

Discrete Mathematics

二维码采用二元域GF上的线性群结构构建纠错码。每个二进制位构成有限域元素，通过异或运算生成冗余校验位，形成满足封闭性、结合律的交换群系统。

1.非对称加密算法

群结构（如循环群、有限域）是RSA和椭圆曲线加密等算法的数学基础，利用群元素运算的不可逆性实现数据安全传输。

2.数字签名与密钥交换

基于离散对数问题的群运算（如Diffie-Hellman协议）用于生成安全密钥，确保通信双方身份验证。

二、通信与编码理论

1. 纠错码设计

线性群（如循环群）用于构建海明码、里德-所罗门码等纠错码，提升数据传输可靠性。

2.信号调制技术

群论中的置换群应用于正交频分复用（OFDM）等调制方案，优化信道资源分配

[illegible]

二维码定位标记采用置换群描述的位置对称性（如三个定位角标），通过群作用原理确保不同旋转角度下的快速识别。

第5章 群——伽罗瓦理论

群是非常重要的代数，对于代码的差错、纠错，自动机理论等各方面的研究，群是基础。

5.1 半群和独异点

定义5-1 半群：对代数系统 $\langle S; * \rangle$ ，若运算 $*$ 是可结合的，则该代数系统称为半群。

代数系统：封闭性

半群满足：封闭性，结合性。

例 $\langle \mathbb{N}; + \rangle$ ， $\langle \mathbb{I}; + \rangle$ ， $\langle \mathbb{N}; \times \rangle$ 半群； $\langle \mathbb{R}; \div \rangle$ ， $\langle \mathbb{R}; - \rangle$ 不是半群。

定义5-2 独异点（幺半群）：对半群 $\langle S; * \rangle$ ，若运算 $*$ 存在单位元 e ，则称该半群为独异点。

独异点满足：封闭性，结合性，单位元。

例 $\langle \mathbb{Z}; \times \rangle$ ， $\langle \mathbb{Z}; + \rangle$ ， $\langle 2^{\mathbb{U}}; \cup \rangle$ ， $\langle 2^{\mathbb{U}}; \cap \rangle$ 独异点。

例 运算 $*$ ： $\pi_1 * \pi_2 = \{x \mid x \in \pi_1 \cap \pi_2\}$ ，集合 $P(S) = \{S \text{ 上的所有分划} \}$

代数系统 $\langle P(S); * \rangle$ 是独异点。

（思考： $\cup$ 行不行？）

浙江大学信息与电子工程学院电子系宋牟平

定义5-3 交换独异点：若独异点 $\langle S; * \rangle$ 中的运算 $*$ 是可交换的，则称为交换独异点。

例 $\langle \mathbb{Z}; \times \rangle, \langle \mathbb{Z}; + \rangle, \langle 2^U; \cup \rangle, \langle 2^U; \cap \rangle, \langle P(S); * \rangle$ 交换独异点。

例 设 R_A 为 A 上所有关系的集合，即 $R_A = 2^{A \times A}$ ， $\cdot$ 为关系的复合运算，代数系统 $\langle R_A; \cdot \rangle$ 是独异点，但不是交换独异点。

若运算存在单位元，可特别定义

$$a^0 = e$$

定义5-4 循环独异点：设 $\langle S; * \rangle$ 为独异点，若存在元素 $g \in A$ ，使得每一个元素 $a \in A$ ，都可表示为

$$a = g^i \qquad i \in \mathbb{Z}$$

则该独异点称为循环独异点， g 称为生成元。

例 $\langle \mathbb{Z}; + \rangle, \langle \mathbb{Z}_6; \oplus_6 \rangle$ 是循环独异点，1是生成元。

例 b 是生成元， c 也是生成元。

$$a = b^0, \quad b = b^1, \quad c = b^2$$

$$a = c^0, \quad c = c^1, \quad b = c^2$$

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

对循环独异点 $\langle S; * \rangle$, S 可表示成

$$S = \{e, g, g^2, \dots, g^i, \dots\}$$

性质:

定理5-1 (1) 所有循环独异点都是可交换的。

定理5-2 (2) 若 $\langle S; * \rangle$ 是有限循环独异点, 则必存在正整数 n 和 m , $m \leq n$, 使

$$g^n = g^m$$

证: 因由生成元可得到无穷序列

$$e, g, g^2, \dots, g^i, \dots$$

但 $g^i \in S$, 若不成立, 则 S 为无限集。如 n 是满足前式的最小正整数, 则

$$e, g, g^2, \dots, g^m, g^{m+1}, \dots, g^{n-1}, g^n = g^m, g^{m+1}, \dots$$

$$\#S = n$$

(3) 有限循环独异点至少有一个除单位元e以外的幂等元。

证明：设 $\langle S; * \rangle$ 为有限循环独异点， $\#S=n$ ，则必存在正整数n和m， $m \leq n$ ，使

$$g^n = g^m \quad e, g, g^2, \dots, g^m, g^{m+1}, \dots, g^{n-1}, \underline{g^n = g^m, g^{m+1}, \dots}$$

令 $l=n-m$ ，则对于任意的 $i \geq m$ ，有 $g^i = g^{i+hl}$ ($h \in \mathbb{Z}$)。取 $i=kl$ ， k 是使得 $kl \geq m$ 的最小正整数，同时取 $h=k$ ，则有

$$g^{kl} = g^{kl} * g^{kl}$$

g^{kl} 是一幂等元。

推论：设 $\langle S; * \rangle$ 是一有限独异点，则对于每一个 $a \in S$ ，存在 $j \geq 1$ ，使得

$$a^j * a^j = a^j$$

还可推广到有限半群，见习题。证明：构造有限循环独异点 $\langle \{a^0, a^1, \dots\}; * \rangle$

注意： $\langle S; * \rangle$ 不一定是循环独异点。

例 生成元 c $1=c^0, c=c^1, b=c^2, a=c^3, d=c^4$

$$a^2 = a, c^3 * c^3 = c^3 = a, b^3 * b^3 = b^3 = a$$

有一个除单位元的幂等元a。

*	1	a	b	c	d
1	1	a	b	c	d
a	a	a	b	d	d
b	b	b	d	a	a
c	c	d	a	b	b
d	d	d	a	b	b

定义5-5 子半群： 设 $\langle S; * \rangle$ 和 $\langle T; * \rangle$ 是半群，若 $T \subseteq S$ ，则称 $\langle T; * \rangle$ 是 $\langle S; * \rangle$ 的子半群。

因条件 $T \subseteq S$ 成立，运算在 T 上必然满足结合性，故条件可弱化为 $\langle T; * \rangle$ 是半群 $\langle S; * \rangle$ 的子代数。

定义5-6 子独异点： 设 $\langle S; * \rangle$ 和 $\langle T; * \rangle$ 是独异点，若 $T \subseteq S$ ，且 $\langle S; * \rangle$ 的单位元 $e \in T$ ，则称 $\langle T; * \rangle$ 是 $\langle S; * \rangle$ 的子独异点。

例

*	1	a	b	c	d
1	1	a	b	c	d
a	a	a	b	d	d
b	b	b	d	a	a
c	c	d	a	b	b
d	d	d	a	b	b

*	a	b	d
a	a	b	d
b	b	d	a
d	d	a	b

右是左的子半群，但不是子独异点，尽管两者都是独异点（单位元不一样）。

生成子： $\langle S; * \rangle$ 半群， $T \subseteq S$ 。若S中任意元素均可由T中的元素经过运算表达出来，称T是 $\langle S; * \rangle$ 的**生成子**。

例 $\langle \mathbb{N}; \times \rangle$ 是独异点，所有素数的集合P是 $\langle \mathbb{N}; \times \rangle$ 的生成子。

定理5-3 若 $\langle S; * \rangle$ 是**可交换的独异点**，则S上的所有幂等元的集合形成 $\langle S; * \rangle$ 的一个子独异点。

证明：

(1) 设T是所有幂等元的集合，则 $T \subseteq S$ 。

(2) 单位元e是幂等元， $e \in T$ ，T非空。

(3) 对任意的 $a, b \in T$ ，有

$$a*a=a, b*b=b$$

因此由可交换性有

$$(a*b)*(a*b)=(a*a)*(b*b)=a*b$$

即 $a*b \in T$ ，封闭性满足， $\langle T; * \rangle$ 是 $\langle S; * \rangle$ 的一个子独异点，问题得证。

定理5-4: 设 h 是从代数系统 $V_1 = \langle S_1; * \rangle$ 到 $V_2 = \langle S_2; \circ \rangle$ 的**满同态**, 其中运算 $*$ 和 $\circ$ 都是二元运算, 则

- (1) 若 **V_1 是半群**, 则 **V_2 也是半群**;
- (2) 若 **V_1 是独异点**, 则 **V_2 也是独异点**。

证明:

(1) 因为 $V_1 = \langle S_1; * \rangle$ 是半群, 所以运算 $*$ 是可结合的, 而 h 是从 V_1 到 V_2 的满同态, 由定理4-5可知, 运算 $\circ$ 也是可结合的, 所以 $V_2 = \langle S_2; \circ \rangle$ 也是半群;

(2) 若 V_1 是独异点, 所以运算 $*$ 是可结合的, 且有单位元 e , 而 h 是从 V_1 到 V_2 的满同态, 由定理4-5可知, 运算 $\circ$ 也是可结合的, 且有单位元 $h(e)$, 所以 $V_2 = \langle S_2; \circ \rangle$ 也是独异点。

5.2 群的定义

群：设 $\langle G; * \rangle$ 是一个独异点，若对于每一个 $a \in G$ ，存在 $a^{-1} \in G$ ，使得

$$a * a^{-1} = a^{-1} * a = e$$

则 $\langle G; * \rangle$ 称为**群**。

半群：封闭性，结合性。

独异点：封闭性，结合性，单位元。

群：封闭性，结合性，单位元，逆元。

例 $\langle \mathbb{I}; + \rangle$ 是群； $\langle \mathbb{I}; \times \rangle$ 是半群，是独异点，但不是群。

