Galois 理论初步

戚天成 ✉

复旦大学 数学科学学院

2024 年 1 月 14 日

这是我过去参考 [Yan13] 学习初等 Galois 理论的笔记汇总, 主要考虑有限扩张的场景. 主要记录了 Galois 基本定理的证明、证明所需相关前置知识以及 Galois 基本定理在下述 Abel–Ruffini 定理的证明上的应用.

Abel–Ruffini theorem. 设正整数 $n \geq 5$, 那么 $\mathbb{C}$ 上 n 次代数方程不存在用根式表达的求根公式.

由于水平有限, 虽然我全力以赴, 但还是无法避免笔记中存在不足与错误, 欢迎指出, 谢谢.

目录

1 基本准备

1.1 可解群

本节我们回顾可解群的概念、关于导群的刻画. 并说明 n 次对称群 S_n 可解当且仅当 $n \leq 4$.

Definition 1.1. 若群 G 有子群列 $G = G_1 \geq G_2 \geq G_3 \geq \cdots \geq G_s \geq G_{s+1} = \{1_G\}$, 这里 s 是正整数, 满足对每个正整数 $1 \leq i \leq s$, G_{i+1} 是 G_i 的正规子群, 则称上述子群列是**群 G 的一个正规列**, 记作 $G = G_1 \trianglerighteq G_2 \trianglerighteq G_3 \trianglerighteq \cdots \trianglerighteq G_s \trianglerighteq G_{s+1} = \{1_G\}$, 每个 G_i/G_{i+1} 称为该正规列的**商因子**. 如果群 G 有个正规列满足每个商因子都是 Abel 群, 则称群 G 是**可解群**.

下面的例子表明对称群 S_n 当 $n \geq 5$ 时不是可解群, 我们将在 Abel-Ruffini 定理的证明中使用该事实.

Example 1.2. 设 n 是正整数, 则当 $n \leq 4$ 时对称群 S_n 可解, 当 $n \geq 5$ 时对称群 S_n 不可解.

Proof. S_1 与 S_2 的可解性是明显的. S_3 有正规列 $S_3 \trianglerighteq A_3 \trianglerighteq \{(1)\}$, 它的两个商因子都是 Abel 群, 所以 S_3 可解. 当 $n = 4$ 时, 记 $K = \{(1), (12)(34), (14)(23), (24)(13)\}$, 易验证 K 是 S_n 的正规子群, 所以 S_4 有正规列 $S_4 \trianglerighteq A_4 \trianglerighteq K \trianglerighteq \{(1)\}$, 它每个商因子都是 Abel 群, 所以 S_4 是可解群. 最后我们来看 $n \geq 5$ 的情形, 假设 S_n 可解, 那么有商因子都是 Abel 群的正规列 $S_n \trianglerighteq G_2 \trianglerighteq G_3 \trianglerighteq \cdots \trianglerighteq G_s \trianglerighteq \{(1)\}$, 那么存在正整数 $i \geq 2$ 使得 $G_i \neq S_n$, 设 l 是使得 $G_l \neq S_n$ 的最小正整数, 因为 S_n 的正规子群只有 $S_n, A_n, \{(1)\}$, 所以 $G_l = A_n$ 或 $\{(1)\}$, 但 G_{l-1}/G_l 是交换群, 所以 $G_l = A_n$. 因为 A_n 不是交换群, 所以存在正整数 $l+1 \leq t \leq s$ 使得 $G_t \neq A_n$, 设 t 是满足条件的最小正整数, 那么由 A_n 是单群知 $G_t = \{(1)\}$, 于是 $G_{t-1}/G_t \cong A_n$ 非交换, 矛盾. □

对群 G, 我们也将 G 的换位子群记作 G' 或 $G^{(1)}$, 将 G' 的换位子群记作 G'' 或 $G^{(2)}$, 递归地可以定义 $G^{(k)} = (G^{(k-1)})', k \geq 2$, 称 $G^{(k)}$ 为 G 的 k **次导群**. G 的零次导群定义为 G 本身. 通过可解群的定义不难验证

Lemma 1.3. 给定群 G, 那么 G 可解的充要条件是存在正整数 k 使得 $G^{(k)} = \{1_G\}$.

Remark 1.4. 通过这一可解性的刻画不难看出可解群的同态像仍可解.

1.2 对称多项式

本节主要回顾线性代数中的对称多项式的基本概念与对称多项式基本定理 (见 [定理1.5]). 给定含幺环 R 上的 n 元多项式环 $R[x_1, x_2, ..., x_n]$, 如果 R 中多项式 $f(x_1, x_2, ..., x_n) \in R[x_1, x_2, ..., x_n]$ 满足 $f(x_1, x_2, ..., x_n) = f(x_{\sigma(1)}, x_{\sigma(2)}, ..., x_{\sigma(n)}), \forall \sigma \in S_n$, 则称 $f(x_1, ..., x_n)$ 是 R 上一个**对称多项式**. 称下面的 n 个对称多项式

$$\begin{aligned}
\sigma_1 &= \sigma_1(x_1, ..., x_n) = x_1 + x_2 + \cdots + x_n, \\
\sigma_2 &= \sigma_2(x_1, ..., x_n) = \sum_{1 \leq i < j \leq n} x_i x_j \\
&\cdots \\
\sigma_n &= \sigma_n(x_1, ..., x_n) = x_1 x_2 \cdots x_n
\end{aligned}$$

为**初等对称多项式**, 易见初等对称多项式都是对称多项式. S_n 可自然地作用到多项式环 $R[x_1, x_2, ..., x_n]$ 上:

$$S_n \times R[x_1, x_2, ..., x_n] \to R[x_1, x_2, ..., x_n],$$

$$\left(\sigma, \sum_{i_1, i_2, ..., i_n} a_{i_1 i_2 \cdots i_n} x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}\right) \mapsto \sum_{i_1, i_2, ..., i_n} a_{i_1 i_2 \cdots i_n} x_{\sigma(1)}^{i_1} x_{\sigma(2)}^{i_2} \cdots x_{\sigma(n)}^{i_n}$$

易见这是定义合理的群作用且该作用的不动点集就是对称多项式全体. 易验证对称多项式的和与积都是对称多项式. 对任给对称多项式 $f_1, f_2, ..., f_m \in R[x_1, x_2, ..., x_n]$ 以及多项式 $g \in R[x_1, x_2, ..., x_m]$ 有 $g(f_1, f_2, ..., f_m)$ 也是对称多项式. 之后我们会用到下面的对称多项式基本定理.

Theorem 1.5. 设 R 是含幺环, $f(x_1, x_2, ..., x_n)$ 是 R 上对称多项式, 则存在 R 上唯一的 n 元多项式

$$g \in R[x_1, x_2, ..., x_n]$$

使得 $f(x_1, x_2, ..., x_n) = g(\sigma_1, \sigma_2, ..., \sigma_n)$, 这里 σ_i 表示第 i 个初等对称多项式.

Proof. 先证明存在性, 不妨设 $f \neq 0$, 并设 $f(x_1, x_2, ..., x_n)$ 在对各单项式幂指数组字典排序意义下的首项是 $ax_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$, 则由 f 是对称多项式知 $i_n \leq i_{n-1} \leq \cdots \leq i_2 \leq i_1$(因为如果有某个 $i_{k+1} > i_k$, 那么 $ax_1^{i_1}\cdots x_k^{i_{k+1}}x_{k+1}^{i_k}\cdots x_n^{i_n}$ 也是 f 中的项, 与 $ax_1^{i_1}x_2^{i_2}\cdots x_n^{i_n}$ 是首项的假定矛盾). 命 $g_1(x_1, x_2, ..., x_n) = a\sigma_1^{i_1-i_2}\sigma_2^{i_2-i_1}\cdots\sigma_{n-1}^{i_{n-1}-i_n}\sigma_n^{i_n}$, 那么 g_1 是对称多项式并且与 f 具有相同的首项, 故 $f_1 = f - g_1$ 要么是零多项式要么是首项后于 f 的非零多项式, 如果 f_1 是零多项式, 存在性成立, 否则, 设 f_1 的首项为 $bx_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}, b \neq 0, i_1 \geq k_1 \geq \cdots \geq k_n \geq 0$, 这样的自然数 $k_1, ..., k_n$ 是有限的, 所以对 f_1 重复上述讨论, 必在有限步后得到某个 $f_s = 0$, 即 $f_1 = f - g_1, f_2 = f_1 - g_2, ..., f_{s-1} = f_{s-2} - g_{s-1}, f_s = f_{s-1} - g_s = 0$, 于是 $f = g_1 + g_2 + \cdots + g_s$ 是初等对称多项式的多项式, 这就证明了存在性. 下证唯一性, 如果 $g(x_1, x_2, ..., x_n)$ 与 $h(x_1, x_2, ..., x_n)$ 满足 $g(\sigma_1, \sigma_2, ..., \sigma_n) = h(\sigma_1, \sigma_2, ..., \sigma_n) = f$, 我们说明 $\varphi(x_1, x_2, ..., x_n) = g(x_1, x_2, ..., x_n) - h(x_1, x_2, ..., x_n)$ 是零多项式. 这里使用反证法, 如果 $\varphi(x_1, x_2, ..., x_n) \neq 0$, 那么由 $\varphi(\sigma_1, \sigma_2, ..., \sigma_n) = 0$ 可知 $\varphi(x_1, x_2, ..., x_n)$ 不可能是非零单项式. 现设 $cx_1^{k_1}x_2^{k_2}\cdots x_n^{k_n}$ 与 $dx_1^{l_1}x_2^{l_2}\cdots x_n^{l_n}$ 是 $\varphi(x_1, x_2, ..., x_n)$ 的两个不是同类项的非零单项式, 那么多项式 $c\sigma_1^{k_1}\sigma_2^{k_2}\cdots\sigma_n^{k_n}$ 的首项 $cx_1^{k_1+k_2+\cdots+k_n}x_2^{k_2+\cdots+k_n}\cdots x_n^{k_n}$ 与多项式 $d\sigma_1^{l_1}\sigma_2^{l_2}\cdots\sigma_n^{l_n}$ 的首项 $dx_1^{l_1+l_2+\cdots+l_n}x_2^{l_2+\cdots+l_n}\cdots x_n^{l_n}$ 不是同类项, 这说明 $\varphi(\sigma_1, \sigma_2, ..., \sigma_n)$ 的首项是这些首项中排在最前面的一个, 所以 $\varphi(\sigma_1, \sigma_2, ..., \sigma_n)$ 的首项非零, 矛盾. 这就证明了唯一性. □

1.3 代数闭包

本节回顾给定域的代数闭包的基本构造并说明其同构唯一性. 先回顾域的代数闭包的定义.

Definition 1.6. 给定域 F, 若域扩张 $E \supseteq F$ 是代数扩张且 E 是代数闭域, 则称 E 是 F 的**代数闭包**.

