第十章 群与环

主要内容

- 群的定义与性质
- 子群与群的陪集分解
- 循环群与置换群
- 环与域

10.1 群的定义与性质

- 半群、独异点与群的定义
- 半群、独异点、群的实例
- 群中的术语
- 群的基本性质

半群、独异点与群的定义

定义10.1

(1) 设$V=<S,\circ>$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.

(2) 设$V=<S,\circ>$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$V=<S,\circ,e>$.

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

实例

例1

(1) $<Z^+,+>$,$<N,+>$,$<Z,+>$,$<Q,+>$,$<R,+>$都是半群，+是普通加法. 这些半群中除$<Z^+,+>$外都是独异点

(2) 设n是大于1的正整数，$<M_n(R),+>$和$<M_n(R),\cdot>$都是半群，也都是独异点，其中+和·分别表示矩阵加法和矩阵乘法

(3) $<P(B),\oplus>$为半群，也是独异点，其中$\oplus$为集合对称差运算

(4) $<Z_n, \oplus>$为半群，也是独异点，其中$Z_n=\{0,1,\ldots,n-1\}$，$\oplus$为模n加法

实例

例2 设$G=\{e, a, b, c\}$，G上的运算由下表给出，称为**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

特征：

1. 满足交换律
2. 每个元素都是自己的逆元
3. a, b, c中任何两个元素运算结果都等于剩下的第三个元素

有关群的术语

定义10.2 (1) 若群G是有穷集，则称G是有限群，否则称为无限群. 群G 的基数称为群 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.

Klein四元群是4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.

群中元素的幂

定义10.3 设G是群，$a \in G$，$n \in Z$，则a 的 n次幂.

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

群中元素可以定义负整数次幂.

在$<Z_3, \oplus>$中有

$$2^{-3} = (2-1)^3 = 1^3 = 1 \oplus 1 \oplus 1 = 0$$

在$<Z, +>$中有

$$(-2)^{-3} = 2^3 = 2+2+2 = 6$$

元素的阶

定义10.4 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，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.

例如，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.

群的性质：幂运算规则

定理10.1 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) $\forall a \in G$，$a^n a^m = a^{n+m}$，$n, m \in \mathbf{Z}$

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

(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. 根据逆元唯一性，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. 根据逆元的唯一性等式得证.

群的性质：方程存在惟一解

定理10.2 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

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

所以$a^{-1}b$ 是该方程的解. 下面证明惟一性.

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 $ya=b$的惟一解.

例3 设群$G=<P(\{a,b\}),\oplus>$，其中$\oplus$为对称差. 解下列群方程：

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

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

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

群的性质：消去律

定理10.3 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 $b = c$.

证明略

群的性质：元素的阶

定理10.4 G为群，$a \in G$且 $|a| = r$. 设k是整数，则

(1) $a^k = e$当且仅当$r \mid k$

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

实例

例 5 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

$$(b^{-1}ab)^r = \underbrace{(b^{-1}ab)(b^{-1}ab)\ldots(b^{-1}ab)}_{r\text{个}}$$

$$= b^{-1}a^r b = b^{-1}eb = e$$

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 $|b^{-1}ab| = |a|$.

实例

(2) 设 $|ab| = r$，$|ba| = t$，则有

$$(ab)^{t+1} = \underbrace{(ab)(ab)...(ab)}_{t+1个}$$

$$= a\underbrace{(ba)(ba)...(ba)}_{t个}b$$

$$= a(ba)^t b = aeb = ab$$

由消去律得 $(ab)^t = e$，从而可知，$r \mid t$.

同理可证 $t \mid r$. 因此 $|ab| = |ba|$.

10.2 子群与群的陪集分解

定义10.5 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$H \leq G$.

(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.

对任何群G都存在子群. G和$\{e\}$都是G的子群，称为G的平凡子群.

子群判定定理1

定理10.5（判定定理一）

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$e \in H$.

子群判定定理2

定理10.6 （判定定理二）

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.

子群判定定理3

定理10.7 （判定定理三）

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$a^{-1}=a^{j-i-1}\in H$.

典型子群的实例:生成子群

定义10.6 设G为群，$a\in G$，令$H=\{a^k \mid k\in \mathbf{Z}\}$，
则H是G的子群，称为由 a 生成的子群，记作$<a>$.

