

离散数学

西安交通大学
计算机学院



离散数学

§ 4.群

- 群的基本概念
- 群的性质
- 群中元素的阶
- 循环群
- 子群



离散数学

§ 4.群

定义1.群 (group)

设 $(G, *)$ 是含幺半群。若 G 中每个元素都有逆元，即 $\forall g(g \in G \Rightarrow g^{-1} \in G)$ ，则称 $(G, *)$ 为群。

注：•群就是每个元素都有逆元的含幺半群；

•验证一个代数系统是群，必须验证以下四点：

- (1) 封闭性
- (2) 结合律
- (3) 有幺元
- (4) 有逆元

离散数学

例1. (I, \times) , $(M_{n \times n}, \times)$, (N_m, \times_m) , $(2^X, \cap)$, $(P[x], \times)$

上一节中的五个例子

(I, \times) , $(M_{n \times n}, \times)$, (N_m, \times_m) , $(2^X, \cap)$, $(P[x], \times)$ 已经验证都是含么半群;

但它们都不是群, 原因就在于不能保证每个元素都有逆元。

离散数学

例2. $(\mathbb{I}, +)$ 是一个群

这里： \mathbb{I} 是整数集合， $+$ 是整数加法， 由算术知识知：

(1)封闭性： 两个整数之和仍为整数， 且结果唯一。 即

$$\forall a, b, a \in \mathbb{I} \wedge b \in \mathbb{I} \Rightarrow a + b \in \mathbb{I} ;$$

(2)结合律： 整数加法满足结合律。 即

$$\forall a, b, c \in \mathbb{I}, (a + b) + c = a + (b + c) ;$$

(3)有么元： 取 $0 \in \mathbb{I}, \forall a \in \mathbb{I},$ 有 $a + 0 = 0 + a = a$ 。

由么元的定义知， 0 是关于 $+$ 的么元；

(4)有逆元： $\forall a \in \mathbb{I},$ 取 $-a \in \mathbb{I},$ 有 $a + (-a) = (-a) + a = 0$ 。

由逆元的定义知 \mathbb{I} 中每个元素都有逆元；

由群的定义知 $(\mathbb{I}, +)$ 是群。

离散数学

例3. $(M_{n \times n}, +)$ 是一个群

这里: $M_{n \times n}$ 是 $n \times n$ 实矩阵的全体, $+$ 是矩阵加法。由线性代数知:

(1) 封闭性: 两个 $n \times n$ 实矩阵相加仍为 $n \times n$ 实矩阵, 且结果唯一。即

$$\forall A, B, A \in M_{n \times n} \wedge B \in M_{n \times n} \Rightarrow A + B \in M_{n \times n};$$

(2) 结合律: 实矩阵加法满足结合律。即

$$\forall A, B, C \in I, (A + B) + C = A + (B + C);$$

(3) 有幺元: 取零矩阵 $0 \in M_{n \times n}, \forall A \in M_{n \times n}$, 有
 $A + 0 = 0 + A = A$ 。由幺元的定义知 0 是关于 $+$ 的幺元;

(4) 有逆元: $\forall A \in M_{n \times n}$, 取 $-A \in M_{n \times n}$, 有
 $A + (-A) = (-A) + A = 0$ 。

由逆元的定义知 $M_{n \times n}$ 中每个元素都有逆元;
由群的定义知 $(M_{n \times n}, +)$ 是群。

离散数学

例4. $(N_m, +_m)$ 是一个群

这里: $N_m = \{[0]_m, [1]_m, \dots, [m-1]_m\}$, $+_m$ 定义如下

$$\forall [i]_m, [j]_m \in N_m, [i]_m +_m [j]_m = [(i+j) \bmod m]_m$$

(1) 封闭性: 由于 $0 \leq (i+j) \bmod m < m$, 且结果唯一。即

$$\forall [i]_m, [j]_m, [i]_m \in N_m \wedge [j]_m \in N_m \Rightarrow [i]_m +_m [j]_m \in N_m;$$

(2) 结合律: 由于 $\forall [i]_m, [j]_m, [k]_m \in N_m$, 有

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

故有 $([i]_m +_m [j]_m) +_m [k]_m = [i]_m +_m ([j]_m +_m [k]_m)$
即 $+_m$ 满足结合律;

离散数学

(3)有幺元：取 $[0]_m \in N_m$, $\forall [i]_m \in N_m$, 有

$$[0]_m +_m [i]_m = [(0+i) \bmod m]_m = [i]_m$$

$$[i]_m +_m [0]_m = [(i+0) \bmod m]_m = [i]_m$$

由幺元的定义知 $[0]_m$ 是关于 $+_m$ 的幺元；

(4)有逆元： $\forall [i]_m \in N_m$, 取 $[m-i]_m \in N_m$, 有

$$[i]_m +_m [m-i]_m = [(i+(m-i)) \bmod m]_m = [0]_m$$

$$[m-i]_m +_m [i]_m = [((m-i)+i) \bmod m]_m = [0]_m$$

由逆元的定义知 N_m 中每个元素都有逆元；

由群的定义知 $(N_m, +_m)$ 是群。

离散数学

例5. $(2^X, \oplus)$ 是一个群

这里： X 是一非空集合， 2^X 是 X 的幂集， \oplus 是集合的环和运算， 即 $A \oplus B = (A \cap B') \cup (B \cap A')$ 。 由集合一章知：

- (1) 封闭性： 环和是 2^X 上的二元运算， 具有封闭性；
 - (2) 结合律： 环和运算满足结合律；
 - (3) 有么元： 关于环和运算的么元是 \emptyset ；
 - (4) 有逆元： $\forall A \in 2^X$ ， A 的逆元是其本身；
- 由群的定义知 $(2^X, \oplus)$ 是群。

离散数学

定理6 .环和运算基本定理

设 X 是全集， A, B, C 是 X 的三个子集。则

$$(1) A \oplus B = (A \cup B) \setminus (A \cap B) = (A \cup B) \cap (A' \cup B') ;$$

$$(2) A \oplus \emptyset = A \quad (\text{空集是环和的幺元}) ;$$

$$A \oplus X = A' ;$$

$$(3) A \oplus A = \emptyset \quad (\text{自己是自己 (环和) 的逆元}) ;$$

$$A \oplus A' = X ;$$

$$(4) A' \oplus B' = A \oplus B ;$$

$$(5) (A \oplus B)' = A' \oplus B = A \oplus B' ;$$

$$(6) \text{交换律: } A \oplus B = B \oplus A ;$$

$$(7) \text{结合律: } A \oplus (B \oplus C) = (A \oplus B) \oplus C ;$$

$$(8) \text{分配律: } A \cap (B \oplus C) = (A \cap B) \oplus (A \cap C) \text{ (交对环和的);}$$

$$(9) \text{消去律: } A \oplus B = A \oplus C \Rightarrow B = C .$$

离散数学

例6. $(P[x], +)$ 是一个群

这里: $P[x]$ 是实系数多项式的全体, $+$ 是多项式的加法。

(1) 封闭性: 由于两个多项式之和仍为多项式, 且结果唯一。

(2) 结合律: 由于实数加法满足结合律, 故多项式的加法满足结合律。

(3) 有么元: 取 $0 \in P[x]$, $\forall p(x) \in P[x]$, 有
$$0 + p(x) = p(x) + 0 = p(x)$$

由么元的定义知 0 是关于 $+$ 的么元;

(4) 有逆元: $\forall p(x) \in P[x]$, 取 $-p(x) \in P[x]$, 有
$$p(x) + (-p(x)) = (-p(x)) + p(x) = 0$$

由逆元的定义知 $P[x]$ 中每个元素都有逆元。

由群的定义知, $(P[x], +)$ 是群。

离散数学

定义2.交换群(Abel群 加群)

设 $(G,*)$ 是群。若 $*$ 运算满足交换律，则称 $(G,*)$ 是交换群。

例7.前面的例2，例3，例4，例5，例6都是交换群。

定义3.群的阶(rank)

设 $(G,*)$ 是群。称 G 的势(基数)为群 $(G,*)$ 的阶。

注：•群的阶反映群的大小；

•由定义3知有限群的阶就是 G 中元素的个数；无限群的阶是 G 的势；群的阶统一记为 $|G|$ 。

离散数学

定理1. 设 $(G, *)$ 是群, $|G| \geq 2$ 。则

- (1) G 中每个元素的逆元是唯一的;
- (2) G 中无零元。

[证]. (1) 由于群有结合律, 所以由书169页定理6.2可知, 逆元唯一;

