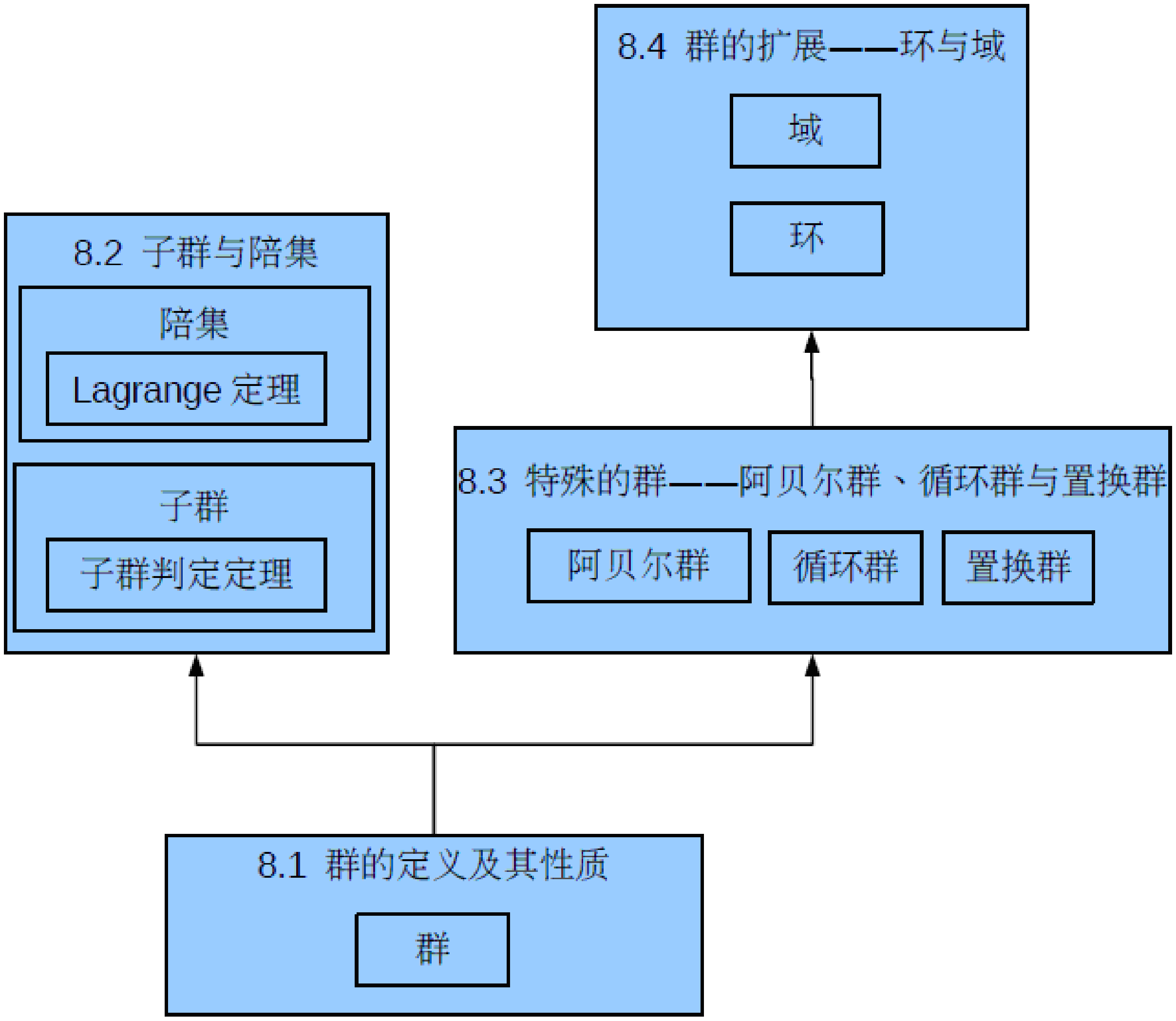
