

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.

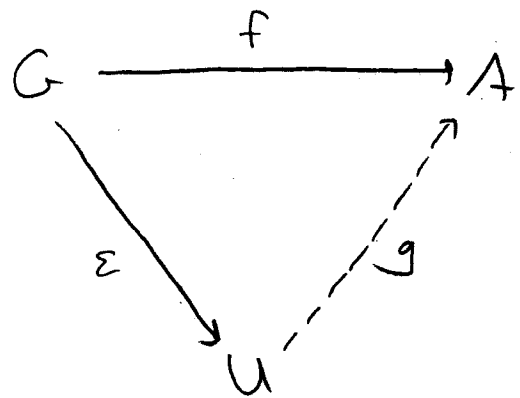
IF G is non-abelian, then $\phi(G)$ is abelian if "ker ϕ is large enough"

We'll show that there is some maximal homomorphic image w.r.t. $\phi(G)$ being abelian.

This will be an example of a universal property.

Def: A pair (U, ε) is universal 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 any other abelian group A with homom. $f: G \rightarrow A$, $\exists!$ homom. $g: U \rightarrow A$ s.t. $f = g\varepsilon$.

In this case, we say that f can be factored through U .



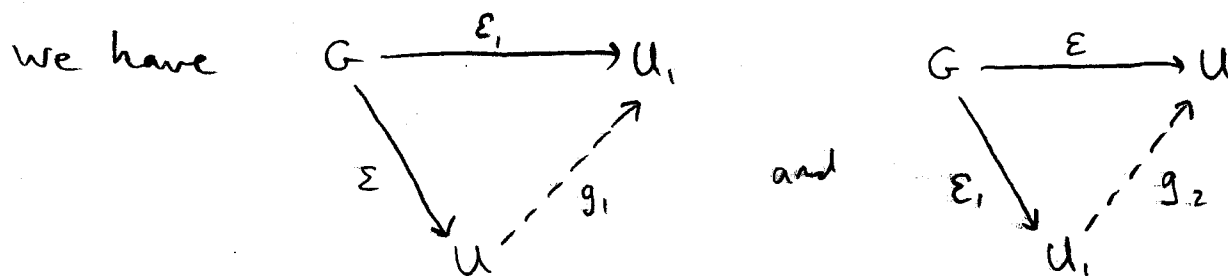
[2]

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

Big question: Does such a universal pair exist?

Prop 5.1: 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_1, ε_1) are universal pairs,



We can "stack" these diagrams:



By uniqueness, $g_2 g_1 = 1_U$

An analogous argument gives $g_1 g_2 = 1_{U_1}$

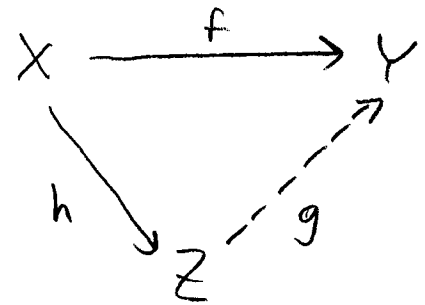
Thus g_1 & g_2 are inverse isomorphisms. \square

Question: Let X, Y, Z be sets, and $f: X \rightarrow Y, h: X \rightarrow Z$

Functions: When does there exist a (unique) $g: Z \rightarrow Y$
s.t. $f = gh$?

Answer: We're forced to define

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



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

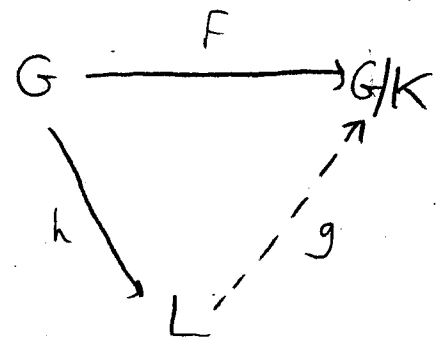
Think: "f collapses X at least as much as h does"

Now, consider the above situation but with groups

(so the maps are homomorphisms).

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

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



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

This is the universal property of quotient groups.

[4]

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 $f: G \rightarrow A$ be a homom, $\varepsilon: A$ 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 $x, y, z \in G$, $[x, y]^{-1} = [y, x]$

$$[x, y]^2 = [x^2, y^2]$$

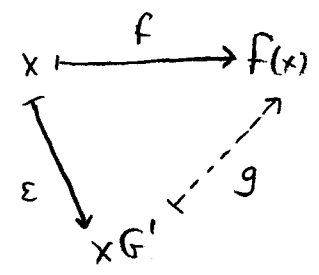
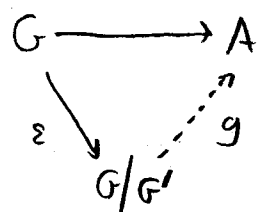
Thus $G' \triangleleft G$.

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 $\varepsilon: G \rightarrow U$ to be the canonical quotient map.

