Chapter 9

Introducing Noncommutative Algebra

We will discuss noncommutative rings and their modules, concentrating on two fundamental results, the Wedderburn structure theorem and Maschke's theorem. Further insight into the structure of rings will be provided by the Jacobson radical.

9.1 Semisimple Modules

A vector space is the direct sum of one-dimensional subspaces (each subspace consists of scalar multiples of a basis vector). A one-dimensional space is simple in the sense that it does not have a nontrivial proper subspace. Thus any vector space is a direct sum of simple subspaces. We examine those modules which behave in a similar manner.

9.1.1 Definition

An R-module M is *simple* if $M \neq 0$ and the only submodules of M are 0 and M.

9.1.2 Theorem

Let M be a nonzero R-module. The following conditions are equivalent, and a module satisfying them is said to be *semisimple* or *completely reducible*.

(a) M is a sum of simple modules;

(b) M is a direct sum of simple modules;

(c) If N is a submodule of M, then N is a direct summand of M, that is, there is a submodule N' of M such that $M = N \oplus N'$.

Proof. (a) implies (b). Let M be the sum of simple modules M_i, $i \in I$. If $J \subseteq I$, denote $\sum_{j \in J} M_j$ by $M(J)$. By Zorn's lemma, there is a maximal subset J of I such that the sum defining $N = M(J)$ is direct. We will show that $M = N$. First assume that $i \notin J$.

Then $N \cap M_i$ is a submodule of the simple module M_i, so it must be either 0 or M_i. If $N \cap M_i = 0$, then $M(J \cup \{i\})$ is direct, contradicting maximality of J. Thus $N \cap M_i = M_i$, so $M_i \subseteq N$. But if $i \in J$, then $M_i \subseteq N$ by definition of N. Therefore $M_i \subseteq N$ for all i, and since M is the sum of all the M_i, we have $M = N$.

(b) implies (c). This is essentially the same as (a) implies (b). Let N be a submodule of M, where M is the direct sum of simple modules M_i, $i \in I$. Let J be a maximal subset of I such that the sum $N + M(J)$ is direct. If $i \notin J$ then exactly as before, $M_i \cap (N \oplus M(J)) = M_i$, so $M_i \subseteq N \oplus M(J)$. This holds for $i \in J$ as well, by definition of $M(J)$. It follows that $M = N \oplus M(J)$. [Notice that the complementary submodule N' can be taken as a direct sum of some of the original M_i.]

(c) implies (a). First we make several observations.

(1) If M satisfies (c), so does every submodule N. [Let $N \leq M$, so that $M = N \oplus N'$. If V is a submodule of N, hence of M, we have $M = V \oplus W$. If $x \in N$, then $x = v + w$, $v \in V$, $w \in W$, so $w = x - v \in N$ (using $V \leq N$). But v also belongs to N, and consequently $N = (N \cap V) \oplus (N \cap W) = V \oplus (N \cap W)$.]

(2) If $D = A \oplus B \oplus C$, then $A = (A + B) \cap (A + C)$. [If $a + b = a' + c$, where $a, a' \in A$, $b \in B$, $c \in C$, then $a' - a = b - c$, and since D is a direct sum, we have $b = c = 0$ and $a = a'$. Thus $a + b \in A$.]

(3) If N is a nonzero submodule of M, then N contains a simple submodule.

[Choose a nonzero $x \in N$. By Zorn's lemma, there is a maximal submodule V of N such that $x \notin V$. By (1) we can write $N = V \oplus V'$, and $V' \neq 0$ by choice of x and V. If V' is simple, we are finished, so assume the contrary. Then V' contains a nontrivial proper submodule V_1, so by (1) we have $V' = V_1 \oplus V_2$ with the V_j nonzero. By (2), $V = (V + V_1) \cap (V + V_2)$. Since $x \notin V$, either $x \notin V + V_1$ or $x \notin V + V_2$, which contradicts the maximality of V.]

To prove that (c) implies (a), let N be the sum of all simple submodules of M. By (c) we can write $M = N \oplus N'$. If $N' \neq 0$, then by (3), N' contains a simple submodule V. But then $V \leq N$ by definition of N. Thus $V \leq N \cap N' = 0$, a contradiction. Therefore $N' = 0$ and $M = N$. ♣

9.1.3 Proposition

Nonzero submodules and quotient modules of a semisimple module are semisimple.

Proof. The submodule case follows from (1) of the proof of (9.1.2). Let $N \leq M$, where $M = \sum_i M_i$ with the M_i simple. Applying the canonical map from M to M/N, we have

$$M/N = \sum_i (M_i + N)/N.$$

This key idea has come up before; see the proofs of (1.4.4) and (4.2.3). By the second isomorphism theorem, $(M_i + N)/N$ is isomorphic to a quotient of the simple module M_i. But a quotient of M_i is isomorphic to M_i or to zero, and it follows that M/N is a sum of simple modules. By (a) of (9.1.2), M/N is semisimple. ♣

Problems For Section 9.1

1. Regard a ring R as an R-module. Show that R is simple if and only if R is a division ring.
2. Let M be an R-module, with x a nonzero element of M. Define the R-module homomorphism $f\colon R \to Rx$ by $f(r) = rx$. Show that the kernel I of f is a proper ideal of R, and R/I is isomorphic to Rx.
3. If M is a nonzero R-module, show that M is simple if and only if $M \cong R/I$ for some maximal left ideal I.
4. If M is a nonzero R-module, show that M is simple if and only if M is cyclic (that is, M can be generated by a single element) and every nonzero element of M is a generator.
5. What do simple $\mathbb{Z}$-modules look like?
6. If F is a field, what do simple $F[X]$-modules look like?
7. Let V be an n-dimensional vector space over a field k. (Take $n \geq 1$ so that $V \neq 0$.) If f is an endomorphism (that is, a linear transformation) of V and $x \in V$, define $fx = f(x)$. This makes V into a module over the endomorphism ring $\mathrm{End}_k(V)$. Show that the module is simple.
8. Show that a nonzero module M is semisimple if and only if every short exact sequence $0 \to N \to M \to P \to 0$ splits.

9.2 Two Key Theorems

If M is a simple R-module, there are strong restrictions on a homomorphism either into or out of M. A homomorphism from one simple R-module to another is very severely restricted, as Schur's lemma reveals. This very useful result will be important in the proof of Wedderburn's structure theorem. Another result that will be needed is a theorem of Jacobson that gives some conditions under which a module homomorphism f amounts to multiplication by a fixed element of a ring, at least on part of the domain of f.

9.2.1 Schur's Lemma

(a) If $f \in \mathrm{Hom}_R(M, N)$ where M and N are simple R-modules, then f is either identically 0 or an isomorphism.

(b) If M is a simple R-module, then $\mathrm{End}_R(M)$ is a division ring.

Proof. (a) The kernel of f is either 0 or M, and the image of f is either 0 or N. If f is not the zero map, then the kernel is 0 and the image is N, so f is an isomorphism.

(b) Let $f \in \mathrm{End}_R(M)$, f not identically 0. By (a), f is an isomorphism, and therefore is invertible in the endomorphism ring of M. ♣

The next result prepares for Jacobson's theorem.

9.2.2 Lemma

Let M be a semisimple R-module, and let A be the endomorphism ring $\mathrm{End}_R(M)$. [Note that M is an A-module; if $g \in A$ we take $g \bullet x = g(x)$, $x \in M$.] If $m \in M$ and $f \in \mathrm{End}_A(M)$, then there exists $r \in R$ such that $f(m) = rm$.

Before proving the lemma, let's look more carefully at $\mathrm{End}_A(M)$. Suppose that $f \in \mathrm{End}_A(M)$ and $x \in M$. If $g \in A$ then $f(g(x)) = g(f(x))$. Thus $\mathrm{End}_A(M)$ consists of those abelian group endomorphisms of M that commute with everything in $\mathrm{End}_R(M)$. In turn, by the requirement that $f(rx) = rf(x)$, $\mathrm{End}_R(M)$ consists of those abelian group endomorphisms of M that commute with R, more precisely with multiplication by r, for each $r \in R$. For this reason, $\mathrm{End}_A(M)$ is sometimes called the *double centralizer* of R.

We also observe that the map taking $r \in R$ to multiplication by r is a ring homomorphism of R into $\mathrm{End}_A(M)$. [Again use $rf(x) = f(rx)$.] Jacobson's theorem will imply that given any f in $\mathrm{End}_A(M)$ and any finite set $S \subseteq M$, some g in the image of this ring homomorphism will agree with f on S. Thus in (9.2.2), we can replace the single element m by an arbitrary finite subset of M.

