课程名称：代数学

第二次作业

中南大學

姓名：　樊昊
学号：242131001

数学与统计学院

环论

题目 8 . 证明 $\mathbb{Z}[x]$ 的任一个主理想非极大。

引理 1. *If $f(x)$ is irreducible in $\mathbb{Z}[x]$, then only the following two possibilities exist:*

1. *$f(x)$ is a prime in $\mathbb{Z}$;*
2. *$f(x)$ is irreducible in $\mathbb{Q}[x]$.*

Proof. In the case $\deg f(x) = 0$: it turns out that it is a prime. In the case $\deg f(x) \geq 1$, we have $f(x) = cf_0(x)$, for a primitive polynomial $f_0(x)$ and $c \in \mathbb{Z}$. We assume $c \in \{\pm 1\}$ by irreducibliity. For a primitive polynomial, it is irreducible in $\mathbb{Z}[x]$ if and only if it is irreducible in $\mathbb{Q}[x]$. □

解答.[1] 我们假设 $\mathbb{Z}[x]$ 中的主理想 $\langle f(x)\rangle$ 是极大的, 则这是极大主理想, 即 $f(x)$ 是不可约元. 而不可约元只有两种: $f(x) = p \in \mathbb{Z}$ 是素数; $f(x)$ 是 $\mathbb{Q}[x]$ 中不可约多项式. 当 $f(x) = p$ 是素数, 有 $\mathbb{Z}[x]/\langle p\rangle = \mathbb{F}_p[x]$ 是整环不是域, 所以主理想非极大. 当 $f(x)$ 是 $\mathbb{Q}[x]$ 中不可约多项式, 有 $\langle f(x)\rangle \subseteq \langle f(x), p\rangle \subsetneq \mathbb{Z}[x]$ 其中 p 是素数; 所以主理想非极大. ■

更多习题

题目 13 . Show that the ideal $(3, x^3 - x^2 + 2x - 1)$ in $\mathbb{Z}[x]$ is not principal.

解答.[2] This ideal is maximal:

$$\mathbb{Z}[x]/(3, x^3 - x^2 + 2x - 1) \cong (\mathbb{F}_3[x])/(x^3 - x^2 + 2x - 1),$$

since $x^3 - x^2 + 2x - 1$ has no roots in $\mathbb{F}_3$; it is irreducible. From 解答 1, we know it is not principal. ■

题目 28 . For a commutative ring with unit, show that the intersection of prime ideals is the set of nilpotent elements.

解答.[3] Let R be a commutative ring with unit. We want to show $\bigcap \operatorname{Spec} R = \sqrt{(0)}$. Here $\sqrt{(0)}$ is the radical ideal of (0). Let $a \in \sqrt{(0)}$, then $a^n = 0$ for some $n \geq 1$. Thus $a^n \in I$ for all $I \in \operatorname{Spec} R$. Write $a^n = a^{n-1}a$. We know $a \in I$ or $a^{n-1} \in I$. If $a \in I$, then we are done; if $a^{n-1} \in I$, then write $a^{n-1} = aa^{n-2}$ when $n - 1 > 1$. Anyway, we have $a \in I$ finally. Thus $a \in I$ for all prime ideals I and $a \in \bigcap \operatorname{Spec} R$. We proved $\bigcap \operatorname{Spec} R \supseteq \sqrt{(0)}$.

Let $a \in \bigcap \operatorname{Spec} R$. Suppose, $a \notin \sqrt{(0)}$, that is $a^n \neq 0, \forall n \geq 1$. Then $S := \{a^n : n \geq 1\}$ is a multiplicative subset of R without 0. Consider the localization $R \to RS^{-1}$, where RS^{-1} is non-trivial. We have a bijection

$$\{I \in \operatorname{Spec} R : I \cap S = \varnothing\} = \operatorname{Spec}(RS^{-1}).$$

By Zorn's Lemma, RS^{-1} has a maximal ideal and hence a prime ideal. Thus $\operatorname{Spec}(RS^{-1}) \neq \varnothing$. The bijection gives an ideal $I \in \operatorname{Spec} R$ with $I \cap S = \varnothing$. Therefore, $a \notin \bigcap \operatorname{Spec} R$. ■