例 $\langle \mathbb{Z}_6; \oplus_6 \rangle$ 是群。

例 由右表定义的代数系统是群。

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

定义5-8 交换群（阿贝尔群）：若 $\langle G; * \rangle$ 的运算*是可交换的，则称为交换群。

例 集合 $A=\{a, b, c\}$ 上的所有置换的集合 $P=\{1, \alpha, \beta, \gamma, \delta, \varepsilon\}$, 其中

$$\begin{aligned} 1 &= \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} & \alpha &= \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} & \beta &= \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \\ \gamma &= \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} & \delta &= \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} & \varepsilon &= \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} \end{aligned}$$

代数系统 $\langle P; \cdot \rangle$ 是群, 其中 $\cdot$ 是复合运算。这种群称为**对称群**, 其任意子群称**置换群**。固体物理中的晶格对称操作就是置换群。书中例5给出了对称操作的例子。

定义 幂

$$a^0 = e^0$$

$$a^{n+1} = a^n * a$$

$$a^{-n} = (a^{-1})^n = (a^n)^{-1}$$

和一般的幂运算相同。

定义5-9 **循环群**: $\langle G; * \rangle$ 是一个群, 若存在一个元素 g , 使得每一个 $a \in G$, 都可表示成

$$a = g^i \quad (i \in I)$$

称该群为**循环群**, g 称为**生成元**。

例 $\langle I; + \rangle$, $\langle \mathbb{Z}_6; \oplus_6 \rangle$ 生成元是1

例 右表的b, c是生成元

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

定义5-10 **有限群**: $\langle G; * \rangle$ 是一个群, 若 G 有限, 称**有限群**, 若 G 无限, 称**无限群**。# G 称群的**阶**。

定义5-11 **元素周期**: 对于群 $\langle G; * \rangle$ 元素 a , 若存在一**最小正整数** r , 使

$$a^r = e$$

称 r 为元素 a 的**周期**。若不存在则称 a 具有**无限周期**。

单位元 e 的周期为1。

定理5-5: 设 $\langle G; * \rangle$ 是一个循环群, 则生成元 g 的周期与群的阶相等。

证明:

(1) g 的周期有限, 设为 n , 则

$$g^n = e$$

对于任一元素 $g^k \in G$, 令 $k = nq + r$ ($0 \leq r \leq n$)

则 $g^k = g^{nq+r} = (g^n)^q * g^r = e * g^r = g^r$

故 $\langle G; * \rangle$ 中任意元素都可表示成 g^r , 而 $0 \leq r \leq n-1$, 因此 G 中只有 n 个不同元素。

(2) 若 g 的周期无限, 由封闭性可知, G 中必有无限多个元素。

在阶大于1的群中没有零元。 (零元没有逆元; 加法没零元, 乘法有零元)

除单位元外, 群没有任何幂等元。

证明: 设 a 是幂等元, 则

$$a = (a^{-1} * a) * a = a^{-1} * (a * a) = a^{-1} * a = e$$

5.3群的基本性质

定理5-6 可解性: 若 $\langle G; * \rangle$ 是一个群, 则对于任意的 $a, b \in G$, 有

(1) 存在唯一的元素 $x \in G$, 使得 $a * x = b$

(2) 存在唯一的元素 $y \in G$, 使得 $y * a = b$

证明:

(1) 因

$$a * (a^{-1} * b) = (a * a^{-1}) * b = e * b = b$$

故至少存在一个元素

$$x = a^{-1} * b$$

使 $a * x = b$

设有另一元素 h 也使

$$a * h = b \quad \text{成立}$$

则

$$h = e * h = (a^{-1} * a) * h = a^{-1} * (a * h) = a^{-1} * b = x$$

定理5-7 消去律: 若 $\langle G; * \rangle$ 是一个群, 则对于任意的 $a, b, c \in G$, 有

(1) 若 $a*b=a*c$, 则 $b=c$

(2) 若 $b*a=c*a$, 则 $b=c$

可解性和消去律都是逆元存在所导致的。

消去律的一个重要推论是, 对于任意 $a \in G$, 有

$$a * G = G$$

运算表的每一行和每一列都是一个排列或置换

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

定理5-9: 若群 $\langle G; * \rangle$ 的元素 a 有周期 r , 则当且仅当 k 是 r 的整数倍时,

$$a^k = e$$

定理5-10: 群中任一元素与它的逆元具有相同的周期。

证明: 若 a 具有有限周期 r , 则 $a^r = e$,

由此可知

$$(a^{-1})^r = (a^r)^{-1} = e^{-1} = e$$

a^{-1} 有有限周期, 设为 r' , 则 $r' \leq r$ 。

又,

$$a^{r'} = ((a^{r'})^{-1})^{-1} = ((a^{-1})^{r'})^{-1} = e^{-1} = e$$

所以 $r \leq r'$, 因此 $r = r'$ 。

定理5-11：有限群 $\langle G; * \rangle$ 的任一元素具有有限周期，且不大于群的阶。

证明：设 a 是 G 中一任意元素，构造序列

$$a^0, a^1, \dots, a^{\#G}$$

由封闭性，序列中的每一个元素都是 G 中的元素，因此至多有 $\#G$ 个是不同的，但该序列有 $\#G+1$ 个元素，故必有两个是相同的，记

$$a^r = a^p \quad 1 \leq p < r \leq \#G$$

$$a^{r-p} = a^r * a^{-p} = a^p * a^{-p} = a^0 = e$$

因此 a 的周期 $\leq r-p \leq \#G$

5.4 子群及陪集

子群及其陪集

定义5-12 子群： 设 $\langle G; * \rangle$ 和 $\langle H; * \rangle$ 是群，如果H是G的非空子集，即 $H \subseteq G$ ，且 $e_G = e_H$ ，则 $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的子群。

子群要满足6个条件

- (1) 封闭性 $a, b \in H; a * b \in H$
- (2) 结合性 $a * (b * c) = (a * b) * c$
- (3) 单位元 e_H
- (4) 逆元 $a \in H; a^{-1} \in H$
- (5) $H \subseteq G$
- (6) $e_G = e_H$

上面六条性质中，

当（1）和（5）满足时，结合性自然满足，不需要。

（6）条也是自然满足的，因对任意的 $a \in H$ ，有

$$a * e_H = e_H * a = a$$

而 $H \subseteq G$ ，可知

$$a * e_G = e_G * a = a$$

由消去律

$$e_G = e_H = e$$

六条性质只需保留四条

（1） 封闭性

（3） 单位元 $e \in H$

（4） 逆元

（5） $H \subseteq G$

可定义子群: 设 $\langle G; * \rangle$ 是群, 如果 $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的**非空子代数**, 且满足

(1) **单位元** $e \in H$

(2) 对任意的 $a \in H$, 有**逆元**存在 $a^{-1} \in H$,

称 $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的**子群**。

真子群: H 是 G 的真子集, 称 $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的真子群。

平凡子群: $\langle G; * \rangle$, $\langle \{e\}; * \rangle$

例 $\langle \mathbb{I}; + \rangle$ 是 $\langle \mathbb{R}; + \rangle$ 的子群。

例 3次对称群 $\langle P; \cdot \rangle$ 。 $P = \{1, \alpha, \beta, \gamma, \delta, \varepsilon\}$ 是集合 $A = \{a, b, c\}$ 上的所有置换的集合, 其中

$$\begin{aligned} 1 &= \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} & \alpha &= \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} & \beta &= \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \\ \gamma &= \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} & \delta &= \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} & \varepsilon &= \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} \end{aligned}$$

$\langle \{1, \alpha\}; \cdot \rangle$, $\langle \{1, \beta\}; \cdot \rangle$, $\langle \{1, \varepsilon\}; \cdot \rangle$ 和 $\langle \{1, \gamma, \delta\}; \cdot \rangle$ 是 $\langle P; \cdot \rangle$ 的子群。

子群成立的条件中，单位元也可去掉。

因（大系统中）逆元存在，即对 $a \in H$ ，存在 $a^{-1} \in H$ ，使

$$a * a^{-1} = a^{-1} * a = e$$

由封闭性 $e \in H$ 。

定理5-12： 设 $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的子代数，则 $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的子群的充要条件是对于任意的 $a \in H$ ，有 $a^{-1} \in H$ 。

对封闭性和逆元还可以进一步合并成一个条件。

定理5-13： 设 $\langle G; * \rangle$ 是群， H 是 G 的非空子集，则当且仅当由 $a, b \in H$ ，可推得 $a * b^{-1} \in H$ 时， $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的子群。

证明：

（1） 设 $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的子群，则对于 $a, b \in H$ ，必有 $b^{-1} \in H$ ，由封闭性可得

$$a * b^{-1} \in H$$

（2） 假定由 $a, b \in H$ ，可推得 $a * b^{-1} \in H$ ，则对 $a \in H$ 有

$$a * a^{-1} = e \in H$$

进一步 $e * a^{-1} = a^{-1} \in H$

若 $a, b \in H$, 由前面的结果 $b^{-1} \in H$, 即 $a, b^{-1} \in H$, 则

$$a * b = a * (b^{-1})^{-1} \in H$$

每一个元素都有逆元, 且封闭的, $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的子群。

对有限群, 逆元的条件也是多余的, 可去掉, 只需要

(1) $H \neq \emptyset, H \subseteq G$

(2) $\langle H; * \rangle$ 是封闭的

定理5-14: $\langle G; * \rangle$ 是一个有限群, 若 $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的子代数, 则 $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的子群。

证明: 设 $a \in H$, 因 H 是有限的, 故 a 有一有限周期 r , 即

$$a^r = e$$

由封闭性, $a^{r-1} \in H$, 但

$$a^{r-1} = a^r * a^{-1} = e * a^{-1} = a^{-1}$$

故 $a^{-1} \in H$ 。

子群的条件还可弱化。（以上证明过程中没有要求G是有限的）

定理5-15: $\langle G; * \rangle$ 是一个群，若 $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的有限子代数，则 $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的子群。

定义5-13 左陪集 右陪集: $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的子群，a是G的任意一个元素，则

(1) $H * a = \{h * a | h \in H\}$ 称为**右陪集**，

(2) $a * H = \{a * h | h \in H\}$ 称为**左陪集**。

若 $a \in H$ ， $H * a = a * H = H$ ，H既是左陪集，又是右陪集。

证明: 因 $a, h \in H$ ，由封闭性

$$a * h \in H, \text{ 即 } a * H \subseteq H \quad \langle 1 \rangle$$

又，对任意的 $h \in H$ ，有

$$h = e * h = a * (a^{-1} * h) = a * h'$$

因 $a^{-1}, h \in H$ ，故 $h' = a^{-1} * h \in H$ ，由右陪集定义知

$$h = a * h' \in a * H$$

$$\text{即 } H \subseteq a * H \quad \langle 2 \rangle$$

定义5-14 正规子群与陪集: $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的**子群**, 如果对于每一个 $a \in G$, 有 $\mathbf{a * H = H * a}$, 即所有的左右陪集相等, 则称 $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的**正规子群**, 左右陪集不用区分, 称**陪集**。

如果群是可交换的, 它的所有子群都是正规子群。

正规子群的判断?

