Chapter 1

Modules

Every ring can be viewed as a ring of operators if we slightly weaken the requirement that it act as linear operators on a vector space. Any ring can be viewed as operators on an abelian group in many ways; the abelian group on which the ring acts is called a module over that ring.

1.1 Definitions and examples

If $(M, +)$ is an abelian group then the set of all group homomorphisms $M \to M$ can be made into a ring by defining

$$(\psi + \theta)(v) := \psi(v) + \theta(v),$$

and

$$\psi\theta = \psi \circ \theta.$$

We denote this ring by $\mathrm{End}_{\mathbb{Z}} M$. Elements in this ring act on M; they are operators $M \to M$. $\mathrm{End}_{\mathbb{Z}} M$ is analogous to $\mathrm{End}_k V$, the ring of linear operators on a vector space.

Now, if $\rho : R \to \mathrm{End}_{\mathbb{Z}} M$ is a ring homomorphism we can think of the elements of R as acting on M through ρ. That is, we can define

$$r.m = \rho(r)(m)$$

for $r \in R$ and $m \in M$. The rule $(r, m) \mapsto r.m$ is a function $R \times M \to M$. Because ρ is a ring homomorphism the following properties hold:

1. $r.(s.m) = (rs).m$;
2. $1.m = m$;
3. $(r \pm s).m = r.m \pm s.m$;
4. $r.(m \pm n) = r.m \pm r.n$
5. $0.m = 0$;

6. $r.0 = 0$;

Compare these properties to the defining properties of vector space over a field k which are expressed in terms of a map $k \times V \to V$.

A left module over a ring R is an abelian group $(M, +)$ together with an action of R on M satisfying conditions (1)–(6) above.

Example 1.1

If k is a field then a k-module is the same thing as a k-vector space.

Of course, there are right modules too.

Every ring R can be considered as both a left and as a right module over itself: the left action of $r \in R$ on $x \in R$ is given by $r.x = rx$, the product obtained by using the multiplication in R. To distinguish these two modules we sometimes denote them by ${}_RR$ and R_R.

Definition 1.2 Let M and N be left R-modules. An R-module homomorphism $f : M \to N$ is a group homomorphism such that

$$f(r.m) = r.f(m)$$

for all $r \in R$ and $m \in M$. The set of all R-module homomorphisms from M to N is denoted by $\mathrm{Hom}_R(M, N)$.

If f is bijective, then its inverse f^{-1} is also an R-module homomorphism. In this case we say that f is an isomorphism and that M and N are isomorphic R-modules; we denote this by $M \cong N$.

A homomorphism $f : M \to M$ is called an endomorphism of M. If f is also an isomorphism from M to itself it is called an automorphism of M. $\Diamond$

Exercises. 1. If f_1 and f_2 are R-module homomorphisms $M \to N$, so is $f_1 + f_2$ defined by $(f_1 + f_2)(m) := f_1(m) + f_2(m)$. In this way, $\mathrm{Hom}_R(M, N)$ becomes an abelian group with identity element the zero map defined by $0(m) = 0$ for all $m \in M$.

2. If $f : M \to N$ and $g : L \to M$ are R-module homomorphisms, so is $fg : L \to N$. Composition gives a homomorphism of abelian groups

$$\mathrm{Hom}_R(M, N) \times \mathrm{Hom}_R(L, M) \to \mathrm{Hom}_R(L, N).$$

3. Let M be a left R-module. Show that the action of $r \in R$ on M is a homomorphism of abelian groups $\rho_r : M \to M$. Hence show that the map $\rho : R \to \mathrm{End}_{\mathbb{Z}} M$ that sends r to ρ_r is a ring homomorphism. Conversely, show that if M is an abelian group and $\rho : R \to \mathrm{End}_{\mathbb{Z}} M$ is a ring homomorphism, then M becomes a left R-module if we define

$$r.m := \rho(r)(m).$$

Example 1.3 If M is a left R-module. The set of all endomorphisms of M is denoted by $\mathrm{End}_R M$. It is a ring with multiplication given by composition of maps, and addition given by pointwise addition, i.e., the product $\theta\psi$ is the map $m \mapsto \theta(\psi(m))$. $\Diamond$

Exercise. If R is commutative and M is an R-module, show that the map $\Phi : R \to \mathrm{End}_R M$ defined by $\Phi(r)(m) = rm$ for $r \in R$ and $m \in M$ is a ring homomorphism. Further, show that the image of Φ is contained in the center of $\mathrm{End}_R M$.

What happens if R is not commutative?

1.2 Submodules and quotient modules.

Definition 2.1 A subgroup N of a left R-module M is a submodule if it is closed under the action of R, i.e., if $rm \in N$ for all $m \in N$ and $r \in R$. Of course, M and 0 are submodules of M. ◊

The submodules of R, viewed as a left R-module, are its left ideals.

Definition 2.2 Let N be a submodule of M. The quotient module M/N is defined as follows: as an abelian group M/N is the quotient group M/N and the action of $r \in R$ on $[m + N] \in M/N$ is defined by

$$r.[m + N] = [rm + N].$$

◊

The construction and verification of the module axioms is analogous to the construction and verification of the quotient vector space axioms.

The natural map $\pi : M \to M/N$, $m \mapsto [m + N]$ is a homomorphism of left R-modules. Its kernel is N.

There is a bijection between the submodules of M/N and the submodules of M that contain N; if $N \subset N' \subset M$ is a submodule of M, then N'/N is a submodule of M/N, and also

$$M/N' \cong \frac{M/N}{N'/N}.$$

Proposition 2.3 *Let $f : M \to N$ be a homomorphism of R-modules.*

1. $\ker f$ *is a submodule of* M *and* $\mathrm{im}\, f$ *is a submodule of* N.

2. $\mathrm{im}\, f \cong M/\ker f$.

Proof. (1) The reader should check this.

(2) Write $K = \ker f$. Define $g : M/\ker f \to \mathrm{im}\, f$ by $g([m + K]) = f(m)$. This is well-defined because if $[m_1 + K] = [m_2 + K]$, then $m_1 - m_2 \in K$, so $f(m_1 - m_2) = 0$, whence $f(m_1) = f(m_2)$. It is easy to check that g is an R-module homomorphism because f is. It is obviously surjective. And it is injective because if $g([m + K]) = 0$, then $f(m) = 0$, whence $m \in K$ and $[m + K] = 0$. Hence g is an isomorphism. □

Exercises. In the following exercises M denotes a left R-module.

1. Show there is a bijection between the submodules of M that contain N and the submodules of M/N, the bijection being $K \longleftrightarrow K/N$.

2. Show that an intersection and sum of submodules is again a submodule. The sum of two submodules L and N is defined to be

$$L + N := \{\ell + n \mid \ell \in L,\ n \in N\}.$$

3. Some people make the mistake of thinking that if M_1 and M_2 are isomorphic modules having isomorphic submodules N_1 and N_2, then the quotients M_1/N_1 and M_2/N_2 are isomorphic. Give an example to show this is not always true.

If M is a left R-module and $m \in M$, then the set of all multiples of m, $Rm := \{rm \mid r \in R\}$, is a submodule of M. It is the analogue of a principal ideal in a commutative ring. We call Rm the submodule of M generated by m.

Definition 2.4 If $M = Rm$ for some $m \in M$, we say that M is cyclic. ◊

For example, ${}_RR$ is a cyclic module because $R = R.1$. If I is any left ideal, then R/I is cyclic because $r.[1 + I] = [r + I]$ for every $r \in R$. The next result shows that, up to isomorphism, these are all the cyclic modules.

Lemma 2.5 *If M is cyclic, then $M \cong R/I$ for some left ideal I of R.*

Proof. If $M = Rm$, define $\psi : R \to M$ by $\psi(r) = rm$. Then ψ is a surjective homomorphism of left R-modules. Its kernel is a left submodule of R, hence a left ideal, so the result follows from Proposition 2.3. □

Notice that the cyclic groups are precisely the cyclic $\mathbb{Z}$-modules.

Example 2.6 Let V be the k-vector space with basis $e_1, \ldots, e_n$ and make V a $k[x]$-module by making x act as the matrix

$$\begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & & & & & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}$$

Then $x.e_j = e_{j+1}$ for $1 \leq j \leq n-1$ and $x.v_n = e_1$, so $V = Re_j$ for every j; in particular, V is a cyclic R-module. ◊

Exercises. 1. Show that the module V in the previous example is generated by $e_1 + \ldots + e_n$. How does the submodule structure of V depend on the field k?

2. The space $V = k^2$ of column vectors is a left module over the ring

$$R = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \gamma \end{pmatrix} \;\middle|\; \alpha, \beta, \gamma \in k \right\}$$

of upper triangular 2×2 matrices over the field k. Write

$$e_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad \text{and} \qquad e_2 = \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Show that ke_1 is an R-submodule of V but ke_2 is not. Show that the R-modules ke_1 and V/ke_1 are not isomorphic. Show that V is not isomorphic to the direct sum of these two modules (after you have looked at definition of the direct sum below).

Many of the basic properties that you are already familiar with in the context of groups and/or vector spaces, extend to modules.

Lemma 2.7 (The second isomorphism theorem) *If A and B are submodules of an R-module M, then*

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

Lemma 2.8 (The modular law) *If A, B, and C, are submodules of M and $B \subset A$, then*

$$A \cap (B + C) = B + A \cap C.$$

1.3 Annihilators

The annihilator of a left R-module M is

$$\mathrm{Ann}M := \{r \in R \mid rm = 0 \text{ for all } m \in M\}.$$

This is a two-sided ideal of R.

If I is an ideal of R and M a left R-module, we write

$$\begin{aligned} IM :&= \left\{ \sum_{i=1}^{n} a_i m_i \;\middle|\; a_i \in I, m_i \in M \right\} \\ &= \text{ the submodule generated by } \{am \mid a \in I, m \in M\}. \end{aligned}$$

If $IM = 0$, we say that I annihilates M. In that case, we can make M and R/I-module by defining

$$[r + I].m = rm.$$

The fact that $Im = 0$ ensures that this is well-defined. We leave the reader to check that the module axioms hold.

Exercises. In these exercises M denotes a left R-module.

1. If S is any subset of M define $\mathrm{Ann}S = \{r \in R \mid rs = 0 \text{ for all } s \in S\}$. Show that $\mathrm{Ann}S$ is a left ideal of R.

2. If S is a submodule of M, show that $\mathrm{Ann}S$ is a two-sided ideal of R.

3. If I is a two-sided ideal of R that is contained in $\mathrm{Ann}M$, show that M can be made into an R/I-module by defining $[r+I].m = rm$. Check this action is well-defined.

4. If I is a two-sided ideal of R, and M is an R/I-module, show that M can be made into an R-module in a natural way, and show that as an R-module I is contained in the annihilator of M.

5. Let I be a two-sided ideal of R. Show that $IM := \{\sum r_j m_j \mid r_j \in I, m_j \in M\}$ is a submodule of M, and that M/IM is an R/I-module via the action

$$[x+I].[m+IM] = [xm+IM].$$

The point is to show that his action is well-defined.

