《伽罗瓦理论》参考答案

胡维

Jan 2025

目录

第二章　域的扩张

习题 2.1

假设 L/K 为域扩张且 $[L:K]$ 为素数。证明：L/K 没有非平凡的中间域。

证明. 假设 M 为 L/K 的中间域，则有

$$[L:M]\cdot[M:K]=[L:K]$$

为素数。由于 $[L:M]$ 和 $[M:K]$ 都是正整数，因此 $[L:M]=1$ 或 $[M:K]=1$。从而 $M=L$ 或者 $M=K$. □

习题 2.2

令 $L=\mathbb{Q}(\sqrt{3},\omega)$, 其中

$$\omega=-\frac{1}{2}+\frac{\sqrt{3}}{2}i$$

是 3 次单位根。计算 $[L:\mathbb{Q}]$ 并找出 L 作为 $\mathbb{Q}$ 向量空间的一组基。

解: 我们有域扩张链

$$\mathbb{Q}\subset\mathbb{Q}(\sqrt{3})\subset\mathbb{Q}(\sqrt{3})(\omega)=L$$

由于 $\sqrt{3}$ 在 $\mathbb{Q}$ 上的极小多项式为 x^2-3, 因此 $[\mathbb{Q}(\sqrt{3}):\mathbb{Q}]=2$. 同时，$\omega\notin\mathbb{Q}(\sqrt{3})$, 因此

$$[\mathbb{Q}(\sqrt{3},\omega):\mathbb{Q}(\sqrt{3})]>1.$$

另一方面，ω 是多项式 x^2+x+1 的根，这说明

$$[\mathbb{Q}(\sqrt{3},\omega):\mathbb{Q}(\sqrt{3})]\leqslant 2.$$

所以

$$[\mathbb{Q}(\sqrt{3},\omega):\mathbb{Q}(\sqrt{3})]=2.$$

从而

$$[L:\mathbb{Q}]=[L:\mathbb{Q}\sqrt{3}]\cdot[\mathbb{Q}(\sqrt{3}):\mathbb{Q}]=4.$$

L 作为 $\mathbb{Q}$ 的一组基:

$$1,\ \sqrt{3},\ \omega,\ \sqrt{3}\omega.$$

实际上，$1,\sqrt{3}$ 是 $\mathbb{Q}(\sqrt{3})$ 作为 $\mathbb{Q}$ 空间的一组基; $1,\omega$ 是 L 作为 $\mathbb{Q}(\sqrt{3})$ 空间的一组基。根据有限扩张链的基的构造方式可得以上基。 □

习题 2.3

设 $f(x)=x^3-3\in\mathbb{Q}[x]$，$u\in\mathbb{C}$ 是 $f(x)$ 的一个根。证明 $\mathbb{Q}(u)$ 不是 $f(x)$ 在 $\mathbb{Q}$ 上的分裂域。

证明. $f(x)$ 的三个根为 $u,\omega u,\omega^2u$, 其中 ω 为第 2 题中的三次单位根。因此 $f(x)$ 在 $\mathbb{Q}$ 上分裂域

$$E=\mathbb{Q}(u,\omega).$$

如果 $E=\mathbb{Q}(u)$，则有 $\omega\in\mathbb{Q}(u)$, 从而 $\mathbb{Q}(\omega)$ 是 $\mathbb{Q}(u)/\mathbb{Q}$ 的中间域。但

$$[\mathbb{Q}(u):\mathbb{Q}]=3,\mathbb{Q}(\omega):\mathbb{Q}]=2$$

且 $2\nmid 3$, 产生矛盾! □

习题 2.4

证明 L 为 $K[x]$ 中多项式的有限集 $f_1,\cdots,f_n$ 在 K 上的分裂域当且仅当 L 为多项式 $f=f_1f_2\cdots f_n$ 在 K 上的分裂域。

证明. 由于 f 在 $L[x]$ 中可以分解为一次因式乘积当且仅当 $f_1,\cdots,f_n$ 在 $L[x]$ 都可以分解为一次因式乘积，而 f 在 L 中的根组合的集合 X 为 $f_i,i=1,\cdots,n$ 在 L 中根的集合 X_i 的并, 即

$$X=\bigcup_{i=1}^{n}X_i$$

根据分裂域的定义, L 是 $f_1,\cdots,f_n$ 的分裂域，当且仅当，$f_1,\cdots,f_n$ 在 $L[x]$ 中都可以分解为一次因式乘积且

$$L=K\left(\bigcup_{i=1}^{n}X_i\right),$$

这等价于 f 在 $L[x]$ 中可分解为一次因式乘积且

$$L=K(X),$$

即 L 是 f 在 K 上分裂域。 □

习题 2.5

计算域扩张的伽罗瓦群 $\mathrm{Aut}_{\mathbb{Q}}\,\mathbb{Q}(\sqrt{d})$, 其中 $0 \leqslant d \in \mathbb{Q}$.

解: 如果 $\sqrt{d} \in \mathbb{Q}$, 则 $\mathbb{Q} = \mathbb{Q}(\sqrt{d})$, 此时

$$\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{d})) = \{\mathrm{id}\}$$

为平凡群。如果 $\sqrt{d} \notin \mathbb{Q}$, 则 $x^2 - d$ 为 $\sqrt{d}$ 在 $\mathbb{Q}$ 上的极小多项式. 所有 $\mathbb{Q}(\sqrt{d})$ 中元素都形如

$$\{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}.$$

任意 $\sigma \in \mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{d}))$ 都将 $x^2 - d$ 的根 $\sqrt{d}$ 映为 $x^2 - d$ 的根 $\pm\sqrt{d}$, 因此

$$\sigma(a + b\sqrt{d}) = a \pm b\sqrt{d}$$

对所有 $a, b \in \mathbb{Q}$ 成立。如果 $\sigma(\sqrt{d}) = \sqrt{d}$, 则 $\sigma = \mathrm{id}$。记映射

$$\tau : a + b\sqrt{d} \mapsto a - b\sqrt{d}.$$

这说明 $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{d}))$ 中元素至多有 id 和 τ. 另一这方面, 由引理 2.10, 存在 $\mathbb{Q}$ 同构

$$\sigma : \mathbb{Q}(\sqrt{d}) \longrightarrow \mathbb{Q}(-\sqrt{d}) = \mathbb{Q}(\sqrt{d})$$

使得 $\sigma(\sqrt{d}) = -\sqrt{d}$. 这导致 $\tau = \sigma \in \mathrm{Aut}_{\mathbb{Q}}\,\mathbb{Q}(\sqrt{d})$. 所以

$$\mathrm{Aut}_{\mathbb{Q}}(\sqrt{d}),$$

可以简单验证, 这与 S_2 同构。 □

习题 2.6

设 K 是域, $f(x) \in K[x]$ 且 $\deg f(x) = n \geqslant 1$。令 E 为 $f(x)$ 在 K 上的分裂域, 证明 $[E : K]$ 整除 $n!$。(提示: 对 $\deg f(x)$ 利用数学归纳法, 从 n 到 $n+1$ 分 $f(x)$ 可约和不可约两种情形)

证明. 我们对 n 用数学归纳法, 当 $n = 1$ 时 $E = K$, $\mathrm{Aut}_K E = \{\mathrm{id}\}$, 结论显然成立。

现假设 $n > 1$, 分两种情形讨论。

情形 1: f 在 $K[x]$ 中不可约, 令 u 为 f 在 E 中根, 则有

$$[K(u) : K] = \deg f = n.$$

在 $K(u)[x]$ 中有分解

$$f(x) = (x - u)g(x)$$

这样 E 为 $g(x)$ 在 $K(u)$ 上分裂域, 由于 $\deg g = n - 1 < n$, 根据归纳假设有 $[E : K(u)] \mid (n-1)!$, 从而

$$[E : K] = [E : K(u)][K(u) : K] = [E : K(u)] \cdot n$$

整除 $(n-1)! \cdot n = n!$.

情形 2: f 在 $K[x]$ 中可约。假设 f 在 $K[x]$ 中有分解 $f = gh$, 其中 g, h 都是 $K[x]$ 中次数小于 n 的正次数多项式, 记 $\deg g = m, \deg h = n - m$. 此时 E 中包含一个 g 在 K 上的分裂域 L, 根据定义, 容易验证 E 为 h 在 L 上分裂域。由于 $m < n, n - m < n$, 根据归纳假设有

$$[L : K] \mid m!, \quad [E : L] \mid (n - m)!$$

从而有

$$[E : K] = [E : L] \cdot [L : K]$$

整除 $m! \cdot (n-m)!$. 由组合数

$$\binom{n}{m} = \frac{n!}{m! \cdot (n-m)!}$$

是整数可得 $m! \cdot (n-m)!$ 整除 $n!$. 所以 $[E : K]$ 整除 $n!$. □

习题 2.7

假设 K 为域, E 为 $f(x) \in K[x]$ 在 K 上的分裂域, $\xi_1, \cdots, \xi_n$ 为 $f(x)$ 在 E 中所有互不相同的根。对于置换 $\sigma \in S_n$, 我们称 σ 保持 $\xi_1, \cdots, \xi_n$ 的代数关系, 如果 n 元多项式 $\phi(x_1, \cdots, x_n)$ 满足 $\phi(\xi_1, \cdots, \xi_n) = 0$ 当且仅当 $\phi(\xi_{\sigma(1)}, \cdots, \xi_{\sigma(n)}) = 0$。记 G_f 为 S_n 中所有保持 $\xi_1, \cdots, \xi_n$ 的代数关系的置换构成的群。证明: $G_f \cong \mathrm{Aut}_K E$.