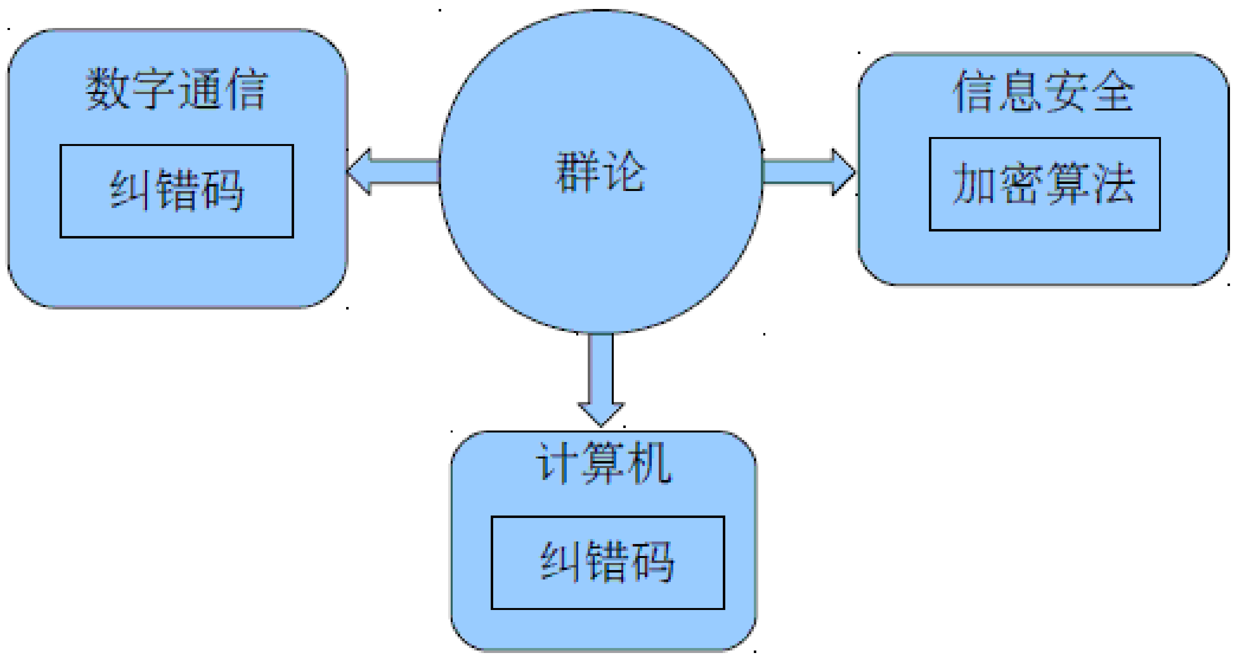
第八章群论初步

