Structure Theory of Rings

Liam McQuay, Manya Singh, Amelie Zhou

Contents

1 Review of ring theory **2**
1.1 Monoids, groups, and rings 2
1.2 Subrings, ideals, and quotients 5
1.3 Homomorphisms and the isomorphism theorems 10

2 Modules **17**
2.1 Definition and motivation 17
2.2 Submodules and quotients 21
2.3 Hom sets and Schur's lemma 24
2.4 Direct products and sums 27

3 Structure theory of modules **35**
3.1 Noetherian and Artinian modules 35
3.2 Composition series 40
3.3 Structure of finite-length modules 47
3.4 Semisimple modules 54

4 Structure theory of rings **61**
4.1 Return of representations – primitivity and semiprimitivity 61
4.2 Measuring semiprimitivity – the Jacobson radical 67
4.3 Classifying our building blocks – the Jacobson density theorem . . . 74
4.4 Putting our blocks together – the Wedderburn-Artin theorem 80
4.5 The simple components – isomorphisms of simple Artinian rings . . 87
4.6 Finally some applications – representations of groups 90

1 Review of ring theory

In this chapter, we collect the necessary ring-theoretic notions and properties we shall need.

1.1 Monoids, groups, and rings

The definition of a ring we give here will not be the standard one. Rather, we define it in terms of two other structures we shall define now. The reason for doing this will be made apparent later.

Definition 1.1.1 A **monoid** is a pair $(M, \cdot)$ where M is a set and $\cdot : M \times M \to M$ is an operation on M satisfying the following properties:

[M1] $\cdot$ is *associative*: for every $x, y, z \in M$ we have $x \cdot (y \cdot z) = (x \cdot y) \cdot z$

[M2] M has an *identity*: there exists some $1 \in M$ satisfying $1 \cdot x = x \cdot 1 = x$ for all $x \in M$.

It's easy to check that the identity 1 is unique. We often abbreviate $x \cdot y$ to just xy if there is no ambiguity.

If M additionally satisfies the following:

[M3] M is *commutative*: for every $x, y \in M$, we have $xy = yx$.

then M is called an **abelian monoid**.

A **group** is a monoid $(G, \cdot)$ that satisfies the following property:

[G] G has *inverses*: for every $g \in G$, there exists an element $h \in G$ for which $gh = hg = 1$.

It's also easy to check that inverses are unique. That is, if $g \in G$ and $h, h' \in G$ are both inverses of g, then we must have $h = h'$.

A group which is an abelian monoid is (unsurprisingly) called an **abelian group**.

Example 1.1.2

(1) The set of natural numbers $\mathbb{N} = \{0, 1, 2, ...\}$ equipped with addition $+$ is a monoid with identity 0. Similarly $\mathbb{N}$ under multiplication $\cdot$ is a monoid with identity 1. Both of these are abelian monoids, but neither of them are groups.

(2) The set of integers $\mathbb{Z}$ is a group under addition (0 is the identity again, and the inverse of x is $-x$). $\mathbb{Z}$ is a monoid under multiplication, but not a group. Both of these structures are of course abelian.

(3) The set of $n \times n$ matrices $M_n(F)$ where F is a field. This is an abelian group under addition (identity is the zero matrix, inverse of $A \in M_n(F)$ is $-A$). This is also a monoid under the usual matrix multiplication, but not abelian when $n \geqslant 2$ and never a group, since for instance the zero matrix has no inverse.

We can however consider the set $\mathrm{GL}_n(F) = \{A \in M_n(F) : A \text{ is invertible}\}$. This is a group under multiplication, called the **general linear group** of degree n over F.

(4) Let $\mathcal{F}(X)$ be the set of functions from a set X to itself. This is a monoid under function composition; the identity being $\mathrm{id}_X \in \mathcal{F}(X)$ given by $\mathrm{id}_X(x) = x$ for all $x \in X$. This is not a group if $|X| \geqslant 2$, but we can consider $\mathrm{Sym}(X) = \{f \in \mathcal{F}(X) : f \text{ is bijective}\}$. This is a group (non-abelian generally). We call this the **symmetric group** on X.

Examples **(3)** and **(4)** illustrate something we can do in general:

Definition 1.1.3 Let $(M, \cdot)$ be a monoid. We define $M^\times = \{x \in M : \exists y \in M \text{ such that } xy = yx = 1\}$. It's easy to check that $M^\times$ is a group with identity 1. We call $M^\times$ the **group of units** of M.

Thus, we have $\mathrm{GL}_n(F) = M_n(F)^\times$ and $\mathcal{F}(X)^\times = \mathrm{Sym}(X)$.

In examples **(2)** and **(3)**, notice that we have both an abelian group structure under addition and a monoid structure under multiplication. These two structures are also "compatible" in the following sense: given x, y, z we have $x(y+z) = xy+xz$ and $(x+y)z = xz+yz$. This motivates the definition of a ring, which we formally give now.

Definition 1.1.4 A **ring** is a triple $(R, +, \cdot)$ where $+$ and $\cdot$ are binary operations on R with the following properties:

[R1] $(R, +)$ is an abelian group.

[R2] $(R, \cdot)$ is a monoid.

[R3] $\cdot$ is *distributive* over $+$: for every $a, b, c \in R$ we have $a(b+c) = ab + ac$ and $(a+b)c = ac + bc$.

If $(R, \cdot)$ is an abelian monoid, we say R is a **commutative ring**.

We call $+$ the **addition** operation and $\cdot$ the **multiplication** operation. The identity of $(R, +)$ is denoted 0 and is called the **zero element** of R. The identity of $(R, \cdot)$ is denoted 1 and is called the **identity element** of R.

So $\mathbb{Z}$ and $M_n(F)$ are both examples of rings. Here are some others.

Example 1.1.5

(1) $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are all commutative rings under the usual addition and multiplication.

(2) Let F be a field and let $F[x]$ denote the set of polynomials. Then under the usual polynomial addition and scalar multiplication, $F[x]$ is a commutative ring whose zero element is 0 and identity is 1.

(3) For $n \geqslant 0$, we define the set $\mathbb{Z}/n\mathbb{Z}$ of *integers modulo* n to be equivalence classes of $\mathbb{Z}$ under the relation $\equiv_n$ given by $a \equiv_n b$ if and only if $n \mid a - b$. Let $[a] \in \mathbb{Z}/n\mathbb{Z}$ denote the equivalence class of $a \in \mathbb{Z}$ (explicitly, $[a] = \{a + nk : k \in \mathbb{Z}\}$). Then we define addition and multiplication as follows:

$$[a] + [b] = [a + b] \quad \text{and} \quad [a] \cdot [b] = [ab]$$

One can check this gives $\mathbb{Z}/n\mathbb{Z}$ a well-defined ring structure, where $[0]$ is the zero and $[1]$ is the identity.

(4) If we view $M_n(F)$ as linear operators on the vector space F^n, then we can make the following generalization: if V is any vector space over F, let $\mathrm{End}_F(V)$ be the set of linear operators on V (that is, linear maps from V to itself). Define addition and multiplication as follows: for $S, T \in \mathrm{End}_F(V)$, set

$$(S+T)v = Sv + Tv \quad \text{and} \quad (ST)v = S(Tv)$$

for all $v \in V$. It's easy to check that we have $S+T$ and ST are both linear maps (elements of $\mathrm{End}_F(V)$). Moreover, the zero map $0v = 0$ and the identity map $Iv = v$ give the zero and identity elements, respectively. Hence, $\mathrm{End}_F(V)$ is a ring, called the **ring of (linear) endomorphisms** on V.

We now fix a ring R for the rest of the chapter.

The point of taking $(R, \cdot)$ to be a monoid instead of a group should be apparent from the following observation: if it was a group, then we would need 0 to have an inverse; that is, there must be a $b \in R$ with $0 \cdot b = b \cdot 0 = 1$. But notice that $0 \cdot b = (0+0) \cdot b = 0 \cdot b + 0 \cdot b$, which means $0 \cdot b = 0$. Thus, we would need to have $0 = 1$. But this would mean for any $a \in R$, $a = 1 \cdot a = 0 \cdot a = 0$, so $R = \{0\}$. We often call $\{0\}$ the **zero ring**, and abbreviate to just 0.

As we did with monoids though, we can consider those elements of R which have inverses.

Definition 1.1.6 The **group of units** of R, denoted $R^\times$, is defined to simply be the group of units of the monoid $(R, \cdot)$. That is,

$$R^\times = \{u \in R : \exists v \in R \text{ such that } uv = vu = 1\}$$

R is called a **division ring** when $R^\times = R \setminus \{0\}$ (notice that this automatically excludes the case $R = \{0\}$; this is not a division ring). If R is both commutative and a division ring, we say R is a **field**.

Thus, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are examples of fields. What examples of non-commutative division rings do we have?

Example 1.1.7 Consider the set $\mathbb{H}$ of **quaternions**. These are defined to be expressions of the form $a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}$ where $a, b, c, d \in \mathbb{R}$ and $\boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}$ are elements that satisfy the relations $\boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = \boldsymbol{ijk} = -1$. One can think of this as an extension of the complex numbers $\mathbb{C}$, where we introduce two more "basis" elements $\boldsymbol{j}$ and $\boldsymbol{k}$ satisfying the given relations. With the relations, we define addition and multiplication the "natural" way, and this has the structure of a division ring. This is not commutative however, since for instance $\boldsymbol{ij} = \boldsymbol{k}$ but $\boldsymbol{ji} = -\boldsymbol{k}$.

A formal construction of $\mathbb{H}$ as well as the verification of the fact that it's a division ring is given in **Exercise 1.4.3** at the end of the chapter.

1.2 Subrings, ideals, and quotients

We next consider what it means for a substructure to sit inside a larger one. First, we have:

Definition 1.2.1 Let $(M, \cdot)$ be a monoid. A **submonoid** of M is a subset $N \subseteq M$ for which:

[SM1] N is closed under $\cdot$: for each $x, y \in N$, we have $xy \in N$.

[SM2] N contains the identity: we have $1 \in N$ where 1 is the identity in M.

It's easy to see then that $(N, \cdot)$ is itself a monoid in its own right, with identity coming from M. If N also satisfies

[SG] N contains inverses: for each $x \in N$, there exists $y \in N$ for which $xy = yx = 1$,

then N is called a **subgroup** of M. In this case $(N, \cdot)$ is a group in its own right.

With this, we make the following

Definition 1.2.2 A **subring** of R is a subset S of R such that:

[SR1] $(S, +)$ is a subgroup of $(R, +)$.

[SR2] $(S, \cdot)$ is a submonoid of $(R, \cdot)$.

In this case it's clear that $(S, +, \cdot)$ is a ring in its own right.

Example 1.2.3

(1) Consider the ring $M_n(F)$ and define:

$$T_n(F) = \{A \in M_n(F) : A \text{ is upper triangular}\}$$

$$D_n(F) = \{A \in M_n(F) : A \text{ is diagonal}\}$$

We see that $D_n(F) \subseteq T_n(F) \subseteq M_n(F)$. Both $T_n(F)$ and $D_n(F)$ are easily checked to be subrings of $M_n(F)$.

(2) The only subring of $\mathbb{Z}$ is $\mathbb{Z}$ itself. Indeed, suppose S is a subring of $\mathbb{Z}$. Then we need both $0, 1 \in S$. By closure under $+$, this means $n \in S$ for each $n \geqslant 1$ as well. By closure under $-$, we must also have $-n \in S$ for each $n \geqslant 1$. Hence, $S = \mathbb{Z}$.

A similar argument shows the only subring of $\mathbb{Z}/n\mathbb{Z}$ is $\mathbb{Z}/n\mathbb{Z}$.

(3) $\mathbb{Z}$ is a subring of $\mathbb{Q}$, $\mathbb{Q}$ is a subring of $\mathbb{R}$, and $\mathbb{R}$ is a subring of $\mathbb{C}$. If we consider the quaternions $\mathbb{H} = \{a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k} : a, b, c, d \in \mathbb{R}\}$ and identify $\mathbb{C}$ with $\{a + b\boldsymbol{i} : a, b \in \mathbb{R}\} \subseteq \mathbb{H}$, then $\mathbb{C}$ is a subring of $\mathbb{H}$.

(4) Let $\mathbb{Q}[\sqrt{2}] = \{p + q\sqrt{2} : p, q \in \mathbb{Q}\}$. Then $\mathbb{Q}[\sqrt{2}]$ is a subring of $\mathbb{R}$.

Given a subset $X \subseteq R$, one can consider the smallest subring of R which contains all the elements of X.

Definition 1.2.4 Let $X \subseteq R$ and let $\mathcal{S}$ denote the collection of subrings of R. The **subring generated by X** is defined to be:

$$\langle X \rangle = \bigcap_{\substack{S \in \mathcal{S} \\ X \subseteq S}} S$$

It's routine to check that this is indeed a subring. If we have $x_1, ..., x_n \in R$, we often write $\langle x_1, ..., x_n \rangle$ instead of $\langle \{x_1, ..., x_n\} \rangle$.

We next consider another type of substructure of R; one similar to that of a subring, but where:

- we drop the condition that the multiplicative structure be a submonoid of $(R, \cdot)$, and
- we replace it with closure under multiplication on the left or right by any element of R.

Let us make this more precise.

Definition 1.2.5 An **ideal** of R is a subset $I \subseteq R$ such that:

[I1] $(I, +)$ is a subgroup of $(R, +)$.

[I2] For every $a \in R$ and $x \in I$, we have $ax \in I$ and $xa \in I$.

Later, we will see the notions of *left* and right ideals. In this situation, we often call an ideal in the sense described above a **two-sided ideal** to distinguish between them.

By dropping the submonoid condition, ideals need not contain 1. Hence, this more often than not captures more examples of substructures than that of subrings.

Definition 1.2.6 Let $X \subseteq R$ and let $\mathcal{I}$ denote the collection of ideals of R. The **ideal generated by X** is defined to be:

$$(X) = \bigcap_{\substack{I \in \mathcal{I} \\ X \subseteq I}} I$$

Like with the subring analogue, it's also easy to check this is an ideal. Likewise if we have $x_1, ..., x_n \in R$, we often write $(x_1, ..., x_n)$ instead of $(\{x_1, ..., x_n\})$. If I is an ideal such that $I = (x)$ for some $x \in R$, we call I a **principal ideal**.

Example 1.2.7

(1) In any ring, we always have the zero ideal $\{0\} = 0$. On the other extreme, suppose I is an ideal with $1 \in I$. Then for any $a \in R$, we have $a = a \cdot 1 \in I$, which means $I = R$. In particular, R is a principal ideal since $R = (1)$.

(2) Given $n \in \mathbb{Z}$, we have the ideal $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$ of all multiples of n. Clearly we have $(n) = n\mathbb{Z}$, and we shall adopt this notation henceforth.

In fact, all ideals of $\mathbb{Z}$ are principal (see **Exercise 1.4.11**).

(3) The polynomial ring $F[x]$ is also an example of a ring in which every ideal is principal. We shall have here that for any $p \in F[x]$, $(p(x)) = \{p(x)h(x) : h \in F[x]\}$.

(4) Let F be a field and suppose I is an ideal of F. If $I \neq 0$, then there is some $0 \neq c \in I$. Now $1 = \frac{1}{c}c \in I$, which means $I = F$. Therefore, the only ideals of F are 0 and F.

(5) The same is true for division rings.

(6) Let I be an ideal of $M_n(F)$ and assume $I \neq 0$. Then there is a non-zero matrix $A = (\alpha_{ij}) \in I$. Suppose $\alpha_{kl} \neq 0$. If E_{ij} denotes the matrix with 1 in the (i, j) position and 0's elsewhere, then we have $\alpha_{kl}E_{kl} = E_{kk}AE_{ll} \in I$. Now $E_{kl} = (\frac{1}{\alpha_{kl}}I)(\alpha_{kl}E_{kl}) \in I$. Applying appropriate row/column operations to E_{kl} shows in general that $E_{ij} \in I$ for all $1 \leqslant i, j \leqslant n$. This must imply $I = M_n(F)$. Therefore, the only ideals of $M_n(F)$ are 0 and $M_n(F)$.

(7) The same is true for $M_n(D)$ if D is a division ring.

The last two examples illustrate the following notion:

Definition 1.2.8 A **simple ring** is a ring R in which $R \neq 0$ and the only ideals are 0 and R.

Let us view some operations on ideals. As part of the verification of the fact that (X) is an ideal for any $X \subseteq R$, we know that the intersection of a given set of ideals is an ideal. It's not true in general that the union of ideals is an ideal. We can however look at the smallest ideal containing this union.

Definition 1.2.9 Let I and J be ideals. We define their **sum** to be

$$I + J = (I \cup J)$$

In general if $\mathcal{J}$ is some set of ideals, we define the sum of the ideals in $\mathcal{J}$ to be:

$$\sum_{J \in \mathcal{J}} J = \left(\bigcup_{J \in \mathcal{J}} J \right)$$

It's often useful to give a more explicit description of (X) – one where if we know what the elements of X are, we know what the elements (X) are.

Proposition 1.2.10 Let $X \subseteq R$. Then:

$$(X) = \left\{ \sum_i a_i x_i b_i : x_i \in X, a_i, b_i \in R \right\}$$

(the sum above is assumed to be finite, of course). In particular, suppose $X = \{x_1, ..., x_n\}$. Then:

$$(x_1, ..., x_n) = \left\{ \sum_{i_1} a_{i_1} x_1 b_{i_1} + \cdots + \sum_{i_n} a_{i_n} x_n b_{i_n} : a_j, b_j \in R \right\}$$

Proof. It is clear that any sum of the form $\sum_i a_i x_i b_i$ described above indeed lies in (X). On the other hand, the set of such sums is easily verified to be an ideal which contains all elements of X. Hence, we have equality. □

We can simplify this description in the case where R is commutative:

$$(X) = \left\{ \sum_i a_i x_i : x_i \in X, a_i \in R \right\}$$

What does this explicit description allow us to do? Here's one thing we obtain from this:

Corollary 1.2.11 If I and J are ideals, then:

$$I + J = \{x + y \in R : x \in I, y \in J\}$$

More generally if $\mathcal{J}$ is a set of ideals, then:

$$\sum_{J \in \mathcal{J}} J = \left\{ \sum_{i=1}^{n} x_i : x_i \in \bigcup_{J \in \mathcal{J}} J \right\}$$

The proof is evident when we consider the fact that any $a_i x_i b_i \in J$ whenever $x_i \in J$.

We've seen that simple rings need not be fields, or even division rings for that matter. But if we add the commutativity assumption, we have:

Proposition 1.2.12 A commutative ring R is simple if and only if it is a field.

Proof. If R is simple, let $0 \neq x \in R$. Then $(x) \neq 0$ which forces $(x) = R$. Therefore, $1 \in (x)$ which means $1 = \sum_{i=1}^{n} a_i x b_i$ for some $a_i, b_i \in R$. Since R is commutative, we have:

$$1 = \sum_{i=1}^{n} a_i b_i x = \left(\sum_{i=1}^{n} a_i b_i \right) x = x \left(\sum_{i=1}^{n} a_i b_i \right)$$

which means $x \in R^\times$. This shows R is indeed a field. Conversely, we've already seen that fields are simple. □

Example 1.2.13 Let's see what the operations $\cap$ and $+$ do on the ideals of $\mathbb{Z}$. We use the fact that every ideal of $\mathbb{Z}$ is principal (**Exercise 1.4.11**).

Suppose $a, b \in \mathbb{Z}$ and look at $(a) \cap (b) = \{c \in \mathbb{Z} : c = ak = bl \text{ for some } k, l \in \mathbb{Z}\}$. Then certainly $\text{lcm}(a, b) \in (a) \cap (b)$ so that $(\text{lcm}(a, b)) \subseteq (a) \cap (b)$. On the other hand,

any element of $(a)\cap(b)$ is a common multiple of a and b, which means each $c \in (a)\cap(b)$ can be written as $c = \text{lcm}(a,b)k$ for some $k \in \mathbb{Z}$. Thus, $(a) \cap (b) = (\text{lcm}(a,b))$.

Now we look at $(a) + (b) = (a,b)$. Any element of the form $ak + bl$ for $k, l \in \mathbb{Z}$ is in (a,b). By Bézout's lemma, there are $k, l \in \mathbb{Z}$ with $\gcd(a,b) = ak + bl \in (a,b)$, which means $(\gcd(a,b)) \subseteq (a,b)$. Now since $\mathbb{Z}$ is commutative, any element of (a,b) is of the form $ak+bl$ for $k, l \in \mathbb{Z}$, and this is divisible by $\gcd(a,b)$. Thus, $ak+bl \in (\gcd(a,b))$, which shows $(a) + (b) = (\gcd(a,b))$.

Given a ring R, an ideal I induces a relation $\equiv$ on R defined as follows: for each $a, b \in R$, we have $a \equiv b$ if and only if $a - b \in I$. It's routine to check this is an equivalence relation on R. Moreover, $\equiv$ preserves the ring structure in the following sense: if $a \equiv a'$ and $b \equiv b'$ in R, then $a + b \equiv a' + b'$ and $ab \equiv a'b'$. This comes from the fact that I is an ideal. We say that $\equiv$ is a *congruence relation* on R.

Conversely, every congruence relation $\equiv$ on R determines uniquely a corresponding ideal $I = \{a \in R : a \equiv 0\}$. We thus have a bijective correspondence between ideals of R and congruence relations on R.

Definition 1.2.14 Let I be an ideal of R and let $R/I = \{\overline{a} : a \in R\}$ be the set of congruence classes of the relation determined by I. That is, $\overline{a} = \{b \in R : b - a \in I\}$. Then R/I has the structure of a ring defined as follows:

$$\overline{a} + \overline{b} = \overline{a + b} \quad \text{and} \quad \overline{a} \cdot \overline{b} = \overline{ab}$$

The zero element is $\overline{0}$ and the identity is $\overline{1}$. We call R/I the **quotient ring** of R by I.

To describe explicitly an equivalence class, notice that

$$\overline{a} = \{b \in R : b - a \in I\} = \{a + b' : b' \in I\} = a + I$$

We shall thus adopt the notation of $a + I$ for an equivalence class rather than $\overline{a}$. The zero element of R/I will often be denoted I or 0.

Example 1.2.15 The prototypical example of a quotient ring is $\mathbb{Z}/n\mathbb{Z}$. Here the ideal determining this quotient is (n). We shall henceforth write $\mathbb{Z}/n\mathbb{Z}$ as $\mathbb{Z}/(n)$.

Let us view some other examples.

Example 1.2.16

(1) If $I = 0$, then R/I can be identified with R, since $a \equiv b$ if and only if $a - b \in I$ if and only if $a = b$. If $I = R$, then R/R can be identified with the zero ring 0, since $a \equiv b$ if and only if $a - b \in R$, which is always true.

(2) Consider $\mathbb{R}[x]$, a ring in which every ideal is principal. We shall consider an explicit example: $(x^2 + 1) = \{(x^2 + 1)h(x) : h \in \mathbb{R}[x]\}$. In $C = \mathbb{R}[x]/(x^2 + 1)$, we have $f + (x^2 + 1) = g + (x^2 + 1)$ if and only if $f - g$ has $x^2 + 1$ as a factor. By polynomial division, we can write $f(x) = (x^2+1)p(x)+r(x)$ for some $p, r \in \mathbb{R}[x]$ with $\deg(r) \leqslant 1$. Similarly $g(x) = (x^2 + 1)q(x) + s(x)$ for some $q, s \in \mathbb{R}[x]$

with $\deg(s) \leqslant 1$. Now $f(x) - g(x) = (x^2+1)(p(x) - q(x)) + (r(x) - s(x))$ and this is divisible by $x^2 + 1$. Therefore, $r(x) - s(x)$ is divisible by $x^2 + 1$. But since $\deg(r - s) \leqslant 1$, it must follow that $r = s$. Therefore, each equivalence class of $f \in \mathbb{R}[x]$ in the quotient ring has a *unique* representative $r \in \mathbb{R}[x]$ with $\deg(r) \leqslant 1$.

We may therefore identify the elements of C as polynomials of the form $ax + b$ for $a, b \in \mathbb{R}$. The addition is the usual one, in which $(ax + b) + (cx + d) = (a + c)x + (b + d)$. But notice that since $x^2 \equiv -1$, we have $(ax + b)(cx + d) = acx^2 + (ad + bc)x + bd \equiv (ad + bc)x + (bd - ac)$. Therefore, we can define multiplication on C by $(ax + b)(cx + d) = (ad + bc)x + (bd - ac)$. This ring's behavior corresponds precisely to that of the complex numbers $\mathbb{C}$. We shall defined this correspondence more formally later.

(3) Let R be a commutative ring. An element $z \in R$ is **nilpotent** when $z^n = 0$ for some $n \geqslant 1$. The **nilradical** is the set $\mathcal{N}(R) = \{z \in R : z \text{ is nilpotent}\}$.

Let $z_1, z_2 \in \mathcal{N}(R)$ and and $a \in R$. Notice $0 \in \mathcal{N}(R)$ so it's non-empty. Also, the fact that R is commutative gives us:

$$(z_1 + z_2)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} z_1^k z_2^k = 0$$

and clearly $(-z_1)^n = 0$, so $\mathcal{N}(R)$ is a subgroup of $(R, +)$. Commutativity also implies $(az_1)^n = a^n z_1^n = 0 = (z_1 a)^n$. Thus, $\mathcal{N}(R)$ is indeed an ideal.

The quotient ring $R/\mathcal{N}(R)$ then contains no non-zero nilpotent elements. Indeed, if $a + \mathcal{N}(R)$ is nilpotent in $R/\mathcal{N}(R)$, then we have $(a + \mathcal{N}(R))^n = a^n + \mathcal{N}(R) = 0 + \mathcal{N}(R)$ for some $n \geqslant 1$. But this means $a^n \in \mathcal{N}(R)$, so $(a^n)^k = a^{nk} = 0$ for some $k \geqslant 1$; in particular, $a \in \mathcal{N}(R)$. Thus, $a + \mathcal{N}(R) = \mathcal{N}(R)$ (the zero element of $R/\mathcal{N}(R)$).

1.3 Homomorphisms and the isomorphism theorems

We next investigate "structure-preserving" maps between two objects with the same structure.

Definition 1.3.1 Let M and N be monoids. A **(monoid) homomorphism** from M to N is a map $f : M \to N$ such that $f(xy) = f(x)f(y)$ and $f(1) = 1$. If G and H are groups, we define a **(group) homomorphism** to be a monoid homomorphism $f : G \to H$.

Remark 1.3.2 In fact, if G and H are groups, suppose $f : G \to H$ satisfies $f(gh) = f(g)f(h)$ for all $g, h \in G$ (so we don't assume $f(1) = 1$). Then $f(g) = f(1 \cdot g) = f(1)f(g)$, which implies $f(g)f(g)^{-1} = f(1)f(g)f(g)^{-1}$ so that $f(1) = 1$. Moreover, $f(g)f(g^{-1}) = f(gg^{-1}) = f(1) = 1$ and similarly $f(g^{-1})f(g) = 1$. Hence, $f(g^{-1}) = f(g)^{-1}$.

Now let R and S be rings.

Definition 1.3.3 A **(ring) homomorphism** from R to S is a map $f : R \to S$ such that:

[RH1] f is a group homomorphism from $(R, +)$ to $(S, +)$.

[RH2] f is a monoid homomorphism from $(R, \cdot)$ to $(S, \cdot)$.

In other words, f is a map such that for all $x, y \in R$:

- $f(x + y) = f(x) + f(y)$,
- $f(xy) = f(x)f(y)$,
- $f(1) = 1$.

If f is bijective (injective and surjective), we say f is an **isomorphism** and that R and S are **isomorphic**. We write $R \cong S$ to denote this.

We have the following to determine if a homomorphism is injective or surjective:

Definition 1.3.4 For a homomorphism $f : R \to S$, we define

- the **kernel** to be $\ker f = \{a \in R : f(a) = 0\}$,
- the **image** to be $\operatorname{im} f = \{f(a) : a \in R\}$.

It's easy to check that $\ker f$ is an ideal of R and $\operatorname{im} f$ is a subring of S. Moreover, f is injective if and only if $\ker f = 0$ and surjective if and only if $\operatorname{im} f = S$.

Example 1.3.5

(1) Let I be an ideal of R. Then we have the quotient map $q : R \to R/I$ taking $a \in R$ to its equivalence class $a + I$. It's easy to check this is indeed a homomorphism. Moreover, this is surjective.

(2) The map $f : \mathbb{Z} \to \mathbb{Q}$ taking $n \in \mathbb{Z}$ to $n = \frac{n}{1} \in \mathbb{Q}$ is an injective homomorphism.

(3) Let F be a field and let $f : F \to R$ be a ring homomorphism, $R \neq 0$. For any $0 \neq a \in F$ we have $1 = f(1) = f(aa^{-1}) = f(a)f(a^{-1})$ and in particular $f(a) \neq 0$ since $R \neq 0$. Thus, $\ker f = 0$, so f is injective. We also see that for $a \neq 0$, $f(a)$ is invertible in R with inverse $f(a)^{-1} = f(a^{-1})$. Hence, $\operatorname{im} f$ is a *subfield* of R (a subring which is also a field).

A consequence of this is any homomorphism between two fields is necessarily injective. The same is true for division rings.

Next we consider the isomorphism theorems.

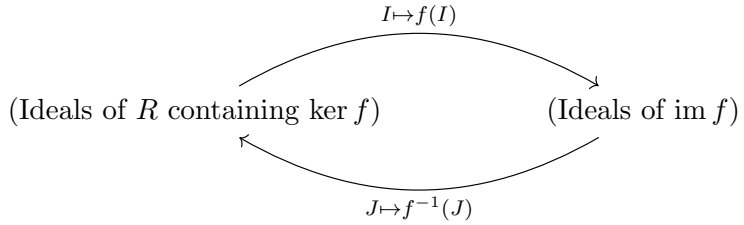
Theorem 1.3.6 (First isomorphism theorem)
Let $f : R \to S$ be a homomorphism and let $q : R \to R/\ker f$ be the quotient map. Then there exists a unique map $\overline{f} : R/\ker f \to S$ satisfying $\overline{f} \circ q = f$.

Moreover, $\overline{f}$ is injective and therefore induces an isomorphism $R/\ker f \cong \operatorname{im} f$.

Proof. Routine. □

One also has a correspondence theorem between ideals of R containing $\ker f$ and the ideals of $\operatorname{im} f$.

Theorem 1.3.7 (Correspondence theorem)
Let $f : R \to S$ be a homomorphism. Then there is a bijective correspondence between the ideals of R which contain $\ker f$ with the ideals of $\operatorname{im} f$:



As a consequence, there is a bijective correspondence between the ideals of R containing $\ker f$ and the ideals of $R/\ker f$.

Proof. Let I be an ideal containing $\ker f$. We check that $f(I)$ is indeed an ideal of $\operatorname{im} f$. Certainly $0 \in f(I)$. Given $x, y \in f(I)$ we have $x = f(a)$ and $y = f(b)$ for $a, b \in I$. Then $a + b$ and $-a$ are in I, so $f(a) + f(b) = f(a + b) \in f(I)$ and $-f(a) = f(-a) \in I$. Also if $z \in \operatorname{im} f$ with $z = f(c)$ then $ca \in I$, so $zx = f(c)f(a) = f(ca) \in f(I)$.

Now we show $f(I)$ is uniquely determined. Suppose I' is another ideal containing $\ker f$ with $f(I) = f(I')$. If $a \in I$ then $f(a) \in f(I) = f(I')$, which means $f(a) = f(a')$ for some $a' \in I'$. But then $a' - a \in \ker f \subseteq I \cap I'$, thus $a' = (a' - a) + a \in I$, which shows $I \subseteq I'$. A similar argument gives the other inclusion, so $I = I'$ and thus $f(I)$ is uniquely determined.

Finally, we show that any ideal J of $\operatorname{im} f$ is of the form $J = f(I)$ for an ideal I of R containing $\ker f$ and that $f^{-1}(J) = I$. Indeed, if J is such an ideal and we set $I = f^{-1}(J)$, it's an easy verification that I is an ideal. Moreover, $0 \in J$ means that $\ker f = f^{-1}(0) \subseteq I$. Clearly $f(I) = J$, so we're done.

The last statement is obtained by identifying $\operatorname{im} f$ with R/I using the first isomorphism theorem. □

We also have the second and third isomorphism theorems for rings, which we state without proof.

Theorem 1.3.8 (Second isomorphism theorem)
Let S be a subring of R and let I be an ideal of R. Then

(i) $S + I = \{a + x : a \in S, x \in I\}$ is a subring of R which has I as an ideal;

(ii) $S \cap I$ is an ideal of S;

(iii) $(S + I)/I \cong S/(S \cap I)$.

Theorem 1.3.9 (Third isomorphism theorem)
Let I and J be ideals of R with $J \subseteq I$. Then

(i) $I/J = \{x + J \in R/J : x \in I\}$ is an ideal of R/J. Moreover, every ideal of R/J is of the form I'/J where I' is an ideal of R containing J.

(ii) $(R/J)/(I/J) \cong R/I$.

Example 1.3.10 Let's use the first isomorphism theorem to make **Example 1.2.16 (2)** more precise. Define a map $\varphi : \mathbb{R}[x] \to \mathbb{C}$ by $\varphi(f) = f(\boldsymbol{i})$ for all $f \in \mathbb{R}[x]$. It's easy to check that this is indeed a ring homomorphism. Moreover, this is surjective since any $z = a + b\boldsymbol{i} \in \mathbb{C}$ has that $\varphi(a + bx) = z$.

Now clearly $f(x^2 + 1) = 0$, and therefore $(x^2 + 1) \subseteq \ker \varphi$. On the other hand, if $f \in \ker \varphi$ so that $f(\boldsymbol{i}) = 0$, then f has $\boldsymbol{i}$ as a root. But since $f \in \mathbb{R}[x]$, f must also have $-\boldsymbol{i}$ as a root by the conjugate root theorem. Therefore, f must have $x^2 + 1$ as a factor, which means precisely that $f \in (x^2 + 1)$. This shows $\ker \varphi = (x^2 + 1)$, so the first isomorphism theorem yields $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$.

Exercises

You are strongly encouraged to work on at least a few of the following exercises after reading through the chapter. Since this is review material, it shouldn't take long to get through most of these exercises. Some of them are hard though – these ones have been marked.

This section will also introduce some new stuff for the exercises. Let R be a ring.

Definition 1.4.1 A **chain of ideals** is a collection $\mathcal{C}$ of ideals such that for any $I, J \in \mathcal{C}$, either $I \subseteq J$ or $J \subseteq I$.

It was pointed out that it isn't generally true that the union of ideals is also an ideal. But if we take the union of an *ascending chain*, it will be.

Exercise 1.4.2 Show that if $\mathcal{C}$ is a chain of ideals of R, then $\bigcup_{I \in \mathcal{C}} I$ is an ideal of R.