证明. 由推论 2.17 前的讨论, 记

$$X = \{\xi_1, \cdots, n\}$$

我们有群的单同态

$$\begin{array}{ccc} \mathrm{Aut}_K E & \longrightarrow & S(X) \cong S_n \\ \theta & \mapsto & \theta|_X. \end{array}$$

$\theta|_X$ 给出 S_n 中置换 $\tilde{\theta}$, 即

$$\theta(\xi_i) = \xi_{\tilde{\theta}(i)}, i = 1, \cdots, n.$$

我们断言 $\tilde{\theta} \in G_f$ 对所有 $\theta \in \mathrm{Aut}_K E$ 成立。实际上，对任意 $\phi \in K[x_1, \cdots, x_n]$, 由 $\theta \in \mathrm{Aut}_K E$ 有

$$\begin{aligned}\theta\phi(\xi_1, \cdots, \xi_n) &= \phi(\theta(\xi_1), \cdots, \theta(\xi_n)) \\ &= \phi(\xi_{\tilde{\theta}(1)}, \cdots, \xi_{\tilde{\theta}(n)})\end{aligned}$$

由于 θ 为域同构，因此 $\phi(\xi_1, \cdots, \xi_n) = 0$, 当且仅当 $\theta\phi(\xi_1, \cdots, \xi_n) = 0$, 当且仅当 $\phi(\xi_{\tilde{\theta}(1)}, \cdots, \xi_{\tilde{\theta}(n)}) = 0$, 也就是说 $\tilde{\theta} \in G_f$. 这就证明了 $\theta \mapsto \tilde{\theta}$ 给出 $\mathrm{Aut}_K E$ 到 G_f 的单的群同态。只需要再证明这个群同态为满射即可。

对任意 $\sigma \in G_f$, 我们现在来证明存在 $\theta \in \mathrm{Aut}_K E$ 使得 $\sigma = \tilde{\theta}$. 由于

$$E = \left\{ \frac{\phi(\xi_1, \cdots, \xi_n)}{\psi(\xi_1, \cdots, \xi_n)} \mid \begin{matrix} \phi, \psi \in K[x_1, \cdots, x_n] \\ \psi(\xi_1, \cdots, \xi_n) \neq 0 \end{matrix} \right\}$$

我们定义

$$\begin{array}{ccc} \theta(\sigma) : E & \longrightarrow & E \\ \frac{\phi(\xi_1, \cdots, \xi_n)}{\psi(\xi_1, \cdots, \xi_n)} & \mapsto & \frac{\phi(\xi_{\sigma(1)}, \cdots, \xi_{\sigma(n)})}{\psi(\xi_{\sigma(1)}, \cdots, \xi_{\sigma(n)})} \end{array}$$

需要证明 $\theta(\sigma)$ 是良定义的。首先，由于 $\psi(\xi_1, \cdots, \xi_n) \neq 0$, 而 $\sigma \in G_f$, 因此 $\psi(\xi_{\sigma(1)}, \cdots, \xi_{\sigma(n)} \neq 0$, 从而有

$$\frac{\phi(\xi_{\sigma(1)}, \cdots, \xi_{\sigma(n)})}{\psi(\xi_{\sigma(1)}, \cdots, \xi_{\sigma(n)})} \in E.$$

另外，如果有

$$\phi_i, \psi_i \in K[x_1, \cdots, x_n], i = 1, 2$$

使得

$$\frac{\phi_1(\xi_1, \cdots, \xi_n)}{\psi_1(\xi_1, \cdots, \xi_n)} = \frac{\phi_2(\xi_1, \cdots, \xi_n)}{\psi_2(\xi_1, \cdots, \xi_n)}.$$

令 $g = \phi_1\psi_2 - \psi_1\phi_2$, 则有 $g(\xi_1, \cdots, \xi_n) = 0$, 由 $\sigma \in G_f$ 得 $g(\xi_{\sigma(1)}, \cdots, \xi_{\sigma(n)}) = 0$, 因此

$$\frac{\phi_1(\xi_{\sigma(1)}, \cdots, \xi_{\sigma(n)})}{\psi_1(\xi_{\sigma(1)}, \cdots, \xi_{\sigma(n)})} = \frac{\phi_2(\xi_{\sigma(1)}, \cdots, \xi_{\sigma(n)})}{\psi_2(\xi_{\sigma(1)}, \cdots, \xi_{\sigma(n)})}.$$

这样就证明了 $\theta(\sigma)$ 是良定义的，即为 E 到 E 的映射。根据定义可验证

$$\theta(\sigma)\theta(\tau) = \theta(\sigma\tau)$$

对所有 $\sigma, \tau \in G_f$ 成立且 $\theta(e) = \mathrm{id}$, 其中 e 为 G_f 中单位元，即 S_n 中单位元，特别的

$$\theta(\sigma)\theta(\sigma^{-1}) = \theta(\sigma^-)\theta(\sigma) = \mathrm{id}\,.$$

这说明 $\theta(\sigma)$ 为双射。简单验证可得 $\theta(\sigma) \in \mathrm{Aut}_K E$. 取 $\phi = x_i$ 有

$$\theta(\sigma)(\xi_i) = \xi_{\sigma(i)}, i = 1, \cdots, n$$

成立。记 $\theta = \theta(\sigma)$ 有 $\tilde{\theta} = \sigma$. 因此群同态

$$\begin{array}{ccc} \mathrm{Aut}_K E & \longrightarrow & G_f \\ \theta & \mapsto & \tilde{\theta} \end{array}$$

是群同构。 □

第三章　伽罗瓦基本定理

习题 3.1

令 $0 \leqslant d \in \mathbb{Q}$。证明 $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ 是伽罗瓦扩张。

证明. 如果 $\sqrt{d} \in \mathbb{Q}$, 则 $\mathbb{Q}(\sqrt{d}) = \mathbb{Q}$, 此时 $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ 显然是伽罗瓦扩张。

如果 $\sqrt{d} \notin \mathbb{Q}$, 由习题 2.5 可得 $\mathrm{Aut}_{\mathbb{Q}}\,\mathbb{Q}(\sqrt{d}) = \{\mathrm{id}, \tau\}$. 其中

$$\tau(a + b\sqrt{d}) = a - b\sqrt{d}, a, b \in \mathbb{Q}.$$

从而被 $\mathrm{Aut}_{\mathbb{Q}}\,\mathbb{Q}(\sqrt{d})$ 固定的元素为

$$\{a + b\sqrt{d} \mid a + b\sqrt{d} = a - b\sqrt{d}, a, b \in \mathbb{Q}\} = \mathbb{Q}.$$

因此 $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ 是伽罗瓦扩张。 □

习题 3.2

设 E/K 为域扩张, L 和 M 是中间域。证明 $\mathrm{Aut}_{LM} E = \mathrm{Aut}_L E \bigcap \mathrm{Aut}_M E$。这里 LM 是含 L 和 M 的最小子域。

证明. 由于 $L \subseteq LM, M \subseteq LM$, 因此

$$\mathrm{Aut}_{LM} E \subseteq \mathrm{Aut}_L E \cap \mathrm{Aut}_M E.$$

根据定义有 $LM = L(M)$. 对任意 $\theta \in \mathrm{Aut}_L E \cap \mathrm{Aut}_M E$, 有 $\theta(u) = u$ 对所有 $u \in L(M) = LM$ 成立, 即 $\theta \in \mathrm{Aut}_{LM} E$. 从而有 $\mathrm{Aut}_{LM} E = \mathrm{Aut}_L E \cap \mathrm{Aut}_M E$. □

习题 3.3

如果 $[E : K] = 2$, 则 E/K 是正规扩张。

证明. 令 $u \in E \backslash K$, 根据习题 2.1 有 $K(u) = E$. 从而 u 在 K 上的首 1 极小多项式 $p(x)$ 是二次多项式。在 $E[x]$ 中有 $x - u \mid p(x)$, 所以在 $E[x]$ 中有因式分解

$$p(x) = (x - u)(x - v)$$

这里 $v \in E$. 因此

$$E = K(u) = K(u, v)$$

是 $p(x)$ 在 K 上分裂域, 从而 E/K 是正规扩张。 □

习题 3.4

设 L 为 E/K 的中间域, 且 E/L 和 L/K 是正规扩张。举例说明 E/K 未必是正规扩张。

解: 令

$$K = \mathbb{Q}, L = \mathbb{Q}(\sqrt{2}), E = \mathbb{Q}(\sqrt[4]{2}).$$

则有

$$[E : L] = [L : K] = 2$$

由习题 3.3, E/L 和 L/K 都是正规扩张。然而 $\mathbb{Q}[x]$ 上不可约多项式 $x^4 - 2$ 在 E 中有根 $\sqrt[4]{2}$, 但 $x^4 - 2$ 在 $\mathbb{C}$ 中的根 $\sqrt[4]{2}i \notin E$, $x^4 - 2$ 在 $E[x]$ 中不能分解为一次因式的乘积。所以 E/K 不是正规扩张。 □

习题 3.5

令 E/K 是正规扩张, L 为中间域。证明 L/K 为正规扩张当且仅当 L 是稳定中间域。

证明. 先证必要性. 假设 L/K 是正规扩张, 对任意 $u \in L$, 假设 $p(x) \in K[x]$ 是 u 在 K 上的首 1 极小多项式。由于 L/K 是正规扩张, 因此 $p(x)$ 在 $L[x]$ 中可以分解为一次因式的乘积, 即

$$p(x) = (x - u_1) \cdots (x - u_m),$$

其中 $u = u_1, u_2, \cdots, u_m \in L$. 根据引理 2.16, 对任意 $\sigma \in \mathrm{Aut}_K E$ 有 $\sigma(u)$ 也是 $p(x)$ 在 E 中的根, 从而存在 $1 \leqslant i \leqslant m$ 使得 $\sigma(u) = u_i \in L$. 所以 L 是 E/K 的稳定中间域。

反过来, 假设 L 是 E/K 的稳定中间域, 而 $p(x)$ 为 $K[x]$ 中首 1 不可约多项式且在 L 中有根 u. 由

于 E/K 是正规扩张，因此 $p(x)$ 在 $E[x]$ 中可分解为一次因式乘积

$$p(x) = (x - u_1) \cdots (x - u_m),$$

其中 $u = u_1$. 对任意 $u_i, 1 \leqslant i \leqslant m$, 由推论 3.18, 存在 $\sigma \in \mathrm{Aut}_K E$ 使得 $\sigma(u) = u_i$. 由于 L 是 E/K 的稳定中间域，因此 $u_i \in L$. 这样 $u_1, \cdots, u_m$ 都属于 L, 从而 $p(x)$ 在 $L[x]$ 中可分解为一次因式乘积。这就证明了 L/K 是正规扩张。 □

习题 3.6

设 K 是域，考虑 $u = \frac{f(x)}{g(x)} \in K(x)$ 且 $u \notin K$, 其中 $f(x)$ 与 $g(x)$ 为 $K[x]$ 中互素的多项式。

(1) 证明:

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

(2) 证明对于 $K(x)/K$ 的任意中间域 $E \neq K$, 均有 $[K(x) : E] < \infty$。

(3) 证明 $x \mapsto u$ 诱导了 $K(x)$ 到 $K(x)$ 的一个同态 σ。特别地，σ 是 $K(x)$ 上的 K 自同构当且仅当 $\max\{\deg f(x), \deg g(x)\} = 1$, 即 $\mathrm{Aut}_K K(x)$ 中的元素均形如

$$x \mapsto \frac{ax + b}{cx + d}, a, b, c, d \in K, ad - bc \neq 0.$$

(4) 设 $G = \{x \mapsto x, x \mapsto \frac{1}{1-x}, x \mapsto \frac{x-1}{x}\} \subset \mathrm{Aut}_K K(x)$。证明 $G \leqslant \mathrm{Aut}_K K(x)$，并求 G'

