

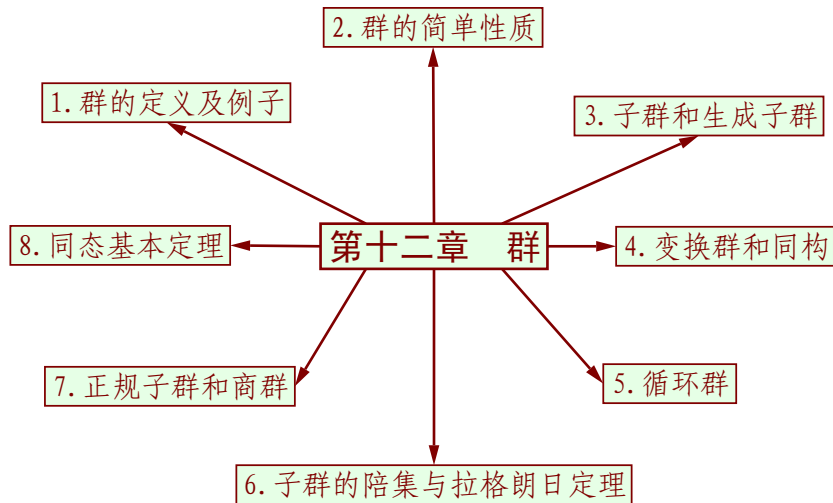
计算机数学基础 群论

任世军

e-mail:renshijun@hit.edu.cn

哈尔滨工业大学计算机学院

November 4, 2019



- 1 群的定义及例子
- 2 群的简单性质
- 3 子群、生成子群
- 4 变换群、同构
- 5 循环群
- 6 子群的陪集、拉格朗日定理
- 7 正规子群、商群
- 8 群的同态基本定理

群的定义及例子 (续)

定义 12.1.1

设 G 是一个非空集合, “ \circ ” 是 G 上的二元代数运算, 称为乘法。如果下列各个条件成立, 则称 G 对它的乘法 “ \circ ” 构成一个群 (Group)。

- 乘法 “ \circ ” 满足结合律, 即对 $\forall a, b, c \in G$, 都有 $(a \circ b) \circ c = a \circ (b \circ c)$
- 对乘法 “ \circ ”, G 中有一个左单位元。即对 $\forall a \in G, e \circ a = a$
- 对乘法 “ \circ ”, G 中每个元素都有左逆元。即对 G 中的每个元素 a , 都有元素 $b \in G$, 使得 $b \circ a = e$

回顾

Definition (定义 11.3.4)

每个元素都有逆元素的么半群称为群。

显然定义 11.3.4 蕴含定义 12.1.1

群的定义及例子 (续)

Example (例 12.1.1)

全体整数集合 \mathbb{Z} 对通常的加法构成一个群。

Example (例 12.1.2)

全体正有理数集合 \mathbb{Q}_+ 对通常的乘法构成一个群。

Example (例 12.1.3)

设 M_n 为所有 $n \times n$ 非奇异实矩阵的集合, 则 M_n 对矩阵的乘法构成一个群。

Example (例 12.1.4)

设 S 是一个集合, $|S| = n$, 则 2^S 对集的对称差运算构成一个群。

群的定义及例子 (续)

Example (例 12.1.5)

设 $S = \{1, 2, \dots, n\}$, S_n 为 S 的所有 n 次置换的集合, 则 S_n 对置换的乘法构成一个群, 称为 n 次对称群。

Definition (定义 12.1.2)

群 G 称为交换群或可换群, 如果乘法“ \circ ”满足交换律, 即对 $\forall a, b \in G$, 都有 $a \circ b = b \circ a$ 。交换群又称为阿贝尔群。

Definition (定义 12.1.3)

群 (G, \circ) 称为有限群, 如果 G 为有限集。 G 的基数称为群 G 的阶。如果 G 有无穷多个元素, 则称 G 为无限群。

Example (例 12.1.6)

