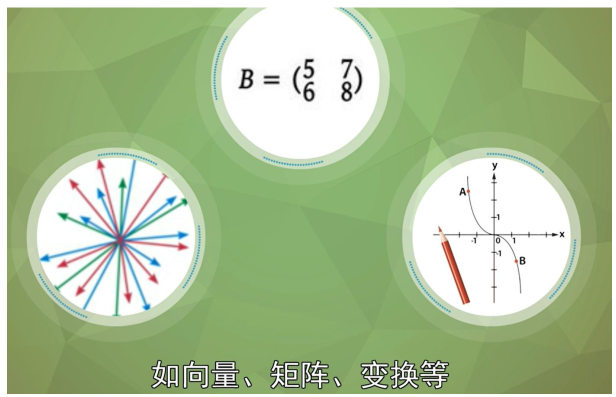
代数系统简介

什么是抽象代数？

- 抽象代数也叫近世代数，产生于19世纪
- 处理各种抽象的公理化代数系统，可以处理除实数、复数以外的集合，例如命题、向量、矩阵、变换等，这些集合有自己的演算定律。



- 抽象代数将各有的演算定律通过抽象手法把共有的内容升华出来，并因此而达到更高层次。


MATH
代数几何
代数数论
代数拓扑
拓扑

- 代数是数学的其中一门分支，大致分为初等代数学和抽象代数学两部分。初等代数学是指19世纪上半叶以前发展的代数方程理论，主要研究某一代数方程（组）是否可解，如何求出代数方程所有的根〔包括近似根〕，以及代数方程的根有何性质等问题。

- 法国数学家伽罗瓦〔1811-1832〕在1832年运用「群」的思想彻底解决了用根式求解多项式方程的可能性问题。他是第一个提出「群」的思想的数学家，一般称他为近世代数创始人。他使代数学由作为解代数方程的科学转变为研究代数运算结构的科学，即把代数学由初等代数时期推向抽象代数即近世代数时期。

群的性质---群方程存在唯一解

定理 G为群，$\forall a,b\in G$，方程 $ax=b$ 和 $ya=b$ 在G中有解且仅有惟一解.

$a^{-1}b$ 是 $ax=b$的解. ba^{-1} 是 $ya = b$ 的唯一解.

