第6章　几个典型的代数系统

6.1 半群和独异点

定义6.1.1半群

设V=<S, °>是代数系统, °为二元运算. 如果°是可结合的,则称V为半群.

例6.1

- $< Z^+, + >$是半群。
- $<N,+>, <Z,+>, <Q,+>, <R,+>$都是半群，其中+表示普通加法。
- $<M_n(R), \cdot>$是半群,其中·表示矩阵乘法。
- $<P(B), \oplus>$是半群,其中⊕表示集合的对称差运算.
- $< Z_n , \oplus >$是半群,其中$Z_n = \{0,1,\ldots,n-1\}$, ⊕表示模n加法。

半群中运算的幂

因为半群$V=<S, \circ>$中的运算$\circ$是可结合的,可以定义运算的幂. 对任意的$x \in S$,规定x^n是

$$x^1=x,$$

$$x^{n+1}= x^n \circ x , \quad n\text{为正整数}。$$

易证x的幂遵从以下规律:

$$x^n \circ x^m= x^{n+m},$$

$$(x^n)^m= x^{nm} ,n\text{为正整数}.$$

例

例如在半群$\langle Z,+\rangle$中,$\forall x\in Z$,x的n次幂是$\underbrace{x+x+\cdots+x}_{n个x}=nx$,而在半群$\langle P(B),\oplus\rangle$中,$\forall x\in P(B)$,$x$的$n$次幂是

$$\underbrace{x\oplus x\oplus\cdots\oplus x}_{n个x}=\begin{cases}\varnothing, & n\text{ 为偶数;}\\ x, & n\text{ 为奇数.}\end{cases}$$

定理6.1.1 若$V=<S, *>$是半群, S为有限集合，则S中必含有幂等元。

证明： 设$=<S, *>$是半群,对任何$a \in S$,有

$a^2, a^3 \ldots \in S$,.由于S为有限集合， 所以必存在$j>i$,使得$a^i = a^j$。

令$p=j-i$,便有 $a^i = a^j = a^p * a^i$

所以， $a^m = a^p * a^m \quad (m>i)$

令$m=kp$,

$$a^{kp} = a^p * a^{kp} = a^p * (a^p * a^{kp}) = a^{2p} * a^{kp} = \ldots = a^{kp} * a^{kp}$$

令$b= a^{kp}$,有$b= b* b$, 即S中含有幂等元

定义6.1.2 可交换半群

如果半群V=<S,*>中的二元运算*是可交换的，则称V为可**交换半群**.

定义6.1.3 独异点

如果半群V=<S,°>中的二元运算**含有幺元**,则称V为**含幺半群**,也可叫做**独异点**.

为了强调幺元的存在,有时将独异点记为<S,°,e>。

例6.2

- $< Z^+, + >$是可交换半群。
- $<N,+>, <Z,+>, <Q,+>, <R,+>$都是可交换半群和独异点，其中+表示普通加法。么元是0。
  $<N,+,0>, \ldots, <R,+,0>$
- $<M_n(R), \cdot>$是半群和独异点,其中·表示矩阵乘法。矩阵乘法的么元是n阶单位矩阵E. $< M_n(R) , \cdot, E >$
- $<P(B), \oplus>$是半群和独异点,其中⊕表示集合的对称差运算. 对称差运算的么元是∅.
- $< Z_n , \oplus >$是半群和独异点,其中$Z_n = \{0,1,\ldots,n-1\}$, ⊕表示模n加法。模n加法的么元是0. $<Z_n, \oplus, 0>$.

独异点中运算的幂

在独异点$V=<S,\circ,e>$中,如果规定$x^0=e$(x是S中的任意元素),那么有关半群中幂的定义可以变成

$$x^0=e$$

$$x^{n+1}=x^n \circ x \quad n\text{为非负整数}.$$

而关于幂的两个运算公式不变,只要其中的m和n是非负整数就可以了。

独异点中运算的幂

在独异点$V=<S,\circ,e>$中,如果规定$x^0=e$(x是S中的任意元素),那么有关半群中幂的定义可以变成

$$x^0=e$$

$$x^{n+1}=x^n \circ x \quad n\text{为非负整数}.$$

而关于幂的两个运算公式不变,只要其中的m和n是非负整数就可以了。

定理6.1.2

一个有限独异点 <S,*, e>的运算表中不会有任何两行或两列元素相同。

注意： 此定理对半群不成立。

子独异点

独异点的子代数叫做**子独异点**.

对独异点$V=<S,\circ,e>$, $<T,\circ,e>$构成V的子独异点，需要满足：

❶ T是S的非空子集，

❷ T要对V中的运算$\circ$封闭，

❸ $e\in T$，

即可。

【例2.2】 设 $A=\left\{\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \middle| a \in R\right\}$，则 A 关于矩阵乘法构成半群 $\langle A, \cdot\rangle$，且它是 $\langle M_2(R), \cdot\rangle$ 的子半群. 令 $V=\left\langle A, \cdot, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\right\rangle$，则 V 是一个独异点，但它不是 $\left\langle M_2(R), \cdot, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\rangle$ 的子独异点. 因为 $M_2(R)$ 中关于 $\cdot$ 运算的单位元不属于 A.

半群同态

定义6.3

设$V_1 =<S,\circ>$, $V_2=<T,*>$为半群, $\varphi : S \to T$, 且对任意$x,y \in S$有

$$\varphi(x \circ y) = \varphi(x) * \varphi(y)$$

则称φ为半群V_1到V_2的**同态**.

例　半群V=<S,.>,其中S= $\left\{\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \middle| a,d\in\mathbb{R}\right\}$

.是矩阵乘法。令$\varphi : S\rightarrow S$, $\varphi\left(\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix}\right)=\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$

那么有

$$\varphi\left(\begin{pmatrix} a_1 & 0 \\ 0 & d_1 \end{pmatrix}\cdot\begin{pmatrix} a_2 & 0 \\ 0 & d_2 \end{pmatrix}\right)=\varphi\left(\begin{pmatrix} a_1a_2 & 0 \\ 0 & d_1d_2 \end{pmatrix}\right)$$

$$=\begin{pmatrix} a_1a_2 & 0 \\ 0 & 0 \end{pmatrix}=\begin{pmatrix} a_1 & 0 \\ 0 & 0 \end{pmatrix}\cdot\begin{pmatrix} a_2 & 0 \\ 0 & 0 \end{pmatrix}$$

$$=\varphi\left(\begin{pmatrix} a_1 & 0 \\ 0 & d_1 \end{pmatrix}\right)\cdot\varphi\left(\begin{pmatrix} a_2 & 0 \\ 0 & d_2 \end{pmatrix}\right)$$

这说明φ是半群V的自同态,但不是单自同态

补充：　独异点的同态

$V_1=<S_1,\circ,e_1>$, $V_2=<S_2,*,e_2>$是独异点，

设$\varphi: S_1 \to S_2$,如果对任意$x,y \in S_1$都有

$$\varphi(x \circ y)= \varphi(x) * \varphi(y)$$

$$\varphi(e_1)=e_2,$$

则称φ为独异点V_1到V_2的同态。

例 独异点V= $\left(S,\cdot,\begin{pmatrix}1&0\\0&1\end{pmatrix}\right)$

其中S= $\left\{\begin{pmatrix}a&0\\0&d\end{pmatrix}\middle|a,d\in\mathbf{R}\right\}$ ， .是矩阵乘法。