Proof. By (9.1.2) part (c), we can express M as a direct sum $Rm \oplus N$. Now if we have a direct sum $U = V \oplus W$ and $u = v + w$, $v \in V$, $w \in W$, there is a natural projection of U on V, namely $u \to v$. In the present case, let π be the natural projection of M on Rm. Then $\pi \in A$ and $f(m) = f(\pi m) = \pi f(m) \in Rm$. The result follows. ♣

Before proving Jacobson's theorem, we review some ideas that were introduced in the exercises in Section 4.4.

9.2.3 Comments

To specify an R-module homomorphism ψ from a direct sum $V^* = \oplus_{j=1}^n V_j$ to a direct sum $W^* = \oplus_{i=1}^m W_i$, we must give, for every i and j, the i^{th} component of the image of $v_j \in V_j$. Thus the homomorphism is described by a matrix $[\psi_{ij}]$, where ψ_{ij} is a homomorphism from V_j to W_i. The i^{th} component of $\psi(v_j)$ is $\psi_{ij}(v_j)$, so the i^{th} component of $\psi(v_1 + \cdots + v_n)$ is $\sum_{j=1}^n \psi_{ij}(v_j)$. Consequently,

$$\psi(v_1 + \cdots + v_n) = [\psi_{ij}] \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}. \tag{1}$$

This gives an abelian group isomorphism between $\mathrm{Hom}_R(V^*, W^*)$ and $[\mathrm{Hom}_R(V_j, W_i)]$, the collection of all m by n matrices whose ij entry is an R-module homomorphism from V_j to W_i. If we take $m = n$ and $V_i = W_j = V$ for all i and j, then $V^* = W^* = V^n$, the direct sum of n copies of V. Then the abelian group isomorphism given by (1) becomes

$$\mathrm{End}_R(V^n) \cong M_n(\mathrm{End}_R(V)), \tag{2}$$

the collection of all n by n matrices whose entries are$R$-endomorphisms of V. Since composition of endomorphisms corresponds to multiplication of matrices, (2) gives a ring isomorphism as well.

9.2.4 Theorem (Jacobson)

Let M be a semisimple R-module, and let A be the endomorphism ring $\mathrm{End}_R(M)$. If $f \in \mathrm{End}_A(M)$ and $m_1, \ldots, m_n \in M$, then there exists $r \in R$ such that $f(m_i) = rm_i$ for all $i = 1, \ldots, n$.

Proof. f induces an endomorphism $f^{(n)}$ of M^n, the direct sum of n copies of M, via

$$f^{(n)}(m_1 + \cdots + m_n) = f(m_1) + \cdots + f(m_n)$$

where $f(m_i)$ belongs to the i^{th} copy of M. Thus the matrix that represents $f^{(n)}$ is the scalar matrix fI, where I is an n by n identity matrix. If $B = \mathrm{End}_R(M^n)$, then since a scalar matrix commutes with everything, $f^{(n)} \in \mathrm{End}_B(M^n)$. If $m_1, \ldots, m_n \in M$, then by (9.2.2), there exists $r \in R$ such that $f^{(n)}(m_1 + \cdots m_n) = r(m_1 + \cdots m_n)$. [Note that since M is semisimple, so is M^n.] This is equivalent to $f(m_i) = rm_i$ for all i. ♣

Before giving a corollary, we must mention that the standard results that every vector space over a field has a basis, and any two bases have the same cardinality, carry over if the field is replaced by a division ring. Also recall that a module is said to be faithful if its annihilator is 0.

9.2.5 Corollary

Let M be a faithful, simple R-module, and let $D = \mathrm{End}_R(M)$, a division ring by (9.2.1(b)). If M is a finite-dimensional vector space over D, then $\mathrm{End}_D(M) \cong R$, a ring isomorphism.

Proof. Let $\{x_1, \ldots, x_n\}$ be a basis for M over D. By (9.2.4), if $f \in \mathrm{End}_D(M)$, there exists $r \in R$ such that $f(x_i) = rx_i$ for all $i = 1, \ldots, n$. Since the x_i form a basis, we have $f(x) = rx$ for every $x \in M$. Thus the map h from R to $\mathrm{End}_D(M)$ given by $r \to g_r =$ multiplication by r is surjective. If $rx = 0$ for all $x \in M$, then since M is faithful, we have $r = 0$ and h is injective. Since $h(rs) = g_r \circ g_s = h(r)h(s)$, h is a ring isomorphism. ♣

Problems For Section 9.2

1. Criticize the following argument. Let M be a simple R-module, and let $A = \mathrm{End}_R(M)$. "Obviously" M is also a simple A-module. For any additive subgroup N of M that is closed under the application of all R-endomorphisms of M is, in particular, closed under multiplication by an element $r \in R$. Thus N is an R-submodule of M, hence is 0 or M.
2. Let M be a nonzero cyclic module. Show that M is simple if and only if ann M, the annihilator of M, is a maximal left ideal.
3. In Problem 2, show that the hypothesis that M is cyclic is essential.
4. Let $V = F^n$ be the n-dimensional vector space of all n-tuples with components in the field F. If T is a linear transformation on V, then V becomes an $F[X]$-module via

$f(X)v = f(T)v$. For example, if $n = 2$, $T(a, b) = (0, a)$, and $f(X) = a_0 + a_1X + \cdots + a_nX^n$, then

$$\begin{aligned} f(X)(1,0) &= a_0(1,0) + a_1T(1,0) + a_2T^2(1,0) + \cdots + a_nT^n(1,0) \\ &= (a_0, 0) + (0, a_1) \\ &= (a_0, a_1). \end{aligned}$$

Show that in this case, V is cyclic but not simple.

5. Suppose that M is a finite-dimensional vector space over an algebraically closed field F, and in addition M is a module over a ring R containing F as a subring. If M is a simple R-module and f is an R-module homomorphism, in particular an F-linear transformation, on M, show that f is multiplication by some fixed scalar $\lambda \in F$. This result is frequently given as a third part of Schur's lemma.

6. Let I be a left ideal of the ring R, so that R/I is an R-module but not necessarily a ring. Criticize the following statement: "Obviously", I annihilates R/I.

9.3 Simple and Semisimple Rings

9.3.1 Definitions and Comments

Since a ring is a module over itself, it is natural to call a ring R *semisimple* if it is semisimple as an R-module. Our aim is to determine, if possible, how semisimple rings are assembled from simpler components. A plausible idea is that the components are rings that are simple as modules over themselves. But this turns out to be too restrictive, since the components would have to be division rings (Section 9.1, Problem 1).

When we refer to a *simple left ideal* I of R, we will always mean that I is simple as a left R-module. We say that *the ring R is simple* if R is semisimple and all simple left ideals of R are isomorphic. [The definition of simple ring varies in the literature. An advantage of our choice (also favored by Lang and Bourbaki) is that we avoid an awkward situation in which a ring is simple but not semisimple.] Our goal is to show that the building blocks for semisimple rings are rings of matrices over a field, or more generally, over a division ring.

The next two results give some properties of modules over semisimple rings.

9.3.2 Proposition

If R is a semisimple ring, then every nonzero R-module M is semisimple.

Proof. By (4.3.6), M is a quotient of a free R-module F. Since F is a direct sum of copies of R (see (4.3.4)), and R is semisimple by hypothesis, it follows from (9.1.2) that F is semisimple. By (9.1.3), M is semisimple. ♣

9.3.3 Proposition

Let I be a simple left ideal in the semisimple ring R, and let M be a simple R-module. Denote by IM the R-submodule of M consisting of all finite linear combinations $\sum_i r_i x_i$, $r_i \in I$, $x_i \in M$. Then either $IM = M$ and I is isomorphic to M, or $IM = 0$.

Proof. If $IM \neq 0$, then since M is simple, $IM = M$. Thus for some $x \in M$ we have $Ix \neq 0$, and again by simplicity of M, we have $Ix = M$. Map I onto M by $r \to rx$, and note that the kernel cannot be I because $Ix \neq 0$. Since I is simple, the kernel must be 0, so $I \cong M$. ♣

9.3.4 Beginning the Decomposition

Let R be a semisimple ring. We regard two simple left ideals of R as equivalent if they are isomorphic (as R-modules), and we choose a representative I_i, $i \in T$ from each equivalence class. We define the basic building blocks of R as

$$B_i = \text{the sum of all left ideals of } R \text{ that are isomorphic to } I_i.$$

We have a long list of properties of the B_i to establish, and for the sake of economy we will just number the statements and omit the words "Lemma" and "Proof" in each case. We will also omit the end of proof symbol, except at the very end.

