Galois 理论复习

温尊

目录

1 基础内容

1.1 正规扩张

定理 1. 若 $f(x) \in F[x]$, 且 $\deg f = n$, 则存在域扩张 K/F 使得 $[K:F] \le n$ 且 K 包含 f 的一个根.

证明. 考虑 f 的一个在 $F[x]$ 的不可约因子 $p(x)$, 对 $\phi : F \to F[x]/(p(x)) := K$ 为 $a \mapsto a + (p(x))$ 有 $F \approx \phi(F)$. 那么将 F 替换为 $\phi(F)$, 考虑 $\alpha = x + (p(x)) \in K$, 不难得知 $p(\alpha) = 0$, 则 K 满足条件, 且 $[K:F] = \deg p \le \deg f = n$. □

引理 1 (IET1)**.** 考虑域同构 $\sigma : F \to F'$, 取不可约多项式 $f(x) \in F[x]$, 设 α 是 f 在扩张 K/F 下的一个根, 取 α' 为 $\sigma(f)$ 的一个在 K'/F' 的根, 则存在 $\tau : F(\alpha) \to F'(\alpha')$ 满足 $\tau|_F = \sigma$ 且 $\tau(\alpha) = \alpha'$.

证明. 考虑两个 F-同构 $\phi : F[x]/(f(x)) \to F(\alpha), g(x) + (f(x)) \mapsto g(\alpha)$ 和 $\psi : F'[x]/(\sigma f(x)) \to F'(\alpha'), g(x) + (\sigma f(x)) \mapsto g(\alpha')$, 对同构 $\nu : g(x) + (f(x)) \mapsto g(x) + (\sigma f(x))$ 有交换图如下

$$
\begin{tikzcd}
F[x]/(f(x)) \arrow[r, "\nu", "\approx"'] \arrow[d, "\phi"] & F'[x]/(\sigma f(x)) \arrow[d, "\psi"] \\
F(\alpha) \arrow[r, "\psi\nu\phi^{-1}"] & F'(\alpha')
\end{tikzcd}
$$

容易验证 $\tau = \psi\nu\phi^{-1}$ 满足条件. □

引理 2 (IET1)**.** 考虑域同构 $\sigma : F \to F'$, 设 $K = \mathrm{Split}(\{f_i\}, F)$, 设 $\tau : K \to K'$ 满足 $\tau|_F = \sigma$, 则 $\tau(K) = \mathrm{Split}(\{\sigma f_i\}, F)$.

证明. 不难验证. □

定理 2. 考虑域同构 $\sigma : F \to F'$, 设 $K = \mathrm{Split}(f, F), K' = \mathrm{Split}(\sigma f, F')$, 存在同构 $\tau : K \to K'$ 满足 $\tau|_F = \sigma$, 且取 $\alpha \in K$, 若 α' 是 $\sigma(\min(F, \alpha))$ 的根, 则 τ 可以选取为 $\tau(\alpha) = \alpha'$.

证明. 对 $n = [K:F]$ 归纳, 取 $L = F(\alpha), L' = F'(\alpha')$, 运用引理 IET1, 存在 $\rho : L \to L'$ 满足 $\rho(\alpha) = \alpha'$, 归纳将 ρ 延展即可. □

定理 3 (IET)**.** 考虑域同构 $\sigma : F \to F'$, 设 $S = \{f_i\}, S' = \{\sigma f_i\}$, 考虑 $K = \mathrm{Split}(S, F), K' = \mathrm{Split}(S', F')$, 存在同构 $\tau : K \to K'$ 满足 $\tau|_F = \sigma$, 且取 $\alpha \in K$, 若 α' 是 $\sigma(\min(F, \alpha))$ 的根, 则 τ 可以选取为 $\tau(\alpha) = \alpha'$.

证明. 用 Zorn 引理, 略去. $\square$

命题 1. *考虑域扩张 $F \subset L \subset K$, 有*

$$\begin{tikzcd}[row sep=small] K \arrow[d, dash] \arrow[dd, dash, bend left=40, "\text{正规}"] \\ L \arrow[d, dash] \\ F \end{tikzcd} \Rightarrow \begin{tikzcd}[row sep=small] K \arrow[d, dash, bend left=40, "\text{正规}"] \arrow[d, dash] \\ L \arrow[d, dash] \\ F \end{tikzcd}$$

1.2 可分和不可分扩张

命题 2. *考虑 $f(x) \in F[x]$ 和 $\deg f \geq 1$, 则 f 在 $\mathrm{Split}(f, F)$ 内无重根当且仅当 $(f, f') = 1$.*

证明. 首先, 不难得知在 $F[x]$ 内 $(f, f') = 1$ 等价于在 $K[x]$ 内 $(f, f') = 1$.

一方面, 若 f 在 $\mathrm{Split}(f, F)$ 内无重根, 则显然 $(f, f') = 1$;

另一方面, 若 $(f, f') = 1$, 取 $K = \mathrm{Split}(\{f, f'\}, F)$, 设 $d = (f, f') \in K[x]$, 则 d 也在 $K[x]$ 内分裂, 则三者有公共根, 这不可能, 则 $\deg d = 0$. $\square$

命题 3. *设 $f \in \mathrm{Irr}(F[x])$, 则*

(a) 若 $\mathrm{char} F = 0$, 则 f 可分; 若 $\mathrm{char} F = p$, 则 f 可分 $\Leftrightarrow f' \neq 0 \Leftrightarrow f \notin F[x^p]$;

(b) 若 $\mathrm{char} F = p$, 则存在 $g \in F[x]$ 为可分不可约多项式使得 $f(x) = g(x^{p^m})$.