模论

第五章

题目 4 . 设 $\mathbb{Q}$ 为有理数域，M 和 M' 是两个左 $\mathbb{Q}$ 模. 证明：若 $\eta: M \to M'$ 是一个加法群同构，则 η 也是一个 $\mathbb{Q}$ 模同构. ($*$ 如果用实数域 $\mathbb{R}$ 替代 $\mathbb{Q}$，问这个命题是否成立？)

解答.[4] 对 $x, y \in M$,$p_1/q_1, p_2/q_2 \in \mathbb{Q}$ 有 $x/q_1, y/q_2 \in M$ 且

$$\eta(rx+sy) = \eta\Big(\sum_{i=1}^{p_1} \frac{x}{q_1} + \sum_{j=1}^{p_2} \frac{y}{q_2}\Big) = \sum_{i=1}^{p_1} \eta\Big(\frac{x}{q_1}\Big) + \sum_{j=1}^{p_2} \eta\Big(\frac{y}{q_2}\Big);$$

另一方面,

$$\eta(x) = \eta\Big(\sum_{i=1}^{q_1} \frac{x}{q_1}\Big) = \sum_{i=1}^{q_1} \eta\Big(\frac{x}{q_1}\Big) = q\eta\Big(\frac{x}{q_1}\Big) \implies \eta\Big(\frac{x}{q_1}\Big) = \frac{1}{q_1}\eta\Big(\frac{x}{q_1}\Big),$$

综上所述,

$$\eta(rx+sy) = \frac{p_1}{q_1}\eta(x) + \frac{p_2}{q_2}\eta(y).$$

此时, η 成 $\mathbb{Q}$ 模同构.

对 $\mathbb{R}$ 模, 命题不成立: 视 $\mathbb{R}$ 为 $\mathbb{Q}$ 模, 依 Zorn 引理可取一组基 $\{e_i\}_{i\in I}$. 定义 $\eta: \mathbb{R} \to \mathbb{R}, \sum_{\text{有限}} r_i e_i \mapsto \sum_{\text{有限}} r_i \lambda_i e_i$. 则 η 的矩阵形式为对角矩阵 $\operatorname{diag}(\lambda_i)_i$; 命这个对角矩阵可逆且 λ_i 不全相同, 则 η 是加法群同构, 但不是 $\mathbb{R}$ 模同构. ■

题目 19 . 将 $\mathbb{Z}/(n)$ 看作 $\mathbb{Z}$ 模，问下列模是否可写成两个非零子模的直和：

(i) $\mathbb{Z}/(p^e), p$ 为素数，$e \geq 1$;

(ii) $\mathbb{Z}/(n), n = p_1^{e_1} \cdots p_r^{e_r}, p_1, \ldots, p_r$ 为不同的素数，$e_i \geq 1, i = 1, \ldots, r$.

解答.[5] 作为 $\mathbb{Z}$ 模的直和分解, 即分解为 Abel 群的直和.

若有分解, 分析子群的阶数, 可知分解必然形如

$$\mathbb{Z}/(p^e) = \mathbb{Z}/(p^r) \oplus \mathbb{Z}/(p^s),$$

其中 $r+s=e$. 此时, 左边有 p^e 阶元, 而右边元素阶数最大为 $\max\{p^r, p^s\}$; 应当相等, 故 $r=e$ 或者 $s=e$, 于是 $\mathbb{Z}/(p^e)$ 的分解一定是平凡的.

根据中国剩余定理, 有分解

$$\mathbb{Z}/(n) = \mathbb{Z}/(p_1^{e_1}) \oplus \mathbb{Z}/(p_2^{e_2} \cdots p_r^{e_r}),$$

这里两个子模均非零. ■

题目 20 . 证明：$\mathbb{Q}$ 作为 $\mathbb{Z}$ 模，它的任一有限生成的子模是循环模. 由此证明，$\mathbb{Q}$ 不是一个自由 $\mathbb{Z}$ 模.

