问题 (1): 本系列问题中, 我们研究域上的可分代数.

问题 (1.1): 对交换环 R, 若 R 的理想降链都终止, 即对 R 的理想 $\{I_n\}_{n=1}^{\infty}$, 若 $I_1 \supset I_2 \supset I_3 \cdots$, 则存在 $N \in \mathbb{Z}_{\geq 0}$, 使得 $I_n = I_N$ 对所有 $n \geq N$ 成立, 则我们称 R 是一个 Artinian 环.请按照下列步骤, 证明 Artinian 环的结构定理:

(1) 请证明: R 只有有限多个极大理想.(**提示**: 若 $\{\mathfrak{m}_n\}_{n=1}^{\infty}$, 则 $\mathfrak{m}_1 \supset \mathfrak{m}_1\mathfrak{m}_2 \supset \cdots$ 是理想降链.)

(2) 记 $I = \mathrm{Rad}(R) = \bigcap_{\mathfrak{m}\text{是}R\text{的极大理想}} \mathfrak{m}$ 是 R 的所有极大理想的交集,请证明: 存在 $n \in \mathbb{Z}_{\geq 1}$, 使得 $I^n = 0$.(**提示**: 由 Artinian 环定义, 存在 n 使得 $I^n = I^{n+1}$. 此时, 考虑理想 $J = \{r \in R : rI^n = 0\}$, 只需证明 $1 \in J$ 即可. 否则, 由 Artinian 性, 可以找到极小的理想 J_0, 使得 $J_0 \supsetneqq J$. 此时 J_0/J 是单 R-模, 故存在 R 的极大理想 $\mathfrak{m}$, 使得 $J_0/J \cong R/\mathfrak{m}$. 此时 $IJ_0 \subset J$, 进而 $J_0I^n = J_0I^{n+1} \subset JI^n = 0$, 矛盾.)

(3) 请证明: 存在环同构 $R \cong \prod_{i=1}^{m} R/\mathfrak{m}_i^n$, 其中 $\mathfrak{m}_1, \ldots, \mathfrak{m}_m$ 是 R 的全部极大理想, 而 $n \in \mathbb{Z}_{\geq 1}$.

(4) 请证明: R 是 Noetherian.(**提示**: 由 (3) 只需证明 $R/\mathfrak{m}_i^n$ 是 Noetherian 的, 即不妨设 R 是只有极大理想 $\mathfrak{m}$ 的局部环. 若 R 不是 Noetherian 的, 由 Artinian 性, 存在极小的理想 I, 使得 I 不是有限生成的. 此时若 $\mathfrak{m}I = I$, 则 $0 = \mathfrak{m}^nI = I$, 矛盾. 故 $\mathfrak{m}I \subsetneqq I$, 进而 $\mathfrak{m}I$ 是有限生成的. 此时, 将 $I/\mathfrak{m}I$ 看作 $R/\mathfrak{m}$-线性空间, 由非有限生成, 则 $I/\mathfrak{m}I$ 一定是无穷维的. 记 $\{e_n\}_{n=1}^{\infty}$ 是 $I/\mathfrak{m}I$ 的线性无关组, 考虑 $e_2, e_3, \ldots$ 生成的子空间 W, 这意味着存在理想 J, 使得 $\mathfrak{m}I \subset J \subsetneqq I$, 且 $J/\mathfrak{m}I$ 是无穷维的, 进而 J 不是有限生成的, 与 I 的极小性矛盾.)

(5) 请证明: 对 R 的极大理想 $\mathfrak{m}$ 和 $n \in \mathbb{Z}_{\geq 1}$, 当 n 足够大时, 有 $R_{\mathfrak{m}} = R/\mathfrak{m}^n$ (你可以用到如下事实:$(R/\mathfrak{m}^n) = (R/\mathfrak{m}^n)_{\mathfrak{m}} = R_{\mathfrak{m}}/\mathfrak{m}^nR_{\mathfrak{m}}$), 进而命题 (3) 告诉我们 $R = \prod_{\mathfrak{m}\text{是极大理想}} R_{\mathfrak{m}}$.(**提示**: 利用 Nakayama 引理.)

