

## 0.1 素理想与极大理想

### 定义 0.1 (素理想)

若交换幺环  $R$  的理想  $P$  满足

- (1)  $P \neq R$ , 即  $P$  是  $R$  的真理想;
- (2) 若  $ab \in P$ , 则  $a \in P$  或  $b \in P$ ,

则称  $P$  为  $R$  的素理想.

### 定义 0.2 (极大理想)

设环  $R$  中的理想  $M \neq R$  且不存在  $R$  的理想  $A$ , 使  $M \subset A \subset R$ , 则称  $M$  为  $R$  的极大理想.

**注** 由定义可知

$$A \text{ 为环 } R \text{ 的极大理想} \iff \forall A \subset M \subseteq R, \text{ 有 } M = R \iff \forall A \subseteq M \subseteq R, \text{ 有 } M = R \text{ 或 } M = A.$$

### 命题 0.1

- (1) 设  $p$  为素数, 则  $\langle p \rangle = p\mathbb{Z}$  为  $\mathbb{Z}$  的素理想, 同时也是  $\mathbb{Z}$  的极大理想.
- (2)  $\mathbb{Z}$  中非平凡理想  $I = m\mathbb{Z}$  为素理想或极大理想当且仅当  $m$  为素数 (或负素数).

**证明**

(1) 设  $ab \in \langle p \rangle = p\mathbb{Z}$ , 即  $p \mid ab$ . 由  $p$  为素数知  $p \mid a$  或  $p \mid b$ , 亦即  $a \in p\mathbb{Z} = \langle p \rangle$  或  $b \in p\mathbb{Z} = \langle p \rangle$ , 因而  $\langle p \rangle$  为素理想.

其次, 设  $\mathbb{Z}$  的理想  $A$  满足  $\langle p \rangle \subseteq A \subseteq \mathbb{Z}$ . 由命题??知  $\mathbb{Z}$  为 p.i.d., 故有  $A = \langle n \rangle$ . 由  $p \in \langle n \rangle$ , 因而  $n \mid p$ . 因  $p$  为素数, 故  $n = \pm 1$  或  $n = \pm p$ . 若  $n = \pm 1$ , 则  $A = \mathbb{Z}$ ; 若  $n = \pm p$ , 则  $A = \langle p \rangle$ . 由此知  $\langle p \rangle$  是  $\mathbb{Z}$  的极大理想.

(2) 若  $m = m_1m_2 (m_i \neq \pm 1, i = 1, 2)$ , 则  $m_1m_2 = m \in I$ . 但  $m_i \notin I (i = 1, 2)$ , 故  $I$  不是素理想. 又  $m\mathbb{Z} \subset m_1\mathbb{Z} \subset \mathbb{Z}$ , 故  $I$  不是极大理想.

□

### 引理 0.1

设  $R$  为交换幺环, 则有

- (1)  $\{0\}$  是  $R$  的素理想当且仅当  $R$  为整环;
- (2)  $\{0\}$  是  $R$  的极大理想当且仅当  $R$  为域.

♡

**证明**

(1) 设  $R$  为整环. 若  $a \neq 0, b \neq 0$ , 即  $a \notin \{0\}, b \notin \{0\}$ , 则  $ab \neq 0$ , 即  $ab \notin \{0\}$ , 因而由素理想的逆否定义知  $\{0\}$  为素理想.

反之, 设  $\{0\}$  为素理想. 又  $a, b \notin \{0\}$ , 故  $ab \notin \{0\}$ , 即  $a \neq 0, b \neq 0$  得出  $ab \neq 0$ . 又  $R$  是交换幺环, 故  $R$  为整环.

(2) 设  $\{0\}$  为极大理想.  $\forall a \in R$  且  $a \neq 0$  有  $\langle a \rangle \supset \{0\}$ , 故  $\langle a \rangle = R$ . 由  $R$  含有幺元 1, 故  $1 \in \langle a \rangle = aR$ . 因而  $\exists a^{-1} \in R$ , 使得  $aa^{-1} = 1$ . 再由  $R$  可交换知  $R$  是一个域.