解答.[6] 设 $M = \langle p_1/q_1, \cdots, p_n/q_n \rangle \subseteq \mathbb{Q}$ 是有限生成子模, 其中 p_i, q_i 互素. 令 $q \coloneqq \operatorname{lcm}(q_1, \cdots, q_n)$, 则

$$M = \left\langle \frac{p_1 r_1}{q}, \cdots, \frac{p_n r_n}{q} \right\rangle, \quad r_i \coloneqq \frac{q}{q_i}.$$

可见 $M = \langle \frac{\gcd(p_1 r_1, \cdots, p_n r_n)}{q} \rangle$, 是循环模.

假设 $\mathbb{Q}$ 是自由 $\mathbb{Z}$ 模, 而前述性质表明, 它没有秩 > 1 的有限生成子模, 故只能是秩为 1 的自由模, 这不可能: 若是秩为 1 的自由 $\mathbb{Z}$ 模, 则正的部分应有最小元. ■

补充

题目 3 . 设 R 是交换环，I 为 R 的理想. M 是有限生成的 R 模，$\varphi \in \operatorname{End}_R(M)$.

(1) 如果 $M \subseteq IM$，证明：存在 $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n (a_1, \ldots, a_n \in I)$，使得

$$f(\varphi)(= \varphi^n + \varphi^{n-1} a_1 + \cdots + \operatorname{id}|_M a_n) = 0 \in \operatorname{End}_R(M)$$

(2) Nakayama 引理 (重要): R 的所有极大理想的交称为 R 的 Jacobson 根，记为 $J(R)$. 如果 $MJ(R) = M$，证明 $M = (0)$.

尝试.

(1) ...

(2) 我们证明 $\operatorname{id}|_M^M = 0$, 从而 $M = (0)$; 简记 $\operatorname{id} = \operatorname{id}|_M^M$. 由 (1), 有 $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n, (a_i \in I)$ 使得

$$f(\operatorname{id}) = \left(1 + \sum_{i=1}^n a_i\right) \operatorname{id} = 0.$$

记 $a = \sum_{i=1}^n a_i \in I$, 下证明 $1 + a$ 是 R 中可逆元: 如果不然, 则主理想 $\langle 1 + a \rangle$ 是非平凡的, 于是有某极大理想 $I_0 \supseteq \langle 1 + a \rangle$, 但是 $a \in J(R) \implies a \in I_0$, 所以 $1 = (1 + a) - a \in I_0$, 矛盾: 极大理想不是平凡理想, 不应该有 1. 综上所述, $1 + a$ 是可逆的, 故 $\operatorname{id} = 0$.

题目 5 . 证明任一 R 模都是某个自由 R 模的同态像。

解答.[8] 设有 R 模 M, 有同态

$$R^M \longrightarrow M, (\lambda_a)_{a \in M} \longmapsto \sum_{a \in M} \lambda_a a.$$

这是满同态, 因为 $\delta_a \mapsto a$, 其中 $\delta_a(a) = 1$; $\delta_a(x) = 0 (\forall x \neq a)$. ■

题目 6 . 设 $\varphi: M \to M$ 是 R 的模同态，且 $\varphi\varphi = \varphi$. 证明：

$$M = \ker\varphi \oplus \operatorname{im}\varphi.$$

解答.[9] 对 $x \in M$,

$$x = \underbrace{x - \varphi x}_{\in\ker\varphi} + \underbrace{\varphi x}_{\in\operatorname{im}\varphi}.$$

另一方面, $x \in \ker\varphi \cap \operatorname{im}\varphi \implies x = 0$; 因为 $x = \varphi y \implies 0 = \varphi x = \varphi y \implies 0 = x$. 综上所述, 分解 $M = \ker\varphi + \operatorname{im}\varphi$ 是直和分解, 即 $M = \ker\varphi \oplus \operatorname{im}\varphi$. ■

题目 10 . Determine $\operatorname{End}(\mathbb{Q}, +, 0)$.

