第五章　　代数结构

§1　代数系统的引入

§2　运算及其性质

§3　半群

§4　群与子群

§5　阿贝尔群和循环群

§7　陪集与拉格朗日定理

§8　同态与同构

§9　环和域

§5-8 同态与同构

这一节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。

2

§5-8 同态与同构

同态公式

先算后映=先映后算

运算的象=象的运算

一、同态

定义1 设<A, ★>和<B,∗ >是两个代数系统，★和∗分别是A和B上的二元运算，f是从A到B的一个映射，使对$\forall a_1, a_2 \in A$，有$f(a_1 ★ a_2)=f(a_1) * f(a_2)$

(1) 称f为由代数结构<A, ★>到<B,∗ >的同态映射；

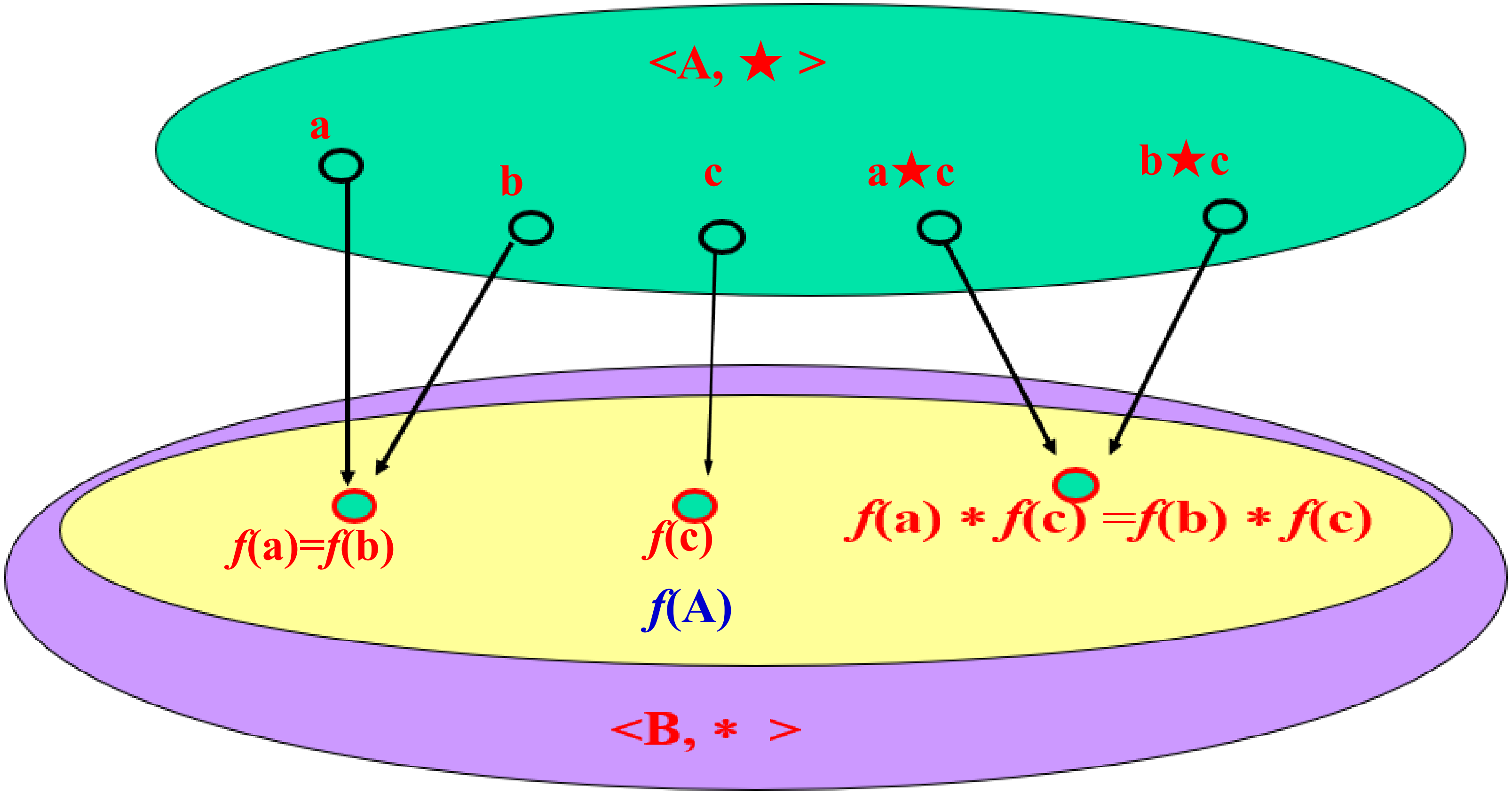
(2) 称代数结构<A, ★>同态于<B,∗ >，记为A~B ；

(3) <f(A),∗ >称为<A, ★>的一个同态象。

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

两个代数系统在同态意义下的相互联系

可以由下图来描述



同态映射示意图

4

§5-8 同态与同构

例1：代数系统<I, · >，I是整数集，· 是普通乘法运算。

若对运算结果只感兴趣于正、负、零之间的特征区别，则代数系统<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，如表所示。

⊙	正	负	零
正	正	负	零
负	负	正	零
零	零	零	零

§5-8 同态与同构

⊙	正	负	零
正	正	负	零
负	负	正	零
零	零	零	零

作映射f：$I \to B$：

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

很显然，对于任意的a, b∈I，有

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

因此，映射f是由$<I, \cdot>$到$<B, \odot>$的一个同态。

6

