Galois 理论及其应用

Instructor: 刘博文

Qiuzhen College, Tsinghua University

2023 Spring

目录

第一章　域扩张回顾

1.1　代数扩张

定义 1.1.1. F 是一个域, 定义域的**特征** (characteristic)为使得 $n \cdot 1 = 0$ 的最小的非负整数 n, 其中 1 是域中的乘法单位, 通常记作 $\operatorname{char} F$.

注记. $\operatorname{char} F$ 要么为零, 要么为素数 p.

例子. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 的特征为零, 有限域 $\mathbb{F}_p$ 的特征为 p, 其中 p 是素数.

定义 1.1.2. 若域 E, F 之间有包含关系 $F \subseteq E$, 则称 E 是 F 的一个**域扩张** (field extension), 记扩张的次数为 $[E : F] = \dim_F E$.

定义 1.1.3. 一个域扩张被称为有限的, 如果其扩张次数有限, 否则被称为无限的.

注记. 显然, 线性代数的知识告诉我们, 如果有 $F \subseteq E \subseteq K$, 则 $[K : F] = [K : E][E : F]$

定义 1.1.4. E/F 是域扩张, $S \subseteq K$ 是一个子集, 则记 $F[S]$ 是 E 中包含 F, S 的最小的子环; $F(S)$ 是 E 中包含 F, S 最小的子域. 特别地, 如果 $S = \{u\}$, 称 $F(u)$ 叫做域 F 的一个**单扩张** (simple extension).

定义 1.1.5. $u \in E$ 称为在 F 上**代数** (algebraic), 如果存在非零多项式 $p(x) \in F[x]$, 使得 $p(u) = 0$, 否则则称 u 在 F 上**超越** (transcendental).

定义 1.1.6. 域扩张 E/F 称为**代数扩张** (algebraic extension), 如果 E 中任何一个元素都在 F 上代数.

注记. 我们还可以如下刻画 u 是否在 F 上代数: 考虑赋值映射 $\theta_u : F[x] \twoheadrightarrow F[u]$, 则 u 在 F 上代数当且仅当 $\ker \theta_u \neq 0$; u 在 F 上超越当且仅当 $\ker \theta_u = 0$, 即 θ_u 是一个同构.

命题 1.1.7. 下面列出一些有关的基本事实:

(1) 如果 u 在 F 上代数, 则 $F[u] = F(u)$, 并且 $[F(u) : F] = \deg p(x)$

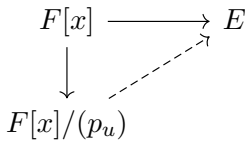
(2) 如果 u, v 都在 F 上代数, 则 $u \pm v, uv, u/v (v \neq 0)$ 都在 F 上代数, 这也就是说 E 中所有在 F 上代数的元素组成了 E 的一个子域,

(3) K/E 是代数扩张, E/F 是代数扩张, 则 K/F 也是代数扩张.

(4) $E/F, E'/F$ 都是代数扩张, 则两者复合 EE'/F 也是代数扩张.

引理 1.1.8. $F(u)/F$ 是单扩张, u 在 F 上代数, 记其极小多项式为 p_u, 如果 E/F 是域扩张, $v \in E$ 使得 $p_u(v) = 0$, 则存在 F 嵌入 $\tau : F(u) \hookrightarrow E$ 使得 $\tau(u) = v, \tau|_F = \mathrm{id}$

证明: 注意到 $F(u) \cong F[x]/(p_u)$, 考虑如下交换图即可:



□

1.2 分裂域与代数闭包

定义 1.2.1. 给定域扩张 E/F, 多项式 $p(x) \in F[x]$ 在 E 中**分裂** (split), 如果 $p(x)$ 在 E 中可以写成:

$$p(x) = c\prod_{i=1}^{n}(x - u_i)$$

其中 $u_i \in E$. E 被称作是 $p(x)$ 的**分裂域** (splitting field), 如果 E 是包含 F 使得 $p(x)$ 分裂的最小的域.

定理 1.2.2. *多项式 $p(x) \in F[x]$ 的分裂域 E 存在, 并在在同构意义下唯一. 并且 $[E : F] \leq n!$, 其中 $n = \deg p(x)$.*

证明: 我们通过对 $p(x)$ 次数的归纳来证明存在唯一性.

1. 存在性: 当 $n = 1$ 时 $E = F$. 下面考虑 $n > 1$: 假设 $p(x)$ 在 F 上不分裂, 取其一个不分裂的不可约因子, 记做 $q(x)$, 则 $F' = F[x]/(q(x))$ 是包含 F 的一个域, 且 $[F' : F] \leq n$, 令 u 是 x 在 F' 中的像, 则 u 是 $p(x)$ 在 F' 的一个根, 则 $p(x)$ 在 $F'[x]$ 中可以写成:

   $$p(x) = (x - u)p_1(x), \quad \deg p_1(x) = n - 1$$

   因此利用归纳假设, 存在 $p_1(x)$ 在 F' 上的唯一的分裂域 E, 并且 $[E : F'] \leq (n - 1)!$, 根据分裂域的定义自然有 E 也是 $p(x)$ 在 F 上的分裂域, 并且 $[E : F] = [E : F'][F' : F] \leq (n - 1)! \cdot n = n!$.
2. 唯一性: 如果 E' 是 $p(x)$ 在 F 上的另一个分裂域, 根据引理1.1.8, 存在嵌入 $F' \hookrightarrow E'$, 那么 E' 也应是 $p_1(x)$ 在 F' 上的分裂域, 因此 $E' \cong E$.

□

定义 1.2.3. 域 F 被称为**代数闭域** (algebraic closed field), 如果不存在真的代数扩张.

定义 1.2.4. 域扩张 E/F 中 E 被称为 F 的**代数闭包** (algebraic closure), 如果 E/F 是代数扩张, E 是代数闭域.

命题 1.2.5 (E. Artin)**.** *任何域 F 都存在一个代数闭域 E 作为其扩张.*

证明: 我们首先构造一个 F 的一个域扩张 E_1 使得任意次数大于等于 1 的 $f \in F[x]$ 在 E_1 中都有根: 考虑集合 $\mathfrak{X} = \{x_f \mid f \in F[x], \deg(f) \geq 1\}$, 以及以集合 $\mathfrak{X}$ 为未定元的多项式环 $F[\mathfrak{X}]$. 令 $I = (f(x_f))$, 我们断言 I 是 $F[\mathfrak{X}]$ 的一个真理想. 假设 $I = F[\mathfrak{X}]$, 则有

$$\sum_{i=1}^{n} g_i f_i(x_{f_i}) = 1$$

由于只有有限多个 f_i, 那么根据分裂域存在性的证明过程不难构造 F 的一个域扩张 F' 使得每一个 f_i 在 F' 中都有根 u_i. 考虑 $F[\mathfrak{X}] \to F'$, 定义为 $x_{f_i} \mapsto u_i$, 其余的 x_f 被映成零, 则考虑上述等式在这个映射下的结果, 我们有 $0 = 1$, 矛盾. 因此 I 是真理想, 我们取 $\mathfrak{m}$ 是包含 I 的一个极大理想, 令 $E_1 = F[\mathfrak{X}]/\mathfrak{m}$, 则

$$F \hookrightarrow F[\mathfrak{X}] \to F[\mathfrak{X}]/\mathfrak{m} = E_1$$

我们用 $\overline{x}_f$ 记 x_f 在 E_1 中的像, 可以发现其为 $f(x)$ 的一个根. 不断进行如上操作则有

$$F = E_0 \subseteq E_1 \subseteq E_2 \subseteq \dots$$

令 $E = \bigcup_{i=0}^{\infty} E_i$, 我们证明 E 是代数闭的. 任取多项式 $f \in E[x]$, 那么其系数总会落在某一个 E_n 中，则它在 E_{n+1} 中有根, 即在 E_{n+1} 中有分解

$$f = (x - u_1)f_1$$

其中 $f_1 \in E_{n+1}[x]$, 继续对 f_1 使用如上操作即可. □

命题 1.2.6. *F 是域, E 是代数闭域, 并且有嵌入 $\tau : F \hookrightarrow E$. 如果 K/F 是代数扩张, 则 τ 可以延拓成 $\tau' : K \to E$. 特别地, 如果 K 是代数闭域, 那么 $\tau' : K \to E$ 是同构.*

证明: 任取 $u \in K$, u 在 F 上的极小多项式记做 p_u, 由于 E 是代数闭域, 那么 $\tau(p_u)$ 在 E 中存在根 v, 那么根据引理1.1.8可知 σ 可以延拓到 $F(u) \to E$. 用 M 记所有的 (K', τ'), 其中 K' 是 K 的包含 F 的子域, τ' 是 τ 的延拓. 并且定义偏序关系 $(K_1', \tau_1') \leq (K_2', \tau_2')$ 为 $K_1' \subseteq K_2'$ 并且 $\tau_2'|_{K_1'} = \tau_1'$. 我们已经知道 M 非空, 从而根据祖恩引理存在极大元 K', 并且再次利用引理1.1.8可知 K' 就是 K. □

定理 1.2.7. *域 F 的代数闭包 $\bar{F}$ 存在且唯一 (在同构意义下).*

证明: 存在性: 根据命题1.2.5, 存在代数闭域 E 使得其是 F 的扩张, 定义

$$\bar{F} := \{u \in E \mid u \text{ 在 } F \text{ 上代数}\}$$

那么有 $\bar{F}$ 是 F 的代数扩张. 并且 $\bar{F}$ 是代数闭域, 因为任取 $f(x) = a_n x^n + \dots + a_0 \in \bar{F}[x]$, 根据韦达定理可知其根在 $F(a_0, \dots, a_n)$ 上面代数, 从而在 F 上代数, 进而属于 $\bar{F}$.

唯一性: 根据命题1.2.6即可. □

注记 (Artin-Schreier). 如果 $[\bar{F} : F] < \infty$, 并且大于 1, 则 $[\bar{F} : F] = 2$, 且 -1 不是 F 中的平方根, $\bar{F} = F(\sqrt{-1})$.

1.3 正规扩张与可分扩张

1.3.1 正规扩张

定义 1.3.1. 域扩张 E/F 被称为**正规扩张** (normal extension), 如果任取不可约多项式 $p(x) \in F[x]$, 如果其在 K 中有一个根, 则其全部的根都在 K 中.

定理 1.3.2. 下列叙述等价:

(1) E/F 是正规扩张.

(2) 任何 F-嵌入 $\tau : E \to \bar{F}$ 满足 $\tau(E) \subseteq E$

(3) $\mathrm{Hom}_F(E, \bar{F}) = \mathrm{Hom}_F(E, E)$

如果 E/F 是有限扩张, 则上述三条还与下面等价:

(4) E 是某个多项式 $p(x) \in F[x]$ 的分裂域.

证明: 显然 (3) 和 (2) 等价, 下面我们只证明 (1) 和 (2) 的等价性:

(1) $\Longrightarrow$ (2): 假设 E/F 是正规扩张, 任取 $u \in E$, 考虑 u 在 F 上的极小多项式 p_u, 那么 p_u 的所有根都落在 E 中. 对于任意的 F-嵌入 $\tau : E \to \bar{F}$, $\tau(u)$ 一定是 p_u 的一个根, 因为 $p_u(\tau(u)) = \tau(p_u(u)) = 0$, 因此 $\tau(u) \in E$, 即 $\tau(E) \subseteq E$.

(2) $\Longrightarrow$ (1): 任取 $u \in E$, 考虑其在 F 上的极小多项式 p_u, 任取其另一个根 $v \in \bar{F}$, 则存在态射 $F(u) \to \bar{F}, u \mapsto v$, 因此根据引理1.1.8可以延拓成 $\tau : K \to \bar{F}$, 因此 $\tau(u) = v \in E$, 即 $F \subseteq E$ 是正规扩张.

现在假设扩张次数有限, 我们来证明 (4) 与上述命题的等价性:

(1) $\Longrightarrow$ (4): 假设 E/F 是正规扩张, 任取 $u_1 \in E \backslash F$, 记其极小多项式为 p_{u_1}, 并且 $[E : F(u_1)] < [E : F]$, 再取 $u_2 \in E \backslash F(u_1)$, 由于扩张次数不断在减小, 因此有限次重复后一定有 $E = F(u_1, \ldots, u_n)$, 令 $P = \prod_{i=1}^{n} p_{u_i}$, 则 K 是 p 的分裂域.

(4) $\Longrightarrow$ (2): 如果 E 是 $p(x)$ 的分裂域, 其所有的根为 $\{u_1, \ldots, u_n\}$, 则 $E = F(u_1, \ldots, u_n)$, 考虑 F-嵌入 $\tau : F(u_1, \ldots, u_n) \to \bar{F}$, 由于 $\tau(u_i)$ 仍然是 p 的根, 因此 $\tau(u_i) \in E$, 即 $\tau(E) \subseteq E$.

□

推论 1.3.3. 对于 $F \subseteq E \subseteq K$, 有:

(1) 如果 K/F 是正规扩张, 那么 K/E 也是正规扩张 (但是 E/F 不一定正规).

(2) 如果 $E/F, E'/F$ 都是正规扩张, 那么 EE'/F 也是正规扩张.

证明: (1) 任取 $u \in K$, 考虑其在 F, E 上的极小多项式, 分别为 p_u, p'_u, 则 $p'_u \mid p_u$. 由于 K/F 是正规扩张, 因此 p_u 的所有根都在 K 中, 因此 p'_u 的所有根也在 K 中, 即 K/E 也是正规扩张.

(2) 给定嵌入 $\tau : EE' \to \bar{F}$, 由于 $E/F, E'/F$ 都是正规扩张, 因此 $\tau(E) \subseteq E, \tau(E') \subseteq E'$, 因此 $\tau(EE') \subseteq EE'$, 即 EE'/F 是正规扩张. □

注记. 如果 K/E 是正规扩张, E/F 是正规扩张, 则 K/F 不一定是正规扩张, 考虑下面的例子:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$$

由于二次扩张都是正规扩张, 从而 $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2})$ 以及 $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[4]{2})$ 都是正规扩张, 但是 $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[4]{2})$ 不是正规扩张: 考虑 $\mathbb{Q}$ 上的不可约多项式 $x^4 - 2$, 其中一个根 $\sqrt[4]{2}$ 在 $\mathbb{Q}(\sqrt[4]{2})$ 中, 但存在一个根 $i\sqrt[4]{2}$ 不在其中.