反之, 设  $R$  是一个域,  $A$  为  $R$  的理想且  $A \neq \{0\}$ , 即  $\exists a \in A, a \neq 0$ . 又  $R$  为域, 故  $\exists a^{-1}$ , 使  $1 = a^{-1}a$ , 再由  $A$  为  $R$  的理想知  $a^{-1}a \in A$ . 进而对  $\forall b \in R$  有  $b = b \cdot 1 \in A$ , 因而  $A = R$ , 故  $\{0\}$  为极大理想.

□

### 定理 0.1

设  $R$  为交换幺环,  $P$  与  $M$  为  $R$  的理想, 则

- (1) 当且仅当  $R/P$  为整环时,  $P$  为素理想;
- (2) 当且仅当  $R/M$  为域时,  $M$  为极大理想.

♡

**证明**

- (1) 设  $\pi$  为  $R$  到  $R/P$  上的自然同态. 若  $P$  为素理想, 由  $\pi$  为满同态, 故可设  $\pi(a), \pi(b) \in R/P$  且  $\pi(a) \neq 0, \pi(b) \neq 0$ , 亦即  $a, b \notin P$ , 则由  $P$  为素理想知  $ab \notin P$ , 即  $\pi(ab) = \pi(a)\pi(b) \neq 0$ , 因而  $R/P$  为整环.  
反之, 若  $R/P$  为整环且  $ab \in P$ , 则有  $\pi(ab) = \pi(a)\pi(b) = 0$ , 因而  $\pi(a) = 0$  或  $\pi(b) = 0$ , 即  $a \in P$  或  $b \in P$ , 所以  $P$  是素理想.
- (2) 设  $R$  的理想  $A$  满足  $M \subseteq A \subseteq R$ , 于是由推论??知  $A/M$  是  $R/M$  的理想. 当  $M$  为极大理想时有  $M = A$  或  $R = A$ . 故  $R/M$  仅有的理想为  $M/M = M = \{0\}$  与  $R/M$ , 即  $\{0\}$  为极大理想, 故由引理 0.1 知  $R/M$  为域.  
反之, 设  $R$  的理想  $A$  满足  $M \subset A \subseteq R$ , 由推论??知  $A/M$  是  $R/M$  的理想且  $A/M \neq M = \{0\}$ . 若  $R/M$  为域, 则由引理 0.1 知  $\{0\}$  为  $R/M$  的极大理想, 于是  $A/M = R/M$ . 故  $A = R$ , 即  $M$  为极大理想.

□

**推论 0.1**交换么环  $R$  的极大理想  $M$  必为素理想.

♡

**证明** 事实上, 由定理 0.1(2) 知  $R/M$  为域, 由命题????知  $R/M$  是整环, 所以再由定理 0.1(1) 知  $M$  为素理想.

□

**定理 0.2**设  $R, R'$  都是交换么环,  $\sigma$  是  $R$  到  $R'$  上的同态,  $N = \ker \sigma$ .若  $H$  是  $R$  中包含  $N$  的素理想(或极大理想), 则  $\sigma(H)$  是  $R'$  中的素理想(或极大理想).反之, 若  $H'$  是  $R'$  的素理想(或极大理想), 则

$$\sigma^{-1}(H') = \{x \in R \mid \sigma(x) \in H'\}$$

为  $R$  中包含  $N$  的素理想(或极大理想).

♡

**证明** 根据定理????有  $R/H \cong R'/\sigma(H)$ , 故由定理 0.1 知  $H(H \supseteq N)$  为素理想(或极大理想)当且仅当  $R/H$  为整环(或域)当且仅当  $R'/\sigma(H)$  为整环(或域), 也当且仅当  $\sigma(H)$  为素理想(或极大理想).

□

**定理 0.3**若  $R$  是交换整环,  $a \in R^*$ , 则由  $a$  生成的主理想  $\langle a \rangle$  为素理想的充分必要条件是  $a$  为素元素.

♡

**证明** 由定理????知当且仅当  $a$  为  $R$  的单位, 即  $a \in U$  时,  $\langle a \rangle = R$ , 故可设  $a \in R^* \setminus U$ . 由  $bc \in \langle a \rangle = aR \iff a \mid bc$ , 故  $\langle a \rangle$  为素理想当且仅当  $b \in \langle a \rangle$  或  $c \in \langle a \rangle$  当且仅当  $a \mid b$  或  $a \mid c$  当且仅当  $a$  为素元素.

