

第14章 代数系统

计算机工程与科学学院 封卫兵

14.3 几个典型的代数系统

14.3.1 半群与独异点

14.3.2 群

14.3.1 半群与独异点

半群与独异点的定义与实例

半群与独异点的幂运算

半群与独异点的子代数和积代数

半群与独异点的同态

14.3.1 半群与独异点

半群与独异点的定义

定义14.12

- 1) 设 $V = \langle S, \circ \rangle$ 是代数系统, \circ 为二元运算, 如果 \circ 运算是可结合的, 则称 V 为半群.
- 2) 设 $V = \langle S, \circ \rangle$ 是半群, 若 $e \in S$ 是关于 \circ 运算的单位元, 则称 V 是含幺半群, 也叫做独异点. 有时也将独异点 V 记作 $V = \langle S, \circ, e \rangle$.

14.3.1 半群与独异点

例：1) $+$ 是普通加法, 则 $\langle \mathbf{Z}^+, + \rangle, \langle \mathbf{N}, + \rangle, \langle \mathbf{Z}, + \rangle, \langle \mathbf{Q}, + \rangle, \langle \mathbf{R}, + \rangle$ 中：

$\langle \mathbf{Z}^+, + \rangle, \langle \mathbf{N}, + \rangle, \langle \mathbf{Z}, + \rangle, \langle \mathbf{Q}, + \rangle, \langle \mathbf{R}, + \rangle$ 是半群,
 $\langle \mathbf{N}, + \rangle, \langle \mathbf{Z}, + \rangle, \langle \mathbf{Q}, + \rangle, \langle \mathbf{R}, + \rangle$ 是独异点.

2) 设 n 是大于 1 的正整数, $+$ 和 \cdot 分别表示矩阵加法和矩阵乘法 .

半群： $\langle M_n(\mathbf{R}), + \rangle$?  $\langle M_n(\mathbf{R}), \cdot \rangle$? 

独异点： $\langle M_n(\mathbf{R}), + \rangle$?  $\langle M_n(\mathbf{R}), \cdot \rangle$? 

3) \oplus 为集合的对称差运算 . 则

$\langle P(B), \oplus \rangle$ 为半群 ?  也是独异点 ? 

14.3.1 半群与独异点

例： (续)

4) $Z_n = \{0, 1, \dots, n-1\}$, \oplus 为模 n 加法.

$\langle Z_n, \oplus \rangle$ 为半群 ?  也是独异点 ? 

5) \circ 为函数的复合运算. 则:

$\langle A^A, \circ \rangle$ 为半群 ?  也是独异点 ? 

6) \mathbf{R}^* 为非零实数集合, \circ 运算定义如下:

$\forall x, y \in \mathbf{R}^*, x \circ y = y$. 则 $\langle \mathbf{R}^*, \circ \rangle$ 为半群 ? 

14.3.1 半群与独异点

半群与独异点的幂运算

定义 1) 在半群 $\langle S, \circ \rangle$ 中, $\forall x \in S$, 规定:

$$x^1 = x, \quad x^{n+1} = x^n \circ x, \quad n \in \mathbf{Z}^+$$

2) 在独异点 $\langle S, \circ, e \rangle$ 中, $\forall x \in S$,

$$x^0 = e, \quad x^{n+1} = x^n \circ x, \quad n \in \mathbf{N}$$

用**数学归纳法**不难证明 x 的幂遵从以下运算规则:

$$x^n \circ x^m = x^{n+m}, \quad (x^n)^m = x^{nm},$$

在半群中 $m, n \in \mathbf{Z}^+$, 在独异点中 $m, n \in \mathbf{N}$.

14.3.1 半群与独异点

半群与独异点的子代数

定义 半群与独异点的子代数分别称为**子半群**与**子独异点**。

判定方法：

设 $V = \langle S, \circ \rangle$ 是半群, $T \subseteq S$, T **非空**, 如果 T 对 V 中的运算 \circ **封闭**, 则 $\langle T, \circ \rangle$ 是 V 的**子半群**。

设 $V = \langle S, \circ, e \rangle$ 是独异点, $T \subseteq S$, T **非空**, 如果 T 对 V 中的运算 \circ **封闭**, 而且 $e \in T$, 那么 $\langle T, \circ, e \rangle$ 构成 V 的**子独异点**。

14.3.1 半群与独异点

例：设半群 $V_1 = \langle S, \cdot \rangle$ ，独异点 $V_2 = \langle S, \cdot, e \rangle$ ，其中 \cdot 为矩阵乘法， e 为 2 阶单位矩阵，且

$$S = \left\{ \begin{pmatrix} a & \mathbf{0} \\ \mathbf{0} & d \end{pmatrix} \mid a, d \in \mathbf{R} \right\}, \quad T = \left\{ \begin{pmatrix} a & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix} \mid a \in \mathbf{R} \right\}$$

则 $T \subseteq S$ ，且 T 是 $V_1 = \langle S, \cdot \rangle$ 的子半群。

T 是 V_2 的子独异点吗？

$\begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} \end{pmatrix}$ 是 T 的单位元， T 本身可以构成独异点，但不是 V_2 的子独异点，因为 V_2 的单位元是 e 。

14.3.1 半群与独异点

半群与独异点的同态

定义14.13 1) 设 $V_1 = \langle S_1, \circ \rangle$, $V_2 = \langle S_2, * \rangle$ 是半群, $f: S_1 \rightarrow S_2$.

若对任意的 $x, y \in S_1$ 有

$$f(x \circ y) = f(x) * f(y),$$

则称 f 为半群 V_1 到 V_2 的同态映射, 简称同态.

2) 设 $V_1 = \langle S_1, \circ, e_1 \rangle$, $V_2 = \langle S_2, *, e_2 \rangle$ 是独异点, $f: S_1 \rightarrow S_2$.

若对任意的 $x, y \in S_1$ 有

$$f(x \circ y) = f(x) * f(y) \text{ 且 } f(e_1) = e_2,$$

则称 f 为独异点 V_1 到 V_2 的同态映射, 简称同态.

14.3.1 半群与独异点

例：设半群 $V_1 = \langle S, \cdot \rangle$ ，独异点 $V_2 = \langle S, \cdot, e \rangle$ ，其中 \cdot 为矩阵乘法， e 为 2 阶单位矩阵，且

$$S = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a, d \in \mathbf{R} \right\}$$

$$\text{令 } f\left(\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}\right) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

则 f 是半群 $V_1 = \langle S, \cdot \rangle$ 的自同态？ 

f 是独异点 $V_2 = \langle S, \cdot, e \rangle$ 的自同态？ 

因为 $f(e) \neq e$.

14.3.2 群

群的定义与实例

群中的术语

群的性质

子群的定义及判别

群的同态与同构

循环群

置换群

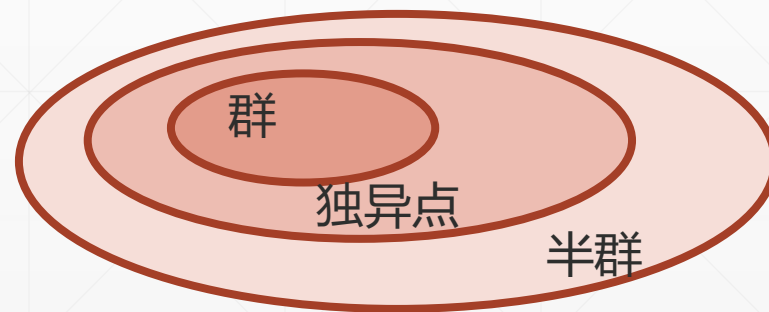
14.3.2 群

群的定义

定义14.14 设 $\langle G, \circ \rangle$ 是代数系统, \circ 为二元运算. 如果 \circ 运算是可结合的, 存在单位元 $e \in G$, 并且对 G 中的任何元素 x 都有 $x^{-1} \in G$, 则称 G 为群.

注: 1) 若非单元代数系统有零元, 则它一定不是群;

2) 群、独异点、半群的关系?



