第六章　群论

主要内容

- 半群与单位半群
- 群的基本概念
- 变换群
- 有限群
- 循环群
- 子群及陪集分解
- 正规子群与同态

6.1 半群与单位半群

- 半群、子半群的定义
- 循环半群的定义
- 单元半群的定义和基本性质

半群、子半群的定义

定义6.1 设$V=\langle S, \circ \rangle$是代数系统，$\circ$为二元运算，如果$\circ$运算满足结合律，则称$V$为**半群**. 如果半群的$\circ$运算还满足交换律, 则称其为**可换半群**.

定理6.1 设$V=\langle S,\circ \rangle$是半群，如果$V$有子代数$\langle M,\circ \rangle$，则此子代数也是半群.

定义6.2 半群$\langle S, \circ \rangle$的子代数亦是半群, 称为半群$\langle S, \circ \rangle$的**子半群**.

实例

例1

(1) $<Z^+,+>,<N,+>,<Z,+>,<Q,+>,<R,+>$都是半群，+是普通加法.

(2) 设n是大于1的正整数，$<M_n(R),+>$和$<M_n(R),\cdot>$都是半群，其中+和·分别表示矩阵加法和矩阵乘法.

(3) $<P(B),\oplus>$为半群，其中$\oplus$为集合对称差运算.

(4) $<Z_n, \oplus>$为半群，其中$Z_n=\{0,1,\ldots,n-1\}$，$\oplus$为模n加法 .

(5) $<A^A,\circ>$为半群，其中A^A为A上的函数集合，$\circ$为函数的复合运算.

(6) $<R^*,\circ>$为半群，其中R^*为非零实数集合，$\circ$运算定义如下：$\forall x, y\in R^*, x\circ y=y$.

循环半群

对半群 <S,∘>的任一元素a, 可以定义它的幂:

(1) $a^1=a$;

(2) $a^2=a\circ a$;

(3) $a^{j+1}=a^j\circ a$.

由结合律成立, 若m, n为正整数, 则

(1) $a^n\circ a^m = a^m\circ a^n = a^{n+m}$

(2) $(a^n)^m = a^{n\times m}$

如果$a^2=a$, 则称a为幂等元素.

定义6.3 如果半群<S, ∘ >的每个元素均为S内的某个固定元素a的幂, 则此半群称为由a生成的循环半群, a叫做此循环半群的生成元素.

循环半群的性质

例2 代数系统<Z⁺,+>中, Z⁺是正整数集, 此代数系统是一个循环半群, 它的生成元素是1.

定理6.2 循环半群一定是可换半群.

证明： 设循环半群 $<S,\circ>$的生成元素为a, 则它的任意两个元素$b = a^m$, $c = a^n$, 且有:

$$b \circ c = a^m \circ a^n = a^{n+m} = a^n \circ a^m = c \circ b$$

定理6.3 半群内任一元素和它所有的幂组成一个由该元素生成的循环子半群.

证明： 显然.

单元半群

定义6.4 设$V=<S,\circ>$是半群，若$e\in S$是关于$\circ$运算的单位元，则称V是**单元半群(含幺半群, 独异点)**，有时也将单元半群V记作$V=<S,\circ,e>$.

例3 整数集Z上的模m相等关系R给出Z的一个划分，等价类为[0], [1], [2], … ,[m-1], 它的商集Z / R可记为Z_m, 即 $Z_m=\{[0], [1], [2], \ldots ,[m-1]\}$

在Z_m上分别定义二元运算$\oplus$,$\otimes$, 对$[i], [j] \in Z_m$有

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

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

此时, $<Z_m, \oplus>$和$<Z_m, \otimes>$都是单元半群, 单位元分别为: [0]和[1].

单元半群的性质

单元半群是半群的扩充, 比半群有更多的性质.

定理6.4 一个有可列个元素的单元半群的运算表, 每行(列)均不相等.

证明: 由于单位元的存在, 造成运算表中每行第一个元素及每列第一个元素均不相同.

$\circ$	1	a	b	c	d	…
1	1	a	b	c	d	…
a	a					
b	b					
c	c					
d	d					
…	…					

Note: 一个单元半群也可以有子单元半群和循环单元半群.

单元半群的性质

定理6.5 如果单元半群$<M,\circ>$存在一个子系统$<M',\circ>$，且其单位元$e\in M'$，则$<M',\circ>$也是一个单元半群.