(2) 采用反证法: 若零元 $0 \in G$, 则对任何元素 $g \in G$, 都有

$$0 * g = g * 0 = 0 \quad (1)$$

由于 G 是群, 每个元都有逆元。设 0 的逆元为 g_0 , 则有

$$0 * g_0 = g_0 * 0 = 0 \quad (2)$$

由逆元定义知 0 无逆元, 与群中每个元素都有逆元矛盾。
所以 G 中无零元。

离散数学

定理2. 设 $(G,*)$ 是群。则 $\forall a,b \in G$, 有

(1)反身律: $(a^{-1})^{-1}=a$;

(2)鞋袜律: $(a*b)^{-1}=b^{-1}*a^{-1}$ 。

[证]. (1) $\forall a \in G$, $(a^{-1})^{-1}=(a^{-1})^{-1}*e$

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

$$=((a^{-1})^{-1}*a^{-1})*a \quad (\text{结合律})$$

$$=e*a$$

$$=a ;$$

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

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

$$=(a*b)^{-1}*(a*b*b^{-1}*a^{-1}) \quad (\text{结合律})$$

$$=((a*b)^{-1}*(a*b))*(b^{-1}*a^{-1}) \quad (\text{结合律})$$

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

$$=b^{-1}*a^{-1}。$$

离散数学

定理3 设 $(G,*)$ 是群，则 $*$ 运算满足消去律。即 $\forall x,y,z \in G$,

$$x * y = x * z \Rightarrow y = z ;$$

$$y * x = z * x \Rightarrow y = z .$$

[证]. 只证第一式。 $\forall x,y,z \in G$,

$$y = e * y$$

$$= (x^{-1} * x) * y$$

$$= x^{-1} * (x * y) \quad (\text{结合律})$$

$$= x^{-1} * (x * z) \quad (\text{条件: } x * y = x * z)$$

$$= (x^{-1} * x) * z \quad (\text{结合律})$$

$$= e * z$$

$$= z$$

离散数学

定理4. 在有限群 $(G, *)$ (设 $|G|=n$) 的 $*$ 运算的运算表中, 每一行(每一列)都与 G 中元素的自然顺序构成一个置换(双射)。

也就是说, 每个元素在每行(每列)必出现一次且只出现一次。

注: • 因此 n 阶有限群的运算表是由 G 中元素的 (n 个行或 n 个列所形成的) n 个置换所构成的。这个性质来源于群中每个元素都有逆元。

离散数学

例8. (G, o) 是一有限群

这里: $G = \{e, a, b, c\}$, o 运算的运算表如右:

(1) 封闭性: 由表1可得;

(2) 结合律: 留待后证;

(3) 有么元: e ;

(4) 有逆元: $e^{-1}=e, a^{-1}=a, b^{-1}=b, c^{-1}=c$ 。

例如其第三行就与表头元素构成一置换 P_3 。

此群一般称为 Klein 4-群, 又称为几何群或运动群。

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

表1

注: •Klein 日耳曼民族, 几何学家, 我国著名几何学家苏步青是他的晚年弟子;

离散数学

- $$P_3 = \begin{pmatrix} e & a & b & c \\ \circ & & & \\ b & c & e & a \end{pmatrix}$$

[证]. 只证关于第 $i(1 \leq i \leq n)$ 行结论成立。我们设

$$G = \{a_1 (=e), a_2, \dots, a_n\}$$

构造自然映射 $f_i: G \rightarrow G$ 使得

$$\text{对任何的 } a \in G, \quad f_i(a) = a_i * a$$

为此, 只须证明 f_i 是一双射函数即可。

①后者唯一:

$$\forall a_j, a_k \in G, \quad a_j = a_k$$

$$\Rightarrow a_i * a_j = a_i * a_k$$

$$\Rightarrow f_i(a_j) = f_i(a_k);$$

离散数学

②单射:

$$\forall a_j, a_k \in G, f_i(a_j) = f_i(a_k)$$

$$\Rightarrow a_i * a_j = a_i * a_k$$

$$\Rightarrow a_j = a_k \quad (\text{消去律});$$

③满射:

$\forall a_j \in G$, 根据群有逆元及运算封闭性知,

$\exists a_k = a_i^{-1} * a_j \in G$, 使得

$$f_i(a_k) = a_i * a_k$$

$$= a_i * (a_i^{-1} * a_j)$$

$$= (a_i * a_i^{-1}) * a_j \quad (\text{结合律})$$

$$= e * a_j$$

$$= a_j \quad \circ$$

离散数学

定义4. 元素的乘幂

设 $(G, *)$ 是群。G 中元素乘幂的定义在半群定义的基础上，增补如下： $\forall x \in G$,

$$x^0 = e ;$$

$$x^{-n} = (x^{-1})^n \quad (\forall n \in \mathbb{N}) .$$

注：• 从而，我们就将半群中元素的乘幂是在自然数 \mathbb{N} 范围内进行扩展到群中元素的乘幂是在整数 \mathbb{I} 范围内进行。

• 同样可以由归纳法证明，当指数为整数时，指数定律在群中成立。即任取 $x \in G$ ， $\forall m, n \in \mathbb{I}$ ，有

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

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

• 证明时，固定整数 m ，对正整数 n 使用归纳法，当 n 是负整数时，就变成 x^{-1} 的正整数指数运算。

离散数学

例9. 在 $(I, +)$ 群中, 取 $1 \in I$, 有

$$1^0 = 0, 1^n = n; \quad 1^{-1} = -1, 1^{-n} = -n; \quad 1^n + 1^{-n} = n - n = 0.$$

例10. 设 X 是由方程 $x^4 = 1$ 的4个根组成的集合, 即

$$X = \{1, -1, i, -i\}$$

其中 $i = \sqrt{-1}$ 。设 \times 是复数乘法,
其运算表如表2。

由表2容易验证 $(X, *)$ 是群。

由表2可知:

$$1^1 = 1, 1^2 = 1, 1^3 = 1, 1^4 = 1, \dots;$$

$$(-1)^1 = -1, (-1)^2 = 1, (-1)^3 = -1, (-1)^4 = 1, (-1)^5 = -1, \dots;$$

$$(i)^1 = i, (i)^2 = -1, (i)^3 = -i, (i)^4 = 1, (i)^5 = i, \dots;$$

$$(-i)^1 = -i, (-i)^2 = -1, (-i)^3 = i, (-i)^4 = 1, (-i)^5 = -i, \dots。$$

\times	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

表2

离散数学

注：•从上例各元素乘幂的结果看，都有一个现象，就是4次乘幂的结果是1，为群的么元；而这正好说明它们都是四次方程 $x^4=1$ 的根；

•群的元素乘幂回归么元是群的元素一个比较普遍的现象；这点被总结成下面的定义。它在寻找群的子群，元素的求逆，元素性质的探讨等方面都有着广泛的作用。

定义5.元素的阶 (rank)

设 $(G,*)$ 是群。 $\forall g \in G$ ，我们称

$$k = \min \{m : m \in \mathbb{N} \setminus \{0\} \wedge g^m = e\}$$

为元素 g 的阶；

若这样的 k 不存在，则称 g 的阶为无穷。

离散数学

- 注：
- 从定义可知，元素 g 的阶 k 是使 $g^m = e$ 成立的最小正整数；
 - 由于元素的自乘幂是一次一次乘的，因此这个无穷只能是可数无穷；
 - 由定义5可知，幺元是群中唯一的一个一阶元素；
 - 这里要强调的是，我们现在有群的阶和群中元素的阶这样两个阶的概念，这是两个根本不同的概念。群的阶是指群中元素的个数，而群中元素的阶是指使 $g^m = e$ 成立的最小正整数 k ；一个是对整体而言，一个是对整体中的个体而言。

例11.在例8的Klein 4-群 (G, o) 中，幺元 e 的阶为1；其它元素 a, b, c 的阶均为2；

在例9的群 $(I, +)$ 中，幺元 0 的阶为1；其他元素的阶均为无穷；

在例10的群 $(X, *)$ 中，幺元 1 的阶为1； -1 的阶为2； i 和 $-i$ 的阶均为4。

离散数学

定理5. 设 $(G,*)$ 是群。 $\forall g \in G$,

(1)若 g 的阶为 n , 则 $g^1, g^2, \dots, g^n (=e)$ 互不相同;

(2)若 g 的阶为无穷, 则 $g^0 (=e), g^1, g^2, \dots, g^n, \dots$ 互不相同。

[证].采用反证法

(1)否则, 设有 $g^i = g^j$ ($1 \leq i < j \leq n$), 于是有

$$\begin{aligned} g^{j-i} &= g^{j+(-i)} \\ &= g^j * g^{-i} && (\text{指数律}) \\ &= g^i * g^{-i} && (\text{反证假设: } g^i = g^j) \\ &= e \end{aligned}$$

