第十七章 群

定义

群$<G,\circ,e,^{-1}>$
$\circ$封闭性,结合律
单位元$e\in G$
$\forall x\in G,\ x^{-1}\in G$

性质

幂运算规则
方程唯一解
消去律
运算表的置换
元素阶的性质

实例

有限群
Abel群
Klein四元群
循环群
置换群

特殊的群

结构

群的分解

共轭类分解

陪集分解

群的分类方程

拉格朗日定理

有限群计数

子代数

子群
判定定理
重要子群

正规子群

商代数

商群
G/H

同余关系
同态映射

积代数

群的直积

17.1 群的定义与性质

- 群的定义
  - 定义与实例
  - 等价定义
  - 相关术语
- 群的性质
  - 幂运算规则
  - 群方程有唯一解
  - 消去律
  - 运算表的置换性质
  - 元素的阶的性质

群的定义

可以将群看成代数系统 $< G, \circ, ^{-1}, e >$

定理1 (等价定义) $<G,\circ>$, $\circ$可结合，若存在右单位元 e，且每个元素 a 相对于e 存在右逆元 a'，则 G 是群

证明　证 e 为左单位元．$\forall a\in G$,

$$e\, e = e \qquad (e \text{ 为右单位元})$$
$$\Rightarrow e\,(a\,a') = a\,a' \Rightarrow (e\,a)\,a' = a\,a'$$
$$\Rightarrow e\,a = a \qquad (\text{右乘 } a' \text{的右逆元})$$

证 a'为 a 的左逆元，即 $a = (a')' = a''$

$$a'' = e\,a'' = (a\,a')\,a'' = a\,(a'a'') = a\,e = a$$

群的有关术语

平凡群 只含单位元的群 $\{e\}$

交换群 Abel群

有限群 与 **无限群**

群 G 的阶 G 的基数，通常有限群记为 $|G|$

元素 a 的 n 次幂

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

元素 a 的阶 $|a|$：使得 $a^k = e$ 成立的最小正整数 k

说明：有限群的元素都是有限阶，为群的阶的因子；

反之，元素都是有限阶的群不一定是有限群.

群的性质 1

定理 2 幂运算规则

1. $(a^{-1})^{-1} = a$
2. $(a\,b)^{-1} = b^{-1}a^{-1}$
3. $a^n\,a^m = a^{n+m}$
4. $(a^n)^m = a^{nm}$
5. 若G为Abel群，则$(a\,b)^n = a^n\,b^n$

说明：

等式 1 和 2 证明用到逆元定义和唯一性

等式 3 和 4 的证明使用归纳法并加以讨论

等式 2 可以推广到有限个元素之积，即

$$(a_1a_2 \ldots a_n)^{-1} = a_n^{-1} \ldots a_2^{-1}a_1^{-1}$$

群的性质 2

定理3 方程 $ax=b$ 和 $ya=b$ 在群 G 中有解且有唯一解.

证　$a^{-1}b$ 是 $ax=b$ 的解.
假设 c 为解，则

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

定理4 (逆命题) 设G是半群，如果对任意 $a,b\in G$，方程 $ax=b$ 和 $ya=b$ 在 G 中有解，则 G 为群.

证　找右单位元和任意元素的右逆元.
　　任取 $b\in G$, 方程 $bx=b$ 的解记为 e.
$\forall a\in G$, $yb=a$ 的解记为 c, 即 $cb=a$.

$$ae=(cb)e=c(be)=cb=a$$

e 为右单位元.
$\forall a\in G$, 方程 $ax=e$ 有解，得到 a 相对于e的右逆元.

群的性质 3

定理5 消去律 $ab = ac \Rightarrow b = c,\ ba = ca \Rightarrow b = a$

定理6 设 G 是有限半群，且不含零元. 若 G 中成立消去律，则 G 是群.

证 设 $G = \{ a_1, a_2, \ldots , a_n \}$，任取 $a_i \in G$,

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

由封闭性, $a_i G \subseteq G$, 假设 $|a_i G| < n$, 则存在 j, k 使得 $a_i a_j = a_i a_k$,
根据消去律，$a_j = a_k$, 矛盾. 所以 $a_i G = G$.
任取a_i, a_j,

$$a_i, a_j \in G \Rightarrow a_j \in a_i G \Rightarrow \text{方程 } a_i x = a_j \text{有解.}$$

同理，方程 $y a_i = a_j$有解. G 是群.

注：$< Z_5, \otimes >$不是群，因为有 0；$<Z^+, \cdot>$ 也不是群，无限.

群的性质 4

定理7 有限群 G 的运算表中每行、每列都是 G 的置换.

$$aG = G \text{ 和 } Ga = G$$

说明:

运算表的行列构成置换的不一定是群

反例: 缺少单位元

	0	1	2
0	1	2	0
1	0	1	2
2	2	0	1

思考:

1. 3元集上的不同的二元运算有多少个?
2. 3元集上二元运算表有多少个能够使得每行每列能够构成置换?
4. 3元集上有多少个不同的运算表代表群?
5. 3元集上同构的群有多少个?

群的性质 5

定理8 G为群，$a \in G$, 且 $|a| = r$, 则

(1) $a^k = e \Leftrightarrow r \mid k$

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

(3) 若 $|G| = n$, 则 $r \le n$.

证 (1) 充分性. $a^k = a^{rl} = (a^r)^l = e^l = e$

必要性. $k = rl + i$, $l \in Z$, $i \in \{0, 1, \ldots, r-1\}$

$$\Rightarrow e = a^k = a^{rl+i} = a^i \Rightarrow i = 0 \Rightarrow r \mid k$$

(2) $(a^{-1})^r = e \Rightarrow |a^{-1}|$ 存在, 令 $|a^{-1}| = t$, 则 $t \mid r$. 同理 $r \mid t$.