6. Let I be a left ideal of R and set $M = R/I$. Show that $\mathrm{Ann}M$ is the largest two-sided ideal of R that is contained in I. In particular, if R is commutative $\mathrm{Ann}(R/I) = I$.

7. If M and N are isomorphic R-modules, show that $\mathrm{Ann}M = \mathrm{Ann}N$. Give an example to show that the converse is false.

8. Observe that a module M is cyclic if and only if there is a surjective module homomorphism $R \to M$, and hence if M is cyclic so is every quotient M/N.

The result in Exercise 7 is very useful for deciding when two modules are not isomorphic so we record it.

Proposition 3.1 *Let M and N be modules such that $\mathrm{Ann}M \neq \mathrm{Ann}N$. Then $M \ncong M$.*

1.4 Direct products and direct sums

If $\{M_i \mid i \in I\}$ is a collection of left R-modules, their direct product $\prod_{i\in I} M_i$ is the set of all tuples $(m_i)_{i\in I}$ with $m_i \in M_i$ and the action of R defined by $r.(m_i) = (r.m_i)$. In other words, $\prod_{i\in I} M_i$ as a set is the cartesian product of the M_is with componentwise addition and R-action as described.

Their direct sum $\oplus_{i\in I} M_i$ is the subset of $\prod_{i\in I} M_i$ consisting of all tuples $(m_i)_{i\in I}$ in which only a finite number of the m_i are non-zero. Check that this *is* a submodule of $\prod_{i\in I} M_i$. When I is finite $\prod_{i\in I} M_i \cong \oplus_{i\in I} M_i$.

Example 4.1 Let L and N be submodules of a module M. If $L \cap N = 0$, then there is an isomorphism $\psi : L \oplus N \to L + N$, given by $\psi(\ell, n) = \ell + n$. Thus, when $L \cap N = 0$ we sometimes denote their sum $L + N$ by $L \oplus N$. $\Diamond$

We will often make use of the previous example, and write

$$M = L \oplus N$$

when L and N are submodules of M such that $M = L + N$ and $L \cap N = 0$; for example, see the statement of Corollary 10.7. Strictly speaking we should only write $M \cong L \oplus N$.

We can extend this notion to sums of more than two submodules. Suppose that $L_1, \ldots, L_n$ are submodules of a module M. Suppose further that $M = L_1 + \ldots + L_n$; i.e., every element of M can be written as $\ell_1 + \ldots + \ell_n$ with $\ell_i \in L_i$. Claim: if the only way to write $0 = \ell_1 + \ldots + \ell_n$ with $\ell_i \in L_i$ is by taking $\ell_1 = \ldots = \ell_n = 0$, then $M \cong L_1 \oplus \ldots \oplus L_n$. To prove this claim we first note that there is a surjective R-module homomorphism

$$\psi : L_1 \oplus \ldots \oplus L_n \to L_1 + \ldots + L_n$$

defined by $\psi(\ell_1, \ldots, \ell_n) = \ell_1 + \ldots + \ell_n$. The condition on the uniqueness of the representation of zero is equivalent to ψ being injective, hence equivalent to ψ being an isomorphism.

We again abuse notation by writing $M = L_1 \oplus \ldots \oplus L_n$ if $L_1, \ldots, L_n$ are submodules of M such that $M = L_1 + \ldots + L_n$ and the only way to write zero as a sum $0 = \ell_1 + \ldots + \ell_n$ with $\ell_i \in L_i$ is to take each ℓ_i to be zero.

Notice the similarity with linear independence in a vector space. If $M = L_1 \oplus \ldots \oplus L_n$, then every element of M can be written in a unique way as $\ell_1 + \ldots + \ell_n$ with $\ell_i \in L_i$. Some authors say that such submodules $L_1, \ldots, L_n$ are independent.

A submodule L of M is called a direct summand of M if there is a submodule N such that $L \oplus N = M$.

Lemma 4.2 *A submodule $L \subset M$ is a direct summand if and only if there is a homomorphism $\theta : M \to L$ such that $\theta|_L = \mathrm{id}_L$.*

Proof. If L is a direct summand, say $L \oplus N = M$, then define θ by $\theta(\ell + n) = \ell$ for $\ell \in L$ and $n \in N$. Conversely, if such θ exists, take $N = \ker\theta$, and observe that $M = L \oplus N$. □

Lemma 4.3 *Suppose that $f : M \to N$ and $g : N \to M$ are such that $fg = \mathrm{id}_N$. Then*

1. *g is injective and f is surjective;*

2. *$M = \ker f \oplus \mathrm{im}(g)$ and $N \cong \mathrm{im}(g)$.*

Proof. (1) Clear.

(2) Let $m \in M$ and write $m = gf(m) + (m - gf(m))$; then $m - gf(m) \in \ker f$ so this shows that $M = \mathrm{im}(g) + \ker f$. If $m \in \mathrm{im}(g) \cap \ker f$, then $m = g(m')$ and $0 = f(m) = fg(m') = m'$ so $m = g(m') = 0$. Hence $\mathrm{im}(g) \cap \ker f = 0$.

Since g is injective it is an isomorphism from N onto its image. □

Since $M = \ker f \oplus \mathrm{im}(g) \cong \ker f \oplus N$, we often say in the context of the previous lemma that N is a (direct) summand of M. What we really mean is that M has a submodule that is isomorphic to N and a direct summand of M.

1.5 Idempotents

The module theory of a ring that is a direct sum of other rings can be easily expressed in terms of the module theory of the individual summands. Such summands correspond to central idempotents.

Lemma 5.1 *Let R be a ring.*

1. *Suppose I and J are left ideals such that $R = I \oplus J$, and write $1 = e + f$ with $e \in I$ and $f \in J$. Then*
   (a) $e = e^2$, $f = f^2$, $ef = fe = 0$;
   (b) $I = Re$ *and* $J = R(1 - e)$.
2. *Conversely, if $e \in R$ is such that $e = e^2$, then $R = Re \oplus R(1 - e)$.*

Proof. (1) We have $e = e^2 + fe$, so $fe = e - e^2 \in I \cap J$. But $I \cap J = 0$, so we deduce that $e^2 = e$ and $fe = 0$. Similarly $f^2 = f$ and $ef = 0$.

Certainly, $Re \subset I$. If $x \in I$, then $x = 1.x = ex + (1 - e)x$, so $(1 - e)x = x - ex \in I \cap J$, so $x = ex$. Thus $I \subset Re$, so $I = Re$.

(2) Certainly $R = Re + R(1 - e)$. If $xe = y(1 - e)$ is in $Re \cap R(1 - e)$, then $xe = xe^2 = y(1 - e)e = y(e - e^2) = 0$. Hence the intersection is zero, and R is the direct sum of these two left ideals. □

Definition 5.2 An element $e \in R$ such that $e^2 = e$ is called an idempotent.

If e and f are idempotents such that $ef = fe = 0$, we say that e and f are orthogonal idempotents.

A set $\{e_1, \ldots, e_n\}$ of pairwise orthognal idempotents is called a complete set of idempotents if $e_1 + \cdots + e_n = 1$.

An idempotent e is primitive if it is not a sum of two non-zero orthogonal idempotents. ◊

Thus, idempotents correspond to decompositions of R into a direct sum of two left ideals. There is nothing special about *left* ideals here, and one easily sees that idenmpotents also correspond to decompositions of R into a direct sum of two right ideals.

Furthermore, if R is a direct sum of left ideals, say $R = I_1 \oplus \cdots \oplus I_n$, we may write $1 = e_1 + \ldots + e_n$ with $e_j \in I_j$. Then $e_j^2 = e_j$ for all j and $e_i e_j = 0$ if $i \neq j$. That is, $\{e_1, \ldots, e_n\}$ is a complete set of orthogonal idempotents.

Example 5.3 Let $R = M_n(k)$ be the ring of $n \times n$ matrices over a field k. Then e_{ii}, the matrix with a 1 in the ii-position and zeroes elsewhere is an idempotent.

The left ideal Re_{ii} consists of those matrices that are zero everywhere except possibly in the i^{th} row. The right ideal $e_{ii}R$ consists of those matrices that are zero everywhere except possibly in the i^{th} column. The left ideal $R(1 - e_{ii})$ consists of those matrices that are zero in the i^{th} row.

Notice here that e_{ii} is orthogonal to e_{jj} if $i \neq j$. Hence $\{e_{11}, \ldots, e_{nn}\}$ is a complete set of primitive orthogonal idempotents. ◊

If e is an idempotent, then eRe is a subring of R in which e is the identity element.

Lemma 5.4 *Let R be a ring.*

1. *Suppose that $\{e_1, \ldots, e_n\}$ is a complete set of orthogonal idempotents. If each e_j is central, then*
   (a) *$e_j R e_j = R e_j$, and*
   (b) *there is an isomorphism of rings $R \cong R_1 \times \cdots \times R_n$ where $R_j = e_j R e_j$.*
2. *Conversely, if there is an isomorphism of rings $R \cong R_1 \times \cdots \times R_n$, then*
   (a) *each R_j becomes a two sided ideal of R, and*
   (b) *$R_j = Re_j = e_j R e_j$ where $e_j = (0, \ldots, 1, \ldots, 0)$ has the identity of R_j in the j^{th} position and zeroes elsewhere, and*
   (c) *$\{e_1, \ldots, e_n\}$ is a complete set of orthogonal central idempotents.*

Now we come to the module theory.

Lemma 5.5 *Suppose $R = R_1 \oplus \cdots \oplus R_n$. Set $e_j = (0, \ldots, 1, \ldots, 0)$ has the identity of R_j in the j^{th} position and zeroes elsewhere.*

1. *If $M_1, \ldots, M_n$ are modules for $R_1, \ldots, R_n$ then $M_1 \oplus \cdots \oplus M_n$ is an R-module via*
$$(r_1, \ldots, r_n).(m_1, \ldots, m_n) := (r_1 m_n, \ldots, r_n m_n).$$
2. *If M is an R-module, then $M_j := e_j M$ is an R-submodule of M, and if we view each M_j as an R_j-module, then $M \cong M_1 \oplus \cdots \oplus M_n$ as in (1). R-submodule of M.*

1.6 Simple Modules

The smallest non-zero modules are the simple modules. An important problem in many branches of algebra is to classify and understand the structure of simple modules.

Definition 6.1 A non-zero left R-module is simple if its only submodules are zero and itself. ◊

Lemma 6.2 *A non-zero map between two simple modules is either an isomorphism or zero.*

Proof. Let $f : M \to N$ be a non-zero homomorphism between simple modules. Then $\ker f$ and $\operatorname{im} f$ are submodules of M and N respectively. Since $f \neq 0$, $\ker f \neq M$ and $\operatorname{im} f \neq 0$. Since M and N are simple this forces $\ker f = 0$ and $\operatorname{im} f = N$; i.e., f is injective and surjective, hence an isomorphism. □

Definition 6.3 A division ring is a ring D such that every non-zero element of D has an inverse. ◊

For example, a field is a division ring. Fields are the commutative division rings.