下述定理的构造来自 E. Artin, 事实上域的代数闭包还在同构意义下唯一, 我们稍后在 [推论1.9] 证明.

Theorem 1.7. 任给域 F, F 的代数闭包 $\overline{F}$ 存在.

Proof. 设 I 是 $F[x]$ 中全体首一不可约多项式构成的集合, 命 $R = F[\{x_f\}_{f\in I}]$ 是以 I 为指标集的未定元集所定义的多元多项式环. 考虑 R 中由集合 $\{f(x_f)|f \in I\}$ 所生成的理想 A, 我们断言 A 是 R 中真理想. 如果 $A = R$, 则存在 $g_1, g_2, ..., g_m \in R, f_1, f_2, ..., f_m \in I$ 使得 $g_1f_1(x_{f_1}) + g_2f_2(x_{f_2}) + \cdots + g_mf_m(x_{f_m}) = 1_F$. 设正整数 $s \geq m$ 使得 $g_1, g_2, ..., g_m \in F[x_{f_1}, x_{f_2}, ..., x_{f_s}]$, 因为 $f_1, f_2, ..., f_m$ 次数均不低于 1, 所以由 Kronecker 定理知存在 F 的扩域 E 使得 $f_1, ..., f_m$ 都在 E 中有根, 设 $\alpha_1, \alpha_2, ..., \alpha_m$ 满足 $f_k(\alpha_k) = 0, \forall 1 \leq k \leq m$. 对 $m < l \leq s$, 记 $\alpha_l = 0$, 考虑赋值映射

$$\mathrm{ev}_{(\alpha_1,\alpha_2,...,\alpha_s)} : F[x_{f_1}, x_{f_2}, ..., x_{f_s}] \to E, \sum_{i_1,i_2,...,i_s} a_{i_1i_2\cdots i_s}x_{f_1}^{i_1}x_{f_2}^{i_2}\cdots x_{f_s}^{i_s} \mapsto \sum_{i_1,i_2,...,i_s} a_{i_1i_2\cdots i_s}\alpha_1^{i_1}\alpha_2^{i_2}\cdots\alpha_s^{i_s}$$

那么

$$0 = g_1(\alpha_1, ..., \alpha_s)f_1(\alpha_1) + g_2(\alpha_1, ..., \alpha_s)f_2(\alpha_2) + \cdots + g_m(\alpha_1, ..., \alpha_s)f_m(\alpha_m) = 1_F$$

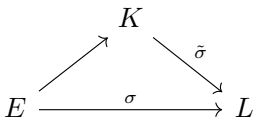
得到矛盾, 所以理想 A 是真理想, 于是存在 R 中极大理想 M 使得 $M \supseteq A$. 于是单环同态 $i_F : F \to R/M, k \mapsto k + M$ 导出 F 的域扩张 $F_1 \supseteq F$ 使得 F 上任意首一不可约多项式在 F_1 中都有根. 递归地, 可以得到扩域链 $F \subseteq F_1 \subseteq F_2 \subseteq \cdots \subseteq F_n \subseteq \cdots$ 满足每个 F_i 上的首一不可约多项式都在 F_{i+1} 中有根, 置

$$L \triangleq \bigcup_{n=1}^{\infty} F_n,$$

则 L 上可天然定义加法与乘法使得 L 成为域. 任取 L 上次数不低于 1 的多项式 $f(x)$, 那么存在某个 F_n 使得 $f(x)\in F_n[x]$, 于是 f 在 $F_{n+1}\subseteq L$ 上有根, 所以 L 是代数闭域. 现设 $\overline{F}$ 是 L 中全体 F 上代数元构成的集合, 易见 $\overline{F}$ 是域, 所以 $\bar{F}$ 是 F 的代数扩张. 我们下面验证 $\overline{F}$ 是 F 的代数闭包, 只需说明 $\overline{F}$ 是代数闭域, 任取 $f(x)\in\overline{F}[x]$, 则由 L 是代数闭域知存在 $c\in L$ 使得 $f(c)=0$, 下证 $c\in\overline{F}$, 因为 $\overline{F}(c)$ 是 $\overline{F}$ 的有限扩张, 所以 $\overline{F}(c)$ 是 F 的代数扩张, 特别地, c 是 F 上代数元, 即 $c\in\overline{F}$. □

下面的结果表明任何域 E 到一代数闭域 L 的保幺环同态都可以延拓至 E 的代数扩张上.

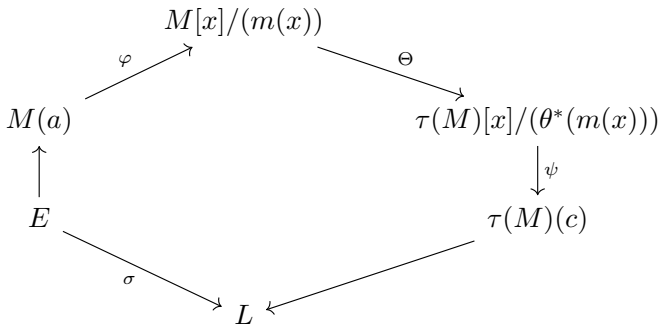
Theorem 1.8. 设 E,L 是域, 其中 L 是代数闭域, $\sigma:E\to L$ 是非零环同态, K 是 E 的代数扩张, 则存在环同态 $\tilde{\sigma}:K\to L$ 使得 $\tilde{\sigma}|_E=\sigma$.



Proof. 命 $S=\{(F,f)|F是K\supseteq E的中间域,f:F\to L是环同态且f|_E=\sigma\}$, 那么 S 是集合且 $(E,\sigma)\in S$ 表明 S 是非空的. 在 S 上定义二元关系 $\leq$:$(F_1,f_1)\leq(F_2,f_2)\Leftrightarrow F_1\subseteq F_2, f_2|_{F_1}=f_1$. 容易验证 $(S,\leq)$ 是非空偏序集, 且任何全序子集 $\{(F_\alpha,f_\alpha)|\alpha\in\Lambda\}$ 有上界 (F,f), 这里 $F=\bigcup\limits_{\alpha\in\Lambda}F_\alpha$, $f:F\to L, x\mapsto f_\alpha(x)$(对每个 $x\in F$, 存在 $\alpha\in\Lambda$ 使得 $x\in F_\alpha$, 这里定义 $f(x)=f_\alpha(x)$, 容易验证 f 是定义合理的环同态), 故由 Zorn 引理知上述偏序集有极大元 (M,τ), 我们断言 $M=K$. 若不然, 设 M 是 K 的真子域, 那么存在 $a\in K-M$, 设 a 在 M 上首一最小多项式是 $m(x)$, 那么 $\varphi:M(a)\to M[x]/(m(x)), g(a)\mapsto g(x)+(m(x))$ 是环同构. 因为 τ 是非零环同态, 所以由 M 是域可知 $\tau:M\to L$ 是单保幺环同态, 进而有域同构 $\theta:M\to\tau(M), x\mapsto\tau(x)$, 这导出多项式环间的同构 $\theta^*:M[x]\to\tau(M)\sum\limits_{i=0}^{l}b_ix^i\mapsto\sum\limits_{i=0}^{l}\tau(b_i)x^i$, 易见 $\tau(M)$ 是 L 的子域. 因为 $m(x)$ 是 $M[x]$ 中不可约多项式, 所以由 θ^* 是同构可知 $\theta^*(m(x))$ 是 $\tau(M)[x]$ 中的不可约多项式. 因为 L 是代数闭域, 所以 $\theta^*(m(x))$ 在 L 中有根 c, 于是有环同构 $\psi:\tau(M)[x]/(\theta^*(m(x)))\to\tau(M)(c), h(x)+(\theta^*(m(x)))\mapsto h(c)$. 并注意到 θ^* 导出环同构 $\Theta:M[x]/(m(x))\to\tau(M)[x]/(\theta^*(m(x))), g(x)+(m(x))\mapsto\theta^*(m(x))+(\theta^*(m(x)))$.

$$M(a)\xrightarrow{\varphi}M[x]/(m(x))\xrightarrow{\Theta}\tau(M)[x]/(\theta^*(m(x)))\xrightarrow{\psi}\tau(M)(c)\longrightarrow L$$

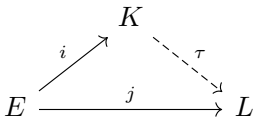
注意到 $\psi\Theta\varphi$ 能够诱导一个 $M(a)$ 到 L 的环同态且容易验证下图交换:



这与 (M,τ) 是极大元矛盾. 因此 $M=K$, 取 $\tilde{\sigma}=\tau$ 即得结果. □

Corollary 1.9. 任何域的代数闭包在同构意义下唯一.

Proof. 设域 E 有代数闭包 K, L, 并设 $i : E \to K, j : E \to L$ 是标准嵌入. 那么由代数闭包的定义以及 [定理1.8] 知存在环同态 $\tau : K \to L$ 使得下图交换:



那么 τ 是单环同态, 下面通过说明 $\tau(K) = L$ 来得到 τ 是环同构. 注意到 L 是 E 的代数扩张且 $\tau(K) \supseteq E$, 所以 L 是 $\tau(K)$ 的代数扩张. 由 K 是代数闭域保证了 $\tau(K)$ 也是代数闭域, 这迫使 $L = \tau(K)$. □

2 Galois 理论初步

这部分我们先引入域扩张的 Galois 群的概念, 针对有限扩张引入 Galois 扩张的概念, 发展 Galois 扩张的基本理论, 推导有限 Galois 基本定理并给出有限 Galois 扩张的刻画, 最后我们引入 Abel 扩张与可解扩张的概念, 建立可解扩张的一些基本理论, 我们将使用它们去证明 Abel-Ruffini 定理.

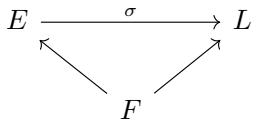
2.1 Galois 扩张

设 F 是域, 记 $\mathrm{Aut}F$ 是全体域 F 到 F 的域同构构成的集合, 那么 $\mathrm{Aut}F$ 关于映射复合构成群, 称为域 F 的**自同构群**. 若域 F, E 都是 K 的域扩张, 容易验证非零环同态 $\sigma : E \to F$ 是 K-线性映射的充要条件是 $\sigma(k) = k, \forall k \in K$. 若非零环同态 $\sigma : E \to F$ 也是 K-线性映射, 我们称 σ 是一个 **K-同态**. 如果域 F 是 K 的域扩张, 自同构 $\sigma \in \mathrm{Aut}F$ 满足 σ 是一个 K-同态, 则称 σ 是 F 的一个 **K-自同构**. 记 $\mathrm{Aut}_K F$ 是 F 的所有 K-自同构构成的集合, 易见它关于映射复合构成 $\mathrm{Aut}F$ 的子群, 称群 $\mathrm{Aut}_K F$ 是 F **在 K 上的 Galois 群**, 以下也称为**域扩张 $F \supseteq K$ 的 Galois 群**. 易见 $\mathrm{Aut}_K F = \{\sigma \in \mathrm{Aut}F | \sigma(k) = k, \forall k \in K\}$, 即 Galois 群中的元素就是那些 F 上固定 K 中每个点的自同构.

