第 三 篇

代 数 系 统

第三篇　代数系统（Algebraic System ）

人们研究和考察现实世界中的各种现象或过程，往往要借助某些数学工具。譬如，在微积分学中，可以用导数来描述质点运动的速度，可以用定积分来计算面积、体积等；在代数学中，可以用正整数集合上的加法运算来描述工厂产品的累计数，可以用集合之间的“并”、“交”运算来描述单位与单位之间的关系等。

第三篇　代数系统（Algebraic System ）

针对某个具体问题选用适宜的数学结构去进行较为确切的描述，这就是所谓的“数学模型”。可见，数学结构在数学模型中占有极为重要的位置。我们这里所要研究的是一类特殊的数学结构—由集合上定义若干个运算而组成的系统。我们通常称它为代数系统。它在计算机科学中有着广泛的应用。

第五章　代数结构（Algebraic Structure）

本章在集合、关系和函数等概念基础上，从一般代数系统的引入出发，研究更为复杂的对象——代数系统，研究代数系统的性质和特殊的元素，代数系统与代数系统之间的关系。如代数系统的同态和同构，这些概念较为复杂也较为抽象，是本课程中的难点。它们将集合、集合上的运算以及集合间的函数关系结合在一起进行研究。

前两章内容是本章的基础，熟练地掌握集合、关系、函数等概念和性质是理解本章内容的关键。

第五章　代数结构（Algebraic Structure ）

5-1 代数系统的引入

5-2 运算及其性质

5-3 半群

5-4 群与子群

5-5 阿贝尔群与循环群

*5-6 置换群与伯恩赛德定理

5-7 陪集与拉格朗日 定理

5-8 同态与同构

5-9 环 和 域

5-1 代数系统的引入

介绍代数系统之前，引进在一个集合A上的运算概念

例1：f：R→R　　g：R→R

f(x)=1/x ， x≠0　　g(x)=[x]

将这些映射称为在集合R上的一元运算；

例2：　f：R^2→R　　g：R^2→R

f(<x,y>)=x+y,　　g(<x,y>)=x*y,

x+y=z　　x*y=z

在集合R上，对任意两个数所进行的普通加法和乘法，都是集合R上的二元运算；

5-1 代数系统的引入

至于对集合R上的三个数x，y，z，程序设计语言中的条件算术表达式:

if x==0 then y else z，

这就是集合R上的三元运算。

上述一些例子，有一个共同的特征，就是其运算结果都是在原来的集合R中，我们称那些具有这种特征的运算是封闭的,简称闭运算。相反地，没有这种特征的运算就是不封闭的。

5-1 代数系统的引入

定义5-1.1 [n元运算]

对于集合A，一个从A^n到B的映射，称为集合A上的一个n元运算。如果$B \subseteq A$，则称该n元运算是封闭的。

定义5-1.2[代数系统]

一个非空集合A连同若干个定义在该集合上的运算$f_1,f_2,\ldots,f_k$所组成的系统就称为一个代数系统，记作$<A,f_1,f_2,\ldots,f_k>$。

5-1 代数系统的引入

正整数集合I^+以及在该集合上的普通加法运算“+”组成一个代数系统$<I^+, +>$。

又如，一个有限集S，由S的幂集$\mathcal{P}(S)$以及在该集合上的集合运算“∪”、“∩”、“~”组成一个代数系统$<\mathcal{P}(S), \cup, \cap, \sim>$。

虽然，有些代数系统具有不同的形式，但是，他们之间可能有一些共同的运算规律。

5-1 代数系统的引入

容易找到与<I,+>具有相同运算规律的一些代数系统，如表所示：

	<I, .>	<R,+>	<P(S),∪>	<P(S), ∩ >
集合 运算 封闭性 交换律 结合律	I为整数集合 ·为普通乘法 $x\cdot y\in I$ $x\cdot y=y\cdot x$ $(x\cdot y)\cdot z=x\cdot(y\cdot z)$	R为实数集合 +为普通加法 $x+y\in R$ $x+y=y+x$ $(x+y)+z=x+(y+z)$	P(S)是S的幂集∪为集合的“并” $A\cup B\in P(S)$ $A\cup B=B\cup A$ $(A\cup B)\cup C=A\cup(B\cup C)$	P(S)是S的幂集∩为集合的“交” $A\cap B\in P(S)$ $A\cap B=B\cap A$ $(A\cap B)\cap C=A\cap(B\cap C)$

5-2 运算及其性质

定义5-2.1[运算封闭]

设*是定义在集合A上的二元运算，如果对于任意的x,y∈A,都有x*y∈A,则称二元运算*在A上是封闭的。

定义5-2.2[运算可交换]

设*是定义在集合A上的二元运算，如果对于任意的x,y∈A,都有x*y=y*x，则称该二元运算*是可交换的，或运算满足交换律。

5-2 运算及其性质

定义5-2.3[运算可结合]

设*是定义在集合A上的二元运算，如果对于任意的x,y,z∈A都有(x*y)*z=x*(y*z),则称该二元运算*是可结合的，或运算满足结合律。

5-2 运算及其性质

定义5-2.4[运算可分配]

设*，Δ是定义在集合A上的两个二元运算，如果对于任意的x,y,z∈A都有

$$x*(y\Delta z)=(x*y)\Delta(x*z)$$

$$(y\Delta z)*x=(y*x)\Delta(z*x)$$

则称运算*对于运算Δ是可分配的。

5-2 运算及其性质

例题1 设$A=\{x|x=2^n,n\in N\}$,问乘法运算是否封闭？对加法运算呢？

解：对于任意的$2^r,2^s\in A$; $r,s\in N$;

$$2^r\cdot 2^s=2^{r+s}\in A(\text{因为}r+s\in N)$$

所以乘法运算是封闭的。

而对于加法运算是不封闭 的，因为至少 有$2+2^2=6\notin A$。

5-2 运算及其性质

例题2 设Q是有理数集合，Δ是Q上的二元运算，对任意的a，b∈Q, aΔb=a+b-a·b，问运算Δ是否可交换。

解：因为aΔb=a+b-a·b=b+a-b·a=bΔa，所以运算Δ是可交换的。

5-2 运算及其性质

例题3 设A是一个非空集合，★是A上的二元运算，对于任意a,b∈A,有a★b=b,证明★是可结合运算。

证明： 因为对于任意的a,b,c∈A，

(a★b)★c=b★c=c，

而 a★(b★c)=a★c=c，

所以 (a★b)★c=a★(b★c)

5-2 运算及其性质

例题 4 设集合A={α，β}，在A上定义两个二运算*和Δ如表所示。运算Δ对于运算*可分配吗？运算*对于运算Δ呢？

*	α	β
α	α	β
β	β	α

Δ	α	β
α	α	α
β	α	β

解：容易验证运算Δ对于运算*是可分配的。

但是运算*对于运算Δ是不可分配的，

因为 β*(αΔβ) =β*α=β，

而（β*α）Δ（β*β）=βΔα=α。

5-2 运算及其性质

定义5-2.5[吸收律]

设*，Δ是定义在集合A上的两个可交换二元运算，如果对于任意的x,y∈A,都有

$$x*(x\Delta y)=x$$

$$x\Delta(x*y)=x$$

则称运算*和运算Δ满足吸收律。

5-2 运算及其性质

例题5： 设集合N为自然数全体，在N上定义两个二元运算*和★，对于任意x,y∈N,有

$$x*y=\max(x,y)$$
$$x★y=\min(x,y)$$

验证运算*和★满足吸收律。

解： 对于任意a,b∈N，

$$a*(a★b)=\max(a,\min(a,b))=a,$$
$$a★(a*b)=\min(a,\max(a,b))=a$$

因此，*和★满足吸收律。

5-2 运算及其性质

定义5-2.6[运算等幂]

设*是定义在集合A上的一个二元运算，如果对于任意的x∈A,都有x*x=x,则称运算*是等幂的，或称运算满足等幂律。

5-2 运算及其性质

定义5-2.7[幺元]

设*是定义在集合A上的一个二元运算，如果有一个元素$e_l \in A$,对于任意的元素$x \in A$都有$e_l * x = x$,则称e_l为A中关于运算*的左幺元；如果有一个元素$e_r \in A$,对于任意的元素$x \in A$都有$x * e_r = x$,则称e_r为A中关于运算*的右幺元；

