第五部分 代数系统简介

主要内容

- 二元运算及其性质

  二元运算和一元运算、二元运算性质、特异元素

- 代数系统的概念
- 几个典型的代数系统

  半群、独异点、群

  环与域

  格与布尔代数

- 代数系统的同构与同态

第十四章 代数系统简介

主要内容

二元运算及其性质

- 一元和二元运算定义及其实例
- 二元运算的性质

代数系统

- 代数系统定义及其实例
- 子代数
- 积代数

代数系统的同态与同构

14.1 代数系统的基本概念

定义14.1 设S为集合，函数f：$S \times S \to S$ 称为S上的二元运算，简称为二元运算．函数 f:$S \to S$ 称为S上的一元运算，简称一元运算.

- S 中任何元素都可以进行运算，且运算的结果惟一.
- S 中任何元素的运算结果都属于 S，即 S 对该运算封闭.

例1 (1) 自然数集合N上的加法和乘法是N上的二元运算，但减法和除法不是.

(2) 整数集合Z上的加法、减法和乘法都是Z上的二元运算，而除法不是．求一个数的相反数是Z上的一元运算.

(3) 非零实数集R*上的乘法和除法都是R*上的二元运算，而加法和减法不是．求倒数是R*上的一元运算.

实例

(4) 设M_n(R)表示所有n 阶(n≥2)实矩阵的集合，即

$$M_n(R)=\left\{\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \cdots & & & \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \middle| \; a_{ij}\in R,\ i,j=1,2,\ldots,n\right\}$$

矩阵加法、乘法是M_n(R)上的二元运算. 转置是一元运算.

(5) S为任意集合，则∪、∩、－、⊕ 为$P(S)$上二元运算. ~运算为一元运算.

(6) S^S为S上的所有函数的集合，则合成运算∘为S^S上二元运算. 求反函数不一定是一元运算.

二元与一元运算的表示

1. 算符

可以用$\circ$, $*$, $\cdot$, $\oplus$, $\otimes$,Δ 等符号表示二元或一元运算，称为算符.

对二元运算$\circ$，如果 x 与 y 运算得到 z，记做 $x\circ y = z$

对一元运算Δ, x的运算结果记作Δx.

2. 表示二元或一元运算的方法: 解析公式和运算表

公式表示

例 设R为实数集合，如下定义R上的二元运算$*$:

$$\forall x, y\in R,\ \ x * y = x.$$

那么 $3*4 = 3$， $0.5*(-3) = 0.5$

运算表

运算表：表示有穷集上的一元和二元运算

$\circ$	a_1	a_2	$\cdots$	a_n
a_1	$a_1 \circ a_1$	$a_1 \circ a_2$	$\cdots$	$a_1 \circ a_n$
a_2	$a_2 \circ a_1$	$a_2 \circ a_2$	$\cdots$	$a_2 \circ a_n$
.		$\cdots$		
.		$\cdots$		
.		$\cdots$		
a_n	$a_n \circ a_1$	$a_n \circ a_2$	$\cdots$	$a_n \circ a_n$

二元运算的运算表

	$\circ a_i$
a_1	$\circ a_1$
a_2	$\circ a_2$
.	.
.	.
.	.
a_n	$\circ a_n$

一元运算的运算表

运算表的实例

例2 设 $S=P(\{a,b\})$，S 上的 $\oplus$ 和 $\sim$ 运算的运算表如下

$\oplus$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\varnothing$	$\varnothing$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a\}$	$\{a\}$	$\varnothing$	$\{a.b\}$	$\{b\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\varnothing$	$\{a\}$
$\{a,b\}$	$\{a,b\}$	$\{b\}$	$\{a\}$	$\varnothing$

x	$\sim x$
$\varnothing$	$\{a,b\}$
$\{a\}$	$\{a\}$
$\{b\}$	$\{b\}$
$\{a,b\}$	$\varnothing$

二元运算的性质

定义14.2-4 设$\circ$为S上的二元运算,

(1) 若对任意$x,y\in S$ 有 $x\circ y=y\circ x$, 则称运算在S上满足交换律.

(2) 若对任意$x,y,z\in S$有 $(x\circ y)\circ z=x\circ(y\circ z)$, 则称运算在$S$上满足结合律.

(3) 若对任意$x\in S$ 有 $x\circ x=x$, 则称运算在S上满足幂等律.

定义14.5-6 设$\circ$和$*$为S上两个不同的二元运算,

(1) 若对任意$x,y,z\in S$有 $(x*y)\circ z=(x\circ z)*(y\circ z)$，

$z\circ(x*y)=(z\circ x)*(z\circ y)$, 则称$\circ$运算对$*$运算满足分配律.

(2) 若$\circ$和$*$都可交换,且对任意$x,y\in S$有 $x\circ(x*y)=x$， $x*(x\circ y)=x$, 则称$\circ$和$*$运算满足吸收律.

实例

Z, Q, R分别为整数、有理数、实数集；$M_n(R)$为n阶实矩阵集合, n≥2；$P(B)$为幂集；A^A为从A到A的函数集，$|A|$≥2

集合	运算	交换律	结合律	幂等律
Z,Q,R	普通加法+ 普通乘法×	有 有	有 有	无 无
$M_n(R)$	矩阵加法+ 矩阵乘法×	有 无	有 有	无 无
$P(B)$	并∪ 交∩ 相对补− 对称差⊕	有 有 无 有	有 有 无 有	有 有 无 无
A^A	函数复合∘	无	有	无

实例

Z, Q, R分别为整数、有理数、实数集；$M_n(R)$为n阶实矩阵集合, $n\geq 2$；$P(B)$为幂集；A^A为从A到A的函数集，$|A|\geq 2$

集合	运算	分配律	吸收律
Z,Q,R	普通加法+与乘法×	×对+可分配 +对×不分配	无
$M_n(R)$	矩阵加法+与乘法×	×对+可分配 +对×不分配	无
$P(B)$	并∪与交∩	∪对∩可分配 ∩对∪可分配	有
	交∩与对称差⊕	∩对⊕可分配	无

特异元素：单位元、零元

定义14.7-9 设$\circ$为S上的二元运算，

(1) 如果存在e_l(或e_r)$\in S$，使得对任意 $x\in S$ 都有

$$e_l \circ x = x \quad (\text{或 } x \circ e_r = x),$$

则称e_l(或e_r)是S中关于$\circ$运算的左(或右)单位元.

