalgebra of $\mathbb{H}$ having basis $1, i, j, k$.

(i) Prove that D is a division algebra over $\mathbb{Q}$.
Hint. Compute the center $Z(D)$.

(ii) For any pair of nonzero rationals p and q, prove that D has a maximal subfield isomorphic to $\mathbb{Q}(\sqrt{-p^2-q^2})$.
Hint. Compute $(pi+qj)^2$.

7.64. (Dickson) If D is a division algebra over a field k, then each $d \in D$ is algebraic over k. Prove that $d, d' \in D$ are conjugate in D if and only if $\operatorname{irr}(d,k) = \operatorname{irr}(d',k)$.

Hint. Use the Skolem–Noether Theorem.

7.65. Prove that if A is a central simple k-algebra with $A \sim \operatorname{Mat}_n(k)$, then $A \cong \operatorname{Mat}_m(k)$ for some integer m.

7.66. Prove that if A is a central simple k-algebra with $[A]$ of finite order m in $\operatorname{Br}(k)$, then there is an integer r with

$$A \otimes_k \cdots \otimes_k A \cong \operatorname{Mat}_r(k)$$

(there are m factors equal to A). In Chapter 9, we shall see that every element in $\operatorname{Br}(k)$ has finite order.

Section 7.8. Abelian Categories

Since representations of a group G are just another way of considering $\mathbb{C}G$-modules, contemplating all the representations of G is the same as contemplating ${}_{\mathbb{C}G}\mathbf{Mod}$. It is natural to ask, more generally, to what extent a category ${}_R\mathbf{Mod}$ determines a ring R. We now prepare the answer to this question; the answer itself is in the next section.

Recall that an object A in a category $\mathcal{C}$ is an *initial object* if there is a unique morphism $A \to X$ for every $X \in \operatorname{obj}(\mathcal{C})$; an object Ω in $\mathcal{C}$ is a *terminal object* if there is a unique morphism $X \to \Omega$ for every $X \in \operatorname{obj}(\mathcal{C})$; and an object is a *zero object* if it is both initial and terminal (Exercise 6.43 on page 435).

Definition. A category $\mathcal{A}$ is ***additive*** if

(i) $\operatorname{Hom}_{\mathcal{A}}(A,B)$ is an (additive) abelian group for every $A, B \in \operatorname{obj}(\mathcal{A})$;

(ii) the distributive laws hold: given morphisms

$$X \xrightarrow{k} A \underset{g}{\overset{f}{\rightrightarrows}} B \xrightarrow{h} Y,$$

where X and $Y \in \operatorname{obj}(\mathcal{A})$, then

$$h(f+g) = hf + hg \quad \text{and} \quad (f+g)k = fk + gk;$$

(iii) $\mathcal{A}$ has a zero object;

(iv) $\mathcal{A}$ has finite products and finite coproducts: for all objects A, B in $\mathcal{A}$, both $A \sqcap B$ and $A \sqcup B$ exist in $\operatorname{obj}(\mathcal{A})$.

Let $\mathcal{A}$ and $\mathcal{C}$ be additive categories. A functor $T\colon \mathcal{A} \to \mathcal{C}$ (of either variance) is ***additive*** if, for all $A, B \in \operatorname{obj}(\mathcal{A})$ and all $f, g \in \operatorname{Hom}_{\mathcal{A}}(A,B)$, we have

$$T(f+g) = Tf + Tg;$$

that is, the function $\mathrm{Hom}_{\mathcal{A}}(A,B) \to \mathrm{Hom}_{\mathcal{C}}(TA,TB)$, given by $f \mapsto Tf$, is a homomorphism of abelian groups.

Example 7.137. It is easy to see that the Hom functors are additive. Let $\mathcal{A}$ be an additive category, let $X \in \mathrm{obj}(\mathcal{A})$, and let $T = \mathrm{Hom}_{\mathcal{A}}(X, \square)\colon \mathcal{A} \to \mathbf{Ab}$. If $h\colon M \to N$, then $Th = h_*\colon \mathrm{Hom}_{\mathcal{A}}(X,M) \to \mathrm{Hom}_{\mathcal{A}}(X,N)$ is given by $h_*\colon f \mapsto h_*(f) = hf$. Hence, if $f, g \in \mathrm{Hom}_{\mathcal{A}}(X,A)$, then

$$T(f+g) = h_*(f+g) = h(f+g) = hf + hg = h_*f + h_*g = Tf + Tg.$$

A similar argument shows that contravariant Hom functors are additive. ◀

Of course, if T is an additive functor, then $T(0) = 0$, where 0 is either a zero object or a zero morphism. Lemma 6.13 shows that ${}_R\mathbf{Mod}$ and $\mathbf{Mod}_R$ are additive categories, while Exercise 7.67 on page 625 shows that neither **Groups** nor **ComRings** is an additive category. We have just seen that if $\mathcal{A}$ is additive, then the Hom functors $\mathcal{A} \to \mathbf{Ab}$ are additive, while Theorem 6.104 shows that the tensor functors ${}_R\mathbf{Mod} \to \mathbf{Ab}$ and $\mathbf{Mod}_R \to \mathbf{Ab}$ are additive.

That finite coproducts and products coincide for modules is a special case of a more general fact: finite products and finite coproducts coincide in all additive categories.

Lemma 7.138. *Let $\mathcal{C}$ be an additive category, and let $M, A, B \in \mathrm{obj}(\mathcal{C})$. Then $M \cong A \sqcap B$ if and only if there are morphisms $i\colon A \to M$, $j\colon B \to M$, $p\colon M \to A$, and $q\colon M \to B$ such that*

$$pi = 1_A, \quad qj = 1_B, \quad pj = 0, \quad qi = 0, \quad \text{and} \quad ip + jq = 1_M.$$

Moreover, $A \sqcap B$ is also a coproduct with injections i and j, and so

$$A \sqcap B \cong A \sqcup B.$$

Proof. The proof of the first statement, left to the reader, is a variation of the proof of Proposition 6.26. The proof of the second statement is a variation of the proof of Proposition 6.42, and it, too, is left to the reader. The last statement holds because two coproducts, here $A \sqcup B$ and $A \sqcap B$, must be isomorphic. •

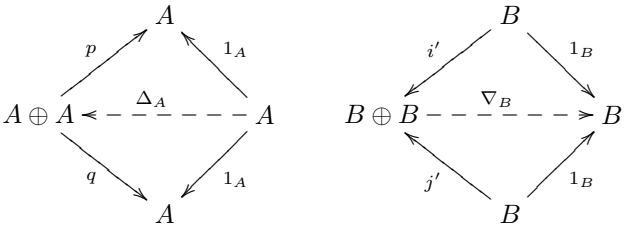
If A and B are objects in an additive category, then $A \sqcap B \cong A \sqcup B$; their common value, denoted by $A \oplus B$, is called their ***direct sum*** (or ***biproduct***).

Addition of homomorphisms in **Ab** can be described without elements. Define the *diagonal* $\Delta\colon A \to A \oplus A$ by $\Delta\colon a \mapsto (a,a)$; dually, the *codiagonal* $\nabla\colon B \oplus B \to B$ is defined by $\nabla\colon (b,b') \mapsto b + b'$. If $f, g\colon A \to B$, we claim that

$$\nabla(f \oplus g)\Delta = f + g.$$

If $a \in A$, then $\nabla(f \oplus g)\Delta\colon a \mapsto (a,a) \mapsto (fa, ga) \mapsto fa + ga = (f+g)(a)$. As usual, the advantage of definitions given in terms of maps (rather than in terms of elements) is that they can be recognized by functors. Diagonals and codiagonals can be defined and exist in additive categories.

Definition. Let $\mathcal{A}$ be an additive category. If $A \in \text{obj}(\mathcal{A})$, then the ***diagonal*** $\Delta_A \colon A \to A \oplus A$ is the unique morphism with $p\Delta_A = 1_A$ and $q\Delta_A = 1_A$, where p, q are projections:



If $B \in \text{obj}(\mathcal{A})$, then the ***codiagonal*** $\nabla_B \colon B \oplus B \to B$ is the unique morphism with $\nabla_B i' = 1_B$ and $\nabla_B j' = 1_B$, where i', j' are injections.

The reader should check that these definitions, when specialized to **Ab**, give our original diagonal and codiagonal homomorphisms.

Lemma 7.139. *If $\mathcal{A}$ is an additive category and $f, g \in \text{Hom}_{\mathcal{A}}(A, B)$, then*

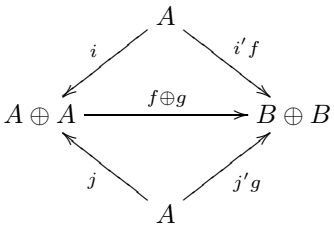
$$\nabla_B(f \oplus g)\Delta_A = f + g.$$

Proof. Let $p, q \colon A \oplus A \to A$ be projections, and let $i, j \colon A \to A \oplus A$ and $i', j' \colon B \to B \oplus B$ be injections. We compute:

$$\begin{aligned}
\nabla_B(f \oplus g)\Delta_A &= \nabla_B(f \oplus g)(ip + jq)\Delta_A \\
&= \nabla_B(f \oplus g)(ip\Delta_A + jq\Delta_A) \\
&= \nabla_B(f \oplus g)(i + j) \quad \text{(because } p\Delta_A = 1_A = q\Delta_A\text{)} \\
&= \nabla_B(f \oplus g)i + \nabla_B(f \oplus g)j \\
&= \nabla_B i' f + \nabla_B j' g \quad \text{(Exercise 6.90 on page 487)} \\
&= f + g. \quad \text{(because } \nabla_B i' = 1_B = \nabla_B j'\text{)} \quad \bullet
\end{aligned}$$

Definition. A functor $T \colon \mathcal{A} \to \mathcal{B}$ between additive categories ***preserves finite direct sums*** if, for all $A, B \in \text{obj}(\mathcal{A})$, whenever $A \oplus B$ is a direct sum with projections p, q and injections i, j, then $TA \oplus TB$ is a direct sum with projections Tp, Tq and injections Ti, Tj.

