




第五章 代数结构

§1 代数系统的引入

§2 运算及其性质

§3 半群

§4 群与子群

 §5 阿贝尔群和循环群

§7 陪集与拉格朗日定理

§8 同态与同构

§9 环和域

§5-5 阿贝尔群和循环群

定义1 如果群 $\langle G, * \rangle$ 中运算 $*$ 是可交换的, 则称该群为**阿贝尔群** (或称为**交换群**)。

例: $\langle \mathbb{I}, + \rangle$ 为阿贝尔群。

例: 代数系统 $\langle F, \circ \rangle$ 是阿贝尔群。

$S = \{a, b, c, d\}$, S 上定义双射函数 $f : S \rightarrow S$

$$f(a)=b \quad f(b)=c \quad f(c)=d \quad f(d)=a$$

构造复合函数 $f^1 = f(x) = \{\langle a, b \rangle, \langle b, c \rangle, \langle c, d \rangle, \langle d, a \rangle\}$

$$f^2 = f \circ f(x) = \{\langle a, c \rangle, \langle b, d \rangle, \langle c, a \rangle, \langle d, b \rangle\}$$

$$f^3 = f \circ f^2(x) = \{\langle a, d \rangle, \langle b, a \rangle, \langle c, b \rangle, \langle d, c \rangle\}$$

$$f^4 = f \circ f^3(x) = \{\langle a, a \rangle, \langle b, b \rangle, \langle c, c \rangle, \langle d, d \rangle\} = f^0$$

$$F = \{f^0, f^1, f^2, f^3\}$$

§5-5 阿贝尔群和循环群

由运算表可见:

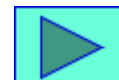
- (1) 运算是**封闭**的;
- (2) “ \circ ”可**结合**;
- (3) **幺元** f^0 ;
- (4) 每一个元素均可**逆**;

f^0 的逆元就是本身, f^1 和 f^3 互为逆元, f^2 的逆元也是本身。

- (5) 以主对角线为**对称**。

$\therefore \langle F, \circ \rangle$ 为阿贝尔群。

\circ	f^0	f^1	f^2	f^3
f^0	f^0	f^1	f^2	f^3
f^1	f^1	f^2	f^3	f^0
f^2	f^2	f^3	f^0	f^1
f^3	f^3	f^0	f^1	f^2





§5-5 阿贝尔群和循环群

例：设 G 为所有 n 阶非奇（满秩）矩阵的集合，矩阵乘法运算 \circ 作为定义在集合 G 上的二元运算，则 $\langle G, \circ \rangle$ 是一个不可交换群。

解：任意两个 n 阶非奇矩阵相乘后，仍是一个非奇矩阵，所以 \circ 是**封闭**的。

矩阵乘法运算是**可结合**的。

n 阶**单位阵** E 是 G 中的**幺元**。

任意一个非奇阵 A 存在着唯一的**逆阵** A^{-1} ，使 $A^{-1} \cdot A = A \cdot A^{-1} = E$ ，但矩阵乘法是不可交换的，因此， $\langle G, \circ \rangle$ 是一个不可交换群。



§5-5 阿贝尔群和循环群

定理1 设 $\langle G, * \rangle$ 是一个群, $\langle G, * \rangle$ 是阿贝尔群的充分必要条件是 $\forall a, b \in G$ 有 $(a*b)*(a*b) = (a*a)*(b*b)$ 。

证明: (1) 先证充分性

$(a*b)*(a*b) = (a*a)*(b*b) \Rightarrow \langle G, * \rangle$ 是阿贝尔群。

对 $\forall a, b \in G$ 有 $(a*b)*(a*b) = (a*a)*(b*b)$ 成立,

$\because *$ 是可结合的

$\therefore a*(a*b)*b = (a*a)*(b*b) = (a*b)*(a*b) = a*(b*a)*b$

得 $a * b = b * a$

$\therefore \langle G, * \rangle$ 是阿贝尔群。



§5-5 阿贝尔群和循环群

(2) 再证必要性

$\langle G, * \rangle$ 是阿贝尔群 $\Rightarrow (a*b) * (a*b) = (a*a) * (b*b)$

\because 阿贝尔群满足交换律, 对 $\forall a, b \in G$ 有 $a*b = b*a$,

$$\begin{aligned}\therefore (a * a) * (b * b) &= a * (a * b) * b \\ &= a * (b * a) * b \\ &= (a * b) * (a * b) .\end{aligned}$$

证毕!