若$e\in S$关于$\circ$运算既是左单位元又是右单位元，则称e为S上关于$\circ$运算的单位元. 单位元也叫做幺元.

(2) 如果存在θ_l(或θ_r)$\in S$，使得对任意 $x\in S$ 都有

$$\theta_l \circ x = \theta_l \quad (\text{或 } x \circ \theta_r = \theta r),$$

则称θ_l(或θ_r)是S 中关于$\circ$运算的左(或右)零元.

若$\theta\in S$ 关于$\circ$运算既是左零元又是右零元，则称θ为S上关于运算$\circ$的零元.

可逆元素和逆元

(3) 设∘为S上的二元运算，令e为S中关于运算∘的单位元.

对于$x \in S$，如果存在y_l (或y_r)$\in S$使得

$$y_l \circ x = e \quad (\text{或} x \circ y_r = e)$$

则称y_l (或 y_r)是x的左逆元（或右逆元）.

关于∘运算，若$y \in S$ 既是 x 的左逆元又是 x 的右逆元，则称 y为x的逆元. 如果 x 的逆元存在，就称 x 是可逆的.

可以证明：

- 对于给定二元运算，单位元或零元如果存在，则是唯一的.
- 对于可结合的二元运算，给定元素若存在逆元，则是唯一的逆元

实例

集合	运算	单位元	零元	逆元
Z,Q,R	普通加法+ 普通乘法×	0 1	无 0	x逆元$-x$ x逆元x^{-1} ($x^{-1}\in$给定集合)
$M_n(R)$	矩阵加法+ 矩阵乘法×	n阶全0矩阵 n阶单位矩阵	无 n阶全0 矩阵	X逆元$-X$ X的逆元X^{-1} （X可逆）
$P(B)$	并∪ 交∩ 对称差⊕	$\varnothing$ B $\varnothing$	B $\varnothing$ 无	$\varnothing$的逆元为$\varnothing$ B的逆元为B X的逆元为X

消去律

定义14.10 设$\circ$为S上的二元运算，如果对于任意的 $x, y, z \in S$ 满足以下条件：

(1) 若$x \circ y = x \circ z$且$x \neq \theta$，则$y=z$；

(2) 若$y \circ x = z \circ x$且$x \neq \theta$，则$y=z$；

称$\circ$运算满足**消去律**，其中(1)为**左消去律**，(2)为**右消去律**.

- 注意被消去的 x 不能是运算的零元 θ.

整数集合上的加法和乘法满足消去律.

$P(S)$上的并和交一般不满足消去律. 对称差运算$\oplus$满足消去律，$\forall A,B,C \in P(S)$，都有

$$A \oplus B = A \oplus C \Rightarrow B = C$$

$$B \oplus A = C \oplus A \Rightarrow B = C$$

代数系统

定义14.11 非空集合S和S上k个一元或二元运算$f_1,f_2,\ldots, f_k$组成的系统称为**代数系统**, 简称代数，记做$<S, f_1, f_2, \ldots, f_k>$.

实例：

(1) $<\mathrm{N},+>$,$<\mathrm{Z},+,\cdot>$,$<\mathrm{R},+,\cdot>$是代数系统，+和·分别表示普通加法和乘法.

(2) $<M_n(R),+,\cdot>$是代数系统，＋和·分别表示 n 阶($n\geq 2$)实矩阵的加法和乘法.

(3) $<\mathrm{Z}_n,\oplus,\otimes>$是代数系统，$\mathrm{Z}_n=\{0,1,\ldots,n-1\}$，⊕和⊗分别表示模$n$的加法和乘法，对于$x,y\in \mathrm{Z}_n$，$x\oplus y=(x+y)\bmod n$，$x\otimes y=(xy)\bmod n$

(4) $<P(S),\cup,\cap,\sim>$是代数系统，∪和∩为并和交，~为绝对补

代数系统的成分与表示

构成代数系统的成分：

- 集合（也叫载体，规定了参与运算的元素）
- 运算（这里只讨论有限个二元和一元运算）
- 代数常数（通常是与运算相关的特异元素：如单位元等）

研究代数系统时，如果把运算具有它的特异元素也作为系统的性质之一，那么这些特异元素可以作为系统的成分，叫做代数常数.

例如：代数系统<Z,+,0>：集合Z, 运算+, 代数常数0

代数系统<*P*(*S*),∪,∩>：集合*P*(*S*), 运算∪和∩，无代数常数

代数系统的表示

(1) 列出所有的成分：集合、运算、代数常数（如果存在）

如<Z,+,0>, <*P*(*S*),∪,∩>

(2) 列出集合和运算，在规定系统性质时不涉及具有单位元的性质（无代数常数）

如<Z,+>, <*P*(*S*),∪,∩>

(3) 用集合名称简单标记代数系统

在前面已经对代数系统作了说明的前提下使用

如代数系统*Z*, *P*(*B*)

同类型与同种代数系统

定义14.12

(1) 如果两个代数系统中运算的个数相同，对应运算的元数相同，且代数常数的个数也相同，则称它们是同类型的代数系统.

(2) 如果两个同类型的代数系统规定的运算性质也相同，则称为同种的代数系统.

例如 $V_1=\langle R, +, \cdot, 0, 1\rangle$，$V_2=\langle M_n(R), +, \cdot, \theta, E\rangle$, θ为 n 阶全0矩阵，E为 n 阶单位矩阵, $V_3=\langle P(B), \cup, \cap, \varnothing, B\rangle$

- V_1, V_2, V_3是同类型的代数系统，它们都含有2个二元运算, 2个代数常数.
- V_1, V_2是同种的代数系统，V_1, V_2与V_3不是同种的代数系统

运算性质比较

V_1	V_2	V_3
+ 可交换、可结合 · 可交换、可结合 + 满足消去律 · 满足消去律 · 对 + 可分配 + 对 · 不可分配 + 与 · 没有吸收律	+ 可交换、可结合 · 可交换、可结合 + 满足消去律 · 不满足消去律 · 对 + 可分配 + 对 · 不可分配 + 与 · 没有吸收律	∪可交换、可结合 ∩可交换、可结合 ∪不满足消去律 ∩不满足消去律 ∩对∪可分配 ∪对∩可分配 ∪与∩满足吸收律

14.2几个典型的代数系统

主要内容

- 半群、独异点与群
- 环与域
- 格与布尔代数

半群、独异点与群的定义

定义14.13

(1) 设$V=\langle S, \circ \rangle$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$V=\langle S,\circ\rangle$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$V=\langle S,\circ,e\rangle$.