例 设 $G=<P(\{a,b\}),\oplus>$，其中$\oplus$为对称差. 群方程

$$\{a\} \oplus X = \varnothing, \qquad Y \oplus \{a,b\} = \{b\}$$

的解 $X = \{a\}^{-1}\oplus\varnothing = \{a\}\oplus\varnothing = \{a\}$,

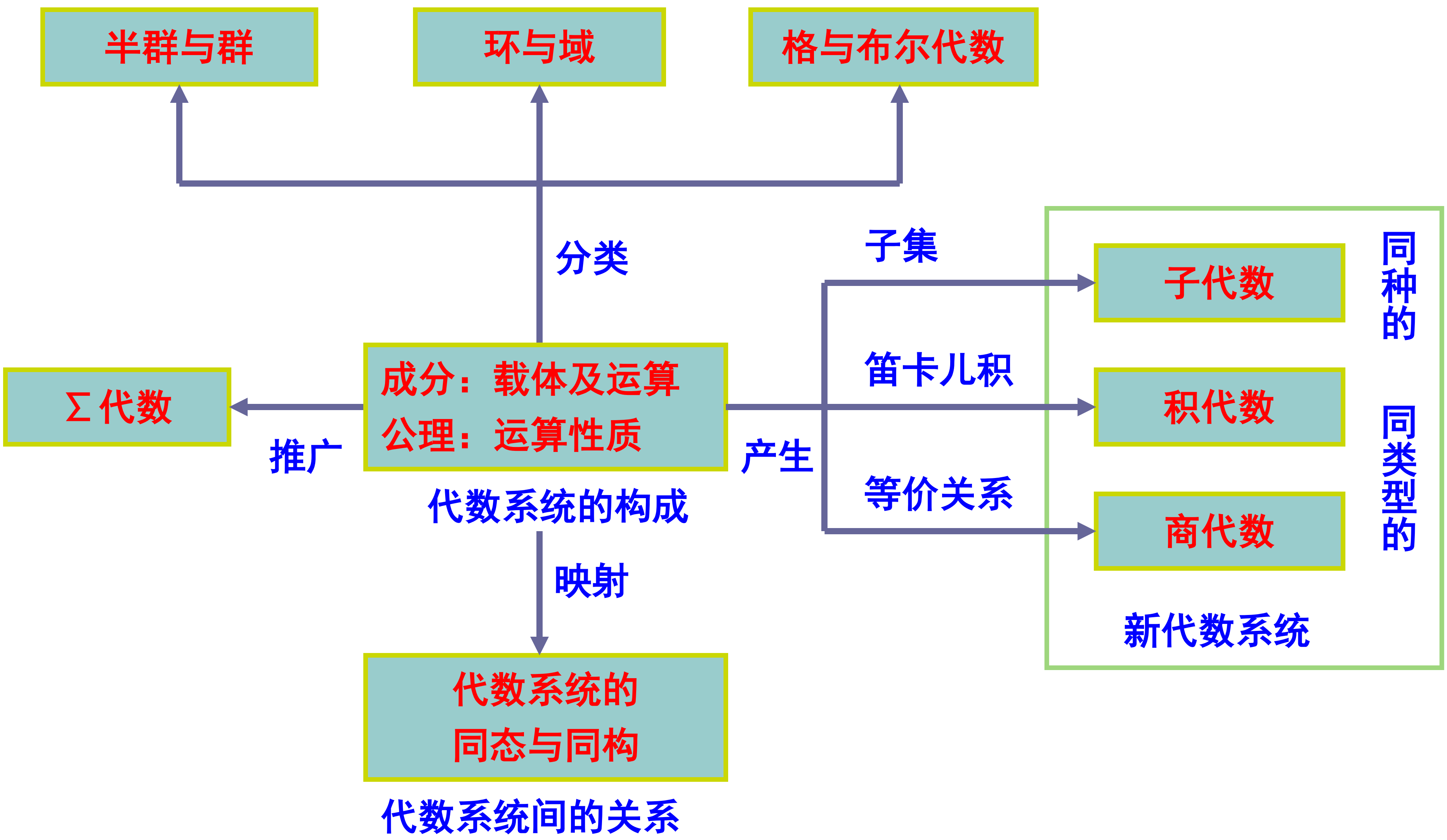
$Y = \{b\}\oplus\{a,b\}^{-1} = \{b\}\oplus\{a,b\} = \{a\}$

人们研究和考察现实世界中的各种现象或过程，往往要借助某些数学工具。我们所接触过的数学结构，连续的或离散的，常常是对研究对象（自然数，实数，多项式，矩阵，命题，集合，图）定义种种 运算（加，减，乘，除，与，或，非，交，并，补等），然后讨论这些对象以及运算有关性质。