证明. (a) 不难得知 $(f, f') = 1$ 或 f. 若 $\mathrm{char} F = 0$, 则显然 $(f, f') = 1$, 故 f 可分; 若 $\mathrm{char} F = p$, 则 $(f, f') = f \Leftrightarrow f | f' \Leftrightarrow f' = 0 \Leftrightarrow f \in F[x^p]$.

(b) 设 $S = \{n : f(x) \in F[x^{p^n}]\}$, 则 S 为有限集, 且 $0 \in S$, 则 S 非空. 设 $m = \max(S)$, 则存在 g 使得 $f(x) = g(x^{p^m})$. 若 g 不可分, 则 $g \in F[x^p]$, 则存在 $h \in F[x]$ 使得 $f(x) = g(x^{p^m}) = h(x^{p^{m+1}})$, 这和 m 最大性矛盾. 由 f 不可约可以得到 g 不可约. $\square$

引理 3 (PIE1)**.** *设 $\mathrm{char} F = p$, 取 F 上的代数元 α, 则 α 在 F 上纯不可分当且仅当 $\alpha^{p^n} \in F$. 此时其极小多项式为 $(x - \alpha)^{p^n}$.*

证明. 一方面, 若 $\alpha^{p^n} \in F$, 则 $\min(F, \alpha) | (x - \alpha)^{p^n}$, 故极小多项式只有一个根, 则其纯不可分; 反之, 若其纯不可分, 则设 $f = \min(F, \alpha)$, 存在可分不可约多项式 g 使得 $f(x) = g(x^{p^m})$. 考虑 g 在分裂域中分裂为 $(x - b_1)...(x - b_r)$, 则 $f = (x^{p^m} - b_1)...(x^{p^m} - b_r)$, 其中 $b_i \neq b_j$. 由于纯不可分, 则 $r = 1$, 则 $f = x^{p^m} - b_1$, 成立. $\square$

引理 4 (PIE2)**.** *考虑代数扩张 K/F.*

(a) 若 α 可分且纯不可分, 则 $\alpha \in F$;

(b) 若 K/F 纯不可分, 则 K/F 是正规扩张, 且 $\mathrm{Gal}(K/F)$ 平凡. 另外若 K/F 是有限扩张且 $p = \mathrm{char}F$, 则 $[K:F] = p^n$;

(c) 设所有的 $\alpha \in S$ 都纯不可分, 则 $K = F(S)/F$ 是纯不可分扩张;

(d) 对域扩张 $F \subset L \subset K$, 有 K/F 纯不可分当且仅当 $K/L, L/F$ 都纯不可分.

证明. (a) 显然;

(b) 显然 K/F 是正规扩张, 且 $\mathrm{Gal}(K/F)$ 平凡. 若 K/F 是有限扩张且 $p = \mathrm{char}F$, 设 $K = F(a_1, ..., a_n)$, 首先 $[F(a_1) : F] = p^{m_1}$, 归纳即可得到结论;

(c) 取 $a \in F(a_1, ..., a_n)$, 考察其极小多项式即可;

(d) 显然. □

命题 4. *考虑域扩张 K/F, 设其可分和纯不可分闭包为 S, I, 则 S/F 是可分扩张且 I/F 是纯不可分扩张, 且 $S \cap I = F$. 若 K/F 是代数扩张, 则 K/S 是纯不可分扩张.*

证明. 首先不难验证 S, I 是域, 且显然 S/F 是可分扩张且 I/F 是纯不可分扩张且 $S \cap I = F$. 若 K/F 是代数扩张, 取 $\alpha \in K$, 存在可分不可约多项式 g 使得 $\min(F, \alpha) = g(x^{p^m})$ 且 $\alpha^{p^m} = a$, 则 $g(a) = 0$, 则 $g(x) = \min(F, a)$, 则 a 可分, 则 $\alpha^{p^m} = a \in S$, 则 K/S 纯不可分. □

定理 4. *设 K 是 F 的正规扩张, 设其可分和纯不可分闭包为 S, I, 则 S/F 是 Galois 扩张, 且 $I = \mathrm{Inv}(\mathrm{Gal}(K/F))$ 且 $\mathrm{Gal}(S/F) \approx \mathrm{Gal}(K/F) \approx \mathrm{Gal}(K/I)$, 则 K/I 是 Galois 扩张, 且 $K = SI$.*

证明. 取 $a \in S, f(x) = \min(F, a)$, 由于 K/F 正规, 则 f 在 K 内分裂, 而且 a 可分, 则 f 的根都可分, 均在 S 内, 则 f 在 S 内分裂. 故得到 S/F 是正规扩张, 则 S/F 是 Galois 扩张. 其次, 定义 $\theta : \mathrm{Gal}(K/F) \to \mathrm{Gal}(S/F)$ 为 $\sigma \mapsto \sigma|_S$. 一方面由同构扩张定理知 θ 是满的, 另一方面由 $\ker\theta = \mathrm{Gal}(K/S)$ 且 K/S 纯不可分, 则 θ 是同构.