(3) 设$V=\langle S,\circ\rangle$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⊕为集合对称差运算

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

(5) $<A^A,\circ>$为半群，也是独异点，其中∘为函数的复合运算

(6) $<R^*,\circ>$为半群，其中R^*为非零实数集合，∘运算定义如下：$\forall x, y \in R^*, x \circ y=y$

半群：Σ上的字代数和语言

例2 设Σ是有穷字母表，$\forall k\in \mathrm{N}$，定义下述集合：

$$\Sigma_k=\{a_1a_2\ldots a_k \mid a_i\in\Sigma\}$$

是Σ上所有长度为k的串的集合. 当k=0时，$\Sigma_0=\{\lambda\}$，λ表示空串. 令 表示Σ上所有有限长度的串的集合，$\Sigma^+=\Sigma^*-\{\lambda\}$则表示$\Sigma$上所有长度至少为1的有限串的集合. 在$\Sigma^*$上可以定义串的连接运算，$\forall\omega_1,\omega_2\in\Sigma^*$，$\omega_1=a_1a_2\ldots a_m$, $\omega_2=b_1b_2\ldots b_n$有

$$\omega_1\omega_2= a_1a_2\ldots a_mb_1b_2\ldots b_n$$

显然Σ^*关于连接运算构成一个独异点, 称为Σ上的字代数. Σ上的语言L就是Σ^*的一个子集.

群码

例3 某二进制码的码字$x=x_1x_2\ldots x_7$由7位构成，其中x_1, x_2, x_3和x_4为数据位，x_5, x_6和x_7为校验位，且满足：

$$x_5=x_1\oplus x_2\oplus x_3$$

$$x_6=x_1\oplus x_2\oplus x_4$$

$$x_7=x_1\oplus x_3\oplus x_4$$

这里的⊕是模2加法.

设G为所有码字构成的集合，在G上定义二元运算如下：

$$\forall x,y\in G,\quad x\circ y= z_1z_2\ldots z_7,\quad z_i=x_i\oplus y_i,\quad i=1,2,\ldots,7.$$

那么$\langle G,\circ\rangle$构成群. 这样的码称为群码

群的相关概念及子群

有限群：若群G是有穷集，则称G是有限群，否则称为无限群

群 G的阶：群G含有的元素数，有限群G的阶记作$|G|$.

交换群或阿贝尔(Abel)群：群中运算可交换

实例：<Z,+>和<R,+>是无限群，$\langle Z_n,\oplus\rangle$是$n$阶群.

上述所有的群都是交换群，但n阶（$n\geq 2$）实可逆矩阵的集合（是M_n(R)的真子集）关于矩阵乘法构成的群是非交换群

子群：群G的非空子集H关于群的运算构成群，称为G的子群.

实例： $H=nZ=\{nk \mid k\in Z\}$，n为给定自然数，是<Z,+>的子群.

当n=0和1时， 子群分别是{0}和Z，称为平凡子群；

2Z由能被2整除的全体整数构成，也是子群.

群的直积

定义14.14 设G_1=<A,∘>和G_2=<B,∗>是群，∘和∗分别为它们的二元运算，在集合$A\times B$上定义新的二元运算▪，$\forall$<a_1,b_1>,<a_2,b_2>$\in A\times B$，有

$$<a_1,b_1>\blacksquare<a_2,b_2>=<a_1\circ a_2,b_1*b_2>$$

称G=<$A\times B$,▪ >为G_1与G_2的**直积**，记作$G_1\times G_2$.

例4 G_1,G_2分别为模2加和模3加群，它们的直积运算

⊕	<0,0>	<0,1>	<1,0>	<1,1>	<2,0>	<2,1>
<0,0>	<0,0>	<0,1>	<1,0>	<1,1>	<2,0>	<2,1>
<0,1>	<0,1>	<0,0>	<1,1>	<1,0>	<2,1>	<2,0>
<1,0>	<1,0>	<1,1>	<2,0>	<2,1>	<0,0>	<0,1>
<1,1>	<1,1>	<1,0>	<2,1>	<2,0>	<0,1>	<0,0>
<2,0>	<2,0>	<2,1>	<0,0>	<0,1>	<1,0>	<1,1>
<2,1>	<2,1>	<2,0>	<0,1>	<0,0>	<1,1>	<1,0>

环与域

定义10.15 设<R,+,·>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,·>构成半群

(3) · 运算关于+运算适合分配律

则称<R,+,·>是一个**环**.

通常称+运算为环中的**加法**，·运算为环中的**乘法**.

定义14.16 设<R,+,·>是环，若

(1) 环中乘法 可交换;

(2) R中至少含有两个元素. 且$\forall a \in R-\{0\}$，都有$a^{-1} \in R$;

则称R是**域**.

- 0指加法单位元， a^{-1}指a的乘法逆元

环与域的实例

例5

(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**. Q、R 和 C 也称为有理数域、**实数域**、**复数域**.

(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.

(4) 设$Z_n=\{0,1, \ldots , n-1\}$，$\oplus$和$\otimes$分别表示模$n$的加法和乘法，则$\langle Z_n,\oplus,\otimes\rangle$构成环，称为**模 n的整数环**. 当n为素数时Z_n构成域.

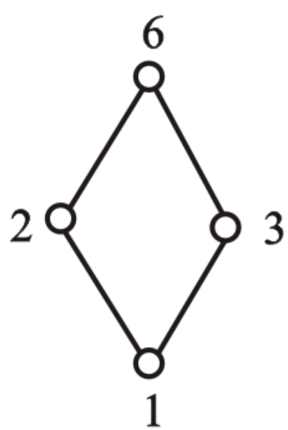
格的定义与性质

定义14.17 设$<S, \preccurlyeq>$是偏序集，如果$\forall x,y \in S$，$\{x,y\}$都有最小上界和最大下界，则称S关于偏序$\preccurlyeq$作成一个**格**.