14.3.2 群

例：下列哪些代数系统是群？

1) $\langle \mathbf{Z}, + \rangle$ ✓ $\langle \mathbf{Q}, + \rangle$ ✓ $\langle \mathbf{R}, + \rangle$ ✓ $\langle \mathbf{R}^*, \times \rangle$ ✓

2) $\langle \mathbf{Z}^+, + \rangle$ ✗ $\langle \mathbf{N}, + \rangle$ ✗ $\langle \mathbf{Z}, \times \rangle$ ✗

3) $\langle M_n(\mathbf{R}), + \rangle$ ✓ $\langle M_n(\mathbf{R}), \cdot \rangle$ ✗

4) $\langle P(B), \oplus \rangle$, \oplus 为对称差运算. ✓ 单位元为 \emptyset

5) $\langle \mathbf{Z}_n, \oplus \rangle$, $\mathbf{Z}_n = \{0, 1, \dots, n-1\}$, \oplus 为模 n 加. ✓

14.3.2 群

Klein四元群

设 $G = \{ e, a, b, c \}$, G 上的运算由下表给出, 称为 Klein四元群.

运算表特征:

- e 为单位元;
- 主对角线元素都是单位元, 每个元素是自己的逆元;
- a, b, c 中任两个元素运算都等于第三个元素;
- 对称性---运算可交换.

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

14.3.2 群

群中的术语

定义14.15 1) 若群 G 是有穷集, 则称 G 是**有限群**, 否则为**无限群**.

群 G 中的元素个数称为群 G 的**阶**, 有限群 G 的阶, 记作 $|G|$.

2) 若群 G 中的二元运算是**可交换的**, 则称 G 为**交换群**或**阿贝尔群**.

例: $\langle \mathbf{Z}, + \rangle$ 和 $\langle \mathbf{R}, + \rangle$ 是 无限 群和 交换 群;

$\langle \mathbf{Z}_n, \oplus \rangle$ 是 n 阶 群和 交换 群;

Klein 四元群是 4 阶 群和 交换 群;

n 阶 ($n \geq 2$) 实可逆矩阵集合关于矩阵乘法构成的群是交换群? **×**

14.3.2 群

群中的术语 (续)

定义14.15 3) 若群 G 中只含单位元, 则称为**平凡群**.

是只有一个元素的群, 例如

$*$	a
a	a

此时, **单位元 = 零元 = 逆元 = a** .

注: 平凡群是唯一有零元的群.

14.3.2 群

群的幂运算

定义14.16 设 G 是群, $x \in G$, $n \in \mathbf{Z}$, 则 x 的 n 次幂 x^n 定义为

$$x^n = \begin{cases} e & n = 0 \\ x^{n-1}x & n > 0 \\ (x^{-1})^m & m = -n, n < 0 \end{cases} \quad n \in \mathbf{Z}$$

例:

在 $\langle \mathbf{Z}_3, \oplus \rangle$ 中有 $2^{-3} = (2^{-1})^3 = 1^3 = 1 \oplus 1 \oplus 1 = 0$;

在 $\langle \mathbf{Z}, + \rangle$ 中有 $(-2)^{-3} = ((-2)^{-1})^3 = 2^3 = 2 + 2 + 2 = 6$.

14.3.2 群

群中的术语 (续)

定义14.17 设 G 是群, $x \in G$, 使得等式 $x^k = e$ 成立的**最小正整数** k 称为 x 的**阶** (或**周期**), 记作 $|x| = k$, 称 x 为 k 阶元. 若不存在这样的正整数 k , 则称 x 为无限阶元.

例: Klein 四元群中, 元素 a 的阶 $|a| = 2$

在 $\langle \mathbb{Z}_6, \oplus \rangle$ 中, 0 是 1 阶元, 1 是 6 阶元, 2 是 3 阶元,
3 是 2 阶元, 4 是 3 阶元, 5 是 6 阶元

在 $\langle \mathbb{Z}, + \rangle$ 中, 0 是 1 阶元, 其它整数是 无限阶元.

14.3.2 群

群的性质——幂运算规则

定理14.3 设 G 为群, 则 G 中的幂运算满足:

- 1) $\forall x \in G, (x^{-1})^{-1} = x;$
- 2) $\forall x, y \in G, (xy)^{-1} = y^{-1}x^{-1};$
- 3) $\forall x \in G, x^n x^m = x^{n+m}, n, m \in \mathbf{Z};$
- 4) $\forall x \in G, (x^n)^m = x^{nm}, n, m \in \mathbf{Z};$
- 5) 若 G 为交换群, 则 $(xy)^n = x^n y^n.$

14.3.2 群

群的性质——幂运算规则 (续)

证明:

1) $(x^{-1})^{-1}$ 是 x^{-1} 的逆元, x 也是 x^{-1} 的逆元. 根据逆元的唯一性, 等式得证.

或: $(x^{-1})x = e$, 因此, $x = (x^{-1})^{-1}$.

2) $(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}y = e,$

同理, $(xy)(y^{-1}x^{-1}) = e$, 故 $y^{-1}x^{-1}$ 是 xy 的逆元.

根据逆元的唯一性得证.

14.3.2 群

群的性质——幂运算规则 (续)

证明： 3) 用数学归纳法证明对于自然数 n 等式为真，
然后讨论 n 为负数的情况。

① $n = 0$: $x^0 x^m = e x^m = x^m = x^{0+m}$, 成立;

② $n > 0$: 设 $n = k$ ($k \geq 0$) 时成立, 即 $x^k x^m = x^{k+m}$,

当 $n = k + 1$: $x^{k+1} x^m = x^k x x^m = x^k x^{1+m} = x^{k+1+m}$, 成立;

③ $n < 0$: 设 $n = -k$ 时成立, 即 $x^{-k} x^m = x^{-k+m}$,

当 $n = -k - 1$: $x^{-k-1} x^m = (x^{-1})^{k+1} x^m = (x^{-1})^k x^{-1} x^m$
 $= x^{-k} x^{-1+m} = x^{-k-1+m}$,

14.3.2 群

群的性质——幂运算规则（续）

注：

1) 定理中的 (2) 中的结果可以推广到有限多个元素的情况，即

$$(x_1 x_2 \dots x_n)^{-1} = x_n^{-1} x_{n-1}^{-1} \dots x_2^{-1} x_1^{-1}$$

2) 定理中的 (5) 只对交换群成立。如果 G 是非交换群，那么

$$(xy)^n = \underbrace{(xy)(xy)\dots(xy)}_{n\uparrow}$$

14.3.2 群

群的性质——群方程存在唯一解

定理14.4 G 为群, $\forall a, b \in G$, 方程 $ax = b$ 和 $ya = b$ 在 G 中有解
且仅有唯一解.

证明: $a^{-1}b$ 代入方程左边的 x , 得

$$a(a^{-1}b) = (aa^{-1})b = eb = b,$$

所以 $a^{-1}b$ 是该方程的解. 下面证明唯一性.

假设 $c \neq a^{-1}b$ 也是方程 $ax = b$ 的解, 必有 $ac = b$, 从而有

$$c = ec = (a^{-1}a)c = a^{-1}(ac) = a^{-1}b,$$

同理可证, ba^{-1} 是方程 $ya = b$ 的唯一解.