证明. (1) 由于 u 不属于 K, 因此 f 和 g 中至少一个为正次数多项式，从而 u 是 K 上的超越元。令 t 为 $K(u)$ 上未定元并考虑 $K(u)[t]$ 中元素

$$p(t, u) = f(t) - ug(t).$$

$p(t, u)$ 可以看成 $K(u)$ 上的一元多项式，并且 x 是 $p(t, u)$ 在 $K(x)$ 中的根，我们将证明 $p(t, u)$ 是 $K(u)[t]$ 中不可约多项式，从而说明

$$[K(x) : K(u)] = \max\{\deg f(t), \deg g(t)\}.$$

将 $p(t, u)$ 看作 $K[u]$ 上的一元多项式，由于其系数都是 u 或者 1, 所有系数整体互素，所以 $p(t, u)$ 作为 $K[u]$ 上的一元多项式是本原的。由于 $K[u]$ 是唯一分解整环，由 Gauss 引理, $p(t, u)$ 在 $K(u)[t]$ 中不可约当且仅当它在 $K[u][t]$ 中不可约。将 $p(t, u)$ 看作 $K[t]$ 上关于 u 的一元多项式也是本原多项式 (f 与 g 互素), 因此 $p(t, u)$ 在 $K[t][u]$ 中不可约当且仅当其在 $K(t)[u]$ 中不可约，但 $K(t)[u]$ 中 $p(t, u)$ 是关于 u 的一次多项式，显然不可约。最后，我们有

$$K[t][u] = K[u, t] = K[u][t].$$

因此 $p(t, u)$ 在 $K(u)[t]$ 中不可约，为 x 在 $K(u)$ 上的极小多项式，所以

$$\begin{aligned}[K(x) : K(u)] &= \max\{\deg f(t), \deg g(t)\} \\ &= \max\{\deg f(x), \deg g(x)\}.\end{aligned}$$

(2) 由于 $E \neq K$, 因此 E 中必含形如

$$u = \frac{f(x)}{g(x)}$$

其中 $f(x)$ 与 $g(x)$ 互素，且至少其中一个为正次数多项式。由 (1) 有

$$[K(x) : E] \leqslant [K(x) : K(u)] < \infty.$$

(3) 由 (1)，σ 为满射当且仅当 $[K(x) : K(u)] = 1$, 当且仅当 $f(x)$ 与 $g(x)$ 互素，且

$$\max\{\deg f(x), \deg g(x)\} = 1,$$

从而 $u = \frac{f(x)}{g(x)}$ 形如

$$\frac{ax + b}{cx + d}, a, b, c, d \in K, ad - bc \neq 0.$$

(4) 记 G 中非恒等映射的两个元素:

$$\sigma : x \mapsto \frac{1}{1 - x}, \quad \tau : x \mapsto \frac{x - 1}{x}$$

直接验证可知 $\sigma\tau = \mathrm{id}, \sigma^2 = \tau$. 因此 G 是由 σ 生成的 3 阶循环群。根据命题 3.14, 我们有

$$[K(x) : G'] = |G| = 3.$$

另一方面，考虑

$$\begin{aligned}u &= x + \sigma(x) + \tau(x) \\ &= \frac{x^3 - 3x + 1}{x(x - 1)}\end{aligned}$$

则有 $u \in G'$, 从而有域扩张链

$$K(u) \subseteq G' \subseteq K(x)$$

由 (1) 有 $[K(x):K(u)]=3$, 从而

$$[G':K(u)]=\frac{[K(x):K(u)]}{[K(x):G']}=1$$

所以 $G'=K(u)$. □

习题 3.7

证明 $\mathbb{Q}(x^2)$ 为 $\mathbb{Q}(x)/\mathbb{Q}$ 闭的中间域，但 $\mathbb{Q}(x^3)$ 不是闭的中间域。

证明. 取 σ 为 $x\mapsto -x$ 诱导的 $\mathbb{Q}(x)$ 的自同构，则 $G=\langle\sigma\rangle$ 为二阶循环群，由上一题的方法容易验证 $G'=\mathbb{Q}(x^2)$, 因此 $\mathbb{Q}(x^2)$ 为 $\mathbb{Q}(x)/\mathbb{Q}$ 的闭的中间域。

现假设 $\mathbb{Q}(x^3)$ 也是 $\mathbb{Q}(x)/\mathbb{Q}$ 闭的中间域, 根据定义有 $\mathbb{Q}(x)/\mathbb{Q}(x^3)$ 是伽罗瓦扩张。记 $u=x^3$, 则有 $\mathbb{Q}(x)=\mathbb{Q}(u)(x)$ 且 $[\mathbb{Q}(x):\mathbb{Q}(u)]=3$. 这说明 x 在 $\mathbb{Q}(u)$ 上极小多项式为 3 次。显然 x 是 $\mathbb{Q}(u)$ 上三次多项式 $p(t)=t^3-u$ 的根，所以 $p(t)$ 为 x 在 $\mathbb{Q}(u)$ 上极小多项式。由于 $\mathbb{Q}(x)/\mathbb{Q}(x^3)$ 是有限伽罗瓦扩张，从而是正规扩张，$p(t)$ 在 $\mathbb{Q}(x)[t]$ 能分解为一次因式的乘积。但 $p(t)$ 在 $\mathbb{C}(x)$ 中的三根 $x,\omega x,\omega^2 x$ 中只有 $x\in\mathbb{Q}(x)$. 这说明 x 是 $p(t)$ 在 $\mathbb{Q}(x)$ 中唯一的根，从而 $p(t)$ 在 $\mathbb{Q}(x)[t]$ 中不能分解为一次因式乘积，产生矛盾。 □

习题 3.8

证明 $\mathbb{Q}(x)$ 作为 $\mathbb{Q}(x,y)/\mathbb{Q}$ 的中间域，满足 $\mathbb{Q}(x)/\mathbb{Q}$ 是伽罗瓦扩张，但 $\mathbb{Q}(x)$ 不是稳定的。

证明. 假设 $\mathbb{Q}(x)/\mathbb{Q}$ 不是伽罗瓦扩张，则存在 $u\notin\mathbb{Q}$ 使得 $\sigma(u)=u$ 对所有 $\sigma\in\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(x)$ 成立，所以

$$\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(x)\leqslant\mathrm{Aut}_{\mathbb{Q}(u)}\mathbb{Q}(x).$$

由习题 3.6, $\mathbb{Q}(x)/\mathbb{Q}(u)$ 是有限扩张，从而 $Aut_{\mathbb{Q}(u)}\mathbb{Q}(x)$ 是有限群，这导致 $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(x)$ 是有限群。但根据习题 3.6 的 (3) 可得

$$\begin{array}{ccc}\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(x) & \cong & \mathrm{PGL}_2(\mathbb{Q})\\ x\mapsto\frac{ax+b}{cx+d} & \mapsto & \begin{bmatrix}a & c\\ b & d\end{bmatrix}\end{array}$$

这里两个映射相同当且仅当对应的两个矩阵中其中一个矩阵是另一个矩阵的非零数量倍。由于 $\mathrm{PGL}_2(\mathbb{Q})$ 是无限群，产生矛盾! □

习题 3.9

对于有限扩张 F/K，证明存在有限扩张 L/F 满足下面三条性质:

(1). L/K 是正规扩张.

(2). 如果 L/F 的中间域 M 是 K 的正规扩张，则 $M=L$.

(3). 如果 E/F 也满足 (1) 和 (2), 那么存在域同构 $\sigma:E\to L$ 使得 $\sigma|_F=\mathrm{id}$.

注: 此时 L 称为 F/K 的正规闭包 (normal closure)

证明. 由于 F/K 是有限扩张，可假设

$$F=K(u_1,\cdots,u_m)$$

其中 $u_1,\cdots,u_m$ 是 K 上的代数元，设它们在 K 上的极小多项式分别为 $f_1(x),\cdots,f_m(x)$ 并令

$$f(x)=\prod_{i=1}^{m}f_i(x).$$

假设 L 为 $f(x)$ 在 L 上的一个分裂域。我们断言 L 满足 (1)(2). 假设 X 为 $f(x)$ 在 L 中所有根组成的集合，则有 $u_1,\cdots,u_m\in X$, 从而

$$K(X)=F(X)=L.$$

所以 L 也是 $f(x)$ 在 K 上的分裂域。因此 L/K 是正规扩张, L 满足 (1).

假设 $M\supseteq F$ 是 L/K 中间域且 M/K 是正规扩张。对任意 $i=1,\cdots,m$, 由于 $K[x]$ 中不可约多项式 $f_i(x)$ 在 M 中有根 u_i, 由正规扩张的定义, $f_i(x)$ 在 $M[x]$ 中可分解为一次因式乘积. 因此 $f(x)$ 在 $M[x]$ 中可分解为一次因式乘积。由分裂域的极小性得 $M=L$. 这说明 L 满足 (2).

现假设 E 是 F 的有限扩张且满足 (1)(2). 由 E/K 是正规扩张可知每个 $f_i(x)$ 在 $E[x]$ 中都可以分解为一次因式的乘积，所以 E 包含 $f(x)$ 在 K 上的一个分裂域 M. 由于 M 含有 $f(x)$ 在 E 中所有根，特别的, $u_1,\cdots,u_m\in M$, 从而 $F\subseteq M$. 这样 $M\supseteq F$ 且 M/K 是正规扩张，根据 (2) 得 $E=M$. 这样 E 也是 $f(x)$ 在 K 上的分裂域，从而也是 $f(x)$ 在 F 上的分裂域。由分裂域的唯一性，存在 F 域同构 $\sigma:E\to L$ 使得 $\sigma|_F=\mathrm{id}$. □

第四章　分裂域作为伽罗瓦扩张

习题 4.1

设 $\operatorname{char} K = p > 0$。证明 $u \in E$ 是 K 上的可分元当且仅当 $K(u) = K(u^p)$。

证明. $\Rightarrow$. 假设 $g(x) \in K(u^p)[x]$ 是 u 在 $K(u^p)$ 上的极小多项式，则

$$g(x) \mid x^p - u^p = (x-u)^p$$

由于 u 是 K 上的可分元，从而也是 $K(u^p)$ 上的可分元，因此 $g(x)$ 在 $K(u)$ 内无重根，因此 $g(x) = x - u$，所以 $u \in K(u^p)$.

