第9-11章 代数系统简介

- 二元运算及其性质
- 代数系统及其子代数和积代数
  - 代数系统
  - 子代数
  - 积代数
- 代数系统的同态与同构
- 典型的代数系统(半群、独异点、群、环、域)

代数结构

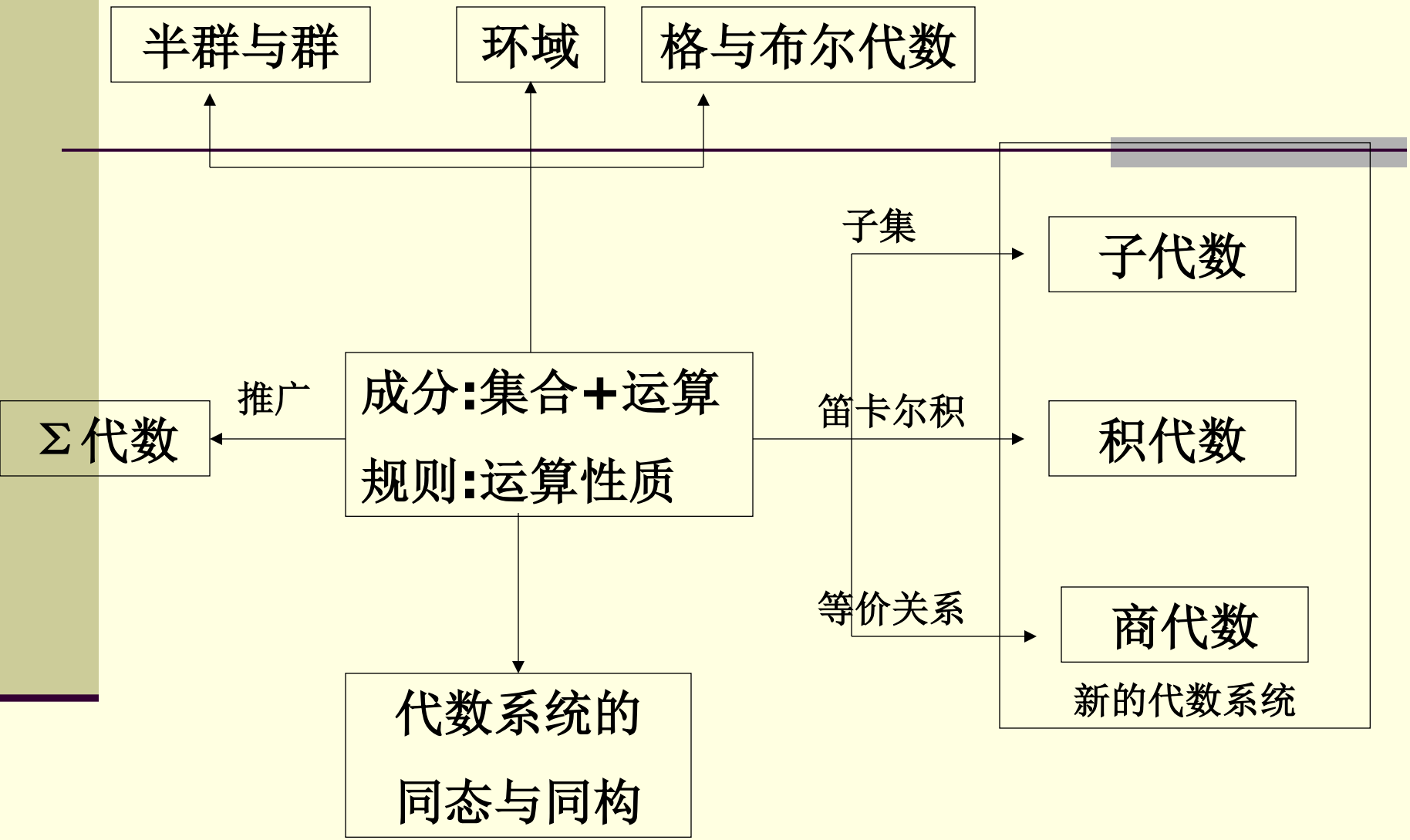
- 发展
- 主要人物：伽罗瓦Galois

埃瓦里斯特 伽罗瓦

（Évariste Galois,1811.10—1832.5）

- 群论的创始人。出生于巴黎，中学时代发表有关循环连分数的论文并向法国科学院提出方程论方面的论文。因参加政治运动，受退学处分，入狱，释放后不久因纠纷而卷入一场决斗，1832年死于决斗中，未满21岁。伽罗瓦最主要的成就是提出了群的概念，用群论彻底的解决了代数方程的可解性问题。人们把用群论方法研究代数方程根式解的理论称之为伽罗瓦理论，这一理论导致了抽象代数的兴起。

- 代数系统的构成
  - 成分：载体（集合）、运算
  - 规则：公理（运算性质）
- 由已知代数系统构造新的代数系统的方法
  - 子代数、积代数、商代数
- 代数系统之间的关系
  - 同态与同构
- 基本代数系统的推广--∑代数



9.1 二元运算及其性质

- 二元运算定义及其实例
- 一元运算定义及其实例
- 运算的表示
- 二元运算的性质
  - 交换律、结合律、幂等律、消去律
  - 分配律、吸收律
- 二元运算的特异元素
  - 单位元、零元、可逆元素及其逆元

二元运算的定义及其实例

定义 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. 也称 S 对 f 封闭.

