


Dedekind 整区

戚天成 

复旦大学 数学科学学院

2024 年 1 月 26 日

这份笔记主要记录离散赋值环和 Dedekind 整区的基本性质与经典例子, 主要参考文献是 [AM69].

Dedekind 整区与离散赋值环间的关系可以理解为“整体”与“局部”间的关系——1 维 Noether 整区是 Dedekind 整区的充要条件是该环在任何极大理想处的局部化是离散赋值环 (见 [定理2.6]). 虽然离散赋值环的原始定义是纯代数的, 但它可以与几何产生联系. 在 [推论1.15] 中我们将看到 1 维 Noether 局部整区是离散赋值环当且仅当它是正则局部环. 由此可知代数闭域上的仿射曲线在给定点处的光滑性等价于该点处的正则函数芽环是离散赋值环 (见 [例1.16]). 相应地, Dedekind 整区对应仿射曲线的整体光滑性 (见 [例2.12]). 事实上, 任何代数数域的整数环都是 Dedekind 整区 (见 [定理2.21]). 我们也会在 [推论2.9] 中看到 Dedekind 整区中任何非零真理想在不计次序下唯一地分解为有限个素理想的乘积. 历史上, Dedekind 整区理论的发展来自 E. Noether (德国, 1882-1935), “Dedekind 整区”的命名用于纪念 Dedekind 在 1871 年对代数数域的整数环率先证明理想关于素理想的分解性质. 在最后, 我们介绍整区的分式理想与可逆理想的概念, 整区 R 的商域的 R -子模是可逆理想当且仅当该子模是非零有限生成投射 R -模 (见 [命题3.5]). 分式理想的可逆性质可用于刻画离散赋值环 (见 [命题3.8]) 和 Dedekind 整区 (见 [推论3.9]).

1 离散赋值环

我们知道代数闭域上仿射簇在一点处光滑的充要条件是该簇在此点处局部环是正则局部环. 本节介绍的离散赋值环是一类特殊的 1 维 Noether 局部整区 (见 [定理1.12]), 它是对应于仿射曲线在一点处光滑性的代数概念. 我们将看到仿射曲线在一点处光滑的充要条件是该曲线在这点处局部环是离散赋值环 [例1.16].

Definition 1.1. 设 F 是域, F 上的离散赋值是指满足下述条件的满射 $v: F^* \rightarrow \mathbb{Z}$:

- (1) $v(xy) = v(x) + v(y), \forall x, y \in F^*$, 即 v 是乘法群 F^* 到加法群 \mathbb{Z} 的群同态;
- (2) $v(x + y) \geq \min\{v(x), v(y)\}, \forall x, y, x + y \in F^*$.

Remark 1.2. 若考虑 F^* 的子集 $\{x \in F^* | v(x) \geq 0\}$, 那么该子集与零元构成 F 的子环 R , 易见 R 是整区并且由 $v(1) = 0$ 以及 $v(1) = v(x) + v(x^{-1}), \forall x \in F^*$ 可知对任何 $x \in F^*$, 有 $x \in R$ 或 $x^{-1} \in R$. 进而知 F 中元素总可表示为 $as^{-1}, a, s \in R$ 的形式, 这说明 F 是 R 的商域. 回忆整区 R 被称为赋值环, 如果 R 的商域中任何非零元 x 满足 $x \in R$ 或 $x^{-1} \in R$. 因此前面的观察表明任何域 F 上的离散赋值 $v: F^* \rightarrow \mathbb{Z}$ 能够产生赋值环 $R = \{x \in F^* | v(x) \geq 0\} \cup \{0\}$, 称为离散赋值 v 的赋值环. 有时通过定义 $v(0) = +\infty$ 将 v 延拓至 F 上.

Example 1.3. 固定素数 p , 定义 $v: \mathbb{Q}^* \rightarrow \mathbb{Z}$ 为: 对任何非零有理数 $x \in \mathbb{Q}$, 可表示为 $p^n y$ 的形式, 其中 n 是整数, y 是分子分母不含素因子 p 的有理数. 算术基本定理保证了 n 不依赖于满足上条件分解的选取方式, 置 $v(x) = n$. 易见如上定义的映射 $v: \mathbb{Q}^* \rightarrow \mathbb{Z}$ 是满射且是 \mathbb{Q} 上的离散赋值. 这时 v 的赋值环同构于 $\mathbb{Z}_{(p)}$.

Remark 1.4. 一般地, 如果 R 是 U.F.D., 取定 R 的素元 p , 都可以类似构造 R 商域上的离散赋值.

在进一步介绍离散赋值环的刻画前, 回忆赋值环所具有的基本性质.

Lemma 1.5. 设整区 R 是赋值环, 那么 R 是局部整闭整区并且 R 和其商域间的整区也是赋值环.

Proof. 要说明 R 是局部环只需验证 R 所有不可逆元构成理想. 由 R 的交换性, 只需验证任意两个非零不可逆元之和也是不可逆元. 设 R 所有不可逆元构成的集合为 \mathfrak{m} , 则对非零元 $a, b \in \mathfrak{m}$, 有 $a^{-1}b \in R$ 或 $ab^{-1} \in R$. 不妨设 $a^{-1}b \in R$, 那么 $a + b = a(1 + a^{-1}b) \in \mathfrak{m}$. 因此赋值环是局部整区. 根据赋值环的定义不难看出介于赋值环与其商域之间的整区都是赋值环. 最后我们需要说明赋值环 R 在其商域 F 内整闭. 任取 $\alpha \in F$ 为 R 上整元, 那么存在正整数 n 以及 $a_0, \dots, a_{n-1} \in R$ 使得 α 满足 $a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} + \alpha^n = 0$. 如果 $\alpha \notin R$, 那么 $\alpha^{-1} \in R$, 于是由 $a_0\alpha^{1-n} + a_1\alpha^{2-n} + \dots + a_{n-1} + \alpha = 0$ 得到 $\alpha \in R$, 矛盾. 故 R 是整闭局部整区. \square

Definition 1.6. 设 R 是整区, 称 R 为离散赋值环, 如果 R 的商域上存在离散赋值 v 使得 R 是 v 的赋值环.

Remark 1.7. 根据 [引理1.5] 可知离散赋值环是局部整区. 设 R 是离散赋值环, 则有其商域上的离散赋值 $v: F^* \rightarrow \mathbb{Z}$ 使得 R 是 v 的赋值环. 如果 $x \in R$ 满足 $v(x) > 0$, 那么 x 是 R 中不可逆元, 否则 $x^{-1} \in R$ 蕴含 $0 = v(1) = v(x) + v(x^{-1}) > 0$, 矛盾. 类似地, 易验证 R 中可逆元在 v 下的像为零. 由此可知 R 中所有不可逆元构成的唯一的极大理想 $\mathfrak{m} = \{x \in R | v(x) > 0\}$ (v 的满射条件保证了 $\mathfrak{m} \neq 0$). 由此可知离散赋值环 R 的任意两个元素 $x, y \in R$ 只要在离散赋值 v 下具有相同的取值, 那么 $(x) = (y)$: 这时有 $v(x) = v(y)$, 如果 $x = y = 0$, 结论直接成立. 下设 $y \neq 0$, 那么 $v(x) = v(y)$ 蕴含 $v(xy^{-1}) = 0$, 因此 $xy^{-1} \in R$ (回忆根据定义 R 便含有 F 中所有在 v 作用下非负的元素) 且 xy^{-1} 是 R 中可逆元. 这意味着 (x) 与 (y) 是 R 的两个相同的主理想.