Recall Exercise 6.90 on page 487: if $i, j \colon A \to A \oplus A$ and $i', j' \colon B \to B \oplus B$ are injections and $f, g \colon A \to B$, then $f \oplus g \colon A \oplus A \to B \oplus B$ is the unique map completing the coproduct diagram



It follows that if T preserves finite direct sums, then $T(f \oplus g) = Tf \oplus Tg$.

Proposition 7.140. *A functor $T\colon \mathcal{A} \to \mathcal{B}$ between additive categories is additive if and only if T preserves finite direct sums.*

Proof. If T is additive, then T preserves finite direct sums, by Lemma 7.138.

Conversely, let T preserve finite direct sums. If $f, g\colon A \to B$, then

$$\begin{aligned} T(f+g) &= T\big(\nabla_B(f \oplus g)\Delta_A\big) && \text{(by Lemma 7.139)} \\ &= (T\nabla_B)T(f \oplus g)(T\Delta_A) \\ &= \nabla_{TB}T(f \oplus g)\Delta_{TA} \\ &= \nabla_{TB}(Tf \oplus Tg)\Delta_{TA} && \text{(Exercise 6.90)} \\ &= Tf + Tg. \quad \bullet \end{aligned}$$

We have been reluctant to discuss injections and surjections in categories; after all, morphisms in a category need not be functions. On the other hand, it is often convenient to have them.

Definition. A morphism $u\colon B \to C$ in a category $\mathcal{C}$ is a ***monomorphism***[11] (or is ***monic***) if u can be canceled from the left; that is, for all objects A and all morphisms $f, g\colon A \to B$, we have $uf = ug$ implies $f = g$.

$$A \underset{g}{\overset{f}{\rightrightarrows}} B \xrightarrow{u} C.$$

It is clear that $u\colon B \to C$ is monic if and only if, for all A, the induced map $u_*\colon \mathrm{Hom}(A, B) \to \mathrm{Hom}(A, C)$ is an injection. In an additive category, $\mathrm{Hom}(A, B)$ is an abelian group, and so u is monic if and only if $ug = 0$ implies $g = 0$. Exercise 7.71 on page 625 shows that monomorphisms and injections coincide in **Sets**, ${}_R\mathbf{Mod}$, and **Groups**. Even in a category whose morphisms are actually functions, however, monomorphisms need not be injections (see Exercise 7.72 on page 625).

Here is the dual definition.

Definition. A morphism $v\colon B \to C$ in a category $\mathcal{C}$ is an ***epimorphism*** (or is ***epic***) if v can be canceled from the right; that is, for all objects D and all morphisms $h, k\colon C \to D$, we have $hv = kv$ implies $h = k$.

$$B \xrightarrow{v} C \underset{k}{\overset{h}{\rightrightarrows}} D.$$

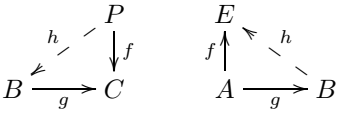
It is clear that $v\colon B \to C$ is epic if and only if, for all D, the induced map $v^*\colon \mathrm{Hom}(C, D) \to \mathrm{Hom}(B, D)$ is an injection. In an additive category, $\mathrm{Hom}(A, B)$ is an abelian group, and so v is monic if and only if $gv = 0$ implies $g = 0$. Exercise 7.71 on page 625 shows that epimorphisms and surjections coincide in **Sets** and in ${}_R\mathbf{Mod}$. Every surjective homomorphism in **Groups** is epic, but we must be clever to show this (Exercise 6.70 on page 460). Even in a category whose morphisms are actually functions, epimorphisms need not be surjections. For example, if R is a domain, then the ring homomorphism $\varphi\colon R \to \mathrm{Frac}(R)$, given by $r \mapsto r/1$, is an epimorphism in **ComRings**. If A is a commutative ring and

[11] A useful notation for a monomorphism $A \to B$ is $A \rightarrowtail B$, while a notation for an epimorphism $B \to C$ is $B \twoheadrightarrow C$.

$h, k\colon \mathrm{Frac}(R) \to A$ are ring homomorphisms agreeing on R, then $h = k$; thus, the inclusion $\mathbb{Z} \to \mathbb{Q}$ is epic.

Projectives and injectives can be defined in any category, but the definitions involve epimorphisms and monomorphisms. Recognizing these morphisms in general categories is too difficult, and so we usually consider projective and injective objects only in additive categories.

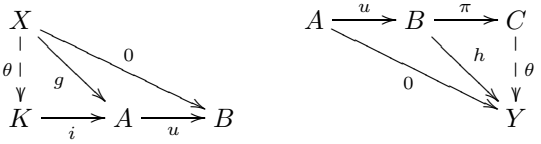
Definition. An object P in an additive category $\mathcal{A}$ is ***projective*** if, for every epic $g\colon B \to C$ and every $f\colon P \to C$, there exists $h\colon P \to B$ with $f = gh$:



An object E in an additve category $\mathcal{A}$ is ***injective*** if, for every monic $g\colon A \to B$ and every $f\colon A \to E$, there exists $h\colon B \to E$ with $f = hg$.

We can describe kernels and cokernels categorically. Recall that we have seen, in Example 6.46, that kernel is a pullback and, in Example 6.49, that cokernel is a pushout. Thus, kernel and cokernel are solutions to universal mapping problems. We promote this fact to a definition.

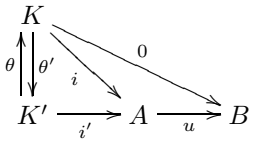
Definition. Let $\mathcal{A}$ be an additive category. If $u\colon A \to B$ and $i\colon K \to A$ in $\mathcal{A}$, then the ***kernel*** of u, denoted by $i = \ker u$, is a solution to the universal mapping problem illustrated in the diagram below on the left: if $ug = 0$, then there exists a unique θ with $i\theta = g$:



Similarly, the ***cokernel*** of u, denoted by $\pi\colon C \to Y$, is a solution to the universal mapping problem illustrated in the above diagram on the right: if $hu = 0$, then there exists a unique θ with $\theta\pi = h$.

Kernels and cokernels are now morphisms; this is not as strange as it first appears, for domains and targets are ingredients of functions and of morphisms (remember that Hom sets in a category are pairwise disjoint, so that each morphism has a unique domain and target).

Let us consider uniqueness of kernels and cokernels. Suppose that i' is another kernel of $u\colon A \to B$; thus, $i'\colon K' \to A$ is another solution to the universal mapping problem:



The maps θ' and θ are inverses, hence are isomorphisms. Thus, the domain of $\ker u$ is unique up to isomorphism.

Let us compare these definitions with the usual notions in **Ab**. If $u\colon A \to B$ is a homomorphism, then $\ker u$ is a subgroup of A and $\operatorname{coker} u = B/\operatorname{im} u$ is a quotient of B. Exercise 6.88 says that the inclusion $i\colon \ker u \to A$ is the kernel in **Ab** and the natural map $\pi\colon B \to B/\operatorname{im} u$ is the cokernel in **Ab**.

Proposition 7.141. *Let $\mathcal{A}$ be an additive category.*

(i) *A morphism u is a monomorphism if and only if $\ker u = 0$, and u is an epimorphism if and only if $\operatorname{coker} u = 0$.*

(ii) *If $i = \ker u$, then i is a monomorphism and $\pi = \operatorname{coker} u$, then π is an epimorphism.*

Proof.

(i) Let u be monic. Since $i = \ker u$, we have $ui = 0$. But $u0 = 0$, so canceling u gives $i = 0$. Conversely, if $i = 0$ and $ug = u0$, then $g = i\theta = i0 = 0$; hence, u is monic. The proof for cokernels is dual.

(ii) Suppose that $X \xrightarrow{g} K \xrightarrow{i} A$ and $ig = 0$. Since $uig = 0$, there is a unique $\theta\colon X \to K$ with $i\theta = ig = 0$. Obviously, $\theta = 0$ satisfies this equation, and so uniqueness gives $g = \theta = 0$; therefore, i is monic. A dual argument shows that cokernels are epimorphisms. •

The converse of Proposition 7.141(ii) is true in *abelian categories*, which are additive categories in which a reasonable notion of exactness can be defined. They are so called because of their resemblance to **Ab**.

Definition. A category $\mathcal{A}$ is an ***abelian category*** if it is an additive category such that

(i) every morphism has a kernel and a cokernel;

(ii) every monomorphism is a kernel and every epimorphism is a cokernel.

In more detail, axiom (i) says that if u is a morphism in $\mathcal{A}$, then $i = \ker u$ and $\pi = \operatorname{coker} u$ exist and lie in $\mathcal{A}$. Axiom (ii) says that if i is monic, then there is a morphism u in $\mathcal{A}$ with $i = \ker u$. Similarly, if π is epic, then there is v in $\mathcal{A}$ with $\pi = \operatorname{coker} v$.

