Recall

$\{e, a\}$ $\quad ea \quad eae \quad aeee \cdots$

$$\begin{cases} ea = ae = e \\ a^2 = e \end{cases}$$

$\{e, a, b\}$.

$ab = ba = e \Rightarrow b = a^{-1}$

$\cdots a^{-2}\, a^{-1}\, e\, a\, a^2\, a^3 \cdots$

§3 Maps and Permutation Groups

Recall: X, Y, f

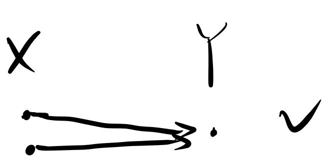
$f: X \to Y$

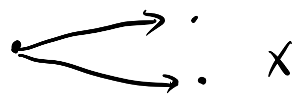
$x \mapsto f(x) = y$ $\qquad f(x) = x^2 : \mathbb{R} \to \mathbb{R}$.

(像)

Def 3.1. y is the image of x under f.

Def 3.2. $f(X) = \{f(x) : x \in X\} \subset Y$ is the image of X under f.





Def 3.3 The map f is one-to-one (injective) if for all $y \in f(X)$ there exists a unique $x \in X$ such that $f(x) = y$. i.e.

① $\boxed{f(x_1) = f(x_2) \Rightarrow x_1 = x_2}$

② $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$

Def 3.4 The map f is onto (在上) (or surjective) if every $y \in Y$, there exists a $x \in X$ such that $f(x) = y$.

Def 3.5 A map f that is one-to-one and onto is called bijective.

$id: x \mapsto x$

- $f: X \to Y$ bijective.

$x \mapsto y$

$\leftarrow$

$f^{-1}: Y \to X$

$y \mapsto x$, $f(x) = y$

$f(f^{-1}(y)) = y$, $f^{-1}(f(x)) = x$.

$f \circ f^{-1}$ $\qquad$ $f^{-1} \circ f$

$id: X \to X$

Thm 3.1 The span of a set of bijective maps of a finite set X to itself forms a group under composition of maps. This is called a permutation group.

$$X = \{1, 2, \cdots, n\}.$$

$$f: X \to X$$

$$k \mapsto i_k$$

$$k \neq k' \Rightarrow i_k \neq i_{k'}$$

$\{1, 2, 3\}$.

$f(1) = 1$, $f(2) = 2$, $f(3) = 3$

$\tilde{f}(1) = 2$, $\tilde{f}(2) = 1$, $\tilde{f}(3) = 3$.

Def 3.6 The set of all permutations of a finite set containing n elements is call the symmetric group S_n.

- $f: \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$.

  $k \mapsto i_k$.

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & \cdots & i_n \end{pmatrix}$$

$1 \mapsto i_1$, $2 \mapsto i_2$, $\dots$, $n \mapsto i_n$.

Exam. $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ $\in S_3$.

- $|S_n| = n!$

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ i_1 & i_2 & & \end{pmatrix}$$

$n \quad (n-1)$

- $|S_3| = 3! = 3\times 2\times 1 = 6.$

$(1)(2)(3) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = a = (1\,2\,3)$

$(1\,3\,2) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = a^2, \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = b = (1\,2)$

$(1\,3) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = ab, \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = a^2b = (2\,3)$

$\cancel{*}$ $S_3 = \{\langle a, b\rangle : a^3 = e,\ b^2 = e,\ ab = ba^2\}$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

- $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1\,2\,3)$ 3-cycle $\quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (1\,3\,2).$

n-cycle

• $\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} = (1\,2)(3) = (1\,2) \leftarrow$ transposition

2-cycle 1-cycle

$$\begin{pmatrix}1&2&3&4&5\\2&3&1&5&4\end{pmatrix} = (1\,2\,3)(4\,5)$$

• $(1\,2\,3) = (1\,3)(1\,2)$

$\|$

$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$$

$$\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix} = (1\,4\,3) = (1\,3)(1\,4) = (4\,1)(4\,3)$$

$$S_3 = \{e,\ (1\,2\,3),\ (1\,3\,2),\ (1\,2),\ (1\,3),\ (2\,3)\}$$

$a \in S_n \qquad a = (\,..\,)(\,..\,)(\,..\,) \cdots (\,..\,)$

• An even permutation is defined as one which can only be written as product of an even number of transpositions.

an odd . . . . .

. . . odd . . . .

$e = (1)(2)\cdots(n)$ $\qquad\qquad$ $(123) = \underline{(13)}(12)$.

- $A_n = \{$ all the even permutation $\}$. $\quad |A_n| = \frac{n!}{2}$

A_n is a subgroup of S_n

$\uparrow$

alternating group.

- $\forall\ \alpha, \tau \in A_n \Rightarrow \alpha\tau \in A_n$.

$\alpha = (i_1 i_2)\cdots(i_k i_\ell)$ $\qquad$ $\tau = (j_1 j_2)\cdots(j_p j_q)$

$\underbrace{(i_1 i_2)\cdots(i_k i_\ell)}_{\text{even}}$ $\qquad$ $\underbrace{(j_1 j_2)\cdots(j_p j_q)}_{\text{even}}$

$\alpha\tau = (i_1 i_2)\cdots(i_k i_\ell)(j_1 j_2)\cdots(j_p j_q)$ $\qquad$ $\underline{\text{even}}$.

