


二次整数环

戚天成 

复旦大学 数学科学学院

2024 年 1 月 29 日

这份笔记主要记录二次域的整数环的计算, 主要参考文献是 [DF04]. 首先我们回忆一些基本概念. 如果域 K 是 \mathbb{Q} 的有限扩张, 则称 K 是代数数域. 将代数数域作为 \mathbb{Q} -线性空间的次数称为该代数数域的次数. 例如当 $[K : \mathbb{Q}] = 2$ 时, 称 K 是二次域. 代数数域 K 的整数环 \mathcal{O}_K 是指 \mathbb{Z} 在 K 中的整闭包. 例如当 $K = \mathbb{Q}$ 时, $\mathcal{O}_{\mathbb{Q}} = \mathbb{Z}$. 代数数域的整数环是代数数论中的中心研究对象, 它是 Dedekind 整区, 所以 \mathcal{O}_K 决定的仿射概形是非奇异的.

1 代数数域的复嵌入

本节我们说明有理数域的任何代数扩张可嵌入复数域. 特别地, 代数数域从同构于复数域的某个子域.

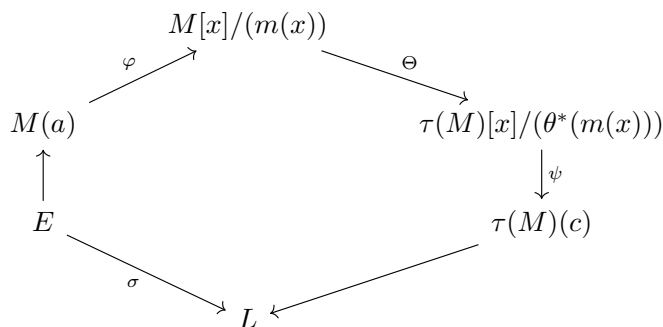
Theorem 1.1. 设 E, L 是域, 其中 L 是代数闭域, $\sigma : E \rightarrow L$ 是非零环同态, K 是 E 的代数扩张, 则存在环同态 $\tilde{\sigma} : K \rightarrow L$ 使得 $\tilde{\sigma}|_E = \sigma$.

$$\begin{array}{ccc} & K & \\ & \nearrow & \searrow \tilde{\sigma} \\ E & \xrightarrow{\sigma} & L \end{array}$$

Proof. 命 $S = \{(F, f) | F \text{ 是 } K \supseteq E \text{ 的中间域, } f : F \rightarrow L \text{ 是环同态且 } f|_E = \sigma\}$, 那么 S 是集合且 $(E, \sigma) \in S$ 表明 S 是非空的. 在 S 上定义二元关系 $\leq : (F_1, f_1) \leq (F_2, f_2) \Leftrightarrow F_1 \subseteq F_2, f_2|_{F_1} = f_1$. 容易验证 (S, \leq) 是非空偏序集, 且任何全序子集 $\{(F_\alpha, f_\alpha) | \alpha \in \Lambda\}$ 有上界 (F, f) , 这里 $F = \bigcup_{\alpha \in \Lambda} F_\alpha, f : F \rightarrow L, x \mapsto f_\alpha(x)$ (对每个 $x \in F$, 存在 $\alpha \in \Lambda$ 使得 $x \in F_\alpha$, 这里定义 $f(x) = f_\alpha(x)$, 容易验证 f 是定义合理的环同态), 故由 Zorn 引理知上述偏序集有极大元 (M, τ) , 我们断言 $M = K$. 若不然, 设 M 是 K 的真子域, 那么存在 $a \in K - M$, 设 a 在 M 上首一最小多项式是 $m(x)$, 那么 $\varphi : M(a) \rightarrow M[x]/(m(x)), g(a) \mapsto g(x) + (m(x))$ 是环同构. 因为 τ 是非零环同态, 所以由 M 是域可知 $\tau : M \rightarrow L$ 是单保么环同态, 进而有域同构 $\theta : M \rightarrow \tau(M), x \mapsto \tau(x)$, 这导出多项式环间的同构 $\theta^* : M[x] \rightarrow \tau(M)[x], \sum_{i=0}^l b_i x^i \mapsto \sum_{i=0}^l \tau(b_i) x^i$, 易见 $\tau(M)$ 是 L 的子域. 因为 $m(x)$ 是 $M[x]$ 中不可约多项式, 所以由 θ^* 是同构可知 $\theta^*(m(x))$ 是 $\tau(M)[x]$ 中的不可约多项式. 因为 L 是代数闭域, 所以 $\theta^*(m(x))$ 在 L 中有根 c , 于是有环同构 $\psi : \tau(M)[x]/(\theta^*(m(x))) \rightarrow \tau(M)(c), h(x) + (\theta^*(m(x))) \mapsto h(c)$. 并注意到 θ^* 导出环同构 $\Theta : M[x]/(m(x)) \rightarrow \tau(M)[x]/(\theta^*(m(x))), g(x) + (m(x)) \mapsto \theta^*(m(x)) + (\theta^*(m(x)))$.

