5. Universal properties, solvable groups and (sub)-normal series

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

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

Consider the abelian homom. images of G.

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"

We'll 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>: A pair (U, ε) is <u>universal</u> for a group G (w.r.t. abelian epimorphic images) if U is an abelian group, $\varepsilon : G \twoheadrightarrow U$ an epimorphism, s.t. for <u>any</u> other abelian group A with homom. $f : G \to A$, $\exists!$ homom. $g : U \to A$ s.t. $f = g\varepsilon$.

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

In this case, we say that f can be <u>factored through</u> U.

<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?

<u>Prop 5.1</u>: If a group G has a universal pair $(\mathcal{U}, \varepsilon)$ wrt some property P, then $\mathcal{U}$ is unique (up to isomorphism).

<u>Pf</u>: Suppose $(\mathcal{U}, \varepsilon)$ and $(\mathcal{U}_1, \varepsilon_1)$ are universal pairs,

we have

$$\begin{tikzcd} G \arrow[r, "\varepsilon_1"] \arrow[d, "\varepsilon"'] & \mathcal{U}_1 \\ \mathcal{U} \arrow[ur, dashed, "g_1"'] & \end{tikzcd} \quad \text{and} \quad \begin{tikzcd} G \arrow[r, "\varepsilon"] \arrow[d, "\varepsilon_1"'] & \mathcal{U} \\ \mathcal{U}_1 \arrow[ur, dashed, "g_2"'] & \end{tikzcd}$$

We can "stack" these diagrams:

$$\begin{tikzcd} G \arrow[r, "\varepsilon"] \arrow[d, "\varepsilon"'] & \mathcal{U} \\ \mathcal{U} \arrow[ur, dashed, "g_2 g_1"'] & \end{tikzcd} \quad \text{but also} \quad \begin{tikzcd} G \arrow[r, "\varepsilon"] \arrow[d, "\varepsilon"'] & \mathcal{U} \\ \mathcal{U} \arrow[ur, dashed, "1_{\mathcal{U}}"'] & \end{tikzcd}$$

By uniqueness, $g_2 g_1 = 1_{\mathcal{U}}$

An analogous argument gives $g_1 g_2 = 1_{\mathcal{U}_1}$

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

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

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

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

$$g(z) = f(h^{-1}(z)).$$

This is well-defined iff $h(x_1) = h(x_2) \Longrightarrow f(x_1) = f(x_2)$

<u>Think:</u> "f collapses X at least as much as h does."

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

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

$h(x_1) = h(x_2) \Rightarrow x_1 x_2^{-1} \in \ker h$

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

Thus, $g: L \to G/K$ is well-defined iff $\boxed{\ker h \leq \ker f = K}$

This is the universal property of quotient groups.

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

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

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

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

* 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: For $x, y, z \in G$, $[x,y]^{-1} = [y, x]$

$$[x, y]^z = [x^z, y^z].$$

Thus $G' \trianglelefteq G$.

Note: If $x, y \in G$, then $x^{-1}y^{-1}xyG' = G' \iff xyG' = yxG'$

Thus G/G' is abelian.

Thm 5.2 If G is a group, then G has a universal pair (w.r.t. abelian homom. images) (U, ε). In fact, we may take $U = G/G'$ and $\varepsilon: G \to U$ to be the canonical quotient map.

Pf: Define $g(xG') = f(x)$.

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

Well-defined: $\ker \varepsilon = G' \leq \ker f$ ✓

(explicitly, $xG' = yG' \iff y^{-1}xG' = G' \iff y^{-1}xG' \iff f(y^{-1}x) \iff f(x) = f(y)$

$\iff g(xG') = g(yG')$. ✓

Homomorphism: $g(xG')g(yG') = f(x)f(y) = f(xy) = g(xyG') = g(xG'yG')$ ✓

Clearly surjective ✓

Uniqueness:

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

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

$g_1\varepsilon = g_2\varepsilon \Rightarrow g_1 = g_2$

$\square$

Lemma: (i) If $G' \leq H \leq G$, then $H \trianglelefteq G$.

(ii) If $K \trianglelefteq G$, then $K' \trianglelefteq G$.

(iii) If $f: G \longrightarrow H$, and $\ker f = K$, then H is abelian iff $G' \leq K$.

In particular, G/K is abelian iff $G' \leq K$.

Pf: HW #4.

Big idea: • G/G' is a "maximal" abelian epimorphic image of G.

i.e., • G' is a "minimal" normal subgp L s.t. G/L is abelian.

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

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

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

<u>Def</u>: The <u>derived series</u> (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 G is <u>solvable</u> if $G^{(k)} = 1$ for some k.

<u>Examples</u>

$\boxed{1}$ If G is abelian, then $G' = 1$, so G is solvable.

$\boxed{2}$ If $G = S_3$, then $G' = A_3$, $G'' = A_3' = 1$, so S_3 is solvable.

$\boxed{3}$ If $G = A_n$ $(n \geqslant 5)$, then A_n is non-abelian & simple,

$A_n' \lhd A_n$, so $A_n' = 1$ or A_n.

A_n / A_n' is abelian $\Longrightarrow A_n = A_n$

Thus A_n is not solvable if $n \geqslant 5$.

<u>Def</u>: A <u>subnormal series</u> for a group G is a sequence

$G = G_0 \geqslant G_1 \geqslant G_2 \geqslant \cdots$, where $G_{i+1} \lhd G_i$ $\forall i$.

