离散数学 II
Discrete Mathematics II

封筠

fengjun@stdu.edu.cn

20-12

课程回顾

陪集和拉格朗日定理：集合的积、逆、左陪集、代表元素、拉格朗日定理和**2**个推论

5-8 同态与同构

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。

●学习本节要熟悉如下术语（10个）：

同态映射、同态象、同态核、满同态、单一同态、自同态、同构映射、自同构、同余关系、同余类

●要求：

掌握5个定理

一、同态

1、同态映射、同态象

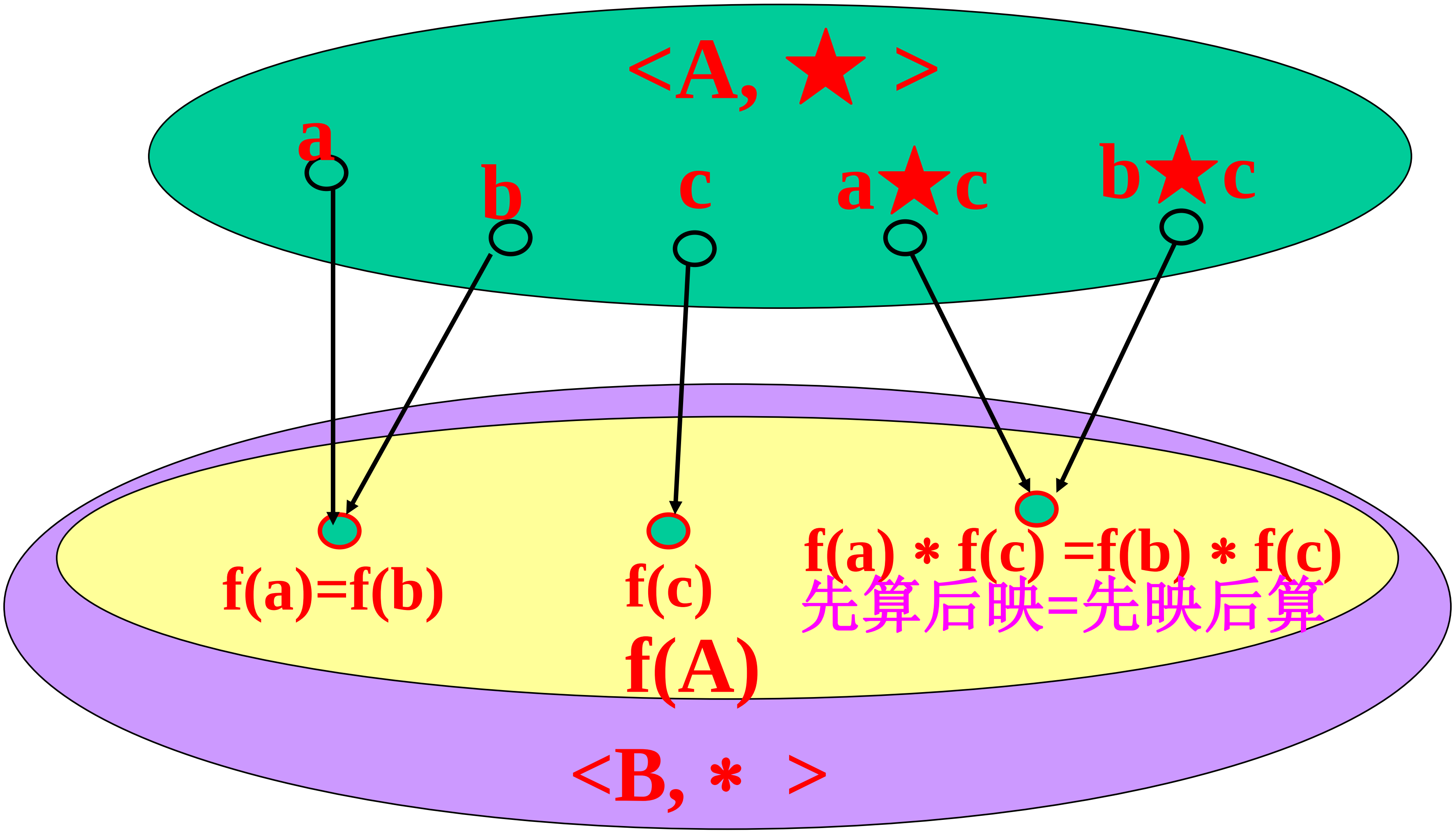
定义5-8.1 设$<A, ★>$和$<B, * >$是两个代数系统，★和$*$分别是A和B上的二元运算，f是从A到B的一个映射，使得对任意$a_1, a_2 \in A$，有

$$f(a_1 ★ a_2) = f(a_1) * f(a_2)$$ （先算后映=先映后算）

则称f为由代数结构$<A, ★>$到$<B, * >$的同态映射（*homomorphism*），称代数结构$<A, ★>$同态于$<B, * >$，记为$A \sim B$。$<f(A), * >$称为$<A, ★>$的一个同态象（*image under homomorphism*）。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