定理5-16 设 $\langle H; * \rangle$ 是群 $\langle G; * \rangle$ 的一个子群, 当且仅当对于任意的 $a \in G$, 有 $\mathbf{a * H * a^{-1} = H}$ 时, $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的正规子群。

证明: 设 $\langle H; * \rangle$ 是群 $\langle G; * \rangle$ 的正规子群, 则对于任意的 $a \in G$,

有 $a * H = H * a$, 因此由运算 $*$ 的可结合性和符号 $a * H * a^{-1}$ 的定义可知

$$a * H * a^{-1} = (a * H) * a^{-1} = (H * a) * a^{-1} = H * (a * a^{-1}) = H * e = H$$

反之, 假设对任意的 $a \in G$, 有 $a * H * a^{-1} = H$

则 $H * a = (a * H * a^{-1}) * a = (a * H) * (a^{-1} * a) = (a * H) * e = a * H$

所以, $\langle H; * \rangle$ 是群 $\langle G; * \rangle$ 的正规子群。

上述 $\langle H; * \rangle$ 为正规子群的充要条件可以削弱，即有：

定理5-17 设 $\langle H; * \rangle$ 是群 $\langle G; * \rangle$ 的一个子群，当且仅当对于任意的 $a \in G$ ，有 $a * H * a^{-1} \subseteq H$ 时， $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的正规子群。

证明：

必要性显然成立。

设对任意的 $a \in G$ ，有 $a * H * a^{-1} \subseteq H$ ， (1)

由于 $a^{-1} \in G$ ，因此以 a^{-1} 代 a 仍有 $a^{-1} * H * a \subseteq H$ 成立，以 a 左乘，以 a^{-1} 右乘得：

$$a * (a^{-1} * H * a) * a^{-1} \subseteq a * H * a^{-1}$$

$$\text{即 } H \subseteq a * H * a^{-1} \quad (2)$$

由(1)和(2)得：

$$a * H * a^{-1} = H$$

因此， $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的正规子群。证毕

定理5-18 设 $\langle H; * \rangle$ 是群 $\langle G; * \rangle$ 的一个子群, 则

(1) 当且仅当 $b*a^{-1} \in H$ 时, $b \in H*a$

(2) 当且仅当 $a^{-1}*b \in H$ 时, $b \in a*H$

证明: 根据消去律

(1) 当且仅当存在某一 $h \in H$, 使得 $b=h*a$ 时, 有

$$b \in H*a$$

因此, 当且仅当存在某一 $h \in H$, 使得 $b*a^{-1}=h$ 时, 有

$$b \in H*a$$

这即是当且仅当 $b*a^{-1} \in H$ 时, 有 $b \in H*a$

(2) 的证明与 (1) 的证明类似。

定理5-19 设 $\langle H; * \rangle$ 是群 $\langle G; * \rangle$ 的一个子群, a 和 b 是 G 的任意两个元素, 则有

$$(1) H * a = H * b \text{ 或者 } (H * a) \cap (H * b) = \Phi$$

$$(2) a * H = b * H \text{ 或者 } (a * H) \cap (b * H) = \Phi$$

证明:

(1) 设 $(H * a) \cap (H * b) \neq \Phi$, 并设 $x \in (H * a) \cap (H * b)$,

则 $x = h_1 * a = h_2 * b$ ($h_1, h_2 \in H$).

而 $e = x^{-1} * x = a^{-1} * h_1^{-1} * h_2 * b$,

因此 $a * b^{-1} = h_1^{-1} * h_2 \in H$, 由定理5-18, $a \in H * b$, 因此

$$a = h * b \ (h \in H), \ h' * a = (h' * h) * b \ (h', h \in H), \text{ 因此 } H * a \subseteq H * b \quad <1>$$

类似, $e = x^{-1} * x = b^{-1} * h_2^{-1} * h_1 * a$,

因此 $b * a^{-1} = h_2^{-1} * h_1 \in H$, 由定理5-18, $b \in H * a$, 因此

$$b = h * a \ (h \in H), \ h' * b = (h' * h) * a \ (h', h \in H), \text{ 因此 } H * b \subseteq H * a \quad <2>$$

故, $H * b = H * a$

(2) 的证明与(1)的证明类似。

例 3次对称群 $\langle P; \cdot \rangle$, $P=\{1, \alpha, \beta, \gamma, \delta, \varepsilon\}$, 其中,

$$\begin{aligned} 1 &= \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix} & \alpha &= \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix} & \beta &= \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \\ \gamma &= \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix} & \delta &= \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} & \varepsilon &= \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix} \end{aligned}$$

它有4个子群: $\langle \{1, \alpha\}; \cdot \rangle$, $\langle \{1, \beta\}; \cdot \rangle$, $\langle \{1, \varepsilon\}; \cdot \rangle$ 和 $\langle \{1, \gamma, \delta\}; \cdot \rangle$ 。

$\langle \{1, \alpha\}; \cdot \rangle$ 的右陪集: 仅有三个不同

$$\{1, \alpha\} \cdot 1 = \{1, \alpha\} \quad \{1, \alpha\} \cdot \alpha = \{\alpha, 1\} \quad \{1, \alpha\} \cdot \beta = \{\beta, \gamma\}$$

$$\{1, \alpha\} \cdot \gamma = \{\gamma, \beta\} \quad \{1, \alpha\} \cdot \delta = \{\delta, \varepsilon\} \quad \{1, \alpha\} \cdot \varepsilon = \{\varepsilon, \delta\}$$

$\langle \{1, \alpha\}; \cdot \rangle$ 的左陪集: 仅有三个不同

$$1 \cdot \{1, \alpha\} = \{1, \alpha\} \quad \alpha \cdot \{1, \alpha\} = \{\alpha, 1\} \quad \beta \cdot \{1, \alpha\} = \{\beta, \delta\}$$

$$\gamma \cdot \{1, \alpha\} = \{\gamma, \varepsilon\} \quad \delta \cdot \{1, \alpha\} = \{\delta, \beta\} \quad \varepsilon \cdot \{1, \alpha\} = \{\varepsilon, \gamma\}$$

从该例可以看出, 所有相异的左陪集构成P的一个分划, 相异的右陪集也构成P的一个分划。

定理5-20: 设 $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的子群, 则 $\langle H; * \rangle$ 的所有相异左陪集构成 G 的一个分划, 称左陪集分划, 所有相异右陪集也构成 G 的一个分划, 称右陪集分划。

证明:

(1) 因 $\langle H; * \rangle$ 是 G 的子群, $e \in G$, 所以对任意的 $a \in G$, 有 $a = a * e \in a * H$, 即 $a * H$ 非空, 且 $G \subseteq \bigcup_{a \in G} a * H$, 又 $\bigcup_{a \in G} a * H \subseteq G$, 所以

$$\bigcup_{a \in G} a * H = G$$

(2) 设元素 $a, b \in G$, 且

$$(a * H) \cap (b * H) \neq \emptyset$$

则必存在元素 x ，满足

$$x \in (a * H) \cap (b * H)$$

即 $x = a * h_1 = b * h_2$ $(h_1, h_2 \in H)$

$$a = b * (h_2 * h_1^{-1}) = b * h_3 \quad (h_3 \in H)$$

对任意的 $h \in H$ ，有

$$a * h = b * (h_3 * h) = b * h_4 \quad (h_4 \in H)$$

因此 $a * H \subseteq b * H$ $\langle 1 \rangle$

同理可证 $b * H \subseteq a * H$ $\langle 2 \rangle$

故有 $a * H = b * H$

两左陪集要么相等，要么交为空：

$$a * H = b * H \quad \text{或} \quad (a * H) \cap (b * H) = \emptyset$$

也就是相异左陪集之交为空

$$(a * H) \cap (b * H) = \emptyset \quad (a * H \neq b * H)$$

同样的可证明相异右陪集构成 G 的一个分划。

当 $\langle H; * \rangle$ 是正规子群时，左右陪集相等，称**陪集分划**。

定理5-21：设 $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的子群，则对任意的 $a \in G$ ，有

$$\#(a * H) = \#(H * a) = \#H。$$

证明：

定义函数 $f: H \rightarrow a * H$ ， $f(h) = a * h$ ，显然 f 是满射。

因有一个 $a * h \in a * H$ ，必存在一个 $h \in H$ ，使 $f(h) = a * h$ 。

设 $a * h_1 \neq a * h_2$ ，则由消去律必有 $h_1 \neq h_2$ ， f 是单射。

因此 f 是双射，有

$$\#(a * H) = \#(H * a) = \#H$$

所有的陪集中的元素数目相等，且等于子群的阶。

定理5-22 拉格朗日定理: $\#G = \#(\bigcup_{a \in G} a * H) = d \#(a * H) = d \#H$

d 是 $\#G$ 的因子, $\#G$ (群)是 $\#H$ (子群)的整数倍。

推论1: 素数阶的群只有平凡子群。当 $\#G$ 为素数时, d 只能取1和 $\#G$ 。

$d=1$, 则 $\#H=\#G$, $\langle H; * \rangle = \langle G; * \rangle$; $d=\#G$, 则 $\#H=1$, $\langle H; * \rangle = \langle \{e\}; * \rangle$ 。