如果A中的一个元素e,它既是左幺元又是右幺元，则称e为A中关于运算*的幺元。显然，对于任一$x \in A$,有$e*x=x*e=x$。

5-2 运算及其性质

例题 6： 设集合S={α，β，γ，δ}，在S上定义的两个二元运算*和★如表示。试指出左幺元或右幺元。

*	α	β	γ	δ
α	δ	α	β	γ
β	α	β	γ	δ
γ	α	β	γ	γ
δ	α	β	γ	δ

★	α	β	γ	δ
α	α	β	δ	γ
β	β	α	γ	δ
γ	γ	δ	α	β
δ	δ	δ	β	γ

解：由表可知：β，δ都是S中关于运算*的左幺元，而α是S中关于运算★的右幺元。

5-2 运算及其性质

定理5-2.1

设*定义在集合A上的一个二元运算，且在A中有关于运算*的左幺元e_l和右幺元e_r,则$e_l=e_r=e$,且A中的幺元是唯一的。

⑩ □ 证明：先证左幺元e_l=右幺元e_r=e

⑩ $e_l= e_l *e_r = e_r=e$

再证幺元e是唯一的

设还有一个幺元e’ ∈A,则

e’ = e’ * e = e □

5-2 运算及其性质

定义5-2.8[零元]

设*是定义在集合A上的一个二元运算，如果有一个元素$\theta_l \in S$，对于任意的元素$x \in A$都有$\theta_l * x = \theta_l$，则称θ_l为A中关于运算*的左零元，如果有一个元素$\theta_r \in A$，对于任意的元素$x \in A$都有$x * \theta_r = \theta_r$，则称θ_r为A中关于运算*的右零元；

如果A中的一个元素θ，它既是左零元又是右零元，则称θ为A中关于运算*的零元。显然，对于任一$x \in A$，有 $\theta * x = x * \theta = \theta$

5-2 运算及其性质

定理5-2.2

设*是定义在集合A上的一个二元运算，且在A中有关于运算*的左零元θ_l和右零元θ_r，那么，$\theta_l=\theta_r=\theta$，且A中的零元是唯一的。

⑩ 证明：**先证**$\theta_l=\theta_r=\theta$

⑩ $\theta_l=\theta_l * \theta_r=\theta_r= \theta$

- **再证零元θ是唯一的**

设还有一个幺元 θ’ ∈A,则

θ’ =θ’ * θ = θ □

5-2 运算及其性质

定理5-2.3

设<A,*>是一个代数系统，且集合A中元素的个数大于1。如果该代数系统中存在幺元e和零元θ,则θ≠e。

⑩ 证明：**用反证法:**

⑩ 设**幺元e =零元θ**，则对于任意**x∈A**，必有

⑩ $$x = e * x = \theta * x = \theta = e$$

⑩ 于是，推出A中所有元素都是相同的，矛盾。

□

5-2 运算及其性质

定义5-2.9[逆元]

设代数系统<A,*>，这里*是定义在A上的一个二元运算，且e是A中关于运算*的幺元。如果对于A中的一个元素a存在着A中的某个元素b,使得b*a=e,那么称b为a的左逆元；如果a*b=e成立，那么称b为a的右逆元；如果一个元素b,它既是a的左逆元又是a右逆元，那么就称b是a的一个逆元。

很明显，如果b是a的逆元，那么a也是b是逆元，简称a与b互为逆元。今后一个元素x的逆元记为x^{-1}。

5-2 运算及其性质

例题 7： 设集合S={浅色，深色}，定义在S上的一个二元运算*如表所示，试指出零元和幺元。

*	浅色	深色
浅色	浅色	深色
深色	深色	深色

解：深色是S中关于运算*的零元，

浅色是S中关于运算*的幺元。

5-2 运算及其性质

例题8： 设集合S={α,β,γ,δ,}，定义在S上的一个二元运算*如表所示。试指出代数系统<S,*>中各个元素的左、右逆元情况。

*	α	β	γ	δ	ε
α	α	β	γ	δ	ε
β	β	δ	α	γ	δ
γ	γ	α	β	α	β
δ	δ	α	γ	δ	γ
ε	ε	δ	α	γ	ε

5-2 运算及其性质

解：α是幺元；β的左逆元和右逆元都是γ；即β和γ互为逆元；δ的左逆元是γ而右逆元是β；β有两个左逆元γ和δ；ε的右逆元是γ，但没有左逆元。

5-2 运算及其性质

定理5-2.4

设代数系统<A,*>, 这里*是定义在A上的一个二元运算，A中存在幺元e，且每一个元素都有左逆元。如果*是可结合的运算，那么，这个代数系统中任何一个元素的左逆元必定也是该元素的右逆元，且每个元素的逆元是唯一的。

5-2 运算及其性质

证明：设a,b,c∈A,且b是a的左逆元，c是b的左逆元。

因为 （b*a）*b=e*b=b （运算可结合）

所以 e=c*b=c*((b*a)*b)

=(c*(b*a))*b

=((c*b)*a)*b

=(e*a)*b

=a*b 因此，b也是a的右逆元。

设元素a有两个逆元b和c,那么

b=b*e=b*(a*c)

=(b*a)*c

=e*c

=c

因此，a的逆元是唯一的。

5-2 运算及其性质

可以指出：<A,*>是一个代数系统，*是A上的一个二元运算，那么该运算的有些性质可以从运算表中直接看出。那就是：

1、运算*具有封闭性，当且仅当运算表中的每个元素都属于A。

2、运算*具有可交换性，当且仅当运算表关于主对角线是对称的。

3、运算*具有等幂性，当且仅当运算表的主对角线上的每一元素与它所在行（列）的表头元素相同。

5-2 运算及其性质

4、A关于*有零元，当且仅当该元素所对应的行和列中元素都与该元素相同。

5、A关于*有幺元，当且仅当该元素所对应的行和列依次与运算表的行和列相一致。

6、设A中有幺元，a和b互逆，当且仅当位于a所在行，b所在列的元素以及其b所在行，a所在列的元素都是幺元。

5-2 运算及其性质

例题9： 试构造一个代数系统，使得其中只有一个元素具有逆元。

解： 设$m,n\in I,T=\{x|x\in I,m\leq x\leq n\}$,那么，代数系统<T,max>中有一个幺元是m,且只有m有逆元，因为m=max(m,m)。

5-2 运算及其性质

例题10： 对于代数系统<R,·>，这里R 是实数的全体，·是普通的乘法运算，是否每个元素都有逆元。

解： 该代数系统中的幺元是1，除了零元素0外，所有的元素都有逆元。

5-2 运算及其性质

例题11： 对于代数系统$<N_k,+_k>$，这里$N_k=\{0，1，2，…，k-1\}$,$+_k$是定义在N_k上的模k加法运算，定义如下：

对于任意$x,y\in N_k$，若 $x+y<k$，则 $x+y= x+y$；

若 $x+y\geq k$ ；则$x +_k y=x+y-k$ ，

试问是否每个元素都有逆元。

解： 可以验证，$+_k$是一个可结合的二元运算，N_k中关于运算$+_k$的幺元是0，N_k中的每一个元素都有唯一的逆元，即0的逆元是0，每个非零元素x的逆元是k-x。

5-2 运算及其性质

练习：N_4是整数中模4同余关系产生的等价类集合，

N_4={［0］，［1］，［2］，［3］},

N_4上运算$+_4$，$\times_4$定义为

$$[m] +_4 [n] = [(m+n) \bmod 4]$$

$$[m] \times_4 [n] = [(m \cdot n) \bmod 4]$$

其中$m,n \in \{[0],[1],[2],[3]\}$, 求特殊元素。

5-2 运算及其性质

$+_4$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$\times_4$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

解 由表5.2.4可知，［0］为幺元，

［1］$^{-1}$ = ［3］，［2］$^{-1}$= ［2］，无零元。

由表5.2.5可知，［1］为幺元，

［3］$^{-1}$= ［3］，［0］,［2］无逆元，［0］为零元。

5-2 运算及其性质

作业 5-1，2

P178 (2)

P185 (1), (2), (5)

5-3 半群

半群与群都是具有一个二元运算的代数系统，群是半群的特殊例子。事实上，群是历史上最早研究的代数系统，它比半群复杂一些，而半群概念是在群的理论发展之后才引进的。群论在各种不同的领域(如量子力学、结晶学）中都有应用。它有半群、含幺半群与群三个基本类型。在计算机科学的不同领域，它们的应用越来越广泛。

