

# 代数 2-H 作业解答



刘博文

Qiuzhen College, Tsinghua University  
2023 Spring

## 目录

第一章 作业解答	2
1.1 第一次作业	2
1.2 第三次作业	6
1.3 第五次作业	9



# 第一章 作业解答

## 1.1 第一次作业

**练习.** 证明  $x^4 + 3x + 3$  是  $\mathbb{Q}[\sqrt[3]{2}]$  上的不可约多项式.

证明: 通过艾森斯坦判别法可知  $x^4 + 3x + 3$  是  $\mathbb{Q}$  上的不可约多项式, 取  $\alpha \in \mathbb{C}$  是其一根, 则  $[\mathbb{Q}[\alpha] : \mathbb{Q}] = 4$ . 另一方面, 由于  $\sqrt[3]{2}$  在  $\mathbb{Q}$  上的极小多项式为  $x^3 - 2$ , 同样根据艾森斯坦判别法可知其在  $\mathbb{Q}$  上不可约, 从而  $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$ . 因此  $3, 4 \mid [\mathbb{Q}[\sqrt[3]{2}, \alpha] : \mathbb{Q}]$ , 即  $[\mathbb{Q}[\sqrt[3]{2}, \alpha] : \mathbb{Q}] \geq 12$ , 即  $[\mathbb{Q}[\sqrt[3]{2}, \alpha] : \mathbb{Q}[\sqrt[3]{2}]] \geq 4$ . 而另一方面, 有

$$[\mathbb{Q}[\sqrt[3]{2}, \alpha] : \mathbb{Q}[\sqrt[3]{2}]] \leq [\mathbb{Q}[\alpha] : \mathbb{Q}] = 4$$

从而  $[\mathbb{Q}[\sqrt[3]{2}, \alpha] : \mathbb{Q}] = 4$ , 并且  $x^4 + 3x + 3$  是  $\alpha$  在  $\mathbb{Q}[\sqrt[3]{2}]$  上的极小多项式, 从而不可约.  $\square$

注记. 证明的关键在于 3, 4 互素, 这里用来确定  $[\mathbb{Q}[\sqrt[3]{2}, \alpha] : \mathbb{Q}]$  的办法在之后还会经常用到.

**练习.** 计算下面的扩张次数

1.  $[\mathbb{Q}[\sqrt{p}, \sqrt{q}] : \mathbb{Q}]$ , 其中  $p, q$  是不同的素数.
2.  $[\mathbb{Q}[\sqrt[3]{2}, \sqrt{2}] : \mathbb{Q}]$ .

证明: (1). 我们断言  $[\mathbb{Q}[\sqrt{p}, \sqrt{q}] : \mathbb{Q}[\sqrt{p}]] = 2$ , 从而  $[\mathbb{Q}[\sqrt{p}, \sqrt{q}] : \mathbb{Q}] = 4$ . 下面我们来证明断言: 若不然, 假设  $\sqrt{q} = a + b\sqrt{p}$ ,  $a, b \in \mathbb{Q}$ , 则

$$q = a^2 + pb^2 + 2ab\sqrt{p}$$

即  $ab = 0$ , 依次分类  $a = 0$  与  $b = 0$  分类讨论得出矛盾即可.

(2). 首先由于  $x^3 - 2$  和  $x^2 - 2$  都是  $\mathbb{Q}$  上的不可约多项式, 从而  $2, 3 \mid [\mathbb{Q}[\sqrt[3]{2}, \sqrt{2}] : \mathbb{Q}]$ . 并且模仿第一题中的论断有

$$[\mathbb{Q}[\sqrt[3]{2}, \sqrt{2}] : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt[3]{2}, \sqrt{2}) : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] \leq 6$$

从而  $[\mathbb{Q}[\sqrt[3]{2}, \sqrt{2}] : \mathbb{Q}] = 6$ .  $\square$

注记. 我们可以给上述的 (2) 另一个更巧妙的证明: 注意到  $\sqrt[6]{2} = (\sqrt{2})(\sqrt[3]{2})^{-1}$ , 而显然有  $\sqrt{2}, \sqrt[3]{2} \in \mathbb{Q}[\sqrt[6]{2}]$ , 从而有  $\mathbb{Q}[\sqrt[3]{2}, \sqrt{2}] = \mathbb{Q}[\sqrt[6]{2}]$ , 即  $[\mathbb{Q}[\sqrt[3]{2}, \sqrt{2}] : \mathbb{Q}] = 6$ .

**练习.** 计算  $\sqrt[3]{2} + \sqrt{3}$  在  $\mathbb{Q}$  上的极小多项式.

证明: 令  $x = \sqrt[3]{2} + \sqrt{3}$ , 则根据  $(x - \sqrt{3})^2 = 2$  可得

$$x^2 + 9x - 2 = \sqrt{3}(3x^2 + 3)$$

即  $\sqrt{3} \in \mathbb{Q}(\sqrt[3]{2} + \sqrt{3})$ , 从而  $\mathbb{Q}(\sqrt[3]{2} + \sqrt{3}) = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3})$ . 利用之前同样的论断可知  $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}) : \mathbb{Q}] = 6$ , 即  $x$  的极小多项式次数为 6. 平方上述关于  $x$  的等式可知