(3) 假设 $r > n$, 令 $G' = \{e, a, a^2, \ldots, a^{r-1}\}$，则$G'$中元素两两不同，否则与 $|a| = r$ 矛盾. 从而 $|G'| > n$，与 $G' \subseteq G$ 矛盾.

17.2 子群

- 子群定义
- 子群判别定理
- 重要子群的实例
  - 生成子群
  - 中心
  - 正规化子
  - 共轭子群
  - 子群的交
- 子群格

子群定义

定义 设G为群, H是G的非空子集，若H关于G中运算构成群，则称H为G的子群，记作$H \le G$.

如果子群H是G的真子集，则称为真子群，记作$H < G$.

说明：

1. 子群H就是G的子代数.

2. 若H的单位元为e', 且x在H中相对e'的逆元为x', 则

$$x\, e' = x = x\, e \Rightarrow e' = e$$

$$x\, x' = e' = e = x\, x^{-1} \Rightarrow x' = x^{-1}$$

子群判定定理一

定理1 G 是群，H 是 G 的非空子集，则

$$H \le G \Leftrightarrow \forall a, b \in H,\ ab \in H,\ b^{-1} \in H$$

证：只证充分性.

H 非空，存在 a 属于H,

由条件2，a^{-1}属于H,

由条件1，有$a\,a^{-1}$属于H, 即 e 属于H

子群判定定理二和三

定理2 G 是群，H 是G 的非空子集，则

$$H \le G \Leftrightarrow \forall a, b \in H, a\, b^{-1} \in H$$

证 充分性. $H \ne \varnothing \Rightarrow \exists b \in H$

$$b \in H \Rightarrow b\, b^{-1} \in H \Rightarrow e \in H$$

$\forall a,$ $\quad a \in H \Rightarrow e\, a^{-1} \in H \Rightarrow a^{-1} \in H$

$\forall a,b,$ $\quad a, b \in H \Rightarrow a, b^{-1} \in H$

$$\Rightarrow a(b^{-1})^{-1} \in H \Rightarrow a\, b \in H$$

定理3 G 是群，H 是 G 的有限非空子集，则

$$H \le G \Leftrightarrow \forall a, b \in H,\ a\, b \in H$$

证明见教科书.

重要子群的实例

1. a生成子群 $<a> = \{ a^k \mid k \in Z \}$， $a \in G$
2. B生成子群 $<B> = \cap\{ H \mid H \le G, B \subseteq H \}, B \subseteq G$

$$<B> = \{ b_1^{e_1} b_2^{e_2} \ldots b_n^{e_n} \mid b_i \in B, e_i = \pm 1, i = 1,2,\ldots,n, n \in Z^+ \}$$

3. 中心 $C = \{ a \mid a \in G, \forall x \in G\,(a x = x a) \}$
4. a 的正规化子 $N(a) = \{ x \mid x \in G, x a = a x \}$， $a \in G$
5. H 的正规化子 $N(H) = \{ x \mid x \in G, x H x^{-1} = H \}, H \le G$
6. 共轭子群 $x H x^{-1} = \{ x h x^{-1} \mid h \in H \}$

   其中 $H \le G$, $x \in G$
7. 子群的交

   $H, K \le G$, 则

   (1) $H \cap K \le G$

   (2) $H \cup K \le G \Leftrightarrow H \subseteq K \vee K \subseteq H$

关于子群的证明

3. 证明中心 C 为子群

证 由于e 属于C, C 非空.

任取 $x, y\in C$，对于任意 $a\in G$有

$$(x\,y^{-1})\,a = x\,(y^{-1}\,a) = x\,(a^{-1}\,y)^{-1} = x\,(y\,a^{-1})^{-1}$$

$$= x\,(a\,y^{-1}) = (x\,a)\,y^{-1} = (a\,x)\,y^{-1} = a\,(x\,y^{-1})$$

因此 $x\,y^{-1}$ 属于 C. 由判定定理 2，命题得证.

子群的证明（续）

7. 设 $H, K \le G$, 则

(1) $H \cap K \le G$

(2) $H \cup K \le G \Leftrightarrow H \subseteq K \vee K \subseteq H$

证 (1) 略.

(2) 只证必要性

假若 $\exists h\,(h \in H, h \notin K), \exists k\,(k \in K, k \notin H)$,

则 $hk \notin H$, 否则 $k = h^{-1}(hk) \in H$, 矛盾.

同理 $hk \notin K$, 从而 $hk \notin H \cup K$

但是 $h, k \in H \cup K$, 与 $H \cup K \le G$矛盾.

AB 构成子群的条件

命题 设$A, B \le G$，定义 $AB = \{ ab \mid a \in A, b \in B \}$, 则

(1) $AB \le G \Leftrightarrow AB = BA$.

(2) $AB \le G \Rightarrow AB = \langle A \cup B \rangle$

证 (1) 略.

(2) $A \subseteq AB, B \subseteq AB \Rightarrow A \cup B \subseteq AB \Rightarrow \langle A \cup B \rangle \subseteq AB$

$\forall ab,\ ab \in AB \Rightarrow a \in A, b \in B \Rightarrow a, b \in A \cup B$

$\Rightarrow a, b \in \langle A \cup B \rangle \Rightarrow ab \in \langle A \cup B \rangle$

例 Klein四元群 $G = \{ e, a, b, c \}$,

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

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

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

子群格

G为群，$S=\{ H \mid H \leq G \}$,
偏序集 $< S, \subseteq >$ 构成格，称为G的子群格

Klein四元群，Z_{12}的子群格.