半群和含幺半群，在自动机理论、形式语言等方面的应用已卓有成效。

群的概念在自动机理论、编码理论和快速加法器的设计等方面都有广泛的应用。它们的逻辑关系见图5.3.1。

5-3 半群

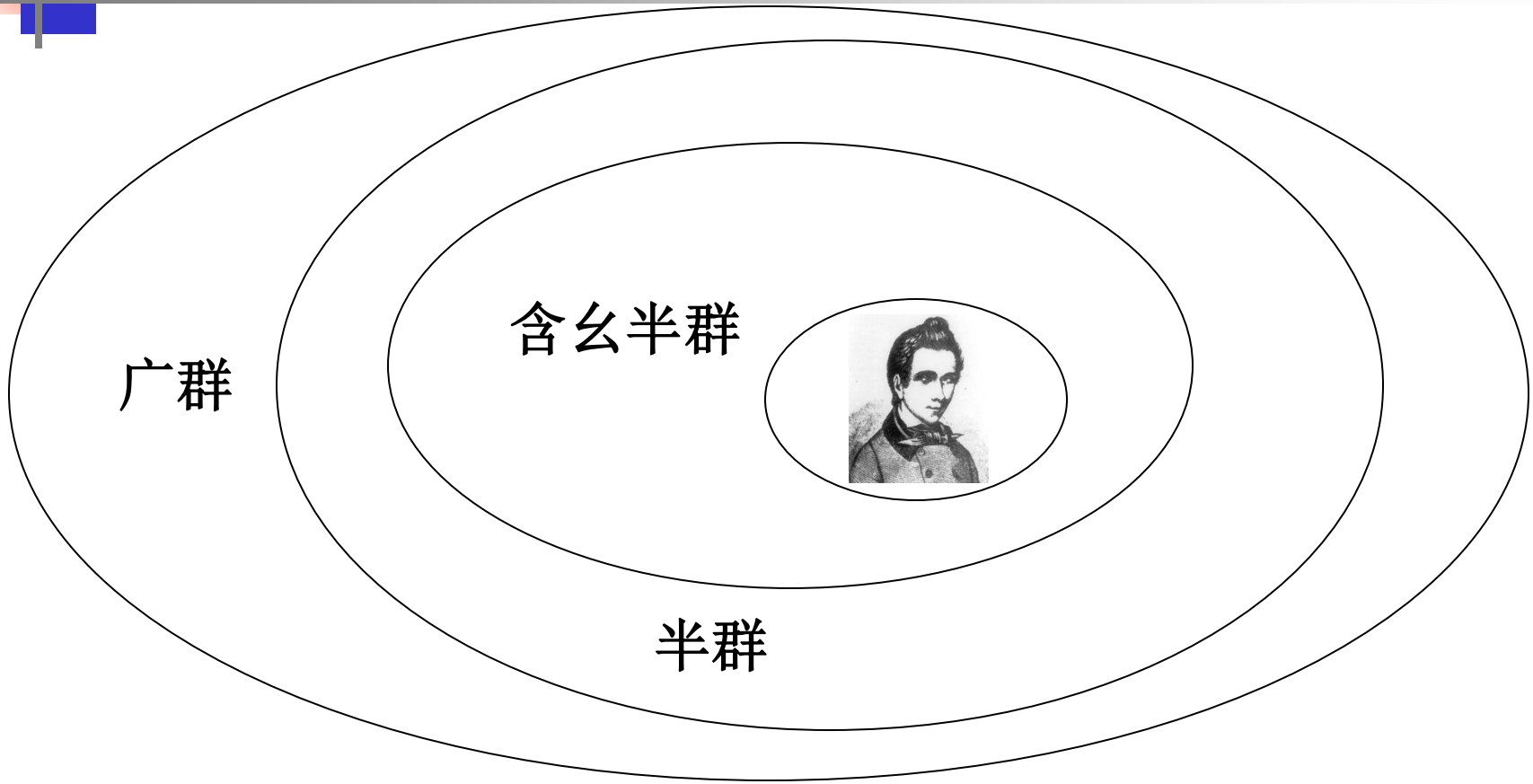

图 5.3.1

5-3 半群

定义5-3.1[广群]

一个代数系统<S,*>,其中S是非空集合，*是S上的一个二元运算，如果

（1） 运算*是封闭的。

则称代数系统<S,*>为广群。

5-3 半群

定义5-3.2[半群]

一个代数系统<S,*>,其中S是非空集合，*是S上的一个二元运算，如果

（1） 运算*是封闭的。

（2） 运算*是可结合的，即对任意的 x,y,z∈S,满足

$$(x*y)*z=x*(y*z)$$

则称代数系统<S,*>为半群。

5-3 半群

许多代数系统都是半群。例如，〈N,+〉，〈Z,×〉均是半群。但〈Z,-〉不是半群。

再如，设Σ是有限字母表，Σ^+是Σ中的字母串$\Sigma^*=\{\Phi\}\cup\Sigma^+$，其中$\Phi$是不含字母的空串，运算$\tau$是字母串的“连接”运算，则〈$\Sigma^*$,$\tau$〉是半群。如Com$\in\Sigma^*$,puter$\in\Sigma^*$,经$\tau$运算后，得Computer仍是字母串。

【例5.3.1】 $S=\left\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \middle| a,b\in R, a\neq 0\right\}$,

则〈S,·〉是半群。这里·代表普通的矩阵乘法运算。

证明 对任意的

$$\begin{bmatrix} a_1 & b_1 \\ 0 & 0 \end{bmatrix}\in S, \begin{bmatrix} a_2 & b_2 \\ 0 & 0 \end{bmatrix}\in S$$ 因为

$$\begin{bmatrix} a_1 & b_1 \\ 0 & 0 \end{bmatrix}\bullet\begin{bmatrix} a_2 & b_2 \\ 0 & 0 \end{bmatrix}=\begin{bmatrix} a_1a_2 & a_1b_2 \\ 0 & 0 \end{bmatrix}$$ 且$a_1a_2\neq 0$,所以

$$\begin{bmatrix} a_1a_2 & a_1b_2 \\ 0 & 0 \end{bmatrix}\in S$$,因此“·”运算封闭。

【例5.3.2】 $S=\{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} | a,b \in R, a \neq 0\}$

,则〈S,+〉不是半群。这里+代表普通的矩阵加法运算。

证明 对任意的 $\begin{bmatrix} a_1 & b_1 \\ 0 & 0 \end{bmatrix} \in S, \begin{bmatrix} a_2 & b_2 \\ 0 & 0 \end{bmatrix} \in S$ 取a_2=-a_1,则

$$\begin{bmatrix} a_1 & b_1 \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} a_2 & b_2 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} a_1+a_2 & b_1+b_2 \\ 0 & 0 \end{bmatrix}$$ 且a_1+a_2=0，所以

$$\begin{bmatrix} a_1+a_2 & b_1+b_2 \\ 0 & 0 \end{bmatrix} \notin S$$ 因此*运算不封闭。

所以〈S,+〉不是半群。

【例5.3.3】 $S=\{\begin{pmatrix} a & b \\ c & 0 \end{pmatrix} | a,b,c \in R\}$

则〈$S,\cdot$〉不是半群。这里·代表普通的矩阵乘法运算。

证明: 取

$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in S, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in S,$ 则 $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix},$

所以 $\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \notin S,$

因此*运算不封闭。

所以〈$S,\cdot$〉不是半群。

【例5.3.4】设$S=\{a, b\}$上的二元运算如下表：

*	a	b
a	b	a
b	a	b

则〈S,*〉为半群。

证：只需验证“*”满足结合律，由于“*”满足交换律所以仅需要考虑以下两种情况：

$$(a*a)*b = b*b = b = a*a = a*(a*b)$$

$$(a*b)*b = a*b = a = a*b = a*(b*b)$$

故〈S,*〉为半群。

5-3 半群

【例5.3.5】设S为任意非空集合，对任意$a,b \in S$,规定$a*b=a$,则〈S,*〉为半群。

证明：$\forall$ $a,b,c \in S$,有

$$(a*b)*c = a*c = a,\quad a*(b*c) = a*b = a$$

所以 $(a*b)*c = a*(b*c)$.

故〈S,*〉为半群。

【例5.3.6】对任意$a,b\in R$,规定$a*b=(a+b)/2$,则〈R,*〉不是半群。

证明：对于$1,2,3\in R$,有

$$(1*2)*3=\frac{1+2}{2}*3=\frac{\frac{3}{2}+3}{2}=\frac{9}{4}$$

$$1*(2*3)=1*\frac{2+3}{2}=\frac{1+\frac{5}{2}}{2}=\frac{7}{4}$$

所以“*” 不满足结合律.