9.3.5

If $i \neq j$, then $B_i B_j = 0$. [The product of two left ideals is defined exactly as in (9.3.3).]

Apply (9.3.3) with I replaced by B_i and M by B_j.

9.3.6

$R = \sum_{i \in T} B_i$

If $r \in R$, then (r) is a left ideal, which by (9.1.2) and (9.1.3) (or (9.3.2)) is a sum of simple left ideats.

9.3.7

Each B_i is a two-sided ideal.

Using (9.3.5) and (9.3.6) we have

$$B_i \subseteq B_i R = B_i \sum_j B_j = B_i B_i \subseteq R B_i \subseteq B_i.$$

Thus $RB_i = B_i R = B_i$.

9.3.8

R has only finitely many isomorphism classes of simple left ideals $I_1, \ldots, I_t$.

By (9.3.6), we can write the identity 1 of R as a finite sum of elements $e_i \in B_i$, $i \in T$. Adjusting the notation if necessary, let $1 = \sum_{i=1}^{t} e_i$. If $r \in B_j$ where $j \notin \{1, \ldots, t\}$, then by (9.3.5), $re_i = 0$ for all $i = 1, \ldots, t$, so $r = r1 = 0$. Thus $B_j = 0$ for $j \notin \{1, \ldots, t\}$.

9.3.9

$R = \oplus_{i=1}^{t} B_i$. Thus 1 has a unique representation as $\sum_{i=1}^{t} e_i$, with $e_i \in B_i$.

By (9.3.6) and (9.3.8), R is the sum of the B_i. If $b_1 + \cdots + b_t = 0$, with $b_i \in B_i$, then

$$0 = e_i(b_1 + \cdots + b_t) = e_i b_1 + \cdots e_i b_t = e_i b_i = (e_1 + \cdots + e_t)b_i = 1b_i = b_i.$$

Therefore the sum is direct.

9.3.10

If $b_i \in B_i$, then $e_i b_i = b_i = b_i e_i$. Thus e_i is the identity on B_i and $B_i = Re_i = e_i R$.

The first assertion follows from the computation in (9.3.9), along with a similar computation with e_i multiplying on the right instead of the left. Now $B_i \subseteq Re_i$ because $b_i = b_i e_i$, and $Re_i \subseteq B_i$ by (9.3.7) and the fact that $e_i \in B_i$. The proof that $B_i = e_i R$ is similar.

9.3.11

Each B_i is a simple ring.

By the computation in (9.3.7), along with (9.3.10), B_i is a ring (with identity e_i). Let J be a simple left ideal of B_i. By (9.3.5) and (9.3.6), $RJ = B_i J = J$, so J is a left ideal of R, necessarily simple. Thus J is isomorphic to some I_j, and we must have $j = i$. [Otherwise, J would appear in the sums defining both B_i and B_j, contradicting (9.3.9).] Therefore B_i has only one isomorphism class of simple left ideals. Now B_i is a sum of simple left ideals of R, and a subset of B_i that is a left ideal of R must be a left ideal of B_i. Consequently, B_i is semisimple and the result follows.

9.3.12

If M is a simple R-module, then M is isomorphic to some I_i. Thus there are only finitely many isomorphism classes of simple R-modules. In particular, if R is a simple ring, then all simple R-modules are isomorphic.

By (9.3.9),

$$R = \sum_{i=1}^{t} B_i = \sum_{i=1}^{t} \sum \{J \colon J \cong I_i\}$$

where the J are simple left ideals. Therefore

$$M = RM = \sum_{i=1}^{t} B_i M = \sum_{i=1}^{t} \sum \{JM \colon J \cong I_i\}.$$

By (9.3.3), $JM = 0$ or $J \cong M$. The former cannot hold for all J, since $M \neq 0$. Thus $M \cong I_i$ for some i. If R is a simple ring, then there is only one i, and the result follows.

9.3.13

Let M be a nonzero R-module, so that M is semisimple by (9.3.2). Define M_i as the sum of all simple submodules of M that are isomorphic to I_i, so that by (9.3.12), $M = \sum_{i=1}^{t} M_i$. Then

$$M = \bigoplus_{i=1}^{t} B_i M \text{ and } B_i M = e_i M = M_i,\ i = 1, \ldots, t.$$

By definition of B_i,

$$B_i M_j = \sum \{JM_j \colon J \cong I_i\}$$

where the J's are simple left ideals. If N is any simple module involved in the definition of M_j, then JN is 0 or N, and by (9.3.3), $JN = N$ implies that $N \cong J \cong I_i$. But all such N are isomorphic to I_j, and therefore $B_i M_j = 0, i \neq j$. Thus

$$M_i = RM_i = \sum_j B_j M_i = B_i M_i$$

and

$$B_i M = \sum_j B_i M_j = B_i M_i.$$

Consequently, $M_i = B_i M = e_i RM = e_i M$ (using (9.3.10)), and all that remains is to show that the sum of the M_i is direct. Let $x_1 + \cdots + x_t = 0$, $x_i \in M_i$. Then

$$0 = e_i(x_1 + \cdots + x_t) = e_i x_i$$

since $e_i x_j \in B_i M_j = 0$ for $i \neq j$. Finally, by (9.3.9),

$$e_i x_i = (e_1 + \cdots + e_t)x_i = x_i.$$

9.3.14

A semisimple ring R is *ring-isomorphic* to a direct product of simple rings.

This follows from (9.3.9) and (9.3.5). For if $a_i, b_i \in B_i$, then

$$(a_1 + \cdots + a_t)(b_1 + \cdots + b_t) = a_1 b_1 + \cdots + a_t b_t. \quad \clubsuit$$

Problems For Section 9.3

In Problems 1 and 2, let M be a semisimple module, so that M is the direct sum of simple modules M_i, $i \in I$. We are going to show that M is a finite direct sum of simple modules if and only if M is finitely generated.

1. Suppose that $x_1, \ldots, x_n$ generate M. It will follow that M is the direct sum of finitely many of the M_i. How would you determine which M_i's are involved?

2. Conversely, assume that M is a finite sum of simple modules. Show that M is finitely generated.
3. A left ideal I is said to be *minimal* if $I \neq 0$ and I has no proper subideal except 0. Show that the ring R is semisimple if and only if R is a direct sum of minimal left ideals.
4. Is $\mathbb{Z}$ semisimple?
5. Is $\mathbb{Z}_n$ semisimple?
6. Suppose that R is a ring with the property that every nonzero R-module is semisimple. Show that every R-module M is projective, that is, every exact sequence $0 \to A \to B \to M \to 0$ splits. Moreover, M is injective, that is, every exact sequence $0 \to M \to A \to B \to 0$ splits. [Projective and injective modules will be studied in Chapter 10.]
7. For any ring R, show that the following conditions are equivalent.
   (a) R is semisimple;
   (b) Every nonzero R-module is semisimple;
   (c) Every R-module is projective;
   (d) Every R-module is injective.

9.4 Further Properties of Simple Rings, Matrix Rings, and Endomorphisms

To reach the Wedderburn structure theorem, we must look at simple rings in more detail, and supplement what we already know about matrix rings and rings of endomorphisms.

9.4.1 Lemma

Let R be any ring, regarded as a left module over itself. If $h\colon R \to M$ is an R-module homomorpbism, then for some $x \in M$ we have $h(r) = rx$ for every $r \in R$. Moreover, we may choose $x = h(1)$, and the map $h \to h(1)$ is an isomorphism of $\mathrm{Hom}_R(R, M)$ and M. This applies in particular when $M = R$, in which case $h \in \mathrm{End}_R(R)$.

Proof. The point is that h is determined by what it does to the identity. Thus

$$h(r) = h(r1) = rh(1)$$

so we may take $x = h(1)$. If $s \in R$ and $h \in \mathrm{Hom}_R(R, M)$, we take $(sh)(r) = h(rs) = rsx$. This makes $\mathrm{Hom}_R(R, M)$ into a left R-module isomorphic to M. (For further discussion of this idea, see the exercises in Section 10.7.) ♣

Notice that although all modules are *left* R-modules, h is given by multiplication on the *right* by x.

9.4.2 Corollary

Let I and J be simple left ideals of the simple ring R. Then for some $x \in R$ we have $J = Ix$.

Proof. By the definition of a simple ring (see (9.3.1)), R is semisimple, so by (9.1.2), $R = I \oplus L$ for some left ideal L. Again by the definition of a simple ring, I and J are isomorphic (as R-modules). If $\tau : I \to J$ is an isomorphism and π is the natural projection of R on I, then $\tau\pi \in \mathrm{End}_R(R)$, so by (9.4.1), there exists $x \in R$ such that $\tau\pi(r) = rx$ for every $r \in R$. Allow r to range over I to conclude that $J = Ix$. ♣

A semisimple ring can be expressed as a direct sum of simple left ideals, by (9.1.2). If the ring is simple, only finitely many simple left ideals are needed.