令φ : S→ S, $\varphi\left(\begin{pmatrix}a&0\\0&d\end{pmatrix}\right)=\begin{pmatrix}a&0\\0&0\end{pmatrix}$

那么对任意x,y∈S都有

$$\varphi\left(\begin{pmatrix}a_1&0\\0&d_1\end{pmatrix}\cdot\begin{pmatrix}a_2&0\\0&d_2\end{pmatrix}\right)=\varphi\left(\begin{pmatrix}a_1&0\\0&d_1\end{pmatrix}\right)\cdot\varphi\left(\begin{pmatrix}a_2&0\\0&d_2\end{pmatrix}\right)$$

但是

$$\varphi\left(\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\right)=\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$$

而 $\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}$ 不是独异点V的么元,因此,

φ不是独异点V 的自同态。

这就是说,如果把V看作半群,则φ是V的自同态 ;如果把V看作独异点,则φ就不是它的自同态了。

定理：设V_1 =<S, * >, V_2=<T, ° >为半群, f为S 到 T的半群同态，则对半群同态有

（1）同态象<f(s), °>为一半群。

（2）若<S, * >为独异点，则<f(s), °> 也为独异点

群

定义 设〈G,∘〉是代数系统,∘为二元运算. 如果

- ∘是可结合的,
- 存在么元$e \in G$,
- 并且G中的任意元素x,都有$x^{-1} \in G$,

则称G是**群**.

例

- $\langle Z,+\rangle,\langle Q,+\rangle,\langle R,+\rangle$都是群;
- $\langle P(B),\oplus,\varnothing\rangle$是群,其中$\oplus$表示集合的对称差运算. 元素的逆元是自身;
- $\langle Z_n,\oplus,0\rangle$是群,其中$Z_n=\{0,1,\ldots,n-1\}$, $\oplus$表示模n加法。0的逆元是0,非0元素的逆元是n-x.
- $\langle Q,\cdot\rangle$不是群; $\langle Q^+,\cdot\rangle$是群;

例

设G＝{e,a,b,c},∘为G上的二元运算,它由以下运算表给出. 不难证明G是一个群.

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

e为G中的幺元,

∘是可交换的.

任何G中的元素与自己运算的结果都等于e.

在a,b,c三个元素中,任何两个元素运算的结果都等于另一个元素.

一般称这个群为Klein四元群.

群的术语

若群G中的二元运算是可交换的,则称群G为**交换群**,也叫做**阿贝尔(Abel)群**.

- $\langle Z,+\rangle,\langle Q,+\rangle,\langle R,+\rangle$都是群,也是阿贝尔(Abel)群;
- $\langle P(B),\oplus,\varnothing\rangle$是群, ,也是阿贝尔(Abel)群;
- $\langle Z_n,\oplus,0\rangle$是群, ,也是阿贝尔(Abel)群.
- Klein四元群也是阿贝尔群.

定理

设<G,*>为一个群，<G,*>为阿贝尔群的充分必要条件是对任意x,y ∈G,有(x*y)*(x*y)=(x*x)(y*y)

无限群 有限群

若群G中有无限多个元素,则称G为**无限群**,否则称为**有限群**.

例如,

$\langle Z, + \rangle$,$\langle R, + \rangle$都是无限群.

$\langle Z_n, \oplus \rangle$是有限群.

Klein四元群也是有限群.

群的阶

对于有限群G,G中的元素个数也叫做G的阶,记作|G|.

$<Z_n,\oplus>$是有限群,其阶是n.

Klein四元群也是有限群,其阶是4.

群中运算的幂

在群G中,由于G中每个元素都有逆元，所以可以定义负的幂，对任意 $x \in G$, n为正整数,那么有关群中幂的定义可以变成

$$x^0 = e$$

$$x^{n+1} = x^n * x \quad n\text{为非负整数}.$$

$$x^{-n} = (x^{-1})^n, \quad n\text{为正整数}$$

而关于幂的两个运算公式不变,只要其中的m和n是任意整数就可以了。

群的性质

定理 设G为群,则G中的幂运算满足

- $\forall x \in G, \quad (x^{-1})^{-1} = x$
- $\forall\ x,y \in G, \ (x*y)^{-1} = y^{-1}{}_{*}x^{-1}$
- $\forall x_1,x_2,\ldots,x_n \in G, (x_1 * x_2 * \ldots x_n)^{-1} = x_n^{-1}\ldots x_2^{-1}x_1^{-1}$
- $\forall\ x \in G, \quad x^n * x^m = x^{n+m}.$
- $\forall\ x \in G, (x^n)^m = x^{nm}.$ m,n是整数

定理6.1.6

设<G,*>为群，则

（1）G有唯一的幺元，G的每个元素恰有一个逆元；

（2）G为群,$\forall a,b\in G$,方程$a*x=b$和$y*a=b$在G中有解,且有唯一解.

（3）当G不等于{e}时，G无零元

证　先证 $a^{-1}b$ 是方程 $ax=b$ 的解.将 $a^{-1}b$ 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G=<P({a,b}), ⊕>,其中⊕为集合的对称差运算,求下列群方程

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

解

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

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

消去律

定理6.1.7

G为群,则G中适合消去律,即对任意a,b,c∈G有

(1)若a*b = a*c,则b = c.

(2)若b*a = c*a,则b = c.

定理

设<G,*>为有限独异点,适合消去律，证明<G,*>为群。

定理6.1.8

设<G,*>为一群,则么元是G的唯一的幂等元。

设<G,*>为群, 用aG和Ga分别表示下列集合

$Ga=\{g*a \mid g \in G\}$　$aG=\{a*g \mid \in G\}$

则有

定理6.1.9

设<G,*>为一群,a为G中任意元素,那么

$aG=G=Ga$

通过运算表判断哪些代数系统不是群

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.

例如:对于集合S={a,b,c,d},将a映射到b,b映射到d,c映射到a,d映射c是一个从S到S的一对一映射,这个置换可以表示为:

$$\begin{pmatrix} a & b & c & d \\ b & d & a & c \end{pmatrix}$$

判断方法

定理 G为有限群,则G的运算表中的每一行(每一列)都是G中元素的一个置换,且不同的行(或列)的置换都不相同。

或者说

G为有限群,则G的运算表中的每一行(每一列)都是G中元素的一个全排列

元素x的阶

设G是群,$x \in G$,使得$x^k = e$成立的**最小**的正整数k叫做x的**阶**(或**周期**).

- 如果不存在正整数k,使$x^k = e$,则称x是**无限阶**的.
- 对有限阶的元素x,通常将它的阶记为$|x|$.
- 在任何群G中么元e的阶都是1.

例

在Klein四元群中,

|a|=?,|b|=?,|c|=?,|e|=?

