4. Universal properties, commutators, and solvable groups

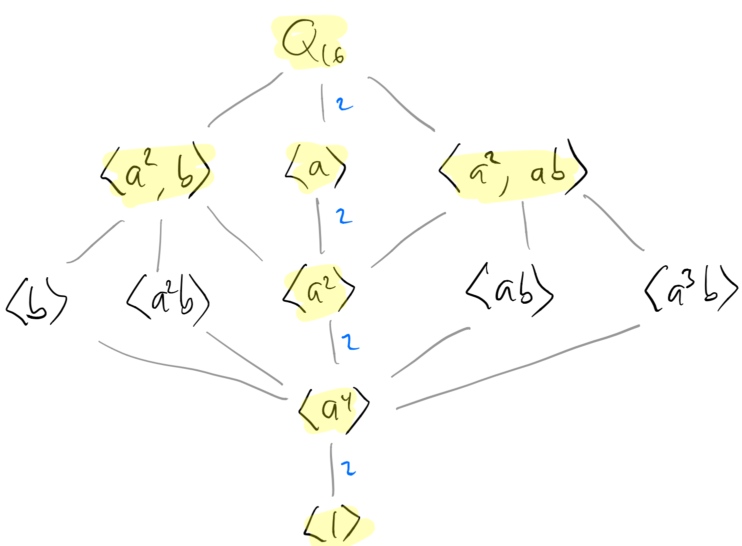
Recall the FHT: $\phi(G) \cong G/\ker\phi$, i.e.,

★ Every homomorphic image of G is isomorphic to some quotient of G.

Examples:

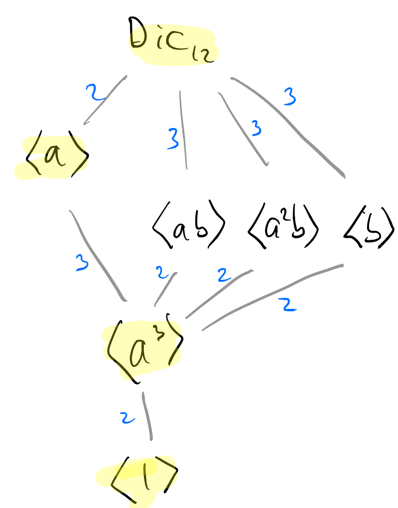
- Generalized quaternion group

$$Q_{16} = \langle a, b, c \mid a^4 = b^2 = c^2 = abc \rangle$$



- Dicyclic group

$$Dic_{12} = \langle a, b, c \mid a^3 = b^2 = c^2 = abc \rangle$$



Note: $Q_{16}/\langle a\rangle \cong \mathbb{Z}_2$

$Q_{16}/\langle a^2\rangle \cong V_4$

$Q_{16}/\langle a^4\rangle \cong D_4$

$Dic_{12}/\langle a\rangle \cong \mathbb{Z}_2$

$Dic_{12}/\langle a^3\rangle \cong D_3$

Question: Which normal subgroups $N \trianglelefteq G$ yield an abelian quotient, G/N?

Clearly, if G is abelian, then $\phi(G)$ is abelian.

If G is non-abelian, then $\phi(G)$ is abelian "if $\ker\phi$ is large enough."

<u>Goal</u>: Show that there is some maximal homomorphic image w.r.t. $\phi(G)$ being abelian.

This will be an example of a <u>universal property</u>.

<u>Def</u>: Let $\varepsilon : G \twoheadrightarrow U$ be a homom. to an abelian group U. Then (U, ε) is a <u>universal pair</u> (w.r.t. abelian epimorphic images) if for any other epimorphism $f : G \twoheadrightarrow A$ to an abelian group A, $\exists!\ g : U \to A$ s.t. $f = g\varepsilon$.

In this case, we say that f <u>factors through</u> U.

$$\begin{tikzcd} G \arrow[rr] \arrow[dr, two heads, "\varepsilon"'] & & A \\ & U \arrow[ur, dashed] & \end{tikzcd}$$

<u>Note</u>: This is an example. We can define universal pairs w.r.t. other properties.

<u>Big question</u>: Does such a universal pair exist?

Non-example: replace "abelian epimorphic images" with "nontrivial epimorphic images."