在阿贝尔群中, 对任一 $a, b \in G$ 有

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

§5-5 阿贝尔群和循环群

定义2 设 $\langle G, * \rangle$ 是一个群， I 是整数集合，若存在一个元素 $a \in G$ ，对于 G 中每一个元素都能表示成 a^n 的形式（ $n \in I$ ），则称 $\langle G, * \rangle$ 是一个循环群， a 称为循环群 G 的生成元。

例： $A = \{1, -1, i, -i\}$

由运算表可见：

$$(1)^1 = 1 \quad (1)^2 = 1 \cdots$$

$$(-1)^1 = -1 \quad (-1)^2 = 1 \quad (-1)^3 = -1 \quad (-1)^4 = 1$$

$$(i)^1 = i \quad (i)^2 = -1 \quad (i)^3 = -i \quad (i)^4 = 1$$

$$(-i)^1 = -i \quad (-i)^2 = -1 \quad (-i)^3 = i \quad (-i)^4 = 1$$

\bullet	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

$\langle A, \bullet \rangle$ 是循环群
 $i, -i$ 是生成元





§5-5 阿贝尔群和循环群

例： 60° ， 300° 就是群 $\langle \{0^\circ, 60^\circ, 120^\circ, 180^\circ, 240^\circ, 300^\circ\}, \star \rangle$

的生成元，所以该群为循环群。

\star	0°	60°	120°	180°	240°	300°
0°	0°	60°	120°	180°	240°	300°
60°	60°	120°	180°	240°	300°	0°
120°	120°	180°	240°	300°	0°	60°
180°	180°	240°	300°	0°	60°	120°
240°	240°	300°	0°	60°	120°	180°
300°	300°	0°	60°	120°	180°	240°

§5-5 阿贝尔群和循环群

例：I为整数集合。“模m同余”是一个等价关系。

设 $m=4$ ， N_4 表示“模4同余”所产生的等价类的集合，

$$N_4=\{[0],[1],[2],[3]\},$$

定义运算 $+_4$ ： $[i]_4+[j]_4=[(i+j)(\text{mod } 4)]$, $(i,j=0,1,2,3)$

则 $\langle N_4, +_4 \rangle$ 是群并且是循环群。

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

由运算表可见：

$$[1]^1=[1] \quad \text{或} \quad [3]^1=[3]$$

$$[1]^2=[2] \quad [3]^2=[2]$$

$$[1]^3=[3] \quad [3]^3=[1]$$

$$[1]^4=[0] \quad [3]^4=[0]$$





§5-5 阿贝尔群和循环群

定理2 每一个循环群必然是阿贝尔群。

证明：循环群 \Rightarrow 是阿贝尔群

设 $\langle G, * \rangle$ 是一个循环群， a 是该群的生成元，则
对于任意的 $x, y \in G$ ，必有 $r, s \in \mathbb{I}$ ，使得

$$x = a^r \text{ 和 } y = a^s$$

而且
$$x * y = a^r * a^s = a^{r+s} = a^{s+r} = a^s * a^r = y * x$$

因此，运算 ***可交换**。

$\therefore \langle G, * \rangle$ 循环群一定是阿贝尔群。



§5-5 阿贝尔群和循环群

定义3 设 $\langle G, * \rangle$ 为群, $a \in G$, 如果 $a^n = e$, 且 n 为满足此式的最小正整数, 则称 a 的阶(*order*)为 n , 如果上述 n 不存在时, 则称 a 为无限阶。