The next exercise gives a construction for the division ring $\mathbb{H}$ considered in **Example 1.1.7**

Exercise 1.4.3 Consider the ring $M_2(\mathbb{C})$ and define:

$$1 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \quad \boldsymbol{i} = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \quad \boldsymbol{j} = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \quad \boldsymbol{k} = \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}$$

in $M_2(\mathbb{C})$. We define $\mathbb{H} = \{a1 + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k} : a, b, c, d \in \mathbb{R}\}$.

(a) Verify that $\boldsymbol{i}^2 = \boldsymbol{j}^2 = \boldsymbol{k}^2 = \boldsymbol{ijk} = -1$.

(b) Show that $\mathbb{H}$ is a subring of $M_2(\mathbb{C})$. It may help to view $\{1, \boldsymbol{i}, \boldsymbol{j}, \boldsymbol{k}\}$ as a basis of $\mathbb{H}$ as an $\mathbb{R}$-vector space.

(c) Use the properties of matrix determinants to show that $\mathbb{H}$ is in fact a division ring and that it's non-commutative.

Definition 1.4.4 The **characteristic** of R, denoted $\text{char}(R)$, is defined as follows:

- If there exists an $m \geqslant 1$ for which $m \cdot 1 = \overbrace{1 + \cdots + 1}^{m \text{ times}} = 0$ in R, then $\text{char}(R) = \min\{m \geqslant 1 : m \cdot 1 = 0\}$.
- Otherwise, $\text{char}(R) = 0$.

For example, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ all have characteristic 0. $\mathbb{Z}/(n)$ has characteristic n. If F is a field of characteristic p, then $M_n(F)$ also has characteristic p.

Exercise 1.4.5 Show that any simple ring must have characteristic p for some prime number p. Conclude that this is therefore true for fields.

We consider next the following notion:

Definition 1.4.6 Let $\mathcal{S}$ denote the set of all subrings of a ring R. The **prime subring** of R is defined to be:

$$R_0 = \bigcap_{S \in \mathcal{S}} S$$

We've seen that the intersection of a collection subrings is indeed a subring. R_0 is therefore the *smallest* subring of R.

Exercise 1.4.7 Let $C(R) = \{x \in R : xy = yx \text{ for all } y \in R\}$. This is called the **center** of the ring R.

(a) Show that $C(R)$ is a commutative subring of R.

(b) Conclude that R_0 is always commutative.

(c) Show that if R is a simple ring, then $C(R)$ is a field.

One example of a ring with the property that $R_0 = R$ is the integers $\mathbb{Z}$. Of course, some examples such as $M_2(F)$ show that we don't always have $R_0 \neq R$. Next we will show that we are pretty restricted as to what R_0 may be.

Exercise 1.4.8

(a) Show that if R is a ring of characteristic n, then $R_0 \cong \mathbb{Z}/(n)$.

(b) Hence deduce that if R is any ring of characteristic n whose only subring is R, then it must be isomorphic to $\mathbb{Z}/(n)$ (in particular, notice that $\mathbb{Z}/(0) \cong \mathbb{Z}$).

For any ring R, we let $M_n(R)$ denote the set of $n \times n$ matrices with entries in R. This is a ring under the usual addition and multiplication (defined similarly to $M_n(F)$). We have seen that $M_n(F)$ is a simple ring for F a field.

Exercise 1.4.9 Show that for any ideal I of R, the set $M_n(I)$ of $n \times n$ matrices with entries in I is an ideal of $M_n(R)$. Conversely show that *every* ideal of $M_n(R)$ is of the form $M_n(I)$ for I an ideal of R, so there is a bijective correspondence between the ideals of R and the ideals of $M_n(R)$. Conclude from this that R is simple if and only if $M_n(R)$ is simple.

(Hint: for the converse, look at **Example 1.2.7 (6)** and try something similar.)

Definition 1.4.10 Let K be a *commutative* ring. An element $z \in K$ is called a **zero divisor** when there exists a *non-zero* element $w \in K$ with $zw = 0$. If $K \neq 0$ and K has no non-zero zero divisors, we say K is an **integral domain**.

If K is an integral domain in which every ideal is principal, we say K is a **principal ideal domain** (or **PID**).

Exercise 1.4.11

(a) Use the fact that $\text{char}(\mathbb{Z}) = 0$ to show that $\mathbb{Z}$ is an integral domain.

(b) Show also that every ideal of $\mathbb{Z}$ is principal, thus $\mathbb{Z}$ is a PID.

(c) Show similarly that $F[x]$ is a PID for F a field.

Definition 1.4.12 An ideal I of R is called **maximal** when $I \neq R$ and if $J \supseteq I$ is another ideal of R, then either $J = I$ or $J = R$.

Exercise 1.4.13

(a) Show that the set $\{(p) : p \in \mathbb{Z},\ p \text{ prime}\}$ is the complete set of maximal ideals of $\mathbb{Z}$.

(b) What are the maximal ideals of $\mathbb{C}[x]$? What about $\mathbb{R}[x]$?

Exercise 1.4.14 Let K be a commutative ring.

(a) Show that K is a field if and only if 0 is a maximal ideal of K.

(b) Hence show that if I is a maximal ideal of K, then K/I is a field.

We recall the following lemma of Zorn:

Lemma 1.4.15 (Zorn)
Let $(P, \leq)$ be a poset. A **chain** in P is a collection $\mathcal{C} \subseteq P$ such that for every $x, y \in \mathcal{C}$, either $x \leq y$ or $y \leq x$ (this is analogous to the definition given for ideals in **Definition 1.4.1**).

If P is such that every non-empty chain $\mathcal{C}$ has an upper bound in P – that is, an element $u \in P$ satisfying $x \leq u$ for all $x \in \mathcal{C}$ – then P itself has an upper bound.

Exercise 1.4.16 Use Zorn's lemma to show that every non-zero ring has a maximal ideal.

---

*The following exercises are considered **hard**.*

Definition 1.4.17 An element $a \in R$ is called **quasiregular** when $1 - a$ is invertible.

Exercise 1.4.18 Show that for any $a, b \in R$, ab is quasiregular if and only if ba is quasiregular.

Definition 1.4.19 Let $u \in R$. A **left (right) inverse** for u is an element $v \in R$ for which $uv = 1$ ($vu = 1$).

Exercise 1.4.20 Let $u \in R$ be such that u has a right inverse. Show that the following are equivalent:

(a) u has more than one right inverse;

(b) u is not invertible;

(c) there exists $0 \neq z \in R$ with $uz = 0$.

Moreover, show that if one of the conditions above hold, then u must in fact have *infinitely-many* right inverses.

Exercise 1.4.21 (Hua's identity)
Suppose $u, v \in R^\times$ are such that uv is quasiregular. Show that $u - v^{-1}$ is invertible and that $(u - v^{-1})^{-1} - u^{-1}$ is invertible. Use this to prove Hua's identity:

$$((u - v^{-1})^{-1} - u^{-1})^{-1} = uvu - u$$

Definition 1.4.22 An **antihomomorphism** from a ring R to a ring S is a map $f : R \to S$ such that:

(i) f is a group homomorphism of $(R, +)$ to $(S, +)$;

(ii) $f(1) = 1$;

(iii) $f(ab) = f(b)f(a)$ for all $a, b \in R$.

Exercise 1.4.23 (Hua's theorem)
Let D_1 and D_2 be division rings and let $\sigma : D_1 \to D_2$ be a function satisfying the following properties for all $a, b \in D_1$:

(i) $\sigma(a + b) = \sigma(a) + \sigma(b)$;

(ii) $\sigma(1) = 1$;

(iii) if $a \neq 0$, we have $\sigma(a) \neq 0$ and $\sigma(a^{-1}) = \sigma(a)^{-1}$.

Use Hua's identity to show that σ is either a homomorphism or an antihomomorphism.

2 Modules

Here we introduce *modules*, which will play a central role in the structure theory of rings.

2.1 Definition and motivation

Let R be a ring.

Definition 2.1.1 A **left R-module** is an abelian group $(M, +)$ (with identity 0) together with a left action $\cdot : R \times M \to M$ of R on M satisfying the following properties for all $x, y \in M$ and $a, b \in R$:

[LM1] $1 \cdot x = x$,

[LM2] $a \cdot (b \cdot x) = (ab) \cdot x$,

[LM3] $a \cdot (x + y) = a \cdot x + a \cdot y$,

[LM4] $(a + b) \cdot x = a \cdot x + b \cdot x$.

We shall often abbreviate $a \cdot x$ to just ax when appropriate.

One can think of an R-module as a vector space over a ring instead of a field. We can also make a similar definition for *right* R-modules:

Definition 2.1.2 A **right R-module** is an abelian group $(M, +)$ together with a right action $\cdot : M \times R \to M$ satisfying the following properties for all $x, y \in M$ and $a, b \in R$:

[RM1] $x \cdot 1 = x$,

[RM2] $(xb)a = x(ba)$,

[RM3] $(x + y)a = xa + ya$,

[RM4] $x(a + b) = xa + xb$.

Generally there is a distinction between the two due to properties **[LM2]** and **[RM2]**. The product $a(bx)$ under the left action would correspond to the product $(xb)a$ under the right action. Yet, we have $a(bx) = (ab)x$ and $(xb)a = x(ba)$, and it's not necessarily the case that $ab = ba$.

We wish to work solely with either left or right modules. To show that there is no loss of generality in choosing either, we make the correspondence between left and right R-modules precise.

Definition 2.1.3 Let $(R, +, \cdot)$ be a ring. We define the **opposite ring** of R, denoted R^{op}, to be the ring $(R, +, \circ)$ where $+$ is the usual addition from R and $\circ$ is defined by $x \circ y = y \cdot x$.

It's an easy verification to check that R^{op} is indeed a ring and it has the same identity element 1. Moreover, it's clear that $(R^{\text{op}})^{\text{op}} \cong R$. With this we have:

Proposition 2.1.4 Any left R-module M with action $\cdot : R \times M \to M$ has the structure of a right R^{op}-module whose action $\circ : M \times R \to M$ is given by $x \circ a = a \cdot x$ for all $a \in R$ and $x \in M$.

Dually, any right R-module has the structure of a left R^{op}-module with the obvious action.

Proof. The only non-trivial thing to check is **[RM2]**. But this is easy: if $a, b \in R$ and $x \in M$, then $(x \circ a) \circ b = b \cdot (a \cdot x) = (ba) \cdot x = x \circ (ba) = x \circ (a \circ b)$. □

Hence, the study of a left R-module amounts to the study of the corresponding right R^{op}-module. As such, there is no loss of generality in the study if we take all R-modules to be left.

We shall briefly list some examples, then get to some motivation.

Example 2.1.5

(1) Any vector space V over F is a left (or right, but usually left) F-module. In this case, there is no distinction between left and right vector spaces because F is commutative.

There is such a thing as vector spaces over division rings. In this case the left/right distinction would need to be made, but interestingly many of the properties that are well-known about vector spaces over fields carry over to vector spaces over division rings (for instance, the fact that every vector space has a basis). There are some nuances in the division ring setting though (see **Exercise 2.5.7** for an example). We shall see later why this was worth mentioning.

(2) Any ring R is itself a left or right R-module with the usual action of multiplication. To distinguish between the two, we often use ${}_RR$ to denote the left R-module and R_R for the right.

(3) More generally, if I is a set we can consider the cartesian product $\prod_I R = \{(a_i)_{i \in I} : \text{each } a_i \in R\}$ of I copies of R. We shall abbreviate the I-tuple $(a_i)_{i \in I}$ to just (a_i). This has the structure of a left R-module by defining $(a_i) + (b_i) = (a_i + b_i)$ and the action $c \cdot (a_i) = (ca_i)$. This is analogous to the F-vector space $\prod_I F$ with the usual structure on it.

Notably, we have $R^n = \prod_{i=1}^n R$ for $n \geqslant 1$ by taking $I = \{1, ..., n\}$, as well as $R^0 = \{0\}$ (the *zero module*) obtained by taking $I = \emptyset$.

(4) Let M be a $\mathbb{Z}$-module. Then M has the pre-existing structure of an abelian group $(M, +)$ with identity 0, and the action of $\mathbb{Z}$ on M is given by:

$$n \cdot x = \overbrace{x + \cdots + x}^{n \text{ times}}$$

for $n > 0$, $0 \cdot x = 0$, and $n \cdot x = (-n) \cdot (-x)$ for $n < 0$. Conversely suppose $(M, +)$ is any abelian group. Then the $\mathbb{Z}$-action on M defined above is the *only* action that can be placed on M to make it a $\mathbb{Z}$-module (why?) Hence, $\mathbb{Z}$-modules are precisely abelian groups.

(5) Let V be a vector space over a field F and let $T \in \mathrm{End}_F(V)$ be a linear operator. Then V has an $F[\lambda]$-module structure induced by T whose action is given by:

$$f(\lambda) \cdot v = f(T)v$$

Much can be said about the structure of V as an $F[\lambda]$-module. Notably, there is the *cyclic decomposition theorem* that gives us a canonical way of breaking V down into a direct sum of T-cyclic subspaces.[1]

For those familiar with groups, recall

Definition 2.1.6 Let G be a group and let X be a set. A ***G*-action** on X is a map $\cdot : G \times X \to X$ which satisfies the following properties for all $x \in X$ and all $g, h \in G$:

(i) $1 \cdot x = x$,

(ii) $g \cdot (h \cdot x) = (gh) \cdot x$.

We wish to consider an analogue of this for rings. That is, we want a *ring action* on some set. In order to achieve this though, we need our set to have additional structure. To see what we need, we shall view group actions from a different perspective.

Recall that $\mathrm{Sym}(X)$ is the group of bijective maps $f : X \to X$ under composition (see **Example 1.1.2 (4)**).

Proposition 2.1.7 Let G be a group and X be a set. There is a bijective correspondence between G-actions on X and group homomorphisms from G to $\mathrm{Sym}(X)$. This is given by:

- mapping an action $\cdot : G \times X \to X$ to the homomorphism $\Phi : G \to \mathrm{Sym}(X)$ given by $\Phi(g)(x) = g \cdot x$, and
- mapping a group homomorphism $\Phi : G \to \mathrm{Sym}(X)$ to the action $\cdot : G \times X \to X$ given by $g \cdot x = \Phi(g)(x)$.

We leave the details to the reader to verify if they so wish. Now we wish to view the ring analogue of a group homomorphism from G to $\mathrm{Sym}(X)$, which suggests we need some suitable ring of functions on our set X. But for this, we have to be able to both add and multiply functions.

[1] See for instance Chapter 7 of Linear Algebra by Hoffman and Kunze.

What allows this is the additional structure we will place on our set. Namely, we shall assume X is some *abelian group*; for the sake of consistency, let's call this $(M, +)$. Then we can consider:

Proposition 2.1.8 Let $\mathrm{End}(M)$ be the set of all groups homomorphisms from M to M (an element of $\mathrm{End}(M)$ is called an **endomorphism**). Then $\mathrm{End}(M)$ is a ring under the usual function addition and function composition.

Proof. It's easy to check that $\mathrm{End}(M)$ under addition has the structure of an abelian group. Under composition, the identity homomorphism id_M is the identity of $\mathrm{End}(M)$, and we clearly have $g \circ f \in \mathrm{End}(M)$ whenever $f, g \in \mathrm{End}(M)$.

Finally, we see that for $f, g, h \in \mathrm{End}(M)$ and $x \in M$:

$$(f \circ (g + h))(x) = f(g(x) + h(x)) = f \circ g(x) + f \circ h(x) = (f \circ g + f \circ h)(x)$$

so that $f \circ (g+h) = f \circ g + f \circ h$. A similar argument shows that $(f+g) \circ h = f \circ h + g \circ h$, making $\mathrm{End}(M)$ a ring. □

We therefore have the following analogue of the G-action and group homomorphism correspondence for rings:

Proposition 2.1.9 Let R be a ring and $(M, +)$ be an abelian group. There is a bijective correspondence between R-actions on M (which make M an R-module) and ring homomorphisms from R to $\mathrm{End}(M)$. This is given by:

- mapping an action $\cdot : R \times M \to M$ to the homomorphism $\Phi : R \to \mathrm{End}(M)$ given by $\Phi(a)(x) = a \cdot x$, and
- mapping a ring homomorphism $\Phi : R \to \mathrm{End}(M)$ to the action $\cdot : R \times M \to M$ given by $a \cdot x = \Phi(a)(x)$.

The proof of this we shall also omit. The salient point here is an R-module can be thought of as the ring analogue of a group action. More precisely, a group acting on a set is analogous to a ring acting on an abelian group.

Example 2.1.10 (Cayley's theorem for rings)
Recall that Cayley's theorem for groups tells us that for any group G, there is an injective group homomorphism $\lambda : G \to \mathrm{Sym}(G)$ given by $\lambda(g) = \lambda_g \in \mathrm{Sym}(G)$ for all $g \in G$, where $\lambda_g(h) = gh$ for all $h \in G$. In other words, every group is isomorphic to a subgroup of $\mathrm{Sym}(G)$.

The ring analogue tells us that for any ring R, there is an injective ring homomorphism $\lambda : R \to \mathrm{End}(R)$ ($\mathrm{End}(R)$ being the endomorphism ring of the group $(R, +)$) given by $\lambda(a) = \lambda_a$ where $\lambda_a(b) = ab$. This reflects the natural left R-module structure on R.

Now let's generalize this example.

Example 2.1.11 (Representations)
A **representation** of a group G is a pair (V, π) where V is a vector space over a field F and $\pi : G \to \mathrm{GL}(V)$ is a group homomorphism from G into the general linear group $\mathrm{GL}(V) = \{T \in \mathrm{End}_F(V) : T \text{ is invertible}\}$ under composition.

In other words, π gives us a way of "representing" each group element $g \in G$ as an invertible linear operator $\pi(g)$ on V. By taking V to be finite-dimensional, we can more explicitly view $\pi(g)$ as an invertible matrix. Studying the group G then amounts to studying the representations of G.

To see why this is a generalization of what was considered earlier, look at **Exercise 2.5.3**.

Similarly, we can define a **representation** of a ring R as a pair (M, ρ) where M is an abelian group and $\rho : R \to \mathrm{End}(M)$ is a ring homomorphism. In this case we are "representing" each ring element $a \in R$ as an abelian group endomorphism $\rho(a)$. But we've seen that ρ determines a unique R-module structure on M. Therefore, if we are study R by studying its representations, we're really just studying R-modules, and in this setting each $a \in R$ is represented as a left multiplication map $x \mapsto ax$ on M.

TLDR: to study a group G, we study its representations. Similarly to study a ring R, we study its representations. But these correspond precisely to R-modules. Thus, an R-module should be thought of as a way of representing the ring R that we are studying, and we shall see down the line that such structures can tell us a whole lot about R!

Example 2.1.12 Consider the ring of quaternions $\mathbb{H} = \{a+b\boldsymbol{i}+c\boldsymbol{j}+d\boldsymbol{k} : a, b, c, d \in \mathbb{R}\}$ as defined in **Example 1.1.7** and let $M = \mathbb{R}^4$ (as an additive group). Then in particular every 4×4 matrix over $\mathbb{R}$ can be thought of as an additive group endomorphism on $\mathbb{R}^4$ in the usual way. One can show that $\rho : \mathbb{H} \to \mathrm{End}(\mathbb{R}^4)$ given by:

$$\rho(a + b\boldsymbol{i} + c\boldsymbol{j} + d\boldsymbol{k}) = \begin{bmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{bmatrix}$$

is an injective ring homomorphism.

Definition 2.1.13 A representation (ρ, M) of R is called **faithful** when ρ is injective.

2.2 Submodules and quotients

We fix a ring R and a (left) R-module M.

Definition 2.2.1 A **submodule** of M is a subset $N \subseteq M$ such that:

[SM1] $(N, +)$ is a subgroup of $(M, +)$;

[SM2] N is closed under the R-action: for any $x \in N$ and $a \in R$, we have $ax \in N$.

The definition is analogous to that of an ideal, except here M only has a left action.

Example 2.2.2 If we consider $M = {}_RR$ (R as a left module), then the submodules are the subsets I of R for which $(I, +)$ is a subgroup of $(R, +)$ and I is closed under multiplication on the left by all elements of R; that is, for all $x \in I$ and $a \in R$, $ax \in I$. We shall call I a **left ideal** of R.

Dually if we consider $M = R_R$ (R as a right module), then the submodules are the subgroups $(I, +)$ of $(R, +)$ which are closed under right multiplication by R. In this case we call I a **right ideal** of R.

Clearly if R is commutative, these both coincide with our usual definition of ideal. It's only when R is non-commutative that there is a distinction.

To see this, let's consider the following more concrete

Example 2.2.3 We've seen that $M_n(F)$ is simple: the only ideals are 0 and $M_n(F)$. Are there any proper non-zero left or right ideals? This won't be the case if $n = 1$, so let's assume $n > 1$. Let $I = \{A = (a_{ij}) \in M_n(F) : a_{i1} = 0 \text{ for all } 1 \leqslant i \leqslant n\}$. The fact that $n > 1$ ensures I is non-zero and certainly I is proper. The elements of I are of the form:

$$\begin{bmatrix} 0 & * & * & \cdots & * \\ 0 & * & * & \cdots & * \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & * & * & \cdots & * \end{bmatrix}$$

so it's clear that $(I, +)$ is a subgroup of $(M_n(F), +)$ and that $AX \in I$ for all $A \in M_n(F)$ and $X \in I$. Therefore, I is a left ideal of $M_n(F)$ (and it certainly can't be a right ideal).

Exercise 2.5.6 gives more generally a classification of all the left/right ideals of $M_n(F)$.

Let's see some more examples of submodules.

Example 2.2.4

(1) If V is a vector space over F (that is, an F-module), then the submodules are precisely the vector subspaces of V.

(2) Since $\mathbb{Z}$-modules are nothing but abelian groups, the submodules in this case are simply subgroups.

(3) If V is a vector space over F and $T \in \mathrm{End}_F(V)$, look at V as an $F[\lambda]$-module with the action induced by T. If W is a submodule of V, then we'll have in particular that W is a vector subspace of V and that $TW = \{Tw : w \in W\} \subseteq W$. We call W a ***T*-invariant subspace** of V.

Now if W is a T-invariant subspace, then it's easy to see that $\{f(T)w : f \in F[\lambda], w \in W\} \subseteq W$ which makes W an $F[\lambda]$-submodule. Therefore, $F[\lambda]$-submodules of V are just T-invariant subspaces of V.

Like with subrings and ideals, we have the usual constructions of new submodules from old ones. We briefly list these constructions without verification.

Definition 2.2.5 Let $\mathcal{L}(M)$ be the set of all submodules of M. Let $\mathcal{C} = \{N_\alpha : \alpha \in I\} \subseteq \mathcal{L}(M)$ be a collection of submodules of M (here I is some index set).

(i) $\bigcap_\alpha N_\alpha$ is a submodule of M.

(ii) If $X \subseteq M$ is a subset, then the **submodule generated by X** is defined by

$$\langle X \rangle = \bigcap_{\substack{N \in \mathcal{L}(M) \\ N \supseteq X}} N$$

and is easily verified to be the smallest submodule of M containing X.

(iii) If $x_1, ..., x_n \in M$ then we write $\langle x_1, ..., x_n \rangle$ in place of $\langle \{x_1, ..., x_n\} \rangle$. We also often write $\langle x \rangle$ as just Rx.

(iv) We define the **sum** of the N_α's to be:

$$\sum_\alpha N_\alpha = \left\langle \bigcup_\alpha N_\alpha \right\rangle$$

which is the smallest submodule containing every N_α. Therefore, if $x_1, ..., x_n \in R$, we may often write $\sum_{i=1}^n Rx_i$ instead of $\langle x_1, ..., x_n \rangle$.

Remark 2.2.6 It's worth pointing out here that we shall usually write a collection of the form $\{N_\alpha : \alpha \in I\}$ as just $\{N_\alpha\}$. This may be seen as abuse of notation, as if we fix a single α then $\{N_\alpha\}$ may refer to the singleton set. But it should always be clear from context which is being referred to.

It's also worth studying the lattice structure that the set of submodule $\mathcal{L}(M)$ has.

Definition 2.2.7 A **lattice** is a poset $(L, \leq)$ equipped with two binary operations $\wedge$ and $\vee$ (called the *meet* and *join*, respectively) such that for all $x, y \in L$, $x \wedge y$ and $x \vee y$ are the greatest lower bound and least upper bound (respectively) of $\{x, y\}$ in L. More precisely, this means:

- $x \wedge y \leq x, y \leq x \vee y$, and
- for all $z \in L$, $z \leq x, y$ implies $z \leq x \wedge y$ and $z \geq x, y$ implies $z \geq x \vee y$.

It's clear that $\mathcal{L}(M)$ has the structure of a poset with respect to inclusion $\subseteq$.

Proposition 2.2.8 The poset $(\mathcal{L}(M), \subseteq)$ is a lattice with meet $\cap$ and join $+$.

Proof. Let $N, P \in \mathcal{L}(M)$. We must verify that $N \cap P$ is the greatest lower bound of $\{N, P\}$ and that $N + P$ is the least upper bound of $\{N, P\}$. First, if $Q \in \mathcal{L}(M)$ is such that $Q \subseteq N, P$, then immediately we have $Q \subseteq N \cap P$. Now if $Q \supseteq N, P$, then for any $x \in N$ and $y \in P$ we find that $x, y \in Q$ so that $x + y \in Q$. Since every element of $N + P$ is of this form, we get $N + P \subseteq Q$. $\square$

Now let N be a submodule of M and consider the set $M/N = \{x + N : x \in M\}$ of cosets. We can equip an R-module structure on M/N as follows: for $x, y \in M$ and $a \in R$, define

$$(x + N) + (y + N) = (x + y) + N \quad \text{and} \quad a(x + N) = ax + N$$

It's routine to check these operations are well-defined and that M/N becomes an R-module.

Definition 2.2.9 Let N be a submodule of M. We call M/N defined above the **quotient module** of M by N.

This is, of course, an analogue of the notion of taking the quotient of a ring with an ideal, which yields a ring structure.

Example 2.2.10

(1) This example will serve as a warning. If R is a ring and I is a left ideal (a submodule of ${}_RR$), then we can consider the R-module R/I. This however is generally **not** a ring. To see why, we can revisit **Example 2.2.3** in the situation where $n = 2$. In this case we would have the left ideal:

$$I = \left\{ \begin{bmatrix} 0 & a \\ 0 & b \end{bmatrix} : a, b \in F \right\}$$

Let $E_1, E_2 \in M_2(F)$ be given by:

$$E_1 = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \quad \text{and} \quad E_2 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

We see that $E_1 + I = E_2 + I$. If R/I were a ring, we would need $(E_1 + I)^2 = (E_2 + I)^2$, which means $E_1^2 + I = E_2^2 + I$. But $E_1^2 = 0$ and $E_2^2 = I_2$ (the 2×2 identity matrix), and clearly $I \neq I_2 + I$.

(2) If M is a $\mathbb{Z}$-module (abelian group) and N is a submodule (subgroup) of M, then it's clear that M/N is simply a quotient group. Of course, the fact that M is abelian means N is normal in M.

(3) If V is a vector space over F (F-module) and W is a subspace, the quotient module V/W is simply the quotient space. If $T \in \mathrm{End}_F(V)$ and we assume W is a T-invariant subspace, then the quotient space V/W is also T-invariant (and is a quotient $F[\lambda]$-module of V by W).

2.3 Hom sets and Schur's lemma

Fix two R-modules M and N.

Definition 2.3.1 An ***R*-module homomorphism** (or simply ***R*-homomorphism**) from M to N is a map $f : M \to N$ which is R-linear: for all $x, y \in M$ and $a \in R$, we have

$$f(ax + y) = af(x) + f(y)$$

This means f is a group homomorphism from $(M,+)$ to $(N,+)$ which preserves the R-multiplication. We write $\mathrm{Hom}_R(M,N)$ to denote the set of all R-homomorphisms from M to N. We also use $\mathrm{End}_R(M)$ to denote the set $\mathrm{Hom}_R(M,M)$ and call these the set of ***R*-endomorphisms** on M.

This is the module analogue of linear maps between vector spaces. We shall see that $\mathrm{Hom}_R(M,N)$ has a considerable amount of structure, and even more so with $\mathrm{End}_R(M)$. Before we study this in detail, we go over quickly the basics of R-homomorphisms, which should be no surprise to the reader.

Definition 2.3.2 Let $f \in \mathrm{Hom}_R(M,N)$. Then

- the **kernel** of f is the set $\ker f = \{x \in M : f(x) = 0\}$;
- the **image** of f is the set $\mathrm{im}\, f = \{f(x) \in N : x \in M\}$.

It's easy to check that $\ker f$ and $\mathrm{im}\, f$ are submodules of M and N, respectively. Moreover, f is injective if and only if $\ker f = 0$ and surjective if and only if $\mathrm{im}\, f = N$. If f is both injective and surjective, f is called an **isomorphism** and we write $M \cong N$. In this case, $f^{-1} : N \to M$ is an isomorphism as well.

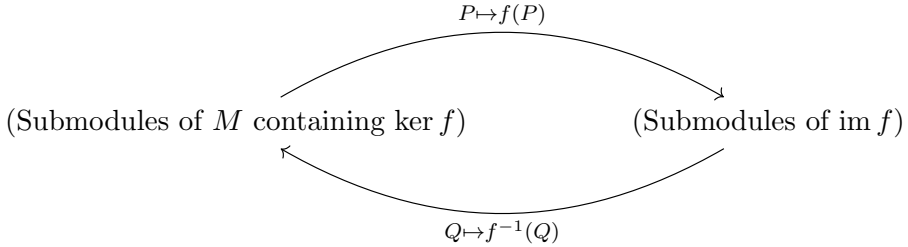
If $f \in \mathrm{End}_R(M)$ is an isomorphism, we say f is an **automorphism** on M. We often write $\mathrm{Aut}_R(M)$ to denote the set of automorphisms.

Remark 2.3.3 At this point we should mention the following notation we shall use for homomorphisms. First, it's clear that if $f : M \to N$ and $g : N \to P$ are R-homomorphisms, then $g \circ f : M \to P$ is also one. We will often abbreviate $g \circ f$ to just gf. This will make working with homomorphisms much cleaner later on.

Note that if P is a submodule of M and $q : M \to M/P$ is the quotient map sending $x \in M$ to $x + P$, then q is a surjective R-homomorphism. We have the analogous isomorphism and correspondence theorems for modules.

Theorem 2.3.4 (First isomorphism theorem)
Let $f \in \mathrm{Hom}_R(M,N)$ and let $q : M \to M/\ker f$ denote the quotient homomorphism. Then f induces a unique $\overline{f} \in \mathrm{Hom}_R(M/\ker f, N)$ satisfying $f = \overline{f}q$. Moreover, $\overline{f}$ is injectve, which means $M/\ker f \cong \mathrm{im}\, f$.

Theorem 2.3.5 (Correspondence theorem)
Let $f \in \mathrm{Hom}_R(M,N)$. Then there is a bijective correspondence between the submodules of M which contain $\ker f$ with the submodules of $\mathrm{im}\, f$:



As a consequence, there is a bijective correspondence between the submodules of M containing $\ker f$ and the submodules of $M/\ker f$.

Like in the last chapter, there are analogous *second* and *third* isomorphism theorems for modules as well.

Theorem 2.3.6 (Second isomorphism theorem)
Let N and P be submodules of M. Then

(i) $N + P = \{y + z : y \in N, z \in P\}$ is a submodule of M;

(ii) $N \cap P$ is a submodule of M;

(iii) $(N + P)/P \cong N/(N \cap P)$.

Theorem 2.3.7 (Third isomorphism theorem)
Let N and P be submodules of M with $P \subseteq N$. Then

(i) N/P is a submodule of M/P. Moreover, every submodule of M/P is of the form N'/P where N' is a submodule of M containing P.

(ii) $(M/P)/(N/P) \cong M/N$.

We now look at the structure of hom sets and work towards proving an important result called *Schur's lemma*. We have seen already that if M is an abelian group, then the set $\mathrm{End}(M)$ of group endomorphisms is a ring under addition and composition. We consider now two modules M and N, and the structures of $\mathrm{Hom}_R(M, N)$ and $\mathrm{End}_R(M)$.

Proposition 2.3.8 $\mathrm{Hom}_R(M, N)$ is an abelian group under addition and $\mathrm{End}_R(M)$ is a ring under addition and composition. Moreover, $\mathrm{Aut}_R(M) = \mathrm{End}_R(M)^\times$, the set of units of the ring $\mathrm{End}_R(M)$. Thus, $\mathrm{Aut}_R(M)$ is a group under composition.

Proof. Routine. □

What's more interesting is what we can say these hom groups are isomorphic to in certain situations.

Example 2.3.9 Consider the $\mathbb{Z}$-module $\mathbb{Z}/(n)$ for $n > 0$ and the hom groups $M = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/(n))$ and $N = \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z})$. We shall show that $M \cong \mathbb{Z}/(n)$ and $N = 0$ as groups. Let $\Phi : M \to \mathbb{Z}/(n)$ be given by $\Phi(f) = f(1)$. We see that $\Phi(f + g) = (f + g)(1) = f(1) + g(1) = \Phi(f) + \Phi(g)$ and therefore Φ is a group homomorphism. Next, if $\Phi(f) = 0$ then $f(1) = 0$, which must imply $f = 0$, so Φ is injective. Finally, given $k + (n) \in \mathbb{Z}/(n)$, we have that the map $f \in M$ satisfying $f(1) = k + (n)$ gives us $\Phi(f) = k + (n)$, so Φ is indeed an isomorphism.

Now for N, we can simply observe that any $f \in N$ must satisfy $f(1) = 0$ because $0 = f(0) = f(n) = nf(1) \in \mathbb{Z}$. This means $f = 0$, so $N = 0$.

Now let's see what we can say about $\mathrm{End}_R(M)$ in certain situations.

Definition 2.3.10 M is called **cyclic** when there exists an $x \in M$ with $Rx = M$. M is called **irreducible** (or **simple**) when $M \neq 0$ and the only submodules of M are

Proposition 2.3.11 Let $M \neq 0$ be an R-module. Then M is irreducible if and only if $Rx = M$ for all $0 \neq x \in M$.

Proof. If M is irreducible, then the fact that $Rx \neq 0$ for any $0 \neq x \in M$ forces $Rx = M$ (as Rx is a submodule). Conversely suppose $Rx = M$ for all $0 \neq x \in M$. If $P \neq 0$ is a submodule of M, then for $0 \neq y \in N$ we have that $Ry = M$. But clearly $Ry \subseteq N$, so we must have $N = M$, which makes M irreducible. □

With this, we can prove the following

Lemma 2.3.12 (Schur's lemma)
Let M and N be irreducible R-modules. Then any $f \in \mathrm{Hom}_R(M, N)$ is either 0 or an isomorphism. Hence, $\mathrm{End}_R(M)$ is a division ring.