推论2: 任一有限群子群的阶必为该群的因子, 即 $\#H$ 是 $\#G$ 的因子。

定理5-23 推论3: 有限群 $\langle G; * \rangle$ 中, 每个元素的周期都是 $\#G$ 的因子。

证明: 设 $a \in G$, 且 a 的周期为 r , 则 a 作为生成元可构成 $\langle G; * \rangle$ 的子群

$$\langle \{e, a^1, a^2, \dots, a^{r-1}\}; * \rangle$$

而该子群的阶等于元素 a 的周期 r , 由拉格朗日定理, r 是 $\#G$ 的因子。

推论4: 素数阶的群必为循环群, 且每个元素都是生成元。(书中习题)

例 求群 $G=\langle Z_6; \oplus_6 \rangle$ 的所有子群和陪集。

解: $Z_6=\{0, 1, 2, 3, 4, 5\}$, $\#Z_6=6=2 \times 3=3 \times 2=1 \times 6=6 \times 1$, 有1、2、3、6四个因子, 根据拉格朗日定理, 有四个子群:

$$\langle H_1; \oplus_6 \rangle = \langle \{0\}; \oplus_6 \rangle \quad \text{平凡子群}$$

$$\langle H_2; \oplus_6 \rangle = \langle \{0, 2, 4\}; \oplus_6 \rangle$$

$$\langle H_3; \oplus_6 \rangle = \langle \{0, 3\}; \oplus_6 \rangle$$

$$\langle H_4; \oplus_6 \rangle = \langle \{0, 1, 2, 3, 4, 5\}; \oplus_6 \rangle \quad \text{平凡子群}$$

陪集: 因 $\langle Z_6; \oplus_6 \rangle$ 是循环群, 所以它的所有子群也是循环群, 可交换, 故左右陪集相等, 不用区分左右陪集。

$$\langle H_1; \oplus_6 \rangle \text{有6个陪集: } \{0\}, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}$$

$$\langle H_2; \oplus_6 \rangle \text{有2个陪集: } \{0, 2, 4\}, \{1, 3, 5\}$$

$$\langle H_3; \oplus_6 \rangle \text{有3个陪集: } \{0, 3\}, \{1, 4\}, \{2, 5\}$$

$$\langle H_4; \oplus_6 \rangle \text{有1个陪集: } \{0, 1, 2, 3, 4, 5\}$$

作业

3, 7, 9, 13, 17, 23, 25, 29

内容提要

1. 半群和独异点

- 半群；
- 独异点；
- 循环独异点；
- 子半群和子独异点.

2. 群

- 群；
- 循环群；
- 元素的周期与群的阶.

3. 群的基本性质

- 群的消去律；
- 元素运算后求逆元；
- 元素的周期.

4. 子群及其陪集

- 子群及其判别；
- 子群的陪集；
- 正规子群及其判别；
- 群中与子群相关的左(右)陪集分划；
- 拉格朗日定理.

例题讲解

例 5-1 设 $\mathbf{R}$ 是实数集, $\mathbf{R}$ 上的二元运算 $\times$ 定义为, $a \times b = |a| \cdot b$ ($\cdot$ 表示数的乘法运算), 问 $\mathbf{R}$ 与运算 $\times$ 能否构成半群?

解 对于任意的 $a, b, c \in \mathbf{R}$, 有

$$(a \times b) \times c = (|a| \cdot b) \times c = ||a| \cdot b| \cdot c = |a| \cdot |b| \cdot c,$$

$$a \times (b \times c) = |a| \cdot (b \times c) = |a| \cdot (|b| \cdot c) = |a| \cdot |b| \cdot c,$$

所以

$$(a \times b) \times c = a \times (b \times c),$$

故 $\langle \mathbf{R}; \times \rangle$ 是一个半群.

例 5-2 考察例 5-1 中的半群 $\langle S; * \rangle$,它是否是一个独异点?

解 对任意的 $b \in S$,若 a 是左单位元,则

$$a \times b = |a| \cdot b = b. \quad (1)$$

要使式(1)成立,只有 $|a| = 1$. 即 $a = 1$ 或 $a = -1$. 因此 1 和 -1 均是运算 $\times$ 的左单位元.

对任意的 $a \in S$,若 b 是右单位元,则有

$$a \times b = |a| \cdot b = a. \quad (2)$$

当 $a > 0$ 时,要使式(2)成立,必须 $b = 1$.

当 $a < 0$ 时,要使式(2)成立,必须 $b = -1$.

因此,1 和 -1 均不能成为运算 $\times$ 的右单位元. 于是运算 $\times$ 不存在单位元. 故半群 $\langle S; * \rangle$ 不是独异点.

例 5-3 设 $A=\{0,1,2,3\}$, $\odot_4$ 为模 4 乘法, 即

$$a \odot_4 b = \text{res}_4(a \cdot b).$$

试问 A 和 $\odot_4$ 能否构成独异点?

解 构造模 4 乘法在 A 上的运算表(见表 5-1). 显然运算结果均是 A 中的元素, 所以 $\langle A; \odot_4 \rangle$ 构成一代数系统.

表 5-1

$\odot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

对于任意的 $a, b, c \in A$, 令

$$a \cdot b = 4m_1 + \text{res}_4(a \cdot b), \quad b \cdot c = 4m_2 + \text{res}_4(b \cdot c),$$

则

$$\begin{aligned} (a \odot_4 b) \odot_4 c &= \text{res}_4(a \cdot b) \odot_4 c = \text{res}_4((\text{res}_4(a \cdot b)) \cdot c) \\ &= \text{res}_4((4m_1 + \text{res}_4(a \cdot b)) \cdot c) = \text{res}_4((a \cdot b) \cdot c), \\ a \odot_4 (b \odot_4 c) &= a \odot_4 \text{res}_4(b \cdot c) = \text{res}_4(a \cdot \text{res}_4(bc)) \\ &= \text{res}_4(a \cdot (4m_2 + \text{res}_4(b \cdot c))) = \text{res}_4(a \cdot (b \cdot c)). \end{aligned}$$

因为数的乘法运算 $\cdot$ 是可结合的, 所以

$$(a \odot_4 b) \odot_4 c = a \odot_4 (b \odot_4 c),$$

即 $\odot_4$ 满足结合律.

由运算表可看出, 1 是 $\odot_4$ 的左单位元, 也是右单位元, 因此 1 是 $\odot_4$ 的单位元. 故 $\langle A; \odot_4 \rangle$ 是一独异点.

例 5-4 考察例 5-3 中的独异点是否为循环独异点?

解 例 5-3 中的独异点 $\langle A; \odot_4 \rangle$ 不是循环独异点. 因为 A 中不存在元素 g 能满足循环独异点的定义条件.

例如, $0^0 = 1, 0^1 = 0^2 = 0^3 = \cdots = 0$;

$1^0 = 1^1 = 1^2 = 1^3 = \cdots = 1$;

$2^0 = 1, 2^1 = 2, 2^2 = 2^3 = 2^4 = \cdots = 0$;

$3^1 = 3^3 = 3^5 = \cdots = 3, 3^0 = 3^2 = 3^4 = \cdots = 1$.

例 5-6 设 $S = \left\{ \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix} \mid a, b \in \mathbf{R} \right\}$ ($\mathbf{R}$ 是实数集), $\cdot$ 是矩阵的乘法运算, 则

$\langle S; \cdot \rangle$ 是一个半群. 因为矩阵 $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ 是其单位元, 所以 $\langle S; \cdot \rangle$ 也是一个独异点. 设

$$T = \left\{ \begin{bmatrix} a & 0 \\ 0 & 0 \end{bmatrix} \mid a \in \mathbf{R} \right\},$$

则 $T \subseteq S$, 且 $\cdot$ 在 T 上封闭, 所以 $\langle T; \cdot \rangle$ 是 $\langle S; \cdot \rangle$ 的子半群.

在 $\langle T; \cdot \rangle$ 中, $\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ 是单位元, 所以 $\langle T; \cdot \rangle$ 是一独异点. 但因为 $\langle S; \cdot \rangle$ 的单位元 $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \notin T$, 所以 $\langle T; \cdot \rangle$ 不是 $\langle S; \cdot \rangle$ 的子独异点. 设

$$H = \left\{ \begin{bmatrix} a & 0 \\ 0 & a \end{bmatrix} \mid a \in \mathbf{R} \right\},$$

则 $H \subseteq S$, 且 $\cdot$ 在 H 上是封闭的, 所以 $\langle H; \cdot \rangle$ 是 $\langle S; \cdot \rangle$ 的子半群. 因为单位元 $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \in H$, 所以 $\langle H; \cdot \rangle$ 是 $\langle S; \cdot \rangle$ 的子独异点.

例 5-7 设 $G = \mathbf{Q} - \{1\}$ ($\mathbf{Q}$ 为有理数集), 定义 G 上的二元运算 $*$ 为 $a * b = a + b - ab$. 试问 $\langle G; * \rangle$ 是群吗?