§5-5 阿贝尔群和循环群

定理3 设 $\langle G, * \rangle$ 是由元素 $a \in G$ 生成的有限循环群, 如果 G 的阶数是 n , 即 $|G|=n$, 则

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

其中 e 是 $\langle G, * \rangle$ 的么元, n 是使 $a^n = e$ 的最小正整数。
(即 n 为元素 a 的阶)

证明: (1) 首先证明 n 是使 $a^n = e$ 的最小正整数, 即 a^1, a^2, \dots, a^{n-1} 都不为 e , 且 $a^n = e$
(a 的阶为 n)





§5-5 阿贝尔群和循环群

假设对于某个正数 m , $m < n$, 有 $a^m = e$ 。

$\therefore \langle G, * \rangle$ 是一个循环群,

$\therefore G$ 中的任何元素都能写为 a^k ($k \in I$) 且 $k = mq + r$,

其中, q 是某个整数, $0 \leq r < m$ 。

则有 $a^k = a^{mq+r} = (a^m)^q * a^r = (e)^q * a^r = a^r$

$\therefore G$ 中每一个元素都可表示成 a^r ($0 \leq r < m$),

这样, G 中最多有 m 个不同的元素, 与 $|G|=n$ 相矛盾。

所以 $a^m = e$ ($m < n$) 是不可能的。



§5-5 阿贝尔群和循环群

(2) 进一步证明 $a, a^2, a^3, \dots, a^{n-1}, a^n$ 互不相同。

用反证法。

假设 $a^i = a^j$, ($1 \leq i < j \leq n$), 则 $a^i = a^i * a^{j-i}$

所以 $a^{j-i} = e$, ($1 \leq j-i < n$), 这已经由上面证明是不可能的。

所以 $a, a^2, a^3, \dots, a^{n-1}, a^n$ 都不相同,

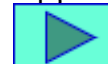
因此 $G = \{a, a^2, a^3, \dots, a^{n-1}, a^n = e\}$



§5-5 阿贝尔群和循环群

注意的问题：

- (1) 群的阶与元素的阶概念不同。
- (2) 群中唯一的一个一阶元素是幺元。
- (3) 循环群中的生成元的阶与群的阶相等。



§5-5 阿贝尔群和循环群

例：设 $G = \{\alpha, \beta, \gamma, \delta\}$ ，二元运算 $*$ 如下表所示。

解： $*$ 是封闭的， α 是幺元。

β, γ 和 δ 的逆元分别是 β, δ 和 γ 。

可以验证运算 $*$ 是可结合的。

所以 $\langle G, * \rangle$ 是一个群。

$$\gamma * \gamma = \gamma^2 = \beta, \quad \gamma^3 = \delta, \quad \gamma^4 = \alpha$$

$$\delta * \delta = \delta^2 = \beta, \quad \delta^3 = \gamma, \quad \delta^4 = \alpha$$

故群 $\langle G, * \rangle$ 是由 γ 或 δ 生成的。

因此 $\langle G, * \rangle$ 是一个循环群。

结论：一个循环群的生成元可以不唯一。

$*$	α	β	γ	δ
α	α	β	γ	δ
β	β	α	δ	γ
γ	γ	δ	β	α
δ	δ	γ	α	β



§5-5 阿贝尔群和循环群

例：整数加群 $\langle \mathbb{I}, + \rangle$ ，任取 $i \in \mathbb{I}$ ，

若 $i > 0$ ，则 $i = 1 + 1 + \cdots + 1 = 1^i$

i个1相加

若 $i = 0$ ，因为0是幺元，由定义，有 $0 = 1^0$ ；

若 $i < 0$ ，设 $i = -j$

$$i = -j = (-1) + (-1) + \cdots + (-1) = (-1)^j = (1^{-1})^j = 1^{-j} = 1^i$$

j个-1相加

所以，群的 $\langle \mathbb{I}, + \rangle$ ，任何元素都可以写成1的幂，即是循环群，1是循环群的生成元。

-1也是循环群 $\langle \mathbb{I}, + \rangle$ 的生成元。



循环群的生成元

定理

设 $G = \langle a \rangle$ 是循环群.