事实上整环的离散赋值性蕴含了 Noether 性质, 具体地, 对每个自然数 k , 记 $\mathfrak{m}_k = \{a \in R | v(a) \geq k\}$, 我们说明离散赋值环 (R, \mathfrak{m}) 的任何非零理想都在理想降链 $R = \mathfrak{m}_0 \supseteq \mathfrak{m}_1 \supseteq \mathfrak{m}_2 \supseteq \dots$ 中. 根据之前的约定, $v(0) = +\infty$, 所以由 R 是离散赋值环不难看到每个 \mathfrak{m}_k 都是 R 的理想. 任取 R 的非零理想 I , 置 $k = \min\{v(a) | a \neq 0 \in I\}$, 下面验证 $I = \mathfrak{m}_k$. 根据 k 的选取方式立即有 $I \subseteq \mathfrak{m}_k$ 且存在 $a \neq 0 \in I$ 使得 $v(a) = k$. 对每个 $b \neq 0 \in R$, 只要 $v(b) \geq k$, 那么存在自然数 n 使得 $v(ba^{-1}) = v(b) - v(a) \geq 0$, 这说明 $ba^{-1} \in R$, 从而 $b \in (a) \subseteq I$, 这就说明了 $\mathfrak{m}_k \subseteq I$. 并注意到 R 唯一的极大理想 $\mathfrak{m} = \mathfrak{m}_1$. 由此得到:

Proposition 1.8. 设 (R, \mathfrak{m}) 是离散赋值环, R 的商域 F 上有离散赋值 $v: F^* \rightarrow \mathbb{Z}$, 对每个自然数 k , 记 $\mathfrak{m}_k = \{a \in R | v(a) \geq k\}$. 那么每个 \mathfrak{m}_k 为 R 的理想并且 R 的任何非零理想都为理想降链 $R = \mathfrak{m}_0 \supseteq \mathfrak{m} = \mathfrak{m}_1 \supseteq \mathfrak{m}_2 \supseteq \dots$ 中的某项 (因为 v 是满射所以该降链严格). 特别地, 离散赋值环总是 Noether 局部整区.

Example 1.9. 设 $R = \mathbb{k}[[x]]$ 是域 \mathbb{k} 上形式幂级数环, 那么 R 是主理想整区, 它的任何非零理想形如 (x^s) , $s \in \mathbb{N}$. 不难看出 $x \in R$ 是 R 作为 P.I.D. 的一个素元, 因此该素元可诱导 R 的商域上的一个离散赋值 $v: \mathbb{k}(x)^* \rightarrow \mathbb{N}$, 这里 v 将每个非零有理函数映射至将有理函数表示为 $x^n f/g$ (这里 f, g 是常数项非零的形式幂级数, n 是整数) 后 x 的幂指数 n . 注意到 R 中元素可逆当且仅当该元素是常数项非零的形式幂级数, 所以 v 的赋值环就是 R , 这说明 R 是离散赋值环.

如果 (R, \mathfrak{m}) 的商域 F 上的离散赋值是 $v : F^* \rightarrow \mathbb{Z}$, 那么由 v 是满射便知存在 $x \neq 0 \in R$ 使得 $v(x) = 1$, 这意味着 $\mathfrak{m} = \mathfrak{m}_1 = (x)$. 于是对任何自然数 k 有 $\mathfrak{m}_k = (x^k)$, 进而知 R 所有非零理想都出现在理想降链 $R \supseteq (x) \supseteq (x^2) \supseteq \cdots$ 中, 这是形式幂级数环理想特征的推广. 我们把这总结为:

Proposition 1.10. 设 (R, \mathfrak{m}) 是离散赋值环, 并设其商域 F 上的离散赋值是 $v : F^* \rightarrow \mathbb{Z}$, 取 $x \in \mathfrak{m}$ 满足 $v(x) = 1$, 那么 R 的任何非零理想形如 $(x^s), s \in \mathbb{N}$. 特别地, 离散赋值环是主理想局部整区, 并且 $\mathfrak{m} \neq 0$.

Remark 1.11. 根据该命题, 离散赋值环 (R, \mathfrak{m}) 的素理想只有 0 与 \mathfrak{m} , 故 $\text{k.dim}R = 1$.

前面我们看到离散赋值环总是 1 维 Noether 局部整区, 现在可以给出离散赋值环的等价刻画.

Theorem 1.12. 设 (R, \mathfrak{m}, k) 是 1 维交换 Noether 局部整区, 其中 $k = R/\mathfrak{m}$, 那么以下六条等价:

- (1) R 是离散赋值环.
- (2) R 是整闭整区.
- (3) \mathfrak{m} 是主理想.
- (4) $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$.
- (5) R 的任何非零理想是 \mathfrak{m} 的自然数幂.
- (6) 存在 $x \in R$ 使得 R 的任何非零理想形如 $(x^s), s \in \mathbb{N}$.

Proof. (1) \Rightarrow (2): 根据 [引理1.5], 任何赋值环是整闭整区, 所以离散赋值环也是整闭整区.

(2) \Rightarrow (3): 因为 R 是 1 维局部整区, 所以 R 的非零素理想只有 \mathfrak{m} . 这意味着 R 的任何非零真理想 I 的根理想 $\sqrt{I} = \mathfrak{m}$, 所以由 R 的 Noether 性立即得到存在正整数 n 使得 $\mathfrak{m}^n \subseteq I$. 现设 $a \neq 0 \in \mathfrak{m}$ 并取 $I = (a)$. 不妨设 n 是满足条件的最小正整数, 那么 $\mathfrak{m}^{n-1} \not\subseteq (a)$ 且 $\mathfrak{m}^n \subseteq (a)$, 所以可取 $b \in \mathfrak{m}^{n-1}$ 满足 $b \notin (a)$. 置 $x = ab^{-1} \in F$, 这里 F 是 R 的商域. 下面说明 $\mathfrak{m} = Rx$ 来得到 \mathfrak{m} 是主理想. 因为 $b \notin (a)$, 所以 $x^{-1} \notin R$, 进而 x^{-1} 不是 R 上整元. 这说明 $x^{-1}\mathfrak{m} \not\subseteq \mathfrak{m}$ (若不然, 注意到 \mathfrak{m} 是有限生成 R -模, 设作为 R -模有生成元集 $\{y_1, \dots, y_n\}$, 那么利用 xy_i 可被 $\{y_1, \dots, y_n\}$ 来 R -线性表出可知存在 $A \in M_n(R)$ 使得 $x^{-1}(y_1, \dots, y_n)^T = A(y_1, \dots, y_n)^T$, 进而知 $\det(x^{-1}I_n - A) \in \text{Ann}_{R[x^{-1}]}\mathfrak{m}$, 因为 \mathfrak{m} 作为 $R[x^{-1}]$ -模是忠实的, 所以 $\det(x^{-1}I_n - A) = 0$, 由此得到 x^{-1} 是 R 上整元). 此外, 由 $b\mathfrak{m} \subseteq \mathfrak{m}^n \subseteq (a)$ 得到 $x\mathfrak{m} = a^{-1}b\mathfrak{m} \subseteq R$, 因此 $x^{-1}\mathfrak{m}$ 是 R 的不含于 \mathfrak{m} 的理想. 于是由 R 是局部环迫使 $x^{-1}\mathfrak{m} = R$, 即有 $\mathfrak{m} = Rx$, 这说明 \mathfrak{m} 是 R 的主理想.

(3) \Rightarrow (4): R 作为 1 维局部整区可得 $\mathfrak{m} \neq 0$, 结合 \mathfrak{m} 是有限生成 R -模, 由 Nakayama 引理得到 $\mathfrak{m} \neq \mathfrak{m}^2$. 因此由 \mathfrak{m} 作为 R -模可由一个元素生成立即得到 $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$.

(4) \Rightarrow (5): 在 (2) \Rightarrow (3) 的过程中已经指出 R 的任何非零理想 I 满足存在正整数 n 使得 $\mathfrak{m}^n \subseteq I$. $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$ 表明 \mathfrak{m} 是主理想. 现考察商环 R/\mathfrak{m}^n , 易见该商环任何素理想是极大的, 所以由 R 是 Noether 环知 R/\mathfrak{m}^n 是 Artin 局部环, 由下面的 [引理1.14] 知 I/\mathfrak{m}^n 是主理想并且是 $\mathfrak{m}/\mathfrak{m}^n$ 的自然数幂. 故 I 是 \mathfrak{m} 的自然数幂.

(5) \Rightarrow (6): 这时 $\mathfrak{m} \neq \mathfrak{m}^2$, 故可取 $x \in \mathfrak{m}$ 满足 $x \notin \mathfrak{m}^2$. 那么由条件知 $(x) = \mathfrak{m}$, 其余明显成立.

