4 Module Theory

4.1 Definitions and Examples

This section of notes roughly follows Section 10.1 in Dummit and Foote.

Let's start with the definition of a module.

Definition 4.1. Let R be a ring (not necessarily commutative nor with 1). A **left R-module** (or **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, $R \times M \to M$) denoted by rm, for all $r \in R$ and for all $m \in M$ that satisfies.

  (a) $(r+s)m = rm + sm$ for all $r, s \in R$ and $m \in M$,

  (b) $(rs)m = r(sm)$ for all $r, s \in R$ and $m \in M$, and

  (c) $r(m+n) = rm + rn$ all $r \in R$ and $m, n \in M$.

  (d) If R has a 1, then we also require: $1m = m$ for all $m \in M$.

We analogously define **right R-modules**. If R is commutative and M is a left R-module, then we can make it a right R-module by defining $mr = rm$ for all $r \in R$ and $m \in M$. Notice that we cannot do this in general if R is not commutative since Axiom (2b) may fail. Unless we explicitly say otherwise, all modules will be left modules. Modules satisfying Axiom (2d) are call **unital modules**. We will assume that all our modules are unital.

The axioms for a module should look familiar. If R is a field, the axioms are precisely those for a vector space over R.

We emphasize that an abelian group M may have many different R-module structures for a fixed ring R (in the same way a group G could act in many ways as a permutation group of some fixed set S).

Definition 4.2. Let R be a ring and let M be an R-module. An **R-submodule** of M is a subgroup N of M that is closed under the action of ring elements, i.e., $rn \in N$ for all $r \in R$ and $n \in N$.

As expected, submodules of M are just subsets of M that are themselves modules under the same action. In particular, if R is a field, submodules are just vector subspaces. Every R-module has at least two submodules: M and $\{0\}$. The latter is often written as just 0 and called the **trivial submodule**.

Example 4.3. Let's see some examples.

(1) Let R be any ring. Then $M = R$ is a left R-module, where the action of a ring element on a module element is just usual ring multiplication. In this case, the submodules of $M = R$ are the left ideals of R.

(2) A special case of the first example is what R is a field. Then R is 1-dimensional vector space over itself.

(3) More generally, if $R = F$ is a field, every vector space over F is an F-module and vice versa. Let $n \in \mathbb{Z}^+$ and let

$$F^n = \{(a_1, \ldots, a_n) \mid a_i \in F \text{ for all } i\}.$$

We can make F^n into an n-dimensional vector space by defining addition and scalar multiplication in the standard way.

(4) Let R be a ring with 1 and let $n \in \mathbb{Z}^+$. As above, define

$$R^n = \{(a_1, \ldots, a_n) \mid a_i \in R \text{ for all } i\}.$$

We can make R^n an R-module by defining addition and multiplication by elements of R in the same manner as when R was a field. The module R^n is called the **free module of rank n over R.**

(5) The same abelian group M may have the structure of a module for several different rings R. In particular, if M is an R-module and S is a subring of R with $1_R = 1_S$, then M is automatically an S-module. For example, the field $\mathbb{R}$ is an $\mathbb{R}$-module, a $\mathbb{Q}$-module, and a $\mathbb{Z}$-module.

(6) If M is an R-module and for some 2-sided ideal I of R, $am = 0$ for all $a \in I$ and $m \in M$, we say M is **annihilated by** I. In this case, we can make M into an (R/I)-module by defining an action of the quotient ring R/I on M. For each $m \in M$ and coset $r + I \in R/I$, define

$$(r + I)m = rm.$$

Since $am = 0$ for all $a \in I$ and $m \in M$, this is well-defined. In the special case that I is a maximal ideal in a commutative ring R and $IM = 0$, M is a vector space over the field R/I.

(7) $\mathbb{Z}$-modules...

(8) $F[x]$-modules...

Theorem 4.4 (Submodule Criterion)**.** Let R be a ring and let M be an R-module. A subset N of M is a submodule of M iff

(1) $N \neq \emptyset$, and

(2) $x + ry \in N$ for all $r \in R$ and $x, y \in N$.

Definition 4.5. Let R be a commutative ring with 1. An R-algebra is a ring A with identity together with a ring homomorphism $f : R \to A$ mapping $1_R \to 1_A$ such that the subring $f(R)$ of A is contained in the center of A (i.e., the set of all elements of A that commute with every element of A).