解 对任意的 $a, b, c \in G$, 有

$$\begin{aligned}(a * b) * c &= (a + b - ab) * c = a + b - ab + c - (a + b - ab)c \\ &= a + b + c - ab - ac - bc + abc,\end{aligned}$$

$$\begin{aligned}a * (b * c) &= a * (b + c - bc) = a + b + c - bc - a(b + c - bc) \\ &= a + b + c - bc - ab - ac + abc,\end{aligned}$$

所以

$$(a * b) * c = a * (b * c).$$

又对于任意 $a \in G$, $0 * a = a * 0 = a$, 所以 0 是 $\langle G; * \rangle$ 的单位元.

对任意 $a \in G$, 有 $a * \frac{a}{a-1} = \frac{a}{a-1} * a = 0$. 所以每一元素 a 均有逆元, 其逆元为

$$\frac{a}{a-1}.$$

由上可知, $\langle G; * \rangle$ 是一个群.

若将集合 $G = \mathbf{Q} - \{1\}$ 改为 $G = \mathbf{Q}$, 则 $\langle \mathbf{Q}; * \rangle$ 不是群. 因为 1 没有逆元, 不符合群的定义.

例 5-8 设有代数系统 $\langle \mathbf{Z}; \circ \rangle$, 其中 $\mathbf{Z}$ 为整数集, 运算 $\circ$ 定义为, 对于任意 $a, b \in \mathbf{Z}$,

$$a \circ b = a + b - 2.$$

试问 $\langle \mathbf{Z}; \circ \rangle$ 是否为循环群?

解 对任意 $a, b, c \in \mathbf{Z}$, 有

$$(a \circ b) \circ c = (a + b - 2) \circ c = a + b - 2 + c - 2 = a + b + c - 4,$$

$$a \circ (b \circ c) = a \circ (b + c - 2) = a + b + c - 2 - 2 = a + b + c - 4,$$

因此

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

又对于任意的 $a \in \mathbf{Z}$, $a \circ 2 = a + 2 - 2 = a$ 且运算 $\circ$ 是可交换的, 所以有单位元 2.

对任意 $a \in \mathbf{Z}$, 若 $a \circ b = a + b - 2 = 2$, 则 $b = 4 - a$. 因此每一元素 a 均有逆元 $a^{-1} = 4 - a$.

由上可知 $\langle \mathbf{Z}; \circ \rangle$ 是一个群.

$\langle \mathbf{Z}; \circ \rangle$ 也是一循环群. 生成元是 1, 不难验证, 对于任意整数 n , $1^n = 2 - n$. 因此对于任意整数 n , $n = 1^{2-n}$. 3 也是生成元, 对于任意整数 n , $3^n = n + 2$.

例 5-9 设有群 $\langle Z_6; \oplus_6 \rangle$, 其中 $Z_6 = \{0, 1, 2, 3, 4, 5\}$, $\oplus_6$ 是模 6 加法, 即对于任意的 $a, b \in Z_6$, $a \oplus_6 b = \text{res}_6(a+b)$. 试求出群 $\langle Z_6; \oplus_6 \rangle$ 的阶和群中每一元素的周期.

解 因为 Z_6 的元素个数是 6, 所以群 $\langle Z_6; \oplus_6 \rangle$ 的阶为 6.

因为 0 是单位元, 所以 0 的周期是 1.

因为 $1^1 = 1, 1^2 = 1 \oplus_6 1 = 2, 1^3 = 1^2 \oplus_6 1 = 2 \oplus_6 1 = 3, 1^4 = 1^3 \oplus_6 1 = 3 \oplus_6 1 = 4, 1^5 = 1^4 \oplus_6 1 = 4 \oplus_6 1 = 5, 1^6 = 1^5 \oplus_6 1 = 5 \oplus_6 1 = 0$, 所以 1 的周期是 6.

因为 $2^1 = 2, 2^2 = 2 \oplus_6 2 = 4, 2^3 = 2^2 \oplus_6 2 = 4 \oplus_6 2 = 0$, 所以 2 的周期是 3.

因为 $3^1 = 3, 3^2 = 3 \oplus_6 3 = 0$, 所以 3 的周期是 2.

因为 $4^1 = 4, 4^2 = 4 \oplus_6 4 = 2, 4^3 = 2 \oplus_6 4 = 0$, 所以 4 的周期是 3.

因为 $5^1 = 5, 5^2 = 5 \oplus_6 5 = 4, 5^3 = 4 \oplus_6 5 = 3, 5^4 = 3 \oplus_6 5 = 2, 5^5 = 2 \oplus_6 5 = 1, 5^6 = 1 \oplus_6 5 = 0$, 所以 5 的周期是 6.

由上也可看出, 群 $\langle Z_6; \oplus_6 \rangle$ 是一循环群. 1 或 5 是其生成元, 且生成元的周期与循环群 $\langle G; * \rangle$ 的阶相等.

例 5-11 设 $\langle G; * \rangle$ 是一个独异点, 且对于任意的 $a \in G$, 均有 $a * a = e$. 试证明 $\langle G; * \rangle$ 是交换群.

证 因为对于任意 $a \in G$, 均有 $a * a = e$, 所以任意元素 a 均有逆元, 且 $a^{-1} = a$. 因此 $\langle G; * \rangle$ 是一个群. 于是对于任意的 $a, b \in G$, 有

$$a * b = (a * b)^{-1}.$$

又根据上述群的性质得 $(a * b)^{-1} = b^{-1} * a^{-1}$, 因此

$$a * b = b^{-1} * a^{-1} = b * a.$$

故 $\langle G; * \rangle$ 是一交换群.

群 $\langle Z_6; \oplus_6 \rangle$ 0 是单位元, 所以 0 的周期是 1.

$1^1 = 1, 1^2 = 1 \oplus_6 1 = 2, 1^3 = 1^2 \oplus_6 1 = 2 \oplus_6 1 = 3, 1^4 = 1^3 \oplus_6 1 = 3 \oplus_6 1 = 4, 1^5 = 1^4 \oplus_6 1 = 4 \oplus_6 1 = 5, 1^6 = 1^5 \oplus_6 1 = 5 \oplus_6 1 = 0$, 所以 1 的周期是 6.

$2^1 = 2, 2^2 = 2 \oplus_6 2 = 4, 2^3 = 2^2 \oplus_6 2 = 4 \oplus_6 2 = 0$, 所以 2 的周期是 3.

$3^1 = 3, 3^2 = 3 \oplus_6 3 = 0$, 所以 3 的周期是 2.

$4^1 = 4, 4^2 = 4 \oplus_6 4 = 2, 4^3 = 2 \oplus_6 4 = 0$, 所以 4 的周期是 3.

$5^1 = 5, 5^2 = 5 \oplus_6 5 = 4, 5^3 = 4 \oplus_6 5 = 3, 5^4 = 3 \oplus_6 5 = 2, 5^5 = 2 \oplus_6 5 = 1, 5^6 = 1 \oplus_6 5 = 0$, 所以 5 的周期是 6.

例 5-14 例 5-9 中群 $\langle Z_6; \oplus_6 \rangle$ 的阶为 6, G 中 每一元素的周期均是 6 的因子. 1 和 5 互为逆元, 其周期均为 6; 2 和 4 互为逆元, 其周期均为 3; 3 以自身为逆元, 其周期为 2. 单位元 0 的周期为 1. $\langle Z_6; \oplus_6 \rangle$ 是一循环群, 生成元 1 和 5 的周期与群的阶相等.

群 $\langle Z_6; \oplus_6 \rangle$ 中周期大于 2 的元素个数是 4 个. 它们分别是 1、5、2、4. 周期等于 2 的元素个数是 1 个, 仅元素 3.

浙江大学信息与电子工程学院电子系宋牟平

设 $V_1 = \langle S_1; * \rangle$ 和 $V_2 = \langle S_2; \circ \rangle$ 是两个代数系统, f 是从 V_1 到 V_2 的同态. 如果 f 不是满同态, 那么 S_1 关于 $*$ 的单位元 e_1 通过 f 映射的像不一定是 S_2 关于 $\circ$ 的单位元. S_1 中任一元素 a 的逆元 a^{-1} 通过 f 映射的像 $f(a^{-1})$ 不一定是 $f(a)$ 的逆元. 但是, 若 V_1 和 V_2 这两个代数系统都是群, 则情形就不一样了.

例 5-15 设 f 是由群 $\langle G_1; * \rangle$ 到群 $\langle G_2; \circ \rangle$ 的同态, e_1 和 e_2 分别是这两个群的单位元, 则

- (1) $f(e_1) = e_2$;
- (2) 对任意的 $a \in G$, 有 $f(a^{-1}) = (f(a))^{-1}$.

证 (1) 因为 f 是同态, 所以 $f(e_1) = f(e_1 * e_1) = f(e_1) \circ f(e_1)$, 即 $f(e_1)$ 是 $\langle G_2; \circ \rangle$ 中的幂等元. 但群中除单位元外, 没有其他任何幂等元, 因此 $f(e_1) = e_2$. 下面给出这一结论的证明.

$$\begin{aligned} f(e_1) &= e_2 \circ f(e_1) = ((f(e_1))^{-1} \circ f(e_1)) \circ f(e_1) \\ &= (f(e_1))^{-1} \circ (f(e_1) \circ f(e_1)) = (f(e_1))^{-1} \circ f(e_1) = e_2. \end{aligned}$$

- (2) 对于任意 $a \in G_1$,

$$f(e_1) = f(a * a^{-1}) = f(a) \circ f(a^{-1}) = e_2.$$

又因 $f(a) \circ (f(a))^{-1} = e_2$, 因此

$$f(a) \circ f(a^{-1}) = f(a) \circ (f(a))^{-1}.$$

由群的消去律, 得

$$f(a^{-1}) = (f(a))^{-1}.$$

例 5-19 设 f 和 g 都是由群 $\langle G_1; * \rangle$ 到群 $\langle G_2; \circ \rangle$ 的同态, 令

$$H = \{a \mid a \in G_1, f(a) = g(a)\},$$

试证明 H 对于运算 $*$ 构成 $\langle G_1; * \rangle$ 的子群.