□

**推论 0.2**设  $R$  为唯一析因环,  $a \in R^*$ , 则  $\langle a \rangle$  为素理想当且仅当  $a$  为不可约元素.

♡

**注** 从这里可认为素理想的概念在一定意义上是素元素概念的推广.**证明** 由定理 0.3 知  $\langle a \rangle$  为素理想当且仅当  $a$  为素元素. 又由定理??的注知  $a$  为素元素当且仅当  $a$  不可约, 故结论得证.

□

**例题 0.1** 设  $F$  是一个域,  $R = F[x_1, x_2, \dots, x_n]$  是  $F$  上  $n$  元多项式环. 由定理??, 定理 0.3 及推论 0.2 知对  $f \in R$ ,  $\langle f \rangle$  为素理想当且仅当  $f$  为不可约多项式. 因  $R/\langle x_1, x_2 \rangle \cong F[x_3, \dots, x_n]$ , 故由定理 0.1 知由  $x_1, x_2$  生成的理想  $\langle x_1, x_2 \rangle$  也是素理想, 而  $\langle x_1, x_2 \rangle$  不是主理想. 当  $n > 2$  时, 看到  $\langle x_1, x_2 \rangle$  也不是极大理想.

**定理 0.4**

设  $R$  为主理想整环,  $a \in R^*$ , 则  $\langle a \rangle$  为极大理想的充分必要条件是  $a$  为素元素.



**证明** 若  $\langle a \rangle$  为极大理想, 由推论 0.1 知  $\langle a \rangle$  为素理想, 再由定理 0.3 知  $a$  为素元素.

反之, 设  $a$  为素元素. 若有  $R$  的理想  $A$ , 使得  $\langle a \rangle \subseteq A \subseteq R$ . 由于  $R$  为 p.i.d., 故有  $n \in R$ , 使得  $A = \langle n \rangle$ . 于是由  $a \in \langle n \rangle = nR$  得  $n | a$ . 因为  $a$  为素元素, 所以由引理 ?? 知  $a$  也是不可约元素. 从而  $n \sim 1$  或  $n \sim a$ , 于是由定理 ??? 有  $A = \langle n \rangle = R$  或  $A = \langle n \rangle = \langle a \rangle$ , 故  $\langle a \rangle$  为极大理想.

**定理 0.5**

设  $F$  是一个域,  $F[x]$  是  $F$  上的一元多项式环,  $S$  为交换整环且  $F \subseteq S, F, S$  有相同的幺元.

- (1) 若  $u \in S$  是  $F$  上的代数元, 则  $F[u]$  是一个域且存在唯一的次数大于等于 1 的首一不可约多项式  $p(x) \in F[x]$ , 使得

$$\{f(x) \in F[x] \mid f(u) = 0\} \supset \{0\} = \langle p(x) \rangle, \quad F[u] \cong F[x]/\langle p(x) \rangle, \quad \langle p(x) \rangle \cap F = \{0\}.$$

反之, 若  $p(x)$  是不可约多项式, 则  $F[x]/\langle p(x) \rangle$  是  $F$  的扩域.

- (2) 若  $u \in S$  是域  $F$  上的超越元, 则  $F[u]$  是  $F$  上的一元多项式环, 且  $F[u] \cong F[x]$ .

