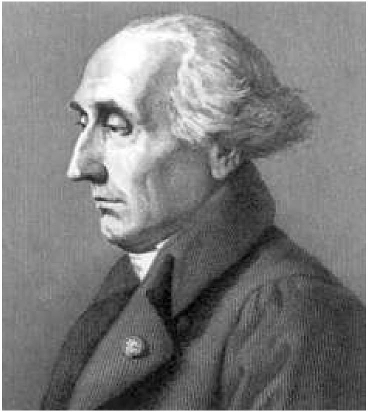
(十四) 群论：子群 (Subgroup)

魏恒峰

hfwei@nju.edu.cn

2021 年 06 月 10 日

Lagrange's Theorem



Joseph-Louis Lagrange ($1736 \sim 1813$)

Fundamental Homomorphism Theorem

Emmy Noether $(1882 \sim 1935)$

Lagrange's Theorem

Help us understand the structure of a group
via its subgroups/normal subgroups

Fundamental Homomorphism Theorem

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 $H \leq G$.

$$(m\mathbb{Z}, +) \leq (\mathbb{Z}, +)$$

$$(m\mathbb{Z}, +) \le (\mathbb{Z}, +)$$

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

Theorem

Suppose that $H \le G$.

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

$$e = e'$$

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

$$a_H^{-1} = a_G^{-1}$$

Theorem

Suppose that $H \leq G$.

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

$$e = e'$$

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

$$a_H^{-1} = a_G^{-1}$$

$$ee = e = ee' \implies e = e'$$

Theorem

Suppose that $H \leq G$.

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

$$e = e'$$

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

$$a_H^{-1} = a_G^{-1}$$

$$ee = e = ee' \implies e = e'$$

$$aa_H^{-1} = e_H = e_G = aa_G^{-1} \implies a_H^{-1} = a_G^{-1}$$

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

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

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

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

Theorem

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

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

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

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

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

Theorem

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

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

Theorem

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

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

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

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

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

Let $M \neq \emptyset$ be a set.

All the permutations/bijections of M, together with the composition operation, is a group, called the symmetric group of M.

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

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

$$S_3$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

S_3

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

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

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

Definition (Permutation Group (置换群))

Let $M \neq \emptyset$ be a set.

A permutation group of M is a subgroup of $\mathrm{Sym}(M)$.

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.

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

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

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

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

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

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

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

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

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

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

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

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

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

Theorem

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

(1)

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

(2)

$$a \in aH$$

(3)

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

(4)

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

(5)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

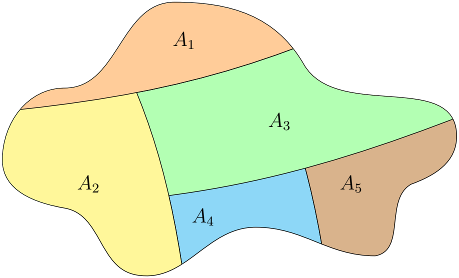
$$\forall a, b \in G.\ (aH \cap bH \neq \emptyset \to aH = bH)$$

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.*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

It is possible that $aH \neq Ha$.

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

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

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

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

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

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

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

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

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

$$\forall a \in S_3.\ aH = Ha$$

Definition (Normal Subgroup (正规子群))

Suppose that $H \leq G$. If

$$\forall a \in G.\ aH = Ha,$$

then H is a normal subgroup of G, denoted $H \lhd G$.

Definition (Normal Subgroup (正规子群))

Suppose that $H \leq G$. If

$$\forall a \in G.\ aH = Ha,$$

then H is a normal subgroup of G, denoted $H \lhd G$.

$$aH = Ha \not\Longrightarrow \forall h \in H.\ ah = ha$$

Definition (Normal Subgroup (正规子群))

Suppose that $H \le G$. If

$$\forall a \in G.\ aH = Ha,$$

then H is a normal subgroup of G, denoted $H \lhd G$.

$$aH = Ha \not\Longrightarrow \forall h \in H.\ ah = ha$$

$$aH = Ha \Longrightarrow \forall h \in H.\ \exists h' \in H.\ ah = h'a$$

Theorem

$$H \lhd G \iff \forall a \in G, h \in H.\ aha^{-1} \in H$$

Theorem

$$H \triangleleft G \iff \forall a \in G, h \in H.\ aha^{-1} \in H$$

$$\begin{aligned} aH = Ha &\implies aHa^{-1} = (Ha)a^{-1} = H(aa^{-1}) = H \\ &\implies aHa^{-1} \subseteq H \\ &\implies \forall h \in H.\ aha^{-1} \in H \end{aligned}$$

