Introduction to Modern Algebra II

Math 818 Spring 2023

January 30, 2023

Contents

Chapter 1

Modules

Modules are a generalization of the concept of a vector space to any ring of scalars. But while vector spaces make for a great first example of modules, many of the basic facts we are used to from linear algebra are often a little more subtle over a general ring. These differences are features, not bugs. We will introduce modules, study some general linear algebra, and discuss the differences that make the general theory of modules richer and even more fun.

1.1 Basic assumptions

In this class, all rings have a multiplicative identity, written as 1 or 1_R is we want to emphasize that we are referring to the ring R. This is what some authors call *unital rings*; since for us all rings are unital, we will omit the adjective. Moreover, we will think of 1 as part of the structure of the ring, and thus require it be preserved by all natural constructions. As such, a subring S of R must share the same multiplicative identity with R, meaning $1_R = 1_S$. Moreover, any ring homomorphism must preserve the multiplicative identity. To clear any possible confusion, we include below the relevant definitions.

Definition 1.1. A **ring** is a set R equipped with two binary operations, $+$ and $\cdot$, satisfying:

(1) $(R, +)$ is an abelian group with identity element denoted 0 or 0_R.

(2) The operation $\cdot$ is associative, so that $(R, \cdot)$ is a semigroup.

(3) For all $a, b, c \in R$, we have

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

(4) there is a multiplicative identity, written as 1 or 1_R, such that $1 \cdot a = a = a \cdot 1$ for all $a \in R$.

To simplify notation, we will often drop the $\cdot$ when writing the multiplication of two elements, so that ab will mean $a \cdot b$.

Definition 1.2. A ring R is a **commutative ring** if for all $a, b \in R$ we have $a \cdot b = b \cdot a$.

Definition 1.3. A ring R is a **division ring** if $1 \neq 0$ and $R \setminus \{0\}$ is a group under $\cdot$, so every nonzero $r \in R$ has a multiplicative inverse. A **field** is a commutative division ring.

Definition 1.4. A commutative ring R is a **domain**, sometimes called an **integral domain** if it has no zerodivisors: $ab = 0 \Rightarrow a = 0$ or $b = 0$.

For some familiar examples, $\mathrm{M}_n(R)$ (the set of $n \times n$ matrices) is a ring with the usual addition and multiplication of matrices, $\mathbb{Z}$ and $\mathbb{Z}/n$ are commutative rings, $\mathbb{C}$ and $\mathbb{Q}$ are fields, and the real Hamiltonian quaternion ring $\mathbb{H}$ is a division ring.

Definition 1.5. A **ring homomorphism** is a function $f\colon R \to S$ satisfying the following:

- $f(a+b) = f(a) + f(b)$ for all $a, b \in R$.
- $f(ab) = f(a)f(b)$ for all $a, b \in R$.
- $f(1_R) = 1_S$.

Under this definition, the map $f\colon \mathbb{R} \to \mathrm{M}_2(\mathbb{R})$ sending $a \mapsto \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix}$ preserves addition and multiplication but not the multiplicative identities, and thus it is not a ring homomorphism.

Exercise 1. For any ring R, there exists a unique homomorphism $\mathbb{Z} \to R$.

Definition 1.6. A subset S of a ring R is a **subring** of R if it is a ring under the same addition and multiplication operations and $1_R = 1_S$.

So under this definition, $2\mathbb{Z}$, the set of even integers, is not a subring of $\mathbb{Z}$; in fact, it is not even a ring, since it does not have a multiplicative identity!

Definition 1.7. Let R be a ring. A subset I of R is an **ideal** if:

- I is nonempty.
- $(I, +)$ is a subgroup of $(R, +)$.
- For every $a \in I$ and every $r \in R$, we have $ra \in I$ and $ar \in I$.

The final property is often called **absorption**. A **left ideal** satisfies only absorption on the left, meaning that we require only that $ra \in I$ for all $r \in R$ and $a \in I$. Similarly, a **right ideal** satisfies only absorption on the right, meaning that $ar \in I$ for all $r \in R$ and $a \in I$.

When R is a commutative ring, the left ideals, right ideals, and ideals over R are all the same. However, if R is not commutative, then these can be very different classes.

One key distinction between unital rings and nonunital rings is that if one requires every ring to have a 1, as we do, then the ideals and subrings of a ring R are very different creatures. In fact, the *only* subring of R that is also an ideal is R itself. The change lies in what constitutes a subring; notice that nothing has changed in the definition of ideal.

Remark 1.8. Every ring R has two **trivial ideals**: R itself and the zero ideal $(0) = \{0\}$.

A **nontrivial ideal** I of R is an ideal that $I \neq R$ and $I \neq (0)$. An ideal I of R is a **proper ideal** if $I \neq R$.

1.2 Modules: definition and examples

Definition 1.9. Let R be a ring with $1 \neq 0$. A **left R-module** is an abelian group $(M, +)$ together with an action $R \times M \to M$ of R on M, written as $(r, m) \mapsto rm$, such that for all $r, s \in R$ and $m, n \in M$ we have the following:

- $(r + s)m = rm + sm$,
- $(rs)m = r(sm)$,
- $r(m + n) = rm + rn$, and
- $1m = m$.

A **right R-module** is an abelian group $(M, +)$ together with an action of R on M, written as $M \times R \to M, (m, r) \mapsto mr$, such that for all $r, s \in R$ and $m, n \in M$ we have

- $m(r + s) = mr + ms$,
- $m(rs) = (mr)s$,
- $(m + n)r = mr + nr$, and
- $m1 = m$.

By default, we will be studying left R-modules. To make the writing less heavy, we will sometimes say **R-module** rather than left R-module whenever there is no ambiguity.

Remark 1.10. If R is a commutative ring, then any left R-module M may be regarded as a right R-module by setting $mr := rm$. Likewise, any right R-module may be regarded as a left R-module. Thus for commutative rings, we just refer to modules, and not left or right modules.

