近世代数 (H) 第七周作业

涂嘉乐 PB23151786

2025 年 4 月 11 日

Exercise 1 证明：$\mathbb{Q}(\sqrt[3]{2})$ 有一组 $\mathbb{Q}$-基 $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$

Proof 考虑赋值映射

$$\begin{aligned} \mathrm{ev}_{\sqrt[3]{2}} : \mathbb{Q}[x] &\longrightarrow \mathbb{Q}[\alpha] \\ x &\longmapsto \sqrt[3]{2} \\ q &\longmapsto q, \forall q \in \mathbb{Q} \end{aligned}$$

注意到 x^3-2 为 $\sqrt[3]{2}$ 在 $\mathbb{Q}$ 上的最小多项式（它在 $\mathbb{Q}$ 上不可约了），下证明 $\mathrm{Ker}\ \mathrm{ev}_{\sqrt[3]{2}} = (x^3-2)$，首先显然有 $(x^3-2) \subseteq \ker\ \mathrm{ev}_{\sqrt[3]{2}}$，其次，对 $\forall g(x) \in \mathrm{Ker}\ \mathrm{ev}_{\sqrt[3]{2}}$，对 x^3-2 做带余除法得

$$g(x) = q(x)(x^3-2) + r(x), \quad \deg r \leq 2$$

作用 $\mathrm{ev}_{\sqrt[3]{2}}$ 得 $r(\sqrt[3]{2}) = 0$，这与 x^3-2 的最小性矛盾！因此 $r(x) = 0$，故 $g(x) = q(x)(x^3-2) \Longrightarrow x^3-2 \mid g(x)$，故 $\mathrm{Ker}\ \mathrm{ev}_{\sqrt[3]{2}} \subseteq (x^3-2)$，因此二者相等

且显然 $\mathrm{ev}_{\sqrt[3]{2}}$ 是满射，由同态基本定理我们有域同态（因为 x^3-2 不可约，故 (x^3-2) 是极大理想，故 $\mathbb{Q}[x]/(x^3-2)$ 是域）

$$\begin{aligned} \overline{\mathrm{ev}}_{\sqrt[3]{2}} : \mathbb{Q}[x]/(x^3-2) &\longrightarrow \mathbb{Q}[\sqrt[3]{2}] \\ \overline{f(x)} &\longmapsto f(\sqrt[3]{2}) \end{aligned} \tag{1}$$

由 (1) 知，$\forall q \in \mathbb{Q}[\sqrt[3]{2}]$，均 $\exists f(x) \in \mathbb{Q}[x]/(x^3-2), \mathrm{s.t.}\ f(\sqrt[3]{2}) = q$，而对 $f(x)$ 作带余除法有

$$f(x) = g(x)(x^3-2) + r(x), \quad \deg r \leq 2$$

则 $\overline{r} = \overline{f} \Longrightarrow r(\sqrt[3]{2}) = f(\sqrt[3]{2})$，故 $\forall q \in \mathbb{Q}[\sqrt[3]{2}], \exists r \in \mathbb{Q}[x], \deg r \leq 2, \mathrm{s.t.}\ r(\sqrt[3]{2}) = q$，设 $r(x) = a_2x^2 + a_1x + a_0$，则

$$q = r(\sqrt[3]{2}) = a_2\sqrt[3]{4} + a_1\sqrt[3]{2} + a_0, \quad \forall q \in \mathbb{Q}[\sqrt[3]{2}]$$

下面证明 $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ 线性无关，若它们线性相关，则 $\exists \lambda_0, \lambda_1, \lambda_2 \in \mathbb{Q}, \mathrm{s.t.}\ \lambda_0 + \lambda_1\sqrt[3]{2} + \lambda_2\sqrt[3]{4} = 0$，故 $h(x) = \lambda_0 + \lambda_1 x + \lambda_2 x^2$ 满足 $h(\sqrt[3]{2}) = 0$，这与 $f(x)$ 是最小多项式矛盾！因此 $\lambda_0, \lambda_1, \lambda_2$ 是线性无关，故它是 $\mathbb{Q}[\sqrt[3]{2}]$ 的一组 $\mathbb{Q}$-基

最后证明 $\mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}[\sqrt[3]{2}]$，由 (1) 知 $\mathbb{Q}[\sqrt[3]{2}]$，而我们有

$$\mathrm{Frac}(\mathbb{Q}[\sqrt[3]{2}]) = \mathbb{Q}(\sqrt[3]{2})$$

上面的等号其实是同构关系，但是我们可以等同起来，而域的分式域是它自身，故 $\mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}(\sqrt[3]{2})$，故 $\mathbb{Q}(\sqrt[3]{2})$ 有一组 $\mathbb{Q}$-基 $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ □

Exercise 2 证明：记 $\omega = e^{\frac{2\pi i}{3}}$，则作为域扩张有

$$\mathbb{Q}(\sqrt[3]{2}\omega)/\mathbb{Q} \cong \mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$$

但作为 $\mathbb{C}$ 的子集 $\mathbb{Q}(\sqrt[3]{2}\omega) \neq \mathbb{Q}(\sqrt[3]{2})$

