(十三) 群论: 群的基本概念 (What are Groups?)

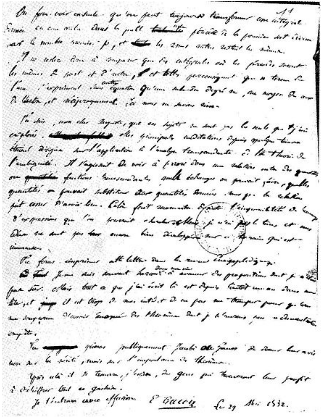
魏恒峰

hfwei@nju.edu.cn

2021 年 06 月 03 日

“这里需要补充说明，可是我没有时间了！”

Évariste Galois
(伽罗瓦; 1811 ∼ 1832)



May 29, 1832

“论五次方程的代数解法问题” (1929)

“论五次方程的代数解法问题” (1929)

Augustin-Louis Cauchy
$(1789 \sim 1857)$

“论五次方程的代数解法问题” (1929)

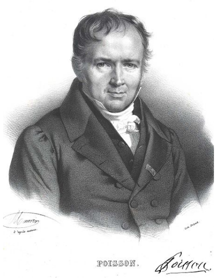
Augustin-Louis Cauchy
($1789 \sim 1857$)

Joseph Fourier
($1768 \sim 1830$)

“论五次方程的代数解法问题” (1929)

Augustin-Louis Cauchy
(1789 ∼ 1857)

Joseph Fourier
(1768 ∼ 1830)



Siméon Denis Poisson
(1781 ∼ 1840)

"Ask Jacobi or Gauss publicly to give their opinion,

not as to the truth, but as to the importance of these theorems."

“Is there a formula for the roots of a ≥ 5 degree polynomial equation

in terms of its coefficients, using only $+, -, \times, \div, \sqrt[r]{\ }$?

$$x^3 + px + q = 0$$

$$x_1 = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

$$x_2 = \omega\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \omega^2\sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

$$x_3 = \omega^2\sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \omega\sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}$$

其中$\omega = \frac{-1+\sqrt{3}i}{2}$。

Girolamo Cardano
(1501 ~ 21/09/1576)

对于一元四次方程

$$ax^4 + bx^3 + cx^2 + dx + e = 0$$

记

$$\begin{cases} \Delta_1 = c^2 - 3bd + 12ae \\ \Delta_2 = 2c^3 - 9bcd + 27ad^2 + 27b^2e - 72ace \end{cases}$$

并记

$$\Delta = \frac{\sqrt[3]{2}\Delta_1}{3a\sqrt[3]{\Delta_2 + \sqrt{-4\Delta_1^3 + \Delta_2^2}}} + \frac{\sqrt[3]{\Delta_2 + \sqrt{-4\Delta_1^3 + \Delta_2^2}}}{3\sqrt[3]{2}a}$$

则有

$$\begin{cases}
x_1 = -\dfrac{b}{4a} - \dfrac{1}{2}\sqrt{\dfrac{b^2}{4a^2} - \dfrac{2c}{3a} + \Delta} - \dfrac{1}{2}\sqrt{\dfrac{b^2}{2a^2} - \dfrac{4c}{3a} - \Delta - \dfrac{-\dfrac{b^3}{a^3} + \dfrac{4bc}{a^2} - \dfrac{8d}{a}}{4\sqrt{\dfrac{b^2}{4a^2} - \dfrac{2c}{3a} + \Delta}}} \\
x_2 = -\dfrac{b}{4a} - \dfrac{1}{2}\sqrt{\dfrac{b^2}{4a^2} - \dfrac{2c}{3a} + \Delta} + \dfrac{1}{2}\sqrt{\dfrac{b^2}{2a^2} - \dfrac{4c}{3a} - \Delta - \dfrac{-\dfrac{b^3}{a^3} + \dfrac{4bc}{a^2} - \dfrac{8d}{a}}{4\sqrt{\dfrac{b^2}{4a^2} - \dfrac{2c}{3a} + \Delta}}} \\
x_3 = -\dfrac{b}{4a} + \dfrac{1}{2}\sqrt{\dfrac{b^2}{4a^2} - \dfrac{2c}{3a} + \Delta} - \dfrac{1}{2}\sqrt{\dfrac{b^2}{2a^2} - \dfrac{4c}{3a} - \Delta + \dfrac{-\dfrac{b^3}{a^3} + \dfrac{4bc}{a^2} - \dfrac{8d}{a}}{4\sqrt{\dfrac{b^2}{4a^2} - \dfrac{2c}{3a} + \Delta}}} \\
x_4 = -\dfrac{b}{4a} + \dfrac{1}{2}\sqrt{\dfrac{b^2}{4a^2} - \dfrac{2c}{3a} + \Delta} + \dfrac{1}{2}\sqrt{\dfrac{b^2}{2a^2} - \dfrac{4c}{3a} - \Delta + \dfrac{-\dfrac{b^3}{a^3} + \dfrac{4bc}{a^2} - \dfrac{8d}{a}}{4\sqrt{\dfrac{b^2}{4a^2} - \dfrac{2c}{3a} + \Delta}}}
\end{cases}$$

