第七章 群环域

大连理工大学软件学院
陈志奎 教授
办公室： 综合楼405，Tel： 62274392
实验室：综合楼
Mobile: 13478461921
Email: zkchen@dlut.edu.cn
zkchen00@hotmail.com

回 顾

- 半群和独异点的定义及性质
- 半群和独异点的同态与同构
- 积半群

7.2.1　群的概念

- **定义7.7**　给定代数系统V＝<G，⊙>，若<G，⊙>是独异点并且每个元素均存在逆元，或满足⊙是可结合的并且关于⊙存在幺元并且G中每个元素关于⊙是可逆的，则称<G，⊙>是群，记为G。

  - 群比独异点具有更强的条件。
  - 在半群、独异点、群这些概念中，由于只含有一个二元运算，所以在不发生混淆的情况下，可以将算符省去。例如将$x*y$写成xy。

代数系统 $\langle S, \odot \rangle$ $\xrightarrow{\odot\text{可结合}}$ $\xrightarrow{\text{有幺元}e}$ $\xrightarrow{\text{有逆元}a^{-1}}$ 群 $\langle S, \odot, e, a^{-1} \rangle$

或

独异点 $\langle S, \odot, e \rangle$ $\xrightarrow{\text{有逆元}a^{-1}}$ 群 $\langle S, \odot, e, a^{-1} \rangle$

- 例7.8 <Z，+>，整数加群，
  <Q，+>，有理数加群，
  <R，+>， 实数加群，
  <C，+>， 复数加群，他们都是群。

- 例7.9 给定<Z，+>和<Q，*>，其中Z和Q分别为整数集和有理数集，+ 和 * 分别是一般意义下的加法和乘法。可知<Z，+>是群，0是幺元，每个元素 $I \in Z$ 的逆元为 $-I$；<Q，*>不是群，1是幺元，0无逆元。但<Q-{0}，*>是群。

- 例7.10 设*G*={e， a， b， c}， *G*上的运算由下表表示，不难验证*G*是一个群。

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

特征：

1. 满足交换律
2. 每个元素都是自己的逆元
3. a, b, c中任何两个元素运算结果都等于剩下的第三个元素。

这个群为**Klein**四元群，简称四元群。

- 例7.11 某二进制码的码字$x = x_1 x_2 \cdots x_7$由7 位构成，其中x_1, x_2, x_3和x_4为数据位，x_5, x_6, x_7为校验位，并且满足：

$$x_5 = x_1 \oplus x_2 \oplus x_3$$

$$x_6 = x_1 \oplus x_2 \oplus x_4$$

$$x_7 = x_1 \oplus x_3 \oplus x_4$$

这里⊕是模2加法。设G为所有码字构成的集合，在G上定义的二元运算如下:

$$\forall x，y \in G,$$

$$x \circ y = z_1 z_2 \ldots z_7,$$

$$z_i = x_i \oplus y_i，i=1,2，\ldots，7$$

证明<G, ∘>构成群。

- 证明：任取$\mathrm{x} = \mathrm{x}_1 \cdots \mathrm{x}_7, \mathrm{y} = \mathrm{y}_1 \cdots \mathrm{y}_7, \mathrm{x} \circ \mathrm{y} = \mathrm{z}_1 \cdots \mathrm{z}_7$。首先验证$\mathrm{z}_5 = \mathrm{z}_1 \oplus \mathrm{z}_2 \oplus \mathrm{z}_3$。

$$
\begin{aligned}
z_1 \oplus z_2 \oplus z_3 &= (x_1 \oplus y_1) \oplus (x_2 \oplus y_2) \oplus (x_3 \oplus y_3) \\
&= (x_1 \oplus x_2 \oplus x_3) \oplus (y_1 \oplus y_2 \oplus y_3) \\
&= x_5 \oplus y_5 \\
&= z_5
\end{aligned}
$$

同理可证 $z_6 = z_1 \oplus z_2 \oplus z_4$，$z_7 = z_1 \oplus z_3 \oplus z_4$.所以$\mathrm{x} \circ \mathrm{y}=\mathrm{z} \in \mathrm{G}$，从而证明了具有封闭性。

任取x，y，$z\in G$ 令（$x\circ y$）$\circ z = a_1\ldots a_7$，$x\circ$（$y\circ z$）$= b_1\ldots b_7$。

