Chapter 6 Isomorphisms

Definition: Two groups are isomorphic if ....

Examples

(1) The function $\exp : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$ is a group isomorphism.

(2) The group $(\mathbb{Z}_n, +)$ is somorhic to $(G_n, \cdot)$, where

$$G_n = \{\exp(i2k\pi/n) : k = 0, 1, \ldots, n-1\}.$$

(3) Every cyclic group is isomorphic to $(\mathbb{Z}_n, +)$ or $(\mathbb{Z}, +)$.

(4) [**Theorem 6.1**] Every group is isomorphic to a subgroup of S_A.

(5) The group S_n is isomorphic to the group of $n \times n$ permutation matrices.

(1) → $(\mathbb{R}, +)$ is a group.

$(\mathbb{R}^+, \cdot)$ is a group.

Define $\exp : \mathbb{R} \to \mathbb{R}^+$ by

$\exp(x) = e^x$.

(a) Then exp is a bijection:

1° well-defined: $\forall x \in \mathbb{R}$, $\exp(x) = e^x > 0$, $\therefore$ $\exp(x) \in \mathbb{R}^+$

2° 1-1; onto. By the properties of $\exp(x)$

(b) $\exp(x+y) = e^{x+y} = e^x e^y = \exp(x)\exp(y)$

$\forall x, y \in \mathbb{R}$

$\therefore$ exp is a group isomorphism

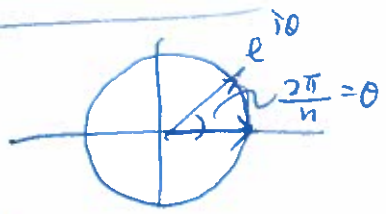
$\exp : (\mathbb{R}, +) \to (\mathbb{R}^+, \cdot)$

$\forall n$ $\mathbb{Z}_n = [1] = [n+1]$

$f([1]) = f([n+1])$

(2) $(\mathbb{Z}_n, +) \cong (G_n, \cdot)$

$G_n = \{ e^{ik\frac{2\pi}{n}} : k = 0, \cdots, n-1 \}$



(a) Define $f : \mathbb{Z}_n \to G_n$ by $f([k]) = e^{ik\frac{2\pi}{n}}$.

~~$\{f[0], \cdots, f[n-1]\} = \{1, e^{\frac{i2\pi}{n}}, \cdots, e^{\frac{i2\pi(n-1)}{n}}\}$~~

If $[k] = [\hat{k}]$, then $k - \hat{k} = nr$. So $f([k]) = e^{\frac{i2\pi k}{n}}$.

$f([\hat{k}]) = e^{\frac{i2\pi\hat{k}}{n}}$ //

If $e^{i2\pi k/n} / e^{i2\pi \hat{k}/n} = e^{i\frac{2\pi}{n}(k-\hat{k})}$

$= e^{i\frac{2\pi}{n} nr}$

$= e^{i2\pi r} = 1$

$\therefore$ f is well-defined. and

$f[0] = 1$

$\vdots$

$f[n-1] = e^{i\frac{2\pi(n-1)}{n}}$

$\Big\}$ $\therefore$ bijective.

(b)

$f([k]+[l]) = f([k+l])$

$\|$

$e^{i\frac{2\pi(k+l)}{n}}$

$\|$

$e^{i\frac{2\pi k}{n}} \cdot e^{i\frac{2\pi l}{n}}$

$\|$

$f([k]) \cdot f([l])$

$\forall\ [k], [l] \in \mathbb{Z}_n$

---

(3) If $ab = ba$ in G_1

Then

$\phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a)$. ⊛

---

(4) Suppose $G_1 = \langle a \rangle := \{ a^m : m \in \mathbb{Z} \}$

Then $G_2 = \phi[G_1] = \{ \phi(x) : x \in G_1 \}$

$= \{ \phi(a^m) : m \in \mathbb{Z} \}$

$= \{ \phi(a)^m : m \in \mathbb{Z} \} = \langle \phi(a) \rangle$

---

(2) If G_2 is cyclic, then $\phi^{-1} : G_2 \to G_1$ is an isomorphism so that G_1 is cyclic.

Lemma: If $\phi : G_1 \to G_2$ is isom. (i.e. ϕ is bijective, $\phi(x_1 x_2) = \phi(x_1)\phi(x_2)$ $\forall x_1, x_2 \in G_1$) then $\phi^{-1} : G_2 \to G_1$

Proof: $\phi^{-1} : G_2 \to G_1$ is a bijection.

Suppose $y_1, y_2 \in G_2$.

Then there are $x_1, x_2 \in G_1$ s.t.

$\phi(x_1) = y_1$ $\phi(x_2) = y_2$

$\phi(x_1 x_2) = \phi(x_1)\phi(x_2) = y_1 y_2$

$\therefore \phi^{-1}(y_1 y_2) = x_1 x_2$

$= \phi^{-1}(y_1)\phi^{-1}(y_2)$

$\therefore \phi^{-1}(y_1 y_2) = \phi^{-1}(y_1)\phi^{-1}(y_2)$.