即有 $1 \leq j-i < n$, 使 $g^{j-i} = e$ 。这与 g 的阶为 n , 具有最小性, 矛盾。故有 g^1, g^2, \dots, g^n 互不相同。

(2)同理可证。

离散数学

例12.在例10的群 $(X,*)$ 中,元素 i 的阶为4, 所以有 i^1, i^2, i^3, i^4 互不相同; $-i$ 的阶也为4, 所以 $(-i)^1, (-i)^2, (-i)^3, (-i)^4$ 也互不相同。

定理6. 设 $(G,*)$ 是群。 $\forall g \in G$, g 与 g^{-1} 有相同的阶。

[证].分两种情况来证:

(1)设 g 的阶有限, 为 n 。从而 $g^n=e$ 。由于

$$\begin{aligned}(g^{-1})^n &= (g^n)^{-1} && \text{(指数律)} \\ &= e^{-1} && (g^n=e) \\ &= e\end{aligned}$$

这说明 g^{-1} 的阶也是有限的, 故可设其阶为 m , 于是有 $(g^{-1})^m=e$ 。从而由阶定义的最小性知 $m \leq n$;

其次, 又由于

$$\begin{aligned}g^m &= ((g^{-1})^m)^{-1} && \text{(指数律)} \\ &= e^{-1} && ((g^{-1})^m=e) \\ &= e\end{aligned}$$

离散数学

从而由阶定义的最小性知 $n \leq m$;

于是(由 \leq 的反对称性)有 $n=m$, 即 g 和 g^{-1} 的阶相同。

(2) 设 g 的阶无穷, 则 g^{-1} 的阶也必是无穷的。否则, 设 g^{-1} 的阶是有限的, 为 m , 从而 $(g^{-1})^m = e$ 。

$$\begin{aligned} \text{于是 } g^m &= ((g^{-1})^m)^{-1} && \text{(指数律)} \\ &= e^{-1} && ((g^{-1})^m = e) \\ &= e \end{aligned}$$

这说明 g 的阶也是有限的, 故与 g 的阶为无穷矛盾。因此当 g 的阶是无穷时, g^{-1} 的阶也是无穷的。

由(1)和(2)知, g 和 g^{-1} 有相同的阶。

例13.在例10的群 $(X, *)$ 中, 元素 i 和 $-i$ 互为逆元, i 和 $-i$ 的阶均为4, 相同。

离散数学

定理7. 设 $(G,*)$ 是群。 $\forall g \in G$

(1)若 g 的阶有限, 设其为 k , 从而 $g^k=e$ 。则

$$(1.1) \forall m \in \mathbb{N}, g^m = e \Leftrightarrow k \mid m ;$$

$$(1.2) \forall m, n \in \mathbb{N}, g^m = g^n \Leftrightarrow k \mid m-n ;$$

(2)若 g 的阶无限, 则

$$\forall m, n \in \mathbb{N}, g^m = g^n \Rightarrow m=n .$$

[证].(1)

(1.1)先证 \Rightarrow):

若 $g^m=e$, 则必有 $k \mid m$ 。

否则 $k \nmid m$, 于是, 由带余除法,

可设 $m=kq+r$ ($0 < r < k$), 故可得 $r=m-kq$, 从而

离散数学

$$\begin{aligned} g^r &= g^{m-kq} \\ &= g^{m+(-kq)} \\ &= g^m * (g^k)^{-q} && (\text{指数律}) \\ &= e * (e)^{-q} && (g^m=e, g^k=e) \\ &= e * e \\ &= e \quad \text{故与} g \text{的阶为} k, \text{具有最小性, 矛盾} \end{aligned}$$

次证 \Leftarrow):

若 $k \mid m$, 则 $m=kq$ 。于是

$$\begin{aligned} g^m &= g^{kq} \\ &= (g^k)^q && (\text{指数律}) \\ &= e^q && (g^k=e) \\ &= e \end{aligned}$$

离散数学

(1.2)

$$\begin{aligned} g^m &= g^n \\ \Leftrightarrow g^m * g^{-n} &= g^n * g^{-n} \\ \Leftrightarrow g^{m+(-n)} &= g^{n+(-n)} && (\text{指数律}) \\ \Leftrightarrow g^{m-n} &= e && (g^0=e) \\ \Leftrightarrow k \mid m-n &&& (\text{根据(1.1)}) \end{aligned}$$

(2) 若 g 的阶无限, 则

$$\begin{aligned} g^m &= g^n \\ \Rightarrow g^m * g^{-n} &= g^n * g^{-n} \\ \Rightarrow g^{m+(-n)} &= g^{n+(-n)} && (\text{指数律}) \\ \Rightarrow g^{m-n} &= e && (g^0=e) \\ \Rightarrow m-n &= 0 && (g \text{ 的阶无限, 只有 } g^0=e) \\ \Rightarrow m &= n \end{aligned}$$

离散数学

例14.在例10的群 $(X,*)$ 中,

元素-1的阶是2,所以

$$(-1)^2=1, (-1)^4=1, (-1)^6=1, \dots, (-1)^{2n}=1, \dots;$$

元素i的阶是4,所以

$$(i)^4=1, (i)^8=1, (i)^{12}=1, \dots, (i)^{4n}=1, \dots;$$

元素-i的阶是4,所以

$$(-i)^4=1, (-i)^8=1, (-i)^{12}=1, \dots, (-i)^{4n}=1, \dots。$$

离散数学

定理8.有限群中每个元素的阶都是有限的。设 $(G,*)$ 是有限群， $|G|=n$ ，则 G 中每个元素的阶 $\leq n$ 。

[证].对任一元素 $g \in G$ ，设其阶为 m ，则由定理5知 g^1, g^2, \dots, g^m 这 m 个元素互不相同；

由群的封闭性知它们同时都在 G 中；因此有 $m \leq n$ 。

所以群 G 中每个元素的阶 $\leq n$ 。

例15.在例8的Klein 4-群 (G, o) 中，么元 e 的阶为1，其他元素 a, b, c 的阶均为2，均小于群的阶4；

在例10的群 $(X,*)$ 中，么元1的阶为1， -1 的阶为2， i 和 $-i$ 的阶均为4，均小于等于群的阶4。

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

离散数学

定义6.循环群(cyclic group)

设 $(G,*)$ 是群。若存在着元素 $g_0 \in G$, 使得

$$(\forall g \in G)(\exists n \in \mathbb{I})(g = g_0^n)$$

则称 $(G,*)$ 为循环群; 同时称 g_0 是该循环群的生成元 (generating element)。并且将 $(G,*)$ 记作 (g_0) 。

例16.群 $(\mathbb{I},+)$ 是循环群

在群 $(\mathbb{I},+)$ 中取 $1 \in \mathbb{I}$, 由于 $0 = 1^0, n = 1^n, -n = (-1)^n = (1^{-1})^n = 1^{-n}$, 故 \mathbb{I} 中的每个元素都可表示成1的整数次幂。由循环群的定义知 $(\mathbb{I},+)$ 是循环群, 1是该循环群的生成元。

例17.群 $(N_m, +_m)$ 是循环群

在群 $(N_m, +_m)$ 中, 取 $[1]_m \in N_m$, 由于 $[0]_m = ([1]_m)^0, [i]_m = ([1]_m)^i$, 故 N_m 中的每个元素都可表示成 $[1]_m$ 的整数次幂。由循环群的定义知 $(N_m, +_m)$ 是循环群, $[1]_m$ 是该循环群的生成元。

离散数学

定理9. 设 $(G,*)$ 是循环群, $|G|=n$ 。那么

(1) g_0 是生成元 $\Leftrightarrow g_0^{-1}$ 是生成元;

(2) g_0 是生成元 $\Leftrightarrow g_0$ 的阶是 n 。

[证]. (1) g_0 是生成元

$$\Leftrightarrow (\forall g \in G)(\exists k \in I)(g = g_0^k)$$

$$\Leftrightarrow (\forall g \in G)(\exists k \in I)(g = (g_0^{-1})^{-k}) \quad (\text{指数律})$$

$$\Leftrightarrow (\forall g \in G)(\exists m \in I)(g = (g_0^{-1})^m) \quad (\text{这里: } m = -k)$$

$$\Leftrightarrow g_0^{-1} \text{是生成元};$$

(2) 由于 $|G|=n$, 所以 $(G,*)$ 是有限群, 根据定理8可知 $g_0 \in G$ 的阶有限, 不妨设其为 m , 并且 $m \leq n$ 。