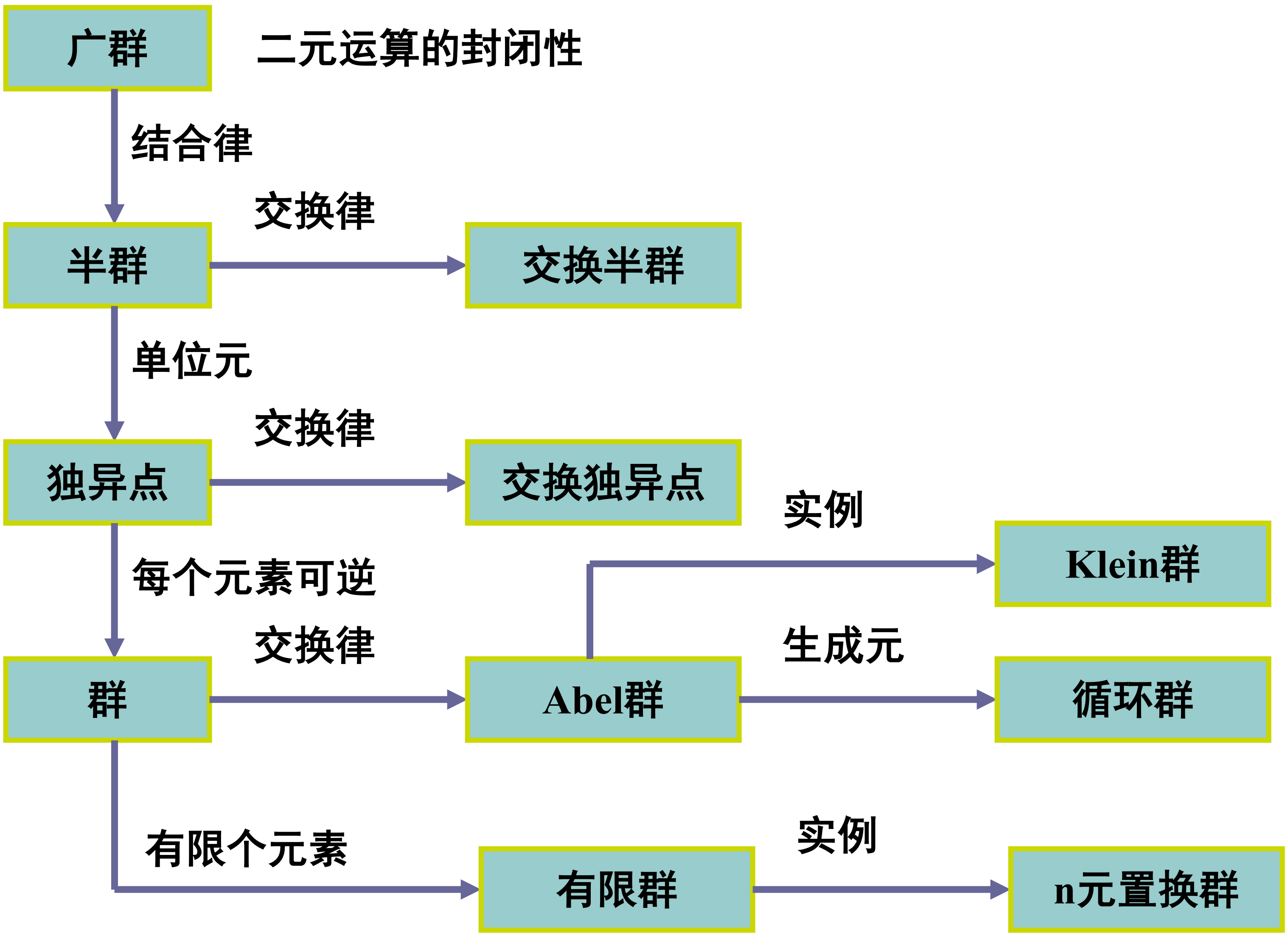
这里我们要研究的是一类特殊的数学结构——由对象集合及运算组成的数学结构，通常称为代数结构。

它在计算机科学中有着广泛的应用。格与布尔代数的理论成为电子计算机硬件设计和通讯系统设计中的重要工具，半群理论在自动机和形式语言研究中发挥了重要的作用，关系代数理论成为最流行的数据库的理论模型；有限域的理论是编码理论的数学基础，在通讯中发挥了重要作用。在计算机算法设计和分析中，代数算法研究占有主导地位，因为它便于形式描述、正确性和终止性证明以及复杂性分析…..

代数结构的知识体系


半群与群
环与域
格与布尔代数
分类
子集
子代数
同种的
笛卡儿积
积代数
同类型的
Σ代数
推广
成分：载体及运算
公理：运算性质
代数系统的构成
产生
等价关系
商代数
新代数系统
映射
代数系统的
同态与同构
代数系统间的关系

群与半群


广群
二元运算的封闭性
结合律
交换律
半群
交换半群
单位元
交换律
独异点
交换独异点
实例
Klein群
每个元素可逆
交换律
生成元
群
Abel群
循环群
有限个元素
实例
有限群
n元置换群

第9章 代数系统简介

- 9.1 二元运算及其性质
- 9.2 代数系统
- 9.3 几个典型的代数系统

9.1 二元运算及其性质

- 二元运算及一元运算的定义
- 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

定义（运算）

设A是非空集合，映射$f:A \times A \times \ldots \times A \to A$称为集合$A$上的$n$元运算。

讨论抽象运算时，"运算"常记为"*"、"。"等。

设*是二元运算，如果a与b运算得到c，记作$a*b=c$；

若*是一元运算，a的运算结果记作$*a$或$*(a)$。

一个运算是否为集合A上的运算必须满足以下两点：

①A中任何元素都可以进行这种运算，且运算的结果是惟一的。

②A中任何元素的运算结果都属于A。

A中任何元素的运算结果都属于A通常称为运算在A是封闭的。

Problem: 自然数集合上的普通加法和减法是不是自然数集合上的二元运算？为什么？

f：$N\times N\rightarrow N$，定义为：$\forall m,n\in N$，$f(m,n)=m+n$，f 是自然数集合N上的二元运算。

f：$N\times N\rightarrow N$，定义为：$\forall m,n\in N$，$f(m,n)=m-n$，普通减法不是自然数集合N上的二元运算。

