5. Modules over a PID

* Throughout, R is a PID, and all modules are unitary.

Def: If M is an R-module, then $x \in M$ is a torsion element if $rx = 0$ for some $r \neq 0$ in R. (generalizes the concept of "finite order")

Def: If $x \in M$ is a torsion element, then its annihilator (or order ideal) is $Ann(x) = \{r \in R : rx = 0\}$.

Def: The ideal $Ann(x)$ is principal, and the generator s_x (i.e, $Ann(x) = (s_x)$) is called its order (unique up to associates).

Example: Let $R = \mathbb{Q}[x]$, and $M = V_T$ where $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, $u = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $v = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$

Then $Ann(u)$ and $Ann(v)$ are ideals of $R = \mathbb{Q}[x]$.

Note: If $f(x) = x - 1$, then $f(x) \cdot u = Tu - u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} - \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$.

$\Rightarrow |u| = x - 1$

If $g(x) = x^2 - 2x + 1$, then $g(x) \cdot v = T^2 v - 2Tv + v$

$= \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} - \begin{pmatrix} 2 \\ 2 \end{pmatrix} + \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$.

Check: $(ax + b) \cdot v \neq \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ and $x^2 - 2x + 1 \in Ann(v)$

$\Rightarrow |v| = x^2 - 2x + 1$

Def: Let $Tor(M)$ be the set of torsion elements of M.

(i) If $Tor(M) = M$, then M is a torsion module.

(ii) If $Tor(M) = \{0\}$, then M is torsion-free.

<u>Prop 5.1</u> $\mathrm{Tor}(M)$ is a submodule of M, and $M/\mathrm{Tor}(M)$ is torsion-free.

<u>Pf:</u> Pick $x, y \in T = \mathrm{Tor}(M)$; $|x| = a$, $|y| = b$.

We must show: $\underline{x - y \in T}$ and $\underline{rx \in T}$ $\forall r \in R$.

Consider $ab(x-y) = b \cdot ax - a \cdot by = 0 \Rightarrow x - y \in T$ ✓

Also, $a(rx) = r(ax) = 0 \Rightarrow rx \in T$ for any $r \in R$. ✓

Therefore, T is a submodule of M. ✓

Now, consider $r(x+T) = rx + T = T \in M/T$. [Goal: show $x \in T$]

Then $rx \in T \Rightarrow \mathrm{Ann}(rx) \neq 0$.

Pick $s \in \mathrm{Ann}(rx)$. Then $s \cdot rx = sr \cdot x = 0 \Rightarrow x \in T$ ✓ □

<u>Def:</u> $\mathrm{Tor}(M)$ is a submodule of M.

<u>Remark 1:</u> If A is an abelian group, then $\mathrm{Tor}(A)$ is the subgroup of elements of finite order.

<u>Remark 2:</u> Prop 5.1 actually holds if R is any integral domain.

<u>Prop 5.2:</u> If M is a finitely generated torsion-free R-module, then M is free of finite rank.

<u>Pf:</u> Let $M = R\langle x_1, \ldots, x_n \rangle$, and let $\{b_1, \ldots, b_k\}$ be a maximal linearly independent subset of $\{x_1, \ldots, x_n\}$.

<u>Claim:</u> $M \hookrightarrow N := R\langle b_1, \ldots, b_k \rangle \Rightarrow M$ is free (Thm 2.12).

For each x_i, $\exists\, s_i \neq 0 \in R$ and $r_{i1}, \dots, r_{ik} \in R$ s.t. $s_i x_i + \underbrace{\sum_{j=1}^{k} r_{ij} b_j}_{\in N} = 0$

$\Rightarrow s_i x_i \in N$.

Put $s = \prod_{i=1}^{n} s_i$. Clearly, $s x_i \in N \ \forall i \Rightarrow sm \in N \quad \forall m \in M$.

Define $f: M \longrightarrow N$, $f(m) = sm$.

Easy: $f \in \mathrm{Hom}_R(M, N)$.

Since M is torsion-free, $f(m) = sm \neq 0 \Rightarrow \ker f = 0$.