$\Leftarrow$. 由 $u \in K(u^p) = K[u^p]$ 知存在 $f(x) \in K[x]$ 使得

$$u = f(u^p).$$

因此 u 在 K 上的极小多项式整除

$$g(x) = f(x^p) - x$$

计算可得 $g'(x) = -1$，因此 $g(x)$ 与 $g'(x)$ 互素，从而 $g(x)$ 在其分裂域内无重根. 所以 u 是 K 上的可分元。 □

习题 4.2

设 $\operatorname{char} K = p > 0$，$[E : K]$ 有限且不能被 p 整除。证明:E/K 是可分扩张。

证明. 令 $f(x) \in K[x]$ 是 $u \in E$ 在 K 上的极小多项式，则

$$\deg f(x) = [K(u) : K] \mid [E : K]$$

但 $p \nmid [E : K]$，因此 $p \nmid \deg f(x)$，从而 $f'(x) \neq 0$. 所以 u 是 K 上的可分元，E/K 为可分扩张。 □

习题 4.3

设 u 在 K 上可分，v 在 $K(u)$ 上可分。证明 v 在 K 上可分。

证明. 令 $f(x) \in K[x]$ 是 u 在 K 上的极小多项式，L 为 $f(x)$ 在 K 上含 u 的分裂域. 由假设 $f(x)$ 是 K 上的可分多项式，从而 L/K 是有限伽罗瓦扩张。令 $g(x)$ 为 v 在 L 上极小多项式，并令 E 为

$$h(x) := \prod_{\sigma \in \operatorname{Aut}_K L} \sigma g(x)$$

在 L 上含 v 的分裂域。由 v 在 $K(u)$ 上可分，而 $K(u) \subseteq L$，因此 v 在 L 上可分，$g(x)$ 是 L 上的可分多项式，从而对任意 $\sigma \in \operatorname{Aut}_K L$，$\sigma g(x)$ 也在 L 上可分。所以 $h(x)$ 是 L 上的可分多项式，从而 E/L 是有限伽罗瓦扩张。对任意 $\sigma \in \operatorname{Aut}_K L$，有 $\sigma h(x) = h(x)$，由定理 2.14，σ 可以扩展为 E 上自同构。由命题 4.4，E/K 为有限伽罗瓦扩张，特别的 v 是 K 上的可分元。 □

习题 4.4

设 $f(x) \in K[x]$ 为 $m \neq 0$ 次不可约多项式，且 $\operatorname{char} K$ 不能整除 m。证明 f 为可分多项式。

证明. 显然 $f'(x)$ 的首项非零，从而 $f(x)$ 可分。 □

习题 4.5

设 $u_1, \cdots, u_n$ 是 K 上的可分元。证明 $K(u_1, \cdots, u_n)/K$ 是可分扩张。

证明. 对 $i = 1, \cdots, n$，令 $f_i(x)$ 为 u_i 在 K 上的极小多项式，由假设可知

$$f(x) = \prod_{i=1}^{n} f_i(x)$$

是 K 上的可分多项式，令 E 为 $f(x)$ 在 K 上含 $u_1, \cdots, u_n$ 的分裂域，则有 E/K 是可分扩张，而 $K(u_1, \cdots, u_n) \subseteq E$，因此 $K(u_1, \cdots, u_n)$ 是 K 的可分扩张。 □

习题 4.6

令 $E=K(u,v)$ 其中 u,v 为 K 上的代数元，且 u 是 K 上的可分元。证明 E/K 是单扩张。

证明. 由上面习题 4.3 的证明可得 E/K 是有限可分扩张，根据引理 4.14 得 E/K 是单扩张。 □

习题 4.7

设 E/K 为代数扩张。
(1) 如果 K 为完全域，问 E 是否为完全域？
(2) 如果 E 为完全域，问 K 是否为完全域？

证明. (1) 正确。实际上，对任意 E 上的代数元 u，由于 E/K 是代数扩张，因此 u 也是 K 上的代数元。由于 K 是完全域，因此 u 是 K 上的可分元，从而也是 E 上可分元。这说明 E 上所有的代数元都是 E 上的代数元，从而 E 是完全域。

(2) 不一定。例如由例 4.9, $K=\mathbb{Z}_p(t)$ 不是完全域，但其代数闭包 E 总是完全域且为 K 的代数扩张。 □

习题 4.8

设 L 和 M 是域扩张 F/K 的两个中间域，且 L/K 是有限伽罗瓦扩张。证明 LM/M 也是有限伽罗瓦扩张，且 $\mathrm{Aut}_M LM \cong \mathrm{Aut}_{L\cap M} L$。

证明. 由于 L/K 是有限伽罗瓦扩张，由定理 4.2 及其证明，L 是 $K[x]$ 中某个可分多项式 $f(x)$ 在 K 上的分裂域。假设 $f(X)$ 在 L 中所胡根组成的集合为 X，则 $L=K(X)$. 由于 $K\subseteq M$, 因此 $f(x)$ 在 M 上也是可分的。现在

$$LM=M(L)=M(K(X))=M(x)$$

是 $f(x)$ 在 M 上分裂域，再由定理 4.2 得 LM/M 是有限伽罗瓦扩张。

现在考虑域扩张 LM/K. 由上一章引理 3.8, L 为 LM/K 的稳定中间域，从而有群同态

$$\begin{array}{rccc}\theta:\mathrm{Aut}_K LM & \longrightarrow & \mathrm{Aut}_K L\\ \sigma & \mapsto & \sigma|_L\end{array}$$

在这个环同态下，$\sigma\in\mathrm{Aut}_M LM$ 的像 $\sigma|_L$ 正好属于 $\mathrm{Aut}_{L\cap M} L$. 这样我们得到交换图

$$\begin{array}{ccc}\mathrm{Aut}_K LM & \xrightarrow{\theta} & \mathrm{Aut}_K L\\ \uparrow & & \uparrow\\ \mathrm{Aut}_M LM & \xrightarrow{\theta} & \mathrm{Aut}_{L\cap M} L\end{array}$$

我们将证明第二行的群同态为群同构。令 $H=\mathrm{Im}\,\theta$. 在域扩张 $L/(L\cap M)$ 中

$$H'=\{u\in L\mid \sigma|_L(u)=u,\forall\sigma\in\mathrm{Aut}_M LM\}$$

显然 $L\cap M\subseteq H'$. 另一方面，由于 LM/M 是伽罗瓦扩张，对任意 $u\in L\backslash M$, 都存在 $\sigma\in\mathrm{Aut}_M LM$ 使得 $\sigma(u)\neq u$. 因此 $H'\subseteq M$. 所以 $H'=L\cap M$. 由于 L/K 是有限伽罗瓦扩张，根据伽罗瓦对应有

$$H=H''=(L\cap M)'=\mathrm{Aut}_{L\cap M} L,$$

即 θ 为满射。另一方面，假设 $\sigma\in\mathrm{Ker}\,\theta$, 则有 $\theta(u)=u$ 对所有 $u\in L$ 成立。由于 $\sigma\in\mathrm{Aut}_M LM$ 本来就固定 M 中元素，由此 θ 固定 LM 中所有元素，从而 $\sigma=\mathrm{id}$. 这说明 θ 为单射。所以 θ 是群同构。 □

习题 4.9

设 $u\in\mathbb{R}$, $n\in\mathbb{N}_+$。若 $u^n\in\mathbb{Q}$ 且 $(u+1)^n\in\mathbb{Q}$, 证明 $u\in\mathbb{Q}$。(提示：考虑 $\mathbb{Q}(u,\zeta)/\mathbb{Q}$，其中 ζ 为 n 次本原单位根。)

证明. 令 $\zeta\in\mathbb{C}$ 为 n 次本原单位根，则 x^n-u^n 在 $\mathbb{C}$ 中的根为

$$u,\zeta u,\cdots,\zeta^{n-1}u,$$

因此 $\mathbb{Q}(u,\zeta)$ 为 $x^n-u^n\in\mathbb{Q}[x]$ 在 $\mathbb{Q}$ 上的分裂域。类似的，它也是 $x^n-(u+1)^n$ 在 $\mathbb{Q}$ 上的分裂域. 所以 $\mathbb{Q}(u,\zeta)/\mathbb{Q}$ 是伽罗瓦扩张。下面这们将证明 u 被 $\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(u,\zeta)$ 中所有元素固定，从而说明 $u\in\mathbb{Q}$.

对任意 $\sigma\in\mathrm{Aut}_{\mathbb{Q}}\mathbb{Q}(u,\zeta)$. $\sigma(u)$ 必为 x^n-u^n 的根，而 $\sigma(u+1)$ 也是 $x^n-(u+1)^n$ 的根，因此存在 $0\leqslant a,b\leqslant n-1$ 使得

$$\sigma(u)=\zeta^a u,\ \sigma(u)+1=\sigma(u+1)=\zeta^b(u+1).$$

所以 $\zeta^a u+1=\zeta^b(u+1)$, 从而

$$\zeta^{a-b}u+\zeta^{-b}=u+1.$$

若 $a=0$ 或者 $b=0$, 则 $\sigma(u)=u$; 若 $a=b$, 则 $\zeta^{-b}=1$, 从而 $a=b=0$, 同样有 $\sigma(u)=u$.

若 a,b 均不为零且不相等，则

$$1,\zeta^{-b},\zeta^{a-b}$$

为三个互不相同的 n 次单位根，同时也是复平面上单位圆上互不相同的三个点。但由上面的等式，我们有

$$u=\frac{1-\zeta^{-b}}{\zeta^{a-b}-1}\in\mathbb{R}.$$

这说明复平面内，$1,\zeta^{-b},\zeta^{a-b}$ 在同一条直线上，这显然不可能。因此我们总有 $\sigma(u)=0$ 对所有 $\sigma\in\mathrm{Aut}_{\mathbb{Q}}\,\mathbb{Q}(u,\zeta)$ 成立，从而 $u\in\mathbb{Q}$. □

第五章　多项式的伽罗瓦群

习题 5.1

令 $x^4+ax^2+b\in K[x](\operatorname{char}K\neq 2)$ 为不可约多项式，其伽罗瓦群为 G。证明：

(1) 如果 b 是 K 中的平方数，则 $G\cong K_4$。

(2) 如果 b 不是 K 中的平方数，$b(a^2-4b)$ 是 K 中的平方数，则 $G\cong C_4$。

(3) 如果 b 和 $b(a^2-4b)$ 都不是 K 中的平方数，则 $G\cong D_4$。

证明. 在这个证明中，我们记

$$f(x)=x^4+ax^2+b.$$

由于 $\operatorname{char}K\neq 2$, 因此 $f'(x)\neq 0$. 这说明 $K[x]$ 中不可约多项式 $f(x)$ 在 K 上可分，因此 $f(x)$ 在 K 上的分裂域 E 是 K 上的伽罗瓦扩张且 f 的伽罗瓦群 $G=\operatorname{Aut}_K E$ 是 $f(x)$ 在 E 中四个根 u_1,u_2,u_3,u_4 的置换群的可迁子群。根据 $f(x)$ 的形式，如果 $f(u)=0$ 则有 $f(-u)=0$, 因此可假设

$$u_2=-u_1,u_4=-u_3$$

对任意 $\sigma\in G$ 有

$$\sigma(u_2)=-\sigma(u_1),\sigma(u_4)=-\sigma(u_3)$$

所有满足这个条件的 u_1,u_2,u_3,u_4 的置换构成的集合为

$$H=\left\{\begin{array}{l}\mathrm{id},(u_1u_2),(u_3u_4),(u_1u_2)(u_3u_4),\\(u_1u_3u_2u_4),(u_1u_3)(u_2u_4),\\(u_1u_4)(u_2u_3),(u_1u_4u_2u_3)\end{array}\right\}$$

G 为 H 的可迁子群。而 H 的可迁子群有 $H\cong D_4$ 本身，

$$K_4=\left\{\begin{array}{l}\mathrm{id},(u_1u_2)(u_3u_4),\\(u_1u_3)(u_2u_4),(u_1u_4)(u_2u_3)\end{array}\right\},$$

$$C_4=\left\{\begin{array}{l}\mathrm{id},(u_1u_3u_2u_4),\\(u_1u_2)(u_3u_4),(u_1u_4u_2u_3)\end{array}\right\}.$$

此时 $b=u_1u_2u_3u_4=(u_1u_3)^2$,

如果 b 是 K 中平方数，则 $u_1u_3\in K$. 此时 G 中所有元素都固定 u_1u_3. 在 H 中 (u_1u_2) 作用在 u_1u_3 上得到 $u_2u_3=-u_1u_3$，这说明 $G\neq H$; 在 C_4 中，$(u_1u_3u_2u_4)$ 作用在 u_1u_3 上得到 $u_3u_2=-u_1u_3$，这说明 $G\neq C_4$，所以此时 $G=K_4$.