§5-8 同态与同构

上例告诉我们，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。

注意: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

(习题) 证明如果f是由<A,★>到<B, ∗>的同态映射，g是由<B, ∗>到<C,△>的同态映射，那么$f\circ g$是由<A,★>到<C,△>的同态映射。

证明：已知$g\circ f$是由<A，★>到<C，△>的映射，

对任意a_1，$a_2 \in A$，有

$$f(a_1 \bigstar a_2)=f(a_1) * f(a_2)$$

$$f\circ g(a_1 \bigstar a_2)= g(f(a_1) * f(a_2))$$

$$= g(f(a_1)) \triangle g(f(a_2))$$

$$= f\circ g(a_1) \triangle f\circ g(a_2)$$

所以$g\circ f$是由<A，★>到<C，△>的同态映射。

8

§5-8 同态与同构

二、同构

定义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的一个单射，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，记作$A \cong B$ 。

9

§5-8 同态与同构

例2： 设f：R→R，对任意x∈R，$f(x)=5^x$

那么，f是从<R，+>到<R，·>的一个单一同态。

证明：设$\forall x1, x2 \in R$

$$f(x1+x2)= 5^{x1+x2} = 5^{x1} \cdot 5^{x2} = f(x1) \cdot f(x2)$$

因为$f(x)=5^x$是单射，

所以f是单一同态。

§5-8 同态与同构

例3： 设$H=\{x|x=dn$，d是某一个正整数，$n\in I\}$，定义映射f：$I\to H$，对$\forall n\in I$，$f(n)=dn$，那么，f是从$\langle I, +\rangle$到$\langle H, +\rangle$的一个同构。