Example 6.4 (The Quaternions.) The ring $\mathbb{H}$ of quaternions is the $\mathbb{R}$-vector space with basis $1, i, j, k$ and multiplication table given by

$$i^2 = j^2 = k^2 = -1 \text{ and } ij = k,\ jk = i,\ ki = j,$$

extended $\mathbb{R}$-linearly.

To check that this really is a ring it is simplest to realize it as a subring of $M_4(\mathbb{R})$ in the following way. As an $\mathbb{R}$-vector space $\mathbb{H}$ has a basis $1, i, j, k$. The multiplication on $\mathbb{H}$ allows us to define a map

$$\rho : \mathbb{H} \to M_4(\mathbb{R})$$

by $\rho(x)$:=the matrix with respect to the basis $\{1, i, j, k\}$ representing the linear transformation $a \mapsto xa$. For example, since $i.1 = i, i.i = -1,\ i.j = k,\ i.k = -j$ we have

$$\rho(i) = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

One now checks that the images of $1, i, j, k$ span a 4-dimensional subspace of $M_4(\mathbb{R})$ and that the products of these images are the same as the images of their products in $\mathbb{H}$. ◊

Lemma 6.5 (Schur's Lemma) *If M is a simple module over a ring R, then* $\mathrm{End}_R M$ *is a division ring.*

Proof. Let $f : M \to M$ be a non-zero R-module map. Then $\ker f$ is a submodule of M and is not equal to M, so is zero. Also, $\mathrm{im}\, f$ is a non-zero submodule of M, so is equal to M. Thus f is both injective and surjective, so is an isomorphism. Hence $\mathrm{End}_R M$ contains f^{-1}. □

Exercise. Consider the ring R of differential operators on $k[x]$ when $\mathrm{char}\, k = 0$. Show that $k[x]$ is a simple left R-module.

Example 6.6 1. Let k be a field. The simple k-modules are the 1-dimensional vector spaces. They are all isomorphic to one another. So we often say that there is a unique simple module, meaning that there is a unique simple module up to isomorphism.

2. The simple $\mathbb{Z}$-modules are the cyclic groups $\mathbb{Z}_p$ with p prime.

3. The module k^n of $n \times 1$ column vectors is a simple left $M_n(k)$-module. To see this, suppose that $0 \neq v \in k^n$. If $u \in k^n$, then there is a matrix A such that $Av = u$ (we can change basis!), so $M_n(k).v = k^n$, whence k^n is simple.

Definition 6.7 A left ideal of R is maximal if it is not equal to R and the only left ideals containing it are R and itself. ◊

Definition 6.8 Let M be an R-module. A submodule N of M is maximal if it is not equal to M and the only submodules containing it are M and itself. ◊

Lemma 6.9 *If M is a non-zero finitely generated R-module, then M has a maximal submodule.*

Proof. Suppose that $M = Rm_1 + \ldots + Rm_n$. By throwing away some of the m_is and renumbering, we can assume that $M \neq Rm_1 + \ldots + Rm_{n-1}$. Hence $\bar{M} := M/Rm_1 + \ldots + Rm_{n-1} \neq 0$, and it suffices to show that $\bar{M}$ has a maximal submodule. However, $\bar{M}$ is cyclic, so $\bar{M} \cong R/I$ for some left ideal $I \neq R$ and it suffices to show that R has a maximal left ideal that contains I.

Let $\mathcal{S} := \{\text{left ideals } J \text{ such that } I \subset J \text{ and } J \neq R\}$. The condition that $J \neq R$ is equivalent to the condition that $1 \notin J$. If $J_1 \subset J_2 \subset \cdots$ is an ascending chain of left ideals belonging to $\mathcal{S}$, then $J := \cup J_i$ is also in $\mathcal{S}$. Hence, by Zorn's Lemma, $\mathcal{S}$ has maximal members. Pick one, say J. Then J is a maximal left ideal of R that contains I. □

Warning. If M is not finitely generated it need not have a maximal submodule. For example, consider the $\mathbb{Z}$-submodule $M = \{a2^n \mid a, n \in \mathbb{Z}\} \subset \mathbb{Q}$. Notice that M is the union of the ascending chain

$$\mathbb{Z} \subset \frac{1}{2}\mathbb{Z} \subset \frac{1}{4}\mathbb{Z} \subset \frac{1}{8}\mathbb{Z} \subset \cdots .$$

If N is a submodule of M that is not equal to N, then N does not contain all $1/2^n$, $n \geq 0$. So, choose n maximal such that $1/2^n \in N$. Hence $1/2^{n+1} \neq N$, and $N' = N + \frac{1}{2^{n+1}}\mathbb{Z}$ is strictly larger than N. However, $N' \neq M$ because $1/2^{n+2}$ is not contained in N'. Hence N is not a maximal submodule of M.

Perhaps this argument is clearer if one simply notes that the only proper submodules of M are $\frac{1}{2^n}\mathbb{Z}$.

Proposition 6.10 *If M is a simple left R-module, then $M \cong R/I$ for some maximal left ideal I.*

Proof. Since a simple module is cyclic, $M \cong R/I$ for some left ideal I. But the submodules of M are in bijection with the left submodules of R (i.e., the left ideals of R) that contain I. Hence M is simple if and only if I is maximal. □

Corollary 6.11 *Over a commutative ring the set of isomorphism classes of simple modules is in bijection with the set of maximal ideals, the bijection being given by*

$$\mathfrak{m} \longleftrightarrow R/\mathfrak{m}.$$

Proof. In a commutative ring left ideals are the same things as two-sided ideals, so the simple modules are $R/\mathfrak{m}$ where $\mathfrak{m}$ is a maximal ideal. If $\mathfrak{m}_1$ and $\mathfrak{m}_2$ are distinct maximal ideals, then $R/\mathfrak{m}_1 \ncong R/\mathfrak{m}_2$ because isomorphic simples have the same annihilator and $\mathfrak{m} = \text{Ann}(R/\mathfrak{m})$. □

Example 6.12 The simple modules over $k[x]$ are in bijection with the monic irreducible polynomials; if k is algebraically closed these are the monic polynomials of degree one, $x - \alpha$, $\alpha \in k$. Hence the simple modules are in bijection with the elements of k. In that case, the simple modules are $k[x]/(x-\alpha)$; this is a one-dimensional vector space where x acts like multiplication by α. Not too interesting! Slightly more interesting is the two-dimensional simple module $\mathbb{R}[x]/(x^2+1)$, which we can view as having an ordered basis $\{\overline{1}, \overline{x}\}$, and the action of x is given by the matrix

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

with respect to this basis; notice that the square of this matrix is -1. The subspace of $M_2(\mathbb{R})$ spanned by 1 and the above matrix is isomorphic to $\mathbb{C}$. ◊

Exercise. Let f be a non-zero polynomial in $k[x,y]$ when k is algebraically closed, and let $R = k[x,y]/(f)$. Show that the simple R-modules are in bijection with the points in k^2 that lie on the curve where f is zero, namely $C = \{(\alpha,\beta) \mid f(\alpha,\beta) = 0\}$. This bijection is the start of algebraic geometry.

Proposition 6.13 *If R is a ring containing an identity $1 \neq 0$, then R has a maximal left ideal, and a maximal two-sided ideal.*

Proof. We use Zorn's lemma. Let $\mathcal{S}$ be the set of (left) ideals not equal to R. This set is non-empty because it contains $\{0\}$. Inclusion provides a partial ordering on $\mathcal{S}$. The union of an ascending sequence of elemnts in $\mathcal{S}$ again belongs to $\mathcal{S}$. Such a union provides an upper bound for the ascending sequence, so Zorn's Lemma ensures that $\mathcal{S}$ has maximal elements. □

Irreducible representations. Let G be a finite group and k a field. The group algebra kG is, first, a k-vector space with basis $\{e_g \mid g \in G\}$ and multiplication defined by

$$e_g e_h := e_{gh}$$

extended to a k-linear multiplication on kG. Then kG is a ring with identity $1 = e_1$. A simple kG-module is also called an irreducible representation of G. The study and classification of such irreducible representations is a central part of algebra. The answers are oftenb extremely beuatiful.

For example, consider $\mathbb{C}S_n$, the group algebra of the symmetric group. The complex irreducible representations of S_n are in bijection with the partitions of n, denoted $\lambda \vdash n$. The dimension of the simple $\mathbb{C}S_n$-module iM_λ corresponding to λ is equal to the number of Young tableaux of shape λ. First, the Young diagram D_λ associated to $\lambda = (\lambda_1 \geq \lambda_2 \geq \ldots)$ is the diagram with λ_i boxes in

the i^{th} row. A tableau is then obtained by putting the numbers $1, 2, \ldots, n$ in the boxes so that each row increases going from left to right, and each column increases going down.

1.7 Composition series

If M is a module and $K \subset L \subset M$ are submodules, we call L/K a slice, or subquotient, of M.

Definition 7.1 A sequence of submodules

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

of a module M is called a composition series if M_i/M_{i-1} is simple for $i = 1, \ldots, n$. The slices M_i/M_{i-1} are called composition factors of M.

If M has such a composition series we say M has finite length and write $\text{length}(M) = n$. ◊

When speaking of the composition factors of a module care about the isomorphism classes of the simple slices and the number of times a particular simple module occurs. We call this the multiplicity of the simple module in the composition series. Thus the composition factors of M form a multi-set.

For example, the composition factors of $\mathbb{Z}_4$ are $\{\{\mathbb{Z}_2, \mathbb{Z}_2\}\}$, but the composition factors of $\mathbb{Z}_2$ are $\{\{\mathbb{Z}_2\}\}$.

The abelian groups $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ have the same composition factors, namely $\mathbb{Z}_2$ counted with multiplicity two in each case.

In general, a module of finite length may have many different composition series, but we shall see that the composition factors are, up to isomorphism, independent of the composition series. Thus we may speak of *the* composition factors of M.

Example 7.2 If $0 \neq f \in k[x]$, then we can write f as a product of irreducible polynomials, say $f = p_1^{n_1} \ldots p_r^{n_r}$. The slices of the series

$$k[x] = (1) \supset (p_1) \supset (p_1^2) \supset \cdots \supset (p_1^{n_1}) \supset (p_1^{n_1} p_2) \supset \cdots \supset (f)$$

are of the form $(g)/(p_i g) \cong k[x]/(p_i)$, and this is a simple module because p_i is irreducible. Hence the composition factors of $k[x]/(f)$ are the $k[x]/(p_i)$ counted with multiplicity n_i. In particular, if k is algebraically closed there is a natural bijection between the compoisition factors of $k[x]/(f)$ counted with multiplicity and the zeroes of f counted with multiplicity. ◊

In order to compare two composition series we introduce a more general notion. A finite filtration of a module M is a sequence of submodules $0 = M_0 \subset M_1 \subset \ldots \subset M_n = M$. There is no requirement that M_i/M_{i-1} be simple; in fact, we even allow it to be zero. We say that a filtration $(M_i, 0 \leq i \leq n)$ is a refinement of a filtration $(M'_j, 0 \leq j \leq p)$ if every M'_j is equal to some M_i.

