1. Modules

Definition 1.1. *Let R be a commutative ring. A* ***module over*** *R is set M together with a binary operation, denoted $+$, which makes M into an abelian group, with 0 as the identity element, together with a rule of multiplication $\cdot$,*

$$R \times M \longrightarrow M \qquad (r, m) \longrightarrow r \cdot m,$$

such that the following hold,

(1) $1 \cdot m = m$,
(2) $(rs) \cdot m = r(s \cdot m)$,
(3) $(r + s) \cdot m = r \cdot m + s \cdot m$,
(4) $r \cdot (m + n) = r \cdot m + r \cdot n$,

for every r and $s \in R$ and m and $n \in M$.

We will also say that M is an R-module and often refer to the multiplication as scalar multipplication. There are three key examples of modules.

Suppose that F is a field. Then an F-module is precisely the same as a vector space. Indeed, in this case (1.1) is nothing more than the definition of a vector space.

Now suppose that $R = \mathbb{Z}$. What are the $\mathbb{Z}$-modules? Clearly given a $\mathbb{Z}$-module M, we get a group. Just forget the fact that one can multiply by the integers. On the other hand, in fact multiplication by an element of $\mathbb{Z}$ is nothing more than addition of the corresponding element of the group with itself the appropriate number of times. That is given an abelian group G, there is a unique way to make it into a $\mathbb{Z}$-module,

$$\mathbb{Z} \times G \longrightarrow G,$$

$$(n, g) \longrightarrow n \cdot g = g + g + g + \cdots + g$$

where we just add g to itself n times. Note that uniqueness is forced by (1) and (3) of (1.1), by an obvious induction. It follows then that the data of a $\mathbb{Z}$-module is precisely the same as the data of an abelian group.

Let R be a ring. Then R can be considered as a module over itself. Indeed the rule of multiplication as a module is precisely the rule of multiplication as a ring. The axioms for a ring, ensure that the axioms for a module hold.

It turns out to be extremely useful to have one definition of an object that captures all three notions: vector spaces, abelian groups and rings.

Here is a very non-trivial example. Let F be a field. What does a $F[x]$-module look like? Well obviously any $F[x]$-module is automatically a vector space over F. So we are given a vector space V, with the additional data of how to multiply by x. Multiplication by x induces a transformation of V. The axioms for a module ensure that this transformation is in fact linear.

On the other hand, suppose we are given a linear transformation ϕ of a vector space V. We can define an $F[x]$-module as follows. Given $v \in V$, and $f(x) \in F[x]$, define

$$f(x) \cdot v = f(\phi)v,$$

where we substitute x for ϕ. Note that ϕ^2, and so on, means just apply ϕ twice and that we can add linear transformations. Thus the data of an $F[x]$-module is exactly the data of a vector space over F, plus a linear transformation ϕ.

Note that the definition of $f(\phi)$ hides one subtelty. Suppose that one looks at polynomials in two variables $f(x, y)$. Then it does not really make sense to substitute for both x and y, using two linear transformations ϕ and ψ. The problem is that ϕ and ψ won't always commute, so that the meaning of xy is unclear (should we replace this by $\phi\psi$ of $\psi\phi$?). Of course the powers of a single linear transformation will automatically commute, so that this problem disappears for a polynomial of one variable.

Lemma 1.2. *Let $\phi\colon R \longrightarrow S$ be a ring homomorphism. Let M be an S-module.*

Then M is an R-module in a natural way.

Proof. It suffices to define a scalar multiplication map

$$R \times M \longrightarrow M$$

and show that this satisifies the axioms for a module.

Given $r \in R$ and $m \in M$, set

$$r \cdot m = \phi(r) \cdot M.$$

It is easy to check the axioms for a module. □

For example, every R-module M is automatically a $\mathbb{Z}$-module. There are two ways to see this. First every R-module is in particular an abelian group, by definition, and an abelian group is the same as a $\mathbb{Z}$-module. Second observe that there is a unique ring homomorphism

$$\mathbb{Z} \longrightarrow R$$

and this makes M into an R-module by (1.2).