Proof 因为 $x^3 - 2 = 0$ 的三个根分别为 $\sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2$，所以 $\sqrt[3]{2}, \sqrt[3]{2}\omega$ 在 $\mathbb{Q}$ 上的最小多项式均为 $x^3 - 2$（三次多项式在 $\mathbb{Q}$ 上无根，故不可约），所以 $\mathbb{Q}(\sqrt[3]{2})$ 有一组 $\mathbb{Q}$-基 $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$；$\mathbb{Q}(\sqrt[3]{2}\omega)$ 有一组 $\mathbb{Q}$-基 $\{1, \sqrt[3]{2}\omega, \sqrt[3]{4}\omega^2\}$

考虑 $\theta_1 : \mathbb{Q} \to \mathbb{Q}(\sqrt[3]{2}), \theta_2 : \mathbb{Q} \to \mathbb{Q}(\sqrt[3]{2}\omega)$，其中 θ_1, θ_2 均为嵌入映射，考虑

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

下证 ϕ 是域同构：

①. $\phi(1) = 1$

②. 保加法、乘法：因为 $\mathbb{Q}(\sqrt[3]{2})$ 有一组 $\mathbb{Q}$-基，所以 $\forall q \in \mathbb{Q}(\sqrt[3]{2}), \exists! \lambda_0, \lambda_1, \lambda_2 \in \mathbb{Q}, \text{s.t. } q = \lambda_0 + \lambda_1\sqrt[3]{2} + \lambda_2\sqrt[3]{4}$，即 $\exists! f(x) = \lambda_2 x^2 + \lambda_1 x + \lambda_0 \in \mathbb{Q}[x], \text{s.t. } f(\sqrt[3]{2}) = q$，同理对于 $\forall q \in \mathbb{Q}(\sqrt[3]{2}\omega), \exists! f(x) \in \mathbb{Q}[x], \text{s.t. } f(\sqrt[3]{2}\omega) = q$，且我们有

$$q = \lambda_0 + \lambda_1\sqrt[3]{2} + \lambda_2\sqrt[3]{4} \Longrightarrow \phi(q) = \lambda_0 + \lambda_1\sqrt[3]{2}\omega + \lambda_2\sqrt[3]{4}\omega^2$$

即若 $q = f(\sqrt[3]{2})$，则 $\phi(q) = f(\sqrt[3]{2}\omega)$，所以对 $\forall q_1, q_2 \in \mathbb{Q}(\sqrt[3]{2}), \exists! f(x), g(x) \in \mathbb{Q}[x], \text{s.t. } f(\sqrt[3]{2}) = q_1, g(\sqrt[3]{2}) = q_2$，因此

$$\begin{cases} \phi(q_1 + q_2) = \phi\big(f(\sqrt[3]{2}) + g(\sqrt[3]{2})\big) = f(\sqrt[3]{2}\omega) + g(\sqrt[3]{2}\omega) = \phi(q_1) + \phi(q_2) \\ \phi(q_1 q_2) = \phi\big(f(\sqrt[3]{2})g(\sqrt[3]{2})\big) = f(\sqrt[3]{2}\omega)g(\sqrt[3]{2}\omega) = \phi(q_1)\phi(q_2) \end{cases} \tag{2}$$

③. 双射：域上的同态必然是单射，下面验证满射。对于每个 $a \in \mathbb{Q}(\sqrt[3]{2}\omega), \exists q_0, q_1, q_2 \in \mathbb{Q}, \text{s.t. } a = q_0 + q_1\sqrt[3]{2}\omega + q_2\sqrt[3]{4}\omega^2$，则它有原像 $b = q_0 + q_1\sqrt[3]{2} + q_2\sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2}), \text{s.t. } \phi(b) = a$

则 ϕ 确实是域同构，且 $\phi \circ \theta_1|_{\mathbb{Q}} = \mathrm{Id}_{\mathbb{Q}} = \theta_2|_{\mathbb{Q}}$，则这两个域扩张是同构的

但作为 $\mathbb{C}$ 的子集，显然 $\omega \in \mathbb{Q}(\sqrt[3]{2}\omega)$，但 $\omega \notin \mathbb{Q}(\sqrt[3]{2})$：假设 $\omega \in \mathbb{Q}(\sqrt[3]{2})$，则 $\exists \lambda_0, \lambda_1, \lambda_2 \in \mathbb{Q}, \text{s.t. } \omega = \lambda_0 + \lambda_1\sqrt[3]{2} + \lambda_2\sqrt[3]{4}$，但是 $RHS \in \mathbb{Q}, LHS \notin \mathbb{Q}$，矛盾！故作为 $\mathbb{C}$ 的子集二者不相等 □

Exercise 3 设有域扩张塔 $k \subset E \subset K$，E/k 有 k-基 $\{u_1, \cdots, u_n\}$，K/E 有 E-基 $\{v_1, \cdots, v_m\}$，求证 K 有一组 k-基

$$\{u_i v_j | 1 \leq i \leq n, 1 \leq j \leq m\}$$

Proof 对 $\forall a \in K, \exists \lambda_1, \cdots, \lambda_m \in E, \text{s.t.}$

$$a = \lambda_1 v_1 + \cdots + \lambda_m v_m$$

对 $\lambda_i \in E, 1 \leq i \leq m, \exists \mu_{1i}, \cdots, \mu_{ni} \in k, \text{s.t.}$

$$\lambda_i = \mu_{1i} u_1 + \cdots + \mu_{ni} u_n$$

因此

$$a = \sum_{i=1}^{m} \lambda_i v_i = \sum_{i=1}^{m} v_i \sum_{j=1}^{n} \mu_{ji} u_j = \sum_{i,j} \mu_{ji} v_i u_j$$

