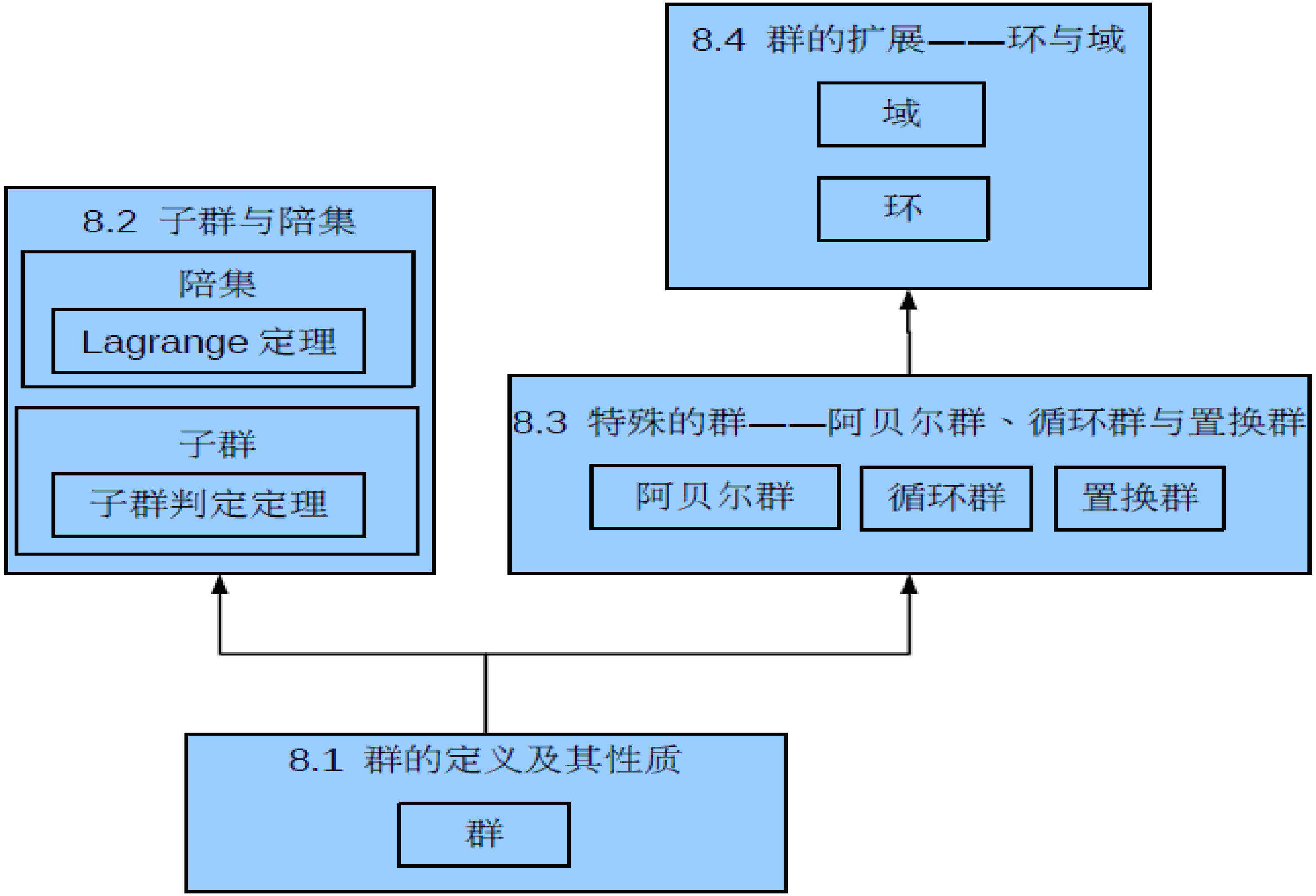
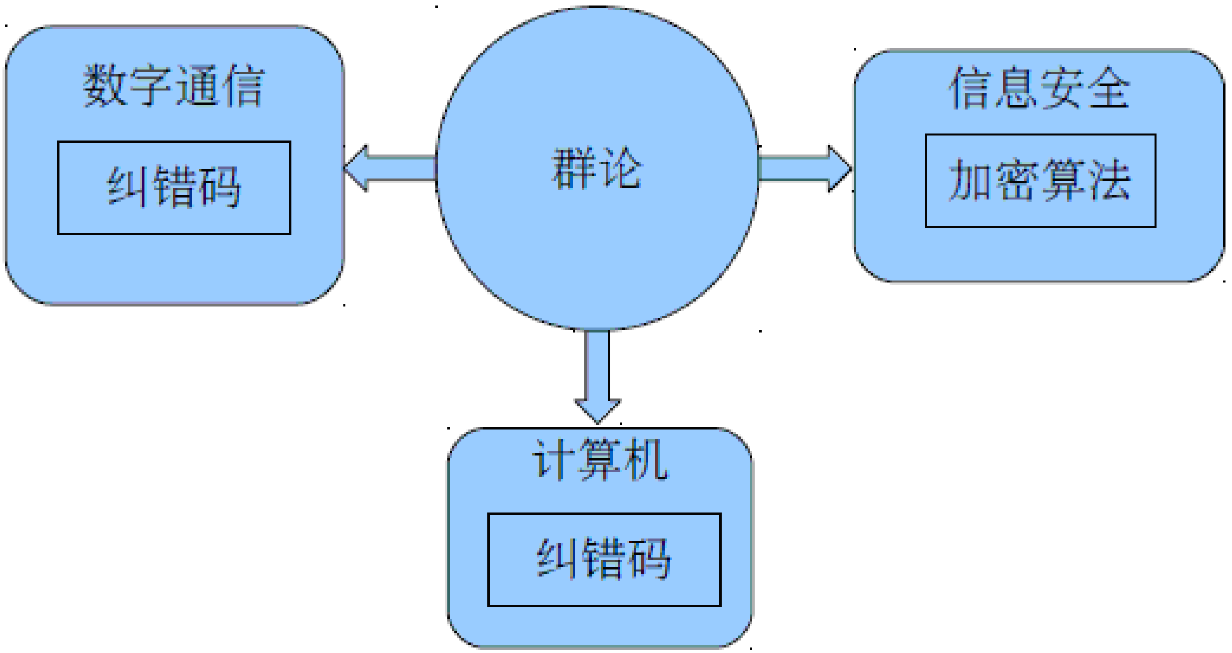
第八章群论初步

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$V=\langle S, \circ\rangle$是代数系统，$\circ$为二元运算，如果$\circ$运算是可结合的，则称$V$为半群。

- 设$\langle G, \bullet\rangle$为一半群,那么$\langle G, \bullet\rangle$的任一子代数都是半群，称为$\langle G, \bullet\rangle$的子半群。

(2) 设$V=\langle S, \circ\rangle$是半群，若$e\in S$是关于$\circ$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$V=\langle S, \circ, e\rangle$.

- 若独异点$\langle S, \circ, e\rangle$的子代数含有幺元$e$，那么它必为一独异点，称为$\langle S, \circ, e\rangle$的子独异点。

(3) 设$V=\langle S, \circ\rangle$是独异点，$e\in S$是关于$\circ$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, ∘>	V=<S, ∘>	V=<S, ∘, e>	G

8.1 群的定义及其性质

实例1：和数集相关的半群、独异点和群

❖ 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(法)群、有理数加(法)群、实数加(法)群、复数加(法)群。

8.1 群的定义及其性质

实例2

❖ 半群

$<M_n(R), +>$, $<M_n(R), \times>$, 其中n是大于1的正整数

❖ 独异点

$<M_n(R), +>$, $<M_n(R), \times>$

❖ 群

$<M_n(R), +>$

$<M_n(R), \times>$不是群, 不是每个n阶矩阵都有乘法逆元

这里，+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

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

8.1 群的定义及其性质

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

8.1 群的定义及其性质

练习1

- 设<R*, ∘>为代数系统, 其中R*为非零实数集合,

  ∘运算定义如下：$\forall x, y \in \mathrm{R}^*, x \circ y = y$

(1) 半群?

(2) 独异点?

(3) 群?

8.1 群的定义及其性质

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，它恰好也是抽象代数系统—独异点的一个实例。

8.1 群的定义及其性质

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: <G, ∘>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$x\circ y=z=z_1z_2\ldots z_7$.

$z_5=x_5\oplus y_5$.

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

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$x\circ y=z\in G$, 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, ⊕ >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,⊕>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$n/(x, n)$确定，其中(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

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

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中运算适合消去律，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 $G=\{a_1, a_2, \cdots, a_n\}$ 是 n 阶群，任给$a_i \in G$，令

$$a_iG=\{a_ia_j \mid j=1, 2, \cdots, n\}$$

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

8.1 群的定义及其性质

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$t \mid r$.

