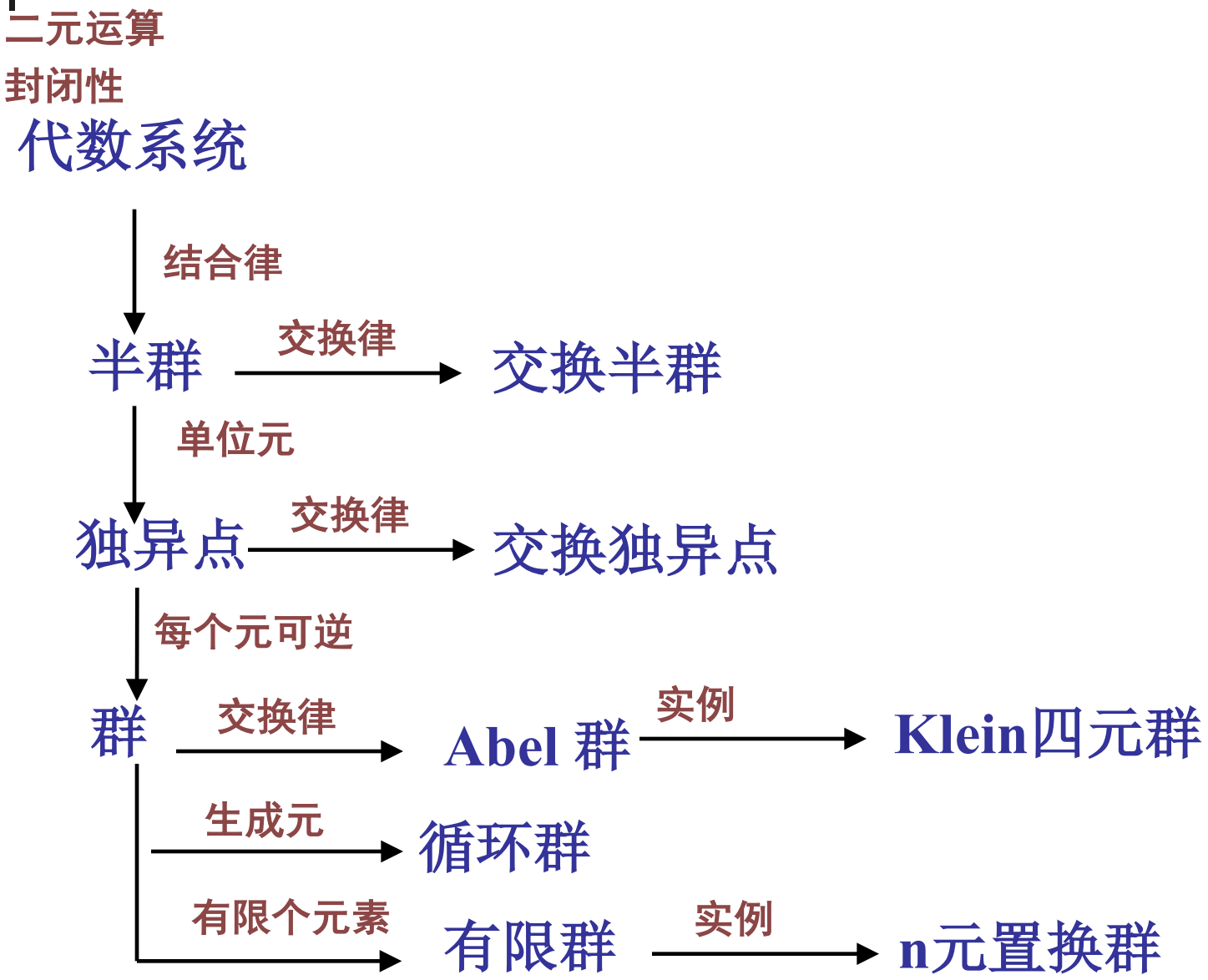
第十七章 群

- 群的定义与性质
- 子群
- 循环群
- 变换群和置换群
- 群的分解
- 正规子群和商群
- 群的同态与同构
- 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
- 习题分析

