问题 (1): 本系列问题是为了期中考试复习而设置的.
问题 (1.1):请你求出 二面体群 D_{2n} 中每个元素的阶数.

证明. 由定义, r 是 n 阶的, 而 s 是 2 阶的. 对于 r^a, 记 a, n 的最大公因数为 d, 由 Bezout 定理, 存在 $s, t \in \mathbb{Z}$, 使得 $sa + tn = d$, 进而 $(r^a)^s = r^{as+tn} = r^d$, 故 $\langle r^a \rangle = \langle r^d \rangle$, 即 r^a 和 r^d 有相同的阶数, 进而只需考虑 d 整除 n 的情形, 此时 r^d 的阶为 $\frac{n}{d}$. 对于 $r^b s$, 注意到 $r^b s r^b s = r^b (s r s^{-1})^b = r^b r^{-b} = 1$, 故 $r^b s$ 都是 2 阶的. □

问题 (1.2):请证明 关于群的可解性我们有如下事实成立:

(1) 若 G 是可解群, 则 G 的子群和商群都是可解的.

(2) 反之, 对群 G 及正规子群 N, 若 N 和 G/N 都是可解的, 则 G 也是可解的.

(3) 群 G 是可解群当且仅当 G 的 Jordan-Hölder 因子都是交换群.

证明. 对于 (1), 对 G 的子群 H, 记 $\mathcal{D}G = \mathcal{D}^1 G = [G, G]$,$\mathcal{D}^{n+1} G = [\mathcal{D}^n G, \mathcal{D}^n G]$, 则可以归纳地证明 $\mathcal{D}^n H \subset \mathcal{D}^n G$, 进而当 G 可解, 则 H 可解. 对于商群 G/N, 记 $p : G \to G/N$ 是投影, 注意到 $[p(x), p(y)] = p([x, y])$, 故可以归纳地证明 $p(\mathcal{D}^n G) = \mathcal{D}^n (G/N)$, 因此 G/N 也是可解的. 对于 (2), 记 $p : G \to G/N$ 是商映射, 由 $p(\mathcal{D}^n G) = \mathcal{D}^n (G/N)$, 故 N 足够大时 $\mathcal{D}^N G \subset N$, 进而 $\mathcal{D}^{N+k} G \subset \mathcal{D}^k N$, 故 G 可解. 对于 (3), 注意到 $\mathcal{D}^k G / \mathcal{D}^{k+1} G$ 是交换群, 故可解群的 Jordan-Hölder 因子是交换群. 反之, 若 G 有合成列 $0 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$, 使得 G_k / G_{k+1} 是交换单群. 由 G/G_{n-1} 交换, 则 $\mathcal{D}G \subset G_{n-1}$, 进而可以归纳地证明 $\mathcal{D}^k G \subset G_{n-k}$ 对所有 k 成立. 特别地,$\mathcal{D}^n G \subset G_0 = 0$, 故 $\mathcal{D}^n G = 0$, 即 G 是可解的. □

问题 (1.3): 对正整数 $n \in \mathbb{Z}_{\geq 1}$, 考虑环 $\mathbb{Z}/n\mathbb{Z}$,请证明: $\mathbb{Z}/n\mathbb{Z}$ 是整环当且仅当 n 是素数.

证明. 对 $s \mod n, t \mod n \in \mathbb{Z}/n\mathbb{Z}$, 则 $st \equiv 0 \mod n$ 当且仅当 n 整除 st. 若 n 是素数, 则 n 整除 s 或整除 t, 进而 $s \equiv 0 \mod n$ 或 $t \equiv 0 \mod n$, 故 $\mathbb{Z}/n\mathbb{Z}$ 是整环. 反之, 当 n 不是素数, 记 $n = ab$, 其中 $0 < a, b < n$, 则 $a, b \not\equiv 0 \mod n$, 而 $ab \equiv 0 \mod n$, 故 $a \mod n$ 和 $b \mod n$ 都是零因子. □

问题 (2): 本系列问题中, 我们考虑集合 X 的幂集 $\mathcal{P}(X)$ 构成的环.
问题 (2.1): 对于集合 X, 我们记 $\mathcal{P}(X)$ 是 X 的所有子集构成的集合,请证明: 若在 $\mathcal{P}(X)$ 中定义加法 $E + F = (E - F) \cup (F - E)$ 以及乘法 $E \times F = E \cap F$, 则 $\mathcal{P}(X)$ 构成一个含幺环.(这里的 $E - F = \{x \in X : x \in E 且 x \notin F\}$)
提示: 事实上, 我们可以将 $\mathcal{P}(X)$ 看作所有从 X 到 $\{0, 1\}$ 的映射的集合. 对于 $E \in \mathcal{P}(X)$, 我们将其映射为 E 的特征函数 χ_E, 这里:$\chi_E(x) = \begin{cases} 1 & 若 x \in E \\ 0 & 若 x \notin E \end{cases}$. 如果我们将 $\{0, 1\}$ 看作 $\mathbb{F}_2$ 的话, 则从 X 到 $\mathbb{F}_2$ 的映射存在自然的加法和乘法:$(f + g)(x) = f(x) + g(x)$,