9.4.3 Lemma

A simple ring R is a finite direct sum of simple left ideals.

Proof. Let $R = \oplus_j I_j$ where the I_j are simple left ideals. Changing notation if necessary, we have $1 = y_1 + \cdots + y_m$ with $y_j \in I_j$, $j = 1, \ldots, m$. If $x \in R$, then

$$x = x1 = \sum_{j=1}^{m} xy_j \in \sum_{j=1}^{m} I_j.$$

Therefore R is a finite sum of the I_j, and the sum is direct because the original decomposition of R is direct. ♣

9.4.4 Corollary

If I is a simple left ideal of the simple ring R, then $IR = R$.

Proof. If J is any simple left ideal of R, then by (9.4.2), $J \subseteq IR$. By (9.4.3), R is a finite (direct) sum of simple left ideals, so $R \subseteq IR$. The reverse inclusion always holds, and the result follows. ♣

We now have some insight into the structure of simple rings.

9.4.5 Proposition

If R is a simple ring, then the only two-sided ideals of R are 0 and R.

Proof. Let J be a nonzero 2-sided ideal of R. By (9.1.3), J is a semisimple left R-module, so by (9.1.2), J is a sum of simple left ideals of J, hence of R. In particular, J contains a simple left ideal I. Since J is a right ideal, it follows that $J = JR$. Using (9.4.4), we have

$$J = JR \supseteq IR = R$$

so $J = R$. ♣

In the literature, a simple ring is often defined as a ring R whose only two-sided ideals are 0 and R, but then extra hypotheses must be added to force R to be semisimple. See the exercises for further discussion.

9.4.6 Corollary

Let I be a simple left ideal of the simple ring R, and let M be a simple R-module. Then $IM = M$ and M is faithful.

Proof. The first assertion follows from a computation that uses associativity of scalar multiplication in a module, along with (9.4.4):

$$M = RM = (IR)M = I(RM) = IM. \tag{1}$$

Now let b belong to the annihilator of M, so that $bM = 0$. We must show that $b = 0$. By a computation similar to (1) (using in addition the associativity of ring multiplication),

$$RbRM = RbM = R0 = 0. \tag{2}$$

But RbR is a two-sided ideal of R (see (2.2.7)), so by (9.4.5), $RbR = 0$ or R. In the latter case, $M = RM = RbRM = 0$ by (2), contradicting the assumption that M is simple. Therefore $RbR = 0$, in particular, $b = 1b1 = 0$. ♣

We are now ready to show that a simple ring is isomorphic to a ring of matrices. Let R be a simple ring, and V a simple R-module. [V exists because R is a sum of simple left ideals, and V is unique up to isomorphism by (9.3.12).] Let $D = \mathrm{End}_R(V)$, a division ring by Schur's lemma (9.2.1(b)). Then (see (9.2.2)), V is a D-module, in other words, a vector space over D. V is a faithful R-module by (9.4.6), and if we can prove that V is finite-dimensional as a vector space over D, then by (9.2.5), R is ring-isomorphic to $\mathrm{End}_D(V)$. If n is the dimension of V over D, then by (4.4.1), $\mathrm{End}_D(V) \cong M_n(D^o)$, the ring of n by n matrices with entries in the opposite ring D^o.

9.4.7 Theorem

Let R be a simple ring, V a simple R-module, and D the endomorphism ring $\mathrm{End}_R(V)$. Then V is a finite-dimensional vector space over D. If the dimension of this vector space is n, then (by the above discussion),

$$R \cong \mathrm{End}_D(V) \cong M_n(D^o).$$

Proof. Assume that we have infinitely many linearly independent elements $x_1, x_2, \ldots$. Let I_m be the left ideal $\{r \in R\colon rx_i = 0 \text{ for all } i = 1, \ldots, m\}$. Then the I_m decrease as m increases, in fact they decrease strictly. [Given any m, let f be a D-linear transformation on V such that $f(x_i) = 0$ for $1 \leq i \leq m$ and $f(x_{m+1}) \neq 0$. By Jacobson's theorem (9.2.4), there exists $r \in R$ such that $f(x_i) = rx_i$, $i = 1, \ldots, m+1$. But then $rx_1 = \cdots = rx_m = 0$, $rx_{m+1} \neq 0$, so $r \in I_m \setminus I_{m+1}$.] Write $I_m = J_m \oplus I_{m+1}$, as in (9.1.2) part (c). [Recall

from (9.1.3) that since R is semisimple, so are all left ideals.] Iterating this process, we construct a left ideal $J_1 \oplus J_2 \oplus \cdots$, and again by (9.1.2(c)),

$$R = J_0 \oplus J_1 \oplus J_2 \oplus \cdots .$$

Therefore 1 is a finite sum of elements $y_i \in J_i$, $i = 0, 1, \ldots, t$. But then

$$R = J_0 \oplus J_1 \oplus \cdots \oplus J_t$$

and it follows that J_{t+1} must be 0, a contradiction. ♣

Problems For Section 9.4

Problems 1–5 are the key steps in showing that a ring R is simple if and only if R is Artinian and has no two-sided ideals except 0 and R. Thus if a simple ring is defined as one with no nontrivial two-sided ideals, then the addition of the Artinian condition gives our definition of simple ring; in particular, it forces the ring to be semisimple. The result that an Artinian ring with no nontrivial two-sided ideals is isomorphic to a matrix ring over a division ring (Theorem 9.4.7) is sometimes called the *Wedderburn-Artin theorem*.

In Problems 1–5, "simple" will always mean simple in our sense.

1. By (9.4.5), a simple ring has no nontrivial two-sided ideals. Show that a simple ring must be Artinian.
2. If R is an Artinian ring, show that there exists a simple R-module.
3. Let R be an Artinian ring with no nontrivial two-sided ideals. Show that R has a faithful, simple R-module.
4. Continuing Problem 3, if V is a faithful, simple R-module, and $D = \mathrm{End}_R(V)$, show that V is a finite-dimensional vector space over D.
5. Continuing Problem 4, show that R is ring-isomorphic to $\mathrm{End}_D(V)$, and therefore to a matrix ring $M_n(D^o)$ over a division ring.

In the next section, we will prove that a matrix ring over a division ring is simple; this concludes the proof that R is simple iff R is Artinian with no nontrivial two-sided ideals. (In the "if" part, semisimplicity of R follows from basic properties of matrix rings; see Section 2.2, Problems 2, 3 and 4.)

6. If an R-module M is a direct sum $\oplus_{i=1}^{n} M_i$ of finitely many simple modules, show that M has a composition series. (Equivalently, by (7.5.12), M is Artinian and Noetherian.)
7. Conversely, if M is semisimple and has a composition series, show that M is a finite direct sum of simple modules. (Equivalently, by Section 9.3, Problems 1 and 2, M is finitely generated.)

9.5 The Structure of Semisimple Rings

We have now done all the work needed for the fundamental theorem.

9.5.1 Wedderburn Structure Theorem

Let R be a semisimple ring.

(1) R is ring-isomorphic to a direct product of simple rings $B_1, \ldots, B_t$.

(2) There are t isomorphism classes of simple R-modules. If $V_1, \ldots, V_t$ are representatives of these classes, let D_i be the division ring $\mathrm{End}_R(V_i)$. Then V_i is a finite-dimensional vector space over D_i. If n_i is the dimension of this vector space, then there is a ring isomorphism

$$B_i \cong \mathrm{End}_{D_i}(V_i) \cong M_{n_i}(D_i^o).$$

Consequently, R is isomorphic to the direct product of matrix rings over division rings. Moreover,

(3) $B_iV_j = 0$, $i \neq j$; $B_iV_i = V_i$.

Proof. Assertion (1) follows from (9.3.5), (9.3.9) and (9.3.14). By (9.3.8) and (9.3.12), there are t isomorphism classes of simple R-modules. The remaining statements of (2) follow from (9.4.7). The assertions of (3) follow from (9.3.13) and its proof. ♣

Thus a semisimple ring can always be assembled from matrix rings over division rings. We now show that such matrix rings can never combine to produce a ring that is not semisimple.

9.5.2 Theorem

The ring $M_n(R)$ of all n by n matrices with entries in the division ring R is simple.

