NOVEMBER 28 NOTES

1. 10.1: Introduction to Modules

Reminder. If G was a group and A was a set, we said that G acted on A if there was a map $G \times A \to A$ such that $(g, a) \mapsto g \cdot a$ satisfying:

(1) $1 \cdot a = a$ and
(2) $g \cdot (h \cdot a) = (gh) \cdot a$.

If we were to analogously define an action of a ring on a set M, we would want it to be compatible with the ring axioms, i.e.: $r(sm) = (rs)m$ and $(r+s)m = rm+sm$. This leads us to the definition of a *module*. Note that the symbols $rm + sm$ having meaning requires that there is a binary operation $+$ on the set M (and commutativity of $+$ in R would require this to be commutative as well).

Definition 1.1. Let R be a ring. A **left R-module** or just an **R-module** is a set M together with

(1) A binary operation $+$ on M for which M is an abelian group
(2) An action of R on M, denoted by rm, satisfying, for all $r, s \in R$, $m, n \in M$
    (a) $(r + s)m = rm + sm$
    (b) $(rs)m = r(sm)$
    (c) $r(m + n) = rm + rn$
    (d) If r has identity, $1m = m$.

Remark 1.2. If R is a field F, these axioms defining a module are exactly the definition of a vector space V. In other words, vector spaces over F are the same as modules over F.

Definition 1.3. If M is an R-module, an R **submodule** of M is a subgroup $N \leq M$ that is closed under the action of the ring elements, i.e. $rn \in N$ for all $r \in R, n \in N$.

Using the criteria to be a subgroup, we have the following criteria to determine is N is a submodule:

Proposition 1.4. *If R is a ring and M is an R module, a subset N of M is a submodule of M if and only if $N \neq \emptyset$ and $x + ry \in N$ for all $r \in R$ and $x, y \in N$.*

Example 1.5.
(1) If R is a ring, then R is a R-module where the action is given by multiplication of ring elements.
(2) Let $R^n = R \times \cdots \times R$ (n times). This is an R-module where $r(a_1, \ldots, a_n) := (ra_1, \ldots, ra_n)$. This is called the **free module** of rank n over R.
(3) If M is an R-module and S is a subring of R (with $1_S = 1_R$), then M is also an S-module. For example, because $\mathbb{R}$ is a $\mathbb{R}$-module, it is also a $\mathbb{Z}$-module.

Definition 1.6. If M is an R-module and I is an ideal of R, we say that I **annihilates** M if $am = 0$ for all $a \in I, m \in M$.

Example 1.7. If M is an R module and I annihilates M, then M is an R/I module by the action $(r + I)m := rm$.

Example 1.8. Let $R = \mathbb{Z}$ and A be any abelian group (written additively). Then, A is a $\mathbb{Z}$ module with action $na = a + a + \cdots + a$ (n times) for $n > 0$, $na = 0$ if $n = 0$, and $na = -a + \cdots + -a$ if $n < 0$. This satisfies the axioms for A to be a $\mathbb{Z}$ module. Note that *any* module is by definition an abelian group, so we have shown that abelian groups are the same as $\mathbb{Z}$-modules.

By definition of submodule, we also have that submodules are the same as subgroups of abelian groups.

If there is some integer n such that $na = 0$ for all $a \in A$ (for example, if $n = |A|$), then A is a $\mathbb{Z}/n\mathbb{Z}$ module.

Example 1.9. Suppose F is a field and $R = F[x]$. Let V be a vector space over F and $T : V \to V$ a linear transformation. We can use T to define an action of R on V so that V is a module over $F[x]$. If $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$ and $v \in V$, then we define

$$p(x)v = (a_n T^n + \cdots + a_1 T + a_0)v$$

where T^i means apply the transformation T i times.

By properties of polynomials and linear transformations, this satisfies the axioms for V to be an $F[x]$-module.

Note that this action depends on T; i.e. any choice of T makes V into a $F[x]$-module, but these module structures can be all different!

A special type of R-module is called an R-algebra.

Definition 1.10. Let R be a commutative ring with identity. An R**-algebra** is a ring A with identity and a ring homomorphism $f : R \to A$ such that $f(1_R) = 1_A$ and $f(R)$ is contained in the center of A.

This is a special type of R-module that happens to be a ring; the action is given by $ra := f(r)a$ (where $f(r)a$ is just the multiplication of $f(r)$and a in the ring A).

Definition 1.11. If A and B are two R-algebra, an R**-algebra homomorphism** is a ring homomorphism $\phi : A \to B$ such that $\phi(1_A) = 1_B$ and $\phi(ra) = r\phi(a)$ for all $r \in R, a \in A$.