取 $a \in I$, 则 $a^{p^n} \in F$, 则取 $\sigma \in \mathrm{Gal}(K/F)$ 有 $a^{p^n} = \sigma(a^{p^n}) = (\sigma(a))^{p^n}$, 则 $\sigma(a) = a$, 故 $I \subset \mathrm{Inv}(\mathrm{Gal}(K/F))$; 反之, 取 $b \in \mathrm{Inv}(\mathrm{Gal}(K/F))$, 则 $b^{p^n} \in S$, 取 $\tau \in \mathrm{Gal}(S/F)$, 则存在 $\sigma \in \mathrm{Gal}(K/F)$ 使得 $\tau = \sigma|_S$, 则 $\tau(b^{p^n}) = \sigma(b^{p^n}) = b^{p^n}$, 则 $b^{p^n} \in \mathrm{Inv}(\mathrm{Gal}(S/F)) = F$, 则 b 纯不可分, 则 $I = \mathrm{Inv}(\mathrm{Gal}(K/F))$.

则 $\mathrm{Gal}(S/F) \approx \mathrm{Gal}(K/F) \approx \mathrm{Gal}(K/I)$, 则 K/I 是 Galois 扩张. 则由于 K/I 可分, 则 K/SI 可分, 且由于 K/S 纯不可分, 则 K/SI 纯不可分, 则 $K = SI$. □

1.3 Galois 基本定理及其推论

定理 5 (Galois 基本定理)**.** *设 K/F 是有限 Galois 扩张, 设 $G = \mathrm{Gal}(K/F)$.*

(a) G 的子群和 K/F 的中间域有一一对应:$L \mapsto \mathrm{Gal}(K/L)$ 且 $H \mapsto \mathrm{Inv}(H)$;

(b) 如果 $L \leftrightarrow H$, 则 $[K:L] = |H|, [L:F] = (G:H)$;

(c) 而且 $H \trianglelefteq G$ 当且仅当 L/F 是 Galois 扩张, 这时有 $\mathrm{Gal}(L/F) \approx G/H$.

定理 6 (自然无理性)**.** *设 K/F 是有限 Galois 扩张, 取任意 F 的域扩张 L, 则 KL/L 是 Galois 扩张, 且 $\mathrm{Gal}(KL/L) \approx \mathrm{Gal}(K/K\cap L)$.*

证明. 即为

$$\begin{tikzcd}
& KL \arrow[dl, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & & L \arrow[dl, dash] \\
& K\cap L \arrow[d, dash] & \\
& F &
\end{tikzcd}$$

首先不难得知 KL/L 是 Galois 扩张, 则考虑同态 $\theta : \mathrm{Gal}(KL/L) \to \mathrm{Gal}(K/F)$ 为 $\sigma \mapsto \sigma|_K$. 那么发现 $\ker\theta = \{\sigma \in \mathrm{Gal}(KL/L) : \sigma|_K = \mathrm{id}, \sigma|_L = \mathrm{id}\} = \{\mathrm{id}\}$, 故 θ 是单射. 而 θ 的像是 $\mathrm{Gal}(K/F)$ 的子群, 故由 Galois 对应, 存在某中间域 E 使得 $\mathrm{Im}\theta = \mathrm{Gal}(K/E)$. 下面证明 $E = K\cap L$. 取 $a \in K\cap L$, 则任取 $\sigma \in \mathrm{Gal}(KL/L)$, 都有 $a = \sigma(a) = \sigma|_K(a)$, 故 $a \in E$. 反之, 取 $a \in E$, 则 $a \in K$, 而且任取 $\sigma \in \mathrm{Gal}(KL/L)$ 有 $\sigma|_K(a) = a$, 故 $\sigma(a) = a$, 则 $a \in L$, 则 $a \in K\cap L$. 故 $E = K\cap L$. □

定理 7 (本原元定理)**.** *有限扩张 K/F 是单扩张当且仅当 K/F 只有有限多个中间域.*

证明. 不难得知有限域的扩张当然是单扩张, 我们只考虑无限域的域扩张.

我们假设 K/F 只有有限多中间域. 设 $K = F(a_1, ..., a_n)$, 对 n 归纳, 当 $n = 1$ 时显然成立, 假设 $n-1$ 时有 $F(a_1, ..., a_{n-1}) = F(b)$, 考虑 $K = F(b, a_n)$. 设 $M_x = F(a_n + xb), x \in F$, 则 M_x 为 $K/F(b)$ 的中间域, 由于中间域有限, 则存在 $x \neq y \in F$ 使得 $M_x = M_y$. 则 $b = \frac{a_n + xb - (a_n + yb)}{x - y} \in M_y$, 且 $a_n = a_n + yb - yb \in M_y$, 则 $K = M_y$ 为单扩张.

