第十八章　环与域

18.1 环的定义及其性质

环的定义

环的性质

特殊的环

有限域

18.2 子环、理想、商环、环同态

子环定义及判别

理想、商环、环同态

环的定义

定义： 设代数系统 $<R,+,\cdot>$ 满足

$<R,+>$ 构成Abel 群

$<R,\cdot>$ 构成半群

$\cdot$ 对+运算满足分配律

符号说明：$0, 1, -x, x^{-1}, nx, x^n, x\text{-}y,$

实例：

数环 Z, Q, R, C 关于普通数的加法与乘法

$<Z_n, \oplus, \otimes>$

$<M_n(R), +, \cdot>$

$<P(B), \oplus, \cap>$

环的性质

1. $a0 = 0a = 0$
2. $(-a)b = a(-b) = -(ab)$
3. $(-a)(-b) = ab$
4. $a(b-c) = ab-ac$, $(b-c)a = ba-ca$
5. $$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{n} a_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$$
6. $(na)b = a(nb) = n(ab)$

证明

证 (1) $\forall a \in A$，$a \bullet 0=0 \bullet a=0$

$a \bullet 0 = a \bullet (0+0) = a \bullet 0 + a \bullet 0$

由加法消去律得$a \bullet 0=0$。

同理可证$0 \bullet a=0$

(2) $\forall a,b \in A$，$a \bullet (-b)=(-a) \bullet b=-(a \bullet b)$

$a \bullet b+(-a) \bullet b = [a+(-a)] \bullet b = 0 \bullet a = 0$

所以$(-a) \bullet b=-(a \bullet b)$

同理可证$(-a) \bullet b=-(a \bullet b)$

证明（续）

(3) $\forall a,b\in A$，$(-a)\bullet(-b)=(a\bullet b)$

根据(2)有

$$(-a)\bullet(-b) =-(a\bullet(-b)) =-(-(a\bullet b)) =a\bullet b$$

(4) $\forall a,b,c\in A$，$a\bullet(b-c)=a\bullet b-a\bullet c$

$$a\bullet(b-c) =a\bullet[b+(-c)] =a\bullet b+a\bullet(-c) =a\bullet b+(-a\bullet c) = a\bullet b-a\bullet c$$

$\forall a,b,c\in A$，$(b-c)\bullet a=b\bullet a- c\bullet a$

$$(b-c)\bullet a =[b+(-c)]\bullet a =b\bullet a+(-c)\bullet a=b\bullet a+(-c\bullet a) =b\bullet a-c\bullet a$$

证明（续）

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{n} a_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$$

先证对任意$i=1,2,\ldots,n$，有

$$a_i(\sum_{j=1}^{m} b_j) = \sum_{j=1}^{m} a_i b_j$$

对m进行归纳.

$m=2$,由环中乘法对加法的分配律有

$a_i(b_1+b_2)=a_ib_1+a_ib_2$

假设$m=k$时等式成立，当$m=k+1$时有

证明（续）

$$a_i(\sum_{j=1}^{k+1} b_j) = a_i(\sum_{j=1}^{k} b_j + b_{k+1}) = a_i\sum_{j=1}^{k} b_j + a_i b_{k+1}$$

$$= \sum_{j=1}^{k} a_i b_j + a_i b_{k+1} = \sum_{j=1}^{k+1} a_i b_j$$

同理可证对任意环中元素b_j有

$$(\sum_{i=1}^{n} a_i) b_j = \sum_{i=1}^{n} a_i b_j$$

因此，

$$(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n} a_i(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n}(\sum_{j=1}^{m} a_i b_j)$$

证明（续）

(6) $(na)b = a(nb) = n(ab)$

证 先证(na)b=n(ab).考虑n>0，对n归纳.

n=1时，ab=ab.

假设n=k时等式成立，则有

$((k+1)a)b=(ka+a)b=(ka)b+ab=k(ab)+ab=(k+1)(ab)$

由归纳法知对一切$n\in Z^+$等式都成立.

当n=0时，等式两边都是0，等式也成立.

当n<0时，令n=-m，$m \in Z^+$，则有

$$(na)b=(-ma)b=(m(-a))b=m((-a)b)=m(-(ab))$$
$$=-m(ab)=n(ab).$$

同理可证$a(nb)=n(ab)$.

