Shandong University | Advanced Modern Algebra

Lecture 4 & 5: Modules

Mar. 17, 2023

Lecturer: Bin Guan

This lecture refers to Chapter 10 in [1]. All the equation numbers without reference labels are from this book.

1 Definitions and examples

1.1 Modules and submodules

We start with the definition of a module.

Definition. *Let R be a ring (not necessarily commutative nor with 1). A **left R-module** or a **left module** over R is a set M together with*

(1) a binary operation $+$ on M under which M is an abelian group, and

(2) an action of R on M (that is, a map $R \times M \to M$) denoted by rm, for all $r \in R$, $m \in M$ which satisfies, for all $r, r' \in R$, $m, m' \in M$, that

$$\text{(a) } (r+r')m = rm + r'm, \quad \text{(b) } (rr')m = r(r'm), \quad \textit{and} \quad \text{(c) } r(m+m') = rm + rm'.$$

If the ring R has a 1 we impose the additional axiom: (d) $1m = m$, *for all $m \in M$.*

If R is a ring with 1 and M is a left R-module, it is obvious that $R^\times$ and M satisfy the two axioms for a group action of the multiplicative group $R^\times$ on the set M (cf. [1] §10.1 Exercise 2).

The descriptor "left" in the above definition indicates that the ring elements appear on the left; "right" R-modules can be defined analogously. If the ring R is commutative and M is a left R-module we can make M into a right R-module by defining $mr := rm$ for $m \in M$ and $r \in R$. If R is not commutative, axiom 2(b) in general will not hold with this definition (so not every left R-module is also a right R-module). Unless explicitly mentioned otherwise the term "module" will always mean "left module".

Modules satisfying axiom 2(d) are called **unital modules**, and in this book all our modules will be unital (this is to avoid "pathologies" such as having $rm = 0$ for all $r \in R$ and $m \in M$).

Let R be a ring and let M be an R-module. An R**-submodule** of M is a subgroup N of M which is closed under the action of ring elements, i.e., $rn \in N$, for all $r \in R$, $n \in N$. Submodules of M are therefore just subsets of M which are themselves modules under the restricted operations. Every R-module M has the two submodules M and 0 (the latter is called the trivial submodule).

Example. *When R is a field F, the axioms for an R-module are precisely the same as those for a vector space over F, so that modules over a field F and vector spaces over F are the same; submodules are the same as subspaces.*

Example. *Let R be any ring. Then $M = R$ is a left R-module, where the action of a ring element on a module element is just the usual multiplication in the ring R (similarly, R is a right module over itself). In particular, every field can be considered as a (1-dimensional) vector space over itself.*

When R is considered as a left module over itself in this fashion, the submodules of R are precisely the left ideals of R (and if R is considered as a right R-module over itself, its submodules are the right ideals). Thus if R is not commutative it has a left and right module structure over itself and these structures may be different (e.g., the submodules may be different, cf. [1] §10.1 Exercise 21).

The same abelian group may have the structure of an R-module for a number of different rings R and each of these module structures may carry useful information. Specifically, if M is an R-module and S is a subring of R with $1_S = 1_R$, then M is automatically an S-module as well. For instance the field $\mathbb{R}$ is an $\mathbb{R}$-module, a $\mathbb{Q}$-module and a $\mathbb{Z}$-module.

1.2 $\mathbb{Z}$-modules

Let $R = \mathbb{Z}$, let A be any abelian group (finite or infinite) and write the operation of A as $+$. Make A into a $\mathbb{Z}$-module as follows: for any $n \in Z$ and $a \in A$ define

$$na := \begin{cases} a + a + \cdots + a \ (n \text{ times}) & \text{if } n > 0 \\ 0 \ (\text{the identity of } A) & \text{if } n = 0 \\ -a - a - \cdots - a \ (|n| \text{ times}) & \text{if } n < 0. \end{cases}$$

This definition of an action of the integers on A makes A into a $\mathbb{Z}$-module, and the module axioms show that this is the only possible action of $\mathbb{Z}$ on A making it a (unital) $\mathbb{Z}$-module. Thus every abelian group is a $\mathbb{Z}$-module.

Conversely, if M is any $\mathbb{Z}$-module, a fortiori M is an abelian group, so

$$\mathbb{Z}\text{-modules are the same as abelian groups.}$$

Furthermore, it is immediate from the definition that

$$\mathbb{Z}\text{-submodules are the same as subgroups.}$$

Note that since $\mathbb{Z}$ is commutative these definitions of left and right actions by ring elements give the same module structure.

If A is an abelian group containing an element x of finite order n then $nx = 0$. Thus, in contrast to vector spaces, a $\mathbb{Z}$-module may have nonzero elements x such that $nx = 0$ for some nonzero ring element n. In particular, if A has order m, then by Lagrange's Theorem (cf. [1] §3.2 Corollary 9) $mx = 0$, for all $x \in A$. Note that then A is a module over $\mathbb{Z}/m\mathbb{Z}$.

In particular, if p is a prime and A is an abelian group (written additively) such that $px = 0$ for all $x \in A$, then A is a $\mathbb{Z}/p\mathbb{Z}$-module, i.e., can be considered as a vector space over the field $\mathbb{F}_p \coloneqq \mathbb{Z}/p\mathbb{Z}$. For instance, the Klein 4-group is a (2-dimensional) vector space over $\mathbb{F}_2$.

Exercise ([1] §10.1 Exercise 9)**.** *Let R be any ring and M be a left R-module. If N is a submodule of M, the* ***annihilator*** *of N in R is defined to be*

$$\mathrm{Ann}(N) \coloneqq \{r \in R \mid rn = 0 \textit{ for all } n \in N\}.$$

Prove that the annihilator of N in R is a 2-sided ideal of R.

In general, if R is any ring and M is an R-module, and for some (2-sided) ideal I of R, $am = 0$ for all $a \in I$ and all $m \in M$ (i.e. $I \subseteq \mathrm{Ann}(M)$), we say M is **annihilated by** I. In this situation we can make M into an R/I-module by defining an action of the quotient ring R/I on M as follows: for each $m \in M$ and coset $r + I$ in R/I let

$$(r + I)m \coloneqq rm.$$

Since $am = 0$ for all $a \in I$ and $m \in M$, this is well defined and one easily checks that it makes M into an R/I-module.

In particular, when I is a maximal ideal in the commutative ring R and $IM = 0$, then M is a vector space over the field R/I.

Exercise ([1] §10.1 Exercise 15)**.** *If M is a finite abelian group then M is naturally a $\mathbb{Z}$-module. Can this action be extended to make M into a $\mathbb{Q}$-module?*

1.3 $F[x]$-modules

Let F be a field, let x be an indeterminate and let R be the polynomial ring $F[x]$. Let V be a vector space over F and let T be a linear transformation from V to V. We have already seen that V is an F-module; the linear map T will enable us to make V into an $F[x]$-module.

Let $p(x)$ be the polynomial

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

where $a_0, \ldots, a_n \in F$. For each $v \in V$ define an action of the ring element $p(x)$ on the module element v by

$$\begin{aligned} p(x)v &\coloneqq (a_n T^n + a_{n-1}T^{n-1} + \cdots + a_1 T + a_0 I)(v) \\ &= a_n T^n(v) + a_{n-1}T^{n-1}(v) + \cdots + a_1 T(v) + a_0 v, \end{aligned}$$

i.e., $p(x)$ acts by substituting the linear transformation T for x in $p(x)$ and applying the resulting linear transformation to v. Put another way, x acts on V as the linear transformation T and we

extend this to an action of all of $F[x]$ on V in a natural way. It is easy to check that this definition of an action of $F[x]$ on V satisfies all the module axioms and makes V into an $F[x]$-module.

The field F is naturally a subring of $F[x]$ (the constant polynomials) and the action of these field elements is by definition the same as their action when viewed as constant polynomials. In other words, the definition of the $F[x]$-action on V is consistent with the given action of the field F on the vector space V, i.e., the definition **extends** the action of F to an action of the larger ring $F[x]$.

