近世代数 (H) 第八周作业

涂嘉乐 PB23151786

2025 年 4 月 20 日

Exercise 1 证明 $|\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})| < \dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2})$

Proof 因为 $\sqrt[3]{2}$ 在 $\mathbb{Q}$ 上的最小多项式为 x^3-2，所以 $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}) = 3$；另一方面，因为 x^3-2 在 $\mathbb{Q}(\sqrt[3]{2})$ 上的根只有一个 $\sqrt[3]{2}$，所以 $\mathrm{Id}_{\mathbb{Q}}$ 只有一种延拓（本质上是因为 $\mathbb{Q}(\sqrt[3]{2})$ 不是 x^3-2 的分裂域）

$$\begin{aligned} \sigma : \mathbb{Q}(\sqrt[3]{2}) &\longrightarrow \mathbb{Q}(\sqrt[3]{2}) \\ \sqrt[3]{2} &\longmapsto \sqrt[3]{2} \\ q &\longmapsto q, \forall q \in \mathbb{Q} \end{aligned}$$

即 $\sigma = \mathrm{Id}_{\mathbb{Q}(\sqrt[3]{2})}$，因此 $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})) = \mathrm{Aut}(\mathbb{Q}[\sqrt[3]{2}]) = \{\mathrm{Id}_{\mathbb{Q}(\sqrt[3]{2})}\} = 1 < 3$ □

Exercise 2 证明不存在 $\delta : \mathbb{Q}(\sqrt[4]{2}) \to \mathbb{Q}(\sqrt[4]{2})$ 使得图交换

$$\begin{array}{ccc} \mathbb{Q}(\sqrt[4]{2}) & \xrightarrow{\nexists \delta} & \mathbb{Q}(\sqrt[4]{2}) \\ \theta \uparrow & & \uparrow \theta \\ \mathbb{Q}(\sqrt{2}) & \xrightarrow{\sigma} & \mathbb{Q}(\sqrt{2}) \end{array}$$

其中 $\sigma(a+b\sqrt{2}) = a - b\sqrt{2}$

Proof 假设存在这样的 δ，设 $\delta(\sqrt[4]{2}) = a$，则 $\delta(\sqrt{2}) = \delta(\sqrt[4]{2})^4 = a^4$，但是 δ 为 σ 的延拓，即 $\delta(\sqrt{2}) = \sigma(\sqrt{2}) = -\sqrt{2}$，故 $a^4 = -\sqrt{2}$，但是任意一个实数的四次方均为正数，矛盾！ □

注记 不存在 δ 的原因是 $\sqrt[4]{2}$ 在 $\mathbb{Q}(\sqrt{2})$ 上的最小多项式为 $x^4-\sqrt{2}$，而 $\sigma(x^4-\sqrt{2}) = x^4+\sqrt{2}$，它在 $\mathbb{Q}(\sqrt[4]{2})$ 上无根！

Exercise 3 设 $k = \mathbb{F}_p(t), f(x) = x^p - t \in k[x]$ 不可约，但有重根

Proof 因为 $\mathbb{F}_p(t) = \mathrm{Frac}\big(\mathbb{F}_p[t]\big)$，所以 x^p-t 在 $\mathbb{F}_p(t)[x]$ 中不可约 $\iff$ x^p-t 在 $\mathbb{F}_p[t][x]$ 中不可约，由 $\mathbb{F}_p$ 为 *UFD* 知，$\mathbb{F}_p[t]$ 为 *UFD*，且 t 为 $\mathbb{F}_p[t]$ 中素元，由 *Eisenstein* 判别法，取 $p=t$ 即有 x^p-t 在 $\mathbb{F}_p[t][x]$ 中不可约

设 E 为 x^p-t 的分裂域，则 $\exists \alpha \in E \backslash k, \text{s.t. } f(\alpha) = 0$，即 $\alpha^p = t$，所以

$$x^p - t = x^p - \alpha^p = (x-\alpha)^p$$

这就说明 $x^p - t$ 有重根，且为 p 重根 □

Exercise 4 证明 $\mathrm{Aut}(\mathbb{F}_9) = \{\mathrm{Id}_{\mathbb{F}_9}, \sigma\}$