证明： 设$\forall n_1$，$n_2\in I$

$$f(n_1+n_2)=d(n_1+n_2)=dn_1+dn_2=f(n_1)+f(n_2)$$

又因为$f(n)=dn$ 是双射

所以，f是从$\langle I, +\rangle$到$\langle H, +\rangle$的一个同构。即$I\cong H$

注意：两个代数系统若是同构，

它们之间的同构映射可

以不唯一。

§5-8 同态与同构

例：设A={a，b，c，d}，B= {α，β，γ，δ} 。

证明<A, ★>和<B,* >是同构的。

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

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

证明：考察映射f，使得

$f(a)=\alpha$　$f(b)=\beta$　$f(c)=\gamma$　$f(d)=\delta$

考察映射g，使得

$g(a)=\delta$　$g(b)=\gamma$　$g(c)=\beta$　$g(d)=\alpha$

12

§5-8 同态与同构

例：代数系统<B, ⊕>,<C, $*$>都与代数系统<A, ★>同构。

<A, ★>

★	a	b
a	a	b
b	b	a

<B, ⊕>

⊕	偶	奇
偶	偶	奇
奇	奇	偶

<C, $*$>

$*$	0°	180°
0°	0°	180°
180°	180°	0°

注意：形式上不同的代数系统，如果同构，就可抽象地把它们看作是本质上相同的代数系统，所不同的只是所用的符号不同。并且，容易看出同构的逆仍是一个同构。

§5-8 同态与同构

三、自同态、自同构

定义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一个等价关系。

证明：（1）自反性：因为任何一个代数系统可以通过恒等映射与它自身同构；

（2）对称性：设<A, ★> ≌ <B,∗ >且有对应的同构映射*f*，则*f*是双射函数，*f*的逆是<B,∗ > 到<A, ★> 的同构映射，即<B,∗ > ≌ <A, ★> ；

（3）传递性：设*f*是A到B的同构映射，*g*是B到C的同构映射，因为*f*和*g*是双射函数，$f \circ g$是A到C的同构映射。即A ≌ C。

所以，同构关系是等价关系。

15

§5-8 同态与同构

定理2 设f是由<A, ★>到<B,* >的一个同态。

（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。

16

§5-8 同态与同构

证明：先证（a）：$<f(A),*>$是半群

1）证$*$运算在$f(A)$上封闭

设$<A,★>$是半群， $<B,*>$是一个代数结构，

如果f是由$<A,★>$到$<B,*>$的一个同态，则$f(A)\subseteq B$。

对于$\forall a, b\in f(A)$，必有$x, y\in A$，使得

$$f(x)=a \ , \ f(y)=b$$

在A中必有$z=x★y$,

所以 $a*b=f(x)*f(y)=f(x★y)=f(z)\in f(A)$

17

§5-8 同态与同构

2）证$*$在$f(A)$上满足结合律

对于$\forall$ a, b, c$\in f(A)$，必有x, y, z$\in$A，使得

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

因为$*$在A上是可结合的，所以

$$\begin{aligned} a*(b*c) &= f(x)*(f(y)*f(z)) = f(x)*f(y\bigstar z) \\ &= f(x\bigstar(y\bigstar z)) \\ &= f((x\bigstar y)\bigstar z) \\ &= f(x\bigstar y)*f(z) \\ &= (f(x)*f(y))*f(z) \\ &= (a*b)*c \end{aligned}$$

所以$<f(A),*>$是半群。

18

§5-8 同态与同构

再证（b）： $<f(A),*>$是独异点

设$<A,\bigstar>$是独异点，e是A中的幺元，那么$f(e)$是$f(A)$中的幺元。

$\because$ 对于$\forall a\in f(A)$，必有$x\in A$，使得$f(x)=a$

$\therefore$ $a*f(e)=f(x)*f(e)=f(x\bigstar e)=f(x)=a$

$$=f(e\bigstar x)=f(e)*f(x)=f(e)*a$$

$\therefore$ $f(e)$是$<f(A),*>$中的幺元， $<f(A),*>$是独异点。

19

§5-8 同态与同构

最后证（c）： $<f(A),*>$是群

设$<A, \bigstar>$是群，对于$\forall a\in f(A)$，必有$x\in A$，使得$f(x)=a$

$\because$ $<A, \bigstar>$是群，

$\therefore$对于$\forall x\in A$，都有逆元$x^{-1}\in A$，且$f(x^{-1})\in f(A)$，

又$\because$ $f(x)*f(x^{-1}) = f(x\bigstar x^{-1}) = f(e) = f(x^{-1}\bigstar x)= f(x^{-1})*f(x)$