即 $\forall a \in K$，均可被 $\{u_i v_j\}$ 线性表出，下面证明它们线性无关，假设 $\exists \{\gamma_{ij}\} \in k, \text{s.t.}$

$$\sum_{i,j} \gamma_{ij} u_i v_j = 0$$

则 $\sum\limits_{j=1}^{m} \left(\sum\limits_{i=1}^{n} \lambda_{ij} u_i \right) v_j = 0$，由 $\{v_j\}$ 是一组 E-基知，$\forall 1 \leq j \leq m, \sum\limits_{i=1}^{n} \lambda_{ij} u_i = 0$，再由 $\{u_i\}$ 是一组 k-基知，$\lambda_{ij} = 0, \forall i, j$，故 $\{u_i v_j\}$ 线性无关 □

Exercise 4 设 K/k 是有限维域扩张，$\alpha \in K$ 在 k 上的最小多项式为 $f(x)$，求证 $\deg f \mid \dim_k K$

Proof 考虑域扩张塔

$$k \subseteq k(\alpha) \subseteq K$$

由维数公式知

$$\dim_k k(\alpha) \cdot \dim_{k(\alpha)} K = \dim_k K$$

而 $\dim_k k(\alpha) = \deg f$，因此 $\deg f \mid \dim_k K$ □

Exercise 5 设 F/K 为域扩张，$u \in F$ 是 K 上奇次代数元素，求证 $K(u) = K(u^2)$

Proof 显然我们有 $K(u^2) \subseteq K(u)$，我们有如下域扩张塔

$$K \subseteq K(u^2) \subseteq K(u) = K(u^2)(u)$$

假设 $K(u) \neq K(u^2)$，则 $u \notin K(u^2)$。考虑 $f(u) = x^2 - u^2 \in K(u^2)[x]$，因为 $f(u) = 0$，所以 u 是 $K(u^2)$ 上的代数元，因为 $x^2 - u^2 = 0$ 的两个根为 $\pm u \notin K(u^2)$，所以 u 在 $K(u^2)$ 上的最小多项式为 $f(x) = x^2 - u^2$，即

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

因为 u 是 K 上奇次代数元素，所以 $[K(u) : K]$ 为奇数，由维数公式知

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

上式左边为奇数，右边为偶数，矛盾！因此 $K(u)=K(u^2)$ □

Exercise 6 求元素 a 在域 K 中的最小多项式，其中

1. $a=\sqrt{2}+\sqrt{3}, K=\mathbb{Q}$
2. $a=\sqrt{2}+\sqrt{3}, K=\mathbb{Q}(\sqrt{2})$
3. $a=\sqrt{2}+\sqrt{3}, K=\mathbb{Q}(\sqrt{6})$

Proof 1. 上次作业求过了，为 x^4-10x^2+1

2. 因为 $x^4-10x^2+1=(x^2-1+2\sqrt{2}x)(x^2-1-2\sqrt{2}x)$，经过计算发现 $f(x)=x^2-2\sqrt{2}x-1$ 是 $\sqrt{2}+\sqrt{3}$ 的零化多项式，且它的根为 $\sqrt{2}+\sqrt{3},\sqrt{2}-\sqrt{3}$，它们均不在 $\mathbb{Q}(\sqrt{2})$ 中，因此 $f(x)$ 是 $\mathbb{Q}(\sqrt{2})$ 中不可约多项式，为 $\sqrt{2}+\sqrt{3}$ 在 $\mathbb{Q}(\sqrt{2})$ 中的最小多项式
3. 注意到 $(\sqrt{2}+\sqrt{3})^2=5+2\sqrt{6}$，所以 $g(x)=x^2-(5+2\sqrt{6})$ 是 $\sqrt{2}+\sqrt{3}$ 的零化多项式，且它的根为 $\sqrt{2}+\sqrt{3},-\sqrt{2}-\sqrt{3}$，它们均不在 $\mathbb{Q}(\sqrt{6})$ 中，因此 $g(x)$ 是 $\mathbb{Q}(\sqrt{6})$ 中的不可约多项式，为 $\sqrt{2}+\sqrt{3}$ 在 $\mathbb{Q}(\sqrt{6})$ 中的最小多项式 □

Exercise 7 设 F/K 为域的代数扩张，D 为整环且 $K\subseteq D\subseteq F$，求证：D 为域

Proof 即证明 $\forall 0\neq d\in D, d^{-1}\in D$，若 $d\in K$，则由 K 是域知 $d^{-1}\in K\subseteq D$；若 $d\notin K$，因为 $d\in F\backslash K$，由代数扩张知，d 在 K 上代数，故 $\exists f(x)=a_nx^n+\cdots+a_0\in K[x],\text{s.t. } f(d)=0$，即

$$a_nd^n+\cdots+a_1d+a_0=0$$

记 $k=\min\{i|0\leq i\leq n, a_i\neq 0\}$，若 $k=0$，即 $a_0\neq 0$，由 K 是域知它可逆，则

$$d(a_nd^{n-1}+\cdots+a_1)=-a_0\Longrightarrow d^{-1}=-(a_nd^{n-1}+\cdots+a_1)a_0^{-1}$$