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

$$a^m(a^l)^{-1}=a^m a^{-l}=a^{m-l}\in<a>$$

根据判定定理二可知$<a>\leq G$.

实例：
例如整数加群，由2生成的子群是 $<2>=\{2^k \mid k\in \mathbf{Z}\}=2\mathbf{Z}$
$<\mathbf{Z}_6,\oplus>$中，由2生成的子群$<2>=\{0,2,4\}$
Klein四元群 $G=\{e,a,b,c\}$的所有生成子群是：

$$<e>=\{e\},\ <a>=\{e,a\},\ <b>=\{e,b\},\ <c>=\{e,c\}.$$

典型子群的实例:中心C

定义10.7 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$C\leq G$.

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$\{e\}$.

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 $K \subseteq H$

子群格

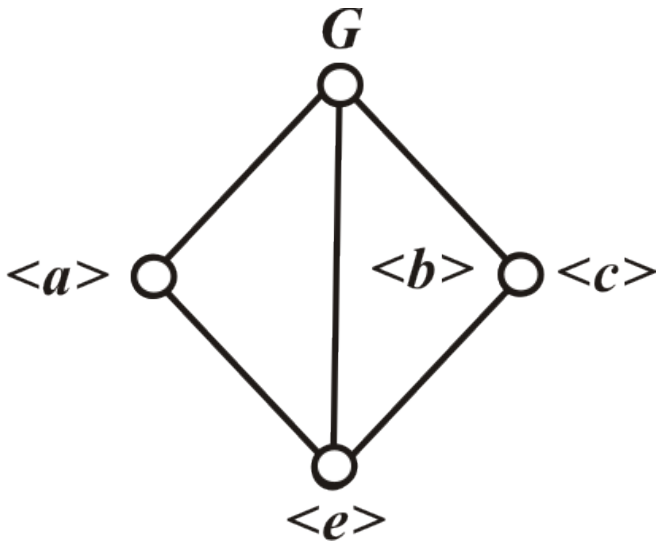
定义10.8 设G为群, 令

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

则偏序集$< L(G), \subseteq >$称为G的子群格

实例：

Klein四元群的子群格如下：



陪集定义与实例

定义10.9 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，$H=<a>$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$\{b,c\}$.

实例

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

$f_1=\{<1,1>,<2,2>,<3,3>\}$，$f_2=\{<1,2>,<2,1>,<3,3>\}$

$f_3=\{<1,3>,<2,2>,<3,1>\}$，$f_4=\{<1,1>,<2,3>,<3,2>\}$

$f_5=\{<1,2>,<2,3>,<3,1>\}$，$f_6=\{<1,3>,<2,1>,<3,2>\}$

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：

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

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

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

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

陪集的基本性质

定理10.8 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$a = ea$ 和 $ea \in Ha$ 得 $a \in Ha$

陪集的基本性质

定理10.9 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 $h_1a\in Ha$，（根据陪集的定义$h_1\in H$）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.

陪集的基本性质

定理10.10 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$b\in G$，（p123等价类）

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

（TH10.9）

推论

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.

定理10.11 设H是群G的子群，则

$$\forall a\in G,\ H\approx Ha$$

证明 略

10.4 环与域

定义10.12 设$<R,+,\cdot>$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) $<R,\cdot>$构成半群

(3) · 运算关于+运算适合分配律

则称$<R,+,\cdot>$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}.

环的实例

例15

(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$M_n(\mathbf{R})$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.

环的运算性质

定理10.16 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) $\forall a_1,a_2,\ldots,a_n,b_1,b_2,\ldots,b_m \in R$ $(n,m \geq 2)$

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

证 (1) $\forall a \in R$有 $a0 = a(0+0) = a0+a0$

由环中加法的消去律得$a0=0$. 同理可证$0a=0$.

