



第三部分 代数结构

北京理工大学 计算机学院
刘琼昕

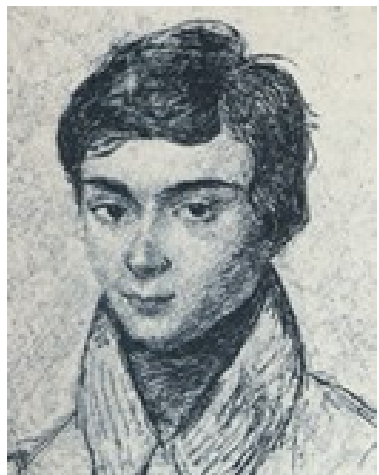
第三部分 代数结构

- 代数通常被认为是符号的操作，其发展分为两个历史阶段。
 - 古典代数（19世纪以前）：“每一个符号总是代表一个数”，以方程根的计算与分布为其研究中心。
 - 近世代数（19世纪以后）：“符号可以代表任何东西”，研究对象为各种代数系统。

第三部分 代数结构

- 近世代数起始于19世纪初，形成于20世纪30年代。
- 代表人物：
 - 法国数学家伽罗瓦 (E.Galois)
 - 挪威数学家阿贝尔 (N.H.Abel)
 - 英国数学家德·摩根(A.De.Morgan)
 - 英国数学家布尔(G.Boole).

“近世代数”的起源



近世代数创始人
伽罗瓦(法)
1811 ~ 1832

方程的根式的求解

- 一元一次方程 公元前1700年
- 一元二次方程 公元前几世纪 巴比伦人
- 一元三次方程

我国：在公元七世纪 一般的近似解法
唐朝数学家王孝通《缉古算经》

西方：16世纪 意大利数学家
卡丹公式《重要的艺术》

失败：Euler L、Lagrange J L、Gauss K F等。

伽罗瓦首先提出根的置换概念，每一个方程都可以与一个置换群联系，从而用群论方法彻底解决的方程根式解问题。

伽罗瓦证明五次方程的一般求根公式是不存在的。

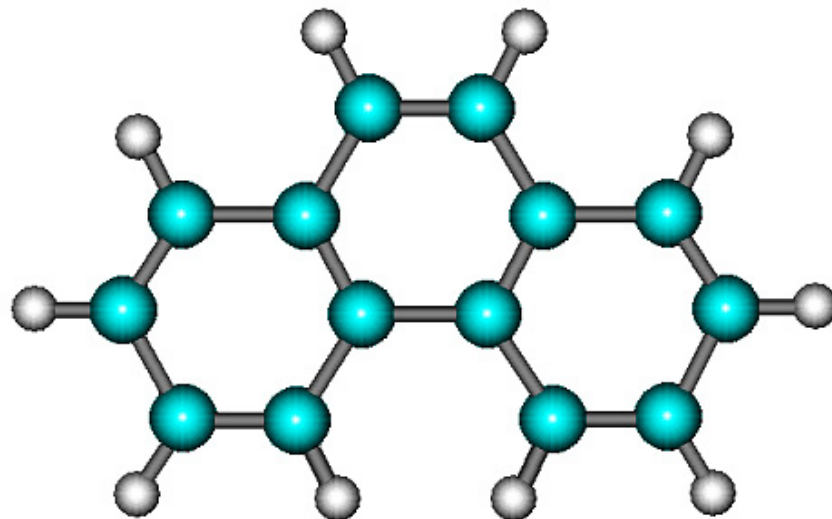
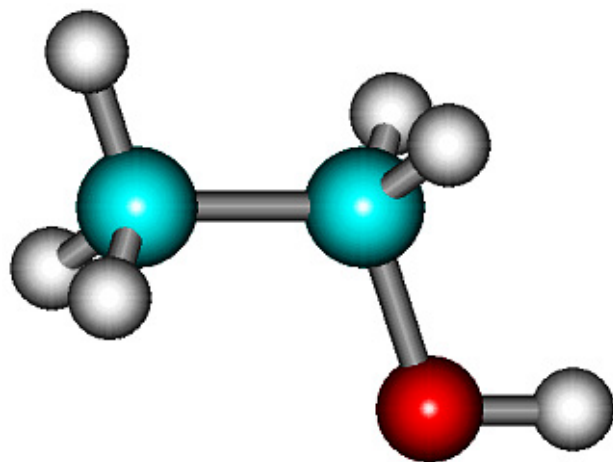
古希腊三大尺规作图问题

条件：用没有刻度的直尺和圆规作图。

- 三等分角：用直尺及圆规把任给的一角三等分。
- 倍立方：给定一立方体（即其一边已知），用直尺及圆规做另一立方体（即做其一边）使其体积为原立方体的两倍。
- 化圆为方：用直尺及圆规做一正多边形使其面积等于一给定圆的面积。