$$M(a) \xrightarrow{\varphi} M[x]/(m(x)) \xrightarrow{\Theta} \tau(M)[x]/(\theta^*(m(x))) \xrightarrow{\psi} \tau(M)(c) \longrightarrow L$$

注意到 $\psi \circ \varphi$ 能够诱导一个 $M(a)$ 到 L 的环同态且容易验证下图交换:



这与 (M, τ) 是极大元矛盾. 因此 $M = K$, 取 $\tilde{\sigma} = \tau$ 即得结果. □

Example 1.2. 取 $E = \mathbb{Q}, K$ 是代数数域且 $L = \mathbb{C}$. 那么标准嵌入 $j: \mathbb{Q} \rightarrow \mathbb{C}$ 诱导域嵌入 $\tilde{j}: K \rightarrow \mathbb{C}$.

Corollary 1.3. 域 E 的任何代数扩张可嵌入 E 的代数闭包.

Proof. 在 [定理1.1] 中取 L 为 E 的代数闭包即可. □

Remark 1.4. 由 [定理1.1], E 的所有代数扩张中, 代数闭包可视为某种意义上“最大”代数扩张.

2 二次整数环的计算

本节固定二次域 K , 即满足 $[K : \mathbb{Q}] = 2$. 根据 [定理1.1], 可设 $K \subseteq \mathbb{C}$. 因为 $\text{char}\mathbb{Q} = 0$, 故由本原元定理知存在 $c \in K$ 使得 $K = \mathbb{Q}(c)$. 设 c 满足的 \mathbb{Q} 上最小多项式是 $m(x)$, 那么 $m(x)$ 是二次的, 设为 $m(x) = x^2 + a_1x + a_0, a_i \in \mathbb{Q}$. 于是 $\sqrt{a_1^2 - 4a_0}$ 不是有理数, 易见 $K = \mathbb{Q}(c) = \mathbb{Q}(\sqrt{a_1^2 - 4a_0})$, 那么存在既不是 0 也不是 1 的无平方因子整数 D 使得 $K = \mathbb{Q}(\sqrt{D})$. 易知 K 中任何元素形如 $a + b\sqrt{D} (a, b \in \mathbb{Q})$.

Lemma 2.1. 如果 D_1, D_2 均为既不是 0 也不是 1 的无平方因子整数, 则 $\mathbb{Q}(\sqrt{D_1}) = \mathbb{Q}(\sqrt{D_2}) \Leftrightarrow D_1 = D_2$.

