Introduction to Module Theory

Definition. Let R be a ring (not necessarily commutative nor with 1). A ***left R-module*** or a *left module over R* is a set M together with

1. a binary operation $+$ on M under which M is an abelian group, and
2. an action of R on M (that is, a map $R \times M \to M$) denoted by rm, for all $r \in R$ and for all $m \in M$ which satisfies
   (a) $(r+s)m = rm + sm, \quad$ for all $r, s \in R,\ m \in M$
   (b) $(rs)m = r(sm), \quad$ for all $r, s \in R,\ m \in M$, and
   (c) $r(m+n) = rm + rn, \quad$ for all $r, s \in R,\ m \in M$.

   If the ring R has 1 we impose the additional axiom:

   (d) $1m = m, \quad$ for all $m \in M$.

Definition. Let R be a ring and let M be an R-module. An ***R-submodule*** of M is a subgroup N of M which is closed under the action of ring elements.

Proposition. *(The Submodule Criterion)* Let R be a ring and let M be an R-module. A subset N of M is a submodule of M if and only if

1. $N \neq \varnothing$, and
2. $x + ry \in N$ for all $r \in R$ and for all $x, y \in M$.

Definition. Let R be a ring and let M and N be R-modules.

1. A map $\varphi : M \to N$ is an ***R-module homomorphism*** if it respects the R-module structures of M and N, i.e.,
   (a) $\varphi(x+y) = \varphi(x) + \varphi(y), \quad$ for all $x, y \in M$ and
   (b) $\varphi(rx) = r\varphi(x), \quad$ for all $r \in R$, $x \in M$.
2. An R-module homomorphism is an ***isomorphism*** if it is both injective and surjective. The modules M and N are said to be ***isomorphic***, denoted $M \cong N$ if there is some R-module isomorphism $\varphi : M \to N$.

3. If $\varphi : M \to N$ is an R-module homomorphism, let $\ker(\varphi) = \{m \in M \mid \varphi(m) = 0\}$ and let $\varphi(M) = \{n \in N \mid n = \varphi(m) \text{ for some } m \in M\}$.
4. Let M and N be R-modules and define $\mathrm{Hom}_R(M, N)$ to be the set of R-module homomorphisms from M to N.

Proposition. Let M, N, and L be R-modules

1. A map $\varphi : M \to N$ is an R-module homomorphism if and only if $\varphi(rx + y) = r\varphi(x) + \varphi(y)$ for all $c, y \in M$ and $r \in R$.
2. Let φ, ψ be elements of $\mathrm{Hom}_R(M, N)$. Define $\varphi + \psi$ by
$$(\varphi + \psi)(m) = \varphi(m) + \psi(m) \qquad \text{for all } m \in M.$$
Then $\varphi + \psi \in \mathrm{Hom}_R(M, N)$ and with this operation $\mathrm{Hom}_R(M, N)$ is an abelian group. If R is a commutative ring the for $r \in R$ define $r\varphi$ by
$$(r\varphi)(m) = r(\varphi(m)) \qquad \text{for all } m \in M.$$
Then $r\varphi \in \mathrm{Hom}_R(M.N)$ and with this action of the commutative ring R the abelian group $\mathrm{Hom}_R(M, N)$ is an R-module.
3. If $\varphi \in \mathrm{Hom}_R(L, M)$ and $\psi \in \mathrm{Hom}_R(M, N)$ then $\psi \circ \varphi \in \mathrm{Hom}_R(L, N)$.
4. With addition as above and multiplication defined as function composition, $\mathrm{Hom}_R(M, M)$ is an R-algebra.

Definition. The ring $\mathrm{Hom}_R(M, M)$ is called the ***endomorphism ring of*** M and will often be denoted by $\mathrm{End}_R(M)$. Elements of $\mathrm{End}(M)$ are called ***endomorphisms***.