If A is an R-algebra, then it is easy to verify that A has a natural left and right unital R-module structure defined by $r \cdot a = a \cdot r = f(r)a$, where $f(r)a$ is just the multiplication in the ring A (which is the same as $af(r)$ since $f(r)$ lies in center). In general, it is possible for an R-algebra A to have other left (or right) R-module structures. Unless stated otherwise, we assume the natural module structure on the algebra will be assumed.

Here is an alternate definition.

Definition 4.6. Let R be a commutative ring with 1. An R-algebra is a ring A that is also an R-module such that the multiplication map $A \times A \to A$ is R-bilinear, that is,

$$r * (ab) = (r * a) \cdot b = a \cdot (rb)$$

for all $a, b \in A$ and $r \in R$, where denotes the R-action on A.

Loosely speaking, the definition above says that an R-algebra is an R-module, where we are also allowed to multiply the module elements.

Theorem 4.7. Definitions 4.5 and 4.6 are equivalent.

Example 4.8. Here are a few quick examples. Throughout assume that R is a commutative ring with 1.

(1) Any ring with 1 is a $\mathbb{Z}$-algebra.

(2) Let A be any ring with 1_A. If R is a subring of the center of A containing 1_A, then A is an R-algebra under $f(r) = r1_A$ for $r \in R$. For example, the polynomial ring $R[x_1, \dots, x_n]$ is an R-algebra.

(3) The group ring $R[G]$ for a finite group G is an R-algebra.

(4) If A is an R-algebra, then the R-module structure of A depends only on the subring $f(R)$ contained in center of A. If we replace R by its image $f(R)$, we see that up to ring homomorphism, every algebra A arises from a subring of the center of A that contains 1_A.

(5) In the special case that $R = F$ is a field, F is isomorphic to its image under f, so we can identify F itself as a subring of A. So, saying that A is an algebra over a field F is the same as saying that the ring A contains the field F in its center and the identity of A and of F are the same.

Definition 4.9. If A and B are two R-algebra, an **R-algebra homomorphism** (respectively, **isomorphism**) is a ring homomorphism (respectively, isomorphism) $\phi : A \to B$ such that

(1) $\phi(1_A) = 1_B$

(2) $\phi(r \cdot a) = r \cdot \phi(a)$ for all $r \in R$ and $a \in A$.

4.2 Quotient Modules and Module Homomorphisms

This section of notes roughly follows Section 10.2 in Dummit and Foote.

There are no big surprises in this section. Essentially, everything works out exactly as you think it should.

Definition 4.10. Let R be a ring and let M and N be R-modules.

(1) A map $\phi : M \to N$ is an R**-module homomorphism** if it respects the R-module structures of M and N:

   (a) $\phi(x+y) = \phi(x)+\phi(y)$ for all $x, y \in M$;

   (b) $\phi(rx) = r\phi(x)$ for all $r \in R$ and $x \in M$.

(2) An R-module homomorphism is an **isomorphism** if it is both injective and surjective. In this case, we say that M and N are isomorphic and write $M \cong N$.

(3) If $\phi : M \to N$ is an R-module homomorphism, define the **kernel** of ϕ via

$$\ker(\phi) := \{x \in M \mid \phi(x) = 0\}$$

and the **image** of ϕ via

$$\phi(M) := \{y \in N \mid \phi(x) = y \text{ for some } x \in M\}.$$

(4) Let M and N be R-modules and define $\mathrm{Hom}_R(M,N)$ to be the set of all R-module homomorphisms from M into N.

Remark 4.11. Every R-module homomorphism is always a group homomorphism of abelian groups. However, not every group homomorphism of abelian groups yields an R-module homomorphism.

Theorem 4.12. If $\phi : M \to N$ is an R-module homomorphism, then $\ker(\phi)$ is an R-submodule of M and $\phi(N)$ is an R-submodule of N.

Example 4.13. Let's see some examples.

(1) If R is a field, then R-module homomorphisms are linear transformations.

(2) If R is a ring and $M = R$ is a module over itself, then R-module homomorphisms (even from R to itself) need not be ring homomorphisms and vice versa. For example, when $R = \mathbb{Z}$, the $\mathbb{Z}$-module homomorphism $\psi : x \mapsto 2x$ is not a ring homomorphism. When $R = F[x]$ for some field F, the ring homomorphism $\phi : f(x) \mapsto f(x^2)$ is not an $F[x]$-module homomorphism since $x^2 = \phi(x) = \phi(x \cdot 1) = x\phi(1) = x$ is a contradiction.

