Modules

There are really two ways to think about modules. On one hand, they generalize the idea of vector spaces to arbitrary rings. In fact, a module over a field is a vector space. On the other hand, they generalize abelian groups, which are modules over $\mathbb{Z}$.

1. Modules and module homomorphisms

Definition 1. Let R be a ring and M an additive abelian group together with a function

$$R \times M \to M$$
$$(r, m) \mapsto rm.$$

Then M is a left R-module provided that for all $r, s \in R$ and $a, b \in M$,

(1) $r(a + b) = ra + rb$;
(2) $(r + s)a = ra + sa$;
(3) $r(sa) = (rs)a$.

If R has an identity element 1_R and

(4) $1_K v = v$.

then M is said to be a unitary R-module. If R is a division ring, then a unitary R-module is called a left vector space.

A right R-module is defined similarly.

The structure of a module M depends not only on the structure of the underlying abelian group but also on the action of R on M. Therefore, it is possible that a given group may have many different module structures (or none at all).

Example 1.
(1) Every additive abelian group G is a unitary $\mathbb{Z}$-module.
(2) If S is a ring and R is a subring, then S is a left R-module with ra being multiplication in S. This implies that S is itself an S-module. Moreover, $R[x_1, \ldots, x_n]$ is an R-module.
(3) If I is a left ideal of R, then I is a left R-module with the product ra ($r \in R$, $a \in I$) being the product. In this case, R/I is an R-module even if I is not two sided.

(4) Let R and S be rings and $\phi : R \to S$ a ring homomorphism. Then every S-module M can be made into an R-module by defining

$$R \times M \to M$$
$$(r, x) \mapsto \phi(r)x$$

(5) Let M be an abelian group and $\operatorname{End} M$ is endomorphism ring. Then M is a unitary $(\operatorname{End} M)$-module, with $(f, m) = f(m)$ for $m \in M$ and $f \in \operatorname{End} M$.

(6) If R is a ring, every abelian group M can be made into an R-module with trivial module structure by defining $rm = 0$ for all $r \in R$ and $m \in M$.

Exercise. Let R be a ring and M a (left) R-module. Verify the following facts:

(1) If 0_M is the additive identity of M, then for all $r \in R$ and $m \in M$,

$$r0_M = 0_M \text{ and } 0_R m = 0_M.$$

(2) For all $r \in R$, $n \in \mathbb{Z}$, and $m \in M$,

$$(-r)m = -(rm) = r(-m) \text{ and } m(rm) = r(nm).$$

(3) If R is commutative, then every left R-module M can be given the structure of a right R-module by defining $(m, r) = rm$.

We will generally assume we are working with left modules unless stated otherwise. However, any result that works for left R-modules works equally as well for right R-modules.

Definition 2. Let M and N be modules over a ring R. A function $f : M \to N$ is an R-module homomorphism provided that for all $m, m' \in M$ and $r \in R$:

$$f(m + m') = f(m) + f(m') \text{ and } f(rm) = rf(m).$$

If R is a division ring, then an R-module homomorphism is called a linear transformation.

The terms monomorphism, epimorphism, isomorphism, kernel, and image are all defined as expected.

Exercise. Let R be a ring. Prove that the set of left modules over R along with module homomorphisms defines a category. This category is denoted ${}_R\operatorname{Mod}$ and the category of right R-modules is denoted Mod_R.

Products and coproducts exist in the category of R-modules. They are the direct product and direct sum, respectively, of a family of R-modules. When the indexing set is finite, these

definitions coincide. We will not formally define them here except in the case of two (and hence finite number) of modules.

Definition 3. Let R be a ring and M, N left R-modules. The direct sum of M and N, denoted $M \oplus N$ is the abelian group $M \oplus N$ with multiplication $(r, (m, n)) \mapsto (rm, rn)$ for all $r \in R$, $m \in M$, and $n \in N$.

The remainder of this section is devoted to stating the Isomorphism Theorems for modules. For this, we need to define the notion of a submodule and a quotient module.

Definition 4. Let R be a ring, M an R-module and N a nonempty subset of A. N is a submodule of M provided that N is an additive subgroup of M and $rn \in N$ for all $r \in R$, $n \in N$.