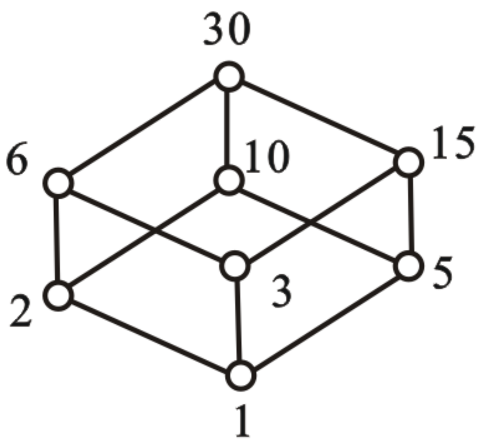
求$\{x,y\}$ 最小上界和最大下界看成 x 与 y 的二元运算$\vee$和$\wedge$，

例6 设n是正整数，S_n是n的正因子的集合. D为整除关系，则偏序集$<S_n,D>$构成格. $\forall x,y \in S_n$，$x \vee y$是$\text{lcm}(x,y)$，即x与y的最小公倍数. $x \wedge y$是$\gcd(x,y)$，即x与y的最大公约数.

(S_8,D)



(S_6,D)



(S_{30},D)

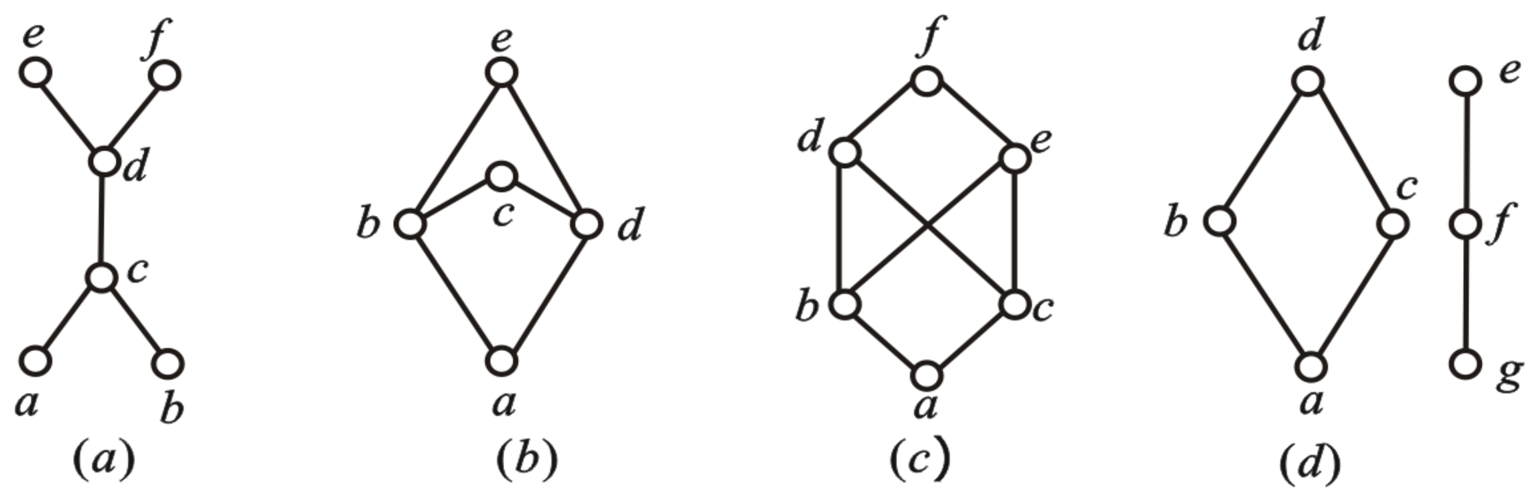
实例

例7 判断下列偏序集是否构成格，并说明理由.

(1) $<P(B),\subseteq>$，其中$P(B)$是集合B的幂集.

(2) $<Z, \leq>$，其中Z是整数集，≤为小于或等于关系.

(3) 偏序集的哈斯图分别在下图给出.



(1) 幂集格. $\forall x,y \in P(B)$，$x \vee y$就是$x \cup y$，$x \wedge y$就是$x \cap y$.

(2) 是格. $\forall x,y \in Z$，$x \vee y = \max(x,y)$，$x \wedge y = \min(x,y)$，

(3) 都不是格. 可以找到两个结点缺少最大下界或最小上界

格的性质：算律

设$<L, \preccurlyeq>$是格, 则运算∨和∧适合交换律、结合律、幂等律和吸收律, 即

(1) $\forall a,b \in L$ 有

$$a \vee b = b \vee a, \quad a \wedge b = b \wedge a$$

(2) $\forall a,b,c \in L$ 有

$$(a \vee b) \vee c = a \vee (b \vee c), \quad (a \wedge b) \wedge c = a \wedge (b \wedge c)$$

(3) $\forall a \in L$ 有

$$a \vee a = a, \quad a \wedge a = a$$

(4) $\forall a,b \in L$ 有

$$a \vee (a \wedge b) = a, \quad a \wedge (a \vee b) = a$$

格作为代数系统的定义

设$<S,*,\circ>$是具有两个二元运算的代数系统, 若对于$*$和$\circ$运算适合交换律、结合律、吸收律, 则可以适当定义S中的偏序 $\preccurlyeq$, 使得 $<S,\preccurlyeq>$ 构成格, 且$\forall a,b\in S$ 有

$$a\wedge b = a*b,\ a\vee b = a\circ b.$$

格的等价定义：设$<S, *, \circ>$是代数系统, $*$和$\circ$是二元运算, 如果$*$和$\circ$满足交换律、结合律和吸收律, 则$<S, *,\circ>$构成格.