而 $a_0,\cdots,a_n,d\in D$，由整环对加、乘封闭知 $d^{-1}\in D$

若 $k\neq 0$，则

$$a_nd^n+\cdots+a_kd^k=0\Longrightarrow a_nd^{n-k}+\cdots+a_k=0\Longrightarrow d^{-1}=-(a_nd^{n-k-1}+\cdots+a_{k-1})a_k^{-1}$$

同理可知 $d^{-1}\in D$，故 D 是域 □

Exercise 8 设 u 是多项式 x^3-6x^2+9x+3 的一个实根

1. 求证：$[\mathbb{Q}(u):\mathbb{Q}]=3$
2. 试将 $u^4,(u+1)^{-1},(u^2-6u+8)^{-1}$ 表示成 $1,u,u^2$ 的线性组合

Proof

1. 取 $p=3$，由 *Eisenstein* 判别法知 $f(x)=x^3-6x^2+9x+3$ 在 $\mathbb{Z}[x]$ 中不可约，进而在 $\mathbb{Q}[x]$ 中不可约，故 $u\notin\mathbb{Q}$，且 u 在 $\mathbb{Q}$ 上代数，最小多项式 $f(x)=x^3-6x^2+9x+3$，所以

$$[\mathbb{Q}(u):\mathbb{Q}]=\deg f=3$$

2. • 因为 $u^3 = 6u^2 - 9u - 3$，所以

$$\begin{aligned} u^4 &= 6u^3 - 9u^2 - 3u \\ &= 6(6u^2 - 9u - 3) - 9u^2 - 3u \\ &= 27u^2 - 57u - 18 \end{aligned}$$

• 由 $x^3 - 6x^2 + 9x + 3$ 不可约知，$(x+1, x^3 - 6x^2 + 9x + 3) = 1$，计算 *Bezout* 等式得

$$(x+1) \cdot \frac{1}{13}(x^2 - 7x + 16) - (x^3 - 6x^2 + 9x + 3) = 1$$

将 u 代入上式得

$$(1+u)^{-1} = \frac{1}{13}(u^2 - 7u + 16)$$

• 同理有 $(x^2 - 6x + 8, x^3 - 6x^2 + 9x + 3) = 1$，由辗转相除法

$$x^3 - 6x^2 + 9x + 3 = x(x^2 - 6x + 8) + (x + 3)$$

$$x^2 - 6x + 8 = (x - 9)(x + 3) + 35$$

则有 *Bezout* 等式

$$\frac{1}{35}(x^2 - 9x + 1)(x^2 - 6x + 8) - (x - 9)(x^3 - 6x^2 + 9x + 3) = 1$$

将 u 代入上式得

$$(u^2 - 6u + 8)^{-1} = \frac{1}{35}(u^2 - 9u + 1)$$

□

Exercise 9 设 $u = \frac{x^3}{x+1}$，求 $[\mathbb{Q}(x) : \mathbb{Q}(u)]$

Proof 因为 $x^3 = u(x+1)$，所以 $f(t) = t^3 - ut - u$ 是 x 在 $\mathbb{Q}(u)$ 上的一个零化多项式，而它在 $\mathbb{Q}(t)$ 上有分解

$$f(t) = (t - x)(t^2 + xt + x^2 - u)$$

因为 $x \notin \mathbb{Q}(u)$，所以若 $f(t)$ 在 $\mathbb{Q}(u)$ 上可约，只能是 $t^2 + xt + x^2 - u$ 在 $\mathbb{Q}(u)$ 上可约，则它可以分解为 $\mathbb{Q}(u)$ 上两个一次因式的乘积，即

$$t^2 + xt + x^2 - u = (t - t_1)(t - t_2) \text{ in } \mathbb{Q}(u)[x]$$

展开得 $t_1 + t_2 = -x \notin \mathbb{Q}(u)$，但这显然是矛盾的，因为根据假设 $t - t_1, t - t_2 \in \mathbb{Q}(u)[x] \Longrightarrow t_1, t_2 \in \mathbb{Q}(u) \Longrightarrow x \in \mathbb{Q}(u)$，但是 $x \notin \mathbb{Q}(u)$，矛盾！

综上 $f(t)$ 不可约，故 x 在 $\mathbb{Q}(u)$ 上的最小多项式次数为 3，即 $[\mathbb{Q}(x) : \mathbb{Q}(u)] = 3$ □

Exercise 10 设有域同构 $\sigma : k \to k'$，设有域扩张 $E/k, E'/k', \alpha \in E$ 在 k 上的最小多项式为 $f(x)$，则对任意域同态 $\tilde{\sigma} : k(\alpha) \to E'$，若 $\tilde{\sigma}|_k = \sigma$，求证 $\tilde{\sigma}(\alpha) \in \mathrm{Root}_{E'}(\sigma(f))$