这三个题目被研究了两千多年，直到近世代数出现后才证明了：这三个作图题都是无解的。

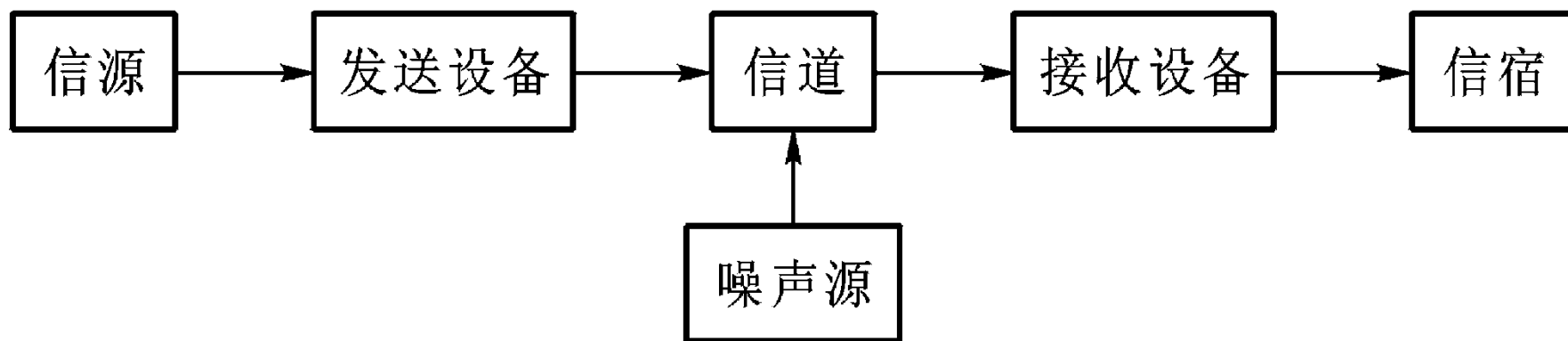
科学计数



19世纪后半叶，科学家发现：

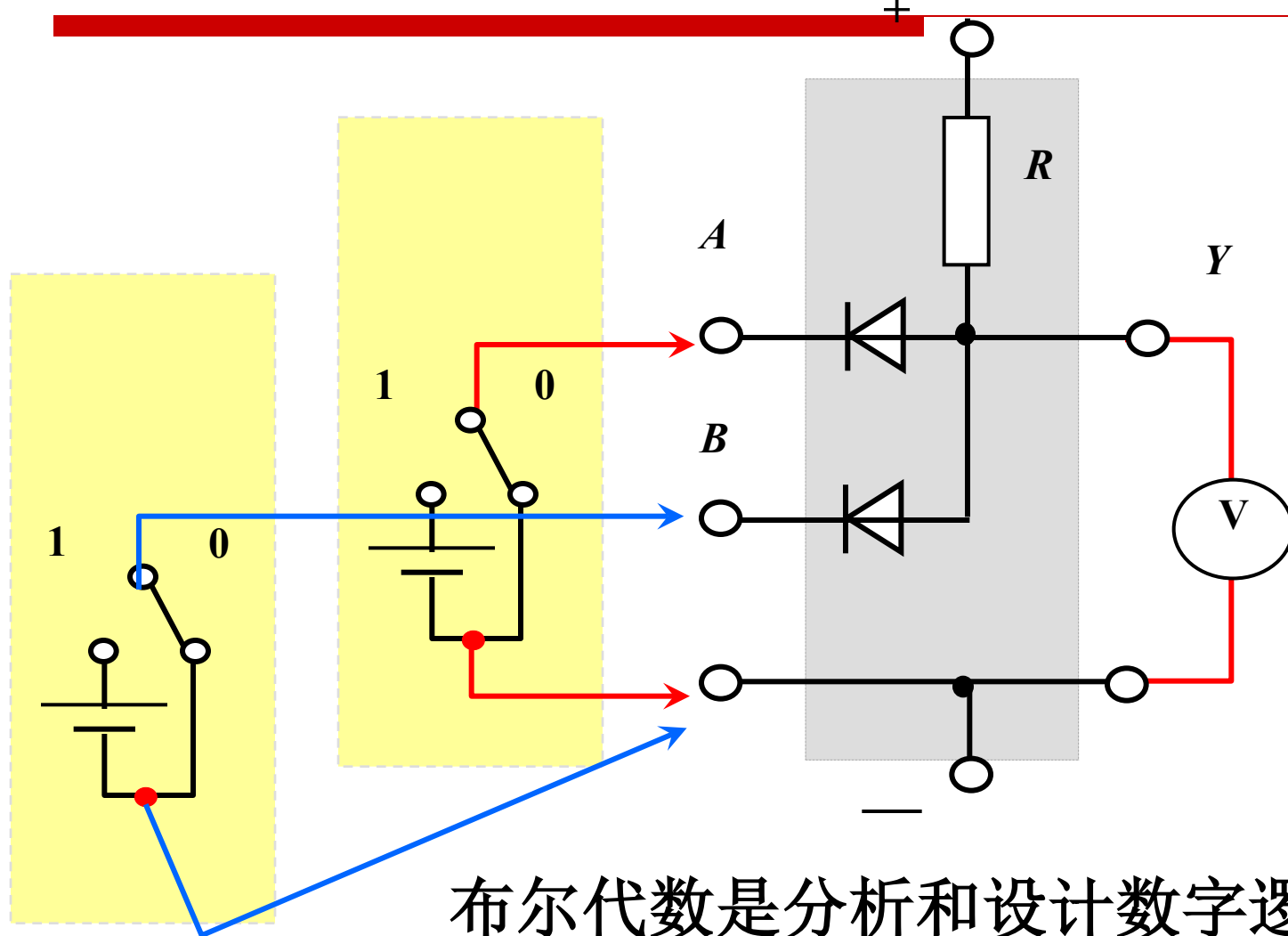
- ❑ 平面晶体对称群（壁纸群）：17种
- ❑ 对称点群：晶体外形的全部对称形式, 32种
- ❑ 空间群：晶体内部构造一切可能的对称形式, 230种。

数字通信的可靠性问题与保密问题



- ❑ 数字通信的可靠性问题：除了改进设备外，还可以采用高效的有检错和纠错能力的编码。利用近世代数方法可以得到更高效的检错码和纠错码。
- ❑ 数字通信的保密性问题：研究数字通信的加密与解密的方法与理论称为密码学，密码学的数学基础主要是数论和近世代数，涉及群、环、域的许多内容。