先证 \Rightarrow): 构造集合

$$S = \{e, g_0, g_0^2, \dots, g_0^{m-1}\}$$

根据定理5可知 $|S|=m$, 并且由群的封闭性知 $S \subseteq G$ 。

离散数学

又对任何 $g \in G$ ，由于 g_0 是生成元，故存在着整数 k ，使得 $g = g_0^k$ 。而 g_0 的阶是 m ，则有 $g_0^m = e$ ；根据带余除法，有 $k = qm + r$ ($0 \leq r < m$)

$$\begin{aligned} \text{从而 } g &= g_0^k \\ &= g_0^{qm+r} \\ &= (g_0^m)^q * g_0^r && (\text{指数律}) \\ &= e^q * g_0^r && (\text{因: } g_0^m = e) \\ &= e * g_0^r && (\text{因: } e^q = e) \\ &= g_0^r \\ &\in S && (\text{因: } 0 \leq r < m) \end{aligned}$$

故 $G \subseteq S$;

从而 $S = G$ ，于是 $m = |S| = |G| = n$

即 g_0 的阶是 n 。

离散数学

次证 \Leftarrow): 若 g_0 的阶是 n , 则构造集合

$$S = \{e, g_0, g_0^2, \dots, g_0^{n-1}\}$$

根据定理5可知 $|S|=n$, 并且由群的封闭性知 $S \subseteq G$, 因此由 $|G|=n$ 可知有 $S = G$ 。

从而, 显然, g_0 是生成元。

离散数学

定理10. 设 $(G,*)$ 是循环群, g_0 是生成元。

(1)若 g_0 的阶为 m , 则 $(G,*)$ 与 $(N_m, +_m)$ 同构;

(2)若 g_0 的阶为无穷, 则 $(G,*)$ 与 $(I,+)$ 同构。

[证]. (1)由条件知

$$G = \{e, g_0, g_0^2, \dots, g_0^{m-1}\}$$

$$N_m = \{[0]_m, [1]_m, [2]_m, \dots, [m-1]_m\}$$

定义自然映射 $h: G \rightarrow N_m$, $h(g_0^k) = [k]_m$ 。由双射函数的定义知 h 是双射函数。

$$\begin{aligned} \text{由于 } h(g_0^i * g_0^j) &= h(g_0^{(i+j) \bmod m}) \\ &= [(i+j) \bmod m]_m \\ &= [i]_m +_m [j]_m \\ &= h(g_0^i) +_m h(g_0^j) \end{aligned}$$

离散数学

故 h 满足同态公式。

由同构的定义知 h 是从 $(G, *)$ 到 $(N_m, +_m)$ 的同构函数，即 $(G, *)$ 和 $(N_m, +_m)$ 同构。

(2) 由于 g_0 的阶为无穷，故根据定理5的(2)有

$$e(= g_0^0), g_0, g_0^2, \dots, g_0^n, \dots \quad \textcircled{1}$$

互不相同。

由于根据定理6， g_0 和 g_0^{-1} 有相同的阶，故与上同理可得

$$g_0^{-1}, g_0^{-2}, \dots, g_0^{-n}, \dots \quad \textcircled{2}$$

互不相同。

离散数学

另外①与②中任何一对元素 g_0^i 和 g_0^j 互不相同。否则有 $i \geq 0, j > 0$ (故有 $i+j > 0$), 使得 $g_0^i = g_0^j$, 于是

$$g_0^{i+j} = e$$

这说明 g_0 的阶有限, 与 g_0 的阶为无穷矛盾。

于是有

$$G = \{ \dots, g_0^{-n}, \dots, g_0^{-2}, g_0^{-1}, e, g_0, g_0^2, \dots, g_0^n, \dots \}$$

定义自然映射 $h: G \rightarrow I, \quad h(g_0^k) = k$ 。

由于 $\forall k \in I$ 有原象 $g_0^k \in G$, 使 $h(g_0^k) = k$ 。故 h 是满射的。

由于若 $h(g_0^i) = h(g_0^j)$, 即 $i=j$, 则有 $g_0^i = g_0^j$, 即 h 是单射的。

于是, 由双射函数的定义可知 h 是双射函数。

离散数学

$$\begin{aligned}\text{由于有 } h(g_0^i * g_0^j) &= h(g_0^{i+j}) \\ &= i+j \\ &= h(g_0^i) + h(g_0^j)\end{aligned}$$

故满足同态公式。

由同构的定义知 h 是从 $(G,*)$ 到 $(I,+)$ 的同构函数，即 $(G,*)$ 和 $(I,+)$ 同构。

定理11. 循环群一定是交换群。

[证]. 设 $(G,*)$ 是循环群，生成元是 $g_0 \in G$ 。于是，

对任何元素 $x, y \in G$, 存在着整数 $m, n \in I$ ，使得 $x = g_0^m$, $y = g_0^n$, 从而

$$\begin{aligned}x * y &= g_0^m * g_0^n \\ &= g_0^n * g_0^m \\ &= y * x\end{aligned}$$

故 $*$ 运算满足交换律；即 $(G,*)$ 是交换群。

定义7.置换群(permutation group)

设 X 是非空有限集合, $|X|=n$ 。 A 是 X 上的置换构成的集合, \diamond 是置换的合成。若 $\langle A, \diamond \rangle$ 是群, 则称 $\langle A, \diamond \rangle$ 是置换群或 n 次置换群。

例18.设在三维空间有一矩形方框如图1所示。四个顶点分别标记为1,2,3,4。用这些标记来表示矩形方框的运动。

令 e:不动 (在平面内
绕原点旋转 360°) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$

a:绕横轴旋转 180°
(上下翻转) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$

b:绕纵轴旋转 180°
(左右翻转) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

c:在平面内绕原
点旋转 180° $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

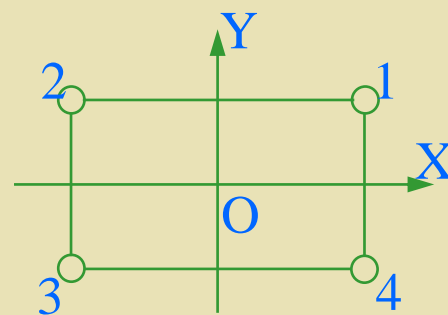



图1



这样就将方框的运动用置换的方式表示出来了。

令 $A=\{e,a,b,c\}$ ， \diamond 为置换的合成运算。

下面用置换的合成来定义旋转的复合运动。


$a \diamond b$ 意味着先旋转 a 再旋转 b 。于是得到 A 上的置换合成表如下：

例如

$$\begin{aligned} a \diamond b &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = c \end{aligned}$$

\diamond	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

表3



由表3知，这正是 在前面例8所讲的Klein 4-群。
由于置换的合成运算 \diamond 就是关系的合成运算 \circ ，故 \diamond 运算满足结合律。

由于Klein 4-群 $\langle A, \diamond \rangle$ 是由几何形刚体在空间的运动所产生的，这正是 把它称为几何群、运动群的原因。

另外由表3明显得知，这个置换群还是一个交换群。

注：•在例18中可以看到刚体在空间的运动可以由4次置换来描述；但并不是任何4次置换都表示刚体在空间中的运动。如在例18中，置换

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

就不代表任何刚体运动。

•由于4个元素的置换应有 $4! = 24$ 个，而在例18中只取了其中的4个置换，没有取完，所以 $A \subset S_4$ 。



定理12. n 个元素的非空集合 X 上的所有 n 次置换构成的集合 S_n , 在置换的合成运算 \diamond 下构成一置换群 $\langle S_n, \diamond \rangle$ 。称为 n 次对称群(group of symmetry), 简记为 S_n 。

[证].