给定域扩张 $E \supseteq F$, 则对该域扩张的任意中间域 K(即 K 是 E 的子域, F 是 K 的子域), 群 $\mathrm{Aut}_K E$ 是群 $\mathrm{Aut}_F E$ 的子群. 对 $\mathrm{Aut}_F E$ 的任何子群 H, 易见 $E^H = \{c \in E | \sigma(c) = c, \forall \sigma \in H\}$ 是域扩张 $E \supseteq F$ 的中间域, 称为 H 的**固定子域**. 所以如果记 $\mathrm{Aut}_F E$ 所有子群构成的集合为 Σ, 域扩张 $E \supseteq F$ 的所有中间域构成的集合是 Ω, 则有映射 $\psi : \Omega \to \Sigma, K \mapsto \mathrm{Aut}_K E$ 以及 $\varphi : \Sigma \to \Omega, H \mapsto E^H$, 容易验证有下面的事实成立 (之后介绍的 Galois 理论基本定理表明在适当条件下这里的 ψ 与 φ 都是双射).

Lemma 2.1. 给定域扩张 $E \supseteq F$, 设 $\psi : \Omega \to \Sigma, K \mapsto \mathrm{Aut}_K E, \varphi : \Sigma \to \Omega, H \mapsto E^H$, 则
(1) 对任给域扩张 $E \supseteq F$ 的中间域 $K_1 \subseteq K_2$, 有 $\psi(K_2) \subseteq \psi(K_1)$, 即 $\mathrm{Aut}_{K_2} E \subseteq \mathrm{Aut}_{K_1} E$;
(2) 对任给 $\mathrm{Aut}_F E$ 的子群 $H_1 \subseteq H_2$, 有 $\varphi(H_2) \subseteq \varphi(H_1)$, 即 $E^{H_2} \subseteq E^{H_1}$;
(3) 对任给域扩张 $E \supseteq F$ 的中间域 K, 有 $K \subseteq E^{\mathrm{Aut}_K E}$, 即 $K \subseteq \varphi\psi(K)$;
(4) 对任给 $\mathrm{Aut}_F E$ 的子群 H, 有 $H \subseteq \mathrm{Aut}_{E^H} E$, 即 $H \subseteq \psi\varphi(H)$

给定设域 E, L 都是域 F 的扩张, 如果单的环同态 $\sigma : E \to L$ 满足 $\sigma(a) = a, \forall a \in F$, 即下图交换:



则称环同态 $\sigma : E \to L$ 是域扩张 $E \supseteq F$ 到 L 的**嵌入**. 下面我们说明当域扩张 $E \supseteq F$ 是有限扩张时, 该域扩张到 L 的嵌入总数是有限的, 并且被该域扩张的次数 $[E : F]$ 控制.

Proposition 2.2. 设 $E \supseteq F$ 是域的有限扩张, $L \supseteq F$ 是域扩张. 则 $E \supseteq F$ 到 L 的嵌入总数不超过 $[E : F]$.

Proof. 为叙述方便, 记 $n = [E : F]$, 假设至少有 $n+1$ 个域扩张 $E \supseteq F$ 到 L 的嵌入 $\sigma_1, \sigma_2, ..., \sigma_{n+1}$, 设 F-线性空间 E 的一个基为 $\alpha_1, \alpha_2, ..., \alpha_n$, L^n 中的 $n+1$ 个列向量

$$\begin{pmatrix} \sigma_1(\alpha_1) \\ \sigma_1(\alpha_2) \\ \vdots \\ \sigma_1(\alpha_n) \end{pmatrix}, \begin{pmatrix} \sigma_2(\alpha_1) \\ \sigma_2(\alpha_2) \\ \vdots \\ \sigma_2(\alpha_n) \end{pmatrix}, ..., \begin{pmatrix} \sigma_{n+1}(\alpha_1) \\ \sigma_{n+1}(\alpha_2) \\ \vdots \\ \sigma_{n+1}(\alpha_n) \end{pmatrix}$$

L-线性相关, 因此存在不全为零的元素 $k_1, k_2, ..., k_{n+1} \in L$ 使得

$$\sum_{i=1}^{n+1} \sigma_i(\alpha_j) k_i = 0, \forall 1 \le j \le n.$$

所以对任给 $\alpha \in E$ 有 $\sum\limits_{i=1}^{n+1} \sigma_i(\alpha) k_i = 0$, 结合 σ_i 是单射可知这与下面的 [引理2.3] 矛盾. □

Lemma 2.3. 给定群 G 与域 F, 设 $\chi_1, \chi_2, ..., \chi_n$ 是 G 到 F 乘法群 F^* 两两不同的同态, $a_1, a_2, ..., a_n$ 是 F 中不全为零的元素, 则存在 $g \in G$ 使得 $a_1\chi_1(g) + a_2\chi_2(g) + \cdots + a_n\chi_n(g) \neq 0$.

Proof. 对正整数 n 作归纳, 当 $n = 1$ 时结论明显成立. 假设结论对 $n-1 (n \ge 2)$ 成立, 现给定不全为零的元素 $a_1, a_2, ..., a_n$, 若某个 $a_k = 0$, 由归纳假设直接得到结果, 下设 $a_1, a_2, ..., a_n \neq 0$. 因为 χ_1, χ_2 是不同的同态, 所以存在 $h \in G$ 使得 $\chi_2(h) - \chi_1(h) \neq 0$, 故 $a_2(\chi_2(h) - \chi_1(h)), a_3(\chi_3(h) - \chi_1(h)), ..., a_n(\chi_n(h) - \chi_1(h))$ 不全为零, 于是对 $\chi_2, ..., \chi_n$ 以及 $a_2(\chi_2(h) - \chi_1(h)), a_3(\chi_3(h) - \chi_1(h)), ..., a_n(\chi_n(h) - \chi_1(h))$ 用归纳假设可知存在 $g \in G$ 使得

$$a_2(\chi_2(h) - \chi_1(h))\chi_2(g) + a_3(\chi_3(h) - \chi_1(h))\chi_3(g) + \cdots + a_n(\chi_n(h) - \chi_1(h))\chi_n(g) \neq 0.$$

因此 $a_1\chi_1(hg) + a_2\chi_2(hg) + \cdots + a_n\chi_n(hg) \neq \chi_1(h)(a_1\chi_1(g) + a_2\chi_2(g) + \cdots + a_n\chi_n(g))$, 于是知 $a_1\chi_1(hg) + a_2\chi_2(hg) + \cdots + a_n\chi_n(hg)$ 与 $a_1\chi_1(g) + a_2\chi_2(g) + \cdots + a_n\chi_n(g)$ 中至少有一个非零. □

因为群 $\mathrm{Aut}_F E$ 中的元素就是所有域扩张 $E \supseteq F$ 到 E 的嵌入, 所以我们得到

Corollary 2.4. 对有限扩张 $E \supseteq F$, 有 $|\mathrm{Aut}_F E| \le [E : F]$.

Definition 2.5. 若有限扩张 $E \supseteq F$ 满足 $|\mathrm{Aut}_F E| = [E : F]$, 我们称该域扩张为 **Galois 扩张**.

根据定义易验证 $\mathbb{C} \supseteq \mathbb{R}$ 就是 Galois 扩张. 一般地, 有

Example 2.6. 设域 F 特征不是 2, 域 E 是 F 的二次扩张, 即 $[E : F] = 2$, 则该扩张是 Galois 扩张.

Proof. 取 $\alpha \in E-F$, 那么 $\{1_F, \alpha\}$ 构成 E 作为 F-线性空间的一个基, 由此可知 $E = F[\alpha]$. 易知 α 作为 F 上代数元, 其在 F 上首一最小多项式是 2 次的, 设为 $m(x) = x^2 + a_1x + a_0$, 它是 $F[x]$ 中不可约多项式. 那么利用 F 的特征不是 2 可得 $m(x)$ 作为 $E[x]$ 中多项式在 E 中无重根, 设另一根为 β, 则 $m(x) = (x-\alpha)(x-\beta), \alpha \neq \beta$ 且 $\beta \notin F$. 容易验证 $\tau : E \to E, a + b\alpha \mapsto a + b\beta$ 是域同构且 $\tau(a) = a, \forall a \in F$, 因此 $\tau \in \mathrm{Aut}_F E$. 故 $2 \leq |\mathrm{Aut}_F E| \leq [E : F] = 2$, 这迫使 $|\mathrm{Aut}_F E| = [E : F] = 2$. □

下面的命题表明有限域的有限扩张总是 Galois 扩张.

Proposition 2.7. 设 E 是有限域 F 是有限扩张, 则该扩张是 Galois 扩张且 Galois 群 $\mathrm{Aut}_F E$ 是循环群.

Proof. 设 $|F| = q$, $[E : F] = n$, 那么 $\varphi : E \to E, a \mapsto a^q$ 是域同构且 $\varphi(k) = k, \forall k \in F$, 即 $\varphi \in \mathrm{Aut}_F E$. 因为 E 是有限域, 所以 E 的乘法群是循环群, 从而知 φ 作为群 $\mathrm{Aut}_F E$ 中元素阶为 n, 所以 $\mathrm{Aut}_F E$ 至少有 n 个元素, 而 $|\mathrm{Aut}_F E| \leq [E : F] = n$, 因此 $|\mathrm{Aut}_F E| = [E : F]$. □

下面的命题表明 Galois 扩张中的大域作为中间域的域扩张也是 Galois 扩张.

Proposition 2.8. 设有限扩张 $E \supseteq F$ 是 Galois 扩张, K 是中间域, 那么域扩张 $E \supseteq K$ 也是 Galois 扩张.

Proof. 由次数公式 $[E : F] = [E : K][K : F]$ 可知 $E \supseteq K, K \supseteq F$ 都是有限扩张, 设 $[E : F] = n, [E : K] = \ell, [K : F] = m$, 则 $n = \ell m$. 记 S 是全体域扩张 $K \supseteq F$ 到 E 的嵌入构成的集合. 命 $\psi : \mathrm{Aut}_F E \to S, \sigma \mapsto \sigma|_K$. 易知对任给 $s \in S$, 原像集 $f^{-1}(s)$ 的元素个数不超过 $|\mathrm{Aut}_K E| \leq \ell$. 下面我们说明 $|\mathrm{Aut}_K E| = \ell$, 一旦证明这一断言便得到 $E \supseteq K$ 也是 Galois 扩张. 假设 $|\mathrm{Aut}_K E| < \ell$, 那么 $n = |\mathrm{Aut}_F E| < \ell m = n$, 矛盾. □

给定一个域的域自同构群的有限子群, 可考虑该子群作用域的不动点集, 那么给定域是该不动点集的域扩张, 下面的命题表明给定域关于域自同构群的有限子群的固定子域的扩张是 Galois 扩张.