Thus $f: M \hookrightarrow N$.

Since R is a PID, M finitely generated & N free,

Thm 2.12 $\Rightarrow$ M is free. $\square$

<u>Thm 5.3</u>: If M is a finitely generated R-module, then M has a free submodule F of finite rank such that $M = \mathrm{Tor} \oplus F$. The rank of F is uniquely determined by M.

<u>Pf</u>: Let $\eta: M \longrightarrow M/\mathrm{Tor}(M)$ be the natural quotient map.

By Prop 3.1, $M = F \oplus \ker \eta = \mathrm{Tor}(M) \oplus F$ for some free R-module F, which is free by Prop 5.2.

By FHT for modules, $F \cong M/\mathrm{Tor}(M)$.

If $M = \mathrm{Tor}(M) \oplus F'$ for another free R-module F', then

$F' \cong M/\mathrm{Tor}(M) \cong F \Rightarrow F \cong F' \Rightarrow \mathrm{rank}\, F = \mathrm{rank}\, F'$. $\square$

Def: If M is a finitely generated R-module, then the rank of M is rank F, where $M = \text{Tor}(M) \oplus F$.

By Thm 5.3, this is well-defined.

Let M be a torsion module. Suppose $\exists\, r \in R^*$ with $rx = 0$ for all $x \in M$.

The set $I = \{ s \in R : sx = 0 \ \forall x \in M \}$ is an ideal of R, and its generator $a \in I$ (i.e, $I = (a)$) is called the exponent of M.

Clearly, $a \mid r$ and a is unique up to associates.

Remark: If M has an exponent $a \in M$, then $a = \text{lcm}\{x : x \in M\}$.

Not every torsion module has an exponent.

For example, $M = \bigoplus_{n=1}^{\infty} \mathbb{Z}_n$.

Finitely generated torsion modules have an exponent:

If $M = R\langle x_1, \ldots, x_n \rangle$ and $r_i \in \text{Ann}(x_i)$, then $r = r_1 r_2 \cdots r_n \in \text{Ann}(x_i) \Rightarrow M$ has an exponent $a \mid r$.

Exercise: If M is an R-module and $x, y \in \text{Tor}(M)$ with $|x| = r$, $|y| = s$, and $(x, y) = 1$ in R. Then $|x+y| = rs$.

Pf: Exercise.

Prop 5.4: If M is a torsion module with exponent $r \in R$, then M has an element of order r.

Pf: Since R is a PID, it is a UFD.

Write $r = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$, p_i's distinct primes $d_i > 0$.

Put $r_i = r/p_i$.

Since $r \nmid r_i$, $\exists\, x_i \in M$ s.t. $r_i x_i \neq 0$ for each i.

Put $y_i = (r/p_i^{d_i})\, x_i$.

Note: $p_i^{d_i} y_i = 0$ but $p_i^{d_i - 1} y_i = r_i x_i \neq 0 \Rightarrow |y_i| = p_i^{d_i}$.

Put $x = y_1 + \cdots + y_k$. By Exercise, $|x| = \prod_{i=1}^{k} |y_i| = r$. $\square$

Def: If M is an R-module and $s \in R$, define $M[s] = \{x \in M : sx = 0\}$ and let $sM = \{sx : x \in M\}$.

Exercise (easy): $M[s]$ & sM are submodules of M.

Notation: To avoid confusion, we'll write $(r,s) = \gcd(r,s)$ and $\langle r, s\rangle$ = ideal generated by r & s.

Prop 5.5: Suppose $M = R\langle y\rangle$ is cyclic of order r, and $s \in R$. Then

(i) $M[s] = R\left\langle \frac{r}{(r,s)} y \right\rangle \cong R/\langle (r,s)\rangle$

(ii) $sM = R\langle sy\rangle \cong R/\left\langle \frac{r}{(r,s)}\right\rangle$.

i.e., $M[s]$ is cyclic of order (r,s)

sM is cyclic of order $\frac{r}{(r,s)}$.

