



第五章 代数结构

§1 代数系统的引入

§2 运算及其性质

 §3 半群

§4 群与子群

§5 阿贝尔群和循环群

§7 陪集与拉格朗日定理

§8 同态与同构

§9 环和域



§5-3 半群

一、半群

定义1 一个代数系统 $\langle S, * \rangle$, S 为非空集合, $*$ 是 S 上的二元运算, 即集合 S 对 $*$ 是封闭的, 则称代数系统 $\langle S, * \rangle$ 为**广群**。

定义2 设 $\langle S, * \rangle$ 是一代数系统, S 为非空集合, $*$ 是 S 上的二元运算, 若**运算 $*$ 满足结合律**, 即对任意的 $x, y, z \in S$,
满足 $(x * y) * z = x * (y * z)$,
则称 $\langle S, * \rangle$ 为**半群**。



§5-3 半群

例：设集合 $S_k = \{x | x \in I \wedge x \geq k\}$, $k \geq 0$, 证明 $\langle S_k, + \rangle$ 是一个半群, 其中 $+$ 是普通的加法运算。

解：因为 1) $+$ 是 S_k 上的二元运算；

2) $+$ 是可结合的。

所以, $\langle S_k, + \rangle$ 是一个半群。

例： $\langle \mathbf{I}_+, - \rangle$ - 不封闭, 不可结合

$\langle \mathbf{R} - \{0\}, / \rangle$ / 封闭, 不可结合

广群

$\langle \mathbf{I}, \times \rangle$ \times 封闭, 可结合

$\langle P(S), \cap \rangle$ \cap 封闭, 可结合

} 半群



§5-3 半群

例2：设 $S=\{a, b, c\}$ ， S 上的一个二元运算 Δ 定义如表，验证 $\langle S, \Delta \rangle$ 是一个半群。

Δ	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

解：从表中可知

1) Δ 是封闭的。

2) a, b, c 都是左幺元。

所以，对于 $\forall x, y, z \in S$ ，都有

$$x \Delta (y \Delta z) = x \Delta z = z \quad (x \Delta y) \Delta z = y \Delta z = z$$

因此， $\langle S, \Delta \rangle$ 是半群。



§5-3 半群

定理1 设 $\langle S, * \rangle$ 是一半群, $B \subseteq S$, 且 $*$ 在 B 上是封闭的,
那么 $\langle B, * \rangle$ 也是半群, 称 $\langle B, * \rangle$ 是 $\langle S, * \rangle$ 的子半群。

证明: 因为 $*$ 在 S 上可结合, 而 $B \subseteq S$, 所以 $*$ 在 B 上也是可结合的。

又因为 $*$ 在 B 上是封闭的,
所以 $\langle B, * \rangle$ 是半群。



§5-3 半群

例：证明 $\langle [0,1], \times \rangle$, $\langle [0,1), \times \rangle$, $\langle I, \times \rangle$ 都是 $\langle R, \times \rangle$ 的子半群。

证明：a) $\because \times$ 在 R 上是封闭且可结合的。

$\therefore \langle R, \times \rangle$ 是一个半群。

b) \times 在 $[0,1]$, $[0,1)$ 和 I 上都是封闭的且

$[0,1] \subset R$, $[0,1) \subset R$, $I \subset R$

所以， $\langle [0,1], \times \rangle$, $\langle [0,1), \times \rangle$, $\langle I, \times \rangle$ 都是半群，并且是 $\langle R, \times \rangle$ 的子半群。



§5-3 半群

补充

定义： 设 $*$ 是 S 上的二元运算，对任一 $x \in S$ ，定义：

$$x^1 = x$$

$$x^2 = x * x$$

...

$$x^n = x^{n-1} * x$$

定理： 设 $*$ 是 S 上的二元运算，且 $x \in S$ ，对任一 $m, n \in I_+$ 有

$$(1) \quad x^m * x^n = x^{m+n}$$

$$(2) \quad (x^m)^n = x^{m \cdot n}$$



§5-3 半群

定理2 设 $\langle S, * \rangle$ 是一半群, 如果 S 为有限集, 则必有 $a \in S$, 使 $a*a=a$ 。

证明: 因 $\langle S, * \rangle$ 是半群, 对 $\forall b \in S$, 由 $*$ 的封闭性可知,

$$b*b \in S, \text{ 记 } b^2 = b*b$$

$$b^2*b = b*b^2 \in S, \text{ 记 } b^3 = b^2*b = b*b^2$$

$$b^3*b = b*b^3 \in S, \text{ 记 } b^4 = b^3*b = b*b^3$$

.....