Proposition 2.9. 设 E 是域, H 是 $\mathrm{Aut}E$ 的一个有限子群, $F = E^H = \{c \in E | \sigma(c) = c, \forall c \in H\}$, 那么 $E \supseteq F$ 是有限扩张且是 Galois 扩张, Galois 群 $\mathrm{Aut}_F E = H$. 特别地, 对任何域 E 和域自同构群的有限子群 $H \subseteq \mathrm{Aut}E$, 总有 $[E : E^H] = |H|$.

Proof. 易见 $E \supseteq F$ 是域扩张. 设 $H = \{h_1, h_2, ..., h_n\}$, 如果能够证明 $[E : F] \leq n$, 则由 $n = |H| \leq |\mathrm{Aut}_F E| \leq [E : F] \leq n$ 得到 $[E : F] = |\mathrm{Aut}_F E|$ 且 $\mathrm{Aut}_F E = H$. 下面我们用反证法证明 $[E : F] \leq n$, 若不然, 则 E 中有 $u_1, u_2, ..., u_{n+1}$ 是 F-线性无关的. 易见下述线性方程组在 E^n 中有非零解:

$$\begin{pmatrix} h_1(u_1) & h_1(u_2) & \cdots & h_1(u_{n+1}) \\ h_2(u_1) & h_2(u_2) & \cdots & h_2(u_{n+1}) \\ \vdots & \vdots & & \vdots \\ h_n(u_1) & h_n(u_2) & \cdots & h_n(u_{n+1}) \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

设 $(a_1, a_2, ..., a_n)^T \in E^n$ 是上述方程的非零解, 且是分量非零元个数最小的非零解, 设 s 是使得 $a_s \neq 0$ 的最小正整数, 不妨设 $a_s = 1_E$. 下面我们构造出上述线性方程组一个新的非零解, 它的非零分量严格小于 $a_1, a_2, ..., a_n$ 中非零元数目, 从而得到矛盾. 易见 $a_1, a_2, ..., a_n$ 必定有元素不在 F 中, 否则易得 $u_1, u_2, ..., u_n$ 是 F-线性相关的, 故存在 $\ell \geq s+1$ 使得 $a_\ell \notin F$, 于是存在 $h \in H$ 使得 $h(a_\ell) \neq a_\ell$, 利用 $h : E \to E$ 是域同构可得 $(h(a_1), h(a_2), ..., h(a_n))^T \in E^n$ 也是上述线性方程组的非零解, 于是 $(h(a_1) - a_1, h(a_2) - a_2, ..., h(a_n) - a_n)^T$

也是该线性方程组的非零解, 并注意到该非零解的非零分量数目严格小于 $(a_1, a_2, ..., a_n)$ 非零分量数目 (因为 $h(a_s) - a_s = 0$), 这与 $(a_1, a_2, ..., a_n)$ 的选取矛盾. 所以 $[E : F] \leq n$. 由此可知 $[E : F] = \mathrm{Aut}_F E = n$, 域扩张 $E \supseteq F$ 是 Galois 扩张, Galois 群 $\mathrm{Aut}_F E = H$. □

下面给出一个有限扩张是 Galois 扩张关于域扩张 Galois 群不动点集的等价刻画.

Proposition 2.10. 设域扩张 $E \supseteq F$ 是有限扩张, 那么该域扩张 Galois 扩张的充要条件是对任给 $c \in E - F$, 存在 $\sigma \in \mathrm{Aut}_F E$ 使得 $\sigma(c) \neq c$, 即有 $F = E^{\mathrm{Aut}_F E}$.

Proof. 必要性：设 $E \supseteq F$ 是 Galois 扩张, 那么 $|\mathrm{Aut}_F E| = [E : F]$ 表明 $\mathrm{Aut}_F E$ 是有限群. 记 $K = E^{\mathrm{Aut}_F E}$, 那么根据 [命题2.9] 知 $E \supseteq K$ 是 Galois 扩张且该扩张的 Galois 群 $\mathrm{Aut}_K E = \mathrm{Aut}_F E$. 于是 $[E : K] = [E : F]$ 迫使 $[K : F] = 1$, 因此 $K = F$, 这说明对任给 $c \in E - F$, 有 $c \notin K$, 进而存在 $\sigma \in \mathrm{Aut}_F E$ 使得 $\sigma(c) \neq c$.

充分性：首先 $E^{\mathrm{Aut}_F E} = F$, 而 $|\mathrm{Aut}_F E| \leq [E : F]$ 保证了 $\mathrm{Aut}_F E$ 是有限群, 再利用 [命题2.9] 即可. □

Remark 2.11. 因此有限扩张是 Galois 扩张等价于小域恰是大域关于 Galois 群作用的不动点集.

Corollary 2.12. 设 $E \supseteq F$ 是有限 Galois 扩张, 那么任何 F 上不可约多项式如果在 E 中有根, 则该多项式在 E 上分裂. 并且 E 中任何元素在 F 上最小多项式都无重根.

Proof. 设 $\mathrm{Aut}_F E$ 中所有元素为 $\sigma_1 = \mathrm{id}, \sigma_2, ..., \sigma_n$, 这里 $n = [E : F]$. 并设 F 上不可约多项式 $p(x)$ 在 E 中有根 α. 考虑 $\alpha, \sigma_2(\alpha), ..., \sigma_n(\alpha)$ 中所有互异的元素 $\alpha_1 = \alpha, \alpha_2, ..., \alpha_r$, 其中 $r \leq n$. 作 $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_r)$, 如果能够说明 $f(x) \in F[x]$, 那么由 $p(x)$ 整除 $f(x)$ 立即得到 $p(x)$ 在 E 上分裂并且 $r = n$, 由此也得到 $p(x)$ 无重根. 因此该推论的证明只需再验证 $f(x) \in F[x]$. 对每个 $\tau \in \mathrm{Aut}_F E$, 因为 Galois 群是有限群所以总有 $\{\tau, \tau\sigma_2, ..., \tau\sigma_n\} = \{\mathrm{id}, \sigma_2, ..., \sigma_n\}$, 那么 $\alpha_1, ..., \alpha_r$ 也是 $\tau\sigma_1(\alpha), ..., \tau\sigma_n(\alpha)$ 中所有互异的元素. 特别地, 有 $\{\alpha_1, ..., \alpha_r\} = \{\tau(\alpha_1), ..., \tau(\alpha_r)\}$. 因此由 $f(x)$ 的系数都是关于 $\alpha_1, ..., \alpha_r$ 的初等对称多项式知 $f(x)$ 的系数关于 $\mathrm{Aut}_F E$ 中元素的作用不动. 现在应用 [命题2.10] 得到 $f(x) \in F[x]$. □

一般地, 如果域的代数扩张 $E \supseteq F$ 满足每个 $\alpha \in E$ 在 F 上的最小多项式都没重根, 则称该代数扩张是**可分的**. 如果代数扩张 $E \supseteq F$ 满足任何 F 上最小多项式只要在 E 上有根则在 E 上分裂, 则称该扩张是**正规的**. 因此 [推论2.12] 表明有限 Galois 扩张总是可分正规扩张. 之后我们会在 [推论2.16] 中看到有限扩张是 Galois 扩张的充要条件是它是可分正规扩张. 为了之后引用方便我们以下面的本原元定理结束本节.

Primitive Element Theorem. 任何有限可分扩张都是单扩张. 即如果 $L \supseteq K$ 是有限可分扩张, 那么存在 $\alpha \in L$ 使得 $L = K(\alpha)$, 这时称 α 是该域扩张的**本原元**.

Proof. 下面分 K 是无限域或是有限域两种情形讨论证明定理. 如果 K 是无限域, 则任何 K 的有限扩张 L 总可写作 $L = K(\alpha_1, ..., \alpha_n)$ 的形式, 其中每个 $\alpha_j \in L$ 是 K 上代数元. 下面对 n 作归纳来证明结论, 不难看出只需验证 $n = 2$ 的情形即可. 即说明对域扩张 $L = K(\alpha_1, \alpha_2)$, 存在 $c \in L$ 使得 $L = K(c)$. 对 $j = 1, 2$, 设 α_j 在域 K 上的最小多项式为 $p_j(x)$, 那么存在 L 的扩域 E 使得 $p_1(x), p_2(x)$ 均在 E 上分裂 (注意可分扩张的条件保证了 $p_j(x)$ 没有重根). 设为 $p_1(x) = (x - \beta_1) \cdots (x - \beta_s), p_2(x) = (x - \gamma_1) \cdots (x - \gamma_t), \beta_i, \gamma_j \in E$. 不妨设 $\beta_1 = \alpha_1, \gamma_1 = \alpha_2$. 因为 K 是无限集而

$$S = \left\{ \frac{\beta_i - \beta_1}{\gamma_1 - \gamma_j} \middle| 1 \leq i \leq s, 2 \leq j \leq t \right\} \subseteq E$$

是有限集, 故存在 $d \in K$ 使得 $d \notin S$. 进而 $\beta_i \neq \beta_1 + d(\gamma_1 - \gamma_j), \forall 1 \leq i \leq s, 2 \leq j \leq t$.

Claim. 对 $c=\alpha_1+d\alpha_2=\beta_1+d\gamma_1$ 有 $L=K(\alpha_1,\alpha_2)=K(c)$.

一旦证明该断言便得到结果. 为证此断言只需要说明 $K(\alpha_1,\alpha_2)\subseteq K(c)$. 下证 $\gamma_1=\alpha_2\in K(c)$, 考虑域 $K(c)$ 上多项式 $p_2(x)$ 以及 $r(x)=p_1(c-dx)$, 它们有公共零点 γ_1, 所以均可被 γ_1 在 $K(c)$ 上最小多项式 $m(x)$ 整除. 下证 $m(x)=x-\gamma_1$ 来得到 $\gamma_1\in K(c)$. 一方面, $m(x)$ 在 E 中的零点集是 $\{\gamma_1,...,\gamma_t\}$ 的子集, 另一方面, 对每个 $2\leq j\leq t$, $r(\gamma_j)=p_1(\beta_1+d(\gamma_1-\gamma_j))\neq 0$. 因此 $m(x)$ 在 E 中的零点只有 γ_1. 而 $E\supseteq K$ 是可分扩张表明 $m(x)$ 在 E 上无重根, 由此得到 $m(x)=x-\gamma_1$. 结合 c 的定义立即看到 $\gamma_1\in K(c)$ 蕴含 $\alpha_1\in K(c)$.