Prop 4.1: If a group G has a universal pair (U, ε) w.r.t. some property P, then U is unique (up to isomorphism.

Pf: Suppose (U, ε) and (U', ε') are universal pairs.

We have:
$$\begin{tikzcd} G \arrow[r, "\varepsilon'"] \arrow[dr, "\varepsilon"'] & U' \\ & U \arrow[u, dashed, "g_1"'] \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} G \arrow[r, "\varepsilon"] \arrow[dr, "\varepsilon'"'] & U \\ & U' \arrow[u, dashed, "g_2"'] \end{tikzcd}$$

We can "stack" the diagrams:

$$\begin{tikzcd} G \arrow[r, "\varepsilon"] \arrow[dr, "\varepsilon"'] & U \\ & U \arrow[u, dashed, "g_2 g_1"'] \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} G \arrow[r, "\varepsilon"] \arrow[dr, "\varepsilon"'] & U \\ & U \arrow[u, dashed, "1_U"'] \end{tikzcd}$$

By uniqueness, $g_2 g_1 = 1_U$.

An analogous argument gives $g_1 g_2 = 1_{U'}$.

Thus g_1 and g_2 are inverse isomorphisms. $\square$

$\boxed{4}$

<u>Question</u>: Let X, Y, Z be <u>sets</u>, and $f: X \twoheadrightarrow Y$, $\pi: X \twoheadrightarrow Z$. When does there exist a unique $g: Z \to Y$ s.t. $f = gh$?

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "\pi"'] & & Y \\ & Z \arrow[ur, dashed, "g"'] & \end{tikzcd}$$

<u>Ans</u>: We're forced to define

$$g(z) = f(\pi^{-1}(z))$$

This is well-defined iff $\pi(x_1) = \pi(x_2) \implies f(x_1) = f(x_2)$.

"f collapses X at least as much as π does."

Now, consider the above situation but with groups. (so the maps are homomorphisms).

$$\pi(x_1) = \pi(x_2) \implies x_1 x_2^{-1} \in \ker \pi$$

$$f(x_1) = f(x_2) \implies x_1 x_2^{-1} \in \ker f.$$

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\pi"'] & & H \\ & G/K \arrow[ur, dashed, "g"'] & \end{tikzcd}$$

Thus, $g: G/K \to H$ is well-defined iff

This is the universal property of quotient groups.

Formally: Let $\pi : G \twoheadrightarrow G/K$ be the natural map.

Then $(G/K, \pi)$ is universal (w.r.t. epimorphic images whose kernels contain K) because for any other $f : G \to H$ whose kernel contains K, $\exists!\ g : G/K \to H$ s.t. $f = g\pi$.

"f factors through G/K iff $K \subseteq \ker f$."

Back to abelian quotients...

Def: The commutator of $x, y \in G$ is $[x,y] := x^{-1}y^{-1}xy$.

Note: $[x,y] = 1 \iff xy = yx$.

Let $f : G \to A$ be a homom. to abelian group.

$$f([x,y]) = f(x)^{-1} f(y)^{-1} f(x) f(y) = 1 \implies [x,y] \in \ker f.$$

Thus, if (U, ε) is a universal pair for G, then $[x,y] \in \ker \varepsilon$.

Def: The derived group (or commutator subgroup) of G is the group $G' = \langle [x,y] : x, y \in G \rangle$.

Exercise: $G' \trianglelefteq G$, because $[x,y]^{-1} = [y,x]$

$$z[x,y]z^{-1} = [zxz^{-1}, zyz^{-1}].$$

<u>Note</u>: If $x, y \in G$, then $x^{-1}y^{-1}xyG' = G' \iff xyG' = yxG'$, so G/G' is abelian.

<u>Thm 4.2</u>: $(G/G', \varepsilon)$ is a universal pair (w.r.t. abelian quotients), where $\varepsilon : G \longrightarrow G/G'$ is the canonical quotient.