Proof. 设 $\mathbb{Q}(\sqrt{D_1}) = \mathbb{Q}(\sqrt{D_2})$, 那么存在有理数 a, b 使得 $\sqrt{D_1} = a + b\sqrt{D_2}$. 假设 $b = 0$, 那么 $D_1 = a^2$ 可得 a 是整数, 这与 D_1 是既不是 0 也不是 1 的无平方因子整数矛盾. 因此 $b \neq 0$. 如果 $a \neq 0$, 那么由 $D_1 = a^2 + 2ab\sqrt{D_2} + b^2D_2$ 可知 $\sqrt{D_2} \in \mathbb{Q}$, 这与 D_2 是既不是 0 也不是 1 的无平方因子整数矛盾. 因此 $a = 0$. 现在我们得到 D_2/D_1 是某个有理数的平方, 假设 $D_2 \neq D_1$, 可设互素的正整数 s, t 满足 $s^2D_2 = t^2D_1$, 并且 s, t 其中一个至少是 2. 这蕴含 D_1 与 D_2 中至少有一个不是无平方因子整数, 矛盾. □

Remark 2.2. 如果 D 是既不是 0 也不是 1 的无平方因子整数, 易验证 $\{1, \sqrt{D}\}$ 是 $\mathbb{Q}(\sqrt{D})$ 的 \mathbb{Q} -基.

由此可知集合 $\mathcal{S} = \{D \in \mathbb{Z} | D \text{ 无平方因子且 } D \neq 0, 1\}$ 与所有二次域 $\mathcal{Q} = \{K \subseteq \mathbb{C} | \mathbb{Q} \subseteq K, [K : \mathbb{Q}] = 2\}$ 间有标准双射 $\mathcal{S} \rightarrow \mathcal{Q}, D \mapsto \mathbb{Q}(\sqrt{D})$. 如果不限制二次域在 \mathbb{C} 中, 那么有双射 $\varphi: \mathcal{S} \rightarrow \{\text{二次域的同构类}\}, D \mapsto [\mathbb{Q}(\sqrt{D})]$. 根据 [例1.2] 和前面的讨论, φ 是满射. 依 [引理2.1] 得到 φ 是单射. 所以二次域都被某个既不是 0 也不是 1 的无平方因子整数决定. 以下我们仍假设考虑的二次域 $K = \mathbb{Q}(\sqrt{D})$ 是 \mathbb{C} 的子域.

当 $D \equiv 1 \pmod{4}$ 时, 记 $\omega = (1 + \sqrt{D})/2$, 易验证 $\omega \in \mathcal{O}_K$. 所以 $\mathbb{Z}[\omega] = \{a + b\omega | a, b \in \mathbb{Z}\} \subseteq \mathcal{O}_K$. 反之, 任取 $a + b\sqrt{D} \in \mathcal{O}_K$, 这里 $a, b \in \mathbb{Q}$. 那么 $a \pm b\sqrt{D}$ 是 $x^2 - 2ax + (a^2 - Db^2) \in \mathbb{Q}[x]$ 的根. 如果 $b = 0$,

那么 $a \in \mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$. 如果 $b \neq 0$, 那么 $x^2 - 2ax + (a^2 - Db^2)$ 是 $a + b\sqrt{D}$ 在 \mathbb{Q} 上的最小多项式, 于是由 $a + b\sqrt{D}$ 也满足某个首一整系数多项式 $g(x)$ 可知 $x^2 - 2ax + (a^2 - Db^2)$ 整除 $g(x)$. 所以 $a \pm b\sqrt{D}$ 都是 $g(x)$ 的根. 那么由 Vieta 定理知 $2a, a^2 - Db^2 \in \mathbb{Z}$. 于是 $4(a^2 - Db^2) - 4a^2 \in \mathbb{Z}$, 于是 $(2b)^2 D \in \mathbb{Z}$, 结合 $b \in \mathbb{Q}$ 易知 $2b \in \mathbb{Z}$. 记 $2a = s, 2b = t$, 那么由 $a^2 - Db^2 \in \mathbb{Z}$ 可得 $s^2 - Dt^2 \equiv 0 \pmod{4}$. 于是 s, t 必定同奇或同偶, 由此可知 $a + b\sqrt{D} \in \mathbb{Z}[\omega]$. 刚刚的讨论证明了

