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。

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 ■

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.[2] 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 $\eta\colon\mathbb{R}\to\mathbb{R},\sum_{\text{有限}}r_ie_i\mapsto\sum_{\text{有限}}r_i\lambda_ie_i$. 则 η 的矩阵形式为对角矩阵 $\mathrm{diag}(\lambda_i)_i$; 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) $\mathbb{Z}/(n),n=p_1^{e_1}\cdots p_r^{e_r},p_1,\dots,p_r$ 为不同的素数，$e_i\geq 1,i=1,\dots,r$.

解答.[3] 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.[4] 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 $q:=\operatorname{lcm}(q_1,\cdots,q_n)$, 则

$$M=\left\langle\frac{p_1r_1}{q},\cdots,\frac{p_nr_n}{q}\right\rangle,\quad r_i:=\frac{q}{q_i}.$$

可见 $M=\langle\frac{\gcd(p_1r_1,\cdots,p_nr_n)}{q}\rangle$, 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. ■

第六章

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 $f(x)=x^n+a_1x^{n-1}+\cdots+a_n(a_1,\ldots,a_n\in I)$，使得

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

(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 $M=(0)$.

解答.[5] ...

我们证明 $\operatorname{id}|_M^M=0$, 从而 $M=(0)$; 简记 $\operatorname{id}=\operatorname{id}|_M^M$. 由 (1), 有 $f(x)=x^n+a_1x^{n-1}+\cdots+a_n,(a_i\in I)$ 使得

$$f(\operatorname{id})=\Big(1+\sum_{i=1}^na_i\Big)\operatorname{id}=0.$$

记 $a=\sum_{i=1}^na_i\in I$, 下证明 $1+a$ 是 R 中可逆元: 如果不然, 则主理想 $\langle1+a\rangle$ 是非平凡的, 于是有某极大理想 $I_0\supseteq\langle1+a\rangle$, 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 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.[6] 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.[7] 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.[8] 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.[9] 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

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

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

有 $K = \mathrm{span}_{\mathbb{Q}}(1, \sqrt{3}, \sqrt{-1}, \sqrt{-3})$, 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) $f(x) = x^3 - 2x - 2$;

(iii) $f(x) = x^3 - 3x - 1$.

解答.[11]

■

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 $\mathrm{Aut}\, F = \mathrm{Gal}(F/P)$.

解答.[12] 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 $\mathrm{Aut}\, F = \mathrm{Gal}(F/P)$ 按照定义直接成立. ■

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

解答.[13] 记所求为 G. 观察中间域 $\mathbb{Q}(\sqrt{2}),\mathbb{Q}(\sqrt{3})$ 得到两个子群 $\langle\sigma\rangle,\langle\tau\rangle$:

$$\sigma\colon K\to K,\ r+s\sqrt{2}+t\sqrt{3}\mapsto r-s\sqrt{2}+t\sqrt{3};$$
$$\tau\colon K\to K,\ r+s\sqrt{2}+t\sqrt{3}\mapsto r+s\sqrt{2}-t\sqrt{3}.$$

这两个子群都是正规的 (因为对应的扩张是正规扩张), 而且交为平凡的 (因为子群的交对应中间域的合成), 所以 $\langle\sigma,\tau\rangle\cong(\mathbb{Z}/\langle 2\rangle)^2$. 计数可得 $G=\langle\sigma,\tau\rangle\cong(\mathbb{Z}/\langle 2\rangle)^2$. ■

题目 6 . 设 F 为多项式环 $\mathbb{F}_p[t]$ 的商域，即 $F=\mathbb{F}_p(t)$. 令 K 为多项式 $f(x)=x^p-t$ 在 F 上的分裂域. 证明 $\mathrm{Gal}(K/F)=\{1\}$.

题目 7 . 设 $F=\mathbb{F}_p(t)$ 如习题 6. 令 K 为 $f(x)=x^{2p}+tx^p+t$ 在 F 上的分裂域. 试决定 $\mathrm{Gal}(K/F)$，并定出 $\mathrm{Gal}(K/F)$ 的不动域和 F 在 K 内的可分闭包.

题目 14 . 设 $K=\mathbb{Q}(\sqrt{2},\sqrt{3})$, $\theta=(2-\sqrt{2})(3+\sqrt{3})$, $E=K(\sqrt{\theta})$. 证明 $E/\mathbb{Q}$ 正规，并决定 $\mathrm{Gal}(E/\mathbb{Q})$.

更多习题

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

解答.[17] 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

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

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.