数字逻辑电路设计



布尔代数是分析和设计数字逻辑电路
的数学工具

主要的代数结构

- 群
- 环
- 域
- 格
- 布尔代数

第三部分 代数结构

□ 主要内容

- 代数系统----二元运算及其性质、代数系统
- 半群与群----半群、独异点、群
- 环与域----环、整环、域
- 格与布尔代数----格、布尔代数

第九章 代数系统

- 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

集合上的运算

□ 集合A上的运算

$\frac{1}{a}$	$(a \neq 0)$	a 的倒数	}	一元运算
$\lceil x \rceil$		大于等于 x 的最小整数		
$\lfloor x \rfloor$		小于等于 x 的最大整数		
$x + y$		$x \cdot y$		二元
$\text{if } x = 0 \text{ then } y \text{ else } z$				三元

9.1 二元运算及其性质

- **定义9.1** 设 S 为集合，函数 $f: S \times S \rightarrow S$ 称为 S 上的**二元运算**，简称为二元运算.
- S 中任何两个元素都可以进行运算，且运算的结果**惟一**.
 - S 中任何两个元素的运算结果都属于 S ，即 S 对该运算**封闭**.

实例

例1 判断下面的运算哪些是相应集合上的二元运算：

□ (1) 自然数集合 \mathbf{N} 上的 $+$, $-$, \times , \div

■ $+$ 和 \times 是.

□ (2) 整数集合 \mathbf{Z} 上 $+$, $-$, \times , \div

■ $+$, $-$ 和 \times 是.

□ (3) 非零实数集 \mathbf{R}^* 上 $+$, $-$, \times , \div

■ \times 和 \div 是

实例

- (4) 设 $M_n(R)$ 表示所有 n 阶 ($n \geq 2$) 实矩阵的集合, 则矩阵加法和乘法:

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

■ 都是二元运算.

- (5) S 为任意集合, $P(S)$ 上的 \cup 、 \cap 、 $-$ 、 \oplus


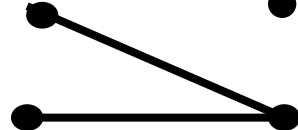

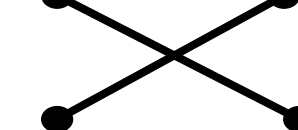
■ 都是二元运算.

实例

□ (6) S^S 为 S 上的所有函数的集合，函数的复合运算 \circ ：

■ \circ 是 S^S 上的二元运算。

□ 例如： $S=\{a, b\}$ ，则 S^S 包含如下函数：

f_1	f_3	\circ	f_1	f_2	f_3	f_4
		f_1	f_1	f_2	f_3	f_4
		f_2	f_2	f_2	f_3	f_3
f_2	f_4	f_3	f_3	f_2	f_3	f_2
		f_4	f_4	f_2	f_3	f_1

一元运算的定义与实例

□ **定义9.2** 设 S 为集合, 函数 $f:S \rightarrow S$ 称为 S 上的一元运算, 简称一元运算.

□ **例2**

- (1) 求相反数是整数集合 \mathbb{Z} , 有理数集合 \mathbb{Q} 和实数集合 \mathbb{R} 上的一元运算
- (2) 求倒数是非零有理数集合 \mathbb{Q}^* , 非零实数集合 \mathbb{R}^* 上一元运算
- (3) 求共轭复数是复数集合 \mathbb{C} 上的一元运算
- (4) 在幂集 $P(S)$ 上规定全集为 S , 则求绝对补运算 \sim 是 $P(S)$ 上的一元运算.

实例

- (5) 设 S 为集合, 令 A 为 S 上所有双射函数的集合, $A \subseteq S^S$, 求一个双射函数的反函数为 A 上的一元运算.
- (6) 在 $n(n \geq 2)$ 阶实矩阵的集合 $M_n(\mathbb{R})$ 上, 求转置矩阵是 $M_n(\mathbb{R})$ 上的一元运算.

二元与一元运算的表示

□ 1. 算符

- 可以用 $\circ, *, \cdot, \oplus, \otimes, \Delta$ 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

实例

□ 解析公式

- 例 设 \mathbf{R} 为实数集合，如下定义 \mathbf{R} 上的二元运算 $*$:

$$\forall x, y \in \mathbf{R}, x * y = x.$$

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	\dots	a_n
a_1	$a_1 \circ a_1$	$a_1 \circ a_2$	\dots	$a_1 \circ a_n$
a_2	$a_2 \circ a_1$	$a_2 \circ a_2$	\dots	$a_2 \circ a_n$
\vdots		\dots		
\vdots		\dots		
\vdots		\dots		
a_n	$a_n \circ a_1$	$a_n \circ a_2$	\dots	$a_n \circ a_n$

二元运算的运算表

a_i	$\circ a_i$
a_1	$\circ a_1$
a_2	$\circ a_2$
\vdots	\vdots
\vdots	\vdots
\vdots	\vdots
a_n	$\circ a_n$

一元运算的运算表

运算表实例

例3 设全集 $S=\{a,b\}$ ，定义在 $P(S)$ 上的 \oplus 和 \sim 运算的运算表如下

\oplus	\emptyset	$\{a\}$	$\{b\}$	$\{a,b\}$	x	$\sim x$
\emptyset	\emptyset	$\{a\}$	$\{b\}$	$\{a,b\}$	\emptyset	$\{a,b\}$
$\{a\}$	$\{a\}$	\emptyset	$\{a.b\}$	$\{b\}$	$\{a\}$	$\{b\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	\emptyset	$\{a\}$	$\{b\}$	$\{a\}$
$\{a,b\}$	$\{a,b\}$	$\{b\}$	$\{a\}$	\emptyset	$\{a,b\}$	\emptyset

二元运算的性质

定义9.3 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**.