$$x^6 - 9x^4 - 4x^3 + 27x^2 - 36x - 23 = 0$$

从而上述多项式就是  $x$  的极小多项式. □

**练习.** 在同构的意义下分类  $\mathbb{Q}$  的所有二次扩张.

证明: 根据课上的结果, 我们有  $\mathbb{Q}$  的所有二次扩张都形如  $\mathbb{Q}[\sqrt{d}]$ ,  $d \in \mathbb{Q}$ , 通过乘以  $\mathbb{Q}$  中可逆元的操作我们不妨假设  $d \in \mathbb{Z} \setminus \{0, 1\}$  且  $d$  无平方因子, 下面我们断言对于不同的  $d_1, d_2$ , 有  $\mathbb{Q}[\sqrt{d_1}]$  与  $\mathbb{Q}[\sqrt{d_2}]$  不同构, 从而给出  $\mathbb{Q}$  上所有二次扩张的分类. 假设  $\sqrt{d_1} \in \mathbb{Q}[\sqrt{d_2}]$ , 那么存在  $a, b \in \mathbb{Q}$  使得  $(a + b\sqrt{d_2})^2 = d_1$ , 即

$$a^2 + d_2b^2 + 2ab\sqrt{d_2} = d_1$$

从而  $ab = 0$ , 再根据  $a = 0$  或  $b = 0$  分类讨论得出矛盾即可. □

注记. 这与第二题的 (1) 的证明思路一致.

**练习.** 假设域  $F$  的特征为 2,  $K$  是  $F$  的二次扩张, 证明要么  $K = F[\alpha], \alpha^2 \in F, \alpha \notin F$ , 或者  $K = F[\alpha], \alpha^2 - \alpha \in F, \alpha \notin F$ . 这两种情况可能同构吗?

证明: 取  $\beta \in K$  使得  $\{1, \beta\}$  构成了  $K$  的一组  $F$ -基, 则存在  $a, b \in F$  使得  $\beta^2 + a\beta + b = 0$ , 则考虑如下两种情况:

1. 若  $a \neq 0$ , 则  $\frac{\beta^2}{-a^2} + \frac{\beta}{-a} + \frac{b}{-a^2} = 0$ , 即  $(\frac{\beta}{a})^2 - \frac{\beta}{a} \in F$ , 且  $\{1, \frac{\beta}{a}\}$  是一组  $F$ -基, 为第一种情况.
2. 若  $a = 0$ , 则  $\beta^2 \in F$ , 为第二种情况.

并且这两种情况不可能同构: 假设存在  $F$ -同构  $\varphi: F[\alpha] \rightarrow F[\beta]$ , 其中  $\alpha^2 \in F, \beta^2 - \beta \in F, \alpha, \beta \notin F$ . 假设  $\varphi(\alpha) = a + b\beta \in F[\beta]$ ,  $a, b \in F, b \neq 0$ . 根据特征为 2 有

$$\alpha^2 = \varphi(\alpha^2) = (a + b\beta)^2 = a^2 + b^2\beta^2$$

从而

$$\beta = \frac{\alpha^2 - a^2}{b^2} \in F$$

矛盾. □

**练习.** 在同构意义下分类  $\mathbb{F}_2(x)$  的所有二次扩张.

证明: 根据上一题的结果,  $\mathbb{F}_2(x)$  的所有二次扩张有如下的两种情况:

1.  $\mathbb{F}_2(x)[t]/(t^2 - u)$ , 其中  $u \in \mathbb{F}_2(x)$ .
2.  $\mathbb{F}_2(x)[t]/(t^2 - t - d)$ , 其中  $d \in \mathbb{F}_2(x)$ .

下面我们要将这两种情况再详细地描述:



1. 由于  $t^2 \in \mathbb{F}_2(x)$ , 不妨找  $f \in \mathbb{F}_2(x)$  使得  $(ft)^2 \in \mathbb{F}_2[x]$ , 并且考虑分解  $(ft)^2 = g_1(x) + xg_2(x)$ , 其中  $g_1(x), g_2(x) \in \mathbb{F}_2[x]$  只有偶次项, 那么由于  $\mathbb{F}_2$  的特征为 2, 上述分解等价于

$$(ft - \sqrt{g_1})^2 = xg_2(x) \iff \left(\frac{ft}{\sqrt{g_2}} - \frac{\sqrt{g_1}}{\sqrt{g_2}}\right)^2 = x$$

其中如果  $g = \sum_k a_k x^{2k}$ , 则  $\sqrt{g} := \sum_k a_k x^k$ , 因此第一种情况等价于向  $\mathbb{F}_2(x)$  中添加  $\sqrt{x}$ , 即第一种情况为  $\mathbb{F}_2(\sqrt{x})$ .

2. 令  $G = \{f^2 - f \in \mathbb{F}_2(x) \mid f \in \mathbb{F}_2(x)\}$ , 我们断言  $\mathbb{F}_2(x)[t]/(t^2 - t - d_1) \cong \mathbb{F}_2(x)[t]/(t^2 - t - d_2)$  当且仅当  $d_1 - d_2 \in G$ : 如果有  $\mathbb{F}_2(x)$ -同构  $\varphi: \mathbb{F}_2(x)[t]/(t^2 - t - d_1) \rightarrow \mathbb{F}_2(x)[t]/(t^2 - t - d_2)$ , 设  $\varphi(t) = a + bt, a, b \in \mathbb{F}_2(x), b \neq 0$ , 那么

$$d_1 = \varphi(d_1) = \varphi(t^2 - t) = a^2 + b^2 t^2 - a - bt = (b^2 - b)t + a^2 - a + b^2 d_2$$