Theorem

$$H \lhd G \iff \forall a \in G, h \in H.\ aha^{-1} \in H$$

$$\begin{aligned} aH = Ha &\implies aHa^{-1} = (Ha)a^{-1} = H(aa^{-1}) = H \\ &\implies aHa^{-1} \subseteq H \\ &\implies \forall h \in H.\ aha^{-1} \in H \end{aligned}$$

$$aha^{-1} \in H \implies ah = (aha^{-1})a \in Ha \implies aH \subseteq Ha$$

Theorem

$$H \lhd G \iff \forall a \in G, h \in H.\ aha^{-1} \in H$$

$$\begin{aligned} aH = Ha &\implies aHa^{-1} = (Ha)a^{-1} = H(aa^{-1}) = H \\ &\implies aHa^{-1} \subseteq H \\ &\implies \forall h \in H.\ aha^{-1} \in H \end{aligned}$$

$$aha^{-1} \in H \implies ah = (aha^{-1})a \in Ha \implies aH \subseteq Ha$$

$$a^{-1}ha = a^{-1}h(a^{-1})^{-1} \in H \implies ha \in aH \implies Ha \subseteq aH$$

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

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

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

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

$$\forall \sigma \in S_3, \tau \in H.\ \sigma\tau\sigma^{-1} \in H$$

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

$$\forall \sigma \in S_3, \tau \in H.\ \sigma\tau\sigma^{-1} \in H$$

Theorem

$$\sigma\tau\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \dots & \sigma(\tau(n)) \end{pmatrix}$$

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

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

$$\forall \sigma \in S_3, \tau \in H.\ \sigma\tau\sigma^{-1} \in H$$

Theorem

$$\sigma\tau\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \dots & \sigma(\tau(n)) \end{pmatrix}$$

$$(1\ 2)(1\ 2\ 3)(1\ 2)^{-1} = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (1\ 3\ 2)$$

Definition (正规子群的陪集)

Suppose that $H \lhd G$.

$$G/H = \{aH \mid a \in G\}$$

is the set of cosets of H in G.

Definition (Quotient Group (商群))

Suppose that $H \triangleleft G$. Define

$$aH \cdot bH = (ab)H.$$

Then $(G/H, \cdot)$ is a group, called the quotient group of G by H (denoted G/H).

$aH \cdot bH = (ab)H$ is well-defined

$$aH \cdot bH = (ab)H \text{ is well-defined}$$

$$aH = a'H \land bH = b'H \implies aH \cdot bH = a'H \cdot b'H$$

结果与代表元的选取无关

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

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

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

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

$$G/H = \{(1)H, (1\ 2)H\}$$

$$G = \mathbb{Z} \qquad H = 6\mathbb{Z} \lhd G$$

$$G/H =$$

$$G = \mathbb{Z} \qquad H = 6\mathbb{Z} \lhd G$$

$$G/H = \{0 + H, 1 + H, \ldots, 5 + H\}$$

Definition (Homomorphism (同态))

Let $(G, \cdot)$ and $(G', *)$ be two groups. Let ϕ be a function such that

$$\forall a, b \in G.\ \phi(ab) = \phi(a)\phi(b).$$

Then ϕ is a homomorphism from G to G'.

Definition (Homomorphism (同态))

Let $(G, \cdot)$ and $(G', *)$ be two groups. Let ϕ be a function such that

$$\forall a, b \in G.\ \phi(ab) = \phi(a)\phi(b).$$

Then ϕ is a homomorphism from G to G'.

