

信息安全数学基础

第二部分 第十章 环

中山大学 数据科学与计算机学院 网络空间安全系

1. 环的基本概念

- 群是有一个二元运算的代数系统, 而环是具有两种二元运算的代数系统.
- 第一个二元运算称为“加法”, 第二个称为“乘法”, 分别用 $+$, \cdot 表示, 但不专指算术中的加法或乘法.

定义

设 $(\mathbb{R}, +, \cdot)$ 是一个代数系统. 若 \mathbb{R} 对于加法是交换群, 而对于乘法满足封闭律和结合律, 并且乘法 \cdot 和加法 $+$ 是相互可分配的, 即对于任意 $x, y, z \in \mathbb{R}$, 均有

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z) \quad \text{和} \quad (y + z) \cdot x = (y \cdot x) + (z \cdot x),$$

则称 $(\mathbb{R}, +, \cdot)$ 是关于加法 $+$ 和乘法 \cdot 的一个环.

- 如果环中乘法也是可交换的, 则称之为交换环.

环的例子

- $(\mathbb{Z}, +, \cdot)$ 是交换环.
- $(\mathbb{Z}_n, +, \cdot)$ 是交换环, 被称为**剩余类环**, 其中加法为 $C_a + C_b = C_{a+b}$, 乘法为 $C_a \cdot C_b = C_{ab}$.
- 整数环上的全体多项式构成的集合

$$\mathbb{Z}[x] = \{a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \mid a_i \in \mathbb{Z}, n \geq 0\}$$

对于多项式的加法和多项式的乘法构成交换环, 被称为**整数环上的多项式环**.

- 整数环上的全体 n 阶矩阵的集合对于矩阵的加法和矩阵的乘法构成环, 但这个环不是交换环.

环内的一些特殊元素

设 $(\mathbb{R}, +, \cdot)$ 是一个环,

- 加群 $(\mathbb{R}, +)$ 中的单位元被称为环的零元, 记作 0 ,
- 环元素 a 在加群中的逆元被称为 a 的负元, 记作 $-a$.
- 环的单位元是指 $(\mathbb{R}$ 对于乘法的单位元, 如果有的话, 记作 1 .
- 环的一个元素 a 的逆元 a^{-1} 都是指它对于乘法的逆元.
- 环中有乘法逆元的元素叫做单位(unit), 不要与单位元(identity element)混淆.

零因子和整环

定义

设 $(\mathbb{R}, +, \cdot)$ 是一个环. 如果 $a, b \in \mathbb{R}$, 且 $a \neq 0, b \neq 0$, 但是 $ab = 0$, 则称 a 为左零因子 (*left zero divisor*), b 为右零因子. 如果一个元素既是左零因子, 又是右零因子, 称之为零因子.

定义

一个无零因子且可交换的环, 被称为整环 (*domain*).

- 整数集合 \mathbb{Z} 对于加法和乘法是整环.
- 整数集合 $(\mathbb{Z}_n, +, \cdot)$ 一般不是整环. 例如, 在 $(\mathbb{Z}_4, +, \cdot)$ 中, $\bar{2} \cdot \bar{2} = \bar{0}$, 有零因子.
- 整数环上的全体 n 阶矩阵的集合对于矩阵的加法和矩阵的乘法构成环. 这个环不是交换环, 有零因子.
- 整数环上的多项式环 $\mathbb{Z}[x]$ 是一个整环, 它是可交换的, 且没有零因子.

无零因子环的消去律

定理

设 0 是环的加法零元, 对于环中的任意元素 a , 有 $0 \cdot a = a \cdot 0 = 0$.

这是因为 $0 + (0 \cdot a) = 0 \cdot a = (0 + 0) \cdot a = (0 \cdot a) + (0 \cdot a)$, 而加法是群, 所以 $(0 \cdot a)$ 的负元存在, 两边同时与 $-(0 \cdot a)$ 做加法, 即得 $0 = 0 \cdot a$. 类似地, 可以证明 $a \cdot 0 = 0$.

定理

一个环是无零因子环当且仅当乘法运算满足消去律, 即对于任意地 $a, b, c \in \mathbb{R}$ 且 $c \neq 0$, 如果 $c \cdot a = c \cdot b$ 则必有 $a = b$; 如果 $a \cdot c = b \cdot c$ 则必有 $a = b$.

如果已知是无零因子, 对于任意地 $a, b, c \in \mathbb{R}$, 满足 $c \cdot a = c \cdot b$ 且 $c \neq 0$, 我们有

$$0 = (c \cdot a) + [-(c \cdot a)] = (c \cdot a) + [-(c \cdot b)] = (c \cdot a) + [c \cdot (-b)] = c \cdot [a + (-b)],$$

于是 $a + (-b) = 0$, 即 $a = b$. 类似可以推出, 如果 $a \cdot c = b \cdot c$ 则必有 $a = b$.

反之, 设消去律成立, 要证明是无零因子环, 即要证明, 如果 $a \neq 0$ 且 $ab \neq 0$, 则必定有 $b \neq 0$. 事实上, $a \cdot b = 0 = a \cdot 0 \Rightarrow b = 0$. \diamond

除环和域

定义

设 $(\mathbb{R}, +, \cdot)$ 是一个环. 如果 \mathbb{R} 中至少有零元0和单位元1两个元素, 且 \mathbb{R} 除去零元0构成乘法群, 则称 $(\mathbb{R}, +, \cdot)$ 是一个除环(*division ring*).