14.3.2 群

群的性质——群方程存在唯一解（续）

例：设群 $G = \langle P(\{a, b\}), \oplus \rangle$ ，其中 \oplus 为对称差。求解下列群方程：

$$\{a\} \oplus X = \emptyset, \quad Y \oplus \{a, b\} = \{b\}.$$

解：

$$X = \{a\}^{-1} \oplus \emptyset = \{a\} \oplus \emptyset = \{a\},$$

$$Y = \{b\} \oplus \{a, b\}^{-1} = \{b\} \oplus \{a, b\} = \{a\}.$$

14.3.2 群

群的性质——群方程存在唯一解（续）

例(续)：群 $G = \langle P(\{a, b\}), \oplus \rangle$ ，其中 \oplus 为对称差。

运算表：

\oplus	\emptyset	$\{a\}$	$\{b\}$	$\{a, b\}$
\emptyset	\emptyset	$\{a\}$	$\{b\}$	$\{a, b\}$
$\{a\}$	$\{a\}$	\emptyset	$\{a, b\}$	$\{b\}$
$\{b\}$	$\{b\}$	$\{a, b\}$	\emptyset	$\{a\}$
$\{a, b\}$	$\{a, b\}$	$\{b\}$	$\{a\}$	\emptyset

这是一个什么群？

Klein 四元群

14.3.2 群

群的性质——消去律

定理14.5 G 为群, 则 G 中适合消去律, 即对任意 $a, b, c \in G$, 有

- 1) 若 $ab = ac$, 则 $b = c$;
- 2) 若 $ba = ca$, 则 $b = c$.

证明: 1) G 为群, $a \in G$, 所以存在 $a^{-1} \in G$,

$$ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac) \Rightarrow (a^{-1}a)b = (a^{-1}a)c \Rightarrow b = c.$$

或: 将 b 作为未知数求解: $b = a^{-1}(ac) = a^{-1}ac = ec = c$.

2) 同理可证.

14.3.2 群

群的性质——消去律 (续)

例：设 $G = \{a_1, a_2, \dots, a_n\}$ 是 n 阶群, $a_i \in G$, 令

$$a_i G = \{ a_i a_j \mid j=1,2, \dots, n \} ,$$

注：对无限群不成立，

例如, $\langle \mathbf{Z}, + \rangle$.

证明： $a_i G = G$.

证明：由群中运算的封闭性有 $a_i G \subseteq G$.

假设 $a_i G \subset G$, 即 $|a_i G| < n$. 必有 $a_j, a_k \in G$, 使得

$$a_i a_j = a_i a_k \quad (j \neq k) \quad (\text{鸽巢原理})$$

由消去律得 $a_j = a_k$, 与 $|G| = n$ 矛盾.

故, $a_i G \subset G$ 不成立, 得证 $a_i G = G$.

14.3.2 群

群中元素阶的性质

定理14.6 G 为群, $a \in G$ 且 $|a| = r$. 设 k 是整数, 则

1) $a^k = e$ 当且仅当 $r \mid k$;

2) $|a^{-1}| = |a|$.

证明: 1) 必要性: 对整数 k , 根据除法, 存在整数 m 和 i 使得

$$k = mr + i, \quad 0 \leq i < r,$$

从而有 $e = a^k = a^{mr+i} = (a^r)^m a^i = e a^i = a^i$.

因为 $|a| = r$, 且 $0 \leq i < r$, 必有 $i = 0$. 这就证明了 $r \mid k$.

14.3.2 群

群中元素阶的性质 (续)

1) 充分性: 由 $r \mid k$, 必存在整数 m 使得 $k = mr$, 所以有

$$a^k = a^{mr} = (a^r)^m = e^m = e.$$

2) 由 $(a^{-1})^r = (a^r)^{-1} = e^{-1} = e$, 可知 a^{-1} 的阶存在.

令 $|a^{-1}| = t$, 根据上面的证明有 $t \mid r$.

a 又是 a^{-1} 的逆元, 则 $a^t = ((a^{-1})^t)^{-1} = e$, 所以 $r \mid t$.

从而证明了 $r = t$, 即 $|a^{-1}| = |a|$.

14.3.2 群

例: 验证 $\langle \mathbf{Z}_6, \oplus \rangle$, $|a^{-1}| = |a|$.

$$2^{-1} = ? \quad 4$$

$$|2| = ? \quad 3$$

$$|4| = ? \quad 3$$

$$|2| = |4|$$

$$\text{又: } 1^{-1} = ? \quad 5$$

$$|1| = ? \quad 6$$

$$|5| = ? \quad 6$$

$$|1| = |5|$$

14.3.2 群

群性质的应用

例：证明单位元为群中唯一幂等元 .

证明：设 G 为群 . a 为 G 中幂等元 . 则 $aa = a$,

从而得到 $aa = ae$. 根据消去律得 $a = e$.

例：设 G 为群, 如果 $\forall a \in G$ 都有 $a^2 = e$, 证明 G 为 Abel 群 .

证明：因为 $aa^{-1} = e$, 所以 $a^2 = e \Leftrightarrow a = a^{-1}$

任取 $x, y \in G$, 则由群的封闭性有 $xy \in G$, 于是

$$xy = (xy)^{-1} = y^{-1}x^{-1} = yx .$$

因此, G 为 Abel 群.

14.3.2 群

子群的定义

定义14.18 设 G 是群, H 是 G 的非空子集, 如果 H 关于 G 中的运算构成群, 则称 H 是 G 的子群, 记作 $H \leq G$. 若 H 是 G 的子群, 且 $H \subset G$, 则称 H 是 G 的真子群, 记作 $H < G$.

注: 子群 H 需满足:

- 1) H 是 G 的非空子集;
- 2) H 关于 G 中运算封闭;
- 3) $e \in H$;
- 4) $\forall x \in H, x^{-1} \in H$.

14.3.2 群

子群的定义 (续)

例:

$n\mathbf{Z}$ (n 是自然数) 是整数加群 $\langle \mathbf{Z}, + \rangle$ 的子群.

当 $n \neq 1$ 时, $n\mathbf{Z}$ 是 \mathbf{Z} 的真子群.

注: 1) 对任何群 G 都存在子群;

2) G 和 $\{e\}$ 都是 G 的子群, 称为 G 的平凡子群.

14.3.2 群

子群判定定理一

定理14.7 设 G 为群, H 是 G 的非空子集. H 是 G 的子群当且仅当

$$\forall a, b \in H \text{ 有 } ab \in H; \forall a \in H \text{ 有 } a^{-1} \in H.$$

证明: 必要性: 显然;

充分性: 即只需证明 $e \in H$.

由于 H 非空, 存在 $a \in H$, 因此有 $a^{-1} \in H$.

根据已知必有 $aa^{-1} \in H$, 即 $e \in H$. H 满足子群定义.

14.3.2 群

子群判定定理一 (续)

例：证明 $n\mathbf{Z}$ 是整数加群 $\langle \mathbf{Z}, + \rangle$ 的子群.

证明：显然 $n\mathbf{Z}$ 是 \mathbf{Z} 的非空子集，因为 $n \in n\mathbf{Z}$.

任取 $nk, nl \in n\mathbf{Z}$,

$$nk + nl = n(k + l), \quad n(k + l) \in n\mathbf{Z},$$






又因为,

$$(nk)^{-1} = -nk = n(-k) \in n\mathbf{Z},$$

根据判定定理一， $n\mathbf{Z}$ 是整数加群的子群.

14.3.2 群

例：判断下列命题的真假：

- 1) $A = \{x \mid x \in \mathbf{N}, \text{且} \gcd(x, 5) = 1\}$, 则 $\langle A, + \rangle$ 构成代数系统,
+ 为普通加法; 
- 2) $\forall x, y \in \mathbf{R}, x * y = |x - y|$, 则 0 为 $\langle \mathbf{R}, * \rangle$ 的单位元; 
- 3) $\forall x, y \in \mathbf{R}, x * y = x + y + xy$, 则 $\forall x \in \mathbf{R}, x^{-1} = -x / (1 + x)$; 
- 4) $A = \{1, 2, \dots, 10\}, \forall x, y \in A, x * y = \gcd(x, y)$, 则 $\langle A, * \rangle$ 是半群; 
- 5) 任何代数系统都存在子代数. 

14.3.2 群


例：设 $A = \{1, 2\}$, B 是 A 上的等价关系的集合.

1) 列出 B 的元素: $B = \{I_A, E_A\}$

2) 给出代数系统 $V = \langle B, \cap \rangle$ 的运算表:

\cap	I_A	E_A
I_A	I_A	I_A
E_A	I_A	E_A

3) V 的单位元是 $\underline{E_A}$ 零元是 $\underline{I_A}$ 可逆元素是 $\underline{E_A}$ 逆元是 $\underline{E_A}$.