$\therefore$ $f(x^{-1})$是$f(x)$的逆元，即$f(x^{-1}) =[f(x)]^{-1}$

$\therefore$ $<f(A),*>$中的任意元素都有逆元, $<f(A),*>$是群。

综合上述(a)、(b)、(c)三步，定理证毕。

141 20

§5-8 同态与同构

四 同态核

定义4 如果f为代数结构<G, ★>到<G’, ∗ >的一个同态映射，G’中有幺元e’，记

$$\mathrm{Ker}(f)=\{x \mid x\in G \wedge f(x)=e'\}$$

称Ker(f) 为同态映射f的核，简称**同态核**（*kernel of homomorphism*），

21

§5-8 同态与同构

定理3 设f为群<G, ★>到群<G',* >的同态映射， 则f的同态核K是G的子群。

$$\mathrm{Ker}(f)=\{x|x\in G\wedge f(x)=e'\}$$

证明：先证★运算在K上封闭

$\underline{e'=f(e)}$，K非空且有单位元e，设$k_1,k_2\in K$，

则$f(k_1★k_2)=f(k_1)*f(k_2)=e'*e'=e'$

故$k_1★k_2\in K$，★运算在K上封闭。

再证K中的元素有逆元

而对$\forall k\in K$，$\underline{f(k^{-1})=[f(k)]^{-1}}=e'^{-1}=e'$

故$k^{-1}\in K$。 结论得证。

22

§5-8 同态与同构

五 同态与同余关系的对应

定义5 设$<A, \bigstar>$是一个代数系统，并设R是A上的一个等价关系。如果对$\forall a_1, a_2, b_1, b_2 \in A$，

当$<a_1,a_2>$，$<b_1,b_2> \in R$时，蕴涵着$<a_1 \bigstar b_1, a_2 \bigstar b_2> \in R$

1) 称R为A上关于★的同余关系(*congruence relations*)。

2) 由这个同余关系将A划分成的等价类称为同余类。

23

§5-8 同态与同构

例：设A={a, b, c, d}，代数系统<A，★>以及在A上定义的等价关系R如下所示。

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

	a	b	c	d
a	√	√		
b	√	√		
c			√	√
d			√	√

$R=\{\langle a,a\rangle,\langle a,b\rangle,\langle b,a\rangle,\langle b,b\rangle,\langle c,c\rangle,\langle c,d\rangle,\langle d,c\rangle,\langle d,d\rangle\}$

等价类$[a]_R=[b]_R=\{a，b\}$，

$[c]_R=[d]_R=\{c，d\}$

24

§5-8 同态与同构

$R=\{<a,a>,<a,b>,<b,a>,<b,b>,<c,c>,<c,d>,<d,c>,<d,d>\}$

容易验证对于任意的$<a_1, b_1>$，$<a_2, b_2>\in R$有

$$<a_1 \bigstar a_2,\ b_1 \bigstar b_2>\in R$$

如$<a\bigstar a, a\bigstar a>=<a, a>\in R$　　$<a\bigstar a, a\bigstar b>=<a, a>\in R$

$<a\bigstar b, a\bigstar a>=<a, a>\in R$　　$<a\bigstar b, a\bigstar b>=<a, a>\in R$

$<a\bigstar c, a\bigstar c>=<d, d>\in R$　　$<a\bigstar c, a\bigstar d>=<d, c>\in R$

$<a\bigstar d, a\bigstar c>=<c, d>\in R$　　$<a\bigstar d, a\bigstar d>=<c, c>\in R$

……………

所以R是A上的同余关系。

同余关系R将A划分为同余类{a，b}和{c，d}。

25

§5-8 同态与同构

定理4 设<A, ★> 是一个代数系统，R为A上的同余关系，$B=\{A_1, A_2, \ldots, A_r\}$是由R诱导的A的一个划分，那么，必定存在新的代数结构<B, ∗ >，它是<A, ★>的同态象。