2、举例

例1 考察代数系统<I, · >，这里I是整数集，·是普通乘法运算。如果我们对运算结果只感兴趣于正、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，如下表所示。

⊙	正	负	零
正	正	负	零
负	负	正	零
零	零	零	零

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。

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。

应该指出，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。

练习 P221（1）

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$g \circ f$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

$$f(a_1 ★ a_2) = f(a_1) * f(a_2)$$

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

$$= g(f(a_1) * f(a_2))$$

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

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

所以$g \circ f$是由<A，★>到<C，△>的同态映射。

二、同构

1、定义

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，记作 $A \cong B$ 。

2、举例

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。

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$\langle N, + \rangle$到$\langle N_k, +_k \rangle$的一个满同态。

例4 设$H=\{x|x=dn$，d是某一个正整数，$n \in I\}$，定义映射f：$I \to H$为对任意$n \in I$

$$f(n)=dn$$

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

例题1　设A ={a,b,c,d}，在A上定义的一个二元运算★ 如表1所示。又设B={ α，β，γ，δ }，在B上定义的一个二元运算*如表2所示。证明<A, ★ >和<B, * >是同构的。

表1

★	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2

*	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

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

显然，f是一个从A到B的双射，由表1和表2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

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

那么，g也是由<A, ★ >到<B, * >的一个同构。

说明同构映射可以是不唯一的。

例5 下表中的代数系统<A, ★ >、<B, Δ >和<C, * >是同构的。

★	a	b
a	a	b
b	b	a

<A, ★ >

Δ	偶	奇
偶	偶	奇
奇	奇	偶

<B, Δ >

*	0°	180°
0°	0°	180°
180°	180°	0°

<C, * >

同构这个概念很重要。从上例中可以看到，形式上不同的代数系统，如果它们是同构的话，那么，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。

3、自同态与自同构

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**。

练习 P221（2）

设<G，*>是一个群，而a∈G，如果*f*是从G到G的映射，使得对每一个x ∈ G，都有

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

试证明*f*是从G到G上的自同构。

即要证明*f*是G上的一个双射，且对任意x，y∈G有 $f(x*y)=f(x)*f(y)$

证明 ①任取x，y∈G， $x \neq y$

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

$$f(y)=a*y*a^{-1}$$

若f(x)=f(y)，则有x=y，与$x \neq y$矛盾。所以f是入射。

②任取y∈G，有

$x=a^{-1}*y*a \in G$，使得

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

所以f是满射。

因此f是G上的一个双射。

③对于任意x，y∈G有

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

$=a*x*a^{-1}*a*y*a^{-1}$

$= f(x)*f(y)$

所以f是从G到G上的自同构。

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**, ★〉可以通过恒等映射与它自身同构，即自反性成立。

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**, ★〉。

传递性，如果**f**是由〈**A**, ★〉到〈**B**, *〉的同构映射，**g**是由〈**B**, *〉到〈**C**, △〉的同构映射，那么**g o f**就是〈**A**, ★〉到〈**C**, △〉的同构映射。因此同构关系是等价关系。 □

定理5-8.2　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。

□证明思路:

先证（a）：< f(A),* >是半群

➩. 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)⊆B。

对于任意的a，b∈f(A)，必有x, y∈A ，使得

f(x)=a ，f(y)=b

在A中必有z=x★y, 所以

$$a*b=f(x)*f(y)=f(x★y)=f(z)\in f(A)$$

⌘.证∗在f(A)上满足结合律

对于任意的$a,b,c\in f(A)$,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

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

$$= f(x★(y★z))\quad = f((x★y)★z)$$

$$= f(x★y) *f(z)\quad =(f(x)*f(y))*f(z)$$

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

证明了< f(A),∗ > 是半群。

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。因对于任意的$a\in f(A)$, 必有$x\in A$, 使得

$$f(x)=a$$

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

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

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

最后证（c）：$< f(A),* >$是群

设$<A, ★>$是群,对于任意的$a \in f(A)$,必有$x \in A$,使得

$$f(x)=a$$

因为 $<A, ★>$是群, 所以对于任意的$x \in A$,都有逆元 $x^{-1} \in A$，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$< f(A),* >$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 □

作业：

P221 （3）、 （4）

The End