The way $F[x]$ acts on V depends on the choice of T so that there are in general many different $F[x]$-module structures on the same vector space V. (In general, an abelian group M may have many different R-module structures, even if the ring R does not vary, in the same way that a given group G may act in many ways as a permutation group on some fixed set Ω.) For instance, if $T = 0$, then $p(x)v = a_0v$, that is, the polynomial $p(x)$ acts on v simply by multiplying by the constant term of $p(x)$, so that the $F[x]$-module structure is just the F-module structure. If, on the other hand, T is the identity transformation (so $T^n(v) = v$ for all n and v), then $p(x)v = a_nv + a_{n-1}v + \cdots + a_0v = (a_n + \cdots + a_0)v$, so that now $p(x)$ multiplies v by the sum of the coefficients of $p(x)$.

Exercise. *For the above two examples, find the annihilators of V in $F[x]$. (Recall that $F[x]$ is a Principal Ideal Domain, so you shall write $\mathrm{Ann}(V)$ as a principal ideal of $F[x]$.)*

Example. *Let $n \in \mathbb{Z}_{>0}$ and let*

$$V = F^n \coloneqq \{(t_1, t_2, \ldots, t_n) \mid t_i \in F \text{ for all } i\}$$

*be the **affine n-space** over F. Let T be the "shift operator"*

$$T(t_1, t_2, \ldots, t_n) \coloneqq (t_2, t_3, \ldots, t_n, 0).$$

Let e_i be the usual i^{th} basis vector $(0, 0, \ldots, 0, 1, 0, \ldots, 0)$ where the 1 is in position i. Then

$$T^k(e_i) = \begin{cases} e_{i-k} & \text{if } i > k \\ 0 & \text{if } i \leq k \end{cases}$$

so for example, if $m < n$,

$$(a_mx^m + a_{m-1}x^{m-1} + \cdots + a_0)(0, 0, \ldots, 1) = (0, \ldots, 0, a_m, a_{m-1}, \ldots, a_0).$$

From this we can determine the action of any polynomial on any vector.

The construction of an $F[x]$-module from a vector space V over F and a linear transformation T from V to V in fact describes all $F[x]$-modules; namely, an $F[x]$-module is a vector space together with a linear transformation which specifies the action of x. This is because if V is any $F[x]$-module, then V is an F-module and the action of the ring element x on V is a linear transformation from V to V. The axioms for a module ensure that the actions of F and x on V uniquely determine the action of any element of $F[x]$ on V. Thus there is a bijection between the collection of $F[x]$-modules and the collection of pairs (V, T)

$$\left\{ \begin{array}{c} V \text{ an } F[x]\text{-module} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} V \text{ a vector space over } F \\ \text{and} \\ T : V \to V \text{ a linear transformation} \end{array} \right\}$$

given by

$$\text{the element } x \text{ acts on } V \text{ as the linear transformation } T.$$

Now we consider $F[x]$-submodules of V where, as above, V is any $F[x]$-module and T is the linear transformation from V to V given by the action of x. An $F[x]$-submodule W of V must first be an F-submodule, i.e., W must be a vector subspace of V. Secondly, W must be sent to itself under the action of the ring element x, i.e., we must have $T(w) \in W$ for all $w \in W$. Any vector subspace U of V such that $T(U) \subseteq U$ is called **T-stable** or **T-invariant**.

If U is any T-stable subspace of V, it follows that $T^n(U) \subseteq U$ for all $n \in \mathbb{Z}_{\geq 0}$. Moreover any linear combination of powers of T then sends U into U, so that U is also stable by the action of any polynomial in T. Thus U is an $F[x]$-submodule of V. This shows that the $F[x]$-submodules of V are precisely the T-stable subspaces of V.

In terms of the bijection above,

$$\left\{ \begin{array}{c} W \text{ an } F[x]\text{-submodule of } V \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} W \text{ a subspace of } V \\ \text{and} \\ W \text{ is } T\text{-stable} \end{array} \right\}$$

which gives a complete dictionary between $F[x]$-modules V and vector spaces V together with a given linear transformation T from V to V.

Example. *If T is the shift operator defined on affine n-space $V = F^n$ and k is any integer in the range $0 \leq k \leq n$, then the subspace*

$$U_k = \{(t_1, t_2, \ldots, t_k, 0, \ldots, 0) \mid t_i \in F\} \cong F^k$$

is clearly T-stable so is an $F[x]$-submodule of V.

We shall see in [1] Chapter 12 that the relatively simple ideal structure of the ring $F[x]$ (recall that $F[x]$ is a Principal Ideal Domain) forces the $F[x]$-module structure of V to be correspondingly uncomplicated, and this in tern provides a great deal of information about the linear transformation T (in particular, gives some nice matrix representations for T: its rational canonical form and its Jordan canonical form). Moreover, the same arguments which classify finitely generated $F[x]$-modules apply to any Principal Ideal Domain R, and when these are invoked for $R = \mathbb{Z}$, we obtain the Fundamental Theorem of Finitely Generated Abelian Groups. These results generalize the theorem that every finite dimensional vector space has a basis.

1.4 Algebras over a ring

Definition. *Let R be a commutative ring with identity. An R-algebra is a ring A with identity together with a ring homomorphism $f : R \to A$ mapping 1_R to 1_A such that the subring $f(R)$ of A is contained in the center of A.*

If A is an R-algebra then it is easy to check that A has a natural left and right (unital) R-module structure defined by $r \cdot a = a \cdot r \coloneqq f(r)a$ where $f(r)a$ is just the multiplication in the ring A (and this is the same as $af(r)$ since by assumption $f(r)$ lies in the center of A). In general it is possible for an R-algebra A to have other left (or right) R-module structures, but unless otherwise stated, this natural module structure on an algebra will be assumed.

Example. *For any ring A with identity, if R is a (commutative) subring of the center of A containing the identity of A, then A is an R-algebra. In particular, a commutative ring A containing 1 is an R-algebra for any subring R of A containing 1.*

*For example, let R be a commutative ring with identity. the polynomial ring $R[x_1, \ldots, x_n]$ is an R-algebra, and the group ring RG for a finite group G is an R-algebra. Recall that the **group***

***ring**, RG, of a finite group G with coefficients in R is the set of all formal sums $\sum_{g\in G} a_g g$ for all $a_g \in R$, with addition defined "componentwise" and multiplication extended by the distributive laws from the product in G.*

Example. *When $R = F$ is a field, F is isomorphic to its image under f (because $\ker f$ is an ideal of F but F only have trivial ideals), so we can identify F itself as a subring of A. Hence, saying that A is an algebra over a field F is the same as saying that the ring A contains the field F in its center and the identity of A and of F are the same.*

Suppose that A is an R-algebra. Then A is a ring with identity that is a (unital) left R-module satisfying $r \cdot (ab) = (r \cdot a)b = a(r \cdot b)$ for all $r \in R$ and $a, b \in A$ (these are all equal to the product $f(r)ab$ in the ring A — recall that $f(R)$ is contained in the center of A). Conversely, these conditions on a ring A define an R-algebra, and are sometimes used as the definition of an R-algebra (cf. [1] §10.1 Exercise 22).

Example. *Any ring with identity is a $\mathbb{Z}$-algebra.*

If A and B are two R-algebras, an R-algebra **homomorphism** (or **isomorphism**) is a ring homomorphism (isomorphism, respectively) $\varphi : A \to B$ mapping 1_A to 1_B such that $\varphi(r \cdot a) = r \cdot \varphi(a)$ for all $r \in R$ and $a \in A$.

1.5 Module homomorphisms

Let R be a ring and let M and N be R-modules. A map $\varphi : M \to N$ is an **R-module homomorphism** if it respects the R-module structures of M and N, i.e.,

$$\text{(a) } \varphi(m + m') = \varphi(m) + \varphi(m') \quad \text{and} \quad \text{(b) } \varphi(rm) = r\varphi(m)$$

for all $r \in R$ and $m, m' \in M$.