设 n 是一个正整数, 整数集 Z 关于模 n 的剩余类的集合 $\{[0], [1], \dots, [n-1]\}$ 对于剩余类的加法构成一个 n 阶阿贝尔群。

- 1 群的定义及例子
- 2 群的简单性质**
- 3 子群、生成子群
- 4 变换群、同构
- 5 循环群
- 6 子群的陪集、拉格朗日定理
- 7 正规子群、商群
- 8 群的同态基本定理

群的简单性质

Theorem (定理 12.2.1)

设 (G, \circ) 是一个群, 则 $\forall a \in G, a$ 的左逆元也是 a 的右逆元。

Theorem (定理 12.2.2)

G 的左单位元也是右单位元。

Theorem (定理 12.2.3)

群的两个定义等价。

Theorem (定理 12.2.4)

设 a, b 是群 G 的任意两个元素, 则

$$(a^{-1})^{-1} = a, \quad (ab)^{-1} = b^{-1}a^{-1}$$

群的简单性质 (续)

Theorem (定理 12.2.5)

对 $\forall a, b \in G$, 在群 G 中, 方程

$$ax = b, \quad ya = b$$

关于未知量 x 与 y 有唯一解。

Theorem (定理 12.2.6)

非空集合 G 对其二元代数运算“ \circ ”构成一个群的充分必要条件是下列两个条件同时成立:

- ① “ \circ ”满足结合律, 即对 $\forall a, b, c \in G$

$$(a \circ b) \circ c = a \circ (b \circ c)$$

- ② 对 $\forall a, b \in G$, 方程

$$a \circ x = b \quad y \circ a = b$$

在 G 中有唯一解。

群的简单性质 (续)

Theorem (定理 12.2.7)

群 G 中的乘法满足消去律, 即对 $\forall a, x, y \in G$,
如果 $ax = ay$, 那么 $x = y$ 。
如果 $xa = ya$, 那么 $x = y$ 。

Theorem (定理 12.2.8)

非空有限集合 G 对其二元代数运算“ \circ ”构成群的充分必要条件是下列两个条件同时成立:

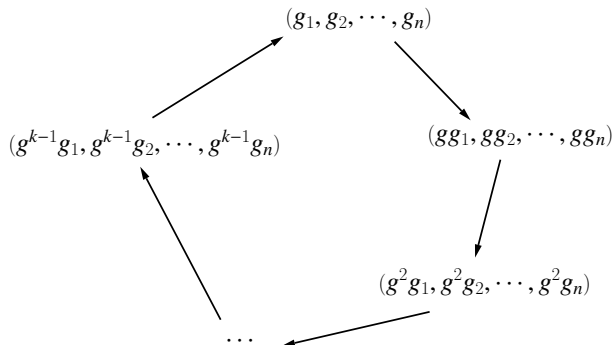
- ① “ \circ ”满足结合律。
- ② “ \circ ”满足左右消去律。

群的简单性质 (续)

$$M = \{(g_1, g_2, \dots, g_n) | g_i \in G, i = 1, 2, \dots, n, |\{g_1, g_2, \dots, g_n\}| = n\}$$

$$\phi : M \rightarrow M \quad \phi : (g_1, g_2, \dots, g_n) \rightarrow (gg_1, gg_2, \dots, gg_n)$$

可以证明 ϕ 为双射



可以得到 g^k 为左单位元素 \rightarrow 为单位元素 $\rightarrow g^{k-1}$ 为逆元素

Save file:/root/group Save file:/root/group Save file:/root/group

群的简单性质 (续)

Definition (定义 12.2.1)

设 G 是一个群, $a \in G$, 使 $a^n = e$ 的最小正整数 n 称为 a 的阶。如果这样的正整数不存在, 则称 a 的阶为无穷大。

Theorem (定理 12.2.9)

有限群的每个元素的阶不超过有限群的阶。

Example

3 阶群是交换群。

群的简单性质 (续)