下面证明$a_i = b_i$，$i = 1,2, \ldots, 7$。

由于⊕运算满足结合律，

因此有

$$a_i = (x_i \oplus y_i) \oplus z_i = x_i \oplus (y_i \oplus z_i) = b_i,$$

从而证明了G中满足结合律。

易知单位元0000000，$\forall x\in G$，$x^{-1}=x$。

综上所述，G构成群。

7.2.2 群的性质

- 群的基本性质：

（1）封闭性： 若$a,b\in G$，则存在唯一确定的$c\in G$,使得$a*b=c$；

（2）结合律成立：任意$a,b,c\in G$，有$(a*b)*c=a*(b*c)$；

（3）单位元存在：存在$e\in G$,对任意$a\in G$，满足$a*e=e*a=a$，称e为单位元，也称幺元；

（4）逆元存在：任意$a\in G$，存在唯一确定的$b\in G$，$a*b=b*a=e$（单位元），则称a与b互为逆元素，简称逆元，记作$a^{-1}=b$。

群中元素的幂

- 定义7.8 设G是群，a∈G，n∈Z，则a 的 n次幂。

$$a^n = \begin{cases} e & n = 0 \\ a^{n-1}a & n > 0 \\ (a^{-1})^m & n < 0, n = -m \end{cases}$$

群中元素可以定义负整数次幂。

在$<Z_3,\oplus>$中有

$$2^{-3} = (2^{-1})^3 = 1^3 = 1\oplus1\oplus1 = 0$$

在$<Z,+>$中有

$$(-2)^{-3} = 2^3 = 2+2+2 = 6$$

群的性质：幂运算规则

- 定理7.7 设G 为群，则G中的幂运算满足：

  (1) $\forall a \in G$，$(a^{-1})^{-1} = a$

  (2) $\forall a, b \in G$，$(ab)^{-1} = b^{-1}a^{-1}$

  (3) $\forall a \in G$，$a^n a^m = a^{n+m}$，$n, m \in Z$

  (4) $\forall a \in G$，$(a^n)^m = a^{nm}$，$n, m \in Z$

  (5) 若G为交换群，则$(ab)^n = a^n b^n$.

- 证明：(1) $(a^{-1})^{-1}$是a^{-1}的逆元，a也是a^{-1}的逆元. 根据逆元唯一性，等式得证。

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

  同理 $(ab)(b^{-1}a^{-1}) = e$，

  故$b^{-1}a^{-1}$是ab的逆元. 根据逆元的唯一性等式得证。

群的性质：方程存在唯一解

- 定理7.8　G为群，$\forall a,b\in G$，方程$ax=b$和$ya=b$在G中有解且仅有惟一解.

- 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. 下面证明惟一性.

假设c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 $ya=b$的惟一解.

- 例7.15　设群$\boldsymbol{G}=<\boldsymbol{P}(\{\boldsymbol{a},\boldsymbol{b}\}),\oplus>$，其中$\oplus$为对称差. 解下列群方程：$\{\boldsymbol{a}\}\oplus\boldsymbol{X}=\emptyset$，$\boldsymbol{Y}\oplus\{\boldsymbol{a},\boldsymbol{b}\}=\{\boldsymbol{b}\}$

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

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

群的性质：消去律

- 定理7.9 **G为群，则G中适合消去律，即对任意$a,b,c \in G$有**

$$(1)\ 若\ ab = ac，则\ b = c.$$

$$(2)\ 若\ ba = ca，则\ b = c.$$

证明略 。

- 例7.16 设$G = \{a_1, a_2, \ldots, a_n\}$是$n$阶群，令

$$a_iG = \{a_i a_j \mid j = 1, 2, \ldots, n\}$$

证明$a_iG = G$.

- 证明： 由群中运算的封闭性有$a_iG \subseteq G$. 假设$a_iG \subset G$，即$|a_iG| < n$.

必有$a_j, a_k \in G$使得

$$a_i a_j = a_i a_k \ (j \neq k)$$

由消去律得$a_j = a_k$, 与$|G| = n$矛盾.