Example 1.12. If R is a commutative ring, let $A = R[x]$. This has a natural homomorphism $f : R \to A$ given by $f(r) = r$. This also satisfies that $f(1_R) = 1_A$ and $f(R)$ is contained in the center of A so A is indeed an R-algebra.

2. 10.2: Quotient modules and module homomorphisms

Definition 2.1. 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, for all $x, y \in M$ and $r \in R$:

$$\phi(x + y) = \phi(x) + \phi(y)$$
$$\phi(rx) = r\phi(x)$$

(2) A bijective homomorphism of modules is an **isomorphism**.

(3) If $\phi : M \to N$ is a homomorphism of modules, then

$$\ker \phi = \{m \in M \mid \phi(m) = 0\}$$
$$\phi(M) = \text{im}\phi = \{n \in N \mid n = \phi(m) \text{ for some } m \in M\}$$

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

Proposition 2.2. *Let M, N, and L be R-modules.*

(1) A map $\phi : M \to N$ is an R-module homomorphism if and only if, for all $x, y \in M$ and $r \in R$,

$$\phi(rx + y) = r\phi(x) + \phi(y).$$

(2) $\text{Hom}_R(M, N)$ is an abelian group, where the group structure is given by $(\phi+\psi)(m) = \phi(m)+\psi(m)$, and if R is commutative, it is an R-module where the action is given by $(r\phi)(m) = r(\phi(m))$.

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

(4) *If we define multiplication as function composition, then* $\mathrm{Hom}_R(M, M)$ *is a ring with identity. If* R *is commutative, it is an* R*-algebra.*

Proof. For (1), the forward implication holds by definition. For the converse, if $r = 1$, then the equality implies $\phi(x + y) = \phi(x) + \phi(y)$, and if $y = 0$, the equality implies that $\phi(rx) = r\phi(x)$, so ϕ is an R-module homomorphism.

For (2), we leave checking that $\mathrm{Hom}_R(M, N)$ is an abelian group as an exercise. To show it is an R-module, since we have defined the action, we just need to verify that $r\phi$ as defined is an R-module homomorphism. This holds because:

$$\begin{aligned}(r\phi)(ax + y) &= r(\phi(ax + y)) && \text{by definition}\\ &= r(a\phi(x) + \phi(y)) && \text{because } \phi \text{ is a homomorphism}\\ &= ra\phi(x) + r\phi(y) && \text{because } N \text{ is a module}\\ &= ar\phi(x) + r\phi(y) && \text{because } R \text{ is commutative}\\ &= a(r\phi)(x) + (r\phi)(y)\end{aligned}$$

so this is an R-module homomorphism.

For (3), we need to show that $\psi \circ \phi$ is an R-module homomoprhism. Using (1), this is straightforward from the definition, so we leave this as an exercise.

For (4), one checks that $\mathrm{Hom}_R(M, M)$ is a ring with identity equal to the identity function–this is an exercise. To show it is an algebra, let $f : R \to \mathrm{Hom}_R(M, M)$ be the function sending r to the homomorphism that is multiplication by r (which we still denote by r), and define $\phi r := r\phi$ for all $r \in R$ and $\phi \in \mathrm{Hom}_R(M, M)$. This makes $\mathrm{Hom}_R(M, M)$ an R-algebra. □

Definition 2.3. The **endomorphism ring** of an R-module is the ring $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$. Elements of this ring are called **endomorphisms**.

Finally, note that modules are abelian groups, so if N is a submodule of M, then N is normal in M. And, if M is an R-module, then the quotient group M/N is an R-module where the action on the cosets is given by $r(x + N) = rx + N$. With this observation, we have the same isomorphism theorems as usual.

Theorem 2.4. (1) *(The First Isomorphism Theorem.) If* $\phi : M \to N$ *is an* R*-module homomorphism, then the kernel of* ϕ *is a submodule of* M *and* $M/\ker\phi \cong \phi(M)$.

(2) *(The Second Isomorphism Theorem.) Let* A, B *be submodules of an* R*-module* M*. Then, defining* $A + B = \{a + b \mid a \in A, b \in B\}$, $(A + B)/B \cong A/(A \cap B)$.

(3) *(The Third Isomorphism Theorem.) Let* M *be an* R*-module and* A, B *be submodules with* $A \subset B$*. Then,* $(M/A)/(B/A) \cong M/B$.

(4) *The submodules of* M/N *are precisely the submodules of* M *containing* N.