克莱茵四元群

\circ	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e



\circ	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e



\circ	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	a	e
c	c	b	e	a

a 和 b 互换

\circ	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e



\circ	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$=$

\circ	e	b	a	c
e	e	b	a	c
b	b	e	c	a
a	a	c	e	b
c	c	a	b	e

四阶循环群

b 和 c 互换

\circ	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e



\circ	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e



\circ	e	a	c	b
e	e	a	c	b
a	a	e	b	c
c	c	b	e	a
b	b	c	a	e

- 1 群的定义及例子
- 2 群的简单性质
- 3 子群、生成子群**
- 4 变换群、同构
- 5 循环群
- 6 子群的陪集、拉格朗日定理
- 7 正规子群、商群
- 8 群的同态基本定理

子群、生成子群

Definition (定义 12.3.1)

设 S 是群 G 的非空子集, 如果 G 的乘法在 S 中封闭且 S 对此乘法也构成一个群, 则称 S 是 G 的子群。

Example (例 12.3.1)

任何一个至少含有两个元素的群 G , 至少有两个不同的子群, 一个是 G 本身, 一个是单位元的集合 $\{e\}$ 。

Example (例 12.3.2)

整数集合 Z 的加法群是有理数集 Q 的加法群的子群。

Example

偶数集合 $2Z$ 构成的加法群是整数集合 Z 的加法群的子群。

子群、生成子群 (续)

Theorem (定理 12.3.1)

设 G_1 是群 G 子群, 则 G_1 的单位元必是 G 的单位元, G_1 的元素 a 在 G_1 中的逆元素也是 a 在 G 中的逆元素。

Theorem (定理 12.3.2)

群 G 的非空子集 S 是 G 的子群的充分必要条件是:

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

Theorem (定理 12.3.3)

群 G 的任意多个子群的交还是 G 的子群。

Example (例 12.3.3)

任何一个群不能是它的两个真子群的并。

子群、生成子群 (续)

Theorem (定理 12.3.4)

群 G 的非空子集 S 是 G 的子群的充分必要条件是 $\forall a, b \in S$, 总有 $ab^{-1} \in S$.

Theorem (定理 12.3.5)

群 G 的有限非空子集 F 是 G 的子群的充分必要条件是 $FF \subseteq F$, 即对 $\forall a, b \in F, ab \in F$.

Definition (定义 12.3.2)

群 G 的元素 a 称为 G 的中心元素, 如果 a 与 G 的每个元素可交换, 即对 $\forall x \in G, xa = ax$. G 的所有中心元素的集合 C 称为 G 的中心。

Theorem (定理 12.3.6)

群 G 的中心 C 是 G 的可交换子群。

子群、生成子群 (续)

Definition (定义 12.3.3)

设 M 是群 G 的非空子集, G 的包含 M 的所有子群的交称为由 M 生成的子群, 记为 $\langle M \rangle$.

Example (例 12.3.4)

设 G 是一个群, $a \in G$, 那么 $\langle a \rangle = \{ \dots, a^{-2}, a^{-1}, e, a, a^2, \dots \}$.

Example (例 12.3.5)

设 G 是一个交换群, $a, b \in G$ 是两个无穷阶的元素, 那么 $\langle a, b \rangle = \{ a^m b^n \mid m, n \text{ 为任意整数} \}$.

Definition (定义 12.3.4)

设 G 是一个群, $a, b \in G$, 称 $aba^{-1}b^{-1}$ 为 a 和 b 的换位子。由 G 的所有换位子生成的子群称为 G 的换位子群。

- 1 群的定义及例子
- 2 群的简单性质
- 3 子群、生成子群
- 4 变换群、同构**
- 5 循环群
- 6 子群的陪集、拉格朗日定理
- 7 正规子群、商群
- 8 群的同态基本定理

变换群、同构

Definition (定义 12.4.1)

设 $(G_1, \circ), (G_2, \star)$ 是群, 如果存在一个一一对应 $\phi: G_1 \rightarrow G_2$, 使得对 $\forall a, b \in G_1$, 都有

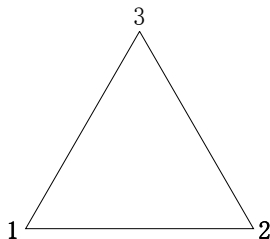
$$\phi(a \circ b) = \phi(a) \star \phi(b)$$