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

(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　$s = q$

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

$s|q$

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

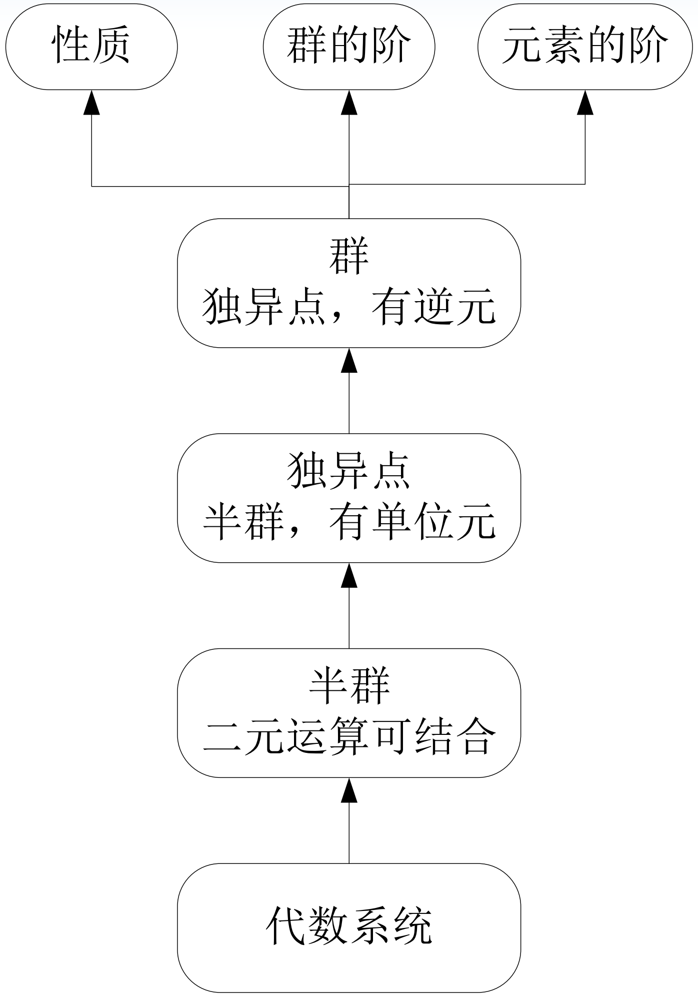
$q|s$　（p, q 互素）

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。



复习

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　$s=q$

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

$s|q$

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

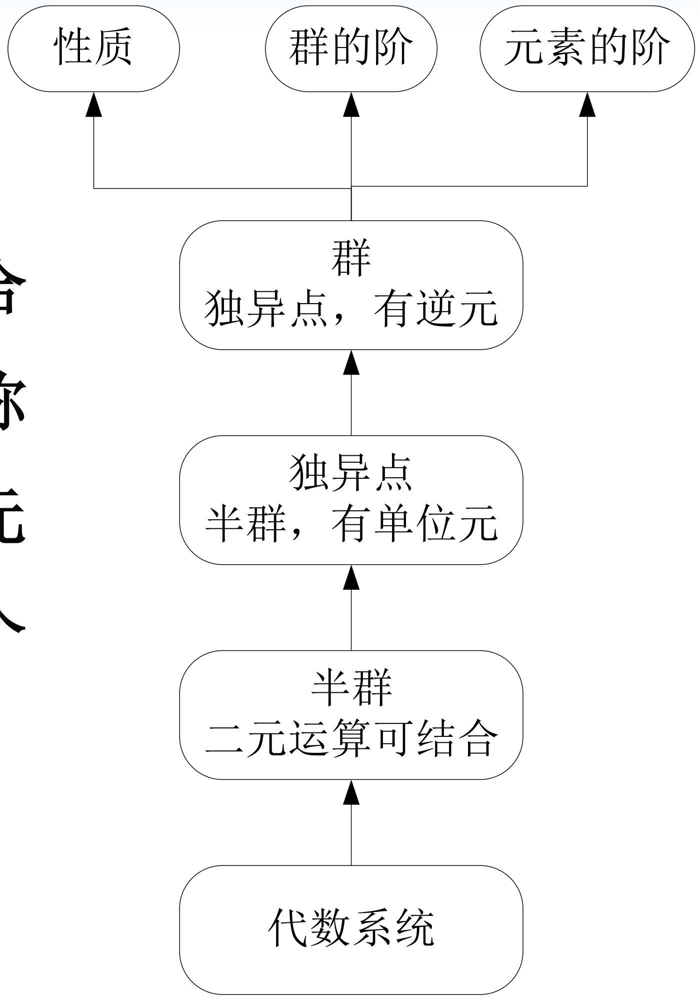
$q|s$　（p, q 互素）

分析：相互整除

$|a|=r, a^k=e$ 当且仅当 $r|k$

复习

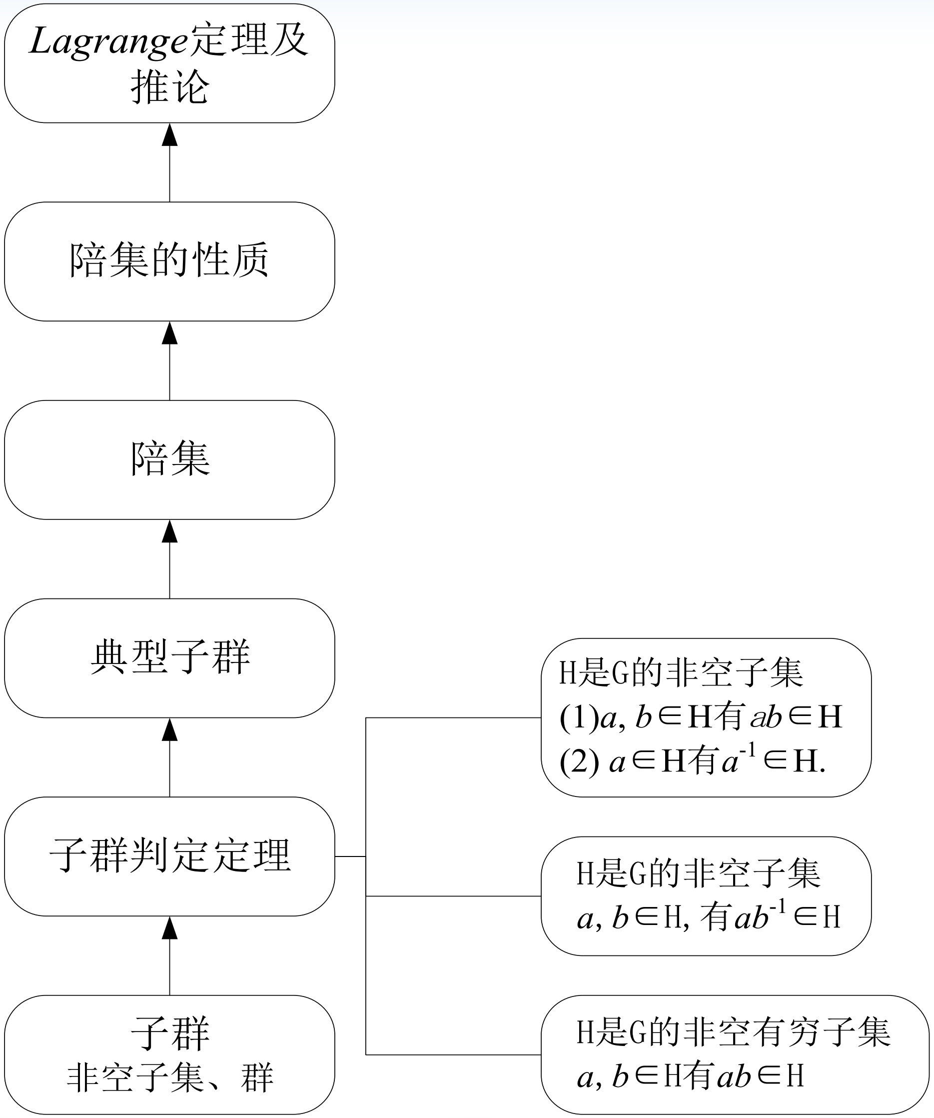
- 集合和该集合上的一个适合结合律的二元运算构成的代数系统称为半群。半群中如果含有单位元素（幺元）则构成独异点。每个元素都可逆的独异点构成群。



8.2 子群与陪集

子群与群的关系：拉格朗日定理。

8.2 子群与陪集


*Lagrange*定理及推论
陪集的性质
陪集
典型子群
子群判定定理
子群
非空子集、群
H是G的非空子集
(1)$a, b \in H$有$ab \in H$
(2) $a \in H$有$a^{-1} \in H$.
H是G的非空子集
$a, b \in H$, 有$ab^{-1} \in H$
H是G的非空有穷子集
$a, b \in H$有$ab \in H$

8.2 子群与陪集

子群定义

定义8.5 设G是群，H是G的非空子集，

(1) 如果H关于G中的运算构成群，则称H是G的子群，记作$H \le G$.

(2) 若H是G的子群，且$H \subset G$，则称H是G的真子群，记作$H < G$.

例如 nZ (n是自然数) 是整数加群<Z,+> 的子群. 当$n \neq 1$时, nZ是Z的真子群.

任何群G都存在子群. G和$\{e\}$都是G的子群，称为G的平凡子群.

8.2 子群与陪集

定理8.5（子群判定定理1）

设G为群，H是G的非空子集，则H是G的子群当且仅当

(1) $\forall a,b\in H$有$ab\in H$

(2) $\forall a\in H$有$a^{-1}\in H$.

证 必要性是显然的.

为证明充分性，只需证明$e\in H$.

因为H非空，存在$a\in H$. 由条件(2) 知$a^{-1}\in H$，根据条件(1) $aa^{-1}\in H$，即$e\in H$.

8.2 子群与陪集

定理8.6 （子群判定定理2 ）

设G为群，H是G的非空子集. H是G的子群当且仅当$\forall a, b \in H$, 有$ab^{-1} \in H$.

证　必要性显然.

只证充分性. 因为H非空，必存在$a \in H$.

根据给定条件得$aa^{-1} \in H$，即$e \in H$.

任取$a \in H$, 由$e, a \in H$ 得 $ea^{-1} \in H$，即$a^{-1} \in H$.

任取$a,b \in H$，知$b^{-1} \in H$. 再利用给定条件得$a(b^{-1})^{-1} \in H$，即 $ab \in H$.

综合上述，可知H是G的子群.

8.2 子群与陪集

定理8.7 （子群判定定理3 ）

设G为群，H是G的非空有穷子集，则H是G的子群当且仅当$\forall a,b\in H$有$ab\in H$.