We can define *image* and *exactness* in any abelian category. If $u\colon A \to B$ in **Ab**, we can choose $\operatorname{coker} u$ to be the natural map $\pi\colon B \to B/\operatorname{im} u$; therefore, $\ker \pi = \operatorname{im} u$. Thus, in **Ab**, we have $\ker(\operatorname{coker} u) = \ker \pi = \operatorname{im} u$. This motivates the definition of *image* in abelian categories.

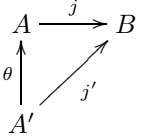
Definition. Let $u\colon A \to B$ be a morphism in an abelian category, and let $\operatorname{coker} u$ be $\pi\colon B \to C$ for some object C. Then its ***image*** is

$$\operatorname{im} u = \ker(\operatorname{coker} u) = \ker \pi.$$

A sequence $A \xrightarrow{u} B \xrightarrow{v} C$ in $\mathcal{A}$ is ***exact*** if there is equality

$$\ker v = \operatorname{im} u.$$

Remark. We have been careless. If B is an object in an additive category $\mathcal{A}$, consider all monomorphisms j with target B. Call two such morphisms $j\colon A \to B$ and $j'\colon A' \to B$ ***equivalent*** if there exists an isomorphism $\theta\colon A' \to A$ with $j' = j\theta$. Define a ***subobject*** of B to be an equivalence class $[j]$ of such monomorphisms:



Our discussion of uniqueness of kernels on page 618 shows that kernels may be viewed as subobjects. The reader can give a dual discussion describing ***quotient objects***.

We need not be so fussy if an abelian category has "honest" subobjects, for we can then choose a "favorite" representative and call it the subobject. For example, if $u\colon B \to C$ in **Ab**, this formal definition says that the kernel of u is an equivalence class of morphisms $i\colon K \to A$. We usually choose K to be the submodule of A and i to be its inclusion. ◀

Remark. Mac Lane (*Categories for the Working Mathematician*, Chapter VIII, Sections 1 and 3) views exactness in another way (which agrees with the definition above). If $u\colon A \to B$ is a morphism in an abelian category, then $u = me$, where $m = \ker(\operatorname{coker} u)$ is monic and $e = \operatorname{coker}(\ker u)$ is epic. Moreover, this factorization is unique in the following sense. If $u = m'e'$, where m' is monic and e' is epic, then there is equivalence of m and m' and of e and e'. In light of this, he defines exactness of a sequence in an abelian category as follows: when $u = me$ and $v = m'e'$ (where m, m' are monic and e, e' are epic), then $A \xrightarrow{u} B \xrightarrow{v} C$ is exact if and only if e and m' are equivalent. ◀

The next two propositions construct new abelian categories from old ones.

Definition. A category $\mathcal{S}$ is a ***subcategory*** of a category $\mathcal{C}$ if

(i) $\operatorname{obj}(\mathcal{S}) \subseteq \operatorname{obj}(\mathcal{C})$;

(ii) $\operatorname{Hom}_{\mathcal{S}}(A, B) \subseteq \operatorname{Hom}_{\mathcal{C}}(A, B)$ for all $A, B \in \operatorname{obj}(\mathcal{S})$;

(iii) if $f \in \operatorname{Hom}_{\mathcal{S}}(A, B)$ and $g \in \operatorname{Hom}_{\mathcal{S}}(B, C)$, the composite $gf \in \operatorname{Hom}_{\mathcal{S}}(A, C)$ is equal to the composite $gf \in \operatorname{Hom}_{\mathcal{C}}(A, C)$;

(iv) if $A \in \operatorname{obj}(\mathcal{S})$, then $1_A \in \operatorname{Hom}_{\mathcal{S}}(A, A)$ is equal to $1_A \in \operatorname{Hom}_{\mathcal{C}}(A, A)$.

A subcategory $\mathcal{S}$ of a category $\mathcal{C}$ is ***full*** if $\operatorname{Hom}_{\mathcal{S}}(A, B) = \operatorname{Hom}_{\mathcal{C}}(A, B)$ for all $A, B \in \operatorname{obj}(\mathcal{S})$.

It is easy to see that the inclusion of a subcategory is a functor. The subcategory **Ab** is a full subcategory of **Groups**, but if we regard **Top** as a subcategory of **Sets**, then it is not a full subcategory, for there are functions between spaces that are not continuous.

Example 7.142.

(i) For every ring R, both ${}_R\mathbf{Mod}$ and $\mathbf{Mod}_R$ are abelian categories. In particular, ${}_{\mathbb{Z}}\mathbf{Mod} = \mathbf{Ab}$ is abelian.

(ii) The full subcategory of $\mathbf{Ab}$ of all finitely generated abelian groups is an abelian category, as is the full subcategory of all torsion abelian groups.

(iii) The full subcategory of $\mathbf{Ab}$ of all torsion-free abelian groups is not an abelian category, for there are morphisms having no cokernel; for example, the inclusion $2\mathbb{Z} \to \mathbb{Z}$ has cokernel $\mathbb{I}_2$ which is not torsion-free.

(iv) The category $\mathbf{Groups}$ is not abelian (it is not even additive). If $S \subseteq G$ is a nonnormal subgroup of a group G, then the inclusion $i\colon S \to G$ has no cokernel. However, if K is a normal subgroup of G with inclusion $j\colon K \to G$, then $\operatorname{coker} j$ does exist. Thus, axiom (ii) in the definition of abelian category essentially says that every subobject in an abelian category is normal. ◀

Remark. Abelian categories are ***self-dual*** in the sense that the dual of every axiom in its definition is itself an axiom; it follows that if $\mathcal{A}$ is an abelian category, then so is its opposite $\mathcal{A}^{\mathrm{op}}$. A theorem using only these axioms in its proof is true in every abelian category; moreover, its dual is also a theorem in every abelian category, and its proof is dual to the original proof. The categories ${}_R\mathbf{Mod}$ and $\mathbf{Mod}_R$ are abelian categories having extra properties; for example, R is a special type of object. Module categories are not self-dual, and this explains why a theorem and its dual, both of which are true in every module category, may have very different proofs. For example, the statements "every module is a quotient of a projective module" and "every module can be imbedded in an injective module" are dual and are always true. The proofs are not dual because these statements are not true in every abelian category. Exercise 7.79 on page 626 shows that the abelian category of all torsion abelian groups has no nonzero projectives, and Exercise 7.80 shows that the abelian category of all finitely generated abelian groups has no nonzero injectives. ◀

Here are more examples of abelian categories.

Proposition 7.143. *Let $\mathcal{S}$ be a full subcategory of an abelian category $\mathcal{A}$. If*

(i) *a zero object in $\mathcal{A}$ lies in $\mathcal{S}$,*

(ii) *for all $A, B \in \operatorname{obj}(\mathcal{S})$, the direct sum $A \oplus B$ in $\mathcal{A}$ lies in $\mathcal{S}$,*

(iii) *for all $A, B \in \operatorname{obj}(\mathcal{S})$ and all $f\colon A \to B$, both $\ker f$ and $\operatorname{coker} f$ lie in $\mathcal{S}$,*

then $\mathcal{S}$ is an abelian category.

Remark. When we say that a morphism $i\colon K \to A$ in $\mathcal{A}$ lies in a subcategory $\mathcal{S}$, we assume that its domain K and target A lie in $\operatorname{obj}(\mathcal{S})$. ◀

Proof. That $\mathcal{S}$ is a full subcategory of $\mathcal{A}$ satisfying (i) and (ii) gives $\mathcal{S}$ additive, by Exercise 7.70 on page 625.

If $f\colon A \to B$ is a morphism in $\mathcal{S} \subseteq \mathcal{A}$, then $\ker f$ and $\operatorname{coker} f$ lie in $\mathcal{A}$, and hence they lie in $\mathcal{S}$, by (iii). Thus, axiom (i) in the definition of abelian category holds; it remains to verify axiom (ii).

Let u be a monomorphism in $\mathcal{S}$; we have just seen that $\ker u$ lies in $\mathcal{S}$. Since u is monic, Proposition 7.141 gives $\ker u = 0$ in $\mathcal{S}$. By hypothesis, $\ker u$ is the same in $\mathcal{A}$ as in $\mathcal{S}$, so that $\ker u = 0$ in $\mathcal{A}$; hence, Proposition 7.141 says that u is a monomorphism in $\mathcal{A}$. As $\mathcal{A}$ is abelian, we have $u = \ker v$ for some $v\colon A \to B$. By hypothesis, $\ker v$ lies in $\mathcal{S}$; that is, $u = \ker v$. The dual argument shows that epimorphisms in $\mathcal{S}$ are cokernels. Therefore, $\mathcal{A}$ is abelian. •

Proposition 7.144. *If $\mathcal{A}$ is an abelian category and $\mathcal{C}$ is a small category, then the functor category $\mathcal{A}^{\mathcal{C}}$ is an abelian category.*

Proof. We assume that $\mathcal{C}$ is small to guarantee that $\mathcal{A}^{\mathcal{C}}$ is a category (Example 6.133). The zero object in $\mathcal{A}^{\mathcal{C}}$ is the constant functor with value 0, where 0 is a zero object in $\mathcal{A}$. If $\tau, \sigma \in \operatorname{Hom}(F, G) = \operatorname{Nat}(F, G)$, where $F, G\colon \mathcal{C} \to \mathcal{A}$ are functors, define $\tau+\sigma\colon F \to G$ by $(\tau+\sigma)_C = \tau_C+\sigma_C\colon FC \to GC$ for all $C \in \operatorname{obj}(\mathcal{C})$. Finally, define $F \oplus G$ by $(F \oplus G)C = FC \oplus GC$. It is straightforward to check that $\mathcal{A}^{\mathcal{C}}$, with these definitions, is an additive category.

