第 19、20 次习题课 (诺特环、准素理想)

回顾，主理想整环 (PID) 的每个理想都是主理想，即由单个元素生成。

定义 1 (诺特环)**.** 一个交换环 R 被称为**诺特环（Noetherian ring）**，如果它的每个理想都是有限生成的。

注. 诺特环是主理想整环（PID）的一种推广。PID 的性质在很多环的构造下不保持，但诺特性可以得到很好的继承。例如，$\mathbb{Z}$ 是 PID，但 $\mathbb{Z}[X]$ 不是 PID，因为理想 $(2, x)$ 不是主理想。(练习：试着证明 $\mathbb{Z}[X]$ 是诺特环。)

定理 1 (诺特环的等价刻画)**.** 设 R 是交换环，则以下条件等价：

(1) R 是诺特环。

(2) R 的每个理想的升链 $I_1 \subseteq I_2 \subseteq \cdots$ 是稳定的，即存在 $k > 0$ 使得 $I_k = I_{k+1} = \cdots$。

证明. (1) $\Rightarrow$ (2): 设 $I_1 \subseteq I_2 \subseteq \cdots$ 是理想的升链。令 $I = \bigcup_{n\geq 1} I_n$，易知 I 是 R 的一个理想。由于 R 是诺特环，所以 I 是有限生成的，即存在 $a_1, \ldots, a_s \in R$ 使得 $I = Ra_1 + \cdots + Ra_s$。由 $I_1 \subseteq I_2 \subseteq \cdots$ 及 $I = \bigcup_{n\geq 1} I_n$ 知存在 $k > 0$ 使得 $a_1, \ldots, a_s \in I_k$。从而 $I \subseteq I_k \subseteq I_{k+1} \subseteq \cdots \subseteq I$。故 $I_k = I_{k+1} = \cdots$。
(2) $\Rightarrow$ (1): 任取 R 的一个理想 I。反设 I 不是有限生成的，我们来构造一个理想的严格升链。选取 $a_1 \in I$，由于 I 不是有限生成的，所以 $(a_1) \subsetneq I$。从而存在 $a_2 \in I \setminus (a_1)$。类似地，$(a_1, a_2) \subsetneq I$，存在 $a_3 \in I \setminus (a_1, a_2)$。如此继续，得到严格升链

$$(a_1) \subsetneq (a_1, a_2) \subsetneq (a_1, a_2, a_3) \subsetneq \cdots \subseteq I.$$

这与条件 (2) 矛盾。因此 I 是有限生成的，从而 R 是诺特环。 $\square$

题 1. 设 R 是诺特环，$\varphi : R \to R$ 是满的环同态，则 φ 是单射，从而是环同构。

证明. 设 $K_n = \ker(\varphi^n)$，只需证明 $K_1 = \ker(\varphi) = \{0\}$。对任意 $r \in R$，若 $\varphi^n(r) = 0$，则 $\varphi^{n+1}(r) = 0$。故 $K_1 \subseteq K_2 \subseteq \cdots$ 是理想的升链。由于 R 是诺特环，存在 $m > 0$ 使得 $K_m = K_{m+1} = \cdots$。
任取 $a \in K_1 = \ker(\varphi)$。由于 $\varphi^m : R \to R$ 为满的环同态，存在 $b \in R$ 使得 $a = \varphi^m(b)$。由 $a \in \ker(\varphi)$ 知 $\varphi^{m+1}(b) = \varphi(a) = 0$，从而 $b \in \ker(\varphi^{m+1}) = K_{m+1} = K_m$。于是 $a = \varphi^m(b) = 0$。所以 φ 是单射，从而是环同构。 $\square$