(1)封闭性: 因为任意两个 n 次置换 P_i, P_j 的合成 $P_i \diamond P_j$ 仍为一个 n 次置换, 且结果唯一, 即

$$\forall P_i, P_j, P_i \in S_n \wedge P_j \in S_n \Rightarrow P_i \diamond P_j \in S_n;$$


(2)结合律: 置换的合成运算 \diamond 满足结合律;

(3)有幺元; 关于 \diamond 运算的幺元是 n 次恒等置换 I , 即

$$\exists I \in S_n, \forall P \in S_n, I \diamond P = P \diamond I = P$$

(4)有逆元; 由于任一 n 次置换 P 的逆置换 P^{-1} 仍是一 n 次置换, 即 $P^{-1} \in S_n$, 故 S_n 中任一元素 P 都有逆元 P^{-1} , 即

$$\forall P \in S_n, \exists P^{-1} \in S_n, P \diamond P^{-1} = P^{-1} \diamond P = I。$$



例19. 此例讨论一个由所有置换构成的群。为了简单起见，取 $X=\{1,2,3\}$ ，3个元素的置换有 $3!=6$ 个。

$$S_3 = \{P_1, P_2, P_3, P_4, P_5, P_6\} = \{e, \tau, \sigma^2\tau, \sigma\tau, \sigma, \sigma^2\}$$

用轮换的形式写出来是

$$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1) = e$$

$$P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12)$$

$$P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13)$$

$$P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23)$$


$$P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$$

$$P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$$

其运算表如下：

◇	P ₁	P ₂	P ₃	P ₄	P ₅	P ₆
P ₁	P ₁	P ₂	P ₃	P ₄	P ₅	P ₆
P ₂	P ₂	P ₁	P ₅	P ₆	P ₃	P ₄
P ₃	P ₃	P ₆	P ₁	P ₅	P ₄	P ₂
P ₄	P ₄	P ₅	P ₆	P ₁	P ₂	P ₃
P ₅	P ₅	P ₄	P ₂	P ₃	P ₆	P ₁
P ₆	P ₆	P ₃	P ₄	P ₂	P ₁	P ₅

表4



由表4知

- (1) \diamond 是 S_3 上的二元运算, 具有封闭性;
- (2) 置换的合成运算 \diamond 满足结合律;
- (3) e 是关于 \diamond 运算的幺元;
- (4) $e, \tau, \sigma^2\tau, \sigma\tau$ 的逆元是其本身; σ, σ^2 互为逆元。

由群的定义可知 $\langle S_3, \diamond \rangle$ 是群, 因而是置换群。称其为三次六阶对称群。由表4易知其不是交换群, 因而它是最小的非交换群。

$\langle S_3, \diamond \rangle$ 实际上可看作是由两个较小的置换群 $\langle H_1, \diamond \rangle$ 和 $\langle H_2, \diamond \rangle$ 的乘积得到的, 这里: $H_1 = \{e, \tau\}$, $H_2 = \{e, \sigma, \sigma^2\}$ 。这就引出了子群及Lagrange定理, 还有群的构造等问题。

定理13.(Cayley定理)

任何 n 阶有限群 $\langle G, * \rangle$ 都与一 n 次置换群同构。

[证]. 设 $|G|=n$, $G=\{a_1(=e), a_2, \dots, a_n\}$ 。则令 $A=\{P_1, P_2, \dots, P_n\}$, 其中:

$$P_i = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ a_1 * a_i & a_2 * a_i & \cdots & a_n * a_i \end{pmatrix} \quad (1 \leq i \leq n)$$

显然 P_1, P_2, \dots, P_n 是 $*$ 运算的运算表中 n 个列置换, 由本节定理4知, 它们是 n 个互不相同的 n 次置换, 即 $|A|=n$ 。
◇ 是置换的合成运算, 则:

(一) $\langle A, \diamond \rangle$ 是一 n 次置换群

(1) 封闭性: 对任何 $P_i, P_j \in A$, 对应着 $a_i, a_j \in G$, 由群 $\langle G, * \rangle$ 的封闭性知, 存在着 $a_k \in G$, 使 $a_i * a_j = a_k$ 。而 a_k 对应着列置换 $P_k \in A$ 。于是对任何 $x \in G$, 都有



$$(P_i \diamond P_j)(x) = P_j(P_i(x)) = (x * a_i) * a_j = x * (a_i * a_j) = x * a_k = P_k(x)$$

所以 $P_i \diamond P_j = P_k \in A$ 。

故合成运算 \diamond 关于置换集合 A 封闭；

(2) 结合律：置换的合成运算 \diamond 满足结合律；

(3) 有么元： $P_1 \in A$ 是关于 \diamond 运算的么元；

因为，对任何 $P_i \in A$ ，都有 对任何 $x \in G$ ，都有


$$(P_1 \diamond P_i)(x) = P_i(P_1(x)) = (x * a_1) * a_i = x * (a_1 * a_i) = x * (e * a_i) = x * a_i = P_i(x)$$

$$(P_i \diamond P_1)(x) = P_1(P_i(x)) = (x * a_i) * a_1 = x * (a_i * a_1) = x * (a_i * e) = x * a_i = P_i(x)$$

所以 $P_1 \diamond P_i = P_i = P_i \diamond P_1$

故 $P_1 \in A$ 是关于 \diamond 运算的么元；

(4) 有逆元：对任何 $P_i \in A$ ，对应着 $a_i \in G$ ，由群 $(G, *)$ 有逆元知，存在着 $a_j \in G$ ，使 $a_i^{-1} = a_j$ 。而 a_j 对应着列置换



$P_j \in A$ 。于是对任何 $x \in G$ ，都有

$$(P_i \diamond P_j)(x) = P_j(P_i(x)) = (x * a_i) * a_j = x * (a_i * a_j) = x * e = x * a_1 = P_1(x)$$

$$(P_j \diamond P_i)(x) = P_i(P_j(x)) = (x * a_j) * a_i = x * (a_j * a_i) = x * e = x * a_1 = P_1(x)$$

所以

$$P_i \diamond P_j = P_1 = P_j \diamond P_i$$

故 $P_i^{-1} = P_j \in A$ 是 P_i 关于 \diamond 运算的逆元；

由群的定义知 $\langle A, \diamond \rangle$ 是群。因此 $\langle A, \diamond \rangle$ 是 n 次置换群。

(二) 群 $\langle G, * \rangle$ 与 n 次置换群 $\langle A, \diamond \rangle$ 同构


定义自然映射 $h: G \rightarrow A$

对任何 $a_i \in G$ ， $h(a_i) = P_i$

(1) h 是双射函数：由定义显然；

(2) h 满足同态公式：

对任何 $a_i, a_j \in G$ ，由群 $\langle G, * \rangle$ 的封闭性知，存在着 $a_k \in G$



使 $a_i * a_j = a_k$ 。于是 对任何 $x \in G$, 都有

$$\begin{aligned} h(a_i * a_j)(x) &= h(a_k)(x) \\ &= P_k(x) \\ &= x * a_k \\ &= x * (a_i * a_j) \\ &= (x * a_i) * a_j \\ &= P_j(P_i(x)) \\ &= (P_i \diamond P_j)(x) \\ &= (h(a_i) \diamond h(a_j))(x) \end{aligned}$$

所以 $h(a_i * a_j) = h(a_i) \diamond h(a_j)$;

因此 $\langle G, * \rangle$ 与 $\langle A, \diamond \rangle$ 同构。

离散数学

定义8.子群(subgroup)

若群 $(G,*)$ 的子代数系统 $(S,*)$ 也是群，则称 $(S,*)$ 是 $(G,*)$ 的子群。

注：•验证子群，除了验证子代数系统的

(1) $S \subseteq G$ ；

(2) $S \neq \emptyset$ ；

(3) $*$ 运算关于 S 封闭；

还应该验证

(4)有幺元(并与群 G 中的幺元重合)；

(5)有逆元(并与群 G 中的同一元的逆元重合)；

而结合律则不须验证，因为根据本章 § 1 定理3可知，遗传。

•群 $(S,*)$ 是群 $(G,*)$ 的子群，我们简记为 $S < G$ ；

•由于群是一种代数系统，因此可以讨论它的子代数系统。子代数系统在群中的反映就是子群的概念。

离散数学

定理14. 设 $(G,*)$ 是群, $S \subseteq G$ 且 $S \neq \emptyset$ 。那么

$(S,*)$ 是 $(G,*)$ 的子群 \Leftrightarrow

$$\left. \begin{array}{l} (1) \text{封闭性: } \forall a \forall b (a \in S \wedge b \in S \Rightarrow a * b \in S) \\ (2) \text{有逆元: } \forall a (a \in S \Rightarrow a^{-1} \in S) \end{array} \right\} (*)$$

[证]. 先证 \Rightarrow):

由于 $(S,*)$ 是 $(G,*)$ 的子群, 故 $(S,*)$ 是群。因而

(1) 有封闭性: $\forall a \forall b (a \in S \wedge b \in S \Rightarrow a * b \in S)$

这就证明了条件 $(*)$ (1);

(2) 有幺元: 暂设其为 e_s ;

(3) 有逆元: 即对任何 $a \in S$, 都存在着 $b \in S$, 使

$$b * a = a * b = e_s ;$$

离散数学

下面我们来证两点：

(a) $e_s = e$ ，即子群 $(S, *)$ 的幺元 e_s 与大群 $(G, *)$ 的幺元 e 重合；从而说明 $e \in S$ 。

(b) $b = a^{-1}$ ，即任一元素 $a \in S$ 在子群 $(S, *)$ 中的逆元 b 与其在大群 $(G, *)$ 中的逆元 a^{-1} 重合；从而说明 $a^{-1} \in S$ ，这就证明了条件(*) (2)。