(5) To prove $|a| = |\phi(a)|$.

$\phi : \langle a \rangle \to \langle \phi(a) \rangle$

Note that $\phi : \{ a^m : m \in \mathbb{Z} \} \to \{ \phi(a)^m : m \in \mathbb{Z} \}$ is a bijection.

$\therefore |a| = |\langle a \rangle| = |\langle \phi(a) \rangle| = |\phi(a)|$

$\mathbb{Z}_3 \to S_{\mathbb{Z}_3}$
$\phi \quad \phi$

$\mathbb{Z}_3 \cong H \leq S_{\mathbb{Z}_3}$

$H = \langle \begin{pmatrix} [0] & [1] & [2] \\ [1] & [2] & [0] \end{pmatrix} \rangle$

Results on group isomorphisms and applications

Theorem 6.2 Suppose $\phi : G_1 \to G_2$ is an isomorphism. (G_1, G_2: group)

1. $\phi(e_1) = e_2$.
2. $\phi(a^n) = \phi(a)^n$ for any $n \in \mathbb{Z}$.
3. Two elements $a, b \in G_1$ commute if and only if $\phi(a)$ and $\phi(b)$ commute.
4. $G_1 = \langle a \rangle$ if and only if $G_2 = \langle \phi(a) \rangle$.
5. $|a| = |\phi(a)|$ for every $a \in G_1$.
6. For every integer k and $b \in G_1$, we have

$$|\{x \in G_1 : x^k = b\}| = |\{y \in G_2 : y^k = \phi(b)\}|.$$

In particular, $|\{x \in G_1 : x^k = e_1\}| = |\{y \in G_2 : y^k = e_2\}|$.

e.g. $|\{x \in G_1 : x^{10} = e_1\}| = |\{y \in G_2 : y^{10} = e_2\}|$

Proof: 1° Let $\phi(e_1) = y$.

$e_1 * e_1 = e_1$

$y \cdot y = \phi(e_1) * \phi(e_1) \Leftrightarrow \phi(e_1 * e_1) = \phi(e_1) = y = y \cdot e_2$

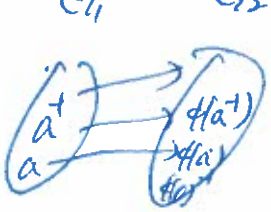
By cancellation law in G_2, $y = e_2$.

2° To prove $\phi(a^n) = \phi(a)^n$.

$\forall a \in G_1$, $n \in \mathbb{N}$, $\phi(a^n) = \phi(a \cdot a^{n-1}) = \phi(a)\phi(a^{n-1})$

$= \phi(a)\phi(a)\phi(a^{n-2}) \cdots = \underbrace{\phi(a) \cdots \phi(a)}_{n} = \phi(a)^n$.

$n = 0$, $\phi(a^0) = \phi(e_1) = e_2 = \phi(a)^0$



need to show

$n \in \mathbb{N}$ $\phi(a^{-n}) = \phi(a)^{-n}$.

Consider want: let $\phi(a^{-1}) = \phi(a)^{-1} \in G_2$

$\phi(a^{-1})\phi(a) = \phi(a^{-1} \cdot a) = \phi(e_1) = e_2 = \phi(a)^{-1}\phi(a)$

By right cancellation, $\phi(a^{-1}) = \phi(a)^{-1}$

Then for $n \in \mathbb{N}$

$\phi(a^{-n}) = \phi((a^n)^{-1}) = \phi(a^n)^{-1} = (\phi(a)^n)^{-1} = \phi(a)^{-n}$

(6)

$k=0$ $\quad \{x \in G_1 : x^0 = b\}$ ~~$, \; y \in G_2$~~

~~$k \in \mathbb{N}$~~ $= \begin{cases} G_1 & \text{if } b = e_1, \\ \phi & \text{if } b \neq e_1, \end{cases}$

Same for $\{x \in G_2 : x^0 = \phi(b)\}$.

$= \begin{cases} G_2 & \text{if } \phi(b) = e_2, \text{ i.e, } e_1 = b. \\ \phi & \text{if } \phi(b) \neq e_2, \text{ i.e, } e_1 \neq b. \end{cases}$

$k \in \mathbb{N}$. Then

$x^k = b$.

$\Leftrightarrow \phi(x^k) = \phi(b)$

$\Leftrightarrow \phi(x)^k = \phi(b)$.

$\therefore \quad \phi : \{x \in G_1 : x^k = b\} \to \{y : y^k = \phi(b)\}$

ϕ is a bijection.

$k \in \mathbb{N}$. Then

$|\{x \in G_1 : x^{-k} = b\}| = |\{y \in G_2 : y^{-k} = \phi(b)\}|$.

$x^{-k} = b \quad \Leftrightarrow \quad \phi(x)^{-k} = \phi(b)$.

So $\phi : \{x \in G_1 : x^{-k} = b\} \to \{y \in G_2 : y^{-k} = \phi(b)\}$

is a bijection.