Proposition. Let R be a ring, let M be an R-module, and let N be a submodule of M. The quotient group M/N can be made into an R-module by defining an action of elements of R by
$$r(x + N) = (rx) + N), \qquad \text{for all } r \in R,\ x + N \in M/N.$$
The natural projection map $\pi : M \to M/N$ is an R-module homomorphism with kernel N.

Definition. Let A, B be submodules of the R-module M. The *sum* of A and B is the set

$$A + B = \{a + b \mid a \in A,\ b \in B\}.$$

Definition. Let M be an R-module and let $N_1, \ldots, N_n$ be submodules of M.

1. The ***sum*** of $N_1, \ldots, N_n$ is the set of all finite sums of elements form the sets N_i : $\{a_1 + \cdots + a_n \mid a_i \in N_i\}$. Denote this sum by $N_1 + \cdots + N_n$.
2. For any subset A of M let

$$RA = \{r_1 a_1 + \cdots + r_m a_m \mid a_i \in A,\ r_i \in R,\ m \in \mathbb{Z}^+\}.$$

   If A is finite we may write $Ra_1 + Ra_2 + \cdots + Ra_m$. Call RA th ***submodule of*** M ***generated by*** A. If N is a submodule of M and $N = RA$ for some subset A of M, we call A a set of generators or a generating set for N,. and we say that N is generated by A.
3. A submodule N of M is ***finitely generated*** if there is some finites subset A of M such that $N = RA$.
4. A submodule N of M is ***cyclic*** if there exists an element $a \in M$ such that $N = Ra$, that is, if N is generated by one element.

Proposition. Let $N_1, N_2, \ldots, N_k$ be submodules of the R-module M. Then the following are equivalent

1. The map $\pi : N_1 \times N_2 \times \cdots \times N_k \to N_1 + N_2 + \cdots + N_k$ defined by

$$\pi(a_1, a_2, \ldots, a_k) = a_1 + a_2 + \cdots + a_k$$

   is an isomorphism (of R-modules)
2. $N_j \cap N_1 + \cdots N_{j-1} + N_{j+1} + \cdots + N_k = 0$ for all $j \in \{1, 2, \ldots, k\}$.
3. Every $x \in N_1 + \cdots + N_k$ can be written *uniquely* in the form $a_1 + a_2 + \cdots + a_k$ for $a_i \in N_i$.

Definition. If an R-module $M = N_1 + N_2 + \cdots + N_k$ is the sum of submodules $N_1, N_2, \ldots, N_k$ of M satisfying the equivalent conditions in the above proposition, then M is said to be the ***(internal) direct sum*** of $N_1, N_2, \ldots, N_k$ written

$$M = N_1 \oplus N_2 \oplus \cdots \oplus N_k.$$

Definition. And R-module F is said to be ***free*** on the subset A of F if for every nonzero element x of F, there exist unique nonzero elements $r_1, r_2, \ldots, r_n$ of R and unique $a_1, a_2, \ldots, a_n$ in A such that $x = r_1a_1 + r_2a_2 + \cdots + r_na_n$, for some $n \in \mathbb{Z}^+$. In this situation we say A is a ***basis*** or ***set of free generators*** for F. If R is a commutative ring the cardinality of A is called the ***rank*** of F.

Theorem 0.1. For any set A there is a free R-module $F(A)$ on the set A and $F(A)$ satisfies the following ***universal property***: if M is any R-module and $\varphi : A \to M$ is any map of sets, then there is a unique R-module homomorphism $\Phi : F(A) \to M$ such that $\Phi(a) = \varphi(a)$, for all $a \in A$, that is, the following diagram commutes.

$$\begin{tikzcd} A \arrow[r, "\iota"] \arrow[dr, "\varphi"'] & F(A) \arrow[d, "\Phi"] \\ & M \end{tikzcd}$$

Corollary.

1. If F_1 and F_2 are free modules on the same set A, there is a unique isomorphism between F_1 and F_2 which is the identity map on A.
2. If F is any free R-module with basis A, then $F \cong F(A)$. In particular, F enjoys the same universal property with respect to A as $F(A)$ does in the previous theorem.