Modules

A *module* M over a ring R is an abelian group together with a ring homomorphism $\phi : R \to \mathrm{End}(M)$.

Since there is a natural homomorphism from the ring of integers $\mathbb{Z}$ to any ring, we see that any abelian group M is a module over $\mathbb{Z}$. Thus, the notion of module generalises the natural "action" of integers on abelian groups.

Given an element a in R and an element m in M, we use the notation $a \cdot m$ for the result $\phi(a)(m)$ of applying the image of a to the element m.

Exercise: Use the fact that $\phi(a)$ is an endomorphism of M to show that if m' is another element of M, then $a \cdot (m + m') = a \cdot m + a \cdot m'$.

Exercise: Use the fact that ϕ preserves addition and the rule of addition of endomorphisms to show that $(a + b) \cdot m = a \cdot m + b \cdot m$ when b is another element of R.

Exercise: Use the rule of composition of endomorphisms and the fact that ϕ preserves multiplication to show that $a \cdot (b \cdot m) = (a \cdot b) \cdot m$.

Exercise: Use the fact that ϕ preserves multiplicative identity to show that $1 \cdot m = m$.

Exercise: Use the fact that ϕ preserves additive identity to show that $0 \cdot m = 0$ where the latter 0 is the additive identity in M.

In summary, we see that we have the identities:

- $a \cdot (m + m') = a \cdot m + a \cdot m'$
- $(a + b) \cdot m = a \cdot m + b \cdot m$
- $a \cdot (b \cdot m) = (a \cdot b) \cdot m$
- $1 \cdot m = m$ and $0 \cdot m = 0$

Exercise: Given an operation $a \cdot m$ of elements a of a ring R on elements m of an abelian group M satisfying the above identities. Check that $\phi(a)(m) = a \cdot m$ defines a ring homomorphism $R \to \mathrm{End}(M)$.

Note that in the special case where R is a field such as $R = \mathbb{Q}$ the field of rational numbers, the above conditions are exactly what are used to define the notion of a vector space over the field. Thus the notion of a module generalises to rings the notion of a vector space over a field.

A *submodule* N of M is a subgroup N of M with the additional property that for every a in R and n in N, we have $a \cdot n$ lies in N. In other words, N is closed under multiplication by elements of R.

Examples

A ring R is a module over itself! We already proved this when we studied the natural homomorphism $R \to \mathrm{End}(R)$.

Exercise: Show that $I \subset R$ is a submodule of R (as a module over R) if and only if I is an ideal of R.

More generally, we get (for free!) modules over a ring R by considering the set R^n of n-tuples of elements of R as a module over R by defining $a \cdot (a_1, \ldots, a_n) = (a \cdot a_1, \ldots, a \cdot a_n)$.

Exercise: Check that this operation makes R^n into a module over R.

The module R^n is called a *free* module over R. The basis theorem for vector spaces over a field asserts that every vector space over a field has a basis; in other words, it is (isomorphic to) a free module over a field. However, it is important to note that this **not** true for modules over other rings.

Exercise: Use the natural multiplication by integers to make $\mathbb{Z}/n$ a module over $\mathbb{Z}$. This is *not* a free module unless $n = 0$!

Note that the natural multiplication is a consequence of the natural ring homomorphism $\mathbb{Z} \to \mathbb{Z}/n$. This can be generalised as follows.

Exercise: Given a ring homomorphism $f : R \to S$, this makes S a module over R by defining $a \cdot b$ as $f(a) \cdot b$ for a in R and b in S.

Thus, we can think of the (field of) complex numbers $\mathbb{C}$ as a module (vector space) over the (field of) real numbers $\mathbb{R}$ and both of these as vector spaces over the field $\mathbb{Q}$ of rational numbers.

Exercise: Show that the endomorphisms $\mathrm{End}(\mathbb{Q})$ of the *abelian group* of rational numbers is (as a ring) isomorphic to $\mathbb{Q}$. (Hint: Identify an endomorphism by what it does to the element 1.)

Exercise: Show that any finitely generated subgroup of the additive group of rational numbers is of the form $\mathbb{Z} \cdot (p/q)$ (i. e. the collection of all multiples of p/q) for some rational number p/q.

Exercise: (Five Stars!) Show that there is a proper subgroup of the rational numbers which is *not* of the above form.

Homomorphisms of modules

Given N and M are modules over a ring R and $f : N \to M$ is a group homomorphism (of the underlying abelian groups), we say that f is a module homomorphism if $f(a \cdot n) = a \cdot f(n)$ for every a in R and for every n in N.

Exercise: If $f : N \to M$ is a module homomorphism, check that its image is a submodule.

Exercise: For a module homomorphism $f : N \to M$, let $K = \{n | f(n) = 0\}$ denote the kernel in the sense of (abelian) groups. Show that it is a submodule of N.