如果 b 不是 K 中的平方数，即 $u_1u_3\notin\in K$，由于 E/K 是伽罗瓦扩张，因此存在 $\sigma\in G$ 使得 $\sigma(u_1u_3)\neq u_1u_3$. 这说明 $G\neq K_4$.

另外，由于

$$a=-(u_1^2+u_3^2),$$

计算可得

$$\begin{aligned}b(a^2-4b)&=(u_1u_3)^2(u_1^2-u_3^2)^2\\&=(u_1u_3(u_1^2-u_3^2))^2\end{aligned}$$

记 $\gamma:=u_1u_3(u_1^2-u_3^2)$.

如果 $b(a^2-4b)$ 是 K 中的平方数，则 $\gamma\in K$，从而被 G 中所有元素固定。由于 H 中 $(u_1u_3)(u_2u_4)$ 不固定 γ, 因此此时 $G\neq H$;

如果 $b(a^2-4b)$ 不是 K 中平方数，则存在 G 中元素 σ 使得 $\sigma(\gamma)\neq\gamma$. 但 C_4 中所有元素都固定 γ, 因此此时 $G\neq C_4$.

综上所述，在情形 (1) 时，b 是平方数，从而 $G=K_4$; 在情形 (2) 时，b 不是平方数，而 $b(a^2-4b)$ 是平方数，G 既不是 K_4，也不是 H, 只能是 C_4; 在情形 (3) 时，G 既不是 K_4，也不是 C_4，只能是 $H\cong D_4$. □

习题 5.2

设 $n>2$，ξ 为 n 次本原单位根。证明 $[\mathbb{Q}(\xi+\xi^{-1}):\mathbb{Q}]=\varphi(n)/2$.

证明. 令 $u=\xi+\xi^{-1}$, 则有

$$\xi^2-u\xi+1=0$$

这说明 $[\mathbb{Q}(\xi):\mathbb{Q}(u)]\leqslant 2$. $n>2$ 保证了 ξ 不是实数，但 u 是实数，因此 $\mathbb{Q}(\xi)\neq\mathbb{Q}(u)$. 因此

$$[\mathbb{Q}(\xi):\mathbb{Q}(u)]=2.$$

另一方面，由于

$$[\mathbb{Q}(\xi):\mathbb{Q}]=|\operatorname{Aut}_{\mathbb{Q}}\mathbb{Q}(\xi)|=|U_n|=\varphi(n),$$

所以 $[\mathbb{Q}(u):\mathbb{Q}]=\varphi(n)/2$. □

习题 5.3

令 K 为域，$\overline{K}$ 为 K 的代数闭包，$\sigma\in\operatorname{Aut}_K\overline{K}$。令 $F=\{u\in\overline{K}\mid\sigma(u)=u\}$。证明 F 是域，且 F 的每个有限扩张都是循环扩张。

证明. 根据定义 F 是由 σ 生成的循环群

$$\langle\sigma\rangle\leqslant\operatorname{Aut}_K\overline{K}$$

固定的所有元素构成的，容易验证 F 是域。

现在假设 L/F 是有限扩张，由于 $\overline{K}$ 也是 F 的代数闭包，我们可以假设 $L\subseteq\overline{K}$. 假设

$$L=F(u_1,\cdots,u_m)$$

并假设 u_i 在 F 上的极小多项式为 $f_i(x), i=1,\cdots,m$. 令 U 为

$$f(x)=f_1(x)\cdots f_m(x)$$

在 $\overline{K}$ 中所有根构成的集合。那么，$E=F(U)$ 包含 L，为 $f(x)$ 在 F 上的分裂域。由于 $\sigma|_F=\mathrm{id}$，因此 $\sigma(U)\subseteq U$，从而 $\sigma(E)\subseteq E$. 这样有 $\sigma|_E\in\operatorname{Aut}_F E$，从而 $G:=\langle\sigma|_E\rangle\leqslant\operatorname{Aut}_F E$ 是有限循环群。另外，显然

$$F=\{u\in E\mid\sigma(u)=u\}$$

是 G 在 E 中固定的所有元素构成的子域。根据命题 3.14，E/F 是有限伽罗瓦扩张且 $\operatorname{Aut}_F E=G$ 是循环群，特别的，$\operatorname{Aut}_F E$ 的所有子群都是正规子群，根据伽罗瓦基本定理，L/F 是伽罗瓦扩张且

$$\operatorname{Aut}_F L\cong\operatorname{Aut}_F E/(\operatorname{Aut}_L E)$$

是循环群 $\operatorname{Aut}_F E$ 的商群，从而也是循环群。所以 L/F 是循环扩张。 □

习题 5.4

设 $\operatorname{char}K=p\neq 0$。令 $K_p=\{u^p-u\mid u\in K\}$。证明：

(1) 存在 K 的 p 次循环扩张 F 当且仅当 $K\neq K_p$。

(2) 如果存在 K 的 p 次循环扩张，则对于任意的 $n\geqslant 1$，存在 K 的 p^n 次循环扩张。

证明. (1) 对 $a\in K$，我们记

$$f_a(x)=x^p-x-a.$$

由于 $f_a'(x)=-1$，与 $f_a(x)$ 互素，因此 $f_a(x)$ 是 K 上的可分多项式。

(1) 如果 $K\neq K_p$，则存在 $a\in K$ 使得 $f_a(x)$ 在 K 中没有根。假设 θ 为 $f_a(x)$ 在 K 上分裂域 L 中的一根。根据 $f_a(x)$ 的特点

$$\theta,\theta+1,\cdots,\theta+p-1$$

均为 $f_a(x)$ 在 L 中的根且互不相同，因此 L/K 是伽罗瓦扩张。对任意 $\operatorname{Aut}_K L$ 中非单位元 σ，有 $\sigma(\theta)=\theta+i$，其中 $0<i<p$. 这样有 $\sigma^m(\theta)\neq\theta$ 对所有 $1\leqslant m<p$ 成立，从而 σ 的阶大于等于 p. 所以

$$p\leqslant|\langle\sigma\rangle|\leqslant|\operatorname{Aut}_K L|=[L:K]=\deg f_a=p.$$

这导致 $|\operatorname{Aut}_K L|=p$ 必为循环群。

假设 L/K 是 p 次循环扩张，并假设 $\operatorname{Aut}_K L=\langle\sigma\rangle$. 根据假设 $o(\sigma)=p$. 由于 $\operatorname{Tr}_{L/K}(1)=p=0$，由习题 5.6 结论 (2)，存在 $\beta\in L$ 使得 $1=\sigma(\beta)-\beta$. 显然 $\beta\notin K$ (否则 $\sigma(\beta)-\beta=0$). 如此一来 $L=K(\beta)$ 且 $\sigma(\beta)=\beta+1$，从而 $L=K(\beta)$ 是 K 系数多项式

$$g(x)=\prod_{\sigma\in\operatorname{Aut}_K L}(x-\sigma(\beta))=\prod_{i=0}^{p-1}(x-\beta-i)$$

在 K 上的分裂域。由上面的讨论可知 $g(x)=x^p-x-1$. 由于 $g(x)$ 在 K 中没有根，这也说明 $1\notin K_p$，从而 $K\neq K_p$.

(2) 我们对 n 用数学归纳法，根据假设结论在 $n=1$ 时成立。现假设 $n>1$ 且 L/K 是 p^{n-1} 次循环扩张且 $\operatorname{Aut}_K L=\langle\sigma\rangle$. 由引理 5.7，存在 $u\in L$ 使得

$$\operatorname{Tr}_{L/K}(u)=\sum_{i=0}^{p^{n-1}-1}\sigma^i(u)\neq 0,$$

其中 $\mathrm{Tr}_{L/K}$ 的定义见习题 5.6. 令

$$\alpha = \frac{u}{\mathrm{Tr}_{L/K}(u)}$$

则有 $\mathrm{Tr}_{L/K}(\alpha) = 1$. 由 $\mathrm{char}\, L = p$ 和 Tr 的定义有

$$\mathrm{Tr}_{L/K}(\alpha^p) = \mathrm{Tr}_{L/K}(\alpha)^p = 1.$$

所以 $\mathrm{Tr}_{L/K}(\alpha^p - \alpha) = 0$. 根据习题 5.6 结论 (2), 存在 $v \in L^*$ 使得

$$\alpha^p - \alpha = \sigma(v) - v.$$

如果 $f_v = x^p - x - v$ 在 E 中有根 β, 那么它的全部根为 $\beta + i, i = 0, \cdots, p-1$. 这样

$$\begin{aligned} \alpha^p - \alpha &= \sigma(v) - v \\ &= \sigma(\beta^p - \beta) - (\beta^p - \beta) \\ &= (\sigma(\beta) - \beta)^p - (\beta^p - \beta). \end{aligned}$$

这说明 α 和 $\sigma(\beta) - \beta$ 都是多项式 $x^p - x - \sigma(v) + v$ 的根, 从而存在 $i = 0, \cdots, p-1$ 使得

$$\alpha + i = \sigma(\beta) - \beta.$$

两边取 $\mathrm{Tr}_{L/K}$ 得

$$\mathrm{Tr}_{L/K}(\alpha) + p^{n-1} i = 0.$$

这导致 $\mathrm{Tr}_{L/K}(\alpha) = 0$, 这与 $\mathrm{Tr}_{L/K}(\alpha) = 1$ 矛盾。所以 $x^p - x - v$ 在 L 中没有根, 根据 (1) 的证明, 其在 L 上的分裂域 E 是 L 上的 p 次循环扩张。