Lemma 1.11 (Arithmetic in modules)**.** *Let R be a ring with $1_R \neq 0_R$ and M be an R-module. Then $0_R m = 0_M$ and $(-1_R)m = -m$ for all $m \in M$.*

Proof. Let $m \in M$. Then

$$0_R m = (0_R + 0_R)m = 0_R m + 0_R m.$$

Since M is an abelian group, the element $0_R m$ has an additive inverse, $-0_R m$, so adding it on both sides we see that

$$0_M = 0_R m.$$

Moreover,

$$m + (-1_R)m = 1_R m + (-1_R)m = (1_R - 1_R)m = 0_R m = 0_M,$$

so $(-1_R)m = -m$. □

Typically, one first encounters modules in an undergraduate linear algebra course: the vector spaces from linear algebra are modules over fields. Later we will see that vector spaces are much simpler modules than modules over other rings. So while one might take linear algebra and vector spaces as an inspiration for what to expect from a module, be warned that this perspective can often be deceiving.

Definition 1.12. Let F be a field. A **vector space** over F is an F-module.

We will see more about vector spaces soon. Note that many of the concepts we will introduce have special names in the case of vector spaces. Here are some other important examples:

Lemma 1.13. *Let M be a set with a binary operation $+$. Then*

(1) M is an abelian group if and only if M is a $\mathbb{Z}$-module.

(2) M is an abelian group such that $nm := \underbrace{m + \cdots + m}_{n \text{ times}} = 0_M$ for all $m \in M$ if and only if M has a $\mathbb{Z}/n$-module structure.

Proof. First, we show 1). If M is a $\mathbb{Z}$-module, then $(M, +)$ is an abelian group by definition of module. Conversely, if $(M, +)$ is an abelian group then there is a unique $\mathbb{Z}$-module structure on M given by the formulas below. The uniqueness of the $\mathbb{Z}$ action follows from the identities below in which the right hand side is determined only by the abelian group structure of M. The various identities follow from the axioms of a module:

$$\begin{cases} i \cdot m = (\underbrace{1 + \cdots + 1}_{i}) \cdot m = \underbrace{1 \cdot m + \cdots + 1 \cdot m}_{i} = \underbrace{m + \cdots + m}_{i} & \text{if } i > 0 \\ 0 \cdot m = 0_M & \\ i \cdot m = -(-i) \cdot m = -(\underbrace{m + \cdots + m}_{-i}) & \text{if } i < 0. \end{cases}$$

We leave it as an exercise to check that this $\mathbb{Z}$-action really satisfies the module axioms.

Now we show 2). If M is a $\mathbb{Z}/n$ module, then $(M, +)$ is an abelian group by definition, and $nm = \underbrace{m + \cdots + m}_{n} = \underbrace{[1]_n \cdot m + \cdots + [1]_n \cdot m}_{n} = [0]_n m = 0_M$.

Conversely, there is a unique $\mathbb{Z}/n$-module structure on M given by the formulas below, which are analogous to the ones above:

$$\begin{cases} [i]_n \cdot m = (\underbrace{[1]_n + \cdots + [1]_n}_{i}) \cdot m = \underbrace{[1]_n \cdot m + \cdots + [1]_n \cdot m}_{i} = \underbrace{m + \cdots + m}_{i} & \text{if } i > 0 \\ 0 \cdot m = 0_M & \\ [i]_n \cdot m = -(-[i]_n) \cdot m = -(\underbrace{m + \cdots + m}_{-i}) & \text{if } i < 0. \end{cases}$$

These formulas are well-defined, meaning they are independent of the choice of representative for $[i]_n$, because of the assumption that $nm = 0_M$. Again checking that this $\mathbb{Z}/n$-action really satisfies the module axioms is left as an exercise. □

The proposition above says in particular that any group of the form

$$G = \mathbb{Z}^\ell \times \mathbb{Z}/d_1 \times \cdots \times \mathbb{Z}/d_m$$

is a $\mathbb{Z}$-module, and if $\ell = 0, m \geqslant 1$ and $d_i \mid n$ for $1 \leqslant i \leqslant m$ then G is also a $\mathbb{Z}/n$-module. In particular, the Klein group is a $\mathbb{Z}/2$-module.

In contrast to vector spaces, for M a module over a ring R, it can happen that $rm = 0$ for some $r \in R$ and $m \in M$ such that $r \neq 0_R$ and $m \neq 0_M$. For example, in the Klein group K_4 viewed as a $\mathbb{Z}$-module we have $2m = 0$ for all $m \in K_4$.

Example 1.14. (1) The trivial R-module is $0 = \{0\}$ with $r0 = 0$ for any $r \in R$.

(2) If R is any ring, then R is a left and right R-module via the action of R on itself given by its internal multiplication.

(3) If I is a left (respectively, right) ideal of a ring R then I is a left (respectively, right) R-module with respect to the action of R on I by internal multiplication.

(4) If R is a subring of a ring S, then S is an R-module with respect to the action of R on S by internal multiplication in S.

(5) If R is a commutative ring with $1 \neq 0$, then $R[x_1, \ldots, x_n]$ is an R-module for any $n \geqslant 1$. This is a special case of (4).

(6) If R is a commutative ring and G is a group, then $R[G]$ is an R-module. This is a special case of (4).

(7) If R is a commutative ring, let $\mathrm{M}_n(R)$ denote set of $n \times n$ matrices with entries in R. Then $\mathrm{M}_n(R)$ is an R-module for $n \geqslant 1$, with the R-action given by multiplying all the entries of the given matrix by the given element of R.