【例1】设N为自然数集合，$*$和$\circ$ 是$N\times N$到N映射，规定为：$\forall m,n\in N$,

$$m*n=\min\{m,n\}$$
$$m\circ n=\max\{m,n\}$$

则$*$ 和$\circ$ 是N上的二元运算。

【例2】设$N_k=\{0,1,\cdots,k-1\}$。N_k上的二元运算$+_k$定义为：对于N_k中的任意两个元素i和j，有

$$i+_k j=\begin{cases} i+j & i+j<k \\ i+j-k & i+j\geq k \end{cases}$$

称二元运算$+_k$为模k加法。

N_k上的二元运算$\times_k$定义为：对于N_k中的任意两个元素i和j，有

$$
i \times_k j = \begin{cases} i \times j & i \times j < k \\ i \times j \text{除以} k \text{的余数} & i \times j \geq k \end{cases}
$$

称二元运算$\times_k$为模k的乘法。

模k加法$+_k$和模k乘法$\times_k$是两种重要的二元运算。

在$N_7=\{0,1,2,3,4,5,6\}$中，有$4+_7 2=6$，$4+_7 5=2$。

如果把N_7中的元素：0，1，2，3，4，5，6分别看作是：星期日、星期一、星期二、星期三、星期四、星期五、星期六。
那么$4+_7 2=6$可解释为：星期四再过两天后是星期六；$4+_7 5=2$可解释为：星期四再过五天后是星期二。

2. 运算的表示

表示运算的方法有两种：解析公式和运算表

(1)解析公式是指用运算符号和运算对象组成的表达式。

$$f(a)=\frac{1}{a}\ , \qquad i +_k j = \begin{cases} i+j & i+j<k \\ i+j-k & i+j\geq k \end{cases}$$

(2) 运算表是指运算对象和运算结果构成的二维表。当有限集合上的二元运算不能用表达式简明地表示时，借助于运算表来定义二元运算会带来方便。

设$N4$={0,1,2,3}，$N4$上的模4加法$+_4$可以用运算表表示，它的运算表如表6.1所示。$N4$上的模4乘法$\times_4$也可以用运算表表示，它的运算表如表6.2所示。

表6.1

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

表6.2

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

定义 （代数系统）

一个非空集合A连同若干个定义在该集合上的运算$*_1, *_2, \cdots, *_k$所组成的系统称为一个代数系统，记作$<A, *_1, *_2, \cdots, *_k>$。

一个代数系统需要满足下面两个条件：

①有一个非空集合A。

②有一些定义在集合A上的运算。

【例3】设B是一个集合，$A=P(B)$是B的幂集合。$<A,\cup,\cap,\sim>$构成一个代数系统，该代数系统称为集合代数。

【例4】设$R-\{0\}$是全体非零实数集合，$*$是$R-\{0\}$上二元运算，定义为：$\forall a,b\in R-\{0\}$，$a*b=b$。则$<R-\{0\},*>$是代数系统。

二元运算的性质（交换律）

定义 设 $\circ$ 为 S 上的二元运算，如果对于任意的 $x, y \in S$ 有

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

则称运算在 S 上满足**交换律**.

例如，设R为实数集合，对于任意的$a,b\in R$，规定

$$a * b=(a-b)^2$$

$$a \circ b=a^2+b^2$$

$$a \cdot b=a+b-ab$$

则运算$*$ 、$\circ$ 和$\cdot$都是可交换的。

二元运算的性质（结合律）

定义 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**.