(6) \Rightarrow (1): 首先 x 不是可逆元, 否则 R 是域. 所以 $\mathfrak{m} = (x)$, 进而 Nakayama 引理保证了 $\mathfrak{m}^n \neq \mathfrak{m}^{n+1}, \forall n \geq 1$. 这也说明 $(x^n) \supseteq (x^{n+1}), \forall n \geq 1$. 所以对任何 $a \neq 0 \in R$, 存在唯一的自然数 k 使得 $(a) = (x^k)$. 于是对任何非零元 $a, b \in R$, 通过定义 $v(ab^{-1}) = v(a) - v(b)$, 可直接验证 $v : F \rightarrow \mathbb{Z}$ 是定义合理的离散赋值映射. 并且 v 的赋值环就是 R , 因此 R 是离散赋值环. \square

Remark 1.13. 如果 1 维 Noether 局部整区 (R, \mathfrak{m}, k) 的 P.I.D., 那么 $\mathfrak{m} \neq \mathfrak{m}^2$ 且 R 的任何主理想 $I \neq 0$ 满足存在正整数 n 使得 $\mathfrak{m}^n \subseteq I$, 进而下面的 [引理1.14] 保证了 Artin 局部环 R/\mathfrak{m}^n 的任何非零理想是 $\mathfrak{m}/\mathfrak{m}^n$ 的

自然数幂, 由此得到 R 的任何非零理想是 \mathfrak{m} 的自然数幂. 所以 1 维 Noether 局部整区是 P.I.D. 的充要条件是它是离散赋值环. 或者说一个整区是离散赋值环当且仅当它是主理想局部整区且不是域.

Lemma 1.14. 设 (R, \mathfrak{m}, k) 是 Artin 局部环, 则以下三条等价:

- (1) R 的任何理想是主理想.
- (2) R 唯一的极大理想 \mathfrak{m} 是主理想.
- (3) $\dim_k \mathfrak{m}/\mathfrak{m}^2 \leq 1$.

并且当 $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$ 时, R 任何非零理想是 \mathfrak{m} 的自然数幂.

Proof. 只需验证 (3) \Rightarrow (1): 如果 $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 0$, 由 Nakayama 引理可知 $\mathfrak{m} = 0$, 所以 R 是域. 下设 $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$, 那么存在 $x \in R$ 使得 $(x) = \mathfrak{m}$. 对 R 的任何非零真理想 I , 由 $\mathfrak{m} = \text{Jac}(R)$ 是幂零理想知存在正整数 n 使得 $I \subseteq \mathfrak{m}^n$ 但 $I \not\subseteq \mathfrak{m}^{n+1}$. 易见 $I \subseteq (x^n)$. 因为 $I \not\subseteq \mathfrak{m}^{n+1}$, 所以存在 $y = ax^n \in I$ 使得 $y \notin \mathfrak{m}^{n+1}$, 这说明 $a \notin \mathfrak{m}$. 于是 a 是 R 中可逆元, 进而 $x^n \in I$, 所以 $I = (x^n) = \mathfrak{m}^n$. \square

Corollary 1.15. 设 R 是 1 维 Noether 局部整区, 那么 R 是正则局部环的充要条件是 R 是离散赋值环.

设 X 是拓扑空间, 称 $\sup\{n \in \mathbb{N} | X_0 \subsetneq X_1 \subsetneq \cdots \subsetneq X_n \text{ 是不可约闭子集链}\}$ 是 X 的 (Krull) 维数, 记作 $\dim X$. 设 $p \in X$, 称 $\sup\{n \in \mathbb{N} | X_0 = \{p\} \subsetneq X_1 \subsetneq \cdots \subsetneq X_n \text{ 是不可约闭子集链}\}$ 为 p 点的局部维数, 记为 $\dim_p X$. 回忆代数闭域 \mathbb{k} 上任何仿射簇 $X \subseteq \mathbb{k}^n$ 坐标环的 Krull 维数与该仿射簇作为拓扑空间的维数一致. 类似地, 局部维数定义立即看到仿射簇 X 在点 p 处局部环 $\mathcal{O}_{X,p}$ 的 Krull 维数就是 p 所在的 X 不可约分支中维数最大者的维数. 特别地, 不可约仿射簇每一点的局部维数就是该仿射簇的维数.

Example 1.16. 设 \mathbb{k} 是代数闭域, $X \subseteq \mathbb{k}^n$ 是仿射簇. 称 X 是仿射曲线, 如果 X 不可约且 $\dim X = 1$. 那么根据仿射簇坐标环的维数刻画知一个仿射簇是曲线等价于说该仿射簇坐标环是整区且 Krull 维数是 1. 回忆仿射簇 X 在点 p 处光滑的充要条件是局部环 $\mathcal{O}_{X,p}$ 是正则局部环. 因此仿射曲线 X 在点 $p \in X$ 处光滑时, $\mathcal{O}_{X,p}$ 是 Noether 局部整区. 通过 X 是仿射曲线, 即由 $\text{k.dim} A(X) = \text{k.dim} \mathbb{k}[x_1, \dots, x_n]/I(X) = 1$ 以及 $I(X)$ 是 $\mathbb{k}[x_1, \dots, x_n]$ 的素理想知 $\mathcal{O}_{X,p}$ 的 Krull 维数恰好是 1 (利用局部化的局部整体性质以及 $I(X)$ 是非极大的素理想). 因此仿射曲线在一点处的局部环总是 1 维 Noether 局部整区. 对交换 Noether 局部环 (R, \mathfrak{m}) , 若记 $k = R/\mathfrak{m}$, 那么总有 $\text{k.dim} R \leq \dim_k \mathfrak{m}/\mathfrak{m}^2$, 这里不等号的等号成立当且仅当 R 是正则局部环. 因此, 一条仿射曲线 X 在一点 p 处光滑的充要条件是该仿射曲线在这点处的局部环 $(\mathcal{O}_{X,p}, \mathfrak{m}, k)$ 满足 $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$. 根据 [定理1.12] 立即得到仿射曲线在一点处光滑的充要条件是该仿射曲线在这点处的局部环是离散赋值环.

2 Dedekind 整区

在上一节我们看到离散赋值性在几何上对应曲线的局部光滑性. 我们马上会看到下面介绍的 Dedekind 整区的概念是曲线整体光滑性这一几何特性对应的代数概念 (见 [例2.12]). Dedekind 整区环类除了包含光滑仿射簇的坐标环外, 还包含任何代数数域的整数环也是 Dedekind 整区 (见 [定理2.21]).

Definition 2.1. 如果 R 是 1 维 Noether 整闭整区, 则称 R 是 Dedekind 整区.

Remark 2.2. 通过 [定理1.12] 知离散赋值环就是 Dedekind 局部整区.

在进一步给出 Dedekind 整区的等价刻画前, 我们指出 1 维 Noether 整区理想的分解性质. 回忆含么交换 Noether 环的任何真理想可分解为有限个准素理想之交, 即有准素分解 (若考察代数闭域上的仿射簇的坐标环, 那么准素分解让我们看到任何仿射簇总可分解为有限个不可约仿射簇之并). 准素理想的根理想总是素理想, 称该素理想为给定准素分解的**相关素理想**. 设 R 的真理想 I 有准素分解 $I = Q_1 \cap Q_2 \cap \cdots \cap Q_s$, 如果

$$I \neq \bigcap_{k \neq j} Q_k, \forall 1 \leq j \leq s,$$

则称该准素分解是**不可缩短的**. 含么交换环的真理想如果存在准素分解, 则必存在不可缩短准素分解. 含么交换环的真理想如果存在准素分解, 那么该真理想不可缩短准素分解定义出的相关素理想集不依赖于具体的准素分解. 如果真理想有不可缩短的准素分解满足不同准素理想的相关素理想不同, 则称该准素分解是**极小的**. 含么交换环的真理想只要有准素分解, 同样也一定存在极小准素分解. 若 R 的真理想 I 有极小准素分解 $I = Q_1 \cap Q_2 \cap \cdots \cap Q_s$, 设 Q_i 的相关素理想为 P_i , 根据极小准素分解的定义立即看到准素理想集合 $\{Q_1, \dots, Q_s\}$ 与相关素理想集 $\{P_1, \dots, P_s\}$ 间有双射. 如果准素理想 Q_i 满足 P_i 是相关素理想集 $\{P_1, \dots, P_s\}$ 的极小元, 则称 Q_i 是 I 在 R 中的一个**孤立分支** (虽然 Q_j 间不可缩短条件保证了不会有包含关系, 但极小准素分解的相关素理想间还是可能有包含关系). 准素分解理论的一个经典结果便是 I 在 R 中的孤立分支集不依赖于具体的极小准素分解. 特别地, 如果 R 满足任何非零素理想是极大理想 (例如主理想整区), 那么任何非零理想 I 只要准素分解存在, 则极小准素分解唯一 (如果 I 有极小准素分解 $I = Q_1 \cap Q_2 \cap \cdots \cap Q_s$, 那么每个 Q_i 的相关素理想是极大理想, 由分解的极小性知每个 Q_i 都是 I 在 R 中的孤立分支, 进而由极小准素分解的孤立分支集唯一立即得到该极小准素分解的唯一性). 有了上述准备便很容易证明下述命题.

