第三篇 代数结构

Algebraic Structures

引言

- 代数结构也称为代数系统，是抽象代数的主要研究对象。
- 抽象代数是数学的一个分支，它用代数的方法从不同的研究对象中概括出一般的数学模型并研究其规律、性质和结构。
- 抽象代数学的研究对象是抽象的，它不是以某一具体对象为研究对象，而是以一大类具有某种共同性质的对象为研究对象，因此其研究成果适用于这一类对象中的每个对象，从而达到了事半功倍的效果。

引言（续）

- 抽象代数学的主要内容：
  - 研究各种各样的代数系统，它是在较高的观点上，把一些形式上很不相同的代数系统，撇开其个性，抽出其共性，用统一的方法描述、研究和推理，从而得到一些反映事物本质的结论，再把它们应用到那些系统中去，高度的抽象产生了广泛的应用。

引言（续）

- 构成一个抽象代数系统有三方面的要素：集合、集合上的运算以及说明运算性质或运算之间关系的公理。

整数集合Z和普通加法$+$构成了代数系统$\langle Z, +\rangle$，n阶实矩阵的集合$M_n(R)$与矩阵加法$+$构成代数系统$\langle M_n(R), +\rangle$。幂集$P(B)$与集合的对称差运算$\oplus$也构成了代数系统$\langle P(B), \oplus\rangle$。

引言（续）

- 考察他们的共性，不难发现他们都含有一个集合，一个二元运算，并且这些运算都具有交换性和结合性等性质。为了概括这类代数系统的共性，我们可以定义一个抽象的代数系统$\langle A, \circ\rangle$，其中 A是一个集合，$\circ$是A上的可交换、可结合的运算，这类代数系统实际上就是交换半群。

引言（续）

- 为了研究抽象的代数系统，我们需要先定义一元和二元代数运算以及二元运算的性质，并通过选择不同的运算性质来规定各种抽象代数系统的定义。在此基础上再深入研究这些抽象代数系统的内在特性和应用。