证 必要性显然.

为证充分性，只需证明 $a\in H$有$a^{-1}\in H$.

任取$a\in H$, 若$a = e$, 则$a^{-1} = e\in H$.

若$a\neq e$，令$S=\{a,a^2,\ldots\}$，则$S\subseteq H$.

由于H是有穷集，必有$a^i = a^j$（$i<j$）.

根据G中的消去律得 $a^{j-i} = e$，由$a \neq e$可知 $j-i>1$，由此得

$$a^{j-i-1}a = e \text{ 和 } a\, a^{j-i-1} = e$$

从而证明了$a^{-1} = a^{j-i-1}\in H$.

根据子群判定定理1，可知H是G的子群。

8.2 子群与陪集

典型子群的实例:生成子群

定义8.6 设G为群，$a\in G$，令$H=\{a^k \mid k\in Z\}$，

则H是G的子群，称为由 a 生成的子群，记作$\langle a\rangle$.

证 首先由$a\in\langle a\rangle$知道$\langle a\rangle\neq\varnothing$. 任取$a^m, a^l\in\langle a\rangle$，则

$$a^m(a^l)^{-1} = a^m a^{-l} = a^{m-l}\in\langle a\rangle$$

根据判定定理二可知$\langle a\rangle\leq G$.

实例：

例如整数加群，由2生成的子群是 $\langle 2\rangle=\{2^k \mid k\in Z\}=2Z$

$\langle Z_6, \oplus\rangle$中，由2生成的子群$\langle 2\rangle=\{0, 2, 4\}$

Klein四元群 $G = \{e, a, b, c\}$的所有生成子群是：

$\langle e\rangle=\{e\}$, $\langle a\rangle=\{e, a\}$, $\langle b\rangle=\{e, b\}$, $\langle c\rangle=\{e, c\}$.

8.2 子群与陪集

典型子群的实例:中心C

定义8.7 设G为群,令

$$C=\{a \mid a\in G\wedge\forall x\in G(ax=xa)\},$$

则C是G的子群，称为G的中心.

证 $e\in C$. C是G的非空子集. 任取$a,b\in C$，只需证明ab^{-1}与G中所有的元素都可交换. $\forall x\in G$，有

$$(ab^{-1})x = ab^{-1}x = ab^{-1}(x^{-1})^{-1}$$

$$= a(x^{-1}b)^{-1} = a(bx^{-1})^{-1} = a(xb^{-1})$$

$$= (ax)b^{-1} = (xa)b^{-1} = x(ab^{-1})$$

由判定定理二可知$C\le G$.

对于阿贝尔群G，因为G中所有的元素互相都可交换，G的中心就等于G. 但是对某些非交换群G，它的中心是$\{e\}$.

8.2 子群与陪集

典型子群的实例:子群的交

例6 设G是群，H, K是G的子群. 证明

(1) $H\cap K$也是G的子群

(2) $H\cup K$是G的子群当且仅当 $H\subseteq K$ 或 $K\subseteq H$

证 (1) 由 $e\in H\cap K$ 知 $H\cap K$ 非空.

任取$a, b\in H\cap K$，则$a\in H, a\in K, b\in H, b\in K$.

必有$ab^{-1}\in H$ 和 $ab^{-1}\in K$，从而$ab^{-1}\in H\cap K$. 因此$H\cap K\leq G$.

(2) 充分性显然，只证必要性. 用反证法.

假设 $H\nsubseteq K$ 且$K\nsubseteq H$，那么存在 h 和 k 使得

$$h\in H\wedge h\notin K,\quad k\in K\wedge k\notin H$$

推出 $hk\notin H$. 否则由$h^{-1}\in H$ 得 $k=h^{-1}(hk)\in H$，与假设矛盾.

同理可证 $hk\notin K$. 从而得到 $hk\notin H\cup K$. 与$H\cup K$是子群矛盾.

8.2 子群与陪集

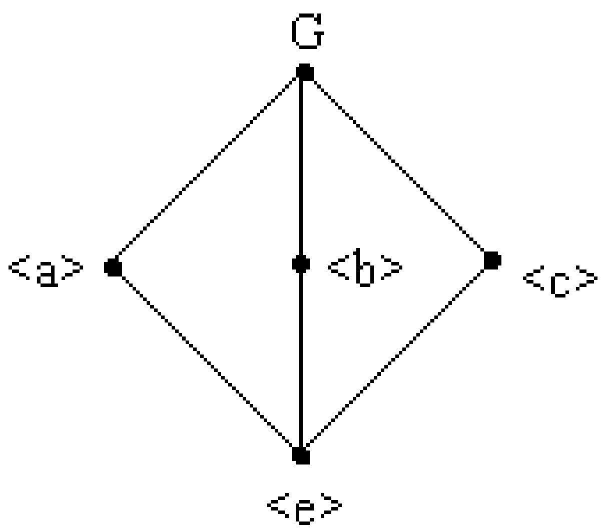
子群格*

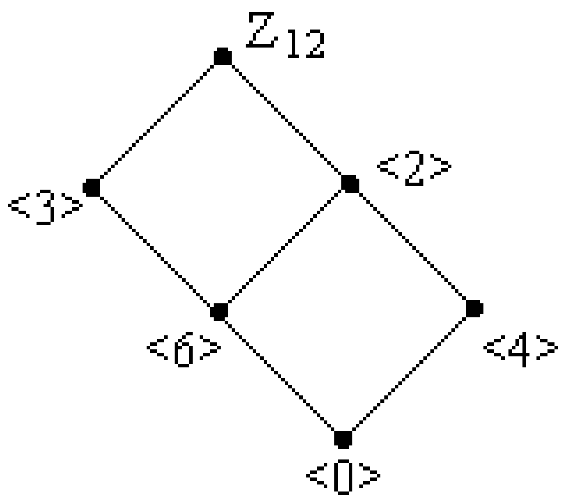
定义8.8 设G为群, 令

$$L(G) = \{H \mid H\text{是}G\text{的子群}\}$$

则偏序集$< L(G), \subseteq >$称为G的**子群格**

实例：Klein四元群的子群格 模12加群Z_{12}





8.2 子群与陪集

陪集定义与实例

定义8.9 设H是G的子群，$a\in G$.令

$$Ha=\{ha \mid h\in H\}$$

称Ha是子群H在G中的右陪集. 称a为Ha的代表元素.

例7 (1) 设$G=\{e, a, b, c\}$是Klein四元群，$H=\langle a\rangle$是G的子群.

H所有的右陪集是:

$$He=\{e, a\}=H,\ Ha=\{a, e\}=H,\ Hb=\{b, c\},\ Hc=\{c, b\}$$

不同的右陪集只有两个，即H和$\{b, c\}$.

8.2 子群与陪集

例7(续)

(2) 设$A=\{1,2,3\}$，$f_1, f_2, \ldots, f_6$是A上的双射函数. 其中

$$f_1=\{\langle 1,1\rangle,\langle 2,2\rangle,\langle 3,3\rangle\}，\quad f_2=\{\langle 1,2\rangle,\langle 2,1\rangle,\langle 3,3\rangle\}$$

$$f_3=\{\langle 1,3\rangle,\langle 2,2\rangle,\langle 3,1\rangle\}，\quad f_4=\{\langle 1,1\rangle,\langle 2,3\rangle,\langle 3,2\rangle\}$$

$$f_5=\{\langle 1,2\rangle,\langle 2,3\rangle,\langle 3,1\rangle\}，\quad f_6=\{\langle 1,3\rangle,\langle 2,1\rangle,\langle 3,2\rangle\}$$

令 $G = \{f_1, f_2, \ldots , f_6\}$，则$G$ 关于函数的复合运算构成群. 考虑 G 的子群$H=\{f_1, f_2\}$. 做出 H 的全体右陪集如下：

$$Hf_1=\{f_1\circ f_1, f_2\circ f_1\}=H\,,\quad Hf_2=\{f_1\circ f_2, f_2\circ f_2\}=H$$

$$Hf_3=\{f_1\circ f_3, f_2\circ f_3\}=\{f_3, f_5\},\quad Hf_5=\{f_1\circ f_5, f_2\circ f_5\}=\{f_5, f_3\}$$

$$Hf_4=\{f_1\circ f_4, f_2\circ f_4\}=\{f_4, f_6\},\quad Hf_6=\{f_1\circ f_6, f_2\circ f_6\}=\{f_6, f_4\}$$

结论： $Hf_1=Hf_2$，$Hf_3=Hf_5$，$Hf_4=Hf_6$.

8.2 子群与陪集

陪集的基本性质

定理8.8 设H是群G的子群，则

(1) $He = H$

(2) $\forall a \in G$ 有$a \in Ha$

证 (1) $He = \{ he \mid h \in H \} = \{ h \mid h \in H \} = H$

(2) 任取 $a \in G$，由$e \in H$，$a = ea$ 和 $ea \in Ha$ 得 $a \in Ha$

8.2 子群与陪集

定理8.9 设H是群G的子群，则$\forall a,b\in G$有

$$a\in Hb \Leftrightarrow ab^{-1}\in H \Leftrightarrow Ha=Hb$$

证 先证$a\in Hb \Leftrightarrow ab^{-1}\in H$

$$a\in Hb \Leftrightarrow \exists h(h\in H\wedge a=hb)$$

$$\Leftrightarrow \exists h(h\in H\wedge ab^{-1}=h) \Leftrightarrow ab^{-1}\in H$$

再证 $a\in Hb \Leftrightarrow Ha=Hb$.

充分性. 若$Ha=Hb$，由$a\in Ha$ 可知必有 $a\in Hb$.

