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

5. 子环

定义（子环）

设$(R,+,\cdot)$是一个环，S是R的一个非空子集．若S对加法$+$和乘法$\cdot$也构成一个环，则称S是R的一个子环，R是S的一个扩环．

- 实数域上的2阶方阵关于矩阵加法和乘法构成环．其子集

$$\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a,b,d \in \mathbb{R} \right\}$$

构成一个子环．

5. 子环

定义（子环）

设$(R,+,\cdot)$是一个环，S是R的一个非空子集. 若S对加法$+$和乘法$\cdot$也构成一个环，则称S是R的一个子环，R是S的一个扩环.

- 实数域上的2阶方阵关于矩阵加法和乘法构成环. 其子集

$$\left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a,b,d \in \mathbb{R} \right\}$$

  构成一个子环.

子环的几个简单性质:

1. $\{0\}$和R本身也是R的子环.
2. 设S是R的非空子集，则S是R的子环的充要条件是对于任意的$a,b\in S$，有$a-b\in$和$ab\in S$.
3. S_1和S_2是R的子环，则$S_1\cap S_2$也是子环.

理想(Ideal)

定义 (理想)

设$(R,+,\cdot)$是一个环, I是一个子环, 对于任意的$a \in I$和任意的$r \in R$,
若满足$ra \in I$, 则称I是R的一个左理想.
若满足$ar \in I$, 则称I是R的一个右理想.
若I同是左理想和右理想, 则称I是R的一个理想.
$\{0\}$和R本身是R的理想, 称为平凡理想.

1. 设$\mathbb{Z}$为整数环. m为一个非负整数, $m\mathbb{Z}$是$\mathbb{Z}$的一个理想.
2. 设$\mathbb{Q}[x]$是有理数上的多项式环, S是关于x的所有常数项为零的一元多项式集合, 则S是$\mathbb{Q}[x]$一个理想.
3. 实数域上的2阶方阵关于矩阵加法和乘法构成环. 其子集

$$\left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in \mathbb{R} \right\}$$

构成一个子环, 但不是一个理想.

理想的判定和性质

定理

设$(R,+,\cdot)$是一个环, I是左(右)理想的充要条件是:

1. 对于任意的$a, b \in I$, 有$a - b \in I$,
2. 对于任意的$a \in I$和任意的$r \in R$, 有$ra \in I (ar \in I)$.

- 对于交换环来说, 不区分左右理想.
- 设环R有单位元, I是理想. 如果$1 \in I$, 则$I = R$.
- 如果I, J都是环R的理想, 则$I + J$, $I \cap J$都是R的理想.

生成理想，主理想和主理想环

定义

设R是环，S是R的一个非空子集. 包含S的最小子环称由S生成的子环，记作(S).
或者，$\{A_i\}$是包含S的所有理想，则$(S)=\cap A_i$.
特别地，由一个元素生成的理想(a)叫做主理想*(principal ideal)*.
如果R的所有理想都是主理想，则称R是主理想环.

定理

当$S=\{a\}$时，由S生成的理想可以表示为:

$$(a)=\left\{\sum r_i a s_i + ra + ar' + na \,|\, r_i, s_i, r, r' \in R, n \in Z\right\}$$

当R是单位元的交换环时，(a)可以简化为:

$$(a)=\{xa \,|\, x\in R\}=aR$$

生成理想的例子

- 设整数环$\mathbb{Z}$, 非负整数m的生成理想是

$$(m) = \{km \mid k \in Z\} = mZ,$$

  且$\mathbb{Z}$中的全部理想为(m), $m = 0, 1, 2, \cdots$. 因此, $\mathbb{Z}$是主理想环.

- 设$\mathbb{Q}[x]$是有理数上的多项式环, 关于x的所有常数项为零的一元多项式集合

$$\{a_1x + a_2x^2 + \cdots + a_nx^n \mid a_i \in F, n \in \mathbb{Z}^+\} = \{xf(x) \mid f(x) \in \mathbb{Q}[x]\}$$

  是x的生成理想.