If ϕ is a bijection, then G and G' are called isomorphic.

$$\phi : G \cong G'$$

$$\begin{aligned} \phi : \mathbb{Z} &\to \mathbb{R}^* \\ n &\mapsto (-1)^n \end{aligned}$$

$$\begin{aligned}\phi : \mathbb{Z} &\to \mathbb{R}^* \\ n &\mapsto (-1)^n\end{aligned}$$

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

$$\begin{aligned}\phi : \mathbb{Z} &\to \mathbb{Z}_6 \\ a &\mapsto [a]_6\end{aligned}$$

$$\phi(a+b) = [a+b]_6 = \phi(a) + \phi(b)$$

$$\begin{aligned}\phi : \mathbb{R}[x] &\to \mathbb{R}[x] \\ f(x) &\mapsto f'(x)\end{aligned}$$

$\mathbb{R}[x]$: 全体实系数多项式关于多项式的加法构成的群

$$\phi(f(x) + g(x)) = (f(x) + g(x))' = \phi(f(x)) + \phi(g(x))$$

Theorem

Suppose that ϕ is a homomorphism from G to G'.
Let e and e' are identities of G and G', respectively.

(1) $\phi(e) = e'$

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

Theorem

Suppose that ϕ *is a homomorphism from* G *to* G'.
Let e *and* e' *are identities of* G *and* G', *respectively.*

(1) $\phi(e) = e'$

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

$$e'\phi(e) = \phi(e) = \phi(ee) = \phi(e)\phi(e) \implies \phi(e) = e'$$

Theorem

Suppose that ϕ is a homomorphism from G to G'.
Let e and e' are identities of G and G', respectively.

(1) $\phi(e) = e'$

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

$$e'\phi(e) = \phi(e) = \phi(ee) = \phi(e)\phi(e) \implies \phi(e) = e'$$

$$\phi(a)\phi(a^{-1}) = \phi(aa^{-1}) = \phi(e) = e' = \phi(a)(\phi(a))^{-1}$$

Theorem

Suppose that ϕ is a homomorphism from G to G'.

(1)

$$H \leq G \implies \phi(H) \leq G'$$

(2)

$$H \triangleleft G \implies \phi(H) \triangleleft G'$$

Theorem

Suppose that ϕ is a homomorphism from G to G'.

(1)

$$H \le G \implies \phi(H) \le G'$$

(2)

$$H \lhd G \implies \phi(H) \lhd G'$$

(3)

$$K \le G' \implies \phi^{-1}(K) \le G$$

(4)

$$K \lhd G' \implies \phi^{-1}(K) \lhd G$$

Definition (核 (Kernel))

Suppose that ϕ is a homomorphism from G to G'.
Let e' be the identity of G'.

$$\phi^{-1}(\{e'\}) = \{a \in G \mid \phi(a) = e'\}$$

is the kernel of ϕ, denoted Ker ϕ.

Definition (核 (Kernel))

Suppose that ϕ is a homomorphism from G to G'.
Let e' be the identity of G'.

$$\phi^{-1}(\{e'\}) = \{a \in G \mid \phi(a) = e'\}$$

is the kernel of ϕ, denoted Ker ϕ.

$$\text{Ker } \phi \lhd G$$

$$\begin{aligned}\phi : \mathbb{Z} &\to \mathbb{R}^* \\ n &\mapsto (-1)^n\end{aligned}$$

$$\text{Ker } \phi =$$

$$\begin{aligned}\phi : \mathbb{Z} &\to \mathbb{R}^* \\ n &\mapsto (-1)^n\end{aligned}$$

$$\text{Ker } \phi = 2\mathbb{Z}$$

$$\phi : \mathbb{Z} \to \mathbb{Z}_6$$

$$a \mapsto [a]_6$$

$$\text{Ker } \phi =$$

$$\phi : \mathbb{Z} \to \mathbb{Z}_6$$
$$a \mapsto [a]_6$$

$$\mathrm{Ker}\ \phi = 6\mathbb{Z}$$

$$
\begin{aligned}
\phi : \mathbb{R}[x] &\to \mathbb{R}[x] \\
f(x) &\mapsto f'(x)
\end{aligned}
$$

$\mathbb{R}[x]$：全体实系数多项式关于多项式的加法构成的群

$$\mathrm{Ker}\ \phi =$$

$$\begin{aligned}\phi : \mathbb{R}[x] &\to \mathbb{R}[x] \\ f(x) &\mapsto f'(x)\end{aligned}$$

$\mathbb{R}[x]$：全体实系数多项式关于多项式的加法构成的群

$$\text{Ker } \phi = \mathbb{R}$$

Theorem (Fundamental Homomorphism Theorem)

Suppose that ϕ is a homomorphism from G to G'. Then

$$G/Ker\,\phi \cong \phi(G).$$

Theorem (Fundamental Homomorphism Theorem)