Proposition 2.3. 设 R 是 1 维 Noether 整区, 那么任何非零真理想在不计次序下唯一地分解为有限个准素理想的乘积使得不同准素理想的相关素理想不同.

Proof. 回忆含么交换环 R 的任意两个理想 A, B 满足 $\sqrt{A+B} = \sqrt{\sqrt{A} + \sqrt{B}}$. 所以如果准素理想 Q_i, Q_j 的相关素理想是不同的极大理想, 那么 $Q_i + Q_j = R$. 由条件, R 任何非零素理想是极大理想, 所以根据前面的讨论知 R 的任何非零真理想存在极小准素分解 $I = Q_1 \cap Q_2 \cap \cdots \cap Q_s$, 这里对不同的指标 i, j 有 Q_i, Q_j 的相关素理想是不同的极大理想. 于是 $Q_1 Q_2 \cdots Q_s = Q_1 \cap Q_2 \cap \cdots \cap Q_s$. 由此得到上述准素理想乘积分解的存在性. 要看到唯一性, 只需注意到若 I 可分解为 $I = Q_1 Q_2 \cdots Q_s$ 使得每个 Q_i 是准素理想且对不同的指标 i, j 有 Q_i, Q_j 的相关素理想不同. 注意到每个 Q_i 的根理想作为非零素理想是极大理想, 所以 $Q_i + Q_j = R, \forall 1 \leq i \neq j \leq s$. 于是知 $Q_1 Q_2 \cdots Q_s = Q_1 \cap Q_2 \cap \cdots \cap Q_s$, 这说明每个满足条件的准素理想乘积分解会产生一个 I 的极小准素分解 (不可缩短性由不同 Q_i 的相关素理想是不同的极大理想保证). 再由极小准素分解的唯一性得到结论. \square

Remark 2.4. 考虑整数环 \mathbb{Z} , 它是 1 维 Noether 整区. \mathbb{Z} 的任何非零准素理想形如 $p^n \mathbb{Z}$, 这里 p 是素数, n 是自然数. 因此上述命题可以视作算术基本定理的推广.

Example 2.5. 设 R 是 P.I.D. 且不是域 (例如 \mathbb{Z} 或域上一元多项式环), 那么 R 是 Dedekind 整区.

Theorem 2.6. 设 R 是 1 维 Noether 整区, 则以下三条等价:

- (1) R 是 Dedekind 整区.
- (2) R 的任何准素理想是某个素理想的幂.
- (3) 对 R 的任何极大理想 \mathfrak{m} , $R_{\mathfrak{m}}$ 是离散赋值环.

Proof. 回忆对含么交换环的扩张 $R \subseteq E$, 对 R 的任何乘闭子集 S , R_S 在 E_S 中的整闭包就是 R 在 E 中的整闭包在 E_S 中的像 (取局部化与取整闭包可交换的性质证明见下面的 [引理2.8]). 同时注意到 $F_m \cong F$ 是 R_m 在非零元全体构成的乘闭子集处的局部化, 故 [定理1.12] 保证了 (1) 和 (3) 等价. 回忆含么交换环 R 所有与乘闭子集 S 不相交的素理想和 R_S 的全体素理想间有自然双射 $\{\mathfrak{p} \in \text{Spec}(R) | \mathfrak{p} \cap S = \emptyset\} \rightarrow \text{Spec}(R_S), \mathfrak{p} \mapsto \mathfrak{p}_S$. 类似地, R 所有与 S 不相交的准素理想全体和 R_S 的准素理想全体也有自然双射 $\{\mathfrak{q} | \mathfrak{q} \text{ 为 } R \text{ 的准素理想且 } \mathfrak{q} \cap S = \emptyset\} \rightarrow \{I \subseteq R_S | I \text{ 为 } R_S \text{ 的准素理想}\}, \mathfrak{q} \mapsto \mathfrak{q}_S$ (验证它). 下面我们证明 (2) 与 (3) 等价. 要看到 (2) 蕴含 (3), 根据 [定理1.12] 以及 [命题2.3], 只需验证对 R 的任何极大理想 \mathfrak{m} , R_m 的非零准素理想是 \mathfrak{m}^m 的正整数幂. 由于 R_m 的非零准素理想形如 Q_m , 这里 $Q \subseteq \mathfrak{m}$ 是 R 的准素理想, 所以一旦 Q 可表为素理想 P 的正整数幂 $Q = P^t$, 那么 $P \subseteq \mathfrak{m}$, 于是由 P 作为非零素理想是 R 的极大理想迫使 $P = \mathfrak{m}$. 最后还需要说明 (3) \Rightarrow (2): 任取 R 的非零准素理想 Q (零理想时结论明显成立), 并取极大理想 $\mathfrak{m} \supseteq Q$, 那么 Q_m 为 R_m 的非零准素理想, 并且根据 [定理1.12] 知存在正整数 t 使得 $Q_m = \mathfrak{m}_m^t$. 进而由 \mathfrak{m}^t 是准素理想 (回忆含么交换环任何理想 I 只要 \sqrt{I} 是极大理想, 则 I 是准素理想) 立即得到 $Q = \mathfrak{m}^t$. 于是 Q 是素理想 \mathfrak{m} 的幂. \square

Remark 2.7. 因此一个 1 维 Noether 整区是正则环当且仅当它是 Dedekind 整区. 特别地, Dedekind 整区的整体维数总是 1. 因此 Dedekind 整区类是遗传环类的子类, 后者是同调环论中的研究对象.

Lemma 2.8. 给定含么交换环的环扩张 $E \supseteq R$, 并设 S 是 R 的乘闭子集且 $0 \notin S$, 若 R' 是 R 在 E 中的整闭包, 则 R'_S 是 R_S 在 E_S 中的整闭包. 因此对环扩张取整闭包和作局部化可交换.

Proof. 设 R_S 在 E_S 中的整闭包为 $(R_S)'$, 任取 $u/s \in R'_S, s \in S, u \in R'$, 则存在 R 上首一多项式 $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ 使得 $f(u) = 0$. 由此得到:

$$\left(\frac{u}{s}\right)^n + \frac{a_{n-1}}{s} \left(\frac{u}{s}\right)^{n-1} + \cdots + \frac{a_1}{s^{n-1}} \left(\frac{u}{s}\right) + \frac{a_0}{s^n} = \frac{0}{s},$$

所以 $R'_S \subseteq (R_S)'$. 任取 $u/s \in (R_S)'$, 则存在正整数 n 以及 $a_{n-1}, \dots, a_1, a_0 \in R, s_{n-1}, s_{n-2}, \dots, s_0 \in S$ 使得

$$\left(\frac{u}{s}\right)^n + \frac{a_{n-1}}{s_{n-1}} \left(\frac{u}{s}\right)^{n-1} + \cdots + \frac{a_1}{s_1} \left(\frac{u}{s}\right) + \frac{a_0}{s_0} = \frac{0}{s},$$

由上式可知存在 $t \in S, b_{n-1}, b_{n-2}, \dots, b_1, b_0 \in R$ 使得 $tu^n + b_{n-1}u^{n-1} + \cdots + b_1u + b_0 = 0$, 两边同乘 t^{n-1} 可得 $tu \in R'$, 所以 $u/s = tu/ts \in R'_S$, 故 $(R_S)' \subseteq R'_S$. \square

Corollary 2.9. 在 Dedekind 整区中任何非零真理想在不计次序下可唯一地分解为有限个素理想之积.

Proof. 根据 [命题2.3], Dedekind 整区任何非零真理想为一些准素理想之积. 而 [定理2.6] 说 Dedekind 整区的准素理想为某个素理想的幂, 所以 Dedekind 整区的非零真理想总可分解为有限个素理想之积. 因为素理想是准素理想, 所以该素理想分解的唯一性也来自 [命题2.3]. \square

Corollary 2.10. 设 R 是 Dedekind 整区, I 是非零理想. 那么 R 中包含 I 的素理想只有有限多个.