从而对照系数则有

$$\begin{cases} b^2 - b = 0 \\ d_1 = a^2 - a + b^2 d_2 \end{cases}$$

注意到  $b \neq 0$ , 从而  $b = 1$ , 进而  $d_1 - d_2 = a^2 - a \in G$ . 另一方面, 如果  $d_1 - d_2 \in G$ , 假设  $d_1 = d_2 + f^2 - f, f \in \mathbb{F}_2[x]$ , 考虑

$$\begin{aligned} \varphi: \mathbb{F}_2(x)[t]/(t^2 - t - d_1) &\rightarrow \mathbb{F}_2(x)[t]/(t^2 - t - d_2) \\ a + bt &\mapsto a + bf + bt \end{aligned}$$

则  $\varphi$  给出了一个  $\mathbb{F}_2(x)$ -同构.

□

**练习.** 正九边形能否通过尺规作图得到?

证明: 不可以, 直接验证  $\cos(2\pi/9)$  不可构造.

□

注记. 尺规可做正  $n$  边形当且仅当  $n = 2^k p_1 \dots p_s$ , 其中  $p_i, 1 \leq i \leq s$  是费马素数, 可直接验证 9 不是如上形式的数.

**练习.** 计算

- $f(x) = x^5 - 2$  的分裂域在  $\mathbb{Q}$  上的扩张次数.
- $f(x) = x^p - x - 1$  的分裂域在  $\mathbb{F}_p$  上的扩张次数.

证明: (1). 不难发现  $\mathbb{Q}[\sqrt[5]{2}, \xi_5]$  是  $x^5 - 2$  的分裂域, 其中  $\xi_5$  是五次单位根. 由于  $x^5 - 2$  是不可约多项式, 从而  $[\mathbb{Q}[\sqrt[5]{2}]: \mathbb{Q}] = 5$ , 同样的, 由于  $x^5 - 1/(x-1)$  是不可约多项式, 从而  $[\mathbb{Q}[\xi_5]: \mathbb{Q}] = 4$ , 即  $[\mathbb{Q}[\sqrt[5]{2}, \xi_5]: \mathbb{Q}] \geq 20$ . 另一方面, 用第一题中的论断可以同样的证明  $[\mathbb{Q}[\sqrt[5]{2}, \xi_5]: \mathbb{Q}] \leq 20$ , 从而  $[\mathbb{Q}[\sqrt[5]{2}, \xi_5]: \mathbb{Q}] = 20$ .

(2). 由于我们已经知道  $x^p - x - 1$  在  $\mathbb{F}_p$  上不可约的, 从而  $K = \mathbb{F}_p[x]/(x^p - x - 1)$  是  $p$  次扩张, 并且包含  $x^p - x - 1 = 0$  的一个根, 而如果  $K$  包含其一个根  $\alpha$ , 则  $\alpha, \alpha + 1, \dots, \alpha + p - 1$  给出了所有的根, 即  $K$  是  $x^p - x - 1$  的分裂域, 从而分裂域在  $\mathbb{F}_p$  上的扩张次数为  $p$ . □

注记. 形如  $x^p - x - a, a \in \mathbb{F}_p$  的多项式被称为 Artin Schreier 多项式.

**练习.** 令  $K$  是  $n$  次多项式  $f(x)$  在  $F$  上的分裂域, 证明  $[K : F] \mid n!$ , 能否对每一个  $n$  都举出一个例子?

证明: 证明见讲义分裂域存在性定理, 而对于每一个  $n$  的例子, 答案依赖于  $F$  的选取: 例如当  $\mathbb{F} = \mathbb{R}$  的时候, 其上最多只有二次扩张, 从而不会对任意的  $n$  成立. 而  $F = \mathbb{Q}$  的时候, 之后我们会证明如下定理:

**定理 1.1.1.** 对于  $n \geq 1$ , 存在一个  $\mathbb{Q}$  上的  $n$  次不可约多项式, 使得其 Galois 群为  $S_n$ .

从而根据 Galois 对应, 可知此时分裂域的扩张次数为  $n!$ . □

**练习.** 判断如下三个域是否同构

1.  $x^2 - t^3 \in \mathbb{Q}(t)$  的分裂域.
2.  $x^2 - t^5 \in \mathbb{Q}(t)$  的分裂域.
3.  $x^2 + t^2 \in \mathbb{Q}(t)$  的分裂域.

证明: 由于上述三个多项式都在  $\mathbb{Q}(t)$  上不可约, 并且若  $\alpha$  是其根, 则  $-\alpha$  也是其根, 从而  $\mathbb{Q}(t)[x]/(x^2 - t^3), \mathbb{Q}(t)[x]/(x^2 - t^5), \mathbb{Q}(t)[x]/(x^2 + t^2)$  分别是它们的分裂域, 记为  $K_1, K_2, K_3$ . 我们先来证明  $K_1, K_2$  同构, 考虑  $\varphi: K_1 \rightarrow K_2$ , 其限制在  $\mathbb{Q}(t)$  上是恒等, 并且

$$\varphi: x + (x^2 - t^3) \mapsto \frac{x}{t} + (x^2 - t^5)$$

其是良好定义的, 因为  $x^2 - t^3 \mapsto (x/t)^2 - t^3 = (x^2 - t^5)/t^2$ , 并且是满射, 再由于域之间的态射都是单的, 从而给出了  $K_1$  和  $K_2$  之间的同构.