证明. (1), (2), (4) 都由提示得到, (3) 由中国剩余定理得到, 对于 (5), 只需证明 n 足够大时 $\mathfrak{m}^nR_{\mathfrak{m}} = 0$. 由 Artinian 性, 存在 n, 使得 $\mathfrak{m}^nR_{\mathfrak{m}} = \mathfrak{m}^{n+1}R_{\mathfrak{m}}$, 进而由 Nakayama 引理, 存在 $x \in \mathfrak{m}R_{\mathfrak{m}}$, 使得 $(1+x)\mathfrak{m}^nR_{\mathfrak{m}} = 0$. 注意到 $1+x$ 在 $R_{\mathfrak{m}}$ 中可逆, 故 $\mathfrak{m}^nR_{\mathfrak{m}} = 0$. $\square$

问题 (1.2): 对域上的有限维 K-代数 A,请证明 下列条件等价:

(1) $A \otimes_K K^{alg}$ 是既约的, 即 $\mathrm{nil}(A \otimes_K K^{alg}) = 0$.

(2) $A \otimes_K K^{alg} = K^{alg} \times K^{alg} \times \cdots \times K^{alg}$.

(3) 存在 K 的有限可分扩张 $L_1, \ldots, L_n$, 使得 $A = \prod_{i=1}^{n} L_i$.

提示: 由 $\dim_K(A) < \infty$, 此时 A 是 Artinian 的, 因而可以利用 Artinian 环的结构定理.

证明. 若 L/K 是有限可分扩张, 则 L/K 是单扩张, 进而存在 $\theta \in L$ 使得 $L = K(\theta)$. 进而 $L = K[X]/(f(X))$, 其中 $f(X)$ 是 θ 的不可约多项式. 记 $f(X)$ 在 K^{alg} 中的全部根是 $\theta_1, \ldots, \theta_n$, 则 $L \otimes_K K^{alg} = K^{alg}[X]/(f(X)) = K^{alg}[X]/(\prod_{i=1}^{n}(X-\theta_i)) = \prod_{i=1}^{n} K^{alg}[X]/(X-\theta_i) = (K^{alg})^n$. 综上所述, 则 (3) 可以推出 (2), 而显然 (2) 可以推出 (1). 当 (1) 成立, 由 Artinian 环的结构定理, 则 $A \otimes_K K^{alg} = \prod_{\mathfrak{m}\text{是极大理想}} (A_{\mathfrak{m}} \otimes_K K^{alg})$, 因而用 $A_{\mathfrak{m}}$ 替代 A, 只需考虑 A 是局部环的情形. 此时 $\mathrm{nil}(A) = \mathfrak{m}$, 这里 $\mathfrak{m}$ 是 A 的唯一极大理想, 故而 $\mathrm{nil}(A) = 0$, 进而 A 是域. 若 A/K 是可分的, 则我们便得到了 (3). 若 A/K 不是可分的, 记 A^{sep} 是 K 在 A 中的可分闭包, 此时 $A \otimes_K K^{alg} = A \otimes_{A^{sep}} (A^{sep} \otimes_K K^{alg})$. 由 (3) 推 (2), 则 $A^{sep} \otimes_K K^{alg} = (K^{alg})^{[A^{sep}:K]}$, 即 $A \otimes_K K^{alg} = (A \otimes_{A^{sep}} K^{alg})^{[A^{sep}:K]}$, 进而不失一般性, 可以用 A^{sep} 替代 K, 不妨设 A/K 是纯不可分的. 此时, 存在 $\alpha \in A - K$, 使得 $\alpha^p \in K$. 记 $L = K(\alpha)$, 则 $L \otimes_K K^{alg}$ 是 $A \otimes_K K^{alg}$ 的子环, 下面我们证明 $L \otimes_K K^{alg}$ 不是既约的. 不失一般性, 不妨设 L 是 K^{alg} 的子域, 即 $\alpha \in K^{alg}$. 此时 $L = K[X]/(X^p - \alpha^p)$, 进而 $L \otimes_K K^{alg} = K^{alg}[X]/(X-\alpha)^p$, 然而后者显然不是既约的, 故得证. □

问题 (2): 本系列问题中, 我们将介绍 Galois 理论的一个简单的例子. 为防同学们不熟悉 Galois 扩张的概念, 这里简要介绍一些本问题中会用到的关于 Galois 扩张的基本事实: 对域的有限扩张 L/K, 记 $G = \mathrm{Aut}_K(L)$. 对 G 的子群 H, 记 $\mathrm{Inv}(H) = \{x \in L : \sigma(x) = x\text{对所有}\sigma \in H\text{成立}\}$. 若 $\mathrm{Inv}(G) = K$, 则称 L/K 是一个 Galois 扩张, 此时记 $\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L)$ 为 L/K 的 Galois 群. 可以证明, L/K 是 Galois 扩张当且仅当 L/K 是正规可分扩张, 当且仅当存在 K 上的多项式 $f(X)$, 使得 $f(X) = \prod_{i=1}^{n}(X-\alpha_i)$, 其中 $\alpha_i \in L$ 且 $L = K(\alpha_1, \ldots, \alpha_n)$. 当 L/K 是 Galois 扩张, 则对 $G = \mathrm{Gal}(L/K)$ 的子群 H, 则 $H \mapsto \mathrm{Inv}(H)$ 给出了 G 的子群与 L/K 的中间域的 1-1 对应, 其逆映射为 $E \mapsto \mathrm{Gal}(L/E)$, 且满足 $[L:E] = |\mathrm{Gal}(L/E)|$.