引言（续）

- 抽象代数在计算机中有着广泛的应用，例如自动机理论、编码理论、密码学、开关电路等等都要用到抽象代数的知识。

代数结构的知识体系

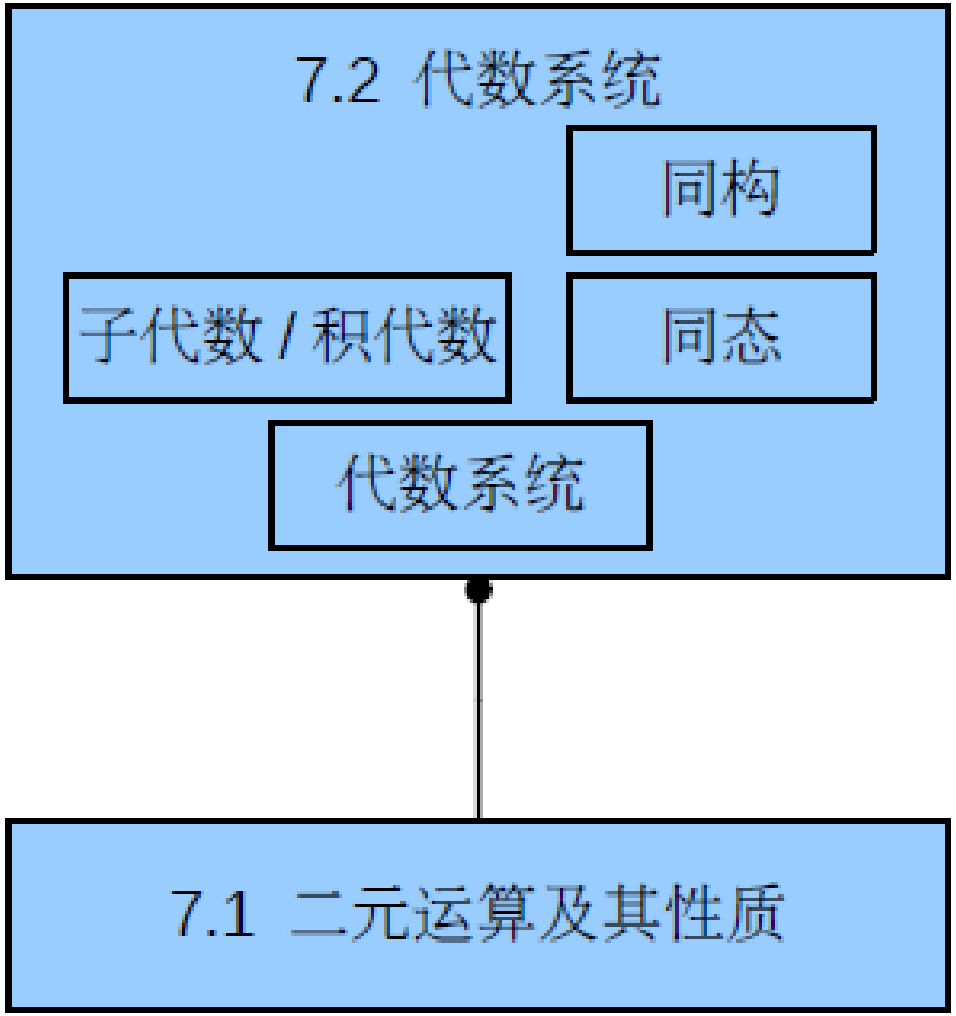
第 7 章 代数系统
（一般的代数系统）

特殊的代数系统

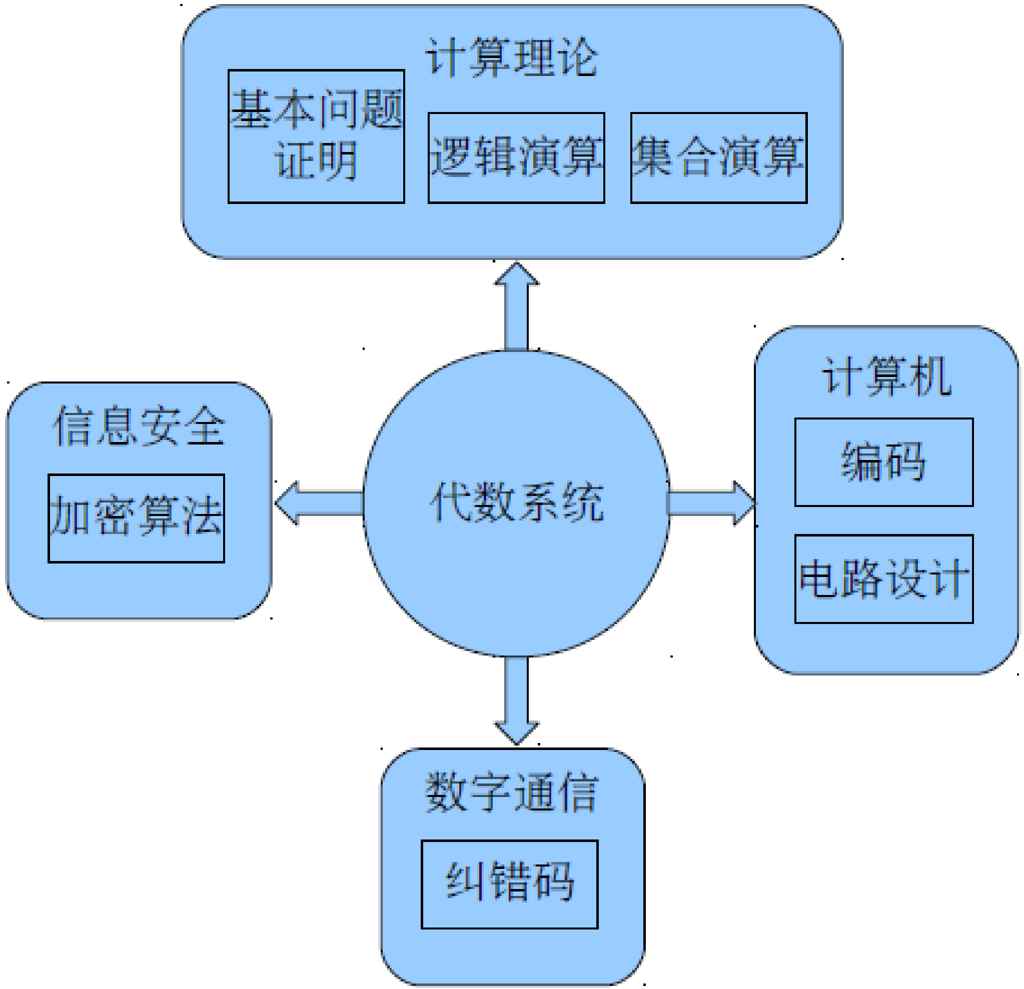
- 第 8 章 群论初步
  - 群 （1 个运算）
  - 扩展
  - 环→域 （2 个运算）
- 第 9 章 格与布尔代数 （2 个运算 + 序）

第七章代数系统

代数系统部分知识逻辑概图



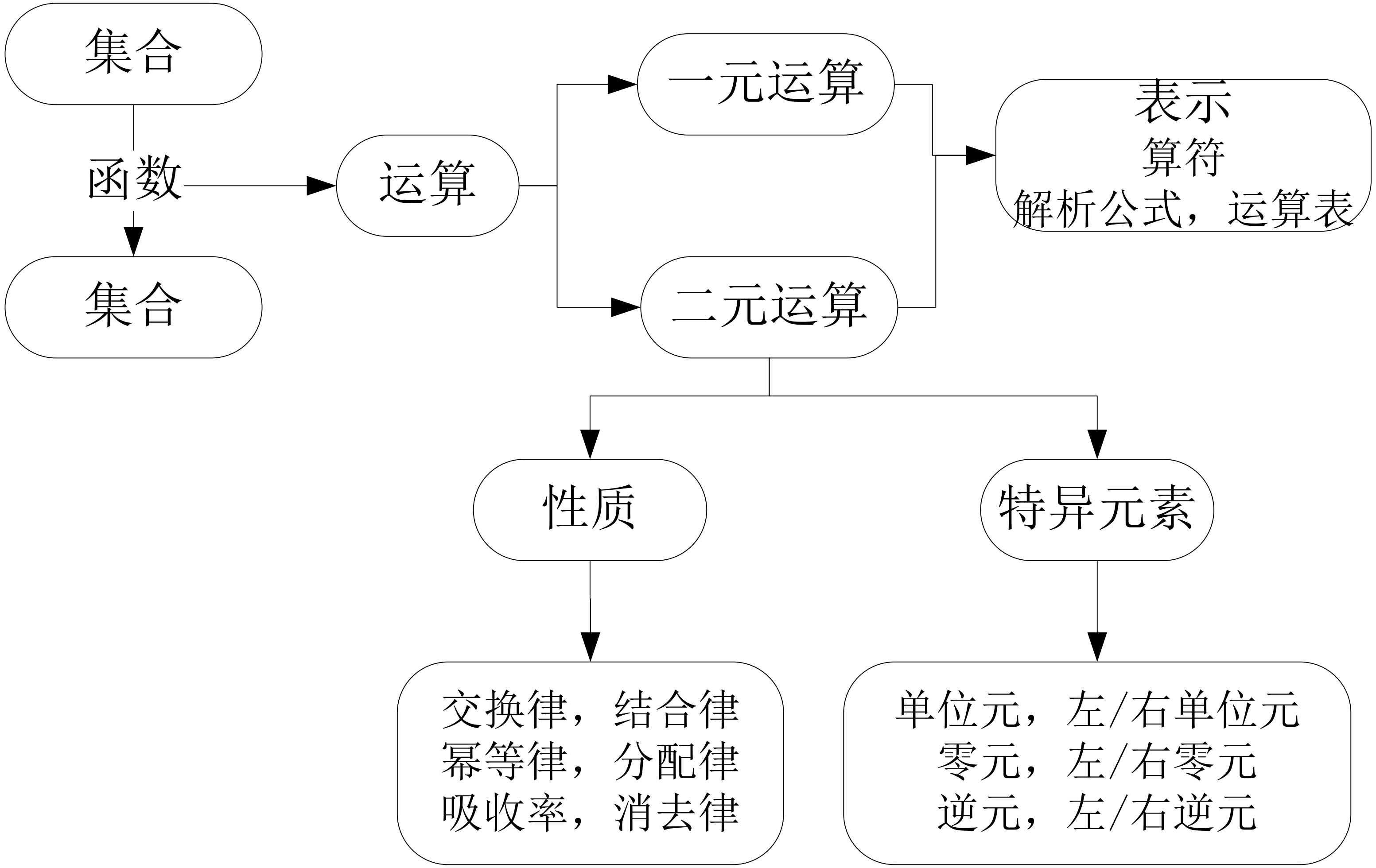
代数系统在计算机科学技术相关领域的应用概图



7.1 二元运算及其性质

二元运算：S×S到S的函数。

7.1 二元运算及其性质


集合
函数
集合
运算
一元运算
二元运算
表示
算符
解析公式，运算表
性质
特异元素
交换律，结合律
幂等律，分配律
吸收率，消去律
单位元，左/右单位元
零元，左/右零元
逆元，左/右逆元