**证明**

- (1) 由代数元的定义知

$$I = \{f(x) \in F[x] \mid f(u) = 0\} \supset \{0\}. \quad (1)$$

显然  $I$  是  $F[x]$  的子环. 由定理 ??? 知  $F[x]$  为 Euclid 环, 再由定理 ?? 知  $F[x]$  为主理想整环, 进而  $I$  也是主理想整环. 于是存在  $p_1(x) \neq 0$ , 使得  $I = \langle p_1(x) \rangle$ . 若  $\deg p_1(x) = 0$ , 则  $I \subseteq F^* = F \setminus \{0\}$ . 从而对  $\forall f(x) \in I$ , 都存在  $a \in F^*$ , 使得  $a = f(u) = 0$ . 故  $I = \{0\}$ , 这与(1)式矛盾! 因此  $\deg p_1(x) \geq 1$ . 于是由定理 ??? 可得

$$\langle p_1(x) \rangle \cap F = p_1(x)F[x] \cap F = \{0\}.$$

令  $g$  为  $F[x]$  到  $F[u]$  的映射, 满足

$$g|_F = \text{id}_F, \quad g(x) = u.$$

显然  $g$  为  $F[x]$  到  $F[u]$  的同态且

$$g(f(x)) = f(u), \quad \forall f(x) \in F[x].$$

从而  $\ker g = I$ . 于是由环的同态基本定理知

$$F[u] \cong F[x]/\langle p_1(x) \rangle.$$

又由  $S$  为整环知  $F[u]$  为  $S$  上添加  $u$  生成的子环也是整环, 故由定理 0.1 知  $\langle p_1(x) \rangle$  为素理想. 由推论 0.2 知  $p_1(x)$  也是不可约多项式. 不妨设  $p_1(x) = up(x)$ , 其中  $u$  是单位,  $p(x)$  是首一多项式. 又由于  $F$  是域, 故由定理 ??? 知  $p_1(x)$  与次数大于等于 1 的首一多项式  $p(x)$  相伴, 从而  $\deg p(x) \geq 1$ . 再由定理 ??? 知  $\langle p(x) \rangle = \langle p_1(x) \rangle$ . 又由命题 ?? 知  $p(x)$  也是不可约多项式, 因而  $p(x)$  为次数大于等于 1 的首一不可约多项式, 且

$$\{f(x) \in F[x] \mid f(u) = 0\} \supset \{0\} = \langle p_1(x) \rangle = \langle p(x) \rangle, \quad F[u] \cong F[x]/\langle p_1(x) \rangle = F[x]/\langle p(x) \rangle, \quad \langle p(x) \rangle \cap F = \langle p_1(x) \rangle \cap F = \{0\}.$$

再由定理 0.1 知  $p(x)$  为  $F[x]$  中的素元素, 再结合定理 0.4 知  $\langle p(x) \rangle$  为极大理想, 由定理 0.1 知  $F[u] \cong F[x]/\langle p(x) \rangle$  为域. 又显然  $F[x]/\langle p(x) \rangle \supseteq F$ , 故  $F[x]/\langle p(x) \rangle$  是  $F$  的扩域.

最后证明  $p(x)$  的唯一性. 若还存在次数大于等于 1 的首一不可约多项式  $p'(x) \in F[x]$ , 使得

$$F[u] \cong F[x]/\langle p'(x) \rangle, \quad \langle p'(x) \rangle \cap F = \{0\}.$$

则

$$F[x]/\langle p(x) \rangle \cong F[u] \cong F[x]/\langle p'(x) \rangle.$$

从而由命题?????知  $\langle p(x) \rangle = \langle p'(x) \rangle$ , 再由定理????知  $p(x) \sim p'(x)$ . 而  $p(x), p'(x)$  都是首一不可约多项式, 故  $p'(x) = p(x)$  或 1. 若  $p'(x) = 1$ , 则与  $\deg p'(x) \geq 1$  矛盾! 因此  $p'(x) = p(x)$ .

反之, 若  $p(x)$  是不可约多项式, 则由推论 0.2 知  $\langle p(x) \rangle$  为素理想, 再由定理 0.3 知  $p(x)$  为  $F[x]$  中的素元素, 于是由定理 0.4 知  $\langle p(x) \rangle$  为极大理想. 故由定理 0.1 知  $F[x]/\langle p(x) \rangle$  是域, 显然  $F[x]/\langle p(x) \rangle \supseteq F$ , 故  $F[x]/\langle p(x) \rangle$  是  $F$  的扩域.

- (2) 因为  $u \in S$  是域  $F$  上的超越元, 所以  $F[u]$  是  $F$  上的一元多项式环. 从推论??知  $u$  是超越元时上述结论成立.

□