Theorem (Abel-Ruffini Thoerem)

There is no solution in radicals to polynomial equations of ≥ 5 *degree.*

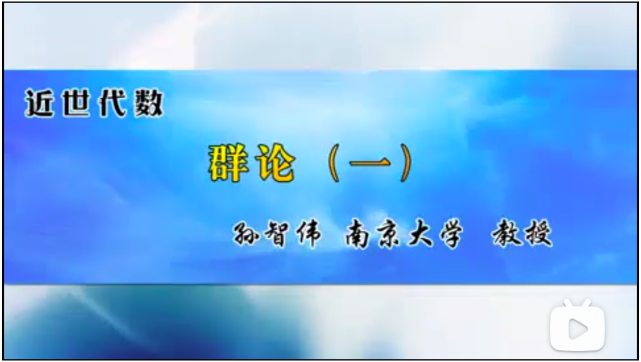
Theorem (Abel-Ruffini Thoerem)

There is no solution in radicals to polynomial equations of ≥ 5 degree.

Niels Henrik Abel (1802 ~ 1929)

Theorem (Galois Theorem)

An equation is solvable in terms of radicals iff the Galois group of its splitting field is solvable.



https://www.bilibili.com/video/BV1Ex411k7wk?share_source=copy_web

"我看出了 *Galois* 用来证明这个美妙定理的方法是完全正确的。在那个瞬间，我体验到一种强烈的愉悦。"

— *J. Liouville (刘维尔; 1846)*

Definition (Group (群))

A group $(G, *)$ is a set G together with a binary operation $*$ such that the following four group axioms are satisfied:

Definition (Group (群))

A group $(G, *)$ is a set G together with a binary operation $*$ such that the following four group axioms are satisfied:

Closure (封闭):

$$\forall a, b \in G.\ a * b \in G$$

Definition (Group (群))

A group $(G, *)$ is a set G together with a binary operation $*$ such that the following four group axioms are satisfied:

Closure (封闭):

$$\forall a, b \in G.\ a * b \in G$$

Associativity (结合律):

$$\forall a, b, c \in G.\ (a * b) * c = a * (b * c)$$

Definition (Group (群))

A group $(G, *)$ is a set G together with a binary operation $*$ such that the following four group axioms are satisfied:

Closure (封闭):

$$\forall a, b \in G.\ a * b \in G$$

Associativity (结合律):

$$\forall a, b, c \in G.\ (a * b) * c = a * (b * c)$$

Identity (单位元):

$$\exists e \in G.\ \forall a \in G.\ e * a = a * e = a$$

Definition (Group (群))

A group $(G, *)$ is a set G together with a binary operation $*$ such that the following four group axioms are satisfied:

Closure (封闭):

$$\forall a, b \in G.\ a * b \in G$$

Associativity (结合律):

$$\forall a, b, c \in G.\ (a * b) * c = a * (b * c)$$

Identity (单位元):

$$\exists e \in G.\ \forall a \in G.\ e * a = a * e = a$$

Inverse (逆元): Let e be the identity of G.

$$\forall a \in G.\ \exists b \in G.\ a * b = b * a = e$$

The inverse of a is denoted a^{-1}.

$$\forall n \in \mathbb{Z}^+ .\ a^n \triangleq \underbrace{a * a * \cdots * a}_{\# = n}$$

$$a^0 \triangleq e$$

$$a^{-n} \triangleq (a^{-1})^n$$

Definition (Commutative Group (交换群); Abelian Group (阿贝尔群))

Let $(G, *)$ be a group. If $*$ is commutative,

$$\forall a, b \in G.\ a * b = b * a,$$

then $(G, *)$ is a commutative group.