最后我们验证 K 是有限域时结论成立. 现设 $K\subseteq L$ 是有限域 K 的有限可分扩张, 设 $\mathrm{char}K=p$, 那么 K 包含素域 $\mathbb{F}_p$, 即 p 元域. 下面说明存在 $\alpha\in L$ 使得 $L=\mathbb{F}_p(\alpha)$ 来得到 $L=K(\alpha)$. 设 $|L|=p^m$, 如果 $\alpha\in L$ 满足 $\mathbb{F}_p(\alpha)$ 的元素数目为 $p^n, n<m$, 那么 α 满足多项式 $x^{p^n}-x$, 这说明对每个正整数 $n<m$, L 中满足 $\mathbb{F}_p(\alpha)$ 的元素数目为 $p^n(n<m)$ 的元素 α 的数目不超过 p^n. 注意到

$$p+p^2+\cdots+p^{m-1}=\frac{p^m-p}{p-1}<p^m,$$

所以 L 中满足 $\mathbb{F}_p(\alpha)\subsetneq L$ 的元素 α 总数严格小于 p^m. 因此存在 $\alpha\in L$ 使得 $L=\mathbb{F}_p(\alpha)$. □

2.2 Galois 理论基本定理

下面的结果是有限 Galois 扩张的基本定理, 也被称为 Galois 理论基本定理.

Fundamental Theorem of Galois Theory. 设有限扩张 $E\supseteq F$ 是 Galois 扩张, 记 Aut_FE 所有子群构成的集合为 Σ, 域扩张 $E\supseteq F$ 的所有中间域构成的集合是 Ω, 记映射 $\psi:\Omega\to\Sigma, K\mapsto \mathrm{Aut}_KE$ 以及 $\varphi:\Sigma\to\Omega, H\mapsto E^H$(这里沿用 [引理2.1] 中的记号), 则有:

$$\begin{array}{ccc} E & \longmapsto & \{\mathrm{id}_E\} \\ | & & | \\ K & \longmapsto & \mathrm{Aut}_KE \\ | & & | \\ F & \longmapsto & \mathrm{Aut}_FE \end{array}$$

(1) ψ 与 φ 都是双射, 它们互为逆映射, 这里的 ψ 也被称为 **Galois 对应**;
(2) 对任给中间域 $K\in\Omega$, 域扩张的次数 $[K:F]$ 就是子群的指数 $[\mathrm{Aut}_FE:\mathrm{Aut}_KE]$;
(3) 对中间域 $K\in\Omega$, 域扩张 $K\supseteq F$ 是 Galois 扩张当且仅当 Aut_KE 是 Aut_FE 的正规子群, 此时有群同构

$$\mathrm{Aut}_FK\cong\mathrm{Aut}_FE/\mathrm{Aut}_KE.$$

Proof. 因为 $E\supseteq F$ 是有限扩张, 所以 Σ 中任何子群 H 都是有限群, 由此可知对中间域 E^H 有 $\mathrm{Aut}_{E^H}E=H$, 即 $\psi\varphi(H)=\mathrm{Aut}_{E^H}E=H$. 由 H 的任意性知 $\psi\varphi=\mathrm{id}_\Sigma$. 任取中间域 K, 因为有限扩张 $E\supseteq F$ 是 Galois 扩张, 所以扩张 $E\supseteq K$ 也是 Galois 扩张, 从而 $K=E^{\mathrm{Aut}_KE}=\varphi\psi(K)$, 这就得到了 $\varphi\psi=\mathrm{id}_\Omega$. 故 ψ 与 φ 互为逆映射, 这就证明了 (1). 对任给中间域 K, 有 $[E:F]=[E:K][K:F]$, 因此 $K\supseteq F$ 与 $E\supseteq K$ 都是有限扩张. 由于 $E\supseteq F$ 与 $E\supseteq K$ 都是 Galois 扩张, 所以 $[E:K]=|\mathrm{Aut}_KE|, [E:F]=|\mathrm{Aut}_FE|$, 进而 $[K:F]=[\mathrm{Aut}_FE:\mathrm{Aut}_KE]$, 因此 (2) 成立. 最后我们证明 (3). 假设域扩张 $K\supseteq F$ 是 Galois 扩张, 我们断

言任何 $\sigma \in \mathrm{Aut}_F E$ 都满足 $\sigma(K) = K$. 因为 $K \supseteq F$ 是 Galois 扩张, 所以 $[K : F] = \mathrm{Aut}_F K$, 因为对任给 $\tau \in \mathrm{Aut}_F K$, 都可以扩张为域扩张 $K \supseteq F$ 到 E 的嵌入 $\tilde{\tau} : K \to E, x \mapsto \tau(x)$, 所以由 $K \supseteq F$ 到 E 的嵌入总数不超过 $[K : F]$ 可知 $A = \{\tilde{\tau} : K \to E | \tau \in \mathrm{Aut}_F K\}$ 是域扩张 $K \supseteq F$ 到 E 的所有嵌入构成的集合. 对任给 $\sigma \in \mathrm{Aut}_F E$, 有 $\sigma|_K$ 是域扩张 $K \supseteq F$ 到 E 的嵌入, 即 $\sigma|_K \in A$, 所以 $\sigma(K) = K$, 断言得证. 于是我们可以定义一个 $\mathrm{Aut}_F E$ 到 $\mathrm{Aut}_F K$ 的群同态：

$$f : \mathrm{Aut}_F E \to \mathrm{Aut}_F K, \sigma \mapsto \overline{\sigma},$$

这里 $\overline{\sigma} : K \to K, x \mapsto \sigma(x)$ 是 K 上的自同构. 易见群同态 f 的核就是 $\mathrm{Aut}_K E$, 所以 $\mathrm{Aut}_K E \trianglelefteq \mathrm{Aut}_F E$. 下设 $\mathrm{Aut}_K E \trianglelefteq \mathrm{Aut}_F E$, 我们说明 $K \supseteq F$ 是 Galois 扩张. 先说明对任给 $k \in K$ 有 $\sigma(k) \in K, \forall \sigma \in \mathrm{Aut}_F E$, 若不然, 存在某个 $b \in K$ 使得 $\sigma(b) \notin K$, 由 $K = E^{\mathrm{Aut}_K E}$ 立即得到存在 $\tau \in \mathrm{Aut}_K E$ 使得 $\tau(\sigma(b)) \neq \sigma(b)$, 这与 $\sigma^{-1}\tau\sigma \in \mathrm{Aut}_K E$ 矛盾. 于是知 $\sigma(K) \subseteq K, \forall \sigma \in \mathrm{Aut}_F E$, 进而 $\sigma(K) = K, \forall \sigma \in \mathrm{Aut}_F E$. 这保证了 $f : \mathrm{Aut}_F E \to \mathrm{Aut}_F K, \sigma \mapsto \overline{\sigma}$ 是定义合理的群同态, 其中 $\overline{\sigma} : K \to K, x \mapsto \sigma(x)$. 利用 $\mathrm{Ker} f = \mathrm{Aut}_K E$ 以及同态基本定理易知 $|\mathrm{Im} f| = |\mathrm{Aut}_F K| = [K : F]$, 所以 $K \supseteq F$ 是 Galois 扩张. 这时 f 是满射, 所以由同态基本定理可得群同构 $\mathrm{Aut}_F K \cong \mathrm{Aut}_F E / \mathrm{Aut}_K E$. □

Remark 2.13. Galois 基本定理告诉我们有限 Galois 扩张的中间域全体与该 Galois 扩张的 Galois 群的子群全体间有标准的双射, 把每个中间域对应到大域作为中间域的域扩张的 Galois 群. 反之, Galois 扩张的每个子群对应大域在该子群作用下的固定子域 (不动点集). 中间域作为小域的域扩张的次数就是中间域关于大域的 Galois 群在大域关于小域的 Galois 群中的指数. 并且中间域是小域的 Galois 扩张当且仅当中间域关于大域的 Galois 群是大域关于小域的 Galois 群的正规子群.

Theorem 2.14. 设域扩张 $E \supseteq F$ 是有限扩张, 那么 $E \supseteq F$ 是 Galois 扩张的充要条件是存在 $\alpha \in E$ 使得 $E = F[\alpha]$ 且 α 在 F 上最小多项式在 $E[x]$ 中可以分解为两两互异的一次多项式乘积.

Proof. 充分性：设 $[E : F] = n$, 且存在 $\alpha \in E$ 使得 $E = F[\alpha]$ 那么可设 α 在 F 上首一最小多项式为 $m(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n), \alpha_1, \alpha_2, ..., \alpha_n \in E$ 两两互异, 不妨设 $\alpha = \alpha_1$. 对每个 $1 \leq k \leq n$, 容易验证 $\sigma_k : E \to E, \sum\limits_{i=0}^{n-1} c_i \alpha^i \mapsto \sum\limits_{i=0}^{n-1} c_i \alpha_k^i$, 这里 $c_i \in F$, 是定义合理的域同构且在 $\mathrm{Aut}_F E$ 中. 因此 $n \leq |\mathrm{Aut}_F E| \leq [E : F] = n$, 进而 $E \supseteq F$ 是 Galois 扩张. 必要性：如果 F 是有限域, 那么 E 也是有限域. 因此由 E 的乘法群是循环群可知存在 $\alpha \in E$ 使得 $E = F[\alpha]$, 设 α 在 F 上的首一最小多项式是 n 次多项式 $m(x)$, 那么由 α 满足多项式 $x^{|E|} - x$ 可知 $m(x)$ 整除 $x^{|E|} - x$. 设 $E = \{\alpha_1, \alpha_2, ..., \alpha_s\}, s = |E|, \alpha = \alpha_1$, 那么 $x^s - x = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_s)$. 这迫使 $m(x)$ 可分解为互异的一次多项式乘积, 这就证明了当 F 是有限域时的结论成立. 下设 F 是无限域, 对每个 $c \in E$, 命 $H_c = \{\sigma \in \mathrm{Aut}_F E | \sigma(c) = c\}$, 那么 H_c 为 $\mathrm{Aut}_F E$ 的子群, 下面说明对任给 $u, v \in E$, 存在 $w \in E$ 使得 $H_u \cap H_v = H_w$. 因为 $\mathrm{Aut}_F E$ 是有限群, 所以存在 $c_1 \neq c_2 \in F$ 使得 $H_{u+c_1 v} = H_{u+c_2 v}$, 记 $w = u + c_1 v = u + c_2 v$, 容易验证 $H_u \cap H_v = H_w$. 归纳地, 可以得到对任给 $u_1, u_2, ..., u_l \in E$, 存在 $w \in E$ 使得 $\bigcap\limits_{i=1}^{l} H_{u_i} = H_w$. 现设 $[E : F] = n$ 且 E 作为 F-线性空间有基 $\{\beta_1, \beta_2, ..., \beta_n\}$, 于是有 $H_{\beta_1} \cap H_{\beta_2} \cap \cdots \cap H_{\beta_n} = \{\mathrm{id}_E\}$, 且存在 $\alpha \in E$ 使得 $H_{\beta_1} \cap H_{\beta_2} \cap \cdots \cap H_{\beta_n} = H_\alpha$, 故 $\mathrm{Aut}_{F[\alpha]} E = H_\alpha = \{\mathrm{id}_E\}$, 而 $\mathrm{Aut}_E E = \{\mathrm{id}_E\}$, 故由 Galois 基本定理可得 $E = F[\alpha]$. 设 $\mathrm{Aut}_{F[\alpha]} E = \{\sigma_1, \sigma_2, ..., \sigma_n\}$, 那么对任给 $1 \leq i \neq j \leq n$ 有 $\sigma_i(\alpha) \neq \sigma_j(\alpha)$, 于是知 $m(x)$ 作为首一 n 次多项式在 E 中有 n 个不同的根 $\sigma_1(\alpha), \sigma_2(\alpha), ..., \sigma_n(\alpha)$, 所以 $m(x)$ 可以在 $E[x]$ 中可以分解为两两互异的一次多项式乘积. □

Remark 2.15. 该定理表明有限扩张是 Galois 扩张当且仅当该域扩张是在小域上添加某个最小多项式在大域可裂无重根的元素得到的单扩张.

