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

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

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

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
- $\forall x \forall y \forall x' \forall y'(x=x' \wedge y=y' \to x*y=x'*y')$
- 封闭性：任何元素参加运算的结果也是S中的元素
- $\forall x \forall y \exists z(x*y=z \to z \in S)$

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**
- $\forall x \forall y \forall z(x,y,z \in S \rightarrow x*(y\#z)=(x*y)\#(x*z))$

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

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**

代数结构的例子

- $<N,+>$是一个代数结构
- 所有2*2实数矩阵M，矩阵乘法*，$<M,*>$
- $<\rho(A), \cup,\cap,\sim>$，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

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 gischen@pku.edu.cn

幺元(identity element)的定义

- 代数结构$<S,*>$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**

幺元的例子

- <N,+>中的0是幺元
- <N,×>中的1是幺元
- <ρ(A),∪>中的∅是幺元
- <ρ(A),∩>中的A是幺元
- <X上的所有函数，函数合成运算>中恒等函数I_X是幺元

幺元的性质

- 一般情况下，左右幺元可能是不同元素，也可能有多个
- 如果存在幺元，那么幺元是唯一的，而且同时是左右幺元
- 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

- <S,*>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：
- $\forall x(x*o_r=o_r)$，称作**右零元**
- $\forall x(o_l*x=o_l)$，称作**左零元**

零元的例子

- <N,+>中没有零元
- <N,×>中0为零元
- <ρ(A),∪>中A是零元
- <ρ(A),∩>中的∅是零元

零元的性质

- 左右零元有和左右幺元相似的性质：
- 如果**存在则唯一**：$o_1=o_1*o_2=o_2$
- 对于一个二元运算：
- 可能同时有零元和幺元；
- 也可能只有零元或幺元；
- 也可能既没有零元，也没有幺元

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

- <S,*>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

逆元的例子

- <I,+,×>，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
- <Q,+,×>，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）
- <A^A, °>，A^A={f|f:A→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

零元的逆元

- 多于1个元素的载体集上零元没有逆元
- <S,*>有幺元e，零元o，并且|S|>1，那么o没有左（右）逆元
- 首先o≠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≠e矛盾

逆元唯一性

- 满足结合律的代数结构中，逆元唯一
- <S,*>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}

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

- <S,*>中元素a，如果对**任意**x,y∈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
- <S,*>中*运算满足结合律，且元素a有逆元：
- a*x=a*y ⊧
- $a^{-1}*(a*x)=a^{-1}*(a*y)$ ⊧
- $(a^{-1}*a)*x=(a^{-1}*a)*y$ ⊧ x=y
- x*a=y*a ⊧
- $(x*a)*a^{-1}=(y*a)*a^{-1}$ ⊧
- $x*(a*a^{-1})=y*(a*a^{-1})$ ⊧ 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

- <{A,∅},∪>，<{1,0},∨>
- 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

∪	∅	A
∅	∅	A
A	A	A

∨	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→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<S,Δ,#>和<S',Δ',#'>，如果有函数h:S→S'，对S中任意元素a,b
- h(Δa)= Δ'(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，称做**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：
- <R,+>和<R,×>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<R,×>改成<R^+,×>
- 则f是**同构**映射，<R,+>和<R^+,×>是同构的

满同态映射例子

- <Σ*,连接>和<N,+>之间
- 存在**满同态映射**length(w)=||w||
- length(u连接v) = ||u连接v|| =
- ||u||+||v|| = length(u)+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。

离散数学：抽象代数：同余关系

陈斌 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<S,Δ,*>中，S上的一个等价关系~，如果满足：
- a~b蕴涵Δa~Δb，称~是S上关于一元运算Δ的同余关系
- a~b,c~d蕴涵a*c~b*d，称~是S上关于二元运算*的同余关系
- 如果~是代数结构上所有的运算的同余关系，则称~是<S,Δ,*>上的同余关系

同余类

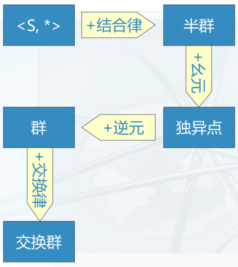
- 同余关系体现了运算保持**等价类**的性质
- 等价类$[x]_\sim$称作同余类
- 例子：
- 相等关系显然是同余关系
- 模k相等是关于整数运算（加、乘、减、负）的同余关系

离散数学：抽象代数：群环域

陈斌 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**幺元**的半群
- **群**group
  - 半群；有幺元；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：<R,+,*>，有两个二元运算
  - <R,+>是阿贝尔群
  - <R,*>是半群
  - *对+可分配：a*(b+c)=a*b+a*c
- **域**field：<F,+,*>
  - <F,+,*>是环
  - <F-{0},*>为交换群