Pf: (i) $M[s] = \{uy : u \in R,\ suy = 0\}$, and $suy = 0$ iff $\frac{r}{(r,s)} \mid u$.

$$\Rightarrow M[S] = R\left\langle \frac{r}{(r,s)} y \right\rangle.$$

Define $\varphi : R \longrightarrow M[S]$

$$v \longmapsto \frac{vr}{(r,s)} y.$$

Clearly, φ is onto and $\ker \varphi = \langle r, s\rangle$. Apply FHT modules. ✓

(ii) Similar (exercise). ✓

Cor: If $(r,s) = 1$, then $M[S] = 0$ and $sM = M$.

Prop 5.6: Suppose $C = R\langle z\rangle$ is cyclic of order r_0, M is a finitely generated torsion R-module whose exponent divides r_0, N is a submodule of M, and $f \in \mathrm{Hom}_R(N, C)$. Then f extends to $g \in \mathrm{Hom}_R(M, C)$.

$$\begin{tikzcd} & C = R\langle z\rangle & \\ N \arrow[ur, "f"] \arrow[rr, hook] & & M = R\langle x_1, \dots, x_n\rangle \arrow[ul, dashed, "g"'] \end{tikzcd}$$

Pf: Say $M = R\langle x_1, \dots, x_k\rangle$.

Put $N_1 = N + R\langle x_1\rangle$, $N_2 = N_1 + R\langle x_2\rangle$, …, $N_k + R\langle x_k\rangle = M$.

By induction, it suffices to show that f extends to $g \in \mathrm{Hom}_R(N_1, C)$.

Let $s = |x_1 + N| \Rightarrow s(x_1 + N) = N \Rightarrow sx_1 \in N$

By def'n, $r_0 x_1 = 0 \Rightarrow r_0 x_1 + N = N \Rightarrow s \mid r_0$ (say $r_0 = st$).

Since $r_0 x_1 = 0$, $f(r_0 x_1) = f(tsx_1) = t\, f(sx_1) = 0 \Rightarrow |f(sx_1)| \,\big|\, t$ in $C = R\langle z \rangle$.

Say that $f(sx_1) = uz$, $u \in R$.

Then $t\, f(sx_1) = tuz = 0 \Rightarrow r_0 \mid tu$

Recall that $r_0 = st \Rightarrow st \mid tu \Rightarrow s \mid u$ in R

So let $u = sv$, $v \in R$.

Now, $f(sx_1) = uz = (sv)z = s(vz)$. Let $z_0 = vz$.

Summary thus far: We don't have $x_1 \in N$, but $sx_1 \in N$,

and $f : sx_1 \longmapsto sz_0$. (Recall: $f : N \longrightarrow R\langle z \rangle$).

Define $f' : N \oplus R \longrightarrow R\langle z \rangle = C$

$(y, r) \longmapsto f(y) + rz_0$

Define $h : N \oplus R \longrightarrow N + R\langle z \rangle = N_1$

$(y, r) \longmapsto y + rx_1$

$$\begin{tikzcd} & & C = R\langle z \rangle & \\ N \arrow[urr, "f"] \arrow[r, hook, "\iota"] & & N \oplus R \arrow[u, "f'"] \arrow[r, two heads, "h"] & N + R\langle z \rangle = N_1 \arrow[ul, dashed, "f_1"'] \end{tikzcd}$$

$$\begin{tikzcd} f(y) + rz_0 & \\ (y, r) \arrow[u, mapsto, "f'"] \arrow[r, mapsto, "h"] & y + rx_1 \arrow[ul, dashed, "f_1"'] \end{tikzcd}$$

<u>Claim:</u> $\ker h \subseteq \ker f'$.

<u>Pf:</u> Take $(y, r) \in \ker h$.

$\Rightarrow y + rx_1 = 0 \Rightarrow rx_1 = -y \in N$

$\Rightarrow rx_1 \in N$

$\Rightarrow r(x_1 + N) = N \Rightarrow s \mid r$ in R

Since $s \mid r$, say $r = -ws$ for some $w \in R$.

Then $y = -rx_1 = swx_1 \Rightarrow (y, r) = (swx_1, -sw)$.