二元运算的性质

定义9.4 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

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

则称 \circ 和 $*$ 运算满足**吸收律**.

实例

集合	运算	交换律	结合律	幂等律
$\mathbf{Z}, \mathbf{Q}, \mathbf{R}$	普通加法+ 普通乘法×	有 有	有 有	无 无
$M_n(\mathbf{R})$	矩阵加法+ 矩阵乘法×	有 无	有 有	无 无
$P(\mathbf{B})$	并 \cup 交 \cap	有 有	有 有	有 有
$\{0,1\}$	合取 \wedge 析取 \vee	有 有	有 有	有 有
A^A	函数复合 \circ	无	有	无

实例

集合	运算	分配律	吸收律
$\mathbf{Z}, \mathbf{Q}, \mathbf{R}$	普通加法+ 普通乘法×	×对+可分配 +对×不分配	无
$M_n(\mathbf{R})$	矩阵加法+ 矩阵乘法×	×对+可分配 +对×不分配	无
$P(B)$	并 \cup 交 \cap	\cup 对 \cap 可分配 \cap 对 \cup 可分配	有
$\{0,1\}$	合取 \wedge 析取 \vee	\wedge 对 \vee 可分配 \vee 对 \wedge 可分配	有

特异元素：单位元

定义9.5 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 $e_l \circ x = x$ (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**.

实例

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

β 、 δ 为左单位元

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

α 为单位元

特异元素：零元

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

\circ	f_1	f_2	f_3	f_4	
f_1	f_1	f_2	f_3	f_4	$f_2 f_3$ 为
f_2	f_2	f_2	f_2	f_2	左零元
f_3	f_3	f_3	f_3	f_3	
f_4	f_4	f_3	f_2	f_1	

可逆元素和逆元

(3) 设 \circ 为 S 上的二元运算, 令 e 为 S 中关于运算 \circ 的单位元.

对于 $x \in S$, 如果存在 y_l (或 y_r) $\in S$ 使得

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

则称 y_l (或 y_r) 是 x 的左逆元 (或右逆元).

关于 \circ 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, 逆元记作 x^{-1} .

实例

集合	运算	单位元	零元	逆元
$\mathbf{Z, Q, R}$	普通加法 普通乘法	$\mathbf{0}$ $\mathbf{1}$	无 $\mathbf{0}$	x 逆元 $-x$ x 逆元 x^{-1} ($x \neq 0$)
$\{0, 1\}$	合取 \wedge 析取 \vee	$\mathbf{1}$ $\mathbf{0}$	$\mathbf{0}$ $\mathbf{1}$	$\mathbf{1}$ 的逆元是 $\mathbf{1}$ $\mathbf{0}$ 的逆元是 $\mathbf{0}$
$P(B)$	并 \cup 交 \cap	\emptyset B	B \emptyset	\emptyset 的逆元是 \emptyset B 的逆元是 B

运算表与运算的性质

- 设代数系统 $\langle A, * \rangle$ ，运算的性质可以从运算表中看出
 - 封闭性：表中的每个元素都属于 A ；
 - 交换性：表关于主对角线对称；
 - 幂等性：主对角线上的每一个元素与它所在行（列）的表头元素相同；
 - 结合律的判断比较复杂。

运算表与特异元素

- 有幺元：该元素所对应的行和列依次与运算表的行和列相一致；
- 有零元：该元素所对应的行和列中的元素都与该元素相同；
- 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 b 所在行， a 所在列的元素都是幺元。

判断运算 $*$ 的性质

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

- ☐ 封闭
- ☐ 可交换
- ☐ 幺元: a
- ☐ a 的逆元是 a , b 和 c 互为逆元

*	<i>a</i>	<i>b</i>	<i>c</i>
<i>a</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>b</i>	<i>b</i>	<i>c</i>	<i>a</i>
<i>c</i>	<i>c</i>	<i>a</i>	<i>b</i>

*	<i>a</i>	<i>b</i>	<i>c</i>
<i>a</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>b</i>	<i>b</i>	<i>c</i>	<i>a</i>
<i>c</i>	<i>c</i>	<i>a</i>	<i>b</i>