分配格、有补格与布尔代数

定义14.18 设<L,∧,∨>是格, 若$\forall a,b,c\in L$,有

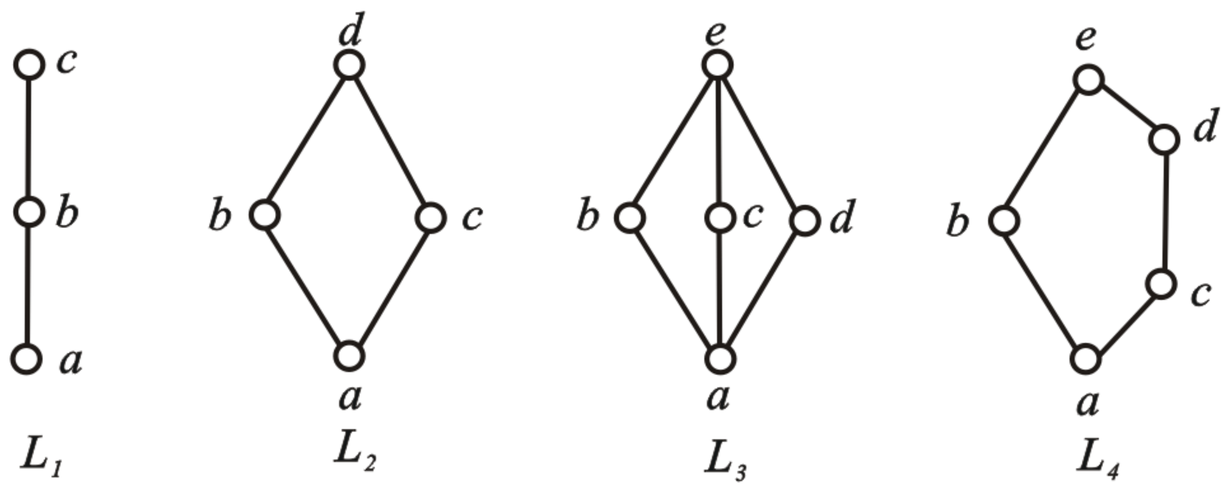
$$a\wedge(b\vee c) = (a\wedge b)\vee(a\wedge c)$$

$$a\vee(b\wedge c) = (a\vee b)\wedge(a\vee c)$$

则称L为分配格.

- 注意：可以证明以上两个条件互为充分必要条件

实例



L_1 和 L_2 是分配格, L_3 和 L_4不是分配格.
称 L_3为钻石格, L_4为五角格.

分配格的判别

分配格的判别：设 L 是格，则 L 是分配格当且仅当 L 不含有与钻石格或五角格同构的子格.

- 小于五元的格都是分配格.
- 任何一条链都是分配格.

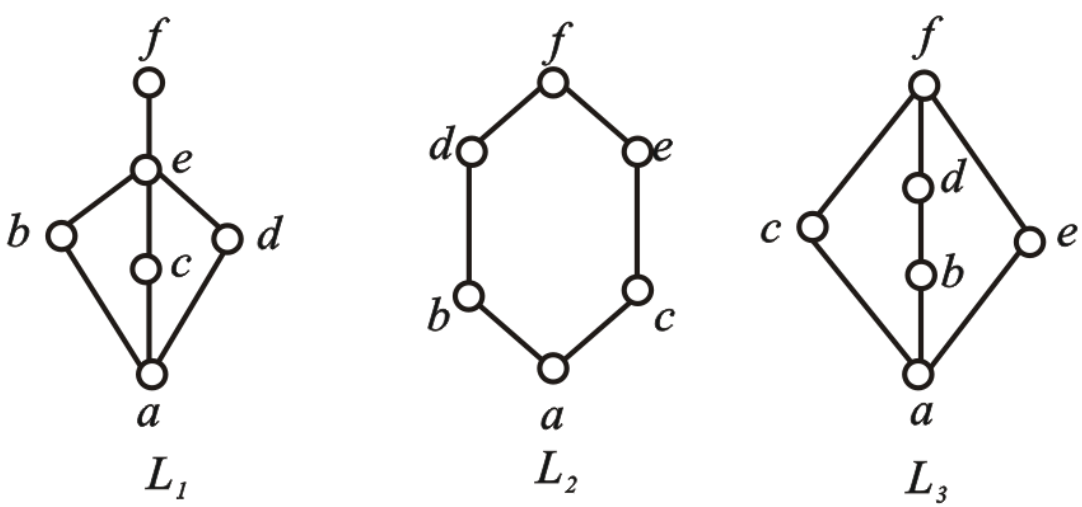
例6 说明图中的格是否为分配格, 为什么？

解 都不是分配格.

$\{a,b,c,d,e\}$是L_1的子格，同构于钻石格

$\{a,b,c,e,f\}$是L_2的子格，同构于五角格；

$\{a,c,b,e,f\}$是L_3的子格同构于钻石格.



有补格的定义

定义14.19 设L是格,

(1) 若存在$a\in L$使得$\forall x\in L$有 $a \preccurlyeq x$, 则称a为L的全下界, 记为0; 若存在$b\in L$使得$\forall x\in L$有 $x \preccurlyeq b$, 则称b为L的全上界, 记为1.

(2) 若L存在全下界和全上界, 则称L 为有界格, 一般将有界格L记为$<L,\wedge,\vee,0,1>$.

定义14.20 设$<L,\wedge,\vee,0,1>$是有界格, $a\in L$, 若存在$b\in L$ 使得

$$a\wedge b = 0 \text{ 和 } a\vee b = 1$$

成立, 则称b是a的补元.

定义14.21 设$<L,\wedge,\vee,0,1>$是有界格, 若L中所有元素都有补元存在, 则称L为有补格.