Proposition 2.3. 设 D 为既不是 0 也不是 1 的无平方因子整数并且 $D \equiv 1 \pmod{4}$, 那么

$$\mathcal{O}_K = \mathbb{Z} \left[\frac{1 + \sqrt{D}}{2} \right].$$

下设 $D \equiv 2, 3 \pmod{4}$, 首先易见 $\mathbb{Z}[\sqrt{D}] \subseteq \mathcal{O}_K$. 反之, 任取 $a + b\sqrt{D} \in \mathcal{O}_K$, 这里 $a, b \in \mathbb{Q}$. 类似前面的讨论可知 $2a, 2b \in \mathbb{Z}$. 同样设 $2a = s, 2b = t$, 那么由 $a^2 - Db^2 \in \mathbb{Z}$ 可得 $s^2 - Dt^2 \equiv 0 \pmod{4}$. 注意到 $s^2 \equiv 0, 1 \pmod{4}$, 所以 t 只可能是偶数, 进而 s 也是偶数. 这说明 $a, b \in \mathbb{Z}$. 于是我们得到

Proposition 2.4. 设 D 为既不是 0 也不是 1 的无平方因子整数并且 $D \equiv 2, 3 \pmod{4}$, 那么 $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$.

现在把 [命题2.3] 和 [命题2.4] 总结为下述定理.

Theorem 2.5. 设 D 为既不是 0 也不是 1 的无平方因子整数, 则 $\mathcal{O}_K = \mathbb{Z}[\omega]$, 其中

$$\omega = \begin{cases} (1 + \sqrt{D})/2, & D \equiv 1 \pmod{4} \\ \sqrt{D}, & D \equiv 2, 3 \pmod{4}. \end{cases}$$

Example 2.6. 如果 $D = -1$, 那么 $K = \mathbb{Q}(i)$. 这时 $\mathcal{O}_K = \mathbb{Z}[i]$ 是 Gauss 整数环.

Example 2.7. 如果 $D = 5$, 那么 $K = \mathbb{Q}(\sqrt{5})$. 这时 $\mathcal{O}_K = \mathbb{Z}[(1 + \sqrt{5})/2] \supsetneq \mathbb{Z}[\sqrt{5}]$.

Definition 2.8. 设 $E \subseteq K$ 是域的有限扩张, $x \in K$, 并记 $\ell_x : K \rightarrow K$ 是 x 决定的左乘变换. 称 E -线性变换 ℓ_x 的迹 $\text{tr}(\ell_x)$ 为 x 关于 E 的迹, 记作 $\text{tr}_{K/E}(x)$. 称 ℓ_x 的行列式 $\det(\ell_x)$ 为 x 关于 K 的范数, 记作 $N_{K/E}(x)$. 将 $\text{tr}_{K/E} : L \rightarrow K, x \mapsto \text{tr}_{K/E}(x)$ 与 $N_{L/K} : L \rightarrow K, x \mapsto N_{K/E}(x)$ 分别称为迹映射与范数映射.

现在取 $E = \mathbb{Q}$, 我们来计算二次域 $K = \mathbb{Q}(\sqrt{D})$, 这里 $D \neq 0, 1$ 且是无平方因子的整数, 的范数映射. 首先 K 作为 \mathbb{Q} -线性空间有基 $\{1, \sqrt{D}\}$, 因此每个 $x = a + b\sqrt{D} \in K (a, b \in \mathbb{Q})$ 对应的 K 上左乘变换 ℓ_x 满足

$$\ell_x(1, \sqrt{D}) = (1, \sqrt{D}) \begin{pmatrix} a & Db \\ b & a \end{pmatrix},$$