Proof. Suppose $f \in \mathrm{Hom}_R(M, N)$ is non-zero. Then $\mathrm{im}\, f$ is a submodule of N and $f \neq 0$ means $\mathrm{im}\, f \neq 0$. Since N is irreducible, we must have $\mathrm{im}\, f = N$, which makes f surjective. Similarly M is irreducible, so we either have $\ker f = 0$ or M. But $\ker f \neq M$ since $f \neq 0$, so $\ker f = 0$ and f must be injective. Thus, f is an isomorphism.

This shows every non-zero element of $\mathrm{End}_R(M)$ is an isomorphism. In other words, $\mathrm{Aut}_R(M) = \mathrm{End}_R(M) \setminus \{0\}$, which means $\mathrm{End}_R(M)$ is indeed a division ring. □

2.4 Direct products and sums

We next see two ways to construct new R-modules out of old ones. First is the direct product:

Definition 2.4.1 Let $\{M_\alpha\}$ be a collection of R-modules and let $M = \prod_\alpha M_\alpha = \{(x_\alpha) : x_\alpha \in M_\alpha\}$ denote the cartesian product of the M_α's (each (x_α) is a tuple indexed by $\{\alpha\}$). Then M has an R-module structure given by:

$$(x_\alpha) + (y_\alpha) = (x_\alpha + y_\alpha)$$

$$c(x_\alpha) = (cx_\alpha)$$

We call M the **direct product** of the set $\{M_\alpha\}$.

Remark 2.4.2 Another way to think about the direct product of a collection of sets $\{X_\alpha\}$ is as follows: suppose $I = \{\alpha\}$ is the indexing set. Then we can identify each tuple $(x_\alpha) \in \prod_\alpha X_\alpha$ as a function $f : I \to \bigcup_\alpha X_\alpha$ where $f(\alpha) = x_\alpha \in X_\alpha$. We can therefore define $\prod_\alpha X_\alpha$ to be the set of functions $f : I \to \bigcup_\alpha X_\alpha$ satisfying $f(\alpha) \in X_\alpha$ for each α. The operations would be defined by $(f+g)(\alpha) = f(\alpha) + g(\alpha)$ and $(af)(\alpha) = af(\alpha)$.

Definition 2.4.3 For a collection $\{M_\alpha\}$ of R-modules, we define their **direct sum** to be:

$$\bigoplus_\alpha M_\alpha = \left\{ (x_\alpha) \in \prod_\alpha M_\alpha : \text{all but finitely-many } x_\alpha = 0 \right\}$$

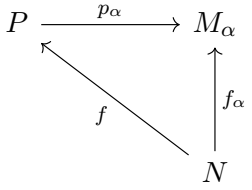
Therefore, it's not generally true that $\prod_\alpha M_\alpha = \bigoplus_\alpha M_\alpha$. If the set $\{\alpha\}$ we're indexing over is finite though, then clearly it will be true. That is, we always have $\prod_{i=1}^n M_i = \bigoplus_{i=1}^n M_i$. We can write this as $M_1 \oplus M_2 \oplus \cdots \oplus M_n$.

One can ask whether we may have $\prod_\alpha M_\alpha \cong \bigoplus_\alpha M_\alpha$ even if $\{\alpha\}$ is infinite and each $M_\alpha \neq 0$. **Exercise 2.5.12** gives an example where these are *not* isomorphic and **Exercise 2.5.13** gives an example where these *are* isomorphic.

There is a more sophisticated way of defining a direct product and direct sum. This doesn't provide concrete constructions, but gives another way of viewing these and gives a categorical relation between products and sums, exhibiting them as being "dual".

Definition 2.4.4 Let $\{M_\alpha\}$ be a collection of R-modules. A **(categorical) direct product** of $\{M_\alpha\}$ is a pair $(P, \{p_\alpha\})$, where P is an R-module and each $p_\alpha : P \to M_\alpha$ is an R-homomorphism, which satisfies the following property: for any R-module N and associated R-homomorphisms $f_\alpha : N \to M_\alpha$, there is a *unique* R-homomorphism $f : N \to P$ such that $f_\alpha = p_\alpha f$ for all α.

This property is often illustrated by saying that there is a unique $f \in \mathrm{Hom}_R(N, P)$ that makes the following diagram *commute* for all α:

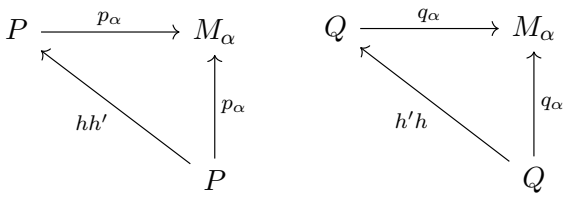


Let $P = \prod_\alpha M_\alpha$ as constructed above and let $p_\alpha : P \to M_\alpha$ be the projection map taking (x_β) to its α coordinate value x_α. Then we have:

Proposition 2.4.5 $(P, \{p_\alpha\})$ is a categorical direct product of $\{M_\alpha\}$. Moreover, if $(Q, \{q_\alpha\})$ is another categorical direct product of $\{M_\alpha\}$, then there exists a unique *isomorphism* $h : Q \to P$ such that $q_\alpha = p_\alpha h$.

Proof. Let N be an R-module and let $f_\alpha : N \to M_\alpha$ be R-homomorphisms. Define $f : N \to P$ by $f(x) = (f_\beta(x))_\beta \in P$. Then we have by construction that $(p_\alpha f)(x) = p_\alpha((f_\beta(x))_\beta) = f_\alpha(x)$ so that $p_\alpha f = f_\alpha$. Thus, $(P, \{p_\alpha\})$ is indeed a categorical direct product.

Now suppose $(Q, \{q_\alpha\})$ is another. Then it satisfies the property that there is a unique $h : Q \to P$ such that $q_\alpha = p_\alpha h$ for all α. It remains to show this is an isomorphism. If we apply the property again in the other direction, there is a unique $h' : P \to Q$ such that $p_\alpha = q_\alpha h'$ for all α. Thus, we find that $p_\alpha = p_\alpha hh'$ and $q_\alpha = q_\alpha h'h$. This means the diagrams:

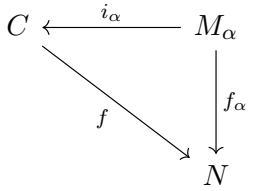


each commute. But hh' and $h'h$ must be the *unique* maps satisfying commutativity by the definition of a categorical direct product, and clearly the identity maps id_M and id_P work here too. Hence, $hh' = \mathrm{id}_M$ and $h'h = \mathrm{id}_P$, which means that h is an isomorphism. □

This shows that any categorical direct product is isomorphic to the usual direct product, so we can simply refer to either as the direct product. We next consider the analogue for direct sums.

Definition 2.4.6 Let $\{M_\alpha\}$ be a collection of R-modules. A **(categorical) direct sum** of $\{M_\alpha\}$ is a pair $(C, \{i_\alpha\})$, where C is an R-module and each $i_\alpha : M_\alpha \to C$ is an R-homomorphism, which satisfies the following property: for any R-module N and associated R-homomorphisms $f_\alpha : M_\alpha \to N$, there is a *unique* R-homomorphism $f : C \to N$ such that $f_\alpha = f i_\alpha$ for all α.

This property is often illustrated by saying that there is a unique $f \in \mathrm{Hom}_R(C, N)$ that makes the following diagram *commute* for all α:



The key observation here is that the definition of a categorical direct sum is the exact same as the definition of a categorical direct product, except that all the homomorphisms considered are in reverse order. This is what we mean by the direct product and direct sum being "dual".

Now let $C = \bigoplus_\alpha M_\alpha$ and let $i_\alpha : M_\alpha \to C$ be the injection map that takes $x \in M_\alpha$ to the tuple (x_β) given by $x_\alpha = x$ and $x_\beta = 0$ for all $\beta \neq \alpha$. Clearly $(x_\beta) \in C$ and i_α is an R-homomorphism. Then we can show:

Proposition 2.4.7 $(C, \{i_\alpha\})$ is a categorical direct sum of $\{M_\alpha\}$. Moreover, if $(D, \{j_\alpha\})$ is another categorical direct sum of $\{M_\alpha\}$, then there exists a unique *isomorphism* $h : C \to D$ such that $j_\alpha = h i_\alpha$.

Proof. **Exercise 2.5.11**. □

Thus, we similarly have that any categorical direct sum is isomorphic to the usual direct sum, so we refer to either as the direct sum.

We now focus our attention to the case where the indexing set $\{\alpha\}$ is of the form $\{1, ..., n\}$ for some $n \geqslant 1$. So we have R-modules $\{M_1, ..., M_n\}$ and we know that $M = \prod_{j=1}^n M_j = \bigoplus_{j=1}^n M_j$. Let $\{p_1, ..., p_n\}$ and $\{i_1, ..., i_n\}$ be the associated projection and injection maps: $p_k : \prod_{j=1}^n M_j \to M_k$ and $i_k : M_k \to \bigoplus_{j=1}^n M_j$. What can we say about these maps?

Proposition 2.4.8 The maps $\{p_1, ..., p_n\}$ and $\{i_1, ..., i_n\}$ satisfy the following properties:

(i) $p_j i_j = \mathrm{id}_{M_j}$ and $p_j i_k = 0$ for all $j \neq k$.

(ii) $\sum_{j=1}^{n} i_j p_j = \mathrm{id}_M$.

Moreover, suppose M' is another R-module and we have R-homomorphisms $\{p'_1, ..., p'_n\}$ and $\{i'_1, ..., i'_n\}$ where $p'_k : M' \to M_k$ and $i'_k : M_k \to M'$ satisfy:

(i') $p'_j i'_j = \mathrm{id}_{M_j}$ and $p'_j i'_k = 0$ for all $j \neq k$.

(ii') $\sum_{j=1}^{n} i'_j p'_j = \mathrm{id}_{M'}$.

Then the map $\theta : M \to M'$ given by

$$\theta = \sum_{j=1}^{n} i'_j p_j$$

is an isomorphism whose inverse is

$$\theta^{-1} = \sum_{j=1}^{n} i_j p'_j$$

Moreover, we have $\theta i_j = i'_j$ and $p_j \theta^{-1} = p'_j$ for all j. Hence, the properties **(i)** and **(ii)** characterize M up to isomorphism.

Proof. We have $p_j i_j(x) = p_j(0, ..., 0, x, 0, ..., 0) = x$ for each $x \in M_j$, so $p_j i_j = \mathrm{id}_{M_j}$. If $j \neq k$, then $p_j i_k(x) = p_j(0, ...0, x, 0, ..., 0) = 0$, so $p_j i_k = 0$. Now if $y = (x_1, ..., x_n) \in M$, then we have $(i_j p_j)(y) = i_j(x_j) = (0, ..., 0, x_j, 0, ..., 0)$, which means $\sum_{j=1}^{n}(i_j p_j)(y) = (x_1, 0, 0, ..., 0) + (0, x_2, 0, ..., 0) + \cdots + (0, 0, ..., x_n) = y$. Thus, **(i)** and **(ii)** hold.

Now we consider an R-module M' with the p'_j and i'_j defined above satisfying **(i')** and **(ii')**. Let $\theta : M \to M'$ be given by $\theta = \sum_{j=1}^{n} i'_j p_j$. We show that this is an isomorphism. If $\theta' : M' \to M$ is given by $\theta' = \sum_{j=1}^{n} i_j p'_j$, then we have:

$$\theta\theta' = \left(\sum_{j=1}^{n} i'_j p_j\right)\left(\sum_{j=1}^{n} i_j p'_j\right) = \sum_{j,k=1}^{n} i'_j p_j i_k p'_k$$

and we know that $p_j i_j = \mathrm{id}_{M_j}$ and $p_j i_k = 0$ for $j \neq k$, so the above reduces to:

$$\sum_{j=1}^{n} i'_j p'_j = \mathrm{id}_{M'}$$

and thus $\theta\theta' = \mathrm{id}_{M'}$. A similar argument shows $\theta'\theta = \mathrm{id}_M$, which means θ is indeed an isomorphism and $\theta^{-1} = \theta'$. Finally, $\theta i_j = (\sum_{k=1}^{n} i'_k p_k) i_j = i'_j p_j i_j = i'_j$ and $p_j \theta^{-1} = p_j(\sum_{k=1}^{n} i_k p'_k) = p_j i_j p'_j = p'_j$. □

We finish by considering a special case of direct sum for submodules of M.

Definition 2.4.9 Let $f, g \in \mathrm{End}_R(M)$ (M is any module here). We say that f is **idempotent** when $f^2 = f$. We say f and g are **orthogonal** when $fg = gf = 0$.

Suppose $M = \bigoplus_{i=1}^n M_i = \prod_{i=1}^n M_i$ where M_i are R-modules and let $p_1, ..., p_n$ and $i_1, ..., i_n$ be the usual projections and injections.

Lemma 2.4.10 Let $e_j = i_j p_j \in \mathrm{End}_R(M)$ for each j. Then:

(i) $e_1, ..., e_n$ are **orthogonal idempotents**: $e_j^2 = e_j$ and $e_j e_k = 0$ for all $j \neq k$;

(ii) $e_1 + \cdots + e_n = \mathrm{id}_M$.

We say that $\{e_1, ..., e_n\}$ is a **partition of the identity** id_M.

Proof. Clear. □

Proposition 2.4.11 Let $M = \bigoplus_{i=1}^n M_i$ and let $\{e_1, ..., e_n\}$ be a partition of id_M as defined above. Set $M_j' = e_j(M) = i_j(M_j) \subseteq M$. Then:

(i) $M = \sum_{j=1}^n M_j'$;

(ii) $M_k' \cap \left(\sum_{j \neq k} M_j'\right) = 0$ for each k.

Conversely, suppose M is any R-module and $M_1', ..., M_n'$ are submodules of M that satisfy **(i)** and **(ii)** above. Then $M = \sum_{j=1}^n M_j' \cong \bigoplus_{j=1}^n M_j'$.

We say then that M is an **internal direct sum** of $M_1', ..., M_j'$ and we just write $M = \bigoplus_{j=1}^n M_j'$. In this case, we have that for each $x \in M$, there are *unique* $x_j \in M_j$ with $x = \sum_{j=1}^n x_j$.

Proof. Given $x \in M$, we have $x_j = e_j(x) \in M_j'$ and that $x_1 + \cdots + x_n = e_1(x) + \cdots + e_n(x) = (e_1 + \cdots + e_n)(x) = \mathrm{id}_M(x) = x$, which proves **(i)**. Next, suppose $x \in M_k' \cap \left(\sum_{j \neq k} M_j'\right)$. Then $x = e_k(y)$ for some $y \in M$ and $x = \sum_{j \neq k} e_j(y_j)$ for some $y_j \in M$. Now $x = e_k(y) = e_k^2(y) = e_k(x) = e_k(\sum_{j \neq k} e_j(y_j)) = \sum_{j \neq k} e_k e_j(y_j) = 0$, which proves **(ii)**.

Now suppose M is an R-module with submodules $M_1', ..., M_n'$ satisfying **(i)** and **(ii)**. Consider the map $\Phi : \bigoplus_{j=1}^n M_j \to M$ given by $\Phi(x_1, ..., x_n) = \sum_{j=1}^n x_i$. It's clear that Φ is an R-homomorphism and surjectivity is given by **(i)**. Now if $\Phi(x_1, ..., x_n) = \sum_{j=1}^n x_j = 0$, then for each k we can write $x_k = -\sum_{j \neq k} x_j$, and property **(ii)** forces $x_k = 0$, which makes Φ injective. □

Exercises

Let R be a ring.

Definition 2.5.1 For a subset $S \subseteq R$, we define the **centralizer** of S in R to be

$$C_R(S) = \{a \in R : as = sa \text{ for all } s \in S\}$$

It's clear that $C_R(S)$ is a subring of R.

Exercise 2.5.2 Consider the additive group $(R, +)$ and the ring $\mathrm{End}(R)$ of group endomorphisms on $(R, +)$. For each $a \in R$, let $\lambda_a, \rho_a \in \mathrm{End}(R)$ be given by $\lambda_a(x) = ax$ and $\rho_a(x) = xa$ for all $x \in R$. Define $\mathcal{L} = \{\lambda_a : a \in R\} \subseteq \mathrm{End}(R)$ and $\mathcal{R} = \{\rho_a : a \in R\} \subseteq \mathrm{End}(R)$.

Show that $\mathcal{L} = C_{\mathrm{End}(R)}(\mathcal{R})$ and $\mathcal{R} = C_{\mathrm{End}(R)}(\mathcal{L})$.

Recall that Cayley's theorem says that for any group G, we can find an injective group homomorphism $\Phi : G \to \mathrm{Sym}(G)$. The following exercise shows that this map can be viewed as a faithful representation of G.

Exercise 2.5.3 Let V be the vector space with basis $\{e_g : g \in G\}$. For each $g \in G$, let $T_g : V \to V$ be given by $T_g e_h = e_{gh}$ for all $h \in G$.

(a) Verify that T_g is a well-defined linear isomorphism of V to itself.

Now define $\pi : G \to \mathrm{GL}(V)$ by $\pi(g) = T_g$.

(b) Show that π is an injective group homomorphism. Conclude that (V, π) is a faithful representation.

(c) Finally, show that $\mathrm{Sym}(G) \cong \mathrm{im}\,\pi$ by finding an appropriate group isomorphism from $\mathrm{Sym}(G)$ to $\mathrm{im}\,\pi$.

The following exercise shows that the lattice $\mathcal{L}(M)$ of submodules is a *modular* lattice.

Exercise 2.5.4 Show that for any $N, P, Q \in \mathcal{L}(M)$, the following hold:

(a) if $P \subseteq N$, then $N \cap (P + Q) = P + N \cap Q$;

(b) if $P \supseteq N$, then $N + (P \cap Q) = P \cap (N + Q)$.

We've seen in **Example 2.1.5 (4)** that if M is an abelian group, then there is only one action that makes M a $\mathbb{Z}$-module.

Exercise 2.5.5

(a) Show similarly that if V is a $\mathbb{Q}$-module (really, a $\mathbb{Q}$-vector space), then this action of $\mathbb{Q}$ on V is the *only* one that makes it a $\mathbb{Q}$-module.

(b) Given a finite abelian group $M \neq 0$, is it possible for M to have the structure of a $\mathbb{Q}$-module?

The next exercise gives a classification for all the left ideals of the ring $M_n(F)$.

Exercise 2.5.6 For a given $A \in M_n(F)$, let $\lambda_A : M_n(F) \to M_n(F)$ be the map given by $\lambda(X) = XA$.

(a) Verify that λ_A is a left module endomorphism on $M_n(F)$, and therefore that $\ker \lambda_A$ is a left ideal of $M_n(F)$.

Now let J be any left ideal of $M_n(F)$ and consider the set $V(J) = \{v \in F^n : Xv = 0 \text{ for all } X \in J\} = \bigcap_{A \in J} \ker A$.

(b) Use Zorn's lemma to show that there exist $B_1, ..., B_k \in J$ with $V(J) = \bigcap_{i=1}^{k} \ker B_i$.

(c) Hence, show that there exists a $B \in J$ with $V(J) = \ker B$.

(d) Conclude therefore that $J = \ker \lambda_B$.

This result tells us something more: every left ideal of $M_n(F)$ is principal (generated by a single element). An analogous classification holds for right ideals.

It is a well-known fact that if V is a vector space over a field F of dimension n, then $\text{End}_F(V) \cong M_n(F)$. We show that this isn't *quite* true if F is replaced with a division ring instead.

Recall that a map $f : R \to S$ between two rings is an *antihomomorphism* when:

- $f(x+y) = f(x) + f(y)$,
- $f(1) = 1$,
- $f(xy) = f(y)f(x)$.

It's easy to see that equivalently an antihomomorphism $f : R \to S$ is simply a homomorphism $f : R \to S^{\text{op}}$. We say f is an **antiisomorphism** when f is also injective and surjective.

Exercise 2.5.7 Let V be a vector space over a division ring D and let $\{v_1, ..., v_n\}$ be a basis for V. Then for any $T \in \text{End}_D(V)$, there exist *unique* $\alpha_{i,j} \in D$ for which $Tv_j = \sum_{i=1}^n \alpha_{i,j} v_i$. This determines a matrix $A_T = (\alpha_{i,j}) \in M_n(D)$.

(a) Show that the mapping $\Phi : \text{End}_D(V) \to M_n(D)$ given by $\Phi(T) = A_T$ is an antiisomorphism.

(b) Show that $M_n(D)^{\text{op}} \cong M_n(D^{\text{op}})$ and that D^{op} is a division ring too. Hence conclude that $\text{End}_D(V) \cong M_n(D^{\text{op}})$.

Exercise 2.5.8 In **Example 2.3.9**, we showed that $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}, \mathbb{Z}/(n)) \cong \mathbb{Z}/(n)$. Show more generally that for any R-module M, we have $\text{Hom}_R(R, M) \cong M$ as abelian groups.

Definition 2.5.9 Let D be an integral domain and let M be a D-module. We define the **torsion submodule** of M to be:

$$\text{Tor}(M) = \{x \in M : ax = 0 \text{ for some } 0 \neq a \in D\}$$

It's easy to see that this is indeed a submodule of M. M is said to be **torsion-free** when $\text{Tor}(M) = 0$. M is said to be **torsion** when $\text{Tor}(M) = M$.

Exercise 2.5.10 In **Example 2.3.9**, we showed that $\text{Hom}_{\mathbb{Z}}(\mathbb{Z}/(n), \mathbb{Z}) = 0$. Show more generally that if D is an integral domain and M and N are D-modules, then $\text{Hom}_D(M, N) = 0$ whenever M is torsion and N is torsion-free. Show also that N is torsion-free if and only if $\text{Hom}_D(M, N) = 0$ for every torsion D-module M.

The next exercise gives a verification that the direct sum in the usual sense is in fact a categorical direct sum.

Exercise 2.5.11 Let $\{M_\alpha\}$ be a collection of R-modules, let $C = \bigoplus_\alpha M_\alpha$, and for each α let $i_\alpha : M_\alpha \to C$ be the injection homomorphism that takes $x \in M_\alpha$ to the tuple (x_β) given by $x_\alpha = x$ and $x_\beta = 0$ for all $\beta \neq \alpha$.

Show that $(C, \{i_\alpha\})$ is a categorical direct sum in the sense of **Definition 2.4.6**.

Exercise 2.5.12 Consider the $\mathbb{Z}$-modules $M = \prod_{n=1}^{\infty} \mathbb{Z}$ and $N = \bigoplus_{n=1}^{\infty} \mathbb{Z}$. It's clear that $N \subsetneq M$. Show that we also have $M \ncong N$.

Exercise 2.5.13 Give an example of an *infinite* collection $\{M_\alpha\}$ of *non-zero* R-modules with $\prod_\alpha M_\alpha \cong \bigoplus_\alpha M_\alpha$.

(Hint: you can do this in vector spaces – the problem reduces to showing that the spaces have bases of the same cardinality.)

3 Structure theory of modules

This chapter will study the structure theory of modules. We shall investigate first the notion of *complete decomposability* (the "breaking down" of a module into *indecomposable* parts) in the finite case, and a special class of modules which have this property. Afterwards, we shall study the stronger notion of *semisimplicity* (the breaking down of a module into *irreducible/simple* parts).

A note on exercises: unlike the last two chapters, there will be a section on exercises at the end of each section. This will encourage you to familiarize yourself with the material covered in a given section before moving on to the next. The chapters that follow will also have this format.

3.1 Noetherian and Artinian modules

We introduce here two special classes of modules, which we shall see later relates to complete decomposability.

Definition 3.1.1 M is called **Noetherian** when it satisfies the following *ascending chain condition*: given a countably-infinite ascending chain $N_1 \subseteq N_2 \subseteq \cdots$ of submodules of M, there exists a $k \in \mathbb{N}$ for which $N_k = N_{k+1} = \cdots$.

In other words, every ascending chain of submodules must eventually stabilize.

There are two useful equivalent characterizations for Noetherianity. We state and prove these now so that we can better study some examples. First we have:

Definition 3.1.2 M is **finitely-generated** when there exist finitely-many $x_1, ..., x_n \in M$ for which $M = Rx_1 + \cdots + Rx_n = \{a_1x_1 + \cdots + a_nx_n : a_i \in R\}$.

Proposition 3.1.3 The following are equivalent:

(i) M is Noetherian.

(ii) M satisfies the following *maximum condition*: every non-empty collection $\mathcal{S}$ of submodules of M has a submodule which is maximal in $\mathcal{S}$. That is, there is a $P \in \mathcal{S}$ such that for all $N \in \mathcal{S}$, $N \supseteq P$ implies $N = P$.

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

Proof. Suppose first that M is Noetherian. Let $\mathcal{C}$ be a non-empty collection of submodules and assume it has no maximal element. Take any $N_1 \in \mathcal{C}$ and we can find an $N_2 \in \mathcal{C}$ with $N_2 \supsetneq N_1$. Likewise we can find $N_3 \in \mathcal{C}$ with $N_3 \supsetneq N_2$. Continuing, we obtain a chain $N_1 \subsetneq N_2 \subsetneq N_3 \subsetneq \cdots$ of submodules which will never stabilize, contradicting Noetherianity. Thus, M must satisfy the maximum condition.

Now suppose M satisfies the maximum condition. Let N be a submodule and let $\mathcal{S}$ be the collection of all finitely-generated submodules of N. Since 0 is finitely-generated, we have $\mathcal{S} \neq \emptyset$. Thus, there is a maximal $P \in \mathcal{S}$. Write $P = Rx_1 + \cdots + Rx_n$ for $x_1, ..., x_n \in P$. If $P \neq N$, then there is a $y \in N \setminus P$ so that $Q =$

$Rx_1 + \cdots + Rx_n + Ry$ satisfies $Q \in \mathcal{S}$. But $P \subsetneq Q$, which contradicts maximality of P. Therefore $P = N$, which means N is finitely-generated.

Finally, suppose every submodule of M is finitely-generated. Let $N_1 \subseteq N_2 \subseteq \cdots$ be a chain and set $N = \bigcup_{i=1}^{\infty} N_i$. It's easy to verify that N is a submodule of M, therefore there are $x_1, ..., x_n \in N$ with $N = Rx_1 + \cdots + Rx_n$. Since each $x_j \in N = \bigcup_{i=1}^{\infty} N_i$, there are $k_1, ..., k_n$ with $x_j \in N_{k_j}$. Taking $k = \max\{k_1, ..., k_n\}$ gives each $x_j \in N_k$, which means $N = Rx_1 + \cdots + Rx_n \subseteq N_k$. This forces $N_k = N$, and thus $N = N_k = N_{k+1} = \cdots$, so M is Noetherian. □

In light of this third condition, one can roughly think of a Noetherian module as one which is "not very large".

Example 3.1.4

(1) Consider the group ($\mathbb{Z}$-module) of integers $\mathbb{Z}$. Since $\mathbb{Z}$ is commutative, all left ideals are (two-sided) ideals. $\mathbb{Z}$ being a PID implies every ideal is finitely-generated, so $\mathbb{Z}$ must be Noetherian.

(2) More generally, any PID D (viewed as a D-module) is Noetherian. This therefore includes examples such as fields and the polynomial ring $F[x]$.

(3) If D is a division ring viewed as a left D-module and $I \neq 0$ is a left ideal, then we can take $0 \neq x \in I$ and see that $1 = x^{-1}x \in I$, which means $I = D$. Hence, the only left ideals are 0 and D, and this must mean D is Noetherian.

(4) Let R be a Noetherian ring and consider the R-module R^n. Let $p_1, ..., p_n : R^n \to R$ and $i_1, ..., i_n : R \to \mathbb{R}^n$ be the associated projection homomorphisms. If N is a submodule of R^n, we can look at $p_j(N) = \{x_j \in R : (x_1, ..., x_n) \in N\}$. This must be a submodule of R, and therefore finitely-generated; say $p_j(N) = Rx_{j,1} + \cdots + Rx_{j,r_j}$. Then the set $S = \{i_j(x_{j,k}) : 1 \leqslant k \leqslant r_j, 1 \leqslant j \leqslant n\}$ generates N. As S is finite, it follows that R^n is Noetherian.

Most of our examples above are rings, so we can make the following

Definition 3.1.5 A ring R is **left (right) Noetherian** when R is Noetherian as a left (right) R-module. If R is both left and right Noetherian, it is called **Noetherian**.

Thus, in any commutative ring, being left or right Noetherian is equivalent to being Noetherian.

We next consider a similar notion, obtained by replacing the ascending chain condition with the *descending* chain condition.

Definition 3.1.6 M is called **Artinian** when it satisfies the following *descending chain condition*: given a countably-infinite descending chain $N_1 \supseteq N_2 \supseteq \cdots$ of submodules of M, there exists a $k \in \mathbb{N}$ for which $N_k = N_{k+1} = \cdots$.

A similar proposition characterizing Artinianity is:

Proposition 3.1.7 The following are equivalent:

(i) M is Artinian.

(ii) M satisfies the following *minimum condition*: every non-empty collection $\mathcal{S}$ of submodules of M has a submodule which is minimal in $\mathcal{S}$. That is, there is a $P \in \mathcal{S}$ such that for all $N \in \mathcal{S}$, $N \subseteq P$ implies $N = P$.

Proof. **Exercise 3.1.15**. □

The lack of a condition analogous to the finitely-generated submodules condition for Noetherianity means we are restricted in ways we can show a module is Artinian.

We've got a similar definition for rings being Artinian:

Definition 3.1.8 A ring R is **left (right) Artinian** when R is Artinian as a left (right) R-module. If R is both left and right Artinian, it is called **Artinian**.

Similarly any commutative ring which is either left or right Artinian is Artinian.

Example 3.1.9

(1) $\mathbb{Z}$ is *not* Artinian. Indeed, the collection of ideals $\{(2^k) : k \in \mathbb{N}\}$ doesn't have a minimal element.

(2) Any division ring D is both left and right Artinian, since the only left/right ideals are 0 and D.

(3) Fix a prime $p > 0$ and consider the $\mathbb{Z}$-module $P = \{\frac{a}{p^k} \in \mathbb{Q} : a \in \mathbb{Z}, k \in \mathbb{N}\}$. Then P is not Noetherian since we have the proper chain of submodules:

$$\mathbb{Z} \subsetneq \mathbb{Z} \cdot \tfrac{1}{p} \subsetneq \mathbb{Z} \cdot \tfrac{1}{p^2} \subsetneq \cdots$$

Moreover, since $\mathbb{Z}$ is itself a submodule of P, it follows that P can't be Artinian either.

We've thus seen examples of modules which are

- Noetherian but not Artinian,
- both Noetherian and Artinian, and
- neither Noetherian not Artinian.

Can we have a module which is Artinian but not Noetherian? **Exercise 3.1.16** shows that this is indeed possible. Remarkably, however, this is not possible if we consider rings (as we shall see later). That is, if a ring is left (right) Artinian, it must also be left (right) Noetherian.

We now collect basic properties of Noetherian and Artinian modules. First we have the easy:

Proposition 3.1.10 Let M be Noetherian (Artinian) and let N a submodule. Then N and M/N are Noetherian (Arinitian), and consequently any homomorphic image of M is Noetherian (Artinian).

Proof. We WLOG prove the Noetherian case (the Artinian case is obtained by replacing "ascending" with "descending" and "$\subseteq$" with "$\supseteq$").

Any ascending chain of submodules of N is an ascending chain of submodules of M, therefore stabilizes. Likewise, every submodule of M/N is of the form P/N where P is a submodule of M containing N. Thus, any chain $P_1/N \subseteq P_2/N \subseteq \cdots$ in M/N corresponds to the chain $P_1 \subseteq P_2 \subseteq \cdots$. This chain of P_i's must stabilize, which means the chain of P_i/N's will also stabilize.

Now if $f : M \to P$ is any R-homomorphism of M into a module P, then the result is immediate from the fact that $\operatorname{im} f \cong M/\ker f$. □

We can establish the converse too: if for any submodule N of M we have that N and M/N are Noetherian (Artinian), then M is also Noetherian (Artinian). In fact, we can say something even stronger!

Proposition 3.1.11 If there exists a submodule N with both N and M/N Noetherian (Artinian), then M is also Noetherian (Artinian).

For this, the following lemma will be useful:

Lemma 3.1.12 If N, P_1, and P_2 are submodules of M which satisfy the conditions:

- $P_1 \subseteq P_2$,
- $P_1 + N = P_2 + N$, and
- $P_1 \cap N = P_2 \cap N$,

then $P_1 = P_2$.

Proof. Let $x \in P_2 \subseteq P_2 + N = P_1 + N$. Then $x = y + z$ for $y \in P_1$ and $z \in N$. Now $y \in P_1 \subseteq P_2$ and thus $z = x - y \in P_2 \cap N = P_1 \cap N$, which means $x \in P_1$. □

Now we give the

Proof of 3.1.11. We again prove the Noetherian case. Let $P_1 \subseteq P_2 \subseteq \cdots$ be an ascending chain. Then $P_1 \cap N \subseteq P_2 \cap N \subseteq \cdots$ is an ascending chain of submodules of N, so there is a $k \in \mathbb{N}$ with $P_k \cap N = P_{k+1} \cap N = \cdots$.

Likewise, $P_1 + N \subseteq P_2 + N \subseteq \cdots$ is a chain of submodules of M, each containing N. Therefore, $(P_1 + N)/N \subseteq (P_2 + N)/N \subseteq \cdots$ is a chain in M/N, so there is an $l \in \mathbb{N}$ with $(P_l + N)/N = (P_{l+1} + N)/N = \cdots$.

Let $m = \max\{k, l\}$. Then for each $i \geqslant m$, we have $P_i \subseteq P_{i+1}$, $P_i + N = P_{i+1} + N$, and $P_i \cap N = P_{i+1} \cap N$, which by the preceding lemma implies $P_i = P_{i+1}$. Thus, the chain $P_1 \subseteq P_2 \subseteq \cdots$ stabilizes. □

Following this result we have:

Corollary 3.1.13 If N and P are Noetherian (Artinian) submodules of M, then $N + P$ is Noetherian (Artinian).

Proof. Recall that the second isomorphism theorem tells us that $(N + P)/N \cong P/(N \cap P)$. P being Noetherian (Artinian) means $P/(N \cap P)$ is as well. Thus, both $(N + P)/N$ and N are too, which means the same holds for $N + P$ by the preceding proposition. □

By induction, we see that if $P_1, ..., P_n$ are Noetherian (Artinian), then so is $P_1 + \cdots P_n$. This fact allows us to establish the following useful

Proposition 3.1.14 Let R be a left Noetherian (Artinian) ring. Then any finitely-generated (left) R-module M is Noetherian (Artinian). The same result holds if R is a right Noetherian (Artinian) ring and M is a right R-module.