$(fg)(x)=f(x)g(x)$. 由 $\mathbb{F}_2$ 是域, 则这里的加法和乘法赋予了 $\mathcal{P}(X)$ 含幺环结构 (幺元是 X, 零元是 $\emptyset$). 因此只需验证 $\chi_E+\chi_F=\chi_{E+F}$, $\chi_E\chi_F=\chi_{E\times F}$ 即可.

证明. 如提示所言, 略. $\square$

问题 (2.2): 对于 $\mathcal{P}(X)$ 的子集 A,请证明:A 构成 $\mathcal{P}(X)$ 的含幺子环当且仅当 A 满足如下的性质:

(1) $\emptyset\in A$.

(2) 若 $E,F\in A$, 则 $E\cup F\in A$.

(3) 若 $E\in A$, 则 $X-E\in A$.

证明. 当 A 是 $\mathcal{P}(X)$ 的含幺子环, 则 $X\in A$, 进而任取 $E\in A$, 有 $E+X=(X-E)\in A$. 特别地, $\emptyset=X-X\in A$. 对 $E,F\in A$, 则 $E\cup F=(E+F)\cup(E\cap F)$, 注意到 $(E+F)\cap(E\cap F)=\emptyset$, 故 $(E+F)+(E\times F)=(E+F)+(E\cap F)=E\cup F$, 故 $E\cup F\in A$. 因此 A 满足以上的 (1), (2), (3).
反之, 若 A 满足以上的 (1), (2), (3). 对 $E,F\in A$, 注意到 $E\cap F=X-(X-E)\cup(X-F)$, 故 $E\cap F\in A$. 进而, 注意到 $E+F=(E\cap(X-E\cap F))\cup(F\cap(X-E\cap F))$, 故 $E+F\in A$. 进而 A 构成 $\mathcal{P}(X)$ 的子环, 且由 $X=X-\emptyset\in A$, 故 A 是含幺的. $\square$

说明: 在测度论中, 我们称满足上述 (1), (2), (3) 的子集族为一个环. 该问题说明, 测度论中定义的环确实构成一个环.
问题 (2.3): 对于集合间的映射 $f:X\to Y$,请证明: $\mathcal{P}(X)\to\mathcal{P}(Y), E\mapsto f(E)$ 不一定是环同态.

证明. 很容易就能找到例子, 使得 $f(E\cap F)\neq f(E)\cap f(F)$. 譬如说, 考虑 $X=\{0,1,2\}$, $E=\{0,1\}$, $F=\{0,2\}$, 令 $f(0)=0$, $f(1)=1$, $f(2)=1$, 则 $f(E\cap F)=\{0\}$, 而 $f(E)\cap f(F)=\{0,1\}$. $\square$

问题 (2.4): 在 (2.3) 的条件下,请证明: $\mathcal{P}(Y)\to\mathcal{P}(X), F\mapsto f^{-1}(E)$ 是环同态.

证明. 不难验证 $f^{-1}(E\cup F)=f^{-1}(E)\cup f^{-1}(F)$, $f^{-1}(E\cap F)=f^{-1}(E)\cap f^{-1}(F)$, $f^{-1}(E-F)=f^{-1}(E)-f^{-1}(F)$, 故得证. $\square$

问题 (2.5): 对环 R, 若 $f^2=f$ 对所有 $f\in R$ 都成立, 则称 f 是一个 Boolean 环.请证明如下事实:

(1) 对集合 X, $\mathcal{P}(X)$ 是 Boolean 环.

(2) 若 R 是 Boolean 环, 则任取 $f\in R$, 都有 $f+f=0$.

(3) 若 R 是 Boolean 环, 则 R 是交换的.