证 f 和 g 都是由群 $\langle G_1; * \rangle$ 到群 $\langle G_2; \circ \rangle$ 的同态, 由例 5-15 可知 $f(e_1) = g(e_1) = e_2$ (e_1 和 e_2 分别是 $\langle G_1; * \rangle$ 和 $\langle G_2; \circ \rangle$ 的单位元), 因此 $e_1 \in H$, H 非空.

设 $a, b \in H$, 则 $f(a) = g(a)$, $f(b) = g(b)$, 又由例 5-15 知, $f(b^{-1}) = (f(b))^{-1}$, $g(b^{-1}) = (g(b))^{-1}$, 于是

$$\begin{aligned} f(a * b^{-1}) &= f(a) \circ f(b^{-1}) = f(a) \circ (f(b))^{-1} = g(a) \circ (g(b))^{-1} \\ &= g(a) \circ g(b^{-1}) = g(a * b^{-1}). \end{aligned}$$

因此 $a * b^{-1} \in H$. 故 $\langle H; * \rangle$ 是群 $\langle G_1; * \rangle$ 的子群.

例 5-20 试对例 5-9 中的群 $\langle Z_6; \oplus_6 \rangle$, 找出它的所有子群.

解 因为群 $\langle Z_6; \oplus_6 \rangle$ 是一阶为 6 的有限群, 所以只要找出对运算 $\oplus_6$ 封闭的子集. 根据这一判别条件, $\langle Z_6; \oplus_6 \rangle$ 有如下子群:

(1) $\langle \{0\}; \oplus_6 \rangle;$

(2) $\langle \{0, 3\}; \oplus_6 \rangle;$

(3) $\langle \{0, 2, 4\}; \oplus_6 \rangle;$

(4) $\langle Z_6; \oplus_6 \rangle.$

例 5-21 非零实数集 $\mathbf{R}-\{0\}$ 对于通常数的乘法运算构成群 $\langle \mathbf{R}-\{0\}; \cdot \rangle$. 集合 $\{-1, 1\}$ 是 $\mathbf{R}-\{0\}$ 的有限子集, 且运算 $\cdot$ 在 $\{-1, 1\}$ 上是封闭的, 因此 $\langle \{-1, 1\}; \cdot \rangle$ 是群 $\langle \mathbf{R}-\{0\}; \cdot \rangle$ 的子群.

例 5-22 例 5-21 中群 $\langle \mathbf{R}-\{0\}; \cdot \rangle$ 的子群 $\langle \{-1, 1\}; \cdot \rangle$ 关于 1, 2, 3 以及关于 -1, -2, -3 的左陪集如下:

$$\begin{aligned} 1 \cdot \{-1, 1\} &= \{-1, 1\}; & -1 \cdot \{-1, 1\} &= \{1, -1\}; \\ 2 \cdot \{-1, 1\} &= \{-2, 2\}; & -2 \cdot \{-1, 1\} &= \{2, -2\}; \\ 3 \cdot \{-1, 1\} &= \{-3, 3\}; & -3 \cdot \{-1, 1\} &= \{3, -3\}. \end{aligned}$$

由上可以看出, 对于任意非零实数 a , 子群 $\langle \{-1, 1\}; \cdot \rangle$ 关于 a 和关于 $-a$ 的左陪集是相等的. 即对于任意 $a \in \mathbf{R}-\{0\}$, 有 $a \cdot \{-1, 1\} = -a \cdot \{-1, 1\}$.

因为运算 $\cdot$ 是可交换的, 所以对于任意 $a \in \mathbf{R}-\{0\}$, 又有

$$a \cdot \{-1, 1\} = \{-a, a\}, \quad \{-1, 1\} \cdot a = \{-a, a\},$$

因此子群 $\langle \{-1, 1\}; \cdot \rangle$ 关于元素 a 的左陪集和右陪集是相等的, 即对于任意的 $a \in \mathbf{R}-\{0\}$, 有 $a \cdot \{-1, 1\} = \{-1, 1\} \cdot a$.

例 5-23 列出例 5-9 中群 $\langle Z_6; \oplus_6 \rangle$ 的子群 $\langle \{0, 2, 4\}; \oplus_6 \rangle$ 的所有右陪集.

解 $\{0, 2, 4\} \oplus_6 0 = \{0, 2, 4\}; \quad \{0, 2, 4\} \oplus_6 1 = \{1, 3, 5\};$

$$\{0, 2, 4\} \oplus_6 2 = \{2, 4, 0\}; \quad \{0, 2, 4\} \oplus_6 3 = \{3, 5, 1\};$$

$$\{0, 2, 4\} \oplus_6 4 = \{4, 0, 2\}; \quad \{0, 2, 4\} \oplus_6 5 = \{5, 1, 3\}.$$

由上看出

$$\{0, 2, 4\} \oplus_6 0 = \{0, 2, 4\} \oplus_6 2 = \{0, 2, 4\} \oplus_6 4;$$

$$\{0, 2, 4\} \oplus_6 1 = \{0, 2, 4\} \oplus_6 3 = \{0, 2, 4\} \oplus_6 5.$$

因此子群 $\langle \{0, 2, 4\}; \oplus_6 \rangle$ 在群 $\langle Z_6; \oplus_6 \rangle$ 中只有两个不同的右陪集.

对于群 $\langle G; * \rangle$ 的子群 $\langle H; * \rangle$,如何判别 $\langle H; * \rangle$ 是否为 $\langle G; * \rangle$ 的正规子群呢? 有如下三种方法.

(1) 根据正规子群的定义,如果对于每一个 $a \in G$,都有 $a * H = H * a$,则 $\langle H; * \rangle$ 是群 $\langle G; * \rangle$ 的正规子群.

(2) 如果对于每一个 $a \in G$,都有 $a * H * a^{-1} = H$,则 $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的正规子群.

(3) 如果对于每一个 $a \in G$,都有 $a * H * a^{-1} \subseteq H$,则 $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的正规子群.

例 5-25 设 $\langle G; * \rangle$ 是一个群,定义 G 的子集 H 为

$$H = \{a \mid a * x = x * a, \text{对于任意的 } x \in G\}.$$

分析 在例 5-17 中证明了 $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的子群. 实际上, $\langle H; * \rangle$ 也是 $\langle G; * \rangle$ 的正规子群. 对此,只要证明对于任意的 $b \in G, b * H * b^{-1} \subseteq H$ 即可.

证 因为对于任意的 $a \in H$ 和任意的 $b \in G$,有

$$b * a * b^{-1} = b * (a * b^{-1}) = b * (b^{-1} * a) = (b * b^{-1}) * a = e * a = a \in H,$$

所以, $b * H * b^{-1} \subseteq H$. 故 $\langle H; * \rangle$ 是群 $\langle G; * \rangle$ 的正规子群.

$$\begin{aligned}\{0,2,4\} \oplus_6 0 &= \{0,2,4\}; & \{0,2,4\} \oplus_6 1 &= \{1,3,5\}; \\ \{0,2,4\} \oplus_6 2 &= \{2,4,0\}; & \{0,2,4\} \oplus_6 3 &= \{3,5,1\}; \\ \{0,2,4\} \oplus_6 4 &= \{4,0,2\}; & \{0,2,4\} \oplus_6 5 &= \{5,1,3\}.\end{aligned}$$

例 5-26 对于例 5-23 求出群 $\langle Z_6; \oplus_6 \rangle$ 中与子群 $\langle \{0,2,4\}; \oplus_6 \rangle$ 相关的右陪集分划和左陪集分划.

解 在例 5-23 中,已求出子群 $\langle \{0,2,4\}; \oplus_6 \rangle$ 关于 Z_6 中每一元素的右陪集,易发现它只有两个不同的右陪集. 这两个右陪集构成 G 的一个分划. 因此与子群 $\langle \{0,2,4\}; \oplus_6 \rangle$ 相关的右陪集分划

$$\Pi = \{\{0,2,4\}, \{1,3,5\}\}.$$

因为 $\langle Z_6; \oplus_6 \rangle$ 是交换群,对于任意 $a \in Z_6$, 均有 $a \oplus_6 \{0,2,4\} = \{0,2,4\} \oplus_6 a$, 所以与子群 $\langle \{0,2,4\}; \oplus_6 \rangle$ 相关的左陪集分划也是 Π .

例 5-27 对于群 $\langle \mathbf{Q}^*; \cdot \rangle$ (其中 $\mathbf{Q}^*$ 为非零有理数集, $\cdot$ 是通常数的乘法), 若令 $H = \{-1, 1\}$, 则 $\langle H; \cdot \rangle$ 构成 $\langle \mathbf{Q}^*; \cdot \rangle$ 的子群. 试求出子群 $\langle H; \cdot \rangle$ 的所有左陪集.

解 对于每一个正有理数 q , 相应的左陪集为

$$q \cdot H = q \cdot \{-1, 1\} = \{-q, q\}.$$

对于每一个负有理数 $-q$, 相应的左陪集为

$$-q \cdot H = -q \cdot \{-1, 1\} = \{q, -q\}.$$

因此有

$$q \cdot H = -q \cdot H.$$

但对于任意两个正有理数 q_1 和 q_2 , 若 $q_1 \neq q_2$, 则

$$q_1 \cdot H \neq q_2 \cdot H.$$

因此 $\langle H; * \rangle$ 的所有左陪集由每一个 $q \in \mathbf{Q}^+$ ($\mathbf{Q}^+$ 表示正有理数集) 相关的左陪集 $q \cdot H = \{-q, q\}$ 组成. 这些左陪集构成 $\mathbf{Q}^*$ 的一个分划, 即

$$\Pi = \{q \cdot H \mid q \in \mathbf{Q}^+\}.$$

因为运算 $\cdot$ 是可交换的, 对于每一个 $a \in \mathbf{Q}^*$, $a * H = H * a$, 所以上述与子群 $\langle H; * \rangle$ 相关的左陪集分划 Π , 也是与 $\langle H; \cdot \rangle$ 相关的右陪集分划. 每一个分划块都由 2 个元素组成.