例1 （1）N上的二元运算：加法、乘法.

（2） Z上的二元运算：加法、减法、乘法.

（3）非零实数集 R^*上的二元运算: 乘法、除法.

（4）设 $S=\{a_1, a_2, \dots, a_n\}$, $a_i \circ a_j = a_i$, $\circ$为S上二元运算.

（5） 设$M_n(R)$表示所有n 阶$(n\geq 2)$实矩阵的集合，即

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

矩阵加法和乘法都是$M_n(R)$上的二元运算.

（6）幂集 $P(S)$上的二元运算： $\cup$、$\cap$、$-$、$\oplus$.

（7）S^S为S上的所有函数的集合：合成运算$\circ$.

一元运算的定义与实例

定义 设S为集合，函数 f：$S\to S$ 称为S上的一元运算，简称为一元运算.

例2（1）Z, Q 和 R上的一元运算: 求相反数

（2）非零有理数集Q^*，非零实数集 R^*上的一元运算 : 求倒数

（3）复数集合C上的一元运算: 求共轭复数

（4）幂集$P(S)$上, 全集为S: 求绝对补运算~

（5）A 为S上所有双射函数的集合，$A\subseteq S^S$: 求反函数

（6）在 $M_n(R)$ $(n\geq 2)$上，求转置矩阵

二元与一元运算的表示

算符：

o, *, ·, ⊕, ⊗ 等符号

表示二元或一元运算

对二元运算 o，如果 x 与 y 运算得到 z，记做 $xoy=z$；

对一元运算 o，x 的运算结果记作 ox

表示二元或一元运算的方法：

公式、 运算表

注意：在同一个问题中不同的运算使用不同的算符

二元与一元运算的表示(续)

公式表示

例3 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（表示有穷集上的一元和二元运算）

二元运算的运算表

$\circ$	a_1	a_2	…	a_n
a_1	$a_1 \circ a_1$	$a_1 \circ a_2$	…	$a_1 \circ a_n$
a_2	$a_2 \circ a_1$	$a_2 \circ a_2$	…	$a_2 \circ a_n$
.		…		
.		…		
.		…		
a_n	$a_n \circ a_1$	$a_n \circ a_2$	…	$a_n \circ a_n$

一元运算的运算表

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

多少个可能的2元运算？

运算表的实例

例4 $A=P(\{a,b\})$,$\oplus$,~分别为对称差和绝对补运算（$\{a,b\}$为全集）

$\oplus$的运算表

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

~的运算表

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

运算表的实例（续）

例5 $Z_5 = \{0, 1, 2, 3, 4\}$, $\oplus, \otimes$ 分别为模 5 加法与乘法

⊕的运算表

⊕	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

⊗的运算表

⊗	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

n元运算的定义

- 定义2 设A为集合，函数$f:A^n \to A$称为A上的**n元运算**
  - **n=0, 0元运算， $f:\to A$**
  - **n=1, 一元运算，$f:A\to A$**
    - 整数集Z,有理数集Q，实数集R: 相反数
    - 集合B：绝对补运算
- **封闭性:** 任何A中元素都可参与运算、运算结果属于A

二元运算的性质

- 涉及一个二元运算的算律
  - 交换
  - 结合——广义结合
  - 幂等
  - 消去
- 涉及二个不同的二元运算的算律
  - 分配---广义分配
  - 吸收（以交换为前提）

二元运算的性质

定义 设 o 为 S 上的二元运算,

（1）如果对于任意的 $x, y \in S$ 有

$$x \circ y = y \circ x,$$

则称运算在 S 上满足交换律.

（2）如果对于任意的 $x, y, z \in S$ 有

$$(x \circ y) \circ z = x \circ (y \circ z),$$

则称运算在 S 上满足结合律.

（3）如果对于任意的 $x \in S$ 有

$$x \circ x = x,$$

则称运算在 S 上满足幂等律.

实例分析

例6　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A上A，$|A|\geq 2$.

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

二元运算的性质（续）

定义 设 $\circ$ 和 $*$ 为 S 上两个不同的二元运算,

（1）如果对于任意的 $x, y, z \in S$ 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）如果 $\circ$ 和 $*$ 都可交换, 并且对于任意的 $x, y \in S$ 有

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

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

则称 $\circ$ 和 $*$ 运算满足吸收律.

实例分析

例7　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A上A，$|A|\geq 2$.

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

二元运算的特异元素

单位元

定义　设 o 为S上的二元运算，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 o 运算的左 (或右) 单位元.

若 $e \in S$ 关于 o 运算既是左单位元又是右单位元，则称 e 为 S 上关于 o 运算的单位元.

单位元也叫做幺元.

二元运算的特异元素（续）

零元

设 o 为 S 上的二元运算, 如果存在θ_l（或θ_r）$\in S$，使得对任意 $x \in S$ 都有

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

则称θ_l(或θ_r)是 S 中关于 o 运算的 左 (或右) 零元.

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

二元运算的特异元素（续）

可逆元素及其逆元

令 e 为 S 中关于运算 o 的单位元. 对于 $x \in S$，如果存在 y_l（或 y_r）$\in S$ 使得

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

则称 y_l (或 y_r)是 x 的左逆元 (或右逆元).