由于 S 是有限集, 必有 $i < j$, 使 $b^i = b^j$

令 $p = j - i$, 则 $b^j = b^p * b^i$, 即: $b^i = b^p * b^i$

当 $q \geq i$ 时, $b^q = b^p * b^q$



§5-3 半群

又因 $p \geq 1$, 总可以找到 $k \geq 1$, 使得 $kp \geq i$,
对S中的 b^{kp} 有

$$b^{kp} = b^p * b^{kp}$$

$$= b^p * (b^p * b^{kp})$$

$$= b^{2p} * b^{kp}$$

$$= b^{2p} * (b^p * b^{kp})$$

$$= b^{3p} * b^{kp}$$

$$= \dots$$

$$= b^{kp} * b^{kp}$$

$$\text{令 } a = b^{kp}, \text{ 则 } a * a = a。$$



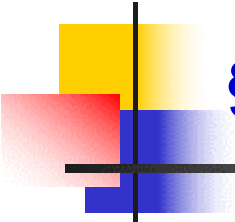
§5-3 半群

二、独异点

定义3 含有幺元的半群称为独异点(*monoid*)。(含幺半群, 拟群, 幺半群)。

例: $\langle \mathbf{R}, + \rangle$, $\langle \mathbf{I}, \times \rangle$, $\langle \mathbf{I}_+, \times \rangle$
 $\langle \mathbf{N}, + \rangle$, $\langle \mathbf{N}, \times \rangle$ 均为独异点
 $\langle \mathbf{N} - \{0\}, + \rangle$, 不是独异点, 是半群

例: 设 S 为非空集合, $P(S)$ 是 S 的幂集,
则 $\langle P(S), \cap \rangle$, $\langle P(S), \cup \rangle$ 均为独异点。



§5-3 半群

例: $\langle I, \max \rangle$, 其中 $\max(x_1, x_2)$ 取二者之大值;

$\langle I, \min \rangle$, 其中 $\min(x_1, x_2)$ 取二者之小值,

均不为独异点 (不存在幺元)。

$\langle \mathbb{N}, \max \rangle$ 为独异点, 其中 $e = 0$

§5-3 半群

例：代数系统 $\langle S, * \rangle$ ，其中 $S=\{a, 0, 1\}$ ，运算 $*$ 由下表定义，证明 $\langle S, * \rangle$ 是独异点。

证明 1) 运算 $*$ 是封闭的。

2) 对于任意 $x, y \in S$,

$$(x * y) * a = x * y \quad x * (y * a) = x * y$$

$$(x * y) * 0 = 0 \quad x * (y * 0) = x * 0 = 0$$

$$(x * y) * 1 = 1 \quad x * (y * 1) = x * 1 = 1$$

所以运算 $*$ 是可结合的。

3) a 是 S 中关于运算 $*$ 的么元。

因此 $\langle S, * \rangle$ 是独异点。

$*$	a	0	1
a	a	0	1
0	0	0	1
1	1	0	1

表中任何两
行或两列都
是不同的。

§5-3 半群

定理3 设 $\langle S, * \rangle$ 是一个独异点，则在关于运算 $*$ 的运算表中任何两行或两列都是不相同的。

证明：设 S 中关于运算 $*$ 的幺元是 e 。

\because 对于 $\forall a, b \in S$ 且 $a \neq b$ 时，总有

$$e * a = a \neq b = e * b \quad (\text{列不同})$$

$$a * e = a \neq b = b * e \quad (\text{行不同})$$

\therefore 在 $*$ 的运算表中不可能有两行或两列是相同的。

$*$	$\dots a \dots b \dots$
\cdot	$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$
\cdot	$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$
e	$\dots a \dots b \dots$
\cdot	$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$
\cdot	$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$

$*$	$\cdot \quad \cdot \quad e \quad \cdot \quad \cdot \quad \cdot$
\cdot	$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$
a	$\cdot \quad \cdot \quad a \quad \cdot \quad \cdot \quad \cdot$
\cdot	$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$
\cdot	$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$
b	$\cdot \quad \cdot \quad b \quad \cdot \quad \cdot \quad \cdot$
\cdot	$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$