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

设 G={0，60，120，180，240，300},在 G 上定义二元运算*,如表所示，说明<G,*>中元素的阶。

*	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

下面一些结论：

定理6.1.10. 设$\langle G,*\rangle$是有限群，$|G|=n$，则G中每个元素的阶$\leqslant n$。

定理6.1.11. 设$\langle G,*\rangle$是群，$a\in G$，a的阶为k，即$|a|=k$. 若$a^n=e$当且仅当k整除n。

定理6.1.12. 设$\langle G,*\rangle$是群，$g\in G$，则g与g^{-1}

相同的阶。

例.

设$\langle G,*\rangle$是n阶有限群，证明

1) G中阶大于2的元素的个数一定是偶数。

2)若n是偶数，则G中阶等于2的元素个数一定是奇数。

定理6.1.13

设<G,*>为一个群，<G,*>为阿贝尔群的充分必要条件是对任意x,y ∈G,有(x*y)*(x*y)=(x*x)(y*y)

群G的应用

群$<Z_n,\oplus>$在计算机科学中有十分重要的应用，下面以图书国际标准书号ISBN号的校验位为例，说明其应用。可以发现错误或顺序颠倒。

例1：书ISBN号为7-5053-8708-1（中国-电子工业出版社-书编号-校验码），由10位数字组成。

$x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{10}$,校验位通过下列余式计算

$$1x_1 + 2x_2 + 3x_3 + 4x_4 + 5x_5 + 6x_6 + 7x_7 + 8x_8 + 9x_9 = x_{10} \pmod{11}$$

$$221 = x_{10} \pmod{11}$$

$$1 = x_{10} \pmod{11}$$

现有错误书号7-5053-8705 计算

$$194 = x_{10} \pmod{11}$$

$$7 = x_{10} \pmod{11}$$ 发现错误。

例2：书号7-5062-0335-7和7-5062-0353-7。前一个错，因为$141 = 7 \pmod{11}$

$9 = 7 \pmod{11}$；后一个$139 = 7 \pmod{11}$，$7 = 7 \pmod{11}$正确。说明有组数据顺序错了。

群G的应用

⑩ 开关线路的计数 一个具有两种状态的电子元件称为一个开关.每一个开关的状态由一个开关变量来表示,如常用0和1来表示开关变量A的两种状态。 由若干个开关A1, A2, …, An组成的一个线路称为开关线路。一个开关线路也有两种状态，1表示线路接通，0表示线路断开。 开关线路的状态由各个开关Ai(i=1,2,…,n)的状态决定。因而可以用一个函数f(A1, A2, …, An)来表示f的取值为0或1. f被称为开关函数。每一个开关线路对应一个开关函数。 对于n个开关变量的开关函数共有)(2^{n2}个，如n=4则有65536个开关函数，这个数量是非常大。在实际应用中设计所有开关函数的开关线路是不现实的。 但注意到有的开关函数对应的开关线路是本质上相同或等价的。因此，现在的问题是由n个开关可组成多少个本质上不同的开关线路？

⑩着色问题 着色计数问题在算法分析中十分重要兹举几例。 取四个黑或白色的小球，用线将之穿成一串，请问有多少种本质不同的穿法？如果要将这四个小球置于正方形的四个顶点上，则有多少种本质不同的置放方法？如果用6种颜色着色立方体的6个面，则有多少种本质不同的着色方法？通过旋转能重合的着色方法被视为本质相同的。

⑩ 如何从一些编码中选取一些码字并附加码字组成新码使其具有一定的纠错能力是一个很重要的课题。 为使一种码具有检错或纠错能力,须对原码字增加多余的码元,以扩大码字之间的差别,即把原码字按某种规则变成有一定剩余度的码字,并使每个码字的码之间有一定的关系。 关系的建立就称为编码。 码字到达接收端后,可以根据编码规则是否满足以判定有无错误。 当不能满足时,按一定规则确定错误所在位置并予以纠正。 纠错并恢复原码字的过程称为译码。 纠错码能够检错或纠错,主要是靠码字之间有较大的差别。

在计算机中经常使用的汉明码(Hamming Code)是利用群的性质实现纠错的一种编码称之为群码。

设信息传输单位字是一个m二进制数,现在选择整数n>m设B={0,1}, B^m是所有的m位二进制数集合,B^n是所有的n位二进制数集合,构造一个双射函数e: $B^m \rightarrow B^n$ 。 称e为(m,n)编码函数.于是可以用一个n位二进制数代表一个m位二进制数。 若$b \in B^m$,则e(b)就是代表b的码字.e(b)中的冗余码元将有助于检出或纠正传输过程中产生的误码。

第6章　几个典型的代数系统

6.1 半群与群

6.2 子群

6.3 循环群和置换群

6.4 陪集与拉格朗日定理

6.5 正规子群、商群和同态基本定理

6.6 环与域

子群

定义6.2.1

设群<G,*>,H是G的非空子集. 如果H关于G中的运算*构成群,则称<H,*>为<G,*>的**子群**,记作$H \leq G$.

例如,在群<Z, +>中,取

$$2Z = \{2x | x \in Z\}$$

则2Z关于加法构成<Z, +>的子群.同样,{0}也是<Z, +>的子群.

例

在Klein四元群中,G={e,a,b,c}中,有5个子群,它们是:

$$\{e\},\{e,a\},\{e,b\},\{e,c\},G$$

平凡子群是...

真子群是...

子群判定定理（有3个）

判定定理1　设<G,*>为群, H是G的非空子集, <H,*>为<G,*>的子群的 充要条件是

(1) G的幺元e ∈H

(2) 若a, b∈H, 则a*b∈H

(3) 若a∈H, 则a^{-1}∈H

子群判定定理

判定定理2

设<G,*>为群,H是G的非空子集.那么 <H ,*> 是<G,*>的子群的充分必要条件是对任意$x,y \in H$都有$x*y^{-1} \in H$

子群判定定理

判定定理3　设<G,*>为群, H是G的非空有限子集,

且H对*运算封闭， 那么<H,*>为<G,*>的子群。

例1 设G为群,

(1)对任何$a \in G$,令

$$H = \{a^k | k \in Z\},$$

即a的所有幂的集合. 不难判定H是G的子群. 因为任取H中的元素a^m, a^l,都有

$$a^m (a^l)^{-1} = a^m a^{-l} = a^{m-l} \in H.$$

称这个子群是由元素a生成的子群,记作<a>.

注意: 由a生成的子群是包含a的最小子群。

群G的中心

设G为群,令C是与G中所有的元素都可交换的元素构成的集合,即

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

称C为群G的中心. C为群G的子群.