Proof 因为 $|\mathrm{Aut}(\mathbb{F}_9/\mathbb{F}_3)| \leq \dim_{\mathbb{F}_3} \mathbb{F}_9 = 2$，且 $\mathrm{Aut}(\mathbb{F}_9/\mathbb{F}_3) = \mathrm{Aut}(\mathbb{F}_9)$，而已知 $\sigma, \mathrm{Id}_{\mathbb{F}_9} \in \mathrm{Aut}(\mathbb{F}_9)$，所以 $\mathrm{Aut}(\mathbb{F}_9/\mathbb{F}_3) = \{\mathrm{Id}_{\mathbb{F}_9}, \sigma\}$ □

Exercise 5 在 $\mathbb{F}_2[x]$ 中将 $x^8 - x, x^{16} - x$ 分解为不可约多项式的乘积

Solution 因为 $\mathbb{F}_2[x]$ 中，一次不可约多项式为 $x, x-1$；二次不可约多项式为 x^2+x+1；三次不可约多项式为 x^3+x^2+1, x^3+x+1；四次不可约多项式为 $x^4+x^3+x^2+x+1, x^4+x^3+1, x^4+x+1$ 所以

$$x^8 - x = x(x-1)(x^3+x^2+1)(x^3+x+1)$$

$$x^{16} - x = x(x-1)(x^2+x+1)(x^4+x^3+x^2+x+1)(x^4+x^3+1)(x^4+x+1)$$

□

Exercise 6 在 $\mathbb{F}_3[x]$ 中将 $x^9 - x$ 分解为不可约多项式的乘积

Solution 因为 $\mathbb{F}_3[x]$ 中，一次不可约多项式为 $x, x-1, x-2$；二次不可以多项式为 x^2+1, x^2+x+2, x^2+2x+2，所以

$$x^9 - x = x(x-1)(x-2)(x^2+1)(x^2+x+2)(x^2+2x+2)$$

□

Exercise 7 设 E 是 p^n 元域，$d \mid n$，$K = \mathrm{Root}_E(x^{p^d} - x) = \{a \in E | \sigma^d(a) = a\}$，其中 σ 为 *Frobenius* 同态，试验证

1. $x^{p^d} - x$ 在 E 上分裂
2. $x^{p^d} - x$ 无重根
3. K 是子域

Proof

1. 对 $\forall a \in \mathrm{Root}_E(x^{p^d} - x)$，若 $a = 0$，则 $a \in E$；若 $a \neq 0$，则 $a^{p^d - 1} = 1$，因为 $d \mid n$，可设 $kd = n$，则
$$p^n - 1 = (p^d - 1)(p^{(k-1)d} + p^{(k-2)d} + \cdots + p^d + 1)$$
因此 $a^{p^n-1} = \left(a^{p^d-1}\right)^{p^{(k-1)d}+p^{(k-2)d}+\cdots+p^d+1} = 1$，因此 $a \in \mathrm{Root}_E(x^{p^n} - x)$，由 $x^{p^n} - x$ 在 E 上分裂知，$x^{p^d} - x$ 在 E 上分裂
2. 因为 $(x^{p^d} - x)' = -1$，故
$$\gcd(x^{p^d} - x, -1) = 1 \Longrightarrow x^{p^d} - x \text{无重根}$$

3. 首先 $1^{p^d}-1=0$，故 $1\in K$，接下来证明 $\forall a,b\in K\backslash\{0\},a^{-1},a+b,ab\in K$，所以

$$a^{p^d}=a\Longrightarrow a^{-1}=\left(a^{p^d}\right)^{-1}=(a^{-1})^{p^d}\Longrightarrow a^{-1}\in K$$

$$a^{p^d}=a,b^{p^d}=b\Longrightarrow (a+b)^{p^d}=a^{p^d}+b^{p^d}=a+b\Longrightarrow a+b\in K$$

$$a^{p^d}=a,b^{p^d}=b\Longrightarrow (ab)^{p^d}=a^{p^d}b^{p^d}=ab\Longrightarrow ab\in K$$

因此 K 是子域

□

Exercise 8 设 E 为 p^n 元域，$n=q_1^{m_1}\cdots q_s^{m_s}$，$\mathbb{F}_{p^{\frac{n}{q_i}}}\overset{\text{def}}{=}K_{\frac{n}{q_i}}$ 证明

$$\left|\bigcup_{i=1}^{s}K_{\frac{q}{n_i}}\right|<|E|$$

Proof 因为 $\left|K_{\frac{n}{q_i}}\right|=p^{\frac{n}{q_i}}$，所以

$$\left|\bigcup_{i=1}^{s}K_{\frac{q}{n_i}}\right|\leq\sum_{i=1}^{s}p^{\frac{n}{q_i}}\leq s\cdot p^{\frac{n}{2}}\leq\frac{n}{2}p^{\frac{n}{2}}<p^n=|E|$$