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

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

$$(\mathbb{Q} \setminus \{0\}, \times)$$

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

$$(\mathbb{Q} \setminus \{0\}, \times)$$

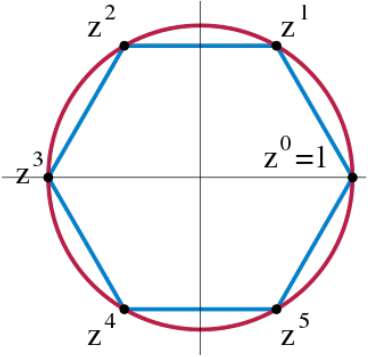
$$(1, -1, \mathbf{i}, -\mathbf{i})$$

Group of n-th Roots of Unity (n 次单位根群)

$$
\begin{aligned}
U_n &= \{z \in \mathbb{C} \mid z^n = 1\} \\
&= \{\cos \frac{2k\pi}{n} + \mathbf{i} \sin \frac{2k\pi}{n} \mid k = 0, 1, \ldots, n-1\}
\end{aligned}
$$

Group of n-th Roots of Unity (n 次单位根群)

$$
\begin{aligned}
U_n &= \{z \in \mathbb{C} \mid z^n = 1\} \\
&= \{\cos \frac{2k\pi}{n} + \mathbf{i} \sin \frac{2k\pi}{n} \mid k = 0, 1, \ldots, n-1\}
\end{aligned}
$$



Quaternion Group (四元数群)

$$(1, i, j, k, -1, -i, -j, -k)$$

×	e	$\bar{e}$	i	$\bar{i}$	j	$\bar{j}$	k	$\bar{k}$
e	e	$\bar{e}$	i	$\bar{i}$	j	$\bar{j}$	k	$\bar{k}$
$\bar{e}$	$\bar{e}$	e	$\bar{i}$	i	$\bar{j}$	j	$\bar{k}$	k
i	i	$\bar{i}$	$\bar{e}$	e	k	$\bar{k}$	$\bar{j}$	j
$\bar{i}$	$\bar{i}$	i	e	$\bar{e}$	$\bar{k}$	k	j	$\bar{j}$
j	j	$\bar{j}$	$\bar{k}$	k	$\bar{e}$	e	i	$\bar{i}$
$\bar{j}$	$\bar{j}$	j	k	$\bar{k}$	e	$\bar{e}$	$\bar{i}$	i
k	k	$\bar{k}$	j	$\bar{j}$	$\bar{i}$	i	$\bar{e}$	e
$\bar{k}$	$\bar{k}$	k	$\bar{j}$	j	i	$\bar{i}$	e	$\bar{e}$

Cayley Table

$$i^2 = j^2 = k^2 = 1 \qquad ij = k, ji = -k, jk = i, kj = -i, ki = j, ik = -j$$

Theorem

Let G be a group.

(1) *The identity is unique.*

Theorem

Let G be a group.

(1) *The identity is unique.*

(2) *The inverse of each element is unique.*

Theorem

Let G be a group.

(1) *The identity is unique.*

(2) *The inverse of each element is unique.*

(3) $\forall a \in G.\ (a^{-1})^{-1} = a.$

Theorem

Let G be a group.

(1) *The identity is unique.*

(2) *The inverse of each element is unique.*

(3) $\forall a \in G.\ (a^{-1})^{-1} = a.$

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

Theorem

Let G be a group.

(1) *The identity is unique.*

(2) *The inverse of each element is unique.*

(3) $\forall a \in G.\ (a^{-1})^{-1} = a.$

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

(5) $\forall a, b, c \in G.\ (ab = ac \implies b = c) \land (ba = ca \implies b = c).$

Theorem

Let G be a group.

