Lecture 7

Last time:

- discussed <u>automorphisms</u> $\varphi: G \xrightarrow{\sim} G$

  ↗

  <u>isomorphism</u> from group to itself

- discussed one nontrivial example of automorphism:

$$S_3 \xrightarrow{\varphi} S_3$$

$$x = (123) \longmapsto (132) = x^2$$

$$y = (12) \longmapsto (12) = y$$

↖ φ is <u>uniquely</u> determined by where it maps x, y

- example above is a <u>particular case</u> of:

$$g \in G \rightsquigarrow \varphi_g: G \xrightarrow{\sim} G \; ; \; h \longmapsto ghg^{-1}$$

for $G = S_3$, $g = (12)$ get φ as above

Question:

For which groups automorphisms φ_g are all equal to id?

Answer: for commutative groups.

$(ghg^{-1} = gg^{-1}h = h)$

In general: $\varphi_g = id \iff ghg^{-1} = h \quad \forall h \in G$

φ equivalent to $gh = hg$

So g commutes with every element of G

such g are called central

Why automorphisms are important?

They allow to "identify" different elements of the group

For example:

Claim. if $\varphi : G \xrightarrow{\sim} G'$ an automorphism,

then for $g \in G$, $g' := \varphi(g)$ we have:

$$\mathrm{ord}(g) = \mathrm{ord}(g')$$

prf: if $g^n = 1 \Rightarrow \varphi(g^n) = \varphi(1) = 1$

$$(g')^n = \varphi(g)^n$$

if $(g')^m = 1 \Rightarrow (\varphi^{-1})(g'^m) = \varphi^{-1}(1) = 1$

$$g^m = \varphi^{-1}(g')^m$$

So $g^n = 1 \iff (g')^m = 1$

$$\mathrm{ord}(g) = \mathrm{ord}(g')$$

Corollary

If $x, x' \in G$ are conjugate

i.e. $\exists g \in G$ s.t. $x' = g x g^{-1}$

then $\text{ord}(x) = \text{ord}(x')$

This means that, for example, $(12), (123) \in S_3$ are not conjugate.

Exercise: cycles $(k_1, \ldots, k_n), (p_1, \ldots, p_m)$ $\in S_N$ are conjugate iff $n = m$.

Example:

$$(1423) = (243)(1234)(234)$$

$$= (243)(1234)(243)^{-1}$$

In general:

$$\sigma \cdot (p_1 \dots p_m) \cdot \sigma^{-1} = (\sigma(p_1) \dots \sigma(p_m))$$

Work out!

Back to homomorphisms

Isomorphism ⇐ bijective

Homomorphism ⇐ in general neither injective nor surjective.

Given homomorphism $\varphi: G \to G'$,

how to "make" it surjective?

Replace G' by the image of φ.

Claim: $\operatorname{im}\varphi = \{\varphi(g) \mid g \in G\}$

is a subgroup of G'

proof: exercise, let's check that $\operatorname{im}\varphi \cap G'$

is closed under multiplication.

$$\varphi(g_1)\cdot\varphi(g_2) = \varphi(g_1 g_2) \in \operatorname{im}\varphi \quad \checkmark$$

Example:

$$\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}, \quad n \longmapsto 2n$$

φ

$$\operatorname{im}(\varphi) = 2\mathbb{Z}$$

$$(\mathbb{R}, +) \xrightarrow{\varphi} (\mathbb{R}^{\times}, \cdot)$$

$$t \longmapsto 2^t \quad \text{and} \quad \operatorname{im}\varphi = \mathbb{R}_{>0}$$

φ

positive real numbers

So, if $\varphi : G \to G'$, then can replace G' by $\operatorname{im}\varphi =: S$ and $\varphi : G \twoheadrightarrow S$

φ

surjective

is not an isomorphism in general

can fail to be injective

How to "measure" non-injectivity of homomorphism $\varphi : G \to S$?