Any R-module homomorphism is also a homomorphism of the additive groups, but not every group homomorphism need be a module homomorphism (because condition (b) may not be satisfied).

Example. *$\mathbb{Z}$-module homomorphisms are the same as abelian group homomorphisms: For the ring $R = \mathbb{Z}$ the action of ring elements (integers) on any $\mathbb{Z}$-module amounts to just adding and subtracting within the (additive) abelian group structure of the module so that in this case condition* (b) *of a homomorphism is implied by condition* (a)*. For example, $\varphi(2x) = \varphi(x + x) = \varphi(x) + \varphi(x) = 2\varphi(x)$, etc.*

Example. *If $R = F$ is a field, F-module homomorphisms are the same as linear transformations.*

An R-module homomorphism is an **isomorphism** (of R-modules) if it is both injective and surjective. The modules M and N are said to be isomorphic, denoted $M \cong N$, if there is some R-module isomorphism $\varphi : M \to N$.

It is an easy exercise to show that the relation "is R-module isomorphic to" is an equivalence relation on any set of R-modules (cf. [1] §10.2 Exercise 2). The unqualified term "isomorphism" when applied to R-modules will always mean R-module isomorphism. (When the symbol $\cong$ is used without qualification it will denote an isomorphism of the respective structures.)

Remark. *If R is a ring and $M = R$ is a module over itself, then R-module homomorphisms (even from R to itself) need not be ring homomorphisms, and ring homomorphisms need not be R-module homomorphisms. For example, when $R = \mathbb{Z}$ the $\mathbb{Z}$-module homomorphism $x \mapsto 2x$ is not a ring homomorphism (1 does not map to 1). When $R = F[x]$ the ring homomorphism $\varphi : f(x) \mapsto f(x^2)$ is not an $F[x]$-module homomorphism (if it were, we would have $x^2 = \varphi(x) = \varphi(x \cdot 1) = x\varphi(1) = x$).*

Proposition ([1] §10.2 Proposition 2)**.** *Let M, N and L be R-modules and define $\mathrm{Hom}_R(M,N)$ to be the set of all R-module homomorphisms from M to N.*

- *For $\varphi, \psi \in \mathrm{Hom}_R(M,N)$, define $\varphi + \psi$ by*

$$(\varphi+\psi)(m) \coloneqq \varphi(m) + \psi(m) \quad \textit{for all } m \in M.$$

  Then $\varphi + \psi \in \mathrm{Hom}_R(M,N)$ and with this operation $\mathrm{Hom}_R(M,N)$ is an abelian group.

- *If R is a commutative ring then for $r \in R$ define $r\varphi$ by*

$$(r\varphi)(m) \coloneqq r(\varphi(m)) \quad \textit{for all } m \in M.$$

  Then $r\varphi \in \mathrm{Hom}_R(M,N)$ and, with this action of the commutative ring R, the abelian group $\mathrm{Hom}_R(M,N)$ is an R-module.

- *If $\varphi \in \mathrm{Hom}_R(L,M)$ and $\psi \in \mathrm{Hom}_R(M,N)$, then $\psi \circ \varphi \in \mathrm{Hom}_R(L,N)$.*

- *With addition as above and multiplication defined as function composition, $\mathrm{Hom}_R(M,M)$ is a ring with 1, which is called the **endomorphism ring** of M and will often be denoted by $\mathrm{End}_R(M)$ (or just $\mathrm{End}(M)$ when the ring R is clear from the context). Elements of $\mathrm{End}(M)$ are called **endomorphisms**. When R is commutative $\mathrm{End}(M)$ is an R-algebra.*

Exercise ([1] §10.2 Exercises 9 & 10)**.** *Let R be a commutative ring with 1. Prove that $f \mapsto f(1)$ defines an isomorphism $\mathrm{Hom}_R(R,M) \cong M$ of left R-modules; and prove that $\mathrm{Hom}_R(R,R)$ and R are isomorphic as rings.*

When R is commutative there is a natural map from R into $\mathrm{End}(M)$ given by $r \mapsto r\mathbf{1}$, where the latter endomorphism of M is just multiplication by r on M. The image of R is contained in the center of $\mathrm{End}(M)$, so if R has an identity, $\mathrm{End}(M)$ is an R-algebra.

The ring homomorphism (cf. [1] §10.2 Exercise 7) from R to $\mathrm{End}(M)$ may not be injective, since for some r we may have $rm = 0$ for all $m \in M$ (e.g., $R = \mathbb{Z}$, $M = \mathbb{Z}/2\mathbb{Z}$, and $r = 2$). When R is a field, however, this map is injective (in general, no unit is in the kernel of this map), and the copy of R in $\mathrm{End}_R(M)$ is called the (subring of) **scalar transformations**.

1.6 Quotient modules

If $\varphi : M \to N$ is an R-module homomorphism, let $\ker\varphi \coloneqq \{m \in M \mid \varphi(m) = 0\}$ (the **kernel** of φ) and let $\varphi(M) \coloneqq \{n \in N \mid n = \varphi(m) \text{ for some } m \in M\}$ (the **image** of φ, as usual). It is an easy exercise to show that kernels and images of R-module homomorphisms are submodules.

The next proposition shows that, every submodule N of an R-module M is "normal" in the sense that we can always form the quotient module M/N, and the natural projection $\pi : M \twoheadrightarrow M/N$ is an R-module homomorphism with kernel N.

The proof of this fact and, more generally, the subsequent proofs of the isomorphism theorems for modules follow easily from the corresponding facts for groups. The reason for this is because a module is first of all an abelian group and so every submodule is automatically a normal subgroup, and any module homomorphism is, in particular, a homomorphism of abelian groups.

What remains to be proved in order to extend results on abelian groups to corresponding results on modules is to check that, the action of R is compatible with these group quotients and homomorphisms. For example, the map π above was shown to be a group homomorphism in [1] Chapter 3, but the abelian group M/N must be shown to be an R-module (i.e. to have an action by R) and property (b) in the definition of a module homomorphism must be checked for π.

Proposition ([1] §10.2 Proposition 3)**.** *Let R be a ring, M be an R-module and N be a submodule of M. The (additive, abelian) quotient group M/N can be made into an R-module by defining an action of elements of R by*

$$r(x+N) \coloneqq (rx)+N \quad \textit{for all } r \in R,\ x+N \in M/N.$$

The natural projection map $\pi : M \twoheadrightarrow M/N$ defined by $\pi(x) \coloneqq x+N$ is an R-module homomorphism with kernel N.

Proof. Based on the results on quotient groups ([1] §3.1 Propositions 5 & 7) we only need to check that

- the action of the ring element r on the coset $x+N$ is well defined,
- the axioms 2(a) $\sim$ 2(d) for an R-module hold for the action of R on M/N, and
- the group homomorphism π is a module homomorphism, i.e., $\pi(rm) = r\pi(m)$.

□

All the isomorphism theorems stated for groups also hold for R-modules. The proofs are similar to that of the proposition above in that they begin by invoking the corresponding theorem for groups and then prove that the group homomorphisms are also R-module homomorphisms.

Theorem ([1] §10.2 Theorem 4(1), the First Isomorphism Theorem for Modules)**.**
Let R be a ring, M, N be R-modules and let $\varphi : M \to N$ be an R-module homomorphism. Then

$$M/\ker\varphi \cong \varphi(M).$$

Theorem ([1] §10.2 Theorem 4(2), the Second Isomorphism Theorem)**.** *Let R be a ring, A, B be submodules of the R-module M. Define the **sum** of A and B to be the set*

$$A+B \coloneqq \{a+b \mid a \in A,\ b \in B\}.$$

Then $A+B$ is also a submodule (it is the smallest submodule which contains both A and B), and

$$(A+B)/B \cong A/(A \cap B).$$

Theorem ([1] §10.2 Theorem 4(3)(4), the Third Isomorphism Theorem)**.** *Let R be a ring, N be a submodule of the R-module M. Then there is a bijection*

$$\{A :\ \textit{a submodule of } M \textit{ s.t. } A \supseteq N\} \longleftrightarrow \{A/N :\ \textit{a submodule of } M/N\}\,.$$

The correspondence is given by

$$A \mapsto A/N \quad \textit{for all } A \supseteq N.$$

This correspondence commutes with the processes of taking sums and intersections; and

$$(M/N)/(A/N) \cong M/A.$$

2 Direct sums and free modules

As in the preceding sections the term "module" will mean "left module".