Lemma 1.3. *Let M be an R-module. Then*

(1) $r \cdot 0 = 0$, for every $r \in R$.
(2) $0 \cdot m = 0$, for every $m \in M$.
(3) $-1 \cdot m = -m$, for every $m \in M$.

Proof. We have

$$\begin{aligned} r \cdot 0 &= r \cdot (0 + 0) \\ &= r \cdot 0 + r \cdot 0. \end{aligned}$$

Cancelling, we have (1). For (2), observe that

$$\begin{aligned} 0 \cdot m &= (0 + 0) \cdot m \\ &= 0 \cdot m + 0 \cdot m. \end{aligned}$$

Cancelling, gives (2). Finally

$$\begin{aligned} 0 &= 0 \cdot m \\ &= (1 + -1) \cdot m \\ &= 1 \cdot m + (-1) \cdot m \\ &= m + (-1) \cdot m, \end{aligned}$$

so that $(-1) \cdot m$ is indeed the additive inverse of m. □

Definition 1.4. *Let M and N be two R-modules.*

*An R-module **homomorphism** is a map*

$$\phi \colon M \longrightarrow N$$

such that

$$\phi(m + n) = \phi(m) + \phi(n) \qquad \text{and} \qquad \phi(rm) = r\phi(n).$$

We will also say that ϕ is R-linear.

In other words, ϕ is a homomorphism of groups that also respects scalar multiplication. If F is a field, then an F-linear map is the same as a linear map, in the sense of linear algebra. If $R = \mathbb{Z}$, a $\mathbb{Z}$-module homomorphism is nothing but a group homomorphism.

Note that we now have a category, the category of all R-modules; the objects are R-modules, and the morphisms are R-linear maps. Given any ring R, the associated category captures a lot of the properties of R.

Lemma 1.5. *Let M be an R-module and let $r \in R$.*

Then the natural map

$$M \longrightarrow M$$

given by $m \longrightarrow rm$ is R-linear.

Proof. Easy check left as an exercise for the reader. $\square$

Definition 1.6. *Let M be an R-module.*

*A **submodule** N of M is a subset that is a module with the inherited addition and scalar multiplication.*

Let F be a field. Then a submodule is the same as a subvector space. Let $R = \mathbb{Z}$. Then a submodule is the same as a subgroup. Consider R as a module over itself. Then a subset I is a submodule if and only if I is an ideal in the ring R.

Lemma 1.7. *Let M be an R-module and let N be a subset of M.*

Then N is a submodule of M if and only if it is closed under addition and scalar multiplication.

Proof. Easy exercise for the reader. $\square$

Definition-Lemma 1.8. *Let $\phi\colon M \longrightarrow N$ be an R-module homomorphism. The **kernel** of ϕ, denoted $\operatorname{Ker}\phi$, is the inverse image of the zero element of N.*

The kernel is a submodule.

Proof. Easy exercise for the reader. $\square$

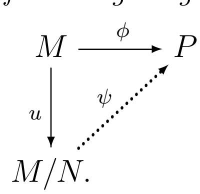
Definition-Lemma 1.9. *Let M be an R-module and let N be a submodule.*

*Then the quotient group M/N can be made into a **quotient module** in an obvious way. Furthermore there is a natural R-module homomorphism*

$$u\colon M \longrightarrow M/N,$$

which is universal in the following sense.

Let $\phi\colon M \longrightarrow P$ be any R-module homomorphism, whose kernel contains N. Then there is a unique induced R-module homomorphism $\psi\colon M \longrightarrow P$, such that the following diagram commutes,



Proof. Easy exercise for the reader. $\square$

As always, a standard consequence is:

Theorem 1.10. *Let*

$$\phi : M \longrightarrow N$$

be a surjective R-linear map, with kernel K.