举例

例2 设$<A,+,\bullet>$是一个环，$a,b,c,d\in A$，

计算$(a+b)\bullet(\mathrm{c}+\mathrm{d})$，$(a-b)^2$

解答 $(a+b)\bullet(\mathrm{c}+\mathrm{d})$

$= (a+b)\bullet c+(a+b)\bullet d$

$= a\bullet c+b\bullet c+a\bullet d+b\bullet d$

$(a-b)^2 = (a-b)\bullet(a-b)$

$= (a-b)\bullet a-(a-b)\bullet \mathrm{b}$

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

几个特殊的环

定义 设$<A,+,\bullet>$是环。

(1) 若$<A,\bullet>$是可交换的，则称$<A,+,\bullet>$是**交换环**。

(2) 若$<A,\bullet>$含有单位元，则称$<A,+,\bullet>$是**含幺环**。

(3) 若对任意的$a,b\in A$，$a\neq\theta\wedge b\neq\theta$ 必有$a\bullet b\neq\theta$，则称$<A,+,\bullet>$是**无零因子环**。

实例： 数环, Z_p 为无零因子环当且仅当p 为素数

定理： R 是环，R 为无零因子环$\Leftrightarrow R$ 中乘法有消去律

说明

无零因子也可以描述为

$\forall a,b\in A$， $a\bullet b=\theta\Rightarrow a=\theta\vee b=\theta$

几个特殊的环（续）

(4) 若$<A,+,\bullet>$既是交换环、含幺环、也是无零因子环，则称$<A,+,\bullet>$是**整环**。

(5) **除环**：$|R|>1, <R^*,\cdot>$ 构成群, $R^*=\{R-\{0\}\}$

(6) **域:** $|R|>1$, 交换的除环或者每个R^*中元素都有逆元的整环

实例： $H=\left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \middle| a,b\in R\right\}$为除环，不是域

$<Q,+,\bullet>,<R,+,\bullet>,<C,+,\bullet>, Z_p$都是域

域一定整环；有限整环必定是域

定理证明

定理 在整环$<A,+,\bullet>$中的无零因子条件等价于乘法满足消去律，即对于$c\neq\theta$和$c\bullet a=c\bullet b$，必有$a=b$。

证明 若无零因子，设$c\neq\theta$和$c\bullet a=c\bullet b$，

则有 $c\bullet a-c\bullet b=c\bullet(a-b)=\theta$

因为$<A,+,\bullet>$是无零因子环，所以必有

$a-b=\theta\Rightarrow a=b$ 所以乘法消去律成立。

反之，若消去律成立，设$a\neq\theta$和$a\bullet b=\theta$，则

$a\bullet b=a\bullet\theta\Rightarrow b=\theta$

同理，设$b\neq\theta$和$a\bullet b=\theta$，必有$a=\theta$。

故无零因子。

举例

例1 设S是一个集合，$<\rho(S),\oplus,\cap>$为S的子集环 ,说明子集环构成哪一种环？

解 $<\rho(S),\oplus>$是可交换群，$\varnothing$是单位元，X的逆元是X，

$<\rho(S),\cap>$是半群，S是单位元，$\cap$有可交换性，

因此子集环是含幺元交换环。

$<\rho(S),\oplus,\cap>$不是无零因子环，也不是整环。

如S={1,2}，则$\rho(S)=\{\varnothing,\{1\},\{2\},\{1,2\}\}$,

$\{1\}\neq\varnothing$，$\{2\}\neq\varnothing$，但$\{1\}\cap\{2\}=\varnothing$.故{1}和{2}是零因子.

或者：$\{1,2\}\cap\{1\}=\{1,2\}\cap\{2\}$,但$\{1\}\neq\{2\}$,不满足消去律

例题

在有限域$<Z_5,\oplus,\otimes>$中，解下列方程和方程组

1）$3x+1=2$

2) $\begin{cases} x+4y=0 \\ 2x+y=2 \end{cases}$

例题（续）

1） $3x+1=2$

解 $(3\otimes x)\oplus 1=2$

$(3\otimes x)\oplus(1\oplus 4)=2\oplus 4$

$3\otimes x=1$

$(2\otimes 3)\otimes x=2\otimes 1$

$x=2$

例题（续）

$$\begin{cases} x+4y=0 \\ 2x+y=2 \end{cases}$$

解 $\begin{cases} \boldsymbol{x \oplus (4 \otimes y) = 0} & \textbf{(1)} \\ \boldsymbol{(2 \otimes x) \oplus y = 2} & \textbf{(2)} \end{cases}$

由(1)式得，

$\boldsymbol{x = 0 \oplus -(4 \otimes y) = -(4 \otimes y) = -4 \otimes y = 1 \otimes y}$
$\boldsymbol{= \mathrm{y}}$

代入第(2)式， $\boldsymbol{(2 \otimes x) \oplus x = 2}$

$\boldsymbol{(2 \otimes x) \oplus (1 \otimes x) = 2,}$ **(2⊕1)⊗*x*=2,**

3⊗*x*=2，(2 ⊗ 3)⊗*x*= 2 ⊗ 2, *x*=4, *y*=4

例题

例2 p,q 为不等的素数，证明无 pq 阶的整环.