(8) The **free module** over R of rank n is the set

$$R^n = \left\{ \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} \mid r_i \in R, 1 \leqslant i \leqslant n \right\}$$

with componentwise addition and multiplication by elements of R, as follows:

$$\begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} + \begin{bmatrix} r_1' \\ \vdots \\ r_n' \end{bmatrix} = \begin{bmatrix} r_1 + r_1' \\ \vdots \\ r_n + r_n' \end{bmatrix} \text{ and } r \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} = \begin{bmatrix} rr_1 \\ \vdots \\ rr_n \end{bmatrix}.$$

We will often write the elements of R^n as n-tuples $(r_1, \ldots, r_n)$ instead. Notice that R is the free R-module of rank 1.

(9) More generally, given a collection of R-modules $\{A_i\}$, the abelian group

$$\bigoplus_i A_i = \{(a_i)_i \mid a_i \in A_i, a_i = 0 \text{ for all } i \text{ but finitely many}\}$$

is an R-module with the R-action $r(a_i) := (ra_i)$.

1.3 Submodules and restriction of scalars

Definition 1.15. Let R be a ring and let M be a left R-module. An **R-submodule** of M is a subgroup N of M satisfying $rn \in N$ for all $r \in R$ and $n \in N$.

The submodules of an R-module M are precisely the subsets of M which are modules in their own right, via the same R-action as we are considering for M.

Exercise 2. Show that if N is a submodule of M, then N is an R-module via the restriction of the action of R on M to the subset N.

Example 1.16. Every R-module M has two **trivial submodules**: M itself and the **zero module** $0 = \{0_M\}$. A submodule N of M is **nontrivial** if $N \neq M$ and $N \neq 0$.

Lemma 1.17 (One-step test for submodules)**.** *Let R be a ring with $1 \neq 0$ and let M be a left R-module. A nonempty subset N of M is an R-submodule of M if and only if $rn + n' \in N$ for all $r \in R$ and $n, n' \in N$.*

Proof. The One-step Test for subgroups says that if for all $n, n' \in N$ we have $n' - n \in N$, then N is a subgroup of M. By Lemma 1.11, by taking $r = -1$ we get $rn + n' = n' - n$, and by assumption this is an element of N. Therefore, N is a subgroup of M. As a consequence, $0_M \in N$. By taking $n' = 0_M$, we see that for all $n \in N$ and all $r \in R$ we have $rn = rn + n' \in N$, and thus we can now conclude that N is a submodule of M. □

Example 1.18. Let R be a ring and let M be a subset of R. Then M is a left (respectively, right) R-submodule of R if and only if M is a left (respectively, right) ideal of R.

Exercise 3. Let R be a ring and let A and B be submodules of an R-module M. Then the **sum** of A and B,

$$A + B := \{a + b \mid a \in A, b \in B\},$$

and $A \cap B$ are both R-submodules of M.

Exercise 4. Let R be a commutative ring with $1 \neq 0$, let I be an ideal of R and let M be an R-module. Show that

$$IM := \left\{ \sum_{k=1}^{n} j_k m_k \mid n \geqslant 0, j_k \in I, m_k \in M \text{ for } 1 \leqslant k \leqslant n \right\}$$

is a submodule of M.

Example 1.19. When R is a field, the submodules of a vector space V are precisely the subspaces of V. When $R = \mathbb{Z}$, then the class of R-modules is simply the class of all abelian groups, by Lemma 1.13. The submodules of a $\mathbb{Z}$-module M coincide with the subgroups of the abelian group M.

Definition 1.20. Let R be a ring with $1 \neq 0$ and let M be an R-module. Given elements $m_1, \ldots, m_n \in M$, the **submodule generated by** $m_1, \ldots, m_n$ is the subset of M given by

$$Rm_1 + \cdots + Rm_n := \{r_1 m_1 + \cdots + r_n m_n \mid r_1, \ldots, r_n \in R\}.$$

Exercise 5. Let R be a ring with $1 \neq 0$ and M be an R-module. Given $m_1, \ldots, m_n \in M$, the submodule generated by $m_1, \ldots, m_n$ is indeed a submodule of M. Moreover, this is the smallest submodule of M that contains $m_1, \ldots, m_n$, meaning that every submodule of M containing $m_1, \ldots, m_n$ must also contain $Rm_1 + \cdots + Rm_n$.

Definition 1.21. Let R be a ring with $1 \neq 0$. An R-module M is **cyclic** if there exists an element $m \in M$ such that

$$M = Rm := \{rm \mid r \in R\}.$$

Given an R-module M, the ring R is often referred to as the **ring of scalars**, by analogy to the vector space case. Given an action of a ring of scalars on a module, we can sometimes produce an action of a different ring of scalars on the same set, producing a new module structure.

Lemma 1.22 (Restriction of scalars)**.** *Let $\phi\colon R \to S$ be a ring homomorphism. Any left S-module M may be regarded via* **restriction of scalars** *as a left R-module with R-action defined by $rm := \phi(r)m$ for any $m \in M$. In particular, if R is a subring of a ring S, then any left S-module M may be regarded via restriction of scalars as a left R-module with R-action defined by the action of the elements of R viewed as elements of S.*

Proof. Let $r, s \in R$ and $m, n \in M$. One checks that the axioms in the definition of a module hold for the given action using properties of ring homomorphisms. For example:

$$(r+s)m = \phi(r+s)m = (\phi(r) + \phi(s))m = \phi(r)m + \phi(s)m = rm + sm.$$

The remaining properties are left as an exercise. □

Note that the second module structure on M obtained via restriction of scalars is induced by the original module structure, so the two are related. In general, one can give different module structures on the same abelian group over different, possibly unrelated, rings.

Example 1.23. If I is an ideal of a ring R, applying restriction of scalars along the quotient homomorphism $q\colon R \to R/I$ tells us that any left R/I-module is also a left R-module. In particular, applying this to the R/I-module R/I makes R/I a left and right R-module by restriction of scalars along the quotient homomorphism. Thus the R-action on R/I is given by

$$r \cdot (a + I) := ra + I.$$

Example 1.24. Given any ring R there exists a unique ring homomorphism $\mathbb{Z} \to R$, by Exercise 1. Thus any R-module can be given the structure of a $\mathbb{Z}$-module by restriction of scalars along this unique map. Note also that a module over any ring is in particular an abelian group, so we can always regard any R-module as a $\mathbb{Z}$-module by forgetting the R-action and focusing only on the abelian group structure. These two constructions – the restriction of scalars to $\mathbb{Z}$ and the *forgetful functor*[1] – actually coincide.