广群，半群，独异点与群


二元运算
封闭性
代数系统
结合律
半群
交换律
交换半群
单位元
独异点
交换律
交换独异点
每个元可逆
群
交换律
Abel 群
实例
Klein四元群
生成元
循环群
有限个元素
有限群
实例
n元置换群

群的定义

定义 设$<G,*>$是一个代数系统，其中G是非空集合，$*$是G上一个二元运算，如果

(1) 运算$*$是**封闭**的;

(2) 运算$*$是**可结合**的;

(3) 存在**单位元**;

(4) 对于每一个元素$x \in G$，**存在逆元** $x^{-1} \in G$;

则称$<G,*>$是一个**群**。

群的举例

(1) $\langle Z,+\rangle,\langle Q,+\rangle,\langle R,+\rangle$是群；$\langle Z^+,+\rangle$，$\langle \mathbf{N},+\rangle$不是群.

(2) $\langle M_n(R),+\rangle$是群，而$\langle M_n(R),\cdot\rangle$不是群.

(3) $\langle P(B),\oplus\rangle$是群，$\oplus$为对称差运算.

(4) $\langle Z_n,+_n\rangle$是群. $Z_n=\{0,1,\ldots,n-1\}$，$+_n$为模 n 加法.

(5) $\langle A^A,\circ\rangle$，当$|A|\geq 2$时不是群。

群的实例——Klein四元群

设$G=\{e, a, b, c\}$，G上的运算*由下表给出，

称<G, *>为 **Klein四元群.**

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

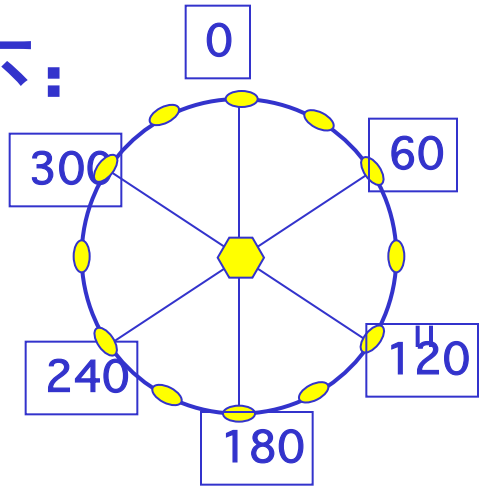
运算表特征：

- 对称性---运算可交换
- $\forall x \in G, x^2=e$,即$x^{-1}=x$
- a, b, c 中任两个元素运算都等于第三个元素。

举例

例1 设R={0°,60°, 120°, 180°, 240°, 300°}表示在平面上几何图形绕形心顺时针旋转角度的六种可能情况，设★是R上的二元运算，对于R中任意两个元素a和b，a★b表示平面图形连续旋转a和b得到的总旋转角度。规定旋转360°等于原来的状态，就看作没有经过旋转。验证<R, ★>是一个群。

解 该系统的图示如下：



举例（续）

★	0^o	60^o	120^o	180^o	240^o	300^o
0^o	0^o	60^o	120^o	180^o	240^o	300^o
60^o	60^o	120^o	180^o	240^o	300^o	0^o
120^o	120^o	180^o	240^o	300^o	0^o	60^o
180^o	180^o	240^o	300^o	0^o	60^o	120^o
240^o	240^o	300^o	0^o	60^o	120^o	180^o
300^o	300^o	0^o	60^o	120^o	180^o	240^o

<*R*, ★>运算表如左：

从★的运算表可看出，运算★在*R*上是封闭的。

∀ a,b,c∈R，由题意，$(a★b)★c=a★(b★c)=(a+b+c) \bmod 360^o$，所以★在*R*上可结合的。

0^o是幺元。

60^o, 120^o, 180^o的逆元分别是300^o,240^o, 180^o。

所以，<R, ★>是一个群。

群的等价定义1

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. $\forall a \in G$,

$$ee = e \quad //e\text{为右单位元}$$

$$\Rightarrow e(aa') = (aa') \Rightarrow (ea)a' = aa' \quad //\text{ 右乘}a'\text{的右逆元}$$

$$\Rightarrow ea = a$$

证 a'为a 的左逆元, 即$a'a = e$,也就是a'的右逆元

$(a')' = a'' = a$.

$$a'' = ea'' = (aa')a'' = a(a'a'') = ae = a$$

群的术语

平凡群　　只含单位元的群 $\{e\}$以及群本身

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，且为群的阶的因子；

反之，元素都是有限阶的群不一定是有限群.