故〈S,*〉不是半群。

【例5.3.7】 设S={a,b,c},在S上的一个二元运算Δ定义如表所示。

Δ	a b c
a b c	a b c a b c a b c

验证 <S,Δ>是一个半群。

解： 从表中可知运算Δ是封闭的，同时a,b和c都是左幺元。所以，对于任意的x,y,z∈S,都有x Δ (y Δ z)=x Δ z=z=y Δ z=(x Δ y) Δ z，因此，<S, Δ>是半群。

5-3 半群

定理5-3.1设<S,*>是一个半群，B⊆S 且*在B上是封闭的，那么<B,*>也是一个半群。通常称<B,*>是半群<S,*>的子半群。

证明：因为*在S上是可结合的，而B⊆S且*在B上封闭，所以*在B上也是可结合的，因此，<B,*>是一个半群。

5-3 半群

【例5.3.8】 设·表示普通的乘法运算，那么<[0,1],·>、< [0,1) ,·>和<I,·>都是<R,·>的子半群。

解： 首先，运算·在R上是封闭的，且是可结合的，所以<R,·>是一个半群。其次，运算·在[0,1]，[0,1)和I上都是封闭的，且[0,1] ⊂R， [0,1) ⊂ R，I ⊂ R。因此，由定理5-3.1可知<[0,1],·>、< [0,1),·>和<I,·>都是<R,·>的子半群。

5-3 半群

定理5-3.2设<S,*>是一个半群，如果S是一个有限集，则必有a∈S,使得a*a=a。

证明： 因为<S,*>是半群。对于任意的b∈S,由*的封闭性可知

$b*b \in S$,记$b^2=b*b$

$b^2*b=b*b^2 \in S$,记$b^3=b^2*b$

…

一个有限半群里必有一个等幂元

因为S是有限集，所以必定存在j>i,使得$b^i=b^j$

令 p=j-i，便有 $b^i = b^p * b^i$ ，所以 $b^q = b^p * b^q$ $q \geq i$

因为 p≥1,所以总可以找到k≥1,

使得kp≥i, 对于S中的元素b^{kp},就有$b^{kp} = b^p * b^{kp} = b^p *(b^p * b^{kp}) = b^{2p} * b^{kp} = \ldots = b^{kp} * b^{kp}$

这就证明了在S中存在元素$a= b^{kp}$, 使得 a*a=a

5-3 半群

定义5-3.3[独异点]

含有幺元的半群称为独异点。

例如：代数系统<R,+>是一个独异点。

因为，<R,+>是一个半群，且0是R中关于运算+的幺元。另外，代数系统<I, ·>, <I^+, ·>, <R,·> 都是具有幺元1的半群，因此它们都是独异点。

5-3 半群

定理 5-3.3设<S,*>是一个独异点，则在关于运算*的运算表中任何两行或两列都是不相同的。

证明：设S中关于运算*的幺元是e。因为对于任意的a,b∈S且a≠b时，

总有e*a=a≠b=e*b 和 a*e=a≠b=b*e

所以，在*的运算表中不可能有两行或两列是相同的。

5-3 半群

例题3: 设Z 是整数集合，m是任意正整数，Z_m 是由模m的同余类组成的同余类集，在Z_m 上定义两个二元运算$+_m$和$\times_m$分别如下：

对于任意的[i], [j] $\in Z_m$

$[i] +_m [j]=[(i+j) \pmod m]$,

$[i]\times_m [j]=[(i\times j) \pmod m]$

试证明在这两个二元运算的运算表中任何两行或两列都不相同。

5-3 半群

上例中，如果给定m=5，那么，+5和×5的运算表分别如表5-3.2和表5-3.3所示。

$+_5$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

$\times_5$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

5-3 半群

证明：考察代数系统$<Z_m,+_m>$和 $<Z_m,\times_m>$。

(1)由运算$+_m$和$\times_m$的定义，可知它们在Z_m上是封闭的。

(2)对于任意$[i],[j],[k]\in Z_m$

$$([i]+_m[j])+_m[k]=[i]+_m([j]+_m[k])$$
$$=[(i+j+k)\ (\mathrm{mod}\ m)]$$
$$([i]\times_m[j])\times_m[k]=[i]\times_m([j]\times_m[k])$$
$$=[(i\times j\times k)\ (\mathrm{mod}\ m)]$$

即$+_m$，$\times_m$都是可结合的。

(3) 因为 $[0]+_m[i]=[i]+_m[0]=[i]$,所以，[0]是$<Z_m,+_m>$中的幺元。
因为$[1]\times_m[i]=[i]\times_m[1]=[i]$,所以[1]是$<Z_m,\times_m>$中的幺元。

因此，代数系统$<Z_m,+_m>$，$<Z_m,\times_m>$都是独异点。由定理5-3.3可知，这两个运算的运算表中任何两行或两列都不相同。

5-3 半群

定理5-3.4 设<S,*>是独异点，对于任意a,b∈S,且a,b均有逆元，

则 a) $(a^{-1})^{-1}=a$

b) a*b有逆元，且$(a*b)^{-1}=b^{-1}*a^{-1}$

证明 a) 因为a^{-1}是a的逆元，即

$a*a^{-1}=a^{-1}*a=e$

所以$(a^{-1})^{-1}=a$

b) 因为 $(a*b)*(b^{-1}*a^{-1})=a*(b*b^{-1})*a^{-1}=a*e*a^{-1}=a*a^{-1}=e$

同理可证 $(b^{-1}*a^{-1})*(a*b)=e$

所以 $(a*b)^{-1}=b^{-1}*a^{-1}$

5-3 半群

作业5-3

P190 (1),(3),(5),(6)

5-4 群与子群(groups and subgroups)

5-4.1 群的基本概念(The concept of group)

5-4.2 群的基本性质(The properties of groups)

5-4.3 子群(Subgroups)

5-4 群与子群(groups and subgroups)

定义5-4.1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） 存在幺元e。

（4） 对于每一个元素x∈G,存在着它的逆元x^{-1}。

则称<G,*>是一个群。

5-4 群与子群(groups and subgroups)

定义5-4.2 [有限群][无限群]

设<G,*>是一个群。如果G是有限集，那么称<G,*>为有限群，G中元素的个数通常称为该有限群的阶数，记为|G|；如果G是无限集，则称<G,*>为无限群。

5-4 群与子群(groups and subgroups)

【例5.4.1】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。并规定旋转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：（见书P191）

【例5.4.2】

(1) $\langle Z,+\rangle$，$\langle Q,+\rangle$，$\langle R,+\rangle$，$\langle C,+\rangle$ 均为群（加群），数0 为其幺元。

(2) $\langle R,\cdot\rangle$，$\langle Z,\cdot\rangle$，$\langle Q,\cdot\rangle$ 都不是群。因为0没有逆元。

(3) $\langle R-\{0\},\cdot\rangle$，$\langle Q-\{0\},\cdot\rangle$，$\langle Q^{+},\cdot\rangle$（正有理数与数乘）均为群，1为其么元。但 $\langle Z-\{0\},\cdot\rangle$ 不是群。

(4) $\langle N_4,+_4\rangle$ 为一4阶群,数0为其么元。

(5) $A\neq\varnothing$，$\langle 2^{A},\cup\rangle$ 是半群，么元为 $\varnothing$，非空集合无逆元， 所以不是群。

5-4 群与子群(groups and subgroups)

【例5.4.3】设$g=\{e,a,b,c\}$,*为G上的二元运算，它由表5.4.1给出,不难证明G是一个群。且e是G中的幺元；G中任何元素的逆元就是它自己，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，这个群称为*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

5-4 群与子群(groups and subgroups)

【例5.4.4】设$g=\{a,b,c,d\}$,*为G上的二元运算，它由表5.4.2给出,不难证明G是一个群，且e是G中的幺元；G中元素b的逆元就是它自己，a与c互逆。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，这是除了*klein*四元群外的另一个四阶群。

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

5-4 群与子群(groups and subgroups)

【例5.4.5】设〈*G*,*〉是一个独异点,并且每个元素都有右逆元,证明〈*G*,*〉为群。

证明 设*e*是〈*G*,*〉中的幺元。每个元素都有右逆元，即 $\forall x \in G$， $\exists y \in G$使得$x*y=e$，而对于此*y*，又 $\exists z \in G$使得 $y*z=e$。由于 $\forall x \in G$均有$x*e=e*x=e$，因此

$$z=e*z=x*y*z=x*e=x$$

即

$$x*y=e=y*z=y*x=e$$

*y*既是*x*的右逆元，又是*x*的左逆元，故$\forall x \in G$均有逆元，〈*G*,*〉为群。

5-4 群与子群(groups and subgroups)

至此，我们可以概括地说：广群仅仅是一个具有封闭二元运算的非空集合；半群是一个具有结合运算的广群；独异点是具有幺元的半群；群是每个元素都有逆元的独异点。即有：

{群}⊆{独异点} ⊆{半群} ⊆{广群}

5-4 群与子群(groups and subgroups)

由定理5-2.4可知，群中任何一个元素的逆元必定是唯一的。由群中逆元的唯一性，我们可以有以下几个定理。

定理5-4.1 群中不可能有零元。

证明:当群的阶为1 时(|G|=1)，它的唯一元素视作幺元。

设|G|>1且群<G,*>有零元θ。
那么群中任何元素x∈G,都有x*θ=θ*x=θ≠e,所以，零元θ就不存在逆元，这与<G,*>是群相矛盾。

定理5-4.2设<G,*> 是一个群，对于a,b∈G,必存在唯一的x∈G,使得a*x=b。

证明：设a的逆元是a^{-1}，令$x=a^{-1}*b$

则 $a*x=a*(a^{-1}*b)$

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

$=e*b$

$=b$

若另有一解x_1,满足$a*x_1=b$,则

$a^{-1}*(a*x_1)= a^{-1}*b$

即 $x_1= a^{-1}*b$

5-4 群与子群(groups and subgroups)