Thus, $f'(y, r) = f'(swx_1, -sw) = f'(swx_1) - f'(sw)$

$= f'(swx_1) - swz_0$

$= f'(swx_1) - wsz_0 = f(swx_1) - wf(sx_1) = 0$ ✓

Since $\ker h \subseteq \ker f'$, $\exists!\ f_1 : N_1 \longrightarrow C$ s.t. $f'h = f_1$ $\square$

<u>Thm 5.7</u>: If M is a finitely generated torsion R-module, then $M = M_1 \oplus M_2 \oplus \cdots \oplus M_k$, where each M_i is cyclic of order r_i, with $r_i \mid r_{i-1}$, $2 \le i \le k$, and r_1 is the exponent of M.

<u>Pf</u>: By Prop 5.4, $\exists\ x_1 \in M$ with $|x_1| = r_1$. Set $M_1 = R\langle x_1 \rangle$.

By Prop 5.6, $id : M_1 \longrightarrow M_1$ extends to $g_1 : M \longrightarrow M_1$.

Set $N_2 = \ker g_1$.

<u>Outline of proof in diagrams</u> (* we need to verify that this works):

$$\begin{tikzcd} & M_1 = R\langle x_1 \rangle & \\ M_1 = R\langle x_1 \rangle \arrow[ur, "id"] \arrow[rr, hook] & & M \arrow[ul, dashed, "g_1"'] \end{tikzcd} \qquad |x_1| = r_1$$

$$M = M_1 \oplus \ker g_1 = M_1 \oplus N_2 \quad \Rightarrow \quad M = M_1 \oplus N_2$$

$$\begin{tikzcd} & M_2 = R\langle x_2 \rangle & \\ M_2 = R\langle x_2 \rangle \arrow[ur, "id"] \arrow[rr, hook] & & N_2 \arrow[ul, dashed, "g_2"'] \end{tikzcd} \qquad x_2 \in N_2, \quad |x_2| = r_2 \mid r_1$$

$$N_2 = M_2 \oplus \ker g_2 = M_2 \oplus N_3 \quad \Rightarrow \quad M = M_1 \oplus (M_2 \oplus N_3)$$

$$\begin{tikzcd} & N_3 = R\langle x_3 \rangle & \\ M_3 = R\langle x_3 \rangle \arrow[ur, "id"] \arrow[rr, hook] & & N_3 \arrow[ul, dashed, "g_3"'] \end{tikzcd} \qquad x_3 \in N_3, \quad |x_3| = r_3 \mid r_2$$

$$N_3 = M_3 \oplus \ker g_3 = M_3 \oplus N_4 \quad \Rightarrow \quad M = M_1 \oplus M_2 \oplus (M_3 \oplus N_4)$$

$\vdots$

Eventually $N_{k+1} = 1$ (M Noetherian) $\quad \Rightarrow \quad M = M_1 \oplus M_2 \oplus \cdots \oplus M_k$.

<u>Why this works</u>:

Prop 5.6 $\Rightarrow$ $id: M_1 \to M_1$ extends to $g_1 : M \to M_1$. Set $N_2 = \ker g_1$.

$$\begin{tikzcd} & R\langle x_1\rangle & \\ R\langle x_1\rangle \arrow[ur, "id"] \arrow[rr, hook] & & M \arrow[ul, "g_1"'] \end{tikzcd}$$

<u>Claim</u>: $M = M_1 \oplus N_2$.

<u>Pf</u>: Pick $x \in M$. <u>Note</u>: $g_1(x) \in R\langle x_1\rangle$ and g_1 extends $id: R\langle x_1\rangle \to R\langle x_1\rangle$

$\Rightarrow$ $g_1(g_1(x)) = g_1(x)$.

Now, $g_1(x - g_1(x)) = g_1(x) - g_1(x) = 0$

$\Rightarrow$ $x - g_1(x) \in \ker g_1 = N_2$

If $x \in M_1 \cap N_2$ then $x = g_1(x) = 0$ $\Rightarrow$ $M = M_1 \oplus N_2$ (Thm 2.3). ✓

Continuing, if N_2 has exponent r_2; then $(r_1) \subseteq (r_2)$ as ideals, so $r_2 \mid r_1$.