1.3.2 可分扩张

定义 1.3.4. 给定域 F, $p(x) \in F[x]$ 被称为**可分多项式** (seperable polynomial), 如果其在 $\bar{F}$ 中不存在重根.

定义 1.3.5. 给定域扩张 E/F, $u \in E$ 被称为 F 上的**可分元** (seperable element), 如果其在 F 上的极小多项式是可分多项式.

定义 1.3.6. 域扩张 E/F 被称为**可分扩张** (seperable extension), 如果 E 中所有元素都在 F 上可分.

引理 1.3.7. *给定域 F, $p(x) \in F[x]$, $p(x)$ 在 $\bar{F}$ 中有重根当且仅当 $(p, p') \neq 1$. 特别地, 如果 p 是不可约多项式, 则这个条件等价于 $p' = 0$.*

证明: 在 $\bar{F}$ 中将 $p(x)$ 写做 $p(x) = c\prod_{i=1}^{n}(x - u_i)$, 则

$$p'(x) = c\sum_{i=1}^{n}(x-u_1)\dots(x-u_{i-1})(x-u_{i+1})\dots(x-u_n)$$

如果 p 有重根, 不妨假设 $u_1 = u_2$, 则 $p'(u_1) = 0$, 即 $(x - u_1) \mid (p, p')$; 另一方面, 如果 $u_i \neq u_j$ 对任意 $i \neq j$ 成立, 则 $p'(u_i) \neq 0$ 对任意 $1 \leq i \leq n$ 成立, 从而 $(p, p') = 1$.

特别地, 如果 p 是不可约的, 从而 $(p, p') = 1$ 或 $(p, p') = p$. 从而 p 有重根当且仅当 $(p, p') = p$, 但是 $\deg p' \leq n - 1$, 从而有 $p' = 0$. □

推论 1.3.8. *如果 $\operatorname{char} F = 0$, 则任何不可约多项式都是可分的.*

证明: 当 $\operatorname{char} F = 0$ 时, 任何非常数的多项式都有非零导数. □

练习. *域 F 被称为**完美域** (perfect field), 如果任何不可约多项式都是可分的. 证明如下结论:*

1. *域 F 是完美域当且仅的 $F^p = F$, 其中 $p = \operatorname{char} F > 0$.*
2. *任何有限域都是完美域.*

注记. 当 $\operatorname{char} F = p$ 时, 并非所有不可约多项式都是可分的: 令 $F = \mathbb{F}_p(t)$, 取 $p(x) = x^p - t \in F[x]$, 则 $p(x)$ 是不可约多项式, 但不是可分的, 因为

$$(p, p') = (x^p - t, px^p) = (x^p - t, 0) = 0 \neq 1$$

这里面关键的原因在于特征不为零时, 一个高次多项式的形式导数可能会为零.

因此, 对于可分多项式的研究, 只有在 $\operatorname{char} F \neq 0$ 时才有趣, 因此在本节剩下的部分中, 都假设 $\operatorname{char} F = p$.

定义 1.3.9. 取 $p(x) \in F[x]$ 是一个不可约的不可分多项式, 那么 $p'(x) = 0$, 因此存在 $p_1(x)$, 使得 $p(x) = p_1(x^p)$, 下面考虑 $p_1(x)$ 是否不可分, 如果仍不可分, 可以继续做下去, 直到 $p = p_e(x^{p^e})$, 其中 $p_e(x)$ 是可分多项式, 记 $n_s := \deg p_e$, 则 $n = n_s \cdot p^e$, 其中 n_s 称为 $p(x)$ 的**可分次数** (seperable degree), p^e 称作 $p(x)$ 的**不可分次数** (inseperable degree).

引理 1.3.10. *对于域扩张 E/F, $u \in E$ 是 F 上的可分元当且仅当 $F(u) = F(u^p)$*

证明: 我们记 $F_1 = F(u^p)$, 显然有 $F_1 \subseteq F(u)$. 假设 $u \in E$ 是可分元, 考虑多项式 $x^p - u^p \in F_1[x]$, 则 u 是其根. 令 $p(x)$ 是 u 在 F_1 中的极小多项式, 则 $p \mid x^p - u^p = (x-u)^p$, 那么 $p(x) = (x-u)^k$ 对某个整数 k 成立. 但是因为 u 在 F 上可分, 从而其在 F_1 上也可分[1], 从而 $k = 1$, 即 $u \in F_1$.

[1]因为 u 在 F_1 上的极小多项式一定整除其在 F 上的极小多项式.

另一方面, 如果 u 的极小多项式 $p(x)$ 不是可分的, 因此可以写成 $p(x) = p_1(x^p)$, 其中 $\deg p_1 < \deg p$. 而由于 $p_1(x)$ 是 u^p 的极小多项式, 那么:

$$\deg p_1 = [F(u^p) : F] = [F(u) : F] = \deg p$$

相矛盾, 因此 u 是可分元. □

引理 1.3.11. *对于域扩张 E/F, 假设 $[E : F] = d < \infty$, 下面叙述等价:*

(1) *E/F 是可分扩张.*

(2) *$E = FE^p$*

(3) *存在 E/F 的一组基 $\{e_1, \ldots, e_d\}$, 使得 $\{e_1^p, \ldots, e_d^p\}$ 也是一组基.*

证明: (1) $\Longrightarrow$ (2): 任取 $u \in E$, 那么 $F(u) = F(u^p) \subseteq FE^p$, 因此 $E \subseteq EK^p$, 另一方面包含关系是显然的.

(2) $\Longrightarrow$ (3): 假设 $E = Fe_1 \oplus \cdots \oplus Fe_n$, 那么任取 $u \in E$, 将其写做 $u = \sum_{i=1}^n f_i e_i$, 则 $u^p = \sum_{i=1}^n f_i^p e_i^p$, 从而 $E^p = F^p e_1^p + \ldots F^p e_d^p$, 进而 $E = Fe_1^p + \ldots Fe_d^p$. 由于 $[E : F] = d$, 从而 $\{e_1^p, \ldots, e_d^p\}$ 也是一组基. (3) $\Longrightarrow$ (2) 是显然的.

(2) $\Longrightarrow$ (1): 假设 $u \in E$ 是不可分的, $p(x)$ 是其极小多项式, 则 $p(x) = p_1(x^p) = \sum_{k=0}^n a_k x^{pk}$. 由于 $p(u) = 0$, 从而 $\{1, u^p, \ldots, u^{np}\}$ 是线性相关的, 并且根据极小多项式的性质可知 $\{1, u, \ldots, u^{np-1}\}$ 是线性无关的. 从 (2) $\Longrightarrow$ (3) 的证明可以看出 $\{1, u^p, \ldots, u^{p(np-1)}\}$ 是线性无关的, 但是 $n \leq 2n - 1 \leq pn - 1$, 即:

$$\{1, u^p, \ldots, u^{np}\} \subseteq \{1, u^p, \ldots, u^{p(np-1)}\}$$

相矛! □

命题 1.3.12. *单扩张 $F(u)/F$ 是可分扩张当且仅当 u 是 F 上的可分元.*

证明: 如果 $F(u)/F$ 是可分扩张, 显然有 u 是 F 上的可分元. 另一方面, 假设 $p(x) = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$ 是 u 的极小多项式, 则 $\{1, u, \ldots, u^{n-1}\}$ 是 $F(u)$ 在 F 上的一组基, 我们只需要证明 $\{1, u^p, \ldots, u^{p(n-1)}\}$ 也是一组基, 则根据引理1.3.11可知 $F(u)/F$ 是可分扩张.

假设 $\{1, u^p, \ldots, u^{p(n-1)}\}$ 不是一组基, 即存在 $\sum_k b_k u^{pk} = 0$, 考虑多项式 $p'(x) = \sum b_k x^k$, 则 $\deg p' \leq n - 1, p'(u^p) = 0$. 那么 $[F(u^p) : F] \leq n - 1$, 但是由于 u 是可分元, 从而根据引理1.3.10有 $F(u) = F(u^p)$, 即 $[F(u^p) : F] = [F(u), F] = n$, 相矛盾! □

推论 1.3.13. *域扩张 $F \subseteq E \subseteq K$, 则 K/F 是可分扩张当且仅当 $K/E, E/F$ 都是可分扩张.*

证明: 假设 K/F 是可分扩张, 那么任取 $u \in K$, 其在 E 上的不可约多项式可以整除其在 F 上的不可约多项式, 即 K/E 是可分扩张; E/F 是可分的更是显然, 因为任取 $u \in E$ 考虑其在 F 上的不可约多项式和将其看成是 K 中的元素考虑其在 F 上的不可约多项式是一样的.

另一方面, 任取 $u \in K$, 其在 E 上的极小多项式记做 $p_u(x) = a_n x^n + \cdots + a_0$. 考虑 $F \subseteq F(a_0, \ldots, a_n) \subseteq E \subseteq E(u) \subseteq K$, 由于 E/F 是可分的, 从而 $F(a_0, \ldots, a_n)/F$ 是可分的. 而 u 在 $F(a_0, \ldots, a_n)$ 上的极小多项式也是 p_u, 即是一个可分多项式, 从而根据命题1.3.12有 $F(u, a_0, \ldots, a_n)/F$ 是可分的. 特别地, u 在 F 上是可分的. □

推论 1.3.14. *$E/F, E'/F$ 都是可分扩张, 则 EE'/F 也是可分扩张.*

证明: 假设 $u \in E, u' \in E$ 以及它们的极小多项式分别为 $p_u, p_{u'}$. 由于 u 是可分的, 从而根据命题1.3.12可知 $F(u)/F$ 是可分的. 由于 u' 在 $F(u)$ 上的极小多项式整除 $p_{u'}$, 从而也是可分的, 即 $F(u,u')/F(u)$ 是可分的, 进而有 $F(u,u')/F$ 是可分的. □

1.3.3 纯不可分扩张

在本节中, F 总是指特征为 p 的域.

定义 1.3.15. $u \in \bar{F}$ 被称为在 F 上**纯不可分** (pure inseperable), 如果 $u^{p^m} \in F$, 对某个正整数 m 成立.

定义 1.3.16. 代数扩张 E/F 被称为**纯不可分扩张** (pure inseperable extension), 如果 E 中的每个元素在 F 上都是纯不可分的.

命题 1.3.17. *对于纯不可分扩张,*

(1) *如果 E/F 是有限纯不可分扩张, 则 $[E:F]$ 是 p 的幂次.*

(2) *如果 $K/E, E/F$ 都是纯不可分扩张, 则 K/F 也是纯不可分扩张.*

(3) *如果 $E/F, E'/F$ 都是纯不可分扩张, 则 EE'/F 也是纯不可分扩张.*

证明: (1). 由于 E/F 是纯不可分扩张, 从而 $u \in E$ 满足某个多项式 $x^{p^m} - c \in F[x]$, 从而其极小多项式整除 $x^{p^m} - c$, 进而极小多项式的次数也是 p 幂次. 对于 E 的任何包含 F 的子域 K, $u \in E$ 在 K 上的极小多项式一定整除其在 F 上的极小多项式, 从而次数也是 p 的幂次, 从而

$$[E:F] = [F(u_1,\dots,u_n) : F(u_1,\dots,u_{n-1})] \dots [F(u_1):F]$$

是 p 的幂次.

(2). 任取 $u \in K$, 由于 K/E 是纯不可分的, 因此存在正整数 m_1 使得 $u^{p^{m_1}} \in E$, 再利用 E/F 是纯不可分的, 可以找到正整数 m_2 使得 $(u^{p^{m_1}})^{p^{m_2}} \in F$, 从而 K/F 是纯不可分的.

(3). 任取 $u \in E, v \in E'$, 存在正整数 m_1, m_2 使得 $u^{p^{m_1}}, v^{p^{m_2}} \in F$, 则 $(uv)^{p^{m_1+m_2}}, (u+v)^{p^{m_1+m_2}} \in F$, 从而 EE'/F 也是纯不可分的. □

引理 1.3.18. *E/F 是域扩张, E 中所有在 F 上可分的元素组成的集合为 E_s, 那么 E_s 是 E 的子域, 并且 E/E_s 是纯不可分扩张.*

证明: 根据推论1.3.14, E_s 是 E 的子域. 取 $u \in E \backslash E_s$, 考虑 u 在 F 上的极小多项式 $p(x)$, 其不是可分多项式, 并且存在可分多项式 p_e 使得 $p = p_e(x^{p^e})$. 由于 p_e 是 u^{p^e} 的极小多项式, 则 $u^{p^e} \in E_s$, 即 E/E_s 是纯不可分扩张. □

定义 1.3.19. 对于域扩张 E/F 来说, 其可分次数 (seperable degree)定义为 $[E:F]_s := [E_s:F]$, 其不可分次数 (inseperable degree)定义为 $[E:F]_i := [E:E_s]$.

命题 1.3.20. *E/F 是有限扩张, 那么:*

$$|\mathrm{Hom}_F(E,\bar{F})| = [E:F]_s \le [E:F]$$

特别地, 等号取得当且仅当 E/F 是可分扩张.

证明: 首先我们证明有如下一一对应:

$$\mathrm{Hom}_F(E,\bar{F})=\mathrm{Hom}_F(E_s,\bar{F})$$

通过 $\tau\mapsto\tau|_{K_s}$ 给出. 对应是满射可根据命题1.2.6; 为了证明对应是单射, 即证明 τ 被 $\tau|_{E_s}$ 所决定: 任取 $u\in E$, 则存在正整数 m 使得 $u^{p^m}\in E_s$, 则 $\tau(u^{p^m})=\tau(u)^{p^m}=v\in\bar{F}$, 因此 $\tau(u)$ 满足方程 $x^{p^m}-v=(x-v')^{p^m}=0$, 可知 $\tau(u)$ 被唯一确定.