下面来证明  $K_1, K_3$  不同构, 注意到  $(x/t)^2 + 1 = 0 \in K_3$ , 即方程  $X^2 + 1 = 0$  在  $K_3$  中有解, 现在我们证明这个方程在  $K_1$  中不存在解: 假设存在解, 不妨假设为  $f(t) + g(t)\sqrt{t}$ , 其中  $f(t), g(t) \in \mathbb{Q}(t)$ , 从而

$$(f(t) + g(t)\sqrt{t})^2 + 1 = 0$$

即

$$f^2(t) + g^2(t)t + 2f(t)g(t)\sqrt{t} + 1 = 0$$

这意味着  $f(t)g(t) = 0$ , 再根据  $f(t) = 0$  或  $g(t) = 0$  分类讨论得出矛盾即可. □

注记. 第二题的 (1) 的证明思路再次出现.



## 1.2 第三次作业

**练习.** 令  $K/F$  是代数扩张,  $K_s$  是由在  $F$  上可分的元素组成的中间域, 证明

1.  $K_s/F$  是可分扩张.
2.  $K/K_s$  是纯不可分扩张.
3. 如果  $K/F$  是有限扩张, 那么  $|\text{Hom}_F(K, \bar{F})| = [K_s : F]$ .
4. 如果  $K/F$  是正规扩张, 那么  $K_s/F$  是正规扩张.

证明: (1). 我们已经在课上证明过域扩张是可分扩张当且仅当其由可分元生成, 从而  $K_s/F$  是可分扩张是显然的.

(2). 任取  $\alpha \in K \setminus K_s$ , 考虑其在  $F$  上的极小多项式  $P_{\alpha, F}$ , 是一个不可分的不可约多项式. 假设其不可分次数为  $p^e$ , 那么  $P_{\alpha, F} = P_e(x^{p^e})$ , 其中  $P_e$  是一个可分多项式, 即  $\alpha^{p^e} \in K_s$ , 即  $E/K_s$  是纯不可分扩张.

(3). 见讲义.

(4). 假设不可约多项式  $p(x)$  在  $K_s$  中有一个根, 那么  $p(x)$  是可分多项式. 并且特别地  $p(x)$  在  $K$  中有一个根, 再根据  $K/F$  是正规扩张可知所有的根都在  $K$  中, 并且由  $p(x)$  是可分多项式可知这些根都在  $K_s$  中.  $\square$

**练习.** 证明单扩张  $F(\gamma)/F$ , 只有有限多中间域.

证明: 任取中间域  $F \subseteq L \subseteq F(\gamma)$ , 考虑  $\gamma$  在  $L$  上的极小多项式

$$p_{\gamma, L} = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$$

那么我们断言  $L = F(a_0, \dots, a_{m-1})$ : 首先  $F(a_0, \dots, a_{m-1}) \subseteq L$ , 并且注意到  $[F(\gamma) : L] = m$ , 因此只需要证明  $[F(\gamma) : F(a_0, \dots, a_{m-1})] \leq m$  即可, 而这是由于  $\gamma$  已经被  $F(a_0, \dots, a_{m-1})$  上的一个  $m$  次多项式零化. 从而任何中间域  $L$  都形如  $F(a_0, \dots, a_{m-1})$ , 其中  $x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$  整除  $p_{\gamma, F}$ , 因此这样的多项式只有有限多个, 从而只有有限多个中间域.  $\square$

**练习.** 令  $k$  是特征为  $p \neq 0$  的域, 考虑  $K = k(t, u)$  和  $F = k(t^p, u^p)$ . 证明如果  $F[t + au] = F[t + bu]$  对  $a, b \in k$  成立, 那么  $a = b$ . 从而证明当  $k$  是无限域的时候,  $K/F$  中存在无穷多个中间域.

证明: 假设  $a, b \in k$  满足  $F(t + au) = F(t + bu)$ , 那么这意味着

$$t + au - (t + bu) = (a - b)u \in F(t + au)$$

如果  $a \neq b$ , 那么  $u \in F(t + au)$ , 从而  $F(t + au) = F(t, u) = K$ . 但是由于  $(t + au)^p = t^p + a^p u^p \in F = k(t^p, u^p)$ , 从而  $[F(t + au) : F] \leq p$ . 另一方面,

$$[K(t, u) : F] = [K(t, u) : F(t)][F(t) : F] = p^2$$

相矛盾.  $\square$

练习. 令  $F$  是域, 证明

$$\text{Aut}_F(F(x)) = \{x \mapsto \frac{ax+b}{cx+d} \mid \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0\}$$

以及有群同构  $\text{Aut}_F(F(x)) = \text{PGL}(2, F)$ .