If $\tau\colon F \to G$, define $K\colon \mathcal{C} \to \mathcal{A}$ on objects by

$$KC = \ker(\tau_C).$$

In the following commutative diagram with exact rows, where $f\colon C \to C'$ in $\mathcal{C}$, there is a unique $Kf\colon KC \to KC'$ making the augmented diagram commute:

$$\begin{array}{ccccccc} 0 & \longrightarrow & KC & \xrightarrow{\iota_C} & FC & \longrightarrow & GC \\ & & \Big\downarrow{\scriptstyle Kf} & & \Big\downarrow{\scriptstyle Ff} & & \Big\downarrow{\scriptstyle Gf} \\ 0 & \longrightarrow & KC' & \xrightarrow[\iota_{C'}]{} & FC' & \longrightarrow & GC' \end{array}$$

The reader may check that K is a functor, $\iota\colon K \to F$ is a natural transformation, and $\ker \tau = \iota$; dually, cokernels exist in $\mathcal{A}^{\mathcal{C}}$. Verification of the axioms for an abelian category is routine. •

The following construction is of fundamental importance in Algebraic Topology and in Homological Algebra.

Definition. A ***complex***[12] in an abelian category $\mathcal{A}$ is a sequence of objects and morphisms in $\mathcal{A}$ (called ***differentials***),

$$\to A_{n+1} \xrightarrow{d_{n+1}} A_n \xrightarrow{d_n} A_{n-1} \to,$$

such that the composite of adjacent morphisms is 0:

$$d_n d_{n+1} = 0 \qquad \text{for all } n \in \mathbb{Z}.$$

We usually denote this complex by $(\mathbf{C}, d)$ or by $\mathbf{C}$.

If $(\mathbf{C}, d)$ and $(\mathbf{C}', d')$ are complexes, then a ***chain map***

$$f\colon (\mathbf{C}, d) \to (\mathbf{C}', d')$$

[12] These are also called ***chain complexes*** in the literature.

is a sequence of morphisms $(f_n\colon C_n \to C'_n)_{n\in\mathbb{Z}}$ making the following diagram commute:

$$\begin{array}{ccccccccc}
\cdots & \longrightarrow & C_{n+1} & \xrightarrow{d_{n+1}} & C_n & \xrightarrow{d_n} & C_{n-1} & \longrightarrow & \cdots \\
 & & \downarrow{\scriptstyle f_{n+1}} & & \downarrow{\scriptstyle f_n} & & \downarrow{\scriptstyle f_{n-1}} & & \\
\cdots & \longrightarrow & C'_{n+1} & \xrightarrow[d'_{n+1}]{} & C'_n & \xrightarrow[d'_n]{} & C'_{n-1} & \longrightarrow & \cdots
\end{array}$$

In Example 6.133(iii), we viewed a complex as a functor $\mathrm{PO}(\mathbb{Z}) \to \mathcal{A}$ and a chain map as a natural transformation.

Definition. If $\mathcal{A}$ is an abelian category, then $\mathbf{Comp}(\mathcal{A})$, the abelian category of *complexes over* $\mathcal{A}$, is the full subcategory of $\mathcal{A}^{\mathbf{PO}(\mathbb{Z})}$ generated by all complexes. If $\mathcal{A} = \mathbf{Ab}$, then we write $\mathbf{Comp}$ instead of $\mathbf{Comp}(\mathbf{Ab})$.

In Algebraic Topology, the simplicial homology groups $H_n(K)$ of a simplicial complex K, for $n \geq 0$, are constructed in two steps. The first step is geometric, constructing *simplicial chain groups* $C_n(K)$ and boundary maps, giving a sequence

$$\mathbf{S}(K) = \to C_{n+1}(K) \xrightarrow{\partial_{n+1}} C_n(K) \xrightarrow{\partial_n} C_{n-1}(K) \to .$$

The second step is algebraic: define $H_n(K) = \ker \partial_n / \operatorname{im} \partial_{n+1}$; the second step is the basic idea underlying Homological Algebra, as we shall see in Chapter 9.

Theorem 7.145. *If $\mathcal{A}$ is an abelian category, then $\mathbf{Comp}(\mathcal{A})$ is also an abelian category.*

Proof. Since $\mathbf{PO}(\mathbb{Z})$ is a small category, Proposition 7.144 says that the functor category $\mathcal{A}^{\mathbf{PO}(\mathbb{Z})}$ is abelian. Proposition 7.143 now says that the full subcategory $\mathbf{Comp}(\mathcal{A})$ is abelian if it satisfies several conditions.

(i) The *zero complex* is the complex each of whose terms is 0.

(ii) The *direct sum* $(\mathbf{C}, d) \oplus (\mathbf{C}', d')$ is the complex whose nth term is $C_n \oplus C'_n$ and whose nth differential is $d_n \oplus d'_n$.

(iii) If $f = (f_n)\colon (\mathbf{C}, d) \to (\mathbf{C}', d')$ is a chain map, define

$$\mathbf{ker} f = \to \ker f_{n+1} \xrightarrow{\delta_{n+1}} \ker f_n \xrightarrow{\delta_n} \ker f_{n-1} \to,$$

where $\delta_n = d_n | \ker f_n$, and

$$\mathbf{im} f = \to \operatorname{im} f_{n+1} \xrightarrow{\Delta_{n+1}} \operatorname{im} f_n \xrightarrow{\Delta_n} \operatorname{im} f_{n-1} \to,$$

where $\Delta_n = d'_n | \operatorname{im} f_n$.

Since these complexes lie in the full subcategory $\mathbf{Comp}(\mathcal{A})$, Proposition 7.143 applies to prove the theorem. •

We end this section by describing the Full Imbedding Theorem, which says, for all intents and purposes, that working in abelian categories is the same as working in $\mathbf{Ab}$.

Definition. Let $\mathcal{C}, \mathcal{D}$ be categories, and let $F\colon \mathcal{C} \to \mathcal{D}$ be a functor. Then F is ***faithful*** if, for all $A, B \in \mathrm{obj}(\mathcal{C})$, the functions $\mathrm{Hom}_{\mathcal{C}}(A, B) \to \mathrm{Hom}_{\mathcal{D}}(FA, FB)$, given by $f \mapsto Ff$, are injections; F is ***full*** if these functions are surjective.

If $\mathcal{A}$ is an abelian category, then a functor $F\colon \mathcal{A} \to \mathbf{Ab}$ is ***exact*** if $A' \to A \to A''$ exact in $\mathcal{A}$ implies $FA' \to FA \to FA''$ exact in $\mathbf{Ab}$.

Theorem 7.146 (Freyd–Heron–Lubkin).[13] *If $\mathcal{A}$ is a small abelian category, then there is a covariant faithful exact functor $F\colon \mathcal{A} \to \mathbf{Ab}$.*

Proof. See Mitchell, *Theory of Categories*, p. 101. •

This imbedding theorem can be improved so that its image is a *full* subcategory of **Ab**.

Theorem 7.147 (Mitchell). *If $\mathcal{A}$ is a small abelian category, then there is a covariant full faithful exact functor $F\colon \mathcal{A} \to \mathbf{Ab}$.*

Proof. Mitchell, *Theory of Categories*, p. 151. •

In his *Theory of Categories*, Mitchell writes, "Let us say that a statement about a diagram in an abelian category is ***categorical*** if it states that certain parts of the diagram are or are not commutative, that certain sequences in the diagram are or are not exact, and that certain parts of the diagram are or are not (inverse) limits or (direct) limits. Then we have the following metatheorem."

Metatheorem. *Let $\mathcal{A}$ be a (not necessarily small) abelian category.*

(i) *Let Σ be a statement of the form p implies q, where p and q are categorical statements about a diagram in $\mathcal{A}$. If Σ is true in* **Ab***, then Σ is true in $\mathcal{A}$.*

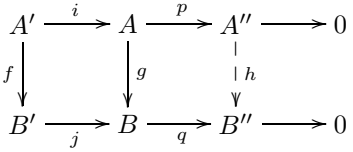
(ii) *Let Σ' be a statement of the form p implies q, where p is a categorical statement concerning a diagram in $\mathcal{A}$, while q states that additional morphisms exist between certain objects in the diagram and that some categorical statement is true of the extended diagram. If the statement can be proved in* **Ab** *by constructing the additional morphisms through diagram chasing, then the statement is true in $\mathcal{A}$.*

Proof. See Mitchell, *Theory of Categories*, p. 97. •

Part (i) follows from the Freyd–Heron–Lubkin Imbedding Theorem. To illustrate, the Five Lemma is true in **Ab**, as is the 3×3 Lemma (Exercise 6.87 on page 486), and so they are true in every abelian category.

[13] I have been unable to find any data about Heron other than that he was a student at Oxford around 1960.

Part (ii) follows from Mitchell's Full Imbedding Theorem. To illustrate, recall Proposition 6.116: given a commutative diagram of abelian groups with exact rows,



there exists a unique map $h\colon A'' \to B''$ making the augmented diagram commute. Suppose now that the diagram lies in an abelian category $\mathcal{A}$. Applying the imbedding functor $F\colon \mathcal{A} \to \mathbf{Ab}$ of the Full Imbedding Theorem, we have a diagram in **Ab** as above, and so there is a homomorphism in **Ab**, say, $h\colon FA'' \to FB''$, making the diagram commute: $F(q)F(g) = hF(p)$. Since F is a full imbedding, there exists $\eta \in \mathrm{Hom}_{\mathcal{A}}(A'', B'')$ with $h = F(\eta)$; hence, $F(qg) = F(q)F(g) = hF(p) = F(\eta)F(p) = F(\eta p)$. But F is faithful, so that $qg = \eta p$.