解答.[10] It is isomorphic to the ring $\mathbb{Q}$:

$$\operatorname{End}(\mathbb{Q}, +, 0) \to \mathbb{Q},\ f \mapsto f(1). \tag{1}$$

It suffices to show the morphism is injective. Suppose $f(1) = g(1)$, then $\forall m \in \mathbb{Z}, \forall n \geq 1$,

$$f(1) = n \cdot f\left(\frac{1}{n}\right) = n \cdot g\left(\frac{1}{n}\right) = g(1);$$
$$f\left(\frac{m}{n}\right) = mf\left(\frac{1}{n}\right) = mg\left(\frac{1}{n}\right) = g\left(\frac{m}{n}\right).$$

Thus $f = g$, (1) is injective. It keeps addition, and also multiplication:

$$f\left(\frac{m}{n}\right) = \frac{m}{n}f(1) \implies (f \circ g)(1) = f(g(1)) = f(1)g(1).$$

■

域论

第七章

题目 2 . 设 K/F 为一有限扩张，$\alpha \in K$ 是 F 上一个 n 次元素，证明 $n \mid [K : F]$.

解答.[11] 有中间域 $F(\alpha)$, 于是

$$[K : F] = [K : F(\alpha)][F(\alpha) : F] = [K : F(\alpha)] \times n$$

因为 $[F(\alpha) : F] = \deg\alpha = n$. ■

题目 4 . 设 K 为 F 上域扩张. 证明：如果 $u \in K$ 是 F 上代数元且次数为奇数，则 u^2 也是 F 上奇次数代数元且 $F(u) = F(u^2)$.

解答.[12] 设 u 在 F 上的极小多项式为 $p_u(x) = x^{2n+1} + \sum_{j=0}^{2n} \lambda_j x^j$. 则

$$p(u) = 0, \quad p(x) \coloneqq \left((u^2)^n + \sum_{j=1}^{n} \lambda_{2j-1} u^{2j-2}\right)x + \sum_{j=0}^{n} \lambda_{2j} (u^2)^j \in F(u^2)[x].$$

所以, u 在 $F(u^2)$ 上的极小多项式的次数不超过 1(也就只能是 1), 故 $[F(u) : F(u^2)] = 1$, 这就是 $F(u) = F(u^2)$. 由

$$[F(u) : F] = [F(u) : F(u^2)][F(u^2) : F]$$

可知 u^2 在 F 上次数也是奇数次. ■

题目 6 . 求下列扩域的一基：

(i) $K = \mathbf{Q}(\sqrt{2}, \sqrt{3})$;

(ii) $K = \mathbf{Q}(\sqrt{3}, \sqrt{-1}, \omega)$, 其中 $\omega = \frac{1}{2}(-1 + \sqrt{-3})$.

解答.[13] 有 $K = \operatorname{span}_{\mathbb{Q}}(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$, 一组基是 $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$.

有 $K = \operatorname{span}_{\mathbb{Q}}(1, \sqrt{3}, \sqrt{-1}, \sqrt{-3})$, 一组基是 $\{1, \sqrt{3}, \sqrt{-1}, \sqrt{-3}\}$. ■

题目 10 . 确定下列多项式在有理数域上的分裂域：

(i) $f(x) = x^4 - 2$;

(ii) $f(x) = x^3 - 2x - 2$.

解答.[14]

(i) 即 $\mathbb{Q}(\sqrt[4]{2}, i)$.

(ii) 有理根只可能是 $\pm 1, \pm 2$, 计算可见没有有理根, 从而他是不可约多项式. 判别式 $\Delta = -4(-2)^3 - 27(-2)^2 = -66$ 不是 $\mathbb{Q}$ 中平方元. 所以分裂域是 $\mathbb{Q}(\alpha, \sqrt{\Delta})$, 其中 α 是 $f(x)$ 的实数根.

■

第八章

题目 2 . 证明域 F 的每个非零自同态都保持 F 内素域的元素不动. 设 P 为含于 F 内的素域，于是 $\operatorname{Aut} F = \operatorname{Gal}(F/P)$.

解答.[15] 设 $\sigma\colon F \to F$ 是非零的自同态, 则 σ 是 F 的自同构, 所以 $\sigma(1)$ 是单位元即 $\sigma(1) = 1$. 于是, σ 保持素域内的元素不动, 因为素域由 1 生成. 现在 $\operatorname{Aut} F = \operatorname{Gal}(F/P)$ 按照定义直接成立. ■

题目 4 . 确定 $\operatorname{Gal}(K/\mathbb{Q})$，其中 $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.