证明： 在B上定义二元运算∗为：对于$\forall A_i, A_j \in B$，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 $f(a)= A_i \quad a \in A_i$

显然，f是从A到B的满映射。

对于任意的$x,y \in A$，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，不防设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。

27

§5-8 同态与同构

例：设A={a, b, c, d}，代数系统<A, ★>如下。R是定义在A上的等价关系，R={<a,a>,<a,b>,<b,a>,<b,b>, <c,c>,<c,d>,<d,c>,<d,d>}

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

已知R是A上的同余关系。

B={{a, b}, {c, d}}是A的一个划分。B上的二元运算*如下表：

*	{a，b}	{c，d}
{a，b}	{a，b}	{c，d}
{c，d}	{c，d}	{a，b}

A到B的映射*f*为：

f(a)={a，b}　*f*(c)={c，d}

f(b)={a，b}　*f*(d)={c，d}

<B，*>是<A，★>的同态象。

§5-8 同态与同构

定理5 设f是由$\langle A, ★\rangle$到$\langle B, *\rangle$的一个同态映射，如果在A上定义二元关系R为：

$\langle a,b\rangle \in R$，当且仅当$f(a)=f(b)$，

那么，R是A上的一个同余关系。

象相同的元素属于一个同余类。

证明：因为$f(a)=f(a)$，所以$\langle a,a\rangle \in R$。

若$\langle a,b\rangle \in R$，则$f(a)=f(b)$ 即$f(b)=f(a)$，所以$\langle b, a\rangle \in R$。

若$\langle a,b\rangle \in R$，$\langle b,c\rangle \in R$则$f(a)=f(b)=f(c)$，所以$\langle a,c\rangle \in R$。

最后，又因为若$\langle a,b\rangle \in R$，$\langle c,d\rangle \in R$，则有

$$f(a★c)=f(a) * f(c)=f(b) * f(d) = f(b★d)$$

所以，$\langle a★c , b★d\rangle \in R$。

因此， R是A上的同余关系。

29

第五章　　代数结构

§1　代数系统的引入

§2　运算及其性质

§3　半群

§4　群与子群

§5　阿贝尔群和循环群

§7　陪集与拉格朗日定理

§8　同态与同构

§9　环和域

§5-9 环和域

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, *>，可将其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。

通常，把第一个二元运算★称为“加法”，

把第二个运算*称为“乘法”。

31

§5-9 环和域

例如，具有加法和乘法这两个二元运算的实数系统 $<R, +, \times>$ 和整数系统 $<I, +, \times>$。

对于 $\forall a, b, c \in R$(或 I)，

都有 $a \times (b+c)=(a \times b)+(a \times c)$

以及 $(b+c) \times a=(b \times a)+(c \times a)$，

这种联系就是乘法运算对于加法运算是可分配的。

§5-9 环和域

一、环

定义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∗对运算★可分配，即对$\forall a,b,c \in A$，

$$a*(b\bigstar c)= (a * b) \bigstar (a * c)$$

$$(b\bigstar c)*a = (b * a) \bigstar (c * a)$$

称代数结构<A, ★, ∗ >为环（*ring*）。

一般将★称为加运算，记为“+”，

将∗称为乘运算，记为“•”。

33

§5-9 环和域

例： 设<K，*>是 Klein四元群，其中K={e, a, b, c}。 *和•的运算如下所示。

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

则<K，*， •>是一个环。

§5-9 环和域

$\bullet$	e	a	b	c
e	e	e	e	e
a	e	a	e	a
b	e	b	e	b
c	e	c	e	c

证明：先证<K, •>是一个半群。

对于$\forall x \in$K，都有$x \bullet e = e \bullet x = e$；

a和c都是关于运算•的右幺元；

对于$\forall x \in$K都有$x \bullet b = e$。

对于$\forall x, y, z \in$K，可以证明必有$(x \bullet y) \bullet z = x \bullet (y \bullet z)$，