则称群 G_1 与 G_2 同构, 记为 $G_1 \cong G_2$ 。此时 ϕ 称为 G_1 到 G_2 上的一个同构。

Definition (定义 12.4.2)

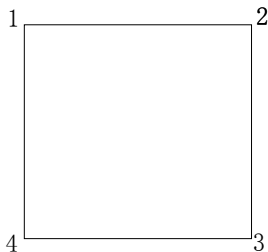
设 S 是一个非空集合, $\text{sym}(S)$ 是从 S 到 S 的一一对应构成的集合, 按照映射的合成构成一个群, 称为 S 上的对称群。当 $S = \{1, 2, \dots, n\}$ 时, 记 $\text{Sym}(S) = S_n$ 。 $\text{Sym}(S)$ 的任一子群称为 S 上的一个变换群。 S_n 的任一子群称为置换群。

对称群



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

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



$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{bmatrix} \quad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{bmatrix}$$

对称群

1		
2	1	
		1

1		
2		1
	1	

2	1	
1		
		1

2		1
1		
	1	

2	1	
		1
1		

2		1
	1	
1		

1		
	1	
2		1

1		
		1
2	1	

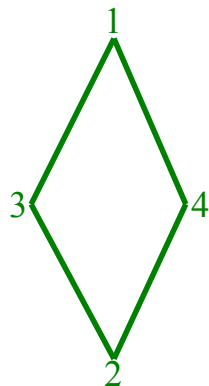
	1	
1		
2		1

		1
1		
2	1	

	1	
2		1
1		

		1
2	1	
1		

对称的例子



	$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$
\circ	(1)	(12)	(34)	(12)(34)
(1)	(1)	(12)	(34)	(12)(34)
(12)	(12)	(1)	(12)(34)	(34)
(34)	(34)	(12)(34)	(1)	(12)
(12)(34)	(12)(34)	(34)	(12)	(1)

菱形的对称群

变换群、同构 (续)

Theorem (定理 12.4.1 群的 Cayley 同构定理)

任何一个群都同构一个变换群。

Corollary (推论 12.4.1)

任何一个 n 阶有限群都同构 n 次置换群 S_n 的一个 n 阶子群。

Definition (定义 12.4.3)

设 (G, \circ) 是一个群, 如果存在 ϕ 在一个从 G 到 G 的一一对应 ϕ 使得对 $\forall a, b \in G$, 都有

$$\phi(a \circ b) = \phi(a) \circ \phi(b)$$

则称 ϕ 是 G 的一个自同构。

变换群、同构 (续)

o	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

← 克莱茵四元群

左变换集合 →

$$\rho_a = \begin{pmatrix} a & b & c & d \\ a & b & c & d \end{pmatrix} \quad \rho_b = \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}$$

$$\rho_c = \begin{pmatrix} a & b & c & d \\ c & d & a & b \end{pmatrix} \quad \rho_d = \begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix}$$

o	(1)	(12)(34)	(13)(24)	(14)(23)
(1)	(1)	(12)(34)	(13)(24)	(14)(23)
(12)(34)	(12)(34)	(1)	(14)(23)	(13)(24)
(13)(24)	(13)(24)	(14)(23)	(1)	(12)(34)
(14)(23)	(14)(23)	(13)(24)	(12)(34)	(1)

← 置换群

置 换

$$\rho_a = (1)$$

$$\rho_b = (12)(34)$$

$$\rho_c = (13)(24)$$

$$\rho_d = (14)(23)$$

变换群、同构 (续)

Example (例 12.4.1)

群 G 上的变换 I_G 是 G 的一个自同构。

Example (例 12.4.2)

设 G 是一个交换群, 对 $\forall a \in G$, 令 $\phi(a) = a^{-1}$, 则 ϕ 是 G 的一个自同构。

Example (例 12.4.3)

