DECEMBER 7 NOTES

1. 10.4: (One more example of) Tensor Products

Example 1.1. Let R be a ring and I an ideal and N an R-module. There is an N-submodule IN defined to be all finite sums of products of elements in I with elements in N.

In this case, $R/I \otimes_R N \cong N/IN$. Because $1 \in R/I$ (the image of 1 in R) generates R/I as an R-module, the elements $1 \otimes n$ generate $R/I \otimes_R N$. There is an R-module homomorphism $N \to R/I \otimes_R N$ sending $n \mapsto 1 \otimes n$, which is surjective because the elements $1 \otimes n$ generate the tensor product. The kernel must contain IN because, if $a_i n_i \in IN$ ($a_i \in I, n_i \in N$), this maps to $1 \otimes a_i n_i = a_i \otimes n_i = 0$ because $a_i = 0 \in R/I$. This gives a surjective map $N/IN \to R/I \otimes_R N$, and we must show it is an isomorphism. But this follows because it has an inverse: $R/I \otimes_R N \to N/IN$ given by $(r, n) \mapsto rn$ can be checked to be the inverse of this map.

A few other properties of the tensor product:

Theorem 1.2. *If $\phi : M \to M'$ and $\psi : N \to N'$ are R-module homomorphisms, then*

$$\phi \otimes \psi : M \otimes_R N \to M' \otimes_R N'$$

given by $(\phi \otimes \psi)(m \otimes n) = \phi(m) \otimes \phi(n)$ is an R-module homomorphism.

Theorem 1.3. *If M, N, L are R-modules, then $(M \otimes_R N) \otimes_R L \cong M \otimes_R (N \otimes_R L)$.*

Theorem 1.4. *Let M, M' and N, N' be R-modules. Then,*

$$(M \oplus M') \otimes_R N \cong (M \otimes_R N) \oplus (M' \otimes_R N)$$
$$M \otimes_R (N \oplus N') \cong (M \otimes_R N) \oplus (M \otimes_R N').$$

Corollary 1.5. If S is a ring and $f : R \to S$ a homomorphism so that S is an R-module via $rs = f(r)s$, then $S \otimes_R \cong R$ and $S \otimes_R R^n \cong S^n$.

Corollary 1.6. For a ring R, $R^s \otimes_R R^t \cong R^{st}$. This says that the tensor product of two free modules of finite rank is again free.

2. 11.5: Tensor Algebras, Symmetric and Exterior Algebras

We will continue to assume that R is a commutative ring with identity.

Definition 2.1. For each $k \geq 1$, let $T^k(M) = M \otimes_R M \otimes_R \cdots \otimes_R M$ (with k M's). Let $T^0(M) = 0$. Define

$$T(M) = R \oplus T^1(M) \oplus T^2(M) \oplus \cdots = \oplus_{k=0}^{\infty} T^k(M).$$

$T(M)$ is called the **tensor algebra** of M. The elements of the summand $T^k(M)$ are called k-tensors.

This is called an algebra because it is an R-algebra (remember, this is a ring that is also an R-module). It is an R-module because it is a sum of R-modules, and hence it is an abelian group, and it becomes a ring when we define multiplication to be

$$(m_1 \otimes \ldots m_i)(m_1' \otimes \cdots \otimes m_j') = m_1 \otimes \cdots \otimes m_i \otimes m_1' \otimes \cdots \otimes m_j'.$$

By definition, $T^i(M) T^j(M) \subset T^{i+j}(M)$.

By definition of tensor product, R commutes with $T(M)$, so this is indeed an R-algebra.

The tensor algebra is a ring, but is actually an example of something called a graded ring.

Definition 2.2. A ring R is called a **graded ring** if $S = S_0 \oplus S_1 \oplus \dots$ such that each S_i is a subgroup and $S_i S_j \subset S_{i+j}$ for all $i, j \geq 0$. The elements of the subgroup S_k are called **homogeneous of degree** k.

An ideal I in a graded ring S is called a **graded ideal** if $I = \oplus_{k=0}^{\infty}(I \cap S_k)$.

A ring homomorphism between graded rings $\phi : S \to T$ is called a **graded homomorphism** if $\phi(S_k) \subset T_k$.

Example 2.3. The polynomial ring $S = R[x]$ is a graded ring, where $S_i = Rx^i$. In this ring, (x) is a graded ideal, but $I = (1 + x)$ is not: it is not homogeneous, and cannot be written as a sum of homogeneous elements where each element is in I.

Example 2.4. By definition, $T(M)$ is a graded ring.

If S is a graded ring and I is a graded ideal, let $I_k = I \cap S_k$. Then, by the first isomorphism theorem, $S/I \cong \oplus_{k=0}^{\infty} S_k/I_k$ (exercise: define a map $S = \oplus S_k \to \oplus S_k/I_k$ by the quotient on each component, and show the kernel is I). Therefore, S/I is a graded ring and the homogeneous part of degree k is just S_k/I_k.

Definition 2.5. The **symmetric algebra** of an R-module M is $S(M) = T(M)/C(M)$, where $C(M)$ is the ideal of $T(M)$ generated by all elements of the form $m_1 \otimes m_2 - m_2 \otimes m_1$.

In effect, the symmetric algebra is *forced* to be commutative. Because $T(M)$ is generated as a ring by R and $T^1(M) = M$ and we are making these commute in the quotient ring, $S(M)$ is commutative. We can say precisely what the graded pieces are:

Theorem 2.6. *The kth graded piece $S^k(M)$ of $S(M)$ is called the kth symmetric power of M and is given by $M \otimes \cdots \otimes M$ modulo the submodule generated by all elements*

$$m_1 \otimes m_2 \otimes \cdots \otimes m_k - m_{\sigma(1)} \otimes m_{\sigma(2)} \otimes \cdots \otimes m_{\sigma(k)}$$

where m_i in M and $\sigma \in S_k$ (the symmetric group).