The subgroups G_i are called <u>subnormal</u> subgroups of G,

and the groups G_i / G_{i+1} are called the <u>factors</u> of the series.

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

<u>ex</u>: $D_4 = \langle r, s \rangle$, $D_4 \geqslant \langle r \rangle \geqslant \langle r^2 \rangle \geqslant 1$
but $\langle r^2 \rangle \ntriangleleft D_4$ (check!)

<u>Def</u>: A subnormal series is <u>normal</u> if each $G_i \lhd G$. The <u>length</u> of a subnormal series is the number of nontrivial factors G_i/G_{i+1}.

<u>Thm 5.3</u>: A group is solvable iff it has a subnormal series $G = G_0 \geq G_1 \geq G_2 \geq \cdots \geq G_m = 1$ with abelian factors.

<u>Pf</u>: $(\Rightarrow)$ ✓

$(\Leftarrow)$ Suppose $G = G_0 \geq G_1 \geq \cdots \geq G_m = 1$ is a subnormal series with abelian factors.

Since $G_0/G_1 = G/G_1$ is abelian, $G' \leq G_1$ (see Lemma (iii)).

Similarly $G_2 \geq G_1' \geq (G')' = G^{(2)}$ since G_1/G_2 is abelian.

By induction, $G^{(k)} \leq G_k$ $\forall k$, thus $G^{(m)} = 1 \Rightarrow G$ is solvable $\square$

<u>Thm 5.4</u>: Suppose $K \lhd G$. Then G is solvable iff K <u>and</u> G/K are solvable.

<u>Pf</u>: $(\Rightarrow)$ We saw earlier that subgps of solvable gps are solvable. Suppose $K \lhd G$. Then $[xK, yK] = x^{-1}y^{-1}xyK = \eta([x,y]) = [\eta(x), \eta(y)]$ where $\eta: G \twoheadrightarrow G/K$ is canonical quotient.

Thus, $(G/K)' = \eta(G')$, & $(G/K)^{(k)} = \eta(G^{(k)})$.

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

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

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

By Thm 1.13, $G_i/G_{i+1} \cong (G_i/K)/(G_{i+1}/K)$, and so

$$G = G_0 \trianglerighteq \cdots \trianglerighteq G_n = K = K_0 \trianglerighteq K_1 \trianglerighteq \cdots \trianglerighteq K_m = 1$$

is a subnormal series for G with abelian factors, so G is solvable by Thm 5.3. $\square$

Def: A subnormal series $G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = 1$ is a <u>composition series</u> for G if each G_{i+1} is a maximal proper normal subgp of G_i.

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

Example: $S_n \trianglerighteq A_n \trianglerighteq 1$ 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 5.5 (Jordan-Hölder): If $|G| < \infty$, and

$$G = G_0 \trianglerighteq G_1 \trianglerighteq \cdots \trianglerighteq G_m = 1 \quad \text{and}$$
$$G = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_k = 1$$

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.

Pf: Induction on m.

Base Case: $m = 1 \Rightarrow G$ 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 $K_2 = G_1 \cap H_1$.

$$\begin{tikzcd}[column sep=small] & G \arrow[dl, dash] \arrow[dr, dash] & \\ G_1 \arrow[dr, dash] & & H_1 \arrow[dl, dash] \\ & K_2 = G_1 \cap H_1 & \end{tikzcd}$$

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

Isom thm $\Longrightarrow$ $G/G_1 \cong H_1/K_2$

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

In particular, $K_2 \lhd G_1$ and $K_2 \lhd H_1$ (in both cases, maximal).

Now, let $K_2 \geqslant K_3 \geqslant \cdots \geqslant K_s = 1$ be a composition series for K_2.

$$\begin{array}{llll} \text{We have} & G = G_0 \geqslant G_1 \geqslant G_2 \geqslant G_3 \geqslant \cdots \geqslant G_m = 1 & & S_1 \\ & G_0 \geqslant G_1 \geqslant K_2 \geqslant K_3 \geqslant \cdots \geqslant K_s = 1 & & S_2 \\ & H_0 \geqslant H_1 \geqslant K_2 \geqslant K_3 \geqslant \cdots \geqslant K_s = 1 & & S_3 \\ & H_0 \geqslant H_1 \geqslant H_2 \geqslant H_3 \geqslant \cdots \geqslant H_s = 1 & & S_4 \end{array}$$

IHOP $\Rightarrow$ S_1 & S_2 have isomorphic factors, as do S_3 & S_4,

and $m-1 = s-1 = k-1$.

By Isom thm, S_2 & S_3 have isomorphic factors. $\square$

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

	Factors
$\mathbb{Z}_{12} \geqslant 2\mathbb{Z}_{12} \geqslant 4\mathbb{Z}_{12} \geqslant 0$	$\mathbb{Z}_2$, $\mathbb{Z}_2$, $\mathbb{Z}_3$
$\mathbb{Z}_{12} \geqslant 2\mathbb{Z}_{12} \geqslant 6\mathbb{Z}_{12} \geqslant 0$	$\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_2$
$\mathbb{Z}_{12} \geqslant 3\mathbb{Z}_{12} \geqslant 6\mathbb{Z}_{12} \geqslant 0$	$\mathbb{Z}_3$, $\mathbb{Z}_2$, $\mathbb{Z}_2$

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 $B \trianglelefteq A$ and $A/B \cong C$.

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