(1) *The identity is unique.*

(2) *The inverse of each element is unique.*

(3) $\forall a \in G.\ (a^{-1})^{-1} = a.$

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

(5) $\forall a, b, c \in G.\ (ab = ac \implies b = c) \land (ba = ca \implies b = c).$

(6) $\forall a, b \in G.\ \exists!\ x \in G.\ ax = b \land ya = b.$

Additive Group of Integers Modulo m (模 m 剩余类加群)

$$(\mathbb{Z}_m = \{0, 1, \ldots, m-1\}, +_m)$$

Additive Group of Integers Modulo m (模 m 剩余类加群)

$$(\mathbb{Z}_m = \{0, 1, \ldots, m-1\}, +_m)$$

$$(\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}, \times_6)$$

Multiplicative Group of Integers Modulo m (模 m 剩余类乘法群)

$$U(m) = \{a \in \mathbb{Z}_m \mid (a, m) = 1\}$$

Multiplicative Group of Integers Modulo m (模 m 剩余类乘法群)

$$U(m) = \{a \in \mathbb{Z}_m \mid (a, m) = 1\}$$

Theorem (Bézout's Identity)

$$(a, b) = d \implies \exists u, v \in \mathbb{Z}.\ au + bv = d$$

Multiplicative Group of Integers Modulo m (模 m 剩余类乘法群)

$$U(m) = \{a \in \mathbb{Z}_m \mid (a, m) = 1\}$$

Theorem (Bézout's Identity)

$$(a, b) = d \implies \exists u, v \in \mathbb{Z}.\ au + bv = d$$

$$(a, m) = 1 \implies \exists u, v \in \mathbb{Z}.\ au + mv = 1$$

Multiplicative Group of Integers Modulo m (模 m 剩余类乘法群)

$$U(m) = \{a \in \mathbb{Z}_m \mid (a, m) = 1\}$$

Theorem (Bézout's Identity)

$$(a, b) = d \implies \exists u, v \in \mathbb{Z}.\ au + bv = d$$

$$(a, m) = 1 \implies \exists u, v \in \mathbb{Z}.\ au + mv = 1$$

$$a^{-1} = u$$

Multiplicative Group of Integers Modulo m (模 m 剩余类乘法群)

$$U(m) = \{a \in \mathbb{Z}_m \mid (a, m) = 1\}$$

Theorem (Bézout's Identity)

$$(a, b) = d \implies \exists u, v \in \mathbb{Z}.\ au + bv = d$$

$$(a, m) = 1 \implies \exists u, v \in \mathbb{Z}.\ au + mv = 1$$

$$a^{-1} = u$$

$$(u, m) = 1$$

Multiplicative Group of Integers Modulo m (模 m 剩余类乘法群)

$$U(m) = \{a \in \mathbb{Z}_m \mid (a, m) = 1\}$$

Theorem (Bézout's Identity)

$$(a, b) = d \implies \exists u, v \in \mathbb{Z}.\ au + bv = d$$

$$(a, m) = 1 \implies \exists u, v \in \mathbb{Z}.\ au + mv = 1$$

$$a^{-1} = u$$

$$(u, m) = 1 \qquad ua = au = au + mv = 1 \pmod m$$

When p is a prime,

$$\mathbb{Z}_p^* \triangleq U(p) = \{1, 2, \ldots, p-1\}$$

Multiplicative Group of Integers Modulo m (模 m 剩余类乘法群)

$$U(m) = \{a \in \mathbb{Z}_m \mid (a, m) = 1\}$$

Multiplicative Group of Integers Modulo m (模 m 剩余类乘法群)

$$U(m) = \{a \in \mathbb{Z}_m \mid (a, m) = 1\}$$

$$\big|U(m)\big| = \varphi(m)$$

Multiplicative Group of Integers Modulo m (模 m 剩余类乘法群)

$$U(m) = \{a \in \mathbb{Z}_m \mid (a, m) = 1\}$$

$$|U(m)| = \varphi(m)$$

Definition (Euler's Totient Function (1763))

$$\varphi(m) = n \prod_{p \mid n \,\land\, p \text{is a prime}} \left(1 - \frac{1}{p}\right)$$