证： 假设 R 为 pq 阶的整环，

则 $<R,+>$ 为 pq 阶的Abel 群.

存在 p 阶元 a， q 阶元 b.

所以 $|a+b|=pq$, $<R,+>$ 为循环群，

令 $c=a+b$ 为生成元.

$$R=\{\ 0, c, 2c, \ldots, (pq-1)c\ \}$$

取 $x=pc$, $y=qc$, 则

$$xy=(pc)(qc) = pqc^2 =0$$

x,y 为零因子.

有限域

- 定义：F 为域，$|F|$有限

  实例：Z_p, p 为素数

  Z_p 为整环，$<Z_p-\{0\}, \cdot>$有限半群，

  无零元，适合消去律，$<Z_p-\{0\}, \cdot>$构成Abel 群

  结论：有限的整环都是域
- 有限域的特征

  F 为有限域，1 在$<F,+>$中的阶为域F 的特征.

  Z_p 的特征为p.
- 定理：有限域F的特征是素数.

有限域的性质

- **定理：设F 为有限域，则存在素数p 使得$|F|=p^n$,**

证明思想:

$A=\langle 1\rangle=\{0, 1, \ldots, p-1\}$

$Ax_1=\{0, x_1, 2x_1, \ldots, (p-1)x_1\}$，$x_1\in F^*$

$|Ax_1|=p$

若 $F=Ax_1$ 则结束；否则 $\exists x_2\in F-Ax_1, x_2\neq 0,$

$Ax_1+Ax_2=\{a_1x_1+a_2x_2 \mid a_1,a_2\in A\}$

可以证明Ax_1+Ax_2 中的元素两两不同，（自学）

因此 $|Ax_1+Ax_2|=p^2$,

照此处理，$|Ax_1+Ax_2+Ax_3|=p^3$, 直到穷尽所有的元素.

有限域应用----素数测试问题

Fermat 小定理：如果n 为素数，则对所有的正整数

$a \neq 0(\mathrm{mod}\, n)$ 有 $a^{n-1} \equiv 1(\mathrm{mod}\ n)$

测试素数的算法：

令a=2, 检测$a^{n-1} \equiv 1(\mathrm{mod}\ n)$?

如果回答“是”，输出“素数”；否则输出“合数”.

分析：

时间 $T(n)=O(\log_3 n)$

问题：

该算法只对a=2 进行测试, 如果n 为合数且输出为“素数”，则称n 为基2 伪素数. 例如341 满足上述条件，但是341 是合数.

素数测试的随机算法

改进方法：

随机选取2--n-2 中的数，进行测试. 例如取a=3，则

3^{340}(mod 341) ≡ 56，341 不是素数.

新问题：

Fermat 小定理的条件只是必要条件，满足条件的可能是合数. 对所有与n 互素的正整数a，都满足上述条件的合数n称为Carmichael 数，如561， 1105， 1729， 2465 等.

Carmichael 数非常少，小于10^8 的只有255 个.

可以证明：如果n 为合数，但不是Carmichael 数，采用随机选取2—n-2 中的数进行测试，测试n 为合数的概率至少为1/2. 但是这个算法不能解决 Carmichael 数的问

素数测试的另一个条件

定理2 如果n为素数，则方程$x^2 \equiv 1 (\bmod n)$的根只有两个，即$x=1$，$x=-1$（或$x=n-1$）

证明 $x^2 (\bmod n) \equiv 1 \Leftrightarrow x^2-1 \equiv 0 (\bmod n)$

$\Leftrightarrow (x+1)(x-1) \equiv 0 (\bmod n)$

$\Leftrightarrow x+1 \equiv 0$ 或 $x-1 \equiv 0$ （域中没有零因子）

$\Leftrightarrow x=-1$ 或 $x=1$

称$x \pm \neq 1$ 的根为非平凡的.