定理5-4.3设<G,*>是一个群，对于任意的a,b,c∈G,如果有a*b=a*c或者b*a=c*a,则必有b=c(消去律，可约性)。

证明　设a*b=a*c,且a的逆元是a^{-1},则有

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

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

e*b=e*c

b=c

当b*a=c*a时，可同样证得b=c。

5-4 群与子群(groups and subgroups)

由定理5-4.3可知：

群的运算表中没有两行（或两列）是相同的。

为了进一步考察群的运算表所具有的性质，现在引进置换的概念。

5-4 群与子群(groups and subgroups)

定义5-4.3 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映射到c，是一个从S到S上的一个一对一映射，这个置换可以表示为

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

即上一行中按任何次序写出集合中的全部元素，而在下一行中写每个对应元素的像。

5-4 群与子群(groups and subgroups)

定理5-4.4 群<G,*>的运算表中的每一行或每一列都是G的元素的一个置换。

证明：首先，证明运算表中的任一行或任一列所含G中的一个元素不可能多于一次。用反证法，如果对应于元素$a \in G$的那一行中有两个元素都是c,即有b_1，$b_2 \in G$

$$a*b_1=a*b_2=c \text{ 且} b_1 \neq b_2$$

由可约性可得$b_1=b_2$,这与$b_1 \neq b_2$矛盾。

5-4 群与子群(groups and subgroups)

其次，要证明G中的每一个元素都在运算表的每一行和每一列中出现。

考察对应于元素a∈G的那一行，设b是G中的任一元素，由于$b=a*(a^{-1}*b)$,所以b必定出现在对应于a的那一行中。

再由运算表中没有两行（或两列）相同的事实，便可得出：<G,*>的运算表中每一行都是G的元素的一个置换，且每一行都是不相同的。同样的结论对于列也是成立的。

5-4 群与子群(groups and subgroups)

由定理5-4.4可知，特别地，当*G*为有限群时，*运算的运算表的每一行（列）都是*G*中元素的一个置换。

对于有限群，运算可用表给出,称为群表。从而有限群〈*G*，*〉的运算表中没有一行（列）上有两个元素是相同的。因此，当*G*分别为1，2，3阶群时,*运算都只有一个定义方式(即不计元素记号的不同,只有一张定义*运算的运算表,分别如表5.4.3、5.4.4和5.4.5所示),于是可以说,1,2,3阶的群都只有一个。

5-4 群与子群(groups and subgroups)

表 5.4.3

*	e
e	e

表 5.4.4

*	e	a
e	e	a
a	a	e

表 5.4.5

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

5-4 群与子群(groups and subgroups)

【例5.4.6】在下表的空白处填入适当的元素,使〈{*a*,*b*,*c*},*〉构成群。

*	*a*	*b*	*c*
a	___	*a*	___
b	*a*	___	*c*
c	___	*c*	___

5-4 群与子群(groups and subgroups)

【例5.4.6】在下表的空白处填入适当的元素,使〈{*a*,*b*,*c*},*〉构成群。

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

5-4 群与子群(groups and subgroups)

定义5-4.4

代数系统<G,*>中，如果存在a∈G,有a*a=a,则称a为等幂元。

5-4 群与子群(groups and subgroups)

定理5-4.5 群<G,*>中，除幺元e外，不可能有任何别的等幂元。

证明： 因为e*e=e,所以e是等幂元。

现设 $a \in A, a \neq e$且$a*a=a$

则有 $a=e*a=(a^{-1}*a)*a= a^{-1}*(a*a)$

$= a^{-1}*a=e$

与假设$a \neq e$相矛盾。

5-4 群与子群(groups and subgroups)

定义5-4.5[子群]

设<G,*>是一个群，S是G的非空子集，如果<S,*>也构成群，则称<S,*>是<G,*>的一个子群。

5-4 群与子群(groups and subgroups)

定理5-4.6设<G,*>是一个群，<S,*>是<G,*>的一个子群，那么，<G,*>中的幺元e必定也是<S,*>中的幺元。

证明：设<S,*>中的幺元为e_1, 对于任一$x \in S \subseteq G$, 必有$e_1*x=x=e*x$, 故$e_1=e$。

5-4 群与子群(groups and subgroups)

定义5-4.6[平凡子群]

设<G,*>是一个群，<S,*>是<G,*>的子群，如果S={e}，或者S=G，则称<S,*>为<G,*>的平凡子群

【例5.4.7】 <I,+>是一个群，设I_E={x|x=2n,n∈I},证明< I_E,+>是<I,+>的一个子群。

证明：（1） 对于任意的x,y∈I_E,不妨设$x=2n_1$,$y=2n_2$, n_1，n_2∈I,则

$x+y=2n_1+2n_2=2(n_1+n_2)$，而 n_1+n_2∈I

所以 x+y∈ I_E ， 即+在I_E 上封闭。

（2） 运算+在I_E 上保持可结合性。

（3） <I,+>中的幺元0也在I_E 中。

（4） 对于任意的x∈ I_E,必有n ∈I使得x=2n,而

-n∈I，即2(-n) =-2n=-x,

所以-x∈ I_E ,而x+(-x)=0, 因此，< I_E ,+>是<I,+>的一个子群。

定理5-4.7设<G,*>是一个群，B是G的非空子集，如果B是一个有限集，那么，只要运算*在B上封闭，<B,*>必定是<G,*>的子群。

证明：设b是B的任一个元素。若*在B上封闭，则元素 $b^2=b*b, b^3=b^2*b, \ldots$都在B中。由于B是有限集，所以必存在正整数i和j,不妨假设i<j,使得

$$b^i = b^j \quad \text{即} \quad b^i = b^i * b^{j-i}.$$

这就说明b^{j-i}是<G,*>中的幺元，且这个幺元也在子集B中。

如果$j-i>1$,那么由$b^{j-i} = b* b^{j-i-1}$可知b^{j-i-1}是b的逆元，且$b^{j-i-1} \in B$;

如果$j-i=1$,那么由$b^i = b^i*b$可知b就是幺元，而幺元是以自身为逆元的。 因此，<B,*>是<A,*>的一个子群。

5-4 群与子群(groups and subgroups)

定理5-4.8设<G,Δ>是群，S是G的非空子集，如果对于S中的任意元素a和b有$a\Delta b^{-1}\in S$,则<S,Δ>是<G,Δ>的子群。

证明：首先证明，G中的幺元e也是S中的幺元。

任取S中的元素$a,a\in S\subseteq G$,所以$e=a\Delta a^{-1}\in S$且 $a\Delta e=e\Delta a=a$,即e也是S中的幺元。

其次证明，S中的每一元素都有逆元。

对任一$a\in S$, 因为$e\in S$, 所以$e\Delta a^{-1}\in S$即$a^{-1}\in S$。

最后证明，Δ在S上是封闭的。

对任意的$a,b\in S$，由上可知$b^{-1}\in S$

而 $b=(b^{-1})^{-1}$

所以 $a\Delta b=a\Delta (b^{-1})^{-1}\in S$

至于运算Δ在S上的可结合性是保持的。

因此，<S,Δ>是<G,Δ>的子群。

5-4 群与子群(groups and subgroups)

【例5.4.8】Klein四元群， <{e}, *>， <{e, a}, *>，<{e, b}, *>， <{e, c}, *>均是其子群。

【例5.4.9】设G为群， a∈G，令$H=\{a^k | a\in Z\}$，即a的所有的幂构成的集合，则H是G的子群，称为由a生成的子群，记作<a>。a称为生成元（Generator）。

证明：（略，依据定理5.4.7）

5-4 群与子群(groups and subgroups)

【例5.4.10】设<H,*>和<K,*>都是群<G,*>的子群，试证明<H∩K,*>也是<G,*>的子群。

证明：设任意的$a,b \in H \cap K$,

因为<H,*>和<K,*>都是子群，

所以$b^{-1} \in H \cap K$,

由于*在H和K中的封闭性，

所以$a*b^{-1} \in H \cap K$,

由定理5-4.8即得<H∩K,*>是<G,*>的子群。

5-4 群与子群(groups and subgroups)

作业5-4

P197 (2)

(3)

5-5 阿贝尔群和循环群

定义 5-5.1：如果群<G,*>中的运算*是可交换的，则称该群为阿贝尔群，或称交换群。

例题 1： 设G为所有n阶非奇异（满秩）矩阵的集合，∘作为定义在集合G上的矩阵乘法运算，则<G,∘>是一个不可交换群。

5-5 阿贝尔群和循环群

解： 任意两个n阶非奇矩阵相乘后，仍是一个非奇矩阵，所以运算·是封闭的。

矩阵乘法运算是可结合的。

n阶单位阵E是G中的幺元。

任意一个非奇阵A存在着唯一的逆阵，使$A \cdot A^{-1}=A^{-1} \cdot A=E$

但矩阵乘法是不可交换的，因此，<G,·>是一个不可交换群。

5-5 阿贝尔群和循环群

定理5-5.1: 设<G,*>是一个群，<G,*>是阿贝尔群的充要条件是对任意的a,b∈G,有 (a*b)*(a*b)=(a*a)*(b*b)。

证明: 充分性

设对任意a,b∈G,有(a*b)*(a*b)=(a*a)*(b*b)