Multiplicative Group of Integers Modulo m (模 m 剩余类乘法群)

$$U(m) = \{a \in \mathbb{Z}_m \mid (a, m) = 1\}$$

$$\big|U(m)\big| = \varphi(m)$$

Definition (Euler's Totient Function (1763))

$$\varphi(m) = n \prod_{p \mid n \,\land\, p \text{is a prime}} \left(1 - \frac{1}{p}\right)$$

$$\varphi(20) = 20(1 - \frac{1}{2})(1 - \frac{1}{5}) = 8$$

Multiplicative Group of Integers Modulo m (模 m 剩余类乘法群)

$$U(m) = \{a \in \mathbb{Z}_m \mid (a, m) = 1\}$$

$$\big|U(m)\big| = \varphi(m)$$

Definition (Euler's Totient Function (1763))

$$\varphi(m) = n \prod_{p \mid n \,\land\, p \text{is a prime}} \left(1 - \frac{1}{p}\right)$$

$$\varphi(20) = 20(1 - \frac{1}{2})(1 - \frac{1}{5}) = 8$$

$$U(20) = \{1, 3, 7, 9, 11, 13, 17, 19\}$$

Theorem

Let G be an abelian group of order n.

$$\forall a \in G.\ a^n = e.$$

Theorem

Let G be an abelian group of order n.

$$\forall a \in G.\ a^n = e.$$

$$G = \{a_1, a_2, \ldots, a_n\}$$

Theorem

Let G be an abelian group of order n.

$$\forall a \in G.\ a^n = e.$$

$$G = \{a_1, a_2, \ldots, a_n\}$$

$$aG \triangleq \{aa_1, aa_2, \ldots, aa_n\} = G$$

Theorem

Let G be an abelian group of order n.

$$\forall a \in G.\ a^n = e.$$

$$G = \{a_1, a_2, \ldots, a_n\}$$

$$aG \triangleq \{aa_1, aa_2, \ldots, aa_n\} = G$$

$$\prod_{i=1}^{n} (aa_i) = a_1 \ldots a_n$$

Theorem

Let G be an abelian group of order n.

$$\forall a \in G.\ a^n = e.$$

$$G = \{a_1, a_2, \dots, a_n\}$$

$$aG \triangleq \{aa_1, aa_2, \dots, aa_n\} = G$$

$$\prod_{i=1}^{n} (aa_i) = a_1 \dots a_n$$

$$a^n a_1 \dots a_n = a_1 \dots a_n$$

Theorem

Let G be an abelian group of order n.

$$\forall a \in G.\ a^n = e.$$

$$G = \{a_1, a_2, \ldots, a_n\}$$

$$aG \triangleq \{aa_1, aa_2, \ldots, aa_n\} = G$$

$$\prod_{i=1}^{n} (aa_i) = a_1 \ldots a_n$$

$$a^n a_1 \ldots a_n = a_1 \ldots a_n \implies a^n = e$$

Theorem (Euler Theorem (1736))

Let $m \in \mathbb{Z}^+$ *and* $a \in \mathbb{Z}$. *If* $(a, m) = 1$, *then*

$$a^{\varphi(m)} \equiv 1 \mod m$$

Theorem (Euler Theorem (1736))

Let $m \in \mathbb{Z}^+$ *and* $a \in \mathbb{Z}$. *If* $(a, m) = 1$, *then*

$$a^{\varphi(m)} \equiv 1 \mod m$$

$$7^{222} \mod 10$$

Theorem (Euler Theorem (1736))

Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. If $(a, m) = 1$, then

$$a^{\varphi(m)} \equiv 1 \mod m$$

$$7^{222} \mod 10$$

$$(7, 10) = 1 \qquad \varphi(10) = 4$$

Theorem (Euler Theorem (1736))

Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. If $(a, m) = 1$, then

$$a^{\varphi(m)} \equiv 1 \mod m$$

$$7^{222} \mod 10$$

$$(7, 10) = 1 \qquad \varphi(10) = 4$$

$$7^4 \equiv 1 \mod 10$$

Theorem (Euler Theorem (1736))

Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. If $(a, m) = 1$, then

$$a^{\varphi(m)} \equiv 1 \mod m$$

$$7^{222} \mod 10$$

$$(7, 10) = 1 \qquad \varphi(10) = 4$$

$$7^4 \equiv 1 \mod 10$$

$$7^{222} \equiv 7^{4 \times 55 + 2} \equiv 7^2 \equiv 9 \mod 10$$

Theorem (Euler Theorem)

Let $m \in \mathbb{Z}^+$ *and* $a \in \mathbb{Z}$. *If* $(a, m) = 1$, *then*

$$a^{\varphi(m)} \equiv 1 \mod m$$

Theorem (Euler Theorem)

Let $m \in \mathbb{Z}^+$ *and* $a \in \mathbb{Z}$. *If* $(a, m) = 1$, *then*

$$a^{\varphi(m)} \equiv 1 \mod m$$

$$U_m = \{a \in \mathbb{Z}_m \mid (a, m) = 1\}$$

Theorem (Euler Theorem)

Let $m \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$. If $(a, m) = 1$, then

$$a^{\varphi(m)} \equiv 1 \mod m$$

$$U_m = \{a \in \mathbb{Z}_m \mid (a, m) = 1\}$$

$$(a, m) = 1 \implies a \in U_m$$

Theorem (Euler Theorem)

Let $m \in \mathbb{Z}^+$ *and* $a \in \mathbb{Z}$. *If* $(a, m) = 1$, *then*

$$a^{\varphi(m)} \equiv 1 \mod m$$

$$U_m = \{a \in \mathbb{Z}_m \mid (a, m) = 1\}$$

$$(a, m) = 1 \implies a \in U_m$$

$$a^{\varphi(m)} \equiv 1 \mod m$$

Theorem (Fermat's Little Theorem (1640))

Let p be a prime. Then for any $a \in \mathbb{Z}^+$,

$$a^{p-1} \equiv 1 \mod p$$

Theorem (Fermat's Little Theorem (1640))

Let p be a prime. Then for any $a \in \mathbb{Z}^+$,

$$a^{p-1} \equiv 1 \mod p$$

$$\varphi(p) = p - 1$$

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 $H \leq G$.

(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.

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

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 $H \le G$.

(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.

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

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

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

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

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

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

$$H_1 \cup H_2?$$

Center (中心)

Let G be a group. Let

$$C(G) \triangleq \{g \in G \mid gx = xg, \forall x \in G\}.$$

Then $C(G) \leq G$.

Definition (Isomorphism (同构))

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

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

Then ϕ is an isomorphism from G to G'.

Definition (Isomorphism (同构))

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

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

Then ϕ is an isomorphism from G to G'.

G and G' are isomorphic

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

$$(\mathbb{R}, +) \cong (\mathbb{R}^+, *)$$

$$(\mathbb{R}, +) \cong (\mathbb{R}^+, *)$$

$$\phi(x) = e^x$$

Theorem

Suppose that $\phi : G \cong G'$*. Let* e *and* e' *are identities of* G *and* G'*, respectively.*

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

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

(3) $\phi^{-1} : G' \cong G$

Theorem

Suppose that $\phi : G \cong G'$. *Let* e *and* e' *are identities of* G *and* G', *respectively.*

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

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

(3) $\phi^{-1} : G' \cong G$

$$ea = a \implies \phi(e)\phi(a) = \phi(ea) = \phi(a) = e'\phi(a)$$

Klein Four-group (四元群; $K_4; V$)

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$$a^2 = b^2 = c^2 = (ab)^2 = e$$

$$ab = c = ba \quad ac = b = ca \quad bc = a = cb$$

Klein Four-group (四元群; $K_4; V$)

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$$a^2 = b^2 = c^2 = (ab)^2 = e$$

$$ab = c = ba \quad ac = b = ca \quad bc = a = cb$$

$$U(8) = \{1, 3, 5, 7\}$$

Definition (Order of Elements (元素的阶))

Let G be a group, e be the identity of G.

The order of e is the smallest positive integer r such that $a^r = e$.

$$\operatorname{ord} a = r$$

Definition (Order of Elements (元素的阶))

Let G be a group, e be the identity of G.

The order of e is the smallest positive integer r such that $a^r = e$.

$$\text{ord } a = r$$

If such r does not exist, then $\text{ord } a = \infty$.