例 5-28 对于群 $\langle \mathbf{Q}; + \rangle$ (其中 $\mathbf{Q}$ 为有理数集, $+$ 为通常数的加法运算), 若令 $\mathbf{Z}$ 为所有整数的集合, 则 $\langle \mathbf{Z}; + \rangle$ 构成 $\langle \mathbf{Q}; + \rangle$ 的子群, 试求出子群 $\langle \mathbf{Z}; + \rangle$ 的所有右陪集.

解 任意两个相邻的整数 i 与 $i+1$ 之间都有无穷多个有理数. 在区间 $[0, 1)$ 内任取一有理数 a , 则

$$\cdots, -3+a, -2+a, -1+a, 0+a, 1+a, 2+a, 3+a, \cdots$$

也都是有理数, 这些有理数构成的集合是 $\langle \mathbf{Z}; + \rangle$ 的一个右陪集

$$\mathbf{Z}+a = \{i+a \mid i \in \mathbf{Z}\}.$$

于是, 子群 $\langle \mathbf{Z}; + \rangle$ 的所有右陪集由与区间 $[0, 1)$ 中的每一个有理数 a 相关的右陪集组成. 注意到当 $a=0$ 时, $\mathbf{Z}+a = \mathbf{Z}$ 也是子群 $\langle \mathbf{Z}; + \rangle$ 的一个右陪集. 上述这些右陪集构成 $\mathbf{Q}$ 的与子群 $\langle \mathbf{Z}; + \rangle$ 相关的右陪集分划

$$\Pi = \{\mathbf{Z}+a \mid 0 \leq a < 1\}.$$

由于运算 $+$ 可交换, 对于任意 $a \in \mathbf{Q}$, $\mathbf{Z}+a = a+\mathbf{Z}$, 所以这个分划简称为与 $\langle \mathbf{Z}; + \rangle$ 相关的陪集分划.

例 5-29 设 $\langle S; \circ \rangle$ 是一个有单位元 e 的半群, 令

$$G = S^S = \{f \mid f: S \rightarrow S\}.$$

对任意的 $f, g \in G$, 任意的 $x \in S$, 定义 $(f * g)(x) = f(x) \circ g(x)$, 试证明 G 相对于运算 $*$ 也构成一个有单位元的半群.

证 因为 $\circ$ 在 S 上是封闭的, 所以对于任意的 $f, g \in G$, 有 $f * g \in G$, 因此 $\langle G; * \rangle$ 是一个代数系统.

对于任意的 $f, g, h \in G$ 和任意的 $x \in S$, 因为 S 上的运算 $\circ$ 是可结合的, 故有

$$\begin{aligned} ((f * g) * h)(x) &= (f * g)(x) \circ h(x) = (f(x) \circ g(x)) \circ h(x) \\ &= f(x) \circ (g(x) \circ h(x)) = f(x) \circ (g * h)(x) \\ &= (f * (g * h))(x). \end{aligned}$$

因此 $(f * g) * h = f * (g * h)$, 即 $*$ 是可结合的, 故 $\langle G; * \rangle$ 是一个半群.

定义 $f_0: S \rightarrow S$, 对于任意 $x \in S$, $f_0(x) = e$. 于是对于任意 $f \in G$ 和任意 $x \in S$, 有

$$(f * f_0)(x) = f(x) \circ f_0(x) = f(x) \circ e = f(x).$$

类似地, 有 $(f_0 * f)(x) = f(x)$. 因此 f_0 是 $\langle G; * \rangle$ 中的单位元.

由上证得, $\langle G; * \rangle$ 是一个有单位元的半群.

浙江大学信息与电子工程学院 电子系 宋牟平

例 5-30 设 $\langle S; * \rangle$ 是一半群, 令 $G = S^S$ (S^S 的意义同例 5-29). 函数的复合运算 $\circ$ 在 G 上显然是封闭的, 且因为函数的复合运算满足结合律, 所以 $\langle G; \circ \rangle$ 是一个半群. 现令 G 的子集

$$H = \{f_a \mid a \in S \text{ 且 } f_a(x) = a * x\}.$$

试证明 H 相对于运算 $\circ$ 构成 $\langle G; \circ \rangle$ 的子半群.

分析 根据子半群的定义, 只要证明运算 $\circ$ 在 H 上封闭即可.

证 对于任意的 $f_a, f_b \in H$ 和任意的 $x \in S$, 有

$$(f_a \circ f_b)(x) = f_a(f_b(x)) = f_a(b * x) = a * (b * x) = (a * b) * x.$$

因为 $\langle S; * \rangle$ 是半群, 所以 $a * b \in S$, 因此 $(f_a \circ f_b) = f_{a * b} \in H$. 故 $\circ$ 在 H 上是封闭的, $\langle H; \circ \rangle$ 是 $\langle G; \circ \rangle$ 的子半群.

例 5-31 设 $\langle S; * \rangle$ 是一个半群, 且对于任意的 $a, b \in S$, 由 $a \neq b$, 必有 $a * b \neq b * a$. 试证明:

- (1) 对任意的 $a \in S$, 有 $a * a = a$;
- (2) 对任意的 $a, b \in S$, 有 $a * b * a = a$;
- (3) 对任意的 $a, b, c \in S$, 有 $a * b * c = a * c$.

证 “由 $a \neq b$, 必有 $a * b \neq b * a$ ”这一条件等价于“由 $a * b = b * a$ 必有 $a = b$ ”. 根据与之等价的后一条件来证明.

(1) 因为运算 $*$ 是可结合的, 所以对于任意 $a \in S$, 有 $(a * a) * a = a * (a * a)$. 于是, 根据题设条件必有 $a * a = a$.

(2) 对任意的 $a, b \in S$, 有

$$(a * b * a) * a = (a * b) * (a * a) = a * b * a,$$

$$a * (a * b * a) = (a * a) * (b * a) = a * b * a,$$

因此

$$(a * b * a) * a = a * (a * b * a),$$

故

$$a * b * a = a.$$

(3) 对任意的 $a, b, c \in S$, 有

$$(a * b * c) * (a * c) = (a * b) * (c * a * c) = a * b * c,$$

$$(a * c) * (a * b * c) = (a * c * a) * (b * c) = a * b * c,$$

因此

$$(a * b * c) * (a * c) = (a * c) * (a * b * c),$$

故

$$a * b * c = a * c.$$

浙江大学信息与电子工程学院电子系宋牟平

例 5-34 试证明凡阶分别为 1,2,3,4 的群都是交换群,举一个阶为 6 且不可交换的群的例子.

表 5-4

e	e	a
e	e	a
a	a	e

证 若 $\langle G; * \rangle$ 是阶为 1 的群,则 G 中只有单位元 e 这唯一一个元素, $e * e = e$. 显然 $\langle G; * \rangle$ 是一交换群.

若 $\langle G; * \rangle$ 阶为 2,设 $G = \{e, a\}$,因为 $e * e = e$,由逆元的唯一性,必有 $a * a = e$,又由 e 是单位元,有 $a * e = e * a = a$,因此 $\langle G; * \rangle$ 是交换群.这种群的运算表如表 5-4 所示.

若 $\langle G; * \rangle$ 阶为 3,设 $G = \{e, a, b\}$,则因为 $e * b = b$,由群的消去律, $a * b \neq b$;因为 $a * e = a$,由群的消去律得 $a * b \neq a$,因此 $a * b = e$. 于是有

$$b * a = b * a * b * b^{-1} = b * (a * b) * b^{-1} = b * e * b^{-1} = e,$$

因此 $a * b = b * a$. 故 $\langle G; * \rangle$ 是一交换群.

这种群的运算表如表 5-5 所示.

由于 $a * e = a, a * b = e$,由群的消去律, $a * a$ 必等于 b . 类似地, $b * b$ 只能等于 a .

若 $\langle G; * \rangle$ 阶为 4,设 $G = \{e, a, b, c\}$,下面分两种情形讨论.

表 5-5

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

浙江大学信息与电子工程学院 电子系 宋牟平

(1) 若 a, b, c 中有两个元素互为逆元. 不妨设 $a * b = b * a = e$, 于是 $c * c = e$. 又由 $e * c = c, a * e = a$, 根据消去律, 只能满足 $a * c = b$. 又因为 $e * a = a, c * e = c, b * a = e$, 所以只能是 $c * a = b$. 因此 $a * c = c * a$.

类似地, 因为 $e * c = c, b * e = b, b * a = e$, 所以只能是 $b * c = a$. 因为 $c * e = c, e * b = b, a * b = e$, 所以只能是 $c * b = a$. 因此 $b * c = c * b$.

由上可知, $\langle G; * \rangle$ 是一交换群. 这种群的运算表如表 5-6 所示.

表 5-6

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

浙江大学信息与电子工程学院电子系宋牟平

(2) 若 a, b, c 中每一元素都以自身为逆元, 即若 $a * a = e, b * b = e, c * c = e$, 则由

$$a * e = a, e * b = b, b * b = e, \text{得 } a * b = c;$$

由 $e * a = a, a * a = e, b * e = b$, 得 $b * a = c$;

因此 $a * b = b * a$.

类似地, 可以证明 $b * c = c * b = a; a * c = c * a = b$. 因此 $\langle G; * \rangle$ 是一交换群. 这种群的运算表如表 5-7 所示.

表 5-7

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

例 5-24 中集合 $A = \{a, b, c\}$ 上所有置换构成的三次对称群 $\langle P; \circ \rangle$ 是一个阶为 6 的非交换群.

例 5-35 设 $\langle G; \circ \rangle$ 是一个群, $u \in G$, 在 G 中定义新的运算 $*$, 使得对于任意的 $a, b \in G, a * b = a \circ u^{-1} \circ b$. 试证明 $\langle G; * \rangle$ 也是一个群.

