(十四) 群论：子群 (Subgroup)

魏恒峰

hfwei@nju.edu.cn

2021 年 06 月 10 日

Definition (Subgroup (子群))

Let $(G, *)$ be a group and $\emptyset \neq H \subseteq G$.

If $(H, *)$ is a group, then we call H a subgroup of G, denoted $H \leq G$.

Definition (Subgroup (子群))

Let $(G, *)$ be a group and $\emptyset \neq H \subseteq G$.

If $(H, *)$ is a group, then we call H a subgroup of G, denoted $H \leq G$.

$H = G, H = \{e\}$ are two trivial (平凡) subgroups.

Definition (Subgroup (子群))

Let $(G, *)$ be a group and $\emptyset \neq H \subseteq G$.

If $(H, *)$ is a group, then we call H a subgroup of G, denoted $H \leq G$.

$H = G, H = \{e\}$ are two trivial (平凡) subgroups.

If $H \subset G$, then H is a proper subgroup (真子群).

$$(H = \{mz \mid z \in \mathbb{Z}\}, +) \leq (\mathbb{Z}, +)$$

$$(H = \{mz \mid z \in \mathbb{Z}\}, +) \leq (\mathbb{Z}, +)$$

$$H = \{1, 2, 4\} \leq G = \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$$

Theorem

Suppose that $H \le G$.

(1) *The identity of* H *is the same with that of* G.

$$e_H = e_G$$

(2) *The inversion of* a *in* H *is the same with that in* G.

$$\forall a \in H.\ a_H^{-1} = a_G^{-1}$$

Theorem

Suppose that $H \leq G$.

(1) *The* *identity* *of H is the same with that of G.*

$$e_H = e_G$$

(2) *The* *inversion* *of a in H is the same with that in G.*

$$\forall a \in H.\ a_H^{-1} = a_G^{-1}$$

$$e_H e_H = e_H = e_H e_G$$

Theorem

Suppose that $H \leq G$.

(1) *The* *identity* *of* H *is the same with that of* G.

$$e_H = e_G$$

(2) *The* *inversion* *of* a *in* H *is the same with that in* G.

$$\forall a \in H.\ a_H^{-1} = a_G^{-1}$$

$$e_H e_H = e_H = e_H e_G \implies e_H = e_G$$

Theorem

Suppose that $H \leq G$.

(1) *The* *identity* *of* H *is the same with that of* G.

$$e_H = e_G$$

(2) *The* *inversion* *of* a *in* H *is the same with that in* G.

$$\forall a \in H.\ a_H^{-1} = a_G^{-1}$$

$$e_H e_H = e_H = e_H e_G \implies e_H = e_G$$

$$a a_H^{-1} = e_H = e_G = a a_G^{-1} \implies a_H^{-1} = a^{-1}(G)$$

Theorem

Let G be a group and $\emptyset \neq H \subseteq G$. $H \leq G$ iff

$$\forall a, b \in H.\ ab^{-1} \in H.$$

Theorem

Let G be a group and $\emptyset \neq H \subseteq G$. $H \leq G$ iff

$$\forall a, b \in H.\ ab^{-1} \in H.$$

$$e = aa^{-1} \in H$$

Theorem

Let G be a group and $\emptyset \neq H \subseteq G$. $H \leq G$ iff

$$\forall a, b \in H.\ ab^{-1} \in H.$$

$$e = aa^{-1} \in H$$

$$a^{-1} = ea^{-1} \in H$$

Theorem

Let G be a group and $\emptyset \neq H \subseteq G$. $H \leq G$ iff

$$\forall a, b \in H.\ ab^{-1} \in H.$$

$$e = aa^{-1} \in H$$

$$a^{-1} = ea^{-1} \in H$$

$$ab = a(b^{-1})^{-1} \in H$$

Theorem

Suppose that $H_1 \le G, H_2 \le G$.

$$H_1 \cap H_2 \le G.$$

Theorem

Suppose that $H_1 \le G, H_2 \le G$.

$$H_1 \cap H_2 \le G.$$

$$H_1 = 2\mathbb{Z} \le \mathbb{Z} \qquad H_2 = 3\mathbb{Z} \le \mathbb{Z}$$

Theorem

Suppose that $H_1 \le G, H_2 \le G.$

$$H_1 \cap H_2 \le G.$$

$$H_1 = 2\mathbb{Z} \le \mathbb{Z} \qquad H_2 = 3\mathbb{Z} \le \mathbb{Z}$$

$$H_1 \cap H_2 = 6\mathbb{Z} \le \mathbb{Z}$$

Theorem

Suppose that $H_1 \le G, H_2 \le G$.

