(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).

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

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

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

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 $H \le G$.

(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.

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

$$e_H e_H = e_H = e_H e_G$$

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 $H \le G$.

(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.

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

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

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

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 $H_1 \leq G, H_2 \leq G.$

$$H_1 \cap H_2 \leq G.$$

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)

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

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

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

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)

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

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

$$S_3$$

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

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

$$S_3$$

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

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

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

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 $\mathrm{Sym}(M)$.

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

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

Definition (Permutation Group (置换群))

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

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

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

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

Definition (Coset (陪集))

Suppose that $H \leq G$. For $a \in G$,

$$aH = \{ah \mid h \in H\}, \quad Ha = \{ha \mid h \in H\},$$

is called the left coset (左陪集) and right coset of H in G, respectively.

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

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

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

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

$$(1)H = H = (1\ 2)H \leq S_3$$

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

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

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

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

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

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

$$(1)H = (1\ 2\ 3)H = (1\ 3\ 2)H = H \le S_3$$

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

Theorem

Suppose that $H \le G$, $a, b \in G$.

(1)

$$|aH| = |H| = |bH|$$

(2)

$$a \in aH$$

(3)

$$aH = H \iff a \in H \iff aH \le G$$

(4)

$$aH = bH \iff a^{-1}b \in H$$

(5)

$$\forall a, b \in G.\ (aH = bH) \vee (aH \cap bH = \emptyset)$$

$$aH = bH \iff a^{-1}b \in H$$

$$aH = bH \iff a^{-1}b \in H$$

$$\boxed{a^{-1}b \in H \iff a^{-1}bH = H}$$

$$aH = bH \iff a^{-1}b \in H$$

$$\boxed{a^{-1}b \in H \iff a^{-1}bH = H}$$

$$aH = bH \implies a^{-1}aH = a^{-1}bH \implies a^{-1}bH = H \implies a^{-1}b \in H$$

$$aH = bH \iff a^{-1}b \in H$$

$$\boxed{a^{-1}b \in H \iff a^{-1}bH = H}$$

$$aH = bH \implies a^{-1}aH = a^{-1}bH \implies a^{-1}bH = H \implies a^{-1}b \in H$$

$$a^{-1}bH = H \implies a(a^{-1}bH) = aH \implies bH = aH$$

$$\forall a, b \in G.\ (aH = bH) \vee (aH \cap bH = \emptyset)$$

$$\forall a, b \in G.\ (aH = bH) \lor (aH \cap bH = \emptyset)$$

$$\forall a, b \in G.\ (aH \cap bH \neq \emptyset \to aH = bH)$$

$$\forall a, b \in G.\ (aH = bH) \vee (aH \cap bH = \emptyset)$$

$$\forall a, b \in G.\ (aH \cap bH \neq \emptyset \to aH = bH)$$

Take any $g \in aH \cap bH$.

$$\forall a, b \in G.\ (aH = bH) \vee (aH \cap bH = \emptyset)$$

$$\forall a, b \in G.\ (aH \cap bH \neq \emptyset \to aH = bH)$$

Take any $g \in aH \cap bH$.

$$\exists h_1, h_2 \in H.\ (ah_1 = g = ah_2) \wedge (h_1 H = H = h_2 H)$$

$$\forall a, b \in G. \ (aH = bH) \lor (aH \cap bH = \emptyset)$$

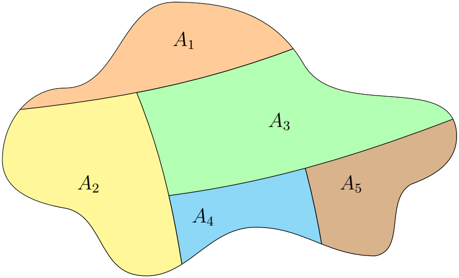
$$\forall a, b \in G. \ (aH \cap bH \neq \emptyset \to aH = bH)$$

Take any $g \in aH \cap bH$.

$$\exists h_1, h_2 \in H. \ (ah_1 = g = ah_2) \land (h_1 H = H = h_2 H)$$

$$aH = a(h_1 H) = (ah_1)H = (bh_2)H = b(h_2 H) = bH$$

A balanced partition of G by its subgraph H



Theorem (Lagrange's Theorem)

Suppose that $H \le G$. Then

$$|G| = [G : H] \cdot |H|$$

Definition (Index (指标))

$$G/H = \{gH \mid g \in G\}$$

$$[G : H] \triangleq |G/H|$$

$$H \leq G \implies |H| \mid |G|$$

$$H \leq G \implies |H| \mid |G|$$

There are *no* subgraphs of order 5, 7, or 8 of a group of order 12.

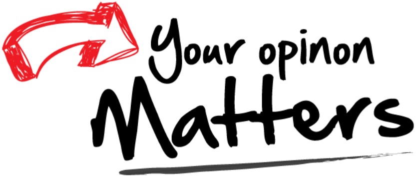
$$H \leq G \implies |H| \mid |G|$$

There are *no* subgraphs of order 5, 7, or 8 of a group of order 12.

Theorem

- *There are only 2 groups of order 4.*
- *There are only 2 groups of order 6.*


Thank
You!



Office 302

Mailbox: H016

hfwei@nju.edu.cn