必要性. 由 $a\in Hb$ 可知存在 $h\in H$ 使得 $a=hb$，即$b=h^{-1}a$

任取 $h_1a\in Ha$，则有

$$h_1a = h_1(hb) = (h_1h)b\in Hb$$

从而得到 $Ha\subseteq Hb$. 反之，任取$h_1b\in Hb$，则有

$$h_1b = h_1(h^{-1}a) = (h_1h^{-1})a\in Ha$$

从而得到$Hb\subseteq Ha$. 综合上述，$Ha=Hb$得证.

8.2 子群与陪集

定理8.10 设H是群G的子群，在G上定义二元关系R：

$$\forall a,b\in G, <a,b>\in R \Leftrightarrow ab^{-1}\in H$$

则 R是G上的等价关系，且$[a]_R = Ha$.

证 先证明R为G上的等价关系.

自反性. 任取$a\in G$，$aa^{-1} = e\in H \Leftrightarrow <a,a>\in R$

对称性. 任取$a,b\in G$，则

$$<a,b>\in R\Rightarrow ab^{-1}\in H\Rightarrow(ab^{-1})^{-1}\in H\Rightarrow ba^{-1}\in H\Rightarrow<b,a>\in R$$

传递性. 任取$a,b,c\in G$，则

$$<a,b>\in R\wedge<b,c>\in R \Rightarrow ab^{-1}\in H\wedge bc^{-1}\in H$$

$$\Rightarrow ac^{-1}\in H \Rightarrow <a,c>\in R$$

下面证明：$\forall a\in G$，$[a]_R = Ha$. 任取$b\in G$，

$$b\in[a]_R \Leftrightarrow <a,b>\in R \Leftrightarrow ab^{-1}\in H \Leftrightarrow Ha=Hb \Leftrightarrow b\in Ha$$

8.2 子群与陪集

推论 设H是群G的子群, 则

(1) $\forall a,b \in G$，$Ha = Hb$ 或 $Ha \cap Hb = \varnothing$

(2) $\cup \{Ha \mid a \in G\} = G$

证明：由等价类性质可得.

由以上定理和推论可知，H的所有右陪集的集合恰好构成G的一个划分。

定理8.11 设H是群G的子群，则

$\forall a \in G$，$H \approx Ha$ （两集合等势，存在从H到Ha的双射函数 ）

证明 略

8.2 子群与陪集

左陪集的定义与性质

设G是群，H是G的子群，H 的左陪集，即

$$aH = \{ah \mid h \in H\}，a \in G$$

关于左陪集有下述性质：

(1) $eH = H$

(2) $\forall a \in G$，$a \in aH$

(3) $\forall a,b \in G$，$a \in bH \Leftrightarrow b^{-1}a \in H \Leftrightarrow aH=bH$

(4) 若在G上定义二元关系R，

$$\forall a,b \in G，\langle a,b \rangle \in R \Leftrightarrow b^{-1}a \in H$$

则R是G上的等价关系，且$[a]_R = aH$.

(5) $\forall a \in G$，$H \approx aH$

8.2 子群与陪集

*Lagrange*定理

定理8.12 （*Lagrange*）设G是有限群，H是G的子群，则

$$|G| = |H|\cdot[G:H]$$

其中$[G:H]$ 是H在G中的不同右陪集(或左陪集) 数，称为H在G 中的**指数**.

证 设$[G:H] = r$，$a_1,a_2,\ldots,a_r$分别是H 的r个右陪集的代表元素，由定理8.10推论，可知

$$G = Ha_1 \cup Ha_2 \cup \ldots \cup Ha_r$$
$$|G| = |Ha_1| + |Ha_2| + \ldots + |Ha_r|$$

由$|Ha_i| = |H|$，$i = 1,2,\ldots,r$, 得

$$|G| = |H|\cdot r = |H|\cdot[G:H]$$

8.2 子群与陪集

*Lagrange*定理推论

推论1 设G是n阶群，则$\forall a\in G$，$|a|$是n的因子，且有$a^n = e$.

证 任取$a\in G$，$\lt a\gt$是G的子群，由*Lagrange*定理知，$\lt a\gt$的阶是n的因子.

$\lt a\gt$是由a生成的子群，若$|a| = r$，则

$$\lt a\gt = \{a^0=e,a^1,a^2,\ldots,a^{r-1}\}$$

即$\lt a\gt$的阶与$|a|$相等, 所以$|a|$是n的因子. 从而$a^n = e$.

推论2 对阶为素数的群G，必存在$a\in G$使得$G = \lt a\gt$.

证 设$|G| = p$，p是素数. 由$p\geq 2$知G中必存在非单位元.

任取$a\in G$，$a\neq e$，则$\lt a\gt$是G的子群. 根据拉格朗日定理，

$\lt a\gt$的阶是p的因子，即$\lt a\gt$的阶是 p或1. 显然$\lt a\gt$的阶不是1，

这就推出$G = \lt a\gt$.

8.2 子群与陪集

*Lagrange*定理的应用

例8 证明 6 阶群中必含有 3 阶元.

证 设G是6 阶群，则G中元素只能是1阶、2阶、3阶或6阶.

若G中含有6 阶元，设为a，则 a^2是3 阶元.

若G中不含6 阶元，下面证明G中必含有3阶元.

如若不然，G中只含1阶和2阶元，即$\forall a \in G$，有$a^2=e$，由前面的结论知G是Abel群.

取G中2阶元 a 和 b，$a \neq b$，令 $H = \{e, a, b, ab\}$，则H 是 G 的子群，但 $|H| = 4$，$|G| = 6$，与拉格朗日定理矛盾.

8.2 子群与陪集

例9 证明阶小于6 的群都是Abel群.

证 1 阶群是平凡的，显然是阿贝尔群.

2, 3和5都是素数，由推论2它们都是单元素生成的群，都是Abel群.

设G是4阶群. 若G中含有4阶元，比如说a，则

G=<a>

由上述分析可知G是Abel群.

若G中不含4阶元，G中只含1阶和2阶元，可知G也是Abel群.

8.2 子群与陪集

- 典型子群的实例:正规子群
- 设G是群，H是G的子群(H $\leq$G), 若H的左陪集与右陪集总是相等（对任何的$a\in$G，aH=Ha）， 则称H是G的正规子群或不变子群，记为H$\trianglelefteq$G。
- 正规子群相关结论:
  - G的平凡子群H={e}和G都是G的正规子群
  - 交换群的任意子群是正规子群

8.2 子群与陪集

- 正规子群相关结论(正规子群的判定定理1):
  - H是G的正规子群的充分必要条件是：对任意的$h \in$H和$g \in$G，都有$g^{-1}hg \in$ H
  - 必要性证明
    - H是G的正规子群，则对任意$g \in$G都有gH=Hg，及对任意的$h \in$H都有$gh \in g$H且$gh \in$ Hg, $hg \in g$H, 可得$g^{-1}hg \in$ H
  - 充分性证明(证gH = Hg):
    - 对任意$g \in$G，如果a $\in g$H，则存在$h \in$H，使得gh=a;又$g \in$G，则$g^{-1} \in$G, 由$g^{-1}hg \in$H，那么$ghg^{-1} \in$ H，即$gh \in$ Hg, 即$a \in$ Hg，即gH $\subseteq$ Hg
    - 同理可证 H$g \subseteq g$H

8.2 子群与陪集

- 正规子群相关结论(正规子群的判定定理2):
  - H是G的正规子群的充分必要条件是：对G中任意元素a，都有$aHa^{-1}=H$
  - 必要性的证明
    - 对任意$x \in aHa^{-1}$，那么一定存在$h \in H$使得$aha^{-1}=x$, 那么$xa = aha^{-1}a = ah \in aH$, 即$xa \in aH$, 又$H \trianglelefteq G$，故$xa \in Ha$，故$x \in H$，即$aHa^{-1} \subseteq H$
    - 若$x \in H$，则$xa \in Ha$，又$H \trianglelefteq G$，故$xa \in aH$，则存在$h \in H$使得$xa=ah$，即$h=a^{-1}xa \in H$,则$x=a(a^{-1}xa)a^{-1} \in aHa^{-1}$,即$H \subseteq aHa^{-1}$
  - 充分性的证明
    - 见下页

