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 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 $R[x_1, \ldots, x_n]$ 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 $a \in A$.