2.1 Direct sums

Let R be a ring with 1 and let $n \in \mathbb{Z}_{>0}$. Following the example about affine spaces over a field, define

$$R^n \coloneqq \{(r_1, r_2, \ldots, r_n) \mid r_i \in R \text{ for all } i\}.$$

Make R^n into an R-module by componentwise addition and multiplication by elements of R in the same manner as when R was a field. The module R^n is called the **free module** of **rank** n over R.

An obvious submodule of R^n is given by the i^{th} component, namely the set of n-tuples with arbitrary ring elements in the i^{th} component and zeros in the j^{th} component for all $j \neq i$. This submodule is isomorphic to R. One easily checks that for each $i \in \{1, \ldots, n\}$ the projection map

$$\pi_i : R^n \twoheadrightarrow R \quad \text{by} \quad \pi_i(r_1, \ldots, r_n) \coloneqq r_i$$

is a surjective R-module homomorphism with kernel equal to the submodule of n-tuples which have a zero in position i.

In general, let $M_1, \ldots, M_k$ be a collection of R-modules. The set of k-tuples $(m_1, m_2, \ldots, m_k)$ where $m_i \in M_i$ with addition and action of R defined componentwise is called the **direct product** or the (**external**) **direct sum** of $M_1, \ldots, M_k$, denoted $M_1 \times \cdots \times M_k$ or $M_1 \oplus \cdots \oplus M_k$.

It is evident that the direct product of a collection of R-modules is again an R-module. The direct product and direct sum of an infinite number of modules (which are different in general) are defined in [1] §10.3 Exercise 20.

Analogous to the direct product of groups, the next proposition indicates when a module is isomorphic to the direct product of some of its submodules.

Proposition ([1] §10.3 Proposition 5, the internal direct sum)**.** *Let $N_1, N_2, \ldots, N_k$ be submodules of the R-module M. The **sum** of $N_1, \ldots, N_k$ is the set of all finite sums of elements from the sets N_i:*

$$N_1 + \cdots + N_k \coloneqq \{a_1 + a_2 + \cdots + a_k \mid a_i \in N_i \textit{ for all } i\}.$$

Then TFAE (the following are equivalent):

(1) The map $\pi : N_1 \times \cdots \times N_k \to M$ defined by

$$(a_1, a_2, \ldots, a_k) \mapsto a_1 + a_2 + \cdots + a_k$$

is an injective homomorphism (of R-modules) and $N_1 \times \cdots \times N_k \cong N_1 + \cdots + N_k$.

(2) $N_j \cap (N_1 + \cdots + \widehat{N_j} + \cdots + N_k) = 0$ for all $j \in \{1, 2, \ldots, k\}$.

(3) Every $x \in N_1 + \cdots + N_k$ can be written uniquely in the form $a_1 + a_2 + \cdots + a_k$ with $a_i \in N_i$.

If an R-module $M = N_1 + \cdots + N_k$ is the sum of submodules $N_1, N_2, \ldots, N_k$ of M satisfying the equivalent conditions of the proposition above, then M is said to be the (**internal**) **direct sum** of $N_1, \ldots, N_k$, written $M = N_1 \oplus \cdots \oplus N_k$.

Part (1) of the above proposition is the statement that the internal direct sum of $N_1, N_2, \ldots, N_k$ is isomorphic to their external direct sum, which is the reason we identify them and use the same notation for both.

Part (3) of the proposition says that, $M = N_1 \oplus \cdots \oplus N_k$ is equivalent to the assertion that every element m of M can be written uniquely as a sum of elements $m = a_1 + a_2 + \cdots + a_k$ with $a_i \in N_i$.

2.2 Generation of modules

Definition. *Let R be a ring with 1, and M be an R-module. A submodule N of M (possibly $N = M$) is **cyclic** if N is generated by one element, i.e., there exists an element $a \in M$ such that*

$$N = Ra = \{ra \mid r \in R\}.$$

If N is a submodule of M (possibly $N = M$) and

$$N = RA \coloneqq \{r_1a_1 + \cdots + r_ka_k \mid r_1, \ldots, r_k \in R,\ a_1, \ldots, a_k \in A,\ k \in \mathbb{Z}_{>0}\}$$

*(where by convention $RA \coloneqq \{0\}$ if $A = \emptyset$) for some subset A of M, we call A a **set of generators** or **generating set** for N, and we say N is the submodule of M **generated** by A.*

*A submodule N of M (possibly $N = M$) is **finitely generated** if there is some finite subset $A = \{a_1, a_2, \ldots, a_n\}$ of M such that $N = RA$, that is, if N is generated by some finite subset. In this case we shall write $Ra_1 + Ra_2 + \cdots + Ra_n$ for RA. Note that cyclic modules are, a fortiori, finitely generated.*

Note that these definitions do not require that the ring R contain a 1, however this condition ensures that A is contained in RA. It is easy to see that for any subset A of M, RA is indeed a submodule of M and is the smallest submodule of M which contains A.

In particular, for submodules $N_1, \ldots, N_n$ of M, $N_1 + \cdots + N_n$ is just the submodule generated by the set $N_1 \cup \cdots \cup N_n$ and is the smallest submodule of M containing N_i for all i. If $N_1, \ldots, N_n$ are generated by sets $A_1, \ldots, A_n$ respectively, then $N_1 + \cdots + N_n$ is generated by $A_1 \cup \cdots \cup A_n$.

Example. *Let $R = \mathbb{Z}$ and let M be any R-module, that is, any abelian group.*

If $a \in M$, then $\mathbb{Z}a$ is just the cyclic subgroup $\langle a \rangle$ of M generated by a.

More generally, M is generated as a $\mathbb{Z}$-module by a set A if and only if M is generated as a group by A (that is, the action of ring elements in this instance produces no elements that cannot already be obtained from A by addition and subtraction).

The definition of finitely generated for $\mathbb{Z}$-modules is identical to that for abelian groups.

Example. *Let R be a ring with 1 and let M be the (left) R-module R itself.*

Note that R is a finitely generated, in fact cyclic, R-module because $R = R1$.

Recall that the submodules of R are precisely the left ideals of R, so saying I is a cyclic R-submodule of the left R-module R is the same as saying I is a principal ideal of R. Also, saying I is a finitely generated R-submodule of R is the same as saying I is a finitely generated ideal.

When R is a commutative ring we often write $(A) \coloneqq RA = AR$ or $(a) \coloneqq Ra = aR$ for the submodule (ideal) generated by A or a respectively. Thus a Principal Ideal Domain is a (commutative) integral domain R with identity in which every R-submodule of R is cyclic.

Submodules of a finitely generated module need not be finitely generated: take M to be the cyclic R-module R itself where $R = F[x_1, x_2, x_3, \ldots]$ is the polynomial ring in infinitely many variables with coefficients in some field F. The submodule (i.e., 2-sided ideal) generated by $\{x_1, x_2, \ldots\}$ cannot be generated by any finite set (note that one must show that no finite subset of this ideal will generate it).

The process of generating submodules of an R-module M by taking subsets A of M and forming all finite "R-linear combinations" of elements of A will be our primary way of producing submodules (this notion is perhaps familiar from vector space theory where it is referred to as taking the **span** of A).

