

# 1. Modules

## Modules: Basics

### How to think of modules

- Modules are to rings as vector spaces are to fields.
- Modules are to rings as sets with group actions are to groups.

### Definition of (left) modules

**Definition:** Let  $R$  be a ring (for now, not necessarily commutative and not necessarily having a unit). A *left  $R$ -module* is an abelian group  $M$  together with a map  $R \times M \rightarrow M$  (written  $(r, m) \mapsto rm$ ) such that:

- $r(m_1 + m_2) = rm_1 + rm_2$
- $(r_1 + r_2)m = r_1m + r_2m$
- $r_1(r_2m) = (r_1r_2)m$

If  $R$  has a unit element 1, we also require  $1m = m$  for all  $m \in M$ .

### Right modules

A right module is defined by a map  $M \times R \rightarrow M$  and written  $(m, r) \mapsto mr$  and satisfying the property

$$(mr_1)r_2 = m(r_1r_2).$$

If  $R$  is not commutative, these really are different, since for a left module:

- $r_1r_2$  acts by "first  $r_2$ , then  $r_1$ "

while for a right module

- $r_1r_2$  acts by "first  $r_1$ , then  $r_2$ ."

### Left and Right modules

If  $R$  is commutative, and  $M$  is a left  $R$ -module, then we can define a right  $R$  module  $M'$  with the same underlying abelian group  $M$  and by defining  $m'r = (rm)'$ . This works because

$$(m'r_1)r_2 = (r_1m)'r_2 = (r_2(r_1m))' = ((r_2r_1)m)' = ((r_1r_2)m)' = m'(r_1r_2)$$

### Remarks

#### Vector spaces

If  $R$  is a field, then a left (or right)  $R$ -module is the same as a vector space.

#### Another definition

If  $M$  is an abelian group, and  $R$  is a ring, then a left  $R$ -module structure on  $M$  is the same as a ring map

$$R \rightarrow \text{End}(M).$$

If  $\phi_r$  is the endomorphism associated to  $r \in R$ , then  $rm = \phi_r(m)$ . The associativity comes from defining the ring structure on

$$\text{End}(M)$$

as the usual composition of functions:

$$\phi_{r_1r_2} = \phi_{r_1} \circ \phi_{r_2}.$$

### Submodules

**Definition:** If  $M$  is a left  $R$ -module, then a submodule  $N$  of  $M$  is a subgroup with the property that, if  $n \in N$ , then  $rn \in N$  for all  $r \in R$ .

**Observation:** A ring  $R$  is a left module over itself by ring multiplication. The (left) ideals of  $R$  are *exactly the left submodules of  $R$* .

### Essential examples

#### Rings as modules over themselves

- Every ring  $R$  is a left module over itself. The submodules of  $R$  are the left ideals.
- $R$  is also a right module over itself, with the right ideals being the right submodules.

If  $F$  is a field and  $n > 1$ , let  $R = M_n(F)$  be the  $n \times n$  matrix ring over  $F$ . The matrices with arbitrary first column and zeros elsewhere form a left ideal  $J$  and therefore a left submodule of  $R$  as left  $R$ -module. But  $J$  is *not* a right  $R$ -submodule.

A field  $F$  is a one-dimensional vector space over itself, and a commutative ring  $R$  is a module (left and right) over itself with the ideals of  $R$  being the submodules.

## Free modules

Let  $R$  be a ring with unity and let  $n \geq 1$  be a positive integer. Then

$$R^n = \{(r_1, \dots, r_n) : r_i \in R \text{ for } i = 1, \dots, n\}$$

is an  $R$  module with componentwise addition and multiplication given by  $r(r_1, \dots, r_n) = (rr_1, \dots, rr_n)$ .

This is called the *free  $R$ -module of rank  $n$* .

## Free modules and vector spaces

- If  $R$  is a field, the free  $R$ -module of rank  $n$  is an  $n$ -dimensional vector space.
- The submodules of a finite dimensional vector space are all subspaces which are copies of  $R^k$  for  $k \leq n$ .
- For more general  $R$  the picture is more complicated. Let  $R = \mathbb{Z}$  and  $M = \mathbb{Z}^2$ . Then:
  - $\{(n, 0) : n \in \mathbb{Z}\}$  is a submodule of  $M$  which “looks like” a subspace.
  - $2M = \{(a, b) : a, b \in 2\mathbb{Z}\}$  is a submodule of  $M$  which does not.

## Change of rings (restriction of scalars)

- An abelian group  $M$  may be an  $R$  module for different rings  $R$ . For example:
  - $\mathbb{Q}$  is a module over  $\mathbb{Q}$ , where it is a one dimensional vector space and its only  $\mathbb{Q}$ -submodules are 0 and itself.
  - $\mathbb{Q}$  is a module over  $\mathbb{Z}$ , and it has many  $\mathbb{Z}$ -submodules, such as  $\mathbb{Z}[1/2]$ .