4) V 是半群?  独异点?  群? 

14.3.2 群

例：设 G 为群, $H \leq G$, 证明如果

$$x \in G, \text{ 且 } xH = \{xh \mid h \in H\}$$

是 G 的子群, 则 $x \in H$.

证明： xH 是 G 的子群, 所以 $e \in xH$,

即存在 $h \in H$, 使得 $xh = e$

因此, $x = h^{-1}$.

又因为, H 是 G 的子群, $h \in H$

由判定定理一, 有 $h^{-1} \in H$, 即 $x \in H$.

作业

14.12

14.13

研 讨 题

1) $\langle P(\{a, b\}), \cup \rangle$ 为哪种代数系统？

2) 设 $V = \langle S, \circ \rangle$ 是一个半群，则对任意的 $a \in S$, 令

$$\langle a \rangle = \{x \mid x = a^n, n > 0\},$$

证明： $\langle a \rangle$ 是一个子半群．若 V 是一个独异点，怎样类似地定义一个子独异点．

3) 设 $V = \langle S, \circ \rangle$ 是一个半群，若二元运算 \circ 满足交换律，则对任意的幂等元 a , 映射 $f_a(x) = a \circ x$ 是一个 V 上的自同态．

14.3.2 群

子群判定定理二

定理14.8 设 G 为群, H 是 G 的非空子集. H 是 G 的子群当且仅当

$$\forall a, b \in H \text{ 有 } ab^{-1} \in H.$$

证明: 只证充分性.

由于 H 非空, 必有 $x \in H$. 由已知有 $xx^{-1} \in H$, 从而得到 $e \in H$.

任取 H 中元素 a , 由 $e, a \in H$, 得 $ea^{-1} \in H$, 即 $a^{-1} \in H$.

任取 $a, b \in H$, 必有 $b^{-1} \in H$, 从而可得 $a(b^{-1})^{-1} \in H$, 即 $ab \in H$.

根据判定定理一 (或子群定义) 得证.

14.3.2 群

子群判定定理二 (续)

例：证明 $n\mathbf{Z}$ 是整数加群 $\langle \mathbf{Z}, + \rangle$ 的子群.

证明：1) 显然 $n\mathbf{Z}$ 是 \mathbf{Z} 的非空子集.

2) $\forall a, b \in n\mathbf{Z}$, 假设 $a = nk_1, b = nk_2, k_1, k_2 \in \mathbf{Z}$

则

$$a + b^{-1} = nk_1 + (-nk_2) = n(k_1 - k_2) \in n\mathbf{Z},$$

由判定定理二，得证.

14.3.2 群

重要的子群 (群的中心)

例：设 G 为群，证明下面的集合是 G 的子群

$$C = \{ a \mid a \in G, \forall x \in G (ax = xa) \}.$$

证明：方法一，根据判定定理一：

1) 设 $e \in G$ 是单位元, $\forall x \in G, ex = x = xe \Rightarrow e \in C$, C 是 G 的非空子集;

2) $\forall a, b \in C$, 则 $a, b \in G$, 且 $ab \in G$. 对于 $\forall x \in G$, 有

$$(ab)x = a(bx) = a(xb) = (ax)b = (xa)b = x(ab) \Rightarrow ab \in C, \text{ 封闭}$$

3) $\forall a \in C$, 要证 $a^{-1} \in C$.

$$\forall x \in G, a^{-1}x = a^{-1}(x^{-1})^{-1} = (x^{-1}a)^{-1} = (ax^{-1})^{-1} = xa^{-1} \Rightarrow a^{-1} \in C$$

14.3.2 群

重要的子群 (群的中心)

例：设 G 为群，证明下面的集合是 G 的子群

$$C = \{ a \mid a \in G, \forall x \in G (ax = xa) \}.$$

证明：方法二，根据判定定理二：

- 1) 设 $e \in G$ 是单位元, $\forall x \in G, ex = x = xe \Rightarrow e \in C$, C 是 G 的非空子集;
- 2) $\forall a, b \in C$, 则 $a, b \in G$, 且 $ab \in G, b^{-1} \in G$. 对于 $\forall x \in G$, 有

$$\begin{aligned} (ab^{-1})x &= a(b^{-1}x) = a(b^{-1}(xb^{-1})^{-1}) = a(x^{-1}b)^{-1} = a(bx^{-1})^{-1} \\ &= a(xb^{-1}) = (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1}) \\ &\Rightarrow ab^{-1} \in C \end{aligned}$$

14.3.2 群

重要的子群 (生成子群)

定义 设 G 为群, $a \in G$, 令

$$H = \{ a^k \mid k \in \mathbb{Z} \},$$

则 H 是 G 的子群, 称为由 a 生成的子群, 记作 $\langle a \rangle$.

证明: 首先由 $a \in \langle a \rangle$, 知道 $\langle a \rangle \neq \emptyset$, 则 $\langle a \rangle$ 是 G 的非空子集.

任取 $x, y \in \langle a \rangle$, $x = a^m$, $y = a^l$, 则

$$xy^{-1} = a^m (a^l)^{-1} = a^m a^{-l} = a^{m-l} \in \langle a \rangle$$

根据子群判定定理二可知, $\langle a \rangle \leq G$.

14.3.2 群

重要的子群 (生成子群)

例：1) 整数加群 $\langle \mathbf{Z}, + \rangle$, 由 2 生成的子群是 $\langle 2 \rangle = \{ 2k \mid k \in \mathbf{Z} \} = 2\mathbf{Z}$;

2) 群 $\langle \mathbf{Z}_6, \oplus \rangle$ 中, 由 2 生成的子群 $\langle 2 \rangle = \{ 0, 2, 4 \}$;

3) Klein 四元群 $G = \{ e, a, b, c \}$ 的所有生成子群是:

$$\langle e \rangle = \{ e \}, \quad \langle a \rangle = \{ e, a \},$$

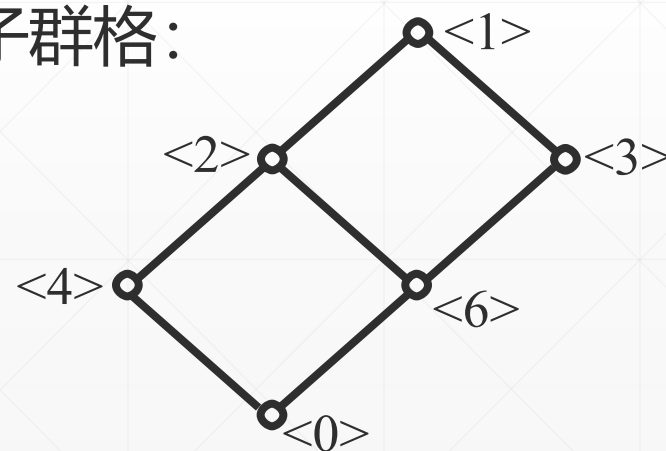
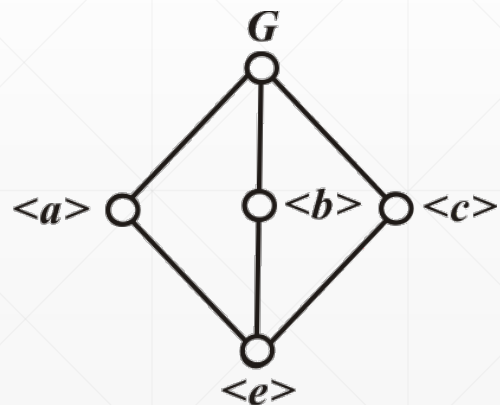
$$\langle b \rangle = \{ e, b \}, \quad \langle c \rangle = \{ e, c \}.$$

14.3.2 群

子群格

定义 设 G 为群, 令 $S = \{ H \mid H \leq G \}$ 是 G 的所有子群的集合, 定义 S 上的偏序 \leq , $\forall x, y \in S, x \leq y \Leftrightarrow x \subseteq y$, 那么 $\langle S, \leq \rangle$ 构成格 (哈斯图), 称为 G 的子群格.