Proof. 设 $I = P_1^{n_1} P_2^{n_2} \cdots P_s^{n_s}$ 是 I 的素理想乘积分解, 其中 $n_j \geq 1$. 那么任何包含 I 的素理想 Q 一定包含某个 P_k . 而 R 作为 1 维整区, 任何非零素理想都是极大理想, 故由 P_k 是极大理想迫使 $Q = P_k$. \square

Corollary 2.11. 设 R 是 Dedekind 整区, 则 R 是 P.I.D. 当且仅当 R 是 U.F.D..

Proof. 只要证充分性. 因为任何非零真理想可分解为有限多个素理想的乘积, 因此只需验证 R 的任何非零素理想是主理想. 设 P 是 R 的非零素理想, 取 $a \neq 0 \in P$, 那么 a 有不可约元标准分解 $a = p_1^{n_1} \cdots p_t^{n_t}$, 这里每个 $n_j \geq 1$. 进而 $P \supseteq (p_1)^{n_1} \cdots (p_t)^{n_t}$. 因此存在某个 p_k 使得 $P \supseteq (p_k)$. 再由 (p_k) 是极大理想便得结论. \square

Example 2.12. 设 $X \subseteq \mathbb{k}^n$ 是代数闭域 \mathbb{k} 上仿射曲线, 则 X 的坐标环 $A(X)$ 总是 1 维 Noether 整区. 在 [例1.16] 中我们看到仿射曲线 X 在点 $p \in X$ 处光滑的充要条件是 $\mathcal{O}_{X,p}$ 是离散赋值环. 因此通过 [定理2.6] 立即得到仿射曲线 X 是光滑曲线的充要条件是坐标环 $A(X)$ 是 Dedekind 整区.

本节最后我们介绍代数数论中的代数整数环, 并证明它也是 Dedekind 整区 (见 [推论2.19]). 称 \mathbb{Q} 的扩域 K 是代数数域, 如果域扩张 $K \supseteq \mathbb{Q}$ 是有限扩张. 因此代数数域 K 总是整数环的环扩张, 称 \mathbb{Z} 在 K 中的整闭包为代数数域 K 的整数环, 记作 \mathcal{O}_K (例如取 $K = \mathbb{Q}$, 则 $\mathcal{O}_K = \mathbb{Z}$). 因为 $\mathcal{O}_K \subseteq K$ 是整闭扩张, 所以 \mathcal{O}_K 是整闭整区. 此外, $\mathbb{Z} \subseteq \mathcal{O}_K$ 是整扩张表明它们有相同的 Krull 维数, 所以 K 的整数环 \mathcal{O}_K 是 1 维整闭整区. 所以要证明 \mathcal{O}_K 是 Dedekind 整区只需说明它是 Noether 环. 为此我们回忆一些域论的必要基础知识.

称域的代数扩张 $L \supseteq K$ 是可分扩张, 如果每个 $\alpha \in L$ 在 K 上的最小多项式都没重根. 例如当 $\text{char}K = 0$ 时, K 上最小多项式都没重根, 所以特征为零的域的域扩张总是可分扩张. 我们之后需要

Lemma 2.13. 设 K 是特征为零的域, 那么任何 K 的有限扩张都是单扩张.

Proof. 任何 K 的有限扩张 L 总可写作 $L = K(\alpha_1, \dots, \alpha_n)$ 的形式, 其中每个 $\alpha_j \in L$ 是 K 上代数元. 下面对 n 作归纳来证明结论, 不难看出只需验证 $n = 2$ 的情形即可. 即说明对域扩张 $L = K(\alpha_1, \alpha_2)$, 存在 $c \in L$ 使得 $L = K(c)$. 对 $j = 1, 2$, 设 α_j 在域 K 上的最小多项式为 $p_j(x)$, 那么存在 L 的扩域 E 使得 $p_1(x), p_2(x)$ 均在 E 上分裂 (注意 $\text{char}K = 0$ 的条件保证了 $p_j(x)$ 没有重根). 设为 $p_1(x) = (x - \beta_1) \cdots (x - \beta_s), p_2(x) = (x - \gamma_1) \cdots (x - \gamma_t), \beta_i, \gamma_j \in E$. 不妨设 $\beta_1 = \alpha_1, \gamma_1 = \alpha_2$. 因为 K 是无限集而

$$S = \left\{ \frac{\beta_i - \beta_1}{\gamma_1 - \gamma_j} \mid 1 \leq i \leq s, 2 \leq j \leq t \right\} \subseteq E$$

是有有限集, 故存在 $d \in K$ 使得 $d \notin S$. 进而 $\beta_i \neq \beta_1 + d(\gamma_1 - \gamma_j), \forall 1 \leq i \leq s, 2 \leq j \leq t$.

Claim. 对 $c = \alpha_1 + d\alpha_2 = \beta_1 + d\gamma_1$ 有 $L = K(\alpha_1, \alpha_2) = K(c)$.

一旦证明该断言便得到结果. 为证此断言只需要说明 $K(\alpha_1, \alpha_2) \subseteq K(c)$. 下证 $\gamma_1 = \alpha_2 \in K(c)$, 考虑域 $K(c)$ 上多项式 $p_2(x)$ 以及 $r(x) = p_1(c - dx)$, 它们有公共零点 γ_1 , 所以均可被 γ_1 在 $K(c)$ 上最小多项式 $m(x)$ 整除. 下证 $m(x) = x - \gamma_1$ 来得到 $\gamma_1 \in K(c)$. 一方面, $m(x)$ 在 E 中的零点集是 $\{\gamma_1, \dots, \gamma_t\}$ 的子集, 另一方面, 对每个 $2 \leq j \leq t, r(\gamma_j) = p_1(\beta_1 + d(\gamma_1 - \gamma_j)) \neq 0$. 因此 $m(x)$ 在 E 中的零点只有 γ_1 . 而 $E \supseteq K$ 是可分扩张表明 $m(x)$ 在 E 上无重根, 由此得到 $m(x) = x - \gamma_1$. 结合 c 的定义立即看到 $\gamma_1 \in K(c)$ 蕴含 $\alpha_1 \in K(c)$. \square

Remark 2.14. 上述引理证明过程表明无限域的有限可分扩张总是单扩张.

事实上上述引理可以加强为有限可分扩张总是单扩张, 这就是下面的本原元定理.

Primitive Element Theorem. 任何有限可分扩张都是单扩张. 即如果 $L \supseteq K$ 是有限可分扩张, 那么存在 $\alpha \in L$ 使得 $L = K(\alpha)$, 这时称 α 是该域扩张的本原元.

Proof. 根据 [引理2.13] 的证明过程知该定理对无限域的有限可分扩张总成立. 因此只需处理有限域的情形. 现设 $K \subseteq L$ 是有限域 K 的有限可分扩张, 设 $\text{char}K = p$, 那么 K 包含素域 \mathbb{F}_p , 即 p 元域. 下面说明存在 $\alpha \in L$ 使得 $L = \mathbb{F}_p(\alpha)$ 来得到 $L = K(\alpha)$. 设 $|L| = p^m$, 如果 $\alpha \in L$ 满足 $\mathbb{F}_p(\alpha)$ 的元素数目为 $p^n, n < m$, 那么 α 满足多项式 $x^{p^n} - x$, 这说明对每个正整数 $n < m$, L 中满足 $\mathbb{F}_p(\alpha)$ 的元素数目为 $p^n (n < m)$ 的元素 α 的数目不超过 p^n . 注意到

$$p + p^2 + \cdots + p^{m-1} = \frac{p^m - p}{p - 1} < p^m,$$

所以 L 中满足 $\mathbb{F}_p(\alpha) \subsetneq L$ 的元素 α 总数严格小于 p^m . 因此存在 $\alpha \in L$ 使得 $L = \mathbb{F}_p(\alpha)$. \square

Proposition 2.15. 设 K 是域, L 是 K 的有限可分扩张, 并设 $n = [L : K]$.

- (1) 若记 \bar{K} 是 K 的代数闭包, 那么恰好存在 n 个不同的嵌入 $\sigma_i : L \rightarrow \bar{K} (1 \leq i \leq n)$ 使得 $\sigma_i(a) = a, \forall a \in K$.
- (2) 上述 n 个嵌入 $\{\sigma_1, \dots, \sigma_n\}$ 是 \bar{K} -线性无关的.