Proof. We have done most of the work in the exercises for Section 2.2. Let C_k be the set of matrices whose entries are 0 except perhaps in column k, $k = 1 \ldots, n$. Then C_k is a left ideal of $M_n(R)$, and if any nonzero matrix in C_k belongs to a left ideal I, then $C_k \subseteq I$. (Section 2.2, Problems 2, 3, 4.) Thus each C_k is a simple left ideal, and $M_n(R)$, the direct sum of $C_1, \ldots, C_n$, is semisimple.

Now let I be a nonzero simple left ideal. A nonzero matrix in I must have a nonzero entry in some column, say column k. Define $f\colon I \to C_k$ by $f(A) = A_k$, the matrix obtained from A by replacing every entry except those in column k by 0. Then f is an $M_n(R)$-module homomorphism, since

$$f(BA) = (BA)_k = BA_k = Bf(A).$$

By construction, f is not identically 0, so by Schur's lemma, f is an isomorphism. Since the C_k are mutually isomorphic, all simple left ideals are isomorphic, proving that $M_n(R)$ is simple. ♣

9.5.3 Informal Introduction to Group Representations

A major application of semisimple rings and modules occurs in group representation theory, and we will try to indicate the connection. Let k be any field, and let G be a finite group. We form the *group algebra* kG, which is a vector space over k with basis vectors corresponding to the elements of G. In general, if $G = \{x_1, \ldots, x_m\}$, the elements of kG are of the form $\alpha_1 x_1 + \cdots + \alpha_m x_m$, where the α_i belong to k. Multiplication in kG is defined in the natural way; we set

$$(\alpha x_i)(\beta x_j) = \alpha\beta x_i x_j$$

and extend by linearity. Then kG is a ring (with identity $1_k 1_G$) that is also a vector space over k, and $\alpha(xy) = (\alpha x)y = x(\alpha y)$, $\alpha \in k$, $x, y \in G$, so kG is indeed an algebra over k. [This construction can be carried out with an arbitrary ring R in place of k, and with an arbitrary (not necessarily finite) group G. The result is the *group ring* RG, a free R-module with basis G.]

Now let V be an n-dimensional vector space over k. We want to describe the situation in which "G acts linearly on V". We are familiar with group action (Section 5.1), but we now add the condition that each $g \in G$ determines a linear transformation $\rho(g)$ on V. We will write $\rho(g)(v)$ as simply gv or $g(v)$, so that $g(\alpha v + \beta w) = \alpha g(v) + \beta g(w)$. Thus we can multiply vectors in V by scalars in G. Since elements of kG are linear combinations of elements of G with coefficients in k, we can multiply vectors in V by scalars in kG. To summarize very compactly,

$$V \text{ is a } kG\text{-module.}$$

Now since G acts on V, $(hg)v = h(gv)$ and $1_G v = v$, $g, h \in G$, $v \in V$. Thus $\rho(hg) = \rho(h)\rho(g)$, and each $\rho(g)$ is invertible since $\rho(g)\rho(g^{-1}) = \rho(1_G) =$ the identity on V. Therefore

$$\rho \text{ is a homomorphism from } G \text{ to } GL(V),$$

the group of invertible linear transformations on V. Multiplication in $GL(V)$ corresponds to composition of functions.

$$\text{The homomorphism } \rho \text{ is called a } \textit{representation} \text{ of } G \text{ in } V,$$

and n, the dimension of V, is called the *degree* of the representation. If we like, we can replace $GL(V)$ by the group of all nonsingular n by n matrices with entries in k. In this case, ρ is called a *matrix representation*.

The above process can be reversed. Given a representation ρ, we can define a linear action of G on V by $gv = \rho(g)(v)$, and thereby make V a kG-module. Thus representations can be identified with kG-modules.

9.5.4 The Regular Representation

If G has order n, then kG is an n-dimensional vector space over k with basis G. We take V to be kG itself, with gv the product of g and v in kG. As an example, let $G = \{e, a, a^2\}$,

a cyclic group of order 3. V is a 3-dimensional vector space with basis e, a, a^2, and the action of G on V is determined by

$$ee = e,\ ea = a,\ ea^2 = a^2;$$
$$ae = a,\ aa = a^2,\ aa^2 = e;$$
$$a^2e = a^2,\ a^2a = e,\ a^2a^2 = a.$$

Thus the matrices $\rho(g)$ associated with the elements $g \in G$ are

$$[e] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix},\ [a] = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix},\ [a^2] = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}.$$

9.5.5 The Role of Semisimplicity

Suppose that ρ is a representation of G in V. Assume that the basis vectors of V can be decomposed into two subsets $v(A)$ and $v(B)$ such that matrix of *every* $g \in G$ has the form

$$[g] = \begin{bmatrix} A & 0 \\ 0 & B \end{bmatrix}.$$

(The elements of A and B will depend on the particular g, but the dimensions of A and B do not change.) The corresponding statement about V is that

$$V = V_A \oplus V_B$$

where V_A and V_B are kG-submodules of V. We can study the representation by analyzing its behavior on the simpler spaces V_A and V_B. Maschke's theorem, to be proved in the next section, says that under wide conditions on the field k, this decomposition process can be continued until we reach subspaces that have no nontrivial kG-submodules. In other words, every kG-module is semisimple. In particular, kG is a semisimple ring, and the Wedderburn structure theorem can be applied to get basic information about representations.

We will need some properties of projection operators, and it is convenient to take care of this now.

9.5.6 Definitions and Comments

A linear transformation π on a vector space V [or more generally, a module homomorphism] is called a *projection* of V (on $\pi(V)$) if π is *idempotent*, that is, $\pi^2 = \pi$. We have already met the natural projection of a direct sum onto a component, but there are other possibilities. For example, let p be the projection of $\mathbb{R}^2 = \mathbb{R} \oplus \mathbb{R}$ given by $p(x, y) = \left(\frac{x-y}{2}, \frac{-x+y}{2}\right)$. Note that π must be the identity on $\pi(V)$, since $\pi(\pi(v)) = \pi(v)$.

If we choose subspaces carefully, we can regard any projection as natural.

9.5.7 Proposition

If π is a projection of V, then V is the direct sum of the image of π and the kernel of π.

Proof. Since $v = \pi(v) + (v - \pi(v))$ and $\pi(v - \pi(v)) = 0$, $V = \operatorname{im} V + \ker V$. To show that the sum is direct, let $v = \pi(w) \in \ker \pi$. Then $0 = \pi(v) = \pi^2(w) = \pi(w) = v$, so $\operatorname{im} \pi \cap \ker \pi = 0$. ♣

9.5.8 Example

For real numbers x and y, we have $(x, y) = (x - cy)(1, 0) + y(c, 1)$, where c is any fixed real number. Thus $\mathbb{R}^2 = \mathbb{R}(1, 0) \oplus \mathbb{R}(c, 1)$, and if we take $p(x, y) = (x - cy, 0)$, then p is a projection of $\mathbb{R}^2$ onto $\mathbb{R}(1, 0)$. By varying c we can change the complementary subspace $\mathbb{R}(c, 1)$. Thus we have many distinct projections onto the same subspace $\mathbb{R}(1, 0)$.

Problems For Section 9.5

1. Show that the regular representation is *faithful*, that is, the homomorphism ρ is injective.
2. Let G be a subgroup of S_n and let V be an n-dimensional vector space over k with basis $v(1), \ldots, v(n)$. Define the action of G on V by

$$g(v(i)) = v(g(i)),\ i = 1, \ldots, n.$$

   Show that the action is legal. (V is called a *permutation module*.)
3. Continuing Problem 2, if $n = 4$, find the matrix of $g = (1, 4, 3)$.
4. Here is an example of how a representation can arise in practice. Place an equilateral triangle in the plane V, with the vertices at $v_1 = (1, 0)$, $v_2 = \left(-\frac{1}{2}, \frac{1}{2}\sqrt{3}\right)$ and $v_3 = \left(-\frac{1}{2}, -\frac{1}{2}\sqrt{3}\right)$; note that $v_1 + v_2 + v_3 = 0$. Let $G = D_6$ be the group of symmetries of the triangle, with $g =$ counterclockwise rotation by 120 degrees and $h =$ reflection about the horizontal axis. Each member of D_6 is of the form $g^i h^j$, $i = 0, 1, 2$, $j = 0, 1$, and induces a linear transformation on V. Thus we have a representation of G in V (the underlying field k can be taken as $\mathbb{R}$).

   With v_1 and v_2 taken as a basis for V, find the matrices $[g]$ and $[h]$ associated with g and h.

5. Continue from Problem 4, and switch to the standard basis $e_1 = v_1 = (1, 0)$, $e_2 = (0, 1)$. Changing the basis produces an *equivalent matrix representation*. The matrix representing the element $a \in G$ is now of the form

$$[a]' = P^{-1}[a]P$$

   where the similarity matrix P is the same for every $a \in G$ (the key point).