关于 o 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.

实例分析

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

特异元素的性质

- 单位元以及零元的唯一性定理
- 如果$|A|>1$，$e \neq \theta$
- 逆元的唯一性定理——x的逆元标记为x^{-1}.

单位元唯一性定理

定理15.2 对于给定集合A和A上的二元运算o，如果存在$e_l \in A$和$e_r \in A$使得$\forall x \in A$满足$e_l \circ x = x \circ e_r = x$，则$e_l = e_r = e$，且e就是A中关于o运算的唯一的单位元.

证： $e_l = e_l \circ e_r = e_r$，令 $e_l = e_r = e$，则e为单位元.假设e'也为单位元，则

$e' = e' \circ e = e$

#

零元唯一性定理

定理15.3 对于给定集合A和A上的二元运算o，如果存在$\theta_l \in A$和$\theta_r \in A$使得$\forall x \in A$满足$\theta_l \circ x = \theta_l$，$x \circ \theta_r = \theta_r$，则$\theta_l = \theta_r = \theta$，且$\theta$就是A中关于o运算的唯一的零元.

#

逆元的唯一性定理

定理15.5　对于集合A和A上可结合的二元运算o，如果对于A中元素x，存在元素y_l和y_r使得$y_l$ox=xoy_r=e，则y_l=y_r=y，且y是x的唯一的逆元.

- 证　y_l=$y_l$oe= y_lo(xoy_r)=($y_l$ox)oy_r = eoy_r=y_r

令y_l=y_r=y，y是x的逆元.

假设y'也是x的逆元，则

y'=y'oe =y'o(xoy)=(y'ox)oy=eoy=y

#

消去律定义及实例

- 定义：设A为集合，o为A上二元运算，

消去律　$\forall a,b,c \in A$,

$aob = aoc \wedge a \neq \theta \Rightarrow b = c$

$boa = coa \wedge a \neq \theta \Rightarrow b = c$

- 实例：
  - Z,Q,R，+，×满足消去律
  - Mn(R), 矩阵+满足消去律，矩阵×不满足消去律
  - P(B), $\oplus$满足消去律，$\cup$、$\cap$一般不满足消去律
  - A^A, o 不满足消去律

例题

- **例1 设A为实数集，$\forall x,y\in A$，$xoy = x+y-2xy$，**
- **(1) 说明o运算是否具有交换、结合、幂等、消去律**
- **(2) 求单位元、零元、幂等元和所有可逆元素的逆元**
- **解: (1) 容易验证交换律、结合律、消去律成立.**
- **$(xoy)\,oz=(x+y-2xy)\,oz = x+y-2xy+z-2(x+y-2xy)z$**
  $=x+y+z-2xy-2xz-2yz+4xyz$
- **$xo(y\,oz)=xo(y+z-2yz)=x+(y+z-2yz)-2x(y+z-2yz)$**
  $= x+y+z-2xy-2xz-2yz+4xyz$

- **$1o1 = 1+1-2 \neq 1$，幂等律不成立**
- 消去律在等到零元之后进行判断

- 例1 设A为实数集，$\forall x,y\in A$，$xoy = x+y-2xy$，
- (2) 求单位元、零元、幂等元和所有可逆元素的逆元
- (2) 设单位元、零元分别为e、θ, 则$\forall x\in A$

  $x+e-2xe = xoe = x \Rightarrow e(1-2x) = 0 \Rightarrow e = 0$

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

  幂等元为x，则

  $x+x-2x^2 = x \Rightarrow x(1-2x) = 0 \Rightarrow x = 0$ 或 $x = 1/2$

  设x的逆元为y，则当$x\neq 1/2$ 有

  $x+y-2xy = xoy = e = 0 \Rightarrow (2x-1)y = x \Rightarrow y = x/(2x-1)$
- 结论：$e = 0, \theta = 1/2$, 幂等元为0和1/2，$x^{-1} = 1/(2x-1)$ $(x \neq 1/2)$

例题（续）

- 例2 (1) 说明下面给定运算是否满足交换,结合,幂等,消去律
- (2) 求每个运算的单位元,零元,幂等元,所有可逆元素的逆元

∘	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

□	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

•	a	b	c
a	a	b	c
b	b	a	c
c	c	c	c

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

1）交换律；幂等律；

2）单位元：零元

3）消去律；

4）结合律：(xoy)oz= xo(yoz)

例题（续）

- 例2 (1) 说明下面给定运算是否满足交换,结合,幂等,消去律
- (2) 求每个运算的单位元,零元,幂等元,所有可逆元素的逆元

∘	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

□	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

•	a	b	c
a	a	b	c
b	b	a	c
c	c	c	c

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

交换, 结合, 消去幺元e=a

幂等元：a

- 逆元：$a^{-1}=a$
- $b^{-1}=c$, $c^{-1}=b$

结合, 幂等

幂等元：a, b, c

交换, 结合, 消去幺元e=a，零元θ=c，

幂等元：a, c

逆元：$a^{-1}=a$

$b^{-1}=b$

交换, 结合幺元e=a

幂等元：a, b

逆元；$a^{-1}=a$

作业

- 习题九：4，10

代数系统定义

定义　非空集合 S 和 S 上 k 个一元或二元运算 f_1, f_2, …, f_k 组成的系统称为一个代数系统, 简称代数，记作$<S, f_1, f_2, \ldots, f_k>$.

