目录

Overview

1 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, 研究不特定的数的性质, 含有未知数的方程和解方程.
- 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.

运算

运算是 S^n 到 S 的一个函数, 称作 n 元运算.
常用记号:

- $*$ 表示二元运算, $*(x,y)$ 常记作 $x*y$.
- 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.

$$\forall x \forall y \forall x' \forall y' (x=x' \land y=y' \to x*y=x'*y')$$

- 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.

$$\forall x \forall y \forall z (x,y,z \in S \to x*(y*z)=(x*y)*z)$$

- 交换律.

$$\forall x \forall y (x, y \in S \to x * y = y * x)$$

- $*$ 运算对 $\#$ 运算满足分配律.

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

代数结构的定义

- 非空集合 S, 称为代数结构的**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**.

幺元的定义

代数结构 $< S, * >$ 中的元素 e, 若对任意 x, 满足:

$$\forall x (x * e = e * x = x)$$

则称 e 为**幺元/单位元** (identity element). 若仅满足:

- $\forall x (x * e_r = x)$, 称作右幺元.
- $\forall x (e_l * x = x)$, 称作左幺元.

幺元的性质

- 一般情况下, 左右幺元可能是不同的元素, 也可能有多个.
- 若存在幺元则是唯一的, 而且同时是左右幺元.

$$e_1 = e_1 * e_2 = e_2$$

零元的定义

$< S, * >$ 中的元素 0, 若对任意 x 满足:

$$\forall x (x * 0 = 0 * x = 0)$$

则称 0 为零元.

- $\forall x (x * 0_r = 0_r)$ 则称作右零元;
- $\forall x (0_l * x = 0_l)$ 则称作左零元;

零元的性质

若存在则唯一: $0_1 = 0_1 * 0_2 = 0_2$.

零元和幺元

对于一个二元运算:

- 可能同时有零元和幺元;
- 可能只有零元或幺元;
- 可能二者都没有.

逆元 (inverse element) 的定义

$< S, * >$ 中有幺元 e, 若 $x * y = e$ 则称. x 为 y 的左逆元, y 为 x 的右逆元. 若 $x * y = y * x = e$, 那么 x, y 互称逆元. x 的逆元通常记作 x^{-1}.
逆元和单位元、零元不同, 前者是载体元素间的关系, 后二者是载体中的元素.

零元的逆元

多余 1 个元素的载体集上零元没有逆元即:
$< S, * >$ 有幺元 e, 零元 o, 且 $\mid S \mid > 1$, 那么 o 没有左 (右) 逆元.
Proof: 首先 $o \neq e$, 否则 S 中另外有非 o或e 的元素 a, $o = o * a = e * a = a$, 矛盾.
若 o 有左 (右) 逆元 x, 那么 $o = x * o(o * x) = e$, 与 $o \neq e$ 矛盾.

逆元的唯一性

满足结合律的代数结构中, 逆元唯一即:
$< S, * >$ 有单位元 e, 且 $*$ 运算满足结合律, 若元素 x 有左逆元 l, 右逆元 r 那么 $l = r = x^{-1}$.
Proof: $l = l * e = l * (x * r) = (l * x) * r = e * r = r = x^{-1}$

可约 (cancelable) 元素

$< S, * >$ 中元素 a, 若对任意 $x, y \in S$ 有:

- $a * x = a * y \to x = y$, 即左可约;
- $x * a = y * a \to x = y$, 即右可约.

则称 a 为可约的.
可约是载体元素的一种性质.

同态和同构

可约性质

满足结合律的代数结构中, 有逆元的元素可约, 即:
$< S, * >$ 中 $*$ 运算满足结合律, 且元素 a 有逆元, 则 a 是可约的.
Proof:

$$\begin{aligned} a*x=a*y &\iff a^{-1}*(a*x)=a^{-1}*(a*y) \iff \\ &(a^{-1}*a)*x=(a^{-1}*a)*y \iff x=y \\ x*a=y*a &\iff (x*a)*a^{-1}=(y*a)*a^{-1} \iff \\ &x*(a*a^{-1})=y*(a*a^{-1}) \iff x=y \\ &\text{因此}a\text{是可约的.} \end{aligned}$$

同类型代数结构: $| S |=| S' |$ 且运算的元数相同.
同构的代数结构: 存在 $S \to S'$ 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: $h(x*y)=h(x)*\prime h(y)$, 其中 $*$ 是 S 上的运算, 而 $*\prime$ 是 S' 上的运算.

同态映射 (homomorphism)

代数结构间更为一般性的相似关系. 对于代数结构 $< S, \Delta, \# >$ 和 $< S', \Delta', \#' >$, 若有函数 h: $S \to S'$, 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**.

- 若 h 是单射函数, 称作单一同态.
- 若 h 是满射函数, 称作满同态.
- 若 h 是双射函数, 称作同构映射 (isomorphism).

同态映射表明了两个代数结构间的相似、等效的关系.
e.g. $< R, + >$ 和 $< R, \cdot >$ 之间存在单同态映射 $f(x)=2^x$:

$$f(x+y)=2^{x+y}=2^x \cdot 2^y=f(x) \cdot f(y)$$

上面的 $< R, \cdot >$ 改成 $< R^+, \cdot >$ 则 f 是同构映射.

满同态映射的例子

$< \Sigma^*, \text{连接} >$ 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.

同余关系 (congruence relation)

代数结构 $< S, \Delta, * >$ 中,S 上的一个等价关系 $\sim$, 若满足:

- $a \sim b \rightarrow \Delta a \sim \Delta b$, 称 $\sim$ 是 S 上关于一元运算 Δ 的同余关系.
- $a \sim b, c \sim d \rightarrow a * c \sim b * d$, 称 $\sim$ 是 S 上关于二元运算 $*$ 的同余关系.
- 若 $\sim$ 是代数结构上所有的运算的同余关系, 则称 $\sim$ 是 $< S, \Delta, * >$ 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 $[x]$ 称作同余类.
e.g. 相等关系, 模 k 相等.

各种类型的代数结构

$< S, * >$ –+ 结合律–> 半群 (semigroup) –+ 幺元–> 独异点 (monoid) –+ 逆元–> 群 (group) –+ 交换律–> 交换群.

- 半群: 运算满足结合律的代数结构.
- 独异点: 含有幺元的半群.
- 群: 半群, 有幺元, 每个元素都有逆元, 没有零元.
- 交换群 (Abel group): 满足交换律的群.

环 (ring): $< R, +, * >$ 有 2 个二元运算, $< R, + >$ 是交换群, $< R, * >$ 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.

Summary

牛逼