Exercise ([1] §10.3 Exercise 9)**.** *Let R be a ring. A nonzero R-module M is said to be **irreducible** (or **simple**) if its only submodules are 0 and M; otherwise M is called **reducible**. Show that M is irreducible if and only if $M \neq 0$ and M is a cyclic module with any nonzero element as generator. Determine all the irreducible $\mathbb{Z}$-modules.*

2.3 Free modules

Let R be a ring with 1 and let $M = R^n$ be the free module of rank n over R. Then M is the external direct sum of n copies of R. For each $i \in \{1, 2, \ldots, n\}$ let $e_i = (0, 0, \ldots, 0, 1, 0, \ldots, 0)$, where the 1 appears in position i. Since

$$(s_1, s_2, \ldots, s_n) = \sum_{i=1}^{n} s_i e_i,$$

it is clear that M is generated by $\{e_1, e_2, \ldots, e_n\}$, and

$$\begin{aligned} R^n &= R \oplus R \oplus \cdots \oplus R \quad \text{(external direct sum)} \\ &= Re_1 \oplus Re_2 \oplus \cdots \oplus Re_n \quad \text{(internal direct sum)}. \end{aligned}$$

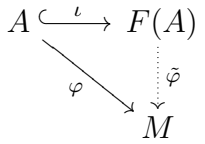
In general, an R-module F is said to be **free** on the subset A of F if for every nonzero element x of F, there exist unique nonzero elements $r_1, r_2, \ldots, r_n$ of R and unique $a_1, a_2, \ldots, a_n$ in A such that $x = r_1a_1 + r_2a_2 + \cdots + r_na_n$ for some $n \in \mathbb{Z}_{>0}$. In this situation we say A is a **basis** or **set of free generators** for F. If R is a commutative ring the cardinality of A is called the **rank** of F.

Remark. *One should be careful to note the difference between the uniqueness property of direct sums ([1] §10.3 Proposition 5(3)) and the uniqueness property of free modules. Namely, in the direct sum of two modules, say $N_1 \oplus N_2$, each element can be written uniquely as $n_1 + n_2$; here the uniqueness refers to the module elements n_1 and n_2. In the case of free modules, the uniqueness is on the ring elements as well as the module elements.*

For example, if $R = \mathbb{Z}$ and $N_1 = N_2 = \mathbb{Z}/2\mathbb{Z}$, then each element of $N_1 \oplus N_2$ has a unique representation in the form $n_1 + n_2$ where each $n_i \in N_i$; however n_1 (for instance) can be expressed as n_1 or $3n_1$ or $5n_1$ ... etc., so each element does not have a unique representation in the form $r_1a_1 + r_2a_2$, where $r_1, r_2 \in R$, $a_1 \in N_1$ and $a_2 \in N_2$. Thus $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is not a free $\mathbb{Z}$-module on the generating set $\{(1, 0), (0, 1)\}$. Similarly, it is not free on any set.

Theorem ([1] §10.3 Theorem 6)**.** *(1) For any set A there is a free R-module $F(A)$ on the set A.*

(2) (The universal property) *If M is any R-module and $\varphi : A \to M$ is any map of sets, then there is a unique R-module homomorphism $\tilde{\varphi} : F(A) \to M$ such that $\tilde{\varphi}(a) = \varphi(a)$ for all $a \in A$, that is, the following diagram commutes.*



If F_1 and F_2 are free modules on the same set A, there is a unique isomorphism between F_1 and F_2 which is the identity map on A.

(3) When $A = \{a_1, a_2, \ldots, a_n\}$ is a finite set, $F(A) = Ra_1 \oplus Ra_2 \oplus \cdots \oplus Ra_n \cong R^n$.

Example. *When $R = \mathbb{Z}$, the free module on a set A is called the **free abelian group** on A. If $|A| = n$, $F(A)$ is called the **free abelian group** of **rank** n and is isomorphic to $\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ (n times).*

Proof of the universal property. Let $F(A) = \{0\}$ if $A = \emptyset$. If A is nonempty let $F(A)$ be the collection of all set functions $f : A \to R$ such that $f(a) = 0$ for all but finitely many $a \in A$. Make

$F(A)$ into an R-module by pointwise addition of functions and pointwise multiplication of a ring element times a function, i.e.,

$$(f+g)(a) \coloneqq f(a)+g(a) \quad \text{and} \quad (rf)(a) = r(f(a))$$

for all $a \in A$, $r \in R$ and $f, g \in F(A)$. It is an easy matter to check that all the R-module axioms hold (the details are omitted).

Identify A as a subset of $F(A)$ by $a \mapsto f_a$, where f_a is the (characteristic) function which is 1 at a and zero elsewhere. We can, in this way, think of $F(A)$ as all finite R-linear combinations of elements of A by identifying each function f with the sum $r_1a_1 + r_2a_2 + \cdots + r_na_n$, where $r_i \coloneqq f(a_i)$ and f takes on the value zero at all other elements of A. Moreover, each element of $F(A)$ has a unique expression as such a formal sum.

To establish the universal property of $F(A)$, suppose $\varphi : A \to M$ is a map of the set A into the R-module M. Define $\tilde{\varphi} : F(A) \to M$ by

$$\tilde{\varphi} : \sum_{i=1}^{n} r_i a_i \mapsto \sum_{i=1}^{n} r_i \varphi(a_i).$$

By the uniqueness of the expression for the elements of $F(A)$ as linear combinations of the a_i we see easily that $\tilde{\varphi}$ is a well defined R-module homomorphism (the details are omitted). By definition, the restriction of $\tilde{\varphi}$ to A equals φ. Finally, since $F(A)$ is generated by A, once we know the values of an R-module homomorphism on A its values on every element of $F(A)$ are uniquely determined, so $\tilde{\varphi}$ is the unique extension of φ to all of $F(A)$. □

If F is a free R-module with basis A, we shall often (particularly in the case of vector spaces) define R-module homomorphisms from F into other R-modules simply by specifying their values on the elements of A and then saying "extend by linearity".

Exercise ([1] §10.3 Exercise 13 & 14)**.** *Let R be a commutative ring with 1, M be a left R-module, and F be the free R-module of rank n. Prove that*

$$\mathrm{Hom}_R(F, R) \cong F \quad \textit{and} \quad \mathrm{Hom}_R(F, M) \cong M \times \cdots \times M \ (n \textit{ times}).$$

3 Tensor products of modules

3.1 Bimodules

In this section we study the tensor product of two modules M and N over a ring R (not necessarily commutative) containing 1. We first consider the general construction of $M \otimes_R N$ as an abelian group, after which we shall return to the question of when this abelian group can be given a module structure.

Definition. *Suppose that N is a left R-module and that M is a right R-module. The quotient of the free $\mathbb{Z}$-module on the set $M \times N$ by the subgroup generated by all elements of the form*

$$\begin{gathered} (m_1+m_2, n) - (m_1, n) - (m_2, n), \\ (m, n_1+n_2) - (m, n_1) - (m, n_2), \quad \textit{and} \\ (mr, n) - (m, rn), \end{gathered} \tag{10.6}$$

*for $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$ and $r \in R$ is an abelian group, denoted by $M \otimes_R N$, or simply $M \otimes N$ if the ring R is clear from the context, and is called the **tensor product** of M and N over R.*

*The elements of $M \otimes_R N$ are called **tensors**, and the coset, $m \otimes n$, of (m, n) in $M \otimes_R N$ is called a **simple tensor**. We have the relations*

$$\begin{gathered}(m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n, \\ m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2, \quad \textit{and} \\ (mr) \otimes n = m \otimes (rn).\end{gathered} \tag{10.7}$$

Every tensor can be written (non-uniquely in general) as a finite sum of simple tensors.

Let S be any ring with 1 and we try to equip $M \otimes_R N$ with a left S-module structure. This involves defining $s(m \otimes n)$, i.e., the action of a ring element $s \in S$ on a tensor $m \otimes n$ in $M \otimes_R N$. One possible approach is to give M a left S-module structure so that we can define $s(m \otimes n) \coloneqq (sm) \otimes n$. However, we must ensure that this new module structure on M is compatible with its existing right R-module structure. An abelian group M is called an (S, R)-**bimodule** if M is a left S-module, a right R-module, and $s(mr) = (sm)r$ for all $s \in S$, $r \in R$ and $m \in M$.