注. 可类比，有限集合 E 上的满射，必是单射，从而是双射。

定义 2 (素元与不可约元)**.** 设 R 是整环。

(1) 称 $r \in R$ 为**素元**，若 r 是非零非可逆的，且若 $r \mid ab$，则 $r \mid a$ 或 $r \mid b$。

(2) 称 $r \in R$ 为**不可约元**，若 r 是非零非可逆的，且若 $r = ab$，则 a 或 b 可逆。

注. 素元总是不可约元，但不可约元未必是素元。

定义 3 (素分解与不可约分解). (1) 称 $r \in R$ 具有**素元分解**，若 r 可分解成有限个素元的乘积。

(2) 称 $r \in R$ 具有**不可约分解**，若 r 可分解成有限个不可约元的乘积。

定理 2. 设 R 是一个诺特整环，则 R 中的任何非零非可逆的元素都具有不可约分解。[这不意味着 R 是 UFD，因为 UFD 是用素元分解定义的。]

证明. 记 $E = \{r \in R \mid r$ 非零非可逆且r 不能分解为有限多个不可约元的乘积$\}$。只需证明 $E = \emptyset$。反设 $E \neq \emptyset$, 则存在 $a \in E$。由于 a 本身不是不可约元, 存在非零非可逆的元素 $b, c \in R$ 使得 $a = bc$。由 $a \in E$ 知 $b \in E$ 或 $c \in E$。不妨设 $b \in E$，记 $a_1 = b \in E$。显然 $(a) \subseteq (a_1)$ [练习: 证明 $a_1 \notin (a)$，需用到 R 是整环]。从而 $(a) \subsetneq (a_1)$。对 a_1 重复上述过程，可找到 $a_2 \in E$ 使得 $(a_1) \subsetneq (a_2)$。如此继续，可得到理想的严格升链

$$(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots$$

这与 R 是诺特环矛盾。故 $E = \emptyset$，即 R 中任何非零非可逆的元素都有不可约分解。 □

注. 唯一分解整环中的非零非可逆元都具有素元分解，诺特整环中的非零非可逆元具有不可约分解。从这个角度上看，UFD 与诺特整环性质上有相似之处。

例 1 (诺特环但不是诺特整环的例子). (1) 设 $n > 1$ 是合数，则 $\mathbb{Z}/n\mathbb{Z}$ 是诺特环，因为 $\mathbb{Z}/n\mathbb{Z}$ 是有限环。显然 n 是合数时，$\mathbb{Z}/n\mathbb{Z}$ 不是整环。

(2) 设 K_1, K_2 是域，则 $R = K_1 \times K_2$ 是诺特环但不是整环。

题 2. 设 I 是环 R 的一个理想。若 R 是诺特环，则 R/I 也诺特。

证明. 易知 R/I 的每个理想都形如 J/I，其中 J 是 R 的理想且 $I \subseteq J$。由于 R 是诺特环，从而 J 是有限生成的。可推出 J/I 是有限生成的，从而 R/I 是诺特的。 □

定理 3 (希尔伯特基定理). 若 R 是诺特环 $\iff$ $R[x]$ 是诺特环，其中 x 是未定元。

证明. $(\Leftarrow)$: 利用同构 $R \cong R[x]/I$ 即可，其中 $I = (x) \lhd R[x]$。
$(\Rightarrow)$: 设 R 是诺特环。任取 $R[x]$ 的一个理想 I，需证明 I 是有限生成的。
反设 I 不是有限生成的，来导出矛盾。由于 I 不是有限生成的，所以 $I \neq (0)$。
(1) 任取 $I \setminus \{0\}$ 中次数最低的一个多项式 f_1，记 $d_1 = \deg(f_1)$。由于 I 不是有限生成的，从而 $(f_1) \subsetneq I$。
(2) 任取 $I \setminus (f_1)$ 中次数最低的一个多项式 f_2，记 $d_2 = \deg(f_2)$，知 $d_1 \leq d_2$。由于 I 不是有限生成的，从而 $(f_1\ f_2) \subsetneq I$。

(3) 任取 $I \setminus (f_1, f_2)$ 中次数最低的一个多项式 f_3，记 $d_3 = \deg(f_3)$，知 $d_1 \le d_2 \le d_3$。如此下去，可得到一个理想的严格升链:

$$(f_1) \subsetneq (f_1, f_2) \subsetneq (f_1, f_2, f_3) \subsetneq \ldots \subseteq I, \quad d_1 \le d_2 \le d_3 \le \ldots$$