By Prop 5.4, $\exists\, x_2 \in N_2$ with $|x_2| = r_2$. Set $M_2 = R\langle x_2\rangle$.

Continue as above to conclude $N_2 = M_2 \oplus \ker g_2 = M_2 \oplus N_3$.

Repeat this process, $\therefore$ it terminates because M is Noetherian, i.e, at some point $N_{k+1} = 1$ and $M = M_1 \oplus \dots \oplus M_k$. $\square$

<u>Cor</u>: $M \cong R/(r_1) \oplus R/(r_2) \oplus \dots \oplus R/(r_k)$.

<u>Pf</u>: Take R and M_i as above, and consider the map

$$R \longrightarrow R\langle x_i\rangle = M_i$$
$$r \longmapsto r x_i .$$

By construction, the kernel is (r_i), so $M_i \cong R/(r_i)$ by FITM. $\square$

Not surprisingly, this decomposition is "unique"

Thm 5.8: Suppose M is a finitely generated torsion R-module and

$$M = M_1 \oplus \cdots \oplus M_k = N_1 \oplus \cdots \oplus N_m$$

with M_i cyclic of order r_i, N_j cyclic of order s_j, $r_i \mid r_{i-1}$ and $s_j \mid s_{j-1}$, and $r_k, s_m \notin U(R)$. Then $k = m$, and $r_i \sim s_i$ (associates in R) and $M_i \cong N_i$ for each i.

Pf: Assume WLOG that $k \geq m$.

Choose a prime $p \in R$ s.t. $p \mid r_k$ (and hence $p \mid r_i$ $i = 1, \ldots, k$).

Since r_1 & s_1 are exponents of M, $r_1 \sim s_1$ (Recall: an exponent is an LCM of the orders of the elements of M; LCM's are unique up to assoc.)

Thus, $p \mid s_k \Rightarrow p \mid s_1$.

Claim: $p \mid s_i$ for all $i = 1, \ldots, k$.

Suppose not, i.e, that $p \mid s_j$ $j = 1, \ldots, n$ but $p \nmid s_{n+1}$.

Note: R is a PID and p prime $\Rightarrow$ $R/\langle p \rangle = K$ is a field.

Plainly, $\langle r_i, p \rangle = \langle p \rangle$

By Prop 5.5 (i), $M_i[p] \cong R/\langle r_i, p \rangle = R/\langle p \rangle = K$

Also, since $p \nmid n+1$, $N_i[p] \cong R/\langle s_{n+1}, p \rangle = R/(1) = 1$.

Therefore, $M[p] = M_1[p] \oplus \cdots \oplus M_k[p] \cong \bigoplus_{i=1}^{k} K$ (k-dim'l vect space)

Similarly, $M[p] = N_1[p] \oplus \cdots \oplus N_n[p] \oplus \cdots \oplus N_m[p]$

$$= N_1[p] \oplus \cdots \oplus N_n[p] \cong \bigoplus_{j=1}^{n} K \quad \text{(n-dim'l vect space)}$$

Since $M[p] \cong \bigoplus_{i=1}^{k} K \cong \bigoplus_{i=1}^{n} K$, (a k-dim'l & n-dim'l vector space, respectively, $k = n$. Also, $n \le m \le k \Rightarrow m = k$. ✓

Now, suppose that $r_n \not\sim s_n$ for some n (and WLOG, $r_i \sim s_i$ for $i < n$).

Also WLOG, assume that $s_n \nmid r_n$

Put $M' = r_n M$. Then $r_n M_n = r M_{n+1} = \dots = 0$ but $r_n N_n \neq 0$.

Thus, $M' = r_n M_1 \oplus \dots \oplus r_n M_{n-1}$

$= r_n N_1 \oplus \dots \oplus r_n N_{n-1} \oplus r_n N_n$ ↯

We conclude that $r_i \sim s_i$ for all i.