Proof. The elements in $C^k(M)$ are finite sums of elements of the form

$$m_1 \otimes \dots m_{i-1} \otimes (m_i \otimes m_{i+1} - m_{i+1} \otimes m_i) \otimes m_{i+2} \otimes \cdots \otimes m_k,$$

but distributing this gives

$$m_1 \otimes \dots m_{i-1} \otimes m_i \otimes m_{i+1} \otimes m_{i+2} \otimes \cdots \otimes m_k - m_1 \otimes \dots m_{i-1} \otimes m_{i+1} \otimes m_i \otimes m_{i+2} \otimes \cdots \otimes m_k$$

which is the difference of two elements that differ by the transposition $\sigma = (i i+1) \in S_k$. Because the symmetric group is generated by transpositions, the theorem follows. □

Definition 2.7. The **exterior algebra** of an R-module M is the algebra obtained by quotienting $T(M)$ by the ideal $A(M)$ generated by elements of the form $m \otimes m$ for $m \in M$. The exterior algebra is denoted $\bigwedge(M)$ and the image of $m_1 \otimes \cdots \otimes m_k$ in $\bigwedge(M)$ is denoted by $m_1 \wedge \cdots \wedge m_k$ (where the $\wedge$ is pronounced 'wedge').

The exterior algebra is the algebra we get where we 'force' tensors to have no repeated elements (those we set equal to 0). Here, the A stands for *alternating* because, for any $m_1, m_2 \in M$,

$$\begin{aligned} 0 &= (m_1 + m_2) \wedge (m_1 + m_2) \\ &= m_1 \wedge m_1 + m_2 \wedge m_1 + m_1 \wedge m_2 + m_2 \wedge m_2 \\ &= m_2 \wedge m_1 + m_1 \wedge m_2 \end{aligned}$$

so $m_2 \wedge m_1 = -m_1 \wedge m_2$. Even if we had a longer tensor with more elements, this says that switching the order of any two adjacent terms just changes the sign. So, a tensor $m_1 \wedge \cdots \wedge m_k = 0$ if and only if there are two repeated terms. This gives the following:

Theorem 2.8. *In $\bigwedge(M)$, the kth exterior power $\bigwedge^k(M)$ is $M \otimes \cdots \otimes M$ modulo the submodule generated by $m_1 \otimes \cdots \otimes m_k$ where $m_i = m_j$ for some $i \neq j$. In particular, $m_1 \wedge \cdots \wedge m_k = 0$ if $m_1 = m_j$ for $i \neq j$.*

These modules are very important! You will see more examples on the homework.

3. 12.1: Finitely generated modules over PIDs

To conclude the class, we will classify finitely generated modules over PIDs. Some preliminaries (linear algebra things); the proofs look like the proofs you've seen in linear algebra, so we omit them. I encourage you to take a look in the book, though, because these results are where 'PID' comes in.

Definition 3.1. For any integral domain R, the **rank** of an R-module M is the maximal number of R-linearly independent elements of M.

Theorem 3.2. *If R is a PID and M is a free R-module of finite rank n, and N is any submodule of M, then:*

1. *N is free of rank $m \leq n$, and*
2. *there is a basis $\{y_1, \ldots, y_n\}$ of M such that $\{a_1y_1, \ldots, a_my_m\}$ is a basis for N, where $a_1, a_2, \ldots, a_m$ are nonzero elements of R.*

This brings us to the main theorem!

Theorem 3.3. *Let R be a PID and M a finitely generated R-module. Then:*

$$M \cong R^r \oplus R/(a_1) \oplus \cdots \oplus R/(a_m)$$

for some integer $r \geq 0$ and nonzero, nonunit elements $a_i \in R$.

*The elements a_i are called the **invariant factors** of M.*

Proof. We prove the existence part. Because M is finitely generated, we can choose a set $\{x_1, \ldots, x_n\}$ that generates M and n is minimal. Then, there is a surjective homomorphism from the free R-module R^n with basis $\{b_1, \ldots, b_n\}$ given by $\pi : R^n \to M$ sending $\pi(b_i) = x_i$.

By the First Isomorphism Theorem, we know $R^n/\ker \pi \cong M$, but by the previous linear algebra theorems, because $\ker \pi$ is a submodule of R^n, we can choose a different basis $\{y_1, \ldots, y_n\}$ of R^n such that $\ker \pi$ has basis $\{a_1y_1, \ldots, a_my_m\}$, and then

$$M \cong R^n/\ker \pi = (Ry_1 \oplus \cdots \oplus Ry_n)/(Ra_1y_1 \oplus \cdots \oplus Ra_my_m) \cong R/(a_1) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m}.$$

We may assume each a_i is not a unit because, if a_i were a unit, then $R/(a_i) = 0$ so we may remove it from the sum. □

We can further decompose using the Chinese Remainder Theorem! Because PIDs are UFDs, for each $a \in \{a_1, \ldots, a_m\}$, we can write $a = up_1^{\alpha_1} \ldots p_s^{\alpha_s}$ where u is a unit and p_i is prime. Then, by the Chinese Remainder Theorem,

$$R/(a) \cong R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_s^{\alpha_s}).$$

Therefore, an alternative version of the previous theorem says:

Theorem 3.4. *Let R be a PID and M a finitely generated R-module. Then:*

$$M \cong R^r \oplus R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_t^{\alpha_t})$$

for some integer $r \geq 0$ and primes p_i. This decomposition is unique up to reordering.

*The elements $p_i^{\alpha_i}$ are called the **elementary divisors** of M.*

If $R = \mathbb{Z}$, this theorem is *exactly* the classification of finitely generated abelian groups!