§5-3 半群

例：设 I 是整数集合， m 是任意正整数， Z_m 是由模 m 的同余类组成的同余类集，在 Z_m 上定义两个二元运算 $+_m$ 和 \times_m 分别如下：对于任意的 $[i], [j] \in Z_m$

$$[i] +_m [j] = [(i+j) \bmod m]$$

$$[i] \times_m [j] = [(i \times j) \bmod m]$$

试证明在这两个二元运算的运算表中任何两行或两列都是不相同的。

考虑：只须证明 $\langle Z_m, +_m \rangle$ 和 $\langle Z_m, \times_m \rangle$ 都是独异点。分三

步证明：1) 证明两个运算在 Z_m 上封闭；

2) 证明两个运算满足结合律；

3) 证明 $[0]$ 是 $\langle Z_m, +_m \rangle$ 的幺元， $[1]$ 是 $\langle Z_m, \times_m \rangle$ 的幺

元。



§5-3 半群

证明：（1）由 $+_m$ 和 \times_m 的定义可知在 Z_m 上是封闭的。

（2）对于任意 $[i], [j], [k] \in Z_m$

$$\begin{aligned}([i] +_m [j]) +_m [k] &= [i] +_m ([j] +_m [k]) \\ &= [(i + j + k) \bmod m]\end{aligned}$$

$$\begin{aligned}([i] \times_m [j]) \times_m [k] &= [i] \times_m ([j] \times_m [k]) \\ &= [(i \times j \times k) \bmod m]\end{aligned}$$

（3）

$\because [0] +_m [i] = [i] +_m [0] = [i] \quad \therefore [0]$ 是 $\langle Z_m, +_m \rangle$ 的么元

$\because [1] \times_m [i] = [i] \times_m [1] = [i] \quad \therefore [1]$ 是 $\langle Z_m, \times_m \rangle$ 的么元

因此， $\langle Z_m, +_m \rangle$ 和 $\langle Z_m, \times_m \rangle$ 是独异点，两个运算表中任何两行或两列都是不相同的。



§5-3 半群

设 $m=5$ ，则 $+_5$ 和 \times_5 运算表分别如下：

$+_5$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

\times_5	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]



§5-3 半群

定理4 设 $\langle S, * \rangle$ 是独异点, 对于任意 $a, b \in S$, 且 a, b 均有逆元, 则

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

b) $a * b$ 有逆元, 且 $(a * b)^{-1} = b^{-1} * a^{-1}$

证明: a) $\because a^{-1}$ 是 a 的逆元, 即

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

$$\therefore (a^{-1})^{-1} = a$$

$$\begin{aligned} \text{b) } \because (a * b) * (b^{-1} * a^{-1}) &= a * (b * b^{-1}) * a^{-1} \\ &= a * e * a^{-1} \\ &= e \end{aligned}$$

$$\text{同理: } (b^{-1} * a^{-1}) * (a * b) = e$$

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




第五章 代数结构

§1 代数系统的引入

§2 运算及其性质

§3 半群

 §4 群与子群

§5 阿贝尔群和循环群

§6 陪集与拉格朗日定理

§7 同态与同构

§8 环和域



§5-4 群与子群

一、群

定义1 设 $\langle G, * \rangle$ 是一代数系统， G 是非空集合， $*$ 为 G 上的二元运算，如果

- (1) 运算 $*$ 是封闭的；
- (2) 运算 $*$ 是可结合的；
- (3) 存在幺元 e ；
- (4) G 中每一个元素 x 都有逆元 x^{-1} 。

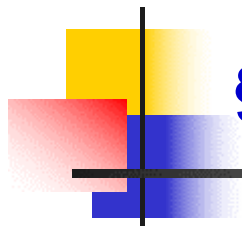
则称 $\langle G, * \rangle$ 为**群** $\langle group \rangle$ 。

例： $\langle \mathbf{I}, + \rangle$, $\langle \mathbf{R} - \{0\}, \times \rangle$, $\langle P(S), \oplus \rangle$ 等均为群。



§5-4 群与子群

例：设 $R = \{0^\circ, 60^\circ, 120^\circ, 180^\circ, 240^\circ, 300^\circ\}$ 表示在平面上
几何图形绕形心顺时针旋转角度的六种可能情况，设
★是 R 上的二元运算，对于 R 中任意两个元素 a 和 b ，
 $a \star b$ 表示平面图形连续旋转 a 和 b 得到的总旋转角度。
并规定旋转 360° 等于原来的状态，就看作没有经过旋
转。验证 $\langle R, \star \rangle$ 是一个群。



§5-4 群与子群

★	0°	60°	120°	180°	240°	300°
0°	0°	60°	120°	180°	240°	300°
60°	60°	120°	180°	240°	300°	0°
120°	120°	180°	240°	300°	0°	60°
180°	180°	240°	300°	0°	60°	120°
240°	240°	300°	0°	60°	120°	180°
300°	300°	0°	60°	120°	180°	240°