- 实数集合上的普通加法和乘法是二元运算，满足结合律；

  矩阵的加法和乘法也是二元运算，也满足结合律；

二元运算*在A满足结合律时$(x*y)*z=x*(y*z)=x*y*z$。这样，可以令

$$a^n = \overbrace{a * a * \cdots * a}^{n\text{个}}$$

当运算*满足结合律时，a^n的也可以递归定义如下：

(1)$a^1=a$

(2)$a^{n+1}=a^n* a$

由此利用数学归纳法，不难证明下列的公式：

(1)$a^m* a^n= a^{m+n}$

(2)$(a^m)^n= a^{mn}$

二元运算的性质（幂等律）

定义 设$*$是非空集合A上的二元运算，如果对于任意的$a \in A$，有$a* a=a$，则称运算$*$是幂等的。如果A的某个元素a满足$a* a=a$，则称a为运算$*$的幂等元。

集合的并、交运算满足幂等律，每一个集合都是幂等元。

定理 设$*$ 是非空集合A上的二元运算，a为运算$*$的幂等元，对任意的正整数n，则$a^n=a$。

•

实例分析

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	函数符合∘	无	有	无

二元运算的性质（分配律）

定义 设$*$和$\circ$是非空集合A上的两个二元运算，如果对于任意$a,b,c \in A$，有

$$a*(b\circ c)=(a*b)\circ(a*c) \quad (\text{左分配律})$$

$$(b\circ c)*a=(b*a)\circ(c*a) \quad (\text{右分配律})$$

则称运算$*$对运算$\circ$是可分配的。

定理 设$*$和$\circ$是非空集合A上的两个二元运算，$*$是可交换的。如果$*$对于运算$\circ$满足左分配律或右分配律，则运算$*$对于运算$\circ$是可分配的。

证明：设$*$对于运算$\circ$满足左分配律，且$*$是可交换的，则对于任意$a,b,c \in A$，有

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

即 $$(b \circ c) * a = (b * a) \circ (c * a)$$

故$*$对于运算$\circ$是可分配的。

同理可证另一半。

二元运算的性质（吸收律）

定义 设$*$和$\circ$ 是非空集合A上的两个可交换的二元运算，如果对于任意$a,b\in A$，有

$$a*(a\circ b)=a$$

$$a\circ (a*b)=a$$

则称运算$*$ 和运算$\circ$ 满足吸收律。

【例】设N为自然数集合，$*$和$\circ$ 是集合N上的二元运算，定义为：$\forall a \in N$，$\forall b \in N$

$$a*b=\max(a,b)，\quad a\circ b=\min(a,b)$$

验证运算$*$和$\circ$ 适合吸收律。

解：$\forall a \in N$，$\forall b \in N$

若$a>b$，$a*(a\circ b)=a*\min(a,b)=a*b=\max(a,b)=a$

若$a<b$，$a*(a\circ b)=a*\min(a,b)=a*a=\max(a,a)=a$

若$a=b$，$a*(a\circ b)=a*\min(a,b)=a*a=\max(a,a)=a$

即 $a*(a\circ b)=a$ 同理可证$a\circ (a*b)=a$

因此运算$*$和$\circ$ 适合吸收律。

实例分析

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 + 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 ⊕ 对 ∩ 不分配	无

二元运算的特异元素（单位元）

定义 设* 是定义在集合A上的二元运算，
如果有一个$e_l \in A$，对于任意的$a \in A$，有$e_l * a = a$，
则称e_l为左单位元；

如果有一个$e_r \in A$，对于任意的$a \in A$，有$a * e_r = a$，
则称e_r为右单位元；

如果在A中有一个元素e，它既是左单位元又是右单位元，则称e为A中关于运算* 的单位元。

定理 设$*$ 是定义在集合A上的二元运算，e_l为A中关于运算$*$ 的左幺元，e_r为A中关于运算$*$ 的右幺元，则$e_l=e_r=e$，且A中的单位元是惟一的。

证明：

（左单位元和右单位元相等）

$e_l=e_l* \ e_r=e_r=e$

（单位元唯一）

设另一幺元$e_1\in A$，则$e_1=e_1* \ e=e$

在实数集R中，对于乘法运算，1是单位元；

集合E的幂集，对于并运算， 空集是单位元；

集合E的幂集，对于交运算，E是单位元。

在命题集合中，对于析取运算，？是单位元；
对于合取运算，？是单位元。

矛盾式是析取的单位元；

重言式是合取的单位元。

二元运算的特异元素（零元）

定义　设$*$ 是集合A上的二元运算，
如果有一个$\theta l \in A$，对于任意的$a \in A$,
有$\theta l * a=\theta l$，称θl为A中关于运算$*$ 的左零元；