例: Klein 四元群 G 和 $\langle \mathbf{Z}_{12}, \oplus \rangle$ 的子群格:



14.3.2 群

群同态的定义与分类

定义14.19 设 G_1, G_2 是群, $f : G_1 \rightarrow G_2$, 若 $\forall a, b \in G_1$ 都有

$$f(a b) = f(a) f(b)$$

则称 f 是群 G_1 到 G_2 的**同态映射**, 简称**同态**.

如果同态 f 为**单射**函数, 则称为**单同态**;

如果是**满射**函数, 则称为**满同态**, 记作 $G_1 \sim G_2$;

如果是**双射**函数, 则称为**同构**, 记作 $G_1 \cong G_2$;

如果 $G_1 = G_2$, 则称为**自同态**.

14.3.2 群

群同态的定义与分类 (续)

例：设 G 是群，

$$f(x) = axa^{-1}, \quad a \in G,$$

f 是不是 G 的自同态？

证明：


$$\forall x, y \in G, f(xy) = axya^{-1} = axa^{-1}aya^{-1} = f(x)f(y),$$

所以 f 是群 G 的自同态

14.3.2 群

群同态的实例

例：1) $G_1 = \langle \mathbf{Z}, + \rangle$ 是整数加群, $G_2 = \langle \mathbf{Z}_n, \oplus \rangle$ 是模 n 的整数加群.

令 $f : \mathbf{Z} \rightarrow \mathbf{Z}_n, f(x) = x \bmod n$, f 是 G_1 到 G_2 的同态? 

$$\forall x, y \in \mathbf{Z},$$

$$f(x + y) = (x + y) \bmod n = x \bmod n \oplus y \bmod n = f(x) \oplus f(y)$$

f 是 G_1 到 G_2 的 满 同态.

2) 设 $G = \langle \mathbf{Z}_n, \oplus \rangle$ 是模 n 整数加群, 可以证明恰有 n 个 G 的自同态,

即 $f_p : \mathbf{Z}_n \rightarrow \mathbf{Z}_n, f_p(x) = (px) \bmod n, p = 0, 1, \dots, n-1$.

14.3.2 群

群同态的实例

例： (续)

3) 设 G_1, G_2 是群, e_2 是 G_2 的单位元.

$$f: G_1 \rightarrow G_2, \quad f(a) = e_2, \quad \forall a \in G_1.$$

则 f 是 G_1 到 G_2 的同态, 称为**零同态**.

$$\forall a, b \in G_1, \quad f(ab) = e_2 = e_2 e_2 = f(a) f(b).$$

4) G 为群, $a \in G$. 令 $f: G \rightarrow G, f(x) = axa^{-1}, \quad \forall x \in G$

则 f 是 G 的自同构, 称为 G 的**内自同构**.

14.3.2 群

群同态的性质

设 f 是群 G_1 到 G_2 的同态映射, 则

1) $f(e_1) = e_2$, e_1 和 e_2 分别是 G_1 和 G_2 的单位元;

证明: $f(e_1)f(e_1) = f(e_1e_1) = f(e_1) = f(e_1)e_2 \Rightarrow f(e_1) = e_2$

2) $\forall x \in G_1, f(x^{-1}) = f(x)^{-1}$;

证明:

$$f(x)f(x^{-1}) = f(xx^{-1}) = f(e_1) = e_2$$

$$f(x^{-1})f(x) = f(x^{-1}x) = f(e_1) = e_2$$

14.3.2 群

群同态的性质

设 f 是群 G_1 到 G_2 的同态映射, 则

3) 设 $H \leq G_1$, 则 $f(H) \leq G_2$.

证明: 因为 $H \leq G_1$, 所以 $e_1 \in H$, 则 $f(e_1) = e_2 \in f(H)$, $f(H) \neq \emptyset$;

$\forall a, b \in f(H)$, $\exists x, y \in H$, 使得 $f(x) = a$, $f(y) = b$,

$ab^{-1} = f(x)f(y)^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$,

$xy^{-1} \in H \Rightarrow f(xy^{-1}) \in f(H) \Rightarrow ab^{-1} \in f(H)$.

14.3.2 群

例：给出 Klein 四元群上所有的自同构。

解： $G = \{e, a, b, c\}$,

- 1) 因为同态 f 满足 $f(e) = e$;
- 2) $\forall x \in G, x \neq e, f(x^2) = f(e) = e, \Rightarrow f(x) \neq e$
- 3) $\forall x, y, z \in G, x \neq y \neq z \neq e, f(xy) = f(x)f(y) = f(z),$

因此只有以下 6 个双射函数是同构映射:

$$f_1(a) = b, f_1(b) = a, f_1(c) = c; \quad f_2(a) = c, f_2(b) = b, f_2(c) = a;$$

$$f_3(a) = a, f_3(b) = c, f_3(c) = b; \quad f_4(a) = b, f_4(b) = c, f_4(c) = a;$$

$$f_5(a) = c, f_5(b) = a, f_5(c) = b; \quad f_6 = I_G,$$

14.3.2 群

例：设 $G_1 = \langle \mathbb{Q}^*, \cdot \rangle$, $G_2 = \langle \mathbb{Q}, + \rangle$, 证明**不存在** G_1 到 G_2 的**同构**.

证明：假设存在 G_1 到 G_2 的同构 f , 那么 $f(1) = 0$. 因此

$$f(-1) + f(-1) = f((-1)(-1)) = f(1) = 0$$

$$\Rightarrow f(-1) = 0$$

与 f 的双射性**矛盾**.

14.3.2 群

循环群

定义14.20 设 G 是群, 若存在 $a \in G$ 使得

$$G = \{ a^k \mid k \in \mathbf{Z} \},$$

则称 G 是循环群, 记作 $G = \langle a \rangle$, 称 a 为 G 的生成元.

例: 整数加群 $G = \langle \mathbf{Z}, + \rangle$ 是循环群 ? 

$$G = \langle \underline{1} \rangle = \langle \underline{-1} \rangle$$

模 6 加群 $G = \langle \mathbf{Z}_6, \oplus \rangle$ 是循环群 ? 

$$G = \langle \underline{1} \rangle = \langle \underline{5} \rangle$$

14.3.2 群

循环群的分类

设循环群 $G = \langle a \rangle$, 根据生成元 a 的阶可以分成两类:

设 $G = \langle a \rangle$ 是循环群, 若 a 是 n 阶元, 则

$$G = \{ a^0 = e, a^1, a^2, \dots, a^{n-1} \},$$

那么 $|G| = n$, 称 G 为 n 阶循环群.

若 a 是无限阶元, 则

$$G = \{ a^0 = e, a^{\pm 1}, a^{\pm 2}, \dots \},$$

这时称 G 为无限循环群.

14.3.2 群

循环群的分类 (续)

注：循环群一定是 Abel 群.

证明：设 $G = \langle a \rangle$ 为循环群，则 $\forall x, y \in G, \exists m, n \in \mathbf{Z}$, 使得 $x = a^n, y = a^m$,
则

$$xy = a^n a^m = a^{n+m} = a^{m+n} = a^m a^n = yx,$$

所以 G 是 Abel 群.

14.3.2 群

循环群的生成元

定理14.9 设 $G = \langle a \rangle$ 是循环群.

- 1) 若 G 是无限循环群, 则 G 只有两个生成元, 即 a 和 a^{-1} ;
- 2) 若 G 是 n 阶循环群, 则 G 含有 $\phi(n)$ 个生成元. 对于任何小于 n 且与 n 互质的自然数 r , a^r 是 G 的生成元.

注: $\phi(n)$ 为欧拉函数, 表示 $\{0, 1, \dots, n-1\}$ 中与 n 互素的整数个数.

