

离散数学：抽象代数：引言

陈斌 北京大学地球与空间科学学院 gischen@pku.edu.cn

什么是代数

- › **算术** arithmetic
 - › 研究整数、有理数、实数和复数的加、减、乘、除等**具体**运算法则和性质
- › **代数** algebra
 - › 算术的**一般化**，允许用字母等符号来代替数进行运算
 - › 运用算术规律，研究不特定的数性质
 - › 含有未知数的方程和解方程

北京大学地球与空间科学学院/陈斌/2015

代数结构和抽象代数

- › **代数结构** algebraic structure
 - › 在一个对象集合上定义若干**运算**，并设定若干**公理**描述**运算的性质**
- › **抽象代数** abstract algebra
 - › 抛弃代数结构中对对象集合与运算的**具体意义**
 - › 研究运算的**一般规律**（交换、结合、分配）
 - › 研究针对运算的**特殊对象**及其性质
 - › 并对代数结构进行**分类**，研究其关系

北京大学地球与空间科学学院/陈斌/2015

离散数学：抽象代数：代数结构

陈斌 北京大学地球与空间科学学院 gischen@pku.edu.cn

什么是运算operator

- › 运算是 S^n 到 S 的一个**函数**，称为 **n 元运算**
- › 常用 $*$ 表示**二元运算**， $*(x,y)$ 常记做 $x*y$
- › 常用 Δ 表示**一元运算**

北京大学地球与空间科学学院/陈斌/2015

运算的基本性质

- › **普遍性**： S 中的所有元素都可参加运算
- › $\forall x \forall y \exists z (x*y=z)$
- › **单值性**：相同的元素运算结果也**相同且唯一**
- › $\forall x \forall y \forall x' \forall y' (x=x' \wedge y=y' \rightarrow x*y=x'*y')$
- › **封闭性**：任何元素参加运算的**结果**也是 S 中的元素
- › $\forall x \forall y \exists z (x*y=z \rightarrow z \in S)$

北京大学地球与空间科学学院/陈斌/2015

二元运算的一般性质

- 结合律, 如果二元运算满足:
 $\forall x \forall y \forall z (x, y, z \in S \rightarrow x^*(y^*z) = (x^*y)^*z)$
- 交换律, 如果满足
 $\forall x \forall y (x, y \in S \rightarrow x^*y = y^*x)$
- *运算对#运算满足分配律
 $\forall x \forall y \forall z (x, y, z \in S \rightarrow x^*(y\#z) = (x^*y)\#(x^*z))$

北京大学地球与空间科学学院/陈斌/2015

运算的例子

- 加法、乘法是自然数集合上的二元运算
- 求负是有理数集合上的一元运算
- 减法、除法不是自然数集合上的二元运算
- 除法甚至不是有理数、实数集合上的二元运算 (除以0无意义)
- 加法、乘法满足结合律、交换律
- 减法不满足结合律、交换律
- 乘法对加法、减法满足分配律

北京大学地球与空间科学学院/陈斌/2015

代数结构的定义

- 非空集合S, 称作代数结构的载体
- 载体S上的若干运算
- 一组刻画载体上各运算性质的公理

北京大学地球与空间科学学院/陈斌/2015

代数结构的例子

- $\langle N, + \rangle$ 是一个代数结构
- 所有 2×2 实数矩阵M, 矩阵乘法*, $\langle M, * \rangle$
- $\langle p(A), \cup, \cap, \sim \rangle$, A幂集, 并、交、补运算, 是一个代数结构
- A上的所有划分, 积划分、和划分运算
- A上的等价关系, 交集、并集+传递闭包运算
- X上的所有函数, 函数合成运算
- X上的所有双射函数, 函数求逆运算

北京大学地球与空间科学学院/陈斌/2015

离散数学：抽象代数：幺元

陈斌 北京大学地球与空间科学学院 gisichen@pku.edu.cn

幺元(identity element)的定义

- 代数结构 $\langle S, * \rangle$ 中的元素e, 如果对任意x, 满足下面的条件:
 $\forall x (x^*e = e^*x = x)$
- 则称e为幺元。
- 如果仅满足
 $\forall x (x^*e_r = x)$, 称作右幺元
- $\forall x (e_l^*x = x)$, 称作左幺元

北京大学地球与空间科学学院/陈斌/2015

么元的例子

- › $\langle \mathbb{N}, + \rangle$ 中的 0 是么元
- › $\langle \mathbb{N}, \times \rangle$ 中的 1 是么元
- › $\langle \rho(A), \cup \rangle$ 中的 \emptyset 是么元
- › $\langle \rho(A), \cap \rangle$ 中的 A 是么元
- › $\langle X \text{ 上的所有函数}, \text{函数合成运算} \rangle$ 中恒等函数 I_X 是么元

么元的性质

- › 一般情况下，左右么元可能是不同元素，也可能有多个
- › 如果存在么元，那么么元是唯一的，而且同时是左右么元
- › 证明： $e_1 = e_1 * e_2 = e_2$