Finally, $M_i \cong R/(r_i) = R/(s_i) \cong N_i$ for each i. □

<u>Def</u>: If $M = M_1 \oplus \dots \oplus M_k$ as above (each M_i cyclic with order r_i), then $r_1, \dots, r_k$ are the <u>invariant factors</u> of M.

<u>Example</u>: $R = \mathbb{Z}$. An finitely generated R-module is an abelian group G.

Take the orders $r_i = n_i$ to be positive integers.

By Thm 5.7, $|G| = n_1 n_2 \cdots n_k \Rightarrow G$ is finite.

Thms 5.7 & 5.8 imply that finite abelian groups are determined up to isomorphism by their invariant factors.

<u>Example 1</u>: $|G| = 100 = 50 \cdot 2 = 20 \cdot 5 = 10 \cdot 10$

$$\Rightarrow G \cong \left.\begin{array}{lcl} \mathbb{Z}_{100}, & \xleftrightarrow{\cong} & \mathbb{Z}_{25} \oplus \mathbb{Z}_4 \\ \mathbb{Z}_{50} \oplus \mathbb{Z}_2, & \longleftrightarrow & (\mathbb{Z}_{25} \oplus \mathbb{Z}_2) \oplus \mathbb{Z}_2 \\ \mathbb{Z}_{20} \oplus \mathbb{Z}_5, & \longleftrightarrow & (\mathbb{Z}_4 \oplus \mathbb{Z}_5) \oplus \mathbb{Z}_5 \\ \text{or } \mathbb{Z}_{10} \oplus \mathbb{Z}_{10} & \longleftrightarrow & (\mathbb{Z}_5 \oplus \mathbb{Z}_2) \oplus (\mathbb{Z}_5 \oplus \mathbb{Z}_2) \end{array}\right\} \begin{array}{c}\text{Classification} \\ \text{as described by} \\ \text{Thm 7.11} \\ \text{(Groups)}\end{array}$$

Example 2: $|G| = 48 = 24\cdot 2 = 12\cdot 4 = 12\cdot 2\cdot 2 = 6\cdot 2\cdot 2\cdot 2$

$$\Rightarrow G \cong \mathbb{Z}_{48} \xleftrightarrow{\cong} \mathbb{Z}_3 \oplus \mathbb{Z}_{16}$$
$$\mathbb{Z}_{24} \oplus \mathbb{Z}_2, \longleftrightarrow \mathbb{Z}_3 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_2$$
$$\mathbb{Z}_{12} \oplus \mathbb{Z}_4, \longleftrightarrow \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_4$$
$$\mathbb{Z}_{12} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2, \longleftrightarrow \mathbb{Z}_3 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$
$$\text{or } \mathbb{Z}_6 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \longleftrightarrow \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

Classification by Thms 4.7 & 4.8	Classification by Thm 7.11 Groups
(by <u>invariant factors</u>)	(by <u>cyclic p_i-subgroups</u>)

Thms 5.3, 5.7, & 5.8 can be combined for a complete description of the structure of finitely generated modules over a PID. (i.e., not necessarily torsion modules).

<u>Thm 5.9</u>: If M is a finitely generated R-module, then $\exists\, m \in \mathbb{Z}_{\geq 0}$ and $r_1, \dots, r_k \in R \setminus U(R)$ with $r_i \mid r_{i-1}$ $(i = 2, \dots, k)$ such that $M = M_1 \oplus \cdots \oplus M_k \oplus F$, where M_i is cyclic of order r_i, and F is free of rank m. Equivalently,

$$M \cong R/(r_1) \oplus \cdots \oplus R/(r_k) \oplus R^m,$$

and this is uniquely determined (up to R-isomorphism) by m & $r_1, \dots, r_m$.

<u>Cor</u>: If G is a finitely generated abelian group, then $\exists\, m \in \mathbb{Z}_{\geq 0}$ and $1 \mid n_1 \mid n_2 \mid \cdots \mid n_k$ such that $G \cong \mathbb{Z}_{n_1} \oplus \cdots \oplus \mathbb{Z}_{n_k} \oplus \mathbb{Z}^m$. G is determined up to isomorphism by the sequence $n_1, \dots, n_k$ of invariant factors, and rank m. The order of the torsion subgroup of G is $n_1 n_2 \cdots n_k$.