Proof. 由条件, 可设 $L = K(c)$ 是单扩张, 并设 c 在域 K 上最小多项式是 $m(x)$, 那么有域同构

$$K[x]/(m(x)) \cong L.$$

设 $\alpha_1, \dots, \alpha_n$ 是 $m(x)$ 在 \bar{K} 中所有的根, 那么域扩张的可分性说明这些根两两互异. 记 $\sigma_i : L \rightarrow \bar{K}, g(c) \mapsto g(\alpha_i)$, 这里 $g(x) \in K[x]$, 则 σ_i 是定义合理的域嵌入且 $\sigma_1, \dots, \sigma_n$ 两两互异且固定 K 中元素. 对任何固定 K 中元素的域嵌入 $\tau : L \rightarrow \bar{K}$, $\tau(c)$ 为 $m(x)$ 的根, 因此 $\tau \in \{\sigma_1, \dots, \sigma_n\}$. 最后证明对 $n \geq 1$ 作归纳来说明 $\{\sigma_1, \dots, \sigma_n\}$ 是 \bar{K} -线性无关的. 假设 $\{\sigma_1, \dots, \sigma_n\}$ 是 \bar{K} -线性相关的, 则存在不全为零的元素 $c_1, \dots, c_n \in \bar{K}$ 使得 $c_1\sigma_1 + \cdots + c_n\sigma_n = 0$. 那么对满足条件的非零 n 元组 $(c_1, \dots, c_n) \in \bar{K}^n$, 总可找到非零分量数目最小的 n 元组. 经过适当重排 $\sigma_1, \dots, \sigma_n$ 可不妨设该 n 元组恰好前 d 个分量非零. 设为 $c_1, \dots, c_d \in \bar{K}^*$ 使得 $c_1\sigma_1 + \cdots + c_d\sigma_d = 0$. 不妨设 $c_1 = 1$, 那么对任给 $x \in L$ 有 $\sigma_1(x) + c_2\sigma_2(x) + \cdots + c_d\sigma_d(x) = 0$. 选取 $y \in L$ 使得 $\sigma_1(y) \neq \sigma_2(y)$, 那么通过 $\sigma_1(xy) + c_2\sigma_2(xy) + \cdots + c_d\sigma_d(xy) = \sigma_1(x)\sigma_1(y) + \cdots + c_d\sigma_d(x)\sigma_d(y) = 0$. 可得

$$c_2(\sigma_1(y) - \sigma_2(y))\sigma_2(x) + \cdots + c_d(\sigma_1(y) - \sigma_d(y))\sigma_d(x) = 0, \forall x \in L.$$

上式中 $c_2(\sigma_1(y) - \sigma_2(y)) \neq 0$, 这与 d 的选取矛盾. \square

Remark 2.16. 设 L 是域 K 的有限可分扩张, 并设 $n = [L : K]$. 那么对每个 $x \in L$, 它决定的 L 上左乘变换 $x_l : L \rightarrow L$ 是 K -线性变换, 故可定义 x 关于扩张 $L \supseteq K$ 的迹 $T_{L/K}(x) \in K$. $T_{L/K} : L \rightarrow K$ 是 K -线性函数. 根据证明过程, 设 $L = K(c)$ 是单扩张, 命题结论中的嵌入 $\{\sigma_1, \dots, \sigma_n\}$ 满足

$$T_{L/K}(c) = \alpha_1 + \cdots + \alpha_n = \sigma_1(c) + \cdots + \sigma_n(c).$$

那么对任何 $x \in K[c] = K(c) = L$ 也有 $T_{L/K}(x) = \sigma_1(x) + \cdots + \sigma_n(x)$. 由此可知迹映射 $T_{L/K}$ 诱导出的对称 K -双线性型 $(-, -) : L \times L \rightarrow K, (x, y) \mapsto T_{L/K}(xy)$ 是非退化的: 如果 $x \in L$ 满足 $(x, y) = 0, \forall y \in L$, 则 $\sigma_1(x)\sigma_1(y) + \cdots + \sigma_n(x)\sigma_n(y) = 0, \forall y \in L$. 进而由 $\{\sigma_1, \dots, \sigma_n\}$ 的 K -线性无关性得到 $\sigma_i(x) = 0, \forall 1 \leq i \leq n$. 于是由 σ_i 是单 K -线性映射得到 $x = 0$. 所以迹映射诱导的对称双线性型是非退化的.

Corollary 2.17. 设 R 是整区, 有商域 K . 那么对 K 的任何有限可分扩张 L , R 在 L 中的整闭包 \mathcal{O} 满足

$$T_{L/K}(\beta) \in \mathcal{O} \cap K, \forall \beta \in \mathcal{O}.$$

Proof. 根据 [命题2.15], 存在 n 个不同的嵌入 $\sigma_i : L \rightarrow \overline{K} (1 \leq i \leq n)$ 使得 $\sigma_i(a) = a, \forall a \in K$ 并且前面的讨论表明 $T_{L/K}(x) = \sigma_1(x) + \cdots + \sigma_n(x), \forall x \in L$. 所以当 $\beta \in \mathcal{O}$ 时, 每个 $\sigma_i(\beta) \in \mathcal{O}$, 进而 $T_{L/K}(\beta) \in \mathcal{O}$. \square

通过前面的讨论, 我们看到域 K 的有限可分扩张 L 上的双线性型 $(-, -) : L \times L \rightarrow K, (x, y) \mapsto T_{L/K}(xy)$ 是非退化的. 设 L 作为 K -线性空间有基 $\{b_1, \dots, b_n\}$ 该双线性型对应的方阵 $(T_{L/K}(b_i b_j))_{n \times n} \in M_n(K)$ 是可逆阵. 若记该可逆阵的逆矩阵是 $C = (c_{ij})_{n \times n}$, 则对

$$b_i^* = \sum_{k=1}^n b_k c_{ki}, k = 1, 2, \dots, n,$$

有 $T_{L/K}(b_i b_j^*) = \delta_{ij}$, 这里 δ_{ij} 是 Kronecker 记号. 称 $\{b_1^*, \dots, b_n^*\} \subseteq L$ 为 $\{b_1, \dots, b_n\}$ 关于域扩张 $L \supseteq K$ 的对偶基 (易见它确实是 L 作为 K -线性空间的基). 下面我们应用对偶基来得到代数整数环的 Noether 性.

Proposition 2.18. 设 R 是整闭整区, 有商域 K . 那么对 K 的任何有限可分扩张 L , R 在 L 中的整闭包 \mathcal{O} 满足存在 L 作为 K -线性空间的基 $\{\alpha_1, \dots, \alpha_n\}$ 使得 $\mathcal{O} \subseteq R\alpha_1 + R\alpha_2 + \cdots + R\alpha_n$.

Proof. 设 L 作为 K -线性空间有基 $\{b_1, \dots, b_n\}$, 不妨设每个 $b_i \in \mathcal{O}$ (否则可通过 b_i 是整元乘上 R 中适当的元素调整成 \mathcal{O} 中元素), 那么可取其关于域扩张 $L \supseteq K$ 的对偶基 $\{b_1^*, \dots, b_n^*\}$. 对每个 $x \in \mathcal{O}$, 有 $xb_i \in \mathcal{O}$, 这时 [推论2.17] 表明 $T_{L/K}(xb_i) \in \mathcal{O}$. 另一方面, $T_{L/K}(xb_i) \in K$, 所以利用 R 是整闭整区得到 $T_{L/K}(xb_i) \in R$. 下面说明 $\mathcal{O} \subseteq Rb_1^* + Rb_2^* + \cdots + Rb_n^*$, 进而再取 $\alpha_j = b_j^*$ 即可. 因为 $\{b_1^*, \dots, b_n^*\}$ 是 L 作为 K -线性空间的基, 故对每个 $x \in \mathcal{O}$, 存在 $k_1, \dots, k_n \in K$ 使得 $x = k_1 b_1^* + \cdots + k_n b_n^*$. 两边右乘上 b_j 再作用迹函数 $T_{L/K}$ 便知 $k_j = T_{L/K}(xb_j) \in R$. 所以 $x \in Rb_1^* + Rb_2^* + \cdots + Rb_n^*$. \square

根据 Noether 模的子模仍 Noether, P.I.D. 上自由模的子模仍自由立即得到下述推论.

Corollary 2.19. 任何代数数域的代数整数环作为 \mathbb{Z} -模是有限生成自由模, 所以是 Noether 环.

Remark 2.20. 交换代数作为起源于代数几何, 代数数论以及不变量理论的学科, 本质上研究的交换环类都起源于几何或是数论. 任何仿射簇的坐标环总是 Noether 环. 该推论让我们看到代数数域的代数整数环来自数论领域的 Noether 环. 因此研究交换 Noether 环类涵盖了几何与数论中的重要研究对象.