问题 (2.1): 对域扩张 L/K, 若 E_1/K 和 E_2/K 是 Galois 子扩张,<u>请证明</u>: E_1E_2/K 也是 Galois 扩张, 且 $\mathrm{Gal}(E_1E_2/K) \to \mathrm{Gal}(E_1/K) \times \mathrm{Gal}(E_2/K), \sigma \mapsto (\sigma|_{E_1}, \sigma|_{E_2})$ 是群的嵌入.

证明. 略. □

问题 (2.2): 从这一问开始, 我们考虑 $\mathbb{Q}$ 的扩域 $K = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_n})$, 其中 $p_1, \ldots, p_n$ 是互不相同的素数,<u>请证明</u>: $K/\mathbb{Q}$ 是 Galois 扩张, 且存在 $0 \leq r \leq n$, 使得 $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r$.

证明. 由 (2.1), 存在嵌入 $\mathrm{Gal}(K/\mathbb{Q}) \to (\mathbb{Z}/2\mathbb{Z})^n$, 进而得证. □

问题 (2.3): 对 $(m_1, \ldots, m_n) \in \{0,1\}^n$,<u>请证明</u>:$\mathbb{Q}(\sqrt{p_1^{m_1} p_2^{m_2} \ldots p_n^{m_n}})$ 是两两不同的域扩张, 即 $K/\mathbb{Q}$ 存在至少 $2^n - 1$ 个不同的 2 次子扩张.

证明. 对于 $d_1, d_2 \in \mathbb{Z}$, 若 $\mathbb{Q}(\sqrt{d_1}) = \mathbb{Q}(\sqrt{d_2}) \neq \mathbb{Q}$, 则存在 $a, b \in \mathbb{Q}$, 使得 $\sqrt{d_1} = a + b\sqrt{d_2}$, 进而 $d_1 = a^2 + b^2 d_2 + 2ad\sqrt{d_2}$. 若 $\sqrt{d_2} \notin \mathbb{Q}$, 则 $a = 0$ 或 $b = 0$. 若 $b = 0$, 则 $\sqrt{d_1} \in \mathbb{Q}$, 矛盾, 故 $a = 0$, 此时 $d_1 = b^2 d_2$. 由此即可得到本题结论. $\square$

问题 (2.4):<u>请证明</u>: $\mathrm{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^n$, 并具体指出其中的每个元素是如何在 K 上作用的.

证明. 由 (2.3), 则 $\mathrm{Gal}(K/\mathbb{Q})$ 存在 $2^n - 1$ 个不同的指数为 2 的子群, 而在 $(\mathbb{Z}/2\mathbb{Z})^r$ 中指数为 2 的子群恰有 $\frac{(2^r-1)(2^r-2)\dots(2^r-2^{r-2})}{(2^{r-1}-1)(2^{r-1}-2)\dots(2^{r-1}-2^{r-2})} = 2^r - 1$ 个, 由 $r \leq n$, 则 $\mathrm{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/2\mathbb{Z})^n$. 此时 $\sigma = (m_1, \dots, m_n) \in (\mathbb{Z}/2\mathbb{Z})^n$ 在 K 上的作用由 $\sigma(\sqrt{p_i}) = (-1)^{m_i}\sqrt{p_i}$ 给出. $\square$

问题 (2.5):<u>请证明</u>: $\sqrt{p_1} + \sqrt{p_2} + \cdots + \sqrt{p_n}$ 不是整数.

证明. 由 (2.4) 不难得到. $\square$

问题 (3): 本系列问题中, 我们研究 Dedekind 整环与域扩张间的关联.

问题 (3.1):<u>请证明</u>: 若 R 是 Dedekind 整环, 则 R 是 Noetherian 的, 整闭的, 且 $\dim(R) = 1$.

证明. 由定义, 则 R 是 Noetherian 的. 由第 7 次习题课的 (1.6), 则 R 是整闭的. 由第 6 次习题课的 (2.7)(2), 则 $\dim(R) = 1$. $\square$

问题 (3.2): 对交换环 R, 若 R 是局部环, 即 R 只有唯一极大理想 $\mathfrak{m}$, <u>请证明</u>: 对 $r \in \mathfrak{m}$, 则 $1 + r$ 是 R 中的可逆元.