主理想环

例: 整数环$\mathbb{Z}$是主理想环.
证明: 设I是$\mathbb{Z}$中的非零理想. 当$a \in I$, 有$0a = 0 \in I$, $a - a = 0 \in I$, $-a \in I$, 因此I中有正整数. 整数有良序性, 设d是I中最小正整数. 则$I = (d)$. 这是因为, $\forall a \in I$, 存在整数d, 使得

$$a = dq + r, \quad 0 \leq r < d.$$

由于$a \in I$, $dq \in I$, 所以$r = a - dq \in I$. 由$r < d$以及d是I中最小正整数, 可得$r = 0$, $a = dq \in (d)$. 从而$I \subseteq (d)$, 显然有$(d) \subseteq I$, 所以$I = (d)$.

例: $\mathbb{Q}[x]$是主理想环.
说明: 设I是$\mathbb{Q}[x]$中的任一理想, $q(x) \in I$, $\deg(q(x)) = d$是最小次多项式. 对于任意的$g(x) \in H$, 有$g(x) = q(x)p(x) + r(x)$, $r(x) \in I$, 由d的最小性, 可得$r(x) = 0$.

商环

定义

设R是环, I是R的一个理想, 在R对I的商集为$R/I = \{a + I \mid a \in R\}$.
在R/I中定义加法

$$(a + I) + (b + I) = (a + b) + I,$$

定义乘法

$$(a + I) \cdot (b + I) = (ab + I),$$

则R对I的商集关于上述的加法和乘法构成环, 被称为商环.

定理（自然同态）

设f是群G到群G'的同态映射, 则f的核$\ker f = f^{-1}(1)$是群G的一个正规子群.
反过来, 如果K是群G的正规子群, 则映射

$$\varphi : G \to G/K, \quad g \mapsto gK$$

是核为K的同态映射, 称为自然同态.

商环

定义

设R是环, I是R的一个理想, 在R对I的商集为$R/I = \{a + I \mid a \in R\}$.
在R/I中定义加法

$$(a + I) + (b + I) = (a + b) + I,$$

定义乘法

$$(a + I) \cdot (b + I) = (ab + I),$$

则R对I的商集关于上述的加法和乘法构成环, 被称为商环.

定理（自然同态）

设f是环R到环R'的同态映射, 则f的核$\ker f = f^{-1}(0)$是环R的一个理想.
反过来, 如果I是环R的理想, 则映射

$$s : R \to R/I, \quad r \mapsto r + I$$

是核为I的同态映射, 称为自然同态.

环同态基本定理

定理（环同态基本定理)

设f是环R到环R'的满同态映射, $I=\ker f$, 则存在R/I到$f(R)$的同构映射

$$\bar{f}: r+I \mapsto f(r)$$

使得$f=\bar{f}\cdot s$, 其中s是环R到商环R/I 得自然同态.

环同态基本定理

定理（环同态基本定理）

设f是环R到环R'的满同态映射，$I=\ker f$，则存在R/I到$f(R)$的同构映射

$$\bar{f}: r+I \mapsto f(r)$$

使得$f=\bar{f}\cdot s$，其中s是环R到商环R/I 得自然同态.

定理（群同态基本定理）

设f是群G到群G'的满同态映射，$K=\ker f$，则存在G/K到$f(G)$的同构映射

$$\bar{f}: gK \mapsto f(g)$$

使得$f=\bar{f}\cdot\varphi$，其中φ是群G到商群G/I的自然同态.

素理想

定义

设P是环R的理想. P被称为素理想, 如果$P \neq R$, 且对任意理想A和B, 当$AB \subset P$时, 有$A \subset P$或者$B \subset P$.

定理

设P是环R的理想, $P \neq R$, 且对任意$a, b \in R$. 如果当$ab \in P$时, 有$a \in P$或者$b \in P$, 则P是环R的素理想.

定理

如果P是环R的素理想, 且R交换环. 对任意$a, b \in R$, 如果$ab \in P$, 则$a \in P$或者$b \in P$.

证明: (必要性) 有理想$A, B, AB \subset P$, 有$A \not\subset P$, 则存在元素$a \in A$, $a \notin P$. $\forall b \in B$, $ab \in AB \subset P$, $a \notin P$ 可得$b \in P$, 即$B \subset P$, 因此P是素理想.
(充分性) P是素理想, 任意$a, b \in R$, 当$ab \in P$时, 有$(a)(b) = (ab) \subset P$, 由素理想的定义, 有$(a) \subset P$或者$(b) \subset P$, 可得$a \in P$或者$b \in P$.