   Find the matrix P corresponding to the switch from $\{v_1, v_2\}$ to $\{e_1, e_2\}$, and the matrices $[g]'$ and $[h]'$.

6. Consider the dihedral group D_8, generated by elements R (rotation) and F (reflection). We assign to R the 2 by 2 matrix

$$A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$$

and to F the 2 by 2 matrix

$$B = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}.$$

Show that the above assignment determines a matrix representation of D_8 of degree 2.

7. Is the representation of Problem 6 faithful?

A very accessible basic text on group representation theory is "Representations and Characters of Groups" by James and Liebeck.

9.6 Maschke's Theorem

We can now prove the fundamental theorem on decomposition of representations. It is useful to isolate the key ideas in preliminary lemmas.

9.6.1 Lemma

Let G be a finite group, and k a field whose characteristic does not divide $|G|$ (so that division by $|G|$ is legal). Let V be a kG-module, and ψ a linear transformation on V as a vector space over k. Define $\theta\colon V \to V$ by

$$\theta(v) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\psi g(v).$$

Then not only is θ a linear transformation on the vector space V, but it is also a kG-homomorphism.

Proof. Since ψ is a linear transformation and G acts linearly on V (see (9.5.3)), θ is linear. Now if $h \in G$, then

$$\theta(hv) = \frac{1}{|G|} \sum_{g \in G} g^{-1}\psi g(hv).$$

As g ranges over all of G, so does gh. Thus we can let $x = gh$, $g^{-1} = hx^{-1}$, to obtain

$$\theta(hv) = \frac{1}{|G|} \sum_{x \in G} hx^{-1}\psi(xv) = h\theta(v)$$

and the result follows. ♣

9.6.2 Lemma

In (9.6.1), suppose that ψ is a projection of V on a subspace W that is also a kG-submodule of V. Then θ is also a projection of V on W.

Proof. If $v \in W$, then $g(v) \in W$ since W is a kG-submodule of V. Thus $\psi g(v) = g(v)$ since ψ is a projection on W. By definition of θ we have $\theta(v) = v$. To prove that $\theta^2 = \theta$, note that since ψ maps V into the kG-submodule W, it follows from the definition of θ that θ also maps V into W. But θ is the identity on W, so

$$\theta^2(v) = \theta(\theta(v)) = \theta(v)$$

and θ is a projection. Since θ maps into W and is the identity on W, θ is a projection of V on W. ♣

9.6.3 Maschke's Theorem

Let G be a finite group, and k a field whose characteristic does not divide $|G|$. If V is a kG-module, then V is semisimple.

Proof. Let W be a kG-submodule of V. Ignoring the group algebra for a moment, we can write $V = W \oplus U$ as vector spaces over k. Let ψ be the natural projection of V on W, and define θ as in (9.6.1). By (9.6.1) and (9.6.2), θ is a kG-homomorphism and also a projection of V on W. By (9.5.7), $V = \operatorname{im}\theta \oplus \ker\theta = W \oplus \ker\theta$ *as kG-modules.* By (9.1.2), V is semisimple. ♣

We have been examining the decomposition of a semisimple module into a direct sum of simple modules. Suppose we start with an *arbitrary* module M, and ask whether M can be expressed as $M_1 \oplus M_2$, where M_1 and M_2 are nonzero submodules. If so, we can try to decompose M_1 and M_2, and so on. This process will often terminate in a finite number of steps.

9.6.4 Definition

The module M is *decomposable* if $M = M_1 \oplus M_2$, where M_1 and M_2 are nonzero submodules. Otherwise, M is *indecomposable.*

9.6.5 Proposition

Let M be a module with a composition series; equivalently, by (7.5.12), M is Noetherian and Artinian. Then M can be expressed as a finite direct sum $\oplus_{i=1}^{n} M_i$ of indecomposable submodules.

Proof. If the decomposition process does not terminate, infinite ascending and descending chains are produced, contradicting the hypothesis. ♣

As the above argument shows, the hypothesis can be weakened to M Noetherian *or* Artinian. But (9.6.5) is usually stated along with a uniqueness assertion which uses the stronger hypothesis:

If M has a composition series and $M = \oplus_{i=1}^{n} M_i = \oplus_{j=1}^{m} N_j$, where the M_i and N_j are indecomposable submodules, then $n = m$ and the M_i are, up to isomorphism, just a rearrangement of the N_i.

The full result (existence plus uniqueness) is most often known as the **Krull-Schmidt Theorem**. [One or more of the names Remak, Azumaya and Wedderburn are sometimes added.] The uniqueness proof is quite long (see, for example, Jacobson's Basic Algebra II), and we will not need the result.

Returning to semisimple rings, there is an asymmetry in the definition in that a ring is regarded as a left module over itself, so that submodules are left ideals. We can repeat the entire discussion using right ideals, so that we should distinguish between left-semisimple and right-semisimple rings. However, this turns out to be unnecessary.

9.6.6 Theorem

A ring R is left-semisimple if and only if it is right-semisimple.

Proof. If R is left-semisimple, then by (9.5.1), R is isomorphic to a direct product of matrix rings over division rings. But a matrix ring over a division ring is right-simple by (9.5.2) with left ideals replaced by right ideals. Therefore R is right-semisimple. The reverse implication is symmetrical. ♣

Problems For Section 9.6

1. Let V be the permutation module for $G = S_3$ (see Section 9.5, Problem 2), with basis v_1, v_2, v_3. Give an example of a nontrivial kG-submodule of V.

In Problems 2–4, we show that Maschke's theorem can fail if the characteristic of k divides the order of G. Let $G = \{1, a, \ldots, a^{p-1}\}$ be a cyclic group of prime order p, and let V be a two-dimensional vector space over the field $\mathbb{F}_p$, with basis v_1, v_2. Take the matrix of a as

$$[a] = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

so that

$$[a^r] = \begin{bmatrix} 1 & r \\ 0 & 1 \end{bmatrix}$$

and $[a^p]$ is the identity.

2. Show that W, the one-dimensional subspace spanned by v_1, is a kG-submodule of V.
3. Continuing Problem 2, show that W is the only one-dimensional kG-submodule of V.
4. Continuing Problem 3, show that V is not a semisimple kG-module.
5. Show that a semisimple module is Noetherian iff it is Artinian.

6. Let M be a decomposable R-module, so that M is the direct sum of nonzero submodules M_1 and M_2. Show that $\mathrm{End}_R(M)$ contains a nontrivial idempotent e (that is, $e^2 = e$ with e not the zero map and not the identity).
7. Continuing from Problem 6, suppose conversely that $\mathrm{End}_R(M)$ contains a nontrivial idempotent e. Show that M is decomposable. (Suggestion: use e to construct idempotents e_1 and e_2 that are *orthogonal*, that is, $e_1e_2 = e_2e_1 = 0$.)

9.7 The Jacobson Radical

There is a very useful device that will allow us to look deeper into the structure of rings.

9.7.1 Definitions and Comments

The *Jacobson radical* $J(R)$ of a ring R is the intersection of all maximal left ideals of R. More generally, the Jacobson radical $J(M) = J_R(M)$ of an R-module M is the intersection of all maximal submodules of M. ["Maximal submodule" will always mean "maximal proper submodule".] If M has no maximal submodule, take $J(M) = M$.

If M is finitely generated, then every submodule N of M is contained in a maximal submodule, by Zorn's lemma. [If the union of a chain of proper submodules is M, then the union contains all the generators, hence some member of the chain contains all the generators, a contradiction.] Taking $N = 0$, we see that $J(M)$ is a proper submodule of M. Since R is finitely generated (by 1_R), $J(R)$ is always a proper left ideal.

Semisimplicity of M imposes a severe constraint on $J(M)$.

9.7.2 Proposition

If M is semisimple, then $J(M) = 0$. Thus in a sense, the Jacobson radical is an "obstruction" to semisimplicity.

Proof. Let N be any simple submodule of M. By (9.1.2), $M = N \oplus N'$ for some submodule N'. Now $M/N' \cong N$, which is simple, so by the correspondence theorem, N' is maximal. Thus $J(M) \subseteq N'$, and therefore $J(M) \cap N = 0$. Since M is a sum of simple modules (see (9.1.2)), $J(M) = J(M) \cap M = 0$ ♣

Here is another description of the Jacobson radical.

9.7.3 Proposition

$J(R)$ is the intersection of all annihilators of simple R-modules.