证明. 对 $E \in \mathcal{P}(X)$, 则 $E^2 = E \times E = E \cap E = E$, 故 $\mathcal{P}(X)$ 是 Boolean 环. 对 (2), 注意到 $2f = (2f)^2 = 4f^2 = 4f$, 故 $2f = 0$, 即 $f + f = 0$. 对 (3), 注意到 $(f+g)^2 = f^2 + fg + gf + g^2 = f + g + fg + gf = (f+g)$, 故 $fg + gf = 0$. 由 (2), 则 $gf = -gf$, 故 $fg = gf$, 进而 R 是交换的. □

补充说明: 可以证明, 若 R 是 Boolean 环, 则 R 同构于某个 $\mathcal{P}(X)$ 的子代数. 如果你熟悉交换代数的话, 上述嵌入是这样构造的: 令 $X = \operatorname{Spec}(R)$, 考虑 $R \to \mathcal{P}(X), f \mapsto D(f)$.

问题 (3): 本系列问题中, 我们研究交换环 R 上的形式幂级数环 $R[[X]]$. 在本系列问题中, 我们固定 R 是一个 (含幺) 交换环.

问题 (3.1): 我们记 $R[[X]]$ 是全体映射 $\mathbb{Z}_{\geq 0} \to R$ 的映射, 当 $a_n = f(n)$, 则我们用符号 $\sum\limits_{n=0}^{\infty} a_n X^n$ 表示 f. 在 $R[[X]]$ 上, 我们定义加法 $\sum\limits_{n=0}^{\infty} a_n X^n + \sum\limits_{n=0}^{\infty} b_n X^n = \sum\limits_{n=0}^{\infty} (a_n + b_n) X^n$ 和乘法 $(\sum\limits_{n=0}^{\infty} a_n X^n)(\sum\limits_{n=0}^{\infty} b_n X^n) = \sum\limits_{n=0}^{\infty} (\sum\limits_{k=0}^{n} a_k b_{n-k}) X^n$.请证明:$R[[X]]$ 构成一个含幺交换环.

证明. 略. □

补充说明: 事实上, 多项式环的严格定义就是通过类似 (3.1) 的方式构造的. 即对于交换环 R, 我们定义:

$$R[X] = \left\{ f\text{是映射}\mathbb{Z}_{\geq 0} \to R : \text{只有有限多个}f(n)\text{非零} \right\},$$

此时, 当 $a_i = f(i)$, 且 n 是使得 $f(n) \neq 0$ 的最大正整数, 则我们用符号 $f(X) = \sum\limits_{i=0}^{n} a_i X^i$ 表示 f, 并记 $\deg(f)$ 为 n. 通过这种方式定义的多项式环满足多项式环的泛性质: 对任意交换环 S 和环同态 $\phi : R \to S$, 任取 $s \in S$, 存在唯一环同态 $\widetilde{\phi} : R[X] \to S$, 满足 $\widetilde{\phi}(X) = s$ 且 $\widetilde{\phi}|_R = \phi$(即多项式环是 R-代数范畴中的自由对象) ——因此这种对多项式环的定义是合理的.

问题 (3.2):请证明: 多项式环 $R[X]$ 在自然的意义下构成 $R[[X]]$ 的子环.

证明. 略. □

问题 (3.3): 我们记 $I_k = \left\{ \sum\limits_{n=0}^{\infty} a_n X^n : \text{当}n < k\text{时}a_n = 0 \right\}$, 请证明: 对所有 $k \in \mathbb{Z}_{\geq 1}$, 都有 I_k 是 $R[[X]]$ 的理想.

证明. 直接验证即可. □

问题 (3.4): 对 $f(X) = \sum\limits_{n=0}^{\infty} a_n X^n \in R[[X]]$,请证明: $f(X)$ 在 $R[[X]]$ 中可逆当且仅当 a_0 在 R 中可逆.

提示: 一个最简单的例子是 $(1-X)^{-1} = \sum\limits_{n=0}^{\infty} X^n$. 当 a_0 可逆, 则可以归纳地构造 $b_0, b_1, \ldots, b_n$, 使得 $f(X)(\sum\limits_{k=0}^{n} b_n X^n) = 1 + X^{n+1} h(X)$, 进而 $f(X)(\sum\limits_{k=0}^{\infty} b_n X^n) = 1$.

