第十八章　环与域

- 环的定义及其性质
  - 环的定义
  - 环的性质
  - 特殊的环
  - 有限域
- 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

- 环定义：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：$0, 1, -x, x^{-1}, nx, x^n, x-y,$
- 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. $$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{j=1}^{m} b_j\right) = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j$$
6. $(na)b = a(nb) = n(ab)$

特殊的环

- 交换环、含幺环
- 无零因子环 $ab=0 \Rightarrow a=0$或$b=0$
  - 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.
- 整环：交换、含幺、无零因子环
- 除环：$|R|>1, <R^*,\cdot>$ 构成群
- 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：$H=\left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} | a,b \in R\right\}$ 为除环，不是域
  - Z_p是域

例题

例1 p, q 为不等的素数，证明无 $p\,q$ 阶的整环.

证：假设 R 为 $p\,q$ 阶的整环，则$<R,+>$为 $p\,q$ 阶的Abel群. 存在 p 阶元 a，q 阶元 b. 所以 $|a+b| = p\,q$, $<R,+>$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

$$x\,y = (pc)\,(qc) = pq\,c^2 = 0$$

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.

有限域的性质

设 F 为有限域，则存在素数 p 使得 $|F| = p^n$,

证明思想：设 F 的特征为 p，

$A = <1> = \{ 0, 1, \ldots, p-1 \}$

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

$|Ax_1| = p$

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

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

$3^{340} \pmod{341} \equiv 56$，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数的问题

素数测试的另一个条件

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

证明 $x^2 (\mathrm{mod}\ n)=1 \Leftrightarrow x^2-1=0\ (\mathrm{mod}\ n)$

$\Leftrightarrow (x+1)(x-1) = 0 (\mathrm{mod} n)$

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

$\Leftrightarrow x=-1$ 或 $x=1$

称 $x \neq \pm 1$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:

$x^2 (\mathrm{mod}\ 5) \equiv 1 \Leftrightarrow x=1$ 或 $x=4$

$x^2 (\mathrm{mod}\ 12) \equiv 1 \Leftrightarrow x=1$ 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

$$a^m \pmod n, a^{2m} \pmod n, a^{4m} \pmod n, \ldots, a^{2^q m} \pmod n$$

的最后一项为$a^{n-1} \pmod n$, 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

$$a^{2^i m} \pmod n$$

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$a \in \{2,3,\ldots, n\text{-}1\}$, 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，平凡子环存在
- 判别：子加群判别 + 半群判别
- 子整环、子除环、子域

理想

- 理想： D是环 $<R, +, \cdot>$ 的非空子集，满足
  - $<D, +>$ 构成 Abel 群
  - $\forall r \in R,\ rD \subseteq D,\ Dr \subseteq D$
- 说明：
  - 左理想 (只满足 $rD \subseteq D$) 与右理想

    $D = \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \mid a,b \in R \right\}$ 为 $M_2(R)$ 的左理想，不是右理想.
  - 理想是 R 的子环，但是子环不一定是理想.

    $<\mathbf{Z}, +, \cdot>$ 是 $<\mathbf{R}, +, \cdot>$ 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 “$\Rightarrow$” 设 D 为理想，$D \neq \{0\}$，$\exists\, x \in D$,

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

$R = D$

“$\Leftarrow$” $\forall x \neq 0, x \in R$, 令 $Rx = \{ rx \mid r \in R \}$. 证明 Rx 为理想.

$\forall r_1 x, r_2 x \in Rx$,

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

因此 $< Rx, + >$ 构成 Abel 群.

$\forall\, r_1 x \in Rx, r_2 \in R$

$$(r_1 x) r_2 = (r_1 r_2) x \in Rx, \quad r_2 (r_1 x) = (r_2 r_1) x \in Rx$$

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，$\forall x \in R$,

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

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

$$\overline{x} + \overline{y} = \overline{x + y}, \quad \overline{x} \cdot \overline{y} = \overline{x \cdot y}$$

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

注：良定义验证

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

$$\overline{x'} \cdot \overline{y'} = \overline{x' \cdot y'} = \overline{(d_1 + x)(d_2 + y)}$$

$$= \overline{d_1 d_2 + x d_2 + d_1 y + xy} = \overline{d + xy} = \overline{xy} = \overline{x} \cdot \overline{y}$$

商环的实例

实例：$< Z_6, \oplus, \otimes >$

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

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

$Z_6 / Z_6 = \{ Z_6 \}$

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

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

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

$$f_c: \mathbf{Z} \to \mathbf{Z},\ f_c(x) = cx,\ c\text{为整数}$$

$$\ker f_0 = \mathbf{Z}$$

$$\ker f_c = \{ 0 \} \qquad c \neq 0$$

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. $\ker f=\{x \mid x\in R_1, f(x)=0\}$，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) 证 $f^{-1}(T)$是 R_1的子环.

$f^{-1}(T)$ 非空，$\forall x, y \in f^{-1}(T)$，$\exists a,\ b \in T$ 使得

$$f(x) = a,\quad f(y) = b,$$

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

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

(3) 证 $f(D)$是理想.

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

证明 $\ker f$ 是 R_1 的理想

证 $\ker f$ 是 $< R_1, + >$ 的正规子群.

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

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

$x r \in \ker f$.

同理 $r x \in \ker f$.