信息安全数学基础

第二部分 第十章 环

中山大学 计算机学院

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

$$\mathbb{Z}[x] = \{a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n | a_i \in \mathbb{Z}, n \geq 0\}$$

  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$b = 0$. 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是一一映设，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.

2. 整除概念的提升：交换环上的整除

设$(\mathbb{R},+,\cdot)$是一个由单位元的整环，$a,b\in\mathbb{R}$

- 整除
  $0\neq a\in\mathbb{R}$，称a整除另外一个元素$b\in\mathbb{R}$. 如果存在一个元素$c\in\mathbb{R}$，使得$b=a\cdot c$. 记作$a\,|\,b$. a是b的因子. b是a的倍元.
- 公因子
  如果$a\,|\,b_i, i=1,2,\cdots,n$，则称$a$是$b_i, i=1,2,\cdots,n$的公因子.
- 最大公因子
  如果d是$b_i, i=1,2,\cdots,n$的公因子，对于$i=1,2,\cdots,n$，如果b_i的任意其它公因子均整除d，则称d是$b_i, i=1,2,\cdots,n$的最大公因子. 记作$d=\gcd(b_1,\cdots,b_n)$.
- 相伴元
  对于任意$a,b\in\mathbb{R}$，如果存在可逆元$u\in R$使得$a=ub$，则称a与b是相伴的，记作$a\sim b$. 这与$a\,|\,b$且$b\,|\,a$是等价的. 例如，在$\mathbb{Q}[x]$中，$\frac{1}{3}$和$3x+3$互为相伴元.
- 不可约元
  若$c=ab$，且a与b都不是单位(都不是可逆元)，则称a(或b)是c的真因子.
  如果p不为0不可逆，且没有真因子，则p称为不可约元.

高斯整环

定理

设$i=\sqrt{-1}$为虚数单位，复数集合

$$Z[i]=\{a+bi\,|\,a,b\in Z\}$$

对复数的加法和复数的乘法构成环，被称为高斯整数环.

- 无零因子. 如果$(a+b\sqrt{-1})(c+d\sqrt{-1})=(ac-bd)+(ad+bc)\sqrt{-1}=0$，则$ac-bd=0$且$ad+bc=0$，于是$ac^2=(bd)c=c(bd)=(cb)d=(bc)d$，进而$a(c^2+d^2)=(bc)d+(-(bc)d)=0$. 所以，或者$a=0$或者$c^2+d^2=0$，即或者$a=b=0$或者$c=d=0$.
- 可逆元.
  在高斯整环中，1，$\sqrt{-1}$和$-\sqrt{-1}$都是可逆元.
- 不可约元.
  在高斯整环中，3是不可约元，而$2=(1+i)(1-i)$是可约元.
  在整环$Z[\sqrt{-5}]$中，2是不可约元，而$9=3\cdot 3=(2+\sqrt{-5})(2-\sqrt{-5})$是可约元.

3. 环的特征

定义

设$\mathbb{R}$是一个环. 如果存在一个最小正整数p使得对于任意的$a \in R$, 都有

$$pa = \underbrace{a + a + \ldots + a}_{p\text{个}a} = 0,$$

则称环R的特征为p. 如果不存在这样的正整数, 则称环R的特征为0.

定理

如果域K的特征不为零, 则其特征必为素数.

域K的特征p不是素数, 则存在整数$1 < p_1, p_2 < p$, 使得$p = p_1 p_2$. 于是对于任意的$a \in K$且$a \neq 0$有

$$(p_1 a)(p_2 a) = (p_1 p_2)a^2 = 0.$$

因为K无零因子, 所以$(p_1 a) = 0$或$(p_2 a) = 0$. 这与特征为p矛盾.

特征的基本性质

定义

设$\mathbb{R}$是一个有单位元的交互环. 如果$\mathbb{R}$的特征为p, 则

1. 对于任意的$a, b \in R$,有
$$(a+b)^p = a^p + b^p.$$
2. 环R到自身的映射$\sigma : a \mapsto a^p$是自同态映射.

定理

设p为素数, $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$是整系数多项式, 则

$$f(x)^p \equiv f(x^p) \bmod p.$$

考虑模p的剩余类环$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$上的多项式环$\mathbb{F}_p[x]$

4. 分式域

定义

设A是一个环. $E = A \times A^*$, 其中$A^* = A \setminus \{0\}$. 如果E上有等价关系

$$(a,b)R(c,d) \quad \text{如果} \quad ad = bc.$$

则E关于等价关系R商集E/R对于如下加法和乘法构成一个域.

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd},$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

这个域E/R被称为整环A的分式域.

从整环到分式域

- 考虑整数环$\mathbb{Z}$的分式域，定义该分式域的等价关系即为有理数相等, 加法和乘法是有理数的加法和乘法, 所以说整数环的分式域是有理数域.
- 设K是一个域, 则K上的多项式环$K[x]$是一个整环. 考虑$K[x]$的分式域, 这样的分式域被称为多项式分式域, 记为$K(x)$. 定义该分式域的等价关系为

$$(f_1(x), g_1(x))R(f_2(x), g_2(x)) \quad \text{如果} \quad f_1(x)g_2(x) = g_1(x)f_2(x),$$

其中$g_1(x), g_2(x) \neq 0$. 加法和乘法是有理数多项式的加法和乘法.