As usual, we have the notion of one-to-one homomorphisms and onto homomorphisms. We say that $f : N \to M$ is an isomorphism if there is a homomorphism $g : M \to N$ so that $f \circ g$ is identity on M and g
$circ f$ is identity on N.

Exercise: If $f : N \to M$ is a homomorphism which is both 1-1 and onto then check that its inverse $g : M \to N$ is a homomorphism.

Exercise: Note that when R is a field, then N and M are vector spaces over R and module homomorphism $N \to M$ is the same as a linear transformation of vector spaces.

Exercise: Given any element m in M, show that $s \mapsto s \cdot m$ defines a module homomorphism $R \to M$ where R is considered as a module over itself in a natural way.

We can generalise the above to many elements.

Exercise: Given a collection $\{m_1, \ldots, m_n\}$ of elements of M, we can define a map $R^n \to M$ by

$$(a_1, \ldots, a_n) \mapsto a_1 \cdot m_1 + \cdots + a_n \cdot m_n$$

Check that this defines a module homomorphism.

We say that M is *finitely generated* as an R-module, if there is a collection $\{m_1, \ldots, m_n\}$ of elements of M for which the module homomomorphism $R^n \to M$ is onto.

We say that the collection $\{m_1, \ldots, m_n\}$ is *linearly independent* over R if the homomorphism $R^n \to M$ is one-to-one.

If the homomorphism $R^n \to M$ is an isomorphism, then we say that M is (isomorphic to) a *free* R-module with *basis* $\{m_1, \ldots, m_n\}$.

Quotient Modules

Given a abelian group M and a subgroup N, we can form the abelian group M/N whose elements consist of equivalence classes under the equivalence relation $m \simeq m'$ if $m - m'$ lies in N. Just to recall the ideas, it is useful to carry out the following exercise.

Exercise: For m, m', n, n' in M, check that if $m \simeq m'$ and $n \simeq n'$, then $m + n \simeq m' + n'$.

Now, if M is an R-module and N is an R-module, then there is a natural R-module structure on the abelian group M/N. One way to see this is that $a \cdot (m - m')$ lies in N. Hence, we have $a \cdot m - a \cdot m'$ in N and so $a \cdot m \simeq a \cdot m'$. Thus, multiplication by elements of R preserves equivalence classes.

Exercise: Given a homomorphism $f : N \to M$, check that if $n \simeq n'$ in $N/\ker(f)$, then $f(n) = f(n')$.

Thus, we have natural map (which we also call f by abuse of notation) $f : N/\ker(f) \to M$ which has the same image as f.

Exercise: Check that the homomorphism $f : N/\ker(f) \to M$ is one-to-one.

This gives the the Noether isomorphism theorem, viz. $N/\ker(f)$ is isomorphic (via f) to the image of f.

Through the fact that $\ker(f)$ and the image of f are R submodules and the above calculation, this is an isomorphism of R-modules.

Sub-modules of free modules

When R is a principal ideal domain, we claim that a submodule of R^n is free. The proof is very similar to the proof that a subgroup of $\mathbb{Z}^n$ is a free abelian group.

Exercise: Let I be an ideal in a principal ideal domain R, then as a module over R it is free. (Hint: If $I = a \cdot R$, then show that the module homomorphism $R \to I$ given by $s \mapsto a \cdot s$ is one-to-one and onto.)

As before, we will prove the above claim by induction on n. The above exercise gives the proof when $n = 1$. Now suppose that the result is known for submodules of R^k for $k < n$.

Let M be a sub-module of R^n. Consider the intersection $M \cap R \cdot e_1$ where $e_1 = (1, 0, \ldots, 0)$ is a sub-module. Now $R \to R \cdot e_1$ is an isomorphism so there is an ideal I in R so that $M \cap R \cdot e_1$ is of the form $I \cdot e_1$. As seen above this means that $M \cap R \cdot e_1$ is of the form $R \cdot (a \cdot e_1)$.

On the other hand, consider the natural homomorphism $f : M \to R^{n-1}$ given by "dropping the first entry"

$$m = (s_1, \ldots, s_n) \mapsto (s_2, \ldots, s_n)$$

The kernel of f is exactly $M \cap R \cdot e_1$. So, we see that $M/(R \cdot (a \cdot e_1))$ is isomorphic to a sub-module of R^{n-1}. By the induction hypothesis this is a free module. In other words, we can find elements $n_2, \ldots, n_k$ of M so that $f(n_2), \ldots, f(n_k)$ give a basis of $M/(R(a \cdot e_1))$.

Now, if $a = 0$, then $R \cdot (a \cdot e_1) = \{0\}$ in M, so that f is an isomorphism between M and $M/(R \cdot (a \cdot e_1))$. It follows that we see that $\{n_2, \dots, n_k\}$ is a basis of M, and M is free as required.