14.3.2 群

循环群的生成元

例: $\phi(18) = \underline{6}$, 与 18 互素的正整数为 1, 5, 7, 11, 13, 17.

对 $G = \langle \mathbf{Z}_{18}, \oplus \rangle$:

生成元 1: 1, 2, 3,, 18 (= 0);

生成元 5:

5, 10, 15, 2, 7, 12, 17, 4, 9, 14, 1, 6, 11, 16, 3, 8, 13, 18 (= 0);

14.3.2 群

例:

- 1) 设 $G = \{e, a, \dots, a^{11}\}$ 是 12 阶循环群, 小于或等于 12 且与 12 互素的数是 1, 5, 7, 11, 则 $\phi(12) =$ 4. 由定理可知 G 的生成元是 a, a^5, a^7 和 a^{11} .
- 2) 设 $G = \langle \mathbf{Z}_9, \oplus \rangle$ 是模 9 的整数加群, 小于或等于 9 且与 9 互素的数是 1, 2, 4, 5, 7, 8, 则 $\phi(9) =$ 6. 根据定理, G 的生成元是 1, 2, 4, 5, 7 和 8.
- 3) 设 $G = 3\mathbf{Z} = \{3z \mid z \in \mathbf{Z}\}$, G 上的运算是普通加法. 那么 G 的生成元是: 3 和 -3.

14.3.2 群

循环群的子群

定理14.10 设 $G = \langle a \rangle$ 是循环群, 则

- 1) G 的子群仍是循环群;
- 2) 若 $G = \langle a \rangle$ 是无限循环群, 则 G 的子群除 $\{e\}$ 以外都是无限循环群;
- 3) 若 $G = \langle a \rangle$ 是 n 阶循环群, 则对 n 的每个正因子 d , G 恰好含有一个 d 阶子群, 就是 $\langle a^{n/d} \rangle$.

14.3.2 群

例：1) $G = \langle \mathbf{Z}, + \rangle$ 是无限循环群，子群有：

$$\langle 0 \rangle = \{ 0 \} = 0\mathbf{Z}$$

对于自然数 $m \in \mathbf{N}$ ，1 的 m 次幂是 m ， m 生成的子群是 $m\mathbf{Z}$ ，

即， $m \in \mathbf{N}$ ，

$$\langle m \rangle = \langle -m \rangle = \{ mz \mid z \in \mathbf{Z} \} = m\mathbf{Z} .$$

14.3.2 群

例：2) $G = \mathbf{Z}_{18} = \langle 1 \rangle$ 是 18 阶循环群. 18 的正因子是 1, 2, 3, 6, 9 和 18, 因此 G 的子群有 6 个, 分别是:

1 阶子群 $\langle 18 \rangle = \langle 0 \rangle = \{0\}$

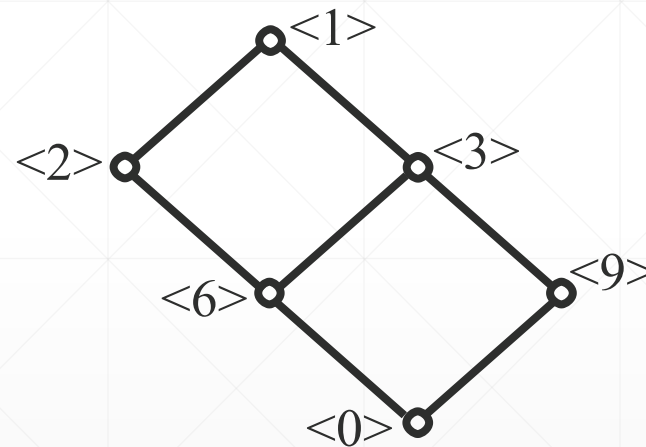
2 阶子群 $\langle 9 \rangle = \{0, 9\}$

3 阶子群 $\langle 6 \rangle = \{0, 6, 12\}$

6 阶子群 $\langle 3 \rangle = \{0, 3, 6, 9, 12, 15\}$

9 阶子群 $\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16\}$

18 阶子群 $\langle 1 \rangle = \langle 5 \rangle = \langle 7 \rangle = \langle 11 \rangle = \langle 13 \rangle = \langle 17 \rangle = \mathbf{Z}_{18}$



14.3.2 群

循环群的子群格

例: $\langle \mathbb{Z}_{30}, \oplus \rangle$ 的子群格.

解: $30 = 1 \times 2 \times 3 \times 5$

0 个因子: $\langle 1 \rangle$;

1 个因子: $\langle 2 \rangle, \langle 3 \rangle, \langle 5 \rangle$;

2 个因子: $\langle 6 \rangle, \langle 10 \rangle, \langle 15 \rangle$;

3 个因子: $\langle 0 \rangle$

$$\langle 0 \rangle = \{0\}$$

$$\langle 1 \rangle = \{0, 1, 2, 3, 4, \dots, 29\}$$

$$\langle 2 \rangle = \{0, 2, 4, 6, 8, 10, \dots, 28\}$$

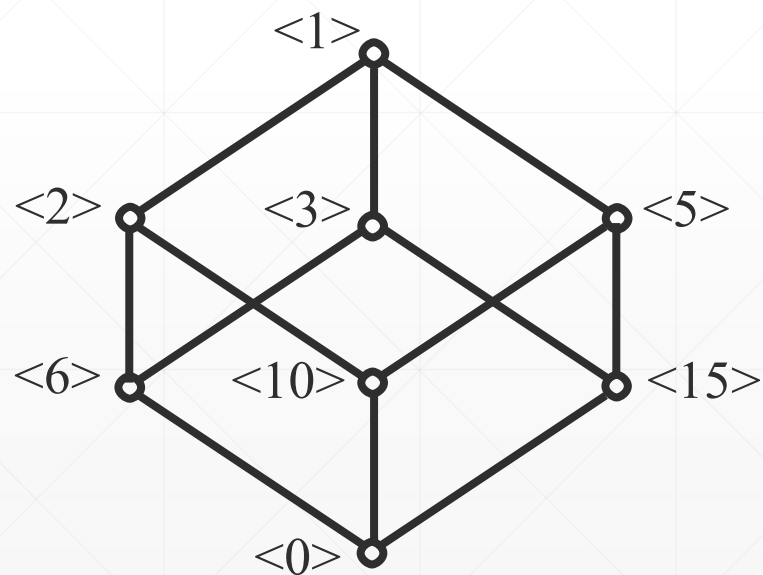
$$\langle 3 \rangle = \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27\}$$

$$\langle 5 \rangle = \{0, 5, 10, 15, 20, 25\}$$

$$\langle 6 \rangle = \{0, 6, 12, 18, 24\}$$

$$\langle 10 \rangle = \{0, 10, 20\}$$

$$\langle 15 \rangle = \{0, 15\}$$



14.3.2 群

循环群的子群格

例: $\langle \mathbb{Z}_{36}, \oplus \rangle$ 的子群格.