群论初步部分知识逻辑概图



群论在计算机科学技术相关领域的应用概图



8.1 群的定义及其性质

群：单位元素、互逆元素和一个可结合运算共同构成的代数系统。

8.1 群的定义及其性质

一、半群、独异点与群的定义

定义 8.1

（1）设 $V=<S, o>$ 是代数系统，o为二元运算，如果o运算是可结合的，则称 V 为半群 .

- 设 <G, •> 为一半群 , 那么 <G, •> 的任一子代数都是半群，称为 <G, •> 的子半群。

（2）设 $V=<S, o>$ 是半群，若 $e\in S$ 是关于o运算的单位元，则称 V 是含幺半群，也叫做独异点 . 有时也将独异点 V 记作 $V=<S, o,e>$.

- 若独异点 $<S, o,e>$ 的子代数含有幺元 e ，那么它必为一独异点，称为 <G, •, e> 的子独异点。

（3）设 $V=<S, o>$ 是独异点， $e\in S$ 是关于o运算的单位元，若$\forall$ a $\in S$ ，有 $a^{-1}\in S$ ，则称 V 为群。通常将群记作 G.

8.1 群的定义及其性质

代数系统	半群	独异点	群
二元运算 （封闭）	+ 可结合	+ 可结合 + 单位元	+ 可结合 + 单位元 + $\forall a \in S$，有 $a^{-1} \in S$
V=<S, o>	V=<S, o>	V=<S, o, e>	G

8.1 群的定义及其性质

实例 1

- **半群**

<Z^+, +>, <N, +>, <Z, +>, <Q, +>, <R, +>, <C, +>, 其中 + 为普通加法 .

- **独异点**

<N, +>, <Z, +>, <Q, +>, <R, +>, <C, +>.

- **群**

<Z, +>, <Q, +>, <R, +>, <C, +>.

分别称为整数加群、有理数加群、实数加群、复数加群。

8.1 群的定义及其性质

实例 2

- **半群**

$\langle M_n(R), +\rangle$, $\langle M_n(R), \cdot\rangle$, 其中 n 是大于 1 的正整数 .

- **独异点**

$\langle M_n(R), +\rangle$, $\langle M_n(R), \cdot\rangle$.

- **群**

$\langle M_n(R), +\rangle$.

$\langle M_n(R), \cdot\rangle$ 不是群，不是每个 n 阶矩阵都有乘法逆元 .

在此，+ 和 . 分别表示矩阵加法和矩阵乘法。

8.1 群的定义及其性质

实例 3

- **半群**

$<P(B), \oplus>, <Z_n, \oplus>$.

- **独异点**

$<P(B), \oplus>, <Z_n, \oplus>$.

- **群**

$<P(B), \oplus>, <Z_n, \oplus>$.

实例 4

- Klein 四元群（四元群）

G={e,a,b,c}.

单位元：e;　　G 中的运算可交换；

每个元素的逆元为其本身；

任何两个元素运算的结果都等于另一个元素．

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

练习 1

- 设 <R*, o> 为代数系统，其中 R* 为非零实数集合，o 运算定义如下

  $\forall x, y \in R^*, x o y = y$

(1) 半群？

(2) 独异点？

(3) 群？

实例 5

- 在形式语言中常将有穷字符表记为∑，由∑上的有限个字符（包括 0 个字符）可以构成一个字符串，称为∑上的字。∑上的全体字符串构成集合∑ * 。设 α,β 是∑ * 上的两个字，将 β 连接在 α 后面得到∑ * 上的字 αβ 。如果将这种连接看作∑ * 上的一种运算，那么这种运算不可交换，但是可结合。集合∑ * 关于连接运算就构成了一个代数系统，它恰好是抽象代数系统 -- 半群的一个实例。
- 集合∑ * 关于连接运算构成了一个代数系统，它恰好是抽象代数系统—独异点的一个实例。

练习 2

- 某二进制码的码字 $x=x_1x_2\ldots x_7$ 由 7 位构成，其中 x_1, x_2, x_3 和 x_4 为数据位，x_5, x_6 和 x_7 为校验位，并且满足：

$x_5 = x_1 \oplus x_2 \oplus x_3$， $x_6 = x_1 \oplus x_2 \oplus x_4$

$x_7 = x_1 \oplus x_3 \oplus x_4$，$\oplus$ 为模 2 加法 .

设 G 为所有码字构成的集合，在 G 上定义二元函数如下：

$\forall x, y \in G$, $x \circ y = z_1z_2\ldots z_7$, $z_i = x_i \oplus y_i$, $i = 1,2,\ldots 7$

证明：$\langle G, \circ \rangle$ 构成群 .

8.1 群的定义及其性质

❖ **证明思路（从定义入手）**

(1) 封闭性

(2) 可结合

有单位元

有逆元

8.1 群的定义及其性质

❖ 封闭性

任取 $x=x_1x_2\ldots x_7$, $y=y_1y_2\ldots y_7$, 令 $xoy=z=z_1z_2\ldots z_7$.

$z_5 = x_5 \oplus y_5$.