例2：证明： G的中心为子群

证： 由于e与G中所有元素可交换可知e∈C.C是G的非空子集。

- 由y*a = a*y可得 $y = a*y*a^{-1}$，因此∀x，y∈C，因为
- $x*y^{-1}=(a*x*a^{-1})*(a*y*a^{-1})^{-1}= a*x*y^{-1}*a^{-1}$
  - 因此 $x*y^{-1}*a= a*x*y^{-1}$
- 所以$x*y^{-1}\in H$，故<C, *>是G的子群。

例3 求群<Z6,©>中由2生成的子群

而在群$\langle \mathbf{Z}_6, \ominus \rangle$中，由 2 生成的子群由 $2^0=0, 2^1=2, 2^2=2 \oplus 2=4$.
$2^3=2 \oplus 2 \oplus 2=0, \cdots$构成，即

$$\langle 2 \rangle = \{0, 2, 4\}$$

例4　求Klein 四元群得所有子群

解：

<{e},*>,<{e,a},*>,<{e,b},*>,<{e,c},*>均是其子群。

第6章　几个典型的代数系统

6.1 半群与群

6.2　子群

6.3 循环群和置换群

6.4 陪集与拉格朗日定理

6.5 正规子群、商群和同态基本定理

6.6 环

6.7 域

6.8 有限域

中国人从何而来？汉人的祖先到底是谁？

- 全世界人口基因来自36个女人 源于“线粒体夏娃”？
- 2003年4月14日,美国科学家在华盛顿庄严宣布:美、英、日、法、德和中国,6个国家联合,经过13年的努力,共同绘制完成了《人类基因序列图》。
- 2005年4月美国《国家地理》杂志研究“人类迁徙遗传地理图谱计划”复旦大学生命科学院承担了远东地区及其东南亚地区的DNA的取样和研究。

- 令人意想不到的是我们60多亿人口可能源自一个母亲。源于15万年前到20万年前非洲大陆上一个科学家命名为“线粒体夏娃”（Mitochondrial Eve）的女人的后代。
- 基因图谱并未显示‘种族’之间有何差异。我们都是10万年前从非洲的少数原始部落迁移和进化而来。人类只有一个种族。
- 极少量基因决定人的肤色和外表，人的智力、艺术天赋和社交能力等却由人类8万个基因中数千甚至数万个基因所决定
- 生活在同一地区的人，某方面基因的差别之大可达90%，而因生活地区不同而产生的基因差别只占10%。
- 华人占大多数的东亚人群起源于非洲。

循环群

定义6.3.1 在群G中如果存在$a \in G$使得

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

而称G为**循环群**,记作$G=\langle a \rangle$,称a为G的**生成元**. (约定$a^0=e$)

所谓循环群，就是群中的每个元素都可表示成某个固定元素a的整数次幂。

n阶循环群

在循环群$G=\langle a\rangle$中,生成元a的阶与群G的阶是一样的.如果a是有限阶元,$|a|=n$,则称G为n阶循环群.如果a是无限阶元,则称G为无限阶循环群.

- $\langle Z,+\rangle$是循环群,1或-1为生成元;
- $\langle 2^i, . \rangle$是循环群,其中2为生成元;
- $\langle Z_8 , \oplus ,0 \rangle$是循环群,其中1,3为生成元;

定理6.3.2

设$\langle G, * \rangle$是由a生成的有限群，则有

$G=\{e, a^1, a^2 \ldots \ a^{n-1}\}$，其中$|G|=n$，也是a的阶。

n阶循环群必同构于$\langle Z_n, +_n \rangle$

证明：设a的阶为k，则$H=\{e, a^1, a^2 \ldots \ a^{k-1}\}$为G的子群，$H \subseteq G$。现证明$G \subseteq H$。

任取$a^m \in G$,如果不属于H，则$m=kt+r \quad r<k$

$a^m = a^{kt+r} = a^{kt} * a^r = a^r \in H$ 矛盾。所以$H = G$

设有映射 f：$G -> Z_n$，任意$f(a^i) = i$ 证明该映射是同构映射。

$\langle G,*\rangle$为有限循环群，有几个生成元？

设$\langle G,*\rangle$是由a生成的有限群，则有

$G=\{e, a^1, a^2 \ldots a^{n-1}\}$，其中$|G|=n$，G有与n互质数的数目个生成元（即欧拉函数）。

例如1：n=6，与6互质的数有1和5，则有两个生成元，分别是$\langle a\rangle$和$\langle a^5\rangle$

例如2：n=12，与12互质的数有1、5、7和11，则有四个生成元，分别是$\langle a\rangle$、$\langle a^5\rangle$、$\langle a^7\rangle$、$\langle a^{11}\rangle$。

设 G={0，60，120，180，240，300},在 G 上定义二元运算*,如表所示，说明<G,*>是个循环群。

*	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

例2： $\langle \{1,-1,i,-i\}, \times \rangle$ 是循环群，生成元为i和-i。

例3：

设 G={a,b,c,d},在 G 上定义二元运算*，如表所示，说明<G,*>是个循环群。

*	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	b	a
d	d	c	a	b

生成元为 c, d

结论：

循环群的生成元可以不唯一，个数为与n的质数的数目

$\langle G, * \rangle$为无限循环群，有几个生成元？

定理6.3.3.

设$\langle G, * \rangle$为无限循环群，且$G=\langle a \rangle$，则G

只有两个生成元a和a^{-1}。且$\langle G, * \rangle$同构于$\langle Z, + \rangle$

证明：（1）证明a^{-1}是生成元。

证：因$\langle a^{-1} \rangle \subseteq \langle a \rangle$，

对任意$a^k \subseteq \langle a \rangle$有$a^k=(a^{-1})^{-k} \subseteq \langle a^{-1} \rangle$，所以$\langle a^{-1} \rangle = \langle a \rangle$。

（2）证只有这两个。

假设还有一个生成元b，

$a \in G$,有$a= b^t$，又因$b \in G$, $b= a^k$，$a= b^t= a^{kt}$，$a^{kt-1}=e$

$kt=1$, $t=k=1$或$t=k=-1$, 因此$b= a$或$b=a^{-1}$

设有映射 $f: G->Z$，任意$f(a^i) =i$ 证明该映射是同构映射。

例1：在 <I,*>群中取1 ∈I,由于0＝1^0,n=1^n,-n=$(-1)^n$=1^{-n} 故I中的每个元素都可表示成1的整数次幂。

由循环群的定义知<I,＋>是循环群，1和-1是循环群的生成元。

定理： 任何一个循环群必定是阿贝尔群。

证明　设 $\langle G, *\rangle$ 是一个循环群，它的生成元是 a，那么，对于任意的 $x, y \in G$，必有 $r, s \in I$，使得

$$x = a^r \quad 和 \quad y = a^s$$

而且

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

因此，$\langle G, *\rangle$ 是一个阿贝尔群。 □

<G,*>是交换群不一定是循环群， 例 Klein 四元群。

Klein 四元群**是交换群但不是循环群。**

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

循环子群的性质

定理6.3.4

循环群的子群都是循环群。

证明：设$\langle G,*\rangle$为a生成的循环群；H为G的子群。（1）若$H=\{e\}$，显然H为循环群。

（2）因为H为G的子群，那么H中元素都是a的指数。假设H中最小的元素为a^k，任取H中元素a^m，只要证明a^m可以表示成a^k的方幂即可。

循环子群的个数

定理6.3.5

设$\langle G,*\rangle$为a生成的循环群，

(1) 若G是无限循环群，则G有**无限**多个子群，它们分别由$e, a^1, a^2 \ldots a^{n-1} \ldots$生成。

(2) 若G是有限循环群，阶为n，则G的子群的阶都是n的因子。对于n的正因子d，在G中**只有一个**d阶子群，就是**由$a^{n/d}$生成的子群。**

例：设 G={a,b,c,d},在 G 上定义二元运算*,如表所示，求<G,*>所有的循环子群。

解：幺元：a;