解: $36 = 1 \times 2 \times 2 \times 3 \times 3$

0 个因子: $\langle 1 \rangle$;

1 个因子: $\langle 2 \rangle, \langle 3 \rangle$;

2 个因子: $\langle 4 \rangle, \langle 6 \rangle, \langle 9 \rangle$;

3 个因子: $\langle 12 \rangle, \langle 18 \rangle$

4 个因子: $\langle 0 \rangle$

$$\langle 0 \rangle = \{0\}$$

$$\langle 1 \rangle = \{0, 1, 2, \dots, 35\} = \mathbb{Z}_{36}$$

$$\langle 2 \rangle = \{0, 2, 4, 6, 8, \dots, 34\}$$

$$\langle 3 \rangle = \{0, 3, 6, 9, \dots, 33\}$$

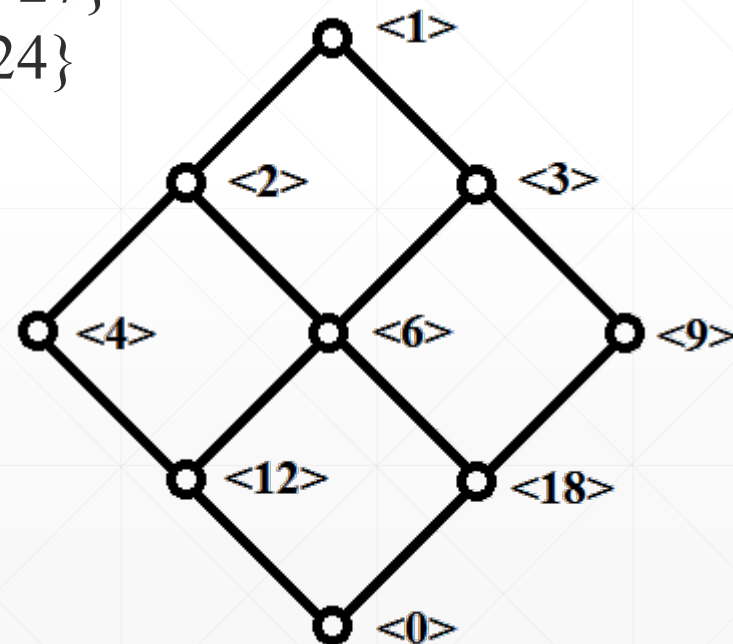
$$\langle 4 \rangle = \{0, 4, 8, \dots, 32\}$$

$$\langle 6 \rangle = \{0, 6, 12, 18, 24, 30\}$$

$$\langle 9 \rangle = \{0, 9, 18, 27\}$$

$$\langle 12 \rangle = \{0, 12, 24\}$$

$$\langle 18 \rangle = \{0, 18\}$$



14.3.2 群

n 元置换

定义14.21 设 $S = \{ 1, 2, \dots, n \}$, S 上的双射函数 $\sigma: S \rightarrow S$, 称为 S 上的 n 元置换. 一般将 n 元置换 σ 记为

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

不重复

例: $S = \{ 1, 2, 3, 4, 5 \}$, 则

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 3 & 2 \end{pmatrix}$$

都是 5 元置换.

14.3.2 群

n 元置换 (续)

定义14.22 设 σ, τ 是 n 元置换, σ 和 τ 的复合 $\sigma \circ \tau$ 也是 n 元置换, 称为 σ 和 τ 的乘积, 记为 $\sigma\tau$.

例:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}$$

则

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 4 & 2 \end{pmatrix}, \quad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{pmatrix}$$

14.3.2 群

k 阶轮换与对换

定义14.23 设 σ 是 $S = \{1, 2, \dots, n\}$ 上的 n 元置换. 若

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1,$$

且保持 S 中的其他元素不变, 则称 σ 为 S 上的 k 阶轮换,

记作 $(i_1 i_2 \dots i_k)$. 若 $k = 2$, 称 σ 为 S 上的对换.

14.3.2 群

k 阶轮换与对换 (续)

例：5元置换：

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 4 & 5 \end{pmatrix}, \lambda = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix}$$

σ 是 4 阶轮换, $\sigma = (\underline{1\ 2\ 3\ 4})$,

τ 是 2 阶轮换, $\tau = (\underline{1\ 3})$, 也叫做对换,

λ 是 4 阶轮换, $\lambda = (\underline{3\ 2\ 1\ 5})$.

14.3.2 群

n 元置换分解为轮换

例：设 $S = \{1, 2, \dots, 8\}$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 6 & 4 & 2 & 1 & 8 & 7 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 4 & 2 & 6 & 7 & 5 & 3 \end{pmatrix}$$

从 σ 中分解出来的轮换式有： $(1\ 5\ 2\ 3\ 6)$, (4) , $(7\ 8)$;

σ 的轮换表示式为： $\sigma = (1\ 5\ 2\ 3\ 6)(4)(7\ 8) = (1\ 5\ 2\ 3\ 6)(7\ 8)$

τ 的分解式为： $\tau = \underline{(1\ 8\ 3\ 4\ 2)} \underline{(5\ 6\ 7)}$.

注：1) 在轮换分解式中，1 阶轮换（恒等置换）可以省略。

2) 任何 n 元置换都可以写为若干个轮换的乘积。

14.3.2 群

分解成对换

任何 n 元置换可以分解成对换的乘积，因为任何轮换都可以表示成对换乘积。一种可行的表示方法是：

$$(i_1 i_2 \dots i_k) = (i_1 i_2) (i_1 i_3) \dots (i_1 i_k)$$

例：

$$\begin{aligned} & \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 6 & 4 & 2 & 1 & 8 & 7 \end{pmatrix} \\ &= (1\ 5\ 2\ 3\ 6)(7\ 8) \\ &= (1\ 5)(1\ 2)(1\ 3)(1\ 6)(7\ 8) \end{aligned}$$

14.3.2 群

奇置换与偶置换

注：1) 轮换分解中的轮换是可以交换的，且分解式是唯一的；

例：

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 6 & 4 & 2 & 1 & 8 & 7 \end{pmatrix}$$
$$= (1\ 5\ 2\ 3\ 6)(7\ 8) = (7\ 8)(1\ 5\ 2\ 3\ 6) = (7\ 8)(2\ 3\ 6\ 1\ 5)$$

2) 对换分解中的对换不能交换，分解式也不是唯一的；

例如：上式 $= (1\ 5)(1\ 2)(1\ 3)(1\ 6)(7\ 8) \neq (1\ 2)(1\ 5)(1\ 3)(1\ 6)(7\ 8)$

又如： $(1\ 2\ 3) = (1\ 2)(1\ 3) = (2\ 3)(2\ 1)$

3) 但是分解式含有对换个数的奇偶性不变。

14.3.2 群

奇置换与偶置换

如果一个 n 元置换在它的对换表示式含有偶数个对换，则称为偶置换，
否则称为奇置换.

使用一一对应的思想可以知道奇置换和偶置换的个数都是 $n!/2$.

n 元置换的乘法与求逆

两个 n 元置换的乘法就是函数的复合运算；

n 元置换的求逆就是求反函数.

14.3.2 群

例：设

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 3 & 2 & 1 & 4 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}$$

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 4 & 2 \end{pmatrix}, \quad \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 5 & 3 & 4 \end{pmatrix}$$

$$\sigma^{-1} = \begin{pmatrix} 5 & 3 & 2 & 1 & 4 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$$

使用轮换表示是：

$$\sigma\tau = \underline{(1\ 5\ 4)(2\ 3)(1\ 4\ 2\ 3)} = \underline{(1\ 5\ 2)}.$$

$$\tau\sigma = \underline{(1\ 4\ 2\ 3)(1\ 5\ 4)(2\ 3)} = \underline{(3\ 5\ 4)}.$$

$$\sigma^{-1} = \underline{(1\ 5\ 4)^{-1}(2\ 3)^{-1}} = \underline{(4\ 5\ 1)(3\ 2)} = \underline{(1\ 4\ 5)(2\ 3)}.$$

14.3.2 群

n 元置换群

考虑所有的 n 元置换构成的集合 S_n , S_n 关于置换的乘法是封闭的.

置换的乘法满足结合律. 恒等置换 (1) 是 S_n 中的单位元. 对于任何

n 元置换 $\sigma \in S_n$, 逆置换 σ^{-1} 是 σ 的逆元. 这就证明了 S_n 关于置换的

乘法构成一个群, 称为 n 元对称群.

n 元对称群的子群称为 n 元置换群.

例: 设 $S = \{1, 2, 3\}$, 3元对称群

$$S_3 = \{(1), (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\}.$$

14.3.2 群

S_3 的运算表

	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1)	(1)	(1 2)	(1 3)	(2 3)	(1 2 3)	(1 3 2)
(1 2)	(1 2)	(1)	(1 2 3)	(1 3 2)	(1 3)	(2 3)
(1 3)	(1 3)	(1 3 2)	(1)	(1 2 3)	(2 3)	(1 2)
(2 3)	(2 3)	(1 2 3)	(1 3 2)	(1)	(1 2)	(1 3)
(1 2 3)	(1 2 3)	(2 3)	(1 2)	(1 3)	(1 3 2)	(1)
(1 3 2)	(1 3 2)	(1 3)	(2 3)	(1 2)	(1)	(1 2 3)

14.3.2 群

例：设 $A = \{a, b, c\}$, \circ 为 A 上的二元运算, 且 $\forall x, y \in A, x \circ y = c$.