(1) 若 G 是无限循环群, 则 G 只有 a 和 a^{-1} 两个生成元.

(2) 若 G 是 n 阶循环群, 则 a^r 是 G 的生成元当且仅当 r 是小于等于 n 且与 n 互质的正整数.



生成元的实例

- (1) 设 $G = \{e, a, \dots, a^{11}\}$ 是 12 阶循环群, 则小于或等于 12 且与 12 互素的数是 1, 5, 7, 11, 由定理可知 a , a^5 , a^7 和 a^{11} 是 G 的生成元.
- (2) 设 $G = \langle \mathbb{Z}_9, \oplus \rangle$ 是模 9 的整数加群, 则小于或等于 9 且与 9 互素的数是 1, 2, 4, 5, 7, 8. 根据定理, G 的生成元是 1, 2, 4, 5, 7 和 8.
- (3) 设 $G = 3\mathbb{Z} = \{3z \mid z \in \mathbb{Z}\}$, G 上的运算是普通加法. 那么 G 只有两个生成元: 3 和 -3 .

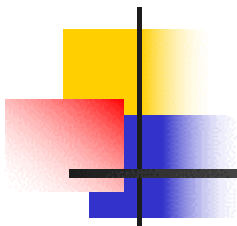


循环群的子群

定理

设 $G = \langle a \rangle$ 是循环群.

- (1) 设 $G = \langle a \rangle$ 是循环群, 则 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.
- (4) 若 $G = \langle a \rangle$ 是 n 阶循环群, 则元素 a^r 的阶 $d = n/(n, r)$, 这里 (n, r) 表示 n 和 r 的最大公约数.



子群的实例

(1) $G=\langle \mathbf{Z}, + \rangle$ 是无限循环群, 对于自然数 $m \in \mathbf{N}$, 1 的 m 次幂是 m , m 生成的子群是 $m\mathbf{Z}$, $m \in \mathbf{N}$. 即

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

$$\langle m \rangle = \{ mz \mid z \in \mathbf{Z} \} = m\mathbf{Z}, \quad m > 0$$

(2) $G=\mathbf{Z}_{12}$ 是12阶循环群. 12的正因子是1, 2, 3, 4, 6 和 12, 因此 G 的子群是:

1 阶子群 $\langle 12 \rangle = \langle 0 \rangle = \{0\}$, 2 阶子群 $\langle 6 \rangle = \{0, 6\}$

3 阶子群 $\langle 4 \rangle = \{0, 4, 8\}$, 4 阶子群 $\langle 3 \rangle = \{0, 3, 6, 9\}$

6 阶子群 $\langle 2 \rangle = \{0, 2, 4, 6, 8, 10\}$, 12 阶子群 $\langle 1 \rangle = \mathbf{Z}_{12}$



n 元置换的定义

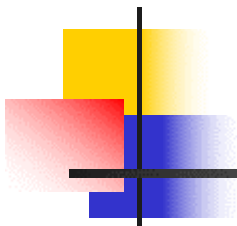
定义 设 $S = \{1, 2, \dots, n\}$, S 上的双射函数 $\sigma: S \rightarrow S$ 称为 S 上的 **n 元置换**. 一般将 n 元置换 σ 记为

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

例如 $S = \{1, 2, 3, 4, 5\}$, 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.



k 阶轮换与对换

定义 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**.