首先，由于 $e_s, e \in G$ ，因此有

$$e_s * e = e_s \quad (\text{因 } e \text{ 是群 } (G, *) \text{ 的幺元})$$

$$e_s * e_s = e_s \quad (\text{因 } e_s \text{ 是群 } (S, *) \text{ 的幺元})$$

故有 $e_s * e_s = e_s * e$

于是由群 $(G, *)$ 的消去律可得

$$e_s = e ;$$

其次 $b = b * e$

离散数学

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

$$=(b*a)*a^{-1} \quad (\text{结合律})$$

$$=e*a^{-1} \quad (b \text{ 是 } a \text{ 在子群 } (S, *) \text{ 中的逆元且 } e_s = e)$$

$$=a^{-1}$$

次证 \Leftarrow): 只需验证 $(S, *)$ 是群即可

(1)封闭性: 条件(*) (1)保证;

(2)结合律: 遗传;

(3)有幺元: 由于 $S \neq \emptyset$, 故必至少有某一元素 $a_0 \in S$, 于是由条件(*) (2)有 $a_0^{-1} \in S$, 从而由条件(*) (1)有

$$e = a_0 * a_0^{-1} \in S \quad ;$$

(4)有逆元: 条件(*) (2)保证;

故 $(S, *)$ 是群; 所以 $(S, *)$ 是 $(G, *)$ 的子群。

离散数学

定理15. 设 $(G,*)$ 是群, $S \subseteq G$ 且 $S \neq \emptyset$ 。那么

$(S,*)$ 是 $(G,*)$ 的子群 \Leftrightarrow

(混合)封闭性: $\forall a \forall b (a \in S \wedge b \in S \Rightarrow a * b^{-1} \in S)$ (**)

[证]. 我们证明: 定理15条件(**) \Leftrightarrow 定理14条件(*)

先证 \Rightarrow):

(1)有逆元: 由于 $S \neq \emptyset$, 故必至少有某一元素 $a_0 \in S$, 于是重复有 $a_0 \in S$, 从而由条件(**) 有

$$e = a_0 * a_0^{-1} \in S$$

因此, 对任何 $a \in S$, 由于 $e \in S$ 已证, 故由条件(**) 有 $a^{-1} = e * a^{-1} \in S$

这样, 定理14条件(*) (2)得证;

离散数学

(2)封闭性：对任何 $a, b \in S$ ，由已证(1)有逆元有 $b^{-1} \in S$ ，从而由条件(**) 有

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

故定理14条件(*) (1)得证。

次证 \Leftarrow)：对任何 $a, b \in S$ ，根据定理14条件(*) (2)有逆元有 $b^{-1} \in S$ ，在根据定理14条件(*) (1)封闭性有

$$a * b^{-1} \in S$$

故条件(**) (混合)封闭性得证。

离散数学

定理16. 设 $(G,*)$ 是有限群, $|G|=n$, $S\subseteq G$ 且 $S\neq\emptyset$ 。那么

$(S,*)$ 是 $(G,*)$ 的子群 \Leftrightarrow

封闭性: $\forall a\forall b(a\in S\wedge b\in S\Rightarrow a*b\in S)$ (***)

[证]. 先证 \Rightarrow):

由于 $(S,*)$ 是 $(G,*)$ 的子群, 故 $(S,*)$ 是群。因而具有封闭性: $\forall a\forall b(a\in S\wedge b\in S\Rightarrow a*b\in S)$

这就证明了条件(***)。

次证 \Leftarrow):

只需验证 $(S,*)$ 是群即可

(1) 封闭性: 条件(***) 保证;

(2) 结合律: 遗传;

离散数学

(3)有么元：由于 $S \neq \emptyset$ ，故必至少有某一元素 $a_0 \in S$ ，由 $S \subseteq G$ 知 $a_0 \in G$ ；由 $|G|=n$ ，根据定理8知 a_0 的阶有限，设其为 k ， $k \leq n$ ，则有 $a_0^k = e$ ，于是由已证之封闭性有

$$e = a_0^k \in S \quad ;$$

(4)有逆元：对任何 $a \in S$ ，由 $S \subseteq G$ 知 $a \in G$ ；由 $|G|=n$ ，根据定理8知 a 的阶有限，设其为 m ， $m \leq n$ ，则有 $a^m = e$ ；于是由已证之封闭性有 $a^{m-1} \in S$ ，从而有

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

$$a^{m-1} * a = a^m = e \quad ;$$

$$\text{所以} \quad a^{-1} = a^{m-1} \in S \quad ;$$

故 $(S, *)$ 是群；所以 $(S, *)$ 是 $(G, *)$ 的子群。

离散数学

例20.平凡子群

设 $(G, *)$ 是群, 则 $(\{e\}, *)$ 和 $(G, *)$ 是 $(G, *)$ 的两个子群。由于每个群都有这样的子群, 且这两个子群对问题的研究价值不大。故称这两个子群是 $(G, *)$ 的平凡子群。

例21.循环群的子群是循环群。即

若 $(G, *)$ 是循环群且 $(S, *)$ 是 $(G, *)$ 的子群, 则 $(S, *)$ 是循环群。

[证]. 由子群的定义知 $(S, *)$ 是群。下证 $(S, *)$ 是循环群。

设 g_0 是 $(G, *)$ 的生成元, 于是由 $S \subseteq G$ 知 S 中的每个元素都可表示成 g_0^n , $n \in I$ 。设 m 是 S 诸元素中方次最小的正幂。下证 g_0^m 是 S 的生成元。

离散数学

任取 $x \in S$ ，则有 $k \in I$ 使 $x = g_0^k$ 。根据带余除法，有

$$k = qm + r \quad (0 \leq r < m)$$

于是有 $g_0^r = g_0^{k - qm}$

$$= g_0^k * (g_0^m)^{-q} \quad (\text{指数律})$$

由于 $g_0^k = x \in S$ ，并且由 $g_0^m \in S$ 可知， $(g_0^m)^{-q} \in S$ ，故由群 $(S, *)$ 的封闭性可得 $g_0^r \in S$ 。而 m 是 S 中诸元素的最小正幂，故有 $r = 0$ 。即有

$$x = g_0^k = g_0^{qm} = (g_0^m)^q$$

即 g_0^m 是 $(S, *)$ 的生成元。

于是由循环群的定义知 $(S, *)$ 是循环群。

离散数学

例22. 设 $(G,*)$ 是群。令

$$S = \{c:c \in G \wedge (\forall g \in G)(c*g=g*c)\}$$

则 $(S,*)$ 是 $(G,*)$ 的子群。

我们称此子群 $(S,*)$ 是群 $(G,*)$ 的中心。

[证]. (1) $S \subseteq G$: 由 S 的定义显然;

(2) $S \neq \emptyset$: 有么元 $e \in G$, 使得 $(\forall g \in G)(e*g=g*e)$, 故有 $e \in S$;

(3)(混合)封闭性: $\forall a \forall b (a \in S \wedge b \in S \Rightarrow a*b^{-1} \in S)$

对于任何的 $a, b \in S$, 则有 $a, b \in G$, 且对任何 $g \in G$,

$$a*g=g*a, \quad b*g=g*b$$

离散数学

对后一等式左右两边，前后同乘 $b^{-1} \in G$ ，我们得到

$$g * b^{-1} = b^{-1} * g \quad \text{即} \quad b^{-1} * g = g * b^{-1}$$

因此有 $a * b^{-1} \in G$ ，使得 对任何 $g \in G$

$$\begin{aligned}(a * b^{-1}) * g &= a * (b^{-1} * g) && \text{(结合律)} \\ &= a * (g * b^{-1}) && (b^{-1} * g = g * b^{-1}) \\ &= (a * g) * b^{-1} && \text{(结合律)} \\ &= (g * a) * b^{-1} && (a * g = g * a) \\ &= g * (a * b^{-1}) && \text{(结合律)}\end{aligned}$$

因此 $a * b^{-1} \in S$ ；

所以，根据定理15可知， $(S, *)$ 是 $(G, *)$ 的子群。



◆陪集和Lagrange定理

定义9.陪集(coset)

设 $\langle G, * \rangle$ 是群, $\langle H, * \rangle$ 是 $\langle G, * \rangle$ 的子群。对于任何元素 $a \in G$,