现在假设 β 为 $f_v(x)$ 在 E 中根, 则 $\alpha + \beta$ 是 $\sigma f_v(x) = x^p - x - \sigma(v)$ 在 E 中的根。容易发现 E 也是 $\sigma f_v(x)$ 在 L 上分裂域。因此 $\sigma \in \mathrm{Aut}_K L$ 可以拓展为 $\tilde{\sigma} \in \mathrm{Aut}_K E$ 且 $\tilde{\sigma}(\beta) = \alpha + \beta$. 对 $k \geqslant 1$:

$$\tilde{\sigma}^k(\beta) = \beta + \sum_{i=0}^{k-1} \sigma^i(\alpha).$$

由于 $o(\sigma) = p^{n-1}$, 因此 $o(\tilde{\sigma}) \geqslant p^{n-1}$. 注意到

$$\tilde{\sigma}^{p^{n-1}}(\beta) = \beta + \mathrm{Tr}_{L/K}(\alpha) = \beta + 1,$$

所以 $o(\tilde{\sigma}) > p^{n-1}$. 同时

$$\tilde{\sigma}^{p^n}(\beta) = \beta + p = \beta,$$

$\tilde{\sigma}^{p^n}|_L = \sigma^{p^n}|_L = \mathrm{id}$, 而 $E = L(\beta)$. 所以 $\tilde{\sigma}^{p^n} = \mathrm{id}$, 从而 $o(\tilde{\sigma}) \mid p^n$. 综合起来有 $o(\tilde{\sigma}) = p^n$. 最后, 由于 $[E : K] = [E : L] \cdot [L : K] = p^n$. 根据命题 4.4, E/K 是伽罗瓦扩张, 这导致

$$|\mathrm{Aut}_K E| = p^n = |\langle \tilde{\sigma} \rangle|,$$

所以 $\mathrm{Aut}_K E = \langle \tilde{\sigma} \rangle$ 为循环群, E/K 为 p^n 次循环扩张。 □

习题 5.5

如果 $\mathrm{char}\, K = p \neq 0$, 则对于 $x^p - a \in K[x]$ 的任意根 u, $K(u) \neq K(u^p)$ 当且仅当 $[K(u) : K] = p$。

证明. 由于

$$x^p - a = x^p - u^p = (x - u)^p,$$

u 在 K 上的首 1 极小多项式 $g(x) = (x-u)^m$ 必然满足 $m \mid p$. 否则, $n = km + r$ 且 $0 < r < m$, 则有 $(x-u)^r \in K[x]$ 且以 u 为根, 从而 $g(x) \mid (x-u)^r$, 产生矛盾。这样可得 $m = 1$ 或者 p。$m = 1$ 当且仅当 $u \in K$, 此时 $K(u) = K = K(u^p)$.

当 $m = p$ 时, $g(x) = (x-u)^m$ 不可约, 此时 $[K(u) : K] = p$, 且 u 不是 K 上的可分元, 根据习题 4.1 的结果知 $K(u) \neq K(u^p)$. □

习题 5.6

假设 L/K 为有限伽罗瓦扩张, $G = \mathrm{Aut}_K L$ 为相应的伽罗瓦群。对任意 $\alpha \in L$, 我们定义:

$$\mathrm{N}_{L/K}(\alpha) = \prod_{\tau \in G} \tau(\alpha), \quad \mathrm{Tr}_{L/K}(\alpha) = \sum_{\tau \in G} \tau(\alpha).$$

则 $\mathrm{N}(\alpha)$ 和 $\mathrm{Tr}(\alpha)$ 都属于 K. 现假设 L/K 是循环扩张而 $\mathrm{Aut}_K L = \langle \sigma \rangle$. 证明: 对 $\alpha \in L^*$, $\mathrm{N}_{L/K}(\alpha) = 1$ 当且仅当存在 $\beta \in L^*$ 使得 $\alpha = \frac{\sigma(\beta)}{\beta}$, $\mathrm{Tr}_{L/K}(\alpha) = 0$ 当且仅当存在 $\beta \in L$ 使得 $\alpha = \sigma(\beta) - \beta$.

证明. 假设 $o(\sigma) = n$. 由定义, 如果 $\alpha = \dfrac{\sigma(\beta)}{\beta}$, 则

$$\mathrm{N}_{L/K}(\alpha) = \prod_{i=0}^{n-1} \frac{\sigma^i \sigma(\beta)}{\sigma^i(\beta)} = 1.$$

如果 $\alpha = \sigma(\beta) - \beta$, 则有

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=0}^{n-1} \sigma^i(\sigma(\beta) - \beta) = 0.$$

反过来，假设 $\mathrm{N}_{L/K}(\alpha)=1$. 令

$$\theta=\sum_{k=0}^{n-1}\left(\prod_{i=0}^{k}\sigma^i(\alpha)\right)\sigma^k.$$

则有

$$\begin{aligned}\alpha\cdot\sigma\theta&=\alpha\cdot\sum_{k=0}^{n-1}\left(\prod_{i=0}^{k}\sigma^{i+1}(\alpha)\right)\sigma^{k+1}\\&=\sum_{k=0}^{n-1}\left(\prod_{i=0}^{k+1}\sigma^i(\alpha)\right)\sigma^{k+1}.\end{aligned}$$

因此

$$\begin{aligned}\alpha\cdot\sigma\theta-\theta&=\left(\prod_{i=0}^{n}\sigma^i(\alpha)\right)\sigma^n-\alpha\,\mathrm{id}\\&=\alpha\,\mathrm{N}_{L/K}(\alpha)\,\mathrm{id}-\alpha\,\mathrm{id}=0.\end{aligned}$$

显然 $\theta\neq 0$, 存在 $u\in L$, 使得 $\theta(u)\neq 0$. 但有

$$\alpha\sigma\theta(u)-\theta(u)=0,$$

令 $\beta=\dfrac{1}{\theta(\beta)}$, 则有 $\alpha=\dfrac{\sigma(\beta)}{\beta}$.

现假设 $\mathrm{Tr}_{L/K}(\alpha)=0$, 类似的，可定义

$$\theta=\sum_{k=0}^{n-1}\left(\sum_{i=0}^{k}\sigma^i(\alpha)\right)\sigma^k.$$

则有

$$\sigma\theta-\theta=-\alpha(\mathrm{id}+\sigma+\cdots+\sigma^{n-1}).$$

令 $u\in L$ 使得 $\mathrm{Tr}_{L/K}(u)\neq 0$, $\beta=-\dfrac{\theta(u)}{\mathrm{Tr}_{L/K}(u)}$, 则

$$\sigma\theta(u)-\theta(u)=-\alpha\,\mathrm{Tr}_{L/K}(u)$$

两边同除以 $-\mathrm{Tr}_{L/K}(u)$ 可得 $\alpha=\sigma(\beta)-\beta$. □

习题 5.7

假设 $f(x)\in K[x]$ 为域 K 上的可分多项式，$\xi_1,\cdots,\xi_n$ 为 $f(x)$ 在 K 上的分裂域 E 中所有互不相同的根。由引理 4.14, 存在 $u\in E$ 使得 $E=K(u)=K[u]$ 为单扩张。因此存在多项式 $\phi_1(x),\cdots,\phi_n(x)\in K[x]$ 使得 $\xi_i=\phi_i(u)$. 令 $p(x)$ 为 u 在 K 上的极小多项式。

(1) 证明：对任意 $p(x)$ 在 E 中的根 v, $\phi_1(v),\cdots,\phi_n(v)$ 是 $\xi_1,\cdots,\xi_n$ 的一个排列。

(2) 在 (1) 中，记

$$\sigma_v=\begin{pmatrix}\xi_1&\cdots&\xi_n\\\phi_1(v)&\cdots&\phi_n(v)\end{pmatrix}$$

为 $\xi_1,\cdots,\xi_n$ 的置换. 令 G 为所有 σ_v 构成的集合，其中 v 取遍 $p(x)$ 在 E 中的所有根。证明: G 是群且与 $\mathrm{Aut}_K E$ 同构。

证明. 在这个证明中，我们假设 $[E:K]=m$. 由于 E/K 是单扩张，因此 $m=\deg p(x)$.

(1) 由于 E 是 $f(x)$ 在 K 上的分裂域，E/K 为伽罗瓦扩张，而 $p(x)$ 在 E 中有根 u, 所以 $p(x)$ 在 $E[x]$ 中可以分解为 m 个互不相同的一次因式乘积，$p(x)$ 在 E 中有 m 个互不相同的根。对任意 $p(x)$ 在 E 中的根 v，有 $K\subseteq K(v)\subseteq E$ 且 $[K(v):K]=\deg p(x)=m$, 从而 $E=K(v)$. 由引理 2.10，存在 $\sigma\in\mathrm{Aut}_K E$ 使得 $\sigma(u)=v$. 由于 σ 给出 $f(x)$ 所有互不相同的根的一个转换，因此

$$\sigma\phi_1(u),\cdots,\sigma\phi_n(u)$$

是 $f(x)$ 的 n 个根的转换。注意到 $\phi_i(x)\in K[x]$, 所以

$$\sigma\phi_i(u)=\phi_i(\sigma(u))=\phi_i(v)$$

对所有 $i=1,\cdots,n$ 成立。因此 $\phi_1(v),\cdots,\phi_n(v)$ 是 $\xi_1,\cdots,\xi_n$ 的一个排列。

(2) 对 $p(x)$ 的根 v, 记 θ_v 为 $\mathrm{Aut}_K E$ 中使得 $\theta_v(u)=v$ 的元素，一共有 m 个这样的元素，但 $|\mathrm{Aut}_K E=[E:K]=m$, 因此 $\mathrm{Aut}_K E$ 恰由所有这样的元素组成。记 $X=\{\xi_1,\cdots,\xi_n\}$, 则 G 是下面群同态的像集

$$\mathrm{Aut}_K E\longrightarrow S(X),\quad \theta\mapsto\theta|_X$$

由推论 2.17 前面的讨论，这个群同态是单射，从而有 $\mathrm{Aut}_K E\cong G$. □

第六章　根式扩张与可解群

习题 6.1

假设 F/K 为根式扩张，E 为中间域。证明：F/E 为根式扩张。

证明. 可假设有域扩张链

$$K \subseteq K(u_1) \subseteq \cdots \subseteq K(u_m) = F,$$

且存在正整数 $n_1, \cdots, n_m$ 使得

$$u_i^{n_i} \in K(u_1, \cdots, u_{i-1}), i = 1, \cdots, m.$$

由于 $K \subseteq E \subseteq F$, 显然有

$$E \subseteq E(u_1) \subseteq \cdots \subseteq E(u_m) = F,$$

且

$$u_i^{n_i} \in E(u_1, \cdots, u_{i-1}), i = 1, \cdots, m.$$

因此 F/E 是根式扩张。 □

习题 6.2

假设 F/E, E/K 为根式扩张。证明：F/K 为根式扩张。

证明. 将两个域的扩张链接起来即得。 □

习题 6.3

假设 F/K 为根式扩张，N/F 为 F/K 的正规闭包 (参见第 3 章习题 9)。证明：N/K 为根式扩张。

证明. 假设 $F = K(u_1, \cdots, u_n)$, 而 $f_i(x) \in K[x]$ 是 u_i 在 K 上的极小多项式。令 E 为 $f(x) = f_1(x) \cdots f_n(x)$ 在 F 上的分裂域。根据定理 6.5 的证明, E/K 是根式扩张。根据习题 3.9 的证明 E 是 F/K 的正规闭包。由正规闭包的唯一性, 存在域的 F 同构 $\sigma : E \to N$. 从而 N/K 也是根式扩张。 □

习题 6.4

令 $f(x) \in K[x]$ 为 $n \geqslant 5$ 次不可约多项式，u 为 $f(x)$ 在其分裂域 F 中的一个根。假定 $\mathrm{Aut}_K F \cong S_n$。证明：

(1) $K(u)/K$ 不是伽罗瓦扩张；$\mathrm{Aut}_K K(u)$ 可解。

(2) 不存在 K 的根式扩域 E 使得 $K \subset K(u) \subset E$.