Proposition 7.3 *Let $\mathbb{F} = (M_i, 0 \leq i \leq n)$ and $\mathbb{F}' = (M'_j, 0 \leq j \leq p)$ be finite filtrations of a module M. Then there are refinements $\mathbb{E}$ of $\mathbb{F}$ and $\mathbb{E}'$ of $\mathbb{F}'$, and a bijection between the non-zero slices of $\mathbb{E}$ and the non-zero slices of $\mathbb{E}'$ such that each slice of $\mathbb{E}$ is isomorphic to the corresponding slice of $\mathbb{E}'$.*

Proof. Define $N_{ij} := M_{i-1} + (M_i \cap M'_j)$. Then

$$M_{i-1} = N_{i,0} \subset N_{i,0} \subset \ldots \subset N_{i,p} = M_i,$$

so this is a refinement $\mathbb{E}$ of $\mathbb{F}$. A typical slice of $\mathbb{E}$ is

$$S_{ij} := \frac{M_{i-1} + (M_i \cap M'_j)}{M_{i-1} + (M_i \cap M'_{j-1})} \tag{7-1}$$

for a suitable i and j.

There is an analogous filtration $\mathbb{E}'$ of $\mathbb{F}'$ slices

$$S'_{ij} := \frac{M'_{j-1} + (M_i \cap M'_j)}{M'_{j-1} + (M_{i-1} \cap M'_j)}. \tag{7-2}$$

There is a module homomorphism

$$\Phi : M_i \cap M'_j \longrightarrow \frac{M_{i-1} + (M_i \cap M'_j)}{M_{i-1} + (M_i \cap M'_{j-1})}$$

given by $\Phi(a) = \bar{a}$. Now $\Phi(a) = 0$ if and only if $a = b + c$ with $b \in M_{i-1}$ and $c \in M_i \cap M'_{j-1}$. However, a and c are in M'_j, so such b must belong to $M_{i-1} \cap M'_j$. Hence $\ker \Phi = (M_{i-1} \cap M'_j) + (M_i \cap M'_{j-1})$. Thus

$$\frac{M_i \cap M'_j}{(M_{i-1} \cap M'_j) + (M_i \cap M'_{j-1})} \cong \frac{M_{i-1} + (M_i \cap M'_j)}{M_{i-1} + (M_i \cap M'_{j-1})} = S_{ij}$$

Similarly,

$$\frac{M_i \cap M'_j}{(M_{i-1} \cap M'_j) + (M_i \cap M'_{j-1})} \cong \frac{M'_{j-1} + (M_i \cap M'_j)}{M'_{j-1} + (M_{i-1} \cap M'_j)} = S'_{ij}.$$

Combining these two isomorphisms we see that $S_{ij} \cong S'_{ij}$. □

Theorem 7.4 *The composition factors of a finite length module are well-defined, i.e., they do not depend on the choice of composition series.*

Proof. Let $\mathbb{F}$ and $\mathbb{F}'$ be composition series for M, and $\mathbb{E}$ and $\mathbb{E}'$ the refinements of each constructed as in Proposition 7.3. It is clear that the non-zero slices of $\mathbb{E}$ are exactly the composition factors for $\mathbb{F}$. Similarly for $\mathbb{E}'$ and $\mathbb{F}'$. The result now follows from the conclusion of Proposition 7.3. □

Corollary 7.5 *Let M be a finite length module and N a submodule of M. Then every composition factor of N, and every composition factor of M/N is a composition factor of M.*

Proof. Choose a composition series for M such that one of its terms is N. The result follows. □

Corollary 7.6 *Let R be a ring containing a field k in its center. Let M be a left R-module such that $\dim_k M < \infty$. Then M has finite length.*

Proof. We argue by induction on $\dim_k M$. If $\dim_k M = 0$, there is nothing to do so suppose that $\dim_k M \geq 1$. Set $M_0 = 0$ and let M_1 be a non-zero submodule of M of smallest dimension. Then M_1 must be a simple module. We may now apply the induction hypothesis to M/M_1, thus obtaining a sequence of submodules of the form $M_2/M_1 \subset \ldots M_n/M_1 = M/M_1$ where $M_1 \subset M_2 \subset \ldots \subset M_n = M$ are submodules of M. Since

$$\frac{M_i}{M_{i-1}} \cong \frac{M_i/M_1}{M_{i-1}/M_1},$$

this is a composition series for M. □

Corollary 7.7 *Let R be a ring that contains a copy of a field k in its center. If $\dim_k R < \infty$, then R has only a finite number of simple modules up to isomorphism.*

Proof. By the previous result R has a composition series, say $0 = I_0 \subset I_1 \subset \ldots \subset I_n = R$. Let $\{\{S_1, \ldots, S_n\}\}$ be the corresponding composition factors.

Let M be a simple R-module. Then $M \cong R/J$ for some left ideal J. Now J has a composition series, say $0 = J_0 \subset J_1 \subset \cdots \subset J_m = J$, and we may extend this to a composition series for R by setting $J_{m+1} = R$. Thus $J_{m+1}/J_m = R/J \cong M$ is a composition factor of R, so M is isomorphic to some S_i. □

A look ahead. Let R be any ring. Let A be the free abelian group with basis given by the isomorphism classes of the simple R-modules. There is a well-defined map from the set of finite length R-modules to A, $M \mapsto [M]$, defined by

$$[M] := a_1[S_1] + \cdots + a_n[S_n]$$

where $S_1, \ldots, S_n$ are the distinct simple modules that occur as composition factors of M and a_j is the number of times that S_j occurs as a composition factor. This assignment has the property that if $0 \to L \to M \to N \to 0$ is an exact sequence of finite length R-modules, then $[M] = [L] + [N]$.

This is the idea behind the Grothendieck group $K_0(R)$.

1.8 Semisimple rings and modules

Definition 8.1 A module is semisimple if it is the sum of its simple submodules. A ring is semisimple if it is semisimple as a module over itself. ◊

Warning. We should really say that R is *left* semisimple if it the sum of its simple left ideals, but we shall see below that R is semisimple as left R-module if and only if it is semisimple as a right R-module.

Proposition 8.2 *The following conditions on a module M are equivalent:*

1. *M is the sum of its simple submodules;*
2. *M is a direct sum of simple modules;*
3. *if N is a submodule of M there is a submodule L of M such that $M = L \oplus N$.*

Proof. □

If $M = L \oplus N$ we call L a complement to N in M.

Lemma 8.3 *Suppose that M is a semisimple module. Then so is every quotient, and submodule of M.*

Lemma 8.4 *If R is (left) semisimple so is every left R-module.*

Proof. If one has a collection M_i, $i \in I$, of semisimple modules, their direct sum is semisimple too. This is clear if the sum is finite. However, even if the sum is infinite then every element in $\oplus_{i\in I} M_i$ belongs to a *finite* direct sum of various M_is, so belongs to a sum of simple submodules; thus the full direct sum is semisimple.

The previous paragraph shows that every free left R-module is semisimple. But every R-module is a quotient of a free module, so is semisimple too by Lemma **??**. □

Lemma 8.5 *A semisimple ring is a finite direct sum of simple submodules.*

Proof. Write $R = \sum_{i\in I} M_i$ as a sum of simple submodules. Then $1 = \sum m_i$, and this is a finite sum so 1 belongs to the direct sum of only finitely many of the M_is; hence R itself is contained in the sum of only a finite number of simple submodules. The result follows. □

Lemma 8.6 *Suppose that R is a semisimple ring, and write $R = I_1 \oplus \cdots \oplus I_t$ as a direct sum of left ideals, each of which is a simple R-module. Then every simple R-module is isomorphic to some I_j.*

Proof. Let M be a simple left R-module and let $0 \neq m \in M$. The map $\pi : R \to M$, $\pi(x) = xm$ is surjective. Hence, $\pi(I_j) \neq 0$ for some j. Since the restriction of π to I_j is a non-zero map between two simple modules it must be an isomorphism. □

Matrix representations of module homomorphisms. Consider an R-module homomorphism

$$f : M = M_1 \oplus \cdots \oplus M_r \longrightarrow N = N_1 \oplus \cdots \oplus N_s.$$

Let $\alpha_i : M_i \to M$ be the obvious inclusion and let $\pi_j : N \to N_j$ be the projection vanishing on the summands N_k for $k \neq j$. We define

$$f_{ij} := \pi_j \circ f \circ \alpha_i : M_i \to N_j$$

and call this the ij-component of f with respect to the given decompositions.

Now let $\rho_i : M \to M_i$ and $\phi_j : N_j \to N$ be the obvious projection and inclusion. Notice that

$$\mathrm{id}_M = \sum_{i=1}^{r} \alpha_i \rho_i, \quad \rho_i \alpha_k = \delta_{ik}, \qquad \mathrm{id}_N = \sum_{j=1}^{r} \phi_j \pi_j, \quad \pi_j \phi_k = \delta_{jk}.$$

It follows that

$$f = \sum_{i=1}^{r} \sum_{j=1}^{s} \phi_j \circ f_{ij} \circ \rho_i.$$

If $g : M_i \to N_j$, then the ij-component of

$$\phi_j \circ g \circ \rho_i : M \to N$$

is g and all other components of $\phi_j g \rho_i$ are zero.

It follows that

$$\mathrm{Hom}_R(M, N) = \bigoplus \mathrm{Hom}_R(M_i, N_j).$$

More precisely,

$$\mathrm{Hom}_R(M, N) = \bigoplus \phi_j \,\mathrm{Hom}_R(M_i, N_j)\rho_i,$$

and the map

$$\mathrm{Hom}_R(M_i, N_j) \to \phi_j \,\mathrm{Hom}_R(M_i, N_j)\rho_i, \quad g \mapsto \phi_j \circ g \circ \rho_i$$

is a bijection onto its image.

One should think of all the f_{ij}s arranged into an $r \times s$ matrix, and write this as

$$f = (f_{ij});$$

if elements of M are written as row vectors, $m = (m_1, \ldots, m_r)$, then the matrix f acts by right multiplication on this vector, and the product is exactly $f(m)$

viewed again as a row vector corresponding to the decomposition $N = N_1 \oplus \cdots \oplus N_s$.

If $L = L_1 \oplus \cdots \oplus L_q$ is a third module, then the composition

$$\mathrm{Hom}_R(M,N) \times \mathrm{Hom}_R(L,M) \to \mathrm{Hom}_R(L,N)$$

is compatible with matrix multiplication. This is because matrix multiplication is defined so as to make this true!

Lemma 8.7 *Let $S_1, \ldots, S_t$ be simple left R-modules that are pair-wise non-isomorphic. Let M be a left R-module and define M_i to be the sum of all submodules of M that are isomorphic to S_i. Then the sum $M_1 + \ldots + M_t$ is direct.*

Proof. We can argue by induction on t. The case $t = 1$ is certainly true, so supppose that $M_1 + \ldots + M_{t-1}$ is a direct sum. We must show that N:=$M_t \cap (M_1 + \ldots + M_{t-1}) = 0$. Suppose $N \neq 0$. Because N is a submodule of M_t, all the composition factors of N are isomorphic to S_t. But it then follows that S_t is a composition factor of $M_1 + \ldots + M_{t-1}$. This is absurd. □

If in the previous lemma $M = M_1 \oplus \cdots \oplus M_t$ we call M_j the S_j-isotypic component of M, and call this the decomposition of M into its isotypic components.