记 $c_k \in R$ 为 f_k 的首项系数，即有 $f_k(x) = c_k x^{d_k} +$ 其它低次项。考虑 R 中的理想的升链:

$$(c_1) \subseteq (c_1, c_2) \subseteq (c_1, c_2, c_3) \subseteq \ldots,$$

由于 R 是诺特的，所以存在 $m \ge 1$ 使得 $(c_1, \ldots, c_m) = (c_1, \ldots, c_m, c_{m+1}) = \cdots$。由 $c_{m+1} \in (c_1, \ldots, c_m, c_{m+1}) = (c_1, \ldots, c_m)$，可设 $c_{m+1} = \sum_{k=1}^{m} r_k c_k$，其中 $r_k \in R$。
我们利用 $f_1, \ldots, f_m, f_{m+1}$ 来造一个多项式 h 满足 $h \in I \setminus (f_1, \ldots, f_m)$ 并且 $\deg(h) < \deg(f_{m+1})$，从而与 f_{m+1} 是 $I \setminus (f_1, \ldots, f_m)$ 中次数最低的一个多项式相矛盾。
对于 $k = 1, \ldots, m$，由于 $f_k(x) = c_k x^{d_k} +$ 低次项，从而

$$\begin{aligned} &r_k x^{d_{m+1} - d_k} f_k(x) = r_k c_k x^{d_{m+1}} + \text{低次项}, \\ &g := \sum_{k=1}^{m} r_k x^{d_{m+1} - d_k} f_k(x) = (\sum_{k=1}^{m} r_k c_k) x^{d_{m+1}} + \text{低次项} = c_{m+1} x^{d_{m+1}} + \text{低次项}. \end{aligned}$$

由于 $f_{m+1} \in I \setminus (f_1, \ldots, f_m)$ 及 $g \in (f_1, \ldots, f_m)$ 知，$h := f_{m+1} - g \in I \setminus (f_1, \ldots, f_m)$。由于 f_{m+1} 与 g 有相同的首项，所以 $\deg(h) = \deg(f_{m+1} - g) < \deg(f_{m+1}) = d_{m+1}$。这与 f_{m+1} 是 $I \setminus (f_1, \ldots, f_m)$ 中次数最低的一个多项式相矛盾。所以 $R[x]$ 的任何理想 I 是有限生成的。因此，$R[x]$ 是诺特环。

□

推论 1. 若 R 是诺特环，则 $R[x_1, \ldots, x_n]$ 是诺特环。

例 2. (1) $\mathbb{Z}$ 诺特 $\Rightarrow \mathbb{Z}[x]$ 诺特 $\Rightarrow \mathbb{Z}[x, y]$ 诺特。
(2) $\mathbb{Z}$ 诺特 $\Rightarrow \mathbb{Z}[x]$ 诺特 $\Rightarrow \mathbb{Z}[\sqrt{2}] \cong \mathbb{Z}[x]/(x^2 - 2)$ 诺特。

定义 4 (可约理想与不可约理想)**.** 设 R 是交换环，真理想 I 称为**可约的**，如果存在理想 $J, J' \supsetneq I$ 使得 $I = J \cap J'$。否则称 I 为**不可约的**，即若存在理想 J, J' 使得 $I = J \cap J'$，则有 $I = J$ 或 $I = J'$。

定理 4 (理想的不可约分解)**.** 设 R 是诺特环，则 R 的每个真理想可写成有限多个不可约理想的交。

证明. 记 $\Omega = \{I \lhd R \mid 1 \notin I,\ I \text{ 不能写成有限多个不可约理想的交}\}$。我们需要证明 $\Omega = \emptyset$。
反设 $\Omega \ne \emptyset$。由于 R 是诺特环，R 中任何理想的升链必稳定，由此易证 Ω 中存在极大元 I（关于包含关系）。由于不可约理想均不能在 Ω 中，从而 $I \in \Omega$ 是可约的。于是存在理想 $J, J' \supsetneq I$ 使得 $I = J \cap J'$。易知 $1 \notin J$ 且 $1 \notin J'$，否则有 $I = J$ 或 $I = J'$。由于