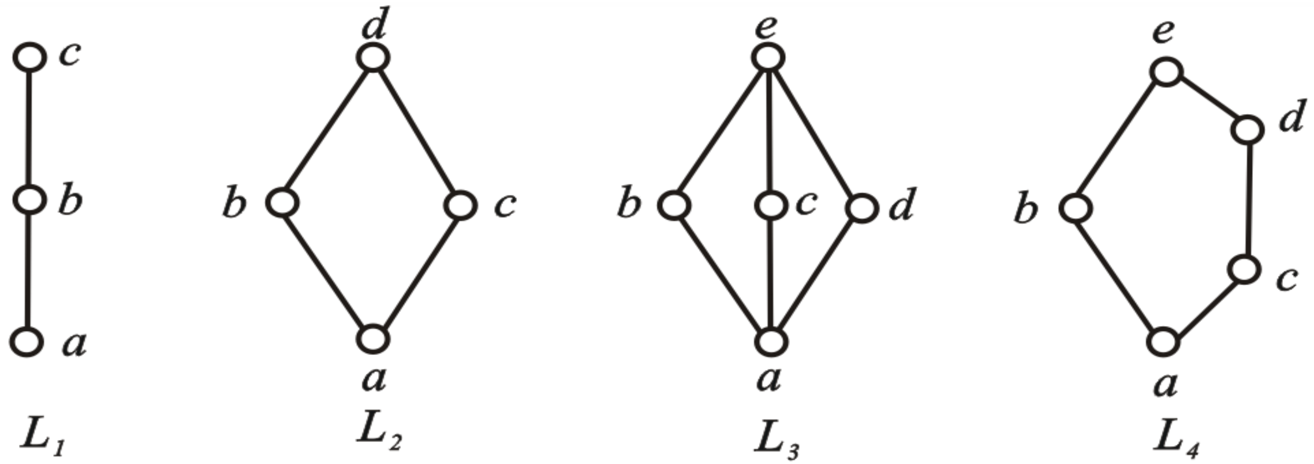
补元的性质

注意:

- 在任何有界格中, 全下界0与全上界1互补.
- 对于一般元素, 可能存在补元, 也可能不存在补元.
- 如果存在补元, 可能是惟一的, 也可能是多个补元.
- 对于有界分配格, 如果元素存在补元, 一定是惟一的.

有界格中的补元及实例

例7



L_1: a 与 c 互补, a 为全下界, c为全上界, b 没有补元.

L_2: a 与 d 互补, a 为全下界, d 为全上界, b与 c互补.

L_3: a 与 e 互补, a 为全下界, e 为全上界, b 的补元是 c 和 d ; c 的补元是 b 和 d ; d 的补元是 b 和 c .

L_4: a 与 e 互补, a 为全下界, e 为全上界, b 的补元是 c 和 d ; c 的补元是 b ; d 的补元是 b .

L_2, L_3和L_4是有补格, L_1不是有补格.

布尔代数的定义与实例

定义14.22 如果一个格是有补分配格, 则称它为布尔格或布尔代数. 布尔代数标记为$<B,\wedge,\vee,', 0, 1>$, $'$为求补运算.

例8 设 S_{110} = {1, 2, 5, 10, 11, 22, 55, 110}是110的正因子集合，gcd表示求最大公约数的运算，lcm表示求最小公倍数的运算，问$<S110, gcd, lcm>$是否构成布尔代数？为什么？

解 (1) 不难验证S_{110}关于gcd 和 lcm 运算构成格. (略)

(2) 验证分配律 $\forall x, y, z \in S_{110}$ 有

$$gcd(x, lcm(y, z)) = lcm(gcd(x, y), gcd(x, z))$$

(3) 验证它是有补格，1作为$S110$中的全下界, 110为全上界, 1和110互为补元, 2和55互为补元, 5和22互为补元, 10和11互为补元, 从而证明了$<S110, gcd, lcm>$为布尔代数.

实例

例9 设B为任意集合, 证明B的幂集格$<P(B), \cap, \cup, \sim, \varnothing, B>$构成布尔代数, 称为集合代数.

证 (1) $P(B)$关于$\cap$和$\cup$构成格, 因为$\cap$和$\cup$运算满足交换律, 结合律和吸收律.

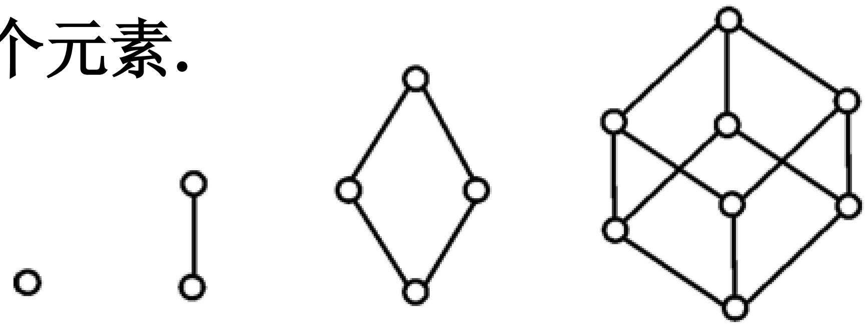
(2) 由于$\cap$和$\cup$互相可分配, 因此$P(B)$是分配格.

(3) 全下界是空集$\varnothing$, 全上界是B.

(4) 根据绝对补的定义, 取全集为B, $\forall x \in P(B)$, $\sim x$是x的补元.

从而证明$P(B)$是有补分配格, 即布尔代数.

- 有限布尔代数含有2^n个元素.



代数系统的同构与同态

定义14.23 设$V_1=<A,\circ>$和$V_2=<B,*>$是同类型的代数系统，$f: A\to B$，且$\forall x,y\in A$有 $f(x\circ y) = f(x)*f(y)$，则称f是V_1到V_2的**同态映射**，简称同态.

f若是单射，称为**单同态**；若是满射，称为**满同态**(V_2是V_1的同态像，记作$V_1\sim V_2$)；若是双射，称为**同构**，记作$V_1\cong V_2$.

V到V的同态f称为自同态. 类似地可以定义单自同态、满自同态和自同构.

同态性质：设 f 是$V_1=<A,\circ>$到$V_2<B,*>$的同态映射，

(1) 若$\circ$运算具有交换律、结合律、幂等律等，那么在$f(V_1)$中$*$运算也具有相同的算律（注意，消去律可能有例外）.

(2) $f(e_1)=e_2$，$f(\theta_1)= \theta_2$，$f(x^{-1})=f(x)^{-1}$

实例

例10 (1) V_1=<Z,+>, V_2=<Z_n,⊕>. Z为整数集合，+为普通加法；Z_n={0,1,…,n−1}，⊕为模n加. 令

$$f: Z \to Z_n,\ f(x)=(x) \bmod n$$

f 是V_1到V_2的满同态.