Proof: 否则 $(1 + r)$ 是 R 的真理想, 进而 $1 + r \in (1 + r) \subset \mathfrak{m}$, 则 $1 = (1 + r) - r \in \mathfrak{m}$, 与 $\mathfrak{m}$ 是极大理想矛盾.

问题 (3.3): <u>请证明:</u> 若 M 是有限生成 R-模, 且 $M = \mathfrak{m}M$, 其中 $\mathfrak{m}M$ 是 rm 生成的子模, 其中 $r \in \mathfrak{m}, m \in M$, 则 $M = 0$.

提示: 利用 Nakayama 引理.

证明. 利用 Nakayama 引理, 存在 $a \in \mathfrak{m}$, 使得 $am = m$ 对所有 $m \in M$ 成立, 进而 $(1 - a)M = 0$. 由 (3.1), 则 $1 - a$ 可逆, 故 $M = 0$. $\square$

问题 (3.4):<u>请根据以下步骤证明</u>, 若 R 是局部整环, $\mathfrak{m}$ 是唯一极大理想, 满足 R 是 Noetherian 的, 整闭的,$\dim(R) = 1$, 则 R 是离散赋值环.

(1) $\mathfrak{m} \neq \mathfrak{m}^2$.

(2) 取 $\pi \in \mathfrak{m} - \mathfrak{m}^2$, 则任取 $x \in \mathfrak{m}$, 存在 n 使得 $x^n \in \pi R$.(**提示**: 否则, 考虑乘性子集 $S = \{1, x, x^2, \dots\}$ 以及局部化 $S^{-1}R$ 中包含 $\pi S^{-1}R$ 的极大理想)

(3) 存在 $n \in \mathbb{Z}_{\geq 0}$, 使得 $\mathfrak{m}^n \subset \pi R$.(**提示**: 利用 $\mathfrak{m}$ 是有限生成的)

(4) 取 n, 使得 $\mathfrak{m}^n \subset \pi R$, 且 $\mathfrak{m}^{n-1} \not\subset \pi R$. 此时, 取 $t \in \mathfrak{m}^{n-1} - \pi R$, 则 $\frac{t}{\pi}\mathfrak{m}$ 是 R 的理想.(**提示**: 注意到 $t\mathfrak{m} \subset \mathfrak{m}^n \subset \pi R$)

(5) 在 (4) 的条件下, 若 $n > 1$, 证明 $\frac{t}{\pi}\mathfrak{m} \subset \mathfrak{m}$, 进而 $\frac{t}{\pi}$ 是 R 上的整元, 故 $\frac{t}{\pi} \in R$, 即 $t \in \pi R$ 矛盾.(**提示**: 若 $\frac{t}{\pi}\mathfrak{m} \not\subset \mathfrak{m}$, 则 $\frac{t}{\pi}\mathfrak{m} = R$)

(6) 由 (4),(5), 则 $\mathfrak{m} = \pi R$ 是主理想. 进而 R 是离散赋值环.(**提示**: 此时 π 是 R 的唯一素元, 只需证明 R 是唯一分解整环即可)

证明. 对于 (1), 若 $\mathfrak{m} = \mathfrak{m}^2$, 则由 (3.4), 有 $\mathfrak{m} = 0$, 与 $\dim(R) = 1$ 矛盾. 对于 (2), 若不存在 n 使得 $x^n \in \pi R$, 考虑乘性子集 $S = \{1, x, x^2, \dots\}$, 则 $S^{-1}R$ 包含 $S^{-1}(\pi R)$ 的极大理想给出 R 的素理想 $\mathfrak{p}$, 满足 $\pi \in \mathfrak{p}$ 且 $x \notin \mathfrak{p}$. 由 $\mathfrak{m}$ 是唯一极大理想, 则 $0 \subsetneq \mathfrak{p} \subsetneq \mathfrak{m}$, 与 $\dim(R) = 1$ 矛盾. 对于 (3), 取 $x_1, \dots, x_r$ 是 $\mathfrak{m}$ 的生成元, 由 (2), 则存在 n_i 使得 $x_i^{n_i} \in \pi R$. 因此, 对 $N > \sum\limits_{i=1}^{r} n_i$, 则 $(\sum\limits_{i=1}^{r} r_i x_i)^N \in \pi R$, 故 $\mathfrak{m}^N \subset \pi R$. 对于 (4), 此时 $t\mathfrak{m} \subset \mathfrak{m}^n \subset \pi R$, 故 $\frac{t}{\pi}\mathfrak{m} \subset R$, 进而是 R 的理想. 对于 (5), 只需证明 $\frac{t}{\pi}\mathfrak{m} \neq R$ 即可. 否则, $1 \in \frac{t}{\pi}\mathfrak{m}$, 进而 $\pi \in t\mathfrak{m} \subset \mathfrak{m}^n \subset \mathfrak{m}^2$, 与 $\pi \in \mathfrak{m} - \mathfrak{m}^2$ 矛盾. 对于 (6), 由 (4),(5) 我们知道 $\mathfrak{m}$ 是主理想. 由于此时 $\mathfrak{m}$ 是唯一非零素理想, 故而 π 是 $\mathfrak{m}$ 的唯一素元. 因而由第 6 次习题课的 (2.6)(4), 只需证明 R 是唯一分解环即可. 此时任取 $x \in R$, 若 $xR \not\subset \pi R$, 则 x 可逆, 故显然可以分解. 否则, 取 n, 使得 $xR \subset \pi^n R$ 且 $xR \not\subset \pi^{n+1}R$. 此时 $\pi^{-n}x \in R$ 且 $\pi^{-n}x \notin \pi R$, 进而 $\pi^{-n}x = u$ 是 R 中的可逆元, 故 $x = u\pi^n$ 可以分解为素元的乘积, 因而 R 是唯一分解整环. □