I 是 Ω 中的极大元，所以有 $J \notin \Omega$ 且 $J' \notin \Omega$。从而 J 和 J' 都可写成有限多个不可约理想的交，所以 $I = J \cap J'$ 也可写成有限多个不可约理想的交，这与 $I \in \Omega$ 矛盾。故 $\Omega = \emptyset$，结论得证。 □

定义 5 (准素理想)**.** 设 R 是交换环，真理想 Q 称为**准素的（primary）**，如果对任意 $a, b \in R$，若 $ab \in Q$，则 $a \in Q$ 或存在 $n \geq 1$ 使得 $b^n \in Q$。

例 3. 取 $R = \mathbb{Z}$, $Q = (p^m) = p^m\mathbb{Z}$，则 Q 是 R 的一个准素理想。

定理 5 (准素分解定理)**.** 设 R 是诺特环，则

(1) R 的不可约理想是准素的。

(2) R 的每个真理想可写成有限多个准素理想的交。

证明. (1) 设 Q 是 R 的一个不可约理想。需要证明 Q 是准素的。
设 $a, b \in R$ 满足 $ab \in Q$，需证明 $a \in Q$ 或存在 $n \geq 1$ 使 $b^n \in Q$。对 $r \in R$，记 $(Q : r) = \{x \in R \mid rx \in Q\}$，易知 $(Q : r)$ 为 R 的理想。我们有如下的理想升链

$$(Q : b) \subseteq (Q : b^2) \subseteq (Q : b^3) \subseteq \cdots$$

由于 R 是诺特环，存在 $n \geq 1$ 使得 $(Q : b^n) = (Q : b^{n+1}) = \cdots$。
我们断言：$(Q + Ra) \cap (Q + Rb^n) = Q$。
显然 $Q \subseteq (Q+Ra) \cap (Q+Rb^n)$。反之，设 $x \in (Q+Ra) \cap (Q+Rb^n)$，则存在 $q_1, q_2 \in Q$，$r_1, r_2 \in R$ 使得

$$x = q_1 + r_1 a = q_2 + r_2 b^n.$$

由于 $ab \in Q$，有 $xb = q_1 b + r_1 ab \in Q$。又 $xb = q_2 b + r_2 b^{n+1}$，于是 $r_2 b^{n+1} = xb - q_2 b \in Q$，从而 $r_2 \in (Q : b^{n+1}) = (Q : b^n)$，故 $r_2 b^n \in Q$。因此 $x = q_2 + r_2 b^n \in Q$。
于是 $(Q + Ra) \cap (Q + Rb^n) = Q$。由 Q 的不可约性，$Q + Ra = Q$ 或 $Q + Rb^n = Q$，即 $a \in Q$ 或 $b^n \in Q$。所以 Q 是准素的。
(2) 由诺特环的不可约分解定理，每个真理想可写成有限多个不可约理想的交。再由 (1)，不可约理想是准素的，故每个真理想可写成有限多个准素理想的交。 □

例 4. 在 $R = \mathbb{Z}$ 中，有素因子分解定理：$\forall n \geq 1$，存在质因子分解 $n = p_1^{m_1} \cdots p_s^{m_s}$。在理想的角度有准素分解：$(n) = (p_1^{m_1} \cdots p_s^{m_s}) = (p_1^{m_1}) \cap \cdots \cap (p_s^{m_s})$。

定义 6 (根理想)**.** 对理想 $I \subseteq R$，其**根理想**定义为

$$\sqrt{I} = \{r \in R \mid \exists n > 0 \text{ 使得 } r^n \in I\}.$$

题 3. 设 Q 是交换环 R 的一个准素理想，则 $\sqrt{Q}$ 是 R 的素理想。

证明. 设 $a,b\in R$ 且 $ab\in\sqrt{Q}$，要证 $a\in\sqrt{Q}$ 或 $b\in\sqrt{Q}$。
由 $ab\in\sqrt{Q}$ 知，存在 $n>0$ 使得 $(ab)^n=a^nb^n\in Q$。由于 Q 是准素的，所以有 $a^n\in Q$ 或存在 $m>0$ 使得 $(b^n)^m=b^{nm}\in Q$。若 $a^n\in Q$，则 $a\in\sqrt{Q}$。若存在 $m>0$ 使得 $b^{nm}\in Q$，则 $b\in\sqrt{Q}$。因此，$\sqrt{Q}$ 是素理想。 □