因为 a*(a*b)*b=(a*a)*(b*b)

=(a*b)*(a*b)

=a*(b*a)*b

所以 $a^{-1}*(a*(a*b)*b)*b^{-1}$

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

即得 a*b=b*a

因此，群<G,*>是阿贝尔群。

5-5 阿贝尔群和循环群

必要性

设<G,*>是阿贝尔群，则对任意的a,b∈G 有

a*b=b*a

因此 (a*a)*(b*b)=a*(a*b)*b

=a*(b*a)*b

=(a*b)*(a*b)

5-5 阿贝尔群和循环群

定义5-5.2： 设<G,*>为群，若在G中存在一个元素a，使得G中的任意元素都由a的幂组成，则称该群为循环群，元素a称为循环群G的生成元。

例如：60°就是群<{0°，60°，120°，180°，240°，300°}，★>的生成元，因此，该群是循环群。

5-5 阿贝尔群和循环群

定理5-5.2：任何一个循环群必定是阿贝尔群。

证明： 设<G,*>是一个循环群，它的生成元是a，那么，对于任意的x,y∈G,必有r,s∈Z，使得$x=a^r$ 和 $y=a^s$而且 $x*y=a^r*a^s=a^{r+s}=a^{s+r}=a^s*a^r=y*x$

因此， <G,*>是一个阿贝尔群。

对于有限循环群，有下面的定理。

5-5 阿贝尔群和循环群

定理5-5.3： 设<G,*>是一个由元素a∈G生成的有限循环群。如果G的阶数是n,即|G|=n,则$a^n=e$且G={a，a^2，a^3，…，a^{n-1},$a^n=e$}，其中，e是<G,*>中的幺元，n是使$a^n=e$的最小正整数（称n为元素a的阶）。

证明： 假设对于某个正数m，m<n，有$a^m=e$。那么，由于<G,*>是一个循环群，所以G中的任何元素都能写为a^k(k∈Z)，而且k=mq+r其中，q是某个整数，0≤r<m。这就有$a^k=a^{mq+r}=(a^m)^q*a^r=a^r$

这就导致G中每一个元素都可表示成a^r(0≤r<m)，这样，G中最多有m个不同的元素，与|G|=n相矛盾。所以$a^m=e$(m<n)是不可能的。

5-5 阿贝尔群和循环群

进一步证明a，a^2，a^3，…，a^{n-1},a^n都不相同。用反证法。假设$a^i = a^j$,其中$1 \le i < j \le n$,就有$a^i = a^i * a^{j-i}$，即$a^{j-i} = e$,而且$1 \le j-i < n$,这已经由上面证明是不可能的。所以，a，a^2，a^3，…，a^{n-1},a^n都不相同，因此

$G=\{a, a^2, a^3, \ldots, a^{n-1}, a^n = e\}$

5-5 阿贝尔群和循环群

例题 2： 设G={α，β，γ，δ}，在G上定义二元运算*如表5-5.2所示。

表5-5.2

*	α	β	γ	δ
α	α	β	γ	δ
β	β	α	δ	γ
γ	γ	δ	β	α
δ	δ	γ	α	β

5-5 阿贝尔群和循环群

解：由运算表5-5.2可知运算*是封闭的， α是幺元。β， γ和δ的逆元分别是β，δ和γ 。

可以验证运算*是可结合的。

所以<G,*>是一个群。

在这个群中，由于 $\gamma*\gamma=\gamma^2=\beta, \gamma^3=\delta, \gamma^4=\alpha,$

以及 $\delta*\delta=\delta^2=\beta , \delta^3=\gamma, \delta^4=\alpha$

故群<G,*>是由γ或δ生成的，因此<G,*>是一个循环群。

从本例可以看到：一个循环群的生成元可以不是唯一的。

5-5 阿贝尔群和循环群

作业 5-5

P200 (1)

(4)

5-7 陪集与拉格朗日定理

定义5-7.1： 设<G,*>是一个群，A，B∈P(G)且A≠∅，B≠∅，记 AB={a*b|a∈A,b∈B}

和 $A^{-1}=\{a^{-1}|a \in A\}$，

分别称为A，B的积和A的逆。

定义5-7.2： 设<H,*>是群<G,*>的一个子群a∈G，则集合{a}H （H{a}） 称为由a所确定的H在G中的左陪集（右陪集）， 简称为H关于a的左陪集（右陪集），记为aH (Ha) 。元素a称为陪集aH (Ha) 的代表元素。

5-7 陪集与拉格朗日定理

例1： $<I_E,+>$是群$<I,+>$的子群，

则 $\{0\}\ I_E = I_E$，$\{2\}\ I_E = I_E$，$\{-2\}\ I_E = I_E$，……

$\{1\}\ I_E = I_o$，$\{-1\}\ I_E = I_o$，$\{3\}\ I_E = I_o$， ……

所以，$\{I_E, I_o\}$ 是对于I(整数集)的一个划分。

5-7 陪集与拉格朗日定理

定理5-7.1（拉格朗日定理）

设<H,*>是群<G,*>的一个子群，那么R={<a,b>|a∈G,b∈G且$a^{-1}*b∈H$}是G中的一个等价关系。对于a∈G,若记$[a]_R$={x|x∈G且<a,x>∈R}，则$[a]_R$=aH。如果G是有限群，|G|=n,|H|=m,则m|n。

证明：(a)对于任一a∈G, 必有a^{-1}∈G, 使$a^{-1}*a=e∈H$, 所以<a,a>∈R。

若<a,b>∈R,则$a^{-1}*b∈H$，因为H是G的子群，故$(a^{-1}*b)^{-1}=b^{-1}*a∈H$，所以, <b,a>∈R。

若<a,b>∈R, <b,c>∈R, 则$a^{-1}*b∈H$, $b^{-1}*c∈H$, 故$a^{-1}*b*b^{-1}*c=a^{-1}*c∈H$, 所以<a,c>∈R。

这就证明了R是G中 的一个等价关系。

5-7 陪集与拉格朗日定理

对于a∈G,我们有：b∈$[a]_R$当且仅当<a,b>∈R,即当且仅当$a^{-1}*b∈H$,而$a^{-1}*b∈H$就是b∈aH。

因此，$[a]_R=aH$。

(b)由于R是G中的一个等价关系，所以必定将G划分成不同的等价类$[a_1]_R,[a_2]_R,\ldots,[a_k]_R$，使得

$$G=\bigcup_{i=1}^{k}[a_i]_R=\bigcup_{i=1}^{k}a_iH$$

又因，H中任意两个不同的元素h_1,h_2,a∈G,必有$a*h_1≠a*h_2$,所以$|a_iH|=|H|=m,i=1,2,\ldots,k$。因此

$$n=|G|=|\bigcup_{i=1}^{k}a_iH|=\sum_{i=1}^{k}|a_iH|=mk$$

5-7 陪集与拉格朗日定理

推论1： 任何质数阶的群不可能有非平凡子群。

这是因为，如果有非平凡子群，那么该子群的阶必定是原来群的阶的一个因子，这就与原来群的阶是质数相矛盾。

5-7 陪集与拉格朗日定理

推论2： 设<G,*>是n阶有限群，那么对于任意的a∈G,a的阶必是n的因子且必有$a^n=e$,这里e是群<G,*>中的幺元。如果n为质数，则<G,*>必是循环群。

这是因为，由G中的任意元素a生成的循环群

$$H=\{a^i \mid i\in I, a\in G\},$$

一定是G的一个子群。如果H的阶是m，那么由定理5-5.3可知$a^m=e$, 即a的阶等于m。由拉格朗日定理必有n=mk, k∈I,因此，a的阶m是n的因子，且有$a^n=a^{mk}=(a^m)^k=e^k=e$ 。

因为质数阶群只有平凡子群，所以，质数阶群必定是循环群。

必须注意，群的阶与元素的阶这两个概念的不同。

5-7 陪集与拉格朗日定理

例题1：设K={e,a,b,c},在K上定义二元运算*如表5-7.1所示。

表 5-7.1

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

证明 <K,*>是一个群，但不是循环群。

5-7 陪集与拉格朗日定理

证明：

由表5-7.1可知，运算*是封闭的和可结合的。幺元是e，每个元素的逆元是自身，所以，<K,*>是群。因为a,b,c都是二阶元，故<K,*>不是循环群。我们称<K,*>为Klein四元群。