下面我们只需要对 E/F 是可分扩张证明 $|\mathrm{Hom}_F(K,\bar{F})|=[K:F]$ 即可. 这实际上约化到对单扩张证明, 对一般情况进行归纳即可: 注意到 $\tau:F(u)\to\bar{F}$ 完全由 $\tau(u)$ 所决定, 但由于 τ 是 F-嵌入, $\tau(u)$ 应该与 u 共轭, 因此嵌入的个数只有 u 的极小多项式不同根的个数个, 再由于 u 是可分元, 因此嵌入的个数等于 u 极小多项式的次数, 即:

$$|\mathrm{Hom}_F(F(u),\bar{F})|=[F(u):F]$$

□

第二章　Galois 理论

2.1　Galois 扩张

在开始之前, 我们固定一些符号: E/F 是域扩张, E 上的 F-自同构群定义为

$$\mathrm{Aut}_F(E) = \{\tau : E \xrightarrow{\cong} E \mid \tau|_F = \mathrm{id}\}$$

对于 $H < \mathrm{Aut}_F(E)$, 记 $E^H = \{u \in E \mid \tau(u) = u, \forall \tau \in H\}$. 对于域扩张 $F \subseteq E \subseteq K$, 有子群的包含关系: $\mathrm{Aut}_E(K) < \mathrm{Aut}_F(K)$.

引理 2.1.1. *如果 E/F 是代数扩张, 则 $\mathrm{Aut}_F(E) = \mathrm{Hom}_F(E, E)$.*

证明: 给定任意 F-自同态 $\tau : K \to K$, 首先其一定是单射, 因为域的理想都是平凡的, 那么我们只需要证明 τ 是满射即可. 任取 $u \in K$, 考虑其在 F 上的最小多项式 $p \in F[x]$, 如果 $\{u_1, \ldots, u_n\}$ 是 p 在 $\bar{F}$ 里面的不同的根, 我们假设 $\{u_1, \ldots, u_r\}$ 在 K 中, 显然 $u \in \{u_1, \ldots, u_r\}$. 由于 τ 固定 F, 那么 $\tau(u_i)$ 也会是 p 的根, 从而有 $\tau : \{u_1, \ldots, u_r\} \to \{u_1, \ldots, u_r\}$. 在这个有限集合上的单射一定是满射, 从而存在 u_i 使得 $\tau(u_i) = u$ □

定义 2.1.2. 代数扩张 E/F 被称为 **Galois 扩张** (Galois extension), 如果其是正规扩张, 且是可分扩张.

注记. 根据正规性可知 $\mathrm{Hom}_F(E, \bar{F}) = \mathrm{Hom}_F(E, E) = \mathrm{Aut}_F(E)$. 在 Galois 扩张时 $\mathrm{Aut}_F(E)$ 通常也被记作 $\mathrm{Gal}(E/F)$, 并且

$$|\mathrm{Gal}(K/F)| = |\mathrm{Hom}_F(K, K)| \overset{(1)}{=} |\mathrm{Hom}_F(K, \bar{F})| \overset{(2)}{=} [K : F]$$

其中 (1) 成立是根据定理1.3.2, (2) 成立是根据命题1.3.20.

命题 2.1.3. *对于域扩张 $F \subseteq E \subseteq K$, 如果 K/F 是 Galois 扩张, 则 K/E 也是.*

证明: 根据推论1.3.3以及推论1.3.13即可. □

注记. 注意, 对于域扩张 $F \subseteq E \subseteq K$, 如果 K/F 是 Galois 扩张, E/F 不一定是 Galois 扩张, 在下一节 Galois 对应中我们将看到 E/F 是 Galois 扩张当且仅当 $\mathrm{Gal}(K/E)$ 是 $\mathrm{Gal}(K/F)$ 的正规子群.

定义 2.1.4. E/F 是可分扩张, 则在 $\bar{F}$ 中包含 K 的最小的 Galois 扩张被称为 E/F 的 **Galois 闭包** (Galois closure).

注记. 对于一个任意的代数扩张 E/F, 我们都可以在 $\bar{F}$ 中寻找 E/F 的正规闭包: 将 E 写成 $F(S)$, 其中 $S=\{s_i\}\subseteq E$ 都是代数元. 对于每一个 s_i, 用 p_i 去记其在 F 上的极小多项式, 那么将这些 p_i 在 $\bar{F}$ 中的所有根都添加到 F 中, 得到的域记做 N, 不难发现 N 就是 K/F 的正规闭包. 特别地, 如果 E/F 是可分扩张, 我们可以选取 s_i 都是可分元, 从而此时的 N/F 也是可分扩张, 从而是 E/F 的 Galois 闭包. 更特别地, 我们可以发现, 如果 E/F 是有限可分扩张, 那么其 Galois 闭包也是 F 的有限扩张.

引理 2.1.5. *E/F 是有限 Galois 扩张, 则 $E^{\mathrm{Gal}(E/F)}=F$.*

证明: 首先显然 $F\subseteq E^{\mathrm{Gal}(E/F)}$; 另一方面, 任取 $u\in E^{\mathrm{Gal}(E/F)}$, 考虑 u 在 F 上的极小多项式 $p(x)$, 任取 $p(x)$ 的一个根 v, 定义嵌入 $F(u)\hookrightarrow\bar{F}$ 为 $u\mapsto v$, 根据命题1.2.6可以将其延拓成 $\tau:E\to\bar{F}$, 而根据 E 是正规扩张, 可知 $\tau(E)=E$, 即 $\tau\in\mathrm{Gal}(E/F)$. 由于 $u\in E^{\mathrm{Gal}(E/F)}$, 因此 $v=\tau(u)=u$, 即 $p(x)=x-u$, 即 $u\in F$. □

引理 2.1.6. *K 是域, $H=\{\tau_1,\dots,\tau_n\}$ 是 $\mathrm{Aut}(K)$ 的有限子集 (不必要是子群). 如果存在 $c_i\in K$ 使得*

$$c_1\tau_1(x)+\cdots+c_n\tau_n(x)=0$$

对任意的 $x\in K$ 成立, 那么 $c_i=0, i=1,\dots,n$.

证明: 假设存在这样的 c_i, 我们不妨假设

$$c_1\tau_1(x)+\cdots+c_r\tau_r(x)=0 \tag{2.1.1}$$

对任意的 $x\in K$ 成立, 并且 $c_i\neq 0, 1\leq i\leq r$, 其中 r 是满足这样条件最小的数. 用 $ax, a\in K^\times$ 替代 x 则有

$$c_1\tau_1(a)\tau_1(x)+\cdots+c_r\tau_r(a)\tau_r(x)=0 \tag{2.1.2}$$

(2.1.2) 减 (2.1.1) 乘 $\tau_r(a)$ 则有

$$c_1[\tau_1(a)-\tau_r(a)]\tau_1(x)+\cdots+c_{r-1}[\tau_{r-1}(a)-\tau_r(a)]\tau_{r-1}(x)=0$$

根据我们对 r 的假设则有 $\tau_i(a)=\tau_r(a)$ 对任意的 $1\leq i\leq r-1$ 以及 $a\in K^\times$ 成立, 从而有 $\tau_1=\tau_r, r\geq 2$, 相矛盾. □

引理 2.1.7 (阿廷引理)**.** *K 是域, $H=\{\tau_1,\dots,\tau_n\}, \tau_1=\mathrm{id}$ 是 $\mathrm{Aut}(K)$ 的有限子群, 记 $E=K^H$, 则 K/E 是 Galois 扩张, 并且扩张次数 $[K:E]=|H|$.*

证明: 我们首先证明 K/E 是 Galois 扩张: 任取 $u\in K$, 记 u 在 E 上的极小多项式为 p, 令 $\mathcal{O}$ 是 u 在 H 作用下的轨道, 考虑:

$$q(x)=\prod_{\alpha\in\mathcal{O}}(x-\alpha)$$

则任取 $\tau\in H$ 有 $\tau(q(x))=q(x)$, 即 $q(x)\in E[x]$. 并且由于 H 是一个子群, 其中含有单位元, 从而 $u\in\mathcal{O}$, 即 $q(u)=0$, 因此 $p(x)\mid q(x)$, 但是 q 没有重根, 并且所有的根都在 K 中, 因此 K/E 是 Galois 扩张.

现在来证明 $[K:E] \leq |H|$: 只需要证明任取 $u_1, \ldots, u_{n+1} \in K$, 它们是 E-线性相关即可: 考虑矩阵 $(\tau_i(u_j)) \in M_{n\times(n+1)}(K)$, 则其 $n+1$ 列 K-线性相关, 即存在 $c_1, \ldots, c_{n+1} \in K$, 且不全为零使得:

$$c_1 \begin{pmatrix} \tau_1(u_1) \\ \tau_2(u_1) \\ \vdots \\ \tau_n(u_1) \end{pmatrix} + c_2 \begin{pmatrix} \tau_1(u_2) \\ \tau_2(u_2) \\ \vdots \\ \tau_n(u_2) \end{pmatrix} + \cdots + c_{n+1} \begin{pmatrix} \tau_1(u_{n+1}) \\ \tau_2(u_{n+1}) \\ \vdots \\ \tau_n(u_{n+1}) \end{pmatrix} = 0 \tag{2.1.3}$$

不妨假设 $c_1, \ldots, c_r \neq 0$, $c_{r+1} = \cdots = c_{n+1} = 0$, 且这样的 r 是最小的. 那么 $r \geq 2$, 并且不妨假设 $c_1 = 1$, 考虑第一行:

$$u_1 + c_2 u_2 + \cdots + c_r u_r = 0 \tag{2.1.4}$$

我们断言 $c_2, \ldots, c_n \in E$, 不然如果存在 $2 \leq i \leq r$, 使得对任意的 $1 \leq j \leq n$ 有 $\tau_j(c_i) \neq c_i$, 用 τ_j 作用 (2.1.4) 可得

$$\tau_j(u_1) + \tau_j(c_2)\tau_j(u_2) + \cdots + \tau_j(c_r)\tau_j(u_r) = 0 \tag{2.1.5}$$

用 (2.1.5) 分别与 (2.1.3) 的每一行相减, 可以得到一个新的更小的 r', 这与 r 的选取相矛盾.

最后来证明 $[K:E] \geq |H|$: 假设 $[K:E] = r < n$, 令 $\{x_1, \ldots, x_r\}$ 是 K 在 E 上的一组基, 那么任取 $y \in K$, 将其写成

$$y = c_1 x_1 + \cdots + c_r x_r$$

考虑 $r \times n$ 矩阵 $(\tau_j(x_i))$, 其秩一定 $\leq r < n$, 因此存在非平凡的 ξ_i 满足

$$\begin{cases} \xi_1\tau_1(x_1) + \ldots + \xi_n\tau_n(x_1) = 0 \\ \qquad\qquad \vdots \\ \xi_1\tau_1(x_r) + \ldots + \xi_n\tau_n(x_r) = 0 \end{cases}$$

将上面第 i 个方程乘以 c_i, 由于 $E = K^H$, 因此 $\tau_j(c_i) = c_i$, 从而

$$\begin{cases} \xi_1\tau_1(c_1x_1) + \ldots + \xi_n\tau_n(c_1x_1) = 0 \\ \qquad\qquad \vdots \\ \xi_1\tau_1(c_rx_r) + \ldots + \xi_n\tau_n(c_rx_r) = 0 \end{cases}$$

因此 $\xi_1\tau_1(y) + \cdots + \xi_n\tau_n(y) = 0$ 对任意的 $y \in K$ 成立, 根据引理2.1.6可知 $\xi_i = 0$, 相矛盾! □

2.2 Galois 对应

定理 2.2.1. *K/F 是有限 Galois 扩张, 则存在如下的一一对应:*

$$\{\mathrm{Gal}(K/F)\text{的子群}\} \overset{1-1}{\Longleftrightarrow} \{K/F\text{的中间域}\}$$

对应法则为 $H \mapsto K^H$ 与 $E \mapsto \mathrm{Gal}(K/E)$; E/F 是 Galois 扩张当且仅当 $\mathrm{Gal}(K/E)$ 是 $\mathrm{Gal}(K/F)$ 的正规子群, 并且:

$$\mathrm{Gal}(E/F) \cong \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)$$

证明: 根据引理2.1.5有

$$E \to \mathrm{Gal}(K/E) \to K^{\mathrm{Gal}(K/E)} = E$$

现在只需要证明下面的对应成立:

$$H \to K^H \to \mathrm{Gal}(K/K^H) = H$$

一方面 $H \subseteq \mathrm{Gal}(K/K^H)$ 是显然的, 而根据引理2.1.7:

$$|\mathrm{Gal}(K/K^H)| \leq |H|$$

即两者相同.

由于根据推论1.3.14, E/F 已经是可分扩张, 从而 E/F 是 Galois 扩张当且仅当 E/F 是正规扩张, 即 $\tau(E) = E$. 任取 $\tau \in \mathrm{Gal}(K/F)$, 可以直接验证:

$$\mathrm{Gal}(K/\tau(E)) = \tau^{-1}\,\mathrm{Gal}(K/E)\tau$$

因此 E/F 是 Galois 扩张当且仅当 $\tau(E) = E$ 当且仅当 $\mathrm{Gal}(K/E)$ 是正规子群. □

推论 2.2.2. *E/F 是有限可分扩张, 则 E/F 中只存在有限多个中间域.*

证明: 考虑其 Galois 闭包 K/F, 由注记2.1可知其 Galois 闭包 K/F 也是有限扩张, 从而根据 Galois 对应 K/F 中只有有限多个中间域, 从而 E/F 中只有有限多个中间域. □

推论 2.2.3 (本原元定理)**.** *如果 E/F 是有限可分扩张, 则 $E = F(u), u \in E$.*

证明: 当 F 是有限域, 则不妨假设 $F = \mathbb{F}_p, E = \mathbb{F}_q, q = p^m$, 根据有限域的结果可知 $\mathbb{F}_q^\times = \langle \xi \rangle$, 因此 $\mathbb{F}_q = \mathbb{F}_p(\xi)$.