反之, 假设 K/F 为单扩张, 设 $K = F(a)$. 取中间域 M, 则 $K = M(a)$, 则 $\min(M,a) | \min(F,a)$, 我们设 $\min(M,a) = a_0 + a_1x + ... + x^r$, 取 $M_0 = F(a_0, ..., a_{r-1}) \subset M$, 则 $\min(M,a) \in M_0[x]$, 且 $\min(M_0,a) | \min(M,a)$. 那么有 $[K : M] = \deg\min(M,a) \geq \deg\min(M_0,a) = [K : M_0] = [K : M][M : M_0]$, 则 $M = M_0$, 故 M 被 $\min(M,a)$ 完全确定. 而 $\min(F,a)$ 的因子有限, 则中间域有限. □

推论 1 (弱本原元定理)**.** *有限可分扩张是单扩张.*

证明. 考虑 K/F 的正规闭包 N, 则知 N/F 是 Galois 扩张, 而 F 是其中间域. 且 $\mathrm{Gal}(N/F)$ 为有限群, 则只有有限多个子群, 由 Galois 对应知 N/F 只有有限多中间域. □

2 重要的 Galois 扩张

2.1 有限域

引理 5. *设 K 是个域, 而 G 是 K^* 的有限子群, 则 G 是循环群.*

证明. 取 $n = |G|, m = \exp G$, 则 $m|n$. 而且对任意的 $g \in G$ 都有 $g^m = 1$, 则其均为 $x^m - 1$ 的根. 而方程只有 m 个根, 则 $m = n$, 则 G 是循环群. □

定理 8. *设有限域 F 为 $\mathrm{char}F = p$, 令 $|F| = p^n$, 则 F 是 $\mathbb{F}_p$ 中多项式 $x^{p^n} - x$ 的分裂域. 则 $F/\mathbb{F}_p$ 是 Galois 扩张, 且 $\mathrm{Gal}(F/\mathbb{F}_p) = \langle\sigma\rangle$ 为 $\sigma(a) = a^p$, 故为循环扩张.*

证明. 由于 $|F^*| = p^n - 1$, 则其中元素为 $x^{p^n-1} = 1$ 的根, 故 F 的元素都满足 $x^{p^n} - x = 0$. 而方程有 p^n 个根, 域 F 有 p^n 个元素, 则 F 就是 $\mathbb{F}_p$ 中多项式 $x^{p^n} - x$ 的分裂域. 而且求导检验知该多项式可分, 则 $F/\mathbb{F}_p$ 是 Galois 扩张.

对于 $\sigma : a \mapsto a^p$, 显然它为 F 的一个 $\mathbb{F}_p$-同构. 显然 $\mathrm{Inv}(\sigma) = \mathbb{F}_p$, 则 $\mathrm{Gal}(F/\mathbb{F}_p) = \langle\sigma\rangle$ 为 $\sigma(a) = a^p$. 定理成立. □

注 1. *(1) 由于阶为 p^n 的域都是 $\mathbb{F}_p$ 中多项式 $x^{p^n} - x$ 的分裂域, 对单位映射用同构扩张定理知这些域都同构;*

(2) 上述 σ 称为 Frobenius 同构.

推论 2. *设 K/F 是有限域的扩张, 则 K/F 是 Galois 扩张, 且 Galois 群是循环群. 设 $\mathrm{char}F = p, |F| = p^n$, 则 $\mathrm{Gal}(K/F) = \langle\tau\rangle$ 为 $\tau(a) = a^{p^n}$.*

证明. 设 $[K : \mathbb{F}_p] = m$, 则 $\mathrm{Gal}(K/\mathbb{F}_p)$ 是 m 阶循环群, 而 $\mathrm{Gal}(K/F)$ 为其子群, 故也为循环群, 设 $s = |\mathrm{Gal}(K/F)|$, 则 $m = ns$, 则其被 σ^n 生成. □

定理 9. *设 N 是 $\mathbb{F}_p$ 的代数闭包, 则对 $n > 0$, 则存在唯一的中间域使得阶为 p^n. 而且如果 N 内 $|K| = p^m, |L| = p^n$, 则 $K \subset L$ 当且仅当 $m|n$. 此时 L/K 是 Galois 扩张, 其 Galois 群被 $\tau : a \mapsto a^{p^n}$ 单生成.*

证明. 由于阶为 p^n 的域都为 $x^{p^n} - x$ 的根, 则唯一.

如果 $K \subset L$, 则 $n = [L : \mathbb{F}_p] = [L : K][K : \mathbb{F}_p] = m[L : K]$, 故 $m|n$. 反之, 若 $m|n$, 则满足 $x^{p^m} - x = 0$ 必满足 $x^{p^n} - x = 0$, 则 $K \subset L$. 其余都为前面的推论. □

考虑完有限域的结构, 我们看有限域上多项式的结构.

推论 3. *设 F 是有限域, 且 $f \in F[x]$ 是首一 n 次不可约多项式.*

(1) 设 a 是 f 在 F 某扩域上的根, 则 $F(a) = \mathrm{Split}(f, F)$. 且 $[F(a) : F] = n$;

(2) 若 $|F| = q$, 则 f 的根为 $\{a^{q^r} : r \geq 1\}$.