Answer: non-injectivity of φ is "controlled" by

$$\ker \varphi = \{ g \in G \mid \varphi(g) = 1_S \}$$

Namely: φ is injective iff $\ker \varphi = \{1_G\}$

↳ will prove that

Example $\mathbb{Z} \xrightarrow{\varphi} \mathbb{Z}/n\mathbb{Z}$, $m \longmapsto m \bmod n$

$\ker \varphi = n\mathbb{Z}$ ← subgroup of $\mathbb{Z}$

In general:

Claim $\ker\varphi$ is a subgroup of G.

Proof: exercise, let's prove that $\ker\varphi$ is closed under multiplication.

$a, b \in \ker\varphi \Rightarrow \varphi(a) = \varphi(b) = 1$

Want: $ab \in \ker\varphi$; $\varphi(ab) = \varphi(a)\varphi(b) = 1 \cdot 1 = 1$

Proposition. $\varphi: G \to G'$ homomorphism, $a, b \in G$

The following conditions are equivalent:

(1) $\varphi(a) = \varphi(b)$

(2) $a^{-1}b \in \ker\varphi$

proof

(1) $\Rightarrow$ (2) if $\varphi(a) = \varphi(b)$ $\Rightarrow$

$$\varphi(a)\varphi(b)^{-1} = 1$$

$$\varphi(a)\varphi(b^{-1}) = 1 \Rightarrow ab^{-1} \in \ker\varphi \checkmark$$

(2) $\Rightarrow$ (1) $\varphi(ab^{-1}) = 1 \Rightarrow \varphi(a)\varphi(b)^{-1} = 1 \Rightarrow$

$\Rightarrow \varphi(a) = \varphi(b)$ $\checkmark$

Corollary. φ is injective iff $\ker\varphi = \{1_G\}$

proof if φ is injective $\Rightarrow$ $\#\varphi^{-1}(\{1\}) \leq 1$

it contains 1_G

$\ker\varphi = \{1_G\}$

If $\ker \varphi = \{1\}$ want to check that

if $\varphi(a) = \varphi(b) \Rightarrow a = b$

We know that $\varphi(a) = \varphi(b) \Leftrightarrow a^{-1}b \in K = \{1\}$

$\Downarrow$

$a^{-1}b = 1 \Rightarrow a = b$ ✓

Corollary $\varphi : G \twoheadrightarrow S$ a surjective homom

Then $\forall x \in S$, $\varphi^{-1}(x) \underset{\varphi}{\simeq} \ker \varphi$

isomorphic as sets
(i.e., exists a bijective map)

In particular: $G = \bigsqcup_{x \in S} \varphi^{-1}(x)$

disjoint decomposition into sets of the same size

proof: want a identify $\varphi^{-1}(x) \simeq \ker \varphi$.

Pick any $a \in G$ s.t. $\varphi(a) = x$.

Then $b \in \varphi^{-1}(x) \iff \varphi(b) = x = \varphi(a) \iff$

proposition
$\iff a^{-1}b \in \ker \varphi$

So, multiplication by a^{-1} defines the identification $\varphi^{-1}(x) \xrightarrow{a^{-1}\cdot}{}_{\sim} \ker\varphi$

Question: who is the inverse?

Answer: left multiplication by a! ($\ker\varphi \xrightarrow{a\cdot}{}_{\sim} \varphi^{-1}(x)$)

Important corollary:

If $\varphi: G \to G'$ ← arbitrary homomorphism of finite groups

then $\#G = \#\mathrm{im}\varphi \cdot \#\ker\varphi$

R will use this corollary next time to describe kernel of some interesting morphism

proof of important corollary.

$G \twoheadrightarrow \operatorname{im}\varphi$

φ surjective homomorphism

$\swarrow\!\!/$ (by Corollary above)

$$G = \bigsqcup_{x \in \operatorname{im}\varphi} \varphi^{-1}(x)$$

all have the same number of elements equal to $\#\ker\varphi$

$\swarrow\!\!/$

$$\#G = \sum_{x \in \operatorname{im}\varphi} \#\varphi^{-1}(x) = \sum_{x \in \operatorname{im}\varphi} \#\ker\varphi =$$

$$= \#\ker\varphi \cdot \#\operatorname{im}\varphi$$