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



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

(explicitly, $xG' = yG' \Leftrightarrow y^{-1}xG' = G' \Leftrightarrow y^{-1}x \in G' \Leftrightarrow f(y^{-1}x) = f(x) = f(y)$
 $\Leftrightarrow g(xG') = g(yG')$. ✓

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

clearly surjective ✓

Uniqueness: $G \xrightarrow{f} A$ If $g_1\varepsilon = f$ and $g_2\varepsilon = f$, then
 $\varepsilon \searrow \begin{array}{c} G \\ \nearrow g_1 \\ G/G' \end{array} \nearrow g_2$ $g_1\varepsilon = g_2\varepsilon \Rightarrow g_1 = g_2$ □

- Lemma:
- (i) If $G' \leq H \leq G$, then $H \triangleleft G$.
 - (ii) If $K \triangleleft G$, then $K' \triangleleft G$.
 - (iii) If $f: G \rightarrow H$, 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 st G/L is abelian.

16

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

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

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

Def: The derived series (or commutator series) of G is

the sequence $G = G^{(0)} \geq G^{(1)} \geq G^{(2)} \geq \dots \geq G^{(k)} \geq \dots$

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

Examples

[1] If G is abelian, then $G' = 1$, 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 & simple,
 $A_n' \triangleleft A_n$, so $A_n' = 1$ or A_n .

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

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

Def: A subnormal series for a group G is a sequence

$G = G_0 \geq G_1 \geq G_2 \geq \dots$, where $G_{i+1} \triangleleft G_i \forall i$,

The subgroups G_i are called subnormal subgroups of G ,

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

Note: Subnormal subgroups need not be normal in G .

ex: $D_4 = \langle r, s \rangle$, $D_4 \geq \langle r \rangle \geq \langle r^2 \rangle \geq 1$
 but $\langle r^2 \rangle \ntriangleleft D_4$ (check!)

Def: A subnormal series is normal if each $G_i \triangleleft G$. The length of a subnormal series is the number of nontrivial factors G_i/G_{i+1} . 7

Thm 5.3: A group is solvable iff it has a subnormal series $G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \dots \triangleright G_m = 1$ with abelian factors.

Pf: (\Rightarrow) ✓

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

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

Similarly $G_2 \triangleright G_1' \triangleright (G_1')' = G^{(2)}$ 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

Thm 5.4: Suppose $K \triangleleft G$. Then G is solvable iff K and G/K are solvable.

Pf: (\Rightarrow) We saw earlier that subgps of solvable gps are solvable. Suppose $K \triangleleft G$. Then $[xK, yK] = x'y^{-1}xyK = \eta([x, y]) = [\eta(x), \eta(y)]$ where $\eta: G \rightarrow G/K$ 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

$$K = K_0 \triangleright K_1 \triangleright \dots \triangleright K_m = 1$$

$$G/K = G_0/K \triangleright G_1/K \triangleright \dots \triangleright G_k/K = K/K$$

18

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

$$G = G_0 \triangleright \dots \triangleright G_n = K = K_0 \triangleright K_1 \triangleright \dots \triangleright K_m = 1$$

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

Def. A subnormal series $G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_m = 1$ 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: $S_n \triangleright A_n \triangleright 1$ 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

$$G = G_0 \triangleright G_1 \triangleright \dots \triangleright G_m = 1 \quad \text{and}$$

$$G = H_0 \triangleright H_1 \triangleright \dots \triangleright H_k = 1$$

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.

PG: Induction on m .

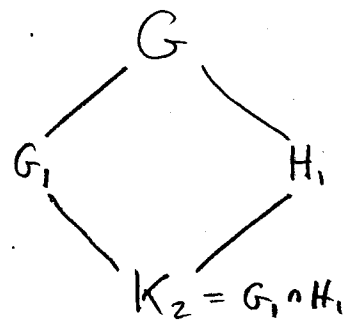
Base case: $m = 1 \Rightarrow G$ is simple

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 $K_2 = G_1 \cap H_1$.

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



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

$G/H_1 \cong G_1/K_2$

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

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

We have	$G = G_0 \supseteq G_1 \supseteq G_2 \supseteq G_3 \supseteq \dots \supseteq G_m = 1$	S_1
	$G_0 \supseteq G_1 \supseteq K_2 \supseteq K_3 \supseteq \dots \supseteq K_s = 1$	S_2
	$H_0 \supseteq H_1 \supseteq K_2 \supseteq K_3 \supseteq \dots \supseteq K_s = 1$	S_3
	$H_0 \supseteq H_1 \supseteq H_2 \supseteq H_3 \supseteq \dots \supseteq H_s = 1$	S_4

ItOP $\Rightarrow S_1 \& S_2$ 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. □

Example: let $G = \mathbb{Z}_{12}$.

Factors

$\mathbb{Z}_{12} \supseteq 2\mathbb{Z}_{12} \supseteq 4\mathbb{Z}_{12} \supseteq 0$

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

$\mathbb{Z}_{12} \supseteq 2\mathbb{Z}_{12} \supseteq 6\mathbb{Z}_{12} \supseteq 0$

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

$\mathbb{Z}_{12} \supseteq 3\mathbb{Z}_{12} \supseteq 6\mathbb{Z}_{12} \supseteq 0$

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

[10]

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

Def: A group 'A' is an extension 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.