$z_1 \oplus z_2 \oplus z_3 = (x_1 \oplus y_1) \oplus (x_2 \oplus y_2) \oplus (x_3 \oplus y_3) = (x_1 \oplus x_2 \oplus x_3) \oplus (y_1 \oplus y_2 \oplus y_3) = x_5 \oplus y_5 = z_5$

所以, $z_5 = z_1 \oplus z_2 \oplus z_3$

同理, $z_6 = z_1 \oplus z_2 \oplus z_4$, $z_7 = z_1 \oplus z_3 \oplus z_4$

于是 $xoy=z \in G$, 从而证明了封闭性（二元运算）.

8.1 群的定义及其性质

❖ 结合律

任取 x, y, z, 设 $(x \circ y) \circ z = a_1a_2\ldots a_7$,

$x \circ (y \circ z) = b_1b_2\ldots b_7$.

$a_i = (x_i \oplus y_i) \oplus z_i = x_i \oplus (y_i \oplus z_i) = b_i$.

❖ 单位元

0000000.

❖ 逆元

$\forall x \in G,\ x^{-1} = x$.

8.1 群的定义及其性质

二、群的术语

定义 8.2

（1）若群 G 是有限集，则称 G 是**有限群**，否则称为**无限群**.

群 G 的基数(对于有限群，指群的元素个数)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：

$<Z,+>$ 和 $<R,+>$ 是无限群，$<Z_n,\oplus>$ 是有限群，也是 n 阶群.

$<\{0\},+>$ 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.

8.1 群的定义及其性质

定义 8.3 设 G 是群，$a\in G$，$n\in Z$，则 a 的 n 次幂 a^n 定义为

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

实例

在 $<Z_3,\oplus>$ 中有 $2^{-3}=(2^{-1})^3=1^3=1\oplus1\oplus1=0$

在 $<Z,+>$ 中有 $(-2)^{-3}=2^3=2+2+2=6$

8.1 群的定义及其性质

定义 8.4 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.

实例

在 $<Z_6,\oplus>$ 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.

8.1 群的定义及其性质

❖ **说明：**

- 对于模 n 整数加群，x 的阶可以根据定义求出，也可以由公式 n/gcd(x,n) 确定，其中 gcd(x,n) 表示 x 与 n 的最大公约数
- 群中元素的阶可能存在，也可能不存在.
- 对于有限群，每个元素的阶都存在，而且是群的阶的因子.
- 对于无限群，单位元的阶存在，是 1 ；而其它元素的阶可能存在，也可能不存在.

8.1 群的定义及其性质

三、群的性质

定理 8.1 设 G 为群，则 G 中的幂运算满足：

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

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

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

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

(5) 若 G 为交换群，则 $(ab)^n = a^n b^n$.

证 (1) $(a^{-1})^{-1}$ 是 a^{-1} 的逆元，a 也是 a^{-1} 的逆元.

根据逆元的惟一性，等式得证.

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

同理 $(ab)(b^{-1}a^{-1}) = e$，故 $b^{-1}a^{-1}$ 是 ab 的逆元.

根据逆元的惟一性等式得证.

8.1 群的定义及其性质

说明:

(3) (4) (5) 的证明：

用数学归纳法证明对于自然数 n 和 m 证等式为真，

然后讨论 n 或 m 为负数的情况.

(2) 中的结果可以推广到有限多个元素的情况，即

$$(x_1x_2\dots x_n)^{-1} = x_n^{-1}x_{n-1}^{-1}\dots x_2^{-1}x_1^{-1}$$

等式 (5) 只对交换群成立. 如果 G 是非交换群，那么

$$(xy)^n = \underbrace{(xy)(xy)\dots(xy)}_{n\text{个}}$$

8.1 群的定义及其性质

定理 8.2 G 为群，则 G 中适合消去律，即对任意 $a,b,c \in G$ 有

(1) 若 $ab=ac$ ，则 $b=c$.

(2) 若 $ba=ca$ ，则 $b=c$.

证 (1) $ab=ac \Rightarrow a^{-1}(ab)=a^{-1}(ac)$

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

$\Rightarrow b=c$

(2) 同理可证.

8.1 群的定义及其性质

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

$$a_iG=\{a_ia_j|j=1,2,\ldots,n\}$$

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

$$a_ia_j=a_ia_k \quad (j\neq k)$$

由消去律得 $a_j=a_k$, 与 $|G|=n$ 矛盾 .