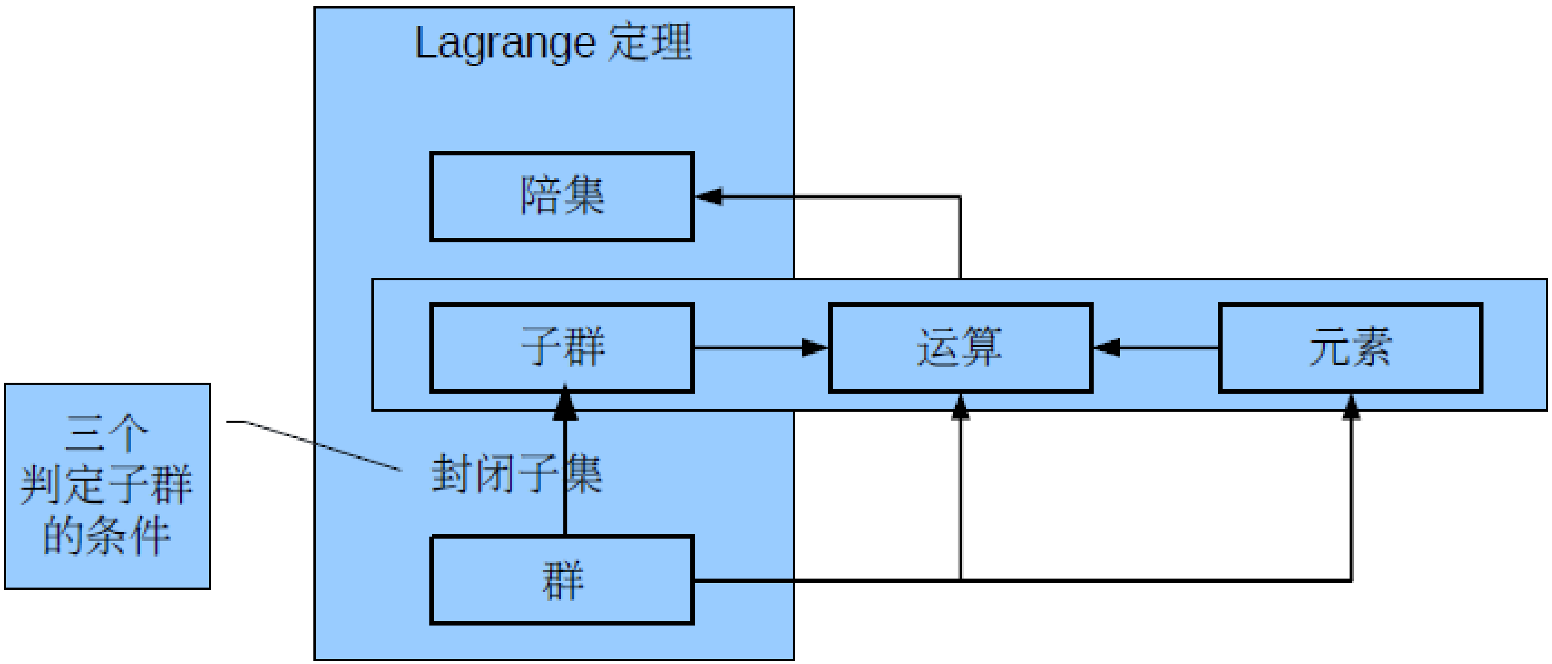
8.2 子群与陪集

- 正规子群相关结论(正规子群的判定定理2):
  - H是G的正规子群的充分必要条件是：对G中任意元素a，都有$aHa^{-1}=H$
  - 充分性的证明
    - 设a为G中任意元素
    - 任取$x\in aH$，则存在$h\in H$使$x=ah$，此时$xa^{-1}\in aHa^{-1}$，又$aHa^{-1}=H$，则$xa^{-1}\in H$，显然$xa^{-1}a\in Ha$，即$x\in Ha$，$aH\subseteq Ha$
    - 同理可证$Ha\subseteq aH$
    - 综上可得$Ha=aH$
    - 又a为G中任意元素，故$H\trianglelefteq G$
- 注：H是G的子群，则对G中任意元素a，$aHa^{-1}=\{aha^{-1}\mid h\in H\}$都是G的子群，称为G的**共轭子群**。

小结

- 群的一个子集和该群上的运算如果能够构成一个群，则称这个群为该群的子群。
- 判定一个群是否是另一个群的子群有三种方法，其中有一种仅适用于有限群。
- 一个群的子群和这个群当中的元素进行运算后得到该子群的陪集。
- *Lagrange*定理揭示了群、子群、陪集之间的关系。

小结



上节复习

*Lagrange*定理及推论

陪集的性质

陪集

典型子群

子群判定定理

子群
非空子集、群

H是G的非空子集
(1)$a, b \in \mathrm{H}$有$ab \in \mathrm{H}$
(2) $a \in \mathrm{H}$有$a^{-1} \in \mathrm{H}$.

H是G的非空子集
$a, b \in \mathrm{H}$, 有$ab^{-1} \in \mathrm{H}$

H是G的非空有穷子集
$a, b \in \mathrm{H}$有$ab \in \mathrm{H}$

8.3 特殊的群——阿贝尔群、循环群和置换群

阿贝尔群、循环群、置换群：各种不同的群。

8.3 特殊的群——阿贝尔群、循环群和置换群

- 什么是阿贝尔群
  - 若群<G, •>的运算•适合交换律，则称<G, •>为阿贝尔群（Abelian Group）或交换群。
- 在一个阿贝尔群<G, •>中，一个乘积可以任意颠倒因子的次序而求其值。
- 在阿贝尔群中，易见有如下指数律成立
  - $(a\bullet b)^m=a^m\bullet b^m$，$m$为任意整数

知识回顾

生成子群

设G为群, $a \in G$,

$$< a > = \{ a^k \mid k \in Z \}$$

即a的所有的幂构成的集合, 为G的子群, 称为由a生成的子群.

8.3 特殊的群——阿贝尔群、循环群和置换群

循环群的定义

定义8.10 设G是群，若存在$a \in G$使得

$$G=\{a^k \mid k \in Z\}$$

则称G是循环群，记作$G=\langle a\rangle$，称 a 为G 的生成元.

循环群的分类：n 阶循环群和无限循环群.

设$G=\langle a\rangle$是循环群，若a是n 阶元，则

$$G = \{ a^0=e, a^1, a^2, \ldots , a^{n-1} \}$$

那么$|G| = n$，称 G 为 n 阶循环群.

若a 是无限阶元，则

$$G = \{ a^0=e, a^{\pm 1}, a^{\pm 2}, \ldots \}$$

称 G 为无限循环群.

实例：$<Z,+>$为无限循环群

$<Zn,\oplus>$为n阶循环群

8.3 特殊的群——阿贝尔群、循环群和置换群

循环群的生成元

定理8.13 设G=<a>是循环群.

(1) 若G是无限循环群，则G只有两个生成元，即a和a^{-1}.

(2) 若G是 n 阶循环群，则G含有$\phi(n)$个生成元. 对于任何小于n且与n互质的数$r\in\{0,1,\ldots,n-1\}$, a^r是G的生成元.

$\phi(n)$称为欧拉函数，例如 n=12，小于或等于12且与12互素的正整数有4个：

1, 5, 7, 11

所以$\phi(12)=4$.

8.3 特殊的群——阿贝尔群、循环群和置换群

定理8.13 设$G=\langle a\rangle$是循环群.

(1) 若G是无限循环群，则G只有两个生成元，即a和a^{-1}.

证 (1) 显然$\langle a^{-1}\rangle\subseteq G$. $\forall a^k\in G$,

$$a^k=(a^{-1})^{-k}\in\langle a^{-1}\rangle,$$

因此$G\subseteq\langle a^{-1}\rangle$，$a^{-1}$是$G$的生成元.

再证明G只有a和a^{-1}这两个生成元. 假设 b 也是G 的生成元,

则 $G=\langle b\rangle$. 由$a\in G$ 可知存在整数 t 使得$a = b^t$. 由$b\in G = \langle a\rangle$

知存在整数 m 使得 $b = a^m$. 从而得到 $a = b^t = (a^m)^t = a^{mt}$

由G中的消去律得 $a^{mt-1} = e$

因为G是无限群，必有$mt-1 = 0$. 从而证明了$m = t = 1$或 $m = t = -1$,

即 $b = a$ 或 $b = a^{-1}$

8.3 特殊的群——阿贝尔群、循环群和置换群

定理8.13 设G=<a>是循环群.

(2) 若G是 n 阶循环群，则G含有$\phi(n)$个生成元. 对于任何小于n且与 n 互质的数$r\in\{0,1,\ldots,n-1\}$, a^r是G的生成元.

(2) 只须证明：对任何正整数 r ($r\le n$)，

$$a^r\text{是}G\text{的生成元}\Leftrightarrow n\text{与}r\text{互质}.$$

充分性. 设r与n互质，且$r\le n$，那么存在整数 u 和 v 使得

$$ur + vn = 1$$

从而 $a = a^{ur+vn} = (a^r)^u(a^n)^v = (a^r)^u$

这就推出$\forall a^k\in G$，$a^k = (a^r)^{uk}\in$<a^r>，即$G\subseteq$<a^r>.

另一方面，显然有<a^r>$\subseteq G$. 从而G = <a^r>.

必要性. 设a^r是G的生成元，则 $|a^r| = n$. 又因为$|a| = n$， $|a^r|$ = n/(n, r) ，所以(n, r)=1

8.3 特殊的群——阿贝尔群、循环群和置换群

实例

例10

(1) 设$G=\{e, a, \ldots, a^{11}\}$是12阶循环群，则$\phi(12)=4$.

小于12且与12互素的数是1, 5, 7, 11, 由定理8.13可知 a, a^5, a^7 和 a^{11}是G的生成元.

(2) 设$G=\langle Z_9,\oplus\rangle$是模9的整数加群，则$\phi(9)=6$.

小于9且与9互素的数是 1, 2, 4, 5, 7, 8. 根据定理8.13，G的生成元是1, 2, 4, 5, 7和8.

(3) 设$G=3Z=\{3z \mid z\in Z\}$, G上的运算是普通加法. 那么G只有两个生成元：3和-3.

8.3 特殊的群——阿贝尔群、循环群和置换群

循环群的子群

定理8.14 设$G=<a>$是循环群.

(1) G的子群仍是循环群.

(2) 若$G=<a>$是无限循环群，则G的子群除$\{e\}$以外都是无限循环群.

(3) 若$G=<a>$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.

8.3 特殊的群——阿贝尔群、循环群和置换群

定理8.14 设$G=<a>$是循环群.

(1) G的子群仍是循环群.

证 (1) 设H是$G=<a>$的子群，若$H=\{e\}$，显然H是循环群，

否则取H中的最小正方幂元a^m，下面证明$H=<a^m>$.

易见$<a^m>\subseteq H$.

下面证明$H\subseteq<a^m>$.

为此，只需证明H中任何元素都可表成a^m的整数次幂.

任取$a^l\in H$，由除法可知存在整数 q 和 r，使得

$$l = qm+r，\quad 其中\ 0\le r\le m-1$$

$$a^r = a^{l-qm} = a^l(a^m)^{-q}$$

由$a^l, a^m\in H$ 且 H 是G 的子群可知$a^r\in H$.