如果有一个$\theta r \in A$，对于任意的$a \in A$,
有$a * \theta r=\theta r$，称θr为A中关于运算$*$ 的右零元；

如果A中有一个元素$\theta \in A$，它既是左零元又是右零元，则称θ为A中关于运算$*$ 的零元。

在实数集R中，对乘法运算，？是零元；
集合E的幂集，对于并运算， ？是零元；
集合E的幂集，对于交运算，？是零元；
在命题集合中，对于析取运算，？是零元；对于合取运算，？是零元。

0，E，空集，重言式，矛盾式

定理 设* 是集合A上的二元运算，θ_l为A中关于运算* 的左零元，θ_r为A中关于运算* 的右零元，则$\theta_l=\theta_r=\theta$，且A中的零元是惟一的。

证明：

（左零元等于右零元）

$\theta_l=\theta_l* \ \theta_r=\theta_r=\theta$

（零元唯一）

$\theta_1\in A$，则$\theta_1=\theta_1 * \ \theta=\theta$

定理（单位元和零元的关系）

设$*$ 是集合A （$|A|>1$）上的二元运算.

如果A中存在单位元e和零元θ，则$e\neq\theta$。

证明：用反证法。

设$e=\theta$，那么对于任意的$a\in A$，必有

$$a=e*a=\theta*a=\theta,$$

于是A中的所有元素都是零元θ，与A中至少有两个元素矛盾。

二元运算的特异元素（逆元）

定义 设$*$ 是集合A上的二元运算，e为A中关于运算$*$ 的单位元。对于A中的元素a，
如果存在A中的元素b，使得$b* a=e$，那么称b为a的左逆元；

如果存在A中的元素b，使得$a* b=e$，那么称b为a的右逆元；

如果存在着A中的元素b，既是a的左逆元又是a的右逆元，那么称b为a的逆元。记为$b=a^{-1}$。
如果$a\in A$存在逆元$a^{-1}\in A$，那么称a为可逆元。。

(1)一个元素的左逆元不一定等于该元素的右逆元。

(2)一个元素可以有左逆元而没有右逆元，同样可以有右逆元而没有左逆元。

(3)一个元素的左逆元或者右逆元还可以不是惟一的。

(4)单位元必有逆元，其逆元为其自身

在自然数集合中，对于数乘运算，只有1有逆元1；

在整数集合中，对于数加运算，每个元素有逆元；

在P(A)中，对于并运算，每个元素B（非空集合）均无逆元；

定理 设$*$为A中的一个二元运算，A中存在单位元e且每个元素都有左逆元。如果$*$是可结合的运算，则在A中任何元素的左逆元等于该元素的右逆元，且每个元素的逆元是惟一的。

证明： 设$a,b,c\in A$，b是a的左逆元，c是b的左逆元。于是 $(b*a)*b=e*b=b$，所以

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

因此，b也是a的右逆元。

设元素a有两个逆元b和d，那么

$$b=b*e=b*(a*d)=(b*a)*d=e*d=d$$

故a的逆元是惟一的。

二元运算的特异元素（可消元）

定义 设$*$ 是集合A上的二元运算，θ为A中关于运算$*$ 的零元，$\forall b,c \in A$，$a \neq \theta$。如果

(1)若$a*b=a*c$，便有$b=c$，则称运算$*$ 满足左消去律，称a为运算$*$ 的左可消元。

(2)若$b*a=c*a$，便有$b=c$，则称运算$*$ 满足右消去律，称a为运算$*$ 的右可消元。

若运算$*$ 既满足左消去律又满足右消去律，则称运算$*$ 满足消去律，称a为运算$*$ 的可消元。

定理（**非零元的可逆元即为可消元**）
设$*$ 是A中可结合的二元运算，如果a的逆存在且$a\neq\theta$，则a为关于$*$ 的可消元。

证明： 设$b,c\in A$，且有$a*b=a*c$或$b*a=c*a$。由于$*$ 为可结合的二元运算、a的逆存在且$a\neq\theta$，则

$$a^{-1}*(a*b)=(a^{-1}*a)*b=e*b=b$$

$$a^{-1}*(a*c)=(a^{-1}*a)*c=e*c=c$$

而

$$a^{-1}*(a*b)=a^{-1}*(a*c)$$

于是$b=c$，同理由$b*a=c*a$，得$b=c$，故a为关于$*$ 的可消元。

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)
$M_n(\mathrm{R})$	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