证明：显然.

定义6.5 称以上$<M',\circ>$为$<M,\circ>$的子单元半群.

定义6.6 如果一个单元半群由它的一个元素a所生成（令$a^0 = e$，故单位元也可由a生成），则称其为由a所生成的循环单元半群，把a称为此单元半群的生成元素.

定理6.6 循环单元半群是可换单元半群.

证明：与定理6.2证明类似.

单元半群的性质

定理6.7 可换单元半群的所有幂等元素构成一个子单元半群.

证明: 设$<M,\circ>$是一个可换单元半群, 它的幂等元素组成的集合为M'.

思路: (1)证M'是一个代数系统; (2)证M'是M的子半群; (3)证M的单位元也是M'的单位元

(1)设$a, b\in M'$, 且它们是幂等元素, 所以有$a\circ a = a$, $b\circ b = b$, 又"$\circ$"满足结合律和交换律, 则

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

由此可知$a\circ b$亦是幂等元素, 所以$a \circ b\in M'$, "$\circ$"对M'封闭, $<M',\circ>$是一个代数系统.

(2) $M'\subseteq M$, 所以$<M',\circ>$是$<M,\circ>$的一个子系统, 是子半群.

(3)由于$e\circ e =e$, 所以单位元亦为幂等元素, $e\in M'$.

6.2 群

- 群的基本概念和性质
- 变换群
- 对称群, 置换群
- 循环群
- 子群及陪集分解
- 正规子群与同态

6.2.1 群的定义及其性质

定义6.7 设$V=<S,\circ>$是单元半群，$e\in S$是关于$\circ$运算的单位元，若$\forall a\in S$，$a^{-1}\in S$，则称V是**群**. 通常将群记作G.

实例：

$<\mathbf{Z},+>$和$<\mathbf{R},+>$是群，$<\mathbf{Z}_n,\oplus>$是群.

n阶$(n\geq 2)$实可逆矩阵集合关于矩阵乘法构成群.

群的定义

定义6.8 (1) 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**，有限群G的阶记作$|G|$.

(2) 只含单位元的群称为**平凡群**.

(3) 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 (Abel) 群**.

实例：

$\langle Z,+\rangle$和$\langle R,+\rangle$是无限群，$\langle Z_n,\oplus\rangle$是有限群，也是$n$阶群. $\langle\{0\},+\rangle$是平凡群.

上述群都是交换群，n阶$(n\geq 2)$实可逆矩阵集合关于矩阵乘法构成的群是非交换群.

群的性质

性质1：群满足消去律 G为群，则G中满足消去律，即对任意 $a,b,c\in G$ 有

(1) 若 $a\circ b = a\circ c$，则 $b = c$.

(2) 若 $b\circ a = c\circ a$，则 $b = c$.

证明略

例4 设$G = \{a_1, a_2, \ldots , a_n\}$是$n$阶群，令

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

证明 $a_iG = G$.

证 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

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

由消去律得 $a_j = a_k$, 与 $|G| = n$矛盾.

群的性质

性质2：方程存在惟一解 G为群，$\forall a,b\in G$，方程$a\circ x=b$和$y\circ a=b$在G中有解且仅有惟一解.

证： $a^{-1}\circ b$ 代入方程左边的x 得

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

所以$a^{-1}\circ b$ 是该方程的解.

下面证明惟一性. 假设c是方程$a\circ x=b$的解，必有$a\circ c=b$，从而有

$$c = e\circ c = (a^{-1}\circ a)\circ c = a^{-1}\circ(a\circ c) = a^{-1}\circ b$$

同理可证$b\circ a^{-1}$是方程 $y\circ a=b$的惟一解.

例5 设群$G=\langle P(\{a,b\}),\oplus\rangle$，其中$\oplus$为对称差. 解下列群方程：

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

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

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

群的性质

性质3：一个阶大于1的群一定没有零元

证 因为零元不存在逆元，故得证.

性质4：除了单位元外，一个群一定没有幂等元素

证 若存在幂等元，即$a∘a=a$, 则必有

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

即幂等元只能是单位元.

