

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 irreducibility. For a primitive polynomial, it is irreducible in  $\mathbb{Z}[x]$  if and only if it is irreducible in  $\mathbb{Q}[x]$ .  $\square$

解答.<sup>1</sup> 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.  $\blacksquare$

### 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.<sup>2</sup> 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 题目 1, we know it is not principal.  $\blacksquare$

## 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  $\eta: M \rightarrow M'$  是一个加法群同构, 则  $\eta$  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.<sup>3</sup> 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

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

另一方面,

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

综上所述,

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

此时,  $\eta$  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  $\eta: \mathbb{R} \rightarrow \mathbb{R}$ ,  $\sum_{\text{有限}} r_i e_i \mapsto \sum_{\text{有限}} r_i \lambda_i e_i$ . 则  $\eta$  的矩阵形式为对角矩阵  $\text{diag}(\lambda_i)_i$ ; 命这个对角矩阵可逆且  $\lambda_i$  不全相同, 则  $\eta$  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.**<sup>4</sup> 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.**<sup>5</sup> 设  $M = \langle p_1/q_1, \dots, p_n/q_n \rangle \subseteq \mathbb{Q}$  是有限生成子模, 其中  $p_i, q_i$  互素. 令  $q := \text{lcm}(q_1, \dots, q_n)$ , 则

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

可见  $M = \left\langle \frac{\gcd(p_1 r_1, \dots, p_n r_n)}{q} \right\rangle$ , 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,  $\varphi \in \text{End}_R(M)$ .

(1) 如果  $M \subseteq IM$ , 证明: 存在  $f(x) = x^n + a_1x^{n-1} + \cdots + a_n$  ( $a_1, \dots, a_n \in I$ ), 使得

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

(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. ...

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

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

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  $\text{id} = 0$ .

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

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

解答.<sup>7</sup> 对  $x \in M$ ,

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

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

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

解答.<sup>8</sup> It is isomorphic to the ring  $\mathbb{Q}$ :

$$\text{End}(\mathbb{Q}, +, 0) \rightarrow \mathbb{Q}, f \mapsto f(1). \quad (1)$$

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

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

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.**<sup>9</sup> 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.**<sup>10</sup> 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

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

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.**<sup>11</sup> 有  $K = \text{span}_{\mathbf{Q}}(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ , 一组基是  $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ .

有  $K = \text{span}_{\mathbf{Q}}(1, \sqrt{3}, \sqrt{-1}, \sqrt{-3})$ , 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.<sup>12</sup>

(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  $\alpha$  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  $\text{Aut } F = \text{Gal}(F/P)$ .

解答.<sup>13</sup> 设  $\sigma: F \rightarrow F$  是非零的自同态, 则  $\sigma$  是  $F$  的自同构, 所以  $\sigma(1)$  是单位元即  $\sigma(1) = 1$ . 于是,  $\sigma$  保持素域内的元素不动, 因为素域由 1 生成. 现在  $\text{Aut } F = \text{Gal}(F/P)$  按照定义直接成立. ■

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

解答.<sup>14</sup> 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  $G = \langle \sigma, \tau \rangle \cong (\mathbb{Z}/\langle 2 \rangle)^2$ . ■

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  $\text{Gal}(K/F) = \{1\}$ .

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  $\text{Gal}(K/F)$ , 并定出  $\text{Gal}(K/F)$  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  $\text{Gal}(E/\mathbb{Q})$ .

## 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.**<sup>18</sup> 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

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

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.**<sup>19</sup> Let  $\beta$  be a root of  $f(x) := x^p - x - a$  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,  $\beta+1, \beta+2, \dots, \beta+p-1$  are also roots of  $f(x)$ . The splitting field is  $F(\beta)$ . There is a automorphism  $\sigma$  of  $F(\beta)$ , determined by  $\beta \mapsto \beta+1$ . We find  $\text{ord } \sigma = p$ . Thus  $\langle \sigma \rangle \cong C_p$ , the cyclic group of order  $p$ . From  $|\text{Gal}(F(\beta)/F)| = [F(\beta) : F] = n$ , we have  $\langle \sigma \rangle = \text{Gal}(F(\beta)/F)$ . ■

**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  $p$ .)

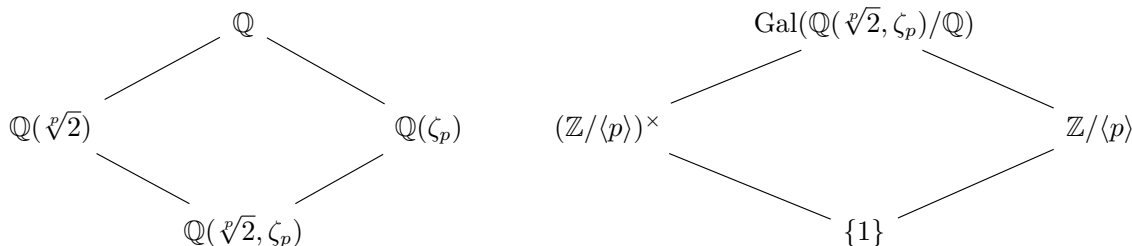
**解答.**<sup>20</sup> The prime field is  $\mathbb{F}_p \hookrightarrow F$ . Then  $\mathbb{F}_p^\times \leq F^\times$  as a subgroup. Langrange's Theorem ensures  $p-1 \mid (|F| - 1)$ . Thus,  $|F| - 1 = (p-1)k$  for some  $k \in \mathbb{Z}$  and thus

$$|F| \equiv 1 \pmod{p-1} \implies (p-1)k \equiv 1 \pmod{p-1}.$$

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

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

**解答.**<sup>21</sup> Let  $G$  denote the Galois group. By the Galois main theorem, we have diagrams:



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

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

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  $\text{Inv}\langle \tau, \sigma \rangle = \mathbb{Q}$ .
- 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:

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

■

**题目 27 .** Please state the Galois main theorem clearly.