证明. 当 $f(X)$ 可逆, 则存在 $g(X)$, 使得 $f(X)g(X) = 1$. 记 $g(X) = \sum_{n=0}^{\infty} b_0 X^n$, 考虑 $f(X)g(X) = 1$ 的常数项, 则 $a_0 b_0 = 1$, 故 a_0 可逆. 反之, 当 a_0 可逆, 我们归纳地构造一列 $b_0, b_1, \ldots$, 使得 $f(X)(\sum_{n=0}^{N} b_n X^n) - 1 = X^{N+1} h_N(X)$. 令 $b_0 = a_0^{-1}$, 则 $b_0 f(X) - 1$ 形如 $X h_0(X)$. 若已经构造出了 $b_0, b_1, \ldots, b_{N-1}$, 则 $f(X)(\sum_{n=0}^{N-1} b_n X^n)$ 的第 N 次项为 $\sum_{n=0}^{N-1} b_n a_{N-n}$. 记 $A_N = \sum_{n=0}^{N-1} b_n a_{N-n}$, 则 $f(X)(\sum_{n=0}^{N-1} b_n X^n - \frac{A_N}{a_0} X^N)$ 的 N 次项为 0, 故令 $b_N = -\frac{A_n}{a_0}$ 即可. 现在, 令 $g(X) = \sum_{n=0}^{\infty} b_n X^n$, 则由上述 b_n 的构造, 一定有 $f(X)g(X) = 1$, 故而 $f(X)$ 可逆. □

问题 (3.5): 若 K 是域, <u>请证明</u>: 若 I 是 $K[[X]]$ 的非平凡理想, 则存在 $k \in \mathbb{Z}_{\geq 0}$, 使得 $I = I_k$.
提示: 对 $f(X) = \sum_{n=0}^{\infty} a_n X^n$, 记 N 是使得 $a_N \neq 0$ 的最小正整数, 则 $f(X) = X^N f_0(X)$, 其中 $f_0(X) = \sum_{n=0}^{\infty} a_{n+N} X^n$. 由 (3.4), 则 $f_0(X)$ 可逆.

证明. 此时, 任取 $f(X) \in K[[X]]$, 记 $f(X)$ 的最低次项为 k, 则 $f(X) = X^k f_0(X)$, 其中 $f_0(X)$ 的常数项非零, 进而 $f_0(X)$ 可逆, 故 $f(X) \in I_k$. 因此, 若 I 是 $K[[X]]$ 的理想, 若 $I \neq 0$, 则存在某个 $k \geq 0$, 使得 $X^k \in I$. 我们记 k 是使得 $X^k \in I$ 的最小正整数. 注意到 I_k 被 X^k 生成, 故 $I_k \subset I$. 反之, 任取 $f \in I$, 记 $f(X) = X^n f_0(X)$, 由 k 的最小性, 则 $n \geq k$, 进而 $f \in I_k$, 故 $I = I_k$. □

问题 (4): 本系列问题中, 我们将研究 $\mathrm{M}_n(R)$ 的理想. 为了避免不必要的麻烦, 在本系列问题中, 我们规定 R 是一个 (含幺) 交换环, 且 R 中有足够数量的元素.
问题 (4.1):<u>请证明</u>:$\mathrm{M}_n(R)$ 对于矩阵的加法和乘法构成一个 (含幺) 环, 且在 $n \geq 2$ 时,$\mathrm{M}_n(R)$ 是非交换的.

证明. $\mathrm{M}_n(R)$ 构成环的验证是平凡的. 非交换性可参考第 1 次习题课的 (1.2). □

问题 (4.2): 若 I 是 R 的理想,<u>请证明</u>:$\mathrm{M}_n(R) \to \mathrm{M}_n(R/I), (a_{ij}) \mapsto (a_{ij} \mod I)$ 是良定的环同态, 进而其核 $\mathrm{M}_n(I)$ 构成 $\mathrm{M}_n(R)$ 的理想.

证明. 直接验证即可. □

问题 (4.3): 若 J 是 $\mathrm{M}_n(R)$ 的 (双边) 理想,<u>请证明</u>:

$$I = \left\{ a \in R : 存在(a_{ij}) \in J以及1 \leq i, j \leq n使得a = a_{ij} \right\}$$

构成 R 的理想.

提示: 对 $A=(a_{ij}),B=(b_{ij})$, 记 E_{ij} 是只有 (i,j)-元为 1, 其余元为 0 的矩阵. 则 $a_{ij}E_{ij}=E_{ii}AE_{jj},b_{kl}E_{kl}=E_{kk}BE_{ll}$, 进而 $(a_{ij}+b_{kl})E_{ij}=a_{ij}E_{ij}+E_{ik}(b_{kl}E_{kl})E_{lj}$, 因此 I 对加法封闭.

证明. 由提示容易得到. □

问题 (4.4): 在 (2.3) 的条件下,请证明: $J=\mathrm{M}_n(I)$.
提示: 对 $A=(a_{ij})\in\mathrm{M}_n(I)$, 则存在 $A_{ij}\in J$, 使得 A_{ij} 的 (k_{ij},l_{ij})-元是 a_{ij}, 进而 $A=\sum\limits_{i,j}E_{i,k_{ij}}A_{ij}E_{l_{ij},j}$.