置换： 设 S 是一个非空集合，从集合 S 到 S 的一个双射称为 S 的一个置换。

8.1 群的定义及其性质

有限群 G 的运算表中每行、每列都是 G 的置换.

$aG=G$ 和 $Ga=G$

运算表的行列构成置换的不一定是群，反例：

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

定理 8.3 设 G 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 ）

（2）$|a^{-1}| = |a|$

证 (1) 充分性．由 $r|k$ ，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．根据带余除法，存在整数 m 和 i 使得

$$k = mr+i,\ 0 \le i \le r-1$$

从而有 $e = a^k = a^{mr+i} = (a^r)^m a^i = ea^i = a^i$

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

(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 a *的阶也是* a^{-1} 的阶的因子，即 $r \mid t$.

从而证明了 $r = t$ ，即 $|a^{-1}|=|a|$.

8.1 群的定义及其性质

群方程存在惟一解 G 为群，$\forall\, a,b \in G$，方程 $ax=b$ 和 $ya=b$ 在 G 中有解且仅有惟一解.

证 $a^{-1}b$ 代入方程左边的 x 得

$$a\,(a^{-1}b) = (a\,a^{-1})\,b = eb = b$$

所以 $a^{-1}b$ 是该方程的解. 下面证明唯一性.

假设 c 是方程 $ax = b$ 的解，必有 $ac = b$，从而有

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

同理可证 ba^{-1} 是方程 $ya = b$ 的唯一解.

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

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

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

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

8.1 群的定义及其性质

例 设 G 是群，$a,b\in G$ 是有限阶元. 证明

（1）$|b^{-1}ab| = |a|$

（2）$|ab| = |ba|$

证（1）设 $|a| = r$，$|b^{-1}ab| = t$，则有

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

从而有 $t\,|r$.

另一方面，由 $a = (b^{-1})^{-1}(b^{-1}ab)b^{-1}$

可知 $r \mid t$. 从而有 $|b^{-1}ab| = |a|$.

（2）设 $|ab| = r$，$|ba| = t$，则有

$$(ab)^{t+1} = a(ba)^t b = ab$$

由消去律得 $(ab)^t = e$，从而可知，$r \mid t$.

同理可证 $t \mid r$. 因此 $|ab| = |ba|$.

8.1 群的定义及其性质

例 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 设 $|ab|=d$. 由 $ab=ba$ 可知

$$(ab)^{nm}=(a^n)^m(b^m)^n=e^me^n=e$$

从而有 $d\mid nm$.

又由 $a^db^d=(ab)^d=e$ 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 $|a^d|\mid n$. 同理有 $|b^d|\mid m$. 从而知道 $|a^d|$ 是 n 和 m 的公因子.

因为 n 与 m 互质，所以 $|a^d|=1$. 这就证明了 $a^d=e$, 从而 $n\mid d$.

同理可证 $m\mid d$，即 d 是 n 和 m 的公倍数. 由于 n 与 m 互质，必有 $nm|d$.

综合前边的结果得 $d=nm$. 即 $|ab|=nm$.

8.1 群的定义及其性质

四、有关群性质的证明题

1 ）有关群性质的简单证明题的主要类型：

证明群中的元素相等，这里的元素通常是若干元素运算的结果.

证明群中的子集相等.

证明与元素的阶相关的命题.

证明群的其它简单命题，如交换性等.