证明: 任取  $\tau \in \text{Aut}_F(F(x))$ , 并且假设  $\tau(x) = f(x)/g(x)$ , 其中  $f, g$  是互素的多项式, 那么根据第二次作业中

$$[F(x) : F(\frac{f(x)}{g(x)})] = \max\{\deg f, \deg g\}$$

可知  $\deg f = \deg g = 1$ , 因此不妨假设

$$\tau(x) = \frac{ax+b}{cx+d}$$

其中  $ax+b$  与  $cx+d$  互素等价于

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0$$

因此有集合间的满射

$$\Phi: \{x \mapsto \frac{ax+b}{cx+d} \mid \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} \neq 0\} \rightarrow \text{Aut}_F(F(x))$$

下面我们来计算映射的核, 若

$$\frac{a_1x+b_1}{c_1x+d_1} = \frac{a_2x+b_2}{c_2x+d_2}$$

那么存在  $\lambda \in F^\times$  使得  $a_1 = \lambda a_2, b_1 = \lambda b_2$ , 即  $\ker \Phi \cong \{\lambda I_2 \mid \lambda \in F^\times\}$ , 从而有集合间的同构

$$\Phi: \text{PGL}(2, F) \rightarrow \text{Aut}_F(F(x))$$

下面验证有作为群的同构: 假设

$$\begin{aligned} \tau_1(x) &= \frac{a_1x+b_1}{c_1x+d_1} \\ \tau_2(x) &= \frac{a_2x+b_2}{c_2x+d_2} \end{aligned}$$

只需验证  $\tau_2 \circ \tau_1$  对应的矩阵由

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} = \begin{pmatrix} a_1a_2+b_1c_2 & a_1b_2+b_1d_2 \\ c_1a_2+d_1c_2 & c_1b_2+d_1d_2 \end{pmatrix}$$

给出, 直接计算即可. □

练习. 考虑  $\mathbb{C}(x)$  的  $\mathbb{C}$ -自同构  $\sigma: x \mapsto \frac{1}{x}$  和  $\tau: x \mapsto e^{\frac{2\pi\sqrt{-1}}{n}}x$ , 证明由  $\sigma$  和  $\tau$  生成的群  $H$  是有限群, 并指出是哪个你熟知的有限群, 最后计算  $\mathbb{C}(x)^H$ .

证明: 直接计算有

$$\begin{aligned} \sigma^2 &= I \\ \tau^n &= I \\ \sigma\tau\sigma^{-1} &= \tau^{-1} \end{aligned}$$



因此  $H \cong D_n$ . 令  $y = x^n + \frac{1}{x^n}$ , 我们断言  $\mathbb{C}(x)^H = \mathbb{C}(y)$ : 一方面显然有  $\mathbb{C}(y) \subseteq \mathbb{C}(x)^H$ , 另一方面根据第二次作业可知

$$[\mathbb{C}(x) : \mathbb{C}(y)] = 2n$$

而根据阿廷引理可知  $[\mathbb{C}(x) : \mathbb{C}(x)^H] = 2n$ , 从而  $\mathbb{C}(x)^H = \mathbb{C}(y)$ .  $\square$

**练习.** 令  $F$  是域, 找出  $\text{Aut}_F F(x_1, \dots, x_n)$  中同构于  $\text{PGL}(n+1, F)$  的子群, 并在  $n \geq 2$  时找出一个不在这个群中的元素.

证明: 考虑如下映射

$$\begin{aligned} \Phi: \text{GL}(n+1, F) &\rightarrow \text{Aut}_F F(x_1, \dots, x_n) \\ (a_{ij})_{(n+1) \times (n+1)} &\mapsto \{x_i \mapsto \frac{\sum_{j=1}^n a_{ij}x_j + a_{i,n+1}}{\sum_{j=1}^n a_{n+1,j}x_j + a_{n+1,n+1}}\} \end{aligned}$$

直接计算可知  $\Phi$  是一个群同态, 并且  $\ker \Phi \cong \{\lambda I_{n+1} \mid \lambda \in F^\times\}$ , 从而有单嵌入  $\Phi: \text{PGL}(n+1, F) \rightarrow \text{Aut}_F(F(x_1, \dots, x_n))$ . 当  $n \geq 2$  的时候, 考虑  $\sigma \in \text{Aut}_F F(x_1, \dots, x_n)$ , 其中  $\sigma(x_1) = x_1 + x_2^2$ , 并且  $i \geq 2$  的时候  $\sigma(x_i) = x_i$ .  $\square$

**练习.** 证明  $F$  是完美域当且仅当  $F$  所有的有限扩张都是可分扩张.

证明: 如果  $F$  是完美域, 那么  $F[x]$  中任何不可约多项式都是可分多项式, 特别地, 假设  $E/F$  是有限扩张, 任取  $\alpha \in E$ , 其在  $F$  上的极小多项式也是可分的, 从而  $E/F$  是可分扩张. 另一方面, 任取  $F$  上的不可约多项式  $p(x)$ , 考虑其分裂域  $E/F$ , 是有限扩张. 根据假设其为可分扩张, 从而  $p(x)$  是可分多项式.  $\square$

**练习.** 令  $K/F$  是有限扩张, 证明  $|\text{Aut}_F(K)|$  整除  $[K : F]$ .

证明: 注意到有域扩张

$$F \subseteq K^{\text{Aut}_F(K)} \subseteq K$$

并且阿廷引理表明

$$[K : K^{\text{Aut}_F(K)}] = |\text{Aut}_F(K)|$$

从而  $|\text{Aut}_F(K)|$  整除  $[K : F]$ .  $\square$

**练习.** 令  $F$  是特征为  $p \neq 0$  的域,  $K/F$  是有限扩张, 证明  $K/F$  可分当且仅当  $FK^p = K$ .

证明: 假设  $K/F$  可分, 由于  $F \subseteq FK^p \subseteq K$ , 从而  $K/FK^p$  可分. 任取  $\alpha \in K$ ,  $\alpha$  满足  $FK^p$  上的多项式  $x^p - \alpha^p$ , 从而由可分性可知  $\alpha \in FK^p$ , 即  $K = FK^p$ . 另一方面, 考虑域扩张  $F \subseteq K_s \subseteq K$ , 由于  $K/K_s$  是纯不可分扩张, 则任取  $\alpha \in K$ , 总存在  $m \geq 0$  使得  $\alpha^{p^m} \in K_s$ , 但是  $FK^p = K$  意味着对任意的  $m \geq 0$  有  $FK^{p^m} = K$ , 从而  $K = K_s$ , 即  $K/F$  是可分扩张.  $\square$