Exercises

∗ **7.67.** Prove that neither **Groups** nor **ComRings** is an additive category.

Hint. Use Lemma 7.138.

7.68. Let $\mathcal{A}$ be an additive category with zero object 0. If $A \in \mathrm{obj}(\mathcal{A})$, prove that the unique morphism $A \to 0$ and the unique morphism $0 \to A$ are the identity elements of the abelian groups $\mathrm{Hom}_{\mathcal{A}}(A, 0)$ and $\mathrm{Hom}_{\mathcal{A}}(0, A)$.

∗ **7.69.** If $\mathcal{A}$ is an additive category and $A \in \mathrm{obj}(\mathcal{A})$, prove that $\mathrm{End}_{\mathcal{A}}(A) = \mathrm{Hom}_{\mathcal{A}}(A, A)$ is a ring with composition as product.

∗ **7.70.** Let $\mathcal{S}$ be a subcategory of an additive category $\mathcal{A}$. Prove that $\mathcal{S}$ is an additive category if $\mathcal{S}$ is full, $\mathcal{S}$ contains a zero object of $\mathcal{A}$, and $\mathcal{S}$ contains the direct sum $A \oplus B$ (in $\mathcal{A}$) of all $A, B \in \mathrm{obj}(\mathcal{S})$.

∗ **7.71.** (i) Prove that a function is epic in **Sets** if and only if it is surjective, and that a function is monic in **Sets** if and only if it is injective.

(ii) Prove that an R-map is epic in ${}_R\mathbf{Mod}$ if and only if it is surjective, and that an R-map is monic in ${}_R\mathbf{Mod}$ if and only if it is injective.

∗ **7.72.** (i) Let $\mathcal{C}$ be the category of all divisible abelian groups. Prove that the natural map $\mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ is monic in $\mathcal{C}$. Conclude that $\mathcal{C}$ is a category whose morphisms are functions and in which monomorphisms and injections do not coincide.

(ii) Let $\mathbf{Top}_2$ be the category of all Hausdorff spaces. If $D \subsetneq X$ is a dense subspace of a space X, prove that the inclusion $i\colon D \to X$ is an epimorphism. Conclude that $\mathbf{Top}_2$ is a category whose morphisms are functions and in which epimorphisms and surjections do not coincide.
Hint. Two continuous functions agreeing on a dense subspace of a Hausdorff space must be equal.

7.73. Prove, in every abelian category, that the injections of a coproduct are monic and the projections of a product are epic.

∗ **7.74.** (i) Prove that every isomorphism in an additive category is both monic and epic.

(ii) Prove that a morphism in an abelian category is an isomorphism if and only if it is both monic and epic.

(iii) Let R be a domain that is not a field, and let $\varphi\colon R \to \mathrm{Frac}(R)$ be given by $r \mapsto r/1$. In **ComRings**, prove that φ is both monic and epic, but that φ is not an isomorphism.

∗ **7.75.** Let G be a (possibly nonabelian) group. If A and G are groups, prove that a homomorphism $\varphi\colon A \to G$ is surjective if and only if it is an epimorphism in **Groups**.

Hint. Use Exercise 6.70 on page 460.

7.76. State and prove the First Isomorphism Theorem in an abelian category $\mathcal{A}$.

∗ **7.77.** (i) Let $\mathcal{S}$ be a full subcategory of an abelian category $\mathcal{A}$ which satisfies the hypotheses of Proposition 7.143. Prove that if $A \xrightarrow{f} B \xrightarrow{g} C$ is an exact sequence in $\mathcal{S}$, then it is an exact sequence in $\mathcal{A}$.

(ii) If $\mathcal{A}$ is an abelian category and $\mathcal{C}$ is a small category, prove that if $A \xrightarrow{f} B \xrightarrow{g} C$ is an exact sequence in $\mathcal{A}$, then it is an exact sequence in $\mathcal{A}^{\mathcal{C}}$.

7.78. Prove that every object in **Sets** is projective and injective (where we use injections and surjections in the definitions of projective and injective).

∗ **7.79.** Let $\mathcal{T}$ be the category of all torsion abelian groups.

(i) Prove that $\mathcal{T}$ is an abelian category having infinite coproducts.

(ii) Prove that $\mathcal{T}$ has infinite products.
Hint. If $(A_i)_{i\in I}$ is a family of groups in $\mathcal{T}$, prove that $t\big(\prod_{i\in I} A_i\big)$ is a categorical product.

(iii) Prove that $\mathcal{T}$ has enough injectives.

(iv) Prove that $\mathcal{T}$ has no nonzero projective objects. Conclude that $\mathcal{T}$ is not isomorphic to a category of modules.

∗ **7.80.** Prove that $\mathcal{T}'$, the abelian category of all finitely generated abelian groups, is an abelian category that has no nonzero injectives.

7.81. A direct limit $\varinjlim_I F$ or an inverse limit $\varprojlim_I F$ is called ***finite*** if the index set I is finite.

Prove that if $\mathcal{A}$ is an additive category having kernels and cokernels, then $\mathcal{A}$ has all finite inverse limits and direct limits. Conclude that $\mathcal{A}$ has pullbacks and pushouts.

Section 7.9. Module Categories

When is a category isomorphic to a module category $\mathbf{Mod}_R$?

Definition. A functor $F\colon \mathcal{C} \to \mathcal{D}$ is an ***isomorphism*** if there exists a functor $G\colon \mathcal{D} \to \mathcal{C}$ with both composites GF and FG being identity functors.

Every category is isomorphic to itself; Exercise 7.85 on page 634 shows that if R is a ring with opposite ring R^{op}, then $\mathbf{Mod}_R$ is isomorphic to ${}_{R^{\mathrm{op}}}\mathbf{Mod}$.

Empirically, isomorphism of functors turns out to be uninteresting, for it does not arise very often. The following example suggests another reason for modifying this notion of isomorphism. Consider the category $\mathcal{V}$ of all finite-dimensional vector spaces over a field k and its full subcategory $\mathcal{W}$ generated by all vector spaces equal to k^n for $n \in \mathbb{N}$. Since functors take identity morphisms to identity morphisms, an isomorphism $F\colon \mathcal{V} \to \mathcal{W}$ would give a bijection $\operatorname{obj}(\mathcal{V}) \to \operatorname{obj}(\mathcal{W})$. But $\mathcal{W}$ is a small category ($|\operatorname{obj}(\mathcal{W})| = \aleph_0$) while $\mathcal{V}$ is not small, and so these categories are not isomorphic. Carefully distinguishing between two such categories does not seem to be a worthy enterprise.

Here is a weaker but more useful definition.

Definition. A functor $F\colon \mathcal{C} \to \mathcal{D}$ is an ***equivalence*** if there is a functor $G\colon \mathcal{D} \to \mathcal{C}$ such that GF and FG are naturally isomorphic to the identity functors $1_{\mathcal{C}}$ and $1_{\mathcal{D}}$, respectively. When $\mathcal{C}$ and $\mathcal{D}$ are abelian categories, we will further assume that an equivalence $F\colon \mathcal{C} \to \mathcal{D}$ is an additive functor.

It is easy to see that the two nonisomorphic categories $\mathcal{V}$ and $\mathcal{W}$ of finite-dimensional vector spaces are equivalent.

Proposition 7.148. *A functor $F\colon \mathcal{C} \to \mathcal{D}$ is an equivalence if and only if*

(i) *F is full and faithful: the function $\operatorname{Hom}_{\mathcal{C}}(C, C') \to \operatorname{Hom}_{\mathcal{D}}(FC, FC')$, given by $f \mapsto Ff$, is a bijection for all $C, C' \in \operatorname{obj}(\mathcal{C})$;*

(ii) *every $D \in \operatorname{obj}(\mathcal{D})$ is isomorphic to FC for some $C \in \operatorname{obj}(\mathcal{C})$.*

Proof. If F is an equivalence, then there exists a functor $G\colon \mathcal{D} \to \mathcal{C}$ with $GF \cong 1_{\mathcal{C}}$ and $FG \cong 1_{\mathcal{D}}$; let $\tau\colon GF \to 1_{\mathcal{C}}$ and $\sigma\colon FG \to 1_{\mathcal{D}}$ be natural isomorphisms. For each $D \in \operatorname{obj}(\mathcal{D})$, there is an isomorphism $\sigma_D\colon FGD \to D$. Thus, if we define $C = GD$, then $FC \cong D$, which proves (ii).

Given a morphism $f\colon C \to C'$ in $\mathcal{C}$, there is a commutative diagram

$$\begin{array}{ccc} GFC & \xrightarrow{\tau_C} & C \\ {\scriptstyle GFf}\downarrow & & \downarrow{\scriptstyle f} \\ GFC' & \xrightarrow[\tau_{C'}]{} & C' \end{array}$$

Since τ is a natural isomorphism, each τ_C is an isomorphism; hence,

$$f = \tau_{C'}(GFf)\tau_C^{-1}. \tag{1}$$

F is faithful: if $f, f' \in \operatorname{Hom}_{\mathcal{C}}(C, C')$ and $Ff' = Ff$ in $\operatorname{Hom}_{\mathcal{D}}(FC, FC')$, then

$$f' = \tau_{C'}(GFf')\tau_C^{-1} = \tau_{C'}(GFf)\tau_C^{-1} = f.$$

Similarly, $FG \cong 1_{\mathcal{D}}$ implies that G is faithful.