Example. *Any ring S is an (S, R)-bimodule for any subring R with $1_R = 1_S$ by the associativity of the multiplication in S.*

More generally, if $f : R \to S$ is any ring homomorphism with $f(1_R) = 1_S$, then S can be considered as a right R-module with the action $s \cdot r \coloneqq sf(r)$, and with respect to this action S becomes an (S, R)-bimodule.

In particular, the quotient ring R/I is an $(R/I, R)$-bimodule (with respect to the canonical projection homomorphism $R \twoheadrightarrow R/I$), where I is an ideal (two-sided) in the ring R. This is also easy to see directly.

Example. *Suppose that R is a commutative ring. Then a left (respectively, right) R-module M can always be given the structure of a right (respectively, left) R-module by defining $mr \coloneqq rm$ (respectively, $rm \coloneqq mr$), for all $m \in M$ and $r \in R$, and this makes M into an (R, R)-bimodule, which is called the **standard** R-module structure on M.*

Suppose now that N is a left R-module and M is an (S, R)-bimodule. Then the (S, R)-bimodule structure on M implies that

$$s\left(\sum_{\text{finite}} m_i \otimes n_i\right) \coloneqq \sum_{\text{finite}} (sm_i) \otimes n_i \tag{10.8}$$

gives a well defined action of S under which $M \otimes_R N$ is a left S-module. (Note that the universal property may be used to give an alternate proof that (10.8) is well defined, replacing the direct calculations on the relations defining the tensor product.) By a completely parallel argument, if M is a right R-module and N is an (R, S)-bimodule, then the tensor product $M \otimes_R N$ has the structure of a right S-module, where $(\sum m_i \otimes n_i)s \coloneqq \sum m_i \otimes (n_i s)$.

Example. *Suppose that M is a right R-module and that N is a left R-module. It is equivalent to say that M is a $(\mathbb{Z}, R)$-bimodule and N is an $(R, \mathbb{Z})$-bimodule. The tensor product $M \otimes_R N$, therefore, is a $(\mathbb{Z}, \mathbb{Z})$-bimodule, which happens to be a **standard** $\mathbb{Z}$-module (i.e. an abelian group).*

The tensor product of two vector spaces (of finite dimensional) could be described by its basis directly. But when considering the tensor product over any ring R, there may be interesting results to explore, since an R-module may have a torsion part.

Example. *We show that* $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z} = 0$.

In $\mathbb{Q}/\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q}/\mathbb{Z}$ *a simple tensor has the form* $(a/b \bmod \mathbb{Z}) \otimes (c/d \bmod \mathbb{Z})$ *for some rational numbers* a/b *and* c/d. *Then*

$$\begin{aligned}(\frac{a}{b} \bmod \mathbb{Z}) \otimes (\frac{c}{d} \bmod \mathbb{Z}) &= d(\frac{a}{bd} \bmod \mathbb{Z}) \otimes (\frac{c}{d} \bmod \mathbb{Z}) \\ &= (\frac{a}{bd} \bmod \mathbb{Z}) \otimes d(\frac{c}{d} \bmod \mathbb{Z}) = (\frac{a}{bd} \bmod \mathbb{Z}) \otimes (c \bmod \mathbb{Z}) = (\frac{a}{bd} \bmod \mathbb{Z}) \otimes 0 = 0.\end{aligned}$$

The last equality is because that $m \otimes 0 = 0$ *in any tensor product* $M \otimes_R N$, *noticing that* $m \otimes 0 = m \otimes (0 + 0) = m \otimes 0 + m \otimes 0$. *Likewise* $0 \otimes n = 0$.

Exercise ([1] §10.4 Exercises 3 & 4)**.** *Show that* $\mathbb{Q} \otimes_{\mathbb{Q}} \mathbb{Q}$ *and* $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Q}$ *are isomorphic as left* $\mathbb{Q}$*-modules, but* $\mathbb{C} \otimes_{\mathbb{C}} \mathbb{C}$ *and* $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C}$ *are not isomorphic left* $\mathbb{R}$*-modules.*

Before we explain the next example, first we introduce the universal property of the tensor product of modules.

Theorem ([1] §10.4 Theorem 10)**.** *Suppose* R *is a ring with* 1, M *is a right* R*-module,* N *is a left* R*-module, and let* L *be an abelian group (written additively).*

A map $\varphi : M \times N \to L$ *is called* R***-balanced*** *or* ***middle linear with respect to*** R *if*

$$\begin{aligned}\varphi(m_1 + m_2, n) &= \varphi(m_1, n) + \varphi(m_2, n), \\ \varphi(m, n_1 + n_2) &= \varphi(m, n_1) + \varphi(m, n_2), \\ \varphi(mr, n) &= \varphi(m, rn),\end{aligned}$$

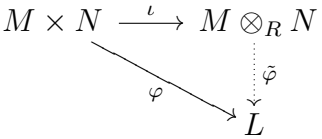
for all $m, m_1, m_2 \in M$, $n, n_1, n_2 \in N$, *and* $r \in R$. *(In addition, if* R *is commutative,* L *is a left* R*-module,* M *is given the standard* R*-module structure, and* $\varphi(mr, n) = \varphi(m, rn) = r\varphi(m, n)$, *we call* φ *an* R***-bilinear map****.) Then*

(1) the map $\iota : M \times N \to M \otimes_R N$ *defined by* $(m, n) \mapsto m \otimes n$ *is* R*-balanced;*

(2) if $\tilde{\varphi} : M \otimes_R N \to L$ *is any group homomorphism from* $M \otimes_R N$ *to an abelian group* L, *then the composite map* $\tilde{\varphi} \circ \iota$ *is an* R*-balanced map from* $M \times N$ *to* L*;*

(3) (the universal property) *for any abelian group* L *and any* R*-balanced map* $\varphi : M \times N \to L$, *there is a unique group homomorphism* $\tilde{\varphi} : M \otimes_R N \to L$ *such that* φ *factors through* ι, *i.e.,* $\varphi = \tilde{\varphi} \circ \iota$.

Equivalently, the correspondence $\varphi \leftrightarrow \tilde{\varphi}$ *in the commutative diagram*



establishes a bijection

$$\left\{ \begin{array}{c} R\text{-balanced maps} \\ \varphi : M \times N \to L \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \text{group homomorphisms} \\ \tilde{\varphi} : M \otimes_R N \to L \end{array} \right\}.$$

Example. *We have* $\mathbb{Z}/(2) \otimes_{\mathbb{Z}} \mathbb{Z}/(3) = 0$*, since* $3a = a$ *for* $a \in \mathbb{Z}/(2)$ *so that*

$$a \otimes b = 3a \otimes b = a \otimes 3b = a \otimes 0 = 0$$

and every simple tensor is reduced to 0*. In particular* $1 \otimes 1 = 0$*. It follows that there are no nonzero balanced (or bilinear) maps from* $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ *to any abelian group.*

Consider the tensor product $\mathbb{Z}/(2) \otimes_{\mathbb{Z}} \mathbb{Z}/(2)$*, which is generated as an abelian group by the elements* $0 \otimes 0 = 1 \otimes 0 = 0 \otimes 1 = 0$ *and* $1 \otimes 1$*. In this case* $1 \otimes 1 \neq 0$ *since, for example, the map* $\mathbb{Z}/(2) \times \mathbb{Z}/(2) \to \mathbb{Z}/(2)$ *defined by* $(a, b) \mapsto ab$ *is clearly nonzero and linear in both* a *and* b*. Since* $2(1 \otimes 1) = 2 \otimes 1 = 0 \otimes 1 = 0$*, the element* $1 \otimes 1$ *is of order* 2*. Hence* $\mathbb{Z}/(2) \otimes_{\mathbb{Z}} \mathbb{Z}/(2) \cong \mathbb{Z}/(2)$*.*

Exercise. *Show that* $\mathbb{Z}/(m) \otimes_{\mathbb{Z}} \mathbb{Z}/(n) \cong \mathbb{Z}/(\mathrm{GCD}(m, n))$*, where* $\mathrm{GCD}(m, n)$ *is the greatest common divisor of the integers* m *and* n*.*

3.2 Extension of scalars

Suppose that the ring R is a subring of the ring S. Throughout this section, we always assume that $1_R = 1_S$ (this ensures that S is a unital R-module). If N is a left S-module, then N can also be naturally considered as a left R-module since the elements of R (being elements of S) act on N by assumption. More generally, if $f : R \to S$ is a ring homomorphism from R into S with $f(1_R) = 1_S$ (for example the injection map if R is a subring of S as above, or the natural map $R \twoheadrightarrow R/I$ if I is a two sided ideal of R) then it is easy to see that N can be considered as an R-module with $rn := f(r)n$ for $r \in R$ and $n \in N$. In this situation S can be considered as an extension of the ring R and the resulting R-module is said to be obtained from N by restriction of scalars from S to R.