$$H_1 \cap H_2 \le G.$$

$$H_1 = 2\mathbb{Z} \le \mathbb{Z} \qquad H_2 = 3\mathbb{Z} \le \mathbb{Z}$$

$$H_1 \cap H_2 = 6\mathbb{Z} \le \mathbb{Z}$$

$$H_1 \cup H_2 ?$$

Definition (Symmetric Group (对称群; Sym(M)))

Let $M \neq \emptyset$ be a set.
All the permutations/bijective functions of M, together with the composition operation, is a group, called the symmetric group of M.

$$M = \{1, 2, \ldots, n\}$$

$$S_n \triangleq \mathrm{Sym}(M)$$

$$S_3$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$\sigma\tau \neq \tau\sigma$$

Cyclic Notation (轮换表示法) & Transposition (对换)

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 1 & 5 & 2 \end{pmatrix}$$

Cyclic Notation (轮换表示法) & Transposition (对换)

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 1 & 5 & 2 \end{pmatrix}$$

$$\sigma = (1\ 4)(2\ 3\ 6)(5)$$

Cyclic Notation (轮换表示法) & Transposition (对换)

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 1 & 5 & 2 \end{pmatrix}$$

$$\begin{aligned} \sigma &= (1\ 4)(2\ 3\ 6)(5) \\ &= (1\ 4)(2\ 3\ 6) \end{aligned}$$

Cyclic Notation (轮换表示法) & Transposition (对换)

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 1 & 5 & 2 \end{pmatrix}$$

$$\begin{aligned} \sigma &= (1\ 4)(2\ 3\ 6)(5) \\ &= (1\ 4)(2\ 3\ 6) \\ &= (2\ 3\ 6)(1\ 4) \end{aligned}$$

Cyclic Notation (轮换表示法) & Transposition (对换)

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 1 & 5 & 2 \end{pmatrix}$$

$$\begin{aligned} \sigma &= (1\ 4)(2\ 3\ 6)(5) \\ &= (1\ 4)(2\ 3\ 6) \\ &= (2\ 3\ 6)(1\ 4) \\ &= (2\ 3\ 6)(4\ 1) \end{aligned}$$

Cyclic Notation (轮换表示法) & Transposition (对换)

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 1 & 5 & 2 \end{pmatrix}$$

$$\begin{aligned}
\sigma &= (1\ 4)(2\ 3\ 6)(5) \\
&= (1\ 4)(2\ 3\ 6) \\
&= (2\ 3\ 6)(1\ 4) \\
&= (2\ 3\ 6)(4\ 1) \\
&= (3\ 6\ 2)(4\ 1)
\end{aligned}$$

Cyclic Notation (轮换表示法) & Transposition (对换)

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 1 & 5 & 2 \end{pmatrix}$$

$$\begin{aligned} \sigma &= (1\ 4)(2\ 3\ 6)(5) \\ &= (1\ 4)(2\ 3\ 6) \\ &= (2\ 3\ 6)(1\ 4) \\ &= (2\ 3\ 6)(4\ 1) \\ &= (3\ 6\ 2)(4\ 1) \\ &= (3\ 6)(6\ 2)(4\ 1) \end{aligned}$$

$$S_3$$

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

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

S_3

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

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

$$(1) \quad (1\ 2) \quad (1\ 3) \quad (2\ 3) \quad (1\ 2\ 3) \quad (1\ 3\ 2)$$

Definition (Permutation Group (置换群))

Let $M \neq \emptyset$ be a set.
A permutation group of M is a subgroup of $\mathrm{Sym}(M)$.

Definition (Permutation Group (置换群))

Let $M \neq \emptyset$ be a set.
A permutation group of M is a subgroup of $\mathrm{Sym}(M)$.

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

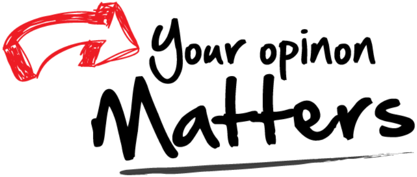
Definition (Permutation Group (置换群))

Let $M \neq \emptyset$ be a set.
A permutation group of M is a subgroup of $\mathrm{Sym}(M)$.

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

$$H = \{(1), (1\ 2)\} \leq S_3$$


Thank You!



Office 302

Mailbox: H016

hfwei@nju.edu.cn