Corollary 2.16. 设域扩张 $E \supseteq F$ 是有限扩张, $E \supseteq F$ 是 Galois 扩张的充要条件是它为可分正规扩张.

Proof. 在 [推论2.12] 中已经证明必要性. 现在说明充分性. 依本原元定理, 存在 $\alpha \in E$ 使得 $E = F[\alpha]$. 那么域扩张的正规性保证了 α 在 F 上最小多项式在 E 上分裂. 现在应用 [定理2.14] 便知 $E \supseteq F$ 是 Galois 扩张. □

在本节最后我们总结一下有限 Galois 扩张的一些等价刻画.

Theorem 2.17. 设 $F \subseteq E$ 是域的有限扩张, 则以下等价:
(1) 该域扩张是 Galois 扩张.
(2) 对任给 $c \in E - F$, 存在 $\sigma \in \mathrm{Aut}_F E$ 使得 $\sigma(c) \neq c$.
(3) 存在 $\alpha \in E$ 使得 $E = F[\alpha]$ 且 α 在 F 上最小多项式无重根且在 E 上分裂.
(4) 该域扩张是可分正规扩张.

Proof. (1)⇔(2) 来自 [命题2.10], (1)⇔(3) 来自 [定理2.14], (1)⇔(4) 来自 [推论2.16]. □

2.3 可解扩张

设有限扩张 $E \supseteq F$ 是 Galois 扩张, 如果 $\mathrm{Aut}_F E$ 是 Abel 群, 那么将该域扩张称为 **Abel 扩张**. 若域扩张 $E \supseteq F$ 满足存在有限个中间域 $K_1, K_2, ..., K_s (s \geq 2)$ 使得 $E = K_1 \supseteq K_2 \supseteq \cdots \supseteq K_{s-1} \supseteq K_s = F$ 且对每个正整数 $1 \leq i \leq s-1$, 域扩张 $K_i \supseteq K_{i+1}$ 是 Abel 扩张, 则称 $E \supseteq F$ 是**可解扩张** (注意这里可解扩张的定义并没有要求是 Galois 扩张). 下面的引理表明有限 Galois 扩张 $E \supseteq F$ 是可解扩张与 $\mathrm{Aut}_F E$ 是可解群等价.

Lemma 2.18. 设有限扩张 $E \supseteq F$ 是 Galois 扩张, 那么 $E \supseteq F$ 是可解扩张当且仅当 $\mathrm{Aut}_F E$ 是可解群.

Proof. 必要性：设 $E \supseteq F$ 是可解扩张, 那么存在有限个中间域 $K_1, K_2, ..., K_s$ 使得 $E = K_1 \supseteq K_2 \supseteq \cdots \supseteq K_{s-1} \supseteq K_s = F$ 且对每个正整数 $1 \leq i \leq s-1$, 域扩张 $K_i \supseteq K_{i+1}$ 是 Abel 扩张. 由 Galois 基本定理可得正规列 $\mathrm{Aut}_F E = \mathrm{Aut}_{K_s} E \trianglerighteq \mathrm{Aut}_{K_{s-1}} E \trianglerighteq \mathrm{Aut}_{K_{s-2}} E \trianglerighteq \cdots \trianglerighteq \cdots \trianglerighteq \mathrm{Aut}_{K_1} E = \mathrm{Aut}_E E = \{\mathrm{id}_E\}$ 且对每个正整数 $1 \leq i \leq s-1$ 有群同构 $\mathrm{Aut}_{K_i} E / \mathrm{Aut}_{K_{i+1}} E \cong \mathrm{Aut}_{K_{i+1}} K_i$ 是 Abel 群, 这就证明了 $\mathrm{Aut}_F E$ 是可解群. 充分性：设 $\mathrm{Aut}_F E$ 是可解群, 则有正规列 $\mathrm{Aut}_F E = G_1 \trianglerighteq G_2 \trianglerighteq \cdots \trianglerighteq G_s = \{\mathrm{id}_E\}$, 由 Galois 基本定理, 我们得到域扩张链 $E = E^{G_s} \supseteq E^{G_{s-1}} \supseteq \cdots \supseteq E^{G_2} \supseteq E^{G_1} = F$, 每个域扩张 $E \supseteq E_{G_i}$ 的 Galois 群是 $\mathrm{Aut}_{E^{G_i}} E = G_i$ 且 $E^{G_{i+1}} \supseteq E^{G_i}$ 是 Galois 扩张, 且由 G_i / G_{i+1} 是 Abel 群可得该扩张是 Abel 扩张. □

下面的引理是之后证明 Abel-Ruffini 定理的必要材料.

Lemma 2.19. 设域 E, K, F 都是域 L 的子域, 满足 $E \supseteq F, K \supseteq F$, 如果 $E \supseteq K$ 是有限 Galois 扩张, 那么 $EK \supseteq K$ 也是有限 Galois 扩张且有群同构 $\mathrm{Aut}_K EK \cong \mathrm{Aut}_{E \cap K} E$. 这里 $EK = E(K)$, 即 L 中包含 E, K 的最小域, 通常将 EK 称为 E 与 K 的**复合域**.

Proof. 因为 $E \supseteq F$ 是有限 Galois 扩张, 所以根据 [定理2.14] 存在 $\alpha \in E$ 使得 $E = F(\alpha)$ 且 α 在 F 上的首一最小多项式 $m(x)$ 在 $E[x]$ 中可分解为一些互异一次多项式的乘积 $m(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$. 易见 $EK = K(\alpha)$(所以 $EK \supseteq K$ 是有限扩张), 且 α 在 K 上的最小多项式 $p(x)$ 整除 $m(x)$, 所以 α 在 K 上

的最小多项式 $p(x)$ 能够在 $EK[x]$ 中分解为一些互异的一次多项式的乘积, 这表明 $EK \supseteq K$ 是有限 Galois 扩张. 易见 $p(x)$ 的系数都在 $E \cap K$ 中, 所以结合 $E = (E \cap K)(\alpha)$ 可得 $E \supseteq E \cap K$ 是有限 Galois 扩张. 此外, 因为 $p(x)$ 是 α 在 K 上的最小多项式, 所以 $p(x)$ 也是 α 在 $E \cap K$ 上的最小多项式, 由此可得 $[EK : K] = [K(\alpha) : K] = [(E \cap K)(\alpha) : E \cap K] = [E : E \cap K]$. 由于 $E \supseteq E \cap K$ 是有限 Galois 扩张, 所以对每个 $\sigma \in \mathrm{Aut}_K EK$, 容易验证 $\sigma(E) = E$, 进而 $\overline{\sigma} : E \to E, x \mapsto \sigma(x)$ 在 $\mathrm{Aut}_{E\cap K}E$ 中. 于是我们得到了群同态 $\psi : \mathrm{Aut}_K EK \to \mathrm{Aut}_{E\cap K}E, \sigma \mapsto \overline{\sigma}$. 容易验证这是单群同态, 故由 $|\mathrm{Aut}_K EK| = [EK : K] = [E : E \cap K] = |\mathrm{Aut}_{E\cap K}E|$ 可得 ψ 也是满射, 进而得到群同构 $\mathrm{Aut}_K EK \cong \mathrm{Aut}_{E\cap K}E$. □

2.4 Abel-Ruffini 定理

下面我们讨论一元 n 次方程的根式求解问题, 根式求解一个方程, 具体地, 就是经过有限次加减乘除以及开根号运算把方程的根表示出来. 历史上对不超过四次的方程都找到了求根公式. 人们原以为对五次及五次以上的方程也可以用根式求解, 但几百年的探索都没有找到. 最早由 N. H. Abel(挪威, 1802-1829) 在 1824 年给出了一般五次方程根式求解不可能性的证明, 但他的证明是有缺陷的, 并且没有解决何时一个高次方程可用根式求解、何时无法根式求解这一问题. 约 1830 年前后, E. Galois(法国, 1811-1832) 借助他创造的群论彻底解决这一问题. 下面我们先把可根式求解用精确的数学语言表达出来.

给定域扩张 $E \supseteq F$, 如果 $\alpha \in E$ 是 F 上代数元, 满足存在正整数 $s \geq 2$ 以及有限个中间域 $K_1, K_2, ..., K_s$ 使得 $E = K_1 \supseteq K_2 \supseteq \cdots \supseteq K_{s-1} \supseteq K_s = F$ 且对每个正整数 $1 \leq i \leq s-1$, 存在 K_i 中元素 d_i 以及正整数 n_i 使得 $K_i = K_{i+1}(d_i), d_i^{n_i} \in K_{i+1}$(这里 d_i 相当于 K_{i+1} 某个元素的 n_i 次方根), 则称 α 是**可根式表示的**, 满足上述性质的域扩张 $E \supseteq F$ 称为**根扩张**. 若域 F 上多项式 $f(x)$(在其分裂域中) 的所有根都是可根式表示的, 具体地, 存在包含 f 分裂域的域 $E \supseteq F$ 使得存在正整数 $s \geq 2$ 以及有限个中间域 $K_1, K_2, ..., K_s$ 使得 $E = K_1 \supseteq K_2 \supseteq \cdots \supseteq K_{s-1} \supseteq K_s = F$ 且对每个正整数 $1 \leq i \leq s-1$, 存在 K_i 中元素 d_i 以及正整数 n_i 使得 $K_i = K_{i+1}(d_i), d_i^{n_i} \in K_{i+1}$, 则称 $f(x)$ 在 F 上是**可根式求解的**. 对于特征为零的域上任意非常数多项式, Galois 都使用多项式的 Galois 群给出了该多项式可根式求解的充要条件, 但这里仅推导 Abel-Ruffini 的工作.