<u>Pf</u>: Define $g(xG') = f(x)$

$$\begin{tikzcd} G \arrow[rr, "f"] \arrow[dr, "\varepsilon"'] & & A \\ & G/G' \arrow[ur, dashed, "g"'] & \end{tikzcd} \qquad \begin{tikzcd} x \arrow[rr, mapsto, "f"] \arrow[dr, mapsto, "\varepsilon"'] & & f(x) \\ & xG' \arrow[ur, dashed, mapsto, "g"'] & \end{tikzcd}$$

- <u>well-defined</u>: Suppose $xG' = yG'$. Then $y^{-1}x \in G'$. Since ker f contains all commutators, $f(y^{-1}x) = 1$ $\Rightarrow f(x) = f(y)$ ✓
- <u>Homom</u>: $g(xG'yG') = g(xyG') = f(xy) = f(x)f(y) = g(xG')\,g(yG')$. ✓
- <u>Surjective</u>: ✓
- <u>Uniqueness</u>:

$$\begin{tikzcd} G \arrow[rr, two heads] \arrow[dr] & & A \\ & G/G' \arrow[ur, shift left, "g_1"] \arrow[ur, shift right, "g_2"'] & \end{tikzcd}$$

If $g_1 \varepsilon = f$ and $g_2 \varepsilon = f$, then

$$\underbrace{g_1 \varepsilon = g_2 \varepsilon \Rightarrow g_1 = g_2}_{\text{because } \varepsilon \text{ is surjective}} \qquad \square$$

(more on this later...)

Lemma: (HW) (i) If $G' \leq H \leq G$, then $H \lhd G$
(ii) If $K \lhd G$, then $K' \lhd G$
(iii) If $f: G \twoheadrightarrow H$ and $\ker f = K$, then
H is abelian iff $G' \leq K$.
In particular, G/K is abelian iff $G' \leq K$.

Big idea:

- G/G' is a "maximal" abelian epimorphic image of G.

i.e.,
- G' is a "minimal" normal subgroup N s.t. G/N is abelian.

Since $G' \lhd G$, we have $G'' := (G')' \lhd G$ (See Lemma (ii))

Define $G^{(0)} = G$, $G^{(1)} = G'$, $G^{(2)} = G''$, ..., $G^{(k+1)} = (G^{(k)})'$.

Then $G^{(k)} \lhd G$ $\forall k$.

Def: The derived series (or "commutator series") of G is the sequence $G = G^{(0)} \geqslant G^{(1)} \geqslant G^{(2)} \geqslant \cdots \geqslant G^{(k)} \geqslant \cdots$

A group is called solvable if some $G^{(k)} = 1$.

Examples:

(1) If G is abelian, the $G' = 1$, so G is solvable.

(2) If $G = S_3$, then $G' = A_3$, $G'' = A_3' = 1$, so S_3 is solvable.

(3) If $G = A_n$ ($n \geq 5$), then A_n is non-abelian and simple.

Since $A_n' \trianglelefteq A_n$, $A_n' = 1$ or A_n.

But A_n/A_n' abelian $\Rightarrow A_n' = A_n \Rightarrow A_n$ is not solvable.

<u>Def</u>: A <u>subnormal series</u> for a group G is a sequence $G = G_0 \geq G_1 \geq G_2 \geq \cdots$ where $G_{i+1} \trianglelefteq G_i$ $\forall i$.

The G_i's are called <u>subnormal</u> subgroups of G, and the groups G_i/G_{i+1} are called the factors of the series.

The <u>length</u> is the number of nontrivial factors.

<u>Note</u>: Subnormal subgroups need not be normal in G.

<u>Ex</u>: $D_4 = \langle r, f \rangle \geq \langle r^2, f \rangle \geq \langle f \rangle \geq 1$

but $\langle f \rangle \ntrianglelefteq D_4$.

<u>Def</u>: A subnormal series is <u>normal</u> if $G_i \trianglelefteq G$.

<u>Thm 4.3</u>: A group is solvable iff it has a subnormal series $G = G_0 \geq G_1 \geq \cdots \geq G_m = 1$ with abelian factors.

<u>Pf</u>: ($\Rightarrow$) ✓

($\Leftarrow$) Suppose each G_i/G_{i+1} is abelian.

Since $G_0/G_1 = G/G_1$ is abelian, $G' \leq G_1$.