(1)由a所确定的H在G中的左陪集(left coset)定义为

$$aH = \{a * h : h \in H\}$$

(2)由a所确定的H在G中的右陪集(right coset)定义为

$$Ha = \{h * a : h \in H\}$$

称元素a是左陪集aH及右陪集Ha的代表元素, 简称代表元。



$X=\{1,2,3\}$ ，3个元素的置换有 $3!=6$ 个。

已知 $\langle S_3, \diamond \rangle$ 是三次六阶置换群。

$$S_3 = \{P_1, P_2, P_3, P_4, P_5, P_6\}$$

用轮换的形式写出来是

$$P_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1) = e$$

$$P_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12)$$

$$P_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13)$$

$$P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23)$$

$$P_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$$

$$P_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132)$$

其运算表如下：

◇	P ₁	P ₂	P ₃	P ₄	P ₅	P ₆
P ₁	P ₁	P ₂	P ₃	P ₄	P ₅	P ₆
P ₂	P ₂	P ₁	P ₅	P ₆	P ₃	P ₄
P ₃	P ₃	P ₆	P ₁	P ₅	P ₄	P ₂
P ₄	P ₄	P ₅	P ₆	P ₁	P ₂	P ₃
P ₅	P ₅	P ₄	P ₂	P ₃	P ₆	P ₁
P ₆	P ₆	P ₃	P ₄	P ₂	P ₁	P ₅

表4

例23. 已知 $\langle S_3, \diamond \rangle$ 是三次六阶置换群。其中

$$S_3 = \{(1), (12), (13), (23), (123), (132)\}$$

$\langle H_1, \diamond \rangle$ 是 $\langle S_3, \diamond \rangle$ 的子群。其中

$$H_1 = \{(1), (12)\} = \{P1, P2\} \quad \text{则}$$

H_1 的左陪集:

$$(1)H_1, (12)H_1; (13)H_1, (132)H_1; (23)H_1, (123)H_1;$$

H_1 的右陪集:


$$H_1(1), H_1(12); H_1(13), H_1(123); H_1(23), H_1(132)$$

注: • $e \in H$, 因为 $\langle H, \diamond \rangle$ 是子群; $a = a * e \in aH$,
 $a = e * a \in Ha$, 代表元在它所代表的陪集之中;

• 一般地, $aH \neq Ha$, 例如, 在上例中

$$(123)H_1 = \{(23), (123)\} \neq \{(13), (123)\} = H_1(123)$$

• 如果 $(\forall a \in G)(aH = Ha)$, 则称 $\langle H, * \rangle$ 是 $\langle G, * \rangle$ 的
正规子群或不变子群, 记为 $H \triangleleft G$ 。



定理17. 设 $\langle H, * \rangle$ 是群 $\langle G, * \rangle$ 的子群。令

$$\left. \begin{array}{l} (1) S_l = \{aH : a \in G\} \\ (2) S_r = \{Ha : a \in G\} \end{array} \right\} \text{(此表示要去掉重复元素)}$$

则 S_l , S_r 均是 G 的划分。

[证]. 只证 S_l 构成 G 上的划分。

为证 S_l 是 G 的划分, 根据划分的定义, 应证明如下两点:

$$(a) \bigcup_{aH \in S_l} aH = G ;$$

$$(b) (\forall a \in G)(\forall b \in G)(aH = bH \vee aH \cap bH = \emptyset) ;$$

先证(a) $\bigcup_{aH \in S_l} aH = G$;

对于任何 $aH \in S_l$, 都有 $a \in G$, $H \subseteq G$, 从而由群 $(G, *)$ 的封闭性得到 $aH \subseteq G$, 故此, 由并是包含关系的上确界可得 $\bigcup_{aH \in S_l} aH \subseteq G$;

又对于任何的 $a \in G$, 有 $a \in aH \subseteq \bigcup_{aH \in S_l} aH$, 故有
 $G \subseteq \bigcup_{aH \in S_l} aH$

所以, 由包含关系的反对称性, 得到

$$\bigcup_{aH \in S_l} aH = G ;$$

次证(b)($\forall a \in G$)($\forall b \in G$)($aH = bH \vee aH \cap bH = \emptyset$) ;

对任何 $a, b \in G$, 若 $aH \cap bH = \emptyset$, 则问题已证; 否则若 $aH \cap bH \neq \emptyset$, 则必至少有一元素 $x_0 \in aH \cap bH$, 从而 $x_0 \in aH \cap bH$

$$\Rightarrow x_0 \in aH \wedge x_0 \in bH$$

$$\Rightarrow x_0 = a * h_1 \wedge x_0 = b * h_2 \quad (\text{这里 } h_1, h_2 \in H)$$

$$\Rightarrow a * h_1 = b * h_2$$


$$\Rightarrow a = b * h_2 * h_1^{-1} \wedge b = a * h_1 * h_2^{-1} \quad (*)$$

下面来证: $aH = bH$ 。为此, 要分证:

① $aH \subseteq bH$;

② $bH \subseteq aH$;

只证① ;



对任何元素 y ,

$$y \in aH$$

$$\Rightarrow y = a * h' \quad (\text{这里 } h' \in H)$$

$$\Rightarrow y = b * h_2 * h_1^{-1} * h' \quad (\text{由 } (*) : a = b * h_2 * h_1^{-1})$$

$$\Rightarrow y = b * h''$$

$$(\text{由 } H \text{ 的封闭性 : } h'' = h_2 * h_1^{-1} * h' \in H)$$


$$\Rightarrow y \in bH$$

所以 $aH \subseteq bH$;

所以, 由包含关系的反对称性, 得到

$$aH = bH \text{ .}$$

所以, 左陪集全体 S_1 是 G 的一个划分。



定理18. 设 $\langle H, * \rangle$ 是群 $\langle G, * \rangle$ 的子群。则有

(1) $(\forall a \in G)(|aH| = |H|)$;

(2) $(\forall a \in G)(|Ha| = |H|)$;

[证]. 只证(1)

建立自然映射 $f: H \rightarrow aH$ 使得

对任何 $h \in H$, $f(h) = a * h$

于是


① 后者唯一: 由 $*$ 运算的结果唯一性可得;

② 满射: 对任何 $y \in aH$, 有 $x = h \in H$, 使得 $y = a * h$, 于是, 有 $f(x) = f(h) = a * h = y$;

③ 单射: $f(h_1) = f(h_2)$

$$\Rightarrow a * h_1 = a * h_2$$

$$\Rightarrow h_1 = h_2 \quad (\text{群有消去律})。$$



定理19.群 $\langle G, * \rangle$ 的子群 $\langle H, * \rangle$ 的不同左陪集的个数等于它的不同右陪集的个数。即

$$|S_l| = |S_r|。$$

[证]. 建立映射 $f: S_r \rightarrow S_l$ 使得

对任何 $Ha \in S_r$, $f(Ha) = a^{-1}H$

于是

(1) 后者唯一: 对任何 $Ha, Hb \in S_r$, 若 $Ha = Hb$, 须证:
 $f(Ha) = f(Hb)$, 即要证: $a^{-1}H = b^{-1}H$;

为此, 要分证:

① $a^{-1}H \subseteq b^{-1}H$;

② $b^{-1}H \subseteq a^{-1}H$;

只证①;

对任何元素 y , $y \in a^{-1}H$

$$\Rightarrow y = a^{-1} * h_1 \quad (\text{这里 } h_1 \in H)$$

$$\Rightarrow y^{-1} = (a^{-1} * h_1)^{-1}$$

$$= h_1^{-1} * a \quad (\text{鞋袜律, 反身律})$$

$$\Rightarrow y^{-1} \in Ha \quad (\text{因为群有逆元故 } h_1^{-1} \in H)$$

$$\Rightarrow y^{-1} \in Hb \quad (\text{条件 } Ha = Hb)$$

$$\Rightarrow y^{-1} = h_2 * b \quad (\text{这里 } h_2 \in H)$$

$$\Rightarrow y = (y^{-1})^{-1} \quad (\text{反身律})$$

$$= (h_2 * b)^{-1}$$

$$= b^{-1} * h_2^{-1} \quad (\text{鞋袜律})$$

$$\Rightarrow y \in b^{-1}H \quad (\text{因为群有逆元故 } h_2^{-1} \in H)$$

所以 $a^{-1}H \subseteq b^{-1}H$;

所以, 由包含关系的反对称性, 得到

$$a^{-1}H = b^{-1}H .$$



(2) 满射：对任何 $aH \in S_1$ ，有 $Ha^{-1} \in S_r$ ，使得

$$f(Ha^{-1}) = (a^{-1})^{-1}H = aH ;$$

(3) 单射：对任何 $Ha, Hb \in S_r$ ，若 $f(Ha) = f(Hb)$ ，即

$$a^{-1}H = b^{-1}H, \text{ 须证: } Ha = Hb ;$$

为此，要分证：

① $Ha \subseteq Hb$;


② $Hb \subseteq Ha$;