Proof. By Section 9.1, Problem 3, simple modules are isomorphic to R/I for maximal left ideals I. If r annihilates all simple R-modules, then for every maximal left ideal I, r annihilates R/I, in particular, r annihilates $1 + I$. Thus $r(1 + I) = I$, that is, $r \in I$. Consequently, $r \in J(R)$.

Conversely, assume $r \in J(R)$. If M is a simple R-module, choose any nonzero element $x \in M$. The map $f_x\colon R \to M$ given by $f_x(s) = sx$ is an epimorphism by simplicity of

M. The kernel of f_x is the annihilator of x, denoted by $\text{ann}(x)$. By the first isomorphism theorem, $M \cong R/\text{ann}(x)$. By simplicity of M, $\text{ann}(x)$ is a maximal left ideal, so by hypothesis, $r \in \cap_{x \in M} \text{ann}(x) = \text{ann}(M)$. Thus r annihilates all simple R-modules. ♣

9.7.4 Corollary

$J(R)$ is a two-sided ideal.

Proof. We noted in (4.2.6) that $\text{ann}(M)$ is a two-sided ideal, and the result follows from (9.7.3). ♣

In view of (9.7.4), one might suspect that the Jacobson radical is unchanged if right rather than left ideals are used in the definition. This turns out to be the case.

9.7.5 Definitions and Comments

The element $a \in R$ is *left quasi-regular* (lqr) if $1 - a$ has a left inverse, *right quasi-regular* (rqr) if $1 - a$ has a right inverse, and *quasi-regular* (qr) if $1 - a$ is invertible. Note that if a is both lqr and rqr, it is qr, because if $b(1 - a) = (1 - a)c = 1$, then

$$b = b1 = b(1 - a)c = 1c = c.$$

9.7.6 Lemma

Let I be a left ideal of R. If every element of I is lqr, then every element of I is qr.

Proof. If $a \in I$, then we have $b(1 - a) = 1$ for some $b \in R$. Let $c = 1 - b$, so that $(1 - c)(1 - a) = 1 - a - c + ca = 1$. Thus $c = ca - a = (c - 1)a \in I$. By hypothesis, c is lqr, so $1 - c$ has a left inverse. But we know that $(1 - c)$ has a right inverse $(1 - a)$ [see above], so c is rqr. By (9.7.5), c is qr and $1 - c$ is the two-sided inverse of $1 - a$. ♣

9.7.7 Proposition

The Jacobson radical $J(R)$ is the largest two-sided ideal consisting entirely of quasi-regular elements.

Proof. First, we show that each $a \in J(R)$ is lqr, so by (9.7.6), each $a \in J(R)$ is qr. If $1-a$ has no left inverse, then $R(1 - a)$ is a proper left ideal, which is contained in a maximal left ideal I (as in (2.4.2) or (9.7.1)). But then $a \in I$ and $1 - a \in I$, and therefore $1 \in I$, a contradiction.

Now we show that every left ideal (hence every two-sided ideal) I consisting entirely of quasi-regular elements is contained in $J(R)$. If $a \in I$ but $a \notin J(R)$, then for some maximal left ideal L we have $a \notin L$. By maximality of L, we have $I + L = R$, so $1 = b + c$ for some $b \in I$, $c \in L$. But then b is quasi-regular, so $c = 1 - b$ has an inverse, and consequently $1 \in L$, a contradiction. ♣

9.7.8 Corollary

$J(R)$ is the intersection of all maximal right ideals of R.

Proof. We can reproduce the entire discussion beginning with (9.7.1) with left and right ideals interchanged, and reach exactly the same conclusion, namely that the "right" Jacobson radical is the largest two-sided ideal consisting entirely of quasi-regular elements. It follows that the "left"and "right" Jacobson radicals are identical. ♣

We can now use the Jacobson radical to sharpen our understanding of semisimple modules and rings.

9.7.9 Theorem

If M is a nonzero R-module, the following conditions are equivalent:

(1) M is semisimple and has finite length, that is, has a composition series;

(2) M is Artinian and $J(M) = 0$.

Proof. (1) implies (2) by (7.5.12) and (9.7.2), so assume M Artinian with $J(M) = 0$. The Artinian condition implies that the collection of all finite intersections of maximal submodules of M has a minimal element N. If S is any maximal submodule of M, then $N \cap S$ is a finite intersection of maximal submodules, so by minimality of N, $N \cap S = N$, so $N \subseteq S$. Since $J(M)$ is the intersection of all such S, the hypothesis that $J(M) = 0$ implies that $N = 0$. Thus for some positive integer n we have maximal submodules $M_1, \ldots, M_n$ such that $\cap_{i=1}^{n} M_i = 0$.

Now M is isomorphic to a submodule of $M' = \oplus_{i=1}^{n}(M/M_i)$. To see this, map $x \in M$ to $(x+M_1, \ldots, x+M_n)$ and use the first isomorphism theorem. Since M' is a finite direct sum of simple modules, it is semisimple and has a composition series. (See Section 9.4, Problem 6) By (9.1.3) and (7.5.7), the same is true for M. ♣

9.7.10 Corollary

The ring R is semisimple if and only if R is Artinian and $J(R) = 0$.

Proof. By (9.7.9), it suffices to show that if R is semisimple, then it has a composition series. But this follows because R is finitely generated, hence is a finite direct sum of simple modules (see Section 9.3, Problem 1). ♣

The Jacobson radical of an Artinian ring has some special properties.

9.7.11 Definitions and Comments

An ideal (or left ideal or right ideal) I of the ring R is *nil* if each element $x \in I$ is nilpotent, that is, $x^m = 0$ for some positive integer m; I is *nilpotent* if $I^n = 0$ for some positive integer n. Every nilpotent ideal is nil, and the converse holds if R is Artinian, as we will prove.

9.7.12 Lemma

If I is a nil left ideal of R, then $I \subseteq J(R)$.

Proof. If $x \in I$ and $x^m = 0$, then x is quasi-regular; the inverse of $1 - x$ is $1 + x + x^2 + \cdots + x^{m-1}$. The result follows from the proof of (9.7.7). ♣

9.7.13 Proposition

If R is Artinian, then $J(R)$ is nilpotent. Thus by (9.7.11) and (9.7.12), $J(R)$ is the largest nilpotent ideal of R, and every nil ideal of R is nilpotent.

Proof. Let $J = J(R)$. The sequence $J \supseteq J^2 \supseteq \cdots$ stabilizes, so for some n we have $J^n = J^{n+1} = \cdots$, in particular, $J^n = J^{2n}$. We claim that $J^n = 0$. If not, then the collection of all left ideals Q of R such that $J^nQ \neq 0$ is nonempty (it contains J^n), hence has a minimal element N. Choose $x \in N$ such that $J^nx \neq 0$. By minimality of N, $J^nx = N$. Thus there is an element $c \in J^n$ such that $cx = x$, that is, $(1 - c)x = 0$. But $c \in J^n \subseteq J$, so by (9.7.7), $1 - c$ is invertible, and consequently $x = 0$, a contradiction. ♣

Problems For Section 9.7

1. Show that an R-module is M cyclic if and only if M is isomorphic to R/I for some left ideal I, and in this case we can take I to be $\text{ann}(M)$, the annihilator of M.
2. Show that the Jacobson radical of an R-module M is the intersection of all kernels of homomorphisms from M to simple R-modules.
3. If $I = J(R)$, show that $J(R/I) = 0$.
4. If f is an R-module homomorphism from M to N, show that $f(J(M)) \subseteq J(N)$.
5. Assume R commutative, so that $J(R)$ is the intersection of all maximal ideals of R. If $a \in R$, show that $a \in J(R)$ if and only if $1 + ab$ is a unit for every $b \in R$.
6. If N is a submodule of the Jacobson radical of the R-module M, show that $J(M)/N = J(M/N)$.

9.8 Theorems of Hopkins-Levitzki and Nakayama

From Section 7.5, we know that a Noetherian ring need not be Artinian, and an Artinian module need not be Noetherian. But the latter situation can never arise for rings, because of the following result.

9.8.1 Theorem (Hopkins and Levitzki)

Let R be an Artinian ring, and M a finitely generated R-module. Then M is both Artinian and Noetherian. In particular, with $M = R$, an Artinian ring is Noetherian.

Proof. By (7.5.9), M is Artinian. Let J be the Jacobson radical of R. By Section 9.7, Problem 3, the Jacobson radical of R/J is zero, and since R/J is Artinian by (7.5.7), it is semisimple by (9.7.9). Now consider the sequence

$$M_0 = M,\ M_1 = JM,\ M_2 = J^2M, \ldots .$$

By (9.7.13), J is nilpotent, so $M_n = 0$ for some n. Since $JM_i = M_{i+1}$, J annihilates M_i/M_{i+1}, so by Section 4.2, Problem 6, M_i/M_{i+1} is an R/J-module.