Finally, F is full: if $g\colon FC \to FC'$, define a morphism $f = \tau_{C'}(Gg)\tau_C^{-1}$. Now $f = \tau_{C'}(GFf)\tau_C^{-1}$, by Equation (1), so that $GFf = Gg$. Since G is faithful, we have $Ff = g$.

Conversely, assume that $F\colon \mathcal{C} \to \mathcal{D}$ satisfies (i) and (ii). For each $D \in \operatorname{obj}(\mathcal{D})$, (ii) gives a unique $C = C_D \in \operatorname{obj}(\mathcal{C})$ with $D \cong FC_D$; choose an isomorphism

$h_D\colon D \to FC_D$. Define a functor $G\colon \mathcal{D} \to \mathcal{C}$ on objects by $GD = C_D$. If $g\colon D \to D'$ is a morphism in $\mathcal{D}$, (i) gives a unique morphism $f\colon C_D \to C_{D'}$ with $Ff = h_{D'} g h_D^{-1}$. It is routine to check that G is a functor, $GF \cong 1_{\mathcal{C}}$, and $FG \cong 1_{\mathcal{D}}$. •

Example 7.149.

(i) If R is a ring with opposite ring R^{op}, then $\mathbf{Mod}_R$ is equivalent to ${}_{R^{\mathrm{op}}}\mathbf{Mod}$, for we have already observed that these categories are isomorphic.

(ii) If R is a ring, then $\mathbf{Mod}_R$ and ${}_R\mathbf{Mod}$ need *not* be equivalent (Exercise 7.87 on page 634).

(iii) If $\mathcal{V}$ is the category of all finite-dimensional vector spaces over a field k, then *double dual* $F\colon \mathcal{V} \to \mathcal{V}$, sending $V \mapsto V^{**}$, is an equivalence (V^* is the dual space), for F satisfies the conditions in Proposition 7.148.

(iv) If $\mathcal{C}$ is a category, let $\mathcal{S} \subseteq \mathrm{obj}(\mathcal{C})$ consist of one object from each isomorphism class of objects. The full subcategory generated by $\mathcal{S}$ (also denoted by $\mathcal{S}$) is called a ***skeletal subcategory*** of $\mathcal{C}$. The inclusion functor $\mathcal{S} \to \mathcal{C}$ is an equivalence, by Proposition 7.148; thus, every category $\mathcal{C}$ is equivalent to a skeletal subcategory. For example, if $\mathcal{V}$ is the category of all finite-dimensional vector spaces over a field k, then the full category $\mathcal{W}$ of $\mathcal{V}$ generated by all k^n for $n \in \mathbb{N}$ is a skeletal subcategory. Hence, $\mathcal{V}$ and $\mathcal{W}$ are equivalent. ◀

We rephrase our original question. When is a category equivalent to a module category $\mathbf{Mod}_R$? The answer will place the Wedderburn–Artin Theorems in perspective.

We know that $\mathbf{Mod}_R$, for any ring R, is an abelian category; it also has arbitrary direct sums.

Definition. An abelian category $\mathcal{A}$ is ***cocomplete*** if it contains $\bigoplus_{i\in I} A_i$ for every family $(A_i)_{i\in I}$ of objects, where the index set I may be infinite.

We now describe some categorical properties of the object R in $\mathbf{Mod}_R$.

Definition. An object P in a cocomplete abelian category $\mathcal{A}$ is ***small*** if the covariant Hom functor $\mathrm{Hom}_{\mathcal{A}}(P, \square)\colon \mathcal{A} \to \mathbf{Ab}$ preserves all coproducts; that is, if $(B_i)_{i\in I}$ is an indexed family of objects and $(j_i)_{i\in I}$, $(p_i)_{i\in I}$ are the injections, projections of $\bigoplus_{i\in I} B_i$, then there is an isomorphism $\theta\colon \mathrm{Hom}_{\mathcal{A}}(A, \bigoplus_{i\in I} B_i) \to \bigoplus_{i\in I} \mathrm{Hom}_{\mathcal{A}}(A, B_i)$ whose injections and projections are $(j_i\theta)_{i\in I}$ and $(\theta p_i)_{i\in I}$.

Example 7.150.

(i) Proposition 6.64 shows that the ring R is a small R-module.

(ii) Every finite direct sum of small modules is small, and every direct summand of a small module is small.

(iii) Since a ring R is a small R-module, it follows from (i) and (ii) that every finitely generated projective R-module is small. ◀

The object R in $\mathbf{Mod}_R$ is not only small; it is projective. If P is a small projective object, then $\mathrm{Hom}_{\mathcal{A}}(P, \square)$ is a right exact functor (in fact, it is an exact functor).

Definition. An object P in a cocomplete abelian category $\mathcal{A}$ is a ***generator of*** $\mathcal{A}$ if every $M \in \mathrm{obj}(\mathcal{A})$ is a quotient of a direct sum of copies of P.

It is clear that R is a generator of $\mathbf{Mod}_R$, as is any free right R-module. However, a projective right R-module may not be a generator. For example, if $R = \mathbb{I}_6$, then $R = P \oplus Q$, where $P = \{[0], [2], [4]\} \cong \mathbb{I}_3$, and the (small) projective module P is not a generator (for $Q \cong \mathbb{I}_2$ is not a quotient of a direct sum of copies of P). You will prove, in Exercise 7.86 on page 634, that small projective generators of $\mathbf{Mod}_R$ are finitely generated.

Recall that a functor $F\colon \mathcal{A} \to \mathcal{B}$ is *faithful* if, for all $A, A' \in \mathrm{obj}(\mathcal{A})$, the function $\mathrm{Hom}_{\mathcal{A}}(A, A') \to \mathrm{Hom}_{\mathcal{B}}(FA, FA')$, given by $\varphi \mapsto F\varphi$, is injective.

Proposition 7.151. *A right R-module P is a generator of $\mathbf{Mod}_R$ if and only if $\mathrm{Hom}_R(P, \square)$ is a faithful functor.*

Proof. Assume that $\mathrm{Hom}_R(P, \square)$ is faithful. Given a right R-module A and a map $f\colon P \to A$, let P_f be an isomorphic copy of P, and let $Y = \bigoplus_{f \in \mathrm{Hom}_R(P,A)} P_f$. Define $\varphi\colon Y \to A$ by $(g_f) \mapsto \sum_f f(g_f)$. If φ is not surjective, then the natural map $\nu\colon A \to A/\operatorname{im}\varphi$ is nonzero. Since $\mathrm{Hom}_R(P, \square)$ is faithful, $\nu_*\colon \mathrm{Hom}_R(P, A) \to \mathrm{Hom}_R(P, A/\operatorname{im}\varphi)$ is also nonzero. Thus, there is $f \in \mathrm{Hom}_R(P, A)$ such that $\nu_*(f) = \nu f \neq 0$. But $f(A) \subseteq \operatorname{im}\varphi$ so that $\nu f(A) = \{0\}$; that is, $\nu_* f = \nu f = 0$, a contradiction. Therefore, P is a generator.

Conversely, assume that every module A is a quotient of a direct sum $Y = \bigoplus_{i \in I} P_i$, where $P_i \cong P$ for all i; say, there is a surjective $\varphi\colon Y \to A$. Now $\varphi = \sum_i \varphi\lambda_i$, where $(\lambda_i\colon P_i \to Y)_{i \in I}$ are the injections. If $\alpha\colon A \to A'$ is nonzero, then $\alpha\varphi = \alpha \sum_i \varphi\lambda_i = \sum_i (\alpha\varphi\lambda_i)$. Now $\alpha\varphi \neq 0$, because φ is surjective. Hence, $\alpha\varphi\lambda_i \neq 0$ for some i. But $P_i \cong P$, so that $0 \neq \alpha\varphi\lambda_i = \alpha_*(\varphi\lambda_i)$; that is, $\alpha_* \neq 0$, and so $\mathrm{Hom}_R(P, \square)$ is faithful. •

Here is the characterization of module categories.

Theorem 7.152 (Gabriel–Mitchell). *A category $\mathcal{A}$ is equivalent to a module category $\mathbf{Mod}_R$ if and only if $\mathcal{A}$ is a cocomplete abelian category having a small projective generator*[14] *P. Moreover, $R \cong \mathrm{End}_{\mathcal{A}}(P)$ in this case.*

Proof. The proof of necessity is easy: $\mathbf{Mod}_R$ is a cocomplete abelian category and R is a small projective generator.

For the converse, define $F = \mathrm{Hom}_{\mathcal{A}}(P, \square)\colon \mathcal{A} \to \mathbf{Ab}$. Note that F is additive, by Example 7.137, and that $R = \mathrm{End}_{\mathcal{A}}(P)$ is a ring, by Exercise 7.85 on page 634. For each $A \in \mathrm{obj}(\mathcal{A})$, we claim that FA is a right R-module. If $f \in FA = \mathrm{Hom}_{\mathcal{A}}(P, A)$ and $\varphi\colon P \to P$ lies in $R = \mathrm{End}(P)$, define scalar multiplication $f\varphi$ to be the composite $P \xrightarrow{\varphi} P \xrightarrow{f} A$. It is routine to check that F actually takes values in $\mathbf{Mod}_R$.

Let us prove that F is an equivalence. Now $F = \mathrm{Hom}_{\mathcal{A}}(P, \square)\colon \mathcal{A} \to \mathbf{Mod}_R$ [where $R = \mathrm{End}(P)$] is faithful, by Proposition 7.151. It remains to prove, by Proposition 7.148, that F is full [the maps $\mathrm{Hom}_{\mathcal{A}}(Y, X) \to \mathrm{Hom}_R(FY, FX)$, given

[14] A small projective generator is often called a ***progenerator***.

by $\varphi \mapsto F\varphi$, are all surjective] and that every $M \in \mathrm{obj}(\mathbf{Mod}_R)$ is isomorphic to FA for some $A \in \mathrm{obj}(\mathcal{A})$.