§5-4 群与子群

解：(1) \star 运算是封闭的

(2) \star 运算是可结合的

对于 $\forall a, b, c \in R$, $(a \star b) \star c$: 将图形依次旋转 a, b 和 c ,

$a \star (b \star c)$: 将图形依次旋转 b, c 和 a ,

而总的旋转角度都等于 $(a+b+c) \pmod{360^\circ}$

因此, $(a \star b) \star c = a \star (b \star c)$ 。

(3) 幺元为 0° ;

(4) 每一个元素均有逆元:

$60^\circ, 180^\circ, 120^\circ$ 的逆元分别是 $300^\circ, 180^\circ, 240^\circ$

$\therefore \langle R, \star \rangle$ 是一个群。





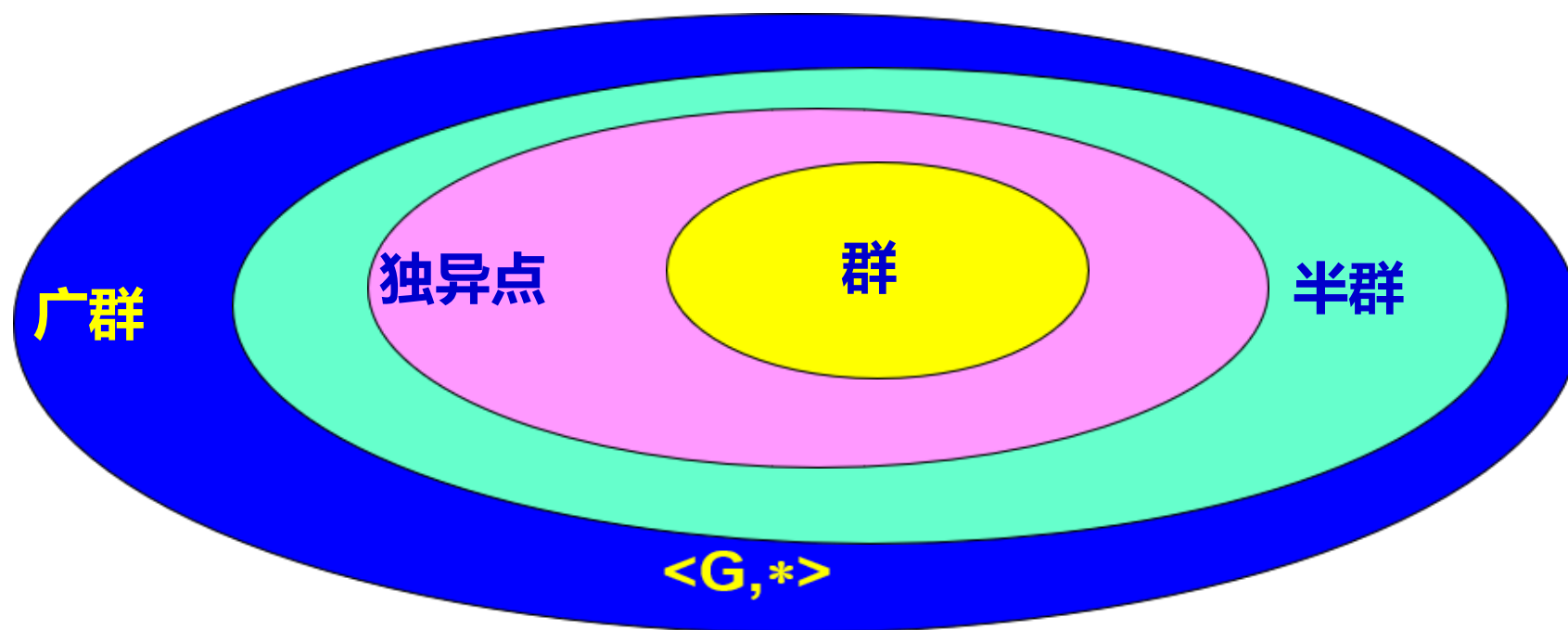
§5-4 群与子群

定义2 设 $\langle G, * \rangle$ 是一个群，如果 G 是有限集合，则称 $\langle G, * \rangle$ 为**有限群** (*finite group*)， G 中元素个数称为**群的阶数**(*order*)，记为 $|G|$ ，如果 G 为无限集合，则称 $\langle G, * \rangle$ 为**无限群** (*infinite group*)。