群的性质：元素的阶

- 定义7.9 设G是群，a∈G，使得等式 a^k=e 成立的最小正整数k称为a的阶，记作$|a|=k$，称 a 为 k 阶元。 若不存在这样的正整数 k，则称 a 为无限阶元。

例如，在$<Z_6,\oplus>$中，

2和4是3阶元，

3是2阶元，

1和5是6阶元，

0是1阶元.

在$<Z,+>$中，0是1阶元，其它整数的阶都不存在.

群的性质：元素的阶

- **定理7.10** 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)$|a^{-1}| = |a|$，（3）$|ab| = |ba|$，$a, b \in G$

- 证明：(1) 充分性. 由于$r|k$，必存在整数m使得$k = mr$，所以有

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

必要性. 根据除法，存在整数 m 和 i 使得

$$k = mr + i, 0 \le i \le r-1$$

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

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

(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，所以 $r \mid t$。从而证了$r = t$，即$|a^{-1}| = |a|$

群的性质：元素的阶

(3) 设 $|ab| = r$，$|ba| = t$，则有

$$(ab)^{t+1} = \underbrace{(ab)(ab)\ldots(ab)}_{t+1\text{个}}$$
$$= a\underbrace{(ba)(ba)\ldots(ba)}_{t\text{个}}b$$
$$= a(ba)^t b = aeb = ab$$

由消去律得 $(ab)^t = e$，从而可知，$r \mid t$.

同理可证 $t \mid r$. 因此 $|ab| = |ba|$。

群的性质：群的阶

- 定义7.10 若群*G*是有穷集，则称*G*是有限群，否则称为无限群。群*G*的基数称为群*G*的阶。只含有单位元的群称为平凡群。
- 例7.18 $<Z,+>$是无穷群，$<S,\ \odot>$，其中$S=\{a，b，c\}$，$\odot$的运算表如下表可以验证，$<S,\ \odot>$是群，a为幺元，*b*和*c*互为逆元；又因为$|G|=3$，故$<S,\ \odot>$是3阶群。

⊙	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

群的性质：Abel群

- 定义7.11 给定群*G*，若⊙是可交换的，则称*G*是可交换群或*G*是**Abel群**。

- 例7.19 具有一般意义下的加法运算的所有整数的集合Z是一个Abel群，如果$a \in Z$，那么a的逆是它的负数$-a$。

- 例7.20 $< Z$，$+>$和$< R$，$+>$是无限群，$<Z_n$，$\oplus>$是有限群也是*n*阶群。klein四元群是四阶群。<{0}, +>是平凡群。上述的所有群都是交换群，但是*n*阶（*n*≥2）实可逆矩阵的集合关于矩阵乘法构成的群是非交换群，因为矩阵乘法不满足交换律。

群的性质：Abel群

- **定理7.11** 给定群$\langle \boldsymbol{G}, \otimes\rangle$，则
  $\langle \boldsymbol{G}, \otimes\rangle$为**Abel**群
  $$\Leftrightarrow (\forall a)(\forall b)(a, b \in G \rightarrow (a \otimes b)^2 = a^2 \otimes b^2)$$
- **证明：** 充分性：
  因为$\langle \boldsymbol{G}, \otimes\rangle$是群，由对任意$a, b \in G$,有
  $$(a\otimes b)^2 = a^2 \otimes b^2$$
  $$\Longrightarrow (a\otimes b)\otimes(a\otimes b) = (a\otimes a)\otimes(b\otimes b)$$
  $$\Longrightarrow a\otimes(b\otimes a)\otimes b = a\otimes(a\otimes b)\otimes b$$
  $$\Longrightarrow (b\otimes a)\otimes b = (a\otimes b)\otimes \mathrm{b}$$
  $$\Longrightarrow b \otimes a = a \otimes \mathrm{b}$$
  可见，$\otimes$是交换的，故$\langle \boldsymbol{G}, \otimes\rangle$是Abel群。

必要性：

$\langle \boldsymbol{G}, \otimes \rangle$是Abel群，故$\langle \boldsymbol{G}, \otimes \rangle$是群；又有，对任意的$a, b \in G$，均有

$$
\begin{aligned}
(a \otimes b)^2 &= (a \otimes b) \otimes (a \otimes b) \\
&= a \otimes (b \otimes a) \otimes b \\
&= a \otimes (a \otimes b) \otimes b \\
&= (a \otimes a) \otimes (b \otimes b) \\
&= a^2 \otimes b^2
\end{aligned}
$$

综上所述，定理得证。

7.3 子 群

- 定义7.12 设G是群，H是G的非空子集，

(1) 如果H关于G中的运算构成群，则称H是G的子群, 记作 $H \le G$.