生成元：c、d

共有 3 个循环子群。分别为<{a},*>, <{a,b},*>,和<G,*>

或写成<a> ,<b>,<c>

*	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	b	a
d	d	c	a	b

设 G={0，60，120，180，240，300},在 G 上定义二元运算*,如表所示， <G,*> 是个循环群。请问共有几个循环子群？分别是什么？

*	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

例： 设G是12阶循环群G=<a >， 找出G的所有生成元和G的所有子群。

解： G的所有生成元a,a^5,a^7,a^{11}

G的所有子群:$\langle a\rangle,\langle a^2\rangle,\langle a^3\rangle,\langle a^4\rangle,\langle a^6\rangle,\langle a^{12}\rangle$

$\langle a\rangle=\langle\{a^0,a^1,a^2,a^3,a^4,a^5,a^6,a^7,a^8,a^9,a^{10},a^{11}\},*\rangle$

$\langle a^2\rangle=\langle\{a^0,a^2,a^4,a^6,a^8,a^{10}\},*\rangle$

$\langle a^3\rangle=\langle\{a^0,a^3,a^6,a^9\},*\rangle$

$\langle a^4\rangle=\langle\{a^0,a^4,a^8\},*\rangle$

$\langle a^6\rangle=\langle\{a^0,a^6\},*\rangle$

$\langle a^{12}\rangle=\langle a^0\rangle=\langle\{a^0\},*\rangle$

第6章　几个典型的代数系统

6.1 半群与群

6.2　子群

6.3 循环群和置换群

6.4 陪集与拉格朗日定理

6.5 正规子群、商群和同态基本定理

6.6 环

6.7 域

6.8 有限域

置换群

定义6.3.2 变换

任意集合A上的双射函数称为变换.

定义6.3.3 置换

有限集上的双射函数称为置换

定义6.3.3 n元置换

设S＝{1,2,…,n},S上的任何双射函数σ:S→S构成了S上n个元素的置换,称为n元置换.

n元置换的表示方法

1. 置换形式

2. 轮换形式

3.对换形式

n元置换的表示方法

1.置换表示

σ将1,2,3分别置换成2,3,1,此置换常被记为

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

采用这种记法,一般的n元置换σ可记为

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

即： S={1,2,3}， 令σ:S→S ， 且有:

σ(1)=2, σ(2)=3, σ(3)=1,

n个不同元素有多少种排列的方法?

n!种排列的方法,所以,S上有n!个置换.

例如,<1,2,3>上有3!=6种不同的置换,

即

$$\sigma_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \sigma_2=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\ \sigma_3=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

$$\sigma_4=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\ \sigma_5=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ \sigma_6=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

2.轮换表示

对于n元置换也可以用不交的轮换之积来表示.

$$\tau=(a_1a_2\ldots a_m),\ \ m\le n$$

那么τ的映射关系是

$$a_1|\rightarrow a_2, a_2|\rightarrow a_3, \ldots a_{m-1}|\rightarrow a_m, a_m|\rightarrow a_1,$$

而其他的元素都有$a|\rightarrow a$. 称τ为m次轮换.

任何n元置换都可表成不交的轮换之积.

例如, σ是$\{1,2,\ldots 6\}$上的置换,且

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

那么σ的映射关系是

$1|\rightarrow 6,\ 2|\rightarrow 5,\ 3|\rightarrow 3,\ 4|\rightarrow 4,\ 5|\rightarrow 2,\ 6|\rightarrow 1.$

去掉3和4这两个保持不变的元素,可得

$1|\rightarrow 6\ ,\ 6|\rightarrow 1\ ,\qquad 2|\rightarrow 5, 5|\rightarrow 2$

所以$\sigma=(1\ 6)\ (2\ 5)\ (3)\ (4)$

又如, τ也是$\{1,2,\ldots 6\}$上的置换,

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

则有

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

为使表达式简洁,可以去掉1次轮换

那么有

$$\sigma=(1\ 6)\ (2\ 5)$$

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

根据这种表法,{1,2,3 }上的置换

$$\sigma_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\ \sigma_2=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},\ \sigma_3=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$$

$$\sigma_4=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\ \sigma_5=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\ \sigma_6=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

可记为:

$\sigma_1=(1)$, $\sigma_2=(12)$, $\sigma_3=(13)$,

$\sigma_4=(23)$, $\sigma_5=(123)$, $\sigma_6=(132)$

轮换有下面性质：

（1）每个置换均可写成一些轮换的乘积，使得不同轮换中没有公共元素。长度为1的轮换往往忽略不写。

（2）同一置换中任何不相交轮换可交换，因为不同轮换中没有公共元素，这些轮换的次序可任意改变。

（3）如果不计这种次序，每个置换可唯一表成没有公共元素的一些轮换之积。

3.对换表示

每个轮换可表成一些对换之积。例如：

（1，2，3，…，n）=(1 n)(1 n-1)…(1 3)(12),

所以每个置换中可表成有限个对换之积。这种表达式（甚至对换的个数）显然不唯一。但是，同一个置换以多种方式表成对换之积时，其所含对换个数的奇偶性是不变的。表成奇（偶）数个对换之积的置换叫做奇（偶）置换。显然，两个奇置换或两个偶置换之积是偶置换，一个奇置换与一个偶置换之积是奇置换

逆置换

n元置换σ

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

σ的逆置换

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

n元对称群、 n元置换群

设$S = \{1,2,\ldots n\}$,S上的n!个置换构成集合S,其中恒等置换$I_s=(1)\in S_n$. 在S_n上规定二元运算°,对于任意n元置换$\sigma, \tau \in S_n$, °表示σ与τ的复合.显然:

（1）σ°τ也是S上的n元置换,所以,S_n对运算°是封闭的

（2）°是可结合的.

（3）恒等置换$I_s=(1)$是S_n中的么元。任取S_n中的置换σ,有 $\sigma^{\circ}I_s = I_s^{\circ}\sigma = \sigma$

（4）σ的逆置换

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

就是σ的逆元。

即:S_n关于置换的复合构成一个群,称之为S上的n元对称群.

S_n的任何子群称为S上的n元置换群.

定义6.3.4　置换群

将n个元素的集合A上的置换全体记为S_n,那么称群$\langle S_n,*\rangle$为n次对称群，它的子群又称为n次置换群。

例如

$S_3=\{(1),(12),(13),(23),(123),(132)\}$,

S_3的运算表如表6.1所示.

∘	(1)	(12)	(13)	(23)	(123)	(132)
(1)	(1)	(12)	(13)	(23)	(123)	(132)
(12)	(12)	(1)	(123)	(132)	(13)	(23)
(13)	(13)	(132)	(1)	(123)	(23)	(12)
(23)	(23)	(123)	(132)	(1)	(12)	(13)
(123)	(123)	(23)	(12)	(13)	(132)	(1)
(132)	(132)	(13)	(23)	(12)	(1)	(123)

从表6.1可以看到

$$(13)\circ(12)\neq(12)\circ(13)$$

所以, S_3不是阿贝尔群,在 S_3 中,(12),(13)和(23)都是2阶元, 而(123)和(132)是3阶元.

