Group Theory
Week #7, Lecture #27

Exercise: There are no simple groups of order 300

Solution $|G| = 300 = 2^2 \cdot 3 \cdot 5^2$ $\qquad n_p = |Syl_p(G)|$ $(p = 2, 3, 5)$

By Sylow III : $n_5 \equiv 1 \pmod 5$ & $n_5 \mid 12 \implies n_5 = 1$ or 6

- If $n_5 = 1$, then there is a unique 5-Sylow subgroup, P, which must be normal, and also $|P| = 25 \implies P \neq \{e\}$ or G
  $\therefore$ G is not simple.

- If $n_5 = 6$, then the conjugation action of G on the set
  $$S = \{\text{conjugates of } P\} = \{gPg^{-1} : g \in G\} \qquad (P \text{ a 5-Sylow})$$
  (of size $|S| = 6$, by Sylow II)

  yields a homomorphism
  $$\varphi : G \longrightarrow Sym(S) = S_6$$
  Orbit: $\quad G \cdot P = S \qquad$ (action is transitive)

Claim Action is not faithful, i.e., $\ker(\varphi) \neq \{e\}$

[Indeed, $|G| = 300$ and $|S_6| = 720$
If φ injective, then $\varphi(G) \leq S_6$, and so, by Lagrange,
$300 \mid 720$ — false]

Moreover, $\ker(\varphi) \neq G$ — since action is transitive
($\ker \varphi = G$ means $S^G = S$, which is false)

Hence $K := \ker(\varphi)$ is a proper, non-trivial normal subgroup of G

$\therefore$ G is not simple.

Sylow subgroup & direct products

Prop Let $G = G_1 \times G_2$ be a direct product of two groups. Then every p-Sylow subgroup of G is a direct product of p-sylow subgroups of G_1 and G_2.

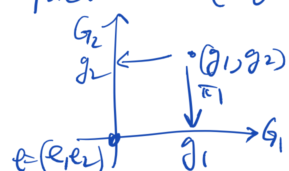
Warning In general, if $H \le G_1 \times G_2$, it is ~~not~~ true that $H = H_1 \times H_2$, for some $H_1 \le G_1$ and $H_2 \le G_2$.

Example $G = \overset{G_1}{\mathbb{Z}_2} \times \overset{G_2}{\mathbb{Z}_2}$ has 3 subgroups of order 2:
$H_1 = \mathbb{Z}_2 \times \{0\} = \langle (1,0) \rangle$, $H_2 = \{0\} \times \mathbb{Z}_2 = \langle (0,1) \rangle$
and $H = \langle (1,1) \rangle$. [Then $H \neq H_1 \times H_2$, for any $H_i \le G_i$
(but H is not 2-sylow. The only 2-sylow subgroup of G is G itself)]

only have:
$H \lneqq H_1 \times H_2 = \mathbb{Z}_2 \times \mathbb{Z}_2$

Proof Let $\boxed{P \in Syl_p(G)}$

- Let $\pi_i : G_1 \times G_2 \twoheadrightarrow G_i$ $\quad \pi_i(g_1, g_2) = g_i \quad (i = 1, 2)$
be the projections onto the two factors (both are homomorphisms).



Then $P_i := \pi_i(P)$ are subgroups of G_i. Done once we prove:

- **Claim**: (i) $P = P_1 \times P_2$
(ii) $P_i \in Syl_p(G_i)$

Pf of claim

(i) $P \le P_1 \times P_2 \le G$

(if $g = (g_1, g_2) \in P$ then $g_i \in P_i$ always the case)

(The product of two subgroups is always a subgroup)

Hence $|P| \le |P_1 \times P_2| = |P_1| \times |P_2|$

But each P_i is also a p-group, since
$o(g_1, g_2) = \mathrm{lcm}(o(g_1), o(g_2))$

so, $g_1, g_2 \in P \Rightarrow o(g_i) = p^{k_i} \Rightarrow o(g_1, g_2) = p^k$ $\left(k = \max(k_1, k_2)\right)$

$\therefore$ $P_1 \times P_2$ is a p-group

$\xrightarrow[P \text{ is } p\text{-Sylow}]{}$ $P = P_1 \times P_2$

(ii) Suppose one of the P_i's, say P_1, is not p-Sylow (in G_1)
But we just saw that P_1 is a p-group, so,

$$\exists Q_1 \in Syl_p(G_1) \quad \text{s.t.} \quad P_1 \lneqq Q_1 \le G_1$$

(by Sylow I)

$\therefore$

$$P = P_1 \times P_2 \lneqq \underbrace{Q_1 \times P_2}_{\text{a } p\text{-group}} \le G_1 \times G_2 = G$$

— contradicts P is p-Sylow!

$\therefore$ P_1 & P_2 are p-Sylow

$\boxed{\text{QED}}$

Theorem Let G be a finite group. If all the Sylow subgroups of G are normal, then G is the direct product of its Sylow subgroups.

$$\boxed{\left(P \trianglelefteq G, \ \forall P \in Syl(G)\right) \Rightarrow \left(G = \prod_{P \in Syl(G)} P\right)}$$

where $Syl(G) = \bigcup_{p \mid |G|} Syl_p(G)$

note The hypothesis of the theorem is equivalent to

$$\boxed{n_p = 1 \quad , \forall p \mid |G|} \qquad \text{(by Sylow III)}$$

That is, if $|G| = p_1^{k_1} \cdots p_n^{k_n}$, and $\boxed{n_{p_i} = 1}$, $\forall i$
then $G = P_1 \times \cdots \times P_n$, where P_i is the p_i-Sylow of G