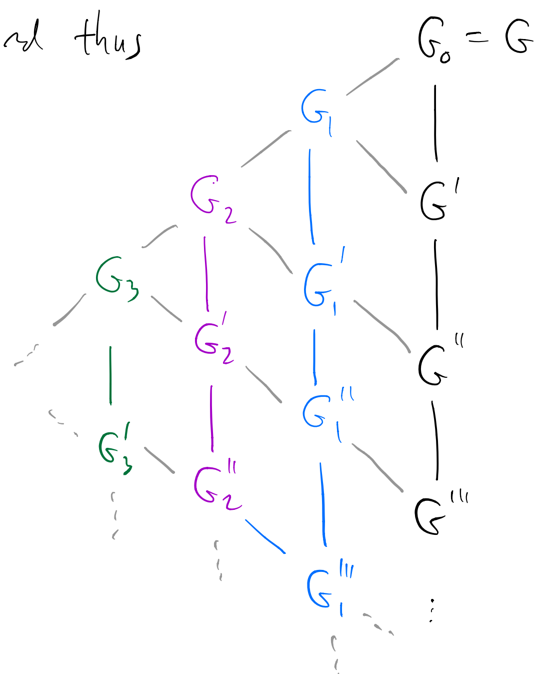
Similarly, G_1/G_2 is abelian, and thus

$$G_2 \geq G_1' \geq (G')' = G^{(2)}.$$

By induction, $G^{(k)} \leq G_k$ $\forall k$,

thus $G^{(m)} = 1$

$\Rightarrow$ G is solvable. $\square$



<u>Thm 4.4</u>: Suppose $K \trianglelefteq G$. Then G is solvable iff K and G/K are solvable.

<u>Pf</u>: ($\Rightarrow$) We've seen that subgroups of solvable groups are solvable.

Let $\eta : G \to G/K$ be the canonical quotient.

Then η maps commutators to commutators, and conversely:

$$\eta([x,y]) = \eta(x^{-1}y^{-1}xy) = x^{-1}y^{-1}xyK = [xK, yK].$$

So $(G/K)' = \eta(G')$, and $(G/K)^{(k)} = \eta(G^{(k)})$. ✓

($\Leftarrow$) Choose a subnormal series with abelian factors for K and for G/K:

$$K = K_0 \geq K_1 \geq \cdots \geq K_m = 1$$

$$G/K = G_0/K \geq G_1/K \geq \cdots \geq G_k/K = K/K$$

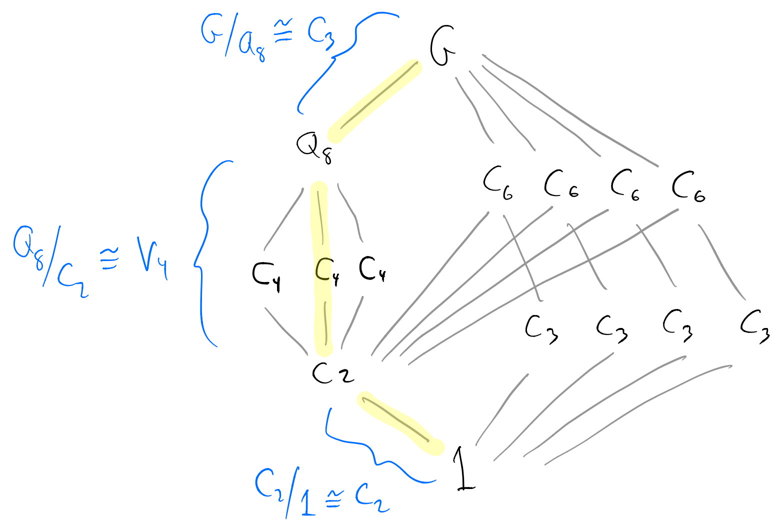
3rd Isom. thm $\Rightarrow$ $G_i/G_{i+1} \cong (G_i/K)/(G_{i+1}/K)$, and so

$\boxed{10}$

$G = G_0 \geq \cdots \geq G_k = K = K_0 \geq K_1 \geq \cdots \geq K_m = 1$ is a subnormal series with abelian factors $\Rightarrow$ G is solvable. $\square$

Example: Let $G = SL(2,3) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a,b,c,d \in \mathbb{Z}_3,\ ad-bc=1 \right\}$.

Smallest solvable group ($|G|=24$) requiring a 3-step chain.