例题分析

【例】实数集R上二元运算$a*b=a+b-ab$是否有单位元，零元和幂等元？若有单位元，哪些元素有逆元？

解：运算$*$的定义为：$a*b=a+b-ab$

(1) 若e是单位元，则对任意元素$a\in R$，有$a*e=e*a=a$，由于元素$*$是可交换的，仅考虑$e*a=a$，

即$e*a=e+a-ea=a$，于是$e-ea=0$，即$e(1-a)=0$。由于a是任意的，要使上式成立，只有$e=0$。因此0是运算$*$的单位元。

(2)若θ是零元，则对任意元素$a \in R$，有$a * \theta = \theta * a = \theta$。仅考虑$\theta * a = \theta$，即$\theta * a = \theta + a - \theta a = \theta$，于是$a - a\theta = 0$，即$a(1-\theta)=0$。由于$a$是任意的，要使上式成立，只有$\theta=1$。因此1是运算$*$的零元。

(3)若$a \in R$是幂等元，则应有$a * a = a$，即$a+a-a^2=a$。于是$a-aa=0$，即$a(1-a)=0$。要使上式成立，只有$a=0$或$a=1$。因此0或1是运算$*$的幂等元。

(4)设b是a的逆元，则应有$a * b = a+b-ab=0$($*$的单位元)，于是$b=\dfrac{a}{a-1}$，因此对于R中的任何元素a(只要$a \neq 1$)均有逆元，其逆元是$\dfrac{a}{a-1}$。

例题分析

例 设 $\circ$ 运算为 Q 上的二元运算，

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

(1) $\circ$ 运算是否满足交换和结合律？说明理由.

(2) 求 $\circ$ 运算的单位元、零元和所有可逆元.

解 (1) $\circ$ 运算可交换，可结合. 任取$x, y\in \mathrm{Q}$,

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

任取$x, y, z\in \mathrm{Q}$,

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

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

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

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

例题分析（续）

(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， $y = -\dfrac{x}{1+2x}$ 是 x 的逆元.

例题分析（续）

例 (1) 说明那些运算是交换的、可结合的、幂等的.
(2) 求出运算的单位元、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

∘	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c

•	a	b	c
a	a	b	c
b	b	c	c
c	c	c	c

解 (1) $*$ 满足交换、结合律；∘ 满足结合、幂等律；
• 满足交换、结合律.

(2) $*$ 的单位元为 b, 没零元， $a^{-1} = c, b^{-1} = b, c^{-1} = a$
∘ 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不可逆.

例题分析（续）

例 设 $A = \{ a, b, c \}$, 构造 A 上的二元运算* 使得 $a*b = c$, $c*b = b$, 且*运算是幂等的、可交换的，给出关于*运算的一个运算表，说明它是否可结合，为什么？

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

根据幂等律和已知条件$a*b = c$, $c*b = b$ 得到运算表

根据交换律得到新的运算表

方框 □ 可以填入a, b, c中任一选定的符号, 完成运算表

不结合，因为 $(a*b)*b = c*b = b$, $a*(b*b) = a*b = c$

由运算表判别算律的一般方法

- 交换律：运算表关于主对角线对称
- 幂等律：主对角线元素排列与表头顺序一致
- 消去律：所在的行与列中没有重复元素
- 单位元：所在的行与列的元素排列都与表头一致
- 零元：元素的行与列都由该元素自身构成
- A 的可逆元：a 所在的行中某列 (比如第 j 列) 元素为 e，且第 j 行 i 列的元素也是 e，那么 a 与第 j 个元素互逆
- 结合律：除了单位元、零元之外，要对所有3个元素的组合验证表示结合律的等式是否成立

本小节学习目标：

- 会判断是否为二元运算（结果唯一、封闭）；
- 会判断或者证明二元运算的性质（交换律、结合律、幂等律、分配律、吸收律）；
- 会求二元运算的特异元素（单位元、零元、逆元、可消元）