证明. 由提示容易得到. □

问题 (4.5): 对含幺交换环 R,请证明: 若 I 是 R 的的非平凡理想, 则 R/I 是域.

证明. 对只需证明 R/I 的非零元都可逆. 对 $x\in R-I$, 考虑 $I+Rx$, 则 $I+Rx$ 是 R 的理想. 由 I 的极大性, 则 $I+Rx=R$, 进而存在 $y\in R$, 使得 $xy\equiv 1 \mod I$, 故 x 在 R/I 中可逆. □

问题 (4.6):请证明: 当 $n\geq 2$, 若 J 是 $\mathrm{M}_n(R)$ 的极大的非平凡 (双边) 理想, 则 $\mathrm{M}_n(R)/J$ 不是除环, 即 $\mathrm{M}_n(R)/J$ 中并非所有非零元都可逆.

证明. 由 (4.4), 则 $J=\mathrm{M}_n(I)$, 其中 I 是 R 种极大的非平凡理想. 由 (4.5), 记 R/I 是域 K, 则由 (4.2), 我们知道 $\mathrm{M}_n(I)/J=\mathrm{M}_n(K)$, 而显然 $\mathrm{M}_n(K)$ 中存在不可逆的非零元, 譬如 $\begin{pmatrix}1&0\\0&0\end{pmatrix}$. □

问题 (5): 本系列问题中, 我们将研究多项式环在置换群作用下的不变量.
问题 (5.1): 对于群 G 和环 R, 若群 G 在集合 R 上有作用, 使得对任意的 $g\in G$, 都有 $r\mapsto gr$ 是 R 的环自同态, 则我们称这个作用是群 G 在环 R 上的一个作用. 我们记:

$$R^G=\left\{r\in R: r=gr\text{对所有}g\in G\text{成立}\right\},$$

请证明: 若群 G 在环 R 上有作用, 则 R^G 是 R 的子环.

证明. 略. □

问题 (5.2): 对交换环 A, 记 $R=A[X_1,\ldots,X_n]$ 是 R 上的 n-元多项式环.请证明: 存在唯一置换群 S_n 在环 R 上的作用, 满足:$\sigma(X_i)=X_{\sigma(i)}$. 我们称 $f(X)\in R^{S_n}$ 为 R 中的对称多项式.

证明. 略. □

问题 (5.3): 我们定义:

$$
\begin{aligned}
e_1(X_1,\dots,X_n) &= \sum_{1\le i\le n} X_i \\
e_2(X_1,\dots,X_n) &= \sum_{1\le i<j\le n} X_iX_j \\
e_3(X_1,\dots,X_n) &= \sum_{1\le i<j<k\le n} X_iX_jX_k \\
&\cdots\cdots \\
e_n(X_1,\dots,X_n) &= X_1X_2\dots X_n
\end{aligned}
$$

请证明:$e_1,e_2,\dots,e_n\in R^{S_n}$, 我们称 $e_1,\dots,e_n$ 为 R 中的初等对称多项式..

证明. 略. $\square$

问题 (5.4): 对 $f(X)\in R$, 记 $f_l(X)$ 是 $f(X)$ 所有只包含 $X_1,\dots,X_{n-1}$ 的项构成的多项式,请证明 下列事实:

(1) 若 $f(X)\in A\left[X_1,\dots,X_n\right]^{S_n}$, 则 $f_l(X)\in A\left[X_1,\dots,X_{n-1}\right]^{S_{n-1}}$.

(2) 对 $f(X),g(X)\in R^{S_n}$, 当 $f(X),g(X)$ 不包含被 $X_1X_2\dots X_n$ 整除的项, 则 $f_l(X)=g_l(X)$ 当且仅当 $f(X)=g(X)$.

提示: 对于 (2), 只需证明若 $f_l=0$, 则 $f=0$. 若 $f\neq 0$, 则 $f(X)$ 中含有非零项 $X_1^{m_1}\dots X_n^{m_n}$. 由 $f(X)$ 没有被 $X_1\dots X_n$ 整除的项, 则 m_i 至少有一个为 0, 进而存在 $\sigma\in S_n$, 使得 $\sigma(X_1^{m_1}\dots X_n^{m_n})$ 中只含 $X_1,\dots,X_{n-1}$, 此时它是 f_l 的项, 故 $f_l\neq 0$.