We claim that each M_i/M_{i+1} has a composition series.

We can assume that $M_i/M_{i+1} \neq 0$, otherwise there is nothing to prove. By (9.3.2), M_i/M_{i+1} is semisimple, and by (7.5.7), M_i/M_{i+1} is Artinian. [Note that submodules of M_i/M_{i+1} are the same, whether we use scalars from R or from R/J; see Section 4.2, Problem 6.] By Section 9.6, Problem 5, M_i/M_{i+1} is Noetherian, hence has a composition series by (7.5.12). Now intuitively, we can combine the composition series for the M_i/M_{i+1} to produce a composition series for M, proving that M is Noetherian. Formally, $M_{n-1} \cong M_{n-1}/M_n$ has a composition series. Since M_{n-2}/M_{n-1} has a composition series, so does M_{n-2}, by (7.5.7). Iterate this process until we reach M. ♣

We now proceed to a result that has many applications in both commutative and noncommutative algebra.

9.8.2 Nakayama's Lemma, Version 1

Let M be a finitely generated R-module, and I a two-sided ideal of R. If $I \subseteq J(R)$ and $IM = M$, then $M = 0$.

Proof. Assume $M \neq 0$, and let $x_1, \ldots, x_n$ generate M, where n is as small as possible. (Then $n \geq 1$ and the x_i are nonzero.) Since $x_n \in M = IM$, we can write $x_n = \sum_{i=1}^m b_i y_i$ for some $b_i \in I$ and $y_i \in M$. But y_i can be expressed in terms of the generators as $y_i = \sum_{j=1}^n a_{ij}x_j$ with $a_{ij} \in R$. Thus

$$x_n = \sum_{i,j} b_i a_{ij} x_j = \sum_{j=1}^n c_j x_j$$

where $c_j = \sum_{i=1}^m b_i a_{ij}$. Since I is a right ideal, $c_j \in I \subseteq J(R)$. (We need I to be a left ideal to make IM a legal submodule of M.) The above equation can be written as

$$(1 - c_n)x_n = \sum_{j=1}^{n-1} c_j x_j$$

and by (9.7.7), $1 - c_n$ is invertible. If $n > 1$, then x_n is a linear combination of the other x_i's, contradicting the minimality of n. Thus $n = 1$, in which case $(1 - c_1)x_1 = 0$, so $x_1 = 0$, again a contradiction. ♣

There is another version of Nakayama's lemma, which we prove after a preliminary result.

9.8.3 Lemma

Let N be a submodule of the R-module M, I a left ideal of R. Then $M = N + IM$ if and only if $M/N = I(M/N)$.

Proof. Assume $M = N + IM$, and let $x + N \in M/N$. Then $x = y + z$ for some $y \in N$ and $z \in IM$. Write $z = \sum_{i=1}^{t} a_i w_i$, $a_i \in I$, $w_i \in M$. It follows that

$$x + N = a_1(w_1 + N) + \cdots + a_t(w_t + N) \in I(M/N).$$

Conversely, assume $M/N = I(M/N)$, and let $x \in M$. Then

$$x + N = \sum_{i=1}^{t} a_i(w_i + N)$$

with $a_i \in I$ and $w_i \in M$. Consequently, $x - \sum_{i=1}^{t} a_i w_i \in N$, so $x \in N + IM$. ♣

9.8.4 Nakayama's Lemma, Version 2

Let N be a submodule of the R-module M, with M/N finitely generated over R. [This will be satisfied if M is finitely generated over R.] If I is a two-sided ideal contained in $J(R)$, and $M = N + IM$, then $M = N$.

Proof. By (9.8.3), $I(M/N) = M/N$, so by (9.8.2), $M/N = 0$, hence $M = N$. ♣

Here is an application of Nakayama's lemma.

9.8.5 Proposition

Let R be a commutative local ring with maximal ideal J (see (8.5.8)). Let M be a finitely generated R-module, and let $V = M/JM$. Then:

(i) V is a finite-dimensional vector space over the *residue field* $k = R/J$.

(ii) If $\{x_1 + JM, \ldots, x_n + JM\}$ is a basis for V over k, then $\{x_1, \ldots, x_n\}$ is a minimal set of generators for M.

(iii) Any two minimal generating sets for M have the same cardinality.

Proof. (i) Since J annihilates M/JM, it follows from Section 4.2, Problem 6, that V is a k-module, that is, a vector space over k. Since M is finitely generated over R, V is finite-dimensional over k.

(ii) Let $N = \sum_{i=1}^{n} Rx_i$. Since the $x_i + JM$ generate $V = M/JM$, we have $M = N + JM$. By (9.8.4), $M = N$, so the x_i generate M. If a proper subset of the x_i were to generate M, then the corresponding subset of the $x_i + JM$ would generate V, contradicting the assumption that V is n-dimensional.

(iii) A generating set S for M with more than n elements determines a spanning set for V, which must contain a basis with exactly n elements. By (ii), S cannot be minimal. ♣

Problems For Section 9.8

1. Let a be a nonzero element of the integral domain R. If $(a^t) = (a^{t+1})$ for some positive integer t, show that a is invertible.
2. Continuing Problem 1, show that every Artinian integral domain is a field.
3. If R is a commutative Artinian ring, show that every prime ideal of R is maximal.
4. Let R be a commutative Artinian ring. If $\mathcal{S}$ is the collection of all finite intersections of maximal ideals of R, then $\mathcal{S}$ is not empty, hence contains a minimal element $I = I_1 \cap I_2 \cap \cdots \cap I_n$, with the I_j maximal. Show that if P is any maximal ideal of R, then P must be one of the I_j. Thus R has only finitely many maximal ideals.
5. An R-module is *projective* if it is a direct summand of a free module. We will study projective modules in detail in Section 10.5. We bring up the subject now in Problems 5 and 6 to illustrate a nice application of Nakayama's lemma.

   Let R be a commutative local ring, and let M be a finitely generated projective module over R, with a minimal set of generators $\{x_1, \ldots, x_n\}$ (see (9.8.5)). We can assume that for some free module F of rank n,

   $$F = M \oplus N.$$

   To justify this, let F be free with basis $e_1, \ldots, e_n$, and map F onto M via $e_i \to x_i$, $i = 1, \ldots, n$. If the kernel of the mapping is K, then we have a short exact sequence

   $$0 \to K \to F \to M \to 0,$$

   which splits since M is projective. [This detail will be covered in (10.5.3).]

   Let J be the maximal ideal of R, and $k = R/J$ the residue field. Show that

   $$F/JF \cong M/JM \oplus N/JN.$$

6. Continue from Problem 5 and show that $N/JN = 0$. It then follows from Nakayama's lemma (9.8.2) that $N = 0$, and therefore $M = F$. We conclude that a finitely generated projective module over a commutative local ring is free.
7. We showed in (9.6.6) that there is no distinction between a left and a right-semisimple ring. This is not the case for Noetherian (or Artinian) rings.

   Let X and Y be *noncommuting indeterminates*, in other words, $XY \neq YX$, and let $\mathbb{Z} < X, Y >$ be the set of all polynomials in X and Y with integer coefficients. [Elements of $\mathbb{Z}$ do commute with the indeterminates.] We impose the relations $Y^2 = 0$ and $YX = 0$ to produce the ring R; formally, $R = \mathbb{Z} < X, Y > /(Y^2, YX)$.

   Consider $I = \mathbb{Z}[X]Y$, the set of all polynomials $f(X)Y$, $f(X) \in \mathbb{Z}[X]$. Then I is a two-sided ideal of R. Show that if I is viewed as a right ideal, it is not finitely generated. Thus R is not right-Noetherian.
8. Viewed as a left R-module, $R = \mathbb{Z}[X] \oplus \mathbb{Z}[X]Y$. Show that R is left-Noetherian.

9. Assume the hypothesis of (9.8.5). If $\{x_1, \ldots, x_n\}$ is a minimal generating set for M, show that $\{\overline{x}_1, \ldots, \overline{x}_n\}$, where $\overline{x}_i = x_i + JM$, is a basis for $M/JM = V$.

10. Continuing Problem 9, suppose that $\{x_1, \ldots, x_n\}$ and $\{y_1, \ldots, y_n\}$ are minimal generating sets for M, with $y_i = \sum_j a_{ij}x_j$, $a_{ij} \in R$. If A is the matrix of the a_{ij}, show that the determinant of A is a unit in R.