7.1 二元运算及其性质

- 定义7.1 设 S是一非空集合，函数f：$S\times S\to S$ 称为集合S上的一个二元运算，简称二元运算.
- 验证一个运算是否为集合S上的二元运算主要考虑两点：
  - (1)S中任何两个元素都可以进行这种运算,且运算的结果是唯一的。
  - (2)S中任何两个元素的运算结果都属于S,即S对该运算是封闭的。
- 若S是一个非空集合，函数f：$S^n\to S$ 称为集合S上的一个n元运算($n\in Z^+$)

7.1 二元运算及其性质

- 例

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

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

则矩阵加法和乘法都是$M_n(R)$上的二元运算。

7.1 二元运算及其性质

- (3) 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。
- (4) S为任意集合,则∪,∩,−, ⊕为S的幂集P(S)上的二元运算。
- (5) S为集合, S^S为S上的所有函数的集合,则函数的复合运算 ∘为S^S上的二元运算。
- (6)逻辑联结词合取∧、析取∨、蕴涵→、等价$\boxed{\leftrightarrow}$都是真值集合{0, 1}上的二元代数运算。

7.1 二元运算及其性质

- 定义7.2 设 S为集合，函数f：S→S 称为集合S上的一个一元运算，简称一元运算.
- 例：(1) 求一个数的相反数是整数集合Z、有理数集合Q和实数集合R上的一元运算。
- (2) 求一个数的倒数是非零有理数集合Q*、非零实数集合R*上的一元运算。
- (3) 求一个复数的共轭复数是复数集合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~是P(S)上的一元运算。

7.1 二元运算及其性质

❖ 二元与一元运算的表示

（1）算符

- 可以用 $\circ$, $*$, $\cdot$, $\square$, $\lozenge$, $\triangle$, $\oplus$, $\otimes$ 等符号表示二元或一元运算,称为算符。对于二元运算 $\circ$,如果x与y运算得到z,记做$x \circ y = z$;
- 对于一元运算 $\circ$，x的运算结果记作 $\circ x$.

7.1 二元运算及其性质

- (2)解析公式和运算表

解析公式法

- 例 设R为实数集合,如下定义R上的二元运算*:

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

  计算3*4, (-5)*0.2, 0*(1/2)

- 解：3*4 = 3, (-5)*0.2 = -5, 0*(1/2) = 0

7.1 二元运算及其性质

运算表法

a_i	$\circ a_i$
a_1	$\circ a_1$
a_2	$\circ a_2$
…	…
a_n	$\circ a_n$

表1一元运算表的一般形式

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

表2 二元运算表的一般形式

7.1 二元运算及其性质

例 设$S=\{1,2\}$, 给出$P(S)$上的运算~和⊕的运算表, 其中全集为S.

解： 所求的运算表如下表。

a_i	$\sim a_i$
$\varnothing$	$\{1,2\}$
$\{1\}$	$\{2\}$
$\{2\}$	$\{1\}$
$\{1,2\}$	$\varnothing$

$\oplus$	$\varnothing$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\varnothing$	$\varnothing$	$\{1\}$	$\{2\}$	$\{1,2\}$
$\{1\}$	$\{1\}$	$\varnothing$	$\{1,2\}$	$\{2\}$
$\{2\}$	$\{2\}$	$\{1,2\}$	$\varnothing$	$\{1\}$
$\{1,2\}$	$\{1,2\}$	$\{2\}$	$\{1\}$	$\varnothing$

7.1 二元运算及其性质

❖ 二元运算的性质

- 定义7.3 设 $\circ$为S上的二元运算,如果对于任意的$x, y \in S$, 有$x \circ y = y \circ x$,
  则称运算 $\circ$在S上满足交换律。
- 定义7.4 设 $\circ$为S上的二元运算,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 $\circ$在S上满足结合律。
- 定义7.5设 $\circ$为S上的二元运算,如果对于任意的$x \in S$有$x \circ x = x$,
  则称运算$\circ$在S上满足幂等律。
  - 如果S中某些x满足$x \circ x = x$, 则称x为运算$\circ$的幂等元。

实例：交换、结合、幂等律

- 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, $n\geq2$；$P(B)$为幂集；A^A为从A到A的函数集，$|A|\geq2$

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∘	无	有	无

7.1 二元运算及其性质

❖ 二元运算的性质（续）

- 定义7.6 设 ∘和*为S上两个不同的二元运算,如果对于任意的$x, y, z \in S$

  有$(x*y) \circ z = (x \circ z)*(y \circ z)$(右分配律)和$z \circ (x*y) = (z \circ x)*(z \circ y)$(左分配律),

  则称运算 ∘对运算*满足分配律。

- 定义7.6 如果 ∘和*都可交换,并且对于任意的$x, y \in S$

  都有$x \circ (x*y) = x$和$x*(x \circ y) = x$,

  则称运算∘和运算*满足吸收律。

实例：分配、吸收律

- 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

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

7.1 二元运算及其性质

例：N是自然数集合，在N上定义运算“*”：

对于任意的$m, n \in N$, $m*n = m+2n$.

(1) “*”是可交换的吗？(2) “*”适合结合律吗？

解：(1)对于任意的 $m, n \in N$

$m*n = m+2n$

$n*m = n+2m$

显然，当$m \neq n$时$m*n \neq n*m$

所以”*”是不可交换的。

7.1 二元运算及其性质

例：N是自然数集合，在N上定义运算“*”：

对于任意的$m, n \in N$, $m*n = m+2n$.

(2) “*”适合结合律吗？

(2)对于任意的 $m, n, l \in N$

因为 $(m*n)*l = (m+2n)*l = (m+2n)+2l = m+2n+2l$

而 $m*(n*l) = m*(n+2l) = m+2(n+2l) = m+2n+4l$

由 l 的任意性知$(m*n)*l \neq m*(n*l)$

7.1 二元运算及其性质

❖ 二元运算的特异元素：单位元、零元和逆元

❖ 定义7.8 设 ∘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 $$e_l \circ x = x \quad (或 x\circ e_r = x)$$

则称e_l(或e_r)是S中关于运算∘的左(或右)单位元。若$e\in S$关于运算∘既是左单位元又是右单位元, 则称e为S上关于运算∘的单位元。单位元也叫做幺元。

❖ 定义7.9 设 ∘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 $$\theta_l \circ x=\theta_l \quad (或 x \circ \theta_r=\theta_r)$$

则称θ_l(或θ_r)是S中关于运算∘的左(或右)零元。若$\theta\in S$关于运算∘既是左零元又是右零元, 则称θ为S上关于运算∘的零元。

7.1 二元运算及其性质

❖ 定义7.10 设$\circ$为S上的二元运算，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 $y_l \circ x = e$（或$x \circ y_r = e$）

则称y_l(或y_r)是x的左逆元(或右逆元)。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。

如果b是a的逆元，那么a也是b的逆元，简称a与b互为逆元。x的逆元记为x^{-1}。

一般，一个元素的左逆元不一定等于右逆元，而且一个元素可以只有左（右）逆元没有右（左）逆元，而且左（右）逆元不一定唯一.