因为：

若$z=e$ 或 $z=b$，则 $(x \bullet y) \bullet z = e = x \bullet (y \bullet z)$

若$z=a$ 或 $z=c$，则 $(x \bullet y) \bullet z = x \bullet y = x \bullet (y \bullet z)$

§5-9 环和

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

其次证明•关于*是可分配的。

先证等式 $(y * z) \bullet x=(y \bullet x) *(z \bullet x)$

若$x=e$ 或 $x=b$，则 $(y * z) \bullet x = e =e * e=(y \bullet x) *(z \bullet x)$

若$x=a$ 或 $x=c$，则 $(y * z) \bullet x = (y \bullet x) *(z \bullet x)$

再证等式$x \bullet(y * z)=(x \bullet y) *(x \bullet z)$

若$y=z$，则 $y * z=e$，

所以 $x \bullet(y * z)=x \bullet e=e$

$(x \bullet y) *(x \bullet z)=(x \bullet y) *(x \bullet y)=e$

§5-9 环和

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

若y与z中有一个等于e，则等式

$$x \bullet (y * z)=(x \bullet y) *(x \bullet z)$$成立。

若y，z均不等于e，且$y\neq z$，那么有三种情况：

(1) $x \bullet (a * b)=x$ 且 $(x \bullet a) *(x \bullet b)=x * e=x$

(2) $x \bullet (a * c)=x \bullet b=e$ 且 $(x \bullet a) *(x \bullet c)=x * x=e$

(3) $x \bullet (b * c)=x \bullet a=x$ 且 $(x \bullet b) *(x \bullet c)=e * x=x$

所以，在代数系统<K，*，•>中运算•对于运算*是可分配的。因此，<K，*，•>是一个环。

37

§5-9 环和域

环的性质

定理1 设<A, +, •>为环，那么对任意a,b,c∈A

（1） $\theta \bullet a = a \bullet \theta = \theta$ （+的么元必为•的零元)

（2） $a \bullet (-b) = (-a) \bullet b = -(a \bullet b)$

（3） $(-a) \bullet (-b) = a \bullet b$

（4） $a \bullet (b-c) = (a \bullet b) - (a \bullet c)$

（5） $(b-c) \bullet a = (b \bullet a) - (c \bullet a)$

其中θ是加法么元,

-a表示a的加法逆元,并将a+(-b)记为a-b。

38

§5-9 环和域

证明思路:

（1）先证$\theta = \theta \bullet a$

因为 $\theta \bullet a = (\theta + \theta) \bullet a = \theta \bullet a + \theta \bullet a$

根据消去律 $\theta = \theta \bullet a$

$\theta \bullet a + \theta = \theta \bullet a + \theta \bullet a$

同理可证 $\theta = a \bullet \theta$ （略）

（2）先证$a \bullet (-b) = -(a \bullet b)$

因为 $a \bullet b + a \bullet (-b) = a \bullet [b + (-b)] = a \bullet \theta = \theta$

所以 $a \bullet (-b)$是$a \bullet b$的加法逆元,

即 $a \bullet (-b) = -(a \bullet b)$

同理可证 $(-a) \bullet b = -(a \bullet b)$ （略）

39

§5-9 环和域

（3） $(-a)\bullet(-b)= a\bullet b$

$\because a\bullet(-b)+ (-a)\bullet(-b) = [a+(-a)]\bullet(-b) = \theta\bullet(-b)=\theta$