结合前面的讨论, 我们得到

Theorem 2.21. 任何代数数域 K 的整数环 \mathcal{O}_K 是 Dedekind 整区.

在 [推论2.11] 中我们看到 Dedekind 整区是 P.I.D. 的充要条件是它是 U.F.D., 所以

Corollary 2.22. 任何代数数域 K 的整数环 \mathcal{O}_K 是 P.I.D. 当且仅当 \mathcal{O}_K 是 U.F.D..

3 分式理想

本节介绍整区的分式理想和可逆理想的概念, 可逆理想是特殊的可逆双模 (见 [例3.6]). 非零分式理想的可逆性可以用于刻画离散赋值环 (见 [命题3.7]) 和 Dedekind 整区 (见 [推论3.9]).

Definition 3.1. 设 R 是整区, F 是 R 的商域, 称 F 的 R -子模 I 为 R 的分式理想, 如果存在 $a \neq 0 \in R$ 使得 $aI \subseteq R$ (注意这里 aI 也是 R 的理想). 易见整区 R 的任何理想都是分式理想.

Remark 3.2. 所以整区 R 商域的 R -子模 I 是分式理想无非是说 I 乘上 R 中某非零元后成为 R 的理想.

Example 3.3. 设 F 是整区 R 的商域, 那么任何 $\alpha \in F$ 生成的 R -子模 (α) 是 R 的分式理想. 一般地, 对 F 任何有限生成 R -子模 I , 容易验证 I 是 R 的分式理想. 如果 R 是 Noether 整区, 那么 F 的 R -子模 I 是 R 的分式理想当且仅当 I 是有限生成 R -模. 充分性是明显的, 要看到必要性只需注意存在非零元 $a \in R$ 使得 aI 是 R 的理想, 所以 I 在 F 内可表示为 $a^{-1}J$ 的形式, 这里 $J = aI$ 是 R 的理想, 故由 J 是有限生成理想即得.

Definition 3.4. 设 R 是整区, F 是 R 的商域, 称 F 的 R -子模 I 为 R 的可逆理想, 若存在 F 的 R -子模 J 使

$$IJ = R.$$

根据定义, 如果 F 的 R -子模 J 满足 $IJ = R$, 那么 $J = \{\alpha \in F \mid \alpha I \subseteq R\}$. 所以 I 只要是可逆理想, 那么定义中的 J 被 I 唯一确定. 并且可逆理想 I 一定是 R -有限生成的, 原因是此时 $IJ = R$ 表明存在 $\alpha_1, \dots, \alpha_n \in I, \beta_1, \dots, \beta_n \in J$ 使得 $\alpha_1\beta_1 + \dots + \alpha_n\beta_n = 1$, 进而对每个 $x \in I$ 有

$$x = (x\beta_1)\alpha_1 + (x\beta_2)\alpha_2 + \dots + (x\beta_n)\alpha_n, x\beta_j \in R,$$

所以 I 作为 R -模可由 $\{\alpha_1, \dots, \alpha_n\}$ 生成. 对每个 $1 \leq j \leq n$, 若命 $\alpha_j^*: I \rightarrow R, x \mapsto \beta_j x$, 那么 $\alpha_j^* \in \text{Hom}_R(I, R)$ 且对任何 $x \in I$ 有 $x = \alpha_1^*(x)\alpha_1 + \dots + \alpha_n^*(x)\alpha_n$. 根据对偶基引理立即得到可逆理想是有限生成投射模. 反之, 如果 F 的非零 R -子模 I 是有限生成投射模, 那么 I 不仅是分式理想而且存在 $\alpha_j \in I, \alpha_j^* \in \text{Hom}_R(I, R) (1 \leq j \leq n)$ 使得 $x = \alpha_1^*(x)\alpha_1 + \dots + \alpha_n^*(x)\alpha_n, \forall x \in I$. 任取 $y \neq 0 \in I$, 并对每个 α_j^* 命 $\beta_j = y^{-1}\alpha_j^*(y)$, 那么 β_j 不依赖于 $y \neq 0 \in I$ 的具体选取, 并且有 $1 = y^{-1} \cdot y = \beta_1\alpha_1 + \dots + \beta_n\alpha_n$ 以及 $\beta_j y = \alpha_j^*(y) \in R$ (这蕴含 $\beta_j I \subseteq R$). 因此记 J 为 β_1, \dots, β_n 在 F 中生成的理想便有 $IJ = R$. 我们将刚刚的讨论总结为

Proposition 3.5. 设 R 是整区, F 是 R 的商域, 那么 F 的 R -子模 I 是 R 的可逆理想的充要条件是 I 是非零有限生成投射 R -模. 特别地, F 中任何非零元 α 生成的 R -子模 (α) 是 R 的可逆理想.

Example 3.6. 回忆对含么环 R 与 R' 上的双模 ${}_R M_R$ 被称为可逆双模, 如果存在 R - R' 双模 ${}_R M'_{R'}$ 满足双模同构 ${}_R M_R \otimes_R {}_R M'_{R'} \cong R'$ 以及 ${}_R M'_{R'} \otimes_{R'} {}_R M_R \cong R$. 如果 R 是整区, 那么 R 的任何可逆理想是可逆 R - R 双模 (这里将交换环上模视作左右模结构一致的双模).

Proof. 设 R 有可逆理想 I , 满足存在 R 的商域的 R -子模 J 使得 $IJ = R$, 下面说明 R -模同构 $I \otimes_R J \cong R$. 易知 $I \times J \rightarrow R, (a, b) \mapsto ab$ 是 R -平衡映射, 导出 R -模同态 $\varphi: I \otimes_R J \rightarrow R, a \otimes b \mapsto ab$, 易见这是满同态. 下面直接构造其逆映射 $\psi: R \rightarrow I \otimes_R J$, 首先存在 $\alpha_1, \dots, \alpha_n \in I, \beta_1, \dots, \beta_n \in J$ 使得 $\alpha_1\beta_1 + \dots + \alpha_n\beta_n = 1$, 命 $\psi: R \rightarrow I \otimes_R J, a \mapsto a\alpha_1 \otimes \beta_1 + a\alpha_2 \otimes \beta_2 + \dots + a\alpha_n \otimes \beta_n$, 因为对每个 $1 \leq j \leq n$ 有 $ab\alpha_j \otimes \beta_j = \alpha_j\beta_j a \otimes b$, 所以容易验证 ψ 与 φ 互为逆映射. \square

设 R 是整区, 考虑 R 所有可逆理想构成的集合 $\mathcal{I}(R)$, 任何 $I, J \in \mathcal{I}(R)$, 定义 $I \cdot J = IJ$, 那么 $\mathcal{I}(R)$ 关于此运算构成交换群, 称为 R 的分式理想群. 下面的命题说整区 R 的商域的 R -子模的可逆性是一个局部性质.

Proposition 3.7. 设 R 是整区, I 是 R 商域的一个 R -子模, 那么以下三条等价:

- (1) I 是可逆理想.
- (2) I 是有限生成 R -模且对 R 的任何素理想 P, I_P 是 R_P 的可逆理想.
- (3) I 是有限生成 R -模对 R 的任何极大理想 M, I_M 是 R_M 的可逆理想.

Proof. (1) \Rightarrow (2): 只需验证可逆性关于素理想处的局部化封闭. 由 [命题3.5] 知 I 是非零有限生成投射 R -模, 因此 I 在任何素理想 P 处局部化是非零有限生成投射 R_P -模, 进而知 I_P 是 R_P 的可逆理想. (2) \Rightarrow (3) 是明显的. 最后说明 (3) \Rightarrow (1): 记 $J = \{x \in F \mid xI \subseteq R\}$, 其中 F 是 R 的商域. 并且记 IJ 为 Q , 那么 F 的 R -子模 Q 是 R 的理想, 利用 I 是有限生成 R -模可计算验证对任何极大理想 M , 有 $J_M = \{x \in F_M \cong f \mid xI_M \subseteq R_M\}$, 于是 $I_M J_M = Q_M$. 由 I_M 是可逆理想得到 $Q_M = R_M$, 因此 $Q \not\subseteq M$. 由 M 的任意性得到 $Q = R$. \square

分式理想的可逆性质可用于刻画离散赋值环.

Proposition 3.8. 设 R 是局部整区, 则 R 是离散赋值环当且仅当 R 任何非零分式理想是可逆理想.