(2) $\forall a,b \in R$，有

$$(-a)b+ab = (-a+a)b = 0b = 0$$

$$ab+(-a)b = (a+(-a))b = 0b = 0$$

$(-a)b$是ab的负元. 由负元惟一性$(-a)b = -ab$，同理$a(-b) = -ab$

证明(4)

(4) 证明思路：用归纳法证明 $\forall a_1, a_2, \ldots, a_n$ 有

$$(\sum_{i=1}^{n} a_i) b_j = \sum_{i=1}^{n} a_i b_j$$

同理可证, $\forall b_1, b_2, \ldots, b_m$ 有

$$a_i (\sum_{j=1}^{m} b_j) = \sum_{j=1}^{m} a_i b_j$$

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

实例

例16 在环中计算$(a+b)^3$, $(a-b)^2$

解 $(a+b)^3 = (a+b)(a+b)(a+b)$

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

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

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

特殊的环

定义10.13 设$<R,+,\cdot>$是环

(1) 若环中乘法$\cdot$适合交换律，则称R是交换环

(2) 若环中乘法$\cdot$存在单位元，则称R是含幺环

(3) 若$\forall a,b\in R$，$ab=0 \Rightarrow a=0 \vee b=0$，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.

实例

例17

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

(3) 设$n\in\mathbf{Z}$, $n\geq 2$, 则n阶实矩阵的集合$M_n(\mathbf{R})$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.

第十章 习题课

主要内容

- 半群、独异点与群的定义
- 群的基本性质
- 子群的判别定理
- 陪集的定义及其性质
- 循环群的生成元和子群
- 环的定义与性质
- 特殊的环

基本要求

- 判断或证明给定集合和运算是否构成半群、独异点和群
- 熟悉群的基本性质
- 能够证明G的子集构成G的子群
- 熟悉陪集的定义和性质
- 会求循环群的生成元及其子群
- 能判断给定代数系统是否为环和域

练习1

1. 判断下列集合和运算是否构成半群、独异点和群.

(1) a 是正整数，$G = \{a^n \mid n \in \mathbf{Z}\}$, 运算是普通乘法.

(2) $\mathbf{Q}^+$是正有理数集，运算为普通加法.

解

(1) 是半群、独异点和群

(2) 是半群但不是独异点和群

方法：根据定义验证，注意运算的封闭性

练习2

2. 设V_1= <Z, +>, V_2 = <Z, ·>,其中Z为整数集合, + 和· 分别代表普通加法和乘法. 判断下述集合S是否构成V_1和V_2的子半群和子独异点.

(1) S= {2k | k∈Z}

(2) S= {2k+1 | k∈Z}

解

(1) S关于V_1构成子半群和子独异点，但是关于V_2仅构成子半群

(2) S关于V_1不构成子半群也不构成子独异点，S关于V_2构成子半群和子独异点

练习3

3. 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$a^{-1} = a$.

练习5

5．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$xy^{-1}\in H$

练习6

6. (1) 设G为模12加群, 求<3> 在G中所有的左陪集

(2) 设 $X=\{x \mid x\in \mathbf{R}, x\neq 0,1\}$, 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) <3> = {0, 3, 6, 9}, <3>的不同左陪集有3个，即

0+<3> = <3>,

1+<3> = 4+<3> = 7+<3> = 10+<3> = {1, 4, 7, 10} ,

2+<3> = 5+<3> = 8+<3> = 11+<3> = {2, 5, 8, 11}.

(2) $\{f_1,f_2\}$有3个不同的陪集，它们是:

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

练习11

11. 在整数环中定义$*$和$\diamond$两个运算, $\forall a,b\in Z$ 有

$$a*b = a+b-1,\ a\diamond b = a+b-ab.$$

证明<Z, $*$,$\diamond$>构成环

证　$\forall a,b\in Z$有$a*b$, $a\diamond b\in Z$, 两个运算封闭. 任取$a,b,c\in Z$

$$(a*b)*c = (a+b-1)*c = (a+b-1)+c-1 = a+b+c-2$$

$$a*(b*c) = a*(b+c-1) = a+(b+c-1)-1 = a+b+c-2$$

$$(a\diamond b)\diamond c = (a+b-ab)\diamond c = a+b+c-(ab+ac+bc)+abc$$

$$a\diamond(b\diamond c) = a\diamond(b+c-bc) = a+b+c-(ab+ac+bc)+abc$$

$*$与$\diamond$可结合，1为$*$的单位元. $2-a$为a关于$*$的逆元. Z关于$*$构成交换群, 关于$\diamond$构成半群.　$\diamond$关于$*$ 满足分配律.

$$a\diamond(b*c) = a\diamond(b+c-1) = 2a+b+c-ab-ac-1$$

$$(a\diamond b)*(a\diamond c) = 2a+b+c-ab-ac-1$$

<Z, $*$,$\diamond$>构成环