实例：

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

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

$<Z_n,\oplus,\otimes>$是代数系统，$Z_n=\{0,1,\ldots,n-1\}$，⊕和⊗分别表示模 n 的加法和乘法，对于$x, y\in Z_n$,

$x\oplus y=(x+y) \bmod n$，$x\otimes y=(xy) \bmod n$

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

同类型与同种代数系统

定义 （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1 $V_1 = \langle R, +, \cdot; 0, 1 \rangle$,

$V_2 = \langle M_n(R), +, \cdot; \theta, E \rangle$,

θ 为 n 阶全 0 矩阵，E 为 n 阶单位矩阵

$V_3 = \langle P(B), \cup, \cap, \varnothing, B \rangle$

同类型与同种代数系统（续）

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 · 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

V_1, V_2, V_3是同类型的代数系统
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

子代数 (Algebraic Subsystem)

定义 1 设 $V=\langle A, o_1, o_2, \cdots, o_r\rangle$是代数系统，B 是 A 的非空子集.

若 B 对于 V 中的所有运算封闭（含 0 元运算在内），则称 $V'=\langle B, o_1, o_2, \cdots, o_r\rangle$为 V 的子代数(Subalgebra)，若 $B\subset A$, 子代数 V’ 称为 V 的真子代数(real subalgebra).

平凡子代数：V 是 V 的平凡子代数.

说明：如果公理是二元运算的性质，子代数与原有代数系统是同种的；子代数一定存在（至少存在平凡子代数）

实例：

V=<Z,+,0>,

- **例(1) 公理： +满足结合律，单位元存在，每个元素可逆**
  - **子代数为：nZ={nk|k∈Z}, n∈N,**
  - **n=0 平凡的真子代数**
  - **n=1 平凡子代数**
  - **n>1 非平凡的真子代数**
- **例(2) 公理：+ 结合律**
  - **子代数为：nZ（n∈N）， N, Z^+等.**

子代数与原代数系统的公理有关.

积代数(Product Algebra)

定义 2 设 $V_1=<A,o_{11},o_{12},\ldots,o_{1r}>$与 $V_2=<B,o_{21},o_{22},\ldots,o_{2r}>$是同类型的代数系统，对于 $i=1,2,\ldots,r$, o_{1i} 和 o_{2i} 是 k_i 元运算，V_1 与 V_2 的积代数是

$$V_1\times V_2=<A\times B, o_1,o_2, \ldots, o_r>$$

其中 o_i 是 k_i 元运算，$i=1,2,\ldots,r$,

对于任意的$<x_1,y_1>,<x_2,y_2>,\ldots,<x_{k_i},y_{k_i}>\in A\times B$,

$$o_i(<x_1,y_1>,<x_2,y_2>,\ldots,<x_{k_i},y_{k_i}>)$$

$$=<o_{1i}(x_1,x_2,\ldots,x_{k_i}),o_{2i}(y_1,y_2,\ldots,y_{k_i})>$$

V 是 V_1 与 V_2 的积代数，也称 V_1 和 V_2 是 V 的因子代数.

例15.15

- 例：$V_1=<R,+,.>,V_2=<M_2(R),+,.>,$

则$V_1 \times V_2=<R \times M_2(R),\oplus,\otimes>$

求：

积代数的性质

- 积代数能够保持因子代数的如下性质：
  - 算律：交换律、结合律、幂等律、分配律、吸收律
  - 特异元素：单位元、零元、幂等元、可逆元素及其逆元
  - 消去律不一定能够保持，
- 反例：$V_1=\langle Z_2, \otimes\rangle, V_2=\langle Z_3, \otimes\rangle$

消去律不一定保持

- $V_1=<Z_2,\otimes>$, $V_2=<Z_3,\otimes>$,V_1和V_2的积代数为$V_1 \otimes V_2$，
- 其中

$<0,1> \otimes <1,0> = <0,1> \otimes <0,0>$,

但$<1,0>$不等于$<0,0>$

积代数说明

- 积代数与因子代数是同类型的
  - 系统公理不含消去律，积代数与因子代数是同种的；
  - 系统公理含消去律，不保证积代数与因子代数是同种的.
- 积代数可以推广到有限多个同类型的代数系统
- 直积分解是研究代数结构的有效手段
- 笛卡尔积是构造同种离散结构的有效手段

代数系统的同态与同构

有各种各样的代数系统，但是，有些代数系统表面上看不同，实际它们运算的性质相似、或完全一样。这就是代数系统间的同态、同构问题。

例　$<R^+, \times>$：是正实数R^+上的乘法$\times$；

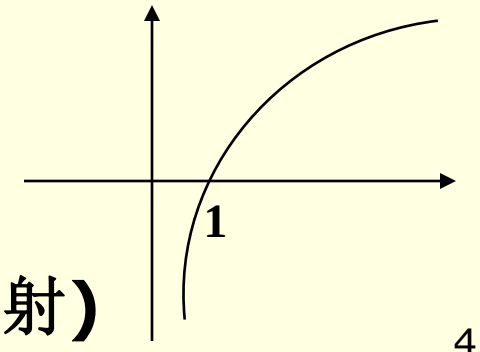
$<R, +>$ ： 是实数R上的加法$+$。

表面上看这两个代数系统完全不同，实际它们运算的性质却完全一样，都满足：可交换、可结合、有幺元、每个元素可逆。

那么如何反映它们间的相同性呢？

通过一个映射　$f: R^+ \to R$

任何$x \in R^+$，$f(x)=\lg x$　　(是双射)