例 5. 取 $R=\mathbb{Z}$，$Q=(p^m)$，其中 p 为素数，$m>0$。知 Q 为 $\mathbb{Z}$ 的准素理想，此时 $\sqrt{Q}=(p)$ 为 $\mathbb{Z}$ 的素理想。

题 4. 设 Q_1,Q_2 为交换环 R 的两个准素理想，满足 $\sqrt{Q_1}=\sqrt{Q_2}$，则 $Q_1\cap Q_2$ 为 R 的准素理想，且 $\sqrt{Q_1\cap Q_2}=\sqrt{Q_1}$。

证明. 设 $a,b\in R$ 且 $ab\in Q_1\cap Q_2$，需证 $a\in Q_1\cap Q_2$ 或存在 $m>0$ 使得 $b^m\in Q_1\cap Q_2$。现假设 $a\notin Q_1\cap Q_2$，只需证存在 $m>0$ 使得 $b^m\in Q_1\cap Q_2$。
由 $ab\in Q_1$ 及 Q_1 是准素的，可有 $a\in Q_1$ 或存在 $m_1>0$ 使得 $b^{m_1}\in Q_1$。同理，由 $ab\in Q_2$ 及 Q_2 是准素的，可有 $a\in Q_2$ 或存在 $m_2>0$ 使得 $b^{m_2}\in Q_2$。
由于 $a\notin Q_1\cap Q_2$，不可能同时有 $a\in Q_1$ 且 $a\in Q_2$。因此，必存在某个 $m>0$ 使得 $b^m\in Q_1$ 或 $b^m\in Q_2$。从而有 $b\in\sqrt{Q_1}$ 或 $b\in\sqrt{Q_2}$。由于 $\sqrt{Q_1}=\sqrt{Q_2}$，所以必有 $b\in\sqrt{Q_1}=\sqrt{Q_2}$。从而存在足够大的 m 使得 $b^m\in Q_1$ 且 $b^m\in Q_2$。从而 $b^m\in Q_1\cap Q_2$。因此，$Q_1\cap Q_2$ 是 R 的准素理想。
现证 $\sqrt{Q_1\cap Q_2}=\sqrt{Q_1}$。由 $\sqrt{Q_1}=\sqrt{Q_2}$ 知 $x\in\sqrt{Q_1}\iff x\in\sqrt{Q_1}\cap\sqrt{Q_2}\iff$ 存在足够大的 m 使 $x^m\in Q_1$ 且 $x^m\in Q_2\iff x\in\sqrt{Q_1\cap Q_2}$。所以，$\sqrt{Q_1\cap Q_2}=\sqrt{Q_1}$。 □

题 5. 设 M 是交换环 R 的一个极大理想，Q 是 R 的一个理想。若存在 $n>0$ 使得 $M^n\subseteq Q\subseteq M$，则 Q 是 R 的准素理想。

证明. 设 $a,b\in R$ 且 $ab\in Q$。若 $a\notin Q$，需证存在 $m>0$ 使得 $b^m\in Q$。
若 $b\in M$，则 $b^n\in M^n\subseteq Q$，取 $m=n$ 即有 $b^m\in Q$。若 $b\notin M$，由 M 是极大理想知 $M+Rb=R$。从而存在 $s\in M$，$r\in R$ 使得 $s+rb=1$。于是 $1-rb=s\in M$，从而 $(1-rb)^n=s^n\in M^n\subseteq Q$。
所以 $a(1-rb)^n\in Q$。将 $(1-rb)^n$ 用二项式定理展开，可得存在 $r'\in R$ 使得

$$a(1-rb)^n=a+r'ab.$$

由 $a+r'ab\in Q$ 及 $ab\in Q$ 可得 $a=(a+r'ab)-r'ab\in Q$，这与 $a\notin Q$ 矛盾。
因此，若 $a\notin Q$，则必有 $b\in M$，此时 $b^n\in M^n\subseteq Q$。所以 Q 是准素理想。 □