设 M_n 是一切可逆的 $n \times n$ 矩阵的集合, 则 M_n 对矩阵乘法形成一个群。令 P 是 M_n 中一个特定的矩阵, 则对 $\forall A \in M_n$

$$\phi(A) = P^{-1}AP$$

则 ϕ 是 M_n 的一个自同构。

变换群、同构 (续)

Theorem (定理 12.4.2)

设 G 是一个群, G 的所有自同构之集 $A(G)$ 对映射的合成构成一个群, 称为 G 的自同构群。

Example (例 12.4.3)

设 a 是 G 的一个固定元素, 对 $\forall x \in G$, 令

$$\phi(x) = axa^{-1}$$

则 ϕ 是 G 的一个自同构。

Definition (定义 12.4.4)

群 G 的由其元素 a 确定的自同构

$$\phi(x) = axa^{-1}, \forall x \in G$$

称为 G 的内自同构。 G 的其他自同构称为外自同构。

变换群、同构 (续)

Theorem (定理 12.4.4)

群 G 的所有内自同构之集是 G 的自同构群的一个子群,称为内自同构群。

Definition (定义 12.4.5)

设 (G, \circ) 是一个群,在 G 上定义二元关系 R 如下:对 $\forall a, b \in G, aRb$ 当且仅当有 G 的内自同构 ϕ ,使得 $b = \phi(a)$ 。称二元关系 R 为 G 的共轭关系,如果 aRb ,则称 a 与 b 共轭。

Theorem (补充定理)

设 (G, \circ) 是一个有限群,则有

$$|G| = |C(G)| + [G : C(a_1)] + [G : C(a_2)] + \cdots + [G : C(a_k)]$$

- 1 群的定义及例子
- 2 群的简单性质
- 3 子群、生成子群
- 4 变换群、同构
- 5 循环群**
- 6 子群的陪集、拉格朗日定理
- 7 正规子群、商群
- 8 群的同态基本定理

Definition (定义 12.5.1)

群 G 称为循环群, 如果 G 是由其中某个元素 a 生成的, 即 $(a) = G$.

Definition (定义 12.5.1)

整数加法群 $(\mathbb{Z}, +)$ 是循环群, 其生成元为 1。

Definition (定义 12.5.2)

整数集在模 n 同余关系下被划分成 n 个同余类 $\{[0], [1], \dots, [n-1]\}$ 。令 $Z_n = \{[0], [1], \dots, [n-1]\}$, 则 Z_n 对同余类加法构成的群 $(Z_n, +)$ 是一个有限循环群, 其生成元为 $[1]$ 。

循环群 (续)

Theorem (定理 12.5.1)

循环群 $G = \langle a \rangle$ 是无穷循环群的充分必要条件是 a 的阶为无穷大。此时,

$$G = \{ \cdots, a^{-n}, \cdots, a^{-2}, a^{-1}, e, a, a^2, \cdots, a^n, \cdots \}$$

循环群 $G = \langle a \rangle$ 是 n 阶循环群的充分必要条件是 a 的阶为 n 。此时

$$G = \{ e, a, a^2, \cdots, a^{n-1} \}$$

Theorem (定理 12.5.2)

1. 无穷循环群同构于整数加群 $(\mathbb{Z}, +)$ 。
2. 阶为 n 的有限循环群同构于模 n 剩余类加群 $(\mathbb{Z}_n, +)$ 。

循环群 (续)

Theorem (定理 12.5.3)

循环群 $G = \langle a \rangle$ 是由 a 生成的循环群, 则

(1) 循环群的子群还是循环群。

(2) 如果 G 是无穷循环群, 则 G 的子群为 $H_0 = \{e\}$, 或是某个具有最小正整数的元 a^m 生成的。于是, 对 $m = 1, 2, \dots$,

$$H_0 = \{e\}, H_m = \langle a^m \rangle$$

是 G 的所有子群。

(3) 无穷循环群中, 除了 $H_0 = \{e\}$ 外, 都是无穷循环子群, 从而都同构于 G 本身。

(4) 阶为 n 的循环群中, 每个子群的阶整除 n 。对 n 的任一因子 q , 必有一个阶为 q 的子群。于是 G 的全部子群为

$$H_0 = \{e\}, H_m = \langle a^m \rangle, m|n$$

每个子群 H_m 的阶为 n/m 。

- 1 群的定义及例子
- 2 群的简单性质
- 3 子群、生成子群
- 4 变换群、同构
- 5 循环群
- 6 子群的陪集、拉格朗日定理**
- 7 正规子群、商群
- 8 群的同态基本定理