Theorem 8.8 *Let R be a semisimple ring. Then there are division rings $D_1, \ldots, D_t$ and positive integers $n_1, \ldots, n_t$ such that*

$$R \cong M_{n_1}(D_1) \oplus \cdots \oplus M_{n_t}(D_t).$$

Proof. If we view R as a right module over itself, there is a ring isomorphism $\Psi : R \to \mathrm{End}_R(R_R)$ given by

$$\Psi(r) = \lambda_r$$

where λ_r is the map "left multiply by r", i.e., $\lambda_r(x) = rx$. (Notice that $\Psi(rs) = \Psi(r)\Psi(s)$; it is for this reason that we viewed R as a *right* module over itself; if we had viewed R as a left module over itself, then $\mathrm{End}_R(R)$ would be anti-isomorphic to R.)

Now, suppose that $S_1, \ldots, S_t$ are the distinct simple right R-modules up to isomorphism. Define

$$R_t := \text{the sum of all right ideals of } R \text{ isomorphic to } S_i.$$

Since R is a sum of simple submodules, $R = R_1 + \ldots + R_t$. By Lemma 8.7, this is a direct sum.

Each R_i is obviously a right ideal of R. It is also a left ideal: if I is a simple right ideal of R and $x \in R$, the map $\phi : I \to R$, $\phi(a) = xa$, is a homomorphism of right R-modules, so its image xI is either zero or isomorphic to I; in particular, if $I \subset R_j$, then $xI \subset R_j$ too.

□

1.9 Finitely generated modules

If $m_1, \ldots, m_n$ are elements of a module M, the submodule they generate is defined to be the smallest submodule that contains them (this makes sense because an intersection of submodules is again a submodule). It is equal to

$$Rm_1 + \ldots + Rm_n := \{r_1m_1 + \ldots + r_nm_n \mid r_1, \ldots, r_n \in R\}.$$

If there is a finite set of elements in M such that $M = Rm_1 + \ldots + Rm_n$ we say that M is finitely generated. We also call $\{m_1, \ldots, m_n\}$ a set of generators for M.

A left R-module M is finitely generated if there is a finite set of elements $m_1, \ldots, m_n \in M$ such that every element in M can be written in the form

$$r_1m_1 + \cdots + r_nm_n \tag{9-3}$$

for suitable elements $r_1, \ldots, r_n \in R$. In general, if $m_1, \ldots, m_n$ are any elements of M we write $Rm_1 + \cdots + Rm_n$ for the set of all elements of the form (9-3) as $r_1, \ldots, r_n$ range over all possibilities. It is an easy exercise to check that $Rm_1 + \cdots + Rm_n$ is a submodule of M.

For example, R is a finitely generated left (and right) R-module because $R = R.1$; every element in R is a left multiple of 1! The reader should be warned that a submodule of a finitely generated module need not be finitely generated. For example, the ideal $(x_1, x_2, \ldots)$ of the infinite polynomial ring $k[x_1, x_2, \ldots]$ is not finitely generated.

In analogy with vector spaces we define the left R-module R^n to consist of n-tuples $(r_1, \ldots, r_n)$ of elements from R with the action given by $r.(r_1, \ldots, r_n) = (rr_1, \ldots, rr_n)$. We call this the free left R-module of rank n. It is finitely generated, a generating set being given by the elements

$$e_1 = (1, 0, \ldots, 0), \cdots, e_n = (0, 0, \ldots, 1).$$

Because each element of R^n can be written in a unique way as $r_1e_1 + \cdots + r_ne_n$ we call $\{e_1, \ldots, e_n\}$ a basis for R^n.

If N is a submodule of a finitely generated R-module M, then M/N is finitely generated: if $\{m_1, \ldots, m_n\}$ generate M, then $M/N = R\bar{m}_1 + \cdots + R\bar{m}_n$, where $\bar{m}_i = [m_i + N]$.

Initially, we only need to consider modules that arise in the following way.

If R is a subring of a ring S, then S is both a left and a right R-module. The multiplication of elements in S can be viewed as restricting to maps $R \times S \to S$ and $S \times R \to S$ giving S the structure of a left and a right R-module, respectively.

For example, every k-algebra is in the first place a k-vector space.

More generally, if $\theta : R \to S$ is a homomorphism of rings, then S becomes a left and a right R-module by defining

$$r.s = \theta(r)s \qquad s.r = a\theta(r)$$

for $r \in R$ and $s \in S$. The module action is induced by the multiplication in S and the fact that S is a ring implies that all the axioms for S to be an R-module are satisfied.

Every left ideal of S is an S-submodule of ${}_SS$, and hence is a left R-submodule of S.

Lemma 9.1 *If $R \subset S \subset T$ be commutative rings. If if T is a finitely generated S-module and S is a finitely generated R-module, then T is a finitely generated R-module.*

Proof. By hypothesis, $S = Ra_1 + \cdots + Ra_m$ and $T = Sb_1 + \cdots + Sb_n$, so

$$T = \sum_{i=1}^{m} \sum_{j=1}^{n} Ra_i b_j,$$

whence the result. □

Let $\psi : R \to S$ be a homomorphism of commutative rings, and let $\mathfrak{m}$ be a maximal ideal of R. The image $\psi(\mathfrak{m})$ need not be an ideal of S, but it does generate an ideal, say J. The composition

$$R \to S \to S/J$$

is a ring homomorphism that sends $\mathfrak{m}$ to zero. The kernel of this composition can be no bigger than $\mathfrak{m}$, so we have an injective ring homomorphism $R/\mathfrak{m} \to S/J$. If S is a finitely generated R-module, say $S = Rs_1 + \cdots + Rs_n$, then it follows at once that S/J is a finitely generated $R/\mathfrak{m}$-module, generated by the images of the s_is. but $R/\mathfrak{m}$ is a field, so S/J is a finite-dimensional vector space over $R/\mathfrak{m}$.

The following innocent looking result is one of the most frequently used results in commutative algebra.

Lemma 9.2 (Nakayama's Lemma) *Let R be a commutative ring having a unique maximal ideal $\mathfrak{m}$. If M is finitely generated R-module such that $\mathfrak{m}M = M$ then $M = 0$.*

Proof. It suffices to show that if M is a non-zero finitely genereated R-module, then $\mathfrak{m}M \neq M$. Choose n minimal such that M is generated by n elements. Modding out the submodule generated by $n-1$ of those elements gives a non-zero cyclic quotient, say $\bar{M} = R/J$. Hence M has a quotient M/N that is isomorphic to $R/\mathfrak{m}$. Thus $\mathfrak{m}$ annihilates M/N, which implies that $\mathfrak{m}M \subset N \neq M$.

In fact, this proof shows that $\mathfrak{m}M$ is contained in every maximal submodule of M, and that M does have maximal submodules. □

Example 9.3 Nakayama's lemma does required the finitely generated hypothesis. To see this, consider the ring $R = \{a/2^n \mid a \in \mathbb{Z}, n \geq 0\} \subset \mathbb{Q}\}$. Then

$\mathfrak{m} = (2)$ is the unique maximal ideal of R. Because R is a subring of $\mathbb{Q}$, multiplication gives $\mathbb{Q}$ the structure of an R-module. However, $\mathfrak{m}\mathbb{Q} = \mathbb{Q}$.

You might try to find a direct proof that $\mathbb{Q}$ is not a finitely generated R-module. You can also try to show that $\mathbb{Q}$ is not a finitely generated $\mathbb{Z}$-module. Does $\mathbb{Q}$ have a maximal $\mathbb{Z}$-submodule? Equivalently, does $\mathbb{Q}$ have a simple quotient $\mathbb{Z}$-module? $\Diamond$

1.10 Free modules

Free modules are (in some respects) the modules most like vector spaces. They have a basis, and elements of a free module can be expressed in a unique way as linear combinations of the basis elements with coefficients in the ring. Every module is a quotient of a free module (possibly in many different ways), and one can use this to get insight into arbitrary modules. For example, every abelian group can be expressed as M/N where M and N are free abelian groups.

Definition 10.1 A subset $\mathcal{B}$ of a left R-module M is linearly dependent over R if there exist elements $r_1, \ldots, r_n \in R$, not all zero, and elements $m_1, \ldots, m_n \in \mathcal{B}$ such that $r_1 m_1 + \ldots + r_n m_n = 0$. If $\mathcal{B}$ is not linearly dependent we say it is linearly independent. We call $\mathcal{B}$ a basis for M if $\mathcal{B}$ is linearly independent and $M = R\mathcal{B}$, i.e., if every element of M is an R-linear combination of elements of $\mathcal{B}$. If an R-module has a basis it is called a free module, and the cardinality of that basis is called the rank of the module. $\Diamond$

If M is generated by elements $\{m_i \mid i \in I\}$, then any R-module homomorphism $\psi : M \to N$ is completely determined by what it does to the m_is. That is, once we know $\psi(m_i)$, we know ψ because if $m \in M$, then $m = \sum_{i \in I} r_i m_i$, for some elements $r_i \in R$, so

$$\psi(m) = \sum_{i \in I} \psi(r_i) m_i$$

because ψ is an R-module homomorphism. Notice that in the expression $\sum_{i \in I} r_i m_i$ only a finite number of the r_is are non-zero, else the sum cannot make sense. If F is a free R-module with basis $\mathcal{B} = \{e_i \mid i \in I\}$, then every element of F can be expressed in a unique way as

$$\sum_{i \in I} r_i e_i,$$

for some $r_i \in R$. The uniqueness is because if $\sum_{i \in I} r_i e_i = \sum_{i \in I} s_i e_i$, then

$$0 = \sum_{i \in I} (r_i - s_i) e_i$$

so the linear independence of the e_is implies that $r_i = s_i$ for all i.

Definition 10.2 The free R-module of rank n is

$$R^n = R \oplus R \oplus \cdots \oplus R,$$

the direct sum of n copies of R with itself. Elements of R^n are n-tuples $(r_1, \ldots, r_n)$, with componentwise addition and action

$$x.(r_1, \ldots, r_n) = (xr_1, \ldots, xr_n).$$

The elements $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, $1 \leq i \leq n$, where the 1 occurs in the i^{th} position, form a basis for R^n. $\Diamond$

The module R^n is analogous to an n-dimensional vector space over R; indeed, over a field the free module of rank n is an n-dimensional vector space. However, when R is not a field there are lots of ways in which R^n does not behave like a vector space. For example, there are rings R for which there is an isomorphism of left R-modules $R \cong R \oplus R$.

Exercises. 1. Let k be a field, and let V be a vector space over k with basis $e_1, e_2, \ldots$. Let $R = \text{End}_k V$. Let $V_o = ke_1 + ke_3 + ke_5 + \ldots$ and let $V_e = ke_2 + ke_4 + \ldots$. Thus $V = V_o \oplus V_e$. Let a and b be elements of R such that $\text{im}(a) = \text{im}(b) = V$ and $\ker(a) = V_e$ and $\ker(b) = V_o$. Show that there are isomorphisms of left R-modules $R \cong Ra \cong Ra$. Show that $Ra \cap Rb = 0$ and $R = Ra + Rb$, whence there is an isomorphism of left R-modules $R \cong Ra \oplus Rb \cong R \oplus R$.