证明. 对 $f(X)\in A\left[X_1,\dots,X_n\right]^{S_n}$, 考虑 $\sigma\in S_{n-1}$ 在 $f(X)$ 上的作用, 则 σ 保持 $X_1,\dots,X_{n-1}$ 构成的项, 故 $\sigma(f)_l=\sigma(f_l)$, 进而 $f_l=\sigma(f)_l=\sigma(f_l)$. 对于 (2), 显然 $f(X)=g(X)$ 时 $f_l(X)=g_l(X)$. 反之, 若 $f_l(X)=g_l(X)$, 不失一般性用 $f(X)-g(X)$ 替代 $f(X)$, 不妨设 $g(X)=0$. 此时, 若 $f(X)\neq 0$, 由 $X_1X_2\dots X_n$ 不整除 $f(X)$, 则存在 $\{1,\dots,n\}$ 的子集 $\{i_1,\dots,i_r\}$, 使得 $f(X)$ 存在非零项 $\prod_{k=1}^{r} X_{i_k}^{n_k}$. 此时, 存在 $\sigma\in S_n$, 使得 $\sigma(\{i_1,\dots,i_r\})\subset\{1,\dots,n-1\}$, 进而 $f(X)$ 的 $\prod_{k=1}^{r} X_{\sigma(i_k)}^{n_k}$ 项系数非 0, 进而 $f_l\neq 0$, 矛盾. $\square$

问题 (5.5): 利用归纳法, 请证明: $R^{S_n}=A\left[e_1,\dots,e_n\right]$, 即若 $f(X)$ 是对称多项式, 则存在 $g(X)\in A\left[X_1,\dots,X_n\right]$, 使得 $f(X)=g(e_1(X),\dots,e_n(X))$.

提示: 这里我认为要同时对变元的个数和 $f(X)$ 的次数进行归纳. 用 $X_1\dots X_n$ 进行带余除法, 则 $f(X)=g(X)+X_1\dots X_nr(X)$, 其中 $g(X)$ 满足 (5.4) 的 (2), 而 $r(X)$ 的次数严格小于 $f(X)$ 的次数. 对前者, 考虑 g_l, 使用关于变元个数的归纳. 对于后者, 使用关于多项式次数的归纳.

证明. 我们首先对 n 进行归纳, $n=1$ 时结论是显然成立的. 对 $n>1$, 我们再对 $f(X) \in R^{S_n}$ 的次数进行归纳. 当 $\deg(f)=1$ 时结论仍是显然成立的. 对 $\deg f(X)>1$, 我们记 $f(X)=X_1 \ldots X_n h(X)+r(X)$, 其中 $\deg(h(X))<\deg(f(X))$, 而 $r(X)$ 不被 $X_1 X_2 \ldots X_n$ 整除. 由归纳假设, 则 $h(X)$ 可以被初等对称多项式生成, 因此只需证明 $r(X)$ 可以被初等对称多项式生成. 考虑 $r_l(X)$, 由 (5.4) 则 $r_l(X) \in A\left[X_1, \ldots, X_{n-1}\right]^{S_{n-1}}$. 由归纳假设, 则存在 $g(X) \in A\left[X_1, \ldots, X_{n-1}\right]$, 使得:

$$r_l(X)=g(e_1(X_1, \ldots, X_{n-1}, 0), \ldots, e_{n-1}(X_1, \ldots, X_{n-1}, 0)).$$

(注意到 $e_k(X_1, \ldots, X_{n-1}, 0)$ 是 $A\left[X_1, \ldots, X_{n-1}\right]$ 中的初等对称多项式) 记 $G(X_1, \ldots, X_n)=g(e_1(X_1, \ldots, X_n), \ldots, e_{n-1}(X_1, \ldots, X_n))$, 则:

$$G_l=g(e_1(X_1, \ldots, X_{n-1}, 0), \ldots, e_{n-1}(X_1, \ldots, X_{n-1}, 0))=r_l.$$