当 F 是无限域, 不妨假设 $E = F(u_1, u_2)$, 一般情况归纳即可: 任取 $r \in F$, 考虑 $F \subseteq F(u_1 + ru_2) \subseteq E$, 由于其中只有有限多个中间域, 并且 F 是无限域, 因此存在不同的 $r_1, r_2 \in F$ 使得:

$$F(u_1 + r_1u_2) = F(u_1 + r_2u_2)$$

考虑 $u = u_1 + r_1u_2$, 我们断言 $F(u) = F(u_1, u_2)$: 显然 $F(u) \subseteq F(u_1, u_2)$; 另一方面, 由于 $u = u_1 + r_1u_2 = u_1 + r_2u_2$, 并且 $r_1 \neq r_2$, 从而 $(r_1 - r_2)u_2 \in F(u)$, 即 $u_2 \in F(u)$, 从而 $u_1 \in F(u)$, 即 $F(u) = F(u_1, u_2)$. □

命题 2.2.4. *如果 $E/F, K/F$ 都是有限 Galois 扩张, 则 EK/F 也是 Galois 扩张, 并且*

(1)

$$\varphi : \mathrm{Gal}(EK/K) \to \mathrm{Gal}(E/E \cap K)$$
$$\tau \mapsto \tau|_E$$

是同构.

(2)

$$\psi : \mathrm{Gal}(EK/F) \to \mathrm{Gal}(E/F) \times \mathrm{Gal}(K/F)$$
$$\tau \mapsto (\tau|_E, \tau|_K)$$

是单射. 如果 $E \cap K = F$, 那么上述映射还是满射, 从而使同构.

证明: 根据推论1.3.3可知 EK/F 是正规扩张. 根据推论1.3.14可知 EK/F 是可分扩张, 从而 EK/F 是 Galois 扩张, 并且由于 $E/F, K/F$ 都是有限的, 从而 EK/F 也是有限 Galois 扩张, 因此 EK/E 也是有限 Galois 扩张.

(1). 任取 $\tau \in \mathrm{Gal}(EK/K)$, 考虑 $\tau|_E : E \to EK \hookrightarrow \bar{F}$, 由于 E/F 是正规的, 从而根据定理1.3.2有 $\tau(E) \subseteq E$, 即 $\tau|_E \in \mathrm{Gal}(E/E\cap K)$. 如果 $\tau|_E = \mathrm{id}_E$, 那么由于 $\tau|_F = \mathrm{id}_F$ 有 $\tau = \mathrm{id}_{EK}$, 即 φ 是单射. 另一方面, $\mathrm{im}\,\varphi$ 是 $\mathrm{Gal}(E/E\cap K)$ 的子群, 并且 $E^{\mathrm{im}\,\varphi} = (EK)^{\mathrm{Gal}(EK/K)} \cap E = K \cap E$, 从而 $\mathrm{im}\,\varphi = \mathrm{Gal}(E/E\cap K)$.

(2). ψ 是单射与 φ 是单射的证明同理. 如果 $E \cap K = F$, 那么任取 $(\sigma_1, \sigma_2) \in \mathrm{Gal}(E/F) \times \mathrm{Gal}(K/F)$, 根据 (1) 有 σ_1, σ_2 可以被延拓成 $\sigma_1' \in \mathrm{Gal}(EK/K)$ 和 $\sigma_2' \in \mathrm{Gal}(EK/E)$. 令 $\tau = \sigma_2' \circ \sigma_1' \in \mathrm{Gal}(EK/F)$, 那么 $\tau|_K = \sigma_2' \circ \sigma_1'|_K = \sigma_2'|_K = \sigma_2$, 同理有 $\tau|_E = \sigma_1$, 从而是满射. □

定义 2.2.5. 一个 Galois 扩张被称为**阿贝尔扩张** (abelian extension), 如果其 Galois 群是阿贝尔群.

定义 2.2.6. 一个 Galois 扩张被称为**循环扩张** (cyclic extension), 如果其 Galois 群是循环群.

推论 2.2.7. *阿贝尔扩张的复合也是阿贝尔扩张, 循环扩张的复合也是循环扩张.*

证明: 注意到阿贝尔群（循环群）的子群还是阿贝尔群（循环群）. □

2.3 一些 Galois 扩张的例子

2.3.1 有限域上的 Galois 扩张

定理 2.3.1. *$q = p^m, m > 0$, 则 $\mathbb{F}_{q^d}/\mathbb{F}_q$ 是 Galois 扩张, 并且 $\mathrm{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q) = \mathbb{Z}/d\mathbb{Z}$, 由 Frobenius 同构 $\sigma : x \mapsto x^q$ 生成.*

2.3.2 分圆扩张

定义 2.3.2. ξ_n 被称为 n **次本原单位根** (n-th primitive root of unity), 如果 $\xi_n^n = 1$ 且 $\xi_n^k \neq 1, \forall k < n$

注记. 对于 n 次本原单位根, 我们有如下两条注记:

1. n 次单位根的全体可以表示为 $\{\xi_n^k \mid 0 \le k \le n-1\}$
2. ξ_n^k 也是 n 次本原单位根当且仅当 $(n, k) = 1$

定义 2.3.3. n **次分圆多项式** (n-th cyclotomic polynomial)被定义为:

$$\Phi_n(x) = \prod_{\xi\text{是 } n \text{ 次本原单位根}} (x - \xi)$$

注记. 不难发现 $\Phi_n(x) \in \mathbb{Q}[x]$, 因为任取 $\tau \in \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$, 其一定将本原单位根映成本原单位根, 即 $\tau(\Phi(x)) = \Phi(x)$. 并且由于 $\Phi_n(x)$ 在 $\mathbb{Q}[x]$ 中整除 $x^n - 1$, 从而根据高斯引理有 $\Phi_n(x) \in \mathbb{Z}[x]$

引理 2.3.4 (Gauss)**.** 令 R 是一个唯一分解整环, $h \in R[x]$ 是一个首一多项式. 如果存在分解 $h = fg$, 其中 $f, g \in Q[x]$, Q 是 R 的分式域, 那么 $f, g \in R[x]$.

引理 2.3.5. 如果记 $P(x)$ 是 ξ_n 在 $\mathbb{Q}$ 上的极小多项式, p 是任意素数, 且 $p \nmid n$, 如果 u 是 $P(x)$ 的一个根, 则 u^p 也是 $P(x)$ 的一个根.

证明: 根据高斯引理, 将 $x^n - 1$ 做如下拆分:

$$x^n - 1 = P(x)Q(x)$$

其中 $P(x), Q(x) \in \mathbb{Z}[x]$. 假设 u^p 不是 $P(x)$ 的根, 则 u^p 是 $Q(x)$ 的根, 即 u 是 $Q(u^p)$ 的根, 即在 $\mathbb{Z}[x]$ 中 $P(x) \mid Q(x^p)$. 我们考虑模 p 以后的结果, 即在 $\mathbb{F}_p[x]$ 中 $\bar{P}(x) \mid \overline{Q(x^p)} = \bar{Q}(x)^p$, 即如果 $\alpha \in \bar{\mathbb{F}}_p$ 是 $\bar{P}(x)$ 的根, 则 α 也是 $\bar{Q}(x)$ 的根, 因此 α 是 $\overline{x^n - 1} \in \mathbb{F}_p[x]$ 的重根, 但是由于 $p \nmid n$, 这是不可能的. □

定理 2.3.6. n 次分圆多项式是 n 次本原单位根在 $\mathbb{Q}$ 的极小多项式

证明: 用 $P(x)$ 记 n 次本元单位根的极小多项式, 其一定整除 n 次分元多项式 $\Phi_n(x)$, 因此只需要证明每个 n 次本原单位根 ξ_n^k 都是 $P(x)$ 的根即可. 对 k 做如下分解:

$$k = \prod_i p_i^{r_i}$$

根据引理2.3.5, $\xi_n^{p_i}$ 都是 $P(x)$ 的根, 再次利用引理2.3.5可知 $\xi_n^{p_i^{r_i}}$ 都是 $P(x)$ 的根, 多次利用引理2.3.5则可知 ξ_n^k 是 $P(x)$ 的根. □

定理 2.3.7. $\mathbb{Q}(\xi_n)/\mathbb{Q}$ 是 *Galois* 扩张, 并且 $\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$.

证明: 首先 $|\mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})| = \deg \Phi_n(x) = \phi(n)$, 并且对于任意满足 $(n, k) = 1$ 的 k, 我们定义 $\tau_k : \xi_n \mapsto \xi_n^k$, 这给出了同构 $(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\cong} \mathrm{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$ □

注记. 下面列出一些有关 $(\mathbb{Z}/n\mathbb{Z})^\times$ 结构的结果:

命题 2.3.8. 如果 $n = p_1^{k_1} \dots p_r^{k_r}$, 则我们有:

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{k_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_r^{k_r}\mathbb{Z})^\times$$

命题 2.3.9. 当 $p \geq 3$ 时, 我们有:

$$(\mathbb{Z}/p^k\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} \times \mathbb{Z}/p^{k-1}\mathbb{Z}$$

是循环群.

命题 2.3.10. 当 $p = 2, k \geq 4$ 时, 我们有:

$$(\mathbb{Z}/2^k\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{k-2}\mathbb{Z}$$

不是循环群.

2.4 Galois 理论的应用

2.4.1 尺规作图问题

对于一个没有刻度的直尺和圆规, 我们只可以通过以下的方式得到新的点:

1. 两条直线的交点.
2. 一条直线与一个圆的交点.
3. 两个圆的交点.

定义 2.4.1. $(a,b)\in\mathbb{R}^2$ 被称为**可构造的** (constructable), 如果我们可以从 $(0,0),(1,0)$ 以及尺规作图得到 (a,b).

注记 (标准构造). 利用尺规, 我们有下面两种基本的做法:

1. 给定线段 AB, 作出以 AB 为直径的圆.
2. 给定直线 l 以及直线外一点 p, 可以作出过 p 与 l 垂直或平行的直线.

推论 2.4.2. *(a,b) 可构造当且仅当 $(a,0),(b,0)$ 可构造.*

定义 2.4.3. $c\in\mathbb{R}$ 称为**可构造的** (constructable), 如果 $(c,0)$ 可构造. 我们用 $\mathfrak{C}$ 记 $\mathbb{R}$ 中所有可构造的点.

命题 2.4.4. *对于 $\mathfrak{C}$, 我们有如下结果:*

(1) *$\mathfrak{C}$ 是 $\mathbb{R}$ 包含 $\mathbb{Q}$ 的子域.*

(2) *如果 $c\in\mathfrak{C},c>0$, 则 $\sqrt{c}\in\mathfrak{C}$*

证明: (1). 由于任何特征零的域都包含 $\mathbb{Q}$ 作为子域, 所以只需要证明 $\mathfrak{C}$ 是一个域即可. 如果 $c\in\mathfrak{C}$, 那么以 $(0,0)$ 为圆心 c 为半径画圆, 则有 $-c\in\mathfrak{C}$. 如果 $ab\in\mathfrak{C}$, 我们可以通过以下方式得到 a^{-1}.

(2). 如果 $c\in\mathfrak{C}$, 那么可以用如下的方式构造 $\sqrt{c}$. □

定义 2.4.5. $K\subseteq\mathbb{R}$ 是子域, K **中的平面** (plane of K)定义为 $K\times K\subseteq\mathbb{R}\times\mathbb{R}$; K **中的直线** (line of K)定义为连接 K 平面中两点的直线; K **中的圆** (circle of K)定义为圆心在 K 平面中, 半径在 K 中的圆.

引理 2.4.6. *我们有如下结果:*

(1) *两条 K 中直线的交点要么是空集, 要么是 K 中的点.*

(2) *一条 K 中的直线与一个 K 中的圆的交点要么是空集, 要么是 $K(\sqrt{u}),u\in K$ 中的点.*

(3) *两个 K 中的圆的交点要么是空集, 要么是 $K(\sqrt{u}),u\in K$ 中的点.*

证明: 只需要注意到 K 中的直线由下面方程定义:

$$ax+by+c=0,\quad a,b,c\in K$$

K 中的圆由下面方程定义:

$$x^2+y^2+ax+by+c=0,\quad a,b,c\in K$$

□

定理 2.4.7. *$c \in \mathfrak{C}$ 当且仅当存在下面的域扩张链:*

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$$

(1) $c \in K_n$.
(2) $[K_n : K_{n-1}] = 2$, 即 $K_{i+1} = K_i(\sqrt{u_i})$, 其中 $u_i > 0 \in K_i$.
特别地, 如果 c 可构造, 则 c 在 $\mathbb{Q}$ 上代数, 并且 $[\mathbb{Q}(c) : \mathbb{Q}]$ 是 2 的幂次.

证明: 假设 $c \in \mathfrak{C}$, 即 $(c, 0)$ 在 $\mathbb{R}^2$ 上可构造, 即 $(c, 0)$ 可以通过有限步画圆或化直线的操作得到. 在每一步中, 新的点由两条线的交点, 线与圆的交点以及圆与圆的交点得到, 从而根据引理2.4.6有期待的域扩张链.

另一方面, 如果我们假设这样域扩张链存在, 那么 c 在 K_{n-1} 上的极小多项式为 $x^2+ax+b \in K_{n-1}[x]$, 那么 $(c, 0)$ 可以通过圆 $(x + \frac{a}{2})^2 + y^2 = \frac{a^2}{4} - b$ 与 x 轴的交点的到. 根据命题2.4.4, 如果 u, v 可构造, 那么 $u \pm v, uv$ 都可构造. 由于 a, b 是 1 和 $\sqrt{u_{n-2}}$ 在 K_{n-2} 上线性组合得到的, 而 K_{n-2} 可由在 K_{n-3} 上构造 $\sqrt{u_{n-3}}$ 的到. 因此问题归结于在 K_{n-2} 上构造 $\sqrt{u_{n-2}}$. 由于 $(\sqrt{u_{n-2}}, 0)$ 是 $x^2 + y^2 = u_{n-2}$ 与 x 轴的交点, 即经过有限步操作后 c 可构造.