例： $\langle \mathbf{I}, + \rangle$ 为无限群，

上例中 $\langle \mathbf{R}, \star \rangle$ 为有限群，群的阶为 $|\mathbf{R}| = 6$ 。

§5-4 群与子群



$$\{\text{群}\} \subset \{\text{独异点}\} \subset \{\text{半群}\} \subset \{\text{广群}\}$$



§5-4 群与子群

群的性质

- (1) 群具有半群和独异点所具有的所有性质；
- (2) 由于群中存在幺元， \therefore 在群的运算表中一定没有相同的行（和列）
- (3) 在群中，每一个元素均存在逆元，而且，群中任何一个元素的逆元必定是唯一的。

由群中逆元的唯一性，我们可以有以下几个定理。

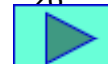


§5-4 群与子群

定理1 群中不存在零元。

证明： 设 $\langle G, * \rangle$ 是一个群。

- 1) 当 $|G|=1$ 时，唯一的元素是幺元 e 。
- 2) 当 $|G|>1$ 时，设 $\langle G, * \rangle$ 中有零元 θ 。
 $\because \forall x \in G$ ，都有 $x * \theta = \theta * x = \theta \neq e$
 \therefore 零元 θ 不存在逆元，与 $\langle G, * \rangle$ 是群矛盾。
所以群中不存在零元。



§5-4 群与子群

定理2 设 $\langle G, * \rangle$ 是一个群, 则对 $\forall a, b \in G$ 有:

- (1) 存在**唯一的**元素 $x \in G$, 使 $a * x = b$;
- (2) 存在唯一的元素 $y \in G$, 使 $y * a = b$ 。

证明: (a) 在 G 中存在 x , 使 $a * x = b$ 成立。

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

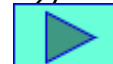
\therefore 至少有一 $x = (a^{-1} * b)$ 满足 $a * x = b$ 成立。

(b) 证明这样的 x 是唯一的。

若 x 是 G 中任一元素, 且能使 $a * x = b$ 成立, 则

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

$\therefore x = (a^{-1} * b)$ 是满足 $a * x = b$ 的唯一元素, 即 x 是唯一的。





§5-4 群与子群

定理3 若 $\langle G, * \rangle$ 是一个群, 则对 $\forall a, b, c \in G$,
如果有 $a*b = a*c$ 或者 $b*a = c*a$, 则必有 $b = c$ 。
(消去律)

证明: 设 $a*b = a*c$, 且 a 的逆元是 a^{-1} , 则有

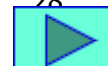
$$a^{-1} * (a * b) = a^{-1} * (a * c)$$

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

$$e * b = e * c$$

$$b = c$$

当 $b*a = c*a$ 时, 可同样证得 $b = c$





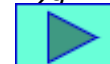
§5-4 群与子群

定义3 设 S 是一个非空有限集合，从集合 S 到 S 的一个**双射**称为 S 的一个**置换**。

譬如，对于集合 $S=\{a,b,c,d\}$ ，将 a 映射到 b ， b 映射到 d ， c 映射到 a ， d 映射到 c 是一个从 S 到 S 上的一个一对一映射，这个置换可以表示为

$$\begin{array}{cccc} a & b & c & d \\ \left[\begin{array}{cccc} & & & \\ d & a & c & \end{array} \right] \end{array}$$

即上一行中按任何次序写出集合中的全部元素，而在下一行中写每个对应元素的象。



§5-4 群与子群

定理4 有限群 $\langle G, * \rangle$ 的运算表中的每一行或每一列都是 G 的元素的置换。

证明：（1）先证运算表中的任一行（列）所含 G 中的一个元素不可能多于一次。（用反证法）

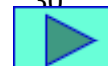
设 a 对应行有两个元素 b_1 、 b_2 对应的都是 c ,

即 $a*b_1=a*b_2=c$, 且 $b_1 \neq b_2$

由消去律得 $b_1=b_2$

与假设 $b_1 \neq b_2$ 矛盾。

$*$	$\dots b_1 \dots b_2 \dots$				
\cdot	\cdot	\cdot	\cdot	\cdot	\cdot
\cdot	\cdot	\cdot	\cdot	\cdot	\cdot
a	\cdot	c	\cdot	c	\cdot
\cdot	\cdot	\cdot	\cdot	\cdot	\cdot
\cdot	\cdot	\cdot	\cdot	\cdot	\cdot