由 (5.4), 则 $G=r$, 故 r 可被初等对称多项式生成, 故得证. □

关于问题 (5) 的补充说明: 记 $K(X_1, \ldots, X_n)$ 是域 K 上有理函数构成的域,(5.5) 说明 $K(X_1, \ldots, X_n)^{S_n}=K(e_1, \ldots, e_n)$. 注意到 $\prod_{i=1}^n(T-X_i)=T^n-e_1 T^{n-1}+\cdots+(-1)^n e_n$. 因此一般 n 次方程 $X^n+a_{n-1} X^{n-1}+\cdots+a_0$ 可以被根式解当且仅当 $X_1, \ldots, X_n$ 可以被表达为关于 $e_1, \ldots, e_n$ 的根式. 利用 Galois 理论, 这当且仅当域扩张 $K(X_1, \ldots, X_n)/K(e_1, \ldots, e_n)$ 的 Galois 群是可解的. 而 (5.5) 说明 $K(X_1, \ldots, X_n)/K(e_1, \ldots, e_n)$ 的 Galois 群恰好是 S_n, 进而 $n \geq 5$ 时一般 n 次方程没有根式解. 事实上, 当 A 是域, 则 (5.5) 可以通过 Galois 理论和一些简单的交换环论得到证明, 你可以在学期结束时回来读一读下面的证明: 记 $L=K(e_1, \ldots, e_n), M=K(X_1, \ldots, X_n)$, 则 M 是 $\prod_{i=1}^n(T-X_i)=X^n-e_1 X^{n-1}+\cdots+(-1)^n e_n$ 在 L 上的分裂域, 进而 M/L 是 Galois 扩张, 且 $\operatorname{Gal}(M/L)$ 在 $X_1, \ldots, X_n$ 上的作用给出嵌入 $\operatorname{Gal}(M/L) \rightarrow S_n$. 注意到 S_n 在 M 上有自然的作用, 且 $L \subset M^{S_n}$, 故 $S_n \subset \operatorname{Gal}(M/L)$, 则 $\operatorname{Gal}(M/L)=S_n$, 进而 $M^{S_n}=L$. 记 $R=K\left[X_1, \ldots, X_n\right], S=K\left[e_1, \ldots, e_n\right]$, 则 $M^{S_n}=\operatorname{Frac}(R^{S_n}), L=\operatorname{Frac}(S)$, 则 S, R^{S_n} 具有相同的分式域. 注意到 R^{S_n}/S 是整扩张, 而 S 是 UFD, 进而是整闭, 故 $R^{S_n}=S$.

问题 (6): 本系列问题是为熟悉分析学的人准备的, 如果你认为自己对分析学的熟练度不足, 你可以忽略本系列问题.

问题 (6.1): 若 W 是 $\mathbb{R}^n$ 中的闭集,请证明: $C_0(W)$ 对函数的逐点加法和逐点乘法构成一个交换环, 且 $C_0(W)$ 中存在幺元当且仅当 W 是紧集. 这里 $C_0(W)$ 是所有满足如下条件的函数 $f: W \rightarrow \mathbb{C}$ 的集合:

(1) f 是连续的, 即若 W 中的序列 w_n 收敛到 w, 则 $f(w_n)$ 收敛到 $f(w)$.

(2) 对所有 $\varepsilon>0$, $\{w \in W:|f(x)| \geq \varepsilon\}$ 是紧集合.

证明. 略. □

问题 (6.2): 对 $C_0(\mathbb{R}^n)$ 中的理想 I, 若对于 I 中的函数列 f_n, 当 f_n 一致收敛到 f, 便有 $f \in I$, 则我们称 I 是 $C_0(\mathbb{R}^n)$ 的一个闭理想.请证明: 对 $\mathbb{R}^n$ 的子集 S, 则 $I(S) = \{f \in C_0(\mathbb{R}^n) : f(s) = 0\text{对所有}s \in S\text{成立}\}$ 是 $C_0(\mathbb{R}^n)$ 的闭理想.

证明. 显然 $I(S)$ 是理想. 若 $I(S)$ 中序列 f_n 一致收敛到 f, 则 $f \in C_0(\mathbb{R}^n)$, 且对 $s \in S$, 由 $f_n(s)$ 逐点收敛到 $f(s)$, 则 $f(s) = 0$, 故 $f \in I(S)$. □

问题 (6.3): 对 $\mathbb{R}^n$ 的闭集 W,请证明: $C_0(\mathbb{R}^n) \to C_0(W), f \mapsto f|_W$ 诱导了环同构 $C_0(\mathbb{R}^n)/I(W) \cong C_0(W)$.

证明. 由 Tietz 扩张定理, 则 $C_0(\mathbb{R}^n) \to C_0(W)$ 是满射 (更详细的论证需要更多的分析技巧, 故此处略). 由定义, 则 $I(W) = \mathrm{Ker}(f \mapsto f|_L)$, 故得证. □

问题 (6.4): 对 $C_0(\mathbb{R}^n)$ 的理想 I,请证明:$V(I) = \{x \in \mathbb{R}^n : f(x) = 0\text{对所有}f \in I\text{成立}\}$ 是 $\mathbb{R}^n$ 中的闭集.