## 1.3 第五次作业

**练习.** 令  $p, q$  是素数,  $G$  是  $pq$  阶群, 证明  $G$  是可解的.

证明: 不妨假设  $p \leq q$ , 假设其西罗  $q$  子群的个数为  $n$ , 那么  $n \equiv 1 \pmod{q}$  以及  $n \mid p$  意味着  $n = 1$ , 从而西罗  $q$  子群  $H$  正规, 从而有

$$\{e\} \triangleleft H \triangleleft G$$

其中  $G/H$  是  $p$  阶循环群, 从而  $G$  可解. □

**练习.** 找到最小的  $n$ , 使得存在一个  $n$  阶不可解群.

证明: 注意到  $A_5$  是最小阶数的非交换单群, 任取阶数小于 60 的群  $G$ , 如果其是交换群, 自然可解. 如果其不是交换群, 那么其不是单群, 考虑其极大正规子群  $N$ , 则  $G/N$  是交换单群, 并且  $N$  的阶数严格比  $G$  小, 从而做归纳法即可. □

**练习.** 令  $f \in F[x]$  是  $n$  次多项式, 其根为  $\alpha_1, \dots, \alpha_n$ , 定义其判别式  $D(f) = \prod_{i < j} (\alpha_i - \alpha_j)^2$ .  $G_f$  在  $\{\alpha_1, \dots, \alpha_n\}$  上的作用诱导了单同态  $\rho: G_f \rightarrow S_n$ . 证明  $\rho$  的像在  $A_n$  中当且仅当  $D(f)$  是  $F$  中的平方数, 并且在  $n = 2, 3$  的时候用  $f$  的系数计算  $D(f)$ .

证明: 任取  $\sigma \in G_f \subseteq S_n$ , 有

$$\sigma \Delta(f) = (-1)^{\text{sign}(\sigma)} \Delta(f)$$

因此  $\sigma \Delta(f) = \Delta(f)$  当且仅当  $\sigma \in A_n$ .  $D(f)$  的具体表达式在  $n = 2, 3$  的时候如下

1.  $f(x) = x^2 + ax + b$ , 则  $D(f) = b^2 - 4c$ .
2.  $f = x^3 + px + q$ , 则  $D(f) = -4p^3 - 27q^2$ .

□

**练习.** 给定 3 次可分不可约多项式  $f(x) \in F[x]$ , 讨论如何去决定  $G_f$ .

证明: 假设  $\alpha_1, \alpha_2, \alpha_3$  是  $f(x)$  的三个根, 考虑如下的情况:

1. 如果  $\{\alpha_1, \alpha_2, \alpha_3\}$  都在  $F$  中, 那么  $G_f = \{e\}$ .
2. 如果  $\alpha_1 \in F, \alpha_2, \alpha_3 \notin F$ , 那么  $G_f = \mathbb{Z}/2\mathbb{Z}$ , 其中生成元把  $\alpha_2, \alpha_3$  置换.
3. 如果  $\alpha_1, \alpha_2, \alpha_3 \notin F$ , 根据上一题的结果,  $D(f) \in F^2$  时  $G_f = \mathbb{Z}/3\mathbb{Z}$ , 否则  $G_f = S_3$ .

□

**练习.** 令  $f(x) \in \mathbb{Q}[x]$  是一个既有实根也有非实根的不可约多项式. 证明  $G_f$  非交换, 如果去掉  $f$  不可约的条件命题是否还成立?

证明: 假设  $r \in \mathbb{R}, z \notin \mathbb{R}$  是  $f(x) = 0$  的根, 由于  $f(x)$  不可约, 从而存在  $\sigma \in G_f$  使得  $\sigma(r) = z$ , 另一方面  $\tau(z) = \bar{z}$  也是  $G_f$  中的元素, 注意到

$$\tau \sigma(r) = \bar{z}$$

$$\sigma \tau(r) = z$$

从而  $\sigma \tau \neq \tau \sigma$ , 进而  $G_f$  不交换. 并且  $f$  不可约的条件不能去掉, 例如考虑  $f(x) = (x^2 + 1)(x^2 - 2)$ . □



**练习.** 令  $f(x) = x^5 + ax + b \in \mathbb{Q}[x]$ , 证明  $G_f \cong D_5$  当且仅当

1.  $f(x) \in \mathbb{Q}[x]$  不可约.
2.  $D(f) = 4^4 a^5 + 5^5 b^4$  是平方数.
3.  $f(x) = 0$  根式可解.