(2) 设V_1=<R,+>, V_2=<R^*,·>，R和R*分别为实数集与非零实数集，+和·分别表示普通加法与乘法. 令

$$f: R \to R^*,\ f(x)= e^x$$

f 是V_1到V_2的单同态.

(3) 设V=<Z,+>，Z为整数集，+为普通加法. $\forall a \in Z$，令

$$f_a: Z \to Z,\ f_a(x)=ax,$$

f_a是V的自同态. f_0为零同态；当a=±1时，称f_a为自同构；除此之外其他的f_a都是单自同态.

第十四章 习题课

主要内容

- 代数系统的构成：非空集合、封闭的二元和一元运算、代数常数
- 二元运算性质和特异元素：交换律、结合律、幂等律、分配律、吸收律、单位元、零元、可逆元和逆元
- 同类型的与同种的代数系统、积代数
- 半群、独异点与群、环与域、格与布尔代数的定义
- 代数系统的同态与同构

基本要求

- 判断给定集合和运算能否构成代数系统
- 判断给定二元运算的性质
- 求二元运算的特异元素
- 计算积代数
- 判断或证明给定集合和运算是否构成半群、独异点、群、环、域、格、布尔代数
- 判断函数是否为同态映射和同构映射

练习1

1．设∘运算为Q上的二元运算，

$$\forall x, y\in Q,\ \ x\circ y = x+y+2xy,$$

(1) 判断∘运算是否满足交换律和结合律，并说明理由.

(2) 求出∘运算的单位元、零元和所有可逆元素的逆元.

(1) ∘ 运算可交换，可结合.

任取 $x, y\in Q$,

$$x\circ y = x+y+2xy = y+x+2yx = y\circ x,$$

任取 $x, y, z\in Q$,

$$(x\circ y)\circ z = (x+y+2xy)+z+2(x+y+2xy)z$$

$$= x+y+z+2xy+2xz+2yz+4xyz$$

$$x\circ(y\circ z) = x+(y+z+2yz)+2x(y+z+2yz$$

$$= x+y+z+2xy+2xz+2yz+4xyz$$

解答

(2) 设∘运算的单位元和零元分别为 e 和 θ，则对于任意 x 有 $x \circ e = x$ 成立，即

$$x+e+2xe = x \Rightarrow e = 0$$

由于∘运算可交换，所以 0 是幺元.

对于任意 x 有$x \circ \theta = \theta$成立，即

$$x+\theta+2x\theta=\theta \Rightarrow x+2x\theta = 0 \Rightarrow \theta = -1/2$$

给定 x，设 x 的逆元为 y, 则有 $x \circ y = 0$ 成立，即

$$x+y+2xy = 0 \Rightarrow y = -\frac{x}{1+2x} \quad (x \neq -1/2)$$

因此当$x \neq -1/2$时，$-\frac{x}{1+2x}$ 是x的逆元.

练习2

2. 下面是三个运算表

(1) 说明那些运算是可交换的、可结合的、幂等的.

(2) 求出每个运算的单位元、零元、所有可逆元素的逆元

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

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

$\cdot$	a	b	c
a	a	b	c
b	b	c	c
c	c	c	c

解答

(1) * 满足交换律，满足结合律，不满足幂等律.

∘ 不满足交换律，满足结合律，满足幂等律.

• 满足交换律，满足结合律，不满足幂等律.

(2) * 的单位元为b，没有零元， $a^{-1}=c$, $b^{-1}=b$,$c^{-1}=a$

∘ 的单位元和零元都不存在，没有可逆元素.

• 的单位元为 a，零元为c，$a^{-1}=a$，b, c不是可逆元素.

说明：关于结合律的判断

需要针对运算元素的每种选择进行验证，若$|A|=n$， 一般需要验证n^3个等式.

单位元和零元不必参与验证.

通过对具体运算性质的分析也可能简化验证的复杂性.

练习3

3. 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，$G = \{a^n \mid n \in Z\}$, 运算是普通乘法.

(2) Q^+是正有理数集，运算为普通加法.

(3) 一元实系数多项式的集合关于多项式加法.

解

(1) 是半群、独异点和群

(2) 是半群但不是独异点和群

(3) 是半群、独异点和群

方法：根据定义验证，注意运算的封闭性

练习4

4. 判断下列集合和给定运算是否构成环和域, 如果不构成, 说明理由.

(1) $A = \{ a+bi \mid a,b\in Q \}$, 其中$i^2= -1$, 运算为复数加法和乘法.

(2) $A=\{ 2z+1 \mid z\in Z\}$, 运算为实数加法和乘法

(3) $A=\{ 2z \mid z\in Z\}$, 运算为实数加法和乘法

(4) $A=\{ x \mid x\geq 0\wedge x\in Z\}$, 运算为实数加法和乘法.

(5) $A=\{a+b\sqrt[4]{5} \mid a,b\in Q\}$, 运算为实数加法和乘法

解 (1) 是环, 也是域.

(2) 不是环, 因为关于加法不封闭.

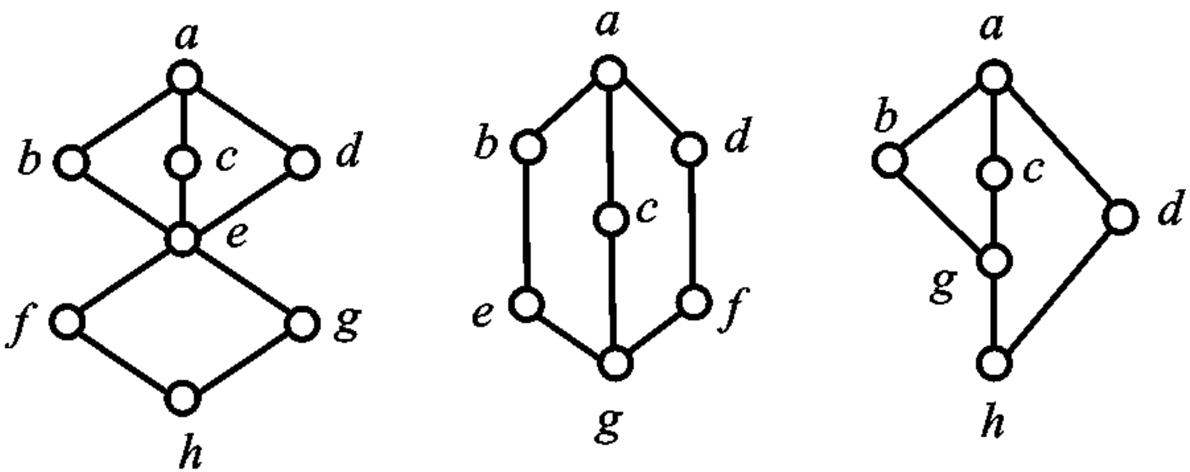
(3) 是环, 但不是域, 因为乘法没有幺元.

