离散数学

Discrete Mathematics

吴梅红

厦门大学计算机科学系

E-mail: wmh@xmu.edu.cn

6.5 环 Ring 与 域 Field

- 半群、独异点和群是只有一个二元运算的代数系统。
- 环和域是具有两个二元运算的代数系统。

定义6.13 设<**R**, + , •> 是具有两个二元运算的代数系统, 如果: /* + , • 次序重要

(1) <**R**, +> 构成**Abel**群, /*环只对+是群

(2) <**R**, •> 构成半群, /*域对+, *都是群

(3) • 对 + 适合分配律,

则称<**R**, +, •>是环, 并称+和*分别为**R**中的加法和乘法 ∎

- 分配律把两个二元运算联系在一起。

例6.23 (1) Z, Q, R, C关于普通数的加法 +和乘法*都构成环, 分别称为整数环, 有理数环, 实数环, 复数环。

(2) 设n≥2, 设$<M_n(R),+,*>$是n阶实矩阵的集合，则$M_n(R)$关于矩阵的加法和乘法构成环, 称为n阶实矩阵环。

(3) $<Z_n, \oplus, \otimes>$ 构成一个环, 其中$Z_n = \{0, 1, \ldots, n-1\}$,

$\forall x, y \in Z_n$, $x \oplus y = (x+y) \bmod n$, $x \otimes y = (x*y) \bmod n$,

称为模n整数环。 /*Abel

(4) $<P(B), \oplus, \cap>$ 构成一个环, 其中⊕是集合的对称差。

$<P(B), \oplus, \cup>$ 不构成一个环。 /*∪对⊕不分配

- 环中加法的 单位元记作**0**,

  元素x关于加法的 逆元称为x的负元, 记作 $-x$ 。

- 如果 环中乘法有单位元, 记作 **1**或**e**。

  如果 x关于乘法存在逆元, 记作 x^{-1}。

- 类似地, 可以用 $x - y$ 表示 $x + (-y)$。

- nx表示x的加法n次幂, 即 $nx = \underbrace{x + x + \cdots + x}_{n个}$。

  而用x^n表示x的乘法n次幂, 即 $x^n = \underbrace{x\,x\,\cdots x}_{n个}$。

例 <2Z, +, •>称为偶环; 但<2Z, •, +>不是环, •无单位元。

- 在环中作公式展开时可以使用定理中的等式。

例 (1) 设R是环, 计算 $(a-b)^2$ 和 $(a+b)^3$ 。

解 $(a-b)^2 = (a-b)(a-b)$

$= a^2 - ba - ab + b^2$

/* $-ba-ab \neq -2ab$, 乘法非交换

$(a+b)^3 = (a+b)(a+b)(a+b)$

$= (a^2 + ba + ab + b^2)(a+b)$

$= a^3 + ba^2 + aba + b^2a + a^2b + bab + ab^2 + b^3$ 。

/* $\neq a^3 + 3a^2b + 3ab^2 + b^3$

例 在模3的 整数环Z_3 中解方程组

$$\begin{cases} x + 2z = 1, & ① \\ y + 2z = 2, & ② \\ 2x + y = 1, & ③ \end{cases}$$

解 ① – ② 得 $x - y = 2$。 ④

③ + ④ 得 $3x = 0$。 /* $\forall x \in Z_3$

② – ① 得 $y - x = 1$。

- 若$x = 0,\ y = 1$, 从而推得 $z = 2$。
- 若$x = 1,\ y = 2$, 从而推得 $z = 0$。
- 若$x = 2,\ y = 0$, 从而推得 $z = 1$。 /* 非惟一解

$$\begin{cases} x_1 = 0, \\ y_1 = 1, \\ z_1 = 2; \end{cases} \quad \begin{cases} x_2 = 1, \\ y_2 = 2, \\ z_2 = 0;, \end{cases} \quad \begin{cases} x_3 = 2, \\ y_3 = 0, \\ z_3 = 1. \end{cases}$$

- 设<R , +, •>是环，如果环中乘法满足**除结合律**以外的**其他算律**, 就得到一些**特殊的环**。

定义 设a , b是环R中的两个非零元素, 如果ab = 0,

则称a是是R中的一个左零因子, b是R中的一个右零因子.

