Last class:

An isomorphism Φ is a map

$$\Phi : G \to \bar{G} \quad , \quad G, \bar{G} \text{ groups}$$

Satisfying

- 1-1 and onto ($\Leftrightarrow$ bijection between G and $\bar{G}$)
- $\Phi(ab) = \Phi(a)\,\Phi(b)$ for all a, b in G

We say that the groups G and $\bar{G}$ are isomorphic (notation: $G \cong \bar{G}$) if there exists an isom. $\Phi : G \to \bar{G}$

Have seen:

① $(\mathbb{R}, +)$ and $(\mathbb{R}_+, \cdot)$ are isomorphic groups

$\Phi(x) = e^x$ isom. $\mathbb{R} \to \mathbb{R}_+$

② if $a \in G$, $\operatorname{ord}(a) = \infty \Rightarrow \langle a \rangle \cong \mathbb{Z}$

$\operatorname{ord}(a) = n \Rightarrow \langle a \rangle \cong \mathbb{Z}_n$

Important Question:

Given two groups G and $\overline{G}$, are they isomorphic?

- to prove that they are isom: Find an isom. $\Phi: G \to \overline{G}$
- to disprove " " " " : use properties of isomorphisms to show that no isom. $G \to \overline{G}$ can exist.

③ example: have seen: If G abelian $\overline{G} \cong G \Rightarrow \overline{G}$ abelian

$\Rightarrow \mathbb{Z}_6$ and S_3 are not isom.

Properties of Isomorphisms

(numbers as in Theorem 6.2 in book).

② $\Phi(a^n) = \Phi(a)^n$

(proof by ind. on n:

$n=2$: $\Phi(a^2) = \Phi(aa) \overset{\text{isom. prop}}{=} \Phi(a)\Phi(a) = \Phi(a)^2$

$n>2$: $\Phi(a^n) = \Phi(a^{n-1}a) = \Phi(a^{n-1})\Phi(a) = \Phi(a)^{n-1}\Phi(a) = \Phi(a)^n$

(ind. assumption)

④ isomorphisms preserve order of group elements

i.e. $\operatorname{ord}\Phi(a) = \operatorname{ord} a \quad \forall a \in G$

(proof- let $n = \operatorname{ord}(a)$

$\Phi(a)^n \overset{②}{=} \Phi(a^n) = \Phi(e) \overset{①}{=} \bar{e}$ identity of $\bar{G}$

$\Rightarrow$ $\operatorname{ord}\Phi(a) \mid n$ ⓐ

let $0<j<n$: $\Phi(a)^j = \Phi(a^j) \neq \Phi(e) = \bar{e}$ (Φ is 1-1!)

$\neq e$ by assumption

ⓑ $\operatorname{ord}\Phi(a) \geq n$

ⓐ & ⓑ $\Rightarrow$ claim

(7) G finite $\Rightarrow$ G and $\bar{G}$ have same # elements of every order.

Example: Is $U(8) \cong \mathbb{Z}_4$?

$U(8) = \{1, 3, 5, 7\} \Rightarrow |U(8)| = |\mathbb{Z}_4|$

additional check: use (7)

have already checked: $\text{ord}(3) = \text{ord}(5) = \text{ord}(7) = 2$

$\Rightarrow U(8)$ has (3) elements of order 2

$\mathbb{Z}_4$: $\text{ord}(1) = 4$, $\text{ord}(2) = 2$, $\text{ord}(3) = 4$ } $\mathbb{Z}_4$ has only (one) element of order 2

by prop. (7) $\Rightarrow$ $\mathbb{Z}_4 \ncong U(8)$

Another result: G cyclic, $G \cong \bar{G} \Rightarrow \bar{G}$ cyclic

Proof. There exists an isom $\phi: G \to \bar{G}$

Let a be a generator, i.e. $G = \langle a \rangle$

$\Rightarrow G = \{ a^j, j \in \mathbb{Z} \}$

$\overline{G} = \underline{\Phi}(G) = \{ \underline{\Phi}(a^j), j \in \mathbb{Z} \}$

$\underline{\Phi}$ surjective.

$= \{ \underline{\Phi}(a)^j, j \in \mathbb{Z} \}$

(27)

$= \langle \underline{\Phi}(a) \rangle$

$\Rightarrow \overline{G}$ is cyclic with generator $\underline{\Phi}(a)$.

Automorphisms

An autom α is an isomorphism from G to itself

Example: $G = (\mathbb{R}, +)$. $\alpha(x) = -x$

obviously $\alpha : \mathbb{R} \to \mathbb{R}$ ✓

only need to check it is an isom.

$x \to -x$ is 1-1 and onto ✓

$$\alpha(x+y) = -(x+y) = -x - y = (-x) + (-y)$$
$$= \alpha(x) + \alpha(y)$$ ✓

Lemma: G a group, $a \in G$

Define map $\alpha_a : G \to G$

$g \mapsto aga^{-1}$ (conjugation by a)

$\Rightarrow \alpha_a$ is an automorphism.

Proof. obviously $\alpha_a(g) = aga^{-1} \in G$

enough to show: α_a is an isomorphism:

1-1: assume $\alpha_a(g) = \alpha_a(h)$

$aga^{-1} = aha^{-1}$ use cancellation properties!

$ga^{-1} = ha^{-1}$ (left cancellation)

$g = h$ ✓ (right ")

onto: Let $h \in G$

need to find $g \in G$ s.t. $\alpha_a(g) = h$

$\Leftrightarrow$ $aga^{-1} = h$ (solve for g)

$\Leftrightarrow$ $g = a^{-1}ha$

$\Rightarrow$ $g = a^{-1}ha$ does the job

$$\alpha_a(gh) = agha^{-1} \overset{!}{=} \alpha_a(g)\alpha_a(h)$$

$$= aga^{-1}aha^{-1}$$

$$= agha^{-1} = \alpha_a(gh)$$ ✓

Def An autom. of the form α_a is called an inner automorphism.

Examples

(1) G abelian

$$\alpha_a(g) = aga^{-1} = aa^{-1}g = g$$

$\curvearrowright$ abelian!

$\Rightarrow \alpha_a = id$ for all $a \in G$

(2) $G = S_3$ $\quad a = (12)$

recall: $\pi(a_1 \dots a_r)\pi^{-1} = (\pi(a_1)\,\pi(a_2) \dots \pi(a_r))$

$\Rightarrow$ $\alpha_{(12)}(12) = (21) = (12)$

$2\ 1$

$\alpha_{(12)}(13) = (23)$

$2\ 3$

$\alpha_{(12)}(23) = (13)$

$1\ 3$

$\alpha_{(12)}(123) = (12)(123)(12)^{-1} = (213) = (132) = \alpha_{(12)}(123)$

$2\ 1\ 3$

$\alpha_{(12}(132) = (123)$