(2) 若H是G的子群，且$H \subset G$，则称H是G的真子群，记作 $H < G$.

- 如果G是一个群，H是G的一个子群，那么H也是关于G中运算的一个群，因为G中的结合性质在H中也成立。

例如 nZ (n是自然数) 是整数加群<Z,+> 的子群. 当$n \ne 1$时, nZ是Z的真子群.

对任何群G都存在子群. G和$\{e\}$都是G的子群，称为G的平凡子群.

7.3.1 子 群

- 例7.21 $\langle \boldsymbol{V},\oplus\rangle$ 是群$\langle \boldsymbol{U},\oplus\rangle$的子群

$\Longrightarrow \boldsymbol{e_V}=\boldsymbol{e_U}$，其中$\boldsymbol{e_V}$，$\boldsymbol{e_U}$分别是两个群的幺元，即群与其子群具有相同的幺元。

- 证明：因为$\langle \mathrm{V},\oplus\rangle$是群$\langle U,\oplus\rangle$的子群，则对任意$a\in V\subseteq U$，有

$$a\oplus e_V=a=a\oplus e_U$$

根据群的可约律，得$\mathrm{e}_V=e_U$。

7.3.2 子群的判定

- 定理7.12（判定定理一）

设G为群，H是G的非空子集，则H是G的子群当且仅当

(1) $\forall \boldsymbol{a},\boldsymbol{b} \in \boldsymbol{H}$，有$\boldsymbol{ab} \in \boldsymbol{H}$;

(2) $\forall \boldsymbol{a} \in \boldsymbol{H}$,有$\boldsymbol{a}^{-1} \in \boldsymbol{H}$。

- 证明：必要性是显然的。 为证明充分性，只需证明$e \in H$。

因为H非空，存在$a \in H$。由条件(2) 知$a^{-1} \in H$，根据条件(1) $aa^{-1} \in H$，即$e \in H$。

- 本定理表明$\langle \boldsymbol{H}, \odot \rangle$是$\langle \boldsymbol{G}, \odot \rangle$的子群的充要条件是H对于$\odot$封闭及H中每个元素存在逆元。

7.3.2 子群的判定

- 定理7.13（判定定理二）

设G为群，H是G的非空子集，则H是G的子群当且仅当

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

- 证明：必要性显然. 只证充分性.

因为H非空，必存在$a \in H$.

根据给定条件得$aa^{-1} \in H$，即$e \in H$.

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

任取a，$b \in H$，知$b^{-1} \in H$. 再利用给定条件得$a(b^{-1})^{-1} \in H$，即$ab \in H$.

综合上述，可知H是G的子群.

7.3.2 子群的判定

- 定理7.14（判定定理三）

设G为群，H是G的非空有穷子集，则H是G的子群当且仅当

$$\forall \boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{H}，有\boldsymbol{ab} \in \boldsymbol{H}。$$

- 证明：必要性显然. 为证充分性，只需证明$a \in H$有$a^{-1} \in H$.

任取$a \in H$，若$a = e$,则$a^{-1} = e \in H$.

若$a \neq e$,令$S = \{a, a^2, \cdots\}$，则$S \subseteq H$.

由于H是有穷集，必有$a^i = a^j (i < j)$.

根据G中的消去律得$a^{j-i} = e$,由$a \neq e$可知$j - i > 1$，由此得

$$a^{j-i-1}a = e和aa^{j-i-1} = e$$

从而证明了$a^{-1} = a^{j-i-1} \in H$.

7.3.2 子群的判定

- 例7.22 设G是群，H，K是G的子群，证明$H \cap K$也是G的子群。

- 证明：由$e \in H \cap K$可知$H \cap K$非空。

任取a，$b \in H \cap K$，则$a \in H$，$a \in K$，$b \in H$，$b \in K$。

由于H和K是G的子群，必有$ab^{-1} \in H$和$ab^{-1} \in K$，因此

$$ab^{-1} \in H \cap K。$$

根据判定定理二（定理7.13）命题得证。

7.3.3 子群的性质：生成子群

- 定义7.14 设G为群，$a \in G$，令$H = \{a^k | k \in Z\}$，则H是G的子群，称为由 a 生成的子群，记作$< a >$.