S_3有6个子群,即

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

$\langle(12)\rangle=\{(1),(12)\}$,

$\langle(13)\rangle=\{(1),(13)\}$,

$\langle(23)\rangle=\{(1),(23)\}$,

$\langle(123)\rangle=\langle(132)\rangle=\{(1),(123),(132)\}$,

所以, $S_3=\{(1),(12),(13),(23),(123),(132)\}$.

其中$\{(1)\}$和S_3是平凡的,除S_3自己以外,都是S_3的真子群.

上面讲了由有限集合X到X的双射即置换，以及置换群；下面不再限于X是有限集，换言之，它可以是个无穷集。这时从集合X到X的双射，称之为一一变换或变换。

因而，可证$<T_X,o>$构成群，在代数中称为变换群，显然，置换群是变换群的特例。

请注意，由T_X中的一些变换与运算o构成的群，都称为变换群，而$<T_X,o>$只不过是个特殊情形而已。

⑩ 定理6.3.6

⑩ 每个群均同构与一个变换群。

第6章　几个典型的代数系统

6.1 半群与群

6.2 子群

6.3 循环群和置换群

6.4 陪集与拉格朗日定理

6.5 正规子群、商群和同态基本定理

6.6 环与域

第6章　几个典型的代数系统

6.1 半群与群

6.2 子群

6.3 循环群和置换群

6.4 陪集与拉格朗日定理

6.5 正规子群、商群和同态基本定理

6.6 环

6.7 域

6.8 有限域

定义6.4.1

设<G,*>为群，$A,B \subseteq G$，，且A,B非空，$AB=\{a*b \mid a \in A, b \in B\}$,称为A,B的乘积。

性质

(1) $(AB)C=A(BC)$

(2) $eA=Ae=A$

定义6.4.2

设<H,*>为<G,*>的子群，那么对任一$g \in G$,称gH为H的左陪集，称Hg为H的右陪集，这里

$$gH = \{g*h \mid h \in H\}$$

$$Hg = \{h*g \mid h \in H\}$$

例6.4.2 在S3中， H={(1),(12)},则

(1)H={(1) (1),(1)(12)}={(1),(12)}

(12)H={(1),(12)}

(13)H={(13) (1),(13)(12)}={(13),(132)}

(23)H={(23)(1),(23)(12)}={(23),(123)}

(132)H={(13),(132)}

(123)H={(123),(23)}

定理6.4.1

设<H,*>为<G,*>的子群，那么

（1）对任意$g \in G$，$|gH|=|H|$

（2）当$g \in H$时，$gH = H$

（1）证明：

令$f: H \to aH$　即$f(h)=a*h$，其中$h \in H$则f是双射。

满射是显然的，下面再证它是单射。

若$a * h_1=a * h_2$，$h_1,h_2 \in H$，则根据群的可约律知

$h_1=h_2$，即$f(h_1)=f(h_2)$导出$h_1=h_2$。

所以　|gH|=|H|

(2) 含义，若$<H,*>$为群$<G$，$*>$的子群，则H为$<G,*>$中的左陪集。

因为若e是$<G,*>$的幺元，则$e*H=\{e*h|h \in H|=H$。

定理6.4. 2

设<H,*>为<G,*>的子群，有

(1) a ∈ aH

(2) 若 b ∈ aH，则 bH = aH

证明:(1)因为$e \in H$，故$a=a*e \in aH$。

(2)若 b ∈ aH ,b=a*h,

bH=(a*h)H=a(hH)=aH

定理6.3 6.

若$<H,*>$是群$<G,*>$的子群，则或者$aH\cap bH=\varnothing$或者$aH=bH$。

定理6.4.4

若$<H,*>$是群$<G,*>$的子群，对任意a,b $\in G$,则a,b属于H的同一左陪集$\Leftrightarrow b^{-1}*a\in H$ 即

$aH=bH\Leftrightarrow b^{-1}*a\in H$

推论 左陪集aH中的任何元素a_1均可决定该陪集，或者说，陪集中的每个元素都可作为陪集的代表。

因为若$a_1 \in aH$，则存在$h_1 \in H$，使得$a1=a*h_1$，于是$a^{-1}*a_1=h_1 \in H$。

再根据定理6.4.4 知，$a_1H=aH$。

定理6.4.5

若<H,*>是群<G,*>的子群，则R={<a,b>|a,b$\in H$，$a^{-1}*b\in H$}是G上的一个等价关系，且$[a]_R$=a H, 称R为群G上H的左陪集等价关系。

由等价关系与划分关系得知：

若$<H,*>$是群$<G,*>$的子群，则$<G，*>$中的H的左陪集簇构成G的一种划分。并且称它为G的对于H的左陪集划分。

假若群$<G，*>$为有限群，其子群是$<H，*>$，且$|G|=n$，$|H|=m$，则G的对于H的左陪集划分可表为$G=a_1H\cup a_2H\cup\cdots\cup a_kH$，其中$k$为不同的左陪集个数，称为$H$在$G$中的指标，由于每个左陪集皆有$m$个元素，故$G$具有$km$个元素，即$n=mk$，这便得到著名拉格朗日(J.L.Lagrange)定理：

定理6.4.6 拉格朗日(J.L.Lagrange)定理

若<H，*>是有限群<G，*>的子群，那么 |H| | |G| (H的阶整除G的阶）。

即：任何有限群的阶均可被其子群的阶所整除。。

推论1: 有限群<G, *>中任何元素的阶均为G的阶因子。

推论2: 质数阶的群没有非平凡子群。

推论3 : 4阶群同构于4阶循环群或 Klein 四元群

例：设 G={0，60，120，180，240，300},在 G 上定义二元运算*,如表所示，

求 G 的所有循环子群？并给出每一个非平凡子群的左陪集

*	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

解：循环子群共4个，分别为：

H1={0，60，120，180，240，300}，H2={0}，

H3={0，120，240}，　　H4={0，180}

其中H1和H2为平凡子群，H3和H4为非平凡子群

H3的左陪集为：{0，120，240}和{60，180,300}

H4的左陪集为：{0，180}、{60，240}、{120，300}

第6章　几个典型的代数系统

6.1 半群与群

6.2　子群

6.3 循环群和置换群

6.4 陪集与拉格朗日定理

6.5 正规子群、商群和同态基本定理

6.6 环

6.7 域

6.8 有限域

第6章　几个典型的代数系统

6.1 半群与群

6.2 子群

6.3 循环群和置换群

6.4 陪集与拉格朗日定理

6.5 正规子群、商群和同态基本定理

6.6 环与域

6.6 环与域

定义6.6.1　环

设<R,+,·>是代数系统,R为集合,+,·为二元运算,如果

(1)<R,+>为阿贝尔群（加群），

(2)<R,·>为半群,

(3)乘法·对加法+适合分配律,

则称<R,+,·>是环

约定：定义中的+,·表示一般二元运算，称为环中的加法和乘法运算，不一定是数乘和数加。

符合说明：0,1，-x, x^{-1}, nx, x^n,x-y

例　如

- ✓ $\langle Z,+,\cdot\rangle$,$\langle Q,+,\cdot\rangle$和$\langle R,+,\cdot\rangle$都是环,+和·表示普通加法和乘法.
- ✓ $\langle M_n(R),+,\cdot\rangle$是环,其中$M_n(R)$是n阶实矩阵的集合,+,·分别是矩阵加法和乘法.
- ✓ $\langle Z_n,\oplus,\odot\rangle$是模n的整数环,其中$Z_n = \{0,1,\ldots,n-1\}$, $\oplus$和$\odot$分别表示模n的加法和乘法.
- ✓ $\langle Mn\times n, +, \times\rangle$是环，其中$Mn\times n$是$n\times n$阶实矩阵的全体，＋与×是矩阵的加法和乘法.