例如 5元置换

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

分别是 5 阶和 2 阶轮换 $\sigma=(1\ 2\ 3\ 4\ 5), \tau=(1\ 3)$, 其中 τ 是对换



n 元置换分解为轮换之积

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 中分解出来的第一个轮换式 $(1\ 5\ 2\ 3\ 6)$ ；第二个轮换为 (4) ；第三个轮换为 $(7\ 8)$. σ 的轮换表示式

$$\sigma = (1\ 5\ 2\ 3\ 6)\ (4)\ (7\ 8) = (1\ 5\ 2\ 3\ 6)\ (7\ 8)$$

用同样的方法可以得到 τ 的分解式

$$\tau = (1\ 8\ 3\ 4\ 2)\ (5\ 6\ 7)$$

注意：在轮换分解式中，1阶轮换可以省略.

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 元置换求逆就是求反函数.

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

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

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

使用轮换表示是:

$$\sigma\tau = (1\ 5\ 4)(2\ 3)(1\ 4\ 2\ 3) = (1\ 5\ 2)$$

$$\tau\sigma = (1\ 4\ 2\ 3)(1\ 5\ 4)(2\ 3) = (3\ 5\ 4)$$

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



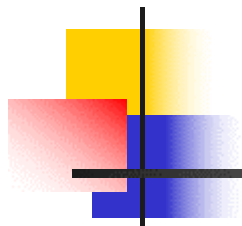
n 元置换群及其实例

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

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



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)



S_3 的子群

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

$$A_3 = \langle (1\ 2\ 3) \rangle = \{(1), (1\ 2\ 3), (1\ 3\ 2)\},$$

$$\langle (1) \rangle = \{(1)\}$$

$$\langle (1\ 2) \rangle = \{(1), (1\ 2)\},$$

$$\langle (1\ 3) \rangle = \{(1), (1\ 3)\},$$

$$\langle (2\ 3) \rangle = \{(1), (2\ 3)\}$$



第五章 代数结构


§1 代数系统的引入

§2 运算及其性质

§3 半群

§4 群与子群

§5 阿贝尔群和循环群

 §7 陪集与拉格朗日定理

§8 同态与同构

§9 环和域



§5-7 陪集和拉格朗日定理

讨论群理论中的又一重要内容：

群 $\langle G, * \rangle$ 的任意子群 $\langle H, * \rangle$ 将 G 分解成 H 在 G 中的陪集。

定义1 设 $\langle G, * \rangle$ 为群, $A, B \in P(G)$, 且 $A \neq \emptyset$, $B \neq \emptyset$, 记

$$AB = \{ a * b \mid a \in A, b \in B \}$$

$$\text{和 } A^{-1} = \{ a^{-1} \mid a \in A \}$$

分别称为 **A** , **B 的积**和 **A 的逆**。

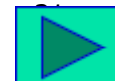


§5-7 陪集和拉格朗日定理

定义2 设 $\langle H, * \rangle$ 为群 $\langle G, * \rangle$ 的子群, $a \in G$, 则集合
 $\{a\}H$ (或 $H\{a\}$) 称为由 a 所确定的 H 在 G 中的左
陪集 (或右陪集),

简称为 H 关于 a 的左陪集 (右陪集), 记为
 aH (或 Ha)。元素 a 称为陪集 aH (或 Ha)的代表
元素。

为确定起见, 下面只对左陪集进行讨论。





§5-7 陪集和拉格朗日定理

例：设 $G=\mathbb{R}\times\mathbb{R}$ ， \mathbb{R} 为实数集， G 上的一个二元运算 $+$ 定义为 $\langle x_1, y_1 \rangle + \langle x_2, y_2 \rangle = \langle x_1+x_2, y_1+y_2 \rangle$
显然， $\langle G, + \rangle$ 是一个具有幺元 $\langle 0, 0 \rangle$ 的阿贝尔群。