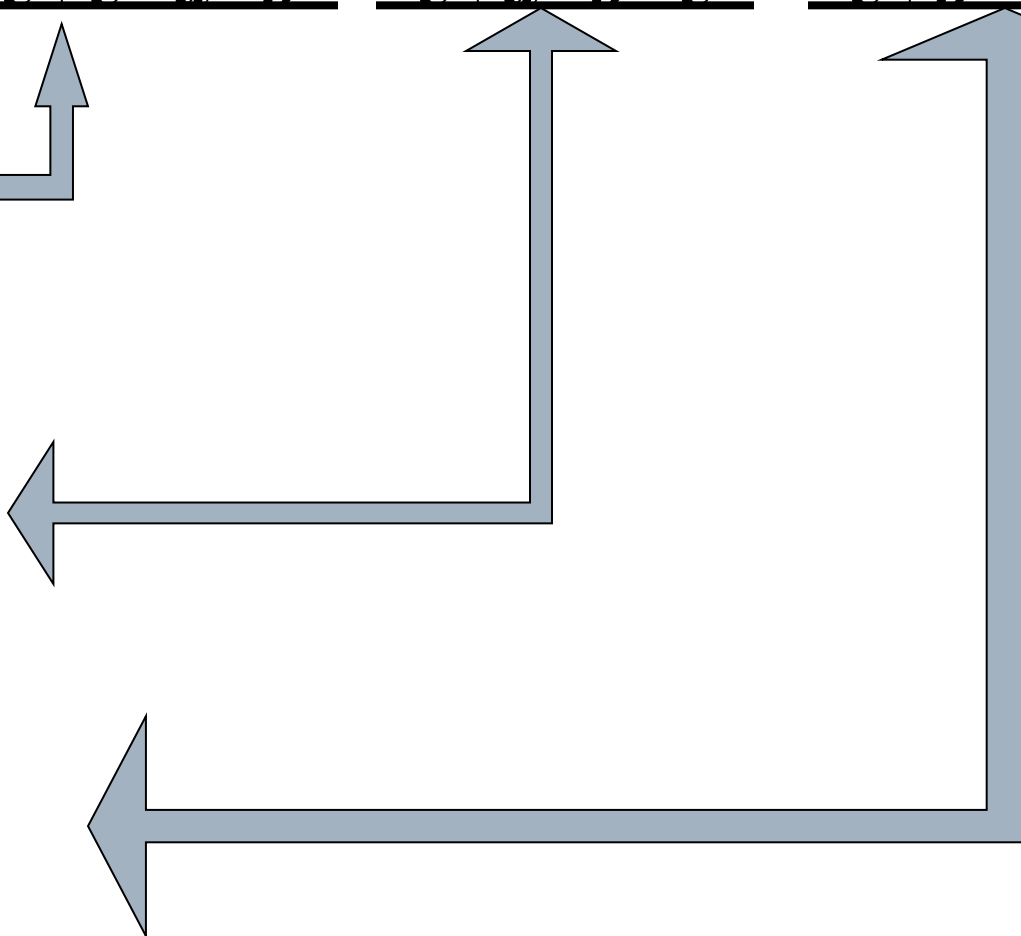
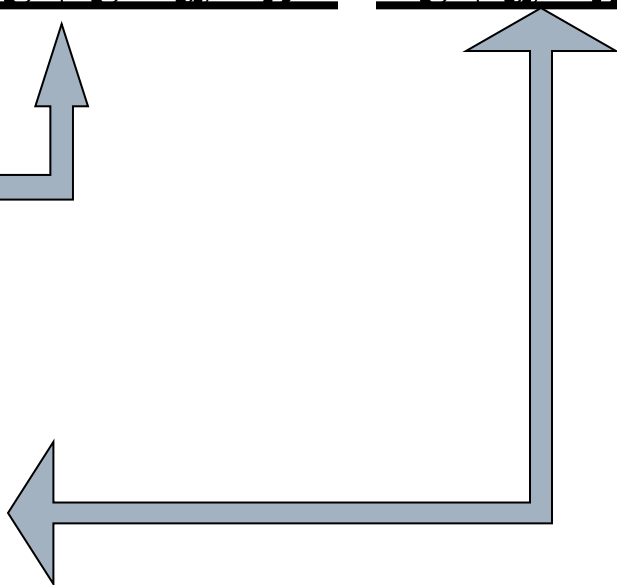
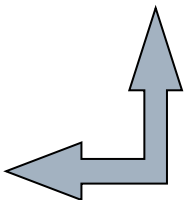
*	<i>b</i>	<i>c</i>	<i>a</i>
<i>a</i>	<i>b</i>	<i>c</i>	<i>a</i>
<i>b</i>	<i>c</i>	<i>a</i>	<i>b</i>
<i>c</i>	<i>a</i>	<i>b</i>	<i>c</i>

*	<i>c</i>	<i>a</i>	<i>b</i>
<i>a</i>	<i>c</i>	<i>a</i>	<i>b</i>
<i>b</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>c</i>	<i>b</i>	<i>c</i>	<i>a</i>

*	<i>a</i>	<i>b</i>	<i>c</i>
<i>a</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>b</i>	<i>b</i>	<i>c</i>	<i>a</i>
<i>c</i>	<i>c</i>	<i>a</i>	<i>b</i>

*	<i>a</i>	<i>b</i>	<i>c</i>
<i>b</i>	<i>b</i>	<i>c</i>	<i>a</i>
<i>c</i>	<i>c</i>	<i>a</i>	<i>b</i>
<i>a</i>	<i>a</i>	<i>b</i>	<i>c</i>

*	<i>a</i>	<i>b</i>	<i>c</i>
<i>c</i>	<i>c</i>	<i>a</i>	<i>b</i>
<i>a</i>	<i>a</i>	<i>b</i>	<i>c</i>
<i>b</i>	<i>b</i>	<i>c</i>	<i>a</i>



满足结合律

惟一性定理

□ **定理9.1** 设 \circ 为 S 上的二元运算, e_l 和 e_r 分别为 S 中关于运算的左和右单位元, 则 $e_l = e_r = e$, 且 e 为 S 上关于 \circ 运算的惟一的单位元.

□ 证: $e_l = e_l \circ e_r$ (e_r 为右单位元)
 $e_l \circ e_r = e_r$ (e_l 为左单位元)

所以 $e_l = e_r$, 将这个单位元记作 e .

假设 e' 也是 S 中的单位元, 则有 $e' = e \circ e' = e$.

惟一性得证.