群的第二种定义

性质5：如果一个代数系统满足结合律和性质(2), 则它是群

证 (1)找单位元 因为$a \circ x=b$, 设对某一个a, 满足方程$a \circ x=a$的x为e_r, 对$\forall b$有$y \circ a=b$的解c. 此时

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

同理可得e_l, 对$\forall b$有 $e_l \circ b = b$, 由于$e_l = e_r = e$, 得到单位元

(2) 找逆元 由$y \circ a=e$, 可得a的唯一左逆元，由$a \circ x=e$,可得a的唯一右逆元, 由于左右逆元相等, 因此可得到逆元.

得证.

定义6.9 一个代数系统G若满足下列条件, 则称为群

(1) 满足结合律;

(2) $\forall a,b \in G$，方程$a \circ x=b$和$y \circ a=b$在G中有解且仅有惟一解.

群的同态和同构

定义6.10 设$<G,\circ>$和$<H,*>$是两个群，若存在一个函数$f:G\to H$使得$\forall a,b\in G$，有 $f(a\circ b) = f(a)*f(b)$，则称f是从$<G,\circ>$到$<H,*>$的群同态；如果f是双射函数，则称为群同构.

定理6.8 对群同态f有

$$f(e_G) = e_H$$

$$f(a^{-1}) = [f(a)]^{-1}$$

其中e_G 和 e_H分别为$<G,\circ>$和$<H,*>$的单位元.

证 用同态性质(定理5.5, 5.6)易证.

定理6.9 如果群G与代数系统$<H,*>$满同态或同构，则$<H,*>$也是群.

证 用满同态和同构性质易证.

6.2.2 变换群

复习: 集合S上的变换是双射函数f: $S \to S$

假设S上的所有变换的集合为S', 则变换的二元运算(复合运算) "$\circ$"构成了一个代数系统$< S', \circ>$, 此代数系统为群.

原因:

(1) 复合运算可结合;

(2) "$\circ$"存在单位元, 即恒等变换 $f(x)=x$, $x \in S$

(3) $<S', \circ>$中的每个变换必存在逆元素, 即逆变换

所以, $<S', \circ>$是群, 若$S'' \subset S'$且$<S'', \circ >$也构成群，有:

定义6.11 集合S上的若干个变换与复合运算若构成一个群, 称为变换群.

变换群的性质

定理6.10 任一群均与一个变换群同构.

证 设<G, $*$>是一个群, 从G中取一元素a, 则存在一个变换

$$f_a: x \to x*a\ ,\ x \in G$$

这样, G中每个元素均有一个变换与之对应, 这些变换f_a, f_b, f_c,… 构成一个变换的集合G'. 下面证明: 存在一个双射函数g: $G \to G'$ 使得:

$$g(a*b) = g(a) \circ g(b)$$

(1) 令函数g为: $g(a) = f_a$, 因此G'中每个元素 f_a,均有G中元素a与之对应, 故g为满射. 如果$a \neq b$, 则由消去律可知

$$x*a \neq x*b\ ,\ x \in G$$

故有$f_a \neq f_b$, 因此 g: $G \to G'$是一个双射函数.

变换群的性质

(2) 由于

$$g(a*b) = f_{a*b}$$

$$g(a) \circ g(b) = f_a \circ f_b$$

而 $f_{a*b}(x) = x*a*b = (x*a)*b = f_b(f_a(x)) = f_a \circ f_b(x)$

所以有

$$g(a*b) = g(a) \circ g(b)$$

因此, <G, $*$>与<G', $\circ$>同构. 由定理6.9可知<G', $\circ$>也是一个群, 且它是一个变换群.

Note: 对群的研究可以归结为对变换群的研究;
任一抽象群均可在变换群中找到它的一个实例.

6.2.3 对称群与置换群

定义6.12 设 $S = \{1, 2, \ldots, n\}$, S上的任何双射函数 $\sigma: S \to S$ 称为S上的**n元置换**.

例如 $S=\{1, 2, 3, 4, 5\}$, 下述为5元置换

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

定义6.13 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与τ 的**乘积**, 记作$\sigma \tau$.

例如

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

定义

定理6.11 所有的 n元置换构成的集合S_n关于置换乘积构成群， 称为n元对称群. n元对称群的子群称为n元置换群.

因为:

(1) “置换乘积”运算封闭;

(2) 单位元是恒等置换;

(3) 每个n元置换均有逆元.

Note:

对称群是变换群的特例（对称群是有限群）.

置换群是有限群的典型代表.