子群的陪集、拉格朗日定理

Definition (定义 12.6.1)

设 H 是群 G 的一个子群, a 为群 G 的任一元素。集合 aH 称为子群 H 的一个左陪集, Ha 称为子群 H 的一个右陪集。

Theorem (定理 12.6.1)

设 H 是群 G 的一个子群, $a \in G$, 则 $aH = H$ 的充分必要条件是 $a \in H$ 。

Theorem (定理 12.6.2)

设 H 是群 G 的一个子群, $a, b \in G$, 则 $aH = bH$ 的充分必要条件是 $a^{-1}b \in H$ 。

Theorem (定理 12.6.3)

设 H 是群 G 的一个子群, 对 $\forall a, b \in G$, 或者 $aH = bH$, 或者 $aH \cap bH = \phi$ 。

子群的陪集、拉格朗日定理 (续)

Theorem (定理 12.6.4)

设 H 是群 G 的一个子群, 对 $\forall a, b \in G, |aH| = |bH|$ 。

Theorem (定理 12.6.5)

设 H 是群 G 的一个子群, 则 H 的所有左陪集构成的集族是 G 的一个划分。

Theorem (定理 12.6.6)

设 H 是群 G 的一个子群, S_l 是 H 的所有左陪集构成的集族, S_r 是 H 的所有右陪集构成的集族, 则 $|S_l| = |S_r|$ 。

Definition (定义 12.6.2)

设 H 是群 G 的一个子群, 若 H 的所有不同的左陪集的个数为有限数 j , 则称 j 为 H 在 G 中的指数, 记为 $j = [G : H]$, 否则说 H 在 G 中的指数为无穷大。

子群的陪集、拉格朗日定理 (续)

Theorem (定理 12.6.7 拉格朗日)

设 G 是一个阶为 N 的有限群, H 是群 G 的一个 n 阶子群, 则

$$N = n \cdot [G : H]$$

Corollary (推论 12.6.1)

有限群中每个元素的阶整除该有限群的阶。

Corollary (推论 12.6.2)

如果群 G 的阶 p 为素数, 则 G 一定是循环群。

Corollary (推论 12.6.3)

设 G 是阶为 N 的群, 则对 G 的每个元素 a , 都有 $a^N = e$ 。

子群的陪集、拉格朗日定理 (续)

Example (例 12.6.1)

证明:阶小于或等于 5 的群是交换群。

- 1 群的定义及例子
- 2 群的简单性质
- 3 子群、生成子群
- 4 变换群、同构
- 5 循环群
- 6 子群的陪集、拉格朗日定理
- 7 正规子群、商群**
- 8 群的同态基本定理

正规子群、商群

设 G 是一个群, G 的任一子集称为群子集。在 2^G 中借助于 G 的乘法引如一个代数运算, 称为群子集的乘法: 对 $\forall A, B \in 2^G$,

$$AB = \{ab | a \in A, b \in B\}$$

显然群子集的乘法是 2^G 的二元代数运算。其次, 对 $\forall A \in 2^G$, 定义

$$A^{-1} = \{a^{-1} | a \in A\}.$$

Theorem (定理 12.7.1)

设 G 是一个群, 则对 $\forall A, B, C \in 2^G$, 有 $(AB)C = A(BC)$ 。其次, 如果 H 是 G 的子群, 则

$$HH = H, H^{-1} = H, HH^{-1} = H.$$

正规子群、商群 (续)

Theorem (定理 12.7.2)

设 A, B 是群 G 的子群, 则 AB 是群 G 的子群的充分必要条件是 $AB = BA$ 。

Example (例 12.7.1)

