NOVEMBER 30 NOTES

1. 10.3: Generation, Direct Sums, and Free Modules

Reminder from last time:

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, $1m = m$.

Now, new stuff: Throughout this section, R will be a ring with 1.

Definition 1.2. 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

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

(2) For any subset A of M, let

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

If $A = \{a\}$ is one element, then $RA = \{ra \mid r \in R\}$.
If $A = \{a_1, \ldots, a_k\}$ is finite, we will write

$$RA = Ra_1 + \cdots + Ra_k.$$

We call RA the **submodule of** M **generated by** A. If N is a submodule of M such that $N = RA$, we say that N is **generated by** A.

(3) A submodule N of M is **finitely generated** if $N = RA$ for some finite set $A \subset M$.
(4) A submodule N of M is **cyclic** if $N = Ra$ for some $a \in M$.

Example 1.3. Let $R = \mathbb{Z}$ and M be an R-module, which is just an abelian group. If $a \in M$, then $\mathbb{Z}a = \{na \mid n \in \mathbb{Z}\} = \langle a \rangle \leq M$.

Example 1.4. Let R be a ring and $M = R$. Then, R is finitely generated and cyclic: $R = R1$. If $I = (a)$ is a principal ideal, it is also cyclic: $I = Ra$, and in fact the cyclic submodules of R are exactly the prinicpal ideals.

If $M = R^n$ is the free R-module of rank n, let $e_i = (0, \ldots, 0, 1, 0 \ldots, 0)$ (the 'standard basis vector' with 1 in the ith place). Then, $M = Re_1 + \cdots + Re_n$.

Definition 1.5. Let $M_1, \ldots, M_k$ be R-modules. The **direct product** of these modules is

$$M_1 \times \cdots \times M_k = \{(m_1, \ldots, m_k) \mid m_i \in M_i\}$$

(just the direct product of the abelian groups) where the R-action is defined component-wise.

This is often called the **direct sum** and denoted $M_1 \oplus \cdots \oplus M_k$.

We always have a homomorphism of R modules

$$\pi : N_1 \times \cdots \times N_k = N_1 + \cdots + N_k$$

defined by $\pi(a_1, \ldots, a_k) = a_1 + \cdots + a_k$. This is surjective by definition, but is not necessarily injective. By definition of injectivity, we have the folllowing:

Proposition 1.6. *The map π defined above is an isomorphism if and only if every $x \in N_1 + \cdots + N_k$ can be written uniquely as $x = a_1 + \cdots + a_k$ for $a_i \in N_i$.*

It turns out that this is equivalent to the following (which you can prove as an exercise; this is just another way of stating what it means for the sum to be unique):

Proposition 1.7. *The map π is an isomorphism if and only if $N_j \cap (N_1 + \ldots N_{j-1} + N_{j+1} + \cdots + N_k) = 0$ for all $j \in \{1, \ldots, k\}$.*

Definition 1.8. If $M = N_1 + \cdots + N_k \cong N_1 \times \cdots \times N_k$, then we use the direct sum notation and write $M = N_1 \oplus \cdots \oplus N_k$.

Definition 1.9. An R module F is **free on a subset** $A \subset F$ if every nonzero element $x \in F$ can be written *uniquely* as $x = r_1 a_1 + \cdots + r_n a_n$ for elements $r_i \in R$, $a_i \in A$. We say that A is a **basis** for F in this setting.

If $A = \{a_1, \ldots, a_k\}$ is a nonempty finite set, then the **free module on the set** A is the module $F(A) = Ra_1 \oplus \cdots \oplus Ra_k$.[1]

If $R = \mathbb{Z}$, we call this module the **free abelian group** on A.

2. 10.4: Tensor Products

We aim to define **tensor products** of modules, which, roughly speaking, allow us to define 'products' mn of elements $m \in M$ and $n \in N$. Your book does this in general, but we will assume that R is commutative with identity to make the notation/definitions simpler.

First, we construct a special case as motivation:

Question 2.1. If R is a subring of another ring S that is commutative with identity, then given any S-module M, it is automatically an R-module. More generally, if $f : R \to S$ is any ring homomorphism, then M is an R-module via $rm := f(r)m$.

In this set-up, we say that S is an *extension* of R, and M is an R-module by *restriction of scalars* (we restrict the action to just elements of R, instead of all elements of S).