题 6. 设 P 是交换环 R 的一个素理想，Q 是 R 的一个准素理想。

(1) 若存在 $n>0$ 使得 $P^n\subseteq Q\subseteq P$，则 $P=\sqrt{Q}$。

(2) 若 R 是诺特环，则存在 $m>0$ 使得 $(\sqrt{Q})^m\subseteq Q\subseteq\sqrt{Q}$。

证明. (1) 由 $P^n \subseteq Q$ 知 $P \subseteq \sqrt{Q}$。任取 $a \in \sqrt{Q}$，则存在 $k > 0$ 使得 $a^k \in Q \subseteq P$。由于 P 是素理想，所以 $a \in P$。从而 $\sqrt{Q} \subseteq P$。综合可有，$P = \sqrt{Q}$。
(2) 由于 R 是诺特环，所以 $\sqrt{Q}$ 是有限生成的。可设 $\sqrt{Q} = (a_1 \ldots, a_s) = \sum_{j=1}^{s} Ra_j$，其中 $a_i \in \sqrt{Q}$。由于 $a_i \in \sqrt{Q}$，从而存在 $m_i > 0$ 使得 $a_i^{m_i} \in Q$。取 $m = m_1 + \cdots + m_s$，易验证 $\forall 1 \leq i_1, \ldots, i_m \leq s$, 有 $a_{i_1} \cdots a_{i_m} \in Q$。又

$$(\sqrt{Q})^m = \sum_{1 \leq i_1, \ldots, i_m \leq s} Ra_{i_1} \cdots a_{i_m},$$

从而有 $(\sqrt{Q})^m \subseteq Q$。因此，$(\sqrt{Q})^m \subseteq Q \subseteq \sqrt{Q}$。 □

题 7. 设 R 是整环，$p \in R \setminus \{0\}$。证明：

(1) p 为素元 $\Leftrightarrow$ (p) 是素理想。

(2) 若 R 是主理想整环（PID），则 (p) 是素理想 $\Leftrightarrow$ (p) 是极大理想 (注意: $p \neq 0$)。

题 8. 设 R 是主理想整环（PID），Q 是 R 的一个非零理想。证明：Q 是准素理想 $\Longleftrightarrow$ 存在素元 $p \in R$ 及 $n > 0$ 使得 $Q = Rp^n$。

证明. $(\Leftarrow)$ 设 $Q = (p^n) = Rp^n$，其中 p 是素元。由 R 是主理想整环，知 Rp 是极大理想。由 $(Rp)^n = Rp^n = Q \subseteq Rp$ 及之前题中的结论知，Q 是准素理想。
$(\Rightarrow)$ 设 Q 是非零的准素理想，则其根理想 $\sqrt{Q}$ 是非零的素理想。由 R 是 PID，知存在 $0 \neq a \in R$ 及素元 p 使得 $Q = Ra$，$\sqrt{Q} = Rp$。由 $p \in \sqrt{Q}$ 知存在 $n > 0$ 使得 $p^n \in Q = Ra$。取 n 是最小的正整数使 $p^n \in Q = Ra$。知存在 $r \in R$ 使得 $p^n = ra$。
我们来证 $p \nmid r$。否则，则存在 $r' \in R$ 使得 $r = r'p$。从而 $p^n = ra = r'pa = pr'a$。从而 $p^{n-1} = r'a \in Ra = Q$。这与 n 的最小性选取矛盾。故 $p \nmid r$。
由 p 是素元，$p \nmid r$ 且 $p^n = ra$ 可知，$p^n \mid a$。从而 $Q = Ra \subseteq Rp^n \subseteq Q$。从而有 $Q = Rp^n$。结论得证。

□