素理想的例子

- 设$\mathbb{Z}$是整数环. $\mathbb{Z}$中任何理想都是主理想，即由一个整数d生成的理想(d). 这种理想是由d的全体倍数构成的集合. (d)是素理想当且仅当d是素数.
- 设$\mathbb{Z}[x]$是整数上的多项式环, 即系数为整数的多项式全体构成的集合. $\mathbb{Z}[x]$中的由x生成的素理想(x)是素理想.
- 设$\mathbb{Q}[x]$是有理数域$\mathbb{Q}$上的多项式环, 即系数取自$\mathbb{Q}$的多项式全体构成的集合. $\mathbb{Q}[x]$中的素理想就是由不可约多项式生成的理想.
- 设R是整环. R的零理想是素理想.

从素理想到整环

- 对于整数环$\mathbb{Z}$的理想(p)，如果$a \in (p)$则$p \mid a$，所以(p)为素理想的充要条件是

$$p \mid ab \Rightarrow p \mid a \text{ 或 } p \mid b.$$

所以p是素数时，(p)是$\mathbb{Z}$中的素理想. 整数集合$\mathbb{Z}$模p得到域$\mathbb{Z}_p$，那么一般整环模素理想得到什么呢?

定理

R是有单位元的交换环，理想P是素理想的充要条件是商环R/P是整环.

证明: (充分性): R/P有单位元$1+P$和零元$0+P$. 由于P是素理想，R中的单位元$1 \notin P$，所以$1+P \neq 0+P$. 若不为零的两个元素$(a+P)(b+P) = P = 0_{R/P}$，则$ab+P = P$，因此$ab \in P$. 由素理想的定义和定理可得$a \in P$或$b \in P$，于是有$a+P = P$或者$b+P = P$为零. 所以R/P中无零因子.

(必要性): $\forall a, b \in R$, $ab \in P$，有$(a+P)(b+P) = ab+P = P = 0_{R/P}$. 因为$R/P$是整环，无零因子，所以$a+P = P$ 或者$b+P = P$，由此$a \in P$或者$b \in P$，根据前述素理想的定义和定理可得P为素理想.

极大理想与素理想

定义

设R是有单位元的交换环，M是R的理想，且$M \neq R$. 称M为R的极大理想，如果对于任意理想N，当$M \subseteq N \subseteq R$时，有$N = R$或者$N = M$，即环$R$除外，不存在一个更大的理想真包含$M$.

定理

整环中的每个素理想都是极大理想.

定理10.6.4

定理

在有单位元的环中，极大理想总是素理想.

定理10.6.5

定理

R是有单位元的交换环, 如下条件等价:

1. R是域.
2. 除$\{0\}$和R之外, R上没有其他理想, 即没有真理想.
3. $\{0\}$是R的极大理想.
4. 每个非零环同态$R \mapsto R'$是单同态.

证明:

($1 \to 2$) 设I是理想, $a \in I$, 则$aa^{-1} \in I$, 所以$1 \in I$, 可得$I = R$.

($2 \to 3$) 极大理想的定义

($3 \to 4$) 设f是$R \mapsto R'$的非零的环同态, 则f的核$\ker f$是一个包含零元素的理想, 而现在$\{0\}$是R的极大理想, 所以有$\ker f = \{0\}$. 于是, 根据f的同态性, f必为单射,

($4 \to 1$) 如果R中存在非零不可逆元素a, 则$(a) \neq \{0\}$且$(a) \neq R$, 即(a)是非平凡理想. 于是, R到R/I的自然同态不是单射, 矛盾, 因此, R是域.

从极大理想到域

定理

设R是有单位元的交换环, M是R中的极大理想的充要条件是商环R/M是域.