2. If R is commutative show that the left R-modules ${}_RR$ and $R \oplus R$ cannot be isomorphic. Hint: consider their endomorphism rings. How would you show that $R \oplus R$ is not isomorphic to $R \oplus R \oplus R$ when R is commutative?

3. Let (V, θ) be a finite dimensional k-vector space and a k-linear endomorphism of it. Make V into a $k[x]$-module by requiring x to act like θ. Show that V is not a free $k[x]$-module. If we allow V to be an infinite dimensional vector space, what conditions on θ are necessary for V to be a free $k[x]$-module of rank one? What conditions on θ are necessary for V to be a free $k[x]$-module?

4. Show that $\mathbb{Q}$ is not a free $\mathbb{Z}$-module.

There is another way of defining R^n. For any set I define $R^{(I)}$ to consist of all functions $f : I \to R$ such that $f(i)$ is non-zero for only a finite number of $i \in I$. Make this into a left R-module by defining $f + g$ to be the map $(f + g)(i) = f(i) + g(i)$ and $r.f$ to be the map $(r.f)(i) = r.f(i)$. Then $R^{(I)}$ becomes a left R-module. It is a free R-module with a basis given by the maps $\{f_j \mid j \in I\}$ where $f_j : I \to R$ is the map defined by

$$f_j(i) = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j. \end{cases}$$

If $I = \{1, \ldots, n\}$, then $R^{(I)} \cong R^n$ the isomorphism being given by sending $\sum_{i=0}^{n} r_i f_i$ to $(r_1, \ldots, r_n)$, i.e. f_i is sent to e_i.

Proposition 10.3 *An R-module M is free if and only if $M \cong R^{(I)}$ for some set I.*

Proof. ($\Rightarrow$) Let $\mathcal{B}$ be a basis for M. Define $\psi : M \to R^{(\mathcal{B})}$ by $\psi(\sum_{b\in\mathcal{B}} r_b b)$ to be the map that sends $c \in \mathcal{B}$ to r_c, the coefficient of c in the sum above. Check this is an isomorphism

($\Leftarrow$) We have already observed that $R^{(I)}$ has a basis. □

Let M and N be free R-modules with bases $\mathcal{B}_M$ and $\mathcal{B}_N$. If these bases have the same cardinality, then M is isomorphic to N.

Theorem 10.4 *Let F be a free module over a commutative ring. Then any two bases for F have the same cardinality.*

Proof. Let $\mathfrak{m}$ be a maximal ideal of R. Such an ideal exists by Zorn's Lemma. Then $V = F/\mathfrak{m}F$ is a module over the field $k = R/\mathfrak{m}$. If b_i, $i \in I$, is a basis for F, then $v_i = [b_i + \mathfrak{m}F]$ is a basis for V over k. Certainly these elements span V since the b_is span F. On the other hand if we have a linear dependence relation

$$[r_1 + \mathfrak{m}][b_1 + \mathfrak{m}F] + \ldots + [r_n + \mathfrak{m}][b_n + \mathfrak{m}F] = 0$$

in V, then $r_1b_1 + \ldots + r_nb_n \in \mathfrak{m}F = \sum_{i\in I} \mathfrak{m}b_i$. Hence there are elements $x_1, \ldots, x_n \in \mathfrak{m}$ such that $r_1b_1 + \ldots + r_nb_n = x_1b_1 + \ldots + x_nb_n$. It follows that $r_i = x_i$ for $i = 1, \ldots, n$, whence $[r_i + \mathfrak{m}] = 0$ in $R/\mathfrak{m}$. In particular, $\{[b_i + \mathfrak{m}F] \mid i \in I\}$ is linearly independent over $R/\mathfrak{m}$.

It follows that the cardinality of an R-basis for F is equal to the cardinality of a k-basis for $F/\mathfrak{m}F$. Since any two bases for a vector space have the same cardinality, the result follows. □

The exercise above showed that a free module can have bases of different cardinality. However, if $\mathcal{B}$ and $\mathcal{C}$ are two bases for a free left R-module, then $\mathcal{B}$ is infinite if and only if $\mathcal{C}$ is. To see this suppose that $\mathcal{B}$ is finite, say $\mathcal{B} = \{b_1, \ldots, b_n\}$. Because $\mathcal{C}$ is a basis there exist a finite number of elements $c_{ij} \in \mathcal{C}$ and $r_{ij} \in R$ such that $b_i = \sum_j r_{ij}c_{ij}$. Since $\mathcal{B}$ generates the module so does the finite set of c_{ij}. Hence if $c \in \mathcal{C}$, then c is in the R-span of the c_{ij}s; but $\mathcal{C}$ is linearly independent so $\mathcal{C}$ must equal the set of c_{ij}s.

Exercise. Let E and F be free modules over a commutative ring R, of ranks m and n respectively. If $\psi : E \to F$ is an injective R-module map show that $m \leq n$. Hint: look first at the cases $n = 1$ and $n = 2$. This is a little tricky.

Much of the importance of free modules derives from the next result. It says that every module is a quotient of a free module.

Theorem 10.5 *Let M be a left R-module, and $\{m_i \mid i \in I\} \subset M$ any collection of distinct elements. Let F be the free R-module with basis $\{e_i \mid i \in I\}$. Then there is a unique R-module homomorphism $\psi : F \to M$ such that $\psi(e_i) = m_i$. Conversely, if F is an R-module having elements $\{e_i \mid i \in I\}$ with this property, then F is free with basis $\{e_i \mid i \in I\}$.*

Proof. Define $\psi : F \to M$ by

$$\psi\left(\sum_{i\in I} r_i e_i\right) = \sum_{i\in I} r_i m_i.$$

Because each element of F can be expressed as $\sum_{i\in I} r_i e_i$ in a unique way, ψ is well-defined. It is clear that ψ is an abelian group homomorphism, and $\psi(r.f) = r.\psi(f)$ for all $rinR$ and $f \in F$, so ψ is an R-module homomorphism. The uniqueness of ψ is due to the fact that a module homomorphism is completely determined by what it does to a set of generators.

For the converse, take $N = R^{(I)}$, and for each $i \in I$, let f_i be the map $I \to R$ sending i to 1 and every other element of I to zero. Then N is free with basis $\{f_i \mid i \in I\}$. By the hypothesis on F there is a map $\psi : F \to N$ with $\psi(e_i) = f_i$ for all i. By the first part of the proof with F playing the role of M, because N is free with the prescribed basis, there is a module homomorphism $\psi' : N \to F$ with $\psi'(f_i) = e_i$ for all i. It follows that $\psi' \circ \psi = \mathrm{id}_F$ and $\psi \circ \psi' = \mathrm{id}_N$, so $F \cong N$. Thus F is free as claimed. □

Corollary 10.6 *If M is an R-module, then there exists a free R-module F and a surjective R-module homomorphism $\psi : F \to M$. If M can be generated by n elements we can take $F = R^n$.*

Thus any R-module is isomorphic to a module of the form F/K for a suitable free module F and suitable submodule $K \subset F$. We call this a presentation of M and call a set of generators for K a set of relations for F/K. There are many ways to write a particular module M as F/K; indeed, each choice of generators for M leads to such a presentation.

This is one method to describe an abelian group. For example, let G be the abelian group with generators a, b, c subject to the relations $2a + 3b + 4c = 0$ and $5a + 4b + 3c = 0$. As an exercise decide whether G has any torsion elements, that is elements $g \neq 0$ such that $n.g = 0$ for some $0 \neq n \in \mathbb{Z}$.

Corollary 10.7 *If $\psi : M \to F$ is a surjective R-module homomorphism and F is free, then there is an R-module homomorphism $\theta : F \to M$ such that $\psi\theta = \mathrm{id}_F$, and $M = \ker\psi \oplus \mathrm{im}\,\theta$. Notice that $\mathrm{im}\,\theta \cong F$ is free.*

Proof. Let $\{f_i \mid i \in I\}$ be a basis for F, and choose elements $m_i \in M$ such that $\psi(m_i) = f_i$. By Theorem 10.5, there is an R-module homomorphism $\theta : F \to M$ such that $\theta(f_i) = m_i$ for all i. Then $\psi\theta(f_i) = f_i$ for all i, so $\psi\theta = \mathrm{id}_F$.

Let $m \in \ker\psi \cap \mathrm{im}\,\theta$. Then $m = \theta(f)$ for some $f \in F$, and $0 = \psi(m) = \psi\theta(f) = f$, so $m = 0$. Hence $\ker\psi \cap \mathrm{im}\,\theta = 0$. On the other hand, if $m \in M$, then $m = (m - \theta\psi(m)) + \theta\psi(m)$; but $m - \theta\psi(m) \in \ker\psi$ and $\theta\psi(m) \in \mathrm{im}\,\theta$, so $M = \ker\psi + \mathrm{im}\,\theta$. Hence $M = \ker\psi \oplus \mathrm{im}\,\theta$. □

Example 10.8 Consider the ring $R = \mathbb{R}[x, y, z]/(x^2 + y^2 + z^2 - 1)$, the ring of polynomial functions on the sphere S^2. Let $F = R^3$ denote the rank three

free R-module. The elements of F are triples (a, b, c) where $a, b, c \in R$, and those elements of R^3 such that $xa + yb + zc = 0$ form a submodule of R^3 which we denote by K. One can consider K as the kernel of the surjective R-module homomorphism $\psi : R^3 \to R$ defined by $\psi(a, b, c) = xa + yb + zc$. Check that this is a homomorphism, and that it is surjective. Hence we have a short exact sequence $0 \to K \to R^3 \to R \to 0$. By Corollary 10.7 there exists a map $\theta : R \to R^3$ such that $\psi\theta = \mathrm{id}_R$. It is a good exercise to show that K is not free. By a theorem of R. Swan this is equivalent to showing that the tangent bundle to S^2 is not trivial. ◊

1.11 Exact sequences, complexes, and (co)homology

The notions of an exact sequence and, more generally, a complex, play a central role in modern algebra. Homology and cohomology groups measure how far a complex is from being exact.

Definition 11.1 A diagram

$$L \xrightarrow{\alpha} M \xrightarrow{\beta} N$$

of R-modules and R-module homomorphisms is exact at M if $\ker \beta = \operatorname{im} \alpha$. ◊

Definition 11.2 A sequence

$$\cdots \longrightarrow M_{n+1} \xrightarrow{\alpha_{n+1}} M_n \xrightarrow{\alpha_n} M_{n-1} \xrightarrow{\alpha_{n-1}} \cdots$$

of R-modules and R-module homomorphisms is a complex if $\alpha_n \alpha_{n+1} = 0$ for all n. ◊

This implies that $\ker \alpha_n \supset \operatorname{im} \alpha_{n+1}$ for all n. The complex is exact at M_n if $\ker \alpha_n = \operatorname{im} \alpha_{n+1}$. If it is exact at all M_n, we say that the sequence is exact. A short exact sequence is a sequence

$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0$$

which is exact at L, M, and N. We do not need to say what the first and last maps are because there is only one R-module homomorphism $0 \to L$ and only one R-module homomorphism $N \to 0$. Exactness at L is equivalent to α being injective, and exactness at N is equivalent to β being surjective.