Proof. M being finitely-generated means $M = Rx_1 + \cdots + Rx_n$ for some $x_1, ..., x_n \in R$. Now $f_i : R \to Rx_i$ given by $f_i(a) = ax_i$ has $\operatorname{im} f_i = Rx_i$. So R being left Noetherian (Artinian) means Rx_i is as well. By the remark above, we have $M = Rx_1 + \cdots + Rx_n$ is Noetherian (Artinian). □

Exercises

The first exercise proves proposition regarding the equivalence of the two conditions defining Artinianity. We repeat this for convenience.

Exercise 3.1.15 Show that for an R-module M, the following are equivalent:

(i) M is Artinian.

(ii) M satisfies the following *minimum condition*: every non-empty collection $\mathcal{S}$ of submodules of M has a submodule which is minimal in $\mathcal{S}$. That is, there is a $P \in \mathcal{S}$ such that for all $N \in \mathcal{S}$, $N \subseteq P$ implies $N = P$.

Exercise 3.1.16 Fix a prime $p > 0$ and consider the $\mathbb{Z}$-module $P = \{\frac{a}{p^k} \in \mathbb{Q} : a \in \mathbb{Z}, k \in \mathbb{N}\}$. We've seen in **Example 3.1.9** that P is neither Noetherian nor Artinian, and that

$$\mathbb{Z} \subsetneq \mathbb{Z} \cdot \tfrac{1}{p} \subsetneq \mathbb{Z} \cdot \tfrac{1}{p^2} \subsetneq \cdots \qquad (*)$$

is a proper ascending chain of submodules of P.

We now consider the quotient module $Q = P/\mathbb{Z}$.

(a) Use the chain $(*)$ along with the correspondence theorem to show that Q is not Noetherian.

(b) Show that every submodule N of P satisfying $\mathbb{Z} \subseteq N$ must be of the form $N = \mathbb{Z} \cdot \frac{1}{p^k}$ for some $k \in \mathbb{Z}$.

(c) Hence, use the correspondence theorem to conclude that Q must be Artinian.

Exercise 3.1.17 Let M be an R-module and let $f \in \mathrm{End}_R(M)$. Show that if M is Noetherian and f is surjective, then f is an isomorphism. Show that the same conclusion holds if we assume instead that M is Artinian and f is injective.

Exercise 3.1.18 Let V be a vector space over a field F. Show that the following conditions are equivalent:

(i) V is finite-dimensional.

(ii) V is Noetherian.

(iii) V is Artinian.

Recall that for any vector space V over F and operator $T \in \mathrm{End}_F(V)$, V has an $F[\lambda]$-module structure given by the action $f(\lambda) \cdot v = f(T)v$. Denote this by V_T.

Exercise 3.1.19 Let V be a vector space with countable basis $\{e_1, e_2, e_3, ...\}$ and let $S, T \in \mathrm{End}_F(V)$ be the left and right shift operators given by:

- $Se_i = e_{i-1}$ for $i > 1$ and $Se_1 = 0$.
- $Te_i = e_{i+1}$ for $i \geqslant 1$.

Show that the $F[\lambda]$-module V_S is Artinian and the $F[\lambda]$-module V_T is Noetherian.

3.2 Composition series

We now seek to obtain a condition on an R-module M which is equivalent to M being both Noetherian and Artinian. For this, we need to introduce the notion of a *composition series* of M.

Definition 3.2.1 A **series** for M is a descending chain of submodules of the form:

$$0 = J_0 \subseteq J_1 \subseteq \cdots \subseteq J_s = M$$

We call s the **length** of the series. The quotient modules J_i/J_{i-1} are called the **factors** of the series. The series is called **proper** when each $J_{i-1} \subsetneq J_i$.

Example 3.2.2

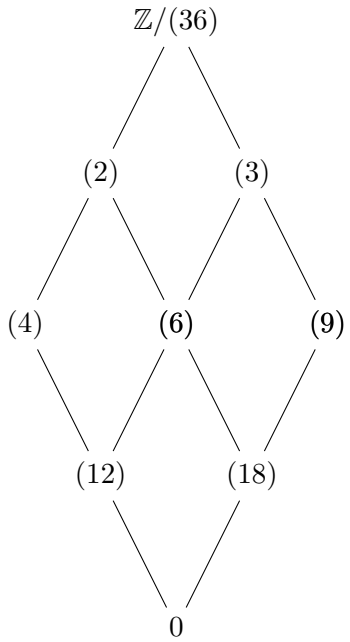
(1) Let V be a vector space over F with basis $\{e_1, ..., e_n\}$. If $W_k = \{e_1, ..., e_k\}$ for $1 \leqslant k \leqslant n$ and $W_0 = 0$, then

$$0 = W_0 \subseteq W_1 \subseteq \cdots \subseteq W_n = V$$

is a series for V. Each quotient W_i/W_{i-1} is a one-dimensional vector space.

(2) Consider the $\mathbb{Z}$-module $\mathbb{Z}/(n)$. The submodules are ideals of the form $(m) = \{mk + (n) : k \in \mathbb{Z}\}$ where $m \mid n$ and $m \geqslant 1$.

For example, the $\mathbb{Z}$-module $\mathbb{Z}/(36)$ has the following lattice of submodules:



Any chain of submodules going from bottom to top (with 0 as the first submodule and $\mathbb{Z}/(n)$ as the last submodule) is a series in $\mathbb{Z}/(n)$. For example, some series in $\mathbb{Z}/(36)$ are:

$$0 \subseteq (12) \subseteq (6) \subseteq (2) \subseteq \mathbb{Z}/(36)$$

$$0 \subseteq (9) \subseteq (3) \subseteq \mathbb{Z}/(36)$$

$$0 \subseteq (6) \subseteq (2) \subseteq \mathbb{Z}/(36)$$

All of these are examples of *proper* series.

Definition 3.2.3 Let

$$0 = J_0 \subseteq J_1 \subseteq \cdots \subseteq J_s = M$$

be a series in M. A **refinement** of the series is any other series of which (J_i) is a *subseries*. More precisely, if

$$0 = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t = M$$

is a series in M, then (K_i) is a refinement of (J_i) when there exist $0 = p_0 < p_1 < \cdots < p_s = t$ for which $K_{p_i} = J_i$ for each i.

For instance, the series $0 \subseteq (12) \subseteq (6) \subseteq (2) \subseteq \mathbb{Z}/(36)$ considered in the example above is a refinement of $0 \subseteq (6) \subseteq (2) \subseteq \mathbb{Z}/(36)$.

Finally, we get to:

Definition 3.2.4 A **composition series** in M is a proper series:

$$0 = J_0 \subsetneq J_1 \subsetneq \cdots \subsetneq J_s = M$$

which has no proper refinement.

Not all modules have a composition series. For instance, if $0 = J_0 \subsetneq J_1 \subsetneq \cdots \subsetneq J_s = \mathbb{Z}$ is a proper series in $\mathbb{Z}$, then the J_i's are just ideals of $\mathbb{Z}$. If $J_1 = (m)$ for some $m \in \mathbb{Z}$, then $m \neq 0$ and we can take $J' = (2m)$ to obtain a proper refinement $0 \subsetneq J' \subsetneq J_1 \subsetneq \cdots \subsetneq J_s = \mathbb{Z}$.

On the other hand, our series $0 \subsetneq (12) \subsetneq (6) \subsetneq (2) \subsetneq \mathbb{Z}/(36)$ is a composition series in $\mathbb{Z}/(36)$, which is easily seen by looking at the lattice considered in **Example 3.2.2 (2)**.

We can understand a composition series in terms of its factor modules. Recall that a module M is *irreducible* when $M \neq 0$ and M contains no proper non-zero submodules.

Proposition 3.2.5 Let

$$0 = J_0 \subseteq J_1 \subseteq \cdots \subseteq J_s = M$$

be a series in M. This is a composition series if and only if each factor J_i/J_{i-1} is irreducible.

Proof. Suppose this is a composition series. The fact that it is proper means $J_i/J_{i-1} \neq 0$. Suppose K/J_{i-1} is a non-zero submodule of J_i/J_{i-1}. Then $J_{i-1} \subsetneq K \subseteq J_i$. Since the series has no proper refinement, this forces $K = J_i$ and $K/J_{i-1} = J_i/J_{i-1}$, making J_i/J_{i-1} irreducible.

Now suppose each factor J_i/J_{i-1} is irreducible. That $J_i/J_{i-1} \neq 0$ implies $J_{i-1} \subsetneq J_i$. If the series had a refinement, then there would be some submodule K with $J_{i-1} \subsetneq K \subsetneq J_i$ for some i. But then K/J_{i-1} would be a proper non-zero submodule of J_i/J_{i-1}, contradicting irreducibility. Therefore, (J_i) must be a composition series. □

We next aim to prove the following

Proposition 3.2.6 M has a composition series if and only if M is both Noetherian and Artinian.

Towards this, we need some preliminary results on series. First we have the following

Definition 3.2.7 Let

$$0 = J_0 \subseteq J_1 \subseteq \cdots \subseteq J_s = M$$

$$0 = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t = M$$

be two series in M. We say these series are **equivalent** when $s = t$ and there exists a permutation σ of $\{1, ..., s\}$ such that $J_i/J_{i-1} \cong K_{\sigma(i)}/K_{\sigma(i)-1}$.

In other words, two series are equivalent when the have the same length and the same collection of factor modules up to isomorphism (counting multiplicity).

Example 3.2.8 In the $\mathbb{Z}$-module $\mathbb{Z}/(36)$, consider the two series:

$$0 \subseteq (12) \subseteq (4) \subseteq (2) \subseteq \mathbb{Z}/(36)$$

$$0 \subseteq (18) \subseteq (6) \subseteq (3) \subseteq \mathbb{Z}/(36)$$

We see that:

- $(12)/0 \cong \mathbb{Z}/(3)$, $(4)/(12) \cong \mathbb{Z}/(3)$, $(2)/(4) \cong \mathbb{Z}/(2)$, and $(\mathbb{Z}/(36))/(2) \cong \mathbb{Z}/(2)$; and
- $(18)/0 \cong \mathbb{Z}/(2)$, $(6)/(18) \cong \mathbb{Z}/(3)$, $(3)/(6) \cong \mathbb{Z}/(2)$, and $(\mathbb{Z}/(36))/(3) \cong \mathbb{Z}/(3)$.

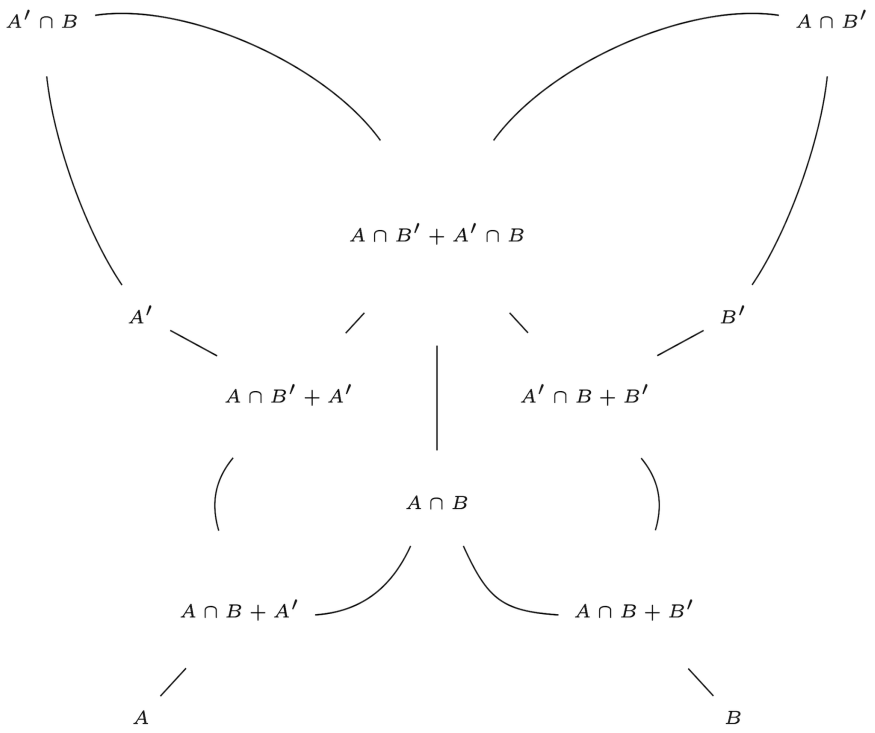
Thus, the collection of factor modules for each series consist of two factors isomorphic to $\mathbb{Z}/(2)$ and two isomorphic to $\mathbb{Z}/(3)$, which means these series are equivalent.

Both series in the example above are composition series. One can also check that the other two composition series of $\mathbb{Z}/(36)$ are equivalent to the two considered above. It is in fact the case that *any* two composition series for a module are equivalent. Towards proving this, we have the following

Lemma 3.2.9 (Butterfly lemma)
Let A, A', B, B' be submodules of M with $A' \subseteq A$ and $B' \subseteq B$. Then

$$\frac{A \cap B + A'}{A \cap B' + A'} \cong \frac{A \cap B + B'}{A' \cap B + B'}$$

Proof. The name comes from the reverse lattice diagram of the submodules considered in this lemma, which can be drawn in the shape of a butterfly:



The key observation to make here is that the left wing of the butterfly is the mirror image of the right wing with the symbols A and B interchanged.

Let $D = A \cap B' + A' \cap B$. This is a submodule of $A \cap B$ of course, so we can consider the quotient $(A \cap B)/D$. D is also "symmetric" in the sense that after interchanging the symbols A and B, D remains the same. Thus, if we can show that

$$\frac{A \cap B + A'}{A \cap B' + A'} \cong \frac{A \cap B}{D} \tag{$*$}$$

then we have by symmetry that $\frac{A \cap B + B'}{A' \cap B + B'} \cong \frac{A \cap B}{D}$, which proves the desired isomorphism.

To that end, let $\varphi : A \cap B + A' \to \frac{A \cap B}{D}$ be defined by $\varphi(x + a) = x + D$ for all $x \in A \cap B$ and all $a \in A'$. To see this is well-defined, suppose $x + a = x' + a'$ for some other $x' \in A \cap B$ and $a' \in A'$. Then $x' - x = a - a' \in A' \cap B \subseteq D$, which means $x + D = x' + D$. It's clear that φ is a surjective R-homomorphism. We show that $\ker \varphi = A \cap B' + A'$.

Indeed, notice first that for $y \in A \cap B'$ and $a \in A'$, we have $\varphi(y + a) = y + D = D$ since $y \in A \cap B' \subseteq D$. Thus $A \cap B' + A' \subseteq \ker \varphi$. On the other hand, suppose $\varphi(x + a) = D$ for a given $x \in A \cap B$ and $a \in A'$. Then $x \in D = A \cap B' + A' \cap B$, so we can write $x = \alpha + \beta$ for $\alpha \in A \cap B'$ and $\beta \in A' \cap B$. Now $x + a = \alpha + (\beta + a) \in A \cap B' + A'$, which shows $\ker \varphi \subseteq A \cap B' + A'$. The first isomorphism theorem then gives $(*)$. $\square$

The technical butterfly lemma can be thought of as a generalization of the second isomorphism theorem. This is due to Zassenhaus, who wrote it in order to give a more elegant proof of the following

Theorem 3.2.10 (Schreier refinement theorem)
Any two series for M have equivalent refinements.

Proof. Let

$$0 = J_0 \subseteq J_1 \subseteq \cdots \subseteq J_s = M$$

$$0 = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_t = M$$

be two series for M. For each $0 \leqslant i < s$ and $0 \leqslant j < t$, let $J_{i,j} = J_{i+1} \cap K_j + J_i$ and $K_{j,i} = J_i \cap K_{j+1} + K_j$. It will also be convenient to set:

- $J_{i,t} = J_{i+1} \cap K_t + J_i = J_{i+1}$,
- $K_{j,s} = J_s \cap K_{j+1} + K_j = K_{j+1}$,
- $J_{s,0} = K_{t,0} = M$

from which we observe that $J_{i,t} = J_{i+1,0}$ and $K_{j,s} = K_{j+1,0}$.

For each $0 \leqslant i < s$ we have:

$$J_i = J_{i,0} \subseteq J_{i,1} \subseteq \cdots \subseteq J_{i,t-1} \subseteq J_{i,t} = J_{i+1,0}$$

and for each $0 \leqslant j < t$:

$$K_j = K_{j,0} \subseteq K_{j,1} \subseteq \cdots \subseteq K_{j,s-1} \subseteq K_{j,s} = K_{j+1,0}$$

Thus, we have the two series:

$$\begin{aligned} 0 &= J_{0,0} \subseteq J_{0,1} \subseteq \cdots \subseteq J_{0,t-1} \\ &\subseteq J_1 = J_{1,0} \subseteq J_{1,1} \subseteq \cdots \subseteq J_{1,t-1} \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &\subseteq J_{s-1} = J_{s-1,0} \subseteq J_{s-1,1} \subseteq \cdots \subseteq J_{s-1,t-1} \\ &\subseteq J_{s,0} = M \end{aligned}$$

and:

$$\begin{aligned} 0 &= K_{0,0} \subseteq K_{0,1} \subseteq \cdots \subseteq K_{0,s-1} \\ &\subseteq K_1 = K_{1,0} \subseteq K_{1,1} \subseteq \cdots \subseteq K_{1,s-1} \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &\subseteq K_{t-1} = K_{t-1,0} \subseteq K_{t-1,1} \subseteq \cdots \subseteq K_{t-1,s-1} \\ &\subseteq K_{t,0} = M \end{aligned}$$

It's clear that the first of these series is a refinement of (J_i) and the second is a refinement of (K_j). Moreover, they have the same length (namely, st). It remains to show that they are equivalent.

Indeed, given $0 \leqslant i < s$ and $0 \leqslant j < t$, we see from the butterfly lemma that:

$$\frac{J_{i,j+1}}{J_{i,j}} = \frac{J_{i+1} \cap K_{j+1} + J_i}{J_{i+1} \cap K_j + J_i} \cong \frac{J_{i+1} \cap K_{j+1} + K_j}{J_i \cap K_{j+1} + K_j} = \frac{K_{j,i+1}}{K_{j,i}}$$

so all the factor modules are in bijection, making the refinements equivalent. □

With this, we can prove the

Theorem 3.2.11 (Jordan-Hölder theorem)
Any two composition series for M are equivalent.

Proof. Let $P_1, ..., P_m$ and $Q_1, ..., Q_n$ be the *factors* of each composition series. These are irreducible (thus non-zero) R-modules. Choose equivalent refinements for the series and let $P'_1, ..., P'_r$ and $Q'_1, ..., Q'_r$ be their respective factors, where $r \geqslant m, n$. These are in isomorphism-preserving bijection: there is a permutation σ on $\{1, ..., r\}$ such that $P'_i \cong Q'_{\sigma(i)}$.

Since the refinements aren't proper, any modules added to each composition series must be duplicates of existing ones. Thus we have WLOG that $P'_i \cong P_i$ for $1 \leqslant i \leqslant m$ and $P'_i = 0$ for $i > m$. Similarly $Q'_j \cong Q_j$ for $1 \leqslant j \leqslant n$ and $Q'_j = 0$ for $j > n$. We have $r - m$ of the $P'_1, ..., P'_r$ are 0 and $r - n$ of the $Q'_1, ..., Q'_r$ are 0. Since the bijection preserves isomorphisms, we must have that the 0 modules are sent to the 0 modules, which means $r - m = r - n$ and thus $m = n$. In particular, this implies both composition series have the same length.

Now $P_i \cong P'_i \cong Q'_{\sigma(i)} \cong Q_{\sigma(i)}$ for each $1 \leqslant i \leqslant m$ and $P_i = Q_i = 0$ for $i > m$, so the composition series must be equivalent. □

Finally, we use this theorem to establish

Proposition 3.2.12 A module M has a composition series if and only if M is both Noetherian and Artinian.

Proof. We can assume $M \neq 0$ (the $M = 0$ case is trivial). Suppose M is Noetherian and Artinian. Let $M_1 = M$ and let $\mathcal{S}_1$ be the set of *proper* submodules of M_1. Since M is Noetherian, there exists a maximal element $M_2 \in \mathcal{S}_1$. If $M_2 = 0$, we can form the series $0 = M_2 \subseteq M_1 = M$ which is a composition series by maximality of M_2 in M_1. Otherwise, let $\mathcal{S}_2$ be the set of proper submodules of M_2 and take maximal $M_3 \in \mathcal{S}_2$.

Repeating this process, we will eventually find an $n \in \mathbb{N}$ for which $M_n = 0$; if not, then we would have a strictly descending chain $M = M_1 \supsetneq M_2 \supsetneq \cdots$ of submodules, contradicting Artinianity. Hence, we form $0 = M_n \subseteq M_{n-1} \subseteq \cdots \subseteq M_1 = M$, which by construction is a composition series since each M_{i+1} is maximal in M_i.

Now suppose M has a composition series; say $0 = J_0 \subseteq J_1 \subseteq \cdots \subseteq J_s = M$. Let $0 \subsetneq N_1 \subsetneq N_2 \subsetneq \cdots$ be a proper ascending chain of submodules of M. Then given any $t \geqslant 1$, $0 = N_0 \subsetneq N_1 \subsetneq \cdots \subsetneq N_t \subsetneq M$ is a proper series in M. We can thus find equivalent refinements of (J_i) and (N_j). Since (J_i) is a composition series, the number of non-zero factors of the refinements must be s, which forces $t \leqslant s$. Thus, every ascending chain must stabilize.

If instead we have a proper descending chain $M \supsetneq N_1 \supsetneq N_2 \supsetneq \cdots$ of submodules, each $t \in \mathbb{N}$ yields a series $0 \subsetneq N_t \subsetneq N_{t-1} \subsetneq \cdots \subsetneq N_1 \subsetneq M$. A similar argument shows then that $t \leqslant s$, so every descending chain must stabilize as well. □

We have in particular that any two composition series of M have the same length. Thus, for modules which are Noetherian and Artinian, it makes sense to define the notion of *length* for the module itself.

Definition 3.2.13 Suppose M is a module which is Noetherian and Artinian. The **length** of M is defined to be the length of a composition series of M. We denote this by $\ell(M)$.

We often say a module M has **finite length** when M is both Noetherian and Artinian. Otherwise we say M has **infinite length**.

It's often useful to define $\ell(M)$ as the longest proper chain (either ascending or descending) of submodules. The proof of the proposition explains why this agrees with the definition given above, as it shows that if $N_1 \subseteq \cdots \subseteq N_t$ is any proper chain of submodules, then its length $t - 1$ can't exceed the length of a given composition series.

Example 3.2.14

(1) The notion of length is a natural generalization of *dimension* of a vector space. We have seen in **Exercise 3.1.18** that a vector space V being finite-dimensional, Noetherian, or Artinian are equivalent. If $\{e_1, ..., e_n\}$ is a basis for V, $W_0 = 0$, and $W_k = \{e_1, ..., e_k\}$ for each $1 \leqslant k \leqslant n$, then

$$0 = W_0 \subseteq W_1 \subseteq \cdots \subseteq W_n = V$$

is a composition series in V, so the length of V is its dimension n.

(2) If M is any module, then $M = 0$ if and only if its length is 0 and M is irreducible if and only if its length is 1.

If M has finite length, then we know that it must be Noetherian, thus every submodule is finitely generated. We therefore have in particular that:

Corollary 3.2.15 Every module of finite length is finitely generated.

Exercises

Exercise 3.2.16 Let N and P be submodules of an R-module M.

(a) Show that M has finite length if and only if N and M/N have finite length, in which case $\ell(N) + \ell(M/N) = \ell(M)$.

(b) Show that if M has finite length, then $\ell(N + P) = \ell(N) + \ell(P) - \ell(N \cap P)$.

Exercise 3.2.17 Consider the $\mathbb{Z}$-module $\mathbb{Z}/(n)$ for $n > 0$.

(a) Show that $\mathbb{Z}/(n)$ is both Noetherian and Artinian.

(b) Compute $\ell(\mathbb{Z}/(n))$ by finding a composition series.

3.3 Structure of finite-length modules

We now consider the structure theory of finite-length modules. First, let M be any module (not necessarily of finite length). Recall that if $M_1, ..., M_k$ is a collection of submodules of M such that

- $M_1 + \cdots + M_k = M$, and
- $M_i \cap (\sum_{j \neq i} M_j) = 0$ for all i,

then $M \cong M_1 \oplus \cdots \oplus M_k$, the direct sum of the M_i's. In this case we simply write $M = M_1 \oplus \cdots \oplus M_k$ and say M is the **internal direct sum** of the M_i's. We also have in this case that each $x \in M$ can be written as $x = x_1 + \cdots + x_k$ for *unique* $x_i \in M_i$.

Definition 3.3.1 M is said to be **indecomposable** when $M \neq 0$ and there are no non-zero submodules M_1 and M_2 such that $M = M_1 \oplus M_2$.

We say M is **(finitely) completely decomposable** when there exist indecomposable submodules $M_1, ..., M_k$ of M for which $M = M_1 \oplus \cdots \oplus M_k$.

We add the term *finitely* to this last definition because complete decomposability extends to the care where M can be written as an arbitrary internal direct sum of submodules. We will not be concerned with this case here, and as such *completely decomposable* will mean *finitely completely decomposable* in this section.

We aim to show that if M has finite length, then M is completely decomposable. Moreover, this decomposition is unique up to isomorphism (and reordering).

Towards this, it will be useful to find an equivalent characterization of indecomposability. Recall that if $M = M_1 \oplus \cdots \oplus M_k$ for submodules $M_1, ..., M_n$, then we have a corresponding *partition of the identity* $e_1, ..., e_k \in \mathrm{End}_R(M)$, which means:

- the e_i's are idempotents: $e_i^2 = e_i$ for each i;
- the e_i's are orthogonal: $e_i e_j = 0$ for $i \neq j$; and
- $e_1 + \cdots + e_k = \mathrm{id}_M$.

Explicitly, if $x = x_1 + \cdots + x_k \in M$ where each $x_i \in M_i$, then e_i is the map given by $e_i(x) = x_i$. Using this, we can show:

Proposition 3.3.2 $M \neq 0$ is indecomposable if and only if the only idempotents in $\mathrm{End}_R(M)$ are 0 and id_M.

Proof. Suppose there exists an idempotent $e \in \mathrm{End}_R(M)$ with $e \neq 0, \mathrm{id}_M$. Then $f = \mathrm{id}_M - e \in \mathrm{End}_R(M)$ is also an idempotent with $f \neq 0, \mathrm{id}_M$. Let $M_1 = \mathrm{im}\, e$ and $M_2 = \mathrm{im}\, f$; certainly $M_1, M_2 \neq 0$. We find then that if $x \in M$ and we set $x_1 = e(x)$ and $x_2 = f(x)$, then $x_1 + x_2 = e(x) + x - e(x) = x$, so $M_1 + M_2 = M$. Moreover, if $y \in M_1 \cap M_2$ then $y = e(x) = f(x') = x' - e(x')$ for some $x, x' \in M$, in which case $y = e(y) = e(x') - e(x') = 0$. Thus, $M = M_1 \oplus M_2$ and M is not indecomposable.

Conversely, suppose $M = M_1 \oplus M_2$ for submodules $M_1, M_2 \neq 0$. Let e_1, e_2 be the corresponding partition of id_M. Since $\mathrm{im}\, e_1 = M_1$, clearly $e_1 \neq 0$. Moreover, $e_2 = \mathrm{id}_M - e_1 \neq 0$ so that $e_1 \neq \mathrm{id}_M$. Hence, e_1 is an example of an idempotent $\neq 0, \mathrm{id}_M$. □

Now let's see some examples.

Example 3.3.3

(1) Suppose M is an irreducible R-module ($M \neq 0$ and has no proper non-zero submodules). By Schur's lemma (**Lemma 2.3.12**), $\mathrm{End}_R(M)$ is a division ring. If $e \in \mathrm{End}_R(M)$ was idempotent with $e \neq 0$, then $e^2 = e$ implies $e = 1$. Hence, M is indecomposable.

(2) On the other hand, being irreducible is *strictly* stronger than being indecomposable. This can be seen with $\mathbb{Z}/(4)$. The only proper non-zero submodule is $(2) = \{0, 2\}$ (which means it isn't irreducible). But suppose $\mathbb{Z}/(4) = M_1 \oplus M_2$ for submodules M_1, M_2. Then we can write $1 = x + y$ for $x \in M_1$ and $y \in M_2$. Clearly at least one of M_1 or M_2 must be $\mathbb{Z}/(4)$ (as there is no way to sum elements from $\{0, 2\}$ to obtain 1), and this forces the other to be 0.

(3) $\mathbb{Z}/(6)$ is neither irreducible nor indecomposable. However, notice that the ideals $(2) = \{0, 2, 4\}$ and $(3) = \{0, 3\}$ of $\mathbb{Z}/(6)$ are indecomposable. Moreover, $(2) \cap (3) = 0$ and since $1 = 2 \cdot 2 + 3$, it's clear that any element of $\mathbb{Z}/(6)$ can be written as $2 \cdot k + 3 \cdot l \in (2) + (3)$. Hence, $\mathbb{Z}/(6) = (2) \oplus (3)$. In particular, $\mathbb{Z}/(6)$ is completely decomposable.

Recall that for a ring R, we have the group of *units* $R^\times = \{u \in R : u \text{ is invertible}\}$.

Definition 3.3.4 R is called **local** when $R \setminus R^\times$ is an ideal.

Note that this condition automatically implies $R \neq 0$. We will not study local rings in detail – we leave some of this to **Exercise 3.3.13**. The property we are interested in is:

Proposition 3.3.5 If R is a local ring, then its only idempotents are 0 and 1.

Proof. Suppose e is idempotent with $e \neq 0, 1$. Then $e(1-e) = 0$. Since $1-e \neq 0$, we have $e \in R \backslash R^\times$. Similarly $1-e \in R \backslash R^\times$ since $e \neq 0$. But then $1 = e+1-e \in R \backslash R^\times$, which is impossible. □

We've seen that $M \neq 0$ is indecomposable if and only if the only idempotents of $\mathrm{End}_R(M)$ are 0 and id_M. Thus, if M is any module where $\mathrm{End}_R(M)$ is a local ring (which implies automatically that $M \neq 0$), then M is indecomposable.

Definition 3.3.6 M is called **strongly indecomposable** when $\mathrm{End}_R(M)$ is a local ring.

We shall show that if M is of finite length, then indecomposability and strong indecomposability are equivalent. For this, we consider the following: let $f \in \mathrm{End}_R(M)$. Then we have the following chains:

- $M = \mathrm{im}\, f^0 \supseteq \mathrm{im}\, f \supseteq \mathrm{im}\, f^2 \supseteq \cdots$
- $0 = \ker f^0 \subseteq \ker f \subseteq \ker f^2 \subseteq \cdots$

Notice we can express $\mathrm{im}\, f^k = f^k(M)$ and $\ker f^k = f^{-k}(0)$ for $k \geqslant 0$. Thus, we define:

$$f^\infty(M) = \bigcap_{k=0}^{\infty} \mathrm{im}\, f^k \quad \text{and} \quad f^{-\infty}(0) = \bigcup_{k=0}^{\infty} \ker f^k$$

and the notation we use makes sense. These are submodules of M (the fact that $\ker f^k \subseteq \ker f^{k+1}$ for each k gives us that $f^{-\infty}(0)$ is indeed a submodule). Moreover, each is f-invariant: if $x \in f^\infty(M)$ then $x \in \mathrm{im}\, f^k$ for each $k \geqslant 0$ and thus $f(x) \in \mathrm{im}\, f^{k+1}$. Clearly also $f(x) \in \mathrm{im}\, f^0$, so $f(x) \in f^\infty(M)$.

Similarly if $x \in f^{-\infty}(0)$, then $f^k(x) = 0$ for some $k \geqslant 0$. Now $y = f(x)$ satisfies $f^k(y) = f^{k+1}(x) = f(f^k(x)) = f(0) = 0$, which means $f(x) \in f^{-\infty}(0)$.

The above shows that $f|_{f^\infty(M)} \in \mathrm{End}_R(f^\infty(M))$ and $f|_{f^{-\infty}(0)} \in \mathrm{End}_R(f^{-\infty}(0))$. What can we say if M is of finite length?

Lemma 3.3.7 (Fitting lemma)
Let M be a finite-length module and $f \in \mathrm{End}_R(M)$. Then we have

$$M = f^\infty(M) \oplus f^{-\infty}(0)$$

This is called the **Fitting decomposition**. Moreover, $f|_{f^\infty(M)}$ is an automorphism and $f|_{f^{-\infty}(0)}$ is nilpotent.

Proof. We consider the chains:

- $M = \operatorname{im} f^0 \supseteq \operatorname{im} f \supseteq \operatorname{im} f^2 \supseteq \cdots$
- $0 = \ker f^0 \subseteq \ker f \subseteq \ker f^2 \subseteq \cdots$

Since M is of finite length, these must stabilize. Take $r \in \mathbb{N}$ large enough so that $\operatorname{im} f^r = \operatorname{im} f^{r+1} = \cdots$ and $\ker f^r = \ker f^{r+1} = \cdots$. Then we have $f^\infty(M) = \operatorname{im} f^r$ and $f^{-\infty}(0) = \ker f^r$.

Now if $x \in \operatorname{im} f^r \cap \ker f^r$, then $x = f^r(y)$ for some $y \in M$. On the other hand, $f^r(x) = f^{2r}(y) = 0$ so $y \in \ker f^{2r} = \ker f^r$. This means $x = f^r(y) = 0$, which gives $\operatorname{im} f^r \cap \ker f^r = 0$.

Let $y \in M$. Then $f^r(y) \in \operatorname{im} f^r = \operatorname{im} f^{2r}$ so that $f^r(y) = f^{2r}(x)$ for $x \in M$. Write $y = f^r(x) + y - f^r(x)$. Then $f^r(x) \in \operatorname{im} f^r$ and $f^r(y - f^r(x)) = f^r(y) - f^{2r}(x) = 0$. Hence, $y \in \operatorname{im} f^r + \ker f^r$, from which we conclude that $M = \operatorname{im} f^r \oplus \ker f^r = f^\infty(M) \oplus f^{-\infty}(0)$.

Finally, $f|_{f^{-\infty}(0)} = f|_{\ker f^r}$, which means $f|^r_{\ker f^r} = 0$ (so $f|_{f^{-\infty}(0)}$ is nilpotent). Now consider $f|_{f^\infty(M)} = f|_{\operatorname{im} f^r}$. Since $\operatorname{im} f^r = \operatorname{im} f^{r+1}$, it's clear that $f|_{\operatorname{im} f^r}$ is surjective. If $f(x) = 0$ for $x \in \operatorname{im} f^r$, then $f^{r+1}(x) = 0$, which means $x \in \ker f^{r+1} = \ker f^r$. Now $x \in \ker f^r \cap \operatorname{im} f^r = 0$, which makes $f|_{\operatorname{im} f^r}$ injective. Thus, $f|_{f^\infty(M)}$ is an automorphism. □

Proposition 3.3.8 Suppose M is indecomposable and has finite length. Then any $f \in \operatorname{End}_R(M)$ is either an automorphism or nilpotent. Moreover, M is strongly indecomposable.