Proof 假设 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in k[x]$，则 $f(\alpha) = a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0$，同时作用 $\tilde{\sigma}$ 得

$$\tilde{\sigma}(a_n\alpha^n + \cdots + a_1\alpha + a_0) = \sigma(a_n)\tilde{\sigma}(\alpha)^n + \cdots + \sigma(a_1)\tilde{\sigma}(\alpha) + \sigma(a_0) = 0$$

所以 $\tilde{\sigma}(\alpha) \in E'$ 是 $\sigma(f) = \sigma(a_n)x^n + \cdots + \sigma(a_1)x + \sigma(a_0)$ 的根，即 $\tilde{\sigma}(\alpha) \in \mathrm{Root}_{E'}(\sigma(f))$ □

Exercise 11 考虑 $\mathbb{F}_2 \hookrightarrow \mathbb{F}_4 = \mathbb{F}_2[x]/(x^2+x+1)$，求证 $\mathbb{F}_4/\mathbb{F}_2$ 是 x^2+x+1 在 $\mathbb{F}_2$ 上的分裂域

Proof 记 $f(x) = x^2+x+1$，因为在 $\mathbb{F}_4$ 中，$u = \bar{x}$ 满足 $f(u) = 0$，所以在 $\mathbb{F}_4$ 中 $f(x)$ *spilt*（见下式）

$$f(x) = (x-u)(x+(1+u)) \Longrightarrow u \in \mathrm{Root}_{\mathbb{F}_4}(f), -(1+u) = 1+u \in \mathrm{Root}_{\mathbb{F}_4}(f)$$

下面证明 $\mathbb{F}_4 = \mathbb{F}_2(u, 1+u)$，我们有域扩张塔

$$\mathbb{F}_2 \subset \mathbb{F}_2(u) \subset \mathbb{F}_2(u, 1+u) \subset \mathbb{F}_4$$

因为 $\mathbb{F}_4$ 有一组 $\mathbb{F}_2$-基 $\{1, u\}$，所以 $\dim_{\mathbb{F}_2}\mathbb{F}_4 = 2$，又因为 u 在 $\mathbb{F}_2$ 中的最小多项式为 x^2+x+1，次数为 2，所以 $\dim_{\mathbb{F}_2}\mathbb{F}_2(u) = 2$，由维数公式

$$\dim_{\mathbb{F}_2(u)}\mathbb{F}_2(u, 1+u) = \dim_{\mathbb{F}_2(u,1+u)}\mathbb{F}_4 = 1$$

我们证明一个引理：域扩张 K/k 的维数是 1 时，有 $K = k$

首先显然有 $k \subset K$，其次对 $\forall \alpha \in K\backslash k$，我们有 $k \subset k(\alpha) \subset K$，故由维数公式可知 $\dim_k k(\alpha) = 1$，这说明 $k(\alpha)$ 的 k-基为 $\{1\}$，即 $\exists \beta \in k, \text{s.t. } \alpha = \beta \cdot 1$，即 $\alpha = \beta \in k$，这与 $\alpha \in K\backslash k$ 矛盾！故 $K\backslash k = \varnothing$，即 $K = k$

因此 $\mathbb{F}_2(u) = \mathbb{F}_2(u, 1+u) = \mathbb{F}_4$，这就说明 $\mathbb{F}_4/\mathbb{F}_2$ 是 $f(x)$ 在 $\mathbb{F}_2$ 上的分裂域 □

Exercise 12 考虑 $\mathbb{F}_3 \hookrightarrow \mathbb{F}_9 = \mathbb{F}_3[x]/(x^2+1)$，求证 $\mathbb{F}_9/\mathbb{F}_3$ 是 x^2+1 在 $\mathbb{F}_3$ 上的分裂域，也是 x^2+2x+2 在 $\mathbb{F}_3$ 上的分裂域

Proof 记 $f(x) = x^2+1$，因为在 $\mathbb{F}_9$ 中，$u = \bar{x}$ 满足 $f(u) = 0$，所以在 $\mathbb{F}_9$ 中 $f(x)$ *spilt*（见下式）

$$f(x) = (x+u)(x-u) \Longrightarrow u, -u \in \mathrm{Root}_{\mathbb{F}_9}(f)$$

下面证明 $\mathbb{F}_9 = \mathbb{F}_3(u, -u)$，我们有域扩张塔

$$\mathbb{F}_3 \subset \mathbb{F}_3(u) \subset \mathbb{F}_3(u, -u) \subset \mathbb{F}_9$$

因为 $\dim_{\mathbb{F}_3}\mathbb{F}_3(u) = \deg f = 2$，而 $\mathbb{F}_9$ 有一组 $\mathbb{F}_3$-基 $\{1, u\}$，故 $\dim_{\mathbb{F}_3}\mathbb{F}_9 = 2$，由维数公式

$$[\mathbb{F}_9 : \mathbb{F}_3(u, -u)] = [\mathbb{F}_3(u, -u) : \mathbb{F}_3(u)] = 1$$

因此 $\mathbb{F}_3(u)=\mathbb{F}_3(u,-u)=\mathbb{F}_9$，这就说明 $\mathbb{F}_9/\mathbb{F}_3$ 是 $f(x)$ 在 $\mathbb{F}_3$ 上的分裂域