$a\bullet(-b)+ \ (a\bullet b) = a\bullet[(-b)+b] = a\bullet\theta = \theta$

$\therefore \ (-a)\bullet(-b) = (a\bullet b)$

（4） $a \bullet(b-c)= (a \bullet b) - (a \bullet c)$

$a\bullet(b-c)=a\bullet[b+(-c)] = a\bullet b + a\bullet(- c)$

$= a\bullet b+(-a\bullet c) = a\bullet b-a\bullet c$

（5） $(b-c) \bullet a = (b \bullet a) - (c \bullet a)$

$(b-c)\bullet a=[b+(- c)]\bullet a= b\bullet a+ (- c) \bullet a$

$=b\bullet a+ (-c\bullet a) =b\bullet a-c\bullet a$

40

§5-9 环和域

一些特殊环

定义 2 设$< A, +, \bullet >$是环。

如果$< A, \bullet >$是可交换的, 称$< A, +, \bullet >$是交换环;

如果$< A, \bullet >$含有么元, 称$< A, +, \bullet >$是含么环。

雨课堂 Rain Classroom

§5-9 环和域

例：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：对于任意的A，B$\in P(S)$

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

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

容易证明$<P(S),+,\cdot>$是一个环，称它为**S的子集环**。

由于集合运算∩是可交换的，$<P(S),\cdot>$含有幺元S，因此子集环是含幺交换环。

42

§5-9 环和域

定义3 设$<A,+,\bullet>$是一个代数结构，如果满足：

1. $<A,+>$是阿贝尔群

2. $<A,\bullet>$ 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$a\bullet b\neq\theta$ 。

3. 运算$\bullet$ 对于运算 $+$ 是可分配的。

则称 $<A,+,\bullet>$为整环。

§5-9 环和域

例: <I，+，•>是整环。

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 环和域

定理2 在环<A, +, •>中的无零因子条件等价于消去律，即对于$c \neq \theta$ 和 $c \bullet a = c \bullet b$，必有$a = b$。

证明：环<A, +, •>中无零因子⇔消去律

先证环<A, +, •>中无零因子⇒消去律

若<A, +, •>中无零因子，并设$c \neq \theta$和$c \bullet a = c \bullet b$,

则有：$c \bullet a - c \bullet b = c \bullet (a - b) = \theta$,

所以，必有 $a = b$ 。

$a - b = \theta$

再证：消去律⇒ <A, +, •>中无零因子

若消去律成立，设 $a \neq \theta$， $a \bullet b = \theta$

则 $a \bullet b = a \bullet \theta$，消去a即得$b = \theta$ 。

§5-9 环和域

二、域

定义4 设< A,+, • >是一个代数结构,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,+, • >为域（*fields*）。

§5-9 环和域

例：$\langle Q, +, \bullet \rangle$, $\langle R, +, \bullet \rangle$, $\langle C, +, \bullet \rangle$都是域。

其中：Q为有理数集合，R是实数集合，C是复数集合，+, •分别是各数集上的加法和乘法运算。

注意： $\langle I, +, \bullet \rangle$是整环，但不是域。

因为$\langle I-\{0\}, \bullet \rangle$不是群。这说明，**整环不一定是域。**

§5-9 环和域

定理3 域一定是整环。

证明：设< A,+, • >是任一个域。

对于a,b,c∈A，且a≠0如果有a•b=a•c，（而1是乘法幺元）则

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

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

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

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

因此，< A,+, • >是一个整环。

48

§5-9 环和域

定理4 有限整环一定是域。

证明：设< A,+, • >是一个有限整环。

所以，对于a,b,c∈A，且c≠0，若a≠b，则a•c ≠ b•c。再由•运算的封闭性，就有A•c=A 。

对于乘法幺元 1，由A•c=A，必有d∈A，使得d •c=1，故d是c 的乘法逆元。

因此，有限整环< A,+, • >是一个域。

§5-9 环和域

三、同态映射

定义5-9.5 设< A,+, • >和< B, ⊕,⊙>是两个代数结构,如果一个从A到B的映射f，满足如下条件：

对于任意的a, b∈A， 有

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

2. $f(a \bullet b)=f(a) \odot f(b)$

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 环和域

设<A,+, •>是一个代数结构，并设R是在A上同时关于运算+和•的同余关系，即R是A上的一个等价关系，并且若$<a_1, a_2>, <b_1, b_2> \in R$，