7.1 二元运算及其性质

特异元素的实例

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 的逆元 $-x$ x 的逆元 x^{-1} ($x^{-1}\in$给定集合)
$Mn(R)$	矩阵加法+ 矩阵乘法×	全 0 矩阵 单位矩阵	无 全 0 矩阵	X 逆元 $-X$ X 的逆元 X^{-1} (X 是可逆矩阵)
$P(B)$	并∪ 交∩ 对称差⊕	∅ B ∅	B ∅ 无	∅的逆元为∅ B 的逆元为 B X 的逆元为 X

7.1 二元运算及其性质

❖ **定理7.1** 设∘为S上的二元运算, e_l和e_r分别为S中关于运算∘的左单位元和右单位元，则有： $e_l = e_r = e$ 且e为S上关于运算∘的唯一的单位元。

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

$$e' = e \circ e' = e。$$

唯一性得证。

7.1 二元运算及其性质

❖ 定理7.2 设$\circ$为S上的二元运算，θ_l和θ_r分别为S中关于运算$\circ$的左零元和右零元，

则有：$\theta_l = \theta_r = \theta$　　且θ为S上关于运算$\circ$的唯一的零元。

证：　$\theta_l = \theta_l \circ \theta_r$　（θ_l为左零元）

$\theta_l \circ \theta_r = \theta_r$　（θ_r为右零元）

所以$\theta_l = \theta_r$，将这个零元记作θ。

假设θ'也是S中的零元，则有

$$\theta' = \theta \circ \theta' = \theta$$

唯一性得证。

7.1 二元运算及其性质

❖ **定理7.3** 设$\circ$为S上的二元运算，e和θ分别为S中关于运算$\circ$的单位元和零元，如果S至少有两个元素，则$e \neq \theta$.

证： 用反证法。假设 $e = \theta$，则对任意$x \in S$有

$$x = x \circ e = x \circ \theta = \theta$$

与S至少有两个元素相矛盾。

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.

7.1 二元运算及其性质

❖ 定理7.4 设∘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的唯一的逆元。

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唯一的逆元。

❖ 说明：对于可结合的二元运算，可逆元素 x 只有惟一的逆元，记作 x^{-1}

7.1 二元运算及其性质

❖ 定义7.11 设∘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$y = z$；

则称运算 ∘满足消去律，（1）称作左消去律，（2）称作右消去律。

❖ 实例：

- Z, Q， R, 运算+， ×满足消去律，
- Mn(R)， 矩阵+满足消去律，矩阵×不满足消去律
- P(B)， ⊕满足消去律，∪、∩、-不满足消去律，

7.1 二元运算及其性质

- 例1 设A为实数集，$\forall x, y\in A$, $x\circ y = x+y-2xy$，

  (1) 说明∘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.