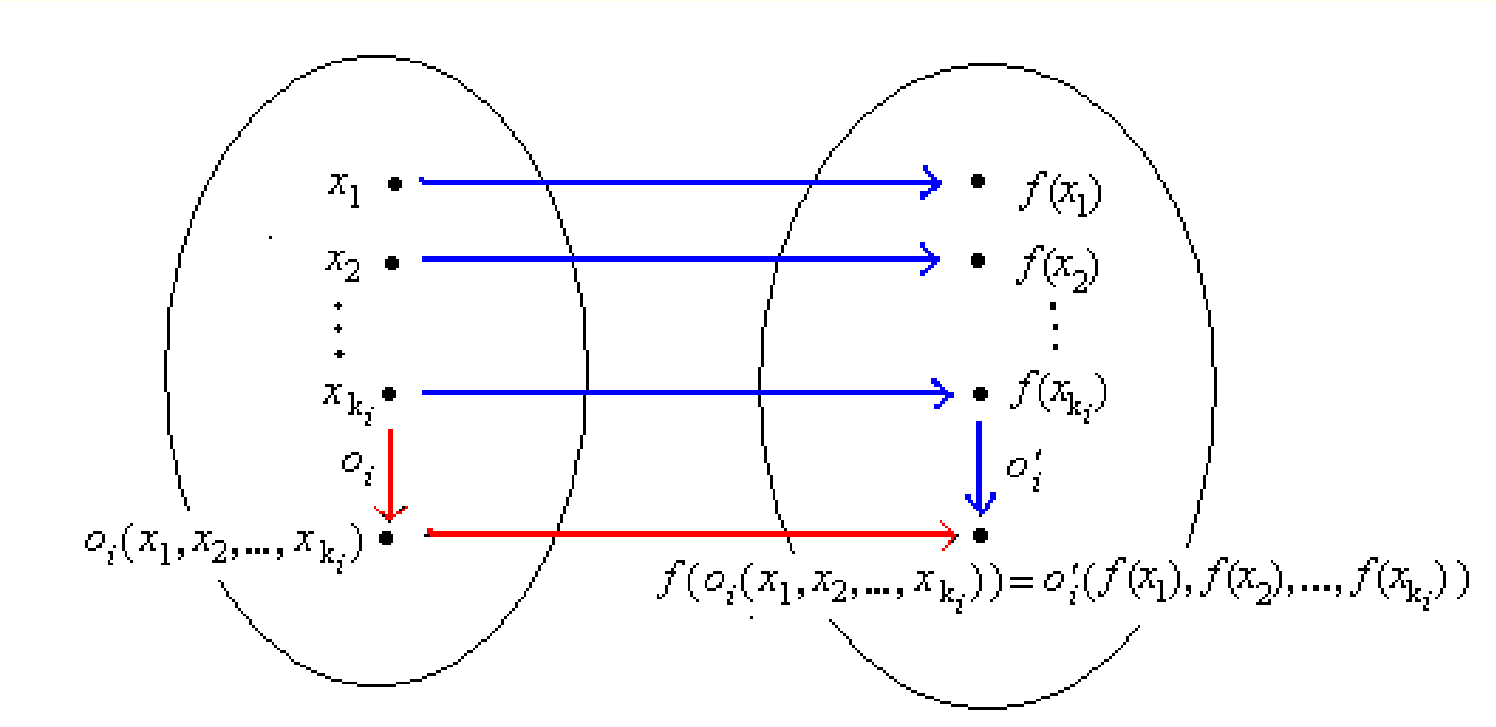
同态映射的定义(Homophormism)

定义 1 设 $V_1 =< A, o_1, o_2, ..., o_r >$ 与 $V_2 =< B, o_1', o_2', ..., o_r' >$ 是同类型的代数系统，对于 i=1,2,...,r， o_i 为 k_i 元运算，函数 $f:A \to B$，如果对于所有的运算 o_i 与 o_i'

$$f(o_i(x_1, x_2, ..., x_{k_i})) = o_i'(f(x_1), f(x_2), ..., f(x_{k_i})) \quad \forall x_1, x_2, ..., x_{k_i} \in A$$

则称 f 是代数系统 V_1 到 V_2 的同态映射，简称同态。

$$f(o_i(x_1, x_2, \ldots, x_{k_i})) = o_i'(f(x_1), f(x_2), \ldots, f(x_{k_i})) \quad \forall x_1, x_2, \ldots, x_{k_i} \in A$$



同态映射的定义（续）

(1) 对于二元运算、一元运算、0 元运算采用下述表示：

$$f(x \circ y) = f(x) \circ' f(y)$$

$$f(\Delta x) = \Delta' f(x)$$

$$f(a) = a'$$

(2) 同态映射必须对所有的运算保持等式，包括 0 元运算在内

例如

$$V = < A, \cdot, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} >, \quad A = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in R \right\}$$

$$f : A \to A, \quad f\left(\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\right) = \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$$

