Modules/PIDs 2: [redacted]

Pf. (cont.) We ~~now~~ prove $rk\, N \leq rk\, M$ & N free of rk

by induction on $m = rk(N)$. If $m=0$, then N is a torsion module, but then $N=0$ as it's a submodule of a ~~torsion~~ free, hence torsion-free, module.

Suppose $m \geq 0$. Then by directness of the sum above, $N \cap \ker(v)$ has rank $m-1$ (see exercises).

By induction, $N \cap \ker(v)$ is free of rank $m-1 \leq n-1$. Again by directness of the sum, adjoining $a_1 y_1$ to a basis of $N \cap \ker v$ gives a basis of $N \Rightarrow N$ is free of rk m. other direct summand

We show the 8th basis statement for M, N.

Applying the rk proof above (pt. (i) of thm)

shows $\ker(v)$ is free, and by direct sum above $rk(\ker(v)) = n-1$. By inductive hypothesis on $\ker v$ and its submodule $\ker(v) \cap N$, there is a basis $y_2, \ldots, y_n$ of $\ker V$ s.t. $a_2 y_2, \ldots, a_m y_m$ is a basis of $N \cap \ker(v)$ for $a_2, \ldots, a_m \in R$, $a_2 | a_3 | \cdots | a_m$.

Since both sums above are direct, $y_1, \ldots, y_n$ is a basis of M, $a_1 y_1, \ldots, a_m y_m$ is a basis of N,

We just have to show $a_1 | a_2$. Consider the hom $\varphi: M \to R$ with $\varphi(y_1) = \varphi(y_2) = 1$, $\varphi(y_i) = 0$, $i \geq 3$,

Then $a_1 = \varphi(a_1 y_1) \Rightarrow a_1 \in \varphi(N) \Rightarrow (a_1) \subseteq \varphi(N)$.

By the maximality of the ideal (a_1) above, $(a_1) \supseteq \varphi(N)$.

Thus, $a_2 = \varphi(a_2 y_2) \in \varphi(N) \Rightarrow a_2 \in (a_1) \Rightarrow a_1 \mid$

Given a cyclic module Rx, consider the hom:

$$\pi : R \to C$$
$$r \mapsto rx$$

It's surjective by assumption, so

$$R/\ker(\pi) \cong C.$$

Now if R is a P.I.D., $\ker(\pi)$ is principal, say (a), and so cyclic modules are those of the form $R/(a)$ where $(a) = \mathrm{Ann}(C)$.

<u>Theorem</u> (Fund. Theorem, existence, invariant factors)

$R =$ P.I.D., $M =$ f.g. R-module.

1). M is isomorphic to a sum of cyclic modules:

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

where $r \geq 0$, $a_1, \ldots, a_m \in R \setminus \{0\}$ are non-units &

$$a_1 \mid a_2 \mid \cdots \mid a_m$$

2). M is torsion-free $\Leftrightarrow$ M is free.

3). $\mathrm{Tor}(M) \cong R/(a_1) \oplus \cdots \oplus R/(a_m)$ and $\mathrm{Ann}(\mathrm{Tor}(M)) = (a_m)$.

<u>Pf</u>: As M is f.g., say gens are $x_1, \ldots, x_n$ (of <u>minimal</u> cardinality). Let R^n have basis $b_1, \ldots, b_n$, and let

$$\pi : R^n \to M$$
$$b_i \mapsto x_i.$$

, is surjective as $\{x_i\}$ generates M.

$\Rightarrow$, $R^n/\ker(\pi) \cong M$. By the Thm above, we can pick another basis $y_1, \ldots, y_n$ of R^n s.t. $a_1y_1, \ldots, a_my_m$ is a basis of $\ker(\pi)$ & $a_1 | a_2 | \cdots | a_m$.

$\Rightarrow M \cong R^n/\ker(\pi) = (Ry_1 \oplus \cdots \oplus Ry_n)/(Ra_1y_1 \oplus \cdots \oplus Ra_my_m)$

To study this quotient, use the surjective hom.

$$Ry_1 \oplus \cdots \oplus Ry_n \to R/(a_1) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m}$$
$$(\alpha_1y_1, \ldots, \alpha_ny_n) \mapsto (\alpha_1 \bmod (a_1), \ldots, \alpha_m \bmod (a_m), \alpha_{m+1}, \ldots, \alpha_n),$$

The kernel of this map is the set of elts with $a_i | \alpha_i$ $\forall i = 1, \ldots, m$

ie, $Ra_1y_1 \oplus \cdots \oplus Ra_my_m \oplus 0 \oplus \cdots \oplus 0$

Thus, $M \cong R/(a_1) \oplus \cdots \oplus R/(a_m) \oplus R^{n-m}$

If $a \in R^\times$, then $R/(a) = 0$, so we can delete these.

This gives the desired decomposition.

Now as $R/(a)$ is torsion $\forall a \in R \setminus \{0\}$, the decomp. implies M is torsion free $\Leftrightarrow M \cong R^r$, ie, iff M is free. The final part follows right away from defn as the annihilator of $R/(a)$ is (a). $\boxtimes$

__Defn__ The integer r in the theorem is the free rank of M.

The ~~elt~~. $a_1, \dots, a_m$ are the <u>invariant factors</u>

Thm (Fund. Theorem, existence, ~~primary facts~~ elementary divisor form)
Assume the notation of last thm. Then

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

where $r \in \mathbb{Z}_{\geq 0}$, $p_1, \dots, p_t$ are primes in R, $\alpha_1, \dots, \alpha_t \in \mathbb{Z}_{\geq 0}$.

Pf/ We start from the invariant factor form.
$R = PID \Rightarrow R = UFD$. Thus, if $a \in R$ has prime factorization

$$a = u p_1^{\alpha_1} \cdots p_s^{\alpha_s}, \quad u \in R^\times,$$
(distinct primes)

the ideals $(p_i^{\alpha_i})$ are pairwise comaximal
(as $(p_i^{\alpha_i}, p_j^{\alpha_j})$ is gen. by a gcd which is 1 if $i \neq j$)
The intersection of $(p_i^{\alpha_i})$ is (a), as a is the lcm of $p_1^{\alpha_1}, \dots, p_s^{\alpha_s}$. Thus the Chinese remainder Thm

$$\Rightarrow R/(a) \cong R/(p_1^{\alpha_1}) \oplus \dots \oplus R/(p_s^{\alpha_s}).$$ (still works as R-modules)

Now apply this to the invariant factors. $\square$

Def: The prime powers in the last form are the <u>elementary divisors</u> of M

Next time: <u>uniqueness</u>

§(4).