Klein四元群的特点为： 群的阶数是4，除e以外的三个元素a,b,c都是二阶元，且a*b=b*a=c, b*c=c*b=a, a*c=c*a=b

5-7 陪集与拉格朗日定理

例题2：任何一个四阶群只能是四阶循环群或者Klein四元群。

证明：

设四阶群为<{e,a,b,c},*>，其中e是幺元。当四阶群含有一个四阶元素时，这个群就是循环群。当四阶群不含有四阶元素时，则由推论2可知，除幺元e外，a,b,c的阶一定都是2。a*b不可能等于a,b或e,否则将导致b=e,a=e或a=b的矛盾，所以a*b=c。同样地有b*a=c以及a*c=c*a=b,b*c=c*b=a。因此，这个群是Klein四元群。

5-7 陪集与拉格朗日定理

作业 5-7

P211 （2）

（5）

5-8 同态与同构

这一节我们将讨论两个代数系统之间的联系。着重研究两个代数系统之间的同态关系和同构关系。

5-8 同态与同构

定义5-8.1： 设<A,★>和<B,*>是两个代数系统，★和*分别是A和B上的二元（n元）运算，设f是从A到B的一个映射，使得对任意的$a_1,a_2 \in A$,

有$f(a_1 ★ a_2)=f(a_1)*f(a_2)$，

则称f为由<A,★>到<B,*>的一个同态映射(homomorphism mapping)，称<A,★>同态于<B,*>,记作A~B。

把<f(A),*>称为<A,★>的一个同态象(image under homomorphism)。

其中$f(A)=\{x|x=f(a), a \in A\} \subseteq B$

5-8 同态与同构

例1 考察代数系统<I, · >，这里I是整数集，· 是普通的乘法运算。如果我们对运算只感兴趣于正、负、零之间的特征区别，那么代数系统<I, · >中运算结果的特征就可以用另一个代数系统<B, ⊙>的运算结果来描述，其中B={正，负，零}，是定义在B上的二元运算，如表5-8.1所示。

表5-8.1

⊙	正	负	零
正	正	负	零
负	负	正	零
零	零	零	零

5-8 同态与同构

作映射f: I→B如下：

$$f(n)=\begin{cases}\text{正} & \text{若}n>0\\ \text{负} & \text{若}n<0\\ \text{零} & \text{若}n=0\end{cases}$$

很明显，对于任意a,b∈I，有

$$f(a\cdot b)=f(a)\odot f(b)$$

因此，映射f是由<I,· >到<B, ⊙>的一个同态。

5-8 同态与同构

例1 告诉我们，

在<I，·>中研究运算结果的正、负、零的特征就等于在<B，⊙>中的运算特征

可以说，代数系统<B，⊙>描述了<I，·>中运算结果的这些基本特征。

而这正是研究两个代数系统之间是否存在同态的重要意义。

注：由一个代数系统到另一个代数系统可能存在着多于一个的同态。

5-8 同态与同构

定义5-8.2： 设f是由<A,★>到<B,*>的一个同态，如果f是从A到B的一个满射，则f称为满同态；如果f是从A到B的一个入射，则f 称为单一同态；如果f是从A到B的一个双射，则f 称为同构映射，并称<A,★>和<B,*>是同构的(isomorphism)，记作A≌B。

5-8 同态与同构

例2.设f: R→R定义为对任意x∈R，$f(x)=5^x$，那么，f是从<R,+>到<R,·>的一个单一同态。

$f(x+y)=5^{x+y}=5^x \cdot 5^y=f(x) \cdot f(y)$

f为入射。因为$x_1 \neq x_2$，则$5^{x1} \neq 5^{x2}$，即$f(x_1) \neq f(x_2)$。

又因为$5^x>0$，所以f 不是满射。

5-8 同态与同构

例3.设f: $N \to N_k$定义为对任意的$x \in N$，$f(x)=x \bmod k$，那么，f是从$<N,+>$到$<N_k,+_k>$的一个满同态。

$f(x+y)=(x+y) \bmod k$

$=(x \bmod k) +_k (y \bmod k)$

$= f(x) +_k f(y)$;

又f是满射。

而$f(1)=f(K+1)=1 \in N_k$, f 不是入射。

5-8 同态与同构

例4. 设H={x|x=dn, d是某一个正整数，n∈I}，定义映射f:I→H为对任意n∈I，f(n)=dn，那么，f是<I,+>到<H,+>的一个同构。所以I≅H。

f(m+n)=d(m+n)=dm+dn=f(m)+f(n);

又f是双射。

5-8 同态与同构

例题5： 设A={a,b,c,d}，在A上定义一个二元运算如表5-8.2所示。又设B={ α , β , γ , δ },在B上定义一个二元运算如表5-8.3所示。证明<A,★>和<B,*>是同构的。

表 5-8.2

★	a	b	c	d
a	a	b	c	d
b	b	a	a	c
c	b	d	d	c
d	a	b	c	d

表 5-8.3

*	α	β	γ	δ
α	α	β	γ	δ
β	β	α	α	γ
γ	β	δ	δ	γ
δ	α	β	γ	δ

5-8 同态与同构

证明：考察映射f, 使得f(a)=α，f(b)=β，f(c)=γ，f(d)=δ

显然，f是一个从A到B的双射，由表5-8.2和表5-8.3，容易验证f是由<A,★>到<B,*>的一个同态。因此，<A,★>和<B,*>是同构的。

如果考察映射g, 使得g(a)=δ，g(b)=γ，g(c)=β，g(d)=α那么，g也是由<A,★>到<B,*>的一个同构。

由此例我们知道，当两个代数系统是同构的话，它们之间的同构映射可以是不唯一的。

5-8 同态与同构

定义5-8.3： 设<A,★>是一个代数系统，如果f是由<A,★>到<A,★>的同态，则称f为自同态。

如果g是由<A,★>到<A,★>的同构，则称g为自同构。

5-8 同态与同构

定理5-8.1： 设G是代数系统的集合，则G中代数系统之间的同构关系是等价关系。

证明： 因为任何一个代数系统<A,★>要以通过恒等映射与它自身同构，即自反性成立。

关于对称性，设<A,★>≌<B,*>且有对应的同构映射f, 因为f 的逆是由<B,*>到<A,★>的同构映射，即<B,*>≌<A,★>。

最后，关于传递性，如果f是由<A,★>到<B,*>的同构映射，g是由<B,*>到<C,Δ>的同构映射，那么g。f就是<A,★>到<C,Δ>的同构映射。

5-8 同态与同构

定理5-8.2： 设f 是从代数系统<A,★>到代数系统<B,*>的同态映射。

（a） 如果<A,★>是半群，那么在f 作用下，同态象<f(A),*>也是半群。

（b）如果<A,★>是独异点，那么在f 作用下，同态象<f(A),*>也是独异点。

（c）如果<A,★>是群，那么在f 作用下，同态象<f(A),*>也是群。

5-8 同态与同构

证明：(a) 设<A,★>是半群且<B,*>是一个代数系统，如果f是由<A,★>到<B,*>的一个同态映射，则$f(A)\subseteq B$。

对于任意的$a,b\in f(A)$，必有$x,y\in A$ 使得 f(x)=a, f(y)=b

在A中，必有z=x★y，所以

$a*b=f(x)*f(y)=f(x★y)=f(z)\in f(A)$

5-8 同态与同构

最后，*在f(A)上是可结合的，这是因为：对于任意的a,b,c∈f(A),必有x,y,z∈A,使得

f(x)=a, f(y)=b,f(z)=c

因为★在A上是可结合的，所以

$$a*(b*c)=f(x)*(f(y)*f(z))=f(x)*f(y\bigstar z)$$
$$=f(x\bigstar(y\bigstar z))=f((x\bigstar y)\bigstar z)$$
$$=f(x\bigstar y)*f(z)=(f(x)*f(y))*f(z)$$
$$=(a*b)*c$$

因此，<f(A),*>是半群。

5-8 同态与同构

(b) 设<A,★>是独异点，e是A中的幺元，那么f(e)是f(A)中的幺元。这是因为对于任意的a∈f(A)必有x∈A使f(x)=a，所以

$$a*f(e)=f(x)*f(e)=f(x★e)=f(x)=a$$

$$=f(e★x)=f(e)*f(x)=f(e)*a$$

因此，<f(A),*>是独异点。

5-8 同态与同构

(c) 设<A,★>是群。

对于任意的a∈f(A)必有x∈A 使f(x)=a，

因为<A,★>是群，故x有逆元,且$f(x^{-1})\in f(A)$，

而 $f(x)*f(x^{-1})=f(x★x^{-1})=f(e)=f(x^{-1}★x)$

$=f(x^{-1})*f(x)$

所以，$f(x^{-1})$是f(x)的逆元。即$f(x^{-1})= f(x)^{-1}$。

因此，<f(A),*>是群。

5-8 同态与同构

定义5-8.4： 设f是由群<G,★>到群<G’，*>的同态映射，e’是G’中的幺元，记Ker(f)={x|x∈G且f(x)=e’}, 称Ker(f)为同态映射f 的核，简称f 的同态核。