The next example explains why restriction of scalars is called a *restriction*.

Example 1.25. Let R be a subring of S, and let $i\colon R \to S$ be the inclusion map, which must by definition be a ring homomorphism. Applying restriction of scalars to an S-module M via i is the same as simply *restricting* our scalars to the elements of R.

[1] This is a concrete abstract nonsense construction that we will discuss in Homological Algebra next Fall.

1.4 Module homomorphisms and isomorphisms

Definition 1.26. Given R-modules M and N, an **R-module homomorphism** from M to N is a function $f\colon M \to N$ such that for all $r \in R$ and $m, n \in M$ we have

- $f(m+n) = f(m) + f(n)$
- $f(rm) = rf(m)$.

Remark 1.27. The condition $f(m+n) = f(m) + f(n)$ says that f is a homomorphism of abelian groups, and the condition $f(rm) = rf(m)$ says that f is R-linear, meaning that it preserves the R-action. Since f is a homomorphism of abelian groups, it follows that $f(0) = 0$ must hold.

Definition 1.28. Let M and N be vector spaces over a field F. A **linear transformation** from M to N is an F-module homomorphism $M \to N$.

Example 1.29. Let R be a commutative ring and M be an R-module. For each $r \in R$, the multiplication map $\mu_r : M \to M$ given by $\mu_r(m) = rm$ is a homomorphism of R-modules: indeed, by the definition of R-module we have

$$\mu_r(m+n) = r(m+n) = rm + rn = \mu_r(m) + \mu_r(n),$$

and

$$\mu_r(sm) = r(sm) = (rs)m = (sr)m = s(rm) = s\mu_r(m).$$

Definition 1.30. An R-module homomorphism $h\colon M \to N$ is an **R-module isomorphism** if there is an R-module homomorphism $g : N \to M$ such that $h \circ g = \mathrm{id}_N$ and $g \circ h = \mathrm{id}_M$. We say M and N are **isomorphic**, denoted $M \cong N$, if there exists an isomorphism $M \to N$.

To check that an R-module homomorphism $f\colon M \to N$ is an isomorphism, it is sufficient to check that it is bijective.

Exercise 6. Let $f\colon M \to N$ be a homomorphism of R-modules. Show that if f is bijective, then its set-theoretic inverse $f^{-1}\colon N \to M$ is an R-module homomorphism. Therefore, every bijective homomorphism of R-modules is an isomorphism.

One should think of a module isomorphism as a relabelling of the names of the elements of the module. If two modules are isomorphic, that means that they are *essentially the same*, up to renaming the elements.

Definition 1.31. Let $f\colon M \to N$ be a homomorphism of R-modules. The **kernel** of f is

$$\ker(f) := \{m \in M \mid f(m) = 0\}.$$

The **image** of f, denoted $\mathrm{im}(f)$ or $f(M)$, is

$$\mathrm{im}(f) := \{f(m) \mid m \in M\}.$$

Exercise 7. Let R be a ring with $1 \neq 0$, let M be an R-module, and let N be an R-submodule of M. Then the inclusion map $i\colon N \to M$ is an R-module homomorphism.

Exercise 8. If $f\colon M \to N$ is an R-module homomorphism, then $\ker(h)$ is an R-submodule of M and $\mathrm{im}(f)$ is an R-submodule of N.

Definition 1.32. Let R be a ring and let M and N be R-modules. Then $\mathrm{Hom}_R(M,N)$ denotes the set of all R-module homomorphisms from M to N, and $\mathrm{End}_R(M)$ denotes the set $\mathrm{Hom}_R(M,M)$. We call $\mathrm{End}(M)$ the **endomorphism ring** of M, and elements of $\mathrm{End}(M)$ are called **endomorphisms** of M.

The endomorphism ring of an R-module M is called that because it *is* a ring, with multiplication given by composition of endomorphisms, 0 given by the zero map (the constant equal to 0), and 1 given by the identity map. However, two homomorphisms from M to N are not composable unless $M = N$, so $\mathrm{Hom}_R(M,N)$ is not a ring.

When R is commutative, $\mathrm{Hom}_R(M,N)$ is, however, an R-module; let us describe its R-module structure. Given $f, g \in \mathrm{Hom}_R(M,N)$, $f+g$ is the map defined by

$$(f+g)(m) := f(m) + g(m),$$

and given $r \in R$ and $f \in \mathrm{Hom}_R(M,N)$, $r \cdot f$ is the R-module homomorphism defined by

$$(r \cdot f)(m) := r \cdot f(m) = f(rm).$$

The zero element of $\mathrm{Hom}_R(M,N)$ is the **zero map**, the constant equal to 0_N.

Lemma 1.33. *Let M and N be R-modules over a commutative ring R. Then the addition and multiplication by scalars defined above make $\mathrm{Hom}_R(M,N)$ an R-module.*

Proof. There are many things to check, including:

- The addition and the R-action are both well-defined: given $f, g \in \mathrm{Hom}_R(M,N)$ and $r \in R$, we always have $f+g, rf \in \mathrm{Hom}_R(M,N)$.
- The axioms of an R-module are satisfied for $\mathrm{Hom}_R(M,N)$.

We leave the details as exercises. □

We will see later that for an n-dimensional vector space V over a field F, there is an isomorphism of vector spaces $\mathrm{End}_F(V) \cong M_n(F)$. This says that every linear transformation $T : V \to V$ corresponds to some $n \times n$ matrix. However, the story for general R-modules is a lot more complicated.