惟一性定理

- **定理9.2** 设 \circ 为 S 上的二元运算, θ_l 和 θ_r 分别为 S 中关于运算的左和右零元, 则
 $\theta_l = \theta_r = \theta$, 且 θ 为 S 上关于 \circ 运算的惟一的零元.
- 证明略。

惟一性定理

- 定理9.3 设 \circ 为 S 上的二元运算, e 和 θ 分别为 \circ 运算的单位元和零元。如果 $|S| > 1$, 则 $e \neq \theta$ 。
- 证明：用反证法。
设 $e = \theta$, 则对于任意的 $x \in S$, 必有
$$x = e * x = \theta * x = \theta = e$$
于是 S 中只有一个元素, 与假设矛盾。
- 注意：当 $|S| \geq 2$, 单位元与零元是不同的；当 $|S| = 1$ 时, 这个元素既是单位元也是零元。

惟一性定理

□ **定理9.4** 设 \circ 为 S 上可结合的二元运算, e 为该运算的单位元, 对于 $x \in S$ 如果存在左逆元 y_l 和右逆元 y_r , 则有 $y_l = y_r = y$, 且 y 是 x 的惟一的逆元, 记作 x^{-1} 。

□ 证: 由 $y_l \circ x = e$ 和 $x \circ y_r = e$ 得

$$y_l = y_l \circ e = y_l \circ (x \circ y_r) = (y_l \circ x) \circ y_r = e \circ y_r = y_r$$

令 $y_l = y_r = y$, 则 y 是 x 的逆元.

假若 $y' \in S$ 也是 x 的逆元, 则

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

所以 y 是 x 惟一的逆元.

本节小结

- 二元及一元运算的定义
- 运算的表示：算符、运算表
- 二元运算的性质：交换律、结合律、幂等律、分配律、吸收律
- 运算的一些特殊元素：单位元、零元、逆元
- 唯一性定理：单位元、零元、逆元唯一
- 如果 $|S| > 1$ 则单位元与零元不同

9.2 代数系统

- **定义9.6** 非空集合 S 和 S 上 k 个一元或二元运算 f_1, f_2, \dots, f_k 组成的系统称为**代数系统**, 简称代数, 记做 $\langle S, f_1, f_2, \dots, f_k \rangle$.
- 例如:
 - (1) $\langle \mathbf{N}, + \rangle, \langle \mathbf{Z}, +, \cdot \rangle, \langle \mathbf{R}, +, \cdot \rangle$ 是代数系统, $+$ 和 \cdot 分别表示普通加法和乘法.
 - (2) $\langle M_n(\mathbf{R}), +, \cdot \rangle$ 是代数系统, $+$ 和 \cdot 分别表示 n 阶($n \geq 2$)实矩阵的加法和乘法.
 - (3) $\langle P(S), \cup, \cap, \sim \rangle$ 是代数系统, \cup 和 \cap 为并和交, \sim 为绝对补.

实例

- (4) $\langle \mathbb{Z}_n, \oplus, \otimes \rangle$ 是代数系统, $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$, \oplus 和 \otimes 分别表示模 n 的加法和乘法, 对于 $x, y \in \mathbb{Z}_n$, $x \oplus y = (x + y) \bmod n$, $x \otimes y = (xy) \bmod n$

\oplus_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

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。

实例

- 代数系统 $\langle \mathbb{Z}, +, 0 \rangle$: 集合 \mathbb{Z} , 运算 $+$, 代数常数 0
- 代数系统 $\langle P(S), \cup, \cap \rangle$: 集合 $P(S)$, 运算 \cup 和 \cap , 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 $\langle \mathbf{Z}, +, 0 \rangle$, $\langle P(S), \cup, \cap \rangle$

- (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 $\langle \mathbf{Z}, + \rangle$, $\langle P(S), \cup, \cap \rangle$

- (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 \mathbf{Z} , $P(B)$

同类型的代数系统

□ **定义9.7** 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.

■ 例如： $V_1 = \langle \mathbf{R}, +, \cdot, 0, 1 \rangle$,
 $V_2 = \langle P(B), \cup, \cap, \emptyset, B \rangle$

V_1, V_2 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.

运算性质比较

V_1	V_2
<ul style="list-style-type: none">+ 可交换、可结合· 可交换、可结合· 对 + 可分配+ 对 · 不可分配+ 与 · 没有吸收律	<ul style="list-style-type: none">∪可交换、可结合∩可交换、可结合∩对∪可分配∪对∩可分配∪与∩满足吸收律

子代数系统

□ **定义9.8** 设 $V = \langle S, f_1, f_2, \dots, f_k \rangle$ 是代数系统, B 是 S 的非空子集, 如果 B 对 f_1, f_2, \dots, f_k 都是封闭的, 且 B 和 S 含有相同的代数常数, 则称 $\langle B, f_1, f_2, \dots, f_k \rangle$ 是 V 的**子代数系统**, 简称子代数. 有时将子代数系统简记为 B .

□ 例如:

- \mathbf{N} 是 $\langle \mathbf{Z}, + \rangle$ 的子代数, \mathbf{N} 也是 $\langle \mathbf{Z}, +, 0 \rangle$ 的子代数
- $\mathbf{N} - \{0\}$ 是 $\langle \mathbf{Z}, + \rangle$ 的子代数, 但不是 $\langle \mathbf{Z}, +, 0 \rangle$ 的子代数

关于子代数的术语

- (1) 最大的子代数：就是 V 本身
- (2) 最小的子代数：如果令 V 中所有代数常数构成的集合是 B ，且 B 对 V 中所有的运算都是封闭的，则 B 就构成了 V 的最小的子代数
- (3) 最大和最小的子代数称为 V 的平凡子代数.
- (4) 若 B 是 S 的真子集，则 B 构成的子代数称为 V 的真子代数.