Proof. By the Fitting lemma, $M = f^\infty(M) \oplus f^{-\infty}(0)$. But since M is indecomposable, either $f^\infty(M) = 0$ or $f^{-\infty}(M) = 0$, in which case either $f^{-\infty}(0) = M$ or $f^\infty(M) = M$. In the former case, it follows that $f = f|_{f^{-\infty}(0)}$ is nilpotent, and in the latter we have $f = f|_{f^\infty(M)}$ is an automorphism.

Now we show that $\operatorname{End}_R(M)$ is local, which means showing $I = \operatorname{End}_R(M) \backslash \operatorname{Aut}_R(M)$ is an ideal. Let $f, g \in I$ and let $h \in \operatorname{End}_R(M)$. Then f and g must be nilpotent, which means they can't be injective or surjective. Therefore, hf and fh can't be automophisms, which means $hf, fg \in I$. Next, suppose $f + g$ is an automorphism. Let $k = (f+g)^{-1}$ so that $k(f+g) = kf + kg = \mathrm{id}_M$. Then $kg = \mathrm{id}_M - kf$, and since kf is nilpotent, kg must be an automorphism (namely, if $(kf)^r = 0$, one can check that $(kg)^{-1} = \mathrm{id}_M + kf + (kf)^2 + \cdots + (kf)^{r-1}$). But this contradicts $kg \in I$. Hence, we must have $f + g \in I$, which makes I an ideal. □

Thus, we've shown that every indecomposable module of finite length is strongly indecomposable, so in our structure theorem for finite-length modules, we equivalently consider a decomposition into strongly indecomposable submodules.

We can now state the structure theorem we wish to show.

Theorem 3.3.9 (Krull-Schmidt)
Let $M \neq 0$ be an R-module of finite length. Then M is completely decomposable. That is, there exist indecomposable submodules $M_1, ..., M_k$ of M for which

$$M = M_1 \oplus \cdots \oplus M_k$$

Moreover, this decomposition is unique up to isomorphism (and reordering) in the following sense: given another decomposition $M = N_1 \oplus \cdots \oplus N_l$ for N_i indecomposable, we have $k = l$ and a bijection $\sigma \in S_k$ with $M_i \cong N_{\sigma(i)}$ for each $i \in \{1, ..., k\}$.

The uniqueness part of the proof is based on a more general result, which requires the following

Lemma 3.3.10 Let M and N be R-modules with $M \neq 0$ and N indecomposable. Let $f \in \mathrm{Hom}_R(M, N)$ and $g \in \mathrm{Hom}_R(N, M)$ be such that $gf \in \mathrm{Aut}_R(M)$. Then f and g must be isomorphisms.

Proof. Let $h \in \mathrm{Aut}_R(M)$ be such that $hgf = gfh = \mathrm{id}_M$. Set $k = hg \in \mathrm{Hom}_R(N, M)$ so that $kf = \mathrm{id}_M$. We now look at $fk \in \mathrm{End}_R(N)$. Notice $(fk)^2 = (fhg)^2 = f(hgf)hg = fhg = fk$, so fk is idempotent. Since N is irreducible, this forces $fk = 0$ or $fk = \mathrm{id}_N$. But if $fk = 0$ then $0 = g(fk)f = gf\,\mathrm{id}_M = gf \in \mathrm{Aut}_R(M)$, which isn't possible since $M \neq 0$. Thus, we have $fk = \mathrm{id}_N$, which means f is an isomorphism with inverse k. Since $g = h^{-1}k$, g is also an isomorphism. □

The aforementioned more general result is the technical

Proposition 3.3.11 Suppose M and N are R-modules with

$$M = M_1 \oplus \cdots \oplus M_k$$

$$N = N_1 \oplus \cdots \oplus N_l$$

where the M_i are strongly indecomposable submodules of M and the N_j are indecomposable submodules of N. If $M \cong N$, then $k = l$ and there exists a bijection $\sigma \in S_k$ with $M_i = N_{\sigma(i)}$ for each $i \in \{1, ..., k\}$.

Proof. We do induction on k. If $k = 1$, then we have $M_1 \cong N = N_1 \oplus \cdots \oplus N_l$. Since M_1 is strongly indecomposable (therefore indecomposable), we must have $l = 1$ and $M_1 \cong N_1$.

Now suppose $k > 1$ and the result holds for a direct sum of $k - 1$ or fewer strongly indecomposable submodules. Let $e_1, ..., e_k \in \mathrm{End}_R(M)$ and $f_1, ..., f_l \in \mathrm{End}_R(N)$ be the respective partitions of the identity for the direct sums above. Let $g : M \to N$ be an isomorphism and for each $j \in \{1, ..., l\}$, set

$$h_j = f_j g e_1 \in \mathrm{Hom}_R(M, N) \quad \text{and} \quad k_j = e_1 g^{-1} f_j \in \mathrm{Hom}_R(N, M)$$

Then we have

$$\textstyle\sum_{j=1}^{l} k_j h_j = \sum_{j=1}^{l} (e_1 g^{-1} f_j)(f_j g e_1) = e_1 g^{-1} \left(\sum_{j=1}^{l} f_j \right) g e_1 = e_1 g^{-1} g e_1 = e_1^2 = e_1$$

Now $e_1|_{M_1} = \mathrm{id}_{M_1}$ and clearly $(k_j h_j)|_{M_1} \in \mathrm{End}_R(M_1)$, so we have $\sum_{j=1}^{l} (k_j h_j)|_{M_1} = \mathrm{id}_{M_1}$. Since $\mathrm{End}_R(M_1)$ is local, at least one of $(k_j h_j)|_{M_1}$ must be an automorphism. Assume WLOG this is true for $(k_1 h_1)|_{M_1}$. Notice that $h_1|_{M_1} \in \mathrm{Hom}_R(M_1, N_1)$ and $k_1|_{N_1} \in \mathrm{Hom}_R(N_1, M_1)$, which means $(k_1 h_1)|_{M_1} = k_1|_{N_1} h_1|_{M_1}$. The preceding lemma thus gives that $h_1|_{M_1}$ and $k_1|_{N_1}$ are isomorphisms.

With this, we show that:

$$M = g^{-1}(N_1) \oplus (M_2 \oplus \cdots \oplus M_k)$$

Indeed, if $x \in g^{-1}(N_1) \cap (M_2 \oplus \cdots \oplus M_k)$, then $y = g(x) \in N_1$ and $e_1(x) = 0$. We can write

$$0 = e_1(x) = e_1 g^{-1}(y) = e_1 g^{-1} f_1(y) = k_1(y) = k_1|_{N_1}(y)$$

which forces $y = 0$ since $k_1|_{N_1}$ is an isomorphism. This gives $x = g^{-1}(0) = 0$, so $g^{-1}(N_1) \cap (M_2 \oplus \cdots \oplus M_k) = 0$.

Now let $M' = g^{-1}(N_1) \oplus (M_2 \oplus \cdots \oplus M_k) \subseteq M$. For any $x \in g^{-1}(N_1)$, we have $x \in M'$ as well as $e_i(x) \in M_i \subseteq M'$ for $i \geqslant 2$. As such, we also have

$$e_1(x) = x - e_2(x) - \cdots - e_k(x) \in M'$$

which shows $e_1 g^{-1}(N_1) \subseteq M'$. But notice:

$$e_1 g^{-1}(N_1) = e_1 g^{-1} f_1(N_1) = k_1(N_1) = M_1$$

Hence, $M_1 \subseteq M'$, so it follows that $M = M' = g^{-1}(N_1) \oplus (M_2 \oplus \cdots \oplus M_k)$.

The isomorphism $g : M \to N$ induces an isomorphism $\widetilde{g} : M/g^{-1}(N_1) \to N/N_1$, which means:

$$M_2 \oplus \cdots \oplus M_k \cong M/g^{-1}(N_1) \cong N/N_1 \cong N_2 \oplus \cdots \oplus N_l$$

By the induction hypothesis, $k = l$ and there is a bijection $\sigma' : \{2, ..., k\} \to \{2, ..., k\}$ with $M_i = N_{\sigma'(i)}$ for each $i \in \{2, ..., k\}$. Now extend this to $\sigma \in S_k$ by defining $\sigma(1) = 1$ and $\sigma(i) = \sigma'(i)$ for $i \in \{2, ..., k\}$. σ then satisfies our desired conclusion. □

Now we can give the

Proof of Krull-Schmidt. Let's first get the uniqueness out of the way. Suppose $M = M_1 \oplus \cdots \oplus M_k = N_1 \oplus \cdots \oplus N_l$ are two decompositions into indecomposable submodules. Since $M_1, ..., M_k$ are also of finite length, these are in fact *strongly* indecomposable, so the preceding proposition gives us $k = l$ and $\sigma \in S_k$ with $M_i \cong N_{\sigma(i)}$ for each $i \in \{1, ..., k\}$.

Now we establish the existence of such M_i. We do this by induction on the length $\ell(M)$ of M. We can't have $\ell(M) = 0$ since otherwise $M = 0$. If $\ell(M) = 1$ then M is irreducible, hence indecomposable. Thus, assume $\ell(M) > 1$ and that the result holds for submodules of length $< \ell(M)$.

If M is indecomposable, we're done. Otherwise, we can write $M = M_1 \oplus M_2$ for non-zero submodules M_1, M_2. These are necessarily proper, so it's clear that $0 < \ell(M_i) < \ell(M)$. By the induction hypothesis, we can thus write $M_1 = M_{1,1} \oplus \cdots \oplus M_{1,k_1}$ and $M_2 = M_{2,1} \oplus \cdots \oplus M_{2,k_2}$ for indecomposable submodules $M_{1,1}, ..., M_{1,k_1}$ of M_1 and $M_{2,1}, ..., M_{2,k_2}$ of M_2. Now $M = M_{1,1} \oplus \cdots \oplus M_{1,k_1} \oplus M_{2,1} \oplus \cdots \oplus M_{2,k_2}$ is our desired decomposition. □

Exercises

Let R be a ring. The following exercise gives equivalent descriptions for what it means for R to be local. First we have:

Definition 3.3.12 A left (right) ideal I is called **maximal** when $I \neq R$ and if J is another left (right) ideal of R with $J \supseteq I$, then $J = I$ or $J = R$.

Exercise 3.3.13 Let R be a ring. Prove that the following are equivalent:

(i) R is local (in that $R \setminus R^\times$ is an ideal).

(ii) R has exactly one maximal left ideal.

(iii) R has exactly one maximal right ideal.

(iv) $1 \neq 0$ and for each $x \in R$, x is invertible or quasiregular.

The next two exercises are on some applications of Krull-Schmidt.

Exercise 3.3.14 (Structure theorem for finite abelian groups)
Let $G \neq 0$ be a finite abelian group ($\mathbb{Z}$-module).

(a) Show that G is of finite length.

(b) Thus, apply the Krull-Schmidt theorem to show that there exist subgroups $H_1, ..., H_k$ of G with $G = H_1 \times \cdots \times H_k$, unique up to isomorphism.

(c) Now suppose H is an indecomposable finite abelian group. Show that we necessarily have $H \cong \mathbb{Z}/(p^k)$ for some prime p and some $k \geqslant 1$.

(d) Conclude that any finite abelian group is either 0 or isomorphic to $\mathbb{Z}/(q_1) \times \cdots \times \mathbb{Z}/(q_k)$ where each $q_i > 1$ is some prime power, and the $q_1, ..., q_k$ are unique up to reordering.

This actually generalizes to *finitely-generated* abelian groups, and more generally to finitely-generated modules over PIDs.

Exercise 3.3.15 (Primary decomposition theorem for linear operators)
Let V be a finite-dimensional vector space over F and $T \in \mathrm{End}_F(V)$ a linear operator. Let $p_T \in F[\lambda]$. We say p_T is a **minimal polynomial** of T when

- p_T is monic;
- $p_T(T) = 0$; and
- if $g \in F[\lambda]$ satisfies $g(T) = 0$, then $p_T \mid g$.

(a) Show that the minimal polynomial p_T indeed exists and is unique.

(b) We consider V as an $F[\lambda]$-module determined by T. Let $p_T = f_1^{r_1} \cdots f_k^{r_k}$ where the f_i's are distinct primes in $F[\lambda]$ and $r_i \geqslant 1$. Set $W_i = \ker f_i(T)^{r_i}$.

Show that the W_i's are indecomposable $F[\lambda]$-submodules of V.

(c) Show also that $V = W_1 \oplus \cdots \oplus W_k$. Conclude from the Krull-Schmidt theorem that any decomposition $V = U_1 \oplus \cdots \oplus U_l$ into indecomposable $F[\lambda]$-submodules U_i must satisfy that $k = l$ and each $U_i \cong W_{\sigma(i)}$ for some $\sigma \in S_k$.

3.4 Semisimple modules

We considered in the previous section modules which are *(finitely) completely decomposable* in that they can be broken down into a finite direct sum of indecomposable submodules, and saw that modules which are of finite length enjoy this property. Now we consider a stronger type of decomposability, where this time:

- we replace indecomposability with *irreducibility*, which makes this consideration stronger because every irreducible module is automatically indecomposable;
- we take *arbitrary* direct sums of submodules, not just finite ones.

Recall that $M \neq 0$ is irreducible if and only if M is generated by every non-zero element of M, and thus M is cyclic. We add yet another equivalent condition.

Proposition 3.4.1 Let $M \neq 0$ be an R-module. Then the following are equivalent:

(i) M is irreducible.

(ii) $Rx = M$ for all $0 \neq x \in M$.

(iii) $M \cong R/I$ for a maximal left ideal I.

(the definition of a maximal left ideal is given in **3.3.12**).

Proof. It remains to show that **(iii)** is equivalent to **(i)** or **(ii)**. Suppose M is irreducible, fix $0 \neq x \in M$, and let $f : R \to M$ be given by $f(a) = ax$. Then f is surjective and $I = \ker f = \{a \in R : ax = 0\}$ is a left ideal. We shall have $R/I \cong M$ by the first isomorphism theorem.

Now clearly $I \neq M$ since $M \neq 0$. The submodules of R/I are of the form J/I where J is a left ideal containing I. But these are in correspondence with the submodules of M, which consist only of 0 and M. Therefore, the only left ideals of R which contain I are I and R, making I maximal.

Now suppose $M \cong R/I$ for I a maximal left ideal. Then the only submodules of R/I are 0 and R/I, which means the only submodules of M are 0 and M, so M is irreducible. □

Let M be an R-module. We proceed to define an *internal* direct sum for an arbitrary collection of submodules. Let $S = \{M_\alpha\}$ be such a collection and recall that $\sum_\alpha M_\alpha$ is the submodule of M which is generated by $\bigcup_\alpha M_\alpha$.

Definition 3.4.2 S is called **independent** when for every α, we have $M_\alpha \cap \left(\sum_{\beta \neq \alpha} M_\beta\right) = 0$. Otherwise, S is called **dependent**.

It's clear that any subset of an independent set is also independent, hence any superset of a dependent set is dependent.

Proposition 3.4.3 If S is independent and $N = \sum_\alpha M_\alpha$, then $N \cong \bigoplus_\alpha M_\alpha$. In this case we say that N is the **internal direct sum** of $\{M_\alpha\}$ and just write $N = \bigoplus_\alpha M_\alpha$.

Proof. Let $f : \bigoplus_\alpha M_\alpha \to N$ be given by $f((x_\alpha)) = \sum_\alpha x_\alpha$, which is well-defined since only finitely-many of the x_α's are non-zero. It's clear that f is a surjective homomorphism, so what's left to check is injectivity.

Suppose $f((x_\alpha)) = \sum_\alpha x_\alpha = 0$. Suppose at least one of the x_α's are non-zero; let $x_{\alpha_1}, ..., x_{\alpha_k}$ be all of them, where $k \geqslant 1$. Then $f((x_\alpha)) = x_{\alpha_1} + \cdots + x_{\alpha_k} = 0$. We have $x_{\alpha_1} = -x_{\alpha_2} - \cdots - x_{\alpha_k}$, which means $x_{\alpha_1} \in M_{\alpha_1} \cap \left(\sum_{\alpha \neq \alpha_1} M_\alpha\right) = 0$ so that $x_{\alpha_1} = 0$, which is a contradiction to the independence of S. Thus, we must have $(x_\alpha) = 0$, making f an isomorphism. □

Example 3.4.4

(1) Perhaps the most illuminating example of independent submodules can be seen in vector spaces; independence of a collection of subspaces is a generalization of linear independence of vectors. If $\{W_\alpha\}$ is a collection of independent subspaces of V and $\mathcal{B}_\alpha$ is a basis for W_α, then one sees that $\bigcup_\alpha \mathcal{B}_\alpha$ is independent and is a basis for $\sum_\alpha W_\alpha$.

(2) Consider the ring $\mathbb{Z}$ and let $a, b \in \mathbb{Z}$. Then (a) and (b) are independent (that is, $\{(a), (b)\}$ is independent) if and only if $a = 0$ or $b = 0$ (since we will always have $ab \in (a) \cap (b)$). It's clear then that any collection of 3 or more ideals of $\mathbb{Z}$ will not be independent.

(3) Now look at $\mathbb{Z}/(n)$ for $n > 0$. Let $a, b \in \mathbb{Z}$ and consider the ideals (a) and (b) in $\mathbb{Z}/(n)$. These are independent if and only if $\text{lcm}(a, b) = n$.

We can actually describe independence in more detail here. There are only finitely-many distinct ideals of $\mathbb{Z}/(n)$. If $n = p_1^{r_1} \cdots p_k^{r_k}$ for distinct primes p_i and $r_i \geqslant 1$, then these are of the form $(p_1^{s_1} \cdots p_k^{s_k})$ for $0 \leqslant s_i \leqslant r_i$. It's evident then that if S is independent and contains two or more ideals, then S must consist of ideals of the form $(\frac{n}{p_i})$. This can be observed by viewing the lattice of ideals in $\mathbb{Z}/(n)$ (try looking at a particular example).

We shall now collect some technical (yet useful) lemmas about independent sets of submodules. First, given any collection S of submodules, we can extract a *maximal* independent subset $T \subseteq S$ by an application of Zorn. In fact, a little more is true:

Lemma 3.4.5 Let S be a collection of submodules of M. For any subset $T \subseteq S$ which is independent, one can find a *maximal* independent subset $T' \subseteq S$ containing T. This means T' is independent, $T \subseteq T'$, and $T' \cup \{N\}$ is dependent for any $N \in S \setminus T'$.

Proof. Let $\mathcal{B} = \{U \subseteq S : U \text{ is independent and } U \supseteq T\}$. Clearly $\mathcal{B}$ is non-empty since $T \in \mathcal{B}$. Let $\mathcal{C}$ be a chain in $\mathcal{B}$. Then $V = \bigcup_{U \in \mathcal{C}} U \subseteq S$ is a collection of submodules containing T. If $N \in V$ and we let

$$x \in N \cap \left(\sum_{P \in V \setminus \{N\}} P \right)$$

then we can write $x = x_1 + \cdots + x_k$ where $x_i \in P_i$ and $P_1, ..., P_k \in V \setminus \{N\}$ are distinct. There exist $U_1, ..., U_k \in \mathcal{C}$ with $P_i \in U_i$. Since $\mathcal{C}$ is a chain though, we

have $P_1, ..., P_k \in U_j$ for some j. Also $N \in W$ for some $W \in \mathcal{C}$, so we shall have $P_1, ..., P_k, N \in U_j$ or $P_1, ..., P_k, N \in W$. In either case though, $\{P_1, ..., P_k, N\}$ is independent, so we must have $x = 0$. Hence, V is independent, so $V \in \mathcal{B}$. We thus have that every chain in $\mathcal{B}$ has an upper bound in $\mathcal{B}$, so Zorn's lemma implies the existence of a maximal element of $\mathcal{B}$, which is our desired T'. □

The next lemma tells us when we can add a submodule to an independent set such that independence is preserved.

Lemma 3.4.6 Let $S = \{M_\alpha\}$ be an independent set of submodules and let N be any submodule of M. If $N \cap \sum_\alpha M_\alpha = 0$, then $S \cup \{N\}$ is independent.

Proof. If $S \cup \{N\}$ is dependent, then there is some α_0 and $0 \neq x_0 \in M_{\alpha_0} \cap \left(N + \sum_{\beta \neq \alpha_0} M_\beta\right)$. We can thus find distinct $\alpha_1, ..., \alpha_k \neq \alpha_0$ and elements $y \in N$ and $x_1, ..., x_k$ with $x_i \in M_{\alpha_i}$ such that $x_0 = y + x_1 + \cdots + x_k$. Now $y = x_0 - x_1 - \cdots - x_k \in \sum_\alpha M_\alpha$, which forces $y = 0$. Hence, $x_0 = x_1 + \cdots + x_k$, which means $0 \neq x_0 \in M_{\alpha_0} \cap \left(\sum_{\alpha \neq \alpha_0} M_\alpha\right)$, contradicting independence of S. □

Combining the previous two lemmas gives a sort of "replacement property" for a collection of irreducible submodules.

Lemma 3.4.7 Let $S = \{M_\alpha\}$ be a set of *irreducible* submodules with $M = \sum_\alpha M_\alpha$, and let N be any submodule of M. Then there exists a subset $T = \{M_\beta\} \subseteq S$ with $T \cup \{N\}$ independent and $M = N + \sum_\beta M_\beta$.

Proof. Since $\{N\}$ is independent, we can find a *maximal* independent subset T' of $S \cup \{N\}$ with $N \in T'$. Let $T = \{M_\beta\} = T' \setminus \{N\}$ and set $M' = N + \sum_\beta M_\beta \subseteq$. If there is an element of M which isn't in M', then there is an α_0 with $M_{\alpha_0} \not\subseteq M'$. Thus, since M_{α_0} is irreducible, $M_{\alpha_0} \cap M' = 0$. Applying the preceding lemma gives independence of $T' \cup \{M_{\alpha_0}\} \subseteq S \cup \{N\}$. But we have $T' \subsetneq T' \cup \{M_{\alpha_0}\}$, contradicting maximality of T'. We therefore must have $M = N + \sum_\beta M_\beta$. □

Definition 3.4.8 We say a module M is **semisimple** when there exists a collection of irreducible submodules $\{M_\alpha\}$ of M for which $M = \bigoplus_\alpha M_\alpha$ (this last condition simply means $\{M_\alpha\}$ is independent and $M = \sum_\alpha M_\alpha$).

Using the lemmas established above, we obtain the following property about semisimple modules.

Proposition 3.4.9 Suppose $M = \sum_\alpha M_\alpha$ where $\{M_\alpha\}$ is a collection of irreducible submodules. Then there exists a subcollection $\{M_\beta\} \subseteq \{M_\alpha\}$ for which $M = \bigoplus_\beta M_\beta$. In particular therefore, M is semisimple.

Proof. Since $M = \sum_\alpha M_\alpha$, **Lemma 3.4.7** applied to $N = 0$ gives us a subcollection $\{M_\beta\}$ with $\{M_\beta\} \cup \{0\}$ independent and satisfying $M = 0 + \sum_\beta M_\beta = \sum_\beta M_\beta$. Now clearly $\{M_\beta\}$ is independent, so $M = \bigoplus_\beta M_\beta$. □

We thus have that M is semisimple if and only if there is a collection of irreducible submodules $\{M_\alpha\}$ with $M = \sum_\alpha M_\alpha$.

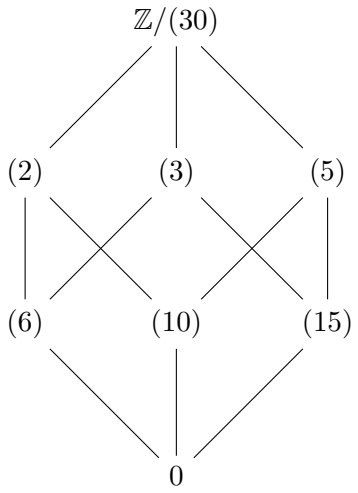
We can obtain another equivalent characterization of semisimplicity. Recall that the set $\mathcal{L}(M)$ of submodules of M has the structure of a lattice.

Definition 3.4.10 A submodule N of M is **complemented** in M when there exists a submodule N' of M with $M = N \oplus N'$. The submodule N' is called a *complement* of N. If M is such that *every* submodule is complemented, we say that the lattice $\mathcal{L}(M)$ is **complemented**.

It's easy to see that if a complement exists, it might not be unique. For instance, in the vector space $\mathbb{R}^2$ with $\{e_1, e_2\}$ the standard basis, the subspace $\mathbb{R}e_1$ has $\mathbb{R}e_2$ as a complement as well as $\mathbb{R}(e_1 + e_2)$, but clearly $\mathbb{R}e_2 \neq \mathbb{R}(e_1 + e_2)$.

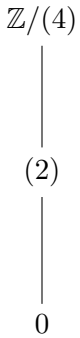
We can obtain some nice examples of complements in situations where $\mathcal{L}(M)$ is finite.

Example 3.4.11 Consider the lattice $\mathcal{L}(\mathbb{Z}/(30))$ given by:



It's easy to check that this lattice is complemented.

An example of a module whose lattice of submodules *isn't* complemented is $\mathbb{Z}/(4)$, which has lattice:



We've seen that $\mathbb{Z}/(4)$ is indecomposable, so naturally (2) isn't complemented.

Lemma 3.4.12 Suppose $\mathcal{L}(M)$ is complemented. For any submodule N of M, $\mathcal{L}(N)$ and $\mathcal{L}(M/N)$ are complemented. Hence, any homomorphic image of M is complemented.

Proof. Let $P \in \mathcal{L}(N)$. Then we can find some $\widehat{P} \in \mathcal{L}(M)$ with $P \oplus \widehat{P} = M$. Let $P' = \widehat{P} \cap N$. We find then that $N = M \cap N = (P + \widehat{P}) \cap N = P + \widehat{P} \cap N = P + P'$, which follows from modularity of $\mathcal{L}(M)$ (**Exercise 2.5.4**). Clearly $P \cap P' = 0$, so $N = P \oplus P'$, which makes $\mathcal{L}(N)$ complemented.

Now let $P/N \in \mathcal{L}(M/N)$ for $P \in \mathcal{L}(M)$ satisfying $P \supseteq N$. Then $N \in \mathcal{L}(P)$, so $P = N \oplus N'$ for some $N' \in \mathcal{L}(P)$. We have $P/N \cong N'$, so the fact that $\mathcal{L}(N')$ is complemented gives us that $\mathcal{L}(P/N)$ is complemented.

As we've seen, any homomorphic image of M is isomorphic to M/N for some submodule N, so the same is true for this as well. □

We shall now work towards showing that M is semisimple if and only if $\mathcal{L}(M)$ is complemented. For this we need the following

Lemma 3.4.13 Suppose $M \neq 0$. If $\mathcal{L}(M)$ is complemented, M contains an irreducible submodule.

Proof. Fix $0 \neq x \in M$ and let $S = \{N \in \mathcal{L}(M) : x \notin N\}$. Clearly $S \neq \emptyset$ since $0 \in S$ and we can order S by inclusion. A Zorn argument shows that S has a maximal element P. We see that any submodule Q that properly contains P must contain x, and so if we have two of these; say Q_1 and Q_2; then $x \in Q_1 \cap Q_2$ which shows $Q_1 \cap Q_2 \supsetneq P$.

In the quotient space M/P, this observation shows that the intersection of any two non-zero submodules of M/P must also be non-zero. Since $\mathcal{L}(M)$ is complemented, $M = P \oplus P'$ for some $P' \in \mathcal{L}(M)$. As such, $M/P \cong P'$, which means the intersection of any two non-zero submodules of P' must be non-zero. But $\mathcal{L}(P')$ is also complemented by the preceding lemma. Hence, P' must be irreducible (since the complement of any proper non-zero submodule is also proper non-zero). □

Theorem 3.4.14 The following conditions on a module M are equivalent:

(i) M is semisimple.

(ii) $M = \sum_\alpha M_\alpha$ for some collection of irreducible submodules $\{M_\alpha\}$.

(iii) $\mathcal{L}(M)$ is complemented.

Proof. Throughout, we may assume $M \neq 0$, since otherwise the result is clear (M is vacuously the sum of an empty collection of irreducible submodules).

We've already shown **(i)** and **(ii)** are equivalent. Now suppose M is semisimple with $M = \bigoplus_\alpha M_\alpha$, where $\{M_\alpha\}$ is a collection of irreducible submodules. Let $N \in \mathcal{L}(M)$. Then by **Lemma 3.4.7**, we can find a subset $\{M_\beta\} \subseteq \{M_\alpha\}$ with $\{M_\beta\} \cup \{N\}$ independent and $N + \sum_\beta M_\beta = M$. Then $N' = \sum_\beta M_\beta$ makes it so that $N + N' = M$ and $N \cap N' = 0$ by independence, so $M = N \oplus N'$. Thus, $\mathcal{L}(M)$ is complemented.

Now suppose $\mathcal{L}(M)$ is complemented. Since $M \neq 0$, we can find an irreducible submodule. Let $\{M_\alpha\}$ be the collection of all irreducible submodules and set $M' = \sum_\alpha M_\alpha$. Since $\mathcal{L}(M)$ is complemented, we can find $M'' \in \mathcal{L}(M)$ with $M = M' \oplus M''$. Now M'' can't contain any irreducible submodules, since that would imply

$M_\alpha \cap M'' \neq 0$ for some α. On the other hand, $\mathcal{L}(M'')$ is complemented, which means M'' must contain some irreducible submodule if $M'' \neq 0$. Hence, we must have $M'' = 0$, which shows $M = \sum_\alpha M_\alpha$, a sum of irreducibles. This means **(ii)** is satisfied, making M semisimple. □

From what we know about complemented lattices, we immediately obtain:

Corollary 3.4.15 If M is semisimple and N is a submodule, both N and M/N are semisimple. Hence, any homomorphic image of M is semisimple too.

Example 3.4.16

(1) Vector spaces are semisimple. If V is a vector space and $\mathcal{B} = \{v_\alpha\}$ is a basis for it, we can let $W_\alpha = \text{span}(v_\alpha)$ and get that $V = \bigoplus_\alpha W_\alpha$. Each W_α is one-dimensional, therefore irreducible.

(2) $\mathbb{Z}$ is not semisimple. Consider the ideal (2) and let J be any other ideal. If $J \neq 0$, we can find $0 \neq a \in J$. Then $2a \in (2) \cap J$, so $(2) \cap J \neq 0$. On the other hand, if $J = 0$ then clearly $\mathbb{Z} \neq (2)$. Hence, (2) doesn't have a complement, so $\mathcal{L}(\mathbb{Z})$ isn't complemented.

(3) When is $\mathbb{Z}/(n)$ semisimple? We've seen that $\mathcal{L}(\mathbb{Z}/(4))$ isn't complemented, so $\mathbb{Z}/(4)$ isn't semisimple. On the other hand, we've seen that $\mathbb{Z}/(30)$ is.

One way to determine this is as follows: write $n = p_1^{r_1} \cdots p_k^{r_k}$ for distinct primes p_i and $r_i \geqslant 1$. The ideals of $\mathbb{Z}/(n)$ are of the form $(p_1^{s_1} \cdots p_k^{s_k})$ for $0 \leqslant s_i \leqslant r_i$. Now if one of the r_i is $\geqslant 2$; say this is r_1; then consider the ideal $I = (p_1)$. If this is complemented by $J = (b)$ where $b = p_1^{s_1} \cdots p_k^{s_k}$, then we must have $I \cap J = 0$ and $I + J = \mathbb{Z}/(n)$, which means we must have $\gcd(p_1, b) = 1$ and $\text{lcm}(p_1, b) = n$. But $\gcd(p_1, b) = 1$ implies $s_1 = 0$ and $\text{lcm}(p_1, b) = n$ implies $s_1 + 1 = r_1 \geqslant 2$, which is a contradiction. Hence, I isn't complemented.

On the other hand, suppose every $r_i = 1$, so $n = p_1 \cdots p_k$ for p_i distinct. Given $a = p_1^{s_1} \cdots p_k^{s_k}$ for $0 \leqslant s_i \leqslant 1$, it's easy to see that $I = (a)$ is complemented by $J = (b)$ where $b = \frac{n}{a} = p_1^{r_1 - s_1} \cdots p_k^{r_k - s_k}$.

From this, we conclude that $\mathbb{Z}/(n)$ is semisimple if and only if n is a product of distinct primes (that is, n is square-free). In this case, it's clear that we have $\mathbb{Z}/(n) = (q_1) \oplus \cdots \oplus (q_k)$ where each $q_i = \frac{n}{p_i}$.

In the next chapter, we shall study *semisimple rings* – rings which are semisimple as left/right modules over themselves. As we shall see, the additional structure afforded by the ring gives us some remarkable results. Notably, left and right semisimplicity are equivalent, and we obtain further characterizations of semisimplicity for rings.

Exercises

Exercise 3.4.17 Let M be an R-module and let N be a submodule of M. We say N is a **maximal submodule** of M when $N \neq M$ and for any submodule P of M with $P \supseteq N$, either $P = N$ or $P = M$.

Notice that if $M = {}_R R$ (R as a left R-module), then the maximal submodules are precisely the maximal left ideals as defined in **3.3.12**.

(a) Use Zorn's lemma to show that if N is a proper submodule of M, then M has a maximal submodule which contains N. Thus conclude that for any ring R, every proper left ideal J of R is contained in a maximal left ideal. (Dually, the same can be said for right ideals.)

(b) Hence, show that if $M \neq 0$, then M contains at least one maximal submodule. Similarly if $R \neq 0$, then R contains at least one maximal left (right) ideal.

(c) Conclude that for every non-zero ring R, there exists an *irreducible* R-module M.

Exercise 3.4.18 Let V be a finite-dimensional vector space over F and let $T \in \mathrm{End}_F(V)$ be a linear operator. View V as an $F[\lambda]$-module determined by T and let $p_T \in F[\lambda]$ be the minimal polynomial of T. Show that V is semisimple if and only if p_T is the product of distinct irreducible factors in $F[\lambda]$.

Exercise 3.4.19 Let M be a semisimple module. Show that M is Noetherian if and only if M is Artinian.

Definition 3.4.20 Suppose M is semisimple and let N be an irreducible submodule. Let $\mathcal{S}(N) = \{N' \in \mathcal{L}(M) : N' \cong N\}$; the set of all submodules isomorphic to N. The **homogeneous component** of M corresponding to N is then defined to be

$$H_N = \sum_{N' \in \mathcal{S}(N)} N'$$

Exercise 3.4.21 Let M be semisimple with $M = \bigoplus_{\alpha,\beta} M_{\alpha,\beta}$, where the irreducible $\{M_{\alpha,\beta}\}$ are chosen such that $M_{\alpha,\beta} \cong M_{\alpha',\beta'}$ if and only if $\alpha = \alpha'$.