证明: 如果  $f(x)$  满足如上条件, 则  $G_f$  是可解群, 并且是包含在  $A_5$  中的可迁子群. 分析  $f(x)$  的根可知其既存在实根也存在虚根, 从而  $G_f$  是非交换群. 假设  $H$  是  $A_5$  的子群, 考虑  $A_5$  在陪集  $\{gH\}_{g \in A_5}$  上的作用, 由于  $A_5$  是单群, 从而上述作用诱导的群同态

$$\rho: A_5 \rightarrow S_{|G/H|}$$

是单射, 即  $|G/H|! \geq 60$ , 从而  $H$  的阶数  $\leq 12$ . 并且由于 5 整除  $|G_f|$ , 从而  $|G_f|$  可能的取值只有 5, 10, 依次如下考虑

1.  $|G_f| = 5$ , 此时是交换群, 矛盾.
2.  $|G_f| = 10$ , 此时可能的情况有  $G_f = \mathbb{Z}/10\mathbb{Z}, D_5$ , 并且由于是非交换群从而此时  $G_f = D_5$ . 从而  $G_f \cong D_5$ .

另一方面, 如果  $G_f \cong D_5$ , 首先  $D_5$  中存在五阶元, 从而  $G_f$  是可迁的, 从而  $f(x)$  是不可约的. 并且由于  $D_5$  是可解群, 从而  $f(x) = 0$  根式可解. 而直接验证则有  $D_5 \subset A_5$ , 即  $D(f)$  是平方数.  $\square$

**练习.** 找一个四次扩张  $E/F$  使得其不存在中间域  $F \subset M \subset E$  满足  $[M:F] = 2$ .

证明: 考虑伽罗瓦群为  $S_4$  的伽罗瓦扩张  $E/\mathbb{Q}$ , 令  $F = E^{S_3}$ , 根据阿廷引理可知  $[E:F] = 4$  是伽罗瓦扩张. 若存在  $F \subset M \subset E$  满足  $[M:F] = 2$ , 那么根据伽罗瓦对应可知  $\text{Gal}(E/M) = A_4$ , 但  $S_3$  不是  $A_4$  的子群, 矛盾.  $\square$

**练习.** 令  $F/\mathbb{Q}$  是伽罗瓦扩张, 令  $\{\alpha = \alpha_1, \dots, \alpha_n\}$  是  $\alpha$  在  $\text{Gal}(F/\mathbb{Q})$  作用下的轨道. 证明:

1.  $F(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_n})/F$  是伽罗瓦扩张, 并且伽罗瓦群是  $(\mathbb{Z}/2\mathbb{Z})^n$  的子群.
2.  $F(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_n})/\mathbb{Q}$  是伽罗瓦扩张, 并且伽罗瓦群是  $(\mathbb{Z}/2\mathbb{Z})^n \rtimes \text{Gal}(F/\mathbb{Q})$  的非交换子群.

证明: 为了符号的简便, 记  $K = F(\sqrt{\alpha_1}, \dots, \sqrt{\alpha_n})$ .

- (1). 注意到任取  $1 \leq i \leq n$ ,  $F(\sqrt{\alpha_i})/F$  是二次伽罗瓦扩张, 从而  $K/F$  是伽罗瓦扩张, 并且

$$\text{Gal}(K/F) \hookrightarrow \prod_{i=1}^n \text{Gal}(F(\sqrt{\alpha_i})/F) = (\mathbb{Z}/2\mathbb{Z})^n$$

- (2). 考虑  $f(x) = (x^2 - \alpha_1) \dots (x^2 - \alpha_n)$ , 任取  $\sigma \in \text{Gal}(F/\mathbb{Q})$ , 由于  $\alpha_1, \dots, \alpha_n$  是  $\alpha$  在  $\text{Gal}(F/\mathbb{Q})$  下的轨道, 从而

$$\sigma(f(x)) = f(x)$$

从而  $f(x) \in \mathbb{Q}[x]$ . 假设  $E$  是  $f(x) \in \mathbb{Q}[x]$  的分裂域, 则  $EF = K$ , 从而  $K/\mathbb{Q}$  是伽罗瓦扩张, 因为  $E/\mathbb{Q}, F/\mathbb{Q}$  都是伽罗瓦扩张. 任取  $\tau \in \text{Gal}(K/\mathbb{Q})$ , 由于  $F/\mathbb{Q}$  是伽罗瓦扩张, 从而  $\tau(F) \subseteq F$ , 假设

$$\tau(\alpha_i) = \alpha_j$$

从而

$$\tau(\sqrt{\alpha_i}) = a_i \sqrt{\alpha_j}$$

其中  $a_i = \pm 1$ , 因此有群同态

$$\begin{aligned} \rho_1: \text{Gal}(K/\mathbb{Q}) &\rightarrow (\mathbb{Z}/2\mathbb{Z})^n & \rho_2: \text{Gal}(K/\mathbb{Q}) &\rightarrow \text{Gal}(F/\mathbb{Q}) \\ \tau &\mapsto (a_i)_{i=1}^n & \tau &\mapsto \tau|_F \end{aligned}$$

记  $\text{Gal}(F/\mathbb{Q})$  在  $\alpha_1, \dots, \alpha_n$  上作用诱导的同态为  $\rho$ , 对  $\varphi \in \text{Gal}(F/\mathbb{Q}), \psi \in (\mathbb{Z}/2\mathbb{Z})^n$ , 定义

$$\varphi(\psi) := \rho(\varphi)(\psi)$$

直接计算有

$$\begin{aligned} \rho_1(\tau\tau') &= \rho_1(\tau')\rho_2(\tau')(\rho_1(\tau)) \\ \rho_2(\tau\tau') &= \rho_2(\tau)\rho_2(\tau') \end{aligned}$$