证 因为 $\langle G; \circ \rangle$ 是一个群, 所以运算 $*$ 在 G 上封闭.

对于任意的 $a, b, c \in G$, 有

$$\begin{aligned}(a * b) * c &= (a \circ u^{-1} \circ b) * c = (a \circ u^{-1} \circ b) \circ u^{-1} \circ c \\ &= a \circ u^{-1} \circ (b \circ u^{-1} \circ c) = a * (b * c),\end{aligned}$$

所以运算 $*$ 可结合.

设 $\langle G; \circ \rangle$ 的单位元为 e , 则对于任意的 $a \in G$, 有

$$\begin{aligned}a * u &= a \circ u^{-1} \circ u = a \circ e = a, \\ u * a &= u \circ u^{-1} \circ a = e \circ a = a,\end{aligned}$$

所以运算 $*$ 有单位元 u .

对于任意的 $a \in G$, 设 a 关于运算 $\circ$ 的逆元是 a^{-1} , 则

$$\begin{aligned}a * (u \circ a^{-1} \circ u) &= a \circ u^{-1} \circ u \circ a^{-1} \circ u = u, \\ (u \circ a^{-1} \circ u) * a &= u \circ a^{-1} \circ u \circ u^{-1} \circ a = u,\end{aligned}$$

所以每一元素 a 关于运算 $*$ 有逆元 $u \circ a^{-1} \circ u$.

由上证得, $\langle G; * \rangle$ 是一个群.

浙江大学信息与电子工程学院电子系宋牟平

例 5-38 设 $\langle G; * \rangle$ 是一循环群, f 是从 $\langle G; * \rangle$ 到 $\langle G'; \circ \rangle$ 的满同态($\circ$ 是二元运算). 试证明 $\langle G'; \circ \rangle$ 也是循环群.

证 因为 f 是从群 $\langle G; * \rangle$ 到 $\langle G'; \circ \rangle$ 的满同态, 由满同态的性质, $\langle G'; \circ \rangle$ 也是一个群.

设 g 是群 $\langle G; * \rangle$ 的生成元, 且 $f(g) = g'$. 对任一 $a' \in G'$, 由 f 是满射, 必存在 $a \in G$, 使得 $f(a) = a'$.

设 $a = g^i$ (i 为某一整数), 则

$$a' = f(a) = f(g^i).$$

若 $i=0$, 则 $a' = f(g^0) = f(e) = e' = (g')^0$.

若 $i>0$, 则

$$a' = f(g^i) = f(\underbrace{g * g * \cdots * g}_{i\text{个}}) = \underbrace{f(g) \circ f(g) \circ \cdots \circ f(g)}_{i\text{个}} = (g')^i.$$

若 $i<0$, 则 $i = -|i|$, 于是由满同态的性质, 得

$$a' = f(g^i) = f((g^{|i|})^{-1}) = (f(g^{|i|}))^{-1} = ((g')^{|i|})^{-1} = (g')^i.$$

由 $a' \in G'$ 的任意性知, $\langle G'; \circ \rangle$ 是一循环群.

例 5-40 设 $\langle A; * \rangle$ 和 $\langle B; * \rangle$ 都是群 $\langle G; * \rangle$ 的正规子群,试证明 $A * B$ 对于运算 $*$ 也构成 $\langle G; * \rangle$ 的正规子群.

分析 (1) $\langle A; * \rangle$ 是 $\langle G; * \rangle$ 的正规子群意味着对于任意的 $g \in G$,有 $g * A = A * g$. 同样地, $\langle B; * \rangle$ 是 $\langle G; * \rangle$ 的正规子群意味着对于任意的 $g \in G$,有 $g * B = B * g$.

(2) $g * A = A * g$ 意味着对于任意的 $a \in A$,必存在元素 $a' \in A$,使得 $g * a = a' * g$.

特别要注意的是,这里不能写作 $g * a = a * g$.

(3) 要证明 $A * B$ 与运算 $*$ 能构成 $\langle G; * \rangle$ 的正规子群,需要证明以下两点.

① $A * B$ 与运算 $*$ 能构成 $\langle G; * \rangle$ 的子群:由 $a_1 * b_1, a_2 * b_2 \in A * B$,可推出 $(a_1 * b_1) * (a_2 * b_2)^{-1} \in A * B$.

② $\langle A * B; * \rangle$ 是 $\langle G; * \rangle$ 的正规子群:对于任意 $g \in G$,有 $g * (A * B) * g^{-1} \subseteq A * B$;即对于任意的 $g \in G$ 和任意的 $a * b \in A * B$,有 $g * (a * b) * g^{-1} \in A * B$.

证 因为 $e \in A, e \in B$, 所以 $e \in A * B$, 因此 $A * B$ 非空.

对于任意的 $a_1 * b_1, a_2 * b_2 \in A * B$, 因为 $\langle A; * \rangle$ 是 $\langle G; * \rangle$ 的正规子群, 所以

$$\begin{aligned}(a_1 * b_1) * (a_2 * b_2)^{-1} &= (a_1 * b_1) * (b_2^{-1} * a_2^{-1}) = a_1 * (b_1 * b_2^{-1}) * a_2^{-1} \\ &= a_1 * (b_3 * a_2^{-1}) = a_1 * (a_3 * b_3) \\ &= (a_1 * a_3) * b_3 \in A * B.\end{aligned}$$

由上式知, $\langle A * B; * \rangle$ 是群 $\langle G; * \rangle$ 的子群.

对于任意的 $g \in G$ 和任意的 $a * b \in A * B$, 因为 $\langle B; * \rangle$ 也是 $\langle G; * \rangle$ 的正规子群, 所以

$$\begin{aligned}g * (a * b) * g^{-1} &= (g * a) * (b * g^{-1}) = (a' * g) * (g^{-1} * b') \\ &= a' * (g * g^{-1}) * b' = a' * b' \in A * B.\end{aligned}$$

这说明对于任意的 $g \in G, g * (A * B) * g^{-1} \subseteq A * B$, 故 $\langle A * B; * \rangle$ 是 $\langle G; * \rangle$ 的正规子群.

例 5-41 设 $\langle A; * \rangle$ 和 $\langle B; * \rangle$ 都是群 $\langle G; * \rangle$ 的子群,试证明 $\langle A * B; * \rangle$ 是 $\langle G; * \rangle$ 的子群的充要条件是 $A * B = B * A$.

证 先证充分性. 因为 $e \in A, e \in B$, 所以 $e \in A * B$, 因此 $A * B$ 非空.

对于任意的 $a_1 * b_1$, 有 $a_2 * b_2 \in A * B$, 因为 $\langle A; * \rangle$ 和 $\langle B; * \rangle$ 都是 $\langle G; * \rangle$ 的子群, 所以

$$\begin{aligned}(a_1 * b_1) * (a_2 * b_2)^{-1} &= (a_1 * b_1) * (b_2^{-1} * a_2^{-1}) = a_1 * (b_1 * b_2^{-1}) * a_2^{-1} \\ &= a_1 * (b_3 * a_2^{-1}) \quad (b_3 \in B, a_2^{-1} \in A).\end{aligned}$$

因为 $A * B = B * A$, 所以必有 $a_3 \in A, b_4 \in B$, 使得

$$b_3 * a_2^{-1} = a_3 * b_4,$$

于是

$$(a_1 * b_1) * (a_2 * b_2)^{-1} = a_1 * (a_3 * b_4) = (a_1 * a_3) * b_4 \in A * B.$$

由此可知, $\langle A * B; * \rangle$ 是 $\langle G; * \rangle$ 的子群.

再证必要性. 设 $b * a \in B * A$, 则有 $b^{-1} \in B, a^{-1} \in A$, 所以 $a^{-1} * b^{-1} \in A * B$. 因为 $\langle A * B; * \rangle$ 是 $\langle G; * \rangle$ 的子群, 所以又有 $(a^{-1} * b^{-1})^{-1} \in A * B$, 即 $b * a \in A * B$, 因此 $B * A \subseteq A * B$.

设 $a * b \in A * B$, 则由 $\langle A * B; * \rangle$ 是 $\langle G; * \rangle$ 的子群, 必有元素 $a_1 * b_1 \in A * B$, 使得 $a * b = (a_1 * b_1)^{-1}$, 即 $a * b = b_1^{-1} * a_1^{-1}$, 而 $b_1^{-1} * a_1^{-1} \in B * A$, 所以 $a * b \in B * A$, 因此 $A * B \subseteq B * A$.

由上证得, $A * B = B * A$.

例 5-42 设 $\langle G; * \rangle$ 是一个群, H 是 G 的非空子集, 试证明 $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的子群的充要条件 $\langle H; * \rangle$ 是一个群.

证 先证充分性. 设 $\langle H; * \rangle$ 是群, 则显然 $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的子代数. 设 e' 是 $\langle H; * \rangle$ 的单位元, 则有 $e' * e' = e'$. 由 e 是群 $\langle G; * \rangle$ 的单位元, 则有 $e * e' = e'$. 于是 $e' * e' = e * e'$. 由消去律得 $e' = e$. 因此 $e \in H$.

对任意 $a \in H$, 设 a' 是 a 在群 $\langle H; * \rangle$ 中的逆元, 于是有 $a * a' = e$. 另一方面, 因 $a * a^{-1} = e$, 由消去律 $a' = a^{-1}$. 因此 $a^{-1} \in H$.

由此证得, $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的子群.

再证必要性. 设 $\langle H; * \rangle$ 是 $\langle G; * \rangle$ 的子群, 则 $\langle H; * \rangle$ 显然是一代数系统, 且运算 $*$ 在 H 上可结合. 单位元 $e \in H$, 显然 e 也是 $\langle H; * \rangle$ 中的单位元, 对于任一 $a \in H$, 有 $a^{-1} \in H$, 满足 $a * a^{-1} = a^{-1} * a = e$. 因此 $\langle H; * \rangle$ 是一个群.

End of Chapter 5