(3) If R is a ring and $M = R^n$, then the **projection map** $\pi_i : R^n \to R$ given by $\phi_i(x_1, \dots, x_n) = x_i$ is a surjective R-module homomorphism with kernel equal to the submodule of n-tuples that have a zero in position i.

(4) For $\mathbb{Z}$-modules, Condition (a) of being a module homomorphism forces Condition (b). This implies that $\mathbb{Z}$-module homomorphisms are the same as abelian group homomorphisms.

(5) Let R be a ring, let I be a 2-sided ideal of R and suppose M and N are R-modules annihilated by I (i.e., $am = 0$ and $an = 0$ for all $a \in I$, $n \in N$, and $m \in M$). Any R-module homomorphism from N to M is then automatically a homomorphism of R/I-modules (see Example 4.3(6)). For example, if A is an additive abelian group such that for some

prime p, $px = 0$ for all $x \in A$, then any group homomorphism from A to itself is a $\mathbb{Z}/p\mathbb{Z}$-module homomorphism, i.e., a linear transformation over the field $\mathbb{Z}_p$. In particular, the group of all group homomorphisms of A is the group of invertible linear transformations from A to itself: $GL(A)$.

Theorem 4.14. Let M, N, and L be R-modules.

(1) A map $\phi : M \to N$ is an R-module homomorphism iff $\phi(rx+y) = r\phi(x) + \phi(y)$ for all $x, y \in M$ and $r \in R$.

(2) Let $\phi, \psi \in \operatorname{Hom}_R(M,N)$. Define $\phi + \psi$ via

$$(\phi + \psi)(m) = \phi(m) + \psi(m)$$

for all $m \in M$. Then $\phi + \psi \in \operatorname{Hom}_R(M,N)$ and with this operation $\operatorname{Hom}_R(M,N)$ is an abelian group. If R is a commutative ring, then for $r \in R$, define $r\phi$ via

$$(r\phi)(m) = r(\phi(m))$$

for $m \in M$. Then $r\phi \in \operatorname{Hom}_R(M,N)$ and with this action of the commutative ring R, the abelian group $\operatorname{Hom}_R(M,N)$ is an R-module.

(3) If $\phi \in \operatorname{Hom}_R(L,M)$ and $\psi \in \operatorname{Hom}_R(M,N)$, then $\psi \circ \phi \in \operatorname{Hom}_R(L,N)$.

(4) With addition as above and multiplication as function composition, $\operatorname{Hom}_R(M,M)$ is a ring with 1. When R is commutative, $\operatorname{Hom}_R(M,M)$ is an R-algebra.

Definition 4.15. The ring $\operatorname{Hom}_R(M,M)$ is called the **endomorphism ring of** M and may be denoted by $\operatorname{End}_R(M)$. Elements of $\operatorname{End}_R(M)$ are called **endomorphisms**.

When R is commutative, there is a natural map from R into $\operatorname{End}_R(M)$ given by $r \mapsto rI$, where the latter endomorphisms of M is just multiplication by r on M. The image of R is contained in the center of $\operatorname{End}_R(M)$, so if R has an identity, $\operatorname{End}_R(M)$ is an R-algebra. The ring homomorphism from R to $\operatorname{End}_R(M)$ may not be injective since for some $r \in R$, we may have $rm = 0$ for all $m \in M$ (e.g., $R = \mathbb{Z}$, $M = \mathbb{Z}/2\mathbb{Z}$, and $r = 2$).

When R is a field, this map is injective (no unit is in the kernel) and the copy of R in $\operatorname{End}_R(M)$ is called the **subring of scalar transformations**.

Recall that if G is a group and $H \leq G$, then we can form the quotient group G/H exactly when H is a normal subgroup of G. However, if G is abelian, then every subgroup is normal. In the case of a module M, every submodule is automatically a normal subgroup of M. We wish to show that we can always form the quotient module M/N for *any* submodule N.

Theorem 4.16. Let R be a ring, let M be an R-module, and let N be a submodule of M. The (additive, abelian) quotient group M/N can be made into an R-module by defining an action of elements of R by

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

for all $r \in R$ and $x + N \in M/N$. The natural projection $\pi : M \to M/N$ defined by $\pi(x) = x + N$ is an R-module homomorphism with kernel N.

Definition 4.17. Let A and B be submodules of the R-module M. The **sum** of A and B is the set

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

Theorem 4.18. Let A and B be submodules of the R-module M. Then $A + B$ is the smallest submodule of M that contains both A and B and $A \cap B$ is the largest submodule of M that is contained in both A and B.

All the isomorphism theorems stated for groups also hold for R-modules.

