Def A group G is simple if it has exactly two normal subgroups, $\{e\}$ and G. (In particular $G \neq \{e\}$)

We can use Sylow's Theorem to exclude certain orders from the class of simple groups

Ex Show that no group of order 56 is simple.

Sol. $56 = 2^3 \cdot 7$. By Sylow's Theorem

$n_2 \equiv 1 \pmod 2$ and $n_2 \mid 7$

so $n_2 \in \{1, 7\}$

$n_7 \equiv 1 \pmod 7$ and $n_7 \mid 8$

so $n_7 \in \{1, 8\}$.

We claim that either $n_2 = 1$ (which means there is a normal subgroup of order 8) or $n_7 = 1$ ($\Rightarrow \exists$ normal subgroup of order 7).

Suppose $n_2 = 7$ and $n_7 = 8$.

Let $\{P_1, \ldots, P_8\} = Syl_7(G)$

Then $P_i \cap P_j$ $(i \neq j)$ is a proper subgroup of P_i, $|P_i| = 7$ so $P_i \cap P_j = \{e\}$

Therefore $|P_1 \cup P_2 \cup \cdots \cup P_8| = \underset{\substack{\uparrow \\ \text{identity} \\ \text{element}}}{1} + 8 \cdot (\underset{\substack{\uparrow \\ \text{the 6} \\ \text{non-identity} \\ \text{elements} \\ \text{of each } P_i}}{7-1}) = 49$

Let $\{Q_1, \ldots, Q_7\} = Syl_2(G)$.

Then $|Q_1 \cap Q_2| \leq 4$ so

$$|(Q_1 \cup Q_2) - \{e\}| \geq 12 - 1 = 11$$

But that means $|G| \geq 49 + 11 = 60$

contradicting $|G| = 56$.

Finitely generated abelian groups

A group G is a *finitely generated abelian group* if there is a surjective group homomorphism

$$\varphi : \mathbb{Z}^n \to G$$

for some $n \geq 0$.

Example Any product of cyclic groups

$$G = \mathbb{Z}_{a_1} \times \mathbb{Z}_{a_2} \times \cdots \times \mathbb{Z}_{a_m} \times \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{r}$$

is a fin. gen. ab. group:

Define

$$\varphi : \mathbb{Z}^{m+r} \to G$$

by $\varphi(k_1, k_2, \ldots, k_{m+r}) = ([k_1], \ldots, [k_m], k_{m+1}, \ldots, k_{m+r})$

Then φ is a surjective group homomorphism.

Theorem (Fundamental Theorem of Finitely Generated Abelian Groups)
Every finitely generated abelian group is isomorphic to a direct product of cyclic groups:

$$G \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k} \times \mathbb{Z}^r$$

Moreover, the integers n_i can be chosen so that $n_1 | n_2 | \cdots | n_k$ and $n_i > 1$ in which case they are unique.

Proof (sketch) We only prove existence of the n_i and skip the uniqueness. Since G is fin. gen. ab. group, there is a surjective group homomorphism

$$\varphi : \mathbb{Z}^n \longrightarrow G.$$

Let $K = \ker \varphi$. For simplicity we assume K is generated by finitely many columns which we put in a matrix A:

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nm} \end{bmatrix} \in M_{n \times m}(\mathbb{Z})$$

By the First Isomorphism Theorem, we know that

$$G \cong \frac{\mathbb{Z}^n}{K} = \frac{\mathbb{Z}^n}{\mathbb{Z}\begin{bmatrix} a_{11} \\ \vdots \\ a_{n1} \end{bmatrix} + \cdots + \mathbb{Z}\begin{bmatrix} a_{1m} \\ \vdots \\ a_{nm} \end{bmatrix}}$$

By changing basis in $\mathbb{Z}^n$ and changing generators in, the following operations on A lead to an isomorphic quotient:

1) Interchange any two columns/rows
2) Multiply any column/row by -1
3) Add an integer multiple of a column/row to another.

Performing these on A, using the division algorithm we can make the top left entry a_{11} be the gcd of all entries. Then clear out entries to the right and below to get a matrix of the form:

$$A' = \begin{bmatrix} a'_{11} & 0 & \cdots & 0 \\ 0 & a'_{22} & \cdots & a'_{2m} \\ \vdots & \vdots & & \vdots \\ 0 & a'_{n2} & \cdots & a'_{nm} \end{bmatrix}$$

where a'_{11} divides all a'_{ij}. Repeating this we eventually end up with

$$A'' = \begin{bmatrix} n_1 & & & & \\ & n_2 & & & \\ & & \ddots & & \\ & & & n_k & \\ & & & & (0) \end{bmatrix}$$

possibly some cols or rows of zeros at the end.