解答.[16] 记所求为 G. 域自同构保持多项式的根集, 所以 $\sqrt{2} \mapsto \sqrt{2}$ 或者 $\sqrt{2} \mapsto -\sqrt{2}$, 且这两种必有一种成立, 同理于 $\sqrt{3}$. 令 $\sigma(\sqrt{2}) = -\sqrt{2}, \sigma(\sqrt{3}) = \sqrt{3}$; $\tau(\sqrt{2}) = \sqrt{2}, \tau(\sqrt{3}) = -\sqrt{3}$. 可知 $G = \langle \sigma, \tau \rangle \cong (\mathbb{Z}/\langle 2 \rangle)^2$. ■

补充

题目 1 . 令 K 是有理数 $\mathbb{Q}$ 上全体代数数做成的数域，证明：K 是 $\mathbb{Q}$ 的代数扩张，但不是有限扩张。

解答.[17] 任取 $x \in K$, 由定义, 存在 $f(X) \in \mathbb{Q}[X]$ 使得 $f(x) = 0$. 于是是代数扩张. 考虑子扩张 $\mathbb{Q}(\{\sqrt[n]{2} \mid n \geq 1\})/\mathbb{Q}$. 这不是有限扩张: 注意 $\mathbb{Q}(\{\sqrt[n]{2} \mid n \geq 1\}) = \bigcup_{n \geq 1} \mathbb{Q}(\sqrt[n]{2})$, 如果这是有限扩张, 则一定有

$$\mathbb{Q}(\{\sqrt[n]{2} \mid n \geq 1\}) = \bigcup_{n \in [N]} \mathbb{Q}(\sqrt[n]{2}),$$

对某个 N 成立. 这不可能, $\sqrt[N+1]{2}$ 不在里面. 综上所述, 这个子扩张无限, 所以问题中的扩张无限. ■

更多习题

题目 1 . Let F be a field of characteristic p, a an element of F not of the form $b^p - b$, $b \in F$. Determine the Galois group over F of a splitting field of $x^p - x - a$.

解答.[18] Let β be a root of $f(x) \coloneqq x^p - x - a$ in the algebraic closure of F. We claim that $x^p - x - a$ splits in $F(\beta)$. Notice that $f(x+1) = f(x)$ by the Frobenius endomorphism. Thus, $\beta+1, \beta+2, \ldots, \beta+p-1$ are also roots of $f(x)$. The splitting field is $F(\beta)$. There is a automorphism σ of $F(\beta)$, determined by $\sigma\beta = \beta + 1$. We find $\operatorname{ord} \sigma = p$. Thus $\langle \sigma \rangle \cong C_p$, the cyclic group of order p. From $|\operatorname{Gal}(F(\beta)/F)| = [F(\beta) : F] = n$, we have $\langle \sigma \rangle = \operatorname{Gal}(F(\beta)/F)$. ■

题目 21 . Let F be a finite field of characteristic p (a prime). Show that $(p-1) \mid (|F| - 1)$. Hence conclude that if $|F|$ is even then the characteristic is two. (We shall see later that $|F|$ is a power of p.)

解答.[19] The prime field is $\mathbb{F}_p \hookrightarrow F$. Then $\mathbb{F}_p^\times \leq F^\times$ as a subgroup. Langrange's Theorem ensures $p - 1 \mid (|F| - 1)$. Thus, $|F| - 1 = (p-1)k$ for some $k \in \mathbb{Z}$ and thus

$$|F| = 0 \pmod 2 \implies (p-1)k = 1 \pmod 2.$$

This can happen in the case $p = 2$ only. ■

题目 22 . Show that any finite group of even order contains an element $a \neq 1$ such that $a^2 = 1$.