- 证明：首先由$a \in \langle a \rangle$知道$\langle a \rangle \neq \emptyset$. 任取$a^m, a^i \in \langle a \rangle$，则

$$a^m \left(a^i\right)^{-1} = a^m a^{-i} = a^{m-i} \in \langle a \rangle$$

根据判定定理二可知$\langle a \rangle \leq G$.

例如整数加群，由2生成的子群$\langle 2 \rangle = \left\{2^k \middle| k \in Z\right\} = 2Z$;

$\langle Z_6, \oplus \rangle$中，由2 生成的子群$\langle 2 \rangle = \{0, 2, 4\}$

Klein四元群$G = \{e, a, b, c\}$的所有生成子群是：

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

7.3.3 子群的性质：中心C

- 定义7.15 设**G**为群,令$\boldsymbol{C} = \{\boldsymbol{a} | \boldsymbol{a} \in \boldsymbol{G} \wedge \forall \boldsymbol{x} \in \boldsymbol{G}(\boldsymbol{ax} = \boldsymbol{xa})\}$,

则**C**是**G**的子群，称为**G**的中心.

- 证明：$e \in C$. C是G的非空子集．任取$a, b \in C$，只需证明ab^{-1}与G中所有的元素都可交换. $\forall x \in G$，有

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

由判定定理二可知$C \leq G$.

对于阿贝尔群G，因为G中所有的元素互相都可交换，G的中心就等于G，但是对某些非交换群G，他的中心是{e}.

7.3.3 子群的性质：子群的交

- 例7.23 设G是群，H,K是G的子群. 证明

(1) $H \cap K$也是G的子群

(2) $H \cup K$是G的子群当且仅当 $H \subseteq K$ 或 $K \subseteq H$

- 证明：(1)由 $e \in H \cap K$ 知 $H \cap K$ 非空.

任取$a, b \in H \cap K$，则$a \in H, a \in K, b \in H, b \in K$.

必有$ab^{-1} \in H$ 和 $ab^{-1} \in K$，从而$ab^{-1} \in H \cap K$. 因此$H \cap K \leq G$.

(2) 充分性显然，只证必要性. 用反证法.

假设 H不是K的子集 且K不是H的子集，那么存在h和k使得

$h \in H \wedge h \notin K$，$k \in K \wedge k \notin H$

推出 $hk \notin H$. 否则由$h^{-1} \in H$ 得 $k = h^{-1}(hk) \in H$，与假设矛盾.

同理可证 $hk \notin K$. 从而得到 $hk \notin H \cup K$. 与$H \cup K$是子群矛盾.

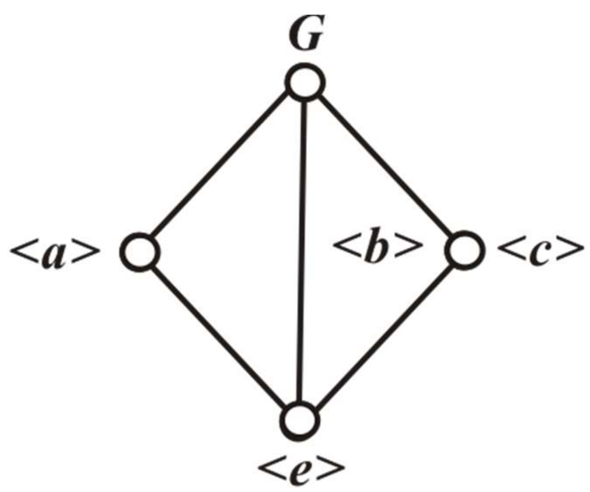
7.3.3 子群的性质：子群的格

- 定义7.16 设G为群，令

$$L(G)=\{H|H\text{是}G\text{的子群}\}$$

则偏序集$\langle L(G),\subseteq\rangle$称为G的子群格

实例：Klein四元群的子群格如下：



总结

- 群的定义与性质
- 子群
- 子群判定定理
- 子群的性质

作业

- **P174:** 7-10