Define $H_\alpha = \bigoplus_\beta M_{\alpha,\beta}$.

(a) Show that for *any* irreducible submodule N of M, we have $H_N = H_\alpha$ for some α. Conclude from this that every irreducible submodule of M is isomorphic to some $M_{\alpha,\beta}$.

(b) Use this to show that $\{H_\alpha\}$ is precisely the collection of all homogeneous components of M, and we have $M = \bigoplus_\alpha H_\alpha$.

An idea for part **(a)**: if N is irreducible, we have $N = Rx$ for every $0 \neq x \in N$. Fix a particular $0 \neq x \in N$ and write $x = x_1 + \cdots + x_k$ where $x_i \in M_{\alpha_i,\beta_i}$. Then $N \subseteq M' = M_{\alpha_1,\beta_1} \oplus \cdots \oplus M_{\alpha_k,\beta_k}$. Let $p_i : M' \to M_{\alpha_i,\beta_i}$ be the projection maps – apply Schur's lemma (**2.3.12**) to $p_i|_N$.

4 Structure theory of rings

It is here that we finally get to the structure theory of rings. Given a ring R, when and how we can "break down" R into a direct sum of "simpler pieces"? Using what we have covered in the previous chapters, we first look at the conditions on R which will allow us to decompose it in this way. Once this is done, we shall see how we can go through with it. First, we need to clarify our problem a little more.

4.1 Return of representations – primitivity and semiprimitivity

Recall that a *representation* of a ring R is a pair (M, ρ) where M is an abelian group (additive) and $\rho : R \to \text{End}(M)$ is a ring homomorphism of R into the endomorphism ring on M. At the beginning of chapter 2, we established a natural correspondence between (left) R-modules and representations of R; namely, any representation (M, ρ) gives M an R-module structure given by $ax = \rho(a)x$ and any R-module M determines a ring homomorphism $\rho : R \to \text{End}(M)$ given by $\rho(a)x = ax$.

It will be useful for this section to take on this perspective and view a module M as a representation of R. We will often use "module" and "representation" synonymously.

Recall that a representation (M, ρ) is *faithful* when the homomorphism ρ is injective. We can translate this to the language of modules. First we need:

Definition 4.1.1 The **annihilator** of M is defined to be:

$$\text{Ann}_R(M) = \{a \in R : ax = 0 \text{ for all } x \in M\}$$

That is, it is the set of all elements of R which annihilate every element of M.

Lemma 4.1.2 $\text{Ann}_R(M)$ is an ideal of R.

Proof. Clearly $\text{Ann}_R(M) \neq \emptyset$. Given $a, b \in \text{Ann}_R(M)$, we see that for all $x \in M$, $(a+b)x = ax + bx = 0 + 0 = 0$, $(-a)x = -ax = 0$, so $\text{Ann}_R(M)$ is a subgroup of $(R, +)$. Now let $c \in R$. Then for all $x \in M$, we have $(ca)x = c(ax) = c \cdot 0 = 0$ and $(ac)x = a(cx) = 0$, where the last equality comes from the fact that $cx \in M$. □

Proposition 4.1.3 A representation (M, ρ) of R is faithful if and only if $\text{Ann}_R(M) = 0$ (of course, viewing M as an R-module under the action induced by ρ). We shall therefore call any module **faithful** when this condition holds.

Proof. We have $a \in \text{Ann}_R(M)$ if and only if $ax = \rho(a)x = 0$ for all $x \in M$, which happens if and only if $\rho(a) = 0$. If ρ is injective, then $\rho(a) = 0$ if and only if $a = 0$, which means $\text{Ann}_R(M) = 0$. Conversely if $\text{Ann}_R(M) = 0$, then $\rho(a) = 0$ if and only if $ax = \rho(a)x = 0$ for all $x \in M$, which is true if and only if $a \in \text{Ann}_R(M) = 0$. Hence, ρ is injective. □

There's another way we can view the annihilator of M.

Definition 4.1.4 Let $x \in M$. The **annihilator** of x is defined to be:

$$\mathrm{Ann}_R(x) = \{a \in R : ax = 0\}$$

We notice that $\mathrm{Ann}_R(x)$ is a subgroup of $(R, +)$ in the same way as $\mathrm{Ann}_R(M)$. Also if $a \in \mathrm{Ann}_R(x)$ and $b \in R$, we have $(ba)x = b \cdot 0 = 0$, but it's *not* necessarily the case that $(ab)x = 0$. Thus, unlike $\mathrm{Ann}_R(M)$, $\mathrm{Ann}_R(x)$ may not be a (two-sided) ideal. But we do at least have:

Lemma 4.1.5 $\mathrm{Ann}_R(x)$ is a left ideal of R. Moreover, if M is irreducible and $x \neq 0$, then $\mathrm{Ann}_R(x)$ is maximal.

Proof. We've shown $\mathrm{Ann}_R(x)$ is a left ideal above. Now suppose M is irreducible and $x \neq 0$. Then $M = Rx$ so the map $f : R \to M$ given by $f(a) = ax$ is a surjective homomorphism with $\ker f = \mathrm{Ann}_R(x)$. Now $M \cong R/\mathrm{Ann}_R(x)$, and irreducibility of M makes $\mathrm{Ann}_R(x)$ maximal. □

If $a \in \mathrm{Ann}_R(M)$, clearly $a \in \mathrm{Ann}_R(x)$ for all $x \in M$, so we have $\mathrm{Ann}_R(M) \subseteq \bigcap_{x \in M} \mathrm{Ann}_R(x)$. On the other hand, if $a \in \mathrm{Ann}_R(x)$ for all $x \in M$, this precisely means $a \in \mathrm{Ann}_R(M)$. Thus, we obtain:

Proposition 4.1.6 $\mathrm{Ann}_R(M) = \bigcap_{x \in M} \mathrm{Ann}_R(x)$.

The simplest types of modules are the irreducible ones. We can make the following

Definition 4.1.7 A representation (M, ρ) is **irreducible** when the R-module M is irreducible. This means $M \neq 0$ and for any subgroup N of $(M, +)$ satisfying $\rho(a)x \in N$ for all $a \in R$ and $x \in N$, we have $N = 0$ or $N = M$.

Then the simplest types of representations are the irreducible ones. Recall that M is irreducible if and only if $M \cong R/I$ where I is a maximal left ideal of R. Thus, if R is a ring and I is a maximal left ideal, then we have an irreducible representation for R given by $M = R/I$. Conversely if R has an irreducible representation M, then $M \cong R/I$ for some maximal left ideal I of R.

Now we notice the following: if I is a left ideal of R and $M = R/I$, then clearly $\mathrm{Ann}_R(M) \subseteq I$. On the other hand, if J is any (two-sided) ideal of R with $J \subseteq I$, then any $r \in J$ satisfies $r(a + I) = ra + I = I$ for all $a \in R$, which means $r \in \mathrm{Ann}_R(M)$. Thus, $\mathrm{Ann}_R(M)$ is the unique largest ideal of R contained in I. We have a special name for this:

Definition 4.1.8 Given a left ideal I of a ring R, we define the **ideal quotient** of I with R to be:

$$(I : R) = \{a \in R : aR \subseteq I\}$$

It is clear that $(I : R) = \mathrm{Ann}_R(R/I) \subseteq I$. It can be thought of as the set of elements of I which are closed under right multiplication by R.

Our observations give the following

Proposition 4.1.9 The following conditions on a ring R are equivalent:

(i) R has a faithful irreducible representation.

(ii) There exists a maximal left ideal I of R which contains no non-zero (two-sided) ideals.

Definition 4.1.10 If R satisfies one of the definitions above, we say R is **(left) primitive**.

Example 4.1.11

(1) Suppose R is a simple ring, which means $R \neq 0$ and the only ideals are 0 and R. Then any maximal left ideal of R can only contain 0 as an ideal. Since every non-zero ring contains a maximal left ideal (**Exercise 3.4.17**), it follows that R is primitive.

This applies in particular to $M_n(D)$ where D is a division ring, and (more generally) for $\mathrm{End}_D(V)$ where V is a finite-dimensional vector space over D. In fact, primitivity of $\mathrm{End}_D(V)$ holds even if V is *not* finite-dimensional (**Exercise 4.1.20**), and this shows that a primitive ring need not be simple.

(2) If F is a field, then F must be primitive. Conversely if R is a commutative ring which is primitive, then any maximal left ideal is a maximal ideal. But if I is a maximal ideal, it can't contain any non-zero ideals, forcing it to be 0. This precisely means R is a field.

(3) When is $\mathbb{Z}/(n)$ primitive? If n is prime, $\mathbb{Z}/(n)$ is a field, thus immediately primitive. On the other hand, suppose n is not prime. Every maximal ideal of $\mathbb{Z}/(n)$ is of the form (p) where p is a prime factor of n, and n not being prime means $(p) \neq 0$. Hence, $\mathbb{Z}/(n)$ can't be primitive.

We define the more general notion of *semiprimitivity* by "localizing" the definition of primitivity. More precisely:

Definition 4.1.12 R is **semiprimitive** when for every $a \in R$ with $a \neq 0$, there exists an irreducible representation (M, ρ) of R with $\rho(a) \neq 0$.

Remark 4.1.13

- The "locality" can be seen when we look at the definition of primitivity again. This is saying that there exists an irreducible (M, ρ) with $\rho(a) \neq 0$ for all $0 \neq a \in R$. For semiprimitivity though, the representation (M, ρ) may depend on a. As such, it is easy to see that every primitive ring is semiprimitive.
- One should think of semiprimitivity as follows: there are enough irreducible representations that allow us to distinguish the elements of R. For, suppose $a, b \in R$ with $a \neq b$. Then $a - b \neq 0$ so there is an irreducible representation (M, ρ) with $\rho(a-b) \neq 0$. This means $\rho(a) \neq \rho(b)$, so ρ "witnesses" that a and b are distinct.

We seek a ring-theoretic characterization for this. It will be convenient to write $\mathcal{M}_L(R) = \{I \subseteq R : I \text{ is a maximal left ideal of } R\}$. Suppose R is semiprimitive and let $0 \neq a \in R$. There is an irreducible representation (M, ρ) with $\rho(a) \neq 0$. Let $M \cong R/I$ for $I \in \mathcal{M}_L(R)$. Then $a \notin (I : R) = \mathrm{Ann}_R(M)$, and in particular $a \notin \bigcap_{J \in \mathcal{M}_L}(J : R)$. This shows that $\bigcap_{J \in \mathcal{M}_L}(J : R) = 0$.

On the other hand, if R is a ring satisfying $\bigcap_{J \in \mathcal{M}_L}(J : R) = 0$, then any $0 \neq a \in R$ will have $a \notin (I : R)$ for some $I \in \mathcal{M}_L(R)$. This means $M = R/I$ with the associated homomorphism ρ is an irreducible representation of R with $aR \not\subseteq I$, and so $ab \notin I$ for some $b \in R$. As such, $a(b+I) = ab+I$ is a non-zero element of M, which means $\rho(a) \neq 0$. We've thus shown:

Proposition 4.1.14 The following conditions on a ring R are equivalent:

(i) For each $a \in R$ with $a \neq 0$, there exists an irreducible representation (M, ρ) with $\rho(a) \neq 0$ (R is semiprimitive).

(ii) $\bigcap_{J \in \mathcal{M}_L(R)}(J : R) = 0$.

It will be useful to also make explicit a structural relation between primitivity and semiprimitivity. Recall that a module is semisimple when it can be written as a direct sum of irreducible submodules. We shall call a representation (M, ρ) **semisimple** when M is semisimple as an R-module.

While primitivity is weaker than simplicity in a ring, we still have that a ring is primitive when it has a faithful irreducible representation. This suggests the following

Proposition 4.1.15 R is semiprimitive if and only if there exists a faithful semisimple representation.

Proof. Suppose R is semiprimitive and choose an irreducible representation (M_a, ρ_a) for each $0 \neq a \in R$ satisfying $\rho_a(a) \neq 0$. Then $M = \bigoplus_{\substack{a \in R \\ a \neq 0}} M_a$ is a semisimple R-module. Let $\rho : R \to \mathrm{End}(M)$ be the corresponding homomorphism. It remains to show that M is faithful. But indeed, if $\rho(b) = 0$ for $b \in R$, then for any $x = (x_a) \in M$ we have $\rho(b)x = b(x_a) = (bx_a) = (\rho_a(b)x_a) = 0$, which implies $\rho_b(b)x_b = 0$. Since x was arbitrary, this means $\rho_b(b) = 0$, which is a contradiction. Hence, ρ is injective, making M faithful.

Now if M is a faithful semisimple representation, write $M = \bigoplus_\alpha M_\alpha$ for irreducible submodules M_α. Then each M_α is a representation of R. Given $a \in R$ with $a \neq 0$, the fact that M is faithful means $ax \neq 0$ for some $x = (x_\alpha) \in M$. Thus, $ax_\alpha \neq 0$ for some α. Then M_α is the desired irreducible representation witnessing that $a \neq 0$, making R semiprimitive. □

Corollary 4.1.16 Let R be a ring in which ${}_RR$ is semisimple. Then R is semiprimitive.

Proof. We show that ${}_RR$ is a faithful representation of R. Indeed, given $0 \neq a \in R$, we have $a \cdot 1 = a \neq 0$, so the map $\rho : R \to \mathrm{End}({}_RR)$ given by $\rho(a)b = ab$ must be injective. □

With this in hand, we can take a look at some examples.

Example 4.1.17

(1) Consider the integers $\mathbb{Z}$. We've seen that this is not semisimple. We show however that it is semiprimitive. One way to do this is to look at the ideal quotients $(I : \mathbb{Z})$ where I is a maximal ideal of $\mathbb{Z}$. The ideals I are simply (p) where p is prime. Now:

$$((p) : \mathbb{Z}) = \{a \in \mathbb{Z} : a\mathbb{Z} \subseteq (p)\} = \{a \in \mathbb{Z} : p \mid a\} = (p)$$

Thus,

$$\bigcap_{J \in \mathcal{M}_L(\mathbb{Z})} (J : \mathbb{Z}) = \bigcap_{\substack{p \in \mathbb{Z} \\ p \text{ prime}}} (p)$$

and it's easy to see that this is 0 (as the only integer divisible by every prime is 0).

(2) Now consider $\mathbb{Z}/(n)$ for $n > 0$. We've seen that, as a $\mathbb{Z}$-module, $\mathbb{Z}/(n)$ is semisimple precisely when n is a product of distinct prime factors. What can we say about semiprimitivity? If it is the case that $\mathbb{Z}/(n)$ is semisimple, it is immediate that $\mathbb{Z}/(n)$ is semiprimitive. Otherwise, suppose $\mathbb{Z}/(n)$ is not semisimple. Write $n = p_1^{r_1} \cdots p_k^{r_k}$ and assume WLOG that $r_1 > 1$. We know that the maximal ideals of $\mathbb{Z}/(n)$ are those of the form (p_i), and:

$$((p_i) : \mathbb{Z}/(n)) = \{a \in \mathbb{Z}/(n) : a(\mathbb{Z}/(n)) \subseteq (p_i)\} = (p_i)$$

It's easy to see that $p_1 \cdots p_k \in (p_i)$ for each i, which means $p_1 \cdots p_k \in \bigcap_{i=1}^{k}((p_i) : \mathbb{Z}/(n))$. But since $r_1 > 1$, $p_1 \cdots p_k \neq 0$ in $\mathbb{Z}/(n)$. Hence, $\mathbb{Z}/(n)$ is not semiprimitive in this case.

(3) We can build semiprimitive rings out of primitive ones. Let $\{R_\alpha\}$ be a collection of primitive rings and let $R = \prod_\alpha R_\alpha$ be the direct (cartesian) product. This has the structure of a ring under coordinate-wise addition and multiplication:

$$(x_\alpha) + (y_\alpha) = (x_\alpha + y_\alpha)$$
$$(x_\alpha) \cdot (y_\alpha) = (x_\alpha y_\alpha)$$

We wish to show that R is semiprimitive, which means finding a faithful semisimple representation for it. Each R_α has a faithful irreducible representation M_α. Each M_α can be viewed as an R-module: if $r = (r_\alpha) \in R$, then define $rx = r_\alpha x$ for each $x \in M_\alpha$. It's easy to check that M_α is irreducible as an R-module (but not necessarily faithful).

Now consider the R-module $M = \bigoplus_\alpha M_\alpha$. This is semisimple. We also see that for $r = (r_\alpha) \in R$, if $rx = 0$ for each $x \in M$, then for ever α we have $r_\alpha x_\alpha = 0$ for all $x_\alpha \in M$. Since M_α is faithful as an R_α-module, this forces $r_\alpha = 0$. Hence, $r = 0$, making M faithful. From this we get that R is semiprimitive.

This generalizes to so-called *subdirect products* of primitive rings. In fact, one can show that semiprimitivity is equivalent to being a subdirect product of primitive rings. See **Exercise 4.1.22**.

As an immediate consequence of the last example, we have

Corollary 4.1.18 If $\{R_\alpha\}$ is a collection of semiprimitive rings, then $\prod_\alpha R_\alpha$ is semiprimitive.

Exercises

Exercise 4.1.19 Let R be a ring and M an R-module. Recall that the annihilator of M is defined to be $\mathrm{Ann}_R(M) = \{a \in R : ax = 0 \text{ for all } x \in M\}$ and this is an ideal of R. Let $I = \mathrm{Ann}_R(M)$.

Show that M has a well-defined R/I-module structure given by $(a+I)x = ax$. Show also that if M is irreducible as an R-module, it's also irreducible as an R/I-module.

Exercise 4.1.20 Let V be a vector space over a division ring D and let $\mathrm{End}_D(V)$ be the ring of D-linear operators on V.

(a) Prove that $\mathrm{End}_D(V)$ *acts transitively* on the non-zero elements of V in the following sense: given any two $v, w \in V$ with $v, w \neq 0$, there exists $T \in \mathrm{End}_D(V)$ with $Tv = w$.

(b) Conclude from this that V is a faithful irreducible representation of $\mathrm{End}_D(V)$, and thus that $\mathrm{End}_D(V)$ is primitive.

(c) Show that if V is infinite dimensional, then the set $F = \{T \in \mathrm{End}_D(V) : \mathrm{rank}\, T < \infty\}$ is a non-zero proper ideal. Conclude that $\mathrm{End}_D(V)$ is not simple.

(d) Show that if V is countably-infinite dimensional, then F defined above is the *only* proper non-zero ideal. Thus, $\mathrm{End}_D(V)/F$ is simple.

(Hint: much of what can be done in vector spaces over fields can be done over division rings. For instance, any linearly-independent subset of V can be extended to a basis for V.)

Definition 4.1.21 Let $\{R_\alpha\}$ be a collection of rings and let $P = \prod_\alpha R_\alpha$ be their product, as defined in **Example 4.1.17 (3)**. Associated to each product is a surjective ring homomorphism $p_\alpha : P \to R_\alpha$ mapping a tuple (r_α) to r_α.

A ring R is called a **subdirect product** of $\{R_\alpha\}$ when there exists an injective ring homomorphism $f : R \to P$ such that each $p_\alpha \circ f : R \to R_\alpha$ is surjective.

It's easy to check that P itself is a subdirect product, by taking f to be the identity map.

Exercise 4.1.22

(a) Show that a ring R is semiprimitive if and only if R is a subdirect product of a collection of primitive rings.

(b) Use this to conclude that if R is commutative, then R is semiprimitive if and only if R is a subdirect product of a collection of fields.

4.2 Measuring semiprimitivity – the Jacobson radical

We've seen both the representation view of primitivity and semiprimitivity as well as the ring-theoretic view which uses ideals. In the view of representations, R is semiprimitive when each $0 \neq a \in R$ has an irreducible representation (M, ρ) with $\rho(a) \neq 0$. Another way to put this is as follows: if $a \in R$ is such that $a \in \ker \rho$ for every irreducible representation (M, ρ), we must have $a = 0$. Or more concisely: $\{a \in R : aM = 0 \text{ for every irreducible module } M\} = 0$. We have a name for this set:

Definition 4.2.1 The **Jacobson radical** of R is defined to be:

$$\mathcal{J}(R) = \{a \in R : aM = 0 \text{ for every irreducible module } M\}$$

That is, $\mathcal{J}(R)$ is the set of all elements of R that annihilate every irreducible representation of R. If $\{(M_\alpha, \rho_\alpha)\}$ is the collection of all irreducible representations of R, then we can write:

$$\mathcal{J}(R) = \bigcap_\alpha \text{Ann}_R(M_\alpha) = \bigcap_\alpha \ker \rho_\alpha$$

Evidently therefore, $\mathcal{J}(R)$ is an ideal of R.

Thus, we have that R is semiprimitive if and only if $\mathcal{J}(R) = 0$. This indicates that $\mathcal{J}(R)$ should be thought of as a measure of how close R is to being semiprimitive, much in the same way as $\ker f$ is a measure of how close a homomorphism f is to being injective. The closer $\mathcal{J}(R)$ is to 0, the closer R is to being semiprimitive.

Our goal for this section is to give a plethora of equivalent characterizations of $\mathcal{J}(R)$:

- in terms of irreducible representations (already done above);
- in terms of *primitive* ideals (which will be defined soon);
- in terms of maximal left ideals;
- in terms of *quasiregular*[2] *elements* of R.

Once this is done, we will dualize and show that the above also hold if we replace "left" with "right" (and this last condition listed permits this remarkable phenomenon).

We've shown that R is semiprimitive if and only if $\bigcap_{I \in \mathcal{M}_L(R)} (I : R) = 0$, where $(I : R) = \{a \in R : aR \subseteq I\}$ is the ideal quotient of I with R and $\mathcal{M}_L(R)$ is the set of maximal left ideals of R. Is there a relation between this intersection and $\mathcal{J}(R)$? These turn out to in fact be the same. In fact, this is easy to see: recall that if (M, ρ) is an irreducible representation, then $M \cong R/I$ for $I \in \mathcal{M}_L(R)$, and we have $\ker \rho = \text{Ann}_R(M) = (I : R)$.

[2]This was seen once a while back, in **Definition 1.4.17**

Definition 4.2.2 An ideal P of R is called **(left) primitive** when $P = (I : R)$ for some $I \in \mathcal{M}_L(R)$ (or equivalently, when $P = \text{Ann}_R(M) = \ker \rho$ for an irreducible representation (M, ρ) of R).

We let $\text{Prim}(R)$ denote the set of all primitive ideals of R.

From this, we have:

Proposition 4.2.3 For any ring R, we have:

$$\mathcal{J}(R) = \bigcap_{P \in \text{Prim}(R)} P$$

Moreover, P is primitive ideal of R if and only if R/P is a primitive ring.

Proof. The intersection above is clear. As for the second statement, if P is primitive then $P = (I : R)$ for $I \in \mathcal{M}_L(R)$. Let $M = R/I$ so that $\text{Ann}_R(M) = (I : R) = P$. This is an irreducible R-module. For each $a + P \in R/P$, define $(a + P)x = ax$. Then M has an irreducible R/P-module structure (**Exercise 4.1.19**). Moreover, if $(a + P)M = 0$, then $aM = 0$ which means $a \in P$ and $a + P = P$. Thus, M is faithful as an R/P-module, making R/P primitive.

Conversely if P is an ideal such that R/P is primitive, then we can find a maximal left ideal $\overline{I}$ of R/P which contains no non-zero ideals. Now $\overline{I} = I/P$ where I is a maximal left ideal of R containing P. The fact that $\overline{I}$ has no non-zero ideals means I/P has no ideals which properly contain P. Now $(I : R)$ is the largest ideal contained in I, which implies $P \subseteq (I : R)$. Hence, $P = (I : R)$, making P primitive. □

It's worth noting that primitivity is *not* symmetric. That is, if we say an ideal P is *right primitive* when $P = \langle J : R \rangle := \{a \in R : Ra \subseteq J\}$ for a maximal right ideal J, then it's not necessarily the case that a (left) primitive ideal is right primitive. Hence, it's not necessarily the case that a (left) primitive ring is right primitive. When we dualize all these concepts at the end of this section, we shall see that semiprimitivity *is* symmetric.

We can also define the Jacobson radical in terms of maximal left ideals themselves (rather than ideal quotients of them).

Proposition 4.2.4 For any ring R, we have:

$$\mathcal{J}(R) = \bigcap_{I \in \mathcal{M}_L(R)} I$$

Proof. We make the observation that for M irreducible,

$$\text{Ann}_R(M) = \bigcap_{x \in M} \text{Ann}_R(x) = \bigcap_{\substack{x \in M \\ x \neq 0}} \text{Ann}_R(x)$$

Each $\text{Ann}_R(x)$ for $x \neq 0$ is a left ideal, and irreducibility of M means these are maximal (**Lemma 4.1.5**). Hence, $\text{Ann}_R(M)$ is an intersection of maximal left ideals, and thus so is $\mathcal{J}(R)$. From this we obtain:

$$\mathcal{J}(R) \supseteq \bigcap_{I \in \mathcal{M}_L(R)} I$$

On the other hand, we know that:

$$\mathcal{J}(R) = \bigcap_{I \in \mathcal{M}_L(R)} (I : R)$$

and that each $(I : R) \subseteq I$. It thus follows that equality in fact holds. □

We get some nice consequences of this characterization.

Corollary 4.2.5 For any ring R, we have $\mathcal{J}(R/\mathcal{J}(R)) = 0$. Hence, $R/\mathcal{J}(R)$ is semiprimitive. Moreover, $\mathcal{J}(R)$ is the unique smallest ideal such that $R/\mathcal{J}(R)$ is semiprimitive. That is, if B is another ideal of R such that R/B is semiprimitive, we must have $\mathcal{J}(R) \subseteq B$.

Proof. Every maximal left ideal of $R/\mathcal{J}(R)$ is of the form $I/\mathcal{J}(R)$ where I is a maximal left ideal of R. As such, we have:

$$\mathcal{J}(R/\mathcal{J}(R)) = \bigcap_{I \in \mathcal{M}_L(R)} I/\mathcal{J}(R) = \mathcal{J}(R)/\mathcal{J}(R) = 0$$

which makes $R/\mathcal{J}(R)$ semiprimitive. Now if B is an ideal of R with R/B semiprimitive, then the maximal left ideals of R/B are of the form I/B where I is a maximal left ideal of R containing B and we have:

$$0 = \mathcal{J}(R/B) = \bigcap_{\substack{I \in \mathcal{M}_L(R) \\ B \subseteq I}} I/B = \left(\bigcap_{\substack{I \in \mathcal{M}_L(R) \\ B \subseteq I}} I \right) /B$$

which means:

$$\mathcal{J}(R) = \bigcap_{I \in \mathcal{M}_L(R)} I \subseteq \bigcap_{\substack{I \in \mathcal{M}_L(R) \\ B \subseteq I}} I = B$$

□

Finally, we get to the characterization of $\mathcal{J}(R)$ in terms of the elements of R. Recall that an element $z \in R$ is *quasiregular* when $1 - z$ is invertible. We can make similar definitions for invertibility on the left and right:

Definition 4.2.6 An element $z \in R$ is **left (right) quasiregular** when $1-z$ is left (right) invertible. That is, there exists $u \in R$ such that $u(1 - z) = 1$ ($(1 - z)u = 1$). It is clear that if z is both left and right quasiregular, then it is quasiregular in the sense of the definition above.

We can also give the following equivalent characterization for quasiregularity.

Proposition 4.2.7 $z \in R$ is left (right) quasiregular if and only if $R(1-z) = R$ ($(1-z)R = R$), where $R(1-z) = \{a(1-z) : a \in R\}$ and $(1-z)R = \{(1-z)a : a \in R\}$.

Proof. Clear. □

What sorts of elements are quasiregular?

Example 4.2.8

(1) Let R be any ring and suppose $z \in R$ is *nilpotent*, which means there is an $n \geqslant 1$ with $z^n = 0$. Then it's easy to check that $(1-z)(1+z+z^2+\cdots+z^{n-1}) = 1$ and similarly $(1+z+z^2+\cdots+z^{n-1})(1-z) = 1$. Thus, every nilpotent element is quasiregular.

(2) Suppose $z \in R$ is such that z^2 is left quasiregular. We see then that $u(1-z^2) = 1$ for some $u \in R$. But $1 - z^2 = (1+z)(1-z) = (1-z)(1+z)$, so it follows that both z and $-z$ are left quasiregular as well. A similar argument shows that if z^2 is right quasiregular, so is z. Thus, z^2 being quasiregular implies z is too.

(3) It's not the case that z being quasiregular implies z^2 is quasiregular. To see this, consider the ring $M_2(\mathbb{R})$ and the matrix $Z = -I$. Then Z is quasiregular since $I - Z = 2I$ is invertible, but $Z^2 = I$, which is not quasiregular.

Definition 4.2.9 If Z is a left ideal of R, we shall say Z is **quasiregular** when every element of Z is *left* quasiregular. Similarly if Z is a right ideal of R, Z is **quasiregular** when every element of Z is *right* quasiregular.

What can we say about quasiregular left/right ideals? We can establish a relation between quasiregular left ideals and the Jacobson radical.

Proposition 4.2.10 $\mathcal{J}(R)$ is a quasiregular left ideal. Moreover, it is the unique largest quasiregular left ideal. That is, if Z is any quasiregular left ideal of R, we must have $Z \subseteq \mathcal{J}(R)$.

Proof. Suppose $z \in \mathcal{J}(R)$ is not left quasiregular. Then $R(1-z)$ is a proper left ideal, so it's contained in some maximal left ideal $I \in \mathcal{M}_L(R)$ (**Exercise 3.4.17**). But $z \in I$ as well since $\mathcal{J}(R) = \bigcap_{J \in \mathcal{M}_L(R)} J$. Hence, $1 = 1 - z + z \in I$ so that $I = R$, contradicting maximality of I. Thus, $\mathcal{J}(R)$ is indeed quasiregular left.

Now let Z be any quasiregular left ideal of R and suppose $Z \not\subseteq \mathcal{J}(R)$. Then there exists some $I \in \mathcal{M}_L(R)$ with $Z \not\subseteq I$. Now $I \subsetneq I + Z$, which forces $I + Z = R$. We can thus write $1 = a + z$ for some $a \in I$ and $z \in Z$, which means $a = 1 - z$. Since z is left quasiregular, there is a $u \in R$ with $1 = u(1-z) = ua \in I$, contradicting maximality of I. Thus, we must have $Z \subseteq \mathcal{J}(R)$. □

As a consequence of this, we can explicitly describe the elements of $\mathcal{J}(R)$ in terms of quasiregularity:

Corollary 4.2.11 $\mathcal{J}(R) = \{z \in R : az \text{ is left quasiregular for all } a \in R\}$.

Proof. If $z \in R$ is such that az is left quasiregular for all $a \in R$, then Rz is a quasiregular left ideal, so $Rz \subseteq \mathcal{J}(R)$. On the other hand, given $z \in \mathcal{J}(R)$ we have $az \in \mathcal{J}(R)$ for all $a \in R$. Since $\mathcal{J}(R)$ is itself left quasiregular, it follows that az is left quasiregular for all $a \in R$. □

Putting together what we have done, we have shown that $\mathcal{J}(R)$ is equivalent to either of the following:

- $\{a \in R : aM = 0 \text{ for every irreducible module } M\}$;
- $\bigcap_{P \in \mathrm{Prim}(R)} P$;
- $\bigcap_{I \in \mathcal{M}_L(R)} I$;
- $\{z \in R : az \text{ is left quasiregular for all } a \in R\}$.

We are now ready to dualize. To do this, simply notice that we can carry out what was done in the previous sections of this chapter in the setting of *right* R-modules (or equivalently, left R^{op}-modules) instead. With this, we arrive at the following dual notions and observations:

- An **antirepresentation** of R is a pair (M, ρ) where M is an abelian group and $\rho : R \to \mathrm{End}(M)$ is an *antihomomorphism*: $\rho(ab) = \rho(b)\rho(a)$. This gives M the structure of a *right* R-module: $xa = \rho(a)x$ for all $a \in R$ and $x \in M$.
- Let $\mathcal{M}_R(R)$ be the set of all maximal right ideals of R. A right R-module M is irreducible if and only if $M \cong R/J$ for some $J \in \mathcal{M}_R(R)$. We define the **right ideal quotient** of a right ideal J with R by $\langle J : R \rangle = \{a \in R : Ra \subseteq J\}$.
- A ring R is **right primitive** when R has a faithful irreducible antirepresentation. An ideal P of R is **right primitive** when R/P is right primitive (or equivalently, when $P = \langle J : R \rangle = \mathrm{Ann}_R(R/J)$ for J a maximal right ideal). Let $\mathrm{Prim}'(R)$ denote the set of all right primitive ideals.
- Now define the **right Jacobson radical** by $\mathcal{J}'(R) = \{a \in R : Ma = 0 \text{ for every irreducible right module } M\}$. Then we have:

$$\mathcal{J}'(R) = \bigcap_{P \in \mathrm{Prim}'(R)} P = \bigcap_{J \in \mathcal{M}_R(R)} J$$

- $\mathcal{J}'(R)$ is the unique largest quasiregular right ideal (that is, it contains every quasiregular right ideal). Moreover:

$$\mathcal{J}'(R) = \{z \in R : za \text{ is right quasiregular for all } a \in R\}$$

Our goal now is to show that we in fact have $\mathcal{J}(R) = \mathcal{J}'(R)$. Thus, the Jacobson radical is a symmetric notion and semiprimitivity is as well.

To do this, we introduce a new structure on R based on the map $a \mapsto 1-a$. Define a binary operation $\circ$ on R by: $a \circ b = a + b - ab$. We see that for $a, b, c \in R$:

$$(a \circ b) \circ c = (a+b-ab) \circ c = (a+b-ab)+c-(a+b-ab)c = (a+b+c)-(ab+ac+bc)+abc$$

$$a \circ (b \circ c) = a \circ (b+c-bc) = a+(b+c-bc)-a(b+c-bc) = (a+b+c)-(ab+ac+bc)+abc$$

and so $\circ$ is associative. We also have $a \circ 0 = 0 \circ a = a$ so $\circ$ has 0 as the identity. This makes $(R, \circ, 0)$ a *monoid* (see **Definition 1.1.1**). Recall that $(R, \cdot, 1)$ is also a monoid. We can establish the following strong relation between these:

Proposition 4.2.12 The map $\sigma : (R, \circ, 0) \to (R, \cdot, 1)$ given by $\sigma(a) = 1 - a$ is a monoid isomorphism.

Proof. Notice that as a function from R to itself, we have $\sigma^2(a) = \sigma(1-a) = a$ so that $\sigma^2 = \mathrm{id}_R$. Hence, σ is bijective. What's left to show is σ is indeed a monoid homomorphism.