若一个元素既是左零因子又是右零因子, 则称它是一个

零因子(divisor of zero)。 [redacted] /* ≠ 零元

例 模6的整数环中, $2 \otimes 3 = 0$, 2是左零因子, 3是右零因子,

又由于$\otimes$是可交换的, 所以2也是右零因子, 3也是左零

因子。 2和3都是零因子。 /* 零因子非惟一

定义 6.14 设$\langle R, +, \bullet \rangle$是环,

(1) 若R中乘法适合交换律, 则称R是交换环。

(2) 若R中存在乘法的单位元, 则称R是含幺环。

(3) 若$\forall$ a, b $\in$ R, $ab = 0 \Rightarrow a = 0$ 或 $b = 0$,

则称R是无零因子环。 ∎ /* = 消去律

等价定义 设R是一个是环, 如果R中任意非零元a和b,

都有 $ab \neq 0$, 则称$(R; +, \bullet)$是无零因子环。 ∎

- 从无零因子(no zero divisor)环的定义可看出,

  无零因子环就是 不含有左和右零因子的环。

  当一个环无左零因子, 这时 必然也无右零因子。

例 整数环、有理数环、实数环复数环, 都是无零因子环.

定义6.14 设R是一个环, /* 区别整数环

(4) 若R是交换的含幺的无零因子环, 则称R是**整环**;

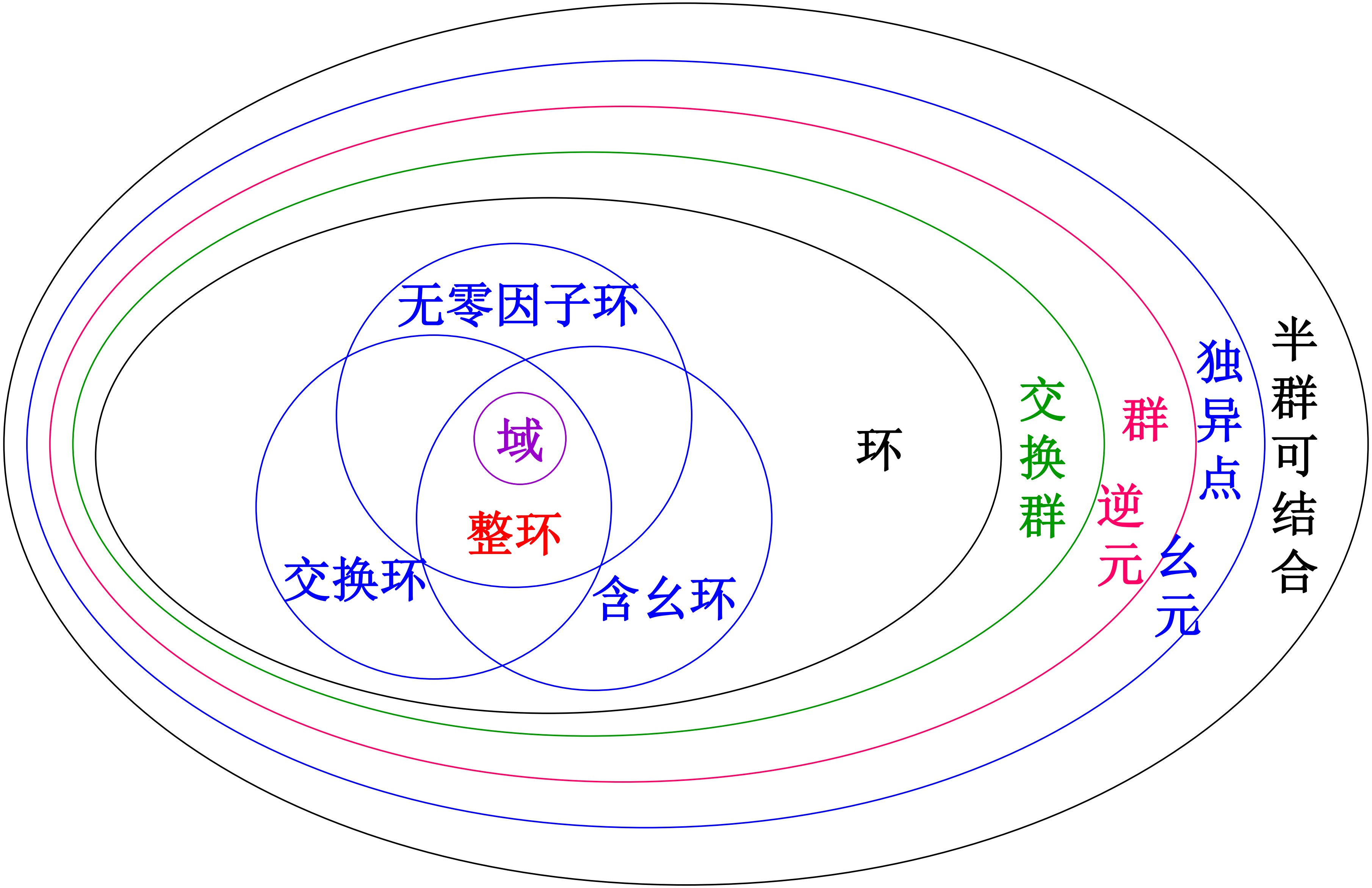
(5) 若R中至少有两个元素, 令$R^* = R - \{0\}$, 且$\langle R^*, \bullet \rangle$构成**群**, 则称R是一个**除环**; /*单位元, 无零因子