For fixed $Y \in \mathrm{obj}(\mathcal{A})$, define the class

$$\mathcal{E} = \mathcal{E}_Y = \{X \in \mathrm{obj}(\mathcal{A}) : \mathrm{Hom}_{\mathcal{A}}(X, Y) \to \mathrm{Hom}_R(FX, FY) \text{ is surjective}\}.$$

We will prove three properties of $\mathcal{E}$.

(i) $P \in \mathcal{E}$.

(ii) If $(X_i)_{i\in I}$ is a family of objects in $\mathcal{E}$, then $\bigoplus_{i\in I} X_i \in \mathcal{E}$.

(iii) If $X, Z \in \mathcal{E}$ and $f\colon X \to Z$ is any morphism, then $\operatorname{coker} f \in \mathcal{E}$.

These properties imply $\mathcal{E} = \mathrm{obj}(\mathcal{A})$. By (i) and (ii), every direct sum of copies of P lies in $\mathcal{E}$; since P is a generator of $\mathcal{A}$, every $Z \in \mathrm{obj}(\mathcal{A})$ is a cokernel of $\bigoplus_{i\in I} P_i \to \bigoplus_{j\in J} P_j$, where all P_i, P_j are isomorphic to P. Thus, $Z \in \mathcal{E}_Y$, which says that $\mathrm{Hom}_{\mathcal{A}}(Z, Y) \to \mathrm{Hom}_{FP}(FZ, FY)$ is surjective; that is, F is full. We now verify these three properties.

To see that $P \in \mathcal{E}_Y$, we must show that $\mathrm{Hom}_{\mathcal{A}}(P, Y) \to \mathrm{Hom}_R(FP, FY)$ is surjective. Since P is a generator of $\mathcal{A}$, there is an exact sequence

$$\bigoplus_{i\in I} P_i \to \bigoplus_{j\in J} P_j \to Y \to 0 \tag{2}$$

which gives the commutative diagram (details below)

$$\begin{array}{ccccccc}
F(\bigoplus_{i\in I} P_i) & \longrightarrow & F(\bigoplus_{j\in J} P_j) & \longrightarrow & FY & \longrightarrow & 0 \\
\downarrow{\scriptstyle =} & & \downarrow{\scriptstyle =} & & \downarrow{\scriptstyle =} & & \\
\mathrm{Hom}_{\mathcal{A}}(P, \bigoplus_{i\in I} P_i) & \longrightarrow & \mathrm{Hom}_{\mathcal{A}}(P, \bigoplus_{j\in J} P_j) & \longrightarrow & \mathrm{Hom}_{\mathcal{A}}(P, Y) & \longrightarrow & 0 \\
\downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \downarrow{\scriptstyle \gamma} & & \\
\mathrm{Hom}_R(FP, F(\bigoplus_{i\in I} P_i)) & \to & \mathrm{Hom}_R(FP, F(\bigoplus_{j\in J} P_j)) & \to & \mathrm{Hom}_R(FP, FY) & \to & 0 \\
\downarrow & & \downarrow & & \downarrow & & \\
\bigoplus_{i\in I} FP_i & \longrightarrow & \bigoplus_{j\in J} FP_j & \longrightarrow & FY & \longrightarrow & 0
\end{array}$$

Now $F = \mathrm{Hom}_{\mathcal{A}}(P, \square)$ is an exact functor (because P is projective), and so the top two rows arise by applying F to (2); the vertical maps between these rows are identities. The third row arises from applying $\mathrm{Hom}_R(FP, \square)$ to the top row; the vertical maps are the maps $\mathrm{Hom}(X, Y) \to \mathrm{Hom}(FX, FY)$ given by $\varphi \mapsto F\varphi$. The bottom row arises from the third row, for F preserves direct sums (because P is small), and $\mathrm{Hom}_R(FP, FY) = \mathrm{Hom}_R(R, FY) = FY$. Finally, since α and β are surjections, so is γ (use the Five Lemma, by adding $\to 0$ at the ends of the middle two rows).

For (ii), let $(X_i)_{i\in I}$ be a family for which all $\mathrm{Hom}(X_i, Y) \to \mathrm{Hom}(FX_i, FY)$ are surjections. To see that $\mathrm{Hom}(\bigoplus X_i, Y) \to \mathrm{Hom}(F(\bigoplus X_i), FY)$ is surjective, use the facts that $\mathrm{Hom}(\bigoplus X_i, Y) \cong \prod \mathrm{Hom}(X_i, Y)$ and $\mathrm{Hom}(F(\bigoplus X_i), FY) \cong \mathrm{Hom}(\bigoplus FX_i, FY) \cong \prod \mathrm{Hom}(FX_i, FY)$ (because F preserves direct sums).

For (iii), use the Five Lemma on a variant of the commutative diagram above. We conclude that F is full.

Lastly, for every right R-module M, we show that there is $A \in \mathrm{obj}(\mathcal{A})$ with $M \cong FA$. There is an exact sequence $\bigoplus_{i\in I} R_i \xrightarrow{f} \bigoplus_{j\in J} R_j \to M \to 0$ in $\mathbf{Mod}_R$, where R_i, R_j are isomorphic to R. If we view each R_i, R_j as FP_i, FP_j, where all P_i, P_j are isomorphic to P, then

$$\begin{aligned} f \in \mathrm{Hom}(\bigoplus_{i\in I} R_i, \bigoplus_{j\in J} R_j) &= \mathrm{Hom}(\bigoplus_{i\in I} FP_i, \bigoplus_{j\in J} FP_j) \\ &= \mathrm{Hom}(F(\bigoplus_{i\in I} P_i), F(\bigoplus_{j\in J} P_j)). \end{aligned}$$

Since F is full, there is $\varphi \in \mathrm{Hom}(\bigoplus_{i\in I} P_i, \bigoplus_{j\in J} P_j)$ with $F\varphi = f$. Using the Five Lemma again, the reader may show that $M \cong F(\mathrm{coker}\,\varphi)$. •

Corollary 7.153. *If R is a ring and $n \geq 1$, there is an equivalence of categories*

$$\mathbf{Mod}_R \cong \mathbf{Mod}_{\mathrm{Mat}_n(R)}.$$

Proof. For any integer $n \geq 1$, the free module $P = \bigoplus_{i=1}^n R_i$, where $R_i \cong R$, is a small projective generator of $\mathbf{Mod}_R$. Theorem 7.152 gives an equivalence $\mathbf{Mod}_R \cong \mathbf{Mod}_S$, where $S = \mathrm{End}_R(P) \cong \mathrm{Mat}_n(R)$. •

We can now understand Proposition 7.37: $\mathrm{Mat}_n(\Delta)$ is semisimple when Δ is a division ring. By Proposition 7.33, a ring R is semisimple if and only if every R-module is projective; that is, every object in $\mathbf{Mod}_R$ is projective. But every Δ-module is projective (even free), so that equivalence of the categories shows that every object in $\mathbf{Mod}_{\mathrm{Mat}_n(\Delta)}$ is also projective. Therefore, $\mathrm{Mat}_n(\Delta)$ is semisimple. We have just seen why matrix rings arise in the study of semisimple rings.

Given rings R and S, Corollary 7.153 raises the question when $\mathbf{Mod}_R$ and $\mathbf{Mod}_S$ are equivalent. The answer is provided by ***Morita Theory***, which arose by analyzing the proof of Theorem 7.152. We merely report the main results; for details, see Jacobson, *Basic Algebra* II, pp. 177–184, Lam, *Lectures on Modules and Rings*, Chapters 18 and 19, McConnell–Robson, *Noncommutative Noetherian Rings*, Chapter 3, §5, Reiner, *Maximal Orders*, Chapter 4, and Rowen, *Ring Theory* I, Chapter 4.

Definition. Call rings R and S ***Morita equivalent*** if their module categories $\mathbf{Mod}_R$ and $\mathbf{Mod}_S$ are equivalent.

For example, Corollary 7.153 says that every ring R is Morita equivalent to the matrix ring $\mathrm{Mat}_n(R)$, where $n \geq 1$.

Given a ring R, every right R-module P determines a ***Morita context***

$$(P, R, Q, S, \alpha, \beta).$$

Here, $Q = \mathrm{Hom}_R(P, R)$ and $S = \mathrm{End}_R(P)$. Both P and Q turn out to be bimodules: $P = {}_SP_R$ and $Q = {}_RQ_S$, and there is an (R,R)-map $\alpha\colon Q \otimes_S P \to R$ and an (R,R)-map $\beta\colon P \otimes_R Q \to S$. When P_R is a small projective generator, both α and β are isomorphisms; in this case, Q_S is also a small projective generator.

Theorem 7.154 (Morita I). *Let P_R be a small projective generator with Morita context $(P, R, Q, S, \alpha, \beta)$.*

(i) $\mathrm{Hom}_R(P, \square)\colon \mathbf{Mod}_R \to \mathbf{Mod}_S$ *is an equivalence, and its inverse is* $\mathrm{Hom}_S(Q, \square)\colon \mathbf{Mod}_S \to \mathbf{Mod}_R$.

(ii) $\mathrm{Hom}_R(Q, \square)\colon {}_R\mathbf{Mod} \to {}_S\mathbf{Mod}$ *is an equivalence and its inverse is* $\mathrm{Hom}_S(P, \square)\colon {}_S\mathbf{Mod} \to {}_R\mathbf{Mod}$.