证明. (1) 由假设 $f(x)$ 在 F 中必有 n 个互不相同的根

$$u = u_1, u_2, \cdots, u_n$$

(如果只有 $m < n$ 个互不相同的根，则 $\mathrm{Aut}_K F$ 同构与 S_m 的一个子群，与 $\mathrm{Aut}_K F \cong S_n$ 矛盾.) 并且，限制映射

$$\mathrm{Aut}_K F \longrightarrow S(u_1, \cdots, u_n)$$

是群同构。

如果 $K(u)$ 是伽罗瓦扩张，由于 $f(x)$ 不可约且在 $K(u)$ 中有根 u, 所以 $f(x)$ 在 $K(u)$ 上可分解为一次因式乘积，从而 $K(u)$ 是 $f(x)$ 在 K 上的分裂域，这导致 $K(u) = F$. 所以

$$n = \deg f = [F : K] \geqslant |\mathrm{Aut}_K F| = n!$$

这导致矛盾!

现计算 $\mathrm{Aut}_{K(u)} F$, 它恰为 $\mathrm{Aut}_K F$ 中保持 $u = u_1$ 不变的元素, 因此 $\mathrm{Aut}_{K(u)} F \cong S_{n-1}$. 假设 $K(u)$ 中有 m 个 $f(x)$ 在 F 中的根，则 $\mathrm{Aut}_{K(u)} F$ 中元素也可解释为 $\mathrm{Aut}_K F$ 中保持这 m 个根不变的元素，从而 $\mathrm{Aut}_{K(u)} F \cong S_{n-m}$, 从而 $S_{n-1} \cong S_{n-m}$. 由于 $n \geqslant 5$, 这导致 $m = 1$, 也就是说 $K(u)$ 中只有 u 这一个 $f(x)$ 根。由于 $\mathrm{Aut}_K K(u)$ 中任意元素必将 u 映为 $f(x)$ 的根，这导致 $\mathrm{Aut}_K K(u) = \{\mathrm{id}\}$, 当然是可解群。

(2) 如果存在根多扩张 E/K 包含 $K(u)$, 令 $\bar{K}$ 为 E 的代数闭包，则它同时也是 K 的代数闭包，

即 $K[x]$ 中所有多项式在 K 上的分裂域，可不妨设 $F \subseteq \bar{K}$. 现对任意 u_i, 存在 K 同构

$$\sigma_i : K(u) \to K(u_i)$$

使得 $\sigma_i(u) = u_i$. 根据分裂域的唯一性 (或者代数闭包的唯一性), σ_i 可以拓展为 $\bar{K}$ 的自同构 $\bar{\sigma}_i$, 令 $E_i = \bar{\sigma}_i(E)$, 则 E_i/K 也是根式扩张，利用定理 6.5 证明中的方法可得

$$\prod_{i=1}^{n} E_i$$

是 K 上的根式扩张且包含 F, 根据推论 6.7, $\mathrm{Aut}_K F$ 为可解群，这与 $S_n (n \geqslant 5)$ 不可解矛盾! □

习题 6.5

判断 $f(x) = x^5 + x^4 - x^3 - 4x^2 - 4x - 2 \in \mathbb{Q}[x]$ 能否根式解。

解: 可以在 $\mathbb{Z}[x]$ 中分解因式

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

从而发现 $f(x)$ 可根式解。

题目修改: 将 $f(x)$ 改为

$$f(x) = x^5 + x^4 - x^3 - 4x^2 - 4x + 2.$$

首先确定 $f(x)$ 在 $\mathbb{Q}[x]$ 中不可约。首先 $f(\pm 1), f(\pm 2)$ 都非零，因此 $f(x)$ 没有有理根，从而在 $\mathbb{Q}[x]$ 中没有一次因式。假设 $f(x)$ 在 $\mathbb{Q}[x]$ 中可约，则其也在 $\mathbb{Z}[x]$ 中可约，必能在 $\mathbb{Z}[x]$ 分解为一个首 1 二次不可约因式和一个首 1 三次因式的乘积, 假设首 1 二次因式为 $h(x) = x^2 + ax + b$, 则有

$$h(0) \mid f(0) = 2, \quad h(-1) \mid f(-1) = 3.$$

从而 $b = h(0) = \pm 1, \pm 2$,

$$h(-1) = 1 - a + b = \pm 1, \pm 3.$$

根据取值可唯一确定 $h(x)$, 再逐一验证发现 $h(x) \nmid f(x)$, 产生矛盾，从而确定 $f(x)$ 没有 2 次整系数因式，所以 $f(x)$ 不可约。进一步计算

$$f'(x) = 5x^4 + 4x^3 - 3x^2 - 8x - 4,$$
$$f''(x) = 20x^3 + 12x^2 - 6x - 8.$$

计算 $g(x) = f''(x - \frac{1}{5})$ 为

$$g(x) = 20x^3 - \frac{42}{5}x - \frac{162}{25}.$$

计算 $g(x)$ 的判别式

$$\Delta^2 = -4 \times \left(-\frac{42}{100}\right)^3 - 27 \times \left(-\frac{162}{500}\right)^2 < 0.$$

这说明 $g(x)$ 只有 1 个实数根，从而 $f''(x)$ 只有一个实数根，$f'(x)$ 只有一个极值点 (极小值)。同时，注意到 $f'(0) = -4 < 0$, 从而 $f'(x)$ 有一正一负两根。这说明 $f(x)$ 有两个极值点, 一个极大值点，一个极小值点。现在由于 $f(0) = 2 > 0$, 而 $f(1) = -6 < 0$, 因此 $f(x)$ 的极大值为正，极小值为负。由此可确定 $f(x)$ 恰有 3 个实数根。根据定理 5.8，$f(x)$ 在 $\mathbb{Q}$ 上的伽罗瓦群为 S_5，不可解，从而 $f(x)$ 不能根式解。 □

第七章　尺规作图

习题 7.1

证明：角 α 可以利用尺规作图三等分，当且仅当，$4x^3-3x-\cos\alpha$ 在 $\mathbb{Q}(\cos(\alpha))$ 中有根。

证明. 令 $\theta=\dfrac{\alpha}{3}$，则 θ 尺规可作当且仅当 $\cos\theta$ 从 $\mathbb{Q}(\cos\alpha)$ 出发尺规可作。

记 $f(x)=4x^3-3x-\cos\alpha$，如果 $f(x)$ 在 $\mathbb{Q}(\cos\alpha)$ 中没有根，那么 $f(x)$ 为 $\mathbb{Q}(\cos\alpha)$ 上不可约多项式，从而有

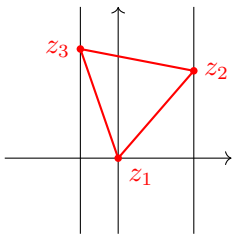
$$[\mathbb{Q}(\cos\alpha,\cos\theta):\mathbb{Q}(\alpha)]=3,$$

这导致 $\cos\theta$ 从 $\mathbb{Q}(\cos\alpha)$ 出发尺规不可作。如果 $f(x)$ 在 $\mathbb{Q}(\alpha)$ 中有根，要么 $\cos\theta$ 属于 $\mathbb{Q}(\cos\alpha)$，要么 $\cos\theta$ 是 $f(x)$ 在 $\mathbb{Q}(\alpha)[x]$ 中二次不可约因式的根。无论哪种情况，$\cos\theta$ 都是从 $\mathbb{Q}(\alpha)$ 出发尺规可作的。 □

习题 7.2

证明：任给平面上三条平行线，通过尺规作图可作正三角形，使得其三个顶点分别在这三条平行线上。

证明. 见下图



可以中间一条线为复平面的虚轴，其余两条中一条直线为复平面上实部为 1 的点对应的直线，此时，另一直线为对应实部为 u 的复数形成的直线。

可假设正三角形的一个顶点为 $z_1=0$，取

$$z_2=1+\frac{1-2u}{\sqrt{3}}i,\quad z_3=u+\frac{2-u}{\sqrt{3}}i$$

显然 z_2,z_3 都从 $\mathbb{Q}(u)$ 出发尺规可作，简单验证可知

$$z_2(\cos\frac{\pi}{3}+i\sin\frac{\pi}{3})=z_3$$

从而 z_1,z_2,z_3 构成正三角形的三个顶点。 □

习题 7.3

正 9 边形是否尺规可作？给定三角形，是否可以通过尺规作图做出一个正方形使得其与所给三角形面积相同？

证明. 由于 $9=3^2$，根据定理 7.8，正 9 边形尺规不可作。

对一个三角形，假设其三边长为 a,b,c，由 Heron 公式，其面积为

$$A=\sqrt{s(s-a)(s-b)(s-c)}$$

其中

$$s=\frac{a+b+c}{2}.$$

要求作的正方形的边长为 $\sqrt{A}$. A 是一个 $\mathbb{Q}(a,b,c)$ 上二次多项式的根，因此从 $Q(a,b,c)$ 出发尺规可作，从而 $\sqrt{A}$ 也从 $Q(a,b,c)$ 出发尺规可作。所以，对任意三角形都可以用尺规作图作出与之面积相同的正方形。 □

习题 7.4

假设 c 为 4 次有理系数不可约多项式 $g(x)$ 的根，$\mathrm{Gal}(g)$ 为 $g(x)$ 在 $\mathbb{Q}$ 上的伽罗瓦群。证明：c 尺规可作当且仅当 $\mathrm{Gal}(g)$ 不同构于 A_4 或者 S_4.