(4) 不是环, 因为正整数关于加法的负元不存在.

(5) 不是环, 因为关于乘法不封闭.

练习5

5．判别下述格L是否为分配格.



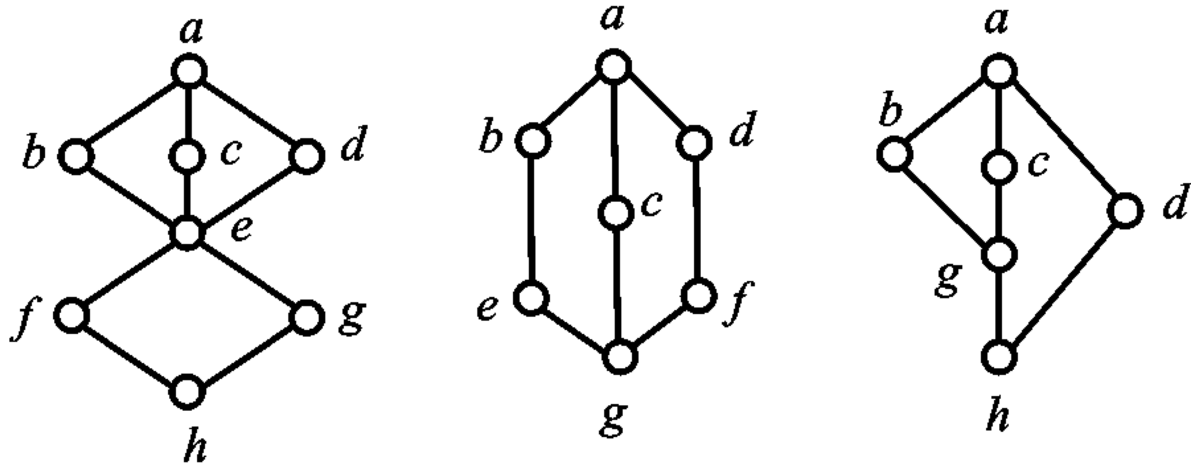
L_1　　L_2　　L_3

L_1不是分配格, 因为它含有与钻石格同构的子格.

L_2和L_3不是分配格, 因为它们含有与五角格同构的子格.

练习6

6．针对下图，求出每个格的补元并说明它们是否为有补格



L_1　　L_2　　L_3

L_1中, a与h互为补元, 其他元素没补元.

L_2中, a与g互为补元. b的补元为c, d, f；c的补元为b, d, e, f；d的补元为b, c, e；e的补元为c, d, f；f的补元为b, c, e.

L_3中, a与h互为补元, b的补元为d；c的补元为d；d的补元为b, c, g；g的补元为d. L_2与L_3是有补格.

练习7

7．对于以下各题给定的集合和运算判断它们是哪一类代数系统（半群、独异点、群、环、域、格、布尔代数），并说明理由.

(1) $S_1 = \{1, 1/2, 2, 1/3, 3, 1/4, 4\}$, $*$为普通乘法.

(2) $S_2 = \{a_1, a_2, ..., a_n\}$, $\forall a_i, a_j \in S_2$, $a_i \circ a_j = a_i$, 这里的 n 为给定正整数, $n>1$.

(3) $S_3 = \{0, 1\}$,$*$为普通乘法.

(4) $S_4 = \{1, 2, 3, 6\}$, $\forall x,y \in S4$, $x \circ y$与$x * y$分别表示 x 与 y 的最小公倍数和最大公约数.

(5) $S_5 = \{0, 1\}$, $*$为模2加法, $\circ$为模2乘法.

解答

(1) 不是代数系统, 因为乘法不封闭, 例如4*4=16.

(2) 是半群但不是独异点, 因为*运算满足结合律, 但是没有单位元.

(3) 是独异点但不是群. 因为*运算满足结合律, 单位元是1, 可是0没有乘法逆元.

(4) 是格, 也是布尔代数. 因为这两个运算满足交换律和分配律；求最小公倍数运算的单位元是1, 求最大公约数运算的单位元是6, 满足同一律；两个运算满足补元律.

(5) 是域. 对于模 n 的环Z_n, 当n为素数时构成域.

练习8

8. 设G为非0实数集R^*关于普通乘法构成的代数系统，判断下述函数是否为G的自同态？如果不是，说明理由. 如果是，判别它们是否为单同态、满同态、同构.

(1) $f(x) = |x| + 1$

(2) $f(x) = |x|$

(3) $f(x) = 0$

(4) $f(x) = 2$

解答

解 (1) 不是同态, 因为 $f(2\times2)=f(4)=5$, $f(2)\times f(2)=3\times3=9$

(2) 是同态，不是单同态，也不是满同态，因为 $f(1)= f(-1)$, 且 $\operatorname{ran} f$ 中没有负数.

(3) 不是G 的自同态，因为 f 不是 G 到 G 的函数

(4) 不是G 的自同态，因为 $f(2\times2)=2$, $f(2)\times f(2)=2\times2=4$

说明：判别或证明同态映射的方法

(1) 先判断（或证明）f 是G_1 到 G_2的映射 $f: G_1\to G_2$. 如果已知 $f: G_1\to G_2$，则这步判断可以省去.

(2) $\forall x, y \in G_1$, 验证 $f(xy) = f(x)\,f(y)$

(3) 判断同态性质只需判断函数的单射、满射、双射性即可.