证明: ($\Rightarrow$) 需要证明商环R/M的元素都有逆元. 设$a+M\neq 0$, 则$a\notin M$.
考察理想$(a)+M=Ra+M$, 显然$M\subset(a)+M$. 由于M是极大理想, 所以
$(a)+M=R$. 单位元$1\in(a)+M$, 于是存在$r\in R, m\in M$, 使得$ra+m=1$, 即

$$(r+M)(a+M)=ra+M=1-m+M=1+M,$$

所以, $a+M$的逆元是$r+M$.
($\Leftarrow$) 设$a\in R\setminus M$, 则$a+M$是R/M的非零元. 因为R/M是域, 所以存在$r+M$, 使得

$$(a+M)(r+m)=1+M,$$

从而有$1+M\in Ra+M=(a)+M$, 即$(a)+M=R+M=R$. 所以M是极大理想.

极大理想和素理想的一个例子

设$\mathbb{Z}[X]$是整数上的多项式环, 环中元素为$f(X) = a_0 + \ldots + a_n X^n$, 其中$n = 0, 1, \ldots$.

- 由X生成的理想为$(X) = \{f(X) | f(X) \in \mathbb{Z}[X], a_0 = 0\}$.
- 由2生成的理想为$(2) = \{f(X) | a_i \equiv 0 \bmod 2\}$.

(2)和(X)都是真理想(非平凡理想), 并且$2 \notin (X)$以及$X \notin (2)$.

考虑3个环同态映射f_1, f_2, f_3:

- $f_1 : \mathbb{Z}[X] \to \mathbb{Z}, \quad f(X) \mapsto a_0$.
- $f_2 : \mathbb{Z}[X] \to \mathbb{Z}_2[X], \quad f(X) \mapsto f(X) \bmod 2$, 即将$f(X)$的系数都 mod 2.
- $f_3 : \mathbb{Z}[X] \to \mathbb{Z}_2, \quad f(X) \mapsto a_0 \bmod 2$.

(X)是素理想, 因为(X)是f_1的核, 而$\mathbb{Z}$是整环. (X)不是极大理想, 因为$(X) \subset (2, X)$.
(2)是素理想, 因为(2)是f_2的核, 而$\mathbb{Z}_2[X]$是整环.
(2)不是极大理想, 因为$(2) \subset (2, X)$, 而$(2, X)$是真理想.
$(2, X)$是极大理想, 因为$\ker f_3 = \{a_0 + Xg(X) \,|\, g(X) \in \mathbb{Z}[X], a_0 = 0 \bmod 2\} = (2, X)$.
因为$\mathbb{Z}_2$是域, 所以$(2, X)$是极大理想

环小结

1. 理解环, 交换环, 有单位元环, 零因子环, 整环, 域的基本概念.
2. 理解交换环上的整除, 以及单位, 相伴元, 不可约元的基本概念.
3. 理解环的同态与同构的基本概念.
4. 理解环特征的基本概念和基本性质.
5. 理解子环, 理想, 商环, 主理想, 素理想, 极大理想的基本概念.
6. 给定集合和运算能够判断是否构成环, 给定环的子集合能够判断是否构成子环或理想.
7. 给定环的理想能够确定其商环, 能够判断该商环是整环还是域, 以及能够判断该理想是素理想还是极大理想.

作业

1. 设D是无平方因数的整数. 证明集合$\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} \mid a, b \in \mathbb{Z}\}$对于通常的加法和乘法构成一个整环.
2. 证明集合$\mathbb{Q}[\sqrt{2}+\sqrt{3}] = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$对于通常的加法和乘法构成一个域.
3. 证明非零有限整环一定是域.
4. 设环$R = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$, 其加法运算和乘法运算为通常的加法和乘法. 令
$$\varphi: R \mapsto R, \quad \varphi(a + b\sqrt{2}) = a - b\sqrt{2}.$$
证明φ是R的一个自同构映射.
5. 设$M_2(\mathbb{R})$是实数上全体2×2矩阵对于加法和乘法构成的环, 令
$$\varphi: \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \det \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$
试问φ是否为一个同态映射.
6. 列出$\mathbb{Z}/6\mathbb{Z}$的所有理想.
7. 设$\mathbb{Q}$是有理数域. 描述多项式环$\mathbb{Q}[x]$的主理想(x^2)包含的所有元素, 以及商环$\mathbb{Q}[x]/(x^2)$包含的所有元素.
8. 设$R = 2\mathbb{Z}$. 证明$I = \{4r \mid r \in R\}$是R的一个理想, 而(4)是R的一个极大理想, 并判断商环$R/(4)$是否为域.