群的性质1—幂运算规则

定理2 幂运算规则

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

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

$a^n a^m=a^{n+m}$

$(a^n)^m=a^{nm}$

若G为Abel群，则$(ab)^n=a^n b^n$

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.

群的性质2—群方程的解

定理3 方程$ax=b$ 和$ya=b$ 在群G 中有解且有唯一解.

证 (存在) 显然$a^{-1}b$ 是$ax=b$ 的解.

(唯一) 假设c 为解，则

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

同理可证ba^{-1}是$ya=b$的解。

群的等价定义2

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，即$be=b$.

$\forall a\in G$, $yb=a$ 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 的右逆元.

群的性质3—消去律

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

定理6 设G是有限半群，且不含零元. 若G中消去律成立，则G是群.(群的等价定义3)

证 【证方程$ax=b$和$ya=b$有解】

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

$a_iG=\{a_ia_j \mid j=1, 2, \dots, n\}$. 下面证$a_iG=G$.

由封闭性, $a_iG \subseteq G$,

假设$|a_iG|<n$, 则存在j, k 使得 $a_ia_j=a_ia_k$.

根据消去律， $a_j=a_k$, 矛盾. 所以$a_iG=G$.

$\forall a_i, a_j,\ a_i, a_j \in G \Rightarrow a_j \in a_iG \Rightarrow$ 方程$a_i x=a_j$ 有解

群的性质4—运算表中的置换

定理7 n元群G的运算表中每行、每列都是G的置换.

$aG=G$和$Ga=G$

证明 在运算表的第i行中存在$a_{ij}=a_{il}$,则$a_ia_j=a_ia_l$,有$a_j=a_l$,与G中有n个元素矛盾。所以G中任何元素在运算表的一行中至多出现一次。

$\forall a_j\in$G,方程$a_ix=a_j$在G中有解,若$x=a_k$,则a_j出现在第i行第k列上,因此任何元素在运算表的每行上至少出现一次.

综上所述,运算的每行是G中元素的一个置换（双射）.

同理可证运算的每列是G中元素的一个置换

- **运算表的行列构成置换的不一定是群，反例：**

*	0	1	2
0	1	2	0
1	0	1	2
2	2	0	1

因为没有单位元.

群的性质5—元素的阶和群的阶

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$t \mid r$. 由于$a=(a^{-1})^{-1}$，故$r \mid t$.

(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.

重要结果

(1) $|a|=1$或2 $\Leftrightarrow a^2=e \Leftrightarrow a=a^{-1}$

(2) $|a|=|a^{-1}|$, $|ab|=|ba|$, $|a|=|bab^{-1}|$

(3) $|a|=r \Rightarrow |a^t|=\dfrac{r}{(t,r)}$ （见例5）

(4) $|a|=n$, $|b|=m$, $ab=ba \Rightarrow |ab| \mid [n,m]$

若$(n,m)=1$, $|ab|=nm$.（见例7）

(t,r)：t和r的最大公约数

$[n,m]$：n和m的最小公倍数

群性质的证明题

证明元素的阶相等或求元素的阶的方法

证$|x|=|y|$：

令$|x|=r$, $|y|=s$,

验证$(x)^s=e \Rightarrow r \mid s$

验证$(y)^r=e \Rightarrow s \mid r$

求$|x|$：

找到n 满足$x^n=e$, 分析n 的因子.

证明群的一些基本性质的方法

工具---幂运算规则、结合律、消去律、群方程的解

例题分析

例：证明单位元e是群中唯一的幂等元。

证 因为$ee=e$，故e是幂等元.