问题 (3.5): 对整环 R,请证明 下列条件等价:

(1) R 是 Dedekind 整环.

(2) R 是 Noetherian, 整闭, $\dim(R) = 1$ 的环.

证明. 由 (3.1), 则 (1) 可以推出 (2). 由 (3.4), 当 (2) 成立, 则对 R 的所有非零素理想 $\mathfrak{p}$, 都有 $R_{\mathfrak{p}}$ 是离散赋值环, 进而 R 是 Dedekind 整环. □

在下面的问题中, 你可以用到如下事实: 若 L/K 是可分扩张,A 是 K 的子环, $K = \mathrm{Frac}(A)$, 且 A 是 Dedekind 环. 记 B 是 A 在 L 中的整闭包, 则 B 是有限生成 A-代数.(该事实的证明涉及较深入的线性代数, 故而此处各位同学可以直接使用)

问题 (3.6): 对 Dedekind 整环 A, 记 $K = \mathrm{Frac}(A)$, 若 L/K 是有限可分扩张, 记 B 是 A 在 L 中的整闭包, 请证明: B 也是 Dedekind 整环. 特别地, 我们称 $\mathbb{Q}$ 的有限扩张 K 是一个数域, 则数域 K 中的所有代数整数构成一个 Dedekind 整环 $\mathcal{O}_K$.

证明. B 是 A 的整闭包, 故 B 是整闭的.B/A 是环的整扩张, 故 $\dim(B) = \dim(A) = 1$. 由问题前的叙述, 则 B 是有限生成 A-代数. 由第 7 次习题课的 (4.4), 则 B 是 Noetherian 的. □

问题 (4): 本系列问题中, 我们研究 $\mathbb{Q}$ 的二次扩张.

问题 (4.1):请证明: 若 $K/\mathbb{Q}$ 是二次扩张, 则 $K=\mathbb{Q}(\sqrt{d})$, 其中 d 是无平方因子的整数.

证明. 对二次方程 X^2+bX+c, 其根为 $\frac{-b\pm\sqrt{b^2-4ac}}{2}$, 而 $\mathbb{Q}(\frac{-b\pm\sqrt{b^2-4ac}}{2})=\mathbb{Q}(\sqrt{b^2-4ac})$. 也就是说, 存在 $r\in\mathbb{Q}$, 使得 $K=\mathbb{Q}(\sqrt{r})$. 记 $r=\frac{p}{q}$, 注意到 $q\sqrt{r}=\sqrt{pq}$, 因而 $K=\mathbb{Q}(\sqrt{pq})$. 另一方面, 对 $d\in\mathbb{Z}$, 若 $d=x^2y$, 则 $\sqrt{d}=|x|\sqrt{y}$, 故 $\mathbb{Q}(\sqrt{d})=\mathbb{Q}(\sqrt{y})$. 综上所述, 则一定能找到无平方因子的整数 d, 使得 $K=\mathbb{Q}(\sqrt{d})$. □

问题 (4.2): 对 $K=\mathbb{Q}(\sqrt{d})$, 其中 d 是无平方因子的整数, 记 $\mathcal{O}_K$ 是 $\mathbb{Z}$ 在 K 中的整闭包, 请证明:

$$\mathcal{O}_K=\begin{cases}\mathbb{Z}\left[\sqrt{d}\right] & d\not\equiv 1 \mod 4\\ \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] & d\equiv 1 \mod 4\end{cases}$$

特别地, 此时 $\mathcal{O}_K$ 是秩为 2 的自由 $\mathbb{Z}$-模.