Thus we consider the case where $a \neq 0$. In this case, we put $n_1 = a \cdot e_1$ and claim that the collection $\{n_1, n_2, \dots, n_k\}$ is a basis of M.

To prove this we examine the corresponding homomorphism $R^k \to M$. Suppose that $(a_1, \dots, a_k)$ is such that $a_1 \cdot n_1 + \dots + a_k n_k$ is 0. It follows that $f(a_1 \cdot n_1 + \dots + a_k n_k) = 0$. However, we know that $f(n_1) = 0$, so this gives $a_2 \cdot f(n_2) + \dots + a_k \cdot f(n_k) = 0$. Now, we know that $f(n_2), \dots, f(n_k)$ is a basis of $M/(R \cdot (a \cdot e_1))$, so it follows that $a_2 = \dots = a_k = 0$. Hence, the above relation simplifies to $a_1 \cdot n_1 = 0$. This means that $a_1 \cdot a \cdot e_1 = 0$ which means that $a_1 \cdot a = 0$. Since $a \neq 0$ and R is a domain, this means that $a_1 = 0$ as required. In other words, we have proved that $\{n_1, \dots, n_k\}$ is linearly independent.

Next, pick an element m of M. Since $\{f(n_2), \dots, f(n_k)\}$ is a basis of $M/(R \cdot n_1)$, there are elements $a_2, \dots, a_k$ in R so that $f(m) = a_2 \cdot f(n_2) + \dots + a_k \cdot f(n_k)$. This gives the identity

$$f(m - (a_2 \cdot n_2 + \dots + a_k \cdot n_k)) = 0$$

Since $m - (a_2 \cdot n_2 + \dots + a_k \cdot n_k)$ is an element of M, its image under f can only be 0 if it lies in $M \cap R \cdot e_1$. The latter group is exactly $R \cdot n_1$. Hence, there is an a_1 in R so that

$$m - (a_2 \cdot n_2 + \dots + a_k \cdot n_k = a_1 \cdot n_1 \text{ equivalently } m = a_1 + n_1 + 2 \cdot n_2 + \dots + a_k \cdot n_k$$

Thus, $\{n_1, \dots, n_k\}$ generate M as well. In conclusion, they form a basis of M and so M is free.

Modules over a PID

If M is a finitely generated module over a principal ideal domain, then there is a finite collection $\{m_1, \dots, m_n\}$ of elements of M so that the resulting homomorphism $f : R^n \to M$ is onto. By the isomorphism theorem M is isomorphic to $R^n/\ker(f)$.

As seem above, $\ker(f)$ is a submodule of R^n and hence is a free module. In other words, there are elements $n_1, \dots, n_k$ of $\ker(f)$ so that the result homomorphism $R^k \to \ker(f)$ is an isomorphism. Viewing the elements n_i as n-tuples of elements of R gives us a $k \times n$ matrix A. Note that the i-th *row* of A consists of the element n_i written out as $(A_{i,1}, \dots, A_{i,n})$ in R^n.

We can see the map $R^k \to R^n$ given by A as being explicitly given by

$(a_1, \ldots, a_k) \mapsto$

$$(a_1 A_{1,1} + a_2 A_{2,1} + \cdots a_k A_{k,1},$$
$$(a_2 A_{1,2} + a_2 A_{2,2} + \cdots a_k A_{k,2}, \ldots,$$
$$(a_1 A_{1,n} + a_2 A_{2,n} + \cdots a_k A_{k,n})$$

More simply, if we write $v = (a_1, \ldots, a_k)$ as a row vector, then the right hand side is $v \cdot A$ which is a row vector of length n by the usual rules of matrix multiplication.

We can thus view *any* finitely generated module over a principal ideal domain as $R^n/\text{image}(A)$ for an $k \times n$ matrix, where multiplication is done "on the right" for row vectors.

Our earlier analysis of matrices over a principal ideal domain can now be brought into play to simplify $R^n/\text{image}(A)$.

As proved earlier, there is an invertible $k \times k$ matrix S over R and an invertible $n \times n$ matrix T so that $S \cdot A \cdot T$ has zero entries outside the diagonal and the diagonal entries $d_1, \ldots, d_k$ satisfy d_{i+1} lies in $d_i \cdot R$.

Exactly as in the case of the theorem on finitely generated abelian groups, we thus have the theorem that a finitely generated module over a principal ideal domain has the form

$$R/(d_1 \cdot R) \times \cdots \times R/(d_k \cdot R) \text{ where } d_{i+1} \in d_i \cdot R \text{ for all } i$$

This "structure theorem for modules over a PID" is one of the most important results in the subject and we will see applications of it shortly.