则 f 不是 V 的自同态，因为 $f\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) \neq \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$，不保持 0 元运算

例15.18

设$V_1 = \langle Z, + \rangle$, $V_2 = \langle Z_n, \oplus \rangle$, $Z_n = \{0, 1, \ldots, n-1\}$, $\oplus$为模n加法，
定义$f: Z \to Z_n$, $f(x) = (x) \bmod n$,则f为V_1到V_2的同态

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

？ =

$f(x) \oplus f(y) = (x \bmod n) \oplus (y \bmod n)$

9.2典型的代数系统

定义 设 $V=<S, \circ>$ 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. 若半群含有单位元e，则称为独异点，若独异点中每个元素x都有逆元，则称为群。

实例

(1) $<Z^+,+>,<N,+>,<Z,+>,<Q,+>,<R,+>$都是半群，+是普通加法. 除$Z^+$外都是独异点，Z, Q, R构成群。

(2) 设 n 是大于1的正整数，$<M_n(R),+>$和$<M_n(R), \cdot>$都是半群，其中+和 ·分别表示矩阵加法和矩阵乘法. ＋法构成群.

(3) $<P(B),\oplus>$为群，其中⊕为集合的对称差运算.

(4) $<Z_n, \oplus>$为群，其中 $Z_n=\{0,1, \ldots, n-1\}$，⊕为模 n 加法

(5) $<A^A, \circ>$为独异点，其中 $\circ$ 为函数的复合运算.

半群与独异点的幂运算

幂运算的定义：

半群	独异点
$a^1 = a$	$a^0 = e$
$a^{n+1} = a^n a$	$a^{n+1} = a^n a$

性质：(1) 幂运算的等式

$$a^n a^m = a^{n+m}$$

$$(a^n)^m = a^{nm}$$

(2) 结合律

实例

例 1 V 为半群，任取 $a,b\in S$，如果 $a\neq b$，则有 $ab\neq ba$，证明

（1） V 中成立幂等律

（2） $\forall a,b\in V,\ aba = a$

（3） $\forall a,b,c\in V,\ abc = ac$

实例

例 1 V 为半群，任取 $a,b\in S$, 如果 $a\neq b$, 则有 $ab\neq ba$，

证明

（1） V 中成立幂等律

（2） $\forall a,b\in V,\ aba = a$

（3） $\forall a,b,c\in V,\ abc = ac$

证 （1）假若 $aa \neq a$, 则

$(aa)a \neq a(aa) \Rightarrow aaa \neq aaa$，矛盾

（2）假若 $aba \neq a$, 则

$(aba)a \neq a(aba) \Rightarrow aba \neq aba$ ，矛盾

（3） 假若 $abc \neq ac$, 则

$(abc)(ac) \neq (ac)(abc) \Rightarrow abcac \neq acabc$

$\Rightarrow ab(cac) \neq (aca)bc \Rightarrow abc \neq abc$ ，矛盾

Klein四元群

设 $G = \{ e, a, b, c \}$，G上的运算由下表给出，

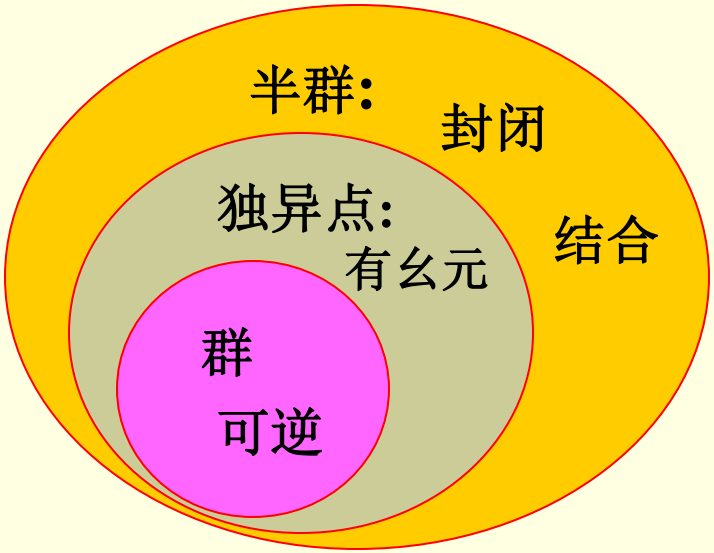
称为 **Klein四元群**

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

运算表特征：

- 对称性---运算可交换
- 主对角线元素都是幺元
  ---每个元素是自己的逆元
- a, b, c 中任两个元素运算都等于第三个元素.

群 Group



群中的术语

定义

(1) 若群 G 是有穷集，则称G是有限群，否则为无限群.
群 G 中的元素个数称为群G的 阶，有限群 G 的阶记作$|G|$.

(2) 若群G中的二元运算是可交换的，则称G为交换群或 阿贝尔(Abel)群.

实例：

$<Z,+>$ 和 $<R,+>$是无限群

$<Z_n,\oplus>$是有限群，也是 n 阶群

Klein四元群是 4 阶群

上述群都是交换群

n 阶 ($n\geq 2$) 实可逆矩阵集合关于矩阵乘法构成的群是非交换群.