实例

- 设 $V = \langle \mathbb{Z}, +, 0 \rangle$, 令 $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$, n 为自然数, 则 $n\mathbb{Z}$ 是 V 的子代数
- 当 $n=1$ 和 0 时, $n\mathbb{Z}$ 是 V 的平凡子代数, 其他的都是 V 的非平凡的真子代数.

积代数

□ **定义9.9** 设 $V_1 = \langle A, \circ \rangle$ 和 $V_2 = \langle B, * \rangle$ 是同类型的代数系统， \circ 和 $*$ 为二元运算，在集合 $A \times B$ 上如下定义二元运算 \square ，

$\forall \langle a_1, b_1 \rangle, \langle a_2, b_2 \rangle \in A \times B$ ，有

$$\langle a_1, b_1 \rangle \square \langle a_2, b_2 \rangle = \langle a_1 \circ a_2, b_1 * b_2 \rangle$$

称 $V = \langle A \times B, \square \rangle$ 为 V_1 与 V_2 的**积代数**，记作 $V_1 \times V_2$ 。这时也称 V_1 和 V_2 为 V 的**因子代数**。

□ **注意：**积代数的定义可以推广到具有多个运算的同类型的代数系统。

实例

□ $Z_2 = \{0,1\}$, $V = \langle Z_2, \oplus \rangle$, $V \times V = \langle Z_2 \times Z_2, \cdot \rangle$
 $Z_2 \times Z_2 = \{ \langle 0,0 \rangle, \langle 1,0 \rangle, \langle 0,1 \rangle, \langle 1,1 \rangle \}$

\cdot	$\langle 0,0 \rangle$	$\langle 0,1 \rangle$	$\langle 1,0 \rangle$	$\langle 1,1 \rangle$
$\langle 0,0 \rangle$	$\langle 0,0 \rangle$	$\langle 0,1 \rangle$	$\langle 1,0 \rangle$	$\langle 1,1 \rangle$
$\langle 0,1 \rangle$	$\langle 0,1 \rangle$	$\langle 0,0 \rangle$	$\langle 1,1 \rangle$	$\langle 1,0 \rangle$
$\langle 1,0 \rangle$	$\langle 1,0 \rangle$	$\langle 1,1 \rangle$	$\langle 0,0 \rangle$	$\langle 0,1 \rangle$
$\langle 1,1 \rangle$	$\langle 1,1 \rangle$	$\langle 1,0 \rangle$	$\langle 0,1 \rangle$	$\langle 0,0 \rangle$

积代数的性质

- **定理9.5** 设 $V_1 = \langle A, \circ \rangle$ 和 $V_2 = \langle B, * \rangle$ 是同类型的代数系统, $V_1 \times V_2 = \langle A \times B, \square \rangle$ 是它们的积代数.
- (1) 如果 \circ 和 $*$ 运算是可交换(可结合、幂等)的, 那么 \square 运算也是可交换(可结合、幂等)的.
 - (2) 如果 e_1 和 e_2 (θ_1 和 θ_2) 分别为 \circ 和 $*$ 运算的单位元(零元), 那么 $\langle e_1, e_2 \rangle$ ($\langle \theta_1, \theta_2 \rangle$) 也是 \square 运算的单位元(零元).
 - (3) 如果 x 和 y 分别为 \circ 和 $*$ 运算的可逆元素, 那么 $\langle x, y \rangle$ 也是 \square 运算的可逆元素, 其逆元就是 $\langle x^{-1}, y^{-1} \rangle$.

9.3 代数系统的同态与同构

□ **定义9.10** 设 $V_1 = \langle A, \circ \rangle$ 和 $V_2 = \langle B, * \rangle$ 是同类型的代数系统, $f: A \rightarrow B$, 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.