根据定理2，如果方程有非平凡的根，则n为合数. 例如:

$x^2 (\bmod 5) \equiv 1 \Leftrightarrow x=1$ 或 $x=4$

$x^2 (\bmod 12) \equiv 1 \Leftrightarrow x=1$ 或 $x=5$ 或 $x=7$ 或 $x=11$

5 和7 是非平凡的根.

Miller-Rabin算法

设n 为奇素数，存在q,m 使得$n-1=2^q m$, ($q\geq 1$). 序列的

$$a^m(\mathrm{mod}\, n), a^{2m}(\mathrm{mod}\, n), a^{4m}(\mathrm{mod}\, n), \ldots, a^{2^q m}(\mathrm{mod}\, n)$$

最后一项为$a^{n-1}(\mathrm{mod}\ n)$, 且每一项是前面一项的平方.

对于任意i（$i=0,1,\ldots q-1$）, 判断

$$a^{2^q m}(\mathrm{mod}\ n)$$

是否为1 和$n-1$,且它的后一项是否为1.

如果其后项为1，但本项不等于1 和$n-1$, 则它就是非平凡的根，从而知道n 不是素数.

Miller-Rabin算法（续）

例如　n=561, n-1=560=$2^4 \cdot 35$, 假设 a=7, 构造的序列为

$7^{35} \pmod{561} = 241$

$7^{2^1 35} \pmod{561} = 7^{70} \pmod{561} = 298$,

$7^{2^2 35} \pmod{561} = 7^{140} \pmod{561} = 166$,

$7^{2^3 35} \pmod{561} = 7^{280} (\pmod{561} = 67$,

$7^{2^4 35} \pmod{561} = 7^{560} \pmod{561} = 1$,

可以判定n 为合数.

随机选择正整数$a \in \{2,3,\ldots, n-1\}$, 然后进行上述测试. 可以证明该算法每次测试出错的概率至多为1/2. 重复运行k 次，可以将出错概率降到至多2^{-k}.

18.2子环、理想、商环、环同态

- 子环
  - 子环定义
  - 子环判别
- 理想
- 商环
- 环同态及其性质

子环定义及其判别

定义: 非空子集关于环中运算$+, \cdot$ 构成环.

实例: nZ 是$<Z,+,\cdot>$的**子环**

子环就是子代数，任何环都存在平凡子环

判别: 子加群判别+子半群判别

类别: 子整环、子除环、子域

举例:

整数环Z，有理数环Q都是实数环R的真子环。

$\{0\}$和R也是实数环R的子环，称为**平凡子环**。

子环判定定理

定理 设$<A,+,\bullet>$是环，S是A的非空子集，若

(1) $\forall a,b\in S$，$a-b\in S$

(2) $\forall a,b\in S$，$ab\in S$

则S是$<A,+,\bullet>$的子环。

证明： 由(1)S关于环中的加法构成子群。

由(2)S关于环中的乘法构成子半群。

显然S中关于加法的交换律以及乘法对加法的分配律成立的。

因此，S是R的子环。

理想

定义：设 D 是环$<R,+,\cdot>$的非空子集，若

(1) $<D,+>$构成Abel 群

(2) $\forall r\in R,\ rD\subseteq D,\ Dr\subseteq D$

则称$<D,+,\cdot>$是环R 的**理想**.

说明：**左理想(只满足$rD\subseteq D$)与右理想**

$$H=\left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\middle| a,b\in R\right\}$$

为$M_2(R)$的左理想，不是右理想.

- **理想D是R 的子环，但是子环不一定是理想.**

如：$<Z,+,\cdot>$是$<R,+,\cdot>$的子环，但不是理想.

平凡理想：$\{0\}$, R 自身.

例题

例1 R 为交换环，$1\in R$, 且$1\neq 0$, 则R 为域当且仅当R 只含有平凡理想.

证 "⇒" 设D 为理想，$D\neq\{0\}$，$\exists x\in D$,

$$x\neq 0 \Rightarrow x^{-1}\in R \Rightarrow 1= x^{-1}x\in D \Rightarrow \forall r\in R, r= r\cdot 1\in D,$$

$$R=D$$

"⇐" $\forall x\neq 0, x\in R$, 令 $Rx = \{ rx \mid r\in R \}$.

$\forall r_1x, r_2x \in Rx$,

$$r_1x-r_2x = (r_1-r_2)x\in Rx$$

因此 $<Rx,+>$构成Abel 群.