因为a^m是H中最小正方幂元，必有$r = 0$. 这就推出$a^l = (a^m)^q\in<a^m>$

定理8.14 设G=<a>是循环群.

(2) 若G=<a>是无限循环群，则G的子群除{e}以外都是无限循环群.

(2) 设G=<a>是无限循环群，H是G的子群.

若H≠{e}可知H =<a^m>，其中a^m为H中最小正方幂元.

假若 |H|=t，则 |a^m|=t，从而得到$a^{mt} = e$. 这与a为无限阶元矛盾.

定理8.14 设G=<a>是循环群.

(3) 若G=<a>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.

(3) 设G=<a>是 n 阶循环群，则 $G = \{ a^0=e, a^1, \ldots , a^{n-1} \}$

下面证明对于n的每个正因子d都存在一个d阶子群.

易见 $H = \langle a^{n/d} \rangle$ 是G的d 阶子群.

假设$H_1=\langle a^m \rangle$也是G的d 阶子群，其中 a^m 为 H_1中的最小正方幂元. 则由 $(a^m)^d = e$

可知 n 整除md，即 n/d 整除 m.

令$m = (n/d)\cdot l$，l是整数，则有 $a^m = (a^{n/d})^l \in H$

这就推出$H_1 \subseteq H$. 又由于 $|H_1| = |H| = d$，得$H_1 = H$.

8.3 特殊的群——阿贝尔群、循环群和置换群

实例

例11

(1) G=<Z,+>是无限循环群，其生成元为1和–1.

对于自然数 $m\in N$，1的m次幂是m，m生成的子群是mZ，$m\in$N. 即

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

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

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

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 $\langle 1\rangle=\mathrm{Z}_{12}$

练习

设G=<a>是15阶循环群。

1）求出G的所有生成元；

2）求出G的所有子群

8.3 特殊的群——阿贝尔群、循环群和置换群

n 元置换及乘法

定义8.11 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8.12 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

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

8.3 特殊的群——阿贝尔群、循环群和置换群

k阶轮换

定义8.13 设σ是S = {1, 2, …, n}上的n元置换,若$\sigma(i_1)=i_2$, $\sigma(i_2)=i_3$, …, $\sigma(i_{k-1})=i_k$, $\sigma(i_k)=i_1$, 且保持S中的其他元素不变, 则称σ为S上的**k阶轮换**, 记为$(i_1, i_2, \ldots, i_k)$.

若k=2, 则称σ为S上的**对换**.

8.3 特殊的群——阿贝尔群、循环群和置换群

n元置换的轮换表示

设 $S = \{1, 2, \ldots, n\}$，对于任何S上的 n 元置换 σ, 存在着一个有限序列 $i_1, i_2, \ldots, i_k$, $k\geq 1$, (可以取$i_1=1$) 使得

$$\sigma(i_1) = i_2, \sigma(i_2) = i_3, \ldots, \sigma(i_{k-1}) = i_k, \sigma(i_k) = i_1$$

令 $\sigma_1 = (i_1\ i_2 \ldots i_k)$, 是 σ 分解的第一个轮换. 将 σ 写作 $\sigma_1\sigma'$,

继续对 σ' 分解. 由于S 只有n 个元素, 经过有限步得到

$$\sigma = \sigma_1\sigma_2 \ldots \sigma_t$$

轮换分解式的特征

轮换的不交性（以上任何两个轮换都作用于不同的元素上）

分解的惟一性：若 $\sigma = \sigma_1\sigma_2 \ldots \sigma_t$ 和 $\sigma = \tau_1\tau_2 \ldots \tau_s$是σ的两个轮换表示式，则有

$$\{\sigma_1, \sigma_2, \ldots, \sigma_t\} = \{\tau_1, \tau_2, \ldots, \tau_s\}$$

8.3 特殊的群——阿贝尔群、循环群和置换群

实例

例12 设$S = \{1, 2, \ldots, 8\}$,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 3 & 6 & 4 & 2 & 1 & 8 & 7 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 4 & 2 & 6 & 7 & 5 & 3 \end{pmatrix}$$

则 轮换分解式为:

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

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

8.3 特殊的群——阿贝尔群、循环群和置换群

置换的对换分解

设$S = \{1,2,\ldots,n\}$，$\sigma = (i_1\ i_2\ \ldots\ i_k)$ 是S上的 k 阶轮换， σ可以进一步表成对换之积，即

$$(i_1\ i_2\ \ldots\ i_k) = (i_1\ i_2)\ (i_1\ i_3)\ \ldots\ (i_1\ i_k)$$

任何n元置换表成轮换之积，然后将每个轮换表成对换之积.

例如 8 元置换

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

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

8.3 特殊的群——阿贝尔群、循环群和置换群

对换分解的特征

对换分解式中对换之间可以有交，分解式也不惟一.

例如4元置换

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

可以有下面不同的对换表示：

$\sigma=(1\ 2)\ (1\ 3)$， $\sigma=(1\ 4)\ (2\ 4)\ (3\ 4)\ (1\ 4)$

表示式中所含对换个数的奇偶性是不变的.

如果n元置换σ可以表示成奇数个对换之积，则称σ为奇置换，否则称为偶置换，不难证明奇置换和偶置换各有$n!/2$个.

8.3 特殊的群——阿贝尔群、循环群和置换群

n元置换群

所有的 n元置换构成的集合S_n关于置换乘法构成群， 称为n元对称群. 其中恒等置换是它的单位元（又称幺置换）。n元对称群的子群称为n元置换群。

例13 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) }

	(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)

8.3 特殊的群——阿贝尔群、循环群和置换群

S_n的子群

设A_n是所有的n元偶置换的集合. 则A_n是S_n的子群， 称为n元交错群。

证 恒等置换(1) 是偶置换，所以A_n非空.

根据判定定理三，只需证明封闭性：

任取$\sigma,\tau\in A_n$， σ, τ都可以表成偶数个对换之积，那么$\sigma\tau$

也可以表成偶数个对换之积，所以$\sigma\tau\in A_n$.