Example 2. If R is a ring and $f : M \to N$ an R-module homomorphism, then $\ker f$ is a submodule of M and $\operatorname{im} f$ is a submodule of N. If L is a submodule of B, then $f^{-1}(L)$ is a submodule of A.

Definition 5. An R-module M is said to be simple if its only submodules are 0 and M.

Definition 6. If X is a subset of a module M over a ring R, then the intersection of all submodules of M containing X is called the submodule generated by X.

If N is a module generated by X, then we say X spans N.

Example 3. Let X be a generating set for a module N.

(1) If $X = \emptyset$, then N is the trivial module.
(2) If $X = \{a\}$, then N is called the cyclic module generated by a.
(3) If $|X| < \infty$, then N is said to be finitely generated.
(4) If $\{B_i \mid i \in I\}$ is a family of submodules of M, then the submodule generated by $X = \bigcup_{i \in I} B_i$ is called the sum of the modules B_i. When $|I| = n < \infty$, then we denote this by $B_1 + \cdots + B_n$.

Definition 7. A subset X of an R-module M is said to be linearly independent provided that for distinct $x_1, \ldots, x_n \in X$ and $r_i \in R$,

$$r_1 x_1 + \cdots + r_n x_n = 0 \Rightarrow r_i = 0 \text{ for every } i.$$

If X is not linearly independent, it is called linearly dependent.

If X is a linearly independent spanning set of M, then we say X is a basis for M.

Let R be a ring and M and R-module. If $m \in M$, then we denote $Rm = \{rm \mid r \in R$. If R is has identity and M is unitary, then this is the cyclic submodule generated by R. In general, if R has identity and M is unitary then the submodule generated by X is

$$RX = \{\sum_{i=1}^{k} r_i x_i \mid r_i \in R, x_i \in X\}.$$

This definition is a bit more complex when R does not have identity. Since few of our examples are of this nature, we will avoid this detail for the time being.

Definition 8. Let M be a module over a ring R and N a submodule of M. The quotient module M/N is defined as the group M/N along with action, $(r, m+N) \mapsto rm+N$ for all $r \in R$, $m \in M$. The map

$$\pi : M \to N$$
$$m \mapsto m + N$$

is called the canonical projection.

Exercise. With notation as in the previous definition, prove that M/N is a true R-module and that the map π is an R-module epimorphism with kernel N.

Theorem 4. Let R be a ring.

(1) (First Isomorphism Theorem) If $f : M \to N$ is a left R-module homomorphism, then $A/\ker f \cong \operatorname{im} f$.
(2) If M is a left R-module with submodules N and L, then $B/(B \cap C) \cong (B + C)/C$.
(3) If M is a left R-module with submodules $L \subset N$, then N/L is a submodule of M/L and $(M/L)/(N/L) \cong M/N$.

2. Free modules

In categorical language, a free (left) R-module is a free object in the category ${}_R\mathrm{Mod}$. We will make the appropriate definition without (too much) reference to category theory.

Definition 9. Let R be a ring with identity and F an R-module. We say F is a free R-module if F has a nonempty basis.

We will not prove the following theorem, but it should remind you of an almost identical theorem we proved last semester for abelian groups.

Theorem 5. Let R be a ring and F an R-module. The following are equivalent.

(1) F is free.
(2) F is the direct sum of a family of cyclic R-modules, each of which is isomorphic as a left R-module to R.
(3) F is isomorphic (as an R-module) to a direct sum of copies of the left R-module R.
(4) F is a free object in ${}_R\,\mathrm{Mod}$.

Corollary 6. Every (unitary) module M over a ring R (with identity) is the homomorphic image of a free R-module F. If M is finitely generated, then F may be chosen finitely generated.

3. Chain conditions

Definition 10. Let M and N be modules over a ring R.

M is said to be noetherian if it satisfies the ascending chain condition. That is, for every chain of submodules $M_1 \subset M_2 \subset M_3 \subset \cdots$ there is an integer m such that $M_i = M_m$ for all $i \geq m$.

N is said to be artinian if it satisfies the descending chain condition. That is, for every chain of submodules $N_1 \supset N_2 \supset N_3 \supset \cdots$ there is an integer n such that $N_i = N_n$ for all $i \geq n$.