Lemma 1.34. *For any commutative ring R with $1 \neq 0$ and any R-module M there is an isomorphism of R-modules $\mathrm{Hom}_R(R,M) \cong M$.*

Before we write a formal proof, it helps to think about *why* this theorem is true. What does it mean to give an R-module homomorphism $f : R \to M$? More precisely, what information do we need to determine such an f? Do we need to be given the values of $f(r)$ for every $r \in R$? Since f is a homomorphism of R-modules, for any $r \in R$ we have

$$f(r) = f(r \cdot 1) = rf(1),$$

so the value of $f(1)$ *completely determines* which R-module homomorphism we are talking about. On the other hand, we can choose *any* $m \in M$ to be the image of 1, since thanks to the axioms for modules, the function

$$f(r) := rm$$

is a well-defined R-module homomorphism for any $m \in M$. In summary, to give an R-module homomorphism $R \to M$ is the same as choosing an element $m \in M$, and $\mathrm{Hom}_R(R, M) \cong M$.

Proof. Let $f\colon M \to \mathrm{Hom}_R(R, M)$ be given for each $m \in M$ by $f(m) = \phi_m$ where ϕ_m is the map defined by $\phi_m(r) = rm$ for all $r \in R$. Now we have many things to check:

- f is well-defined, meaning that for any $m \in M$, its image $f(m) = \phi_m$ is an element of $\mathrm{Hom}_R(R, M)$, since

$$\phi_m(r_1 + r_2) = (r_1 + r_2)m = r_1m + r_2m = \phi_m(r_1) + \phi_m(r_2)$$

$$\phi_m(r_1r_2) = (r_1r_2)m = r_1(r_2m) = r_1\phi_m(r_2)$$

  for all $r_1, r_2 \in R$.

- f is an R-module homomorphism, since

$$\phi_{m_1+m_2}(r) = r(m_1 + m_2) = rm_1 + rm_2 = \phi_{m_1}(r) + \phi_{m_2}(r)$$

$$\phi_{r'm}(r) = r(r'm) = (rr')m = r'(rm) = r'\phi_m(r)$$

- f is injective, since $\phi_m = \phi_{m'}$ implies in particular that $\phi_m(1_R) = \phi_{m'}(1_R)$, which by definition of ϕ_- means that $m = m'$.

- f is surjective, since for $\psi \in \mathrm{Hom}_R(R, M)$ we have $\psi(r) = \psi(r1_R) = r\psi(1_R)$ for all $r \in R$, so $\psi = \phi_{\psi(1_R)}$.

This shows that f is an R-module isomorphism. □

Definition 1.35. Let R be a commutative ring with $1_R \neq 0_R$. An **R-algebra** is a ring A with $1_A \neq 0_A$ together with a ring homomorphism $f\colon R \to A$ such that $f(R)$ is contained in the center of A.

Given an R-algebra A, the R-algebra structure on A induces a natural R-module structure: given elements $r \in R$ and $a \in A$, the R-action is defined by

$$r \cdot a := f(r)a,$$

where the product on the right is the multiplication in A. Similarly, we get a natural right R-module structure on A, and since by definition $f(R)$ is contained in the center of A, we obtain what is called a *balanced bimodule* structure on A. We will discuss these further in Homological Algebra next Fall.

Example 1.36. Let R be a commutative ring with $1_R \neq 0_R$. The ring $R[x_1, \ldots, x_n]$ together with the inclusion map $R \hookrightarrow R[x_1, \ldots, x_n]$ is an R-algebra. More generally, any quotient of $R[x_1, \ldots, x_n]$ is an R-algebra.

The ring of matrices $M_n(R)$ with the homomorphism $r \mapsto rI_n$ is also an R-algebra, as is the group ring $R[G]$ for any group G with the inclusion of R into $R[G]$ given by $r \mapsto re_G$.

Lemma 1.37. *Let R be a commutative ring with $1 \neq 0$ and let M be an R-module. Then $\mathrm{End}_R(M)$ is an R-algebra, with addition and R-action defined as above, and multiplication defined by composition $(fg)(m) = f(g(m))$ for all $f, g \in \mathrm{End}_R(M)$ and all $m \in M$.*

Proof. There are many things to check here, including that:

- The axioms of a (unital) ring are satisfied for $\mathrm{End}_R(M)$.
- There is a ring homomorphism $f\colon R \to \mathrm{End}_R(M)$ such that $f(1_R) = 1_{\mathrm{End}_R(M)} = \mathrm{id}_M$ and $f(R) \subseteq Z(\mathrm{End}_R(M))$.

We will just check the last item and leave the others as exercises. Define $f : R \to \mathrm{End}_R(M)$ by $f(r) = r\,\mathrm{id}_M$. Then

$$f(r+s) = (r+s)\,\mathrm{id}_M = r\,\mathrm{id}_M + s\,\mathrm{id}_M = f(r) + f(s)$$

and

$$f(rs) = (rs)\,\mathrm{id}_M = (r\,\mathrm{id}_M) \circ (s\,\mathrm{id}_M) = f(r)f(s)$$

show that f is a ring homomorphism. Moreover, $\mathrm{id}_M \in Z(\mathrm{End}_R(M))$ that $f(R) \subseteq \mathrm{End}_R(M)$. □

Remark 1.38. Let R be a commutative ring with $1 \neq 0$ and let M be an R-module. Then M is also an $\mathrm{End}_R(M)$-module with the action $\phi m = \phi(m)$ for any $\phi \in \mathrm{End}_R(M)$, $m \in M$.

Definition 1.39. Let R be a ring, let M be an R-module, and let N be a submodule of M. The quotient module M/N is the quotient group M/N with R action defined by

$$r(m+N) := rm + N$$

for all $r \in R$ and $m + N \in M/N$.