设 $H=\{\langle x, y \rangle | y=2x\}$

容易验证 $\langle H, + \rangle$ 是 $\langle G, + \rangle$ 的子群。

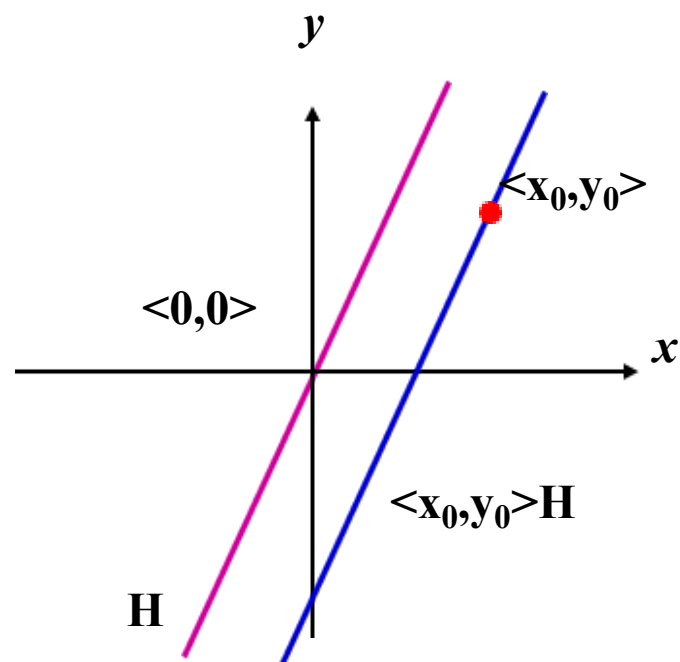
对于 $\langle x_0, y_0 \rangle \in G$ ，
 H 关于 $\langle x_0, y_0 \rangle$ 的左陪集为 $\langle x_0, y_0 \rangle H$ 。

§5-7 陪集和拉格朗日定理

这个例子的几何意义为：

G 是笛卡尔平面， H 是通过原点的直线 $y=2x$ ，

陪集 $\langle x_0, y_0 \rangle H$ 是通过点 $\langle x_0, y_0 \rangle$ 且平行于 H 的直线。





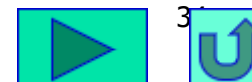
§5-7 陪集和拉格朗日定理

对于有限群，有下面一个很重要的结论。

定理1 (拉格朗日定理)

设 $\langle H, * \rangle$ 为 $\langle G, * \rangle$ 的子群， $a, b \in G$ ，那么

- (a) $R = \{ \langle a, b \rangle \mid a \in G, b \in G \text{ 且 } a^{-1} * b \in H \}$ 是 G 中的一个等价关系。对于 $a \in G$ ，若记 $[a]_R = \{ x \mid x \in G \text{ 且 } \langle a, x \rangle \in R \}$ ，则 $[a]_R = aH$
- (b) 设 $\langle H, * \rangle$ 为有限群 $\langle G, * \rangle$ 的子群， $|G|=n$ ， $|H|=m$ ，那么 H 的阶整除 G 的阶，即 $m \mid n$ 。



3

§5-7 陪集和拉格朗日定理

证明: 先证 (a) $R = \{ \langle a, b \rangle \mid a \in G, b \in G \text{ 且 } a^{-1} * b \in H \}$

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

$\because a^{-1} * a = e \in H, \therefore \langle a, a \rangle \in R$ 。 R 是自反的。

(2) 若 $\langle a, b \rangle \in R$, 则 $a^{-1} * b \in H$,

$\because H$ 是 G 的子群, 故 $(a^{-1} * b)^{-1} = b^{-1} * a \in H$

$\therefore \langle b, a \rangle \in R$ 。 R 是对称的。

(3) 若 $\langle a, b \rangle \in R, \langle b, c \rangle \in R$, 则 $a^{-1} * b \in H, b^{-1} * c \in H$,

$\therefore a^{-1} * b * b^{-1} * c = a^{-1} * c \in H, \langle a, c \rangle \in R$, R 是传递的。

