

# Introduction to Modern Algebra II

---

Math 818 Spring 2023

January 25, 2023

# Contents

<b>1</b>	<b>Modules</b>	<b>2</b>
1.1	Basic assumptions . . . . .	2
1.2	Modules: definition and examples . . . . .	4
1.3	Submodules and restriction of scalars . . . . .	7
1.4	Module homomorphisms and isomorphisms . . . . .	8

# 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  $1_R$  if 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,  $M_n(R)$  (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  $f: R \rightarrow S$  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  $f: \mathbb{R} \rightarrow M_2(\mathbb{R})$  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  $\mathbb{Z} \rightarrow R$ .

**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  $R \times M \rightarrow M$  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  $M \times R \rightarrow M$ ,  $(m, r) \mapsto mr$ , 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.  $\square$

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  $\ell = 0, m \geq 1$  and  $d_i \mid n$  for  $1 \leq i \leq m$  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 an  $R$ -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  $R[x_1, \dots, x_n]$  is an  $R$ -module for any  $n \geq 1$ . 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  $M_n(R)$  denote set of  $n \times n$  matrices with entries in  $R$ . Then  $M_n(R)$  is an  $R$ -module for  $n \geq 1$ , 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

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

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

$$\begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} + \begin{bmatrix} r'_1 \\ \vdots \\ r'_n \end{bmatrix} = \begin{bmatrix} r_1 + r'_1 \\ \vdots \\ r_n + r'_n \end{bmatrix} \quad \text{and} \quad r \begin{bmatrix} r_1 \\ \vdots \\ r_n \end{bmatrix} = \begin{bmatrix} rr_1 \\ \vdots \\ rr_n \end{bmatrix}.$$

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

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.

### 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  $n \in N$ .

**Lemma 1.16** (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.* Exercise. □

**Example 1.17.**

- (1) Let  $R$  be a ring and let  $M$  be a subset of  $R$ . Then  $M$  is a left (right)  $R$ -submodule of  $R$  if and only if  $M$  is a left (right) ideal of  $R$ .
- (2) Let  $R$  be a commutative ring with  $1 \neq 0$ , let  $I$  be an ideal of  $R$  and let  $M$  be an  $R$ -module. Then one can prove that

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

is a submodule of  $M$ .

**Example 1.18.** If  $R$  is a field, submodules are the same thing as subspaces. If  $R = \mathbb{Z}$ , then recall that  $\mathbb{Z}$ -modules are the same as abelian groups, by Lemma 1.13. Submodules of  $\mathbb{Z}$ -modules coincide with the subgroups of abelian groups.

**Definition 1.19.** Let  $R$  be a ring with  $1 \neq 0$  and let  $M$  be an  $R$ -module. Given elements  $m_1, \dots, m_n \in M$ , the **submodule generated by**  $m_1, \dots, m_n$  is the subset of  $M$  given by

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

**Exercise 2.** Let  $R$  be a ring with  $1 \neq 0$  and  $M$  be an  $R$ -module. Given  $m_1, \dots, m_n \in M$ , the submodule generated by  $m_1, \dots, m_n$  is a submodule of  $M$ . Moreover, this is the smallest submodule of  $M$  that contains  $m_1, \dots, m_n$ , meaning that every submodule of  $M$  containing  $m_1, \dots, m_n$  must contain  $Rm_1 + \dots + Rm_n$ .

**Definition 1.20.** Let  $R$  be a ring with  $1 \neq 0$ . An  $R$ -module  $M$  is **finitely generated** if there exist elements  $m_1, \dots, m_n$  such that  $M = Rm_1 + \dots + Rm_n$ .

**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

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

We will discuss finitely generated modules and sets of generators in more detail later.

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. Note that in general a particular abelian group might be given many module structures over different rings.



**Lemma 1.22** (Restriction of scalars). *Let  $\phi : R \rightarrow S$  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  $R$ -module  $M$  may be regarded via restriction of scalars as a left  $S$ -module with  $S$ -action defined by the action of the elements of  $s$  viewed as elements of  $R$ .*

*Proof.* Let  $r, s \in R$  and  $m, n \in M$ . One checks that the properties in the definition of 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. □

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

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

Note that the second module structure on  $M$  obtained via restriction of scalars is induced by the original module structure, so the two structures are related. In general, however, it is possible to give different module structures on the same abelian group over different rings that are unrelated to each other.

## 1.4 Module homomorphisms and isomorphisms

**Definition 1.24.** Let  $R$  be a ring and let  $M$  and  $N$  be  $R$ -modules. An  **$R$ -module homomorphism** from  $M$  to  $N$  is a function  $f: M \rightarrow N$  such that for all  $r \in R$  and  $m, n \in M$  we have

- $f(m + n) = f(m) + f(n)$ , so that  $f$  is a homomorphism of abelian groups, and
- $f(rm) = rf(m)$ .

**Definition 1.25.** Let  $F$  be a field and let  $M$  and  $N$  be vector spaces over  $F$ . A **linear transformation** from  $M$  to  $N$  is an  $F$ -module homomorphism  $M \rightarrow N$ .