证明. 对 $\alpha=x+y\sqrt{d}$, 其中 $x,y\in\mathbb{Q}$, 则 α 满足多项式 $f(X)=X^2-2xX+(x^2-dy^2)$. 因此 α 是 $\mathbb{Z}$ 上的整元当且仅当 $2x\in\mathbb{Z}$ 且 $x^2-dy^2\in\mathbb{Z}$. 我们首先考虑 $x\in\mathbb{Z}$ 的情形, 此时 $dy^2\in\mathbb{Z}$, 由于 d 无平方因子, 因此 $y\in\mathbb{Z}$. 当 $x\notin\mathbb{Z}$, 则 x 形如 $\frac{n}{2}$, 其中 n 是奇数. 此时 $n^2-d(2y)^2\in\mathbb{Z}$, 同理上述过程, 则 $2y\in\mathbb{Z}$. 记 $y=\frac{m}{2}$, 则 $\frac{n^2-dm^2}{4}\in\mathbb{Z}$, 进而 $n^2\equiv dm^2 \mod 4$. 当 $d\equiv 1 \mod 4$, 则 m 也是奇数, 因此 $\alpha\in\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$——容易验证此时 $\frac{1+\sqrt{d}}{2}$ 确实是整元, 因此 $\mathcal{O}_K=\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$. 而当 $d\not\equiv 1 \mod 4$, 则 $1\equiv dm^2 \mod 4$ 无解, 因此只能有 $x\in\mathbb{Z}$, 进而 $y\in\mathbb{Z}$, 故 $\mathcal{O}_K=\mathbb{Z}\left[\sqrt{d}\right]$. □

问题 (4.3):请按照以下步骤 求出 $p\mathcal{O}_K$ 如何分解为 $\mathcal{O}_K$ 中素理想的乘积.

(1) $|\mathcal{O}_K/p\mathcal{O}_K|=p^2$.

(2) $\mathfrak{p}$ 出现在 $p\mathcal{O}_K$ 的素理想分解中当且仅当 $\mathfrak{p}\cap\mathbb{Z}=p\mathbb{Z}$, 此时 $\mathcal{O}_K/\mathfrak{p}$ 是有限域 $\mathbb{F}_p$ 的有限扩张.

在下面你可以直接用到如下事实: 若 $\mathfrak{p}$ 是 $\mathcal{O}_K$ 的素理想, 则 $\mathfrak{p}^k/\mathfrak{p}^{k+1}$ 是维数 1 的 $\mathcal{O}_K/\mathfrak{p}$-线性空间.(该命题的证明要么涉及相对复杂的初等技巧, 要么需要引入模的局部化的概念, 故而此处略去)

(3) 若 $\mathfrak{p}$ 是 $\mathcal{O}_K$ 的素理想, 则 $[\mathcal{O}_K:\mathfrak{p}^n]=[\mathcal{O}_K:\mathfrak{p}]^n$.

(4) 若 $p\mathcal{O}_K=\mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\ldots\mathfrak{p}_g^{e_g}$, 记有限域 $\mathcal{O}_K/\mathfrak{p}_k$ 的元素个数为 p^{f_k}, 则 $\sum_{k=1}^{g}e_kf_k=2$(**提示**: 利用中国剩余定理).

证明. 由 (4.2), 我们知道 $\mathcal{O}_K$ 是秩为 2 的 $\mathbb{Z}$-自由模, 因而 $\mathcal{O}_K\cong\mathbb{Z}^2$, 故 $\mathcal{O}_K/p\mathcal{O}_K\cong(\mathbb{Z}/p\mathbb{Z})^2$, 进而 $|\mathcal{O}_K/p\mathcal{O}_K|=p^2$. 对于 (2), 前半部分是显然的, 而由 $\mathcal{O}_K$ 是有限生成 $\mathbb{Z}$-模, 则 $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}\to\mathcal{O}_K/\mathfrak{p}$ 是有限生成整扩张, 进而是有限扩张. 对于 (3), 其由命题

前的事实容易得到. 对于 (4), 由中国剩余定理, 则 $p^2 = [\mathcal{O}_K : p\mathcal{O}_K] = \prod_{i=1}^{g} [\mathcal{O}_K : \mathfrak{p}_i^{e_i}] = \prod_{i=1}^{g} [\mathcal{O}_K : \mathfrak{p}_i]^{e_i} = p^{\sum_{k=1}^{g} e_k f_k}$, 故得证. $\square$

问题 (4.4): 固定 $K = \mathbb{Q}(\sqrt{3})$, $\mathcal{O}_K = \mathbb{Z}\left[\sqrt{3}\right]$,请证明 下列事实:

(1) 对 $x + y\sqrt{3} \in \mathcal{O}_K$, 记 $N(x + y\sqrt{3}) = |x^2 - 3y^2|$, 则 N 是乘性的. 即对 $\alpha, \beta \in \mathcal{O}_K$, 有 $N(\alpha\beta) = N(\alpha)N(\beta)$. 进一步地, $u \in \mathcal{O}_K$ 是单位当且仅当 $N(u) = 1$.