证明. 这是显然的. □

问题 (6.5): 对 $\mathbb{R}^n$ 的子集 S,请证明:$V(I(S)) = \overline{S}$, 这里 $\overline{S}$ 是 S 的闭包.

证明. 对 $x \notin \overline{S}$, 取 x 的邻域 U, 使得 $U \cap \overline{S} = \emptyset$. 此时, 取鼓包函数 $f_U \in C_c(\mathbb{R}^n)$ 使得 $f_U(x) = 1$ 而 $\mathrm{Supp}(f_U) \subset U$. 此时 $f_U(s) = 0$ 对所有 $s \in S$ 成立, 故 $f_U \in I(S)$, 进而 $x \notin V(I(S))$, 故 $V(I(S)) \subset \overline{S}$, 而另一个方向的包含是显然的. □

问题 (6.6): 对于 $C_0(\mathbb{R}^n)$ 的理想 I,请证明: $I(V(I))$ 是包含 I 的最小的闭理想 (即 I 在 $C_0(\mathbb{R}^n)$ 中的闭包)

证明. 对 $x \notin V(I)$, 我们首先证明存在 x 附近的鼓包函数 f_U, 使得 $f_U \in I$. 由 $x \notin V(I)$, 则存在 $g \in I$, 使得 $g(x) \neq 0$. 进而 g 在 x 附近的一个开邻域 U 上恒大于 0, 这里 $U \cap V(I) \neq \emptyset$. 此时, 对鼓包函数 f, 若 $\mathrm{Supp}(f) \subset U$, 我们定义:

$$(\frac{f}{g})(x) \begin{cases} \frac{f(x)}{g(x)} & \text{当}x \in U \\ 0 & \text{当}x \neq U \end{cases}$$

则 $\frac{f}{g} \in C_c(\mathbb{R}^n)$, 且 $f = \frac{f}{g}g \in I$. 因此, 任取 $x \in X - V(I)$, 则 I 包含 X 附近的鼓包函数. 此时, 对 $f \in I(V(I))$, 对 $\varepsilon > 0$, 记 $E_\varepsilon = \{x \in X : |f(x)| \geq \varepsilon\}$, 则 $E_\varepsilon \cap V(I) = \emptyset$. 此时任取 $x \in E_\varepsilon$, I 包含 x 附近的鼓包函数. 注意到 E_ε 是紧的, 因此 I 包含 E_ε 附近的鼓包函数. 也就是说, 存在 $f \in I$, $f \in C_c(\mathbb{R}^n)$, 使得 $0 \leq f \leq 1$, 且 $f(E_\varepsilon) = 1$. 此时我们有 $gf \in I$, 而 $\|gf - g\| \leq 2\varepsilon$, 故而 gf 一致收敛到 g, 进而 $I(V(I))$ 是包含 I 的最小闭理想. □

问题 (6.7):请证明: $I \mapsto V(I)$ 和 $S \mapsto I(S)$ 给出了 $\mathbb{R}^n$ 中的闭集与 $C_0(\mathbb{R}^n)$ 中闭理想的 1-1 对应. 特别地, 对 $C_0(\mathbb{R}^n)$ 的闭理想 I, 则 I 是极大的非平凡闭理想当且仅当 $V(I)$ 是单点集.

证明. 由 (6.5) 和 (6.6) 容易看出. $\square$

问题 (6.8): 利用上述结果,<u>请证明</u>: 对 $f \in C_0(\mathbb{R}^n)$, 则 f 可以被 $C_c(\mathbb{R}^n)$ 中的函数逼近.

证明. 不难看出 $C_c(\mathbb{R}^n)$ 是 $C_0(\mathbb{R}^n)$ 的理想, 且 $V(C_c(\mathbb{R}^n)) = \emptyset$, 故 $\overline{C_c(\mathbb{R}^n)} = C_0(\mathbb{R}^n)$. $\square$

说明: 事实上, 对一般的局部紧拓扑空间 X, 本系列问题的结论依旧对 $C_0(X)$ 成立. 进一步地, 对交换 C^* 代数 $\mathcal{A}$, 通过 Gelfand 表示, 则局部紧拓扑空间 X, 使得我们有等距同构 $\mathcal{A} \cong C_0(X)$. 因此, 本命题事实上说明, 对任意 C^* 代数 $\mathcal{A}$ 的理想 I, 都有 $\overline{I} = \bigcap_{\substack{\mathfrak{m}\text{是极大理想} \\ \mathfrak{m} \supset I}} \mathfrak{m}$——换而言之, 本系列问题给出了 Hilbert 零点定理的 C^* 代数版本.