由此可知 $N_{K/\mathbb{Q}}(a + b\sqrt{D}) = a^2 - Db^2$. 如果 $D \equiv 2, 3 \pmod{4}$, 那么 $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$, 于是每个 $a + b\sqrt{D} \in \mathcal{O}_K (a, b \in \mathbb{Z})$ 的范数为 $a^2 - Db^2 \in \mathbb{Z}$. 于是由范数映射保持乘法, $N_{K/\mathbb{Q}}(1) = 1$ 以及 $(a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - Db^2$ 可知 \mathcal{O}_K 中元素 α 是乘法可逆元当且仅当 $N_{K/\mathbb{Q}}(\alpha) = \pm 1$. 如果 $D \equiv 1 \pmod{4}$, 那么每个 $a + b(1 + \sqrt{D})/2 \in \mathcal{O}_K$ 诱导的左乘变换在 $\{1, \sqrt{D}\}$ 下表示矩阵的行列式为 $a^2 + ab + (1 - D)b^2/4$. 如果记 $\omega = (1 + \sqrt{D})/2, \bar{\omega} = (1 - \sqrt{D})/2$, 那么 $N_{K/\mathbb{Q}}(a + \omega) = (a + b\omega)(a + b\bar{\omega})$. 同样可得 \mathcal{O}_K 中元素 α 是乘法可逆元当且仅当 $N_{K/\mathbb{Q}}(\alpha) = \pm 1$. 因此代数数域上的范数映射可刻画其整数环中的可逆元. 将前面的讨论总结为

Theorem 2.9. 设 D 为既不是 0 也不是 1 的无平方因子整数, $K = \mathbb{Q}(\sqrt{D})$, 并记

$$\omega = \begin{cases} (1 + \sqrt{D})/2, & D \equiv 1 \pmod{4} \\ \sqrt{D}, & D \equiv 2, 3 \pmod{4}, \end{cases} \quad \bar{\omega} = \begin{cases} (1 - \sqrt{D})/2, & D \equiv 1 \pmod{4} \\ -\sqrt{D}, & D \equiv 2, 3 \pmod{4}, \end{cases}$$

那么对任何 $a + b\omega \in \mathcal{O}_K (a, b \in \mathbb{Z})$, 有

$$N_{K/\mathbb{Q}}(a + b\omega) = (a + b\omega)(a + b\bar{\omega}) = \begin{cases} a^2 + ab + (1 - D)b^2/4, & D \equiv 1 \pmod{4} \\ a^2 - Db^2. & D \equiv 2, 3 \pmod{4}, \end{cases}$$

特别地, $N_{K/\mathbb{Q}}(\mathcal{O}_K) \subseteq \mathbb{Z}$. 并且 $\alpha \in \mathcal{O}_K$ 是可逆元当且仅当 $N_{K/\mathbb{Q}}(\alpha) = 1$.

Example 2.10. 设 D 是无平方因子的正整数, 称方程 $x^2 - Dy^2 = 1$ 是 **Pell 方程**. 人们感兴趣该方程的整数解. 我们不妨设 $D \neq 1$, 否则由 $(x - y)(x + y) = 1$ 不难得到该方程所有的整数解. 如果 (s, t) 是 $x^2 - Dy^2 = 1$ 的整数解, 那么 $(s + \sqrt{D}t)(s - \sqrt{D}t) = 1$, 由此得到 $s + \sqrt{D}t$ 是 $\mathbb{Z}[\sqrt{D}]$ 中的可逆元. 因此求解 Pell 方程的整数解可化归为求出二次域 $K = \mathbb{Q}(\sqrt{D})$ 的整数环 \mathcal{O}_K 中的所有可逆元.

Example 2.11. 设 $D = -1$, 则 $K = \mathbb{Q}(i)$, $\mathcal{O}_K = \mathbb{Z}[i]$. **Fermat 二平方和定理**说素数 p 可表示为两个整数的平方和的充要条件是 $p = 2$ 或 $p \equiv 1 \pmod{4}$. 我们可以在 $\mathbb{Z}[i]$ 中研究素数是否可表为二整数平方和问题. 如果有整数 a, b 使得 $p = a^2 + b^2$, 那么 $p = (a + bi)(a - bi) = N_{K/\mathbb{Q}}(a + bi)$. 因此素数 p 可表示为某两个整数的平方和等价于存在 $\alpha \in \mathcal{O}_K = \mathbb{Z}[i]$ 使得 $p = N_{K/\mathbb{Q}}(\alpha)$.

参考文献

[DF04] D.S. Dummit and R.M. Foote. *Abstract Algebra*, volume 3. Wiley Hoboken, 2004.