Suppose now that R is a subring of S and we try to reverse this, namely we start with an R-module N and attempt to define an S-module structure on N that extends the action of R on N to an action of S on N. In general this is impossible, even in the simplest situation: the ring R itself is an R-module but is usually not an S-module for the larger ring S. For example, $\mathbb{Z}$ is a $\mathbb{Z}$-module but it cannot be made into a $\mathbb{Q}$-module (if it could, then $\frac{1}{2} \circ 1 =: z$ would be an element of $\mathbb{Z}$ with $z + z = 1$, which is impossible).

Although $\mathbb{Z}$ itself cannot be made into a $\mathbb{Q}$-module, it is contained in a $\mathbb{Q}$-module, namely $\mathbb{Q}$ itself. Similarly the ring R can always be embedded as an R-submodule of the S-module S. This raises the question of whether an arbitrary R-module N can be embedded as an R-submodule of some S-module, or more generally, the question of what R-module homomorphisms exist from N to S-modules.

Example. *Suppose* N *is a nontrivial finite abelian group, say* $N = \mathbb{Z}/2\mathbb{Z}$*, and consider possible* $\mathbb{Z}$*-module homomorphisms (i.e. abelian group homomorphisms) of* N *into some* $\mathbb{Q}$*-module.*

A $\mathbb{Q}$*-module is just a vector space over* $\mathbb{Q}$*, and every nonzero element in a vector space over* $\mathbb{Q}$ *has infinite (additive) order. Since every element of* N *has finite order, every element of* N *must map to* 0 *under such a homomorphism. In other words there are no nonzero* $\mathbb{Z}$*-module homomorphisms from this* N *to any* $\mathbb{Q}$*-module, much less embeddings of* N *identifying* N *as a submodule of a* $\mathbb{Q}$*-module.*

The two $\mathbb{Z}$*-modules* $\mathbb{Z}$ *and* $\mathbb{Z}/2\mathbb{Z}$ *exhibit extremely different behaviors when we try to "extend scalars" from* $\mathbb{Z}$ *to* $\mathbb{Q}$*: the first module maps injectively into some* $\mathbb{Q}$*-module, the second always maps to* 0 *in a* $\mathbb{Q}$*-module.*

The tensor product $S \otimes_R N$ privides a structure of a left S-module for a general left R-module N that is the "best possible" target in which to try to embed N. The module $S \otimes_R N$ is called the

(left) S-module obtained by **extension of scalars** from the (left) R-module N. We shall also see that this module determines all of the possible R-module homomorphisms of N into S-modules, in particular determining when N is contained in some S-module (cf. [1] §10.4 Corollary 9). In the case of $R = \mathbb{Z}$ and $S = \mathbb{Q}$ this construction will give us $\mathbb{Q}$ when applied to the module $N = \mathbb{Z}$, and will give us 0 when applied to the module $N = \mathbb{Z}/2\mathbb{Z}$.

Example (Extension of scalars for free modules)**.** *If $N \cong R^n$ is a free module of rank n over R, then*

$$S \otimes_R R^n \cong S^n$$

is a free module of rank n over S (cf. [1] §10.4 Corollary 18). In this case the module obtained by extension of scalars contains (an isomorphic copy of) the original R-module N. For example, $\mathbb{Q} \otimes_{\mathbb{Z}} \mathbb{Z}^n \cong \mathbb{Q}^n$, and $\mathbb{Z}^n$ is a subgroup of the abelian group $\mathbb{Q}^n$.

Another special case of this example is that, when F is a subfield of the field K and V is an n-dimensional vector space over F (i.e. $V \cong F^n$), $K \otimes_F V \cong K^n$ is a vector space over the larger field K of the same dimension, and the original vector space V is contained in $K \otimes_F V$ as an F-vector subspace.

Example. *Let $R = \mathbb{Z}$, $S = \mathbb{Q}$ and let A be a finite abelian group of order n. In this case the $\mathbb{Q}$-module $\mathbb{Q} \otimes_{\mathbb{Z}} A$ obtained by extension of scalars from the $\mathbb{Z}$-module A is 0. To see this, for any simple tensor $q \otimes a$ we can write the rational number q as $(q/n)n$. Then since $na = 0$ in A by Lagrange's Theorem, we have*

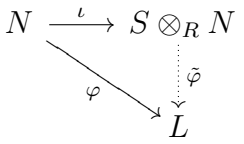
$$q \otimes a = (\frac{q}{n} \cdot n) \otimes a = \frac{q}{n} \otimes (na) = \frac{q}{n} \otimes 0 = 0.$$

It follows that $\mathbb{Q} \otimes_{\mathbb{Z}} A = 0$.

In particular, the map $\iota : A \to S \otimes_R A$ is the zero map. The universal property of extension of scalars shows again that, any homomorphism of a finite abelian group into a rational vector space is the zero map. In particular, if A is nontrivial, then the original $\mathbb{Z}$-module A is not contained in the $\mathbb{Q}$-module obtained by extension of scalars.

Theorem ([1] §10.4 Theorem 8 & Corollary 9)**.** *Let R be a subring of S with $1_R = 1_S$, N be a left R-module, and ι be the R-module homomorphism defined by $\iota(n) := 1 \otimes n$.*

(1) (the universal property) *For any left S-module L (hence also a left R-module) and any R-module homomorphism $\varphi : N \to L$, there is a unique S-module homomorphism $\tilde{\varphi} : S \otimes_R N \to L$ such that φ factors through ι, i.e., $\varphi = \tilde{\varphi} \circ \iota$ and the diagram*



commutes.

(2) $N/\ker \iota$ is the unique largest quotient of N that can be embedded in any S-module. In particular, N can be embedded as an R-submodule of some left S-module if and only if ι is injective (in which case N is isomorphic to the R-submodule $\iota(N)$ of the S-module $S \otimes_R N$).

Example. *For any ring R and any left R-module N we have $R \otimes_R N \cong N$ (so "extending scalars from R to R" does not change the module). This follows by taking φ to be the identity map from N to itself (and $S = R$) in the above theorem: ι is then an isomorphism with inverse isomorphism given by $\tilde{\varphi}$.*

In particular, if A is any abelian group (i.e., a $\mathbb{Z}$-module), then $\mathbb{Z} \otimes_{\mathbb{Z}} A = A$.

3.3 Change of base (a generalization)

Let $f : R \to S$ be a ring homomorphism with $f(1_R) = 1_S$. Then $s \cdot r := sf(r)$ gives S the structure of a right R-module with respect to which S is an (S, R)-bimodule. Then for any left R-module N, the resulting tensor product $S \otimes_R N$ is a left S-module obtained by **changing the base** from R to S. This gives a slight generalization of the notion of extension of scalars (where R was a subring of S).