(2) $\mathcal{O}_K$ 关于 N 构成一个欧几里得整环, 进而 $\mathcal{O}_K$ 是主理想整环.

(3) 若 $(x + y\sqrt{3})$ 是 $\mathcal{O}_K$ 的非零素理想, 则 $(x - y\sqrt{3})$ 也是 $\mathcal{O}_K$ 的非零素理想.

(4) 若 $(x + y\sqrt{3})$ 是 $\mathcal{O}_K$ 的素理想, 且 $x, y \neq 0$, 则 $|x^2 - 3y^2| = p^n$, 其中 p 是素数, 且 $(x + y\sqrt{3})$ 和 $(x - y\sqrt{3})$ 都出现 $p\mathcal{O}_K$ 的素理想分解中.

(5) 当 $p = 2$ 或 3, 则 $p\mathcal{O}_K = \mathfrak{p}^2$, 其中 $\mathfrak{p}$ 是 $\mathcal{O}_K$ 的素理想.(**提示**: $\frac{1+\sqrt{3}}{1-\sqrt{3}}$ 是 $\mathcal{O}_K$ 中的单位)

(6) 当 $p \neq 2, 3$, 若素理想 $\mathfrak{p} = (x + y\sqrt{3})$ 出现在 $p\mathcal{O}_K$ 的分解中, 则要么 $\mathfrak{p} = p\mathcal{O}_K$, 要么 $(x + y\sqrt{3})$ 和 $(x - y\sqrt{3})$ 是不同的素理想. 进而 $p\mathcal{O}_K$ 要么是 $\mathcal{O}_K$ 中的素理想, 要么分解为 $\mathcal{O}_K$ 中两个互不相同的素理想的乘积.

(7) 在 (6) 中, 若 $(x + y\sqrt{3}) = p\mathcal{O}_K$, 则 $N(x + y\sqrt{3}) = p^2$. 若 $(x + y\sqrt{3})(x - y\sqrt{3}) = p\mathcal{O}_K$, 则 $N(x + y\sqrt{3}) = p$.

(8) 对素数 p, 当 $p > 3$, 则丢番图方程 $X^2 - 3Y^2 = \pm p$ 存在整数解当且仅当 p 在 $\mathcal{O}_K$ 中分解为两个互不相同的素理想的乘积.

证明. 对于 (1), 注意到 $N(x + y\sqrt{3}) = |(x + y\sqrt{3})(x - y\sqrt{3})|$, 证明是容易的.

对于 (2), 只需证明 $\mathbb{Z}\left[\sqrt{3}\right]$ 上存在带余除法. 对于 $\alpha = a + b\sqrt{3}$, $\beta = c + d\sqrt{3}$, 此时 $\frac{\alpha}{\beta} = \frac{(ac-3bd)+(bc-ad)\sqrt{3}}{c^2-3d^2} = r + s\sqrt{3}$, 其中 $r, s \in \mathbb{Q}$. 我们取 e, f 分别是距离 r, s 最近的整数, 则 $|e - r| \leq \frac{1}{2}, |f - s| \leq \frac{1}{2}$, 记 $\gamma = e + f\sqrt{3}$, 则 $N(\frac{\alpha}{\beta} - \gamma) = ||e - r|^2 - 3|f - s|^2|$. 注意到 $||a| - |b|| \leq \max(|a|, |b|)$, 故 $N(\frac{\alpha}{\beta} - \gamma) \leq \frac{3}{4}$, 进而 $N(\alpha - \gamma\beta) \leq \frac{3}{4}N(\beta)$, 因而带余除法存在.

对于 (3), 若 $x - y\sqrt{3}$ 不是非零素理想, 则存在 $(x - y\sqrt{3}) \subsetneq (z + w\sqrt{3})$, 其中 $1 \notin (z + w\sqrt{3})$ 是极大理想, 此时 $(x + y\sqrt{3}) \subsetneq (z - w\sqrt{3})$ 且 $1 \notin (z - w\sqrt{3})$, 与 $(x + y\sqrt{3})$ 极大矛盾.