证明. 根据定理 7.5(3)，c 尺规可作当且仅当 $g(x)$ 在 $\mathbb{Q}$ 上分裂域 E 是 $\mathbb{Q}$ 上扩张次数是 2 的方幂。由于 $g(x)$ 在 $\mathbb{Q}$ 可分，因此 $E/\mathbb{Q}$ 是伽罗瓦扩张，从而 $|\mathrm{Gal}(g)|=[E:\mathbb{Q}]$ 是 2 的方幂。由于 $\mathrm{Gal}(g)$ 是 S_4 的可迁子群 (C_4,D_4,A_4,S_4)，其中阶数为 2 的方幂的是 C_4 和 D_4，即不同构于 A_4 或者 S_4. □

习题 7.5

利用 $\cos 5\theta = 16\cos^5\theta - 20\cos^3\theta + 5\cos\theta$ 证明：如果角 φ 满足 $\cos\varphi = \dfrac{5}{7}$，那么不能用尺规作图将 φ 五等分。

证明. 令 $\theta = \dfrac{\varphi}{5}$. 则 $\cos\theta$ 是多项式

$$f(x) = 16x^5 - 20x^3 + 5x - \frac{5}{7}$$

的根。根据 Eisenstein 差别法 (取 $p = 5$), $7f(x)$ 在 $\mathbb{Q}$ 上不可约，从而有

$$[\mathbb{Q}(\cos\theta) : \mathbb{Q}] = 5$$

不是 2 的方幂，根据推论 7.6，$\cos\theta$ 尺规不可作，从而 θ 尺规不可作，尺规作图不能将 φ 五等分。 □

第八章　e 和 π 的超越性

习题 8.1

假设 F/K 为域扩张，$\alpha_1,\cdots,\alpha_n \in \mathbb{F}$. 证明：$\alpha_1,\cdots,\alpha_n$ 在 K 上代数无关当且仅当 $\alpha_1,\cdots,\alpha_{n-1}$ 在 K 上代数无关且 α_n 是 $K(\alpha_1,\cdots,\alpha_{n-1})$ 上的超越元。

证明. 对任意 $r \geqslant 0$, 关于 $a_1,\cdots,a_{n-1}$ 的多项式

$$f_r(a_1,\cdots,a_{n-1}) = \sum \lambda^{(r)}_{d_1,\cdots,d_{n-1}} a_1^{d_1}\cdots a_{n-1}^{d_{n-1}}$$

则等式 $(*)$:

$$\sum_{r\geqslant 0} f_r(a_1,\cdots,a_{n-1})a_n^r = 0$$

等价于

$$\sum \lambda^{(r)}_{d_1,\cdots,d_{n-1}} a_1^{d_1}\cdots a_{n-1}^{d_{n-1}} a_n^r = 0$$

如果 $a_1,\cdots,a_n$ 在 K 上代数无关，当然有 $a_1,\cdots,a_{n-1}$ 在 K 上代数无关，并且上式中所有系数

$$\lambda^{(r)}_{d_1,\cdots,d_{n-1}} = 0$$

从而 $f_r = 0$ 对所有 $r \geqslant 0$ 成立，所以 a_n 在 $K[a_1,\cdots,a_{n-1}]$ 上是超越的。

反过来，任意 $a_1,\cdots,a_n$ 的多项式都可以写成如上 $(*)$ 的形式，如果 a_n 在 $K[a_1,\cdots,a_{n-1}]$ 上是超越的，那么 $(*)$ 中 $f_r = 0$ 对所有 r 成立，再利用 $a_1,\cdots,a_{n-1}$ 在 K 上代数无关可得到所有系数

$$\lambda^{(r)}_{d_1,\cdots,d_{n-1}} = 0$$

所以 $a_1,\cdots,a_n$ 在 K 上代数无关。 □

习题 8.2

假设 F/K 为域扩张，$S \subseteq F, v \in S, u \in F$. 证明：如果 u 是 $K(S)$ 上的代数元，但不是 $K(S\backslash\{v\})$ 上的代数元，则 v 是 $K((S\backslash\{v\})\cup\{u\})$ 上的代数元。

证明. 令 $L = K(S\backslash\{v\})$，则有 $K(S) = L(v)$. 由于 u 是 $L(v)$ 上代数元，存在不全为零的 $a_r \in L(v)$ 使得

$$\sum_{r\geqslant 0} a_r u^r = 0.$$

存在非零的 $h \in L[v]$ 使得 $ha_r \in L[v]$ 对所有 $r \geqslant 0$ 成立，因此

$$sum_{r\geqslant 0} h a_r u^r = 0$$

这个等式可写成

$$\sum \lambda_{s,r} v^s u^r = 0$$

形式，其中 $\lambda_{s,r}$ 不全为零，将等式左边看作关于 v 的多项式，根据假设 u 在 L 上是超越元，因此这个关于 v 的多项式相应的系数

$$\sum_{r\geqslant} \lambda_{s,r} u^r$$

不全为零，从而 v 是 $L(u)$ 上的代数元。 □

习题 8.3

假设 α 为非零代数数，证明：$\sin\alpha, \cos\alpha, \tan\alpha, \cot\alpha$ 都是超越数。

证明. 反证法，假设 $\sin\alpha$ 是代数数，则

$$\cos\alpha = \pm\sqrt{1-\sin^2\alpha}$$

也是代数数，从而

$$e^{i\alpha} = \cos\alpha + i\sin\alpha$$

也是代数数，这与林德曼-魏尔斯特拉斯定理矛盾。

注意到

$$\sin\alpha = \pm\sqrt{1-\cos^2\alpha}$$
$$\cos\alpha = \pm\frac{1}{\sqrt{1+\tan^2\alpha}}$$
$$\sin\alpha = \pm\frac{1}{\sqrt{1+\cot^2\alpha}}$$

可类似证明 $\cos\alpha, \tan\alpha, \cot\alpha$ 都是超越数。 □

习题 8.4

证明：如果 Schanuel 猜想成立，则 e,π 在 $\mathbb{Q}$ 上代数无关，$e+\pi, e\pi$ 为超越数。

证明. 取 $z_1 = 1, z_2 = i\pi$, 它们在 $\mathbb{Q}$ 上线性无关, 如果 Schanuel 猜想成立，那么

$$1, i\pi, e^1, e^\pi = -1$$

中至少有 2 个在 $\mathbb{Q}$ 上代数无关，而这两个数只能是 e 和 $i\pi$, 由于 i 是 $\mathbb{Q}$ 上代数元，因此 e,π 在 $\mathbb{Q}$ 上代数无关，这样就导致 $e+\pi$ 和 $e\pi$ 都是超越数。(需要指出的是，目前还不能证明这两个数是无理数) □

第九章　模 p 法求伽罗瓦群 *

习题 9.1

证明：x^5+3x^2+2x+3 在 $\mathbb{Q}$ 上的伽罗瓦群为 S_5.

证明. 记 $f(x)=x^5+3x^2+2x+3$, 很容易证明 $f(x)$ 在 $\mathbb{Z}_2[x]$ 中不可约, 从而 $f(x)$ 不可约, 从而 $\mathrm{Gal}(f)$ 是 S_5 的可迁子群且 $5\mid|\mathrm{Gal}(f)|$, 因此 $\mathrm{Gal}(f)$ 包含一个 5 循环。另一方面, $f(x)$ 在 $\mathbb{Z}_3[x]$ 中 $f(x)$ 可分解为

$$x(x+1)(x+2)(x^2+1)$$

由定理 9.4, $\mathrm{Gal}(f)$ 中包含一个 2 循环, 根据引理 5.7 有 $\mathrm{Gal}(f)=S_5$. □

习题 9.2

证明：x^7-x-1 在 $\mathbb{Q}$ 上的伽罗瓦群为 S_7.

证明. 令 $f(x)=x^7-x-1$. 取模 2, 在 $\mathbb{Z}_2[x]$ 中考虑有所有次数不超过 3 的不可约多项式

$$x, x+1, x^2+x+1, x^3+x^2+1, x^3+x+1$$

都不整除 $f(x)$, 因此 $f(x)$ 模 2 后在 $\mathbb{Z}_2[x]$ 中不可约, 从而在 $\mathbb{Q}[x]$ 中不可约, $\mathrm{Gal}(f)$ 是 S_7 的可迁子群且包含一个 7 循环。

在模 3 的情形下 x^7-x-1 可分解为:

$$(x^2+x+2)(x^5+2x^4+2x^3+2x+1)$$

容易验证这两个因式在模 3 的意义下是不可约的。根据定理 9.4, $\mathrm{Gal}(f)$ 中包含 $\tau\sigma$ 形式的元素, 其中 τ 为对换, 而 σ 为一个与 τ 不相交的 5 循环。这样 $\mathrm{Gal}(f)$ 包含 $(\tau\sigma)^5=\tau^5=\tau$ 这个对换。根据引理 5.7 可得 $\mathrm{Gal}(f)=S_7$. □

习题 9.3

证明：如果 H 是 S_n 的可迁子群且同时包含一个对换和 $n-1$ 循环，则 $H=S_n$.

证明. 可假设 $n-1$ 循环为 $\sigma=(12\cdots n-1)$, 而对换为 $\tau=(i\,j)$. 由于 H 是可迁的, 因此存在 $\eta\in H$ 使得 $\eta(j)=n$, 从而有

$$\eta\tau\eta^{-1}=(\eta(i)\,\eta(j))=(a\,n)$$

其中 $a\neq n$. 对任意 $1\leqslant i<n$, 存在 k 使得 $\sigma^k(a)=i$, 从而

$$\sigma^k(a\,n)\sigma^{-k}=(i\,n).$$

这说明 $(i\,n)\in H$ 对所有 $1\leqslant i<n$ 成立, 从而 $H=S_n$. □

习题 9.4

确定多项式 $f(x)=x^6-12x^4+15x^3-6x^2+15x+12$ 在 $\mathbb{Q}$ 上的伽罗瓦群。

解. 取素数 $p=3$, 根据 Eisenstein 判别法, $f(x)$ 是 $\mathbb{Q}[x]$ 中不可约多项式, 从而 $\mathrm{Gal}(f)$ 是 S_6 的可迁子群。在模 2 和模 5 下 $f(x)$ 分解成不可约多项式乘积如下:

$$x(x^5+x^2+1)$$

$$(x^2+3)\prod_{i=1}^{4}(x+i)$$

根据定理 9.4, $\mathrm{Gal}(f)$ 含一个 5 循环和一个对换, 根据习题 9.3, $\mathrm{Gal}(f)=S_6$. □

习题 9.5

构造一个整系数多项式 $f(x)$, 使得 $f(x)$ 在 $\mathbb{Q}$ 上的伽罗瓦群为 S_4.

解. 根据引理 9.5 后面的方法，我们可以取

$$f_1(x)=x^4+x+1$$

在 $\mathbb{Z}_2[x]$ 中不可约；取

$$f_2(x)=(x-1)(x^3+2x+1),$$

这里 x^3+2x+1 在 $\mathbb{Z}_3[x]$ 中不可约；取

$$f_3(x)=(x^2+2)(x-1)x$$

其中 x^2+2 在 $\mathbb{Z}_5[x]$ 中不可约。最后令

$$\begin{aligned} f(x) &= -15f_1(x)+10f_2(x)+6f_3(x) \\ &= x^4-16x^3+32x^2-17x-25 \end{aligned}$$

则有 $\mathrm{Gal}(f)=S_4$. □