Def: A torsion R-module M is <u>primary</u> or <u>p-primary</u>, if its exponent is p^d for some prime $p \in R$.

<u>Prop 5.10</u>: Suppose M is a torsion module with exponent $r \in R$. If $r = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$ for distinct primes $p_i \in R$, then $M = M[p_1^{d_1}] \oplus \cdots \oplus M[p_k^{d_k}]$, a direct sum of primary submodules.

<u>Pf</u>: It suffices to show that if $r = st$, $(s,t) = 1$, then $M = M[s] \oplus M[t]$ (the full result will then follow by induction).

Write $1 = as + bt$ for some $a, b \in R$ (See Prop 3.2 Rings).

For any $x \in M$, $x = t \cdot bx + s \cdot ax \in M[s] + M[t]$.

If $x \in M[s] \cap M[t]$, then $sx = 0$ and $tx = 0$, so $x = asx + btx = 0$. By Thm 2.3, $M = M[s] \oplus M[t]$.

□

<u>Remark</u>: The primary submodules $M[p_i^{d_i}]$ above are unique because $M[p_i^{d_i}]$ consists precisely of the elements of M having order a prime power $p_i^{d_i}$, where $p_i \mid r$ (the exponent).

The Invariant Factor Theorem (5.7) said that a finitely generated torsion R-module M can be decomposed into cyclic R-modules $M = M_1 \oplus \cdots \oplus M_k$ of order $r_i \mid r_{i-1}$. Applying this to each cyclic R-module M_i yields the following theorem:

<u>Thm 5.11</u>: Suppose M is a finitely generated torsion R-module of exponent $r = \prod_{i=1}^{k} p_i^{d_i}$ (p_i's distinct primes, $d_i > 0$). Then

$M = M_1 \oplus \cdots \oplus M_k$, where M_i is p_i-primary, and

$M_i = M_{i1} \oplus \cdots \oplus M_{ik_i}$, where M_{ij} is cyclic of order $p_i^{d_{ij}}$ with

$$1 \le e_{ij} \le e_{i(j-1)} \le e_i \quad \forall i, j.$$

Moreover, M is determined up to isomorphism by the set $\{p_i^{d_{ij}} : 1 \le j \le k_i,\ 1 \le i \le k\}$, called the <u>elementary divisors</u> of M.

<u>Application</u>: Classification of abelian groups of order $72 = 2^3 \cdot 3^2$.

Let $p_1 = 2$, $p_2 = 3$. Then $\sum_j e_{1j} = 3$ and $\sum_j e_{2j} = 2$.

We have 6 possible sets of elementary divisors:

	Elementary divisors	Invariant factors	
$\mathbb{Z}_8 \oplus \mathbb{Z}_9 \longleftrightarrow$	$\{2^3, 3^2\} \longleftrightarrow$	$72 \longleftrightarrow$	$\mathbb{Z}_{72}$
$\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \longleftrightarrow$	$\{2^3, 3, 3\} \longleftrightarrow$	$24 \cdot 3 \longleftrightarrow$	$\mathbb{Z}_{24} \oplus \mathbb{Z}_3$
$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \longleftrightarrow$	$\{2^2, 2, 3^2\} \longleftrightarrow$	$36 \cdot 2 \longleftrightarrow$	$\mathbb{Z}_{36} \oplus \mathbb{Z}_2$
$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \longleftrightarrow$	$\{2^2, 2, 3, 3\} \longleftrightarrow$	$12 \cdot 6 \longleftrightarrow$	$\mathbb{Z}_{12} \oplus \mathbb{Z}_6$
$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \longleftrightarrow$	$\{2, 2, 2, 3^2\} \longleftrightarrow$	$18 \cdot 2 \cdot 2 \longleftrightarrow$	$\mathbb{Z}_{18} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$
$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \longleftrightarrow$	$\{2, 2, 2, 3, 3\} \longleftrightarrow$	$6 \cdot 6 \cdot 2 \longleftrightarrow$	$\mathbb{Z}_6 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_2$