$\forall r_1x\in Rx, r_2\in R$

$$(r_1x)r_2 = (r_1r_2)x \in Rx , r_2(r_1x) = (r_2r_1)x\in Rx,$$

Rx 是理想，因此$Rx=R$, 存在y 使得$yx=1$, x 有逆元.

商环

定义 D 为 R 的理想，$\forall x \in R$,

$$\overline{x} = D + x = \{d + x \mid d \in D\}$$

$$R/D = \{\overline{x} \mid x \in R\}$$

$$\overline{x} + \overline{y} = \overline{x + y}$$

$$\overline{x} \cdot \overline{y} = \overline{x \cdot y}$$

称 $<R/D,+,\cdot>$ 构成环，为 R 关于 D 的**商环**.

注：良定义验证

$$\overline{x} = \overline{x'}, \overline{y} = \overline{y'} \Rightarrow x' = d_1 + x, y' = d_2 + y$$

$$\overline{x'}\,\mathrm{g}\,\overline{y'} = \overline{(d_1 + x)(d_2 + y)} = \overline{d_1 d_2 + x d_2 + d_1 y + xy}$$

$$= \overline{d + xy} = \overline{xy} = \overline{x} \cdot \overline{y}$$

商环的实例

实例：$\langle Z_6,\oplus,\otimes\rangle$

理想 $\{0\}$, $\{0,2,4\}$, $\{0,3\}$, Z_6

商环 $Z_6/\{0\} = \{\ \{0\}, \{1\}, \{2\}, \{3\}, \{4\}, \{5\}\ \}$,

$Z_6/Z_6 = \{\ Z_6\ \}$

$Z_6/\{0,3\} = \{\ \{0,3\}, \{1,4\}, \{2,5\}\ \}$,

$Z_6/\{0,2,4\} = \{\ \{0,2,4\}, \{1,3,5\}\ \}$

$Z_6/\{0,3\}$上的运算表

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{1}$

环同态

环同态 $f: R_1 \to R_2$

$$f(x+y) = f(x) + f(y)$$

$$f(xy) = f(x)\, f(y)$$

同态核： $\ker f = \{\, x \mid x \in R_1, f(x) = 0 \,\}$

实例： $f_c: Z \to Z_c, f_c(x) = x \bmod c$，$c$ 为整数

$$\ker f_c = cZ$$

环同态的性质

1. $f(0)=0, f(1)=1$，$f(-x)=-f(x), f(x^{-1}) = f(x)^{-1}$

2．(1) S 是R_1 的子环，则$f(S)$是R_2 的子环

(2) T 是R_2 的子环，则$f^{-1}(T)$是R_1 的子环

(3) D 是R_1 的理想，则$f(D)$是$f(R_1)$的理想

(4) I 是R_2 的理想，则$f^{-1}(I)$是R_1 的理想

3．$\ker f = \{x|x\in R_1, f(x)=0\}$，则$\ker f$ 是R_1 的理想

4．同态基本定理

环R 的任何商环R/D 是R 的同态像

若$R \sim R'$, 则 $R' \cong R/\ker f$

性质的证明

证：

2. (2) $f^{-1}(\mathrm{T})$非空，$\forall x,y\in f^{-1}(T)$，

$\exists a,b\in T$ 使得$f(x)=a, f(y)=b$,

$$f(x-y)=f(x)-f(y)=a-b\in T,\ x-y\in f^{-1}(T)$$

$$f(xy)=f(x)f(y)=ab\in T,\ xy\in f^{-1}(T)$$

(3) $f(D)$是$f(R_1)$的子加群，且为Abel 群.

$\forall x\in f(D),\ r\in f(R_1)$,

$\exists a\in D$,使得$f(a)=x$, $\exists b\in R_1, f(b)=r$,

$$xr=f(a)f(b)=f(ab)\in f(D)$$

同理，$rx\in f(D)$

性质证明（续）

3．$\ker f = \{ x \mid x \in R_1, f(x)=0 \}$

证　$\ker f$ 是R_1 的理想

$\ker f$ 是$<R_1,+>$的正规子群.

$\forall x \in \ker f, r \in R_1,$

$f(xr) = f(x)f(r) = 0\, f(r) = 0$

$xr \in \ker f$，同理$rx \in \ker f$.

作业

- 复习要点

  环的定义

  特殊环的判别

  有限域的元素数满足什么性质

  商环的定义

  环同态的性质

- 书面作业：

  习题十八，4, 5, 7,

- 自学有限域上的多项式环