Then $G \cong \dfrac{\mathbb{Z}^n}{\mathbb{Z}\begin{bmatrix} n_1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} + \cdots + \mathbb{Z}\begin{bmatrix} 0 \\ \vdots \\ n_k \\ (0) \end{bmatrix}} \cong \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \times \mathbb{Z}^r$

where r is the number of zero ~~columns~~ rows in A''. By construction $n_1 | n_2 | \cdots | n_k$. ∎

<u>Def</u> $(n_1, n_2, \ldots, n_k)$ or $(\mathbb{Z}_{n_1}, \mathbb{Z}_{n_2}, \ldots, \mathbb{Z}_{n_k})$ are the <u>invariant factors</u> of G.

Example. Find the invariant factors of $G = \dfrac{\mathbb{Z}^2}{\mathbb{Z}\begin{bmatrix}1\\3\end{bmatrix} + \mathbb{Z}\begin{bmatrix}2\\4\end{bmatrix}}$

Sol $\begin{bmatrix}1 & 2\\ 3 & 4\end{bmatrix} \overset{-2}{\sim} \begin{bmatrix}1 & 0\\ 3 & -2\end{bmatrix} 2-3 \sim \begin{bmatrix}1 & 0\\ 0 & -2\end{bmatrix} (-1) \sim \begin{bmatrix}1 & 0\\ 0 & 2\end{bmatrix}$

So $G \cong \mathbb{Z}_1 \times \mathbb{Z}_2 \cong \boxed{\mathbb{Z}_2}$ $\left(\mathbb{Z}_1 = \dfrac{\mathbb{Z}}{1\mathbb{Z}} = \{e\}\right)$

Example Let $H \leq \mathbb{Z}^4$ be generated by $\begin{bmatrix}8\\0\\0\\0\end{bmatrix}, \begin{bmatrix}0\\6\\10\\-2\end{bmatrix}, \begin{bmatrix}0\\4\\-12\\-20\end{bmatrix}$. Find the invariant factors of $G = \mathbb{Z}^4/H$.

Sol. $\begin{bmatrix}8 & 0 & 0\\ 0 & 6 & 4\\ 0 & 10 & -12\\ 0 & -2 & -20\end{bmatrix}$ We see gcd(all entries) $= 2$ so we try to get that in pos. $(1,1)$.

$\sim \begin{bmatrix}0 & -2 & -20\\ 0 & 6 & 4\\ 0 & 10 & -12\\ 8 & 0 & 0\end{bmatrix} (-1)$

$\sim \begin{bmatrix}2 & 0 & 20\\ 6 & 0 & 4\\ 10 & 0 & -12\\ 0 & 8 & 0\end{bmatrix} 2(-3),\ (-5) \sim \begin{bmatrix}2 & 0 & 20\\ 0 & 0 & -56\\ 0 & 0 & -112\\ 0 & 8 & 0\end{bmatrix} \begin{matrix}\\ \cdot(-1)\\ \cdot(-1)\\ \\ \end{matrix} \overset{(-10)}{\sim} \left[\begin{array}{c|cc}2 & 0 & 0\\ \hline 0 & 0 & 56\\ 0 & 0 & 112\\ 0 & 8 & 0\end{array}\right] 2$

$\gcd(8, 56, 112) = 8$ so we get

$\sim \begin{bmatrix}2 & 0 & 0\\ 0 & 8 & 0\\ 0 & 0 & 56\\ 0 & 0 & 112\end{bmatrix} 2(-2) \sim \begin{bmatrix}2 & 0 & 0\\ 0 & 8 & 0\\ 0 & 0 & 56\\ 0 & 0 & 0\end{bmatrix} \Rightarrow G \cong \underline{\underline{\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_{56} \times \mathbb{Z}}}$

<u>Remark</u> Using that

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn} \Leftrightarrow \gcd(m,n) = 1$$

we can also write

$$G \cong \left(\mathbb{Z}_{p_1^{\alpha_{11}}} \times \cdots \times \mathbb{Z}_{p_1^{\alpha_{1r_1}}}\right) \times \cdots \times \left(\mathbb{Z}_{p_s^{\alpha_{s1}}} \times \cdots \times \mathbb{Z}_{p_s^{\alpha_{sr_s}}}\right) \times \mathbb{Z}^r$$

Where p_i are distinct primes. These numbers (or groups) $p_j^{\alpha_{ji}}$ ($\mathbb{Z}_{p_j^{\alpha_{ji}}}$) are called <u>elementary divisors</u> of G.

<u>Example</u> $\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_{56} \cong$

$$\cong \mathbb{Z}_2 \times \mathbb{Z}_8 \times (\mathbb{Z}_8 \times \mathbb{Z}_7)$$

$$\cong \left(\mathbb{Z}_{2^3} \times \mathbb{Z}_{2^3} \times \mathbb{Z}_{2^1}\right) \times \left(\mathbb{Z}_{7^1}\right)$$

So the elementary divisors are

$$(\mathbb{Z}_{2^3}, \mathbb{Z}_{2^3}, \mathbb{Z}_{2^1}, \mathbb{Z}_{7^1}).$$