对称群的性质

定理6.12 若有限集S的阶为n, 则S的对称群$<S_n,\circ>$的阶为$n!$.

证 由排列组合理论 易证.

定理6.13 对于代数系统$<G,\circ>$, 若G有限且满足结合律和消去律, 则该代数系统是一个群.（有限群的另一种定义）

证 用群的第二个定义证明.

即只要证明$a\circ x=b$和$y\circ a=b$在G中有惟一解.

设G有n个元素$G=\{a_1, a_2, \ldots, a_n\}$, 作集合$G'=\{a\circ a_1, a\circ a_2, \ldots, a\circ a_n\}$, 则$G'\subseteq G$, 根据消去律, 当$i\neq j$时, $a\circ a_i\neq a\circ a_j$

所以G'也有n个不同的元素, 故$G'=G$.

这样, 对G中的元素b必有一a_k, 使得$b=a\circ a_k$, 而且a_k惟一.

同理, 可证$y\circ a=b$有惟一解. 得证.

群的运算表（群表）

有限群的运算表称为群表. 群表对研究有限群的性质很有用。设有限群$\langle G,\circ\rangle$, 其中$G=\{1,2,3\}$, 其群表为:

∘	1	2	3
1	1	2	3
2	2	3	1
3	3	1	2

可看出群表的一些性质:

(1) 第一行, 第一列与群元素相同, 且顺序相同;

(2) 每一行(列)内元素各不相同, 且任意两行(列)对应元素亦均不相同;

原因: 每行(列)具有$a\circ a_1$, $a\circ a_2$, …, $a\circ a_n$的形式, 由定理6.13或例4的证明可知, 成立.

群表的性质

(3) 如果一个群是可换群, 其可换性与群表的对称性一致.

由群表可知, 以上有限群<G,∘>是可换的.

Note:

(1) 一个有限代数系统是否构成群, 是否可换从群表可以看出来;

(2) 有限群<G,∘>中的每个元素对应G的一个置换. 即对G= {a_1, a_2, …, a_n}, 存在一个函数φ :

$$\varphi(a_i)=\begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_i\circ a_1 & a_i\circ a_2 & \cdots & a_i\circ a_n \end{pmatrix}=p_{ki}\quad (i=1,2,\ldots,n)$$

由这些置换组成一个集合P = {p_{k1}, p_{k2}, …, p_{kn}}. 由于置换是变换的特例, 由定理6.10可知, 这些置换与其置换乘积构成群, 且与其对应的有限群同构.

群表的性质

定理6.14 每个有限群均与一个置换群同构.

Note:

(1) 研究有限群的问题可以归结为研究置换群问题;

(2) 阶为1的群是仅由单位元构成的群;

(3) 阶为2的群的群表唯一（对应置换群唯一），且为可换群;

(4) 阶为3的群的群表唯一（对应置换群唯一），且为可换群;

(5) 阶≥ 4的群的群表不唯一，对应置换群不再唯一。

6.2.4 循环群

定义6.14 设G是群，$a\in G$，$n\in Z$，则a 的 n次幂.

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

群中元素可以定义负整数次幂.

在<Z_3,⊕ >中有

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

在<Z,+>中有

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

元素的阶

定义6.15 设G是群，$a\in G$，使得等式 $a^k=e$ 成立的**最小正整数**k 称为a 的阶(或**周期**)，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$_6$,⊕>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.

幂运算规则

定理6.15 设G为群，则G中的幂运算满足：

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

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

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

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

(5) 若G为交换群，则 $(a \circ b)^n = a^n \circ b^n$.

证 (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) $$(b^{-1} \circ a^{-1}) \circ (a \circ b) = b^{-1} \circ (a^{-1} \circ a) \circ b = b^{-1} \circ b = e,$$

同理 $$(a \circ b) \circ (b^{-1} \circ a^{-1}) = e,$$

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

元素的阶

定理6.16 $<G,\circ>$为群，$a\in G$且 $|a| = r$. 设k是整数，则

(1) $a^k = e$当且仅当 $r \mid k$ （ r 整除 k ） 因此 r 又称为a的周期

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

证 (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 $e = a^k = a^{mr+i} = (a^r)^m\circ a^i = e\circ a^i = a^i$

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

a的逆元的阶是a的阶的因子

(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 $r \mid t$. 从而证明了$r = t$，即$|a^{-1}| = |a|$