设有另一个幂等元a,有$aa=a=ae$，所以$a=e$.

例：证明 群中不存在零元。

例题分析

例1 设G为群，若$\forall x \in G$有$x^2 = e$, 则G为Abel群.

证 $\forall x,y \in G$, $x^2=e \Leftrightarrow x=x^{-1}$

$xy = (xy)^{-1} = y^{-1}x^{-1} = yx$

例2 若群G中只有唯一2阶元，则这个元素与G中所有元素可交换.

证 设$|x|=2$, $\forall y \in G$,

$|yxy^{-1}|=|x|=2 \Rightarrow yxy^{-1} = x \Rightarrow yx = xy$

例题分析

例3 设$<G,*>$为有限群，则G中阶大于2的元素有偶数个.

证： 显然$a^2=e \Leftrightarrow a=a^{-1}$。

因此，对G中阶大于2的元素a，必有$a\neq a^{-1}$。

又由于$|a|=|a^{-1}|$，所以G中阶大于2的元素一定成对出现.

G中若含有阶大于2的元素，一定是偶数个。

若G中不含阶大于2的元素，即0个，也是偶数。

例题分析

例4 若G为偶数阶群，则G中必存在2阶元.

证 若$\forall x \in G$, $|x|>2$，则$x \neq x^{-1}$.

由于$|x|=|x^{-1}|$, 大于2 阶的元素成对出现，其个数是偶数个。由于G中元素个数为偶数,所以

G 中小于等于2阶的元素必有偶数个.

又1 阶元只有单位元，因此2 阶元必有奇数个。

例题分析

例5 G为群，$a \in G$，$|a|=r$, 证明$|a^t| = r/(t,r)$

证　令$|a^t| = s$,

$(t, r) = d \Rightarrow t = dp, r = dq \Rightarrow r/(t,r) = r/d = q$,且$p$, q互素

下面只要证 $s = q$

$(a^t)^q = (a^t)^{r/d} = (a^r)^{t/d} = e^p = e$

$\therefore s \mid q$

$(a^t)^s = e \Rightarrow a^{ts} = e \Rightarrow r \mid ts \Rightarrow q \mid ps$

因为p, q互素，所以 $q \mid s$

例题分析

例6 设G为有限群，$x, y \in G$, y为2阶元，$x \neq e$, 且$x^2y = yx$, 求$|x|$.

解： $x^2y = yx \Rightarrow yx^2y = x$

$\Rightarrow (yx^2y)(yx^2y) = x^2$

$\Rightarrow yx^4y = x^2 = yxy$

$\Rightarrow x^4=x \Rightarrow x^3=e$

$\Rightarrow |x|=3\ (x \neq e)$

分析 关键是导出关于$x^k = e$ 的等式

根据$x^k = e \Leftrightarrow |x| \mid k$,

使用幂运算规则, 结合律，消去律，$|x|=2 \Leftrightarrow x=x^{-1}$

例题分析

例7 设$<G,*>$为群，$a,b\in G$，且$ab=ba$。如果$|a|=n,|b|=m$,且n与m互质，证明$|ab|=nm$。

证明: 设$|ab|=d$。由$ab=ba$ 可知

$(a*b)^{nm}=(a^n)^m*(b^m)^n=e^m*e^n=e$。从而有 $d|nm$。

又由$a^d*b^d=(a*b)^d=e$，可知 $a^d=b^{-d}$，即$|a^d|=|b^{-d}|=|b^d|$。

再根据 $(a^d)^n=(a^n)^d=e^d=e$ 得$|a^d||n$。

同理有$|a^d||m$。从而知道$|a^d|$是n和m的公因子。

因为n与m互质，所以$|a^d|=1$。即 $a^d=e$，从而 $n|d$。

$|b^d|=|a^d|=1$，所以$m|d$。即d是n和m的公倍数。

由于n与m互质，必有 $nm|d$。故有 $d=nm$。即$|ab|=nm$。

作业

- 复习要点:

  群的定义

  证明代数系统是群有哪些方法

  群的性质及其应用

- 书面作业：

  习题十七，2, 4, / 3,14