Proof First treat the case $n=2$, i.e. $|G| = p_1^{k_1} \cdot p_2^{k_2}$ $(p_1 \ne p_2)$
and $n_{p_1} = n_{p_2} = 1$. Let P_1 & P_2 be the corresponding

Sylow subgroups. $(|P_i| = p_i^{k_i})$. Then:

(i) $P_1 \cap P_2 = \{e\}$

(*) [Since $g \in P_1 \cap P_2 \xRightarrow{\text{Lagrange}} o(g) = p_1^{\ell_1} = p_2^{\ell_2} \Rightarrow \ell_1 = \ell_2 = 0 \Rightarrow g = \{e\}$]

(ii) $P_1 \cdot P_2 = G$ ← Since $|P_1 \cdot P_2| \underset{\text{General formula}}{=} \dfrac{|P_1| \cdot |P_2|}{|P_1 \cap P_2|} \underset{\text{by (i)}}{=} |P_1| \cdot |P_2| \underset{\text{by assumption}}{=} |G|$

(iii) $\forall g_i \in P_i \Rightarrow g_1 g_2 = g_2 g_1$

$$\left[g_1 g_2 g_1^{-1} g_2^{-1} = \underbrace{(g_1 g_2 g_1^{-1})}_{\text{in } P_2,\ \text{since } P_2 \trianglelefteq G} \cdot g_2^{-1} = g_1 \underbrace{(g_2 g_1^{-1} g_2^{-1})}_{\text{in } P_1,\ \text{since } P_1 \trianglelefteq G} \in P_2 \cap P_1 \underset{\text{by (i)}}{=} \{e\} \right]$$

Hence, by the Decomposition Theorem:

$$\boxed{G = P_1 \times P_2}$$

The general case follows exactly the same way.

$\boxed{\text{QED}}$

Rem The argument in (*) shows:

[If $H_1, H_2 \leq G$, and $\gcd(|H_1|, |H_2|) = 1$, then $H_1 \cap H_2 = \{e\}$]

(follows at once from Lagrange)

Finite Abelian Groups

- We shall write Abelian groups additively: $(G, +, 0)$
- Products of subgroups are also written additively

$$G = H \cdot K \xrightarrow[G \text{ Abelian}]{} G = H + K \qquad \left(\begin{array}{c}\text{i.e. } g = h + k \\ \forall g,\ \text{where} \\ h \in H,\ k \in K\end{array}\right)$$

- Direct products are written as <u>direct sums</u>

$$G = G_1 \times G_2 \xrightarrow[G \text{ Abelian}]{} G = G_1 \oplus G_2 \qquad \left(\begin{array}{c}\text{i.e. } g = g_1 + g_2 \\ \text{uniquely}\end{array}\right)$$

- All subgroups are normal.

Hence, by the above Theorem:

$$\boxed{G \cong G_1 \oplus \cdots \oplus G_n} \qquad (*)$$

where G_i are (abelian) maximal p-subgroups, for $p \mid |G|$

- This reduces the classification of finite Abelian groups to that of finite Abelian p-groups, such as $\mathbb{Z}_p, \mathbb{Z}_{p^2}, \ldots, \mathbb{Z}_p \oplus \mathbb{Z}_p, \mathbb{Z}_{p^2} \oplus \mathbb{Z}_p, \ldots$ max. cyclic

Key technical tool:

Lemma Let G be a finite abelian p-group. If $\langle a \rangle$ is a cyclic subgroup of maximal order (i.e. $\langle a \rangle \leq \langle b \rangle \Rightarrow \langle a \rangle = \langle b \rangle$)

Then $\exists\, H \leq G$ such that

$$\boxed{G = \underbrace{\langle a \rangle}_{\text{maximal cyclic}} \oplus \underbrace{H}_{\text{"complement"}}}$$

Theorem (Fundamental Theorem of Finite Abelian Groups)

Every finite Abelian group G is isomorphic to a direct sum of cyclic groups of prime power order:

$$\boxed{G \cong \mathbb{Z}_{p_1^{k_1}} \oplus \cdots \oplus \mathbb{Z}_{p_r^{k_r}}} \qquad \left(\begin{matrix} p_i \text{ prime} \\ k_i \geq 1 \end{matrix}\right)$$

Moreover, any two such decompositions only differ by a permutation of the factors.

Proof. Existence follows from $(*)$ + Lemma.

- Uniqueness is proved by induction on $|G|$ by looking at $p \cdot G$ and using $p \cdot \mathbb{Z}_{p^k} \cong \mathbb{Z}_{p^{k-1}}$

QED

<u>Example</u> Abelian groups of order $60 = 2^2 \cdot 3 \cdot 5$

- Abelian groups of order 4 : $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_4$
- " 3 : $\mathbb{Z}_3$
- " 5 : $\mathbb{Z}_5$

Answer:
- $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{30} \oplus \mathbb{Z}_2$
- $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \cong \mathbb{Z}_{60}$

In general, using the isomorphism

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

We can rewrite these finite Abelian groups as

$$\boxed{G = \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \cdots \oplus \mathbb{Z}_{n_k}}$$

with $n_1 \geq \cdots \geq n_k$ and $\boxed{n_i \mid n_{i-1} \text{ for } i = 2, \ldots, k.}$

<u>Example</u> $|G| = 24 = 2^3 \cdot 3$

$\mathbb{Z}_8 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{24}$ — 1 gen

$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12} \oplus \mathbb{Z}_2$ — 2 gen

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_6 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ — 3 gen