To that end, let $a, b \in R$. Then:

$$\sigma(a \circ b) = \sigma(a+b-ab) = 1-(a+b-ab) = 1-a-b+ab = (1-a)(1-b) = \sigma(a)\sigma(b)$$

and $\sigma(0) = 1 - 0 = 1$. □

This isomorphism then gives us information above invertibility with respect to $\circ$.

Corollary 4.2.13 An element $z \in R$ is (left/right) invertible in $(R, \circ)$ if and only if z is (left/right) quasiregular.

Proof. z is left invertible in $(R, \circ)$ if and only if $\sigma(z) = 1 - z$ is left invertible with respect to $\cdot$, which precisely means z is left quasiregular. A similar argument shows that z is right invertible in $(R, \circ)$ if and only if z is right quasiregular, and thus z is invertible in $(R, \circ)$ if and only if z is quasiregular. □

The result that allows us to establish the symmetry of the Jacobson radical is:

Proposition 4.2.14 If Z is a quasiregular left (right) ideal, then Z is a subgroup of $(R, \circ)$.

Proof. We shall assume Z is a left ideal (the right ideal case is similar). First observe that $0 \in Z$. Also if $z, w \in Z$ then $z \circ w = z + w - zw \in Z$. Suppose $z \in Z$ and let $u \in R$ be such that $u(1-z) = 1$. Then we can let $w = 1 - u$ so that $1 = (1-w)(1-z) = 1-w-z+wz$, which gives $w \circ z = w+z-wz = 0$. Notice that $w = wz - z \in Z$. So by a similar argument, we have some $z' \in Z$ with $z' \circ w = 0$. Now z' is a left inverse of w and z is a right inverse of w, which means they must coincide: $z = z'$. From this it follows that $z \circ w = w \circ z = 0$, so $w \in Z$ is an inverse for z. □

Corollary 4.2.15 $\mathcal{J}(R) = \mathcal{J}'(R)$.

Proof. Since $\mathcal{J}(R)$ is a quasiregular left ideal, it is a subgroup of $(R, \circ)$. Similarly $\mathcal{J}'(R)$ being quasiregular right means it's also a subgroup of $(R, \circ)$. Hence, every element of $\mathcal{J}(R)$ is in fact invertible in $(R, \circ)$, therefore quasiregular in R. The same goes for $\mathcal{J}'(R)$. Therefore $\mathcal{J}(R)$ is a quasiregular right ideal and $\mathcal{J}'(R)$ is a quasiregular left ideal, which shows $\mathcal{J}(R) \subseteq \mathcal{J}'(R)$ and $\mathcal{J}'(R) \subseteq \mathcal{J}(R)$. □

We can finally give a list of all equivalent characterizations of the Jacobson radical that we have established:

Theorem 4.2.16 The Jacobson radical $\mathcal{J}(R)$ of R is equal to all of the following:

- $\{a \in R : aM = 0 \text{ for every irreducible (left) module } M\}$;
- $\bigcap_{P \in \mathrm{Prim}(R)} P$, the intersection of all (left) primitive ideals;
- $\bigcap_{I \in \mathcal{M}_L(R)} I$, the intersection of all maximal left ideals;
- the unique largest quasiregular left ideal of R;
- $\{z \in R : az \text{ is left quasiregular for all } a \in R\}$;
- $\{a \in R : Ma = 0 \text{ for every irreducible right module } M\}$;
- $\bigcap_{P \in \mathrm{Prim}'(R)} P$, the intersection of all right primitive ideals;
- $\bigcap_{I \in \mathcal{M}_R(R)} I$, the intersection of all maximal right ideals;
- the unique largest quasiregular right ideal of R;
- $\{z \in R : za \text{ is right quasiregular for all } a \in R\}$.

Exercises

Let R be a ring.

Exercise 4.2.17 Show that $R = \mathcal{J}(R)$ if and only if $R = 0$.

Recall that R is *local* when the set $R \setminus R^\times$ is an ideal.

Exercise 4.2.18 Use **Exercise 3.3.13** to show that R is local if and only if $R/\mathcal{J}(R)$ is a division ring, in which case $\mathcal{J}(R) = R \setminus R^\times$.

Exercise 4.2.19 Consider $\mathbb{Z}/(n)$ for $n > 0$ and write $n = p_1^{r_1} \cdots p_k^{r_k}$ for distinct primes p_i and $r_i \geqslant 1$. Show that $\mathcal{J}(\mathbb{Z}/(n)) = (p_1 \cdots p_k)$. Conclude (again) that $\mathbb{Z}/(n)$ is semiprimitive if and only if n is a product of distinct primes.

Exercise 4.2.20 Show that $z \in \mathcal{J}(R)$ if and only if for every $a \in R$, there exists a $w \in R$ with $z + w = waz = zaw$.

Definition 4.2.21 An element $a \in R$ is called **von Neumann regular** when a has a "weak inverse": there exists an element $b \in R$ with $aba = a$.

If every element of R is von Neumann regular, then R is called **von Neumann regular**.

Exercise 4.2.22 Show that if $a \in \mathcal{J}(R)$ is von Neumann regular, then $a = 0$. Hence conclude that every von Neumann regular ring is semiprimitive.

Recall that an element $e \in R$ is *idempotent* when $e^2 = e$.

Exercise 4.2.23 Let $e \in R$ be idempotent with $e \neq 0$.

(a) Show that the set $eRe = \{eae : a \in R\}$ is a ring under $+$ and $\cdot$, but where the identity element is e (thus, eRe is *not necessarily* a subring of R).

(b) Show that if R is primitive, then eRe is primitive.

(c) Show also that $\mathcal{J}(eRe) = e\mathcal{J}(R)e = \{eze : z \in \mathcal{J}(R)\}$, and that this is equal to $eRe \cap \mathcal{J}(R)$. Conclude that if R is semiprimitive, then so is eRe.

We've seen in **Exercise 1.4.9** the ideals of R and the ideals of $M_n(R)$ (the matrix ring with entries in R) are in bijective correspondence via $I \mapsto M_n(I)$. Hence, $M_n(R)$ is simple if and only if R is simple.

Exercise 4.2.24

(a) Show that if R is primitive, then so is $M_n(R)$.

(b) Show that $\mathcal{J}(M_n(R)) = M_n(\mathcal{J}(R))$. Thus conclude that R is semiprimitive if and only if $M_n(R)$ is semiprimitive.

(Hint for **(b)**: $E_{1,1}$ denote the matrix with 1 in the $(1,1)$ entry and 0 elsewhere. Consider the map $f : R \to E_{1,1}M_n(R)E_{1,1}$ given by $f(a) = aE_{1,1}$. Show that f is a ring isomorphism and therefore $f(\mathcal{J}(R)) = \mathcal{J}(E_{1,1}M_n(R)E_{1,1})$. Now apply the previous exercise.)

Exercise 4.2.25 (Nakayama's lemma)
Let M be a finitely-generated R-module. For an ideal I, we define $IM = \{ax : a \in I, x \in M\}$. Show that if $\mathcal{J}(R)M = M$, then $M = 0$.

(Hint: suppose $M \neq 0$. Then there exists a *minimum* $n \geqslant 1$ for which M is generated by some $x_1, ..., x_n \in M$.)

4.3 Classifying our building blocks – the Jacobson density theorem

In this section, we give a way of identifying any primitive ring R as a "dense" subring of $\mathrm{End}_D(V)$ where V is a vector space over a division ring D. After this, we will narrow down to the case where R is also left Artinian and see that things become even nicer. Before this, we of course need to make precise what we mean by "dense" here.

Let V be a vector space over a division ring D. Recall in **Exercise 4.1.20** that we've seen $\mathrm{End}_D(V)$ *acts transitively* in that for any $0 \neq v \in V$ and $w \in V$, there is $T \in \mathrm{End}_F(V)$ with $w = Tv$. This fact generalizes in the following way: given a finite set $v_1, ..., v_n \in V$ of *linearly-independent* vectors and corresponding $w_1, ..., w_n \in V$, there exists $T \in \mathrm{End}_D(V)$ with $w_i = Tv_i$.

One can ask if a given subset $\mathcal{S} \subseteq \mathrm{End}_D(V)$ exhibits this property too, and if it does we call $\mathcal{S}$ *dense*. For instance if V is a vector space with countable basis $\{e_1, e_2, ...\}$ and we let $\mathcal{S} = \{T \in \mathrm{End}_F(V) : \mathrm{rank}\, T < \infty\}$, the set of finite-rank operators, then it's easy to see that $\mathcal{S}$ is dense (and proper). On the other hand, it's easy to see that if V is finite-dimensional and $\mathcal{S} \subseteq \mathrm{End}_D(V)$ is dense, then we must in fact have $\mathcal{S} = \mathrm{End}_D(V)$.

Thus, we seek to show that every primitive ring is isomorphic to a dense (in the above sense) subring of $\mathrm{End}_D(V)$ for V a vector space over D. Towards this, we consider a generalization. Let R be a ring and let M be a *semisimple* R-module. Then:

Definition 4.3.1 Let $R' = \mathrm{End}_R(M)$, the ring of R-endomorphisms on M. We shall call R' the **commutant** of R in M.

It is easy to verify that M has an R'-module structure given by $f \cdot x = f(x)$ for all $f \in R'$ and $x \in M$. We then let $R'' = (R')' = \mathrm{End}_{R'}(M)$, the ring of R'-endomorphisms on M. We shall call R'' the **bicommutant** of R in M.

We'll often stick to writing R' and R'' when the choice of M is clear (which is almost always the case), but otherwise we'll write $R'(M)$ and $R''(M)$ if indication of the module M is required.

Remark 4.3.2 The choice of name for R' and R'' can be explained as follows: first, the elements of $R' = \mathrm{End}_R(M)$ are characterized as those group endomorphisms $f \in \mathrm{End}(M)$ satisfying $f(ax) = af(x)$ for all $a \in R$ and $x \in M$. Hence, R' can be seen as precisely the elements of $\mathrm{End}(M)$ which "commute" with every element of R in this sense.

Similarly, the elements of R'' are precisely those $\varphi \in \mathrm{End}(M)$ which satisfy $\varphi(f(x)) = f(\varphi(x))$ for all $f \in R'$ and $x \in M$ (in other words, $\varphi f = f\varphi$ for all $f \in R'$). Thus, R'' are all the elements of $\mathrm{End}(M)$ which "commute" with the elements of R'.

Finally, for each $a \in R$ let $\lambda_a \in \mathrm{End}(M)$ be the left multiplication map: $\lambda_a(x) = ax$. Then for any $f \in R'$, we have $\lambda_a(f(x)) = af(x) = f(ax) = f(\lambda_a(x))$ for all $x \in M$, which means $\lambda_a \in R''$. This yields a ring homomorphism $\lambda : R \to R''$ given by $a \mapsto \lambda_a$ (which is injective if and only if M is faithful as an R-module).

We shall refer to λ as the *natural map* of R to R''.

If N is an R-submodule of M, it's not necessarily the case that it is also an R'-submodule (even given that M is semisimple). An example can be seen with a vector space V over F of dimension 2 or higher. In this case $F' = \mathrm{End}_F(V)$ and if we fix any proper non-zero subspace W of V, it's clear that W can't be an F'-submodule thanks to the transitivity property described earlier. However, we do have:

Lemma 4.3.3 If N is an R-submodule of M, it is an R''-submodule.

Proof. Since M is semisimple, we can write $M = N \oplus P$ for a submodule P of M. Let $e \in R'$ be the projection map onto N. Then $\operatorname{im} e = N$ and $e(x) = x$ for all $x \in N$. Thus, given any $\varphi \in R''$ and any $x \in N$, we have $\varphi(x) = \varphi e(x) = e\varphi(x) \in N$, so N is indeed an R''-submodule. □

We shall now give the statement of the

Theorem 4.3.4 (Jacobson density theorem)
Let M be a semisimple R-module with commutant and bicommutant $R' = \mathrm{End}_R(M)$ and $R'' = \mathrm{End}_{R'}(M)$ in M. Then the image of the natural map $\lambda : R \to R''$ is *dense* in R'' in the following sense: for any $x_1, ..., x_n \in M$ and any $\varphi \in R''$, there exists an $a \in R$ such that $\varphi(x_i) = ax_i$ for each i.

Moreover, if M is finitely-generated as an R'-module, then in fact $\operatorname{im} \lambda = R''$.

Our method of proof will be a sort of induction on n, but one where we only need the base case $n = 1$ to establish the result for general n. For this, we require the following

Lemma 4.3.5 For $n \geqslant 1$, let $M^{(n)} = \bigoplus_{i=1}^n M$. Then $R'(M^{(n)}) = \mathrm{End}_R(M^{(n)})$ is the set of maps $(x_1, ..., x_n) \mapsto (y_1, ..., y_n)$ where each $y_j = \sum_{k=1}^n f_{j,k}(x_k)$ for some $f_{j,k} \in R' = \mathrm{End}_R(M)$.

Also for every $\varphi \in R'' = \mathrm{End}_{R'}(M)$, the map $(x_1, ..., x_n) \mapsto (\varphi(x_1), ..., \varphi(x_n))$ is in $R''(M^{(n)}) = \mathrm{End}_{R'(M^{(n)})}(M^{(n)})$.

Proof. It's clear that any such mapping is an element of $R'(M^{(n)})$. Conversely, suppose $f \in R'(M^{(n)})$. Let $p_j : M^{(n)} \to M$ and $i_j : M \to M^{(n)}$ be the projection and injection corresponding to the j^{th} coordinate. For each $j, k \in \{1, ..., n\}$, let $f_{j,k} = p_j f i_k \in R' = \mathrm{End}_R(M)$. Then the j^{th} coordinate of $f(x_1, ..., x_n)$ is given by:

$$p_j f(x_1, ..., x_n) = \sum_{k=1}^n p_j f i_k(x_k) = \sum_{k=1}^n f_{j,k}(x_k)$$

which proves the first statement. Now let $\varphi \in R''$ and let $\psi(x_1, ..., x_n) = (\varphi(x_1), ...\varphi(x_n))$. It's easy to check this is an R-homomorphism. If $f \in R'(M^{(n)})$ then we can write $f(x_1, ..., x_n) = (\sum_{k=1}^n f_{1,k}(x_k), ..., \sum_{k=1}^n f_{n,k}(x_k))$. Now the j^{th} coordinate of $\psi f(x_1, ..., x_n)$ is:

$$\varphi\left(\sum_{k=1}^n f_{j,k}(x_k)\right) = \sum_{k=1}^n \varphi f_{j,k}(x_k) = \sum_{k=1}^n f_{j,k}\varphi(x_k)$$

which is precisely the j^{th} coordinate of $f\psi(x_1, ..., x_n)$. ψ therefore commutes with f, which means $\psi \in \mathrm{End}_{R'(M^{(n)})}(M^{(n)})$. □

Now we can give the

Proof of the Jacobson density theorem. If $n = 1$, then we have just $x_1 \in M$. Consider the R-submodule Rx_1. Since M is semisimple, Rx_1 is also an R''-submodule of M by **Lemma 4.3.3**. Hence, for any $\varphi \in R''$, we have $\varphi(x_1) \in Rx_1$, which means $\varphi(x_1) = ax_1$ for some $a \in R$.

Now suppose $n > 1$. Let $x_1, ..., x_n \in M$ and $\varphi \in R''$. We consider $M^{(n)}$, which is also semisimple. Notice that $x = (x_1, ..., x_n) \in M^{(n)}$ satisfies that the map $(x_1, ..., x_n) \mapsto (\varphi(x_1), ..., \varphi(x_n))$ is in $R''(M^{(n)}) = \mathrm{End}_{R'(M^{(n)})}(M^{(n)})$ by the preceding lemma. Hence, by the base case above, we have some $a \in R$ for which $(\varphi(x_1), ..., \varphi(x_n)) = a(x_1, ..., x_n)$, which precisely means $\varphi(x_i) = ax_i$ for all i.

Finally, suppose M is finitely-generated as an R'-module so that $M = R'x_1 + \cdots + R'x_n$. Let $\varphi \in R''$ and choose $a \in R$ with $\varphi(x_i) = ax_i$ for all i. Given any $x \in M$, write $x = f_1(x_1) + \cdots + f_n(x_n)$ for $f_i \in R'$. Then since φ commutes with f_i, we have

$$\begin{aligned}
\varphi(x) &= \varphi f_1(x_1) + \cdots + \varphi f_n(x_n) \\
&= f_1\varphi(x_1) + \cdots + f_n\varphi(x_n) \\
&= f_1(ax_1) + \cdots + f_n(ax_n) \\
&= a(f_1(x_1) + \cdots + f_n(x_n)) \\
&= ax
\end{aligned}$$

and thus $\varphi = \lambda_a$. □

How do we relate this theorem to the classification of primitive rings? More precisely, given a primitive ring R, how do we find a division ring D and a vector space V over D which allows us to realize R as a dense subring of $\mathrm{End}_D(V)$? The key to this is in *Schur's lemma* (**2.3.12**). The proof is quite nice.

Corollary 4.3.6 (classification of primitive rings)
R is primitive if and only if it is isomorphic to a dense subring L of $\mathrm{End}_D(V)$ for D a division ring and V a vector space over D.

We recall that by density of L in $\mathrm{End}_D(V)$, we mean that for any $v_1, ..., v_n \in V$ linearly independent and corresponding $w_1, ..., w_n \in V$, there exists $T \in L$ with $w_i = Tv_i$ for each i.

Proof. Suppose first that R is primitive and let (V, λ) be a faithful irreducible (thus semisimple) representation of R. Notice here that $\lambda : R \to \mathrm{End}(V)$ is the natural map $\lambda(a) = \lambda_a$. Since λ is injective, $R \cong \mathrm{im}\,\lambda$. Since V is irreducible, $D = R' = \mathrm{End}_R(V)$ is a division ring by Schur's lemma. Now V is a vector space over D and $R'' = \mathrm{End}_D(V)$. It's clear that $\lambda : R \to \mathrm{End}_D(V)$. Thus, $L = \mathrm{im}\,\lambda$ is a subring of $\mathrm{End}_D(V)$. It remains to show that L is dense in $\mathrm{End}_D(V)$.

Let $v_1, ..., v_n \in V$ be linearly independent over D and let $w_1, ..., w_n \in V$. By independence of the v_i's, there is a linear map $T \in \mathrm{End}_D(V)$ with $w_i = Tv_i$ for all i. By the Jacobson density theorem, there exists an $a \in R$ with $av_i = Tv_i = w_i$ for all i; in other words, $\lambda_a v_i = w_i$. Since $\lambda_a \in L$, it follows that L is dense in $\mathrm{End}_D(V)$.

Now suppose $R \cong L$ where L is a dense subring of $\mathrm{End}_D(V)$ for some vector space V over a division ring D. Let $\lambda : R \to L$ be an isomorphism and equip an R-module structure on V by $av = \lambda(a)v$ for each $a \in R$. Then (V, λ) is a faithful representation of R. Moreover, if $U \neq 0$ is an R-submodule of V, then for any $0 \neq u \in U$ and any $w \in V$, there exists an $a \in R$ with $au = \lambda(a)u = w$ by density of L. Hence, we have that $U = V$, which makes V irreducible as an R-module. As such, R is primitive. □

Let's revisit the (few) primitive rings we've studied and see if we can realize them as dense subrings of linear operators.

Example 4.3.7

(1) If D is any division ring, we've seen that $M_n(D)$ is primitive. Clearly this is isomorphic to $\mathrm{End}_D(V)$ where V is any n-dimensional vector space over D (and this is of course dense in itself).

(2) We've seen that $\mathbb{Z}/(n)$ is primitive if and only if $n = p$ for p prime. In this case $\mathbb{Z}/(p)$ is a field and we simply have $\mathbb{Z}/(p) \cong \mathrm{End}_{\mathbb{Z}/(p)}(V)$ for any one-dimensional vector space V over $\mathbb{Z}/(p)$.

(3) If V is any infinite-dimensional vector space over D and $\mathcal{F} = \{T \in \mathrm{End}_D(V) : \mathrm{rank}\, T < \infty\}$ is the set of finite-rank operators, it's clear that $\mathcal{F}$ is a proper dense subring in $\mathrm{End}_D(V)$. Hence, $\mathcal{F}$ is a primitive ring.

Now we restrict to the case where R is primitive and left Artinian. Recall that this latter condition means the left R-module ${}_RR$ is Artinian – in other words, the following equivalent conditions hold:

- any descending chain $I_1 \supseteq I_2 \supseteq \cdots$ of left ideals stabilizes;
- every non-empty collection of left ideals has a minimal element.

What can we say now? We know that all simple rings are primitive. Artinianity also gives us the converse, and in this case we obtain a concrete description of what such a ring is. We have the following:

Proposition 4.3.8 Let R be a ring. Then the following are equivalent:

(i) R is simple and left Artinian;

(ii) R is primitive and left Artinian;

(iii) $R \cong \mathrm{End}_D(V)$ where V is a *finite-dimensional* vector space over a division ring D;

(iv) $R \cong M_n(D)$ for D a division ring.

Proof. We've already seen that **(i)** implies **(ii)**, and clearly **(iii)** and **(iv)** are equivalent (since if $\dim(V) = n$, then $\mathrm{End}_D(V) \cong M_n(D^{\mathrm{op}})$ – see **Exercise 2.5.7**).

If R is primitive and left Artinian, then R is isomorphic to a dense subring L of $\mathrm{End}_D(V)$ where V is a vector space over a divison ring D. Notably L is also left Artinian. We show that V is finite-dimensional; it will follow then that $L = \mathrm{End}_D(V)$

since $\mathrm{End}_D(V)$ is the only dense subset in this case. If V is not finite-dimensional, then there is an independent set $\{v_1, v_2, ...\}$. For each $i \geqslant 1$, let $I_i = \mathrm{Ann}_L(v_i) = \{T \in L : Tv_i = 0\}$. These are left ideals in L. For each $k \geqslant 1$, let $J_k = \bigcap_{i=1}^{k} I_i$. Explicitly, $J_k = \{T \in L : Tv_i = 0 \text{ for all } 1 \leqslant i \leqslant k\}$.

Now for each $k \geqslant 1$, the density of L and the independence of $v_1, ..., v_{k+1}$ mean there is a $T \in L$ for which $Tv_i = 0$ for $1 \leqslant i \leqslant k$ and $Tv_{k+1} \neq 0$. Thus, $T \in I_k$ but $T \notin I_{k+1}$. As such:

$$J_1 \supsetneq J_2 \supsetneq \cdots$$

is a proper descending chain of left ideals. But this contradicts that L is left Artinian. Thus, we must have V is finite-dimensional, which proves **(iii)**.

Finally, suppose **(iv)** holds. We've seen that $M_n(D)$ is a simple ring, so it remains to show that it is left Artinian. Let $J_1 \supseteq J_2 \supseteq \cdots$ be a descending chain of left ideals in $M_n(D)$. Since these are closed under the left action of $M_n(D)$, we have in particular that they are closed under the left action of D: for any $a \in D$ we have $aJ_i = (aI)J_i \subseteq J_i$. As such, the J_i's can be viewed as subspaces of the D-vector space $M_n(D)$. But $M_n(D)$ is finite dimensional, so if the chain was proper the dimensions of the subspaces would be strictly decreasing. Hence, it must stabilize. □

For the implication **(iv)** $\implies$ **(i)** in showing $M_n(D)$ is left Artinian, the same argument holds if we take $J_1 \supseteq J_2 \supseteq \cdots$ to be a descending chain of *right* ideals. In this case we view $M_n(D)$ as a *right* D-vector space and the subspaces J_i must stabilize. Hence, $M_n(D)$ is also right Artinian. As a consequence, we have the following interesting

Corollary 4.3.9 A simple ring R is left Artinian if and only if it's right Artinian.

Proof. If R is left Artinian, $R \cong M_n(D)$ for D a division ring. Since $M_n(D)$ is right Artinian, R is too. Conversely if R is right Artinian, then R^{op} is simple and left Artinian. Now $R^{\mathrm{op}} \cong M_n(D)$, so $R \cong M_n(D)^{\mathrm{op}} \cong M_n(D^{\mathrm{op}})$, which is also left Artinian. □

When speaking of a *simple* ring R, we may thus drop the specification of left or right in Artinianity and simply say it is Artinian. Simple Artinian rings will be our "building blocks" for the structure of a semisimple ring, as we will see soon.

Exercises

Let R be a ring.

Exercise 4.3.10 Suppose R is primitive with faithful irreducible R-module V and let $D = \mathrm{End}_R(V)$. Show that either:

- $R \cong M_n(D)$ for some n, or
- for each $k \geqslant 1$ there exists a subring S of R having $M_k(D)$ as a homomorphic image.

Exercise 4.3.11 Use the previous exercise to show that if R is a primitive ring such that for each $a \in R$ there is an $n \geqslant 2$ with $a^n = a$, then R must be a division ring.

Exercise 4.3.12 Let M be a semisimple R-module and let B be an ideal of R. Prove that the following are equivalent:

(i) $BM = M$ (where $IM = \{bx : b \in B, x \in M\}$);

(ii) for all $x \in M$, $Bx = 0$ implies $x = 0$;

(iii) for all $x \in M$, $x \in Bx$.

(Hint: it may help to write $M = \bigoplus_\alpha M_\alpha$ where M_α are irreducible submodules.)

Exercise 4.3.13 Let M and B be as in the preceding exercise, with $BM = M$. Consider the natural map $\lambda : R \to R''$ and its restriction $\lambda|_B : B \to R''$. Show that $\operatorname{im} \lambda|_B$ is dense in R''.

This shows that the Jacobson density theorem generalizes to the fact that the image of the natural map under any ideal B satisfying $BM = M$ is dense in R''.

Exercise 4.3.14 Let R be a simple Artinian ring. Show that any two irreducible R-modules are isomorphic.

(Hint: since R is Artinian, the set $\{I \subseteq R : I \text{ is a left ideal and } I \neq 0\}$ has a minimal element I_0. Show that I_0 is an irreducible R-module and that it is isomorphic to any other irreducible R-module M.)

4.4 Putting our blocks together – the Wedderburn-Artin theorem

Let us do a quick recap of what we have done so far in this chapter:

- We first looked at two classes of "nice" rings: primitive and semiprimitive. The former constitutes rings which admit a faithful irreducible representation and the latter constitutes rings which admit a faithful semisimple representation.
- We found a nice characterization of semiprimitive rings via the Jacobson radical: R is semiprimitive if and only if $\mathcal{J}(R) = 0$. We moreover found multiple ways of defining the Jacobson radical and showed that it has a kind of left-right symmetry; an interesting consequence being the intersection of maximal left ideals coincides with the intersection of maximal right ideals.
- Finally, we studied primitive rings in more detail via the important Jacobson density theorem for semisimple modules. Most notably, we determined the structure of primitive Artinian rings, and showed that these are simply isomorphic to $M_n(D)$ for some division ring D. Such rings will be the "building blocks" for the structure theory we study in this section.

We've seen that a primitive ring which is left Artinian is a simple (left) Artinian ring. Now we look at *semisimple* rings and see that these are exactly rings which are semiprimitive and left Artinian. In fact, more is true!

First, let's fix a ring R.

Definition 4.4.1 R is called **(left) semisimple** when R is semisimple as a left module over itself (that is, ${}_RR$ is semisimple). Explicitly this means $R = \bigoplus_\alpha I_\alpha$ for a collection of irreducible left ideals $\{I_\alpha\}$ of R.

We will call a left ideal I which is irreducible a **minimal left ideal**. This makes sense because $I \neq 0$ and I contains no proper non-zero left ideals.

Proposition 4.4.2 R is semisimple if and only if every R-module is semisimple.

Proof. The backwards direction is immediate, so suppose R is semisimple. Consider $R^{(M)} = \bigoplus_{x \in M} R$, the direct sum indexed by M, and let $f : R^{(M)} \to M$ be the map $f((a_x)_{x \in M}) = \sum_{x \in M} a_x x$ (this sum is finite because only finitely-many of the a_x's are non-zero). It is clear that this is a surjective homomorphism. Now R being semisimple means $R^{(M)}$ is as well. Thus, M is the homomorphic image of a semisimple R-module, so M is semisimple as well. □

Note that the left R-module ${}_RR$ is necessarily a faithful representation of R. For, if $\lambda : R \to \mathrm{End}({}_RR)$ is the map $\lambda(a) = \lambda_a$ where $\lambda_a(x) = ax$ for all $x \in R$, then $\lambda(a) = \lambda_a = 0$ implies $ax = 0$ for all $x \in R$; so $a = 0$ by taking $x = 1$.

Hence, if R is semisimple, it must be semiprimitive. When is a semiprimitive ring semisimple? Precisely when it's left Artinian!

Proposition 4.4.3 R is semisimple if and only if it is semiprimitive and left Artinian.

Moreover, if R is semisimple then R is left Noetherian and can be written as a *finite* direct sum of minimal left ideals.

Proof. If R is semisimple, write $R = \bigoplus_\alpha I_\alpha$ for minimal left ideals I_α. Hence, there are distinct $\alpha_1, ..., \alpha_k$ for which $1 = e_1 + \cdots + e_k$ for $e_i \in I_{\alpha_i}$. Since the I_{α_i}'s are left ideals, this shows $R = I_{\alpha_1} \oplus \cdots \oplus I_{\alpha_k}$. Now it's easy to see that:

$$0 \subsetneq I_{\alpha_1} \subsetneq I_{\alpha_1} \oplus I_{\alpha_2} \subsetneq \cdots \subsetneq I_{\alpha_1} \oplus \cdots \oplus I_{\alpha_k} = R$$

is a composition series for ${}_RR$. Hence, R is left Artinian, and in fact also left Noetherian.

Now suppose R is semiprimitive and left Artinian. We make the following observations:

- Every left ideal of R contains a *minimal* left ideal since R is left Artinian.
- Every minimal left ideal of R is complemented: given a minimal left ideal I, $I \neq 0 = \mathcal{J}(R)$, so there exists a *maximal* left ideal J which doesn't contain I. Now $I \cap J \subsetneq I$ so that $I \cap J = 0$, and $I + J \supsetneq J$ so that $I + J = R$. Thus, $R = I \oplus J$.

Assume R is *not* semisimple. Then R contains a minimal left ideal I_1. This is complemented, so $R = I_1 \oplus J_1$ for some left ideal J_1. Since R is not semisimple, we must have $J_1 \neq 0$, so J_1 contains a minimal left ideal I_2. This too is complemented, so $R = I_2 \oplus J_2'$ for a left ideal J_2'. Now $J_1 = I_2 \oplus (J_2' \cap J_1)$; letting $J_2 = J_2' \cap J_1$ gives $J_1 = I_2 \oplus J_2$. In particular, $J_1 \supsetneq J_2$ since $I_2 \neq 0$.

Continuing this way, we obtain a proper descending chain $J_1 \supsetneq J_2 \supsetneq \cdots$ of left ideals, contradicting that R is left Artinian. Hence, we must indeed have that M is semisimple. $\square$

This has given us a very nice characterization for a (left) semisimple ring R in terms of semiprimitivity and left Artinianity. Moreover, we have that R can be written as a direct sum of *finitely*-many minimal left ideals and that R is also Noetherian.

We now seek another characterization of semisimplicity for a ring: one that can be written as a product of finitely-many simple Artinian rings. This turns out to be quite a bit of work to prove. Towards this, we collect a few preliminary results.

Definition 4.4.4 Let I and J be left ideals and define:

$$IJ = \{xy \in R : x \in I, y \in J\}$$

It's clear that $IJ \subseteq J$ and that this is a left ideal. If I is a two-sided ideal, we also have $IJ \subseteq I$.

A similar definition and corresponding properties hold for right ideals. In particular, if both I and J are two-sided ideals, then IJ is two-sided as well.

Lemma 4.4.5 Let R be a semisimple ring and let $\{I_\alpha\}$ be a collection of minimal left ideals. Then the relation $\sim$ given by $I_\alpha \sim I_\beta \iff I_\alpha I_\beta \neq 0$ is an equivalence relation on $\{I_\alpha\}$.

Proof. If $I_\alpha^2 = 0$, then each element of I_α is nilpotent, thus quasiregular. From this it follows that I_α is a quasiregular left ideal, so $I_\alpha \subseteq \mathcal{J}(R) = 0$, which contradicts $I_\alpha \neq 0$. Thus, $I_\alpha^2 \neq 0$ so $I_\alpha \sim I_\alpha$.

Suppose then that $I_\alpha I_\beta \neq 0$. Notice that $I_\alpha I_\beta \subseteq I_\beta$, so by minimality we must have $I_\alpha I_\beta = I_\beta$. Thus, $I_\beta I_\alpha I_\beta = I_\beta^2 \neq 0$, which must mean $I_\beta I_\alpha \neq 0$ as well.

Finally, suppose $I_\alpha I_\beta, I_\beta I_\gamma \neq 0$. Then similarly $I_\alpha I_\beta = I_\beta$ and $I_\beta I_\gamma = I_\gamma$ so that $I_\gamma I_\alpha = I_\alpha I_\gamma = I_\alpha I_\beta I_\gamma = I_\beta I_\gamma \neq 0$. $\square$

Lemma 4.4.6 Let $R_1, ..., R_n$ be semisimple rings. Then their product $R = R_1 \times \cdots \times R_n$ is also semisimple.

Proof. Write $R_i = \bigoplus_{j=1}^{r_i} I_{i,j}$ for minimal left ideals $I_{i,j}$ of R_i. Let $e_i = (0, ..., 0, 1, 0, ..., 0) \in R$ with 1 is in the i^{th} position. Then we can identify R_i with the ideal $R_i e_i$ in R, and therefore identify $I_{i,j}$ with $I_{i,j} e_i$; this is also a minimal left ideal of R. Now:

$${}_R R = \bigoplus_{i=1}^{n} R_i e_i = \bigoplus_{i=1}^{n} \bigoplus_{j=1}^{r_i} I_{i,j} e_i$$

which makes R semisimple. $\square$

Theorem 4.4.7 (Wedderburn's theorem)
R is semisimple if and only if R is isomorphic to a finite product of simple Artinian rings.

Proof. The converse is easy. Write $R = R_1 \times \cdots \times R_k$ for simple Artinian rings R_i. Then the R_i are also semisimple, so the result follows from the preceding lemma.

Now suppose R is semisimple. Write ${}_RR = I_1 \oplus \cdots \oplus I_r$ where I_i are minimal left ideals. Then equip $\{I_1, ..., I_r\}$ with the equivalence relation $I_i \sim I_j \iff I_iI_j \neq 0$. Let $\{\mathcal{E}_1, ..., \mathcal{E}_k\}$ be the equivalence classes of this relation and let $R_i = \bigoplus_{I \in \mathcal{E}_i} I$. Then R_i is also a left ideal of R and moreover, $R_iI_j = 0$ if $I_j \notin \mathcal{E}_i$ and $R_iI_j = I_j \subseteq R_i$ if $I_j \in \mathcal{E}_i$. Hence, $R_iR \subseteq R_i$, which makes R_i a right ideal as well.