特别地, 如果 c 可构造, 那么 $\mathbb{Q} \subseteq \mathbb{Q}(c) \subseteq K_n$, 从而 $[K_n : \mathbb{Q}(c)][\mathbb{Q}(c) : \mathbb{Q}] = 2^n$, 从而 $[\mathbb{Q}(c) : \mathbb{Q}]$ 也是 2 的幂次. □

一、化圆为方

构造一个正方形, 使得其面积为给定的圆的面积: 这等价于 $\sqrt{\pi}$ 是否可构造? 显然是不可以的, 因为 π 在 $\mathbb{Q}$ 上超越.

二、倍立方体

构造一个立方体, 使得其体积为给定立方体的二倍, 这等价于 $\sqrt[3]{2}$ 是否可构造? 也是不可以的, 因为 $[\mathbb{Q}\sqrt[3]{2} : \mathbb{Q}] = 3$, 不是 2^n.

三、三等分角

给定角 θ, 三等分角即等价于构造 $\cos\theta/3$, 我们有如下的三角公式:

$$\cos\theta = 4\cos^3\theta/3 - 3\cos\theta/3$$

即等价于构造 $4x^3 - 3x - a = 0$ 的根, 我们给出下面的一些例子, 来说明这并非总是可以构造的:

例子. 如果 $a = \cos\frac{\pi}{3} = \frac{1}{2}$, 则此时是不可构造的, 因为等价于构造 $8x^3 - 6x - 1 = 0$ 这个不可约多项式的根, 这是三次扩张.

例子. 如果 $a = \cos\frac{\pi}{4}$, 此时是可以构造的, 此时下述多项式:

$$4x^3 - 6x - \frac{\sqrt{2}}{2} \in \mathbb{Q}(\sqrt{2})[x]$$

是可约的, $-\frac{\sqrt{2}}{2}$ 是其一个根, 因此实际上此时是二次扩张.

四、尺规作正 n 边形状问题

这等价于构造 $\theta_n = 2\pi/n$, 我们有下述引理:

引理 2.4.8. *尺规可作正 n 边形等价于 $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = 2^n$.*

证明: 令 $\xi_n = \cos\theta_n + i\sin\theta_n$, 只需要注意到:

$$[\mathbb{Q}(\xi_n) : \mathbb{Q}(\theta_n)] \leq 2$$

即可. □

定理 2.4.9. *尺规可作正 n 边形等价于 n 有如下分解:*

$$n = 2^k p_1 \dots p_k$$

其中 p_k 是费马素数.

证明: 由于 $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \phi(n)$, 令 $n = 2^k p_1^{r_1} \dots p_s^{r_s}$, 则

$$\phi(n) = 2^{k-1}(p_1 - 1)p^{r_1 - 1} \dots (p_s - 1)p^{r_s - 1}$$

若为 2 的幂次, 应该有 $r_i \leq 1$, p_i 形如 $2^m + 1$, 但是形如 $2^m + 1$ 的素数一定是 $2^{2^n} + 1$ 的形式, 即为费马素数. □

注记. 有关费马素数, 是形如 $2^{2^n} + 1$ 的素数, 实际上, 现在对费马素数的所知仍然很少, 已知的五个费马素数为 $n = 0, 1, 2, 3, 4$ 的情况, 对于 $n > 4$ 的情况, 所能验证的都不是素数, 但是否仅仅只有这五个费马素数, 还是一个猜想.

2.4.2 根式可解问题

在本节中, 所有的域的特征都是 0.

定义 2.4.10. 有限扩张 E/F 被称为**根式扩张** (radical extension), 如果存在 $u_1, \dots, u_n \in E, m_1, \dots, m_n \in \mathbb{N}$, 使得:

1. $K = F(u_1, \dots, u_n)$
2. $u_1^{m_1} \in F$, 并且对 $2 \leq i \leq n$ 有 $u_i^{m_i} \in F(u_1, \dots, u_{i-1})$.

即:

$$F \subseteq F(u_1) \subseteq \dots \subseteq F(u_1, \dots, u_n)$$

其中每一步被称为**单根式扩张** (simple radical extension).

注记. 根式扩张不一定是 Galois 扩张, 例如 $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$.

命题 2.4.11. *有关根式扩张的一些结果:*

(1) *如果 $F \subseteq E \subseteq K$, 其中 K/F 是根式扩张, 则 K/E 也是根式扩张, 但 E/F 不一定是根式扩张.*[1]

[1] 这条性质与正规扩张类似.

(2) 如果 $K/E, E/F$ 都是根式扩张, 则 K/F 也是根式扩张.

(3) 如果 $E/F, E'/F$ 都是根式扩张, 则 EE'/F 也是根式扩张.

(4) 如果 E/F 是根式扩张, 则其 *Galois* 闭包 K/F 也是根式扩张.

证明: (1). 如果 K/F 是根式扩张, 那么有 $K = F(u_1, \ldots, u_n)$, 其中 $u_1, \ldots, u_n$ 满足定义里的要求, 那么自然有 $K = E(u_1, \ldots, u_n)$, 即 K/E 也是根式扩张.

(2). 如果 $E = F(u_1, \ldots, u_n), K = E(u_{n+1}, \ldots, u_m)$, 那么 $K = F(u_1, \ldots, u_m)$, 即 K/F 是根式扩张.

(3). 假设 $E = F(u_1, \ldots, u_n)$, 那么 $EE' = E'(u_1, \ldots, u_n)$, 并且 $u_i^{m_i} \in F(u_1, \ldots, u_{i-1}) \subseteq E'(u_1, \ldots, u_{i-1})$, 从而 EE'/E' 是根式扩张, 从而根据 (2) 可知 EE'/F 也是根式扩张.

(4). 假设 $E = F(u_1, \ldots, u_n)$, 其中 $u_i^{m_i} \in F(u_1, \ldots, u_{i-1})$, P_i 是 u_i 在 F 上的极小多项式, 那么 Galois 闭包 K 由所有 P_i 的根生成. 令 $G = \mathrm{Gal}(K/F)$, 任取 $\tau \in G$, 那么 $\tau(E) = F(\tau(u_1), \ldots, \tau(u_n))$ 在 F 上也是根式扩张, 因为 $\tau(u_i)^{m_i} = \tau(u_i^{m_i}) \in \tau(F(u_1, \ldots, u_{i-1})) = F(\tau(u_1), \ldots, \tau(u_{i-1}))$. 从而根据 (3) 有 $K = \prod_\tau \tau(E)$ 是根式扩张. □

定义 2.4.12. 群 G 被称为**可解群** (solvable group), 如果 G 存在一个子群链 $G = G_0 \supset G_1 \supset \cdots \supset G_n = \{e\}$, 满足:

1. $G_{i+1} \triangleleft G_i$.
2. G_i/G_{i+1} 是阿贝尔群.

命题 2.4.13. *有关可解群的一些事实.*

1. *如果 G 是可解群, $H < G$, 则 H 也是可解群.*
2. *如果 G 是可解群, $H \triangleleft G$, 那么 G/H 也是可解群.*
3. *如果 $H \triangleleft G$, 且 $H, G/H$ 都是可解群, 则 G 也是可解群.*
4. *如果 G 是可解群, 则 G 有个极大正规子群, 其指数为素数 p.*

命题 2.4.14. *E/F 是有限 Galois 根式扩张, 则 $\mathrm{Gal}(E/F)$ 是可解群.*

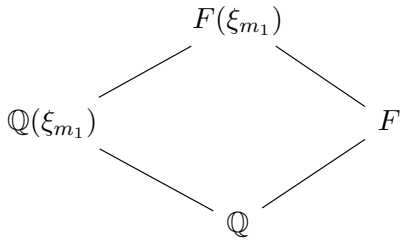
证明: 假设 $E = F(u_1, \ldots, u_n)$, 其中 $u_i^{m_i} \in F(u_1, \ldots, u_{i-1})$, 我们对 n 做归纳法. 当 $n = 1$ 时, $E = F(u_1)$, 并且 $u_1^{m_1} \in F$, 注意到 $E \subseteq F(u_1, \xi_{m_1})$, 从而根据命题2.4.13的 (1) 可知只需要证明 $\mathrm{Gal}(F(u_1, \xi_{m_1})/F)$ 是可解群即可. 考虑下图

$$\begin{array}{c} F(u_1, \xi_{m_1}) \\ | \\ F(\xi_{m_1}) \\ | \\ F \end{array}$$

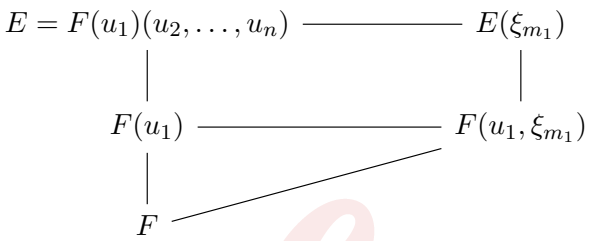
由于 $F(\xi_{m_1})$ 是 m_1 次本元多项式的分裂域, 从而 $F(\xi_{m_1})/F$ 是 Galois 扩张. 根据 Galois 对应, $\mathrm{Gal}(F(u_1, \xi_{m_1})/F(\xi_{m_1}))$ 是 $\mathrm{Gal}(F(u_1, \xi_{m_1})/F)$ 的正规子群, 并且

$$\mathrm{Gal}(F(\xi_{m_1})/F) \cong \mathrm{Gal}(F(u_1, \xi_{m_1})/F)/\mathrm{Gal}(F(u_1, \xi_{m_1})/F(\xi_{m_1}))$$

那么根命题2.4.13的 (3), 我们只需要证明 $\mathrm{Gal}(F(\xi_{m_1})/F)$ 和 $\mathrm{Gal}(F(u_1, \xi_{m_1})/F(\xi_{m_1}))$ 是可解群即可. 考虑如下图



我们有嵌入 $\mathrm{Gal}(F(\xi_{m_1})/F) \hookrightarrow \mathrm{Gal}(\mathbb{Q}(\xi_{m_1})/\mathbb{Q}) \cong (\mathbb{Z}/m_1\mathbb{Z})^\times$, 从而 $\mathrm{Gal}(F(\xi_{m_1})/F)$ 是阿贝尔群, 从而是可解群. 另一方面, 任取 $\tau \in \mathrm{Gal}(F(u_1, \xi_{m_1})/F(\xi_{m_1}))$, τ 完全由其在 u_1 上的值决定, 由于 $x^{m_1} - u_1^{m_1}$ 的所有根是 $u_1\xi_{m_1}^k$, 其中 $0 \le k \le m_1 - 1$, 因此 $\tau(u_1) = u_1\xi_{m_1}^k$, 并且由于 $\tau(\xi_{m_1}) = \xi_{m_1}$, 从而可知 $\mathrm{Gal}(F(u_1, \xi_{m_1})/F(\xi_{m_1}))$ 是一个阿贝尔群, 从而是个可解群, 至此我们解决了 $n = 1$ 的情况. 对于一般情况, 我们考虑下图



首先我们有 $\mathrm{Gal}(F(u_1, \xi_{m_1})/F)$ 是可解群, 并且根据归纳假设 $\mathrm{Gal}(E(\xi_{m_1})/F(u_1, \xi_{m_1}))$ 是可解群, 根据命题2.4.13的 (3) 有 $\mathrm{Gal}(E(\xi_{m_1})/F)$ 是可解群, 再根据命题2.4.13的 (1) 有 $\mathrm{Gal}(E/F)$ 是可解群. □

定义 2.4.15. $f(x) \in F[x]$ 被称为**根式可解** (solvable by radical), 如果其分裂域包含在 F 的某个根式扩张中.

引理 2.4.16. *E/F 是 Galois 扩张, $[E : F] = p$ 是素数, 假设 F 包含 p 次单位根 ξ_p, 则 E/F 是单根式扩张.*

证明: 由于 $\mathrm{Gal}(E/F) = \langle\tau\rangle$ 是一个 p 阶循环群, 构造 $u \in E$ 如下:

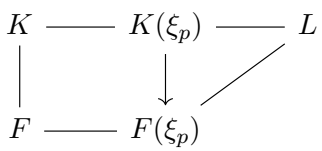
$$u = \sum_{i=0}^{p-1} \xi_p^i \tau^i(v), \quad v \in K$$

直接计算可得 u 满足 $\tau(u) = \xi_p^{-1}u, \tau(u^p) = u^p$, 即 $E = F(u)$, 是单根式扩张. □

注记. 将 E 视作 F 上的 p 维线性空间, $\tau : E \to E$ 是线性变换, 满足 $\tau^p = 1$, 因此其特征值为 $\{1, \xi_p, \ldots, \xi_p^{p-1}\}$, 构造的 u 则是 ξ_p^{-1} 对应的特征向量.

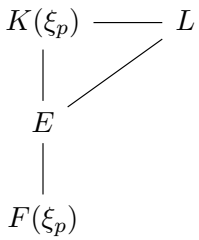
定理 2.4.17. *K/F 是有限 Galois 扩张, 并且 $\mathrm{Gal}(K/F)$ 是可解群, 那么 K 包含在 F 的某个根式扩张中.*

证明: 我们对 $[K : F] = n$ 进行归纳. 假设 $n = 2$, 由于任何二次方程 $x^2 + ax + b = 0$ 有求根公式, 从而 E/F 本身就是根式扩张. 假设命题对 $[K : F] \le n - 1, n \ge 2$ 时成立, 考虑如下图



由于 $\mathrm{Gal}(K/F)$ 是可解群, 根据命题2.4.13的 (4) 可知其存在一个指数是素数 p 的正规子群, 我们将 p 次本元单位根 ξ_p 添加到 E 中, 那么由于 $F \subseteq K$, 则 $[K(\xi_p) : E] \leq [F(\xi_p) : F]$, 因此 $[K(\xi_p) : K] \leq n$. 我们分以下两种情况考虑:

1. 如果 $[K(\xi_p) : F(\xi_p)] < n$, 那么根据归纳假设 $K(\xi_p)$ 包含在某个 F 的根式扩张 L 中，进而 L/F 是根式扩张, 并且包含 K.
2. 如果 $[K(\xi_p) : K(\xi_p)] = n$. 我们令 $E = K(\xi_p)^H$, 其中 H 是 $\mathrm{Gal}(K/F)$ 指数为 p 的正规子群. 考虑下图



由于 H 是正规子群, 从而 $E/F(\xi_p)$ 是次数为 p 的 Galois 扩张, 那么根据引理2.4.16可知其为单根式扩张, 再根据归纳假设有 $K(\xi_p)/E$ 包含在某个根式扩张 L/E 中, 因此 $L/F(\xi_p)$ 也是根式扩张.