$1\circ 1 = 1+1-2 \neq 1$，幂等律不成立

(2) 设单位元、零元分别为e、θ, 则$\forall x\in A$

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

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

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

7.1 二元运算及其性质

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

交换, 结合, 消去

幺元 e=a

幂等元：a

逆元：$a^{-1}=a$

$b^{-1}=c$, $c^{-1}=b$

□	a	b	c
a	a	b	c
b	a	b	c
c	a	b	c

结合, 幂等

幂等元：a, b, c

•	a	b	c
a	a	b	c
b	b	a	c
c	c	c	c

交换, 结合, 消去

幺元 e=a,

零元 θ=c,

幂等元：a, c

逆元：$a^{-1}=a$

$b^{-1}=b$

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

交换, 结合

幺元 e=a

幂等元：a, b

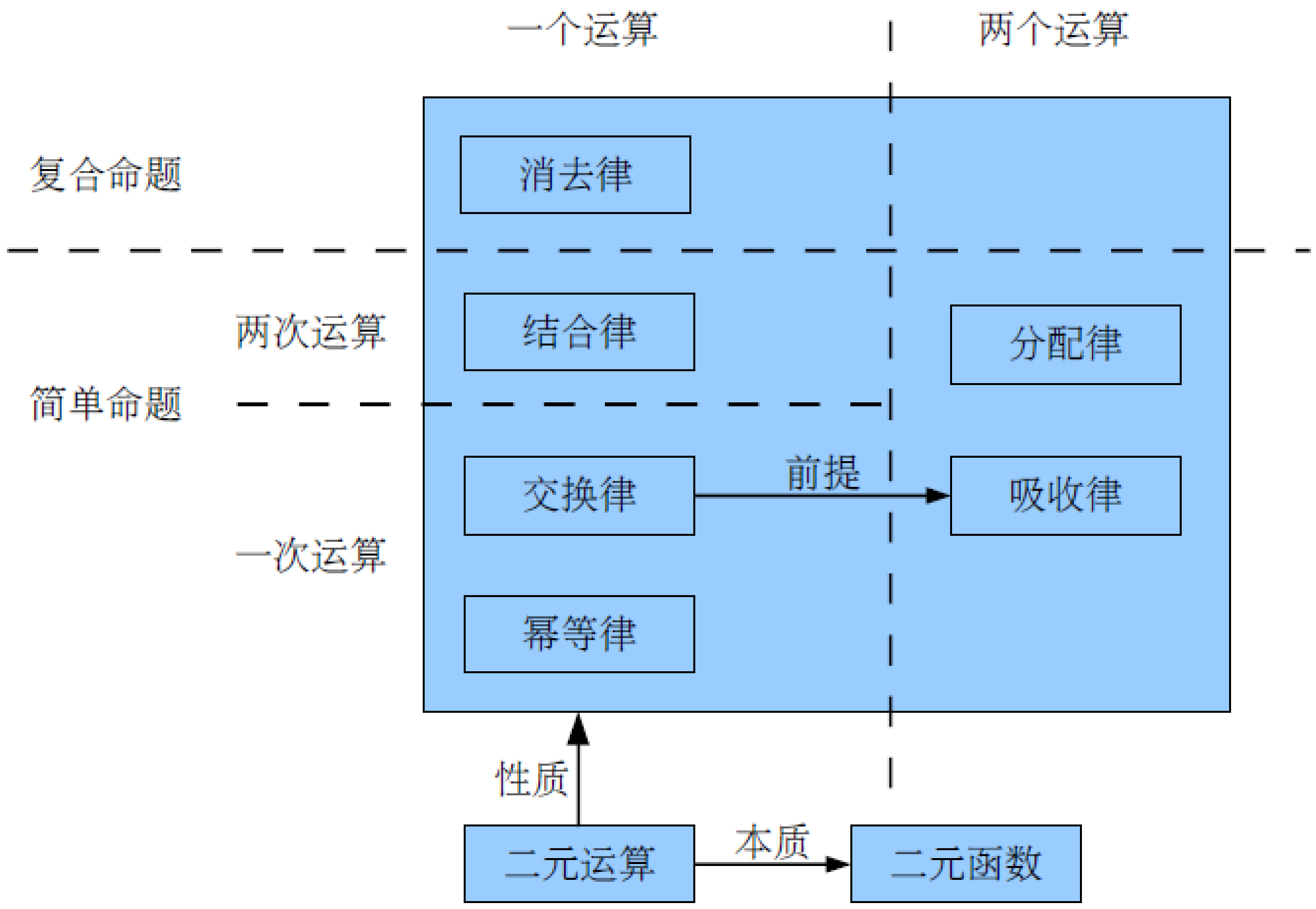
逆元；$a^{-1}=a$

通过运算表可以判断运算性质，也可以求运算的特异元素。

- 如果运算表的元素关于主对角线成对称分布，那么运算是可交换的。
- 如果主对角线元素的排列顺序与表头元素的排列顺序一样，那么运算是幂等的。
- 如果一个元素所在的行和列的元素排列顺序都与表头元素排列顺序一致，那么这个元素就是单位元。
- 如果一个元素的行和列的元素都是这个元素自身，那么这个元素是零元。
- 如果元素x在主对角线中排列的位置与表头中的位置一致，那么这个元素是幂等元。

小结

- 集合上的二元运算实质上是一个从该集合的笛卡尔积到该集合的函数，它的性质主要包括交换律、结合律、幂等律、分配律、吸收律和消去律。



7.2 代数系统

代数系统：集合及其上的运算。

7.2 代数系统

- 一.什么是代数系统?
  - 粗略地说，代数系统是由一个特定的“集合”，以及定义于该集合上的若干“运算”所组成，换言之，它是一个“有组织的集合”。
  - 定义7.12 非空集合S和S上k个一元或二元运算$f_1, f_2, \ldots, f_k$组成的系统称为一个代数系统，简称代数，记作$<S, f_1, f_2, \ldots, f_k>$.
  - 现代科学在研究各种不同现象时，为了探索它们之间的共同特点，常常利用代数系统这个框架进行研究，得出深刻的结果。

7.2 代数系统

❖ 实例：

- $<\mathrm{N}, +>$, $<\mathrm{Z}, +, \cdot>$, $<\mathrm{R}, +, \cdot>$是代数系统，
  +和·分别表示普通加法和乘法.
- $<M_n(\mathrm{R}), +, \cdot>$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，$Z_n = \{0, 1, \ldots, n-1\}$，
  $\oplus$和$\otimes$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，
  $\cup$和$\cap$为并和交，$\sim$为绝对补

7.2 代数系统

- 二. 代数系统的成分与表示
- （1）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

7.2 代数系统

❖ （2）代数系统的表示

- 列出所有的成分：集合、运算、代数常数（如果存在）

  如$<Z, +, 0>$, $<P(S), \cup, \cap, \sim, \Phi, S>$

- 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$<Z, +>$, $<P(S), \cup, \cap, \sim>$

- 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, $P(S)$

7.2 代数系统

❖ 三. 同类型与同种代数系统

▪ **定义7.13**

- 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，则称它们具有相同的构成成分，也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.

7.2 代数系统

❖ 实例——三个代数系统的比较

- $V_1 = <\mathrm{R}, +, \cdot, 0, 1>$,
- $V_2 = <Mn(\mathrm{R}), +, \cdot, \theta, E>$, θ 为 n 阶全 0 矩阵，E 为 n 阶单位矩阵
- $V_3 = <P(B), \cup, \cap, \varnothing, B>$

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

- V_1, V_2, V_3是同类型的代数系统
- 都不是同种的代数系统

7.2 代数系统

❖ 从代数系统的构成成分和遵从的算律出发，将代数系统分类，然后研究每一类代数系统的共同性质，并将研究的结果运用到具体的代数系统中去，这种方法就是抽象代数的基本方法，也是代数结构课程的主要内容。

7.2 代数系统

❖ 四、子代数系统

- 定义7.14设$V=<S, f_1, f_2, \ldots, f_k>$是代数系统，$B$是$S$的非空子集，如果$B$对$f_1, f_2, \ldots, f_k$都是封闭的，且$B$和$S$含有相同的代数常数，则称$<B, f_1, f_2, \ldots, f_k>$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.
- 实例
  - N是$<Z, +>$的子代数，N也是$<Z, +, 0>$的子代数
  - $N-\{0\}$是$<Z, +>$的子代数，但不是$<Z, +, 0>$的子代数
- 说明：
  - 子代数和原代数是同种的代数系统
  - 对于任何代数系统$V=<S, f_1, f_2, \ldots, f_k>$，其子代数一定存在.

7.2 代数系统

❖ 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）平凡的子代数：最大和最小的子代数称为V的平凡的子代数
- （4）真子代数：若B是S的真子集，则B构成的子代数称为V的真子代数.

❖ 例 设$V=\langle Z, +, 0\rangle$, 令 $nZ=\{nz \mid z\in Z\}$, n为自然数，则nZ是V的子代数

当n=1和0时，nZ是V的平凡的子代数，其他的都是V的非平凡的真子代数.

7.2 代数系统

❖ 设V=<Z, +>，问3Z, {0}, V是否为V的子代数系统？为什么？如果是，说明其中哪些是平凡的，哪些是真子代数？

解：都是V的子代数。

显然 {0} 和V关于 + 运算是封闭的。

对于任意的$3m, 3n \in 3Z$,

$$3m+3n=3(m+n) \in 3Z$$

3Z关于 + 运算也是封闭的。

{0}和V是平凡的，{0}和3Z是真子代数。

7.2 代数系统

❖ 例. 设V＝<A, ⊕>, 其中A＝P({1,2,3})，⊕为集合的对称差，试给出V的所有的子代数，并说明哪些是平凡的子代数？哪些是真子代数？

解：A={Φ,{1}, {2}, {3}, {1,2}, {1,3}, {2,3}, {1,2,3}}

平凡的：B_1={Φ}, V

2元的：B_2 = {Φ, {1}}, B_3 = {Φ, {2}}, B_4 = {Φ, {3}},

B_5 = {Φ, {1, 2}}, B_6 = {Φ, {1, 3}}, B_7 = {Φ, {2, 3}}, B_8＝{Φ,{1, 2, 3}}.