对于 (4), 此时 $(x + y\sqrt{3}) \cap \mathbb{Z} = p\mathbb{Z}$ 是 $\mathbb{Z}$ 的非零素理想. 注意到 $(x + y\sqrt{3})(x - y\sqrt{3}) \in (x + y\sqrt{3})$, 故 $N(x + y\sqrt{3}) \in p\mathbb{Z}$. 反之, 若 q 是 $N(x + y\sqrt{3})$ 的其它素因数, 记 $(z + w\sqrt{3})$ 是 $q\mathcal{O}_K$ 分解中的素理想, 则 $(x + y\sqrt{3})(x - y\sqrt{3}) \in (z + w\sqrt{3})$, 由 $(z + w\sqrt{3})$ 是素理想, 则 $x + y\sqrt{3} \in (z + w\sqrt{3})$ 或 $x - y\sqrt{3} \in (z + w\sqrt{3})$, 然而这是不可能的.

对于 (5), 当 $p = 3$, 则 $p\mathcal{O}_K = (\sqrt{3})^2$. 由 (4.3)(4) 则 $(\sqrt{3})$ 是 $\mathcal{O}_K$ 的素理想. 当 $p = 2$, 则 $p\mathcal{O}_K = (1+\sqrt{3})(1-\sqrt{3})$, 注意到 $\frac{1+\sqrt{3}}{1-\sqrt{3}} = \frac{4+2\sqrt{3}}{-2} = -(2+\sqrt{3}) \in \mathcal{O}_K$, 故 $(1+\sqrt{3}) \subset (1-\sqrt{3})$. 同理 $(1-\sqrt{3}) \subset (1+\sqrt{3})$, 进而 $(1-\sqrt{3}) = (1+\sqrt{3})$. 此时与 $p = 3$ 的情形同理, 我们知道 $(1+\sqrt{3})$ 是 $\mathcal{O}_K$ 的素理想.

对于 (6), 若 $(x+y\sqrt{3}) \neq (x-y\sqrt{3})$, 则 $p\mathcal{O}_K$ 分解为两个不同的素理想的乘积. 若 $\mathfrak{p} = (x+y\sqrt{3}) = (x-y\sqrt{3})$, 则 $2x, 2y\sqrt{3} \in \mathfrak{p}$. 由 $p \neq 2, 3$, 则 $2, \sqrt{3} \notin \mathfrak{p}$, 故 $x, y \in \mathfrak{p}$, 进而 $x, y \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$, 即 x, y 都被 p 整除, 进而 $(x+y\sqrt{3}) \subset p\mathcal{O}_K$, 故 $\mathfrak{p} = p\mathcal{O}_K$, 即 $p\mathcal{O}_K$ 是 $\mathcal{O}_K$ 的素理想.

对于 (7), 当 $(x+y\sqrt{3}) = p\mathcal{O}_K$, 则存在单位 $u \in \mathcal{O}_K$, 使得 $u(x+y\sqrt{3}) = p$, 进而 $N(x+y\sqrt{3}) = N(u)N(x+y\sqrt{3}) = N(p) = p^2$. 当 $(x+y\sqrt{3})(x-y\sqrt{3}) = p\mathcal{O}_K$, 则存在单位 $u \in \mathcal{O}_K$, 使得 $u(x+y\sqrt{3})(x-y\sqrt{3}) = p$, 进而 $u(x^2-3y^2) = p$. 此时只能有 $u \in \mathbb{Z}$, 进而 $u = \pm 1$. 此时, 无论如何都有 $|x^2-3y^2| = N(x+3\sqrt{3}) = p$.

对于 (8), 当 p 在 $\mathcal{O}_K$ 中分解为两个互不相同的素理想的乘积, 则由 (7) 知道 $X^2 - 3Y^2 = \pm p$ 有解. 反之, 若 $x^2 - 3y^2 = \pm p$, 则 $p\mathcal{O}_K \subset (x+y\sqrt{3})$. 若 $p\mathcal{O}_K = (x+y\sqrt{3})$, 由 (7), 则 $N(x+y\sqrt{3}) = p^2$ 矛盾, 因此 $p\mathcal{O}_K = (x+y\sqrt{3})(x-y\sqrt{3})$ 分解为两个不同的素理想的乘积 (这两个素理想不同是由 (6) 保证的). □

问题 (4.5): 同理 (4.4),请证明: 对素数 p, 当 $p > 2$, 则丢番图方程 $X^2 + 2Y^2 = p$ 存在整数解当且仅当 p 在 $\mathbb{Z}\left[\sqrt{-2}\right]$ 中分解为两个互不相同的素理想的乘积.

证明. 略. □