**Example 1.26.** Let  $R$  be a commutative ring and  $M$  be an  $R$ -module. For each  $r \in R$ , the map  $\mu_r: M \rightarrow M$  given by multiplication by  $r$ , meaning the map defined 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 1.27.** An  $R$ -module homomorphism  $h$  is an  **$R$ -module isomorphism** if  $h$  is also a bijection. Two modules  $M$  and  $N$  are **isomorphic** if there exists an isomorphism between them, in which case we write  $M \cong N$ .

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.

**Lemma 1.28.** *Let  $R$  be a ring with  $1 \neq 0$  and let  $M$  be an  $R$ -module.*

- (1) *Let  $N$  be an  $R$ -submodule of  $M$ . Then the inclusion map  $i: N \rightarrow M$  is an  $R$ -module homomorphism.*
- (2) *If  $f: M \rightarrow N$  is an  $R$ -module homomorphism, then  $\ker(f)$  is an  $R$ -submodule of  $M$  and  $\operatorname{im}(f)$  is an  $R$ -submodule of  $N$ .*

*Proof.* Exercise. □

**Definition 1.29.** Let  $R$  be a ring and let  $M$  and  $N$  be  $R$ -modules. Then  $\operatorname{Hom}_R(M, N)$  denotes the set of all  $R$ -module homomorphisms from  $M$  to  $N$ , and  $\operatorname{End}_R(M)$  denotes the set  $\operatorname{Hom}_R(M, M)$ . We call  $\operatorname{End}(M)$  the **endomorphism ring** of  $M$ , and elements of  $\operatorname{End}(M)$  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. Note, however, that two homomorphisms from  $M$  to  $N$  are not composable unless  $M = N$ , so  $\operatorname{Hom}_R(M, N)$  is not a ring. It is, however, an  $R$ -module. Given  $f, g \in \operatorname{Hom}_R(M, N)$ ,  $f + g$  is the  $R$ -module homomorphism defined by

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

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

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

**Lemma 1.30.** *Let  $M$  and  $N$  be  $R$ -modules. Then the addition and multiplication by scalars defined above make  $\operatorname{Hom}_R(M, N)$  an  $R$ -module.*

*Proof.* There are many things to check, including:

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

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  $\operatorname{End}_F(V) \cong M_n(F)$ . This says that every linear transformation  $T: V \rightarrow V$  corresponds to an  $n \times n$  matrix. However, the story for general  $R$ -modules is a lot more complicated.

**Lemma 1.31.** *For any commutative ring  $R$  with  $1 \neq 0$  and any  $R$ -module  $M$  there is an isomorphism of  $R$ -modules  $\text{Hom}_R(R, M) \cong M$ .*

*Proof.* Let  $f : M \rightarrow \text{Hom}_R(R, M)$  be given for each  $m \in M$  by  $f(m) = \phi_m$  where  $\phi_m$  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  $\text{Hom}_R(R, M)$ , 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  $\phi_m$  means that  $m = m'$ .
- $f$  is surjective, since for  $\psi \in \text{Hom}_R(R, M)$  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.  $\square$

**Definition 1.32.** 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  $f : R \rightarrow A$  such that  $f(R)$  is contained in the center of  $A$ .

An  $R$ -algebra is a ring with an  $R$ -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  $A$ .

**Example 1.33.** Let  $R$  be a commutative ring with  $1_R \neq 0_R$ . The ring  $R[x_1, \dots, x_n]$  together with the inclusion map  $R \hookrightarrow R[x_1, \dots, x_n]$  is an  $R$ -algebra. More generally, any quotient of  $R[x_1, \dots, x_n]$  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 1.34.** *Let  $R$  be a commutative ring with  $1 \neq 0$  and let  $M$  be an  $R$ -module. Then  $\text{End}_R(M)$  is an  $R$ -algebra, with addition and  $R$ -action defined as above, and multiplication defined by composition  $(fg)(m) = f(g(m))$  for all  $f, g \in \text{End}_R(M)$  and all  $m \in M$ .*

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

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

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

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

and

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

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

**Remark 1.35.** Let  $R$  be a commutative ring with  $1 \neq 0$  and let  $M$  be an  $R$ -module. Then  $M$  is also an  $(\text{End}_R(M))$  module with the action  $\phi m = \phi(m)$  for any  $\phi \in \text{End}_R(M)$ ,  $m \in M$ .

**Definition 1.36.** 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 1.37.** *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  $q : M \rightarrow M/N$  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  $rm + N = rm' + N$ .  $\square$

**Example 1.38.** 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.

# Index

- $IM$ , 7
- $M \cong N$ , 9
- $R$ -algebra, 10
- $R$ -module, 4
- $R$ -module homomorphism, 8
- $R$ -module isomorphism, 9
- $R$ -submodule, 7
- absorption, 3
- commutative ring, 2
- cyclic, 7
- division ring, 3
- domain, 3
- endomorphism ring, 9
- endomorphisms, 9
- field, 3
- finitely generated module, 7
- free module, 6
- generated by, 7
- ideal, 3
- integral domain, 3
- isomorphic, 9
- left  $R$ -module, 4
- left ideal, 3
- linear transformation, 8
- nontrivial ideal, 3
- proper ideal, 3
- restriction of scalars, 8
- right  $R$ -module, 4
- right ideal, 3
- ring, 2
- ring homomorphism, 3
- ring of scalars, 7
- submodule generated by, 7
- subring, 3
- trivial ideals, 3
- vector space, 5
- zerodivisors, 3