下面我们主要证明任给 $n \geq 5$, n 次复系数多项式不存在用根式表达的求根公式 (只需要考虑首一的多项式即可). 下面我们说清楚什么叫有求根公式: 设 $n \geq 2$, 任给特征为零的域 F 上的未定元 $a_1, a_2, ..., a_n$(满足对每个正整数 $1 \leq i \leq n-1$, a_{i+1} 是 $F[a_1, ..., a_i]$ 上未定元), 那么对 $F(a_1, a_2, ..., a_n)$ 上的多项式

$$f(x) = x^n - a_1 x^{n-1} + a_2 x^{n-2} + \cdots + (-1)^{n-1} a_{n-1} x + (-1)^n a_n,$$

设 E 是 $f(x)$ 在 $F(a_1, a_2, ..., a_n)$ 上的分裂域且 $f(x)$ 在 $E[x]$ 中有分解 $f(x) = (x - x_1)(x - x_2) \cdots (x - x_n)$, 易见 $E = F(x_1, x_2, ..., x_n)$. 如果 f 在 $F(a_1, a_2, ..., a_n)$ 上是可根式求解的, 即存在域 $K \supseteq E$ 使得存在扩域链 $K = K_1 \supseteq K_2 \supseteq \cdots \supseteq K_{s-1} \supseteq K_s = F(a_1, a_2, ..., a_n)$ 且对每个正整数 $1 \leq i \leq s-1$, 存在 K_i 中元素 d_i 以及正整数 n_i 使得 $K_i = K_{i+1}(d_i), d_i^{n_i} \in K_{i+1}$, 则称 F **上的 n 次多项式 (或代数方程) 存在用根式表达的求根公式**. 如今我们已做好充分的准备, 下面我们证明对大于等于 5 的复系数多项式不存在用根式表达的求根公式.

Abel-Ruffini theorem. 设正整数 $n \geq 5$, 那么 $\mathbb{C}$ 上 n 次代数方程不存在用根式表达的求根公式.

Proof. 我们使用反证法证明, 假设对正整数 $n \geq 5$, $\mathbb{C}$ 上 n 次代数方程存在用根式表达的求根公式, 那么对 $\mathbb{C}$ 上未定元 $a_1, a_2, ..., a_n$(这里满足对每个正整数 $1 \leq i \leq n-1$, a_{i+1} 是 $\mathbb{C}[a_1, ..., a_i]$ 上未定元), 域 $\mathbb{C}(a_1, a_2, ..., a_n)$

上的多项式 $f(x)=x^n-a_1x^{n-1}+a_2x^{n-2}+\cdots+(-1)^{n-1}a_{n-1}x+(-1)^na_n$, 设 E 为 $f(x)$ 在 $\mathbb{C}(a_1,a_2,...,a_n)$ 上的分裂域, 存在域 $K\supseteq E$ 使得有扩域链

$$K=K_1\supseteq K_2\supseteq\cdots\supseteq K_{s-1}\supseteq K_s=\mathbb{C}(a_1,a_2,...,a_n)$$

满足对每个正整数 $1\leq i\leq s-1$, 存在 K_i 中元素 d_i 以及正整数 n_i 使得 $K_i=K_{i+1}(d_i), d_i^{n_i}\in K_{i+1}$. 我们总可以假设每个 n_i 是素数, 因为当 $n_i=1$ 时, $d_i\in K_{i+1}$, 所以 $K_i=K_{i+1}=K_{i+1}(d_i^2)$. 当 $n_i\geq 2$ 时, 它可分解为一些素数的乘积 $n_i=p_1p_2\cdots p_t$, 于是可在 K_i 与 K_{i+1} 间加入中间域:

$$K_i=K_{i+1}(d_i^{p_1\cdots p_{t-1}},d_i^{p_1\cdots p_{t-2}},...,d_i^{p_1})(d_i)\supseteq K_{i+1}(d_i^{p_1\cdots p_{t-1}},d_i^{p_1\cdots p_{t-2}},...,d_i^{p_1p_2})\supseteq\cdots\supseteq K_{i+1}(d_i^{p_1\cdots p_{t-1}})\supseteq K_i$$

因此有扩域链 $K=K_1\supseteq K_2\supseteq\cdots\supseteq K_l=\mathbb{C}(a_1,a_2,...,a_n)$, 这里 $l\geq 2$ 且对每个正整数 $1\leq i\leq l-1$, 存在 $\alpha_i\in K_i$ 以及素数 p_i 使得 $K_i=K_{i+1}(\alpha_i),\alpha_i^{p_i}\in K_{i+1}$. 下面分三步证明 Abel-Ruffini 定理.

Step 1. 设 $f(x)$ 在 $E[x]$ 中有分解式 $f(x)=(x-x_1)(x-x_2)\cdots(x-x_n)$, 我们断言 $x_1,x_2,...,x_n$ 在 $\mathbb{C}$ 上代数无关 (特别地, $x_1,x_2,...,x_n$ 两两互异), 进而 $\mathbb{C}[x_1,x_2,...,x_n]$ 与复 n 元多项式环同构. 记 σ_i 是多项式环 $\mathbb{C}[y_1,y_2,...,y_n]$ 中第 i 个初等对称多项式, 那么

$$f(x)=x^n-\sigma_1(x_1,...,x_n)x^{n-1}+\cdots+(-1)^{n-1}\sigma_{n-1}(x_1,x_2,...,x_n)x+(-1)^n\sigma_n(x_1,x_2,...,x_n),$$

所以对每个正整数 $1\leq i\leq n$, 我们有 $a_i=\sigma_i(x_1,x_2,...,x_n)$. 假设 $x_1,x_2,...,x_n$ 在 $\mathbb{C}$ 上不是代数无关的, 那么存在非零多项式 $h(y_1,y_2,...,y_n)\in\mathbb{C}[y_1,y_2,...,y_n]$ 使得 $h(x_1,x_2,...,x_n)=0$. 命

$$H(y_1,y_2,...,y_n)\triangleq\prod_{\sigma\in S_n}h(y_{\sigma(1)},y_{\sigma(2)},...,y_{\sigma_n}),$$

这是 $\mathbb{C}[y_1,y_2,...,y_n]$ 中的非零对称多项式, 且满足 $H(x_1,x_2,...,x_n)=0$. 依 [定理1.5], 存在 $\mathbb{C}[y_1,y_2,...,y_n]$ 中唯一的多项式 $P(y_1,y_2,...,y_n)$ 使得 $H(y_1,y_2,...,y_n)=P(\sigma_1,\sigma_2,...,\sigma_n)$, 因为 H 是非零多项式所以 P 也非零. 对上述多项式等式两边代入 $y_1=x_1,y_2=x_2,...,y_n=x_n$ 可得 $P(a_1,a_2,...,a_n)=0$, 这与 $a_1,a_2,...,a_n$ 是 $\mathbb{C}$ 上 (无关的) 未定元矛盾, 得证. 故 $x_1,x_2,...,x_n$ 在 $\mathbb{C}$ 上代数无关, 并得到环同构 $\mathbb{C}[x_1,x_2,...,x_n]\cong\mathbb{C}[y_1,y_2,...,y_n]$.

Step 2. 将对称群 S_n 作用在 $E=\mathbb{C}(x_1,x_2,...,x_n)$ 上:

$$\begin{aligned}S_n\times\mathbb{C}(x_1,x_2,...,x_n)&\to\mathbb{C}(x_1,x_2,...,x_n)\\(\tau,\frac{g(x_1,x_2,...,x_n)}{h(x_1,x_2,...,x_n)})&\mapsto\frac{g(x_{\tau(1)},x_{\tau(2)},...,x_{\tau(n)})}{h(x_{\tau(1)},x_{\tau(2)},...,x_{\tau(n)})}\end{aligned}$$

因为 $x_1,x_2,...,x_n$ 在 $\mathbb{C}$ 上代数无关, 所以上述群作用定义合理. 上述群作用导出的群同态记为 $\rho:S_n\to\mathrm{Sym}(E)$, 易见 ρ 的像集含于 $\mathrm{Aut}E$, 所以可将 ρ 修正为群同态 $\varphi:S_n\to\mathrm{Aut}(E)$, 这是单群同态. 命 $F=\{c\in\mathbb{C}(x_1,x_2,...,x_n)|\tau(c)=c,\forall\tau\in\varphi(S_n)\}$, 因为 $\varphi(S_n)$ 是 $\mathrm{Aut}(E)$ 的一个有限子群, 所以由 [命题2.9] 知 $\mathbb{C}(x_1,x_2,...,x_n)\supseteq F$ 是有限 Galois 扩张且它的 Galois 群是 $\varphi(S_n)$, 特别地, 有 $[E:F]=n!$. 我们断言 $F=\mathbb{C}(a_1,a_2,...,a_n)$. 易见 $F\supseteq\mathbb{C}(a_1,a_2,...,a_n)$, 由于 $x_1,x_2,...,x_n$ 都是域 $\mathbb{C}(a_1,a_2,...,a_n)$ 上多项式 $f(x)$ 的根, 所以 $[E:\mathbb{C}(a_1,a_2,...,a_n)]=[\mathbb{C}(x_1,x_2,...,x_n):\mathbb{C}(a_1,a_2,...,a_n)]\leq n!$. 于是由 $n!\geq[E:\mathbb{C}(a_1,a_2,...,a_n)]=[E:F][F:\mathbb{C}(a_1,a_2,...,a_n)]\geq n!$ 可知 $F=\mathbb{C}(a_1,a_2,...,a_n)$. 故 $E\supseteq F$ 是有限 Galois 扩张且它的 Galois 群同构于 S_n. 因为 $n\geq 5$ 所以 [例1.2] 表明域扩张 $E\supseteq F$ 的 Galois 群 Aut_FE 不可解.

Step 3. 我们断言在最开始的假设下有限扩张 $K \supseteq F = \mathbb{C}(a_1, a_2, ..., a_n)$ 是可解扩张. 首先由每个 $[K_i : K_{i+1}] \leq p_i$ 可知 $K \supseteq F$ 是有限扩张, 对每个正整数 $1 \leq i \leq l-1$, 由下面的 [引理2.20] 知 $K_i = K_{i+1}(\alpha_i) \supseteq K_{i+1}$ 是 Galois 扩张且 Galois 群 $\mathrm{Aut}_{K_{i+1}} K_i$ 是循环群. 因此 $K \supseteq F$ 是可解扩张, 于是由下面的 [引理2.22] 知我们可以找到扩域 $L \supseteq K$ 使得域扩张 $L \supseteq F$ 是有限可解 Galois 扩张. 于是 Galois 群 $\mathrm{Aut}_F L$ 是可解群. 对有限 Galois 扩张 $L \supseteq F$ 应用 Galois 基本定理, 对于 Galois 扩张 $E \supseteq F$, $\mathrm{Aut}_E L$ 是 $\mathrm{Aut}_F L$ 的正规子群且有群同构 $\mathrm{Aut}_F L / \mathrm{Aut}_F L \cong \mathrm{Aut}_F E$, 于是 $\mathrm{Aut}_F E$ 同构于可解群 $\mathrm{Aut}_F L$ 的一个商群, 故 $\mathrm{Aut}_F E$ 也可解, 矛盾.

