Application:

Prop. Let F be a field and $F^\times = F \setminus \{0\}$.

Let $G \subseteq F^\times$ a finite subgp. Then G is cyclic

In particular, $F^\times$ is cyclic if F is a finite field.

Pf. $G \cong \mathbb{Z}_{p_1^{s_1}} \times \cdots \times \mathbb{Z}_{p_r^{s_r}}$.

Let $m = \operatorname{lcm}(p_1^{s_1}, \cdots, p_r^{s_r})$. Then $g^m = 1 \ \forall g \in G$.

In other words, all the elt of G are the roots of

$$x^m - 1 \text{ over } F.$$

But $x^m - 1$ has at most m roots in a field.

So $|G| \leq m$. Thus $|G| = m$ and G is cyclic $\square$.

Computation of quotient groups.

Observation: If G is abelian, then G/N is abelian
cyclic cyclic.

Example. $G = \mathbb{Z}_2 \times \mathbb{Z}_4$. $N \cong \mathbb{Z}_2$.

Case 1: $N = \mathbb{Z}_2 \times \{0\} \subseteq G$. Then $G/N \cong \mathbb{Z}_4$

Case 2: $N = \langle (1,2) \rangle \subseteq G$. Then $G/N = \langle \overline{(1,1)} \rangle \cong \mathbb{Z}_4$.

Case 3. $N = \langle (0,2) \rangle \subseteq G$. Then $G/N \cong \mathbb{Z}_2 \times \mathbb{Z}_2$

So the quotient G/N depends not only on the isom class of N, but also on how N sits inside G.

Example. Let $G = \mathbb{Z}_4 \times \mathbb{Z}_6$, $N = \langle (2,3) \rangle \leq G$.

Compute the quotient G/N.

First, the order. $|G/N| = |G|/|N| = 24/2 = 12$.

By classification thm, 2 abelian gps: $\mathbb{Z}_2 \times \mathbb{Z}_6$ and $\mathbb{Z}_{12}$

The difference between these 2 gps is that the first gp does not have an elt of order 4.

Note that $(1,0)+N$ has order 4 in G/N.

So $G/N \cong \mathbb{Z}_{12}$.

In fact, $(1,1)+N$ is a generator.

Next topic: to measure how a gp is different from "abelian".

Def. The center of G

$$Z(G) = \{g \in G \mid gx = xg \quad \forall x \in G\}$$

Prop. $Z(G) \trianglelefteq G$.

Pf. ① check $Z(G)$ is a subgp.

$1_G \in Z(G)$. So nonempty.

If $g_1, g_2 \in Z(G)$, then $x(g_1 g_2) = (x g_1) g_2 = (g_1 x) g_2$

$$= g_1(x g_2) = g_1(g_2 x) = (g_1 g_2) x.$$

Also $g_1 x = x g_1$. So $g_1^{-1} x = x g_1^{-1}$.

So $Z(G)$ subgp.

② Normality. Let $a \in G$, $g \in Z(G)$, then

$$a g a^{-1} = g a a^{-1} = g.$$

So normal. $\square$

Rmk. G is abelian iff $Z(G) = G$.

Example: $Z(S_n) = \{1\}$. if $n \geq 3$.

Def. $[G,G]$ is the subgp of G generated by $aba^{-1}b^{-1}$ for $a, b \in G$.

Prop. (1) $[G,G] \lhd G$.

(2) For a normal subgp $N \lhd G$, G/N is abelian iff $[G,G] \subseteq N$.

Rmk. $G/[G,G]$ is called the abelianization of G.

Lem. Let $S \subset G$ be a subset and H_S be the subgp gen by S.

If $gSg^{-1} = S$ $\forall g \in G$, then $H_S \lhd G$.

Pf. $H_S = \{a_1^{\pm 1} \cdots a_k^{\pm 1} \mid a_i \in S\}$.

So $g(a_1^{\pm 1} \cdots a_k^{\pm 1}) g^{-1} = (g a_1 g^{-1})^{\pm 1} \cdots (g a_k g^{-1})^{\pm 1}$

So $g H_S g^{-1} \subset H_S$ and $H_S \lhd G$ $\square$

Pf of Prop. (1). Let $S = \{aba^{-1}b^{-1} \mid a, b \in G\}$. Then

$$g(aba^{-1}b^{-1})g^{-1} = a'b'a'^{-1}b'^{-1}, \text{ where } a' = gag^{-1}, \quad b' = gbg^{-1}.$$

So by Lem, $[G, G] = H_S \trianglelefteq G$.

(2) G/N is abelian $\Leftrightarrow abN = aNbN = bNaN = baN \quad \forall a, b \in G$

$\Leftrightarrow a^{-1}b^{-1}ab \in N \quad \forall a, b \in G$

$\Leftrightarrow aba^{-1}b^{-1} \in N \quad \forall a, b \in G$

$\Leftrightarrow [G, G] \subseteq N$.

Example. Let $G = S_3$, then $[G, G] = A_3$.

Note that $A_3 = \langle (123) \rangle$.

$$(12)(13)(12)^{-1}(13)^{-1} = (12)(13)(12)(13) = (12)(23) = (123)$$

So $A_3 \subseteq [G, G]$.

On the other hand, $A_3 \trianglelefteq G$ and $G/A_3 \cong \mathbb{Z}_2$ abelian

So $[G, G] \subseteq A_3$. Thus $[G, G] = A_3$

Let H, N be subgp of G. Then

$$HN := \{hn \mid h \in H, n \in N\}$$

In general, HN is not a subgp of G.

Prop. (1) If $N \triangleleft G$, then HN is a subgp of G

(2) If $H, N \triangleleft G$, then $HN \triangleleft G$.

Pf. (1) $HN \ni \{1\}$. So nonempty.

For $h_1, h_2 \in H$, $n_1, n_2 \in N$,

$(h_1 n_1)(h_2 n_2) = (h_1 h_2)(h_2^{-1} n_1 h_2 n_2) \in HN$.

$(h_1 n_1)^{-1} = n_1^{-1} h_1^{-1} = h_1^{-1}(h_1 n_1^{-1} h_1^{-1}) \in HN$.

So HN is a subgp

(2) Let $g \in G$. $gHNg^{-1} = (gHg^{-1})(gNg^{-1}) = HN$.

So $HN \triangleleft G$. □

2^{nd} isom thm. For $H < G$ and $N \triangleleft G$, $HN/N \cong H/H \cap N$.

Pf. Consider $\varphi: H \to HN/N$, $h \mapsto hN$

This is a gp hom. surj.

$\ker \varphi = H \cap N$. So by 1^{st} iso thm, $H/H\cap N \cong HN/N$.

3^{rd} Isom thm. Let $H, K \triangleleft G$ with $H \subseteq K$. Then

$(G/H)/(K/H) \cong G/K$.

Pf. Consider $G/H \to G/K$, $gH \mapsto gK$.

This is well-defined, surj. gp hom.

Moreover $\ker = K/H$. So by 1st isom thm
$$(G/H)/(K/H) \cong G/K$$
□