4元的：B_9 = {Φ, {1}, {2}, {1,2}}，B_{10} = {Φ, {1}, {3}, {1,3}}，B_{11} = {Φ, {2}, {3}, {2,3}}，B_{12} = {Φ, {1,2}, {1,3}, {2,3}}, B_{13} = {Φ, {2}, {1,3}, {1,2,3}},

B_{14} = {Φ, {3}, {1,2}, {1,2,3}}, B_{15} = {Φ, {1}, {2,3}, {1,2,3}}

以上子代数中除了V之外，都是真子代数。

7.2 代数系统

❖ 五、积代数

- 定义7.15　设 $V_1=\langle A,\circ\rangle$和 $V_2=\langle B,*\rangle$是同类型的代数系统，其中∘和 $*$ 是二元运算，在集合A×B上如下定义二元运算•，　$\forall\langle a_1,b_1\rangle$，$\langle a_2,b_2\rangle\in A\times B$，有　　$\langle a_1,b_1\rangle\bullet\langle a_2,b_2\rangle=\langle a_1\circ a_2,\ b_1*b_2\rangle$

  称$V=\langle A\times B,\bullet\rangle$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。

- 例　$V_1=<Z,+>$, $V_2=<M_2(R),\cdot>$, 积代数$<Z\times M_2(R),\circ>$

  $\forall<z_1,M_1>,<z_2,M_2>\in Z\times M_2(R)$，

  $$<z_1,M_1>\circ<z_2,M_2> = <z_1+z_2,\ M_1\cdot M_2>$$

  $$<5,\begin{pmatrix}1&0\\1&1\end{pmatrix}>\circ<-2,\begin{pmatrix}2&-1\\0&1\end{pmatrix}>=<3,\begin{pmatrix}2&-1\\2&0\end{pmatrix}>$$

7.2 代数系统

❖ 积代数的性质

- 定理7.5 设 $V_1=\langle S_1,\circ\rangle$和 $V_2=\langle S_2,*\rangle$是同类型的代数系统，其中$\circ$和 $*$是二元运算. V_1 与 V_2 的积代数是 $V=\langle S_1\times S_2,\cdot\rangle$
  - (1) 若 $\circ$ 和 $*$ 运算是可交换（可结合、幂等）的，那么$\cdot$ 运算也是可交换（可结合、幂等）的
  - (2) 若 $\circ$和 $*$ 运算分别具有单位元 e_1 和 e_2，那么$\cdot$ 运算也具有单位元$\langle e_1, e_2\rangle$
  - (3) 若 $\circ$和 $*$ 运算分别具有零元 θ_1 和 θ_2，那么$\cdot$ 运算也具有零元$\langle \theta_1, \theta_2\rangle$
  - (4) 若 x 关于 $\circ$的逆元为 x^{-1}, y 关于 $*$ 的逆元为 y^{-1}，那么$\langle x, y\rangle$关于$\cdot$ 运算也具有逆元$\langle x^{-1}, y^{-1}\rangle$

7.2 代数系统

$V_1=<Z_3, \oplus_3>$, $V_2=<A, \oplus_6>$, $Z_3=\{0,1,2\}$, $A = \{0,2,4\}$, 其运算表为

$\oplus_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\oplus_6$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

把左边表中1和2分别换成2和4, 就可以得到右边的表.这个替换可以表示为函数:

$$f = \{<0,0>, <1,2>, <2,4>\}$$

在双射函数f的作用下, 代数系统V_1转换为V_2.

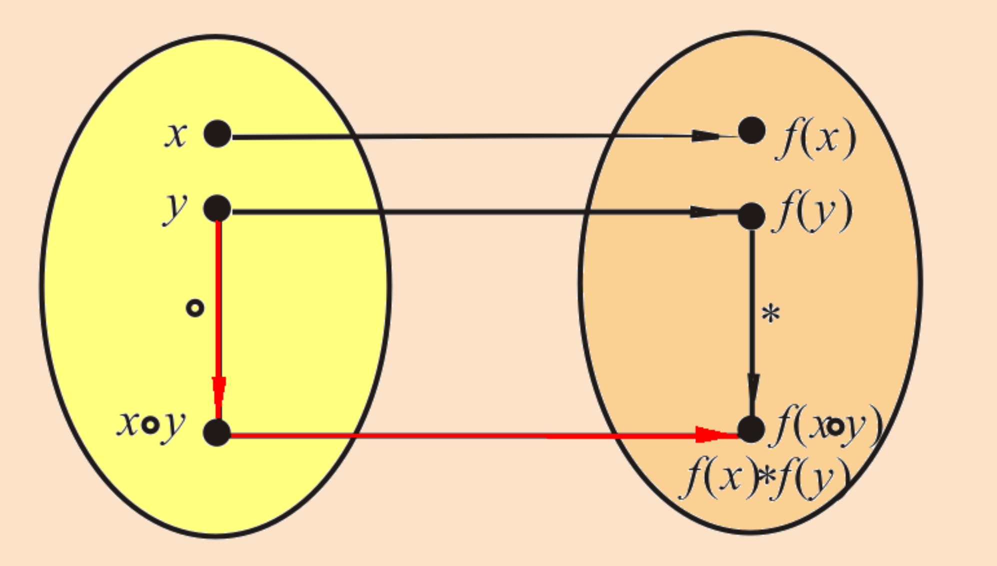
7.2 代数系统

❖ 六、同态映射的定义

- 定义7.16 设 $V_1=\langle A,\circ\rangle$和 $V_2=\langle B,*\rangle$是同类型的代数系统，其中 $\circ$ 和 $*$ 是二元运算. $f:A\rightarrow B$，且 $\forall x,y\in A$，有

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

则称 f 为V_1 到 V_2的同态映射，简称同态.