§5-4 群与子群

(2) 证明 G 中的每一个元素都在运算表的每一行和每一列中出现。

对于元素 $a \in G$ 的那一行，设 b 是 G 中任意一个元素，

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

$\therefore b$ 必定出现在对应于 a 的那一行。

又 \because 运算表中没有两行或两列是相同的。

$\therefore \langle G, * \rangle$ 的运算表中的每一行都是 G 的元素的一个置换，且每一行都是不相同的。

同样，对于每一列结论同样成立。

§5-4 群与子群

独异点

$\langle G, * \rangle$

*	a	0	1
a	a	0	1
0	0	0	1
1	1	0	1

表中任何两
行或两列都
是不同的。

群

*	a	0	1
a	a	0	1
0	0	1	a
1	1	a	0

表中任何行
或列都是集
合的置换。



§5-4 群与子群

定义4 代数系统 $\langle G, * \rangle$ 中, 如果存在 $a \in G$, 有 $a * a = a$, 则称 a 为幂等元。

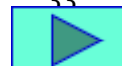
定理5 群 $\langle G, * \rangle$ 中, 除幺元 e 外, 不可能有任何别的等幂元。

证明: 因为 $e * e = e$, 所以 e 是等幂元。

设 $a \in G$, $a \neq e$ 且 $a * a = a$

$$\begin{aligned} \text{则有 } a &= e * a = (a^{-1} * a) * a \\ &= a^{-1} * (a * a) \\ &= a^{-1} * a = e \end{aligned}$$

与假设 $a \neq e$ 相矛盾。





§5-4 群与子群

例：在实数集合 \mathbf{R} 中， $+$ 是可交换，可结合的，“0”对 $+$ 是幂等元，而其它不为幂等元；

例：设 $P(S)$ 是集合 S 的幂集，在 $P(S)$ 上定义的两个二元运算 \cap 和 \cup 。

(1) 对于 $\forall A \in P(S)$ ，有 $A \cap A = A$ $A \cup A = A$ ，

$\therefore \cap$ 和 \cup 满足幂等律，

$P(S)$ 中任一元素，对 \cap ， \cup 均是幂等元。

(2) 对称差 \oplus ，除 $P(S) = \{\Phi\}$ 以外不满足幂等律。

$\because \Phi \oplus \Phi = \Phi$ ，

而除 Φ 以外的 $A \in P(S)$ 有 $A \oplus A \neq A$ 。

§5-4 群与子群

二、子群

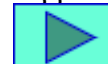
定义5 设 $\langle G, * \rangle$ 是一个群, 且 S 是 G 的非空子集。若 $\langle S, * \rangle$ 也构成群, 称 $\langle S, * \rangle$ 是 $\langle G, * \rangle$ 的一个子群(subgroup)。

定理6 设 $\langle G, * \rangle$ 为群, $\langle S, * \rangle$ 为 $\langle G, * \rangle$ 的子群, 那么, $\langle G, * \rangle$ 中的幺元 e 必定也是 $\langle S, * \rangle$ 中的幺元. 且元素在子群 S 中的逆元即为在群 G 中的逆元.

证明: 设 $\langle S, * \rangle$ 中的幺元为 e_1 , 对于 $\forall x \in S \subseteq G$, 必有

$$e_1 * x = x = e * x$$

故 $e_1 = e$ (消去律)





§5-4 群与子群

定义6 设 $\langle G, * \rangle$ 是一个群， $\langle S, * \rangle$ 是 $\langle G, * \rangle$ 的子群，如果 $S = \{e\}$ ，或者 $S = G$ ，则称 $\langle S, * \rangle$ 为 $\langle G, * \rangle$ 的平凡子群。

讨论：

- (1) 假设 G 的阶不是1，则任一群 $\langle G, * \rangle$ 至少可找到二个子群（平凡子群），即 $\langle \{e\}, * \rangle$ 和 $\langle G, * \rangle$
- (2) 除了平凡子群以外的子群称为非平凡子群。
- (3) 若 S 是 G 的真子集，则称子群 $\langle S, * \rangle$ 是 $\langle G, * \rangle$ 的真子群。

§5-4 群与子群

例: $\langle I, + \rangle$ 是一个群, $I_E = \{x | x = 2n, n \in I\}$, 证明 $\langle I_E, + \rangle$ 是 $\langle I, + \rangle$ 的一个子群。