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$$

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$$

$$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$$

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$$

$$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$$

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

Theorem

Let G be a group and e be the identity of G.

$$((ord\, a = n) \wedge (\exists m \in \mathbb{Z}.\ a^m = e)) \implies n \mid m.$$

Theorem

Let G be a group and e be the identity of G.

$$((ord\, a = n) \land (\exists m \in \mathbb{Z}.\ a^m = e)) \implies n \mid m.$$

$$m = nq + r \qquad (0 \le r < n)$$

Theorem

Let G be a group and e be the identity of G.

$$((ord\, a = n) \land (\exists m \in \mathbb{Z}.\ a^m = e)) \implies n \mid m.$$

$$m = nq + r \qquad (0 \le r < n)$$

If $r > 0$,

$$a^r = a^{m-nq} = a^m \cdot (a^n)^{-q} = e \cdot e = e$$

Theorem

Let G be a group and e be the identity of G.

$$((ord\, a = n) \land (\exists m \in \mathbb{Z}.\ a^m = e)) \implies n \mid m.$$

$$m = nq + r \qquad (0 \le r < n)$$

If $r > 0$,

$$a^r = a^{m-nq} = a^m \cdot (a^n)^{-q} = e \cdot e = e$$

$$\text{ord}\ a \neq n$$

Theorem

Let G be a group and e be its identity.

$$ord\ a = n \implies \forall m \in \mathbb{Z}.\ ord\ a^m = \frac{n}{(n, m)}$$

Theorem

Let G be a group and e be its identity.

$$ord\, a = n \implies \forall m \in \mathbb{Z}.\ ord\, a^m = \frac{n}{(n, m)}$$

$$(a^m)^d = e$$

Theorem

Let G be a group and e be its identity.

$$ord\, a = n \implies \forall m \in \mathbb{Z}.\ ord\, a^m = \frac{n}{(n, m)}$$

$$\begin{aligned} & (a^m)^d = e \\ \iff & a^{md} = e \end{aligned}$$

Theorem

Let G be a group and e be its identity.

$$ord\, a = n \implies \forall m \in \mathbb{Z}.\ ord\, a^m = \frac{n}{(n, m)}$$

$$\begin{aligned} & (a^m)^d = e \\ \iff & a^{md} = e \\ \iff & n \mid md \end{aligned}$$

Theorem

Let G be a group and e be its identity.

$$ord\ a = n \implies \forall m \in \mathbb{Z}.\ ord\ a^m = \frac{n}{(n, m)}$$

$$\begin{aligned} & (a^m)^d = e \\ \iff & a^{md} = e \\ \iff & n \mid md \\ \iff & \frac{n}{(m, n)} \mid \frac{m}{(m, n)} d \end{aligned}$$

Theorem

Let G be a group and e be its identity.

$$ord\, a = n \implies \forall m \in \mathbb{Z}.\ ord\, a^m = \frac{n}{(n,m)}$$

$$\begin{aligned}
& (a^m)^d = e \\
\iff & a^{md} = e \\
\iff & n \mid md \\
\iff & \frac{n}{(m,n)} \mid \frac{m}{(m,n)} d \\
\iff & \frac{n}{(m,n)} \mid d
\end{aligned}$$

Definition (Cyclic Group (循环群))

Let G be a group. If

$$\exists a \in G.\ G = \langle a \rangle \triangleq \{a^0 = e, a, a^2, a^3, \dots\},$$

then G is a cyclic group.

Definition (Cyclic Group (循环群))

Let G be a group. If

$$\exists a \in G.\ G = \langle a \rangle \triangleq \{a^0 = e, a, a^2, a^3, \dots\},$$

then G is a cyclic group.

If $G = \langle a \rangle$, then a is a generator (生成元) of G.