只证①；

对任何元素 y ， $y \in Ha$

$$\Rightarrow y = h_1 * a \quad (\text{这里 } h_1 \in H)$$

$$\begin{aligned} \Rightarrow y^{-1} &= (h_1 * a)^{-1} \\ &= a^{-1} * h_1^{-1} \end{aligned} \quad (\text{鞋袜律})$$


$$\Rightarrow y^{-1} \in a^{-1}H \quad (\text{因为群有逆元故 } h_1^{-1} \in H)$$

$$\Rightarrow y^{-1} \in b^{-1}H \quad (\text{条件 } a^{-1}H = b^{-1}H)$$

$$\Rightarrow y^{-1} = b^{-1} * h_2 \quad (\text{这里 } h_2 \in H)$$

$$\Rightarrow y = (y^{-1})^{-1} \quad (\text{反身律})$$

$$= (b^{-1} * h_2)^{-1}$$

$$= h_2^{-1} * b \quad (\text{鞋袜律, 反身律})$$

$$\Rightarrow y \in Hb \quad (\text{因为群有逆元故 } h_2^{-1} \in H)$$

所以 $Ha \subseteq Hb$;

所以, 由包含关系的反对称性, 得到

$$Ha = Hb \text{ 。}$$

注：• 实际上已经证明了： $Ha = Hb \Leftrightarrow a^{-1}H = b^{-1}H$ ；

在(1)后者唯一中 证明的是： $Ha = Hb \Rightarrow a^{-1}H = b^{-1}H$ ；

在(3)单射中 证明的是： $a^{-1}H = b^{-1}H \Rightarrow Ha = Hb$ ；

• 因此 实际上也可得到： $aH = bH \Leftrightarrow Ha^{-1} = Hb^{-1}$ ；

因为 $aH = bH \Leftrightarrow (a^{-1})^{-1}H = (b^{-1})^{-1}H$

$\Leftrightarrow Ha^{-1} = Hb^{-1}$ (利用 $Ha = Hb \Leftrightarrow a^{-1}H = b^{-1}H$)。

定义10. 指数(exponent)

子群 $\langle H, * \rangle$ 关于群 $\langle G, * \rangle$ 的不同左陪集(或右陪集)的个数(或势)称为群 $\langle G, * \rangle$ 关于子群 $\langle H, * \rangle$ 的指数。记为 $|G/H|$ 。

注：• 根据定义有 $|G/H| = |S_l| = |S_r|$ ；



定理20.拉格朗日(Lagrange)定理

设 $\langle H, * \rangle$ 是有限群 $\langle G, * \rangle$ 的子群。则有

$$|G| = |G/H| \cdot |H| \quad (\text{或 } |G/H| = |G|/|H|)。$$

[证]. 由于 $\langle G, * \rangle$ 是有限群，故指数 $|G/H|$ 是有限的(分类个数不会超过总元素个数)，故可设 $|G/H| = k$ 。

于是，由定理17，有 k 个元 $a_1, a_2, \dots, a_k \in G$ ，使得


$$G = a_1H \cup a_2H \cup \dots \cup a_kH \quad \text{并且} \quad a_iH \cap a_jH = \emptyset \quad (1 \leq i \neq j \leq k)$$

从而有

$$\begin{aligned} |G| &= |a_1H| + |a_2H| + \dots + |a_kH| \\ &= |H| + |H| + \dots + |H| \quad (\text{定理18 } (\forall a \in G)(|aH| = |H|)) \end{aligned}$$

$$= k \cdot |H|$$

$$= |G/H| \cdot |H|。$$



注：•在定理的证明中，用的是左陪集；根据定理19，用右陪集一样可证得拉氏定理。

•根据拉氏定理显然可得：


①子群的阶一定整除大群的阶；即 $|H| \mid |G|$

因此，寻找子群，只须寻找以大群阶的因子为阶数的子群；

②左陪集的个数一定整除大群的阶；即 $|S_l| \mid |G|$ ；

右陪集的个数一定整除大群的阶；即 $|S_r| \mid |G|$ ；

大群关于子群的指数一定整除大群的阶；即 $|G/H| \mid |G|$ ；
即，左陪集的个数、右陪集的个数、指数都是大群阶的因子。




例24.在例23中三次对称群 S_3 的阶是6,故 S_3 的非平凡子群是:

$$2\text{阶群 } H_1 = \{(1), (12)\} = \{P1, P2\}$$

$$3\text{阶群 } H_2 = \{(1), (123), (132)\} = \{P1, P5, P6\}$$

H_1 (不同)的左陪集为三个: $\{(1), (12)\} = \{P1, P2\}$,
 $\{(13), (132)\} = \{P3, P6\}$, $\{(23), (123)\} = \{P4, P5\}$

H_1 (不同)的右陪集为三个: $\{(1), (12)\} = \{P1, P2\}$,
 $\{(13), (123)\} = \{P3, P5\}$, $\{(23), (132)\} = \{P4, P6\}$



H_2 (不同)的左陪集为二个:

$$\{(1), (123), (132)\} = \{P1, P5, P6\} ,$$

$$\{(12), (13), (23)\} = \{P2, P3, P4\}$$

H_2 (不同)的右陪集为二个:

$$\{(1), (123), (132)\} = \{P1, P5, P6\} ,$$


$$\{(12), (13), (23)\} = \{P2, P3, P4\}$$

因此 $2 \times 3 = 6, 3 \times 2 = 6$ 所以, 满足拉氏定理。

注: •三次对称群 S_3 的2阶子群还有: $H_1' = \{(1), (13)\} = \{P1, P3\}$,

$$H_1'' = \{(1), (23)\} = \{P1, P4\} ;$$

•子群 $\langle H_2, \diamond \rangle$ 显然是群 $\langle S_3, \diamond \rangle$ 的正规子群, 记为 $H_2 \trianglelefteq S_3$ 。



推论1.素数阶群的子群只有两个，即两个平凡子群。

[证].设 $\langle G, * \rangle$ 是有限群， $|G| = p$ 。由于 p 是素数，故 p 的因子只能是1和 p 。因此由Lagrange定理知，素数阶群的子群只能是1阶子群和它本身，即两个平凡子群：

$\langle \{e\}, * \rangle$ 和 $\langle G, * \rangle$ 。

推论2.在有限群中，每个元素的阶都是群的阶的因子。

[证].设 $\langle G, * \rangle$ 是有限群， $|G| = n$ 。对任何元素 $g \in G$ ，由定理8知， g 的阶有限，故可设 g 的阶为 m ，且有 $m \leq n$ 。令 $S = \{e, g, g^2, \dots, g^{m-1}\}$ ，由定理5知 S 中元素互不相同，因此 $|S| = m$ ； $*$ 运算关于 S 是封闭的，根据定理16知 $\langle S, * \rangle$ 是群 $\langle G, * \rangle$ 的子群，且是循环子群。由Lagrange定理知， $m \mid n$ 。故每个元素的阶是群的阶的因子。



推论3.每个素数阶群都是循环群。

[证].设 $\langle G, * \rangle$ 是有限群, $|G| = p$, p 是素数。由于 $p > 1$, 故

必有元素 $g \in G$ 且 $g \neq e$ 。由定理8知, g 的阶有限, 故可设 g 的阶为 m , 且有 $1 < m \leq p$ (若 $m=1$, 则 $g=e$, 矛盾)。令 $S = \{e, g, g^2, \dots, g^{m-1}\}$, 由定理5知 S 中元素互不相同, 因此 $|S| = m$; $*$ 运算关于 S 是封闭的, 根据定理16知 $\langle S, * \rangle$ 是群 $\langle G, * \rangle$ 的子群, 且是循环子群。由Lagrange定理知, $m \mid p$, 由 p 是素数及 $m \neq 1$ 知 $m=p$, 于是有 $G=S$, 故群 $\langle G, * \rangle$ 是循环群, 而元素 g 正好是这个群的生成元。

注: •实际上证明了: 素数阶群的每个非么的元素都是这个群的生成元, 它们的阶都相同, 全都等于群的阶。

推论4.四阶不同构的群只有两个，一个是4阶循环群，一个是Klein 4一群。

[证].在四阶群中，若有一个元素的阶为4，则该群就是4阶循环群(参见表5);

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

4阶循环群

表5

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

Klein4一群

表6

若没有4阶元素，由推论2知除幺元外，每个元素的阶只能是2。而除幺元外，每个元素的阶为2的群就是Klein4一群(参见表6)。

离散数学

从同构的意义上来说，四阶群只有两个，一个是4阶循环群，一个是Klein4一群。

Lagrange定理的推论：

- (1) 素数阶群的子群只有两个，即两个平凡群。
- (2) 在有限群中，每个元素的阶是群的阶的因子。
- (3) 每个素数阶的群是循环群。
- (4) 四阶不同构的群只有两个，一个是四阶循环群，一个是Klein-4群。

离散数学

◆ 第六章 代数系统

§ 4. 群

到此已经结束！