Example 11.3 Let L and N be submodules of a module M. There is a short exact sequence of the form

$$0 \longrightarrow L \cap N \xrightarrow{\alpha} L \oplus N \xrightarrow{\beta} L + N \longrightarrow 0$$

where $\alpha(m) = (m, -m)$ and $\beta(\ell, n) = \ell + n$. Check this. ◊

The homology groups of a complex

$$\cdots \longrightarrow M_{n+1} \xrightarrow{\alpha_{n+1}} M_n \xrightarrow{\alpha_n} M_{n-1} \longrightarrow \cdots$$

are defined to be

$$H_n = \ker \alpha_n / \operatorname{im} \alpha_{n+1}.$$

Thus the homology groups measure the failure of the complex to be exact.

Half-exactness of Hom-functors

Let D be an R-module. There are two functors associated to D, namely $\mathrm{Hom}_R(D,-)$ and $\mathrm{Hom}_R(-,D)$. The first of these is covariant, meaning that if $f : L \to M$ is a homomorphism of R-modules, one obtains a homomorphism

$$f^* : \mathrm{Hom}_R(D,L) \to \mathrm{Hom}_R(D,M), \quad g \mapsto fg.$$

The other functor is contravariant, meaning that if $f : L \to M$ is a homomorphism of R-modules, one obtains a homomorphism

$$f^\sharp : \mathrm{Hom}_R(M,D) \to \mathrm{Hom}_R(L,D), \quad g \mapsto gf.$$

Suppose that $0 \to L \to M \to N \to 0$ is an exact sequence of R-modules. Then the sequences

$$0 \to \mathrm{Hom}_R(D,L) \to \mathrm{Hom}_R(D,M) \to \mathrm{Hom}_R(D,N)$$

and

$$0 \to \mathrm{Hom}_R(N,D) \to \mathrm{Hom}_R(M,D) \to \mathrm{Hom}_R(L,D)$$

are exact. You should check this. However, in general, neither of these sequences extends to a short exact sequence by placing $\to 0$ at the right-hand end. You should check this too, and find examples that verify the claims about failure of exactness.

When I say that $\mathrm{Hom}_R(D,-)$ and $\mathrm{Hom}_R(-,D)$ are functors I mean that they are functors from $\mathsf{Mod}R$, the category of left R-modules, to Ab, the category of abelian groups. That is, evaluating the functor at a left R-module produces an abelian group, and a homomorphism between two modules induces a homomorphism between the associated abelian groups in such a way that the induced homomorphism of a composition is the composition of the induced homomorphisms. Moreover, these functors provide group homomorphisms from

$$\mathrm{Hom}_R(M,N) \to \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_R(D,M), \mathrm{Hom}_R(D,N)) \qquad \text{and}$$
$$\mathrm{Hom}_R(M,N) \to \mathrm{Hom}_{\mathbb{Z}}(\mathrm{Hom}_R(N,D), \mathrm{Hom}_R(M,D))$$

respectively.

Of course, Ab is the same thing as $\mathsf{Mod}\mathbb{Z}$ so we may speak of exactness for abelian groups. A functor $F : \mathsf{Mod}R \to \mathsf{Ab}$ is said to be exact if it sends an exact sequence in $\mathsf{Mod}R$ to an exact sequence in Ab. The functors $\mathrm{Hom}_R(D,-)$ and $\mathrm{Hom}_R(-,D)$ are not exact, but we say they are half-exact, more precisely, left

exact, because when applied to short exact sequences they produce sequences that are exact at the left.

Split short exact sequences. If $M = L \oplus N$ there is an obvious exact sequence

$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\pi} N \longrightarrow 0$$

given by $\alpha(\ell) = (\ell, 0)$ and $\pi(\ell, n) = n$. An exact sequence of this form is said to be split.

Lemma 11.4 *Let*

$$0 \longrightarrow L \xrightarrow{\alpha} M \xrightarrow{\beta} N \longrightarrow 0 \tag{11-4}$$

be an exact sequence. The following are equivalent:

1. *there is an isomorphism $\delta : M \to L \oplus N$ such that $\delta\alpha(\ell) = (\ell, 0)$ for all $\ell \in L$ and $\beta\delta^{-1}(\ell, n) = n$ for all $(\ell, n) \in L \oplus N$;*

2. *there is a map $\alpha' : M \to L$ such that $\alpha'\alpha = \mathrm{id}_L$;*

3. *there is a map $\beta' : N \to M$ such that $\beta\beta' = \mathrm{id}_N$.*

Proof. (1) $\Rightarrow$ (2) Let $m \in M$. We define $\alpha'(m) := \ell$ if $\delta(m) = (\ell, n)$. If $\ell \in L$, then $\delta\alpha(\ell) = (\ell, 0)$, so $\alpha'\alpha(\ell) = \ell$. Thus $\alpha'\alpha = \mathrm{id}_N$.

(2) $\Rightarrow$ (1) Define $\delta : M \to L \oplus N$ by $\delta(m) := (\alpha'(m), \beta(m))$.

To see that δ is injective, suppose that $\delta(m) = 0$. Then $\beta(m) = 0$ so $m = \alpha(\ell)$ for some $\ell \in L$ because $\ker\beta = \mathrm{im}(\alpha)$. Also $\alpha'(m) = 0$, so $0 = \alpha'\alpha(\ell) = \ell$, whence $m = \alpha(\ell) = 0$.

To see that δ is surjective, let $\ell \in L$ and $n \in N$. Then $n = \beta(m)$ for some $m \in M$. By Lemma 4.3, $M = \ker\alpha' \oplus \mathrm{im}(\alpha) = \ker\alpha' \oplus \ker\beta$. Hence $m - \alpha(\ell) = u + v$ for some $u \in \ker\alpha'$ and $v \in \ker\beta$. Now $m - u = \alpha(\ell) + v$ so

$$\delta(m - u) = \big(\alpha'(\alpha(\ell) + v), \beta(m - u)\big) = (\ell, n).$$

We have shown that δ is an isomorphism. Also, $\delta(\alpha(\ell)) = (\alpha'\alpha(\ell), \beta\alpha(\ell)) = (\ell, 0)$ and $\beta\delta^{-1}(\alpha'(m), \beta(m)) = \beta(m)$. Thus (1) holds.

We leave the reader to show that (1) $\Leftrightarrow$ (3). □

If the equivalent conditions in the lemma hold we say that the sequence (11-4) splits, or is a split exact sequence, that α is split monic, and that β is split epic.

If the sequence splits, then

$$M = \alpha L \oplus \ker\alpha' = \ker\beta \oplus \beta' N.$$

1.12 Projective and injective modules

An R-module D is projective if $\mathrm{Hom}_R(D, -)$ is an exact functor, i.e., when applied to an exact sequence $0 \to L \to M \to N \to 0$ it produces an exact sequence

$$0 \to \mathrm{Hom}_R(D, L) \to \mathrm{Hom}_R(D, M) \to \mathrm{Hom}_R(D, N) \to 0.$$

Given what has been said above, this is equivalent to the requirement that the map $\mathrm{Hom}_R(D, M) \to \mathrm{Hom}_R(D, N)$ is surjective. In other words, D is projective if for every surjective module homomorphism $f : M \to N$ and every module homomorphism $\alpha : D \to N$, there is a factorization $\alpha = f\beta$ for some module homomorphism $\beta : D \to M$.

Proposition 12.1 *1. A free module is projective.*

2. *A module is projective if and only if it is a direct summand of a free module.*

3. *A module D is projective if and only if for every surjective map $f : M \to D$ there is a map $g : D \to M$ such that $fg = \mathrm{id}_D$.*

Proof. (1) Let F be a free module with basis $\{e_i \mid i \in I\}$. Let $f : M \to N$ be surjective and let $\alpha : F \to N$ be any map. Since f is surjective there are elements $m_i \in M$ such that $f(m_i) = \alpha(e_i)$ for all i. By Theorem 10.5, there is a homomorphism $\psi : F \to M$ such that $\psi(e_i) = m_i$ for all i. It follows that $f\psi(e_i) = f(m_i) = \alpha(e_i)$. Since $f\psi$ and α are module homomorphisms that agree on a set of generators for F, they are equal. Thus $\alpha = f\psi$ as required.

(2) Suppose that D is projective. There is a surjective map $f : F \to D$ from some free module F. By (1), there is a map $g : D \to F$ such that $fg = \mathrm{id}_D$. It now follows from Lemma 4.3 that D is a direct summand of F.

Conversely, suppose that P free and $P = D \oplus E$.Let $\pi : P \to D$ and $\iota : D \to P$ be the maps $\pi(d, e) = d$ and $\alpha(d) = (d, 0)$. Then $\pi\iota = \mathrm{id}_D$. Let $f : M \to N$ be a surjective homomorphism, and $\alpha : D \to N$ an arbitrary module homomorphism. Then $\alpha\pi : P \to N$, so there is a $\delta : P \to M$ such that $\alpha\pi = f\delta$. Hence $f\delta\iota = \alpha\pi\iota = \alpha$, so $\delta\iota : D \to M$ has the required property and we see that D is projective.

(3) If D is projective and $\alpha = \mathrm{id}_D$, there is a $g : D \to M$ such that $\mathrm{id}_D = fg$.

Conversely, suppose that D has this property. There is a surjective map $\psi : F \to D$ from a free module F. By hypothesis, there is a map $g : D \to F$ such that $\psi g = \mathrm{id}_D$. It follows from Lemma 4.3 that $F = \ker\psi \oplus \mathrm{im}(g) \cong \ker\psi \oplus D$, so D is a summand of a free module and hence projective by (2). □

Proposition 12.2 *If N is a projective R-module then every short exact sequence $0 \to L \to M \to N \to 0$ splits.*

Proof. Let $\alpha : L \to M$ and $\beta : M \to N$ be the maps in the short exact sequence. Because N is projective and β is surjective, there is a map $\beta' : N \to M$ such that $\beta\beta' = \mathrm{id}_N$. Hence the sequence splits. □

Remarks. 1. The converse of Proposition 12.2 is also true: if N has the property that every short exact sequence $0 \to L \to M \to N \to 0$ splits, then N is projective. This is because there is such a sequence with M free, so splitting implies that N is (isomorphic to) a direct summand of M, and hence projective.

2. A direct sum of two projective modules is again projective: if P_i, $i = 1, 2$, is a direct summand of a free module F_i, then $P_1 \oplus P_2$ is a direct summand of the free module $F_1 \oplus F_2$.

Injective modules. An R-module E is injective if the functor $\mathrm{Hom}_R(-, E)$ is exact. Injectives are very different from projectives. For one thing, they are rarely finitely generated modules. For example, $\mathbb{Q}$ is an injective $\mathbb{Z}$-module.

There are results for injectives that are analogous to the results we have just proved for projectives. For example, E is injective if and only if for every injective map $f : L \to M$ and every map $\alpha : L \to E$, there is a factoring $\alpha = \beta f$ for some $\beta : M \to E$. Likewise, E is injective if and only if for every injective map $f : E \to M$ there is a map $g : M \to E$ such that $gf = id_E$.