定理6.6.1

设<R,+,·>是环,0为加法幺元, -a为a的逆元, 那么对

(1) $\forall\ a \in R,\quad a\cdot 0 = 0\cdot a = 0.$

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

(3) $\forall\ a,b \in R,\quad (-a)(-b) = ab.$

(4) $\forall\ a,b,c \in R,\quad a(b-c)=ab-ac,$

$(b-c)a = ba - ca.$

(1) $\forall\ a\in R, a\cdot 0=0\cdot a=0.$

证明: $a\cdot 0=a\cdot(0+0)=a\cdot 0+a\cdot 0,$

由加法消去律得

$$0=a\cdot 0.$$

同理可证 $0\cdot a=0.$

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

证明: $(-a)b+ab=(-a+a)b=0.b=0$

类似地有 $ab+(-a)b=0,$

所以$(-a)b$是ab的加法逆元,即$-(ab)$.

同理可证 $a(-b)=-(ab)$

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

证明:

$$(-a)(-b)=-(a(-b))=-(-(ab))=ab,$$

(4) $\forall\ a,b,c\in R,a(b-c)=ab-ac,$

$$(b-c)a=ba-ca.$$

证明:

$$a(b-c)=a(b+(-c))=ab+a(-c)=ab-ac$$

同理有 $(b-c)a=ba-ca$

定义6.6.2： 交换环、含幺环

在环<R,+,·>中,如果乘法·适合交换律,则称R是**交换环**.

如果对于**乘法有幺元**,则称R是**含幺环**.

以

为了区别含幺环中加法幺元和乘法幺元,通常把**加法幺元记作0,乘法幺元记作1**.可证明加法幺元0恰好是乘法的零元.

定义6.6.3：零因子环

在环<R,+,·>中,如果存在
$a,b \in R, a \neq 0, b \neq 0$,但$ab = 0$,则称a,b为R的零因子，并称R为零因子环，否则称R为无零因子环.

或者：若ab=0 有a=0或b=0，则R为无零因子环

$\langle Z,+,\cdot\rangle$,$\langle Q,+,\cdot\rangle$和$\langle R,+,\cdot\rangle$

都是无零因子环,

$\langle Z_n,\oplus,\odot\rangle$

不一定是无零因子环.

例:

$\langle Z_6,\oplus,\odot\rangle$中有$2\odot 3=0$,但2和3都不是0.$\langle Z_6,\oplus,\odot\rangle$不是无零因子环,

$\langle Z_5,\oplus,\odot\rangle$是无零因子环.

定理6.6.2

设<R,+,·>是环，那么R中无零因子当且仅当R中乘法运算满足消去律。

证明：必要性

设R 中无零因子，a≠0,若a·b=a·c,有

a(b-c）=0,因无零因子，所以b-c=0，即c=b

充分性：反证法

假设R中有零因子，a≠0，b≠0,但是a·b=0;

有a·b=a·0，已知满足消去律，所以b=0,矛盾。

整环、域

定义6.6.4 :整环: 若环<R,+,·>是交换、含幺和无零因子的,则称R为整环.

例1: p,q为不等的素数，证明无pq阶的整环。

证明；（反证法）假设R为pq阶的整环，则<R,+>为pq阶的Abel群。

存在p阶元a, 阶元b,所以|a+b|=pq,<R,+>为循环。

令c=a+b为生成元，R={0,c,2c,…(pq-1)c}

取x=pc,y=qc,则xy=(pc)(qc)=（pqc）c=0

则x,y为零因子。与假设矛盾。原命题成立。

子环

定义6.6.5 :子环

设$\langle R, +, \cdot \rangle$是环，如果有集合S满足

1. $\langle S, + \rangle$ 为$\langle R, + \rangle$的子群；
2. $\langle S, \cdot \rangle$ 为$\langle R, \cdot \rangle$的子半群；

则称$\langle S, +, \cdot \rangle$ 为$\langle R, +, \cdot \rangle$ 的子环。

例6.7.8 设〈R，+，·〉是含幺环，对任意x∈R，都有x·x = x，证明：对任意x，y∈R
（1）x + x = 0 。 （2）x·y = y·x。

证明 （1）∀x∈R，由运算的封闭性知，x+x ∈R，由题设（x+x）·（x+x）= x+x，所以

- （x·x + x·x）+（x·x + x·x）= x+x
- 即 （x+x）+（x+x）= x+x
- 因为〈R，+〉是交换群，所以x+x的逆元是–（x+x），故
- （x+x）+（x+x）-（x+x）=（x+x）-（x+x）= 0
- 得 x+x = 0

2. （2）任取x，y∈R，由于x+y∈R，所以
   - （x+y）·（x+y）= x+y
   - 即 x·x + x·y + y·x + y·y = x+y
   - x + y + x·y + y·x = x+y
   - 推得 x·y + y·x = 0
- 由（1）的结果推得 x·y = y·x

第6章　几个典型的代数系统

6.1 半群与群

6.2　子群

6.3 循环群和置换群

6.4 陪集与拉格朗日定理

6.5 正规子群、商群和同态基本定理

6.6 环

6.7 域

6.8 有限域

域 (Field)

定义 设$\langle F, +, \cdot \rangle$是一个代数系统，若满足

1. $\langle F, + \rangle$是阿贝尔群；
2. $\langle F - \{0\}, \cdot \rangle$是阿贝尔群；
3. 运算$\cdot$对运算$+$是可分配的

则称$\langle F, +, \cdot \rangle$是域。

例6.5 设S为下列集合,+和.为普通加法和乘法.

$(1)S=\{x \mid x=2n \wedge n\in Z\}.$

$(2)S=\{x \mid x=2n+1 \wedge n\in Z\}.$

$(3)S=\{x \mid x\in Z \wedge x\geq 0\}=N,$

$(4)S=\{x \mid x=a+b\sqrt{3},a,b\in Q\}.$

问S和+,·能否构成域？为什么？

解：

(1) 不是域,因为乘法么元是$1,1\notin S$.

(2) 也不是域,因为S不是环,普通加法的么元是$0,0\notin S$,

(3)S不是环,因为除0以外任何正整数x的加法逆元是-x,而

$-x\notin S$当然也不是域.