7.2 代数系统

例1 $V=\langle R^*,\cdot\rangle$, 判断下面的哪些函数是$V$到$V$ 的同态？($\cdot$为数集上的乘法)

(1) $f(x)=2x$ (2) $f(x)=x^2$

(3) $f(x)=1/x$ (4) $f(x)=-x$

解： (1) 不是同态，$f(2\cdot 2)=f(4)=8$, $f(2)\cdot f(2)=4\cdot 4=16$

(2) 是同态， $f(x\cdot y)=(x\cdot y)^2=x^2\cdot y^2=f(x)\cdot f(y)$

(3) 是同态， $f(x\cdot y)=1/(x\cdot y)=1/x\cdot 1/y=f(x)\cdot f(y)$

(4) 不是同态，$f(1\cdot 1)=f(1)=-1$, $f(1)\cdot f(1)=(-1)\cdot(-1)=1$

7.2 代数系统

❖ 七、同态映射的分类

- 同态映射f
  - 如果是单射，则称为单一同态（或单同态）；
  - 如果是多对一的映射，则称为多一同态；
  - 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 $V_1 \sim V_2$；
  - 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 $V_1 \cong V_2$.
  - 对于代数系统 V，它到自身的同态称为自同态.
  - 类似地可以定义单自同态、满自同态和自同构.
  - 任意x属于V_1，若$f(x)=e'$,其中e'是V_2的单位元，则f称作零同态

7.2 代数系统

❖ 八、同态映射的实例

(1) 设V=<Z,+>，$\forall a\in$Z，令 f_a : Z→Z，$f_a(x)=ax$

那么 f_a是V的自同态. 因为$\forall x, y\in$Z，有： $f_a(x+y) = a(x+y) = ax+ay = f_a(x)+f_a(y)$

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.

(2) 设V_1=<Q, +>, V_2=<Q*, ·>，其中Q* = Q−{0}，令 f : Q→Q*, $f(x) = e^x$

那么 f 是V_1到V_2的同态映射，因为$\forall x, y\in$Q有： $f(x+y) = e^{x+y} = e^x\cdot e^y = f(x)\cdot f(y)$.

不难看出 f 是单同态.

7.2 代数系统

（3）$V=<Z_6,\oplus>$，$f_p:Z_6\to Z_6$，$f_p(x)=(px)\ \mathrm{mod}\ 6$，$p=0,1,2,3,4,5$

$p=0$，f_0零同态

$p=1$，f_1恒等映射，自同构

$p=2$，$f_2=\{<0,0>,<1,2>,<2,4>,<3,0>,<4,2>,<5,4>\}$，

$p=3$，$f_3=\{<0,0>,<1,3>,<2,0>,<3,3>,<4,0>,<5,3>\}$

$p=4$，$f_4=\{<0,0>,<1,4>,<2,2>,<3,0>,<4,4>,<5,2>\}$

$p=5$，$f_5=\{<0,0>,<1,5>,<2,4>,<3,3>,<4,2>,<5,1>\}$自同构

可以推广到f_p: $Z_n\to Z_n$，存在n个自同态

$f_p(x\oplus y)=(p(x\oplus y))\mathrm{mod}n=(px)\mathrm{mod}n\oplus(py)\mathrm{mod}n=f_p(x)\oplus f_p(y)$

7.2 代数系统

(4) V_1=<Z,+>, V_2=<Z_n,⊕>, f : Z→Z_n,

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

$\forall x, y \in Z$,

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

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

例如，n=3.

$$f(3x)=0,\ f(3x+1)=1,\ f(3x+2) = 2$$

f为满同态.

7.2 代数系统

❖ 九、同态映射的性质

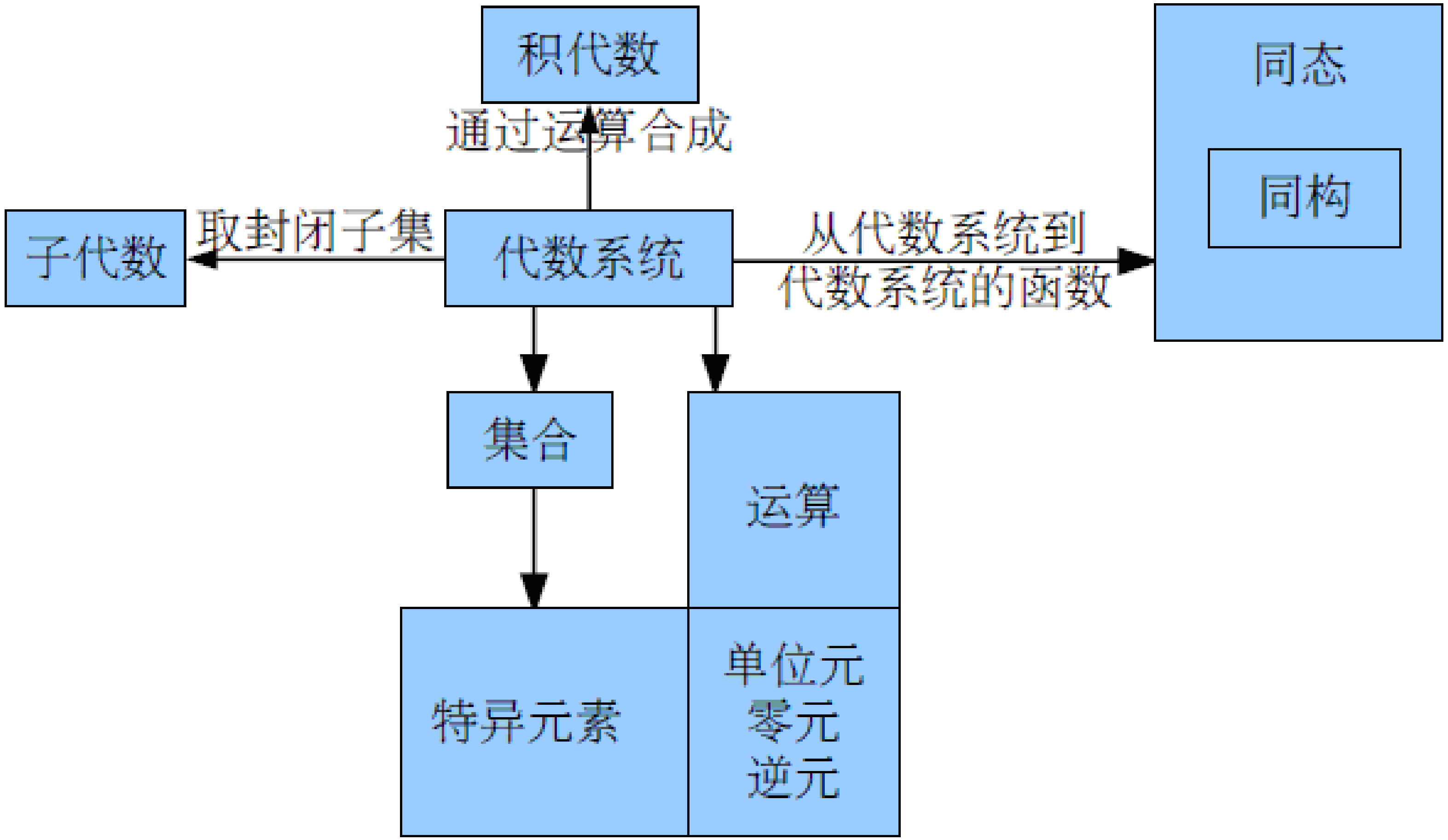
- 设 V_1和 V_2是代数系统，$f: V_1 \to V_2$ 是满同态映射, 则