证明. (1) 设 K 为 f 分裂域, 则对其某根 a, 域 $F(a)$ 是 F 的 n 次扩张, 且其为 Galois 扩张, 则其为分裂域;

(2) 不难得知 $\mathrm{Gal}(K/F) = \langle\tau\rangle$ 为 $\tau(a) = a^q$, 则其根为 $\{a^{q^r} : r \geq 1\}$. $\square$

命题 5. 设 $n > 0$, 则 $x^{p^n} - x$ 在 $\mathbb{F}_p$ 内分解成所有次数整除 n 的首一不可约多项式的乘积.

证明. 设 $|F| = p^n$, 则 F 为 $x^{p^n} - x$ 分裂域, 取 $a \in F$, 则 $m = [\mathbb{F}_p(a) : \mathbb{F}_p] | [F : \mathbb{F}_p]$ 且 $\min(\mathbb{F}_p, a) | x^{p^n} - x$. 反之, 设 f 是 $m|n$ 次首一不可约多项式, 设 $K = \mathrm{Split}(f, \mathbb{F}_p)$, 则取一个根 a, 则 $K = \mathbb{F}_p(a)$, 则 $[K : \mathbb{F}_p] = m|n$, 则 $K \subset F$, 则 $a \in F$, 则 $f | x^{p^n} - x$, 由 $x^{p^n} - x$ 的可分性知命题成立. $\square$

2.2 分圆扩张

定理 10. 设 $\mathrm{char}F$ 不整除 n, 设 $K = \mathrm{Split}(x^n - 1, F)$, 则 K/F 是 *Galois* 扩张, 且对任意本原单位根 ω 有 $K = F(\omega)$. 且 $\mathrm{Gal}(K/F)$ 同构于 $(\mathbb{Z}/n\mathbb{Z})^*$ 的一个子群, 则 $\mathrm{Gal}(K/F)$ 是 *Abel* 群且 $[K : F] | \phi(n)$.

证明. 由于 $\mathrm{char}F$ 不整除 n, 则 $x^n - 1$ 可分, 故 K/F 是 Galois 扩张. 任取本原单位根 ω, 其他 n 次单位根都是 ω 的某次方, 故 $K = F(\omega)$.

任何 K 的 F-同构都只和作用在 ω 上有关, 且把 ω 映到另一个本原单位根上, 不妨设为 ω^t. 则我们给出映射 $\theta : \mathrm{Gal}(K/F) \to (\mathbb{Z}/n\mathbb{Z})^*$ 为 $\sigma \mapsto t + n\mathbb{Z}$, 其中 $\sigma(\omega) = \omega^t$. 则不难验证 θ 是良定义的单同态, 则命题成立. $\square$

我们现在考虑 $F = \mathbb{Q}$ 时的特例, 定义 n 次分圆多项式为 $\Psi_n(x) = \prod_{i=1}^r (x - \omega_i)$, 其中 ω_i 为所有本原 n 次单位根.

引理 6. 对 $n > 0$, 有 $x^n - 1 = \prod_{d|n} \Psi_d(x)$, 且 $\Psi_n(x) \in \mathbb{Z}[x]$.

证明. 知 $x^n - 1 = \prod (x - \omega)$, 且所有 n 次单位根都是本原 d 次单位根, 其中 $d|n$, 反之亦然, 则显然有 $x^n - 1 = \prod_{d|n} \Psi_d(x)$.

归纳法, 当 $n = 1$ 时显然成立, 假设 $\Psi_d(x) \in \mathbb{Z}[x]$ 对所有 $d < n$ 成立, 则 $x^n - 1 = \Psi_n(x) \prod_{d|n, d<n} \Psi_d(x)$, 则命题成立. $\square$

定理 11. 对 $n > 0$, 多项式 $\Psi_n(x)$ 在 $\mathbb{Q}$ 上不可约.

证明. 假设其可约, 则在 $\mathbb{Z}$ 上也可约, 设 $\Psi_n(x) = f(x)h(x)$, 其中 f 在 $\mathbb{Z}$ 上不可约. 取 ω 为 f 的一个根, 则我们断言对任意不整除 n 的素数 p, 都有 ω^p 也为 f 的根. 否则, 设 ω^p 不是 f 的根, 则其为 h 的根, 则 $f(x) | h(x^p)$. 考虑典范同态 $\mathbb{Z}[x] \to \mathbb{F}_p[x]$, 则 $\overline{\Psi_n(x)} = \bar{f}\bar{g}$. 由于 $\overline{\Psi_n(x)} | x^n - \bar{1}$, 则检验知其在 $\mathbb{F}_p$ 的任意扩张上无重根. 另一方面 $\bar{f} | \bar{h}^p$, 则对 $\bar{f}$ 的因式 $\bar{q}$ 有 $\overline{q^2} | \overline{\Psi_n(x)}$, 这和无重根矛盾, 则断言成立. $\square$

推论 4. *若 $K = \mathrm{Split}(x^n - 1, \mathbb{Q})$, 则 $[K : \mathbb{Q}] = \phi(n)$ 且 $\mathrm{Gal}(K/\mathbb{Q}) \approx (\mathbb{Z}/n\mathbb{Z})^*$. 另外, 取本原 n 次单位根 ω, 则 $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_i : (i, n) = 1\}$.*

证明. 运用上面的定理, 显然. □

2.3 循环扩张

我们只考虑包含本原 n 次单位根的 n 次循环扩张和特征 p 域的 p 次循环扩张. 当然我们熟知一个 n 次循环扩张可以分解成一堆 p 次循环扩张和一个和 p 互素的循环扩张.