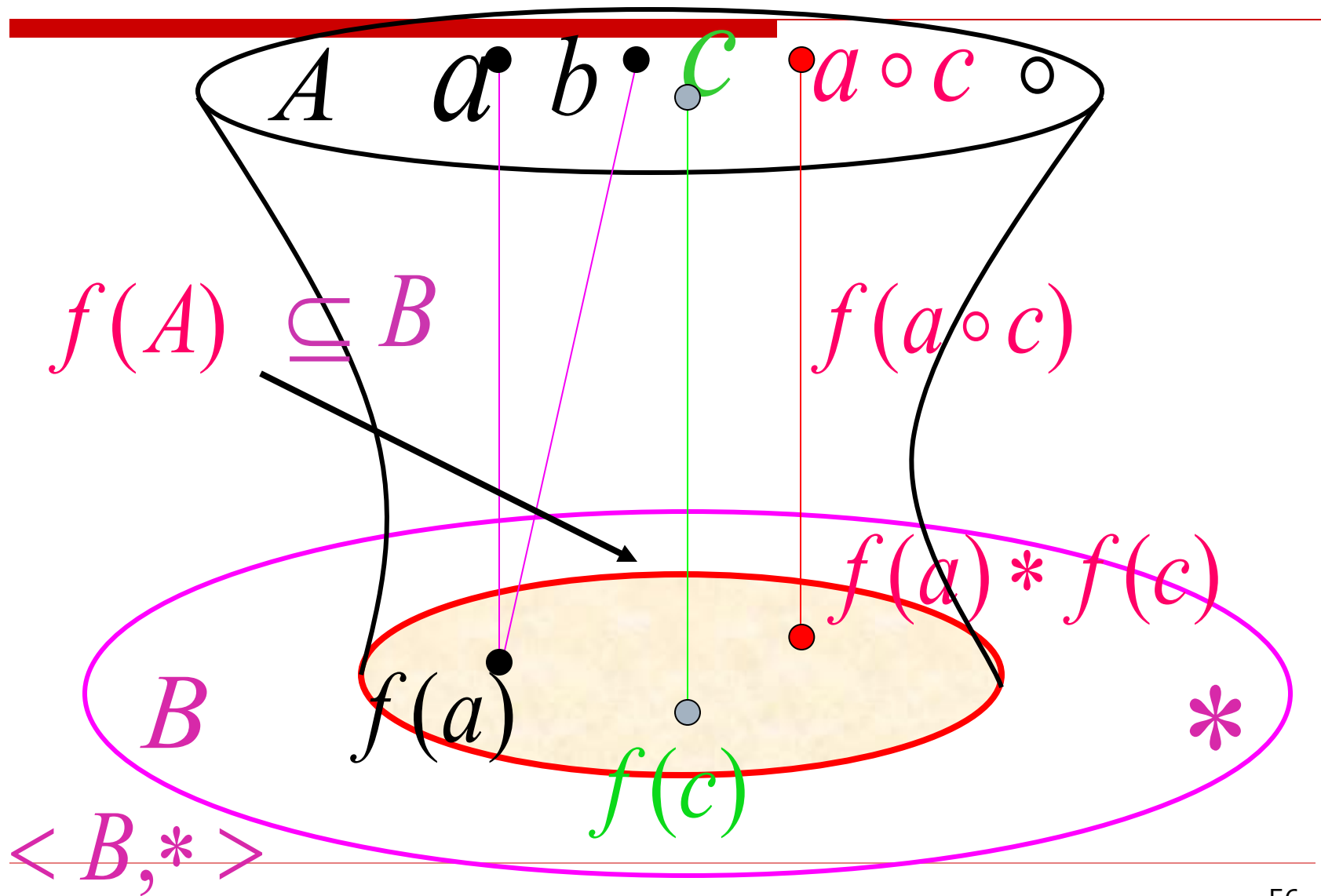
□ 例: $\langle \mathbb{Z}, \times \rangle$; $\langle B, * \rangle, B = \{\text{正}, \text{负}, \text{零}\}$

*	正	负	零
正	正	负	零
负	负	正	零
零	零	零	零

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

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

$\langle A, \circ \rangle$



同态分类

- (1) f 如果是单射, 则称为**单同态**.
- (2) f 如果是满射, 则称为**满同态**, 这时称 V_2 是 V_1 的**同态像**, 记作 $V_1 \sim V_2$.
- (3) f 如果是双射, 则称为同构, 也称代数系统 V_1 **同构** 于 V_2 , 记作 $V_1 \cong V_2$.
- (4) 如果 $V_1 = V_2$, 则称作**自同态**.

实例

□ (1) 设 $V_1 = \langle \mathbb{Z}, + \rangle$, $V_2 = \langle \mathbb{Z}_n, \oplus \rangle$. 其中 \mathbb{Z} 为整数集, $+$ 为普通加法; $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$, \oplus 为模 n 加.

□ 令 $f: \mathbb{Z} \rightarrow \mathbb{Z}_n$, $f(x) = (x) \bmod n$

f 显然是满射, 并且

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

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

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

所以 f 是 V_1 到 V_2 的满同态.

实例（续）

□ (2) 设 $V_1 = \langle \mathbf{R}, + \rangle$, $V_2 = \langle \mathbf{R}^*, \cdot \rangle$, 其中 \mathbf{R} 和 \mathbf{R}^* 分别为实数集与非零实数集, $+$ 和 \cdot 分别表示普通加法与乘法.

□ 令 $f: \mathbf{R} \rightarrow \mathbf{R}^*$, $f(x) = e^x$

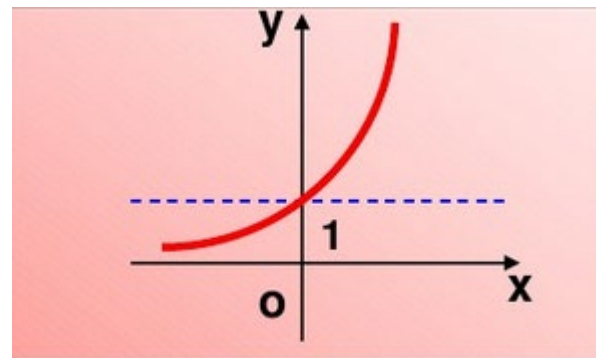
f 显然是单射, 并且

$$f(x+y) = e^{x+y}$$

$$= e^x \cdot e^y$$

$$= f(x) \cdot f(y)$$

则 f 是 V_1 到 V_2 的单同态.



实例（续）

×	正	负	+	偶	奇
正	正	负	偶	偶	奇
负	负	正	奇	奇	偶

- (3) 设 $V_1 = \langle \{\text{正}, \text{负}\}, \times \rangle$, $V_2 = \langle \{\text{奇}, \text{偶}\}, + \rangle$.
令 $f(\text{正}) = \text{偶}$, $f(\text{负}) = \text{奇}$
这两个代数系统是同构的。

实例（续）

- (4) 设 $V = \langle \mathbb{Z}, + \rangle$, 其中 \mathbb{Z} 为整数集, $+$ 为普通加法. $\forall a \in \mathbb{Z}$,
- 令 $f_a: \mathbb{Z} \rightarrow \mathbb{Z}$, $f_a(x) = ax$,
那么 f_a 是 V 的自同态.
当 $a=0$ 时称 f_0 为零同态;
当 $a=\pm 1$ 时, 称 f_a 为自同构;
除此之外其他的 f_a 都是单自同态.