(4)S是域.对任意$x_1,x_2 \in S$有

$x_1 = a_1+b_1\sqrt{3}, x_2=a_2+b_2\sqrt{3}$,

$x_1+x_2=a_1+a_2+(b_1+b_2)\sqrt{3} \in S.$

$x_1x_2=(a_1a_2+3b_1b_2)+(a_1b_2+a_2b_1)\sqrt{3} \in S$

S对+和.是封闭的.又乘法么元$1\in S$,易证<S,+,·>是整环,$\forall x\in S, x\neq 0, x=a+b\sqrt{3}$有

$$\frac{1}{x}=\frac{1}{a+b\sqrt{3}}$$
$$=\frac{a-b\sqrt{3}}{\sqrt{a^2-3b^2}}$$
$$=\frac{a}{a^2-3b^2}-\frac{b}{a^2-3b^2}\sqrt{3}$$

所以<S,+,·>是域.

域都是整环

定理6.7.2

有限整环都是域。

证明：设$<R,+,\cdot>$是有限整环，则$<R,\cdot>$是有限含么、交换、无零因子（满足消去律）半群。只需要证明每个元素有逆元。

定义6.6.5 :**子域**

设$\langle F,+,\cdot\rangle$是域，$\langle S,+,\cdot\rangle$为F的子环，且$\langle S,+,\cdot\rangle$为一域，则称$\langle S,+,\cdot\rangle$为$\langle R,+,\cdot\rangle$的**子域**。

定理6.6.5 :

设$\langle F,+,\cdot\rangle$是域，F'是F的子集，且F'中至少有两个元素，那么$\langle F',+,\cdot\rangle$为$\langle F,+,\cdot\rangle$的子域当且仅当F'满足

(1) $\langle F',+\rangle$为$\langle F,+\rangle$的子群；

(2) $\langle F',\cdot\rangle$为$\langle F,\cdot\rangle$的子群；

第6章　几个典型的代数系统

6.1 半群与群

6.2　子群

6.3 循环群和置换群

6.4 陪集与拉格朗日定理

6.5 正规子群、商群和同态基本定理

6.6 环

6.7 域

6.8 有限域

$\langle Z_p, +_p, \times_p \rangle$为域当且仅当 p为素数。

证明：必要性

设p不是素数，那么Z_p有零因子（p的因子），故$\langle Z_p, +_p, \times_p \rangle$不是域.

- 充分性
- 当p为素数时，只需证Z_p中所有非零元素都有$\times_p$运算的逆元，从而Z_p是含么交换环$\langle Z_p, +_p, \times_p \rangle$为域。

设q是Z_p中任一非零元素，那么q与p互质．据有整数m, n使 $mp + nq = 1$;

- 从而$(mp+nq) \pmod p = 1$
  - 即$mp \pmod p +_p nq \pmod p = 1$;
  - $0 + n \pmod p \times_p q \pmod p = 1$，或 $n \pmod p \times_p q = 1$
  - 因此，q有逆元$n \pmod p$ 。　　得证。

素数与密码(RSA码)

本世纪七十年代，几位美国数学家提出一种编码方法，这种方法可以把通讯双方的约定公开，然而却无法破译密码，这种奇迹般的密码就与素数有关。

人们知道，任何一个自然数都可以分解为素数的乘积，如果不计因数的次序，分解形式是唯一的。这叫做算术基本定理，欧几里得早已证明了的。可是将一个大整数分解却没有一个简单通行的办法，只能用较小的素数一个一个去试除，耗时极大。如果用电子计算机来分解一个100位的数字，所花的时间要以万年计。可是将两个100位的数字相乘，对计算机却十分容易。美国数学家就利用了这一点发明了编制容易而破译难的密码方式。这种编码方式以三位发明者姓氏的首字母命名为RSA码。

素数与密码(RSA码)

例如，A、B两位通讯者约定两个数字N和e，A想要将数字M发给B，他不是直接将M发出，而是将M连乘e次，然后除以N，将余数K发给B。B有一个秘密的数字d，连A也不知道，他将K连乘d次，然后除以N，得到的余数就是原来的数M。

数字是这样选择的，$N=p\times q$，**p、q是选定的两个大的素数**，选取e、d，使ed-1是$(p-1)\times(q-1)$的倍数，而且使e和p-1、q-1没有公因数，这是容易做到的。根据这个方法，编码规则可以公开，可是由于N太大，分解得到p、q几乎是不可能的，他人也就无从知道d，不可能破译密码了。

RSA提出后，悬赏100美元破译，他们预言人们至少需要20000年，计算机也需要200年。但只过了不到18年，这个密码就被人利用计算机网络，不到一年的时间，就将129位的N分解成64位和65位的两个素数的积。计算机网络将分解效率提高了近万倍，但是，如果提高位数到200或300位，工作量将会大的不可思议，即使计算机技术有重大突破，破译也几

素数测试

素数的研究和密码学有很大的关系，而素数的测试又是素数研究中的一个重要课题。

费尔马小定理：如果n是一个素数，且0<a<n，则$a^{n-1} \equiv 1 \pmod{n}$。

二次探测定理：如果n是一个素数，且0<x<n，则方程$x^2 \equiv 1 \pmod{n}$的解为x=1， x= -1。

证明 $x^2 \pmod{n} \equiv 1 \Leftrightarrow x^2 - 1 \equiv 0 \pmod{n}$

$\Leftrightarrow (x+1)(x-1) \equiv 0 \pmod{n}$

$\Rightarrow x+1=0$ 或 $x-1=0$ （域中没有零因子）

$\Leftrightarrow x=-1$ 或 $x=1$

称$x \neq \pm 1$的根为非平凡的.

素数测试

- 素数的研究和密码学有很大的关系，而素数的测试又是素数研究中的一个重要课题。
- **费尔马小定理**：如果p是一个素数，且0<a<p，则$a^{p-1} \equiv 1 (\text{mod } p)$。
- 利用该定理设计一个判断n是否为素数的可能性。
- 算法 指数运算后求模
- 输入：正整数a,n,m,m<n
- 输出：$a^m \ (\text{mod } n)$

```
Int exp_mod(int n, int a, int m)
{   int i,c,k=0;
    int *b=new int (n)
   While (m!=0) {b[k++]=m %2;  m/=2;}/*把m转换为二进制数字于b[k]*
   c=1;
    For (i=k-1; i>=0; i- -)            /*计算a^m (mod n)*/
            { c=(c*c)%n;
              if (b[k]==1  c=(a*c)%n}
    Return c;
}
```

算法**prime**是一个偏假3/4正确的蒙特卡罗算法。通过多次重复调用错误概率不超过$(1/4)^k$。这是一个很保守的估计，实际使用的效果要好得多。

设n为大于等于5的奇素数，写为$n-1=2^q m$，因为n-1是偶数，所以q>=1，由Femat定理，序列

$a^m \pmod n$, $a^{2m} \pmod n$, $a^{4m} \pmod n$，…..

必定以1结束

，而且在第一次出现1至前的值必定是n-1,这是因为当n是素数时，$x^2 \equiv 1 \pmod n$的唯一解是x=1或x=-1 。

作 业

P190-194

6.1 ; 6.3; 6.4; 6.5; 6.5;6.6,6.7;

6.8; 6.9; 6.10; 6.11; 6.15(1) ;6.16

6.17; 6.18; 6.22 ; 6.23; 6.27

6.30; 6.32; 6.41; 6.43; 6.44