More generally, if  $R \subset S$  is a subring, and  $M$  is an  $S$ -module, then it is an  $R$ -module. This is called *restriction of scalars*.

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

Let  $M$  be an abelian group. Then it is automatically a  $\mathbb{Z}$ -module where we define

$$nx = \overbrace{x + x + \dots + x}^n.$$

Furthermore, given any  $\mathbb{Z}$ -module, it must be the case that

$$nx = (\overbrace{1 + 1 + \dots + 1}^n)x = \overbrace{x + x + \dots + x}^n.$$

(Note: this is why we require  $1x = x$  when  $R$  is a ring with unity in the module axioms).

Further, submodules of  $M$  (as  $\mathbb{Z}$ -module) are just the subgroups of  $M$  (as abelian group).

### Change of rings (quotients)

Suppose that  $M$  is a left  $R$  module and  $I \subset R$  is a two-sided ideal with the property that, for all  $y \in I$ , and all  $x \in M$ , we have  $yx = 0$ . In this case we say that  $I$  annihilates  $M$  or that  $IM = 0$ .

With this hypothesis, we may view  $M$  as an  $R/I$  module by defining  $(r + I)m = rm$  for any coset representative  $r + I \in R/I$ . This is well-defined since two different coset representatives  $r, r'$  satisfy  $r' = r + i$  for some  $i \in I$  and therefore  $r'm = (r + i)m = rm$  since  $im = 0$ .

If  $M$  is an abelian group and  $m \in \mathbb{Z}$  is a positive integer such that  $mM = 0$ , then  $M$  can be viewed as a module over  $\mathbb{Z}/m\mathbb{Z}$  by this process.

This operation is a special case of a general operation called *base change* or *extension of scalars* that we will study in more detail later.

## Modules over $F[x]$

### Basic construction

Let  $F$  be a field, let  $V$  be a vector space over  $F$ , and let  $T : V \rightarrow V$  be an  $F$ -linear transformation. Define a homomorphism

$$F[x] \rightarrow \text{End}(V)$$

by sending

$$x^k \mapsto T^k = \overbrace{T \circ T \circ \cdots \circ T}^n.$$

This construction makes  $V$  into a module for  $F[x]$  which depends on the choice of the linear transformation  $T$ .

### Polynomials and linear transformations

For example let  $V = F^2$  and let  $T$  be the linear transformation given by the matrix

$$T = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$$

If  $e_0$  and  $e_1$  are the standard basis elements of  $F^2$  then

$$\begin{aligned} T e_0 &= e_1 \\ T^2 e_0 = T e_1 &= e_0 + e_1 = e_0 + T e_0 = (1 + T) e_0 \end{aligned}$$

from which we see that  $(T^2 - T - 1)e_0 = 0$  and

$$(T^2 - T - 1)e_1 = (T^2 - T - 1)T e_0 = T(T^2 - T - 1)e_0 = 0$$

so the polynomial  $x^2 - x - 1$  is in the kernel of the map from  $F[x] \rightarrow \text{End}(V)$ .

By the base change construction above this means that  $V$  can be viewed as a module over  $F[x]/(x^2 - x - 1)$ .

### Characterization of $F[x]$ modules

We saw above that, given an  $F$ -vector space  $V$  with a linear transformation  $T$ , we get an  $F[x]$  module where  $x$  acts on  $V$  through  $T$ .

Conversely, suppose that  $M$  is an module over  $F[x]$ . Then  $M$  is an  $F$  vector space (via the restriction of scalars from  $F[x]$  to  $F$ ). Furthermore, the element  $x \in F[x]$  acts on  $M$  as an  $F$ -linear transformation because that's what the module axioms amount to.

Therefore there is an equivalence between

$$\{F[x]\text{-modules}\} \Leftrightarrow \{\text{vector spaces } V \text{ over } F \text{ with a given linear map } T : V \rightarrow V\}$$

### Submodules of $F[x]$ modules

In the correspondence above, a submodule of an  $F[x]$  module  $M$  corresponds to a subspace  $W \subset V$  that is *preserved by*  $T$ , meaning  $TW \subset W$ .

Thus, not all subspaces of  $V$  correspond to submodules.

In the example given earlier, the only  $T$ -stable proper subspace of  $V$  is the zero subspace.

If we consider instead the linear map on  $F^2$  satisfying  $Ue_0 = 0$  and  $Ue_1 = e_0$ , then the one dimensional subspace spanned by  $e_0$  is  $U$ -stable and  $F^2$  viewed as an  $F[x]$  module via  $U$  has a submodule corresponding to that subspace.

### Checking the submodule property

**Proposition:** A subset  $N$  of a left  $R$ -module  $M$  is a submodule if it is nonempty and, for all  $x, y \in N$  and  $r \in R$ , we have  $x + ry \in N$ . Alternatively, if  $N$  is a subgroup of the abelian group  $M$  and  $rN \subset N$  for all  $r \in R$  then  $N$  is a submodule.