解答.[20] Define an equivalence relation $\sim$ on G, generated by $g \sim g^{-1}$. Then there is $\Gamma \subseteq G$ s.t.

$$G = \{e\} \sqcup \bigsqcup_{g \in \Gamma} [g] \ ,$$

where $[g]$ is the equivalence class of g; which is $\{g\}$ if $g^2 = e$, and $\{g, g^{-1}\}$ else. We have

$$\sharp G = 1 + \sum_{g \in \Gamma} \sharp [g] \ ;$$

so there must be some $a \in G$ makes $\sharp [a] = 1$. Thus, $a^2 = 1$. ■

题目 26 . Determine the Galois group $\mathrm{Gal}(\mathbb{Q}(\sqrt[p]{2}, \zeta_p)/\mathbb{Q})$.

解答.[21] Let G denote the Galois group. By the Galois main theorem, we have diagrams:

$$\begin{tikzcd}[column sep=small]
 & \mathbb{Q} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{Q}(\sqrt[p]{2}) \arrow[dr, dash] & & \mathbb{Q}(\zeta_p) \arrow[dl, dash] \\
 & \mathbb{Q}(\sqrt[p]{2}, \zeta_p) &
\end{tikzcd}
\qquad
\begin{tikzcd}[column sep=small]
 & \mathrm{Gal}(\mathbb{Q}(\sqrt[p]{2}, \zeta_p)/\mathbb{Q}) \arrow[dl, dash] \arrow[dr, dash] & \\
(\mathbb{Z}/\langle p \rangle)^\times \arrow[dr, dash] & & \mathbb{Z}/\langle p \rangle \arrow[dl, dash] \\
 & \{1\} &
\end{tikzcd}$$

Let $\mathbb{Z}/\langle p \rangle = \langle \tau \rangle$ and $(\mathbb{Z}/\langle p \rangle)^* = \langle \sigma \rangle$, where

$$\tau : \begin{cases} \zeta_p \mapsto \zeta_p \\ \sqrt[p]{2}\zeta_p^i \mapsto \sqrt[p]{2}\zeta_p^{i+1} \quad i \in [p] \end{cases} , \quad \sigma : \begin{cases} \zeta_p \mapsto \zeta_p^a \\ \sqrt[p]{2} \mapsto \sqrt[p]{2} \end{cases} ,$$

where $a \in (\mathbb{Z}/\langle p \rangle)^*$. Thus we find two subgroups $\mathbb{Z}/\langle p \rangle, (\mathbb{Z}/\langle p \rangle)^*$ of G, where $(\mathbb{Z}/\langle p \rangle)^*$ is normal (because it is the Galois group of a Galois extension). For the structure of the group:

- They have trivial intersection: because $\mathbb{Q}(\sqrt[p]{2}) \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$;
- They generate the group G because $\mathrm{Inv}\langle \tau, \sigma \rangle = \mathbb{Q}$.
- They satisfy: $\sigma \tau \sigma^{-1} = \tau^a$.

Above all, we have $G \cong \mathbb{Z}/\langle p \rangle \rtimes (\mathbb{Z}/\langle p \rangle)^*$, which is isomorphic to the matrix group:

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in (\mathbb{Z}/\langle p \rangle)^*, b \in \mathbb{Z}/\langle p \rangle \right\} \subseteq \mathrm{GL}(2, \mathbb{Z}/\langle p \rangle)$$

■

题目 27 . Please state the Galois main theorem clearly.

解答.[22] Let E/F be a finite Galois extension and $G \coloneqq \mathrm{Gal}(E/F)$. We have the following results:

1. For a subgroup $H \leq G$, we have $\mathrm{Gal}(E/\operatorname{Inv} H) = H$. For an intermediate field K, we have $\mathrm{Inv}(Gal(E/K)) = K$.
2. The dimensions $[E : K] = |\,\mathrm{Gal}(E/K)|$, $[K : F] = [G : \mathrm{Gal}(E/K)]$.
3. Both of Gal, Inv are order-reversing.
4. If $H \leq G$ and $\alpha \in G$, and $\operatorname{Inv} H = K$. Then $\mathrm{Inv}(\alpha H \alpha^{-1}) = \alpha(K)$.
5. The extension K/F is Galois if and only if $H = \mathrm{Gal}(E/K)$ is a normal subgroup of G. At that time, $\mathrm{Gal}(K/F) = G/H$.

■