定义

如果一个环 $(\mathbb{R}, +, \cdot)$, 既是除环也是可交换环, 称这个环为域(*field*).

除环和域

定义

设 $(\mathbb{R}, +, \cdot)$ 是一个环. 如果 \mathbb{R} 中至少有零元0和单位元1两个元素, 且 \mathbb{R} 除去零元0构成乘法群, 则称 $(\mathbb{R}, +, \cdot)$ 是一个除环(*division ring*).

定义

如果一个环 $(\mathbb{R}, +, \cdot)$, 既是除环也是可交换环, 称这个环为域(*field*).

- 全体有理数集合 (\mathbb{Q}) 对于加法和乘法构成域, 被称为有理数域.

除环和域

定义

设 $(\mathbb{R}, +, \cdot)$ 是一个环. 如果 \mathbb{R} 中至少有零元0和单位元1两个元素, 且 \mathbb{R} 除去零元0构成乘法群, 则称 $(\mathbb{R}, +, \cdot)$ 是一个除环(*division ring*).

定义

如果一个环 $(\mathbb{R}, +, \cdot)$, 既是除环也是可交换环, 称这个环为域(*field*).

- 全体有理数集合 (\mathbb{Q}) 对于加法和乘法构成域, 被称为有理数域.
- 全体实数集合 (\mathbb{R}) 对于加法和乘法构成域, 被称为实数域.

除环和域

定义

设 $(\mathbb{R}, +, \cdot)$ 是一个环. 如果 \mathbb{R} 中至少有零元0和单位元1两个元素, 且 \mathbb{R} 除去零元0构成乘法群, 则称 $(\mathbb{R}, +, \cdot)$ 是一个除环(*division ring*).

定义

如果一个环 $(\mathbb{R}, +, \cdot)$, 既是除环也是可交换环, 称这个环为域(*field*).

- 全体有理数集合 (\mathbb{Q}) 对于加法和乘法构成域, 被称为有理数域.
- 全体实数集合 (\mathbb{R}) 对于加法和乘法构成域, 被称为实数域.
- 全体复数集合 (\mathbb{C}) 对于加法和乘法构成域, 被称为复数域.

除环和域

定义

设 $(\mathbb{R}, +, \cdot)$ 是一个环. 如果 \mathbb{R} 中至少有零元0和单位元1两个元素, 且 \mathbb{R} 除去零元0构成乘法群, 则称 $(\mathbb{R}, +, \cdot)$ 是一个除环(*division ring*).

定义

如果一个环 $(\mathbb{R}, +, \cdot)$, 既是除环也是可交换环, 称这个环为域(*field*).

- 全体有理数集合 (\mathbb{Q}) 对于加法和乘法构成域, 被称为有理数域.
- 全体实数集合 (\mathbb{R}) 对于加法和乘法构成域, 被称为实数域.
- 全体复数集合 (\mathbb{C}) 对于加法和乘法构成域, 被称为复数域.
- 集合 $\{0, 1\}$ 对于模2加法和模2乘法构成域, 通常被称为二元域(binary field), 记为 $GF(2)$, 或 \mathbb{F}_2 .

除环和域

定义

设 $(\mathbb{R}, +, \cdot)$ 是一个环. 如果 \mathbb{R} 中至少有零元0和单位元1两个元素, 且 \mathbb{R} 除去零元0构成乘法群, 则称 $(\mathbb{R}, +, \cdot)$ 是一个除环(*division ring*).

定义

如果一个环 $(\mathbb{R}, +, \cdot)$, 既是除环也是可交换环, 称这个环为域(*field*).

- 全体有理数集合 (\mathbb{Q}) 对于加法和乘法构成域, 被称为有理数域.
- 全体实数集合 (\mathbb{R}) 对于加法和乘法构成域, 被称为实数域.
- 全体复数集合 (\mathbb{C}) 对于加法和乘法构成域, 被称为复数域.
- 集合 $\{0, 1\}$ 对于模2加法和模2乘法构成域, 通常被称为二元域(binary field), 记为 $GF(2)$, 或 \mathbb{F}_2 .
- 如果 p 是素数, 则模 p 的剩余类环 $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$ 对于模 p 加法和模 p 乘法构成域, 记为 $GF(p)$, 或 \mathbb{F}_p . 它的元素只有有限个, 是一类最简单的有限域.

有限整环和有限除环

定理

有限除环一定是可交换环, 即有限除环一定是域.

定理

有限整环一定是除环, 即有限整环一定是域.

环的同态与同构

定义 (同态)

设 R 和 R' 是两个环, 如果有一个 R 到 R' 的映射 f 满足对于任意的 $a, b \in R$ 有:

$$f(a + b) = f(a) + f(b)$$

$$f(ab) = f(a)f(b)$$

则称 f 是 R 到 R' 的同态映射, R 与 R' 关于 f 同态.

- \mathbb{Z} 是整数环, $\mathbb{Z}/n\mathbb{Z}$ 是模 n 的剩余类环, 则 \mathbb{Z} 和 $\mathbb{Z}/n\mathbb{Z}$ 关于映射 f 同态, 其中 $f: k \mapsto k + n\mathbb{Z}$.
- 如果 f 是单设, 则称 f 是单同态. 如果 f 是满设, 则称 f 是满同态. 如果 f 是一一映射, 则称 f 是同构.

定义 (同构)

设 R 和 R' 是两个环, 若存在一个 R 到 R' 的同构映射 f , 则称 R 和 R' 是同构的.