离散数学：抽象代数：零元

陈斌 北京大学地球与空间科学学院 gischen@pku.edu.cn

零元(zero element)的定义

- › $\langle S, * \rangle$ 中的元素 o ，如果对任意 x ，满足下面的条件
- › $\forall x (x * o = o * x = o)$
- › 则称 o 为零元
- › 如果仅满足：
- › $\forall x (x * o_i = o_i)$ ，称作右零元
- › $\forall x (o_l * x = o_l)$ ，称作左零元

零元的例子

- › $\langle \mathbb{N}, + \rangle$ 中没有零元
- › $\langle \mathbb{N}, \times \rangle$ 中 0 为零元
- › $\langle \rho(A), \cup \rangle$ 中 A 是零元
- › $\langle \rho(A), \cap \rangle$ 中的 \emptyset 是零元

零元的性质

- › 左右零元有和左右么元相似的性质：
- › 如果存在则唯一： $o_1 = o_1 * o_2 = o_2$
- › 对于一个二元运算：
- › 可能同时有零元和么元；
- › 也可能只有零元或么元；
- › 也可能既没有零元，也没有么元

离散数学：抽象代数：逆元

陈斌 北京大学地球与空间科学学院 gischen@pku.edu.cn

逆元(inverse element)的定义

- › $\langle S, * \rangle$ 中有幺元 e ，如果 $x * y = e$
- › 那么 x 称作 y 的左逆元， y 为 x 的右逆元
- › 如果 $x * y = y * x = e$ ，那么 x, y 互称逆元
- › x 的逆元通常记做 x^{-1}
- › 如果运算被称为“加法”的话， x 的逆元可以记做 $-x$
- › 逆元是载体元素之间的关系

北京大学地球与空间科学学院/陈斌/2015

逆元的例子

- › $\langle \mathbb{I}, +, \times \rangle$ ，加法幺元是 0 ，每个整数 (x) 都有加法逆元 ($-x$)，乘法幺元是 1 ，只有 $1, -1$ 有乘法逆元
- › $\langle \mathbb{Q}, +, \times \rangle$ ，加法幺元是 0 ，每个有理数 (x) 都有加法逆元 ($-x$)，乘法幺元是 1 ，除 0 以外，都有乘法逆元 ($1/x$)
- › $\langle A^A, \circ \rangle$ ， $A^A = \{f | f: A \rightarrow A\}$ ，幺元是恒等函数 E_A ，所有双射函数的逆元是其逆函数；
- › 所有单射函数都有左逆函数，是左逆元；
- › 所有满射函数都有右逆函数，是右逆元

北京大学地球与空间科学学院/陈斌/2015

零元的逆元

- › 多于1个元素的载体集上零元没有逆元
- › $\langle S, * \rangle$ 有幺元 e ，零元 o ，并且 $|S| > 1$ ，那么 o 没有左 (右) 逆元
- › 首先 $o \neq e$ ，否则 S 中另外有非 o/e 的元素 a
- › $o = o * a = e * a = a$ ，矛盾
- › 如果 o 有左 (右) 逆元 x ，那么
- › $o = x * o (o * x) = e$ ，与 $o \neq e$ 矛盾

北京大学地球与空间科学学院/陈斌/2015

逆元唯一性

- › 满足结合律的代数结构中，逆元唯一
- › $\langle S, * \rangle$ 有幺元 e ，且 $*$ 运算满足结合律
- › 如果元素 x 有左逆元 l ，右逆元 r
- › 那么 $l = r = x^{-1}$
- › 证明：
- › $l = l * e = l * (x * r) = (l * x) * r = e * r = r = x^{-1}$

北京大学地球与空间科学学院/陈斌/2015

离散数学：抽象代数：可约元素

陈斌 北京大学地球与空间科学学院 gischen@pku.edu.cn

可约(cancelable)元素

- › $\langle S, * \rangle$ 中元素 a ，如果对任意 $x, y \in S$ 有
- › $a * x = a * y$ 蕴涵 $x = y$ (左可约)
- › $x * a = y * a$ 蕴涵 $x = y$ (右可约)
- › 那么 a 称为可约的
- › 可约是载体元素的一种性质

可约性质

- › 满足结合律的代数结构中，有逆元的元素可约
- › $\langle S, * \rangle$ 中 $*$ 运算满足结合律，且元素 a 有逆元：
- › $a * x = a * y \vdash$
- › $a^{-1} * (a * x) = a^{-1} * (a * y) \vdash$
- › $(a^{-1} * a) * x = (a^{-1} * a) * y \vdash x = y$
- › $x * a = y * a \vdash$
- › $(x * a) * a^{-1} = (y * a) * a^{-1} \vdash$
- › $x * (a * a^{-1}) = y * (a * a^{-1}) \vdash x = y$
- › 因此， a 是可约的。

