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 $I = \mathrm{Rad}(R) = \bigcap_{\mathfrak{m}是R的极大理想} \mathfrak{m}$ 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 $J_0 \supsetneq J$. 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 $\mathfrak{m}I \subsetneq I$, 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 $\mathfrak{m}I \subset J \subsetneq I$, 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 $R = \prod_{\mathfrak{m}是极大理想} R_{\mathfrak{m}}$.(**提示**: 利用 Nakayama 引理.)

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.

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 $\mathrm{Inv}(H) = \{x \in L : \sigma(x) = x对所有\sigma \in H成立\}$. 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,请证明: 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.

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,请证明: $K/\mathbb{Q}$ 是 Galois 扩张, 且存在 $0 \le r \le n$, 使得 $\mathrm{Gal}(K/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^r$.

问题 (2.3): 对 $(m_1, \ldots, m_n) \in \{0, 1\}^n$,请证明:$\mathbb{Q}(\sqrt{p_1^{m_1}p_2^{m_2}\ldots p_n^{m_n}})$ 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.

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

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

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):请证明: 若 R 是 Dedekind 整环, 则 R 是 Noetherian 的, 整闭的, 且 $\dim(R) = 1$.

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 $\mathfrak{m}$, 请证明: 对 $r \in \mathfrak{m}$, 则 $1 + r$ 是 R 中的可逆元.

问题 (3.3): 请证明: 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.

问题 (3.4):请根据以下步骤证明, 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 $S = \{1, x, x^2, \ldots\}$ 以及局部化 $S^{-1}R$ 中包含 $\pi S^{-1}R$ 的极大理想)

(3) 存在 $n \in \mathbb{Z}_{\ge 0}$, 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)

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.

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 $\mathcal{O}_K$.

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.

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.

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

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**: $\frac{1\pm\sqrt{3}}{1-\sqrt{3}}$ 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.

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.