Theorem 4.19 (Isomorphism Theorems for Modules)**.** Let M and N be R-modules.

(1) (First) Let $\phi : M \to N$ be an R-module homomorphism. Then $\ker(\phi)$ is a submodule of M and $M/\ker(\phi) \cong \phi(M)$.

(2) (Second) If A and B are submodules of M, then $(A+B)/B \cong A/(A \cap B)$.

(3) (Third) If A and B are submodules of M such that $A \subseteq B$, then $(M/A)/(B/A) \cong M/B$.

(4) (Fourth) Let N be a submodule of M. There is a bijection between the submodules of M that contain N and the submodules of M/N. The correspondence is given by $A \leftrightarrow A/N$, for all $A \supseteq N$. This correspondence commutes with the process of taking sums and intersections (i.e., is a lattice isomorphism between the lattice of submodules of M/N and the lattice of submodules of M that contain N).

4.3 Generation of Modules, Direct Sums, and Free Modules

This section of notes roughly follows Section 10.3 in Dummit and Foote.

Let R be a ring with 1. We begin with a series of definitions.

Definition 4.20. Let M be an R-module and $N_1,\dots,N_n$ be submodules of M.

(1) The **sum** of $N_1,\dots,N_n$ is the set of all finite sums of elements from the set N_i:

$$N_1+\cdots+N_n := \{a_1+\cdots+a_n \mid a_i \in N_i\}.$$

(2) For any subset A of M, let

$$RA := \{r_1a_1+\cdots+r_ma_m \mid r_1,\dots,r_m \in R, a_1,\dots,a_m \in A, m \in \mathbb{Z}^+\}$$

By the convention $RA=\{0\}$ if $A=\emptyset$. If A is the finite set $\{a_1,\dots,a_n\}$, we write $Ra_1+\cdots+Ra_n$ for RA. If N is a submodule of M (possibly $N=M$) and $N=RA$, for some subset A of M, we call A a **set of generators** or **generating set** for N, and we say N is **generated by** A.

(3) A submodule N of M (possibly $N=M$) is **finitely generated** if there is some finite subset A of M such that $N=RA$, that is, if N is generated by some finite subset.

(4) A submodule N of M (possibly $N=M$) is **cyclic** if there exists an element $a\in M$ such that $N=Ra$, that is, if N is generated by one element:

$$N=Ra=\{ra \mid r\in R\}.$$

Remark 4.21.

(1) These definitions do not require R to contain a 1. However, this condition ensures that A is contained in RA.

(2) For any subset A of M, it's easy to check that RA is the smallest submodule of M containing A.

(3) For submodules $N_1,\dots,N_n$, $N_1+\cdots+N_n$ is the submodule generated by $N_1\cup\cdots\cup N_n$ and is the smallest submodule containing all N_i. If $N_1,\dots,N_n$ are generated by $A_1,\dots,A_n$, respectively, then $N_1+\cdots N_n$ is generated by $A_1\cup\cdots\cup A_n$.

(4) A submodule N of an R-module M may have many different generating sets. If N is finitely generated, then there is a smallest nonnegative integer d such that N is generated by d elements and no fewer. Any generating set consisting of d elements will be called a **minimal set of generators** for N.

(5) The process of generating submodules of an R-module M by taking subsets A of M and forming all finite R-linear combinations of elements of A is similar to taking the span of a subset of vectors of a vector space.

Example 4.22. Here are a few examples.

(1) Let $R=\mathbb{Z}$ and let M be any R-module, i.e., any abelian group. If $a\in M$, then $\mathbb{Z}a$ is just the cyclic subgroup of M generated by a. More generally, M is generated as a $\mathbb{Z}$-module by a set A iff M is generated as a group by A.

(2) Let R be a ring with 1 and let M be the left R-module R itself. In this case, R is cyclic since $R=R1$. Recall that the submodules of R are precisely the left ideals of R, so saying I is a cyclic R-submodule of the left R-module R is the same as saying I is a principal ideal of R. Saying I is a finitely generated R-submodule of R is the same as saying I is a finitely generated ideal.

When R is a commutative ring, we may write AR or aR for the submodule generated by A or a, respectively. In this situation, $AR = RA$ and $aR = Ra$. A PID is a commutative integral domain R with identity in which every R-submodule of R is cyclic.

(3) Submodules of a finitely generated module need not be finitely generated. For example, take M to be the cyclic R-module R itself, where R is the polynomial ring in infinitely variables $x_1, x_2, \ldots$ with coefficients in some field F. The submodule generated by $\{x_1, x_2, \ldots\}$ cannot be generated by any finite set.