□

Lemma 2.20. 设 p 是素数, F 是特征为零的域, 且 $x^p - 1_F$ 在代数闭包 $\overline{F}$ 中的根都在 F 中, $E \supseteq F$ 是域扩张, $\alpha \in E$ 满足 $\alpha^p \in F$, 则 $F[\alpha] \supseteq F$ 是 Galois 扩张且该域扩张的 Galois 群是循环群.

Proof. 因为 $\mathrm{char} F = 0$, 所以 $x^p - 1$ 在 $\overline{F}$ 上无重根, 因此 $x^p - 1$ 的零点集是 F^* 的 p 阶子群, 它是循环群, 设生成元为 ξ, 那么全体 p 次单位根是 $1_F, \xi, \xi^2, ..., \xi^{p-1}$. 记 $c = \alpha^p \in F$, 那么 F 上多项式 $x^p - c$ 在 $\overline{F}$ 中有分解 $x^p - c = (x - \alpha)(x - c\alpha) \cdots (x - c\alpha^{p-1})$. 不妨设 $\alpha \notin F$(如果 $F[\alpha] = F$ 结论直接成立), 设 α 在 F 上首一最小多项式为 $m(x)$, 那么 $m(x)$ 次数至少为 2. 于是由 $m(x)$ 整除 $x^p - c$ 知存在 $1 \leq d \leq p-1$ 使得 $m(x)$ 有零点 $\alpha\xi^d$. 所以存在 $\sigma \in \mathrm{Aut}_F F[\alpha]$ 使得 $\sigma(\alpha) = \alpha\xi^d$. 对每个正整数 $1 \leq k \leq p-1$, 易见 $\sigma^k(\alpha) = \alpha\xi^{kd}$, 并且对 $0 \leq i \neq j \leq p-1$, 有 $\xi^{id} \neq \xi^{jd}$, 所以 $\{\mathrm{id}_E, \sigma, \sigma^2, ..., \sigma^{p-1}\} \subseteq \mathrm{Aut}_F F[\alpha]$, 结合 $|\mathrm{Aut}_F F[\alpha]| \leq [F[\alpha] : F] \leq p$ 迫使 $\{\mathrm{id}_E, \sigma, \sigma^2, ..., \sigma^{p-1}\} = \mathrm{Aut}_F F[\alpha]$. 于是知 $F[\alpha] \supseteq F$ 是 Galois 扩张 (前面的不等式迫使 $|\mathrm{Aut}_F F[\alpha]| = [F[\alpha] : F] = p$) 且该域扩张的 Galois 群是循环群. □

Lemma 2.21. 设域扩张 $E \supseteq K, K \supseteq F$ 是有限 Galois 扩张, $\overline{E}$ 是 E 的代数闭包, 那么存在 $\overline{E}$ 的一个子域 L 满足：(1)$L \supseteq E$; (2) 域扩张 $L \supseteq F$ 是有限 Galois 扩张; (3) 存在正整数 n 以及扩域链 $K = L_0 \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_n = L$ 使得每个 $L_i \supseteq L_{i-1}$ 是有限 Galois 扩张且 Galois 群 $\mathrm{Aut}_{L_{i-1}} L_i$ 同构于 $\mathrm{Aut}_K E$ 的某个子群.

Proof. 设 $[E : K] = n$, 由条件可知域扩张 $E \supseteq K$ 到 $\overline{E}$ 的嵌入恰好 n 个, 设为 $\sigma_1, \sigma_2, ..., \sigma_n$, 记 $E_i = \sigma_i(E)$, 那么 $E_i \supseteq K, \forall 1 \leq i \leq n$. 定义 $L_0 = K, L_1 = E_1, L_i = E_1 E_2 \cdots E_i (1 \leq i \leq n)$, 那么 $L_i = L_{i-1} E_i, \forall 1 \leq i \leq n$. 每个 σ_i 给出 K-线性空间 E 到 K-线性空间 E_i 的线性同构 θ_i, 所以 $[E : K] = [E_i : K], \forall 1 \leq i \leq n$, 并设 $L = L_n$. 并注意到对每个正整数 $1 \leq i \leq n$, 有群同构 $\mathrm{Aut}_K E \to \mathrm{Aut}_K E_i, \tau \mapsto \theta_i \tau \theta_i^{-1}$, 因此 $|\mathrm{Aut}_K E_i| = |\mathrm{Aut}_K E| = [E : K] = [E_i : K]$, 这说明 $E_i \supseteq K$ 是有限 Galois 扩张. 于是知 $L_1 \supseteq K$ 是有限 Galois 扩张, 如果对正整数 $1 \leq i \leq n-1$ 有 L_i 是 K 的有限 Galois 扩张, 那么 $L_{i+1} = L_i E_{i+1}$ 也是 K 的有限 Galois 扩张, 所以 $L_1, L_2, ..., L_n = L$ 都是 K 的有限 Galois 扩张. 进而由前面的引理可得 L_i 是 L_{i-1} 的 Galois 扩张, 这里 $1 \leq i \leq n$. 每个 Galois 群 $\mathrm{Aut}_{L_{i-1}} L_i \cong \mathrm{Aut}_{E_i \cap L_{i-1}} E_i$, 即同构于 $\mathrm{Aut}_K E_i$ 的一个子群, 所以每个 $\mathrm{Aut}_{L_{i-1}} L_i$ 同构于 $\mathrm{Aut}_K E$ 的某个子群. 因此我们构造的域 L 满足 (3), 而 $E \supseteq K$ 到 $\overline{E}$ 的嵌入中有 E 的标准嵌入, 所以 $L \supseteq E$, 这就得到了 (1). 最后我们证明 $L \supseteq K$ 满足 (2). 我们先说明每个域扩张 $L \supseteq F$ 到 $\overline{E}$ 的嵌入 σ 都满足 $\sigma(L) = L$, 进而可诱导 $\mathrm{Aut}_F L$ 中的元素 $\hat{\sigma} : L \to L, x \mapsto \sigma(x)$. 因为域扩张 $L \supseteq F$ 到 $\overline{E}$ 的嵌入 σ 满足 $\sigma(E_i) = \sigma(\sigma_i(E)) \subseteq L$, 所以 $E_i \subseteq \sigma^{-1}(L), \forall 1 \leq i \leq n$. 易知 $\sigma^{-1}(L)$ 是 L 的子域, 所以 $L \subseteq \sigma^{-1}(L)$, 这表明 $\sigma(L) \subseteq L$. 这说明 σ 可诱导 F-线性空间 L 上的线性变换, 而 $[L : K], [K : F]$ 有限表明 L 是有限维 F-线性空间, 所以 $\sigma(L) = L$, 从而每个 σ 可诱导 $\mathrm{Aut}_F L$ 中元素 $\hat{\sigma}$. 现在我们说明有限扩张 $L \supseteq F$ 是 Galois 扩张. 只需说明对任意 $c \in L - F$, 存在 $\sigma \in \mathrm{Aut}_F L$ 使得 $\sigma(c) \neq c$. 如果 $c \in K$, 那么 $c \in K - F$, 利用 $K \supseteq F$ 是有限 Galois 扩张知存在 $\delta \in \mathrm{Aut}_F K$ 使得 $\delta(c) \neq c$, δ 视作 $K \supseteq F$ 到 $\overline{E}$ 的嵌入, 因为 $\overline{E}$ 是代数闭域, 所以 δ 可延

拓为 L 到 $\overline{E}$ 的嵌入, 由前面的讨论知该嵌入给出 $\mathrm{Aut}_F L$ 中的元素, 且该自同构变动 c. 如果 $c \in L - K$, 那么存在正整数 i 使得 $c \in L_i - L_{i-1}$, 利用 $L_i \supseteq L_{i-1}$ 是有限 Galois 扩张, 仿照前面的讨论可构造 $\mathrm{Aut}_{L_{i-1}} L$ 中变动 c 的自同构, 而这也是 $\mathrm{Aut}_F L$ 中元素. 这就证明了 $L \supseteq F$ 是 Galois 扩张. □

Lemma 2.22. 任给有限可解扩张 $E \supseteq F$, 存在 E 的扩域 L 使得 $L \supseteq F$ 是有限可解 Galois 扩张.

Proof. 因为域扩张 $E \supseteq F$ 是有限可解扩张, 所以存在中间域 $E_0, E_1, ..., E_n (n \geq 1)$ 使得

$$F = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_{n-1} \subseteq E_n = E,$$

满足对每个正整数 $1 \leq i \leq n-1$, $E_{i+1} \supseteq E_i$ 是有限 Galois 扩张且 $\mathrm{Aut}_{E_i} E_{i+1}$ 是 Abel 群. 我们对正整数 n 作归纳证明这一结论. 当 $n = 1$ 时, 取 $L = E$ 即得结果. 假设结论对 $n-1 (n \geq 2)$ 的情形成立, 那么对 n 的情形, 此时 $E_{n-1} \supseteq F$ 是有限可解扩张, 所以由归纳假设, 存在 E_{n-1} 的扩域 K' 使得 $K' \supseteq F$ 是有限可解 Galois 扩张. 设 $\overline{E}$ 是 E 的代数闭包, 那么存在域扩张 $K' \supseteq E_{n-1}$ 到 $\overline{E}$ 的嵌入 (由 E_{n-1} 到 $\overline{E}$ 的标准嵌入得到), 记 $K = \sigma(K')$, 那么利用 $K \supseteq F$ 是有限可解 Galois 扩张易得 $K = \sigma(K') \supseteq \sigma(F) = F$ 也是有限可解 Galois 扩张. 因为 σ 固定 E_{n-1} 中每个元素, 所以 K 也是 E_{n-1} 的有限扩张 (由此我们看到 $E_{n-1} \subseteq E \cap K$), 因此由 $E \supseteq E_{n-1}$ 是有限 Galois 扩张得到 $KE \subseteq K$ 是有限 Galois 扩张且 $\mathrm{Aut}_K KE \cong \mathrm{Aut}_{E \cap K} E$, 后者是 Abel 群 $\mathrm{Aut}_{E_{n-1}} E$ 的子群, 所以 $\mathrm{Aut}_K KE$ 也是 Abel 群. 记 $\overline{KE}$ 是 KE 在 $\overline{E}$ 中的代数闭包, 利用 $\overline{E}$ 是代数闭域易证它是 KE 的代数闭包. 对有限 Galois 扩张 $KE \supseteq K, K \supseteq F$ 以及代数闭包 $\overline{KE}$ 应用 [引理2.21] 可得存在域扩张 $L \supseteq F$ 使得它是有限 Galois 扩张且 $L \supseteq K$ 是可解扩张, 故结合 $K \supseteq F$ 是可解扩张可得域扩张 $L \supseteq F$ 是有限可解 Galois 扩张. □

参考文献

[Yan13] Jin-Gen Yang. *Modern Algebra.* Alpha Science, 2013.