证明: (1) 对于 $\forall x, y \in I_E$, 设 $x = 2n_1, y = 2n_2$ ($n_1, n_2 \in I$)

$$x + y = 2n_1 + 2n_2 = 2(n_1 + n_2), \text{ 而 } n_1 + n_2 \in I$$

$\therefore x + y \in I_E$, 即 $+$ 在 I_E 上**封闭**。

(2) $+$ 在 I_E 上保持**可结合性**。

(3) **么元** $0 \in I_E$ 。

(4) 对于 $\forall x \in I_E$, 必有 n 使得 $x = 2n$

$$\text{而 } -x = -2n = 2(-n), -n \in I$$

$$\therefore \textbf{-x} \in I_E \quad \text{而 } x + (-x) = (-x) + x = 0$$

因此, $\langle I_E, + \rangle$ 是 $\langle I, + \rangle$ 的一个子群。

§5-4 群与子群

定理7 设 $\langle G, * \rangle$ 是一个群, B 是 G 的非空子集 ($B \subseteq G$, $B \neq \Phi$), 若 B 是一个有限集, 则只要运算 $*$ 在 B 上封闭, $\langle B, * \rangle$ 必定是 $\langle G, * \rangle$ 的子群。(教材定理6.6.7)

证明: 设 $\forall b \in B$, 已知 $*$ 在 B 上封闭, 则

$$b^2 = b * b \in B, \quad b^3 = b^2 * b \in B, \quad \dots$$

$\because B$ 是有限集,

\therefore 必存在正整数 i 和 j ($i < j$), 使得 $b^i = b^j$, 即 $b^i = b^i * b^{j-i}$
则 b^{j-i} 是 $\langle G, * \rangle$ 中的么元, 且 $b^{j-i} \in B$ 。

若 $j-i > 1$, 由 $b^{j-i} = b * b^{j-i-1}$ 可知 b^{j-i-1} 是 b 的逆元, 且 $b^{j-i-1} \in B$

若 $j-i = 1$, 由 $b^i = b^i * b$ 可知 b 是么元, 且以自身为逆元。

因此, $\langle B, * \rangle$ 是 $\langle G, * \rangle$ 的一个子群。

§5-4 群与子群

例：设 $G_4 = \{ p = \langle p_1, p_2, p_3, p_4 \rangle \mid p_i \in \{0, 1\} \}$, \oplus 是 G_4 上的二元运算，定义为对任意 $X = \langle x_1, x_2, x_3, x_4 \rangle$,

$$Y = \langle y_1, y_2, y_3, y_4 \rangle \in G_4,$$

$$X \oplus Y = \langle x_1 \nabla y_1, x_2 \nabla y_2, x_3 \nabla y_3, x_4 \nabla y_4 \rangle,$$

其中 ∇ 的运算表如表所示。

证明 $\langle \{ \langle 0, 0, 0, 0 \rangle, \langle 1, 1, 1, 1 \rangle \}, \oplus \rangle$ 是群 $\langle G_4, \oplus \rangle$ 的子群。

∇	0	1
0	0	1
1	1	0



§5-4 群与子群

∇	0	1
0	0	1
1	1	0

证明：先证明 $\langle G_4, \oplus \rangle$ 是群。

取任意的 $X = \langle x_1, x_2, x_3, x_4 \rangle$, $Y = \langle y_1, y_2, y_3, y_4 \rangle$,

$Z = \langle z_1, z_2, z_3, z_4 \rangle \in G_4$,

$$(1) \because x_i \nabla y_i \in \{0, 1\}$$

$$\therefore X \oplus Y \in G_4 \quad \text{—— 封闭性}$$

$$(2) \because (x_i \nabla y_i) \nabla z_i = x_i \nabla (y_i \nabla z_i)$$

$$\therefore (X \oplus Y) \oplus Z = X \oplus (Y \oplus Z) \quad \text{—— 结合性}$$

(3) $\langle 0, 0, 0, 0 \rangle$ 是幺元

(4) $X \oplus X = \langle 0, 0, 0, 0 \rangle$, 即任一 X , 以它自身为逆元。

所以 $\langle G_4, \oplus \rangle$ 是一个群。





§5-4 群与子群

其次, 由于 $\{ \langle 0,0,0,0 \rangle, \langle 1,1,1,1 \rangle \} \subset G_4$,
且 \oplus 在 $\{ \langle 0,0,0,0 \rangle, \langle 1,1,1,1 \rangle \}$ 上是封闭的,
由 定理7 可知 $\langle \{ \langle 0,0,0,0 \rangle, \langle 1,1,1,1 \rangle \}, \oplus \rangle$ 是群 $\langle G_4, \oplus \rangle$ 的
子群。

§5-4 群与子群

定理8 设 $\langle G, \Delta \rangle$ 是群, S 是 G 的非空子集, $\langle S, \Delta \rangle$ 是 $\langle G, \Delta \rangle$ 的子群 当且仅当 对于 S 中的任意元素 a 和 b 有 $a \Delta b^{-1} \in S$.