Then

$$N \simeq M/K.$$

Definition 1.11. *Let M be an R-module and let X be a subset.*

*The R-module **generated by X, denoted** $\langle X \rangle$, is equal to the smallest submodule that contains X.*

*We say that the set X **generates** M if the submodule generated by X is the whole of M. We say that M is **finitely generated** if it is generated by a finite set. We say that M is **cyclic** if it is generated by a single element.*

Note that the definition of $\langle X \rangle$ makes sense; it is easy to adapt the standard arguments. Suppose that R is a field, so that an R-module is a vector space. Then a vector space is finitely generated if and only if it is of finite dimension and it is cyclic if and only if it has dimension at most one. If $R = \mathbb{Z}$, then these are the standard definitions.

Note that a ring R is automatically finitely generated. In fact it is cyclic, considered as a module over itself, generated by 1, that is $R = \langle 1 \rangle$. This is clear, since if $r \in R$, then $r = r \cdot 1 \in \langle 1 \rangle$. This is our first indication that the notion of being finitely generated is not strong enough.

Lemma 1.12. *Let M be a cyclic R-module.*

Then M is isomorphic to a quotient of R.

Proof. Let $m \in M$ be a generator of M. Define a map

$$\phi\colon R \longrightarrow M,$$

by sending $r \in R$ to rm. It is easy to check that this map is R-linear. Since the image of ϕ contains $m = \phi(1)$, and m generates M, it follows that ϕ is surjective. The result follows by the Isomorphism Theorem. □

Definition 1.13. *Let M and N be two R-modules.*

*The **direct sum of** M **and** N, denoted $M \oplus N$, is the R-module, which as a set is the Cartesian product of M and N, with addition and multiplication defined coordinate by coordinate:*

$$(m_1, n_1) + (m_2, n_2) = (m_1 + m_2, n_1 + n_2) \qquad \textit{and} \qquad r(m, n) = (rm, rn).$$

Note that the direct sum is a direct sum in the category of R-modules. Note that the direct sum of R with itself is generated by $(1, 0)$ and $(0, 1)$.

Definition 1.14. *Let M be an R-module.*

*We say that M is **free** if it is isomorphic to a direct sum of copies (possibly infinite) of R. We say that generators X of M are **free***

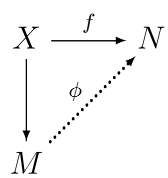
generators *if there is an identification of M with a direct sum of copies of R, under which the standard generators of the direct sum corresponds to X.*

Suppose that F is a field. Then a set of free generators for a vector space V is the same as a basis of V. Since every vector space admits a basis, it follows that every vector space is free. R is a free module over itself, generated by 1, or indeed by any unit.

A set of free generators, comes with an extremely useful universal property.

Lemma 1.15. *Let M be a free R-module, freely generated by X. Let N be any R-module and let $f \colon X \longrightarrow N$ be any map.*

Then there is unique induced ring homorphism $\phi \colon M \longrightarrow N$ which makes the following diagram commute



Proof. Let $m \in M$. By assumption, there are $x_1, x_2, \dots, x_k \in X$ and $r_1, r_2, \dots, r_k \in R$, such that

$$m = r_1 x_1 + r_2 x_2 + \cdots + r_k x_k.$$

In this case, we are obliged to send m to

$$r_1 f(x_1) + r_2 f(x_2) + \cdots + r_k f(x_k),$$

if we want ϕ to be a ring homomorphism. It suffices to check that this does indeed define an R-linear map, which is easy to check. □

If R is a field, this is equivalent to saying that a linear map is determined by its action on basis and that given any choice of where to send the elements of a basis, there is a unique linear map. One obvious consequence of (1.15) and (1.10) is that every module is a quotient of a free module, that is a direct sum of copies of R. In particular

Lemma 1.16. *Let M be a finitely generated R-module. Then M is a quotient of R^n, the direct sum of R with itself n times.*