Def: A subnormal series $G = G_0 \geq G_1 \geq \cdots \geq G_m = 1$ is a composition series for G if each G_{i+1} is a maximal proper normal subgroup of G_i.

Equivalently, each factor G_i/G_{i+1} is a nontrivial simple group.

Example: $S_n \geq A_n \geq 1$ is a composition series (if $n \geq 5$).

If $|G| < \infty$, then any subnormal series can be "refined" to a composition series by inserting subgroups.

Thm 4.5 (Jordan-Hölder). If $|G| < \infty$, and

$G = G_0 \geq G_1 \geq \cdots \geq G_m = 1$ and

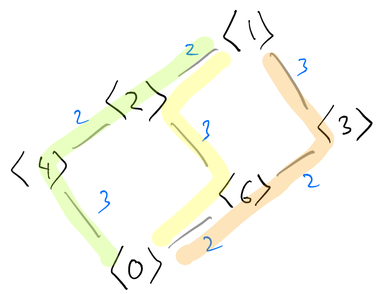
$G = H_0 \geq H_1 \geq \cdots \geq H_k = 1$

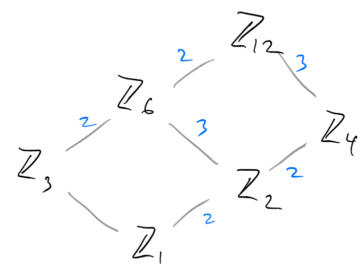
are composition series, then $m=k$, and there is a 1-1 correspondence b/w the sets of factors s.t. the corresponding factors are isomorphic.

<u>Example</u>: $G = \mathbb{Z}_{12}$

Factors are

$\mathbb{Z}_2, \mathbb{Z}_2, \mathbb{Z}_3$.





<u>Pf</u>: Induction on m.

<u>Base case</u>: $m=1 \Rightarrow G$ is simple.

Assume it's true for groups having comp. series of length $m-1$.

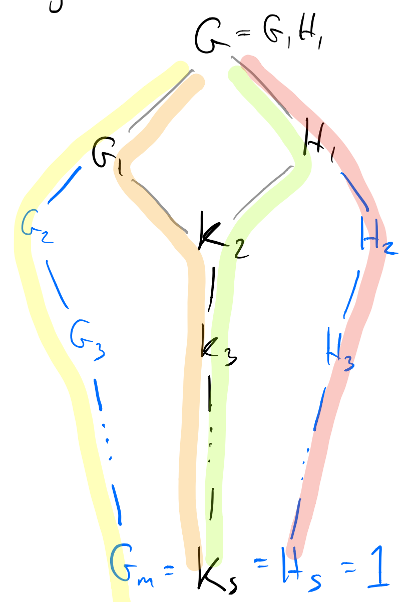
If $G_1 = H_1$, then the thm holds by IHOP.

If $G_1 \neq H_1$, set $K_2 = G_1 \cap H_1$.

Since G_1, H_1 are maximal, $G = G_1 H_1$.

2^{nd} Isom thm $\Rightarrow G/G_1 \cong H_1/K_2$

$$G/H_1 \cong G_1/K_2$$



Consider the following 4 comp. series: $S_1, \dots, S_4$:

S_2 & S_3 have isomorphic factors (2^{nd} isom. thm)

S_1 & S_2 " " " (IHOP)

S_3 & S_4 " " " (IHOP)

$\square$

By Jordan-Hölder, each finite group can be associated with a finite collection of simple groups (composition factors).

<u>Def</u>: A group A is an <u>extension</u> of B by C if $B \triangleleft A$ and $A/B \cong C$.

By understanding the classification of finite simple groups, we can better understand the structure of finite groups.

Just for fun...

<u>Theorem</u>: Let $|G| < \infty$.

(1) (Burnside). If $|G| = p^a q^b$, primes $p, q \Rightarrow G$ is solvable

(2) (P. Hall). If for all $p \mid |G|$: $|G| = p^n m$, $(p \nmid m)$ and $\exists$ subgroup $H \leq G$ of order M, then G is solvable.

(3) (Feit-Thompson). If $|G|$ is odd, G is solvable. (255 page proof)

(4) (Thompson) If $\langle x, y \rangle$ is solvable for all $x, y \in G$, then G is solvable (475 page proof, depends on Feit-Thompson).