Lemma 1.40. *Let R be a ring, let M be an R-module, and let N be a submodule of M. The quotient module M/N is an R-module, and the quotient map $q\colon M \to M/N$ is an R-module homomorphism with kernel $\ker(q) = N$.*

Proof. Among the many things to check here, we will only check the well-definedness of the R-action on M, and leave the others as exercises. To check well-definedness, consider $m + N = m' + N$. Then $m - m' \in N$, so $r(m - m') \in N$ by the definition of submodule. This gives that $rm - rm' \in N$, hence $rm + N = rm' + N$. □

Definition 1.41. Given an R-module M and a submodule N of M, the map $q\colon M \to M/N$ is the **canonical quotient map**, or simply the canonical map from M to N.

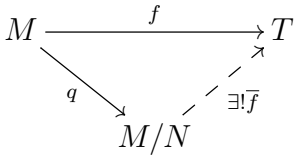
Example 1.42. If R is a field, quotient modules are the same thing as quotient vector spaces. When $R = \mathbb{Z}$, recall that $\mathbb{Z}$-modules are the same as abelian groups, by Lemma 1.13. Quotients of $\mathbb{Z}$-modules coincide with quotients of abelian groups.

Theorem 1.43. *Let N be a submodule of M, let T be an R-module, and let $f : M \to T$ be an R-module homomorphism. If $N \subseteq \ker f$, then the function*

$$\begin{aligned} M/N &\xrightarrow{\overline{f}} T \\ m + N &\longmapsto f(m) \end{aligned}$$

is a well-defined R-module homomorphism. In fact, $\overline{f} : M/N \to T$ is the unique R-module homomorphism such that $\overline{f} \circ q = f$, where $q \colon M \to M/N$ denotes the canonical map.

We can represent this in a more visual way by saying that $\overline{f}$ is the unique R-module homomorphism that makes the diagram



commute.

Proof. By 817, we already know that $\overline{f}$ is a well-defined homomorphism of groups under $+$ and that it is the unique one such that $\overline{f} \circ q = f$. It remains only to show $\overline{f}$ is an R-linear map:

$$\overline{f}(r(m+N)) = \overline{f}(rm+N) = f(rm) = rf(m) = r\overline{f}(m+N).$$

where the third equation uses that f preserves scaling. □

Theorem 1.44 (First Isomorphism Theorem)**.** *Let N be an R-module and let $h : M \to N$ be an R-module homomorphism. Then* $\ker(h)$ *is a submodule of M and there is an R-module isomorphism* $M/\ker(h) \cong \operatorname{im}(h)$.

Proof. If we forget the multiplication by scalars in R, by the First Isomorphism Theorem for Groups, we know that there is an isomorphism of abelian groups under $+$, given by

$$\begin{aligned} \overline{h} : M/\ker(h) &\xrightarrow{\cong} \operatorname{im}(h) \\ m + \ker(f) &\longmapsto h(m). \end{aligned}$$

It remains only to show this map preserves multiplication by scalars. And indeed:

$$\begin{aligned} \overline{h}(r(m+\ker(h))) &= \overline{h}(rm + \ker(h)) && \text{by definition of the } R\text{-action on } M/\ker(h) \\ &= h(rm) && \text{by definition of } \overline{h} \\ &= rh(m) && \text{since } h \text{ is an } R\text{-module homomorphism} \\ &= r\overline{h}(m + \ker h) && \text{by definition of } h. \end{aligned}$$

Theorem 1.45 (Second Isomorphism Theorem)**.** *Let A and B be submodules of M, and let $A+B=\{a+b \mid a\in A, b\in B\}$. Then $A+B$ is a submodule of M, $A\cap B$ is a submodule of A, and there is an R-module isomorphism $(A+B)/B\cong A/(A\cap B)$.*

Proof. By Exercise 3, $A+B$ and $A\cap B$ are submodules of M. By the Second Isomorphism Theorem for Groups, there is an isomorphism of abelian groups

$$\begin{aligned} h\colon A/(A\cap B) &\xrightarrow{\cong} (A+B)/B \\ a+(A\cap B) &\longmapsto a+B \end{aligned}$$

It remains only to show h preserves multiplication by scalars:

$$h(r(a+(A\cap B))) = h(ra+A\cap B) = ra+B = r(a+B) = rh(a+(A\cap B)). \qquad \square$$

Theorem 1.46 (Third Isomorphism Theorem)**.** *Let A and B be submodules of M with $A\subseteq B$. Then there is an R-module isomorphism $(M/A)/(B/A)\cong M/B$.*

Proof. From 817, we know that B/A is a subgroup of M/A under $+$. Given $r\in R$ and $b+A\in B/A$ we have $r(b+A)=rb+A$ which belongs to B/A since $rb\in B$. This proves B/A is a submodule of M/A. By the Third Isomorphism Theorem for Groups, there is an isomorphism of abelian groups

$$\begin{aligned} (M/A)/(B/A) &\longrightarrow M/B \\ (m+A)+B/A &\longmapsto m+B \end{aligned}$$

and it remains only to show this map is R-linear:

$$\begin{aligned} h(r((m+A)+B/A)) =& h(r(m+A)+B/A) = h((rm+A)+B/A) \\ &= rm+B = r(m+B) \\ &= rh((m+A)+B/A). \qquad \square \end{aligned}$$

Theorem 1.47 (Lattice Isomorphism Theorem)**.** *Let R be a ring, let N be a R-submodule of an R-module M, and let $q\colon M\to M/N$ be the quotient map. Then the function*

$$\begin{aligned} \{R\text{-submodules of } M \text{ containing } N\} &\xrightarrow{\Psi} \{R\text{-submodules of } M/N\} \\ K &\longmapsto K/N \end{aligned}$$

is a bijection, with inverse defined by

$$\Psi^{-1}(T) := q^{-1}(T) = \{a\in M \mid a+N\in T\}$$

for each R-submodule T of M/N. Moreover, Ψ and Ψ^{-1} preserve sums and intersections of submodules.