(4) Let R be a ring with 1 and let M be the free module of rank n over R (see Example 4.3(4)). For each $i \in \{1, \ldots, n\}$, let $e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, where the 1 appears in position i. Since

$$(s_1, \ldots, s_n) = \sum_{i=1}^{n} s_i e_i,$$

it is clear that M is generated by $\{e_1, \ldots, e_n\}$. If R is commutative, then this is a minimal generating set.

Definition 4.23. Let $M_1, \ldots, M_k$ be a collection of R-modules. The collection of k-tuples $(m_1, \ldots, m_k)$, where $m_i \in M_i$ with addition and action of R defined componentwise is called the **direction product** of $M_1, \ldots, M_k$, denoted $M_1 \times \cdots \times M_k$.

Remark 4.24. The direct product of $M_1, \ldots, M_k$ is also referred to as the **direct sum** of $M_1, \ldots, M_k$ and is denoted $M_1 \oplus \cdots \oplus M_k$. The direct product and direct sum of an infinite number of modules are different in general.

Theorem 4.25. Let $N_1, \ldots, N_k$ be submodules of the R-module M. Then the following are equivalent:

(1) The map $\pi : N_1 \times \cdots \times N_k \to N_1 + \cdots + N_k$ defined by

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

is an isomorphism of R-modules:

$$N_1 \times \cdots \times N_k \cong N_1 + \cdots + N_k$$

(2) $N_j \cap (N_1 \cap \cdots \cap N_{j-1} \cap N_{j+1} \cap \cdots \cap N_k) = 0$ for all $j \in \{1, \ldots, k\}$.

(3) Every $x \in N_1 + \cdots + N_k$ can be written uniquely in the form $a_1 + \cdots + a_k$ with $a_i \in N_i$.

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

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

By the theorem, this is equivalent the condition that every element $m \in M$ can be written uniquely as the sum of elements $m = n_1 + \cdots + n_k$ for $n_i \in N_i$. Part (1) of the theorem is the statement that the internal direct sum of $N_1, \ldots, N_k$ is isomorphic to the external direct sum, which is why we identity them and use the same notation.

Definition 4.26. An R-module F is said to be *free* on the subset A of F if for every nonzero element $x \in F$, there exist unique nonzero elements $r_1, \ldots, r_n \in R$ and unique $a_1, \ldots, a_n \in A$ such that

$$x = r_1 a_1 + \cdots + r_n a_n,$$

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.

There is a difference between the uniqueness property of direct sum and the uniqueness property of free modules. In the direct sum of two modules, say $N_1 \oplus N_2$, each element can be written uniquely as $n_1 + n_2$, where uniqueness refers to the module elements n_1 and n_2. In free modules, the uniqueness is on the ring elements (scalars) and the module elements.

Example 4.27. Let $R = \mathbb{Z}$ and $N_1 = N_2 = \mathbb{Z}/2\mathbb{Z}$. Then each element of $N_1 \oplus N_2$ can be written uniquely in the form $n_1 + n_2$, where $n_i \in N_i$. However, n_1 can be expressed as n_1 or $3n_1$ or $5n_1$, etc. So, each element does not have a unique representation in the form $r_1 a_1 + r_2 a_2$, where $r_1, r_2 \in R$, $a_1 \in N_1$, and $a_2 \in N_2$. Thus, $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is not a free $\mathbb{Z}$-module on the set $\{(1,0),(0,1)\}$ (or any set actually).

Theorem 4.28. For any set A, there is a free R-module $F(A)$ on the set A, where $F(A)$ satisfies the following *universal property*: If M is any R-module and $\phi : A \to M$ is any map of sets, then there is a unique R-module homomorphism $\Phi : F(A) \to M$ such that $\Phi(a) = \phi(a)$ for all $a \in A$. When A is the finite set $\{a_1, \ldots, a_n\}$, $F(A) = Ra_1 \oplus \cdots \oplus Ra_n \cong R_n$.

Corollary 4.29.

(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 that is the identity 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 Theorem 4.28.

Part (2) of the corollary guarantees that we can specify an R-module homomorphism from a free module F into some other R-module by simply stating its value on the elements of a basis and then extending linearly.

When $R = \mathbb{Z}$, the free module on a set A is called the **free abelian group on** A. If $|A| = n$, $F(A)$ is called the free abelian group of **rank** n and is isomorphic to $\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ (n summands).