$\therefore R$ 是 G 中的一个等价关系。

对于 $a \in G$, 有 $b \in [a]_R$ 当且仅当 $\langle a, b \rangle \in R$, 即当且仅当 $a^{-1} * b \in H$, 而 $a^{-1} * b \in H$ 就是 $b \in aH$ 。因此 $[a]_R = aH$ 。





§5-7 陪集和拉格朗日定理

再证(b) H 的阶整除 G 的阶，即 $m|n$

由于 R 是 G 中的一个等价关系，所以必定将 G 划分成两两不交的等价类 $[a_1]_R, [a_2]_R, \dots, [a_k]_R$ ，使得

$$G = \bigcup_{i=1}^k [a_i]_R = \bigcup_{i=1}^k a_i H$$

又因为 H 中任意两个不同的元素 h_1, h_2 ，设 $a \in G$ 必有 $a * h_1 \neq a * h_2$ ，

所以 $|a_i H| = |H| = m, i=1, 2, \dots, k$ 。

因此， $n = |G| = |\bigcup_{i=1}^k a_i H| = \sum_{i=1}^k |a_i H| = mk$

所以 H 阶的整除 G 的阶 $m|n$ 。



§5-7 陪集和拉格朗日定理

根据拉格朗日定理，可直接得到以下几个推论。

推论1 任何质数阶的群不可能有非平凡子群。

证明：因为对于其任何子群，

该子群的阶必定是原来群的阶的一个正因子，

而原来群的阶是质数 p ，正因子只能是1或 p ，

只能是平凡子群。



§5-7 陪集和拉格朗日定理

推论2 设 $\langle G, * \rangle$ 为 n 阶有限群, 那么对于任意 $a \in G$, a 的阶必是 n 的因子且必有 $a^n = e$, 这里 e 是群 $\langle G, * \rangle$ 的么元。如果 n 为质数, 则 $\langle G, * \rangle$ 必是循环群。

证明: 由 G 中的任意元素 a 生成的循环群

$H = \{a^i | i \in \mathbb{I}, a \in G\}$, 一定是 G 的一个子群。

如果 H 的阶是 m , 那么由定理5-5.3可知

$a^m = e$, 即 a 的阶等于 m 。

由拉格朗日定理知: 必有 $n = mk$, $k \in \mathbb{N}$,

因此, a 的阶 m 是 n 的因子, 且有 $a^n = a^{mk} = (a^m)^k = e^k = e$





§5-7 陪集和拉格朗日定理

因为质数阶群只有平凡子群，

所以，质数阶群必定是循环群。

并且除幺元以外的其它元素都是生成元。

§5-7 陪集和拉格朗日定理

例： 设 $K=\{e,a,b,c\}$ ，在 K 上定义二元运算 $*$ 如表所示。
证明 $\langle K, * \rangle$ 是一个群，但不是循环群。

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

称 $\langle K, * \rangle$ 为Klein四元群。

证明：由表可知，运算 $*$ 是封闭的和可结合的。幺元是 e ，每个元素的逆元是自身， $\langle K, * \rangle$ 是群。
因为 a, b, c 都是二阶元，故 $\langle K, * \rangle$ 不是循环群。





§5-7 陪集和拉格朗日定理

例：任何一个四阶群只能是四阶循环群或者Klein四元群。

证明：设四阶群为 $\langle \{e, a, b, c\}, * \rangle$ ，其中 e 是幺元。

1) 当四阶群含有一个四阶元素时，

这个群就是循环群。

2) 当四阶群不含有四阶元素时，

则由推论2可知，除幺元 e 外， a, b, c 的阶一定都是2。



§5-7 陪集和拉格朗日定理

若 $a*b=a$ ，将导致 $b=e$

若 $a*b=b$ ，将导致 $a=e$

若 $a*b=e$ ，将导致 $a=b$

所以 $a * b=c$ 。

同样有 $b * a=c$ 以及 $a * c=c * a=b$, $b * c=c * b=a$ 。

因此，这个群是Klein四元群。