Proof. From 817, we know there is a bijection between the set of subgroups of M and that contain N and subgroups of the quotient group M/N, given by the same map Ψ. We just need to prove that these maps send submodules to submodules. If K is a submodule of M containing N, then by the Third Isomorphism Theorem we know that K/N is a submodule of M/N. If T is a submodule of M/N, then $\pi^{-1}(T)$ is an abelian group, by 817. For $r \in R$ and $m \in \pi^{-1}(T)$, we have $\pi(m) \in T$, and hence $\pi(rm) = r\pi(m) \in T$ too, since T is a submodule. This proves $\pi^{-1}(T)$ is a submodule. □

We come to a very important class of examples which will help us study linear transformations using module theory.

Lemma 1.48 ($F[x]$-modules)**.** *Let F be a field. There is a bijection*

$$\{V \text{ an } F[x]\text{-module}\} \longleftrightarrow \{V \text{ an } F\text{-vector space and } T \in \mathrm{End}_F(V)\}.$$

Proof. If V is an $F[x]$ module then V is an F-vector space by restriction of scalars along the inclusion $F \hookrightarrow F[x]$. Let $T : V \to V$ be defined by $T(v) = xv$. It can be shown that $T \in \mathrm{End}_F(V)$ since $T(v_1+v_2) = x(v_1+v_2) = xv_1+xv_2 = T(v_1)+T(v_2)$ and $T(cv) = x(cv) = c(xv)$ for any $c \in F$, $v, v_1, v_2 \in V$ by the axioms of the $F[x]$-module.

Conversely, let V be an F-vector space and $T \in \mathrm{End}_F(V)$. Consider the evaluation homomorphism $\varphi : F[x] \to \mathrm{End}_F(V)$, $\varphi(f(x)) = f(T)$. (For example, if $f(x) = x^2 + 5$ then $\varphi(f(x)) = T \circ T + 5 \cdot \mathrm{id}_V$.) Since V is an $\mathrm{End}_F(V)$-module by Remark 1.38, then V is also an $F[x]$-module by restriction of scalars along ϕ. Concretely, this action is given by

$$f(x)v = (f(T))(v).$$

(For example, if $f(x) = x^2 + 5$, then $f(x)v = T(T(v)) + 5v$.) □

Notation 1.49. We shall denote the $F[x]$-module structure on an F-vector space V induced by $T \in \mathrm{End}_F(V)$ by V_T.

Example 1.50. The proposition above says that if we fix an F-vector space V then any linear transformation T gives a different $F[x]$ module structure on V. For example,

- for $T = 0$ the $F[x]$ module V_0 carries an action given by scaling by the constant coefficient of f, that is if $f(x) = a^n x^n + \cdots + a_0$ then
$$f(x)v = (f(0))v = a_0 v \text{ for all } f \in F[x].$$
- for T the "shift operator" that takes $T(e_i) = e_{i-1}$, where e_i is the i-th standard basis vector, the $F[x]$ module V_T is has the action $x^m \begin{bmatrix} v_1 \\ \vdots \\ v_{n-m} \\ v_{n-m+1} \\ \vdots \\ v_n \end{bmatrix} = \begin{bmatrix} v_{m+1} \\ \vdots \\ v_n \\ 0 \\ \vdots \\ 0 \end{bmatrix}$.

1.5 Module generators, bases and free modules

Definition 1.51. Let M be an R-module. A **linear combination** of finitely many elements $a_1, ..., a_n$ of M is an element of M of the form $r_1m + 1 + \cdots + r_nm_n$ for some $r_1, \ldots, r_n \in R$.

Definition 1.52. Let R be a ring with $1 \neq 0$ and let M be an R-module. For a subset A of M, the submodule of M **generated by** A is

$$RA := \{r_1a_1 + \cdots + r_na_n \mid n \geq 0, r_i \in R, a_i \in A\}.$$

We M is **generated by** A if $M = RA$. If M is an F-vector space, we say that M is **spanned by** a set A instead of generated by A.

A module M is **finitely generated** if there is a finite subset A of M that generates M. If $A = a$ has a single element, the module $RA = Ra$ is called *cyclic*.

Exercise 9. Let M be an R-module and let $A \subseteq M$. Then RA is the smallest submodule of M containing A, that is

$$RA \quad = \bigcap_{A \subseteq N, N \text{ submodule of } M} N.$$

Exercise 10. Being finitely generated and being cyclic are R-module isomorphism invariants.

Example 1.53. Let R be a ring with $1 \neq 0$.

(1) $R = R1$ is cyclic.

(2) $R \oplus R$ is generated by $\{(1, 0), (0, 1)\}$.

(3) $R[x]$ is generated as an R-module by the set $\{1, x, x^2, \ldots, x^n, \ldots\}$ of monic monomials in the variable x.

(4) Let $M = \mathbb{Z}[x, y]$. M is generated by

- $\{1, x, y\}$ as a ring,
- $\{1, y, y^2, \ldots, y^n, \ldots\}$ as an $\mathbb{Z}[x]$-module, and
- $\{x^iy^j \mid i, j \in \mathbb{Z}_{\geqslant 0}\}$ as a group ($\mathbb{Z}$-module).

Lemma 1.54. *Let R be a ring with $1 \neq 0$, let M be an R-module, and let N be an R-submodule of M.*

(1) If M is finitely generated as an R-module, then so is M/N.

(2) If N and M/N are finitely generated as R-modules, then so is M.

Proof. The proof of (2) will be a problem set question. To show (1), note that if $M = RA$ then $M/N = R\bar{A}$, where $\bar{A} = \{a + N \mid a \in A\}$. □

Definition 1.55. Let M be an R-module and let A be a subset of M. The set A is **linearly independent** if whenever $r_1, \ldots, r_n \in R$ and $a_1, \ldots, a_n$ are distinct elements of A satisfying $r_1a_1 + \cdots + r_na_n = 0$, then $r_1 = \cdots = r_n = 0$. Otherwise A is **linearly dependent**.

Definition 1.56. A subset A of an R-module M is a **basis** of M if A is linearly independent and generates M. An R-module M is a **free** R-module if M has a basis.