则$<a_1+b_1, a_2+b_2>, <a_1 \cdot b_1, a_2 \cdot b_2> \in R$。

设$B=\{A_1, A_2, \ldots, A_r\}$是由同余关系R诱导的A的划分，其中，$A_i$ $(i=1,2,\ldots,r)$ 都是同余类。

在B上定义两个二元运算⊕和⊙如下：

$$A_i \oplus A_j = A_k \qquad a_1+a_2 \in A_k \quad (\text{其中} a_1 \in A_i, a_2 \in A_j)$$

$$A_i \odot A_j = A_l \qquad a_1 \cdot a_2 \in A_l \quad (\text{其中} a_1 \in A_i, a_2 \in A_j)$$

51

§5-9 环和域

定义一个从A到B的映射f，满足如下条件：

对于$\forall a \in A$，有$f(a) = A_i \quad a \in A_i$

那么，对于$\forall x,y \in A$，必有$x \in A_i$，$y \in A_j$以及

$$f(x+y) = A_k \qquad x+y \in A_k$$

而 $A_k = A_i \oplus A_j = f(x) \oplus f(y)$

所以 $f(x+y) = f(x) \oplus f(y)$

类似地 $f(x \bullet y) = f(x) \odot f(y)$

所以，f是由$<A,+,\bullet>$到$<B,\oplus,\odot>$的一个同态映射，故$<B,\oplus,\odot>$是$<A,+,\bullet>$的同态象。

§5-9 环和域

例：设<N,+, •>是一个代数系统，N 是自然数集， +和•是普通的加法和乘法运算，并设代数系统<{偶，奇}， ⊕， ⊙ >，其运算表如下：

⊕	偶	奇
偶	偶	奇
奇	奇	偶

⊙	偶	奇
偶	偶	偶
奇	偶	奇

容易验证 $f(n)=\begin{cases} \text{偶} & \text{若} n=2k,\ k=0,1,2\cdots \\ \text{奇} & \text{若} n=2k+1,\ k=0,1,2\cdots \end{cases}$

是由<N,+, •>到<{偶，奇}， ⊕， ⊙ >的同态映射。

因此， <{偶，奇}， ⊕， ⊙ >是<N,+, •>的一个同态象。

§5-9 环和域

定理5-9.5 任一环的同态象是一个环。

证明：设< A,+, •>是一个环，且<B, ⊕,⊙>是关于同态映射f的同态象。

由 <A,+>是阿贝尔群，易证<B, ⊕ >也是阿贝尔群。

由 <A,•>是半群，易证<B,⊙>也是半群。

对于$\forall b_1, b_2, b_3 \in B$，必有相应的$a_1, a_2, a_3 \in A$，使得

$$f(a_i)= b_i \quad (i=1, 2, 3)$$

54

§5-9 环和域

于是 $b_1 \odot (b_2 \oplus b_3) = f(a_1) \odot (f(a_2) \oplus f(a_3))$

$$= f(a_1) \odot (f(a_2+a_3))$$

$$= f(a_1 \bullet (a_2+a_3))$$

$$= f((a_1 \bullet a_2) + (a_1 \bullet a_3))$$

$$= f(a_1 \bullet a_2) \oplus f(a_1 \bullet a_3)$$

$$= (f(a_1) \odot f(a_2)) \oplus (f(a_1) \odot f(a_3))$$

$$= (b_1 \odot b_2) \oplus (b_1 \odot b_3)$$

同理可证 $(b_2 \oplus b_3) \odot b_1 = (b_2 \odot b_1) \oplus (b_3 \odot b_1)$

因此 $< B, \oplus, \odot >$ 也是一个环。

55