- $\alpha^{-1} = [\underline{(i_1 i_2)\cdots(i_k i_\ell)}]^{-1}$ $\qquad$ $\alpha^{-1} = (i_k i_\ell)\cdots(i_1 i_2)$ $\qquad$ $\underline{\text{even}}$

$\underline{A_n \leq S_n}$.

$\underline{\S 4}$. Homomorphisms and isomorphisms.

$\underline{\text{Def 4.1}}$. Let G_1 and G_2 be groups. A map $\phi: G_1 \to G_2$ is a homomorphism if $\phi(g_1 g_2) = \phi(g_1)\phi(g_2)$, $\forall g_1, g_2 \in G_1$.

$\underline{\text{Exam}}$. $\phi: S_2 \to S_3$

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

- exercise. Prove ϕ is a homomorphism.

$$\phi : (\mathbb{R}, +) \to (\mathbb{C}, \cdot)$$

$$x \mapsto e^{ix}$$

$$\phi(x+y) = e^{i(x+y)} = e^{ix} \cdot e^{iy} = \phi(x) \cdot \phi(y)$$

Def 6.2. An isomorphism is a homomorphism that is bijective.

Thm 6.1 ϕ. G_1, G_2

(1) $\phi(e_1) = e_2$

(2) $\phi(g^{-1}) = [\phi(g)]^{-1}$, $\forall g \in G_1$.

Pf. (1) $e_1 = e_1 e_1$.

$\phi(e_1) = \phi(e_1 e_1) = \phi(e_1)\phi(e_1) \Rightarrow \phi(e_1) = e_2$.

(2) $gg^{-1} = e_1$

$$e_2 = \phi(gg^{-1}) = \phi(g)\phi(g^{-1})$$

$\Rightarrow$ $\phi(g^{-1}) = [\phi(g)]^{-1}$.

<u>Def 4.3</u>. The groups G_1 and G_2 are isomorphic if there exists an isomorphism.

<u>Thm 4.2</u>. The "isomorphic" relation is an equivalence relation which we denote by $\cong$.

- <u>equivalence relation</u>.

  (1) Reflexive. $G \cong G$.

  (2) Symmetric. $A \cong B \Rightarrow B \cong A$.

  (3) Transitive. $A \cong B$, $B \cong C \Rightarrow A \cong C$.

<u>Pf</u>. (1) $\underline{id: G \to G}$. $\Rightarrow$ $G \cong G$.

(2) $\phi: G_1 \to G_2$ isomorphism. $h_1 = \phi(g_1)$ $h_2 = \phi(g_2)$

$\underline{\phi^{-1}: G_2 \to G_1}$ $\phi^{-1}(h_1 h_2) = \underline{\phi^{-1}(h_1)\phi^{-1}(h_2)}$

(3) $\phi_1 : G_1 \to G_2$

$\phi_2 : G_2 \to G_3$

$\Rightarrow \phi_2 \circ \phi_1 : G_1 \to G_3$

$\Leftarrow$ $\phi^{-1}(\phi(g_1)\phi(g_2)) = \phi^{-1}(\phi(g_1))\,\phi^{-1}(\phi(g_2))$

ϕ isomorphism

$\Leftarrow$ $\phi^{-1}(\phi(g_1 g_2)) = g_1 g_2$

$\Leftarrow$ $g_1 g_2 = g_1 g_2$

- $G_1 \cong G_2 \Rightarrow |G_1| = |G_2|$.

Def 6.4. The order of an element g in a group is the smallest positive k such that $g^k = e$.

- isomorphism preserve the order of elements.

Thm 6.3. Two cyclic group of the same order are isometric.

Pf. $G_1 = \langle g_1 \rangle$, $G_2 = \langle g_2 \rangle$. $N = |G_1| = |G_2|$.

$G_1 = \{e_1, g_1, g_1^2, \ldots, g_1^{N-1}\}$, $G_2 = \{e_2, g_2, g_2^2, \ldots, g_2^{N-1}\}$.

$\phi : G_1 \to G_2$, $\phi(g_1^k) = g_2^k$.

- ϕ bijective.
- $\phi(g_1^m \cdot g_1^n) = \phi(g_1^{m+n}) = g_2^{m+n} = g_2^m \cdot g_2^n = \phi(g_1^m)\,\phi(g_1^n)$. $\boxed{\checkmark}$

$|G|=n$, $(\mathbb{Z}_n = \{0, 1, \cdots, n-1\}, +)$

$(C_n = \{e, a, a^2, \cdots, a^{n-1}\}, \cdot)$

$G_1 = G_2$ $G_1 \cong G_2$

$|G|=2$ $\mathbb{Z}_2$

$|G|=3$, $\mathbb{Z}_3$

$|G|=4$. $\mathbb{Z}_4$ or K_4

S_n

题.

1. 证明下列性质也可以定义群.

(1) 结合律.

(2) $\forall x$. $ex=x$.

(3) $\forall x$, $\exists y$ $yx=e$.

2. $(G, \cdot)$ 满足消去律. ($xy=xz \Rightarrow y=z$, $\forall x,y,z \in G$)

证明 G 是一个群.

Example 1.1.

3. 设 $\varphi: G \to G'$ 满同态. 证明若 G 是循环群,则 G' 也是循环群、若 G 是交换群,则 G' 也是交换群.

4. $\varphi: (\mathbb{R}, +) \to (\mathbb{C}, \cdot)$ 同态.

$$x \mapsto e^{ix}$$