## Algebras

**Definition:** Let  $R$  be a commutative ring with unity. An  $R$ -algebra is a (not necessarily commutative) ring  $S$  with a ring homomorphism  $f : R \rightarrow S$  carrying  $1_R$  to  $1_S$  such that  $f(R)$  is in the center of  $S$ .

The polynomial ring  $F[x]$  is an  $F$ -algebra, as is the matrix ring  $M_n(F)$  where the homomorphism  $f : F \rightarrow M_n(F)$  embeds  $F$  as the diagonal matrices. More generally, any  $F$ -algebra  $A$ , where  $F$  is a field, contains  $F$  in its center and the identities of  $A$  and  $F$  are the same.

The ring  $\mathbb{Z}/p\mathbb{Z}$  is a  $\mathbb{Z}$ -algebra. In fact any ring  $S$  with 1 is a  $\mathbb{Z}$  algebra by the map sending  $n \in \mathbb{Z}$  to  $n1_S$ .

The ring  $\mathbb{Q}[x]$  is a  $\mathbb{Z}[x]$  algebra.

We typically omit the explicit map  $f$  and just think of  $R$  as “contained in”  $A$ ; this can be misleading since  $f$  doesn’t need to be injective, but it works in practice.

## Algebra morphisms

**Definition:** A map of  $R$ -algebras  $f : A \rightarrow B$  is a ring homomorphism that is  $R$ -linear in the sense that  $f(ra) = rf(a)$  for all  $r \in R$  and  $a \in A$ .

Any homomorphism of rings with unity is a  $\mathbb{Z}$ -algebra morphism.

## Modules Homomorphisms, Quotient Modules, and Mapping Properties

### Module homomorphisms

**Definition:** Let  $R$  be a ring and let  $M$  and  $N$  be (left)  $R$ -modules. A function  $f : M \rightarrow N$  is an  $R$ -module homomorphism if:

- it is a homomorphism between the abelian group structures on  $M$  and  $N$
- it is  $R$ -linear, meaning  $f(rm) = rf(m)$  for all  $r \in R$ .

Note that, if  $R$  is a field, then  $M$  and  $N$  are vector spaces and an  $R$ -module homomorphism is just a linear map.

A module isomorphism is a bijective homomorphism.

We let  $\text{Hom}_R(M, N)$  denote the set of  $R$ -module homomorphisms from  $M$  to  $N$ .

### Kernels and images

Let  $R$  be a ring and let  $M$  and  $N$  be  $R$ -modules. Let  $f : M \rightarrow N$  be a homomorphism.

- Let  $\ker(f) = \{m \in M : f(m) = 0\}$  (the *kernel* of  $f$ ). This is a submodule of  $M$ .

- Let  $f(M) \subset N$  be the image of  $f$ . Then  $f(M)$  is a submodule of  $N$ .

### Quotient modules

Let  $M$  be an  $R$  module and let  $N \subset M$  be a submodule.

**Definition:** Let  $M/N$  be the quotient abelian group. Then  $M/N$  is an  $R$ -module where  $R$  acts on cosets by

$$r(x + N) = rx + N.$$

This is called the quotient module of  $M$  by  $N$ .

The  $R$ -module structure is well defined because if  $x + N = y + N$ , then  $x = y + n$  for some  $n \in N$ , and  $rx = ry + rn$ . Since  $N$  is a submodule,  $rn \in N$  so  $rx + N = ry + N$ .

Notice that  $N$  can be any submodule, there is no “normality” condition like for groups.

There is always a “projection” homomorphism  $\pi : M \rightarrow M/N$  defined by  $\pi(m) = m + N$  which has kernel  $N$ .

### Mapping Properties

Let  $M$ ,  $N$ , and  $K$  be  $R$  modules, and let  $f : M \rightarrow K$  be a homomorphism with  $N \subset \ker(f)$ . Then there is a unique homomorphism  $\bar{f} : M/N \rightarrow K$  making this diagram commutative:

$$\begin{array}{ccc} M & & \\ \downarrow \pi & \searrow f & \\ M/N & \xrightarrow{\bar{f}} & K \end{array}$$

### Isomorphism theorems

The isomorphism theorems for abelian groups give isomorphism theorems for modules.

- If  $f : M \rightarrow K$  is a homomorphism, then the map  $\bar{f}$  gives an isomorphism between  $M/\ker(f)$  and  $f(M) \subset K$ .
- $(M + N)/N$  is isomorphic to  $M/(M \cap N)$ .
- $(M/A)/(N/A)$  is isomorphic to  $M/N$ .
- There is a bijection between the lattice of submodules of  $M/N$  and submodules of  $M$  containing  $N$  given by  $K \leftrightarrow K/N$ .

The proofs of all of these facts are found by checking that the group isomorphisms respect the action of the ring  $R$ .

`<a href="slides/01-modules.html"> View as slides </a>`