  - (1)若V_1中的$\circ$运算是可交换 (可结合, 幂等) 的，那么V_2中对应的 $\circ'$ 运算也是可交换 (可结合、幂等的) 的.
  - (2)若V_1中的$\circ$对$*$运算是可分配的，那么V_2中对应的 $\circ'$ 对$*'$ 运算也是可分配的.
  - (3)若V_1中的$\circ$和$*$运算是可吸收的，那么V_2中对应的 $\circ'$ 和$*'$ 运算也是可吸收的.
  - (4)若V_1中$\circ$运算具有单位元 e_1 (或零元θ_1)，那么 $f(e_1)$ (或 $f(\theta_1)$)是V_2中关于对应的$\circ'$运算的单位元 (或零元).
  - (5) 若 x 关于V_1中 $\circ$运算的逆元为 x^{-1}, 那么 $f(x)$在V_2中关于对应的$\circ'$ 运算的逆元为 $f(x^{-1})$.

小结

- 集合和集合上的运算共同构成代数系统。
- 集合中如果存在一些元素在运算中呈现出特定的性质，那么这些元素被称为特异元素（或代数常数）。
- 如果一个代数系统的子集和该代数系统上的运算也构成一个代数系统，则此代数系统是原来代数系统的子代数系统，简称子代数。
- 两个代数系统可以组合成一个新的代数系统——积代数。
- 代数系统之间满足一定条件的函数称为同态。

小结


积代数
通过运算合成
子代数
取封闭子集
代数系统
从代数系统到
代数系统的函数
同态
同构
集合
运算
特异元素
单位元
零元
逆元

常见题型解析

- 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
- 子代数的判定
- 计算积代数
- 判断或证明函数是某一类型的同态

举例

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.

解：(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 $x, y, z\in Q$,

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

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

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

$$= x+y+z+2xy+2xz+2yz+4xyz= (x\circ y)\circ z$$

举例

(2) 求出∘运算的单位元、零元和所有可逆元素的逆元.

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.

举例

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

举例

解：

(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.

举例

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) $f(x) = 2$

(1) $f(x) = |x| +1$ (2) $f(x) = |x|$
(3) $f(x) = 0$ (4) $f(x) = 2$

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 $\mathrm{ran}\, f$ 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 $f(2\times2)=2$, $f(2)\times f(2)=2\times2=4$

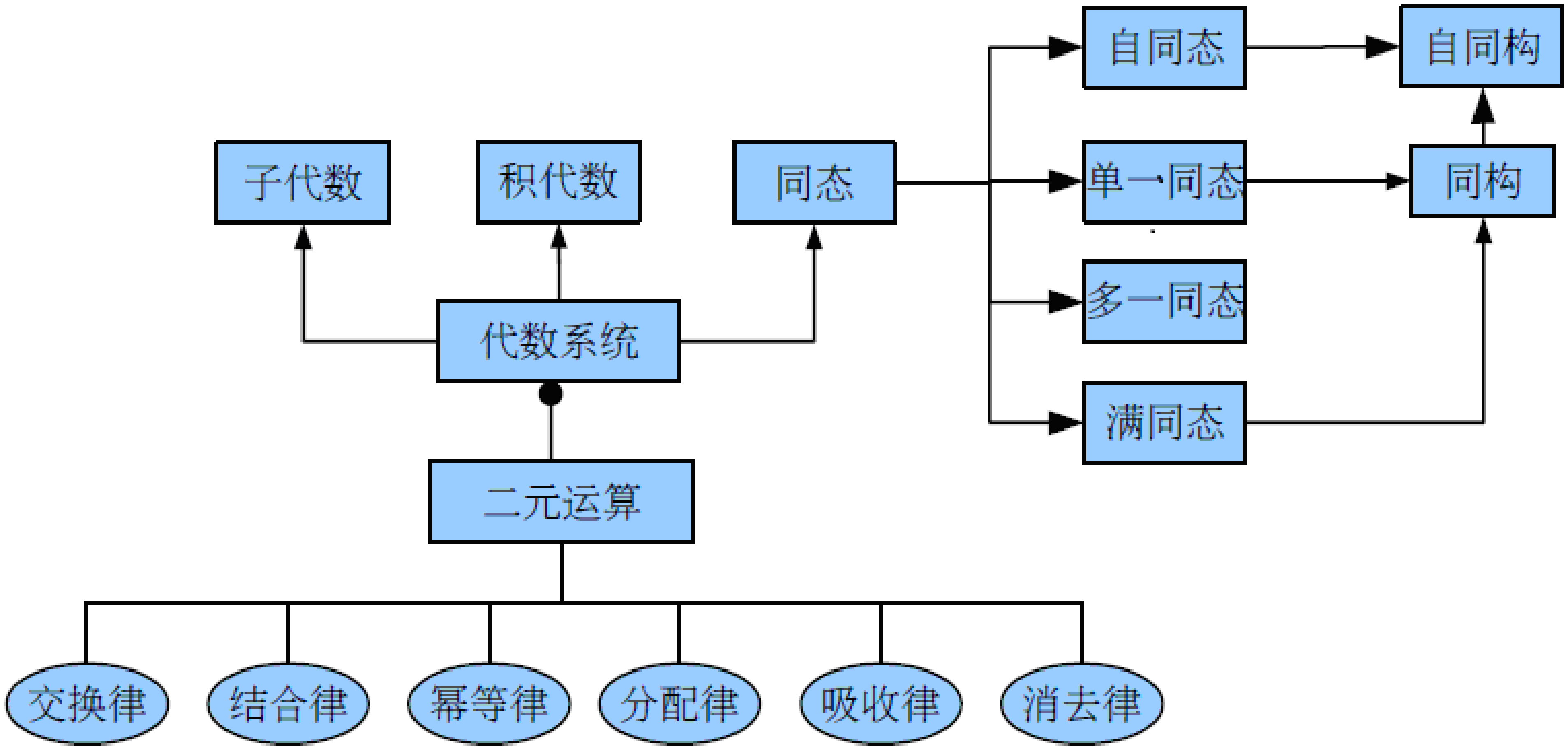
说明：判别或证明同态映射的方法

(1) 先判断（或证明）f 是 G_1 到 G_2 的函数 $f: G_1\to G_2$. 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.

本章小结


自同态
自同构
子代数
积代数
同态
单一同态
同构
多一同态
代数系统
满同态
二元运算
交换律
结合律
幂等律
分配律
吸收律
消去律