8.1 群的定义及其性质

2 ）证明方法：

证明群中元素相等的基本方法就是用结合律、消去律、单位元及逆元的惟一性、群的幂运算规则等，对等式进行变形和化简．

证明子集相等的基本方法就是证明两个子集相互包含．

证明与元素的阶相关的命题，如证明阶相等，阶整除等．证明两个元素的阶 r 和 s 相等或证明某个元素的阶等于 r ，基本方法是证明相互整除．在证明中可以使用结合律、消去律、幂运算规则以及关于元素的阶的性质．

8.1 群的定义及其性质

3）常用的证明手段或工具是：

算律：结合律、消去律

和特殊元素相关的等式，如单位元、逆元等

幂运算规则

和元素的阶相关的性质．

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

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

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

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

若 $(n,m)=1, \quad |ab|=nm$

8.1 群的定义及其性质

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

证 $\forall x, y \in G$, $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$

分析： $x^2 = e \Leftrightarrow x = x^{-1}$,

幂运算规则

例 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 2 阶元为 x, $\forall y \in G$,

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

分析： $|yxy^{-1}| = |x|$

8.1 群的定义及其性质

例 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，总数有偶数个.

G 中 1 阶和 2 阶元也有偶数个.由于 1 阶元只有单位元，因此 2 阶元有奇数个，从而命题得证.

分析：$|x|=|x^{-1}|$,

$$x^2=e \Leftrightarrow x=x^{-1}$$

8.1 群的定义及其性质

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

证 令$|a^t|=s$,

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

只要证 $s=q$

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

$s|q$

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

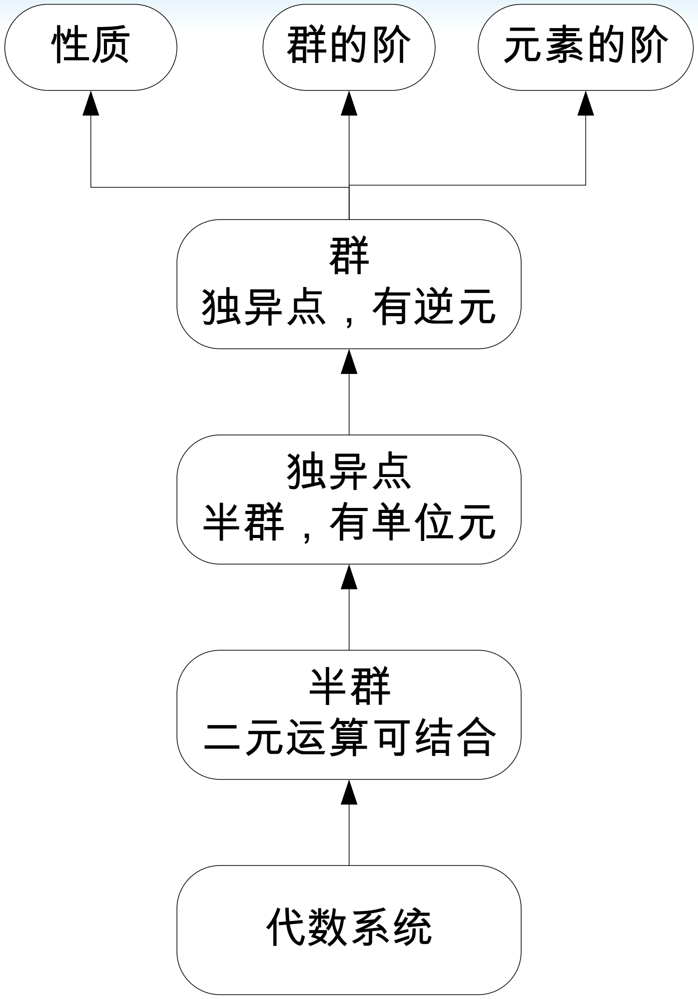
$q|s$ （p,q 互素）

分析：相互整除

$|a|=r$, $a^k=e$ 当且仅当 $r|k$

小结

- 集合和该集合上的一个适合结合律的二元运算构成的代数系统称为**半群**。半群中如果含有单位元素（幺元）则构成**独异点**。每个元素都可逆的独异点构成**群**。



作业

- 补充习题 8.1

1. 设 $V=\langle\{a, b\}, *\rangle$ 是半群，且 $a*a=b$，求证

(1) $a*b=b*a$;

(2) $b*b=b$.

2. 设 Z 为整数集合，在 Z 上定义二元运算*如下：

$\forall x, y \in Z, \ x*y=x+y-2$

问 Z 关于*能否构成群？为什么？