因此有群同态

$$\begin{aligned} \text{Gal}(K/\mathbb{Q}) &\rightarrow (\mathbb{Z}/2\mathbb{Z})^n \rtimes \text{Gal}(F/\mathbb{Q}) \\ \tau &\mapsto (\rho_1(\tau), \rho_2(\tau)) \end{aligned}$$

并且由于  $\rho_1(\tau), \rho_2(\tau)$  完全决定了  $\tau$ , 从而上述同态还是单同态. 并且直接计算可知  $\tau\tau' = -\tau'\tau$ , 从而是  $(\mathbb{Z}/2\mathbb{Z})^n \rtimes \text{Gal}(F/\mathbb{Q})$  的非交换子群.  $\square$

**练习.** 假设  $F$  中有  $n$  次单位根, 任取素数  $p \mid n$ ,  $a \in F$  在  $F$  中没有  $p$  次根, 证明  $x^n - a$  在  $F[x]$  中不可约.

证明: 假设  $\alpha$  是  $x^n - a = 0$  的一个根, 由于  $F$  中有  $n$  次单位根  $\xi_n$ , 那么  $x^n - a$  的所有根为  $\{\alpha, \alpha\xi_n, \dots, \alpha\xi_n^{n-1}\}$ . 假设  $x^n - a$  在  $F[x]$  中可约, 不妨假设  $g \mid f$ , 那么

$$g(x) = (x - \alpha\xi_n^{a_1}) \dots (x - \alpha\xi_n^{a_k}) \in F[x]$$

从而  $\alpha^k \in F$ , 即  $(\alpha^k)^{\frac{n}{k}} \in F$ . 任取  $p \mid \frac{n}{k}$  有  $\alpha \in F^p$ , 相矛盾.  $\square$

**练习.** 描述  $x^8 - 2 \in \mathbb{Q}[x]$  的伽罗瓦群, 并找出所有的中间域.

证明:  $f(x) = x^8 - 2 \in \mathbb{Q}[x]$  的分裂域为  $\mathbb{Q}(\sqrt[8]{2}, i)$ , 考虑

$$\sigma: \begin{cases} \sqrt[8]{2} \mapsto \sqrt[8]{2}\xi_8 \\ i \mapsto i \end{cases} \quad \tau: \begin{cases} \sqrt[8]{2} \mapsto \sqrt[8]{2} \\ i \mapsto -i \end{cases}$$

直接计算有

$$G_f = \langle \sigma, \tau \mid \sigma^8 = \tau^2 = e, \tau\sigma\tau^{-1} = \sigma^3 \rangle$$

考虑如下四种情况:

1.  $H \cap \langle \sigma \rangle = \{e\}$ , 此时  $H = \langle \tau, \langle \tau\sigma^2 \rangle, \langle \tau\sigma^4 \rangle, \langle \tau\sigma^6 \rangle, \{e\} \rangle$ , 对应的中间域分别为  $\mathbb{Q}(\sqrt[8]{2}), \mathbb{Q}(\sqrt[8]{2}(1+i)), \mathbb{Q}(\sqrt[8]{2}i), \mathbb{Q}(\sqrt[8]{2}(1-i)), \mathbb{Q}(\sqrt[8]{2}, i)$ .
2.  $H \cap \langle \sigma \rangle = \langle \sigma \rangle$ , 此时  $H = \langle \sigma, \langle \sigma, \tau \rangle \rangle$ , 对应的中间域分别为  $\mathbb{Q}[i], \mathbb{Q}$ .
3.  $H \cap \langle \sigma \rangle = \langle \sigma^2 \rangle$ , 此时  $H = \langle \sigma^2, \langle \sigma^2, \tau \rangle, \langle \sigma^2, \tau\sigma \rangle \rangle$ , 对应的中间域分别为  $\mathbb{Q}(\sqrt{2}, i), \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{2}i)$ .



4.  $H \cap \langle \sigma \rangle = \langle \sigma^4 \rangle$ , 此时  $H = \langle \sigma^4 \rangle, \langle \sigma^4, \tau \rangle, \langle \sigma^4, \tau\sigma \rangle, \langle \sigma^4, \tau\sigma^2 \rangle, \langle \sigma^4, \tau\sigma^3 \rangle$ , 对应的中间域分别为  $\mathbb{Q}(\sqrt[4]{2}, i), \mathbb{Q}(\sqrt[4]{2}), \mathbb{Q}(\sqrt[4]{2}(1+i)), \mathbb{Q}(\sqrt[4]{2}i), \mathbb{Q}(\sqrt[4]{2}(1-i))$ .

□

**练习.** 找出  $\text{Aut}_{\mathbb{Q}}(\mathbb{C})$  中复共轭的中心化子.

证明: 假设  $\sigma \in \text{Aut}_{\mathbb{Q}}(\mathbb{C})$  落在复共轭的中心化子中, 即  $\sigma(\bar{z}) = \overline{\sigma(z)}$ , 特别地可知  $\sigma(\mathbb{R}) \subseteq \mathbb{R}$ , 即  $\sigma|_{\mathbb{R}} \in \text{Hom}_{\mathbb{Q}}(\mathbb{R}, \mathbb{R})$ , 从而  $\sigma|_{\mathbb{R}} = \text{id}$ , 从而  $\sigma$  完全由  $\sigma(i)$  决定, 注意到

$$-\sigma(i) = \overline{\sigma(i)}$$

因此  $|\sigma(i)|^2 = -1$ , 因此  $\sigma(i) = \pm i$ , 即复共轭的中心化子为恒等映射以及复共轭.

□