记 $g(x)=x^2+2x+2$，因为在 $\mathbb{F}_9=\mathbb{F}_3/(x^2+1)$ 中，$g(x)$ *spilt*（见下式）

$$g(x)=(x-(u+2))(x+(u+1))\Longrightarrow u+2\in \mathrm{Root}_{\mathbb{F}_9}(g),-u-1=2u+2\in \mathrm{Root}_{\mathbb{F}_9}(g)$$

下面证明 $\mathbb{F}_9=\mathbb{F}_3(u+2,2u+2)$，我们有域扩张塔

$$\mathbb{F}_3\subset\mathbb{F}_3(u+2)\subset\mathbb{F}_3(u+2,2u+2)\subset\mathbb{F}_9$$

因为 $u+2$ 在 $\mathbb{F}_3$ 上的最小多项式为 x^2+2x+2，所以 $\dim_{\mathbb{F}_3}\mathbb{F}_3(u+2)=2$，又因为 $\dim_{\mathbb{F}_3}\mathbb{F}_9=2$，由维数公式

$$[\mathbb{F}_9:\mathbb{F}_3(u+2,2u+2)]=[\mathbb{F}_3(u+2,2u+2):\mathbb{F}_3(u+2)]=1$$

因此 $\mathbb{F}_3(u+2,2u+2)=\mathbb{F}_9$，这就说明 $\mathbb{F}_9/\mathbb{F}_3$ 是 $g(x)$ 在 $\mathbb{F}_3$ 上的分裂域 □

Exercise 13 $E=\mathbb{Q}(\sqrt[3]{2},\omega),\delta_{i,j}\in\mathrm{Aut}(E/\mathbb{Q})=\mathrm{Aut}(E)$，计算 $\delta_{i,j}^{-1}$，并计算 $\mathrm{Aut}(E)$ 的乘法表

Solution 由课上定义，$\sigma_i,i=0,1,2,\delta_{i,j},i=0,1,2;j=1,2$ 分别如下：

$$\begin{aligned}
&\sigma_0:\mathbb{Q}(\sqrt[3]{2})\longrightarrow\mathbb{Q}(\sqrt[3]{2}) && \sigma_1:\mathbb{Q}(\sqrt[3]{2})\longrightarrow\mathbb{Q}(\sqrt[3]{2}\omega) && \sigma_2:\mathbb{Q}(\sqrt[3]{2})\longrightarrow\mathbb{Q}(\sqrt[3]{2}\omega^2)\\
&\quad\sqrt[3]{2}\longmapsto\sqrt[3]{2} && \quad\sqrt[3]{2}\longmapsto\sqrt[3]{2}\omega && \quad\sqrt[3]{2}\longmapsto\sqrt[3]{2}\omega^2\\
&\quad q\longmapsto q,\forall q\in\mathbb{Q} && \quad q\longmapsto q,\forall q\in\mathbb{Q} && \quad q\longmapsto q,\forall q\in\mathbb{Q}
\end{aligned}$$

以下 $E=\mathbb{Q}(\sqrt[3]{2})(\omega)$

$$\begin{aligned}
&\delta_{0,1}:E\longrightarrow E && \delta_{1,1}:E\longrightarrow E && \delta_{2,1}:E\longrightarrow E\\
&\quad\omega\longmapsto\omega && \quad\omega\longmapsto\omega && \quad\omega\longmapsto\omega\\
&\quad q\longmapsto\sigma_0(q),\forall q\in\mathbb{Q}(\sqrt[3]{2}) && \quad q\longmapsto\sigma_1(q),\forall q\in\mathbb{Q}(\sqrt[3]{2}) && \quad q\longmapsto\sigma_2(q),\forall q\in\mathbb{Q}(\sqrt[3]{2})
\end{aligned}$$

$$\begin{aligned}
&\delta_{0,2}:E\longrightarrow E && \delta_{1,2}:E\longrightarrow E && \delta_{2,2}:E\longrightarrow E\\
&\quad\omega\longmapsto\omega^2 && \quad\omega\longmapsto\omega^2 && \quad\omega\longmapsto\omega^2\\
&\quad q\longmapsto\sigma_0(q),\forall q\in\mathbb{Q}(\sqrt[3]{2}) && \quad q\longmapsto\sigma_1(q),\forall q\in\mathbb{Q}(\sqrt[3]{2}) && \quad q\longmapsto\sigma_2(q),\forall q\in\mathbb{Q}(\sqrt[3]{2})
\end{aligned}$$