设 H 是 G 的一个子群且 $H \neq \{e\}$ 。如果存在一个元素 $x_0 \in G$, 使得 $H(x_0^{-1}Hx_0) = G$, 则

$$H \cap x_0^{-1}Hx_0 \neq \{e\}.$$

Definition (定义 12.7.1)

设 H 是 G 的子群, 如果对 $\forall a \in G$, 都有 $aH = Ha$, 则称 H 是 G 的正规子群。

正规子群、商群 (续)

S_3 是 3 次置换群, $H_1 = \{(1), (1\ 2)\}$ 是 S_3 的一个子群。显然

$$(1\ 3)H_1 = \{(1\ 3), (1\ 3\ 2)\}, H_1(1\ 3) = \{(1\ 3), (1\ 3\ 2)\}$$

因此, $(1\ 3)H_1 \neq H_1(1\ 3)$ 。但是对于 S_3 的子群 $H_2 = \{(1), (1\ 2\ 3), (1\ 3\ 2)\}$, 就有

$$\begin{aligned}(1)H_2 &= H_2(1) \\ (1\ 2)H_2 &= \{(1\ 2), (1\ 3), (2\ 3)\} = H_2(1\ 2) \\ (1\ 3)H_2 &= \{(1\ 3), (2\ 3), (1\ 2)\} = H_2(1\ 3) \\ (2\ 3)H_2 &= \{(2\ 3), (1\ 2), (1\ 3)\} = H_2(2\ 3) \\ (1\ 2\ 3)H_2 &= H_2(1\ 2\ 3) \\ (1\ 3\ 2)H_2 &= H_2(1\ 3\ 2)\end{aligned}$$

即对 $\forall \sigma \in S_3$, 都有 $\sigma H_2 = H_2 \sigma$

正规子群、商群 (续)

Theorem (定理 12.7.3)

设 H 是群 G 的一个子群, 则下列三个命题等价:

- ① H 是 G 的正规子群。
- ② 对 $\forall a \in G, aHa^{-1} = H$.
- ③ 对 $\forall a \in G, aHa^{-1} \subseteq H$.

Example (例 12.7.2)

群 G 的换位子群是 G 的正规子群。

Theorem (定理 12.7.4)

设 H 是群 G 的一个正规子群当且仅当对 G 的任一内自同构 ϕ , 都有 $\phi(H) = H$ 。

正规子群、商群 (续)

Theorem (定理 12.7.5)

设 H 是 G 的正规子群, 则 H 的所有左陪集构成的集族 S_l 对群子集的乘法形成一个群。

Proof.

1. $(aH)(bH) = a(Hb)H = a(bH)H = (ab)(HH) = (ab)H$. 可以作为代数运算的定义。
2. 群子集的结合律显然成立。
3. 么元为 H 。
4. 每个元素 aH 的逆元素为 $a^{-1}H$ 。



Definition (定义 12.7.3)

群 G 的正规子群 H 的所有左陪集构成的集族对群子集的乘法构成的群称为 G 对 H 的商群, 记为 G/H 。

- 1 群的定义及例子
- 2 群的简单性质
- 3 子群、生成子群
- 4 变换群、同构
- 5 循环群
- 6 子群的陪集、拉格朗日定理
- 7 正规子群、商群
- 8 群的同态基本定理**

群的同态基本定理

Theorem (定理 12.8.1)

设 G 和 K 是两个群, $\phi: G \rightarrow K$ 是一个从 G 到 K 上的同态映射, 则 $K \cong G/\text{Ker}(\phi)$ 。

Theorem (定理 12.8.2)

设 H 和 K 是群 G 的两个子群, 如果 $K \triangleleft G$, 那么

$$H/(H \cap K) \cong HK/K$$

Theorem (定理 12.8.3)

设 $H \triangleleft K \triangleleft G$, $H \triangleleft G$, 那么 $K/H \triangleleft G/H$ 并且

$$\frac{G/H}{K/H} \cong G/K$$