证明: 必要性显然。下证充分性. 分四步

(1) 证明 G 中的幺元 e 也是 S 中的幺元。

$\forall a \in S \subseteq G$, 有 $a \Delta a^{-1} \in S$,

而 $a \Delta a^{-1} = e \in S$ 且 $a \Delta e = e \Delta a = a$,

即 e 也是 S 中的幺元。

(2) 证明 S 中的每一元素都有逆元。

对 $\forall a \in S$, 因为 $e \in S$, 所以 $e \Delta a^{-1} \in S$, 即 $a^{-1} \in S$ 。



§5-4 群与子群

(3) 证明 Δ 在 S 上是封闭的。

对 $\forall a, b \in S$, 由(2)可知 $b^{-1} \in S$

而 $b = (b^{-1})^{-1}$

所以 $a \Delta b = a \Delta (b^{-1})^{-1} \in S$

(4) 运算 Δ 在 S 上的可结合性是保持的。

因此, $\langle S, \Delta \rangle$ 是 $\langle G, \Delta \rangle$ 的子群。



§5-4 群与子群

例：设 $\langle H, * \rangle$ 和 $\langle K, * \rangle$ 都是群 $\langle G, * \rangle$ 的子群，试证明 $\langle H \cap K, * \rangle$ 也是 $\langle G, * \rangle$ 的子群。

证明：设 $\forall a, b \in H \cap K$ ，有 $a, b \in H$ ， $a, b \in K$
 $\because \langle H, * \rangle$ 和 $\langle K, * \rangle$ 都是 $\langle G, * \rangle$ 的子群

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

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

由定理8得 $\langle H \cap K, * \rangle$ 是 $\langle G, * \rangle$ 的子群。





§5-4 群与子群

习题:

设 $\langle H, \cdot \rangle$ 和 $\langle K, \cdot \rangle$ 都是群 $\langle G, \cdot \rangle$ 的子群, 令

$$HK = \{h \cdot k \mid h \in H, k \in K\}$$

证明 $\langle HK, \cdot \rangle$ 是 $\langle G, \cdot \rangle$ 的子群的充要条件是 $HK = KH$ 。

证明: (1) 充分性 (已知 $HK = KH$)

对于 $\forall h_1 \cdot k_1, h_2 \cdot k_2 \in HK$

$\because \langle H, \cdot \rangle$ 和 $\langle K, \cdot \rangle$ 都是群

$$\therefore (h_2 \cdot k_2)^{-1} = k_2^{-1} \cdot h_2^{-1} \in KH$$

又 $\because HK = KH$

\therefore 必有 $h_3 \in H, k_3 \in K$, 使得 $k_2^{-1} \cdot h_2^{-1} = h_3 \cdot k_3$



§5-4 群与子群

$$\begin{aligned} (h_1 \cdot k_1) \cdot (h_2 \cdot k_2)^{-1} &= (h_1 \cdot k_1) \cdot (h_3 \cdot k_3) \\ &= h_1 \cdot (k_1 \cdot h_3) \cdot k_3 \\ &= h_1 \cdot (h_4 \cdot k_4) \cdot k_3 \\ &= (h_1 \cdot h_4) \cdot (k_4 \cdot k_3) \\ &= h_5 \cdot k_5 \in HK \end{aligned}$$

\therefore 由定理8可知 $\langle HK, \cdot \rangle$ 是 $\langle G, \cdot \rangle$ 的子群



§5-4 群与子群

(2) 必要性 (已知 $\langle HK, \cdot \rangle$ 是 $\langle G, \cdot \rangle$ 的子群)

对于 $\forall k \cdot h \in KH$, $(k \cdot h)^{-1} = h^{-1} \cdot k^{-1} \in HK$

$\therefore \langle HK, \cdot \rangle$ 是群

$\therefore ((k \cdot h)^{-1})^{-1} \in HK$ 即 $k \cdot h \in HK$

$\therefore KH \subseteq HK$

对于 $\forall h \cdot k \in HK$, $(h \cdot k)^{-1} \in HK$

即存在 $h_1 \in H$, $k_1 \in K$, 使得 $(h \cdot k)^{-1} = h_1 \cdot k_1$

$\therefore h \cdot k = (h_1 \cdot k_1)^{-1} = k_1^{-1} \cdot h_1^{-1} \in KH$

$\therefore HK \subseteq KH$

因此: $HK = KH$