引理 7. *设 F 包含本原 n 次单位根 ω, 取 n 次循环扩张 K/F, 设 σ 生成 $\mathrm{Gal}(K/F)$, 则存在 $a \in K$ 使得 $\sigma(a) = \omega a$.*

证明. 只需证明 ω 是 σ 的一个特征值, 即 ω 是 σ 特征多项式的一个根. 不难得知 σ 适合 $x^n - 1$, 如果还有次数更低的多项式 $g(x)$ 被 σ 适合, 则 $\mathrm{id}, \sigma, ..., \sigma^{m-1}$ 线性相关, 这和 Dedekind 无关性引理矛盾, 故 $x^n - 1$ 是其极小多项式, 不难得知也是特征多项式, 得证. □

定理 12. *设 F 包含本原 n 次单位根 ω, 取 n 次循环扩张 K/F, 则存在 $b \in F$ 使得 $K = F(\sqrt[n]{b})$.*

证明. 由引理知存在 $a \in K$ 使得 $\sigma(a) = \omega a$, 则 $\sigma^i(a) = \omega^i a$. 当且仅当 $n|i$ 时才能固定 a, 也就是当且仅当 id 才能固定 a, 则 $\mathrm{Gal}(F(a)/F) = \{\mathrm{id}\}$, 由 Galois 对应知 $K = F(a)$. 且 $\sigma(a^n) = \omega^n a^n = a^n$, 则 $a^n \in F$, 我们设 $b = a^n$, 则 $K = F(\sqrt[n]{b})$. □

不难证明反之也对.

推论 5. *设 F 包含本原 n 次单位根 ω, 取 n 次循环扩张 $K = F(\sqrt[n]{a})/F$, 则所有中间域都形如 $F(\sqrt[m]{a})/F$, 其中 $m|n$.*

下面看特征 p 域的 p 次循环扩张.

定理 13. *设 $\mathrm{char}F = p$, 设 K/F 是 p 次循环扩张, 则 $K = F(\alpha)$, 其中 $\alpha^p - \alpha - a = 0, a \in F$.*

证明. 取 $\mathrm{Gal}(K/F)$ 生成元 σ, 考虑变换 $T = \sigma - \mathrm{id}$, 则 $\ker T = F$. 且 $T^p = \sigma^p - \mathrm{id} = 0$, 则 $\mathrm{Im}T^{p-1} \subset \ker T = F$, 而且 $\mathrm{Im}T^{p-1}$ 是 F-线性变换, 则 $\mathrm{Im}T^{p-1} = F$, 故存在 $c \in K$ 使得 $T^{p-1}c = 1$, 设 $\alpha = T^{p-2}c$, 则 $T\alpha = 1$, 则 $\sigma\alpha = \alpha + 1$. 由于 σ 无法固定 α, 则 $K = F(\alpha)$, 且不难验证 $\alpha^p - \alpha - a = 0, a \in F$. □

另一方面, 我们知道多项式 $x^p - x - a$ 在 F 内要不分裂, 要不不可约, 则可以得到上述定理的逆.

2.4 Kummer 理论

定理 14. *设 F 包含本原 n 次单位根 ω, 设 K/F 是有限扩张, 则 K/F 是 n 次 Kummer 扩张当且仅当存在 $a_i \in F$ 使得 $K = F(\sqrt[n]{a_1}, ..., \sqrt[n]{a_r})$.*

证明. 若 $K = F(\alpha_1, ..., \alpha_r)$, 其中 $\alpha_i^n = a_i \in F$, 则不难得知 $K = \mathrm{Split}(\{x^n - a_i\}, F)$, 且由于这些多项式可分, 则 K/F 是 Galois 扩张. 任取 $\sigma \in \mathrm{Gal}(K/F)$, 则 $\sigma^n(\alpha_i) = \alpha_i$, 则 $\sigma^n = \mathrm{id}$, 故 $\exp(\mathrm{Gal}(K/F))||G|$. 接下来只需证明其是 Abel 扩张. 任取 $\sigma, \tau \in \mathrm{Gal}(K/F)$, 则设 $\sigma(\alpha_i) = \omega^j \alpha_i, \tau(\alpha_i) = \omega^t \alpha_i$, 其交换性显然, 故 K/F 是 n 次 Kummer 扩张.

若 K/F 是 n 次 Kummer 扩张, 则设 $G = \mathrm{Gal}(K/F)$, 由于其 Abel 性, 我们有 $G = \prod_{j=1}^r C_j$, 其中 C_j 为阶数整除 n 的循环群. 考虑 $H_i = \prod_{j \neq i} C_j$, 则 $G/H_i \approx C_i$. 设 $L_i = \mathrm{Inv}(H_i)$, 则由于正规性我们知道 L_i/F 是循环 Galois 扩张. 设 $[L_i : F] = m_i$, 则 $m_i = |C_i|, m_i | n$, 则 F 存在本原 m_i 次单位根, 故 $L_i = F(\alpha_i)$, 其中 $\alpha_i^{m_i} \in F$, 则 $\alpha_i^n \in F$. 由 Galois 对应我们发现 $F(\alpha_1, ..., \alpha_r) = L_1 ... L_r$ 对应群 $\bigcap_{j=1}^r H_j = \{\mathrm{id}\}$, 则 $K = F(\alpha_1, ..., \alpha_r) = F(\sqrt[n]{a_1}, ..., \sqrt[n]{a_r})$. □

那么不难证明经典题, 也就是说对互不相同的素数 p_i, 我们有 2 次 Kummer 扩张 $[\mathbb{Q}(\sqrt{p_1}, ..., \sqrt{p_r}) : \mathbb{Q}] = 2^r$. 但一般情况下 n 次 Kummer 扩张的次数不一定是 n^r.