Suppose that ϕ is a homomorphism from G to G'. Then

$$G/Ker\,\phi \cong \phi(G).$$

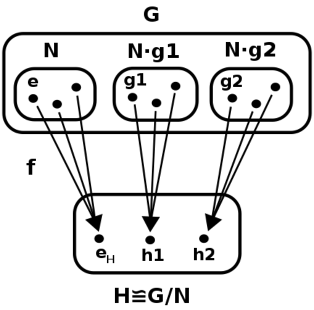
同态核可以看作群 G 与其同态像 $\phi(G)$ 之间相似程度的一种度量

Theorem (Fundamental Homomorphism Theorem)

Suppose that ϕ is a homomorphism from G to G'. Then

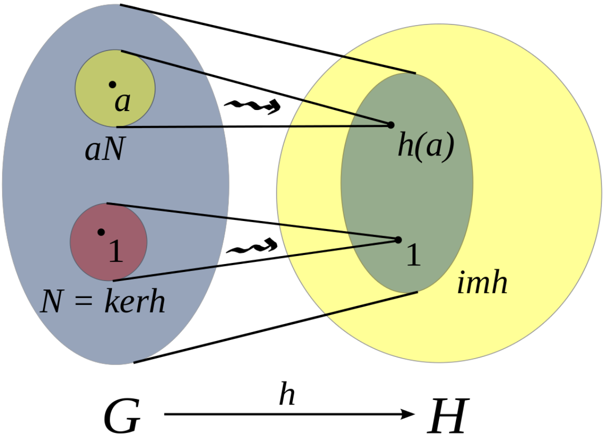
$$G/Ker\,\phi \cong \phi(G).$$

同态核可以看作群 G 与其同态像 $\phi(G)$ 之间相似程度的一种度量



$$N = \text{Ker}\ \phi$$

$$G/(N \triangleq \mathrm{Ker}\ h) \cong (h(G) \triangleq \mathrm{im}\ h)$$



$$aN \mapsto h(a)$$

$$\phi : \mathbb{Z} \to \mathbb{R}^*$$
$$n \mapsto (-1)^n$$

$$\text{Ker } \phi = 2\mathbb{Z}$$

$$\phi : \mathbb{Z} \to \mathbb{R}^*$$
$$n \mapsto (-1)^n$$

$$\text{Ker } \phi = 2\mathbb{Z}$$

$$\mathbb{Z}/(2\mathbb{Z}) = (2\mathbb{Z}, 2\mathbb{Z}+1) \cong \phi(\mathbb{Z}) = (-1, 1)$$

$$\phi : \mathbb{Z} \to \mathbb{Z}_6$$
$$a \mapsto [a]_6$$

$$\text{Ker } \phi = 6\mathbb{Z}$$

$$\phi : \mathbb{Z} \to \mathbb{Z}_6$$
$$a \mapsto [a]_6$$

$$\text{Ker } \phi = 6\mathbb{Z}$$

$$\mathbb{Z}/(6\mathbb{Z}) = \{0 + H, 1 + H, \ldots, 5 + H\} \cong \phi(\mathbb{Z}) = \mathbb{Z}_6$$

$$\begin{aligned} \phi : \mathbb{R}[x] &\to \mathbb{R}[x] \\ f(x) &\mapsto f'(x) \end{aligned}$$

$\mathbb{R}[x]$: 全体实系数多项式关于多项式的加法构成的群

$$\text{Ker}\ \phi = \mathbb{R}$$

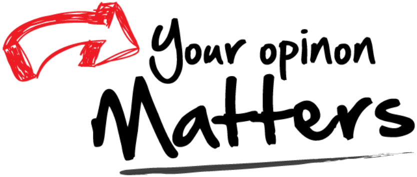
$$\begin{aligned} \phi : \mathbb{R}[x] &\to \mathbb{R}[x] \\ f(x) &\mapsto f'(x) \end{aligned}$$

$\mathbb{R}[x]$：全体实系数多项式关于多项式的加法构成的群

$$\text{Ker } \phi = \mathbb{R}$$

$$\mathbb{R}[x]/\mathbb{R} \cong \phi(\mathbb{R}[x]) = \mathbb{R}[x]$$


Thank
You!



Office 302

Mailbox: H016

hfwei@nju.edu.cn