□

定理 2.4.18. *$f(x) \in F[x]$ 根式可解当且仅当其对应的 Galois 群 G_f 是一个可解群.*

证明: 如果 $f(x)$ 根式可解, 因此分裂域 E 包含在 F 的某个根式扩张 K 中, 并且不妨假设 K/F 是 Galois 的, 因为根据命题2.4.11的 (4) 根式扩张的 Galois 闭包依然是根式扩张. 根据命题2.4.14有 $\mathrm{Gal}(K/F)$ 是可解群, 则 $G_f = \mathrm{Gal}(E/F) \hookrightarrow \mathrm{Gal}(K/F)$, 也是一个可解群. 另一方面, 根据定理2.4.17即可. □

2.5 多项式 Galois 群的计算

在本节中 F 是特征为零的域.

2.5.1 低次数多项式的 Galois 群的计算

多项式的判别式

对于判断一个多项式是否不可约, 我们通常有如下的办法:

1. (高斯引理) $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ 是本原多项式, 则 $f(x)$ 在 $\mathbb{Z}$ 上不可约当且仅当其在 $\mathbb{Q}$ 上不可约.
2. (艾森斯坦判别法) $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, 如果存在素数 p 使得 $p \nmid a_n, p \mid a_{n-1}, \ldots, a_0$, 且 $p^2 \nmid a_0$, 则 $f(x)$ 在 $\mathbb{Q}$ 上不可约.
3. 假设 $r \in \mathbb{Q}$ 是 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ 的根, 记 $r = c/d, (c, d) = 1$, 则 $c \mid a_0, d \mid a_n$. 特别地, 如果 $a_n = 1$, 则 $r \in \mathbb{Z}$, 是 a_0 的因子.
4. 如果 $f \in \mathbb{Z}[x]$ 在模 p 后不可约, 则 f 本身不可约.

引理 2.5.1. $\deg f(x)=n, f(x)\in\mathbb{Q}[x]$, 是不可约多项式, 则 $G_f\cong H<S_n$, 是一个可递子群, 并且 n 整除 $|G_f|$.

证明: 令 $u_1,\ldots,u_n$ 是 $f(x)$ 全部的根, 任取 $\sigma_f\in G_f$, 其完全被 $\sigma(u_i)$ 所决定, 因此 $G_f\hookrightarrow S_n$, 并且是可递的, 因为可以定义:

$$\sigma':u_i\to u_j$$

将其延拓成 G_f 中的元素. 注意到 $\mathbb{Q}\subseteq\mathbb{Q}(u_1)\subseteq K$, 由于 $[\mathbb{Q}(u_1):\mathbb{Q}]$ 的扩张次数是 n, 因此 n 整除 $|G_f|$. □

定义 2.5.2. 考虑 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\in F[x]$, 其所有的根为 $\alpha_i, 1\le i\le n$, 定义:

$$\Delta(f)=\prod_{1\le i<j\le n}(\alpha_i-\alpha_j)$$

$$D(f)=\Delta(f)^2$$

其中 $D(f)$ 被称为多项式 f 的**判别式** (discriminant).

例子. 如果 $f=x^2+bx+c$, 则 $D(f)=b^2-4c$.

例子. 如果 $f=x^3+px+q$, 则 $D(f)=-4p^3-27q^2$.

例子. 如果 $f=x^4+ax^2+bx+c$, 则 $D(f)=144ab^2c-128a^2c^2-4a^3b^2+16a^4c-27b^2+256c^3$.

引理 2.5.3. 若 f 是 n 次不可约多项式, 则 $G_f\subseteq A_n$ 当且仅当 $\Delta(f)\in F$.

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

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

因此 $\sigma\Delta(f)=\Delta(f)$ 当且仅当 $\sigma\in A_n$. □

低次数多项式的 Galois 群

定理 2.5.4. 如果 $f(x)\in\mathbb{Q}[x]$ 是二次不可约多项式, 则 $G_f\cong\mathbb{Z}/2\mathbb{Z}$.

定理 2.5.5. 如果 $f(x)\in\mathbb{Q}[x]$ 是三次不可约多项式, 则 $G_f\cong A_3$ 或 S_3, 且 $G_f=A_3$ 当且仅当 $\Delta(f)\in\mathbb{Q}$.

例子. 考虑 $x^3-3x+1\in\mathbb{Q}[x]$, 利用第三种方法可以容易判断其不可约, 并且 $D(f)=81$, 因此 $G_f=A_3$

例子. 考虑 $x^3+3x+1\in\mathbb{Q}[x]$, 利用第三种方法可以容易判断其不可约, 并且 $D(f)=-135$, 因此 $G_f=S_3$

对于四次不可约多项式 $f(x)\in\mathbb{Q}[x]$ 的情形, 略微有一些复杂, 我们首先将 S_4 的所有子群列举如下:

命题 2.5.6. S_4 的所有子群分类如下:

1. 平凡子群 $\{\mathrm{id}\}, S_n$.

2. $\{\mathrm{id}, (12)(34)\}$, 不是可递子群.
3. $C_4 = \langle (1234) \rangle$, 是可递子群.
4. $V_4 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$, 是可递子群, 并且还是正规子群.
5. $\langle (12), (34) \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, 不是可递子群.
6. 二面体群, $D_4 = \{(1234), (13)\}$, 是可递子群, 并且是 S_4 的 *Sylow-2* 子群.
7. $A_3, S_3 \hookrightarrow S_4$, 不是可递子群.
8. A_4, 是可递子群.

注记. 因此所有可能作为 Galois 群出现的只有:

$$C_4, V_4, D_4, A_4, S_4$$

引理 2.5.7. 假设 x_1, x_2, x_3, x_4 是 f 的根, 令

$$\begin{cases} \alpha = x_1x_2 + x_3x_4 \\ \beta = x_1x_3 + x_2x_4 \\ \gamma = x_1x_4 + x_2x_3 \end{cases}$$

那么有

$$\begin{array}{c} \mathbb{Q}(x_1, x_2, x_3, x_4) \\ \Big| \ \mathrm{Gal}_f \cap V_4 \\ \mathbb{Q}(\alpha, \beta, \gamma) \\ \Big| \ \mathrm{Gal}_f \,/\, \mathrm{Gal}_f \cap V_4 \\ \mathbb{Q} \end{array}$$

证明: 注意到 S_4 可以作用在 $\{\alpha, \beta, \gamma\}$ 上, 并且 $\mathrm{Stab}(\alpha) \cap \mathrm{Stab}(\beta) \cap \mathrm{Stab}(\gamma) = V_4$, 从而 $\mathrm{Gal}(\mathbb{Q}(x_1, \ldots, x_4)/\mathbb{Q}(\alpha, \beta, \gamma)) = \mathrm{Gal}_f \cap V_4$.

考虑多项式 $g(x) = (x-\alpha)(x-\beta)(x-\gamma)$, 称作 f 的**三次预解** (cubic resolvent), 由于 S_4 作用在 $\{\alpha, \beta, \gamma\}$ 上, 那么任取 $\tau \in S_4$, 有 $\tau(g) = g$, 即 $g(x) \in \mathbb{Q}[x]$. 那么任取 $\tau \in G_f$, $\tau(g) = g$, 即 $g \in \mathbb{Q}[x]$, 其分裂域是 $\mathbb{Q}(\alpha, \beta, \gamma)$. 从而 $\mathbb{Q}(\alpha, \beta, \gamma)/Q$ 是 Galois 扩张, 并且根据 Galois 对应可知 $\mathrm{Gal}_g = \mathrm{Gal}_f \,/\, \mathrm{Gal}_f \cap V_4$. □

引理 2.5.8. f, g 有着相同的判别式, 并且如果 $f = x^4 + bx^3 + cx^2 + dx + e$, 则 $g = x^3 - cx^2 + (bd - 4e)x - b^2e + 4ce - d^2$. 特别地, 如果 $f = x^4 + dx + e$, 则 $g = x^3 - 4ex - d^2$.

定理 2.5.9. 令 $M = \mathbb{Q}(\alpha, \beta, \gamma) = G_g$, $E = \mathbb{Q}(x_1, x_2, x_3, x_4)$, 以及 $[M : \mathbb{Q}] = m$, 则

(1) $m = 1$ 时 $G_f = V_4$.
(2) $m = 2$ 时 $G_f = C_4$ 或 D_4. 并且 $\mathrm{Gal}_f = D_4$ 当且仅当 f 在 M 上不可约.
(3) $m = 3$ 时 $G_f = A_4$.
(4) $m = 6$ 时 $G_f = S_4$.

证明: (1). 如果 $m = 1$, 那么 Gal_g 是平凡群, 从而 $\mathrm{Gal}_f \cap V_4 = V_4$, 即 $\mathrm{Gal}_f \subseteq V_4$. 但是 V_4 没有可递的真子群, 从而 $\mathrm{Gal}_f \cong V_4$.

(2). 如果 $m = 2$, 即 $|\mathrm{Gal}_f \,/\, \mathrm{Gal}_f \cap V_4| = 2$, 我们分如下的情况讨论:

(a) 如果 $|\mathrm{Gal}_f \cap V_4| = 1$, 那么 $|\mathrm{Gal}_f| = 2$, 但是 S_4 没有这样的可递子群.

(b) 如果 $|\mathrm{Gal}_f \cap V_4| = 2$, 那么 $|\mathrm{Gal}_f| = 4$, 这种情况时 $\mathrm{Gal}_f = C_4$.

(c) 如果 $|\mathrm{Gal}_f \cap V_4| = 4$, 那么 $|\mathrm{Gal}_f| = 8$, 这种情况时 $\mathrm{Gal}_f = D_4$.

(d) 注意到 $\mathrm{Gal}_f = D_4$ 当且仅当 $|\mathrm{Gal}_f \cap V_4| = 4$, 这也等价于说 $[E : M] = 4$. 如果 f 在 M 上不可约, 那么 $[E : M] \geq 4$, 但是 $[E : M]$ 本身就 ≤ 4, 从而 $[E : M] = 4$. 当 f 在 M 上可约, 那么对于 f 的根 x, 如果 x 的极小多项式是一次的, 那么此时 $[E : M] = 1$; 如果 x 的极小多项式是二次的, 那么 f 在 $M(x)$ 中有两个根, 不妨是 x_1, x_2. 利用

$$\begin{cases} \frac{\beta}{x_1} = x_3 + \frac{x_2}{x_1} x_4 \\ \frac{\gamma}{x_1} = \frac{x_2}{x_1} x_3 + x_4 \end{cases}$$

可知 x_3, x_4 也在 $M(x)$ 中, 从而 $[E : M] = 2$. 因此 $\mathrm{Gal}_f = D_4$ 当且仅的 f 在 M 上不可约.

(3). 如果 $m = 3$, 那么 $|\mathrm{Gal}_f / \mathrm{Gal}_f \cap V_4| = 3$, 即 3 整除 $|\mathrm{Gal}_f|$. 那么 Gal_f 只能是 A_4 或者 S_4. 然而 $|S_4/V_4| = 6$, 从而 Gal_f 只能是 A_4.

(4). 如果 $m = 6$, 那么 $|\mathrm{Gal}_f / \mathrm{Gal}_f \cap V_4| = 6$, 从而 Gal_f 只能是 S_4. □

例子. $f(x) = x^4 + 4x^2 + 2 \in \mathbb{Q}[x]$, 此时三次预解 $g(x) = x^3 - 4x^2 - 8x + 32 = (x - 4)(x^2 - 8)$, 因此 $M = \mathbb{Q}(\sqrt{2})$, 即 $m = 2$, 并且 $f(x)$ 在 M 上可以分解成:

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

因此 $G_f \cong C_4$

例子. $f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$, 此时三次预解 $g(x) = x^3 - 8x - 4$, 是不可约多项式, 根据三次不可约多项式的理论, 计算其判别式 $D(g) = 1616$, 因此 $\sqrt{1616} \notin \mathbb{Q}$, 即此时 $[M : \mathbb{Q}] = 6$, 因此 $G_f \cong S_4$.

2.5.2 Galois 群为 S_n 的多项式

引理 2.5.10. 令 $f \in \mathbb{Z}[x]$ 是首一多项式, 对于任何给定的素数 p, 用 $\bar{f} \in \mathbb{F}_p[x]$ 记 f 模 p 之后的结果, 并且假设 $\bar{f}$ 可分, 则 $G_{\bar{f}} < G_f$.

引理 2.5.11. $G < S_n$ 是 S_n 可递子群, 假设 G 包含一个 2 轮换 σ 和 $n-1$ 轮换 τ, 那么 $G = S_n$.