设 G, H 是有限 Abel 群, 而 C 是循环群, 考虑双线性对 $B : G \times H \to C$, 我们称其为非退化的, 如果对任意的 $h \in H$ 都有 $B(g, h) = e$, 则 $g = e$, 反之亦然.

引理 8. *考虑双线性对 $B : G \times H \to C$, 定义 $B_h : G \to C$ 为 B 的限制, 则映射 $\phi : h \mapsto B_h$ 是 $H \to \hom(G, C)$ 的群同态. 若 B 非退化, 则 $\exp(G)||C|$ 且 ϕ 是单射, 那么诱导同构 $G \approx H$.*

证明. 前半部分验证即可, 最后一部分考虑 $\hom(G/C) \approx \hom(G, \mathbb{C}^*) \approx G$ 即可. □

考虑 n 次 Kummer 扩张 K/F, 设 $\mu(F)$ 是 F 内所有 n 次单位根, 其构成一个循环群, 设 $\mathrm{KUM}(K/F) = \{a \in K^* : a^n \in F\}$, 其为 K^* 的一个子群, 且其包含了 F^* 和 K 的生成元. 考虑 $\mathrm{kum}(K/F) = \mathrm{KUM}(K/F)/F^*$.

定义 Kummer 对为 $B : \mathrm{Gal}(K/F) \times \mathrm{kum}(K/F) \to \mu(F)$ 为 $(\sigma, \alpha F^*) \mapsto \sigma(\alpha)/\alpha$. 不难验证其良定, 则

定理 15. *若 K/F 是 n 次 Kummer 扩张, 考虑其 Kummer 对为 $B : \mathrm{Gal}(K/F) \times \mathrm{kum}(K/F) \to \mu(F)$ 为 $(\sigma, \alpha F^*) \mapsto \sigma(\alpha)/\alpha$, 则 B 非退化, 且 $\mathrm{kum}(K/F) \approx \mathrm{Gal}(K/F)$.*

证明. 运用 $\sigma(\alpha)/\alpha \in F$ 为 n 次单位根, 则不难验证 B 是双线性对. 若 B 非退化, 则由引理得到 $\mathrm{kum}(K/F) \approx \mathrm{Gal}(K/F)$.

只需证明 B 非退化. 若 $B(\sigma, \alpha F^*) = 1$ 对任意 $\alpha F^* \in \mathrm{kum}(K/F)$ 成立, 则 $\sigma(\alpha) = \alpha$ 对任意的 $\alpha \in \mathrm{KUM}(K/F)$ 成立, 则显然有 $\sigma = \mathrm{id}$. 反之, 若 $B(\sigma, \alpha F^*) = 1$ 对任意 $\sigma \in \mathrm{Gal}(K/F)$ 成立, 则 $\alpha \in \mathrm{Inv}(\mathrm{Gal}(K/F)) = F$, 则 $\alpha F^* = F^*$, 这就说明了 B 非退化. □

命题 6. 若 K/F 是 n 次 *Kummer* 扩张, 则存在单的群同态 $f:\mathrm{kum}(K/F)\to F^*/F^{*n}$ 为 $\alpha F^*\mapsto \alpha^n F^{*n}$.

证明. 取 $\alpha F^*\in\ker f$, 则 $\alpha^n\in F^{*n}$, 则存在 $a\in F$ 使得 $\alpha^n=a^n$, 即 α/a 是 n 次单位根, 故 $\alpha/a\in F$, 则 $\alpha\in F$. □

3 Galois 理论应用

3.1 根式可解性

定义 1. 扩张 K/F 称为根式扩张如果 $K=F(a_1,...,a_r)$, 且存在 $n_1,...,n_r$ 使得 $a_i^{n_i}\in F$ 且 $a_i^{n_i}\in F(a_1,...,a_{i-1})$. 如果 $n=n_1=...=n_r$, 则称为 n 次根式扩张.

取 $f(x)\in F[x]$, 称 f 可根式解的, 如果存在根式扩张 L/F 使得 f 在 L 内分裂.

注 2. *(1)* 上述根式扩张也是 $n=n_1...n_r$ 次根式扩张;

(2) 根据根式扩张的定义, 我们有域链 $F=F_0\subset F_1\subset\cdots\subset F_r=K$, 其中 $F_{i+1}=F_i(a_i)$, 而且由定义, 根式扩张的根式扩张还是根式扩张.

引理 9. 设 K/F 是 n 次根式扩张, 设其正规闭包为 N, 则 N/F 也是 n 次根式扩张.