子群

定义 设 G 是群，H 是 G 的非空子集，如果 H 关于 G 中的运算构成群，则称 H 是 G 的子群, 记作 $H \leq G$.
若 H 是 G 的子群，且 $H \subset G$，则称 H 是 G 的真子群，记作 $H < G$.

实例
nZ（n是自然数）是整数加群 $<Z,+>$ 的子群.
当 $n \neq 1$ 时, nZ 是 Z 的真子群.

对任何群 G 都存在子群. G 和$\{e\}$都是 G 的子群，称为G的平凡子群.

n元置换群

A上的n元置换：|A|=n时A上的一一变换表示法

置换的表示法：令A={1,2,…,n},

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

A上的所有置换和所有排列之间一一对应，n元集有n!个排列，所以有n!个n元置换，所有这些置换的集合记作S_n，S_n关于置换的乘法构成一个群，称为n元对称群，S_n的子群称为n元置换群。

例

- $S_3=\{\sigma_1, \sigma_2,\ldots, \sigma_6\}$,其中

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

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

n元置换的表示

- 轮换表示：若σ将{1,2,…,n}中的k个元素$i_1,i_2,\ldots,i_k$进行如下变换：

$\sigma(i_1)=i_2,\ \sigma(i_2)=i_3,\ldots,\ \sigma(i_k)=i_1$

并且保持其他的元素不变，则可将σ记为$(i_1 i_2 \ldots i_k)$称为一个**k阶轮换(cycle)**。

当k=1时$\sigma=(i_1), i_1 \in \{1,2,\ldots,n\}$是恒等置换

当k=2时$\sigma=(i_1\ i_2)$称为一个对换(Transposition)

- 不相交：设$\sigma_1=(i_1 i_2 \ldots i_k)$和$\sigma_2=(j_1 j_2 \ldots j_k)$是两个轮换，若$\{i_1,i_2,\ldots,i_k\}$和$\{j_1,j_2,\ldots j_k\}=\varnothing$,则称$\sigma_1$ 和σ_2是不相交的

举例

- 例:(1,2),(1,3),(1,2,3)都是(1,2,3)上的轮换，其中(1,2),(1,3)是对换，(123)是3阶轮换

- 例如σ_1 , $\sigma_2 \in S_5$, $\sigma_1=(1,3,4)$, $\sigma_2=(2,5)$, σ_1 和σ_2是不相交的

例17.20

- 设σ,τ∈S_8,写出σ和τ的不交轮换表示

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 5 & 8 & 1 & 4 & 6 & 7 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 2 & 3 & 8 & 7 & 6 & 1 & 4 \end{pmatrix}$$

σ=(1235)(4876)

τ=(157)(48)

注：当σ是恒等置换时,不可以省去σ中所有的1阶轮换，应该保留一个(i), i∈{1,2,...,n}

置换的乘法与求逆

置换的乘法：函数的合成

例如：8 元置换$\sigma=(132)(5648)$，$\tau=(18246573)$，则

$\tau\sigma=(15728)(3)(4)(6)=(15728)$

置换求逆：求反函数

$\sigma=(132)(5648)$，$\sigma^{-1}=(8465)(231)$,

令 S_n 为$\{1,2,\ldots,n\}$上所有 n 元置换的集合.

S_n 关于置换乘法构成群，称为 **n 元对称群.**

S_n 的子群称为 **n 元置换群.**

例　3 元对称群 $S_3=\{(1),(12),(13),(23),(123),(132)\}$

Polya定理

定理 设$N=\{1,2,\dots,n\}$,

令$G=\{\sigma_1,\sigma_2,\dots,\sigma_g\}$为$N$上置换群,

用m种颜色涂色N中的元素,

$c(\sigma_k)$是σ_k的轮换表示中轮换的个数,

则在G作用下不同的涂色方案数为

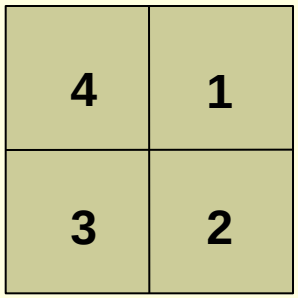
$$M=\frac{1}{|G|}\sum_{k=1}^{g}m^{c(\sigma_k)}$$

实例

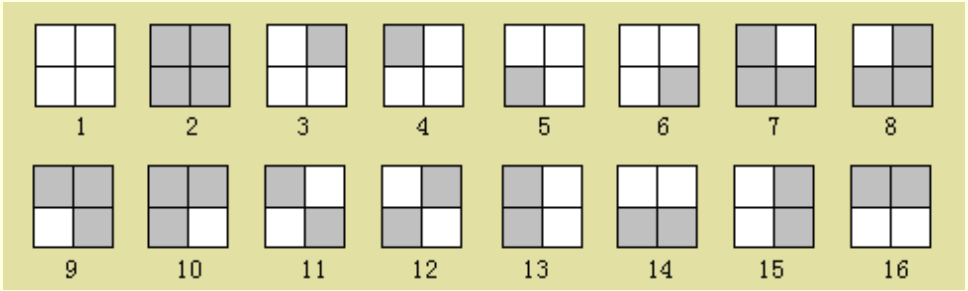
例2 用2色涂色2×2方格棋盘，每个方格一种颜色，只考虑旋转，求方案数

群$G = \{\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$

$\sigma_1 = (1)(2)(3)(4)$	旋转0度
$\sigma_2 = (1\ 2\ 3\ 4)$	旋转90度
$\sigma_3 = (1\ 3)(2\ 4)$	旋转180度
$\sigma_4 = (1\ 4\ 3\ 2)$	旋转270度



$M = (2^4 + 2^1 + 2^2 + 2^1)/4 = 6$



环的定义

定义 设$<R,+,\cdot>$是代数系统，$+$和$\cdot$是二元运算. 如果满足以下条件:

(1) $<R,+>$构成交换群

(2) $<R,\cdot>$构成半群

(3) $\cdot$运算关于$+$运算适合分配律

则称$<R,+,\cdot>$是一个环.