We will later see that over a field, every module is free. However, when R is not a field, there are R-modules that are not free; in fact, *most* modules are not free.

Example 1.57. Here are some examples of free modules:

(1) If we think of R as a module over itself, it is free with basis $\{1\}$.

(2) The module $R \oplus R$ is free with basis $\{(1,0),(0,1)\}$.

(3) The R-module $R[x]$ is free, and $\{1, x, x^2, \ldots, x^n, \ldots\}$ is a basis.

(4) Let $M = \mathbb{Z}[x,y]$. Then $\{1, y, y^2, \ldots, y^n, \ldots\}$ is a basis for the $\mathbb{Z}[x]$-module M, and $\{x^iy^j \mid i,j \in \mathbb{Z}_{\geqslant 0}\}$ is a basis for the $\mathbb{Z}$-module M.

Example 1.58. $\mathbb{Z}/2$ is not a free $\mathbb{Z}$-module. Indeed suppose that A is a basis for $\mathbb{Z}/2$ and $a \in A$. Then $2a = 0$ so A cannot be linearly independent, a contradiction.

Lemma 1.59. *If A is a basis of M then every nonzero element $0 \neq m \in M$ can be written uniquely as $m = r_1a_1 + \cdots + r_na_n$ with a_i distinct elements of A and $r_i \neq 0$.*

Proof. Suppose that if $m \neq 0$ and A_1, A_2 are finite subsets of A such that

$$m = \sum_{a \in A_1} r_a a = \sum_{b \in A_2} s_b b$$

for some $r_a, s_b \in R$. Then

$$\sum_{a \in A_1 \cap A_2} (r_a - s_a)a + \sum_{a \in A_1 \setminus A_2} r_a a - \sum_{a \in A_2 \setminus A_1} s_a a = 0.$$

Since A is a linearly independent set, we conclude that $r_a = s_a$ for $a \in A_1 \cap A_2$, $r_a = 0_R$ for $a \in A_1 \setminus A_2$, and $s_a = 0_R$ for $a \in A_2 \setminus A_1$. Set

$$B := \{a \in A_1 \cap A_2 \mid r_a \neq 0_R\}.$$

Then

$$m = \sum_{a \in B} r_a a$$

is the unique way of writing m as a linear combination of elements of A with nonzero coefficients. □

Theorem 1.60. *Let R be a ring, M be a free R-module with basis B, N be any R-module, and let $j : B \to N$ be any function. Then there is a unique R-module homomorphism $h : M \to N$ such that $h(b) = j(b)$ for all $b \in B$.*

Proof. We have two things to prove: existence and uniqueness.
Existence: By Lemma 1.59, any $0 \neq m \in M$ can be written uniquely as

$$m = r_1 b_1 + \cdots + r_n b_n$$

with $b_i \in B$ distinct and $0 \neq r_i \in R$. Define $h \colon M \to N$ by

$$\begin{cases} h(r_1 b_1 + \cdots + r_n b_n) = r_1 j(b_1) + \cdots + r_n j(b_n) & \text{if } r_1 b_1 + \cdots + r_n b_n \neq 0 \\ h(0_M) = 0_N \end{cases}$$

One can check that this satisfies the conditions to be an R-module homomorphism (exercise!).

Uniqueness: Let $h : M \to N$ be an R-module homomorphism such that $h(b_i) = j(b_i)$. Then in particular $h \colon (M, +) \to (N, +)$ is a group homomorphism and therefore $h(0_m) = 0_N$ by properties of group homomorphisms. Furthermore, if $m = r_1 b_1 + \cdots + r_n b_n$ then

$$h(m) = h(r_1 b_1 + \cdots + r_n b_n) = r_1 h(b_1) + \cdots + r_n h(b_n) = r_1 j(b_1) + \cdots + r_n j(b_n)$$

by the definition of homomorphism, and because $h(b_i) = j(b_i)$. □

Corollary 1.61. *If A and B are sets of the same cardinality, and fix a bijection $j : A \to B$. If M and N are free R-modules with bases A and B respectively, then there is an isomorphism of R-modules $M \cong N$.*

Proof. Let $g : M \to N$ and $h : N \to M$ be the module homomorphisms induced by the bijection $j : A \to B$ and its inverse $j^{-1} : B \to A$, which exist by Theorem 1.60. We will show that h and g are inverse homomorphisms. First, note that $g \circ h : N \to N$ is an R-module homomorphism and $(g \circ h)(b) = g(j^{-1}(b)) = j(j^{-1}(b)) = b$ for every $b \in B$. Since the identity map id_N is an R-module homomorphism and $id_N(b) = b$ for every $b \in B$, by the uniqueness in Theorem 1.60 we have $g \circ h = \mathrm{id}_n$. Similarly, one shows that $h \circ g = \mathrm{id}_M$. □

The corollary gives that, up to isomorphism, there is only one free module with basis A, provided such a module exists. But does a free module generated by a given set A exist? It turns out it does.

Definition 1.62. Let R be a ring and let A be a set. The free R-module generated by A, denoted $F_R(A)$ is the set of formal sums

$$\begin{aligned} F_R(A) &= \{r_1 a_1 + \cdots + r_n a_n \mid n \geq 0, r_i \in R, a_i \in A\} \\ &= \left\{ \sum_{a \in A} r_a a \mid r_a \in R, r_a = 0 \text{ for all but finitely many } a \right\}, \end{aligned}$$

with addition defined by

$$\left(\sum_{a \in A} r_a a \right) + \left(\sum_{a \in A} s_a a \right) = \sum_{a \in A} (r_a + s_a) a$$

and R-action defined by

$$r \left(\sum_{a \in A} r_a a \right) = \sum_{a \in A} (r r_a) a.$$

Exercise 11. This construction $F_R(A)$ results in an R-module, which is free with basis A, and $F_R(A) \cong \bigoplus_{a \in A} R$.

Index