实例：S_3的子群格

S_3={(1), (12), (13), (23),

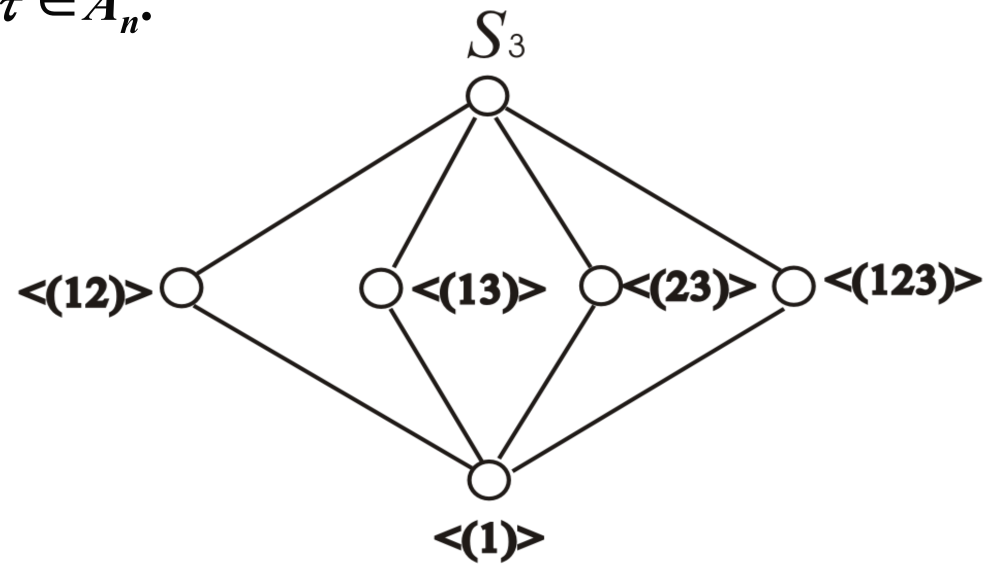
(123), (132)},

A_3={(1), (123), (132)},

{(1)},

{(1), (12)}, {(1), (13)},

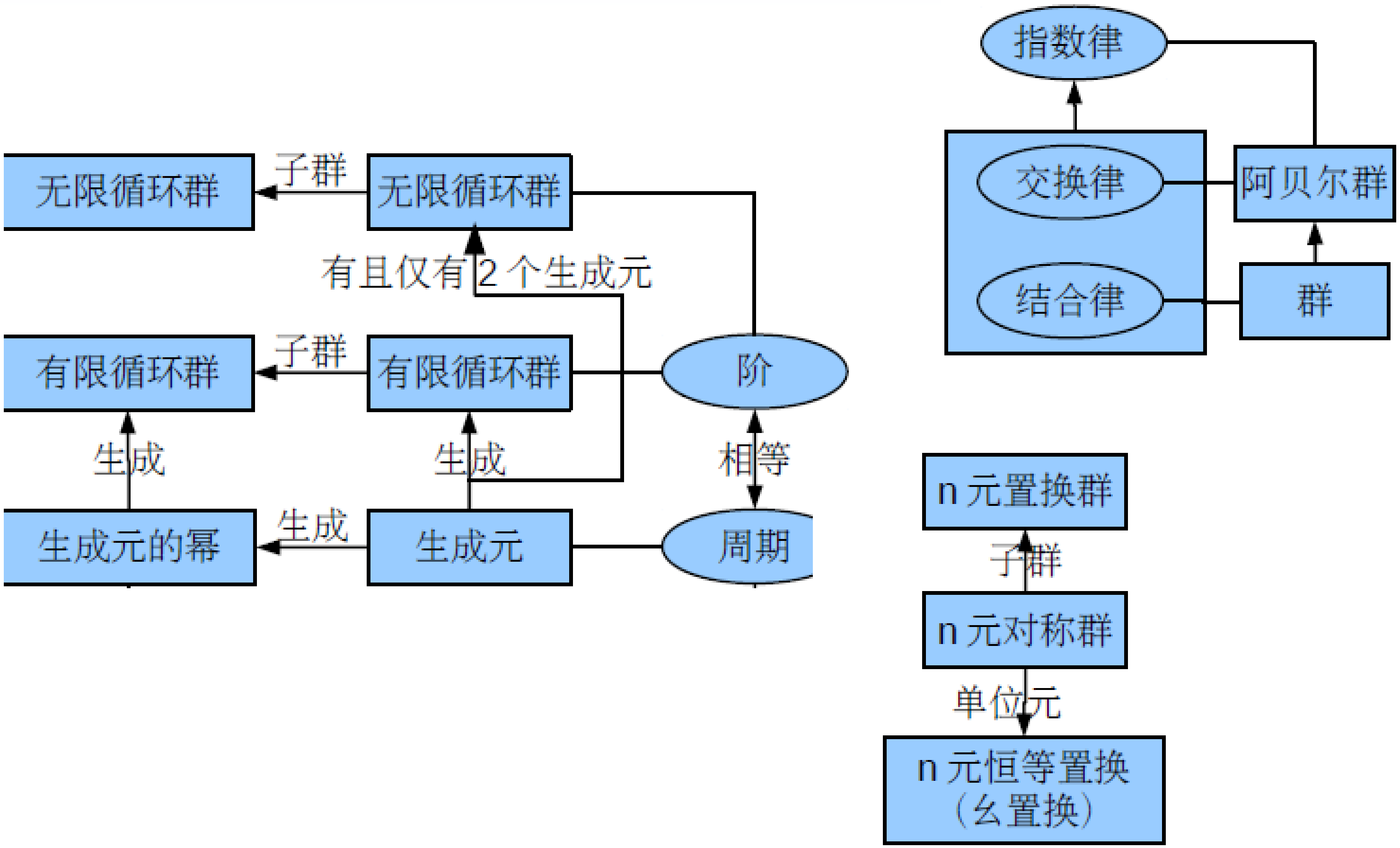
{(1), (23)}.



小结

- 适合交换律的群称为阿贝尔群，阿贝尔群适合指数律。
- 由一个元素的幂构成的群称为循环群，循环群中各元素的的阶是循环群的重要性质。
- 由n元置换的集合和置换的复合构成的群称为n元置换群，特别地，由全部n元置换构成的群称为n元对称群。

小结


无限循环群
子群
无限循环群
有且仅有 2 个生成元
有限循环群
子群
有限循环群
阶
生成
生成
相等
生成元的幂
生成
生成元
周期
指数律
交换律
阿贝尔群
结合律
群
n 元置换群
子群
n 元对称群
单位元
n 元恒等置换
（幺置换）

8.4 群的扩展——环与域

环、域：群扩展后得到的具有两个运算的代数系统。

8.4 群的扩展——环与域

环定义

定义8.13 设<R,+,·>是代数系统，+和·是二元运算. 如果满足以下条件:

(1) <R,+>构成交换群

(2) <R,·>构成半群

(3) · 运算关于+运算适合分配律

则称<R,+,·>是一个环.

通常称+运算为环中的加法，·运算为环中的乘法.

环中加法单位元记作 0，乘法单位元（如果存在）记作1.

对任何元素 x，称 x 的加法逆元为负元，记作$-x$.

若 x 存在乘法逆元的话，则称之为逆元，记作x^{-1}.

8.4 群的扩展——环与域

环的实例

例14

(1) 整数集、有理数集、实数集和复数集关于普通的加法和乘法构成环，分别称为整数环Z，有理数环Q，实数环R和复数环C.

(2) $n(n\geq 2)$阶实矩阵的集合$M_n(\mathrm{R})$关于矩阵的加法和乘法构成环，称为 n 阶实矩阵环.

(3) 集合的幂集$P(B)$关于集合的对称差运算和交运算构成环.

(4) 设$\mathrm{Z}_n=\{0,1, \ldots , n-1\}$，$\oplus$和$\otimes$分别表示模$n$的加法和乘法，则$<\mathrm{Z}_n,\oplus,\otimes>$构成环，称为模 n的整数环.

8.4 群的扩展——环与域

环的运算性质

定理8.15 设 $<R,+,\cdot>$ 是环，则

(1) $\forall a \in R$，$a0 = 0a = 0$

(2) $\forall a,b \in R$，$(-a)b = a(-b) = -ab$

(3) $\forall a,b,c \in R$，$a(b-c) = ab-ac$， $(b-c)a = ba-ca$

(4) $\forall a_1,a_2,\ldots,a_n,b_1,b_2,\ldots,b_m \in R$ $(n,m \geq 2)$

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$$

8.4 群的扩展——环与域

实例

例15 在环中计算$(a+b)^3$, $(a-b)^2$

解 $(a+b)^3 = (a+b)(a+b)(a+b)$

$= (a^2+ba+ab+b^2)(a+b)$

$=a^3+ba^2+aba+b^2a+a^2b+bab+ab^2+b^3$

$(a-b)^2 = (a-b)(a-b) = a^2-ba-ab+b^2$

8.4 群的扩展——环与域

特殊的环

定义8.14 设<R,+,·>是环

(1) 若环中乘法 · 适合交换律，则称R是交换环

(2) 若环中乘法 · 存在单位元，则称R是含幺环

(3) 若$\forall a,b\in R$，$ab=0 \Rightarrow a=0\lor b=0$，则称$R$是无零因子环

(4) 若R既是交换环、含幺环、无零因子环，则称R是整环

(5) 设R是整环，且R中至少含有两个元素. 若$\forall a\in R^*$，其中$R^*=R-\{0\}$，都有$a^{-1}\in R$，则称R是域.

8.4 群的扩展——环与域

实例

例16

(1) 整数环Z、有理数环Q、实数环R、复数环C都是交换环,含幺环,无零因子环和整环. 除了整数环以外都是域.

(2) 令$2Z=\{2z \mid z\in Z\}$，则$<2Z,+,\cdot>$构成交换环和无零因子环. 但不是含幺环和整环.

(3) 设$n\in Z$, $n\geq 2$, 则n阶实矩阵的集合$M_n(R)$关于矩阵加法和乘法构成环，它是含幺环，但不是交换环和无零因子环，也不是整环.

(4) $<Z_6,\oplus,\otimes>$构成环，它是交换环, 含幺环, 但不是无零因子环和整环.
$2\otimes 3=3\otimes 2=0$，2和3是零因子.

注意：对于一般的n, Zn是整环当且仅当n是素数.

8.4 群的扩展——环与域

实例

例17 设 p为素数，证明Z_p是域.

证　p为素数，所以 $|Z_p|\geq 2$. 易见Z_p关于模p乘法可交换，单位元是1

对于任意的 $i, j\in Z_p$, $i\neq 0$有

$$i\otimes j=0\Rightarrow p \text{ 整除 } ij\Rightarrow p|j\Rightarrow j=0$$

所以 Z_p 中无零因子，Z_p为整环.

Z_p关于乘法⊗构成有限半群，且Z_p关于⊗适合消去律。

下面证明每个非零元素关于模p乘法都有逆元. 任取 $i\in Z_p$，$i\neq 0$，令

$$i\otimes Z_p=\{\, i\otimes j\mid j\in Z_p\}$$

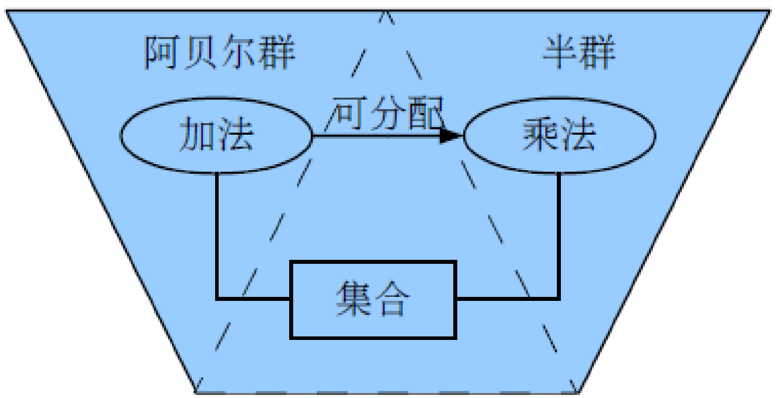
则 $i\otimes Z_p=Z_p$，否则$\exists j, k\in Z_p$，使得 $i\otimes j=i\otimes k$，由消去律得 $j=k$.

由$1\in Z_p$，存在 $j\in Z_p$，使得 $i\otimes j=1$. 由于交换性可知 j 就是i 的逆元.