离散数学：抽象代数：同构与同态

陈斌 北京大学地球与空间科学学院 gischen@pku.edu.cn

两个代数结构

- › $\langle \{A, \emptyset\}, \cup \rangle$, $\langle \{1, 0\}, \vee \rangle$
- › 除了符号之外，结构完全相同
- › 可以通过符号的变换 (一一映射) 相互转化

\cup	\emptyset	A
\emptyset	\emptyset	A
A	A	A

\vee	0	1
0	0	1
1	1	1

代数结构之间的相似关系

- › 同类型代数结构：
- › $|S| = |S'|$ ，并且，运算的元数相同
- › 同构的代数结构
- › 存在 $S \rightarrow S'$ 的一一映射 h
- › S 中运算的像等于运算数像在 S' 的运算结果
- › $h(x * y) = h(x) *' h(y)$
- › 其中 $*$ 是 S 上的运算，而 $*$ ' 是 S' 上的运算

同态映射(homomorphism)

- › 代数结构之间，更为一般性的相似关系
- › 对于代数结构 $\langle S, \Delta, \# \rangle$ 和 $\langle S', \Delta', \#' \rangle$ ，如果有函数 $h: S \rightarrow S'$ ，对 S 中任意元素 a, b
- › $h(\Delta a) = \Delta'(h(a))$, $h(a \# b) = h(a) \#' h(b)$
- › 函数 h 就称作代数结构 S 到 S' 的同态映射
- › 如果 h 是单射函数，称作单一同态
- › 如果 h 是满射函数，称作满同态
- › 如果 h 是双射函数，称作同构映射 isomorphism

同态映射

- 同态映射表明了两个代数结构之间的相似、等效的关系
- 例子：
 - $\langle R, + \rangle$ 和 $\langle R, \times \rangle$ 之间
 - 存在**单一同态映射** $f(x) = 2^x$
 - $f(x+y) = 2^{x+y} = 2^x \times 2^y = f(x) \times f(y)$
 - 上面的 $\langle R, \times \rangle$ 改成 $\langle R^+, \times \rangle$
 - 则 f 是**同构映射**, $\langle R, + \rangle$ 和 $\langle R^+, \times \rangle$ 是同构的

北京大学地球与空间科学学院/陈域/2015

满同态映射例子

- $\langle \Sigma^*, \text{连接} \rangle$ 和 $\langle \mathbb{N}, + \rangle$ 之间
- 存在**满同态映射** $\text{length}(w) = ||w||$
- $\text{length}(u \text{ 连接 } v) = ||u \text{ 连接 } v|| =$
- $||u|| + ||v|| = \text{length}(u) + \text{length}(v)$
- 表明了字符串连接和自然数加法之间的相似性
- 可以用连接操作来模拟加法运算, 如DNA计算中的片段连接。

北京大学地球与空间科学学院/陈域/2015

离散数学：抽象代数：同余关系

陈域 北京大学地球与空间科学学院 gischen@pku.edu.cn

同余关系congruence relation

- 代数结构 $\langle S, \Delta, * \rangle$ 中, S 上的一个等价关系 \sim , 如果满足：
 - $a \sim b$ 蕴涵 $a \sim \Delta b$, 称 \sim 是 S 上关于一元运算 Δ 的同余关系
 - $a \sim b, c \sim d$ 蕴涵 $a * c \sim b * d$, 称 \sim 是 S 上关于二元运算 $*$ 的同余关系
 - 如果 \sim 是代数结构上所有的运算的同余关系, 则称 \sim 是 $\langle S, \Delta, * \rangle$ 上的同余关系

北京大学地球与空间科学学院/陈域/2015

同余类

- 同余关系体现了运算保持**等价类**的性质
- 等价类 $[x]$ 称作同余类
- 例子：
 - 相等关系显然是同余关系
 - 模 k 相等是关于整数运算 (加、乘、减、负) 的同余关系

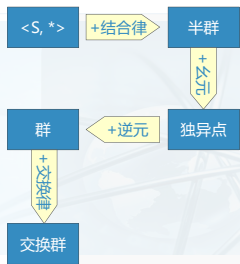
北京大学地球与空间科学学院/陈域/2015

离散数学：抽象代数：群环域

陈域 北京大学地球与空间科学学院 gischen@pku.edu.cn

各种类型的代数结构

- › **半群** semigroup
- › 运算满足**结合律**的代数结构
- › **独异点** monoid
- › 含有**么元**的半群
- › **群** group
- › 半群；有么元；每个元素都有逆元
- › 群没有零元（零元没有逆元）
- › **交换群**（阿贝尔群 Abel group）
- › 满足交换律的群



各种类型的代数结构

- › **环** ring : $\langle R, +, * \rangle$, 有两个二元运算
- › $\langle R, + \rangle$ 是阿贝尔群
- › $\langle R, * \rangle$ 是半群
- › $*$ 对 $+$ 可分配 : $a*(b+c) = a*b + a*c$
- › **域** field : $\langle F, +, * \rangle$
- › $\langle F, +, * \rangle$ 是环
- › $\langle F - \{0\}, * \rangle$ 为交换群