(6) 若R是一个**交换的除环**, 称为**域Field**。 ■

例 整数环Z, 有理数环, 实数环, 复数环C都是整环。

- n阶实矩阵$M_n(R)$不是整环, 因矩阵乘法不是可交换的.
- 模n整数环Z_n只有当n是素数时才是整环. /*无零因子

代数系统 (广群): 封闭性



例6.24(1) 整数环, 有理数环, 实数环中的乘法适合交换律, 含有单位元1, 不含零因子,

因此它们都是交换环、含幺环、无零因子环和整环。

其中有理数环, 实数环也是域, 因为a (a≠0) 存在乘法逆元, 就是它的倒数1/a。

- 但是整数环不是域, 因为很多整数的倒数不再是整数。

(2) 模n整数环$<Z_n, \oplus, \otimes>$是交换环、含幺环。

- 当n为素数时可以证明Z_n构成域;

  当n为合数时不构成整环和域。

- 例如 合数n = pq, p, q是大于1的整数,

  那么 $p \otimes q = 0$, p和q是零因子。

例6.24 (3)设n≥2, n阶实矩阵环<$M_n(R)$, +, •>不是交换环，因为矩阵乘法不可交换。

- 但它是含幺环，单位矩阵是乘法的幺元。
- 它不是无零因子环，因为存在两个非零矩阵相乘为零矩阵的情况，这样的非零矩阵分别为左零因子和右零因子。因此它也不是整环和域。

- 域是一类重要的代数系统, 一般常把域表示为<F, +, •>.
- 域中的运算有着非常良好的性质。其中<F, +>构成Abel群, +有交换律、结合律、单位元, 每个元素都有负元;
- <F, •>也构成Abel群, •也有交换律、结合律、单位元, 除了零以外, 每个元素都有逆元。
- 此外, 乘法对加法还有分配律。正由于这些良好的性质, 域有着广泛的应用。特别是伽罗华域(Galosi field) GF(p)在密码学中是很重要的基础。

例 有理数环, 实数环都是域, 分别称为有理数域, 实数域

- 环就其 + 运算而言是**Abel群**,
- 域就其 +, • 运算而言都是**Abel群**。

定理 域一定是整环。

证 交换的除环, 除环的乘法**R*群**含单位元, 无零因子. ■

- 域等价定义为每个非零元素都有乘法逆元的整环。

例 $\langle \mathbf{Q}, +, \bullet \rangle$为域, 但$\langle \mathbf{Z}, +, \bullet \rangle$不是域, 整数无乘法逆元。

例 $\langle \mathbf{Z}_6, +_6, \bullet_6 \rangle$不是域, 甚至不是整环, 它有零因子,

如2和3, 2和3没有乘法逆元。

例 证明 Z_p 为无零因子环 当且仅当 p为素数。

**证 必要性 反证法 假设p不是素数,

必存在小于p大于1的正整数s, t 使得 $p = st$ 。

易见 $(st) \bmod p = 0$, s和t是Z_p 中的零因子,

与Z_p 为无零因子环矛盾, $\therefore$ p是素数。

- 充分性 $\forall a, b \in Z_p$, 若 $ab = 0$, 不妨设$a \neq 0$,

我们证明必有 $b = 0$。由 $ab = 0$ 可知 $p \mid ab$。

由 $a, b \in \{0, 1, \ldots , p-1\}$ 知 $p \nmid a$。

而p又是素数, 所以 $p \mid b$, 从而 $b = 0$。 ▮

定理 有限整环必定是域。

**证1 设F $<F, +, \bullet>$是有限整环, $<F, \bullet>$为有限含幺交换半群,

群,

令$F^* = F - \{0\}$, 则 $\forall x \in F^*$, 有 $xF^* = F^*$, /*封闭性

$\exists y \in F^*$, 使得 $xy = 1$。 /*定理 17. 1右幺右逆

所以, $<F^*, \bullet>$构成群, $<F, +, \bullet>$是域。 ∎

证2 设$<F, +, \bullet>$是有限整环, $<F, \bullet>$为有限含幺交换半群,

根据有限子群判定定理的证明, $<F, \bullet>$为循环群可交换,

所以, $<F, +, \bullet>$是域。 ∎