证明: 不妨取 $\tau = (23 \ldots n)$, 因为任何 $n - 1$ 轮换都可以生成它. 并且因为 G 是可递的, 我们可以取 $\sigma = (1a)$, 因为任取 $\sigma' \in S_n$, 我们有:

$$\sigma'(ij)\sigma'^{-1} = (\sigma'(i)\sigma'(j))$$

因此只需根据可递性取 σ' 满足 $\sigma'(i) = 1$, 即可. 用 τ^k 作用在 $(1a)$ 上, 即

$$\tau^k(1a)\tau^{-k} = (1\tau^k(a))$$

可以得到 $(12), (13), \ldots, (1n)$, 即 $G = S_n$. □

下面回顾一些有关有限域上的多项式的 Galois 群的结果, 我们知道有限域上的 Galois 扩张的 Galois 群都是循环群, 因此任取 $\bar{f} \in \mathbb{F}_p[x]$ 是一个 d 次不可约多项式, 那么 $G_{\bar{f}} \cong \mathbb{Z}/d\mathbb{Z} < S_d$, 生成元为 Frobenius 同构 $x \mapsto x^p \in G_{\bar{f}}$, 这对应了一个 d 轮换.

更一般的, 如果 $\bar{f} = \bar{f}_1 \dots \bar{f}_r \in \mathbb{F}_p[x]$, $G_{\bar{f}}$ 是 S_d 的一个循环子群, 其中 $d = d_1 + \cdots + d_r, \deg \bar{f}_i = d_i, i = 1, \dots, r$, 其生成元形如:

$$(d_1\text{轮换})(d_2\text{轮换}) \dots (d_r\text{轮换})$$

特别地, 如果 $\bar{f} = \bar{f}_1\bar{f}_2$, 其中 $d_1 = d - 2, d_2 = 2$, 则 $G_{\bar{f}}$ 包含一个 $(d-2)$ 轮换, 一个 2 轮换.

定理 2.5.12. *对于 $n \geq 1$, 存在一个 $\mathbb{Q}$ 上的 n 次不可约多项式, 使得其 Galois 群为 S_n.*

证明: 不妨假设 $n \geq 4$, 因为对于低次数的情况在上一节已经完全研究清楚.

第一步: 首先构造 n 次多项式 $f_1 \in \mathbb{Z}[x]$, 使得 $f_1 \pmod 2$ 可以在 $\mathbb{F}_2[x]$ 中分解成 xh_1, 并且在 $h_1 \in \mathbb{F}_2[x]$ 是不可约的. (这样的 f_1 也是存在的, 因为在 $\mathbb{F}_p[x]$ 中, 任意次数的不可约多项式总是存在的, 因此 h_1 存在, 再将 xh_1 进行提升即可.)

第二步: 再构造 n 次首一多项式 $f_2 \in \mathbb{Z}[x]$, 使得 $f_2 \pmod 3 \in \mathbb{F}_3[x]$ 可以分解为 $h_1'h_2'$, 满足 $\deg h_1' = n-2, \deg h_2' = 2$, 其中 h_2' 是不可约多项式, 而对于 h_1' 来说, 如果 n 是奇数, 则 h_1' 是不可约多项式, 如果 n 是偶数, 则 $h_1' = xh_1''$, 其中 h_1'' 是 $n-3$ 次不可约多项式. 并且还要要求 $\bar{f}_2$ 是可分的.

注记. 为什么要如此构造呢? $G_{\bar{f}_2}$ 中的元素形如:

$$\begin{cases} (n-2\text{轮换})(2\text{轮换}), & n = 2k \\ (n-3\text{轮换})(2\text{轮换}), & n = 2k+1 \end{cases}$$

不妨记作 $\sigma_1\sigma_2$, 则 $n = 2k$ 时, $(\sigma_1\sigma_2)^{n-2} = \sigma_2^{n-2} = \sigma_2$, 同样, $n = 2k+1$ 时, $(\sigma_1\sigma_2)^{n-3} = \sigma_2^{n-3} = \sigma_2$, 即使得 $G_{\bar{f}_2}$ 中包含一个 2 轮换.

第三步: 构造不可约多项式 $f \in \mathbb{Z}[x]$ 使得: $f \equiv f_1 \pmod 2, f \equiv f_2 \pmod 3$. 我们选次数不超过 $n-1$ 的多项式 f_3, 使得:

$$f = 3f_1 - 2f_2 + 6f_3$$

并且 f 对于素数 5 来说是一个艾森斯坦多项式. 这样的 f_3 是可以找到的: 假设 $3f_1 - 2f_2 = x^n + f_4$, 其中 $f_4 = a_{n-1}x^{n-1} + \cdots + a_0$, 由于 $6 \equiv 1 \pmod 5$, 那么总可以找到 b_i 使得 $5 \mid a_i + 6b_i$, 如果 $25 \mid a_0 + 6b_0$, 那么用 $b_0 + 5$ 替换 b_0 则有 $25 \nmid a_0 + 6b_0 + 30$.

因此根据引理2.5.10有 $\mathrm{Gal}_{\bar{f}_1}$ 和 $\mathrm{Gal}_{\bar{f}_2}$ 都是 Gal_f 的子群, 从而 Gal_f 含有 2 轮换和 $n-1$ 轮换, 从而根据引理2.5.11可知 $G_f \cong S_n$. □

例子. *对于 $n = 4$, 首先在 $\mathbb{F}_2[x]$ 选取 3 次不可约多项式 $x^3 + x + 1$, 令 $f_1 = x(x^3 + x + 1)$ 即可; 在 $\mathbb{F}_3[x]$ 中, 选取 2 次不可约多项式 $x^2 + x + 2$, 那么令 $f_2 = x(x-1)(x^2 + x + 2)$ 即可, 计算:*

$$3f_1 - 2f_2 = x^4 + x^2 + 7x$$

不妨取 $f_3 = -x^2 - 2x + 5$, 那么:

$$3f_1 - 2f_2 + 6f_3 = x^4 - 5x^2 - 5x + 30$$

就是我们寻找的 4 次不可约多项式, 其 Galois 群为 S_4.

如果 n 是一个素数, 则 Galois 群为 S_n 的不可约多项式的存在性的证明则更容易一些:

引理 2.5.13. *p 是素数, $G < S_p$, 并且 G 包含一个 2 轮换和 p 轮换, 则 $G = S_p$.*

定理 2.5.14. *p 是素数, f 是 $\mathbb{Q}$ 上的不可约 p 次多项式, 恰有两个虚根. 则 $G_f \cong S_p$.*

证明: 首先复共扼 $c : a + bi \mapsto a - bi$ 属于 G_f, 对应于一个 2 轮换; 并且柯西定理保证, 对于一个有限群, 素数 p 整除群的阶数, 则其中包含一个 p 阶的元素, 这对应于 S_p 中的一个 p 轮换. □

第三章　无穷 Galois 理论

3.1　Krull 拓扑

在本节中, K/F 是 Galois 扩张, 并且我们假定读者对拓扑群以及逆极限有一些基础, 见附录A.1以及B.1.

定义 3.1.1. $\mathrm{Gal}(K/F)$ 上的 **Krull 拓扑** (Krull topology)如下定义: $1 \in \mathrm{Gal}(K/F)$ 的开邻域基 $\mathcal{N}$ 定义为:

$$\{\mathrm{Gal}(K/E) : E/F\text{是有限 Galois 扩张}\}$$

由这个开邻域基诱导的拓扑称为 $\mathrm{Gal}(K/F)$ 上的 Krull 拓扑.

注记. 我们要验证上述给出的 $\mathcal{N}$ 真的是 1 的一个开邻域基: 首先 1 在其中式显然的, 并且任取 $E/F, E'/F$ 是有限 Galois 扩张, 那么根据命题2.2.4可知 EE'/F 也是有限 Galois 扩张, 并且 $\mathrm{Gal}(K/EE') = \mathrm{Gal}(K/E) \cap \mathrm{Gal}(K/E')$, 从而 $\mathcal{N}$ 中两个开邻域的交还是一个开邻域, 即构成了一个开邻域基.

引理 3.1.2. *任取 $F \subseteq E \subseteq K$, E/F 是有限 Galois 扩张, 则*

$$\begin{aligned} \varphi : \mathrm{Gal}(K/F) &\to \mathrm{Gal}(E/F) \\ \sigma &\mapsto \sigma|_E \end{aligned}$$

是一个连续的满射.

证明: 满射是显然的, 因为任何 F 自同构 $\sigma : E \to E$ 可以延拓到 $\sigma' : K \to K$.

由于 $\mathrm{Gal}(E/F)$ 是有限群, 其上带有离散拓扑, 因此只需要证明 $\ker\varphi$ 是开集即可. $\tau \in \ker\varphi$ 当且仅当 $\tau|_E = \mathrm{id}$, 这也当且仅当 $\tau \in \mathrm{Gal}(K/E)$. 根据 Krull 拓扑的定义, 其本身就是开集. □

注记. 实际上, Krull 拓扑可以视作使得上述类型的映射连续的最粗糙的拓扑.

定理 3.1.3. *有如下作为拓扑群的同构*

$$\tau : \mathrm{Gal}(K/F) \xrightarrow{\cong} \varprojlim \mathrm{Gal}(E/F) \hookrightarrow \prod_{\substack{F\subseteq E\subseteq K \\ E/F\text{有限 Galois 扩张}}} \mathrm{Gal}(E/F)$$

证明: 先证明作为群是同构的: 首先任取 $\sigma \in \mathrm{Gal}(K/F), \tau(\sigma) = (\sigma|_E) \in \varprojlim \mathrm{Gal}(E/F)$, 这是因为如果 $E \subseteq E'$, 那么 $(\sigma|_E)|_{E'} = \sigma|_{E'}$; 反之, 任取 $(\sigma_E) \in \varprojlim \mathrm{Gal}(E/F)$, 构造 $\sigma \in \mathrm{Gal}(K/F)$ 使

得 $\sigma|_E = \sigma_E$ 如下: 任取 $x \in K$, 选择足够大的 E, 使得 E/F 是有限 Galois 扩张, 并且 $x \in E$, 定义为:

$$\sigma(x) := \sigma_E(x)$$

这是良定义的, 因为任取包含 x 的 F 另一个有限 Galois 扩张 E', 可以考虑 EE'/F 这个 Galois 扩张, 并且:

$$\sigma_E(x) = \sigma_{EE'}(x) = \sigma_{E'}(x)$$

下面证明拓扑上是同胚的: 首先 τ 是连续的, 因为 $\mathrm{Gal}(K/F) \to \varprojlim \mathrm{Gal}(E/F) \to \mathrm{Gal}(E/F)$ 是连续的. 下面只需要证明任取 $\mathrm{Gal}(K/F)$ 的开邻域 $U - \mathrm{Gal}(K/E')$, 验证 $\tau(U)$ 是开集即可:

$$\tau(\mathrm{Gal}(K/E')) = (\prod_{E \subseteq E'} \{1\} \times \prod_{E \not\subseteq E'} \mathrm{Gal}(E/F)) \cap \varprojlim \mathrm{Gal}(E/F)$$

□

推论 3.1.4. $\mathrm{Gal}(E/F)$ *带有 Krull 拓扑是一个射有限群.*

注记. 令 $\mathcal{N}' = \{\mathrm{Gal}(K/E) : E/F\text{是有限扩张}\}$, 如果我们定义 $\mathcal{N}'$ 作为 1 的开邻域基, 则其中“看似包含了更多的开集”, 但实际上是相同的拓扑: 考虑 E 的 Galois 闭包 E', 则我们有包含关系 $\mathrm{Gal}(K/E') < \mathrm{Gal}(K/E)$. 然而在拓扑群中, 如果 $H' < H$, 且 H' 是开集, 则 H 也是开子集 (利用陪集分解), 因此 $\mathrm{Gal}(K/E')$ 是开集可以推出 $\mathrm{Gal}(K/E)$ 是开集. 因此 $\mathcal{N}$ 与 $\mathcal{N}'$ 生成的拓扑是一致的.

推论 3.1.5. *如果 K/F 是有限 Galois 扩张, 则 $\mathrm{Gal}(K/F)$ 上的 Krull 拓扑就是离散拓扑.*

推论 3.1.6. *任取 $F \subseteq E \subseteq K$, 则 $\mathrm{Gal}(K/E)$ 是闭集.*

证明: 实际上 E 可以写成 F 上所有满足 $F \subseteq L \subseteq E$ 的有限扩张 L 的复合, 因此:

$$\mathrm{Gal}(K/E) - \bigcap \mathrm{Gal}(K/L)$$

由于 $\mathrm{Gal}(K/L)$ 是开集, 那么根据引理A.1.5也是闭集, 因此 $\mathrm{Gal}(K/E)$ 作为任意闭子集的交也是闭的. □

3.2 无穷 Galois 理论

下面来介绍无穷 Galois 理论的主要内容:

命题 3.2.1. K/F *是 Galois 扩张, 则*

1. $K^{\mathrm{Gal}(K/F)} = F$
2. *令* $H < \mathrm{Gal}(K/F)$, *则* $\mathrm{Gal}(K/K^H) = \bar{H}$

证明: (1). 任取 $x \in K$, 考虑其包含在 F 的某个有限 Galois 扩张 E 中, 如果 $x \in K^{\mathrm{Gal}(K/F)}$, 则 $x \in E^{\mathrm{Gal}(E/F)} = F$

(2). 根据推论3.1.6, $\mathrm{Gal}(K/K^H)$ 是闭集, 因此 $\bar{H} \subseteq \mathrm{Gal}(K/K^H)$; 另一方面, 任取 $\sigma \notin \bar{H}$, 证明 $\sigma \notin \mathrm{Gal}(K/K^H)$, 由于 $\sigma \notin \bar{H}$, 则存在 $\mathrm{Gal}(K/E)$, 其中 E/F 是有限 Galois 扩张, 使得 $\sigma\,\mathrm{Gal}(K/E) \cap H = \varnothing$, 考虑下面的短正合列:

$$1 \to \mathrm{Gal}(K/E) \to \mathrm{Gal}(K/F) \xrightarrow{\varphi} \mathrm{Gal}(E/F) \to 1$$

上述条件等价于 $\varphi(\sigma) \notin \varphi(H)$, 根据有限 Galois 对应:

$$\varphi(H) = \mathrm{Gal}(E/E^{\varphi(H)})$$

即存在 $x \in E^{\varphi(H)} = K^H$, 使得 $\varphi(\sigma)$ 移动 x, 因此 $\sigma \notin \mathrm{Gal}(K/K^H)$ □