证明. 设 $K=F(\alpha_1,...,\alpha_r)$, 其中 $\alpha_i^n\in F(\alpha_1,...,\alpha_{i-1})$. 对 r 归纳. 当 $r=1$ 时 $K=F(\alpha),\alpha^n=a\in F$, 取正规闭包 $N=F(\beta_1,...,\beta_m)$, 其中 β_i 为 $\min(F,\alpha)$ 的根, 由于 $\min(F,\alpha)|x^n-a$, 故 $\beta_i^n=a$, 则 N/F 是根式扩张. 设 N_0 是 $F(\alpha_1,...,\alpha_{r-1})$ 的正规闭包, 由归纳假设知 N_0/F 是根式扩张. 设 $\gamma_1,...,\gamma_m$ 为 $\min(F,\alpha_r)$ 的根, 则 K/F 的正规闭包为 $N=N_0(\gamma_1,...,\gamma_m)$. 由同构扩张定理我们知道存在 $\sigma_i\in\mathrm{Gal}(N/F)$ 使得 $\sigma_i(\alpha_r)=\gamma_i$. 由正规性知 $\gamma_i^n=\sigma_i(b)$, 其中 $b=\alpha_r^n\in F(\alpha_1,...,\alpha_{r-1})\subset N_0$, 则 $\sigma_i(b)\in N_0$, 则 N/N_0 是根式扩张, 则 N/F 也是. □

定理 16 (Galois)**.** 设 $\mathrm{char}F=0$, 取 $f(x)\in F[x]$, 设 $K=\mathrm{Split}(f,F)$, 则 f 可以被根式解当且仅当 $\mathrm{Gal}(K/F)$ 可解.

证明. 一方面, 假设 f 根式可解, 则存在 n 次根式扩张 M/F 使得 $K\subset M$, 取本原 n 次单位根 ω, 则 $M(\omega)/M$ 是 n 次根式扩张, 故 $M(\omega)/F$ 也是 n 次根式扩张. 取该扩张的正规闭包 L, 则由引理知 L/F 还是 n 次根式扩张.

那么存在域链 $F=F_0\subset F_1=F(\omega)\subset\cdots\subset F_r=L$, 其中 $F_{i+1}=F_i(\alpha_i),\alpha_i^n\in F_i$. 那么发现 F_1/F_0 是分圆扩张, 其是 Abel 扩张, 而对 $i\geq 1$, 扩张 F_{i+1}/F_i 是循环扩张, 因为其包含本原 n 次单位根. 而显然 L/F 是 Galois 扩张.

我们假设 $G=\mathrm{Gal}(L/F),H_i=\mathrm{Gal}(L/F_i)$, 则有链 $\{\mathrm{id}\}=H_r\leq H_{r-1}\leq\cdots\leq H_1\leq H_0=G$. 由于 F_{i+1}/F_i 是 Galois 扩张, 则 $H_{i+1}\trianglelefteq H_i$, 则由 Galois 对应我们知道 $H_i/H_{i+1}\approx\mathrm{Gal}(F_{i+1}/F_i)$ 是 Abel 的, 故 $\mathrm{Gal}(K/F)\approx G/\mathrm{Gal}(L/K)$ 可解.

反之, 假设 $\mathrm{Gal}(K/F)$ 可解, 则有群链 $\mathrm{Gal}(K/F) = H_0 \supset H_1 \supset \cdots \supset H_r = \{\mathrm{id}\}$, 其中 $H_{i+1} \trianglelefteq H_i$ 且 H_i/H_{i+1} 是 Abel 群. 设 $F_i = \mathrm{Inv}(H_i)$, 根据 Galois 基本定理我们知道 K_{i+1}/K_i 是 Galois 的, 且 $\mathrm{Gal}(K_{i+1}/K_i) \approx H_i/H_{i+1}$. 设 $n = \exp(\mathrm{Gal}(K/F))$, 对本原 n 次单位根 ω, 添加为 $L_i = K_i(\omega)$, 则有域链 $F \subset L_0 \subset \cdots \subset L_r$ 和 $K \subset L_r$. 注意到 $L_{i+1} = L_i K_{i+1}$, 根据自然无理性我们知道 L_{i+1}/L_i 是 Galois 扩张, 而且 $\mathrm{Gal}(L_{i+1}/L_i) \approx \mathrm{Gal}(K_{i+1}/K_{i+1} \cap L_i) \leq H_i/H_{i+1}$, 这是个 Abel 群, 故我们得知 L_{i+1}/L_i 是个 n 次 Kummer 扩张, 则根据其结构我们知道 L_{i+1}/L_i 是 n 次根式扩张, 由于 L_0/F 是根式扩张, 则 L_r/F 也是, 且 $K \subset L_r$, 故 f 根式可解. $\square$

【例】考虑 $f(x) = \prod_1^n (x - t_i) = x^n - s_1 x^{n-1} + ... + (-1)^n s_n \in k(t_1, ..., t_n)[x]$, 取 $K = k(t_1, ..., t_n)$, 则 $\mathfrak{S}_n$ 是 K 的一组自同构, 且 $\mathrm{Inv}(\mathfrak{S}_n) = F = k(s_1, ..., s_n)$, 则 $\mathrm{Gal}(K/F) \approx \mathfrak{S}_n$, 当 $n \geq 5$ 时 $\mathfrak{S}_n$ 不可解.