$(\mathbb{Z}, +)$ is an infinite cyclic group

$(\mathbb{Z}, +)$ is an infinite cyclic group

$$(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$$

$(\mathbb{Z}, +)$ is an infinite cyclic group

$$(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$$

$(\mathbb{Z}_n, +)$ is a finite cyclic group of order n

$(\mathbb{Z}, +)$ is an infinite cyclic group

$$(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$$

$(\mathbb{Z}_n, +)$ is a finite cyclic group of order n

$$(\mathbb{Z}_m, +) = \langle 1 \rangle$$

$$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$$

$$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$$

$$\mathbb{Z}_5^* = \langle 2 \rangle = \langle 3 \rangle$$

Theorem

(1) *Let* $G = \{e, a, a^{-1}, a^2, a^{-2}, \dots\}$ *be an infinite cyclic group.*

$$\forall k, l \in \mathbb{Z}.\ (a^k = a^l \to k = l).$$

Theorem

(1) *Let* $G = \{e, a, a^{-1}, a^2, a^{-2}, \dots\}$ *be an infinite cyclic group.*

$$\forall k, l \in \mathbb{Z}.\ (a^k = a^l \to k = l).$$

(2) *Let* $G = \{e, a, a^2, \dots, a^{n-1}\}$ *be a finite cyclic group of order* n.

$$\forall k, l \in \mathbb{Z}.\ (a^k = a^l \leftrightarrow n \mid (k - l)).$$

Theorem (Structure Theorem of Cyclic Groups (循环群结构定理))

Let $G = \langle a \rangle$ be a cyclic group.

(1) *If $|G| = \infty$, then $G \cong (\mathbb{Z}, +)$.*

(2) *If $|G| = n$, then $G \cong (\mathbb{Z}_n, +)$.*

Theorem (Structure Theorem of Cyclic Groups (循环群结构定理))

Let $G = \langle a \rangle$ be a cyclic group.

(1) *If $|G| = \infty$, then $G \cong (\mathbb{Z}, +)$.*

(2) *If $|G| = n$, then $G \cong (\mathbb{Z}_n, +)$.*

$$\begin{aligned} \phi : \mathbb{Z} &\to G \\ k &\mapsto a^k, \quad \forall k \in \mathbb{Z} \end{aligned}$$

Theorem (Structure Theorem of Cyclic Groups (循环群结构定理))

Let $G = \langle a \rangle$ be a cyclic group.

(1) *If $|G| = \infty$, then $G \cong (\mathbb{Z}, +)$.*

(2) *If $|G| = n$, then $G \cong (\mathbb{Z}_n, +)$.*

$$\begin{aligned} \phi : \mathbb{Z} &\to G \\ k &\mapsto a^k, \quad \forall k \in \mathbb{Z} \end{aligned}$$

$$\begin{aligned} \phi : \mathbb{Z}_n &\to G \\ k &\mapsto a^k, \quad \forall k \in \mathbb{Z}_n \end{aligned}$$

Theorem (Generators of Cyclic Groups)

Let $G = \langle a \rangle$ be a cyclic group.

(1) *If $|G| = \infty$, then a and a^{-1} are the only generators of G;*

Theorem (Generators of Cyclic Groups)

Let $G = \langle a \rangle$ be a cyclic group.

(1) *If $|G| = \infty$, then a and a^{-1} are the only generators of G;*

(2) *If $|G| = n$, then a^r is a generator of G iff $(r, n) = 1$.*

Theorem (Generators of Cyclic Groups)

Let $G = \langle a \rangle$ be a cyclic group.

(1) *If $|G| = \infty$, then a and a^{-1} are the only generators of G;*

(2) *If $|G| = n$, then a^r is a generator of G iff $(r, n) = 1$.*

Theorem (Generators of Cyclic Groups)

Let $G = \langle a \rangle$ be a cyclic group.

(1) *If $|G| = \infty$, then a and a^{-1} are the only generators of G;*

(2) *If $|G| = n$, then a^r is a generator of G iff $(r, n) = 1$.*

$$\operatorname{ord} a^r = \frac{n}{(n, r)}$$

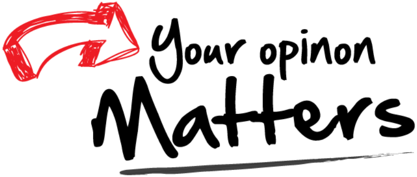
$$(\mathbb{Z}_{12}, +)$$

$$\text{Generators} : 1, 5, 7, 11$$

Theorem (Subgroups of Cyclic Groups)

Every subgroup of a cyclic group is cyclic.


Thank You!



Office 302

Mailbox: H016

hfwei@nju.edu.cn