The ring R is said to be left noetherian (resp. artinian) if it satisfies the acc (resp. dcc) on left ideals. Right noetherian and right artinian are defined similarly.

Example 7.
(1) A division ring is both noetherian and artinian since the only left or right ideals are D and 0.
(2) $\mathbb{Z}$ and $\mathbb{Z}_n$ are noetherian. As is $F[x]$ for F a field. In fact, any commutative PID is noetherian.
(3) The ring of $n \times n$ matrices over a division ring is both noetherian and artinian.

Lemma 8. Suppose a module M satisfies the ascending chain condition. Then every nonempty set of submodules contains a maximal element.

Proof. Let S be a nonempty set of submodules of M. Choose $N_0 \in S$. If S has no maximal element, then there exists N_1 such that $N_0 \subsetneq N_1$. But then, there exists N_2 such that $N_1 \subsetneq N_2$. Continuing in this way we get a chain of proper inclusions $N_0 \subset N_1 \subset N_2 \subset \cdots$, contradicting the ascending chain condition. □

Theorem 9. A module M satisfies the ascending chain condition on submodules if and only if every submodule of A is finitely generated.

Proof. ($\Rightarrow$) Given a chain of submodules of M, $M_1 \subset M_2 \subset M_3 \subset \cdots$, then $\mathcal{M} = \bigcup M_i$ is also a submodule of M. Hence, $\mathcal{M}$ is finitely generated, say by $m_1, \ldots, m_k$. Since each m_i is an element of some M_j, then there is an index n such that $m_i \in M_n$ for $i = 1, \ldots, k$ (just take that maximum such j). Hence, $\mathcal{M} \subset M_n$, whence $M_i = M_n$ for $i \geq n$.

($\Leftarrow$) Let N be a submodule of M and let S be the set of all finitely generated submodules of B. Since S is nonempty, S contains a maximal element L by the previous lemma. L is finitely generated say by $\ell_1, \ldots, \ell_k$. For each $n \in N$ let D_n be the submodule of B generated by $n, \ell_1, \ldots, \ell_k$. Then $D_n \in S$. But L is maximal and $L \subset D_n$ so $D_n = L$. This holds for every $n \in B$ so $B = L$. Thus, B is finitely generated. $\square$

Corollary 10. A ring R is left noetherian if and only if every left ideal of R is finitely generated.

Theorem 11 (Hilbert Basis Theorem)**.** If R is a left noetherian ring, then so is $R[x]$.

Proof. By the previous corollary, it suffices to show that every left ideal of R is finitely generated.

Let I be a left ideal of R. We may assume that $I \neq 0$. Let J be the set of leading coefficients of polynomials in I along with 0. Then J is a left ideal of R (see exam 1) and hence finitely generated by hypothesis. Let $\{r_1, \ldots, r_n\}$ be a generating set of J. Each r_i occurs as the leading coefficient of some polynomial p_i. By multiplying by sufficient powers of x we may assume that each p_i has the same degree n.

Let $N = \{f \in R[x] \mid \deg(f) < n\}$. This is a left R-submodule and hence finitely generated. Therefore $I \cap N \subset N$ is finitely generated, say by $q_1, \ldots, q_t$.

Let I_0 be the ideal generated by $p_1, \ldots, p_n, q_1, \ldots, q_t$. Clearly $I_0 \subset I$. The claim is that $I_0 = I$, whence I is finitely generated.

We proceed by induction. Assume I_0 contains all polynomials in I of degree less than $m \geq n$. Let $p \in I$ with $\deg(p) = m$ and leading coefficient r. Then $r \in J$ so $r = a_1 r_1 + \cdots + a_k r_k$ for some $a_i \in R$. Set $q = (a_1 p_1 + \cdots + a_k p_k) x^{m-n}$. Then $q \in I_0$, $\deg(q) = m$, and the leading coefficient of q is r. Hence, $p - q \in I$ with $\deg(p - q) < m$, whence $p - q \in I_0$. Thus, $p \in I_0$.

It follows that $I_0 = I$ and I is finitely generated. $\square$