1) 找出 A 上所有的双射函数.

2) 说明这些函数是否为 $\langle A, \circ \rangle$ 的自同构, 为什么?

解: 1) 所有的双射函数:

$$f_1(a) = a, f_1(b) = b, f_1(c) = c; \quad f_2(a) = a, f_2(b) = c, f_2(c) = b;$$

$$f_3(a) = b, f_3(b) = a, f_3(c) = c; \quad f_4(a) = b, f_4(b) = c, f_4(c) = a;$$

$$f_5(a) = c, f_5(b) = b, f_5(c) = a; \quad f_6(a) = c, f_6(b) = a, f_6(c) = b.$$

采用置换的表示为:

$$f_1 = \underline{(a)}, f_2 = \underline{(bc)}, f_3 = \underline{(ab)}, f_4 = \underline{(abc)}, f_5 = \underline{(ac)}, f_6 = \underline{(acb)}.$$

14.3.2 群

例：设 $A = \{a, b, c\}$, \circ 为 A 上的二元运算, 且 $\forall x, y \in A, x \circ y = c$.

- 1) 找出 A 上所有的双射函数.
- 2) 说明这些函数是否为 $\langle A, \circ \rangle$ 的自同构, 为什么?

解：2) 因为 $\forall x, y \in A, x \circ y = c$, 如果 f 是同态, 则

$$f(a \circ b) = f(c) = f(a) \circ f(b) = x \circ y = c$$

所以, 只有 f_1 和 f_3 为自同构, 他们能满足同态映射条件,
将零元 c 映到零元 c , 即 $f(c) = c$.

14.3.2 群

例：设群 $G = \langle M_2(\mathbf{R}), + \rangle$,

$$H = \{ A \mid A \in M_2(\mathbf{R}), \text{ 且 } A = A' \},$$

其中 A' 表示 A 的转置, 证明 H 是 G 的子群.

证明：显然 H 非空.

$$\forall \begin{pmatrix} a & b \\ b & c \end{pmatrix}, \begin{pmatrix} d & e \\ e & f \end{pmatrix} \in H$$

$$\begin{pmatrix} a & b \\ b & c \end{pmatrix} - \begin{pmatrix} d & e \\ e & f \end{pmatrix} = \begin{pmatrix} a-d & b-e \\ b-e & c-f \end{pmatrix} \in H$$

根据子群判定定理, H 是子群.

14.3.2 群

例：设 f 是群 G_1 到 G_2 的同态映射, H 是 G_1 的子群, 证明 $f(H)$ 是 G_2 的子群.

证明：因为 H 非空, 因此 $f(H)$ 非空.

任取 $x, y \in f(H)$, 则存在 $a, b \in H$ 使得 $f(a) = x, f(b) = y$. 于是

$$xy^{-1} = f(a)f(b)^{-1}$$

因为 f 是群 G_1 到 G_2 的同态映射, 所以

$$f(b)^{-1} = f(b^{-1}), \text{ 且 } f(a)f(b^{-1}) = f(ab^{-1}),$$

综上, $xy^{-1} = f(ab^{-1})$, 由于 H 是子群, $ab^{-1} \in H$,

所以 $f(ab^{-1}) \in f(H)$, 即 $xy^{-1} \in f(H)$,

根据子群判定定理, $f(H)$ 是 G_2 的子群.

14.3.2 群

例：如果 G 为非 Abel 群，证明 G 的所有自同构构成的群 $\text{Aut}G$ 至少含有2个元素.

证明： G 为非Abel群, 必存在 $a, b \in G$, 满足 $ab \neq ba$.

令 $f: G \rightarrow G, f(x) = a^{-1}xa$, 则 $\forall x, y \in G$ 有

$$f(xy) = a^{-1}xya = (a^{-1}xa)(a^{-1}ya) = f(x)f(y),$$

所以 f 为同态映射. 再由

$$f(x) = f(y) \Rightarrow a^{-1}xa = a^{-1}ya \Rightarrow x = y,$$

则 f 为单射. 且对任意 $c \in G$, 有

$$f(aca^{-1}) = a^{-1}aca^{-1}a = c,$$

于是 f 为满射. 所以 f 为同构.

如果 $\text{Aut}G$ 只含有 1 个元素, 即恒等映射. 那么对于所有的 $x \in G$, $x \in G, f(x) = a^{-1}xa = x$, 即 $xa = ax$, 从而得到 $ab = ba$, 与 $ab \neq ba$ 矛盾.

14.3.2 群

例：求循环群 $\langle \mathbf{Z}_{16}, \oplus \rangle$ 的所有生成元和子群 .

解： $\langle \mathbf{Z}_{16}, \oplus \rangle$ 是 16 阶循环群，含有 $\phi(16)$ 个生成元. 对于任何小于16且与16互质的自然数 r , 1^r 是 $\langle \mathbf{Z}_{16}, \oplus \rangle$ 的生成元. 所以循环群 $\langle \mathbf{Z}_{16}, \oplus \rangle$ 的所有生成元为 1, 3, 5, 7, 9, 11, 13, 15 .

若 $G = \langle a \rangle$ 是 n 阶循环群，则对 n 的每个正因子 d , G 恰好含有一个 d 阶子群，就是 $\langle a^{n/d} \rangle$.

因为： $16 = 1 \times 2 \times 2 \times 2 \times 2$, 正因子有： 1, 2, 4, 8, 16

所以，子群有 $\langle 0 \rangle, \langle 8 \rangle, \langle 4 \rangle, \langle 2 \rangle, \langle 1 \rangle$.

14.3.2 群

例：设 m 整除 n , 证明 n 阶循环群 $G = \langle a \rangle$ 中的方程 $x^m = e$ 恰好有 m 个解.

证明：设 $x = a^t$ 是解, $0 \leq t < n$, 则

$$x^m = e \Rightarrow a^{tm} = e \Leftrightarrow n \mid tm$$

已知 m 整除 n , 即存在正整数 k , 使得 $n = km$. 于是 k 整除 t .

假设 $t = sk$, 其中 s 为整数, 又由于 $t < n$, 则 $t < km$, 因此

$$t = 0, k, \dots, (m-1)k.$$

从而得到 $x = a^0, a^k, \dots, a^{(m-1)k}$.

容易验证以上 a 的幂都是方程的解, 且两两不等.

14.3.2 群

例：设多项式 $p = (x_1 + x_2)(x_3 + x_4)$ ，找出使得 p 保持不变的所有下标的置换，这些置换是否构成 S_4 的子群。

解：所有的置换 是：

$$\begin{array}{cccc} (1), & (1\ 2), & (3\ 4), & (1\ 2)(3\ 4), \\ (1\ 3)(2\ 4), & (1\ 4)(2\ 3), & (1\ 4\ 2\ 3), & (1\ 3\ 2\ 4) \end{array}$$

根据乘法的封闭性可知这些置换构成 S_4 的子群。

作业

14.18

14.19

研 讨 题

1) 设 $\langle G, \circ \rangle$ 是群, f 和 g 是两个 G 上的自同态, 令

$$H = \{ x \mid f(x) = g(x), x \in G \},$$

证明: H 是 G 的子群.

2) 设 $\langle G, \circ \rangle$ 是交换群, n 是任意给定的整数, 令

$$G_n = \{ x \mid x = a^n, \forall a \in G \},$$

证明: G_n 是 G 的子群.

3) 写出群 $\langle \mathbb{Z}_{42}, \oplus \rangle$ 的所有生成元和子群, 并画出子群格.