□

Exercise 9 求证 $K_{d_1}\cap K_{d_2}=K_{\gcd(d_1,d_2)}$，其中 $\mathbb{F}_{p^d}\overset{\text{def}}{=}K_d$

Proof 首先 $K_{d_1}\cap K_{d_2}$ 是 K_{d_1},K_{d_2} 的子域，因为它的任意运算均在 K_{d_1},K_{d_2} 中成立，因为 p^n 元域的子域一定是 p^d 元域，其中 $d\mid n$，所以可设 $|K_{d_1}\cap K_{d_2}|=p^d$，且 $d\mid d_1,d\mid d_2$，因此 $d\mid\gcd(d_1,d_2)$

另一方面 $K_{\gcd(d_1,d_2)}\subset K_{d_1},K_{\gcd(d_1,d_2)}\subset K_{d_2}$，所以 $K_{\gcd(d_1,d_2)}\subset K_{d_1}\cap K_{d_2}=K_d$，这就说明 $\gcd(d_1,d_2)=d$，因此 $K_{d_1}\cap K_{d_2}=K_{\gcd(d_1,d_2)}$ □

Exercise 10 设 $E=\mathbb{F}_{p^n}$，K_d 为 E 的 p^d 元子域，记 $K_{d_1}\vee K_{d_2}$ 为包含 $K_{d_1}\cup K_{d_2}$ 的最小子域，则 $K_{d_1}\vee K_{d_2}=K_{\operatorname{lcm}(d_1,d_2)}$

Proof 即证明 $\forall E$ 的包含 $K_{d_1}\cup K_{d_2}$ 的子域，均包含 $K_{\operatorname{lcm}(d_1,d_2)}$，设 F 为 E 的包含 $K_{d_1}\cup K_{d_2}$ 的子域，则 $|F|=p^d$，其中 $d\mid n$，且由 $K_{d_1}\subseteq F$ 知，$d_1\mid d$，同理 $d_2\mid d$，因此 $\operatorname{lcm}(d_1,d_2)\mid d$，这就说明 $K_{\operatorname{lcm}(d_1,d_2)}\subseteq F$（由有限域的结构定理，对任意 d 的因子，此处取 $\operatorname{lcm}(d_1,d_2)$，一定存在唯一的 $p^{\operatorname{lcm}(d_1,d_2)}$ 元子域，即为 $K_{\operatorname{lcm}(d_1,d_2)}$） □

Exercise 11 设 k 是域，ω 为 k 中的 d 次本原单位根，即 $\operatorname{Ord}(\omega)=d,\operatorname{Char}(k)=p>0$，求证 $p\nmid d$

Proof 假设 $qp=d$，则

$$\omega^d=1\Longrightarrow 0=\omega^d-1=\left(\omega^q\right)^p-1^p=(\omega^q-1)^p\Longrightarrow\omega^q=1$$

这与 $\operatorname{Ord}(\omega)=d$ 蕴含的 d 的最小性矛盾！ □

Exercise 12 设 $f(x), g(x) \in \mathbb{Z}[x], g(x)$ 首一，若 $f(x) = g(x)h(x), h(x) \in \mathbb{C}[x]$，求证 $h(x) \in \mathbb{Z}[x]$

Proof 首先 $h(x) \in \mathbb{Q}[x]$，否则 $f(x)$ 系数中会出现无理数或者虚数。则对 $h(x)$ 进行谨慎通分得 $h(x) = ah_1(x)$，其中 $h_1(x) \in \mathbb{Z}[x]$ 本原，因此

$$f(x) = ag(x)h_1(x)$$

由于 $g(x)$ 首一，所以它是本原多项式，由 *Gauss* 引理，$g(x)h_1(x)$ 是本原多项式，由 $f(x) \in \mathbb{Z}[x]$ 和 $g(x)h_1(x)$ 本原知，$a \in \mathbb{Z}$，因此 $h(x) = ah_1(x) \in \mathbb{Z}[x]$ □