由于 $E/\mathbb{Q}$ 的一组 $\mathbb{Q}$-基为 $\{1,\omega,\omega^2,\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2\}$，且 $\delta_{i,j}|_{\mathbb{Q}}=\mathrm{Id}_{\mathbb{Q}}$，所以 $\delta_{i,j}$ 完全由这组基所决定，我们只需考虑这组基在 $\delta_{i,j}$ 下的像即可，因为

$$\begin{cases}\delta_{0,1}(1,\omega,\omega^2,\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2)=(1,\omega,\omega^2,\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2)\\ \delta_{0,2}(1,\omega,\omega^2,\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2)=(1,\omega^2,\omega,\sqrt[3]{2},\sqrt[3]{2}\omega^2,\sqrt[3]{2}\omega)\\ \delta_{1,1}(1,\omega,\omega^2,\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2)=(1,\omega,\omega^2,\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2,\sqrt[3]{2})\\ \delta_{1,2}(1,\omega,\omega^2,\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2)=(1,\omega^2,\omega,\sqrt[3]{2}\omega,\sqrt[3]{2},\sqrt[3]{2}\omega^2)\\ \delta_{2,1}(1,\omega,\omega^2,\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2)=(1,\omega,\omega^2,\sqrt[3]{2}\omega^2,\sqrt[3]{2},\sqrt[3]{2}\omega)\\ \delta_{2,2}(1,\omega,\omega^2,\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2)=(1,\omega^2,\omega,\sqrt[3]{2}\omega^2,\sqrt[3]{2}\omega,\sqrt[3]{2})\end{cases}$$

所以

1. $\delta_{0,1}=\mathrm{Id}_{\mathrm{Aut}(E)},\delta_{0,1}^{-1}=\delta_{0,1}$
2. $\delta_{0,2}\circ\delta_{0,2}=\mathrm{Id}_{\mathrm{Aut}(E)},\delta_{0,2}^{-1}=\delta_{0,2}$
3. $\delta_{1,1}\circ\delta_{2,1}=\mathrm{Id}_{\mathrm{Aut}(E)},\delta_{1,1}^{-1}=\delta_{2,1},\delta_{2,1}^{-1}=\delta_{1,1}$
4. $\delta_{1,2}\circ\delta_{1,2}=\mathrm{Id}_{\mathrm{Aut}(E)},\delta_{1,2}^{-1}=\delta_{1,2}$
5. $\delta_{2,2}\circ\delta_{2,2}=\mathrm{Id}_{\mathrm{Aut}(E)},\delta_{2,2}^{-1}=\delta_{2,2}$

$\mathrm{Aut}(E)$ 的乘法表如下（复合时列在左，行在右）

$\circ$	$\delta_{0,1}$	$\delta_{0,2}$	$\delta_{1,1}$	$\delta_{1,2}$	$\delta_{2,1}$	$\delta_{2,2}$
$\delta_{0,1}$	$\delta_{0,1}$	$\delta_{0,2}$	$\delta_{1,1}$	$\delta_{1,2}$	$\delta_{2,1}$	$\delta_{2,2}$
$\delta_{0,2}$	$\delta_{0,2}$	$\delta_{0,1}$	$\delta_{2,2}$	$\delta_{2,1}$	$\delta_{1,2}$	$\delta_{1,1}$
$\delta_{1,1}$	$\delta_{1,1}$	$\delta_{1,2}$	$\delta_{2,1}$	$\delta_{2,2}$	$\delta_{0,1}$	$\delta_{0,2}$
$\delta_{1,2}$	$\delta_{1,2}$	$\delta_{1,1}$	$\delta_{0,2}$	$\delta_{0,1}$	$\delta_{2,2}$	$\delta_{2,1}$
$\delta_{2,1}$	$\delta_{2,1}$	$\delta_{2,2}$	$\delta_{0,1}$	$\delta_{0,2}$	$\delta_{1,1}$	$\delta_{1,2}$
$\delta_{2,2}$	$\delta_{2,2}$	$\delta_{2,1}$	$\delta_{1,2}$	$\delta_{1,1}$	$\delta_{0,2}$	$\delta_{0,1}$

表 1: $\mathrm{Aut}(E)$ 的乘法表

□

Exercise 14 求 $\mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})$

Solution 因为在 $\mathbb{Q}$ 上的自同构只有 $\mathrm{Id}_{\mathbb{Q}}$,所以 $\mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})=\mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3}))$,首先 $|\mathrm{Aut}(E)|\leq\dim_{\mathbb{Q}}\mathbb{Q}(\sqrt{2},\sqrt{3})=4$，考虑

$$\mathbb{Q}\subset\mathbb{Q}(\sqrt{2})\subset\mathbb{Q}(\sqrt{2},\sqrt{3})$$

因为 $\sqrt{2}$ 在 $\mathbb{Q}$ 上的最小多项式为 $f(x)=x^2-2$,而在 $\mathbb{Q}(\sqrt{2},\sqrt{3})$ 上,$f(x)$ 的根集为 $\mathrm{Root}_{\mathbb{Q}(\sqrt{2},\sqrt{3})}(f)=\{\sqrt{2},-\sqrt{2}\}$，所以存在两个 $\mathrm{Id}_{\mathbb{Q}}$ 的延拓

$$\begin{array}{ll}\sigma_0:\mathbb{Q}(\sqrt{2})\longrightarrow\mathbb{Q}(\sqrt{2}) & \sigma_1:\mathbb{Q}(\sqrt{2})\longrightarrow\mathbb{Q}(-\sqrt{2})=\mathbb{Q}(\sqrt{2})\\ \sqrt{2}\longmapsto\sqrt{2} & \sqrt{2}\longmapsto-\sqrt{2}\\ q\longmapsto q,\forall q\in\mathbb{Q} & q\longmapsto q,\forall q\in\mathbb{Q}\end{array}$$