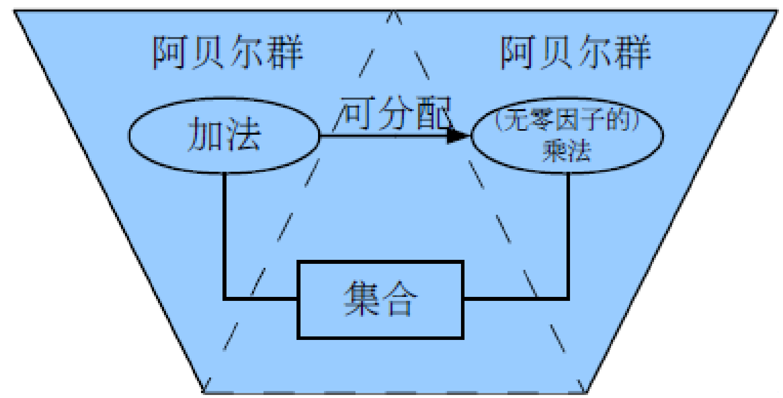
小结

- 在群的基础上进行扩展而具有两个运算后，得到一些新的代数系统。
- 环和域就是这样的两个代数系统，而环又是特殊的域。
- 扩展后，两个运算分别要满足一些条件，两个运算之间也要具有特定的关系——可分配。

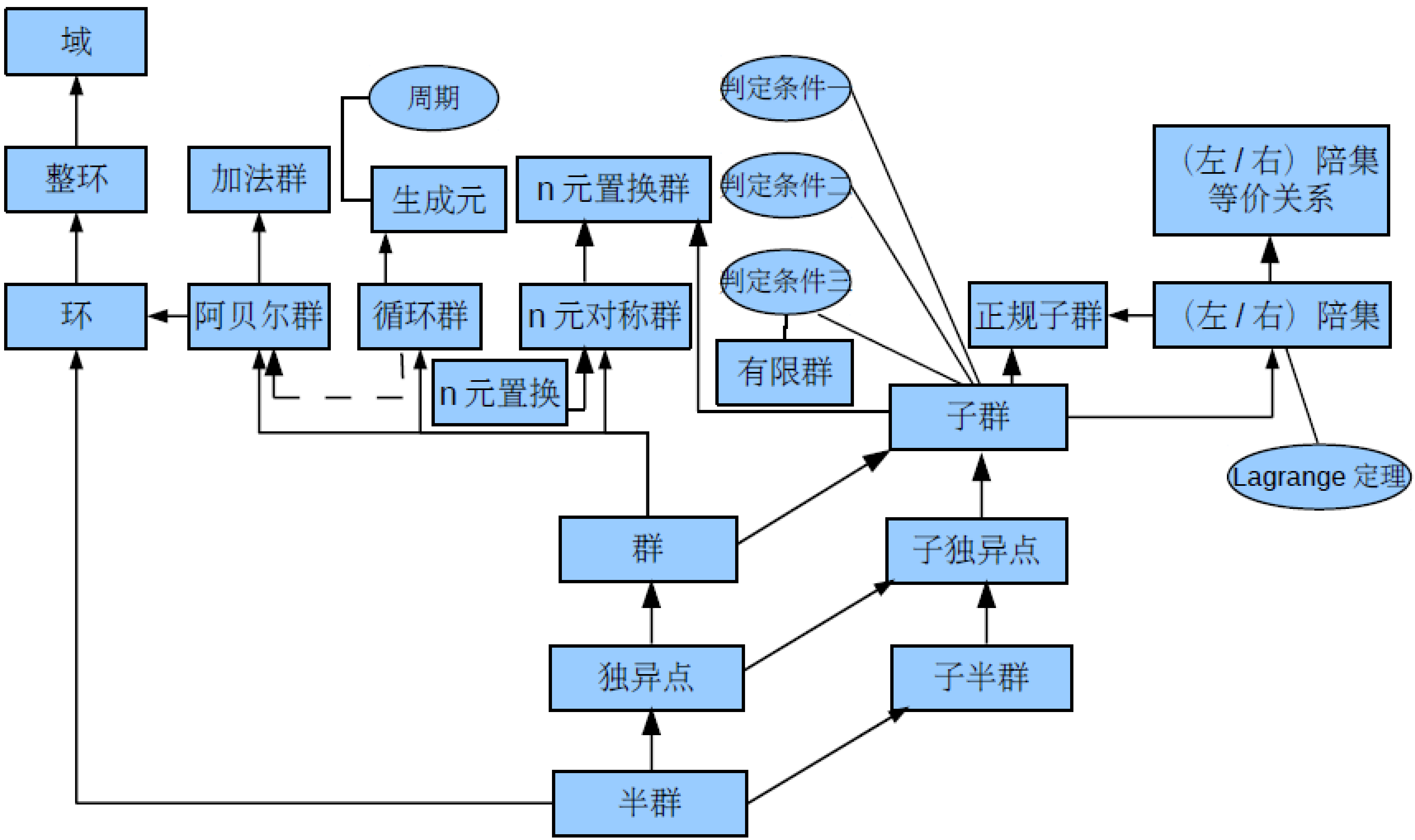
环



域



本章小结


域
周期
判定条件一
整环
加法群
生成元
n 元置换群
判定条件二
（左 / 右）陪集
等价关系
判定条件三
环
阿贝尔群
循环群
n 元对称群
正规子群
（左 / 右）陪集
有限群
n 元置换
子群
Lagrange 定理
群
子独异点
独异点
子半群
半群

常见题型

- 判断或证明给定集合和运算是否构成半群、独异点和群、环、域
- 求群中元素的阶、元素的幂、子群的陪集等
- 群中简单性质和子群的证明
- 拉格朗日定理的应用
- 求循环群的生成元及其子群

举例

设群G的运算表如表所示，问G是否为循环群？如果是，求出它所有的生成元和子群.

	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	d	e	f	a
c	c	d	e	f	a	b
d	d	e	f	a	b	c
e	e	f	a	b	c	d
f	f	a	b	c	d	e

解

易见 a 为单位元.

由于$|G|=6$, $|b|=6$, 所以 b 为生成元.

$G=\langle b\rangle$为循环群. $|f|=6$, 因而 f 也是生成元

$|c|=3$, $|d|=2$, $|e|=3$, 因此 c,d, e不是生成元.

子群：$\langle a\rangle=\{a\}$, $\langle c\rangle=\{c, e, a\}$,

$\langle d\rangle=\{d, a\}$, G .

举例

设Z_{18} 为模18整数加群, 求所有元素的阶.

解:

|0| = 1,　　|9| = 2，　　|6| = |12| = 3,　　|3| = |15| = 6,

|2| = |4| = |8| = |10| = |14| = |16| = 9,

|1| = |5| = |7| = |11| = |13| = |17| =18,

- 说明:
- 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.（可能所有元素的阶都存在，但是群还是无限群）.

有关群性质的证明方法

- 有关群的简单证明题的主要类型
  - 证明群中的元素某些运算结果相等
  - 证明群中的子集相等
  - 证明与元素的阶相关的命题.
  - 证明群的其它性质，如交换性等.
- 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. 特别地，a为1阶或2阶元的充分必要条件是$a^{-1}= a$.

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. 特别地，可能用到a为1阶或2阶元的充分必要条件是$a^{-1} = a$.

举例

设G为群，a是G中的2 阶元，证明G中与a可交换的元素构成G的子群.

证　令$H = \{ x \mid x \in G \wedge xa = ax \}$, 下面证明$H$是$G$的子群.

首先e属于H，H是G的非空子集.

任取$x, y \in H$，有

$$(xy^{-1})\, a = x(y^{-1}a\,) = x(a^{-1}y)^{-1} = x(ay)^{-1}$$

$$= x(ya)^{-1} = xa^{-1}y^{-1} = xay^{-1} = axy^{-1} = a(xy^{-1})$$

因此 xy^{-1}属于H. 由判定定理命题得证.

- 分析：
  - 证明子群可以用判定定理，特别是判定定理二.
- 证明的步骤是：
  - 验证 H 非空
  - 任取 $x, y \in H$，证明$xy^{-1} \in H$

举例

(1) 设G为模12加群, 求<3> 在G中所有的左陪集

(2) 设 $X=\{x \mid x\in\mathrm{R}, x\neq 0,1\}$, 在$X$上如下定义6个函数:

$f_1(x)=x$， $f_2(x)=1/x$， $f_3(x)=1-x$，

$f_4(x)=1/(1-x)$， $f_5(x)=(x-1)/x$， $f_6(x)=x/(x-1)$，

则$G=\{f_1,f_2,f_3,f_4,f_5,f_6\}$关于函数合成运算构成群. 求子群

$H=\{f_1,f_2\}$ 的所有的右陪集.

解 (1) $\langle 3\rangle=\{0, 3, 6, 9\}$, <3>的不同左陪集有3个，即

$0+\langle 3\rangle=\langle 3\rangle$,

$1+\langle 3\rangle=4+\langle 3\rangle=7+\langle 3\rangle=10+\langle 3\rangle=\{1, 4, 7, 10\}$,

$2+\langle 3\rangle=5+\langle 3\rangle=8+\langle 3\rangle=11+\langle 3\rangle=\{2, 5, 8, 11\}$.

(2) $\{f_1,f_2\}$有3个不同的陪集，它们是:

H，$Hf_3=\{f_3,f_5\}$，$Hf_4=\{f_4,f_6\}$.

举例

设 H_1,H_2分别是群G 的 r, s 阶子群，若$(r,s) = 1$，证明$H_1 \cap H_2 = \{e\}$.

证 $H_1 \cap H_2 \leq H_1$，$H_1 \cap H_2 \leq H_2$. 由*Lagrange*定理，$|H_1 \cap H_2|$ 整除r，也整除s. 从而 $|H_1 \cap H_2|$ 整除 r与s 的最大公因子. 因为$(r,s) = 1$, 从而 $|H_1 \cap H_2|$ $= 1$. 即 $H_1 \cap H_2 = \{e\}$.

- 某些有用的数量结果：设a是群G元素，C为G的中心
- $N(a)=\{ x \mid x \in G, xa=ax \}$,
- $|C|$ 是 $|N(a)|$ 和 $|G|$ 的因子，$|a|$ 是 $|N(a)|$ 和 $|G|$ 的因子
- $|H| = |xHx^{-1}|$
- $|a^n|$ 是 $|a|$ 的因子
- $a^2=e \Leftrightarrow a=a^{-1} \Leftrightarrow |a|=1,2$