Proof. Lam, *Lectures on Modules and Rings*, states and proves this with tensor products, using $\mathrm{Hom}_R(P, \square) \cong \square \otimes_R Q$ and $\mathrm{Hom}_S(Q, \square) \cong \square \otimes_S P$ in part (i) and $\mathrm{Hom}_S(P, \square) \cong Q \otimes_S \square$ and $\mathrm{Hom}_R(Q, \square) \cong P \otimes_R \square$ in part (ii). •

Theorem 7.155 (Morita II). *Let R and S be rings, and let $F\colon \mathbf{Mod}_R \to \mathbf{Mod}_S$ be an equivalence with inverse $G\colon \mathbf{Mod}_S \to \mathbf{Mod}_R$. Then F and G arise as in* Morita I*; that is, $F \cong \mathrm{Hom}_R(P, \square)$ and $G \cong \mathrm{Hom}_S(Q, \square)$, where $P = G(S)$ and $Q = F(R)$.*

Corollary 7.156. $\mathbf{Mod}_R$ *and* $\mathbf{Mod}_S$ *are equivalent if and only if* ${}_R\mathbf{Mod}$ *and* ${}_S\mathbf{Mod}$ *are equivalent.*

Exercise 7.85 on page 634 shows that $\mathbf{Mod}_R$ and ${}_{R^{op}}\mathbf{Mod}$ are equivalent, but Exercise 7.87 shows that $\mathbf{Mod}_R$ and ${}_R\mathbf{Mod}$ may not be equivalent.

Corollary. *Two rings R and S are Morita equivalent if and only if $S \cong \mathrm{End}_R(P)$ for some small projective generator P of* $\mathbf{Mod}_R$.

If $\mathcal{A}$ is a category, then an ***endomorphism*** of the identity functor $1_{\mathcal{A}}$ is a natural transformation $\tau\colon 1_{\mathcal{A}} \to 1_{\mathcal{A}}$; that is, for every pair of objects A and B and every morphism $f\colon A \to B$, there is a commutative diagram

$$\begin{array}{ccc} A & \xrightarrow{\tau_A} & A \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ B & \xrightarrow[\tau_B]{} & B \end{array}$$

Definition. If R is a ring, define

$$\mathrm{End}(\mathbf{Mod}_R) = \{\tau\colon 1_{\mathbf{Mod}_R} \to 1_{\mathbf{Mod}_R} \mid \tau \text{ is an endomorphism}\}.$$

It is easy to see that the pointwise sum of two endomorphisms is another such; that is, define $\tau + \sigma$ as the family $(\tau_A + \sigma_A)_{A \in \mathbf{Mod}_R}$. It should follow that $\mathrm{End}(\mathbf{Mod}_R)$ is a ring with composition as multiplication, but it is not obvious whether $\mathrm{End}(\mathbf{Mod}_R)$ is a set.

Proposition 7.157. *For any ring R, there is a ring isomorphism*

$$Z(R) \cong \mathrm{End}(\mathbf{Mod}_R).$$

Proof. If $c \in Z(R)$ and A is a right R-module, define $\tau_A^c\colon A \to A$ to be multiplication by c:

$$\tau_A^c\colon a \mapsto ac.$$

Since $c \in Z(R)$, the function τ_A^c is an R-map. It is easily checked that $\tau^c = (\tau_A^c)_{A \in \mathbf{Mod}_R}$ is an endomorphism of $1_{\mathbf{Mod}_R}$. Define $\varphi\colon Z(R) \to \mathrm{End}(\mathbf{Mod}_R)$ by

$$\varphi\colon c \mapsto \tau^c = (\tau_A^c)_{A \in \mathbf{Mod}_R}.$$

We claim that φ is a bijection [so that $\mathrm{End}(\mathbf{Mod}_R)$ is a set] and a ring isomorphism. The only point which is not obvious is whether φ is surjective. Let σ be an endomorphism of $1_{\mathcal{A}}$ and let A be a right R-module. If $a \in A$, define $f\colon R \to A$ by $f(1) = a$. There is a commutative diagram

$$\begin{array}{ccc} R & \xrightarrow{\sigma_R} & R \\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f} \\ A & \xrightarrow[\sigma_A]{} & A \end{array}$$

Define $c = \sigma_R(1)$. Now $f\sigma_R(1) = f(c) = f(1 \cdot c) = f(1)c = ac$. On the other hand, $\sigma_A f(1) = \sigma_A(a)$. Commutativity gives $\sigma_A(a) = ac$; that is, $\sigma_A = \tau_A^c$. •

Corollary 7.158. *Let R and S be rings.*

(i) *If R and S are Morita equivalent, then $Z(R) \cong Z(S)$.*

(ii) *If R and S are commutative, then $\mathbf{Mod}_R$ and $\mathbf{Mod}_S$ are equivalent if and only if $R \cong S$.*

Proof.

(i) If $\mathcal{A}$ and $\mathcal{B}$ are equivalent abelian categories, then $\mathrm{End}(1_{\mathcal{A}}) \cong \mathrm{End}(1_{\mathcal{B}})$. If $\mathcal{A} = \mathbf{Mod}_R$ and $\mathcal{B} = \mathbf{Mod}_S$, then $Z(R) \cong Z(S)$, by Proposition 7.157.

(ii) Sufficiency is obvious. For necessity, part (i) gives $Z(R) \cong Z(S)$. Since R and S are commutative, $R = Z(R) \cong Z(S) = S$. •

Exercises

7.82. Let $F\colon \mathcal{C} \to \mathcal{D}$ be an *isomorphism* of categories with inverse $G\colon \mathcal{D} \to \mathcal{C}$; that is, $GF = 1_{\mathcal{C}}$ and $FG = 1_{\mathcal{D}}$. Prove that both (F, G) and (G, F) are adjoint pairs.

7.83. If $F\colon \mathcal{A} \to \mathcal{B}$ is an equivalence of abelian categories, prove the following statements.

(i) If f is monic in $\mathcal{A}$, then Ff is monic in $\mathcal{B}$.

(ii) If f is epic in $\mathcal{A}$, then Ff is epic in $\mathcal{B}$.

(iii) If $A \in \mathrm{obj}(\mathcal{A})$, then $f \mapsto Ff$ is a ring isomorphism $\mathrm{End}(A) \to \mathrm{End}(FA)$.

(iv) If $0 \to A' \to A \to A'' \to 0$ is exact in $\mathcal{A}$, then $0 \to FA' \to FA \to FA'' \to 0$ is exact in $\mathcal{B}$. Moreover, the first sequence is split if and only if the second sequence is split.

(v) If $(A_i)_{i \in I}$ is a family of objects in $\mathcal{A}$, then

$$F\Big(\bigoplus_{i \in I} A_i\Big) \cong \bigoplus_{i \in I} FA_i \quad \text{and} \quad F\Big(\prod_{i \in I} A_i\Big) \cong \prod_{i \in I} FA_i.$$

(vi) If P is projective in $\mathcal{A}$, then FP is projective in $\mathcal{B}$.

(vii) If P is injective in $\mathcal{A}$, then FP is injective in $\mathcal{B}$.

7.84. Let $F\colon \mathbf{Mod}_R \to \mathbf{Mod}_S$ be an equivalence. Prove that a right R-module A has any of the following properties if and only if FA does: simple; semisimple; ACC; DCC; indecomposable. Moreover, A has a composition series if and only if FA does; both have the same length, and $S_1, \ldots, S_n$ are composition factors of A if and only if $FS_1, \ldots, FS_n$ are composition factors of FA.

∗ **7.85.** If R is a ring with opposite ring R^{op}, prove that $\mathbf{Mod}_R$ is equivalent to ${}_{R^{\mathrm{op}}}\mathbf{Mod}$.

Hint. For each right R-module M, show that there is an isomorphism τ with $\tau(M) = M'$, where M' is M made into a left R-module as in Proposition 6.15.

∗ **7.86.** Prove that every small projective generator P of $\mathbf{Mod}_R$ is finitely generated.

∗ **7.87.** (i) Let R and S be rings, and let $F\colon \mathbf{Mod}_R \to \mathbf{Mod}_S$ (or $F\colon \mathbf{Mod}_R \to {}_S\mathbf{Mod}$) be an equivalence. Prove that a right R-module M is finitely generated if and only if FM is a finitely generated right (or left) S-module.

Hint. Use Exercise 6.17 on page 416.

(ii) Call a category $\mathbf{Mod}_R$ (or ${}_R\mathbf{Mod}$) ***noetherian*** if every submodule of a finitely generated right (or left) R-module M is finitely generated.

Let $\mathcal{A}$ and $\mathcal{B}$ be equivalent categories of modules; that is, $\mathcal{A}$ is equivalent to $\mathbf{Mod}_R$ or ${}_R\mathbf{Mod}$ for some ring R, and $\mathcal{B}$ is equivalent to $\mathbf{Mod}_S$ or ${}_S\mathbf{Mod}$ for some ring S. Prove that $\mathcal{A}$ is noetherian if and only if $\mathcal{B}$ is noetherian.

(iii) Prove that $\mathbf{Mod}_R$ is a noetherian category if and only if R is a right noetherian ring, and that ${}_R\mathbf{Mod}$ is a noetherian category if and only if R is a left noetherian ring.

(iv) Give an example of a ring R such that ${}_R\mathbf{Mod}$ and $\mathbf{Mod}_R$ are not equivalent.
Hint. Let R be the ring in Exercise 6.16 on page 416 which is left noetherian but not right noetherian.