Section 12.1 Modules over a PID : Basic Theory (Continued)

Today we explore a major structure theorem for modules, but first, recall the following results, which we will need.

Theorem 17 (Chapter 7) Chinese Remainder Theorem
Suppose $A_1\ A_2\ \cdots\ A_K$ are ideals in a commutative ring R.
If $A_i + A_j = R \quad \forall\, i \neq j$ (i.e. A_i are comaximal) then:

$$R/A_1A_2A_3\cdots A_K \cong R/A_1 \times R/A_2 \times \cdots \times R/A_K$$

Consequence: Suppose R is a PID, $p_1\ p_2\ \cdots\ p_k \in R$ and $\gcd(p_i, p_j) = 1 \quad \forall\, i \neq j$ [i.e. $(p_i) + (p_j) = (1) = R$]. Then $(p_1)(p_2)\cdots(p_k) = (p_1 p_2 \cdots p_k)$ and

$$R/(p_1 p_2 \cdots p_k) \cong R/(p_1) \times R/(p_2) \times \cdots \times R/(p_k)$$
$$= R/(p_1) \oplus R/(p_2) \oplus \cdots \oplus R/(p_k)$$

Theorem 4 Suppose M is a free R-module, rank m, over a PID R, and $N \subseteq M$ is a submodule. Then:

(1) N is a free module, rank $n \leq m$.

(2) M has basis $\{y_1\ y_2\ \cdots\ y_n\ \cdots\ y_m\}$ such that N has basis $\{a_1y_1\ a_2y_2 \cdots\ a_ny_n\}$, where $a_i \in R$ and $a_1 \mid a_2 \mid a_3 \mid \cdots \mid a_n$

Next, lets look at some known examples of R-modules over a PID R to set the stage for our theorem:

Example Suppose M is cyclic, i.e. $M = Rx_0$ for some $x_0 \in M$.
Then we have surjective R-module homomorphism

$$\varphi : R \longrightarrow M$$
$$r \longmapsto r x_0$$

Thus $M \cong R/\ker\varphi = R/(a)$.

$$M \cong R/(a)$$

Module structure of M identical to a quotient of R

This is the way things tend to work

<u>Example</u> M is finitely generated R-module for field R.
Thus M is just a finite-dimensional vector space, and

Then $M \cong R \oplus R \oplus R \oplus \cdots \oplus R$
$= R/(0) \oplus R/(0) \oplus \cdots \oplus R/(0)$

Module structure built up by quotients of R.

<u>Example</u> M is a finitely generated $\mathbb{Z}$-module
Thus M is just an abelian group.

Then $M \cong \mathbb{Z}/(p_1) \oplus \mathbb{Z}/(p_2) \oplus \cdots \oplus \mathbb{Z}/(p_k) \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$

$= \mathbb{Z}/(0)$, etc.

Again module structure is built up by quotients of $R = \mathbb{Z}$

Our structure theorem says its <u>always</u> like this!

<u>Theorem 5</u> Suppose M is a finitely generated module over a PID R.

(1) $M \cong R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$
where $a_1 | a_2 | a_3 | \cdots | a_m$.

(2) M is torsion-free $\iff M \cong R^m$

(3) $\operatorname{Tor}(M) = R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$

Elements $a_1\ a_2 \ldots a_n$ are called <u>invariant</u> <u>factors</u> of M
Integer r is called the <u>free</u> <u>rank</u> of M

<u>Proof</u> Let $\{x_1\ x_2 \ldots x_m\}$ be minimal set of generators of M.
Let R^m be free with basis $\{b_1\ b_2 \ldots b_m\}$.
Surjective homomorphism: $\pi : R^m \longrightarrow M$
$$\sum r_i b_i \mapsto \sum r_i x_i$$

Theorem 4 Says
R^m has basis $\{y_1\ y_2\ y_3 \ldots y_n \ldots y_m\}$
$\operatorname{Ker}(\pi)$ has basis $\{a_1y_1\ a_2y_2\ a_3y_3 \ldots a_ny_n\}$
with $a_1 | a_2 | a_3 | \cdots | a_n$

Thus $M \cong R^m / \ker(\pi)$

$$= Ry_1 \oplus Ry_2 \oplus \cdots \oplus Ry_m \,/\, Ra_1y_1 \oplus Ra_2y_2 \oplus \cdots \oplus Ra_ny_n \oplus 0 \oplus 0 \oplus \cdots \oplus 0.$$

$$= \underbrace{Ry_1/Ra_1y_1 \oplus \cdots \oplus Ry_m/Ra_ny_n}_{} \oplus \underbrace{Ry_{n+1}/0 \oplus \cdots \oplus Ry_m/0}_{}$$

$$= R/(a_1) \oplus \cdots \oplus R/(a_n) \oplus R \oplus R \oplus \cdots \oplus R$$

$$= R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_n)$$

<u>Note</u>: $Ry_1/Ra_1y_1 \cong R/(a_1)$

$ry_1 + Ra_1y_1 \longmapsto r + (a_1)$ etc

$\blacksquare$

Now look at factor

$$R/(a) = R/(\underbrace{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}}_{\text{prime factoring of } a}) = R/(p_1^{\alpha_1}) \oplus \cdots \oplus R/(p_k^{\alpha_k})$$

(Chinese remainder Theo.)

Applying this to our previous theorem yields:

<u>Theorem 6</u> Suppose M is finitely generated module over PID R. Then $M \cong R^r \oplus R/(p_1^{\alpha_1}) \oplus R/(p_2^{\alpha_2}) \oplus \cdots \oplus R/(p_t^{\alpha_t})$ where the p_i are primes in R.

The $p_i^{\alpha_i}$ are called <u>elementary divisors</u>

<u>Theorem 9</u> Suppose R is PID and M_1 & M_2 are f.g. R-modules.

(1) $M_1 \cong M_2 \iff M_1$ & M_2 have same free rank and list of invariant factors (up to mult. by units)

(2) $M_1 \cong M_2 \iff M_1$ & M_2 have same free rank and list of elementary divisors (up to mult by units)

<u>Application</u> Let $R = \mathbb{Z}$ (PID) so any R-module is an abelian group. Today's results become the structure theorems for finitely generated abelian groups from Section 5.2. So finally we have a proof of that theorem!

<u>Next Time</u> Applications to Linear Algebra