Can we go the other way? Meaning, if we have an R-module N, can we consider it as an S-module? Or can we modify it/enlarge it to be an S-module? This is what the tensor product will do.

Construction. Suppose that R is a subring of S, and that N is an R-module. Then, $S \times N$ is an abelian group. If N were to be an S module, we would have to define an action $S \times N \to N$ where $(s, n) \mapsto sn$ satisfying that $(s_1 + s_2)n = s_1 n + s_2 n$ and the rest of the module axioms. This doesn't quite work, but gives the inspiration for the construction.

Consider the free $\mathbb{Z}$-module $F(S \times N)$ on the set $S \times N$, which is the collection of all finite sums of elements (s_i, n_i) with $s_i \in S$ and $n_i \in N$. Let H be the subgroup generated by all elements of the form:

$$(s_1 + s_2, n) - (s_1, n) - (s_2, n)$$
$$(s, n_1 + n_2) - (s, n_1) - (s, n_2)$$
$$(sr, n) - (s, rn)$$

for elements $s, s_1, s_2 \in S$, $n, n_1, n_2 \in N$, and $r \in R$.

[1] One can generalize to infinite sets–see the book for more.

Denote by $S \otimes_R N$ ('S tensor N', where the symbol $\otimes$ is typeset by 'otimes') the quotient of $F(S \times N)$ by this subgroup H. Let $s \otimes n$ be the coset of the element (s, n) in this quotient. The group $S \otimes_R N$ is called the *tensor product* of S and N, elements of $S \otimes_R N$ are called *tensors* and elements of the form $s \otimes n$ are called *simple tensors*.

By construction, every element of the tensor product can be written as a finite sum of simple tensors, and we have forced the relations:

$$(s_1 + s_2) \otimes n = s_1 \otimes n + s_2 \otimes n$$
$$s \otimes (n_1 + n_2) = s \otimes n_1 + s \otimes n_2$$
$$sr \otimes n = s \otimes rn.$$

We define an action of S on $S \otimes_R N$ by

$$s(s_1 \otimes n_1 + \cdots + s_k \otimes n_k) = (ss_1) \otimes n_1 + \cdots + (ss_k) \otimes n_k.$$

One has to check that this is well defined (because there is typically no unique way of writing a tensor as a sum of simple tensors), but that follows by construction.

Finally, one can show that this action makes $S \otimes_R N$ into an S module. For example:

$$\begin{aligned}(s + s') \otimes (s_i, n_i) &= ((s + s')s_i) \otimes n_i \\ &= (ss_i + s's_i) \otimes n_i \\ &= (ss_i) \otimes n_i + (s's_i) \otimes n_i \\ &= s(s_i \otimes n_i) + s'(s_i \otimes n_i).\end{aligned}$$

The remaining axioms are checked similarly.

So, we have 'extended' the R-module N to the S-module $S \otimes_R N$. This is usually referred to as *extension of scalars*.

Note that there is a natural R-module homomorphism $i : N \to S \otimes_R N$ given by $i(n) = 1 \otimes n$. Using this homomorphism, we can show that module $S \otimes_R N$ is, in a precise sense, the 'smallest' S module we can make that admits a homomorphism from N. This is why this is usually referred to as 'extension' to S. We'll introduce this as a theorem next time. But first, an example!

Example 2.2. What is $\mathbb{Q} \otimes_{\mathbb{Z}} A$, where A is an abelian group? We'll do the finite abelian group case today. First observe that $s \otimes 0 = s \otimes (0 + 0) = s \otimes 0 + s \otimes 0$, so subtracting one $s \otimes 0$ from both sides shows that $s \otimes 0 = 0$. (This is true in any tensor product!)

Now suppose A is a finite abelian group with $|A| = n$. By Lagrange's Theorem, this means $na = 0$ for any $a \in A$. Let $q \otimes a \in \mathbb{Q} \otimes_{\mathbb{Z}} A$ be any simple tensor. Because $q = (q/n)n$, we can write

$$q \otimes a = ((q/n)n) \otimes a = q/n \otimes na = q/n \otimes 0 = 0$$

so any simple tensor is just equal to 0. Because every element of $\mathbb{Q} \otimes_{\mathbb{Z}} A$ is a sum of simple tensors, this implies that $\mathbb{Q} \otimes_{\mathbb{Z}} A = 0$ for all finite abelian groups.