Algebraic K-theory. The group $K_0(R)$ is defined as the quotient of the free abelian group with basis $[P]$, the isomorphism classes of the finitely generated projective left R-modules, modulo the subgroup generated by all $[P] + [Q] - [P \oplus Q]$. Thus, the addition in $K_0(R)$ is given by $[P] + [Q] = [P \oplus Q]$. The identity/zero is $[0]$.

If R is commutative, then $K_0(R)$ also has a multiplication making it a commutative ring. The multiplication is *tensor product*, i.e., $[P].[Q] := [P \otimes_R Q]$.

Tensor product. I haven't defined the tensor product of two modules yet! But perhaps this makes you curious enough to read about it. Here is a very slick and short definition of the tensor product: let M be a right R-module and N a left R-module. Then their tensor product, denoted $M \otimes_R N$, is the unique abelian group with the property that there is an isomorphism of abelian groups

$$\mathrm{Hom}_{\mathbb{Z}}(M \otimes_R N, L) \cong \mathrm{Hom}_R(M, \mathrm{Hom}_{\mathbb{Z}}(N, L)) \qquad (12\text{-}5)$$

for every abelian group L. In even fancier language, the functor $- \otimes_R N : R - \mathsf{Mod} \to \mathsf{Ab}$ is left adjoint to the functor $\mathrm{Hom}_{\mathbb{Z}}(N, -) : \mathsf{Ab} \to R - Mod$.

Let's postpone for a moment the question of whether $M \otimes_R N$ exists, i.e., whether there is an abelian group with the desired property, and try to make sense of the definition. It is implicit in the right-hand side of (12-5) that $\mathrm{Hom}_{\mathbb{Z}}(N, L)$ is a right R-module; we make $\mathrm{Hom}_{\mathbb{Z}}(N, L)$ a right R-module by declaring $(f.r)(n) := f(rn)$ for all abelian group homomorphisms $f : N \to L$, all $r \in R$, and all $n \in N$. One sees easily that $f.r$ is a group homomorphism $N \to L$ so does belong to $\mathrm{Hom}_{\mathbb{Z}}(N, L)$; it is also easy to check that this gives $\mathrm{Hom}_{\mathbb{Z}}(N, L)$ the structure of a right R-module (you should check this at least once in your life). Thus the right-hand side of (12-5) makes sense. The isomorphism in (12-5) is an isomorphism of abelian groups.

Notice that nothing is said about whether or not $M \otimes_R N$ is an R-module; in general it can not be given an R-module structure; all we can say is that it is an abelian group. Notice too that M is a *right* R-module and N is a *left* R-module. One can not tensor together two left modules!

However, if R is commutative then right and left R-modules are the same things so one only speaks of R-modules, and one can tensor together any two R-modules. It is also true that $M \otimes_R N$ can be made into an R-module when R is commutative, and that is why the definition $[M].[N] = [M \otimes_R N]$ makes sense in $K_0(R)$ when R is commutative; of course, we also need to check that $M \otimes_R N$ is finitely generated and projective if M and N are.

We show the existence of $M \otimes_R N$ by showing that the following abelian group gives the isomorphism (12-5):

1.13 Noetherian modules

A module M is noetherian, or has the ascending chain condition, if every chain of submodules $M_1 \subset M_2 \subset \cdots$ is eventually stationary.

Theorem 13.1 *The following conditions on an R-module M are equivalent:*

1. *M is noetherian;*
2. *if $\mathcal{S}$ is a non-empty collection of submodules of M, then $\mathcal{S}$ has a maximal member by which we mean there is an $N \in \mathcal{S}$ such that if $N' \in \mathcal{S}$ and $N \subset N'$, then $N = N'$;*
3. *every submodule of M is finitely generated.*

Proof. (1)⇒(2) Choose $M_1 \in \mathcal{S}$. If M_1 is a maximal member of $\mathcal{S}$, (2) is true. If not, there is an $M_2 \in \mathcal{S}$ that properly contains M_1. If M_2 is a maximal member of $\mathcal{S}$, (2) is true. If not, repeat the process, thus obtaining a chain of submodules $M_1 \subset M_2 \subset \cdots$. By hypothesis, this chain is eventually constant; but that can only happen when we encounter a maximal member of $\mathcal{S}$.

(2)⇒(3) Let L be a submodule of M, and define

$$\mathcal{S} = \{\text{submodules of } L \text{ that are finitely generated}\}.$$

Let N be a maximal member of $\mathcal{S}$. If $N \neq L$, then there is some $\ell \in L \backslash N$. But now $N + R\ell$ is a submodule of L that is finitely generated, so belongs to $\mathcal{S}$, and is strictly larger than N, contradicting the choice of N. We conclude that $L = N$, so (3) holds.

(3)⇒(1) Let $M_1 \subset M_2 \subset \cdots$ be an ascending chain of submodules of M. Set $N = \cup_i M_i$. Then N is a submodule of M, so is finitely generated by hypothesis. But any finite subset of N is contained in some M_j, so some M_j contains a set of generators for N. It follows that $N = M_j$, so the chain becomes constant $M_j = M_{j+1} = \cdots$. Hence M is noetherian. □

Warning: Read part (2) of Theorem 13.1 carefully. It does not say that $\mathcal{S}$ contains a maximal submodule of M (a maximal submodule of M is a submodule

M' that is not equal to M and is not contained in any submodules of M other than itself and M). Nor does it say that $\mathcal{S}$ contains an N that contains all other members of $\mathcal{S}$. For example, if $R = \mathbb{Z}$ and $\mathcal{S} = \{(p^2) \mid p \text{ is a positive prime}\}$, then every member of $\mathcal{S}$ is a maximal member!

Definition 13.2 A ring R is left noetherian if it is noetherian as a left module over itself. A ring R is right noetherian if it is noetherian as a right module over itself. A ring R is noetherian if it is both left and right noetherian. $\Diamond$

A principal ideal domain is noetherian since all its submodules (=ideals!) are generated by one element.

The polynomial ring in n variables over a field is noetherian (see Theorem **??**).

Proposition 13.3 *1. All submodules and quotient modules of a noetherian module are noetherian.*

2. If L and M are noetherian submodules of a module N, then $L + N$ is noetherian.

3. A finite sum of noetherian submodules of a module is noetherian.

4. If N is a submodule of a module M, then M is noetherian if and only if M/N and N are noetherian.

5. A finitely generated left module over a left noetherian ring is noetherian.

Proof. (3) ($\Rightarrow$) Every submodule of M/N is of the form N'/N where N' is a submodule of M containing N. By hypothesis, N' is finitely generated, so N'/N is finitely generated. Hence M/N is noetherian. Every submodule of N is a submodule of M, so is finitely generated. Hence N is noetherian.

($\Leftarrow$) Let $M_1 \subset M_2 \subset \ldots$ be submodules of M. Because N is noetherian, there is an n such that $M_n \cap N = M_{n+1} \cap N = \cdots$. Also the chain of submodules

$$M_1 + N/N \subset M_2 + N/N \subset \cdots$$

in M/N is eventually stable, so $M_n + N = M_{n+1} + N = \cdots$ for n sufficiently large. Hence

$$M_{n+1} = M_{n+1} \cap (M_{n+1} + N) == M_{n+1} \cap (M_n + N) = M_n + (M_{n+1} \cap N)$$

by the modular law. But this equals $M_n + (M_n \cap N) = M_n$, so M is noetherian.

(1) There is an isomorphism $L \oplus M/L \cong M$, so it follows from (3) that $L \oplus M$ is noetherian. But there is a surjective homomorphism $L \oplus M \to L + M$, so $L + M$ is a quotient of a noetherian module, and hence noetherian by (3).

(2) This follows from (1) by induction: write $L_1 + \cdots + L_n = (L_1 + \cdots + L_{n-1}) + L_n$.

(4) Suppose that M is generated by $m_1, \ldots, m_n$. Let $F = Re_1 \oplus \cdots Re_n$ be the free module with basis $e_1, \ldots, e_n$. By (2), F is noetherian because each $Re_i \cong R$ is. And there is a surjective map $F \to M$, $e_i \mapsto m_i$, so M is noetherian by (3). $\square$

1.14 More about simples

One often encounters modules that are direct sums of simple modules, so we record some results about such sums.

Lemma 14.1 *Let N be a cyclic R-module and S a simple R-module. Suppose that S is not isomorphic to a simple quotient of N. Then $N \oplus S$ is a cyclic R-module.*

Proof. Choose generators n and s for N and S respectively, and define $I = \mathrm{Ann}(n)$ and $J = \mathrm{Ann}(s)$. Then J is a maximal left ideal of R, and $I \not\subset J$ because if it were there would be a surjective map $R/I \to R/J$; but $R/I \cong N$ and $R/J \cong S$. Hence $I + J = R$. Write $1 = i + j$ with $i \in I$ and $j \in J$. We now show that (n, s) generates $N \oplus S$. First, $R(n, s)$ contains $i(n, s) = (in, is) = (0, is) = (0, s)$, so $R(n, s)$ contains $R(0, s) = (0, S)$. Similarly, $R(n, s)$ contains $j(n, s) = (n, 0)$, and therefore contains $R(n, 0) = (N, 0)$. Hence $R(n, s)$ contains $(N, 0) + (0, S) = (N, S) = N \oplus S$. □

Lemma 14.2 *Let S be a simple R-module. Let N be an R-module with the property that $\mathrm{Hom}_R(N', S) = 0$ for all submodules $N' \subset N$. If L is a submodule of $N \oplus S$, then $L = K \oplus T$ for submodules $K \subset N$ and $T \subset S$.*

Proof. Let $\pi : N \oplus S \to S$ and $\rho : N \oplus S \to N$ be the projections with kernels N and S respectively. It is clear that $L \subset \rho(L) + \pi(L)$.

If $\pi(L) = 0$, then $L \subset N$ and we are done.

Suppose that $\pi(L) \neq 0$. Then L contains an element of the form (n, s) with $s \neq 0$. By the argument in Lemma 14.1, L contains S. Hence if $\ell = (n', s')$ is any element of L, L contains n'. In other words, $\rho(L) \subset L$. Hence $\rho(L) + S \subset N \subset \rho(L) + \pi(L)$, so $L = \rho(L) + S$, as claimed. □

Lemma 14.3 *Suppose that $M_1, \ldots, M_n$ are non-isomorphic simple modules over a ring R. Then $M := M_1 \oplus \cdots \oplus M_n$ has exactly 2^n submodules, namely $M_I = \sum_{i \in I} M_i$ as I ranges over all subsets of $\{1, \ldots, n\}$.*

Proof. This follows from the previous lemma by induction on n. The result is certainly true when $n = 1$.

Suppose that $n \geq 2$, and let L be a submodule of M. Write $N = M_1 \oplus \cdots \oplus M_{n-1}$ and $S = M_n$. By the previous lemma, $L = N' + T$ where N' is a submodule of N and T is a submodule of M_n. Now apply the induction hypothesis to $N' \subset N$. □