Example. *Let $f : R \to S$ be a ring homomorphism with $f(1_R) = 1_S$. One can show that $S \otimes_R R \cong S$ as left S-modules.*

- *The map $\varphi : S \times R \to S$ defined by $(s, r) \mapsto sr$ (where $sr := sf(r)$ by definition of the right R-action on S), is an R-balanced map.*
- *The R-balanced map φ induces, via the universal property, an S-module homomorphism $\tilde{\varphi} : S \otimes_R R \to S$ with $\tilde{\varphi}(s \otimes r) = sr$.*
- *The map $\tilde{\varphi}' : S \to S \otimes_R R$ with $s \mapsto s \otimes 1$ is an S-module homomorphism that is inverse to $\tilde{\varphi}$.*

Exercise ([1] §10.4 Exercise 24)**.** *Prove that the extension of scalars from $\mathbb{Z}$ to the Gaussian integers $\mathbb{Z}[i]$ of the ring $\mathbb{R}$ is isomorphic to $\mathbb{C}$ as a ring: $\mathbb{Z}[i] \otimes_{\mathbb{Z}} \mathbb{R} \cong \mathbb{C}$ as rings (see [1] §10.4 Proposition 21 for the definition of multiplication in the tensor product of two R-algebras).*

Exercise ([1] §10.4 Exercise 25)**.** *Let R be a subring of the commutative ring S and let x be an indeterminate over S. Prove that $S[x]$ and $S \otimes_R R[x]$ are isomorphic as S-algebras.*

Let R be a ring (not necessarily commutative), let I be a two sided ideal in R, and let N be a left R-module. Then as previously mentioned, R/I is an $(R/I, R)$-bimodule, so the tensor product $R/I \otimes_R N$ is a left R/I-module. This is an example of "extension of scalars" with respect to the natural projection homomorphism $R \twoheadrightarrow R/I$.

Proposition. *Define*

$$IN := \left\{ \sum_{\text{finite}} a_i n_i \;\middle|\; a_i \in I,\ n_i \in N \right\}.$$

Then IN is a left R-submodule of N ([1] §10.1 Exercise 5), and

$$(R/I) \otimes_R N \cong N/IN$$

as left R-modules.

Proof. Exercise (cf. [1] §10.4 p.370). □

Example. *As an example, let $R = \mathbb{Z}$ with ideal $I = (m)$ and let N be the $\mathbb{Z}$-module $\mathbb{Z}/(n)$. Then*

$$IN = m(\mathbb{Z}/n\mathbb{Z}) = (m\mathbb{Z} + n\mathbb{Z})/n\mathbb{Z} = \mathrm{GCD}(m, n)\mathbb{Z}/n\mathbb{Z}.$$

Then $N/IN \cong \mathbb{Z}/\mathrm{GCD}(m, n)\mathbb{Z}$ and we recover the isomorphism

$$\mathbb{Z}/m\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/\mathrm{GCD}(m, n)\mathbb{Z}$$

of an previous example.

3.4 When the base is commutative

Proposition ([1] §10.4 Corollary 15)**.** *Suppose R is commutative and M, N, and L are left R-modules. Then*

$$(M \otimes N) \otimes L \cong M \otimes (N \otimes L)$$

as R-modules for the standard R-module structures on M, N and L.

Proposition ([1] §10.4 Corollary 19)**.** *Let R be a commutative ring and let $M \cong R^s$ and $N \cong R^t$ be free R-modules with bases $m_1, \ldots, m_s$ and $n_1, \ldots, n_t$, respectively. Then $M \otimes_R N$ is a free R-module of rank st, with basis $m_i \otimes n_j$, $1 \leq i \leq s$ and $1 \leq j \leq t$, i.e.,*

$$R^s \otimes_R R^t \cong R^{st}.$$

More generally, the tensor product of two free modules of arbitrary rank over a commutative ring is free.

Proposition ([1] §10.4 Proposition 20)**.** *Suppose R is a commutative ring and M, N are left R-modules, considered with the standard R-module structures. Then there is a unique R-module isomorphism*

$$M \otimes_R N \cong N \otimes_R M$$

mapping $m \otimes n$ to $n \otimes m$.

Proposition ([1] §10.4 Proposition 21)**.** *Let R be a commutative ring and let A and B be R-algebras. Then the multiplication $(a \otimes b)(a' \otimes b') := aa' \otimes bb'$ is well defined and makes $A \otimes_R B$ into an R-algebra.*

4 Exact sequences

4.1 The extension problem

We first introduce a very convenient notation.

Definition. *Let X, Y, Z, X_i be some algebraic objects (e.g., groups, rings, or modules).*

*(1) The pair of homomorphisms $X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z$ is said to be **exact** (at Y) if* $\operatorname{image} \alpha = \ker \beta$.

*(2) A **sequence** $\cdots \to X_{n-1} \to X_n \to X_{n+1} \to \cdots$ of homomorphisms is said to be an **exact sequence** if it is exact at every X_n between a pair of homomorphisms.*

*(3) The exact sequence $0 \to X \xrightarrow{\psi} Y \xrightarrow{\varphi} Z \to 0$ is called a **short exact sequence**. (If X, Y and Z are groups written multiplicatively, the sequence will be written $1 \to X \xrightarrow{\psi} Y \xrightarrow{\varphi} Z \to 1$ where 1 denotes the trivial group.) Y is called an **extension** of Z by X.*

Proposition ([1] §10.5 Proposition 22 & Corollary 23)**.** *Let X, Y, Z be some algebraic objects.*

(1) The sequence $0 \to X \xrightarrow{\psi} Y$ is exact (at X) if and only if ψ is injective (denoted by $X \xhookrightarrow{\psi} Y$).

(2) The sequence $Y \xrightarrow{\varphi} Z \to 0$ is exact (at Z) if and only if φ is surjective (denoted by $Y \xrightarrow{\varphi} \!\!\!\!\rightarrow Z$).

(3) The sequence $0 \to X \xrightarrow{\psi} Y \xrightarrow{\varphi} Z \to 0$ is exact if and only if

- *ψ is injective,*
- *φ is surjective, and*
- $\operatorname{image} \psi = \ker \varphi$.

Proof. The (uniquely defined) homomorphism $0 \to A$ has image 0 in A. This will be the kernel of ψ if and only if ψ is injective.

Similarly, the kernel of the (uniquely defined) zero homomorphism $C \to 0$ is all of C, which is the image of φ if and only if φ is surjective. □

Note that any exact sequence can be written as a succession of short exact sequences, since to say $X \xrightarrow{\alpha} Y \xrightarrow{\beta} Z$ is exact at Y is the same as saying that the sequence

$$0 \to \alpha(X) \to Y \to Y/\ker\beta \to 0$$

is a short exact sequence.

Example. *Given (left) R-modules A and C we can always form their direct sum $B = A \oplus C$, and the sequence*

$$0 \to A \xrightarrow{\iota} A \oplus C \xrightarrow{\pi} C \to 0$$

where $\iota(a) \coloneqq (a, 0)$ and $\pi(a, c) \coloneqq c$ is a short exact sequence.

This is also valid for groups (not necessarily abelian), for example,

$$1 \to \mathrm{SL}_2(\mathbb{C}) \to \mathrm{SL}_2(\mathbb{C}) \oplus \mathbb{C}^\times \to \mathbb{C}^\times \to 1$$

is a short exact sequence.

Example. *If $\varphi : B \to C$ is any homomorphism we may form an exact sequence:*

$$0 \to \ker\varphi \xrightarrow{\iota} B \xrightarrow{\varphi} \varphi(B) \to 0$$

where ι is the inclusion map. In particular, if φ is surjective, the sequence $B \xrightarrow{\varphi} C$ may be extended to a short exact sequence with $A = \ker\varphi$. For example,

$$1 \to \mathrm{SL}_2(\mathbb{C}) \hookrightarrow \mathrm{GL}_2(\mathbb{C}) \xrightarrow{\det} \mathbb{C}^\times \to 1$$

is a short exact sequence.

Other related exercises in [1]

§10.1 5 8 10 11 18 19 20 21
§10.2 3 5 6 8 13
§10.3 3 4 8 10 11 15 18 23 25
§10.4 2 6 7 10 15 16 18 20 27
§10.5

References

[1] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.