通常称$+$运算为环中的加法， $\cdot$运算为环中的乘法.

环中加法单位元记作0，乘法单位元（如果存在）记作1.

对任何元素x，称x的加法逆元为负元，记作$-x$.

若x存在乘法逆元的话，则称之为逆元，记作x^{-1}.

环的实例

例

(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.

(2) $n(n\geq 2)$阶实矩阵的集合$M_n(R)$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.

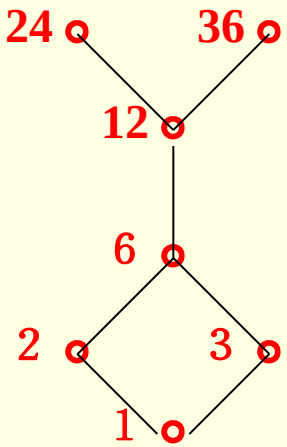
(4) 设$Z=\{0,1,...,n-1\}$，$\oplus$和$\otimes$分别表示模n的加法和乘法，则$<Zn,\oplus,\otimes>$构成环，称为模n的整数环.

格的定义和性质

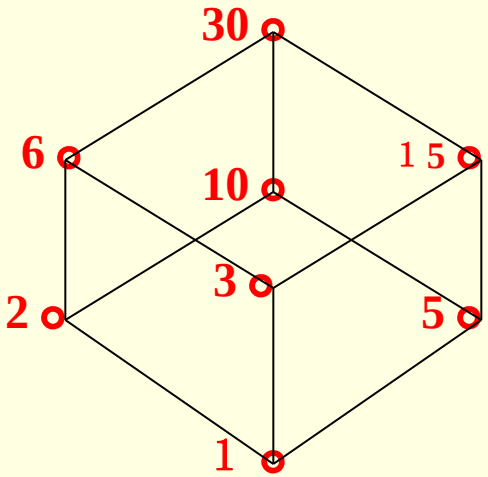
格的定义

<S,≤>是偏序集，如果任何a,b∈S,使得{a,b}都有最大下界和最小上界，则称<S,≤>是格。

右图的三个偏序集,哪个是格？



<A,≤>

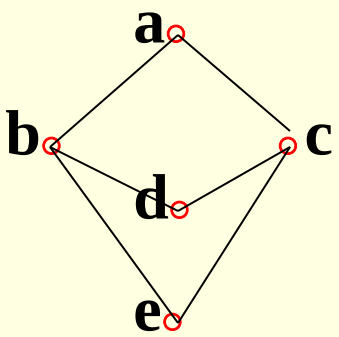


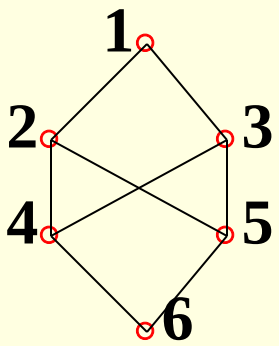
<B,≤>

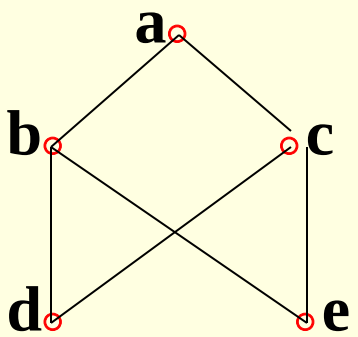
<C,≤>

<A,≤>不是格，因为{24,36}无最小上界。

<B,≤>和<C,≤>是格。再看下面三个偏序集，哪个是格？







这三个偏序集，都不是格，第一个与第三个是同构的。

因为 **d**和**e**无下界，也无最小上界；**b,c**虽有下界，但无最大下界。 第二个图：**2,3**无最大下界，**4,5**无最小上界。

格的代数定义

定理 设<S,*,o>是具有两个二元运算的代数系统，

若*和 o 运算满足交换、结合、吸收律，

则可以适当定义 S 上偏序≤，使得<S,≤>构成格，

且<S, ≤>导出的代数系统就是<S,*,o>.

$x \vee y = x \circ y,\ x \wedge y = x * y$

$x \vee y$, {x,y}的最小上界.

$x \wedge y$, {x,y}的最大下界.

格的偏序集定义

格中的运算∧,∨

格<L,≤>与导出的代数系统<L,∧,∨>的对应关系

格的实例：

P(B)是集合 B 的幂集，则 P(B)关于集合的包含关系构成一个格，称为 B 的幂集格

n 为正整数，An 为 n 的所有正因子的集合，则 An 关于整除关系构成格，n 的正因子格

G 为群，L(G)={H|H 是 G 的子群}，L(G)关于包含关系构成格，子群格