We have ${}_RR = R_1 \oplus \cdots \oplus R_k$. We shall show that each R_i is a simple Artinian ring and that $R \cong R_1 \times \cdots \times R_k$ as rings. For this, write $1 = e_1 + \cdots + e_k$ for $e_i \in R_i$. Notice that $R_iR_j = 0$ for $i \neq j$. Thus, given any $a \in R_i$, we have $ae_j = e_ja = 0$ for $i \neq j$ which means $a = a(e_1 + \cdots + e_k) = ae_i$ and similarly $e_ia = a$. Hence, e_i is the identity for R_i, which makes it a ring.

Consider the left R-module isomorphism $f : R_1 \times \cdots \times R_k \to {}_RR = R_1 \oplus \cdots \oplus R_k$ given by $f(a_1, ..., a_k) = a_1 + \cdots + a_k$. Since $R_iR_j = 0$ for $i \neq j$, it follows that

$$\begin{aligned} f(a_1b_1, ..., a_kb_k) &= a_1b_1 + \cdots + a_kb_k \\ &= (a_1 + \cdots + a_k)(b_1 + \cdots + b_k) \\ &= f(a_1, ..., a_k)f(b_1, ..., b_k) \end{aligned}$$

Moreover, $f(e_1, ..., e_k) = e_1 + \cdots + e_k = 1$. Hence, f is in fact an isomorphism of rings. Since R is semisimple and therefore left Artinian, it follows that each R_i is left Artinian as well (since R_i is the homomorphic image of the projection map $p_i : R = R_1 \oplus \cdots \oplus R_k \to R_i$).

What's left to show is R_i is simple. For this, we consider $R_i = \bigoplus_{I \in \mathcal{E}_i} I$, a direct sum of minimal left ideals, and let $J \neq 0$ be a (two-sided) ideal in R_i. Then $JI \subseteq I$ is a left ideal for all $I \in \mathcal{E}_i$, which by minimality means $JI = 0$ or $JI = I$. But if $JI = 0$ for some $I \in \mathcal{E}_i$, then the fact that $II' = I'$ for all $I' \in \mathcal{E}_i$ means $JI' = 0$ for all $I' \in \mathcal{E}_i$, which would give $J = JR_i = 0$. Thus, we must have $JI = I$ for all $I \in \mathcal{E}_i$, which gives $JR_i = R_i$. But $JR_i = J$ since J is an ideal, so $J = R_i$ and R_i is simple. $\square$

With the Wedderburn theorem, we have proved

Corollary 4.4.8 The following are equivalent:

(i) R is semisimple (in that ${}_RR$ is a semisimple R-module);

(ii) R is semiprimitive and left Artinian;

(iii) $R \cong R_1 \times \cdots \times R_k$ for simple Artinian rings $R_1, ..., R_k$.

Example 4.4.9 We show that $M_n(D)$ for D a division ring is semisimple. We know that $M_n(D)$ is in fact a simple ring and therefore (semi)primitive. Moreover, we've seen that $M_n(D)$ is left (and in fact right) Artinian. Hence, $M_n(D)$ is left (and right) semisimple. As a consequence, we get that any product of the form $M_{n_1}(D_1) \times \cdots \times M_{n_k}(D_i)$ for division rings D_i is (left and right) semisimple as well.

We also have that $M_n(D)$ is Noetherian, therefore has finite length. If $E_{i,j}$ denotes the standard basis matrix (1 in the $(i,j)^{\text{th}}$ entry and 0 elsewhere) and we let $I_j = \{c_1E_{1,j} + \cdots + c_nE_{n,j} : c_i \in D\}$, then it's easy to check that I_j is a minimal left ideal of $M_n(D)$ and $M_n(D) = I_1 \oplus \cdots \oplus I_n$. Now

$$0 \subsetneq I_1 \subsetneq I_1 \oplus I_2 \subsetneq \cdots \subsetneq I_1 \oplus \cdots \oplus I_n = M_n(D)$$

is a composition series for $M_n(D)$ as a left module over itself (this holds if the I_i's are *any* minimal left ideals). Hence, it follows that the length of $M_n(D)$ as an $M_n(D)$-module is n and the Krull-Schmidt theorem tells us that any such decomposition $M_n(D) = J_1 \oplus \cdots \oplus J_r$ into minimal left ideals must satisfy $r = n$.

As it turns out, the product of matrix rings over division rings described above is, up to isomorphism, the *complete* set of semisimple rings. We have the celebrated:

Theorem 4.4.10 (Wedderburn-Artin theorem)
Let R be a ring. Then R is semisimple if and only if there exist finitely-many integers $n_1, ..., n_k \geqslant 1$ and corresponding division rings $D_1, ..., D_k$ for which:

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

Moreover, the number k and the pairs $(n_1, D_1), ..., (n_k, D_k)$ are unique up to isomorphism and reordering. That is, if $R \cong \prod_{j=1}^{l} M_{n'_j}(D'_j)$ is another such product, then $k = l$ and there exists a permutation $\sigma \in S_k$ for which $M_{n_i}(D_i) \cong M_{n'_{\sigma(i)}}(D'_{\sigma(i)})$.

Proof. We've already seen that such a product of matrix rings is semisimple. Suppose now that R is semisimple. By Wedderburn's theorem we can write $R \cong R_1 \times \cdots \times R_k$ for simple Artinian rings $R_1, ..., R_k$. By **Proposition 4.3.8**, each $R_i \cong M_{n_i}(D_i)$ for $n_i \geqslant 1$ and a division ring D_i. The isomorphism thus follows.

Now for uniqueness. Suppose we also have $R \cong \prod_{j=1}^{l} M_{n'_j}(D'_j)$. Each piece $M_{n_i}(D_i)$ is (ring-)isomorphic to a minimal (two-sided) ideal R_i of R, and we have $R = R_1 \oplus \cdots \oplus R_k$. Similarly, each $M_{n'_j}(D'_j)$ is isomorphic to a minimal ideal R'_j and $R = R'_1 \oplus \cdots \oplus R'_l$.

Since the R_i's and R'_j's are minimal, they are indecomposable. By the Krull-Schmidt theorem (**3.3.9**), we must have $k = l$ and a bijection $\sigma \in S_k$ with ${}_RR_i \cong {}_RR'_{\sigma(i)}$ (isomorphic as left R-modules) for all i. We can say more than this, however.

Observe that if B is any minimal ideal of R, then:

$$B = BR = B(R_1 \oplus \cdots \oplus R_k) = BR_1 \oplus \cdots \oplus BR_k$$

since $BR_i \subseteq R_i$. Moreover, minimality of R_i gives us that $BR_i = 0$ or R_i. There must however be some i for which $BR_i \neq 0$, and thus $BR_i = R_i$. But $BR_i \subseteq B$ as well, and minimality of B gives $BR_i = B$ as $BR_i \neq 0$. Thus, $B = BR_i = R_i$.

A similar argument shows that there exists some j with $R_jB = B = R_j$. But then $B = BR_i = R_jB^2R_i \subseteq R_j \cap R_i = 0$ if $j \neq i$. Thus, we also have $B = BR_i = R_iB = R_i$ for this i, and it moreover must be the only such i.

Applying this argument to $B = R'_j$ for each j, we find that $R'_j = R_{\sigma(j)}$ for some $\sigma(j) \in \{1, ..., k\}$. But if $\sigma(j) = \sigma(j')$, then we would have $R'_j = R_{\sigma(j)} = R_{\sigma(j')} = R'_{j'}$, which must mean $j = j'$. σ thus determines an injection from $\{1, ..., k\}$ to itself, and therefore it must be a bijection. Hence, we have found a $\sigma \in S_k$ with $R_i = R_{\sigma(i)}$ for all i. Thus, $M_{n_i}(D_i) \cong R_i = R_{\sigma(i)} \cong M_{n'_{\sigma(i)}}(D'_{\sigma(i)})$. □

Remark 4.4.11

- In the proof, we showed that if $R = R_1 \oplus \cdots \oplus R_k = R'_1 \oplus \cdots \oplus R'_l$ where the R_i, R'_j are minimal ideals (and rings), then $k = l$ and there must be a bijection $\sigma \in S_k$ satisfying $R_i = R'_{\sigma(i)}$ for all i. There is hence a unique way of breaking down a semisimple ring into minimal ideals. We call the R_i's the **simple components** of R.
- We considered *left* semisimplicity throughout. However, each we've seen that $\prod_{i=1}^k M_{n_i}(D_i)$ is *right* semisimple as well. Hence, it follows from the Wedderburn-Artin theorem that R is left semisimple if and only if it's right semisimple. It therefore makes sense to say a ring is *semisimple* (without needing to specify if it's left or right). This moreover shows that a semisimple ring must also be right Artinian and right Noetherian.

We've shown earlier that any module over a semisimple ring is also semisimple. The Wedderburn-Artin theorem tells us more about this:

Corollary 4.4.12 Let R be semisimple. Then there is a bijective correspondence between the isomorphism classes of irreducible R-modules and the simple components of R. Namely, if $R = R_1 \oplus \cdots \oplus R_k$ is the decomposition into simple components and I_j is a minimal left ideal in R_j, then $\{I_1, ..., I_k\}$ is a set of representatives of the isomorphism classes of irreducible R-modules.

Proof. Write $R_i = \bigoplus_{j=1}^{r_i} I_{i,j}$ for minimal left ideals $I_{i,j}$ of R_i. We've seen that $R_kI_{i,j} = 0$ whenever $k \neq i$, so $I_{i,j}$ is a minimal left ideal of R as well.

If M is an irreducible R-module, then for any $0 \neq x \in M$ we have $Rx = M$ and hence $I_{i,j}x \neq 0$ for some i and j. Since $I_{i,j}x$ is a submodule of M, we must have $I_{i,j}x = M$. Also since $I_{i,j}$ is irreducible as an R-module, Schur's lemma tells us that $M = I_{i,j}x \cong I_{i,j}$. Thus, every irreducible R-module is isomorphic to some $I_{i,j}$.

What's left is to show that if I and J are any minimal left ideals in R_i and R_j, respectively, then $I \cong J$ (as R-modules) if and only if $i = j$. First, if $i = j$ then I and J are in $R_i = R_j$. As such, I and J are irreducible R_i-modules, so **Exercise 4.3.14** gives $I \cong J$ (as R_i-modules, hence as R-modules). On the other hand, suppose $i \neq j$. Then $R_iI = I$ but $R_iJ = 0$. Thus, if $f : I \to J$ is any R-homomorphism, then $f(ax) = af(x) = 0$ for any $a \in R_i$ and $x \in J$, so $f = 0$ and f can't be an isomorphism. □

Let's see a small illustration of the Wedderburn-Artin theorem.

Example 4.4.13 Let $n = p_1 \cdots p_k$ for distinct primes p_i. We have seen that $\mathbb{Z}/(n)$ is semisiple and for $q_i = \frac{n}{p_i}$, we have the decomposition $\mathbb{Z}/(n) = (q_1) \oplus \cdots \oplus (q_k)$ into minimal ideals. What can we say about the ring (q_i)? Write $1 = e_1 + \cdots + e_k$ where $e_i \in (q_i)$. We've seen that e_i is the identity element of (q_i).

Define a map $f_i : \mathbb{Z} \to (q_i)$ by $f_i(k) = ke_i$. Then f_i is a ring homomorphism. Notice that since $e_i \in (q_i)$, we have $(p_i) \subseteq \ker f_i$. Conversely if $k \in \ker f_i$ then $ke_i = 0$ in $\mathbb{Z}/(n)$, which means $p_i \mid ke_i$. But $p_i \nmid e_i$ since e_i is non-zero in (q_i). Hence, $p_i \mid k$ so that $k \in (p_i)$. Hence, $\ker f_i = (p_i)$. It's clear that f_i is surjective. Therefore, we have $\mathbb{Z}/(p_i) \cong (q_i)$. As such, $\mathbb{Z}/(n) \cong \mathbb{Z}/(p_1) \times \cdots \times \mathbb{Z}/(p_k)$. Notice that each $\mathbb{Z}/(p_i)$ is a field, so $\mathbb{Z}/(p_i) \cong M_1(\mathbb{Z}/(p_i))$.

The next section of this chapter will be the last section, and will be concerned with looking at what it means for $M_n(D)$ to be ring-isomorphic to $M_{n'}(D')$ for given $n, n' \geqslant 1$ and division rings D and D'.

Exercises

Fix a ring R.

Definition 4.4.14 Let I be a left (or right) ideal of R. I is called **nil** when every element of I is nilpotent.

I is called **nilpotent** when there exists an $n \in \mathbb{N}$ for which $I^n = 0$. In other words, we have $x_1 \cdots x_n = 0$ whenever $x_1, ..., x_n \in I$.

It's clear that every nilpotent ideal is a nil ideal. The converse isn't generally true though.

Exercise 4.4.15 Let R be left Artinian.

(a) Show that $\mathcal{J}(R)$ is nilpotent and contains every nil left/right ideal.

(b) Conclude from this that every nil ideal is nilpotent.

(c) Conclude from this that every quasiregular left/right ideal is also nilpotent.

(Hint: consider the descending chain $\mathcal{J}(R) \supseteq \mathcal{J}(R)^2 \supseteq \cdots$. This must stabilize – say $\mathcal{J}(R)^n = \mathcal{J}(R)^{n+1} = \cdots$ for some $n \geqslant 1$. Let $N = \mathcal{J}(R)^n$ and suppose $N \neq 0$. Show that the set of all left ideals J satisfying $J \subseteq N$ and $NJ \neq 0$ is non-empty and thus has a minimal element J_0. Use this to arrive at a contradiction.)

Exercise 4.4.16 Suppose M is a semisimple module which is finitely generated. Show that there exist finitely-many irreducible submodules $M_1, ..., M_n$ of M for which $M = M_1 \oplus \cdots \oplus M_n$.

We've seen that any (Artinian) semisimple ring is Noetherian as well. It turns out that *any* ring which is left (right) Artinian must be left (right) Noetherian as well. This is a consequence of the *Hopkins-Levitzki thereom.*

Definition 4.4.17 R is called **semiprimary** when $\mathcal{J}(R)$ is nilpotent and $R/\mathcal{J}(R)$ is semisimple.

Notice that if R is left Artinian, then $\mathcal{J}(R)$ is nilpotent (as shown in the preceding exercise) and $R/\mathcal{J}(R)$ is semiprimitive and left Artinian, therefore semisimple. Hence, every left Artinian ring is semiprimary.

Exercise 4.4.18 (Hopkins-Levitzki theorem)
Suppose R is semiprimary and let M be an R-module. Prove that the following are equivalent:

(i) M is Noetherian

(ii) M is Artinian

(iii) M has finite length.

Hence conclude that every left Artinian ring is left Noetherian.

(Hint: it is clear that **(iii)** implies **(i)** and **(ii)** by what we've studied in chapter 3. So for the other directions, let $n \geqslant 1$ be the least integer satisfying $\mathcal{J}(R)^n = 0$ (which exists since $\mathcal{J}(R)$ is nilpotent) and consider the series $0 \subseteq \mathcal{J}(R)^{n-1}M \subseteq \cdots \subseteq \mathcal{J}(R)^2M \subseteq \mathcal{J}(R)M \subseteq M$. Let $F_k = \mathcal{J}(R)^k M/\mathcal{J}(R)^{k+1}M$ for $0 \leqslant k < n$. Show that we can view each F_k as an $R/\mathcal{J}(R)$-module and that if M is Noetherian or Artinian, each F_k has a composition series as an $R/\mathcal{J}(R)$-module – **Exercise 3.4.19** may help here. What can you conclude from this?)

A similar argument holds to show that right Artinian rings must be right Noetherian, thus Artinian rings must be Noetherian.

4.5 The simple components – isomorphisms of simple Artinian rings

We've shown that if R is semisimple then $R = R_1 \oplus \cdots \oplus R_k$ for *unique* minimal ideals $R_1, ..., R_k$ which are also themselves simple rings. The $R_1, ..., R_k$ are called the *simple components* of R. Here we take a closer look at these components.

Wedderburn's theorem tells us that each R_i is isomorphic to the ring $M_{n_i}(D_i)$ for a given $n_i \geqslant 1$ and a division ring D_i. Equivalently R_i is isomorphic to $\mathrm{End}_{D_i}(V_i)$ for a finite-dimensional vector space V_i over a division ring D_i. Thus, we ask the following question: if V_1 and V_2 are finite-dimensional vector spaces over the division rings D_1 and D_2, respectively, and they satisfy $\mathrm{End}_{D_1}(V_1) \cong \mathrm{End}_{D_2}(V_2)$, what can we say about the relation between D_1 and D_2 and between V_1 and V_2?

It doesn't necessarily make sense to say that V_1 and V_2 are isomorphic vector spaces since D_1 and D_2 aren't necessarily the same. But there is a simple way to get around this obstacle.

Definition 4.5.1 Let $\sigma : D_1 \to D_2$ be an isomorphism. A **σ-semilinear map** from V_1 to V_2 is a map $T : V_1 \to V_2$ such that for all $v, w \in V_1$ and $a \in D_1$:

(i) $T(v + w) = Tv + Tw$;

(ii) $T(av) = \sigma(a)Tv$.

If T is bijective, we call T a **σ-semilinear isomorphism**. In this case, it's easy to check that T^{-1} is a σ^{-1}-semilinear isomorphism.

We'll say that the spaces V_1 and V_2 are **semilinearly isomorphic** when there exists an isomorphism $\sigma : D_1 \to D_2$ and a σ-linear isomorphism from V_1 to V_2.

Lemma 4.5.2 Let V_1 and V_2 be vector spaces (not necessarily finite dimensional) over D_1 and D_2, respectively. Then V_1 and V_2 are semilinearly isomorphic if and only if $D_1 \cong D_2$ and $\dim V_1 = \dim V_2$.

Proof. Suppose $\Phi : V_1 \to V_2$ is a σ-semilinear isomorphism. Then immediately we have $D_1 \cong D_2$. Let $\{e_\alpha\}$ be a basis for V_1 and consider the set $\{\Phi e_\alpha\}$ in V_2. We see that for any $\alpha_1, ..., \alpha_n$ and $b_1, ..., b_n \in D_2$

$$\begin{aligned} b_1\Phi e_{\alpha_1} + \cdots + b_n\Phi e_{\alpha_n} = \Phi(\sigma^{-1}(b_1)e_{\alpha_1} + \cdots + \sigma^{-1}(b_n)e_{\alpha_n}) = 0 \\ \implies \sigma^{-1}(b_1)e_{\alpha_1} + \cdots + \sigma^{-1}(b_n)e_{\alpha_n} = 0 \\ \implies \text{each } \sigma^{-1}(b_i) = 0 \\ \implies \text{each } b_i = 0 \end{aligned}$$

which means $\{\Phi e_\alpha\}$ is independent. Moreover, given any $w \in V_2$, we can write $w = \Phi v$ for some $v \in V_1$. If $v = a_1 e_{\alpha_1} + \cdots + a_n e_{\alpha_n}$, then $w = \sigma(a_1)\Phi e_{\alpha_1} + \cdots + \sigma(a_n)\Phi e_{\alpha_n}$. Hence, $\{\Phi e_\alpha\}$ is a basis for V_2, which shows $\dim V_1 = \dim V_2$.

Conversely, suppose $D_1 \cong D_2$ and $\dim V_1 = \dim V_2$. Let $\sigma : D_1 \to D_2$ be an isomorphism and choose bases $\{e_\alpha\}$ and $\{f_\alpha\}$ for V_1 and V_2, respectively, which are in bijection since they have the same dimension. We may assume our bijection is simply $e_\alpha \mapsto f_\alpha$. Define $\Phi : V_1 \to V_2$ by mapping $v = a_1 e_{\alpha_1} + \cdots + a_n e_{\alpha_n} \in V_1$ to $\Phi v = \sigma(a_1) f_{\alpha_1} + \cdots + \sigma(a_n) f_{\alpha_n} \in V_2$. It's easy to check that this is a well-defined σ-semilinear isomorphism. □

We have therefore established a condition for when two vector spaces are semilinearly isomorphic. Next we look at the endomorphism rings. Let V be a vector space over a division ring D and recall that the commutant and bicommutant of D in V are:

$$D' = \mathrm{End}_D(V)$$

$$D'' = \mathrm{End}_{D'}(V) = \{\varphi \in \mathrm{End}(V) : \varphi(Tv) = T\varphi(v)\ \forall T \in \mathrm{End}_D(V)\}$$

respectively. We also have the natural map $\lambda : D \to D''$ given by $\lambda(a) = \lambda_a$ where $\lambda_a(v) = av$ for all $v \in V$. We studied these in the more general context of semisimple modules over a ring in a previous section, but now we have:

Lemma 4.5.3 The natural map $\lambda : D \to D''$ is an isomorphism.

Proof. Since V is a semisimple D-module, the Jacobson density theorem tells us that $\mathrm{im}\,\lambda$ is dense in D''. Thus, if $\varphi \in D''$ and $0 \neq v \in V$, there exists $a \in D$ with $av = \varphi(v)$, hence $\varphi(v) \in \mathrm{span}(v)$. Similarly if $0 \neq w \in V$ is another vector, there is some $b \in D$ such that $bw = \varphi(w)$.

Now since $v \neq 0$, there is some $T \in \mathrm{End}_D(V)$ with $Tv = w$. Thus, $bw = \varphi(w) = \varphi(Tv) = T\varphi(v) = T(av) = aTv = aw$, which means $a = b$ since $w \neq 0$. We have thus shown that there is some $a \in D$ with $\varphi(v) = av$ for all $v \in V$, and so $\varphi = \lambda_a$, making λ surjective.

The injectivity is obvious: $\ker\lambda$ is an ideal in D, but D being a division ring forces $\ker\lambda = 0$. $\square$

With this at hand, we can finally state and prove the

Theorem 4.5.4 (isomorphism theorem for simple Artinian rings) Let V_1 and V_2 be finite-dimensional vector spaces over division rings D_1 and D_2, respectively. Suppose $\varphi : \mathrm{End}_{D_1}(V_1) \to \mathrm{End}_{D_2}(V_2)$ is an isomorphism. Then there exists a semilinear isomorphism $\Phi : V_1 \to V_2$ satisfying $\varphi(T) = \Phi T\Phi^{-1}$ for all $T \in \mathrm{End}_{D_1}(V_1)$.

Proof. We may assume V_1 and V_2 are non-zero. Let $R_1 = \mathrm{End}_{D_1}(V_1)$. Since V_1 is finite-dimensional, R_1 is simple Artinian. We look at V_1 as an R_1-module via the usual action and we can view V_2 as an R_1-module via $Tw := \varphi(T)w$ for all $T \in R_1$ and $w \in V_2$. V_1 and V_2 are irreducible as R_1-modules. Thus, since R_1 is simple Artininan, there is an R_1-module isomorphism $\Phi : V_1 \to V_2$. This means $\Phi(Tv) = T\Phi v = \varphi(T)\Phi v$ for all $T \in R_1 = \mathrm{End}_{D_1}(V_1)$ and $v \in V_1$. As such, we have $\Phi T = \varphi(T)\Phi$ for all $T \in R_1$, which means $\varphi(T) = \Phi T\Phi^{-1}$. What's left to show is Φ is a σ-semilinear isomorphism for some isomorphism $\sigma : D_1 \to D_2$.

Let $R_2 = \mathrm{End}_{D_2}(V_2)$. We have the map $\overline{\varphi} : \mathrm{End}(V_1) \to \mathrm{End}(V_2)$ given by $\overline{\varphi}(T) = \Phi T\Phi^{-1}$. Since Φ is a group isomorphism, $\overline{\varphi}$ is an isomorphism and clearly $\overline{\varphi}|_{\mathrm{End}_{D_1}(V_1)} = \varphi$. Then for $D_1'' = R_1' = \mathrm{End}_{R_1}(V_1)$ and $D_2'' = R_2' = \mathrm{End}_{R_2}(V_2)$, we have $\psi = \overline{\varphi}|_{R_1'} : R_1' \to R_2'$ is an isomorphism. By **Lemma 4.5.3**, we have $D_1 \cong R_1'$ and $D_2 \cong R_2'$, from which it follows that there exists an isomorphism $\sigma : D_1 \to D_2$ given by $\sigma = (\lambda^{(2)})^{-1}\psi\lambda^{(1)}$, where $\lambda^{(i)} : D_i \to D_i'' = R_i'$ are the natural maps. Therefore, we obtain $\Phi\lambda_a\Phi^{-1} = \lambda_{\sigma(a)}$ for all $a \in D_1$.

Finally, we see that for any $v \in V_1$ and $a \in D_1$, letting $w = \Phi v$ gives:

$$\Phi(av) = \Phi(\lambda_a v) = \Phi(\lambda_a(\Phi^{-1}w)) = (\Phi\lambda_a\Phi^{-1})w = \sigma(a)w = \sigma(a)\Phi v$$

which completes the proof. $\square$

In terms of the matrix rings, this (along with **Lemma 4.5.2**) tells us:

Corollary 4.5.5 $M_{n_1}(D_1) \cong M_{n_2}(D_2)$ if and only if $D_1 \cong D_2$ and $n_1 = n_2$.

As a consequence, if R is any simple Artinian ring with $R \cong M_n(D)$ for $n \geqslant 1$ and D a division ring, this n is *unique*. We've seen that $M_n(D)$ can be written as the direct sum of n minimal left ideals, so we have $R = I_1 \oplus \cdots \oplus I_n$ for minimal left ideals I_i of R. Also since $I_i \cong I_j$, we can set $I = I_1$ to give us ${}_RR \cong I^{(n)}$.

Now consider the situation where R is semisimple and M is a *finitely-generated* R-module. Write $R = R_1 \oplus \cdots \oplus R_k$ for simple components $R_i \cong M_{n_i}(D_i)$. Choose minimal left ideals $I_1, ..., I_k$ where I_i is in R_i. Then since M is semisimple, **Exercise 4.4.16** tells us we can write M as a direct sum of *finitely-many* irreducible submodules. Each irreducible submodule is isomorphic to exactly one I_i. Thus, we can write M as $M = M_{1,1} \oplus \cdots \oplus M_{1,r_1} \oplus \cdots \oplus M_{k,1} \oplus \cdots \oplus M_{k,r_k}$ where $r_i \geqslant 0$ and each $M_{i,j} \cong R_i$ (the case $r_i = 0$ means $M_{i,j}$ doesn't show up in the sum). With this we have:

Definition 4.5.6 Given any irreducible R-module N, we have $N \cong I_i$ for a unique i. We call r_i the **multiplicity** of N in M. This is the "number of copies" of N contained in M.

Exercises

None this time.

4.6 Finally some applications – representations of groups

We haven't seen many examples of Wedderburn-Artin decompositions. In **Example 4.4.13**, we saw that if $n = p_1 \cdots p_k$ for p_i distinct primes, then $\mathbb{Z}/(n) \cong \mathbb{Z}/(p_1) \times \cdots \times \mathbb{Z}/(p_k)$. This is simply a product of fields, however. Are there any examples where more interesting decompositions arise?

It turns out a wide range of examples come from groups. Before getting to concrete examples though, we will spend some time establishing what we need to study such examples. Let us fix a group G and a field F.

Definition 4.6.1 The **group algebra** of G over F is the ring $F[G]$ obtained as follows:

- the elements of $F[G]$ are formal (finite) linear combinations of the elements of G: $\sum_{g\in G} a_g g$ where all by finitely-many $a_g \in F$ are non-zero;
- the addition and scalar multiplication are the obvious ones:
$$c\sum_{g\in G} a_g g + \sum_{g\in G} b_g g = \sum_{g\in G} (ca_g + b_g)g$$
- the multiplication is the one induced by the group product and extending to all of $F[G]$ by bilinearity:
$$\left(\sum_{g\in G} a_g g\right)\left(\sum_{g\in G} b_g g\right) = \sum_{g,h\in G} a_g b_h (gh)$$

It's easy to check that $F[G]$ is indeed a ring; the zero element is 0 and the identity is $1 \cdot 1_G = 1_G$ (the identity of G). Moreover, $F[G]$ is a vector space over F under the obvious action.

For brevity, we shall write $\sum_{g\in G} a_g g$ as just $\sum_g a_g g$.

Now recall:

Definition 4.6.2 A **representation** of G over F is a pair (V, ρ) where V is a vector space over F and $\rho : G \to \mathrm{GL}(V)$ is a group homomorphism. The dimension of V is called the **degree** of the representation.

Notice that for any representation (V, ρ), we have the extension $\widetilde{\rho} : F[G] \to \mathrm{End}_F(V)$ given by $\widetilde{\rho}(\sum_g a_g g) = \sum_g a_g \rho(g)$. It's clear that this is a linear ring homomorphism. We thus obtain a representation $(V, \widetilde{\rho})$ of the ring $F[G]$. Thus, V has the structure of an $F[G]$-module.

Conversely, given any $F[G]$-module V, V has the structure of a vector space over F given by $cv = (ce)v$ for all $v \in V$ and $c \in F$, where $e \in G$ is the identity. The corresponding map $\widetilde{\rho} : F[G] \to \mathrm{End}(V)$ is therefore linear, so in fact $\widetilde{\rho} : F[G] \to \mathrm{End}_F(V)$. Now $\widetilde{\rho}(e) = I$, the identity map, so for any $g \in G$ we have

$$\widetilde{\rho}(g)\widetilde{\rho}(g^{-1}) = \widetilde{\rho}(gg^{-1}) = \widetilde{\rho}(e) = I$$

and similarly $\widetilde{\rho}(g^{-1})\widetilde{\rho}(g) = I$. As such, $\widetilde{\rho}(g)$ is invertible and therefore $\widetilde{\rho}$ restricts to $\rho = \widetilde{\rho}|_G : G \to \mathrm{GL}(V)$. Now (V, ρ) is a representation of the group G.

We have therefore established a bijective correspondence between group representations of G over F and $F[G]$-modules. Thus, we will use the terms "representation of G" and "$F[G]$-module" synonymously. This allows us to speak of *irreducible* representations, *faithful* representations, *semisimple* representations, etc.

Recall that the *characteristic* of a ring R is defined to be:

- the least $n \geqslant 1$ for which $n \cdot 1 = 0$ in R,
- 0 if such an n doesn't exist.

This was seen in **Definition 1.4.4**. We denote this as $\mathrm{char}(R)$. We also recall that any field F has $\mathrm{char}(F) = 0$ or $\mathrm{char}(F) = p$ for a prime p. Related to this, we have:

Theorem 4.6.3 (Maschke's theorem)
Suppose G is finite with order $n = |G|$ (the number of elements of G). If $\mathrm{char}(F)$ doesn't divide n, then the group algebra $F[G]$ is semisimple.

As a consequence, every representation of G over F is semisimple and can be written as a finite direct sum of irreducible representations.

Proof. We will show directly that every representation of G over F is semisimple (this will also apply to $F[G]$ as a module over itself). Let V be a representation of G over F (that is, an $F[G]$-module) and let $\rho : F[G] \to \mathrm{End}_F(V)$ be the corresponding homomorphism (which, we recall, restricts to $\rho|_G : G \to \mathrm{GL}(V)$). We will show that every subrepresentation ($F[G]$-submodule) is complemented.

Indeed, let U be a subrepresentation of V. Then in particular U is a vector subspace of V, which means there exists a subspace W_0 of V for which $V = U \oplus W_0$. W_0 may not be a subrepresentation though.

Consider the linear projection map $P : V \to U$ onto U. With this, define another map $f : V \to V$ by:

$$f = \frac{1}{n} \sum_{g \in G} \rho(g^{-1}) P \rho(g)$$

Note that $\frac{1}{n} \in F$ is defined since $\mathrm{char}(F)$ doesn't divide n. It's clear that f is a linear map. We will also show that f is an $F[G]$-module homomorphism. For this,

we need only show that $f\rho(h) = \rho(h)f$ for all $h \in G$ (the rest will follow by linearity of f). Indeed, we do an "add-and-subtract" trick to obtain:

$$\begin{aligned} f\rho(h) &= \frac{1}{n}\sum_{g\in G}\rho(g^{-1})P\rho(g)\rho(h) \\ &= \frac{1}{n}\sum_{g\in G}\rho(g^{-1})P\rho(gh) \\ &= \frac{1}{n}\rho(h)\sum_{g\in G}\rho(h^{-1}g^{-1})P\rho(gh) \\ &= \frac{1}{n}\rho(h)\sum_{g\in G}\rho((gh)^{-1})P\rho(gh) \end{aligned}$$

Now applying a substitution trick by letting $k = gh$, we see that above is equal to

$$\begin{aligned} &= \frac{1}{n}\rho(h)\sum_{k\in G}\rho(k^{-1})P\rho(k) \\ &= \rho(h)f \end{aligned}$$

Thus, f is indeed an $F[G]$-homomorphism.

Since U is a subrepresentation, we have for all $u \in U$ that $\rho(g)u \in U$ for all $g \in G$ and thus $P\rho(g)u = \rho(g)u$. From this we get:

$$\begin{aligned} f(u) &= \frac{1}{n}\sum_{g\in G}\rho(g^{-1})P\rho(g)u \\ &= \frac{1}{n}\sum_{g\in G}\rho(g^{-1})\rho(g)(u) \\ &= \frac{1}{n}\sum_{g\in G}u \\ &= u \end{aligned}$$

Also for any $v \in V$, we have $f(v) \in U$ from the fact that $\operatorname{im} P = U$ and U is a subrepresentation. From this we get that f is another projection onto U. Letting $W = \operatorname{im}(\mathrm{id}_V - f)$ then gives us $V = U \oplus W$, and W is a subrepresentation of V since $\mathrm{id}_V - f$ is an $F[G]$-homomorphism. Hence, U is complemented, so V is semisimple.

That V is a *finite* direct sum follows from the Wedderburn-Artin considerations. Namely, we have the decomposition $F[G] = R_1 \oplus \cdots \oplus R_k$ into simple components $R_i \cong M_{n_i}(D_i)$, and **Corollary 4.4.12** tells us that if we take a minimal left ideal I_i in R_i, then $\{I_1, ..., I_k\}$ is a set of representatives for the equivalence classes of irreducible representations of G. □

This result applies in particular to fields of characteristic 0. Thus, if we look at representations of a finite group G over $\mathbb{C}$ for instance, these must be semisimple.

We shall restrict ourselves now to representations over $\mathbb{C}$ which are of finite degree. That is, given a finite group G, we consider a representation V of G ($\mathbb{C}[G]$-module) where V is finite-dimensional as a $\mathbb{C}$-vector space. Then V is finitely-generated as a $\mathbb{C}[G]$-module, which means V decomposes as $V = \bigoplus_{i=1}^{k} \bigoplus_{j=1}^{r_i} V_{i,j}$ where $V_{i,j}$ are irreducible and $V_{i,j} \cong V_{i',j'}$ if and only if $i = i'$.