又因为在 $\mathbb{Q}(\sqrt{2})$ 上，$\sqrt{3}$ 的最小多项式为 $g(x)=x^2-3$，而在 $\mathbb{Q}(\sqrt{2},\sqrt{3})$ 上，$g(x)$ 的根集为 $\mathrm{Root}_{\mathbb{Q}(\sqrt{2},\sqrt{3})}(g)=\{\sqrt{3},-\sqrt{3}\}$，所以对每个 $\sigma_i, i=0,1$，存在两个延拓

$$\begin{aligned}\delta_{0,1}:\mathbb{Q}(\sqrt{2},\sqrt{3})&\longrightarrow\mathbb{Q}(\sqrt{2},\sqrt{3})\\ \sqrt{3}&\longmapsto\sqrt{3}\\ q&\longmapsto\sigma_0(q),\forall q\in\mathbb{Q}(\sqrt{2})\end{aligned}\qquad\begin{aligned}\delta_{0,2}:\mathbb{Q}(\sqrt{2},\sqrt{3})&\longrightarrow\mathbb{Q}(\sqrt{2},\sqrt{3})\\ \sqrt{3}&\longmapsto-\sqrt{3}\\ q&\longmapsto\sigma_0(q),\forall q\in\mathbb{Q}(\sqrt{2})\end{aligned}$$

$$\begin{aligned}\delta_{1,1}:\mathbb{Q}(\sqrt{2},\sqrt{3})&\longrightarrow\mathbb{Q}(\sqrt{2},\sqrt{3})\\ \sqrt{3}&\longmapsto\sqrt{3}\\ q&\longmapsto\sigma_1(q),\forall q\in\mathbb{Q}(\sqrt{2})\end{aligned}\qquad\begin{aligned}\delta_{1,2}:\mathbb{Q}(\sqrt{2},\sqrt{3})&\longrightarrow\mathbb{Q}(\sqrt{2},\sqrt{3})\\ \sqrt{3}&\longmapsto-\sqrt{3}\\ q&\longmapsto\sigma_1(q),\forall q\in\mathbb{Q}(\sqrt{2})\end{aligned}$$

所以 $\mathrm{Aut}(\mathbb{Q}(\sqrt{2},\sqrt{3}))=\{\delta_{0,1},\delta_{0,2},\delta_{1,1},\delta_{1,2}\}$，其中 $\delta_{i,j}|_{\mathbb{Q}}=\mathrm{Id}_{\mathbb{Q}},\forall i,j$，且对 $\mathbb{Q}$-基 $\{1,\sqrt{2},\sqrt{3},\sqrt{6}\}$，有

$$\begin{cases}\delta_{0,1}(1,\sqrt{2},\sqrt{3},\sqrt{6})=(1,\sqrt{2},\sqrt{3},\sqrt{6})\\ \delta_{0,2}(1,\sqrt{2},\sqrt{3},\sqrt{6})=(1,\sqrt{2},-\sqrt{3},-\sqrt{6})\\ \delta_{1,1}(1,\sqrt{2},\sqrt{3},\sqrt{6})=(1,-\sqrt{2},\sqrt{3},-\sqrt{6})\\ \delta_{1,1}(1,\sqrt{2},\sqrt{3},\sqrt{6})=(1,-\sqrt{2},-\sqrt{3},\sqrt{6})\end{cases}$$

□

Exercise 15 求 $\mathrm{Aut}(\mathbb{F}_4/\mathbb{F}_2)$

Solution 因为 $\mathbb{F}_2$ 到自身的自同构只能是 $\mathrm{Id}_{\mathbb{F}_2}$，所以 $\mathrm{Aut}(\mathbb{F}_4/\mathbb{F}_2)=\mathrm{Aut}(\mathbb{F}_4)$；由于 *Exercise 11* 中已经证明 $\mathbb{F}_4=\mathbb{F}_2(u)$，其中 u 在 $\mathbb{F}_2$ 上的最小多项式为 $f(x)=x^2+x+1$，而在 $\mathbb{F}_4$ 上，$f(x)$ 的根集 $\mathrm{Root}_{\mathbb{F}_4}(f)=\{u,1+u\}$，所以存在两个 $\mathrm{Id}_{\mathbb{F}_2}$ 的延拓

$$\begin{aligned}\sigma_0:\mathbb{F}_2(u)&\longrightarrow\mathbb{F}_2(u)\\ u&\longmapsto u\\ a&\longmapsto a,\forall a\in\mathbb{F}_2\end{aligned}\qquad\begin{aligned}\sigma_1:\mathbb{F}_2(u)&\longrightarrow\mathbb{F}_2(1+u)=\mathbb{F}_2(u)\\ u&\longmapsto 1+u\\ a&\longmapsto a,\forall a\in\mathbb{F}_2\end{aligned}$$

由于 $\mathbb{F}_4=\mathbb{F}_2(u)$，所以 $\mathrm{Aut}(\mathbb{F}_4)=\{\sigma_0,\sigma_1\}$，其中 $\sigma_i|_{\mathbb{F}_2}=\mathrm{Id}_{\mathbb{F}_2},\forall i$，且对 $\mathbb{F}_2$-基 $\{1,u\}$，有

$$\begin{cases}\sigma_0(1,u)=(1,u)\\ \sigma_1(1,u)=(1,1+u)\end{cases}$$

□