(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

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}.

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.

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

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

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

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

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

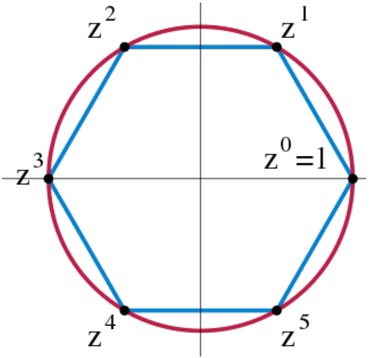
$$(1, -1, \mathbf{i}, -\mathbf{i})$$

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

$$(\mathcal{P}(A), \cup)$$

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)

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

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

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

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

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)

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

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

Definition (Euler's Totient Function (1763))

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

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))

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

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

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.

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

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

Theorem

Let G be an Abelian group of order n.

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

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

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

Theorem

Let G be an Abelian group of order n.

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

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

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

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

Theorem

Let G be an Abelian group of order n.

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

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

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

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

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

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 $a \in \mathbb{Z}^+$,

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

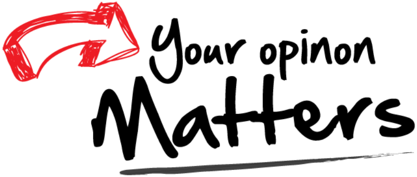
Theorem (Fermat's Little Theorem (1640))

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

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

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


Thank
You!



Office 302

Mailbox: H016

hfwei@nju.edu.cn