5-8 同态与同构

定理5-8.3： 设f是由群<G,★>到群<G′,*>的同态映射，则f的同态核K是G的子群。

证明： 由定理5-8.2可知，$e' = f(e)$。

设$k_1, k_2 \in K$,则

$f(k_1 ★ k_2) = f(k_1) * f(k_2) = e' * e' = e'$ 故$k_1 ★ k_2 \in K$。

对任意的$k \in K$,由定理5-8.2可知

$f(k^{-1}) = f(k)^{-1} = e'^{-1} = e'$

故$k^{-1} \in K$。

因此，<K,★>是<G,★>的子群。

5-8 同态与同构

定义5-8.5： 设<A,★>是一个代数系统，并设R是A上的一个等价关系。

如果当$<a_1,a_2>,<b_1,b_2>\in R$时，蕴涵着

$<a_1★b_1,a_2★b_2>\in R$,

则称R为A上关于★的同余关系。由这个同余关系将A划分成的等价类就称为同余类。

5-8 同态与同构

定理5-8.4： 设<A,★>是一个代数系统，R是A上的一个同余关系，$B=\{A_1, A_2, \ldots, A_r\}$是由R诱导的A的一个划分，那么，必定存在新的代数系统<B,*>,它是<A,★>的同态象。

证明：在B上定义二元运算*为：

对于任意的$A_i, A_j \in B$,任取$a_1 \in A_i, a_2 \in A_j$,如果$a_1 ★ a_2 \in A_k$, 则$A_i * A_j = A_k$。

由于R是A上的同余关系，所以，以上定义的$A_i * A_j = A_k$是唯一的。

5-8 同态与同构

作映射 $f(a)=A_i$ ，$a \in A_i$。 显然，f是从A到B的满映射。

对于任意的x,y∈A，x,y必属于B中的某两个同余类，不妨设$x \in A_i, y \in A_j, 1 \le i,j \le r$;同时，x★y必属于B中某个同余类，不妨设$x★y \in A_k$,于是，就有

$$f(x★y) = A_k = A_i * A_j = f(x)*f(y)$$

因此，f是由<A,★>到<B,*>的满同态，即<B,*>是<A,★>的同态象。

5-8 同态与同构

定理5-8.5： 设f是由<A,★>到<B,*>的一个同态映射，如果在A上定义二元关系R为：<a,b>∈R当且仅当f(a)=f(b)，那么，R是A上的一个同余关系。

证明： 因为f(a)=f(a),所以<a,a>∈R。

若<a,b>∈R,则f(a)=f(b)即f(b)=f(a),所以<b,a>∈R。

若<a,b>∈R,<b,c>∈R则f(a)=f(b)=f(c),所以<a,c>∈R。最后，又因为若<a,b>∈R,<c,d>∈R,则有

$$f(a★c)=f(a)*f(c)=f(b)*f(d)=f(b★d)$$

所以，<a★c,b★d>∈R。

因此，R是A上的同余关系。

5-8 同态与同构

形象地说，一个代数系统的同态象可以看作是当抽去该系统中某些元素的次要特性的情况下，对该系统的一种粗糙描述。如果我们把属于同一个同余类的元素看作是没有区别的，那么原系统的性态可以用同余类之间的相互关系来描述。

作业（5-8）

P221 (2), (3)

5-9 环与域

以上，我们已初步研究了具有一个二元运算的代数系统——半群、独异点、群。接着，我们将讨论具有两个二元运算的代数系统。对于给定的两个代数系统<A,★>和<A,*>，容易将它们组合成一个具有两个二元运算的代数系统<A,★,*>。我们感兴趣于两个二元运算★和*之间有联系的代数系统<A,★,*>，通常，我们把一个二元运算★称为“加法”，把第二个运算*称为“乘法”。

5-9 环与域

例如，具有加法和乘法这两个二元运算的实数系统<R,+,×>和整数系统<I,+, ×>都是我们很熟悉的代数系统。

它们运算之间的联系是乘法对加法满足分配律。

5-9 环与域

定义5-9.1： 设<A,★,*>是一个代数系统，如果满足：

1.<A,★>是阿贝尔群。

2.<A,*>是半群。

3.运算*对于运算★是可分配的。

则称<A,★,*>是环。

根据定义可以清楚地看到，整数集合、有理数集合、偶数集合、复数集合以及定义在这些集合上的普通加法和乘法运算都是可构成环的例子。

5-9 环与域

例1 系数属于实数的所有x的多项式所组成的集合记作R[x]，那么，R[x]关于多项式的加法和乘法构成一个环。

例2 元素属于实数的所有n阶矩阵所组成的集合记作$(R)_n$，那么，$(R)_n$关于矩阵的加法和乘法构成一个环。

5-9 环与域

定理5-9.1： 设<A,+, ·>是一个环，则对于任意的a,b,c∈A，有

1. a · θ = θ · a = θ
2. a·(-b) =(-a) ·b = -(a·b)
3. (-a) · (-b) = a·b
4. a·(b-c) = a·b - a·c
5. (b-c) ·a =b·a -c·a

其中，θ是加法幺元，- a是a的加法逆元，并将a+(-b)记为a-b。

我们还可以根据<A , ·>的结构来定义一些常见的特殊环。

5-9 环与域

定义5-9.2： 设<A , +, ·>是环。如果<A , ·>是可交换的，则称<A, +, ·>是交换环。如果<A , ·>含有幺元，则称<A, +, ·>是含幺环。

设S是一个集合，P(S)是它的幂集，如果在P(S)上定义二元运算+和·如下：对任意的A，B∈ P(S)

$$A+B=\{x|(x\in S)\wedge(x\in A\vee x\in B)\wedge(x\notin A\cap B)\}$$

$$A\cdot B= A\cap B$$

容易证明<P(S) , + ,·>是一个环，称它为S的子集环。

由于集合交运算是可交换的，且<P(S) , ·>含有幺元S，因此子集环是含幺交换环。

5-9 环与域

定义5-9.3： 设<A, +, ·> 是一个代数系统，如果满足：

1. <A, +>是阿贝尔群。

2. <A, ·>是可交换独异点，且无零因子，即对任意的$a, b \in A$, $a \neq \theta$, $b \neq \theta$, 必有$a \cdot b \neq \theta$。

3. 运算 · 对于运算 + 是可分配的。

则称<A ,+, ·>是整环。

5-9 环与域

下面我们来考察<I , +, ·>是否为整环

因为<I, +>是一个具有加法幺元0，且对任意n有逆元-n的阿贝尔群；

<I, ·>是可交换独异点，

且满足无零因子条件；

运算 · 对于运算 + 是可分配的，

故<I ,+, ·>是整环。

5-9 环与域

定理5-9.2： 在整环<A, +, ·>中的无零因子条件等价于乘法消去律，即对于$c\neq\theta$和$c\cdot a=c\cdot b$，必有$a=b$。

证明：“⇒”若无零因子并设$c\neq\theta$和$c\cdot a=c\cdot b$，

则有 $c\cdot a - c\cdot b = c\cdot(a-b)=\theta$

所以，必有$a=b$。

“⇐”反之，若消去律成立，

设$a\neq\theta$，$a\cdot b=\theta$

则$a\cdot b= a\cdot\theta$ 消去a

即得$b=\theta$。

5-9 环与域

定义5-9.4： 设<A ,+, ·> 是一个代数系统，如果满足：

1. <A,+>是阿贝尔群。
2. <A-{θ} , ·>是阿贝尔群。
3. 运算 · 对于运算 + 是可分配的。

则称<A ,+, ·>是域。

例如，<Q ,+, ·>，<R ,+, ·>，<C ,+, ·>都是域，这里，Q为有理数集合，R是实数集合，C是复数集合，而+, ·分别是各数集上的加法和乘法运算。

必须指出，<I ,+, ·>是整环，但不是域，

因为<I-{0}, ·>不是群。这说明，整环不一定是域。

5-9 环与域

定理5-9.4： 有限整环必定是域。

证明：见P226

定义5-9.5： 设<A ,+, ·> 和<B ,⊕ ,⊙>是两个代数系统，如果一个从A到B得映射f，满足如下条件：

对于任意的a,b∈A，有

$f(a+b)=f(a)\oplus f(b)$

$f(a\cdot b)=f(a)\odot f(b)$

则称f为由<A ,+, ·> 到<B , ⊕, ⊙>的一个同态映射，并称<f(A) , ⊕, ⊙>是<A ,+, ·>的同态象。

5-9 环与域

定理5-9.5： 任一环的同态象是一个环。

证明：P228

5-9 环与域

作业：(5-9)

P228 (4) a) b)

(7) a) c)

结　束

谢　谢！