Similarly, $\phi^{-1}: G_2 \to G_1$ satisfies

$$\phi^{-1}(Z(G_2)) \subseteq Z(G_1)$$

i.e., $Z(G_2) \subseteq \phi(Z(G_1))$.

$\therefore \quad \phi(Z(G_1)) = Z(G_2)$.

Example. 1° $\mathbb{Z}_6 \not\cong S_3$ because $\mathbb{Z}_6$ is Abelian but S_3 is not

2° $(\mathbb{R}, +) \not\cong (\mathbb{R}^*, \cdot)$

because $x = 0$ is the only element say in $\mathbb{R}$ satisfying $x + x = 0$

but $y = 1, -1$ in $\mathbb{R}^*$ satisfy $y \cdot y = 1$.

3° $(\mathbb{Z}, +) \not\cong (\mathbb{R}, +)$ ∵

because $|\mathbb{Z}| \neq |\mathbb{R}|$

4° $(\mathbb{R}^*, \cdot) \not\cong (\mathbb{C}^*, \cdot)$

$\because \quad \{x \in \mathbb{R}^* : x^4 = 1\}$ has 2 elements

$\{y \in \mathbb{C}^* : y^4 = 1\}$ has 4 elements.

Theorem 6.3 Suppose $\phi : G_1 \to G_2$ is an isomorphism.

1. $\phi^{-1} : G_2 \to G_1$ is an isomorphism. ✓
2. G_1 is Abelian if and only if $\phi(G_1) = G_2$ is Abelian. ✓
3. G_1 is cyclic if and only if $\phi(G_1) = G_2$ is.

   In particular, $G_1 = \langle a \rangle$ if and only if $G_2 = \langle \phi(a) \rangle$. ✓
4. If $K \leq G_1$, then $\phi(K) \leq G_2$.
5. If $H \leq G_2$, then $\phi^{-1}(H) \leq G_1$.
6. $\phi(Z(G_1)) = Z(G_2)$.

(a) (b)

Proof: (4) Let $K \leq G_1$, i.e., $e_1 \in K$, $a, b \in K \Rightarrow ab^{-1} \in K$.

$\phi(K) = \{ \phi(x) : x \in K \}$.

(a) $e_1 \in K \Rightarrow \phi(e_1) = e_2 \in \phi(K)$.

(b) $y_1, y_2 \in \phi(K) \Rightarrow \exists\, x_1, x_2 \in K$ s.t. $\phi(x_1) = y_1, \phi(x_2) = y_2$

$\therefore y_1 y_2^{-1} = \phi(x_1)\phi(x_2)^{-1} = \phi(x_1 x_2^{-1}) \in \phi(K)$ $\because x_1 x_2^{-1} \in K$.

$\therefore \phi(K) \leq G_2$.

(5) Suppose $H \leq G_2$, i.e., (a) $\exists\, e_2 \in H$.

(b) $y_1, y_2 \in H \Rightarrow y_1 y_2^{-1} \in H$.

$\phi^{-1} : G_2 \to G_1$ is an isomorphism.

$\therefore \phi^{-1}(H)$ is a subgroup of G_1

(6) $Z(G_1) = \{ x \in G_1 : xg = gx \ \forall g \in G_1 \}$

$Z(G_2) = \{ y \in G_2 : y\hat{g} = \hat{g}y \ \forall \hat{g} \in G_2 \}$

$\phi(Z(G_1)) = \{ \phi(x) \in G_2 : x \in Z(G_1) \} \subseteq Z(G_2)$

$= \{ \phi(x) \in G_2 : \phi(x)\hat{g} = \hat{g}\phi(x) \ \forall \hat{g} \in G_2 \}$

because for every $\subseteq Z(G_2)$

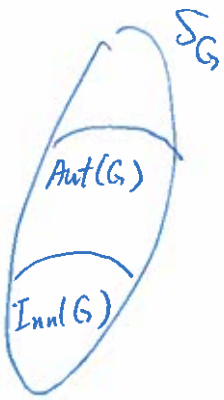
because for every $\hat{g} \in G_2$ there is $\hat{x} \in G_1$ s.t. $\phi(\hat{x}) = \hat{g}$.

$\therefore \phi(x)\hat{g} = \phi(x)\phi(\hat{x}) = \phi(x\hat{x}) = \phi(\hat{x}x) = \phi(\hat{x})\phi(x) = \hat{g}\phi(x)$.

Define: A group isom. $\phi: G \to G$ is called a group automorphism

Definition Let G be a group, and $a \in G$. Then $\phi_a : G \to G$ defined by $\phi_a(x) = axa^{-1}$ is an automorphism. (called an inner automorphism)

Theorem 6.4 Under function composition, the set $Aut(G)$ of group automorphisms is a group, and the set $Inn(G)$ of inner automorphisms is a subgroup. $\leq S_G$



Theorem 6.5 [Automorphisms of $\mathbb{Z}_n$] The groups $Aut(\mathbb{Z}_n)$ is isomorphic to $(U(n), \cdot)$ with

$$U(n) = \{k \in \mathbb{Z}_n : \gcd(k, n) = 1\}.$$