Proof. 必要性: 设 (R, \mathfrak{m}) 是离散赋值环, 其商域 F 上有离散赋值 $v: F^* \rightarrow \mathbb{Z}$. 设 \mathfrak{m} 可由 x 生成, 那么 R 的任何非零理想是由 x 的某个自然数幂生成的主理想 (回忆 [定理1.12]). 对任何非零分式理想 I , 存在 $a \neq 0 \in R$ 使得 aI 是 R 的非零理想, 可设为 $aI = (x^s)$, 其中 $s \in \mathbb{N}$. 设 $v(a) = t \in \mathbb{N}$, 那么 $(a) = (x^t)$. 于是由 R 是整区可知 I 是由 $x^{s-t} \in R$ 生成的 F 的 R -子模. 由此不难看出 I 是 R 的可逆理想.

充分性: 因为 R 的任何非零理想都是非零分式理想, 故 [命题3.5] 表明 R 的任何非零理想是有限生成的, 由此知 R 是 Noether 环. 下面证明 R 的任何非零理想是 \mathfrak{m} 的幂次, 一旦证明该断言, 则 R 的非零素理想只有 \mathfrak{m} , 且根据 [定理1.12] 便知 R 是离散赋值环. 假设 R 存在不能表示为 \mathfrak{m} 的幂次的非零理想, 作

$$S = \{J \subseteq R \mid J \text{ 是 } R \text{ 的非零理想且 } J \text{ 不能表示为 } \mathfrak{m} \text{ 的自然数幂}\},$$

那么由 R 是 Noether 环知非空理想集 S 中有极大元 I . 进而 $I \neq \mathfrak{m}$, 于是 $I \subsetneq \mathfrak{m}$. 记 R 的商域的 R -子模 \mathfrak{m}^{-1} 满足 $\mathfrak{m}\mathfrak{m}^{-1} = R$, 那么 $\mathfrak{m}^{-1}I \subseteq R$ 是 R 的理想. 并且 $\mathfrak{m}I \subseteq I$ 表明 $I \subseteq \mathfrak{m}^{-1}I$. 如果 $I = \mathfrak{m}^{-1}I$, 则 $I = \mathfrak{m}I$. 因此由 Nakayama 引理知 $I = 0$, 这与 I 的选取矛盾. 因此 $I \subsetneq \mathfrak{m}^{-1}I$, 由 I 的极大性保证了 $\mathfrak{m}^{-1}I$ 是 \mathfrak{m} 的幂. 由此得到 I 也是 \mathfrak{m} 的自然数幂, 这与 I 的选取矛盾. \square

Corollary 3.9. 设 R 是整区, 则 R 是 Dedekind 整区的充要条件是 R 的任何非零分式理想是可逆理想.

Proof. 必要性: 设 $I \neq 0$ 是 R 的非零分式理想, 那么对 R 的任何极大理想 \mathfrak{m} , $I_{\mathfrak{m}}$ 是 $R_{\mathfrak{m}}$ 的非零分式理想. 并注意到 R 的 Noether 性保证了 I 是有限生成 R -模. 因此由 [命题3.7] 与 [命题3.8] 得到 I 是 R 的可逆理想. 充分性: 因为 R 的非零理想总是分式理想, 故由可逆理想是有限生成 R -模知 R 是 Noether 环. 如果能够证明 R 在每个极大理想 \mathfrak{m} 处的局部化是离散赋值环, 那么由 $k.\dim R$ 一定是 R 在某个极大理想处局部化的 Krull 维数可得 $k.\dim R = 1$, 进而由 R 是 1 维 Noether 整闭整区以及 [定理2.6] 可知 R 是 Dedekind 整区. 对 R 的任何极大理想 \mathfrak{m} , $R_{\mathfrak{m}}$ 的任何非零分式理想可表示为 $R_{\mathfrak{m}}$ 的某个非零理想与 $R_{\mathfrak{m}}$ 的某个非零元在 $R_{\mathfrak{m}}$ 商域中的逆元的乘积, 所以结合 [定理3.8] 知只要证 $R_{\mathfrak{m}}$ 的任何非零理想是可逆理想即可. 而 $R_{\mathfrak{m}}$ 的任何非零理想形如 $I_{\mathfrak{m}}$, 这里 I 是 R 的非零理想. 所以由 I 是 R 的非零分式理想得到 I 是 R 的可逆理想. 于是由 [命题3.7] 得到 $I_{\mathfrak{m}}$ 也是 $R_{\mathfrak{m}}$ 的可逆理想. 因此由前面的讨论, R 是 Dedekind 整区. \square

因此如果 R 是 Dedekind 整区, R 的分式理想群 $\mathcal{I}(R)$ 恰好就是所有非零分式理想构成的集合. 根据 [命题3.5], R 的商域 F 中任何非零元生成的主理想是 R 的分式理想, 故这时也是可逆理想, 称为主分式理想. 易见 $\mathcal{I}(R)$ 中所有的主分式理想构成 $\mathcal{I}(R)$ 的子群, 称为主分式理想子群, 记作 $\mathcal{P}(R)$.

Corollary 3.10. 设 R 是 Dedekind 整区, 那么 R 是 U.F.D. 当且仅当 $\mathcal{P}(R) = \mathcal{I}(R)$.

Proof. 必要性: 根据 [推论2.11], 这时任何 $I \in \mathcal{I}(R)$ 满足存在非零元 $a, b \in R$ 使得 $aI = (b)$. 因此 $I \in \mathcal{P}(R)$. 充分性: 只要证 R 是 P.I.D., 任取 R 的非零理想 J , 则 J 是 R 的可逆理想. 所以存在 $a/s \neq 0 \in F$ 使得 $J = aR/s$, 这里 F 表示 R 的商域. 因此 $sJ = (a)$. 于是在 R 中 s 整除 a , 这说明 J 是主理想. \square

[推论3.10] 表明 Dedekind 整区的主分式理想子群在分式理想群中的大小可以衡量该环与 U.F.D. 的距离.

Definition 3.11. 设 R 是 Dedekind 整区, 称商群 $\mathcal{I}(R)/\mathcal{P}(R)$ 为 R 的理想类群, 记作 $\mathcal{C}(R)$.

Remark 3.12. 如果 $R = \mathcal{O}_K$ 是代数数域 K 的整数环, 也称 $\mathcal{C}(\mathcal{O}_K)$ 是 K 的理想类群.

用理想类群的语言, [推论3.10] 表明 Dedekind 整区 R 是 U.F.D. 当且仅当理想类群 $\mathcal{C}(R)$ 平凡. 在最后我们指出 Dedekind 整区的理想类群是由其所有素理想生成的自由 Abel 群.

Proposition 3.13. 设 R 是 Dedekind 整区, 则 $\mathcal{I}(R)$ 是以 $\text{Spec}R$ 为基的自由 \mathbb{Z} -模.

Proof. 先说明 R 的素理想可生成 $\mathcal{I}(R)$. 任取 R 的非零分式理想 I , 则存在 R 中非零元 a 使得 aI 是 R 的理想. 现在应用 [推论2.9] 知有素理想分解 $aI = P_1^{n_1} P_2^{n_2} \cdots P_s^{n_s}$, 其中 $n_j \geq 1$. 于是存在 $s \neq 0 \in R$ 使得 $as \in P_1^{n_1} P_2^{n_2} \cdots P_s^{n_s}$. 将 (a) 和 (s) 写成一些素理想的乘积, 利用 [推论2.9] 结论中的唯一性知存在自然数 m_1, \dots, m_s 使得 $(a) = P_1^{m_1} P_2^{m_2} \cdots P_s^{m_s}$. 因此利用每个 P_j 是可逆理想可得 $I = P_1^{n_1-m_1} P_2^{n_2-m_2} \cdots P_s^{n_s-m_s}$, 这说明乘法群 $\mathcal{I}(R)$ 可被 $\text{Spec}R$ 生成. 可逆理想被素理想 \mathbb{Z} -线性表出的唯一性来自 [推论2.9] 的唯一性. \square

参考文献

- [AM69] M.F. Atiyah and L.G. Macdonald. *Introduction to Commutative Algebra*. Addison-Wesley Publishing Company, 1969.
- [Eis04] David Eisenbud. *Commutative Algebra with a View Toward Algebraic Geometry*. Springer Science+Business Media, 2004.
- [Neu13] Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.
- [Yic] Tian Yichao. Lectures on algebraic number theory.