定理 3.2.2. *K/F 是 Galois 扩张, 则存在如下的一一对应:*

$$\{\mathrm{Gal}(K/F)\text{的闭子群}\} \xLeftrightarrow{1\text{–}1} \{F \subseteq E \subseteq K\}$$

并且:

1. *H 是开子群当且仅当 K^H 在 F 上次数有限;*
2. *H 是正规子群当且仅当 K^H/F 是 Galois 扩张, 并且 $\mathrm{Gal}(K^H/F) \cong G/H$*

证明: 一一对应是命题3.2.1的直接结果, 需要证明的只有 (1), 其余的都与有限 Galois 对应相同: 根据拓扑群的结果, 由于 $\mathrm{Gal}(K/F)$ 是紧群, 因此 H 是开子群当且仅当 H 是有限指数的闭子群, 并且由于 H 的指数等于 $[K^H : F]$, 因此 H 是开子群当且仅当 K^H/F 是有限扩张; □

例子. *固定 p, 对任意 n, 用 ξ_{p^n} 记 p^n 次本原单位根, 则令 $K = \bigcup_n \mathbb{Q}(\xi_{p^n})$, 则*

$$\mathrm{Gal}(K/\mathbb{Q}) \cong \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times = \mathbb{Z}_p^\times$$

例子. *$\mathbb{F}_{p^n}/\mathbb{F}_p$ 是有限 Galois 扩张, 并且 $\bigcup_{n\geq 1} \mathbb{F}_{p^n} = \bar{\mathbb{F}}_p$, 则*

$$\mathrm{Gal}(\mathbb{F}_p/\mathbb{F}_p) \cong \varprojlim_n (\mathbb{Z}/n\mathbb{Z}) = \hat{\mathbb{Z}}$$

第四章　Galois 上同调与 Kummer 理论

4.1　范与迹

定义 4.1.1. E/F 是有限扩张, 对于 $\alpha \in E$, 其**范数** (norm)定义为 F-线性映射 $m_\alpha(x) = \alpha x$ 的行列式, 即

$$\mathrm{N}_{E/F}(\alpha) = \det(m_\alpha)$$

其**迹** (trace)定义为

$$\mathrm{Tr}_{E/F}(\alpha) = \mathrm{trace}(m_\alpha)$$

注记. 根据线性代数的知识, 我们有

1. $\mathrm{N}_{E/F}$ 是可乘的.
2. 如果 $a \in F$, 则 $\mathrm{N}_{E/F}(a\alpha) = a^{[E:F]}\,\mathrm{N}_{E/F}(\alpha)$.
2. $\mathrm{Tr}_{E/F}$ 是可加的.
4. 如果 $a \in F$, 则 $\mathrm{Tr}_{E/F}(a\alpha) = a\,\mathrm{Tr}_{E/F}(\alpha)$.
5. 如果 $\alpha \in F$, 则

$$\mathrm{N}_{E/F}(\alpha) = \alpha^{[E:F]}$$
$$\mathrm{Tr}_{E/F}(\alpha) = [E:F]\alpha$$

引理 4.1.2. 如果 $F \subseteq E \subseteq K, \alpha \in E$, 则

$$\mathrm{N}_{K/F}(\alpha) = \mathrm{N}_{E/F}(\alpha)^{[K:E]}$$
$$\mathrm{Tr}_{K/F}(\alpha) = [K:E]\,\mathrm{Tr}_{E/F}(\alpha)$$

证明: 假设 $\{x_1, \ldots, x_n\}$ 是 E/F 的一组基，$\{y_1, \ldots, y_n\}$ 是 K/E 的一组基, 那么根据线性代数的结果 $\{x_i y_j\}$ 是 K/F 的一组基. 如果 $A \in M_{n\times n}(F)$ 是 m_α 在 E/F 上对应的矩阵, 即

$$\alpha \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

那么则有

$$\alpha\begin{pmatrix} x_1y_1 \\ x_2y_1 \\ \vdots \\ x_ny_1 \\ x_1y_2 \\ \vdots \\ x_ny_2 \\ \vdots \\ x_ny_m \end{pmatrix} = \begin{pmatrix} A & & & \\ & A & & \\ & & \ddots & \\ & & & A \end{pmatrix} \begin{pmatrix} x_1y_1 \\ x_2y_1 \\ \vdots \\ x_ny_1 \\ x_1y_2 \\ \vdots \\ x_ny_2 \\ \vdots \\ x_ny_m \end{pmatrix}$$

从而有 $\mathrm{N}_{K/F}(\alpha) = \det(A)^m = N_{E/F}(\alpha)^{[K:E]}$ 以及 $\mathrm{Tr}_{K/F}(\alpha) = m\,\mathrm{Tr}_{E/F}(\alpha) = [K:E]\,\mathrm{Tr}_{E/F}(\alpha)$. □

注记. 实际上, 上述引理是如下传递性的特殊情况.

$$\mathrm{N}_{K/F} = \mathrm{N}_{K/E} \circ \mathrm{N}_{E/F}$$
$$\mathrm{Tr}_{K/F} = \mathrm{Tr}_{K/E} \circ \mathrm{Tr}_{E/F}$$

引理 4.1.3. *如果 $E = F(\alpha)$, α 在 F 上的极小多项式为 $P(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, 则*

$$\mathrm{N}_{E/F}(\alpha) = (-1)^n a_0$$
$$\mathrm{Tr}_{E/F}(\alpha) = -a_{n-1}$$

证明: 选取基 $\{1, \alpha, \ldots, \alpha^{n-1}\}$ 即可. □

命题 4.1.4. *如果 E/F 是有限扩张, 任取 $\alpha \in K$, 则*

$$\mathrm{N}_{E/F}(\alpha) = \prod_{\sigma \in \mathrm{Hom}_F(E,\bar{F})} \sigma(\alpha)^{[E:F]_i}$$
$$\mathrm{Tr}_{E/F}(\alpha) = [E:F]_i \sum_{\sigma \in \mathrm{Hom}_F(E,\bar{F})} \sigma(\alpha)$$

其中 $[K:F]_i$ 为扩张的纯不可分次数[1].

证明: 下面只对范数证明, 迹的证明是类似的: 任取 $\alpha \in E$, 考虑域扩张 $F \subseteq F(\alpha) \subseteq E$, 根据引理4.1.2有:

$$\mathrm{N}_{E/F}(\alpha) = \mathrm{N}_{F(\alpha)/F}(\alpha)^{[E:F(\alpha)]}$$

而考虑满射:

$$\mathrm{Hom}_F(E,\bar{F}) \twoheadrightarrow \mathrm{Hom}_F(F(\alpha),\bar{F})$$

其每个纤维都包含 $[E:F(\alpha)]$ 个元素: 这是因为 $\mathrm{Hom}_F(E,\bar{F}) = \mathrm{Hom}_F(E_s,\bar{F})$ 中恰有 $[E:F]_s$ 个元素, $\mathrm{Hom}_F(F(\alpha),\bar{F}) = \mathrm{Hom}_F(F(\alpha)_s,\bar{F})$ 中恰有 $[F(\alpha):F]_s$ 个元素. 因此:

$$\Big(\prod_{\sigma \in \mathrm{Hom}_F(K,\bar{F})} \sigma(\alpha)\Big)^{[K:F]_i} = \prod_{\mathrm{Hom}_F(F(\alpha),\bar{F})} \sigma(\alpha)^{[K:F(\alpha)]_s[K:F]_i}$$

[1] 见定义1.3.19.

由于 $[K:F(\alpha)]=[K:F(\alpha)]_i[K:F(\alpha)]_s$, 因此只需要证明:

$$N_{F(\alpha)/F}(\alpha)=\prod_{\mathrm{Hom}_F(F(\alpha),\bar{F})}\sigma(\alpha)^{[F(\alpha):F]_i}$$

即单扩张的情形, 而根据引理4.1.3直接可以得到想要的结果. □

推论 4.1.5. *E/F 是有限扩张, 则 E/F 可分当且仅当 $\mathrm{Tr}_{E/F}$ 是满射, 这也当且仅当 $\mathrm{Tr}_{E/F}$ 是非零映射.*

证明: 根据线性代数的知识, $\mathrm{Tr}_{E/F}$ 非零当且仅当其为满射是显然的. 如果 E/F 不可分, 假设 $\mathrm{char}\,F=p$, 则根据命题4.1.4可知 $\mathrm{Tr}_{E/F}(\alpha)$ 中含有 $[K:F]_i$ 作为因子, 然而其为 p 的幂次, 因此 $\mathrm{Tr}_{E/F}(\alpha)$ 恒为零映射. 另一方面, 如果 E/F 是可分的, 需要证明 $Tr_{E/F}$ 不是零映射, 这只需要寻找 α 使得:

$$\sum_{\sigma\in\mathrm{Hom}_F(E,\bar{F})}\sigma(\alpha)\neq 0$$

□

命题 4.1.6. *E/F 是有限域上的有限扩张, 则 $\mathrm{N}_{E/F},\mathrm{Tr}_{E/F}$ 都是满射.*

证明: 不妨记 $E=\mathbb{F}_{q^d},F=\mathbb{F}_q$. 根据推论4.1.5可知 $\mathrm{Tr}_{E/F}$ 是满射, 因为有限域上的扩张都是可分的. 另一方面, 注意到 $\mathrm{N}_{E/F}$ 是可乘的, 并且 $E^\times$ 是循环群, 因此我们只需要考虑 $\mathrm{N}_{E/F}$ 在 x 上的取值即可:

$$\mathrm{N}_{E/F}(x)=\prod_{\sigma\in\mathrm{Gal}(E/F)}\sigma(x)=x\cdot x^q\cdot\cdots\cdot x^{q^{d-1}}=x^{\frac{q^d-1}{q-1}}:=a\in\mathbb{F}_q^\times$$

并且 a 的阶为 $q-1$, 而注意到 $\mathbb{F}_q^\times$ 是一个 $q-1$ 阶循环群, 因此 a 是其一个生成元, 因此 $\mathrm{N}_{K/F}$ 也是满射. □

注记. 希尔伯特 90 问题断言: 如果 $\mathrm{Gal}(E/F)=\langle\sigma\rangle$ 是一个循环群, $\alpha\in E$ 满足其范数为 1, 则 $\alpha=\dfrac{\sigma(\beta)}{\beta}$, 对于某个 $\beta\in E^\times$ 成立. 对于有限域来说, 这个命题的答案可以显式的构造出来: 不妨沿用命题4.1.6中的记号, 如果 $\alpha=x^k$ 满足范数为 1, 则由于可乘性:

$$\mathrm{N}_{E/F}(\alpha)=\mathrm{N}_{E/F}(x)^k=a^k=1$$

因此 $q-1\mid k$, 不妨记作 $k=(q-1)r$, 则

$$\alpha=x^{(q-1)r}=\frac{x^{qr}}{x^r}=\frac{\sigma(x^r)}{x^r}$$

4.2 Galois 上同调

定义 4.2.1. G 是一个有限群, 一个 G **模** (module)是指一个阿贝尔群 A 以及一个 G 作用 $\mu:G\times A\to A$ 满足:

1. $1\cdot a=a$
2. $gg'\cdot a=g\cdot(g'\cdot a)$

3. $g\cdot(a+a')=g\cdot a+g\cdot a'$

并且 G 模之间的**态射** (morphism)为是满足 $f(ga)=gf(a), g\in G, a\in A$ 的群同态.

注记. 模论中的结果告诉我们阿贝尔群可以与 $\mathbb{Z}$ 模等同起来，则上述定义的 G 模可以与 $\mathbb{Z}[G]$ 模等同起来，其中 $\mathbb{Z}[G]=\{\sum_{g\in G}a_g g \mid a_g\in\mathbb{Z}\}$ 是 G 的群代数。

注记. 在上述定义中我们为了叙述方便假设 G 是乘法群, A 是加法群, 这并不关键, 之后可能会根据情况需要而调整, 请读者留心.

例子. *E/F 是有限 Galois 扩张, 令 $G=\mathrm{Gal}(E/F)$, 则 $G\curvearrowright(E,+), G\curvearrowright(E^\times,\times)$ 都是 G 模.*

定义 4.2.2. 给定有限群 G 和群 A, 定义

$$C^n(G,A)=\begin{cases}A & n=0\\ \{f:G^n\to A\} & n\geq 1\end{cases}$$

并且定义 $\mathrm{d}^n: C^n(G,A)\to C^{n+1}(G,A)$ 如下:

$$\begin{cases}\mathrm{d}^0 a(g)=ga-a\\ \mathrm{d}^n f(g_1,\dots,g_{n+1})=g_1 f(g_2,\dots,g_{n+1})+\sum_{i=1}^n(-1)^i f(g_1,\dots,g_ig_{i+1},\dots,g_{n+1})+(-1)^{n+1}f(g_1,\dots,g_n)\end{cases}$$

可以验证, (C,d) 构成了一个链复形, 定义上**群的上同调** (group cohomology)[2]为:

$$H^n(G,A)=\frac{\ker\mathrm{d}^n}{\mathrm{im}\,\mathrm{d}^{n-1}}$$

例子. *当 $n=0$ 时, $H^0(G,A)=\ker\mathrm{d}^0$. 若 $a\in\ker\mathrm{d}^0$, 当且仅当对任意的 $g\in G$, 有 $ga-a=0$, 当且仅当 $a\in A^G$, 即:*

$$H^0(G,A)=A^G$$

这实际上与一般的导出函子是一致的, 零阶导出函子就是其自身.

例子. *当 $n=1$ 时:*

$$\mathrm{d}^1 f(g_1,g_2)=g_1f(g_2)-f(g_1g_2)+f(g_2)$$

因此:

$$\ker\mathrm{d}^1=\{f:G\to A\mid f(g_1g_2)=f(g_1)+g_1f(g_2)\}$$

*满足上述条件的函数也被称为**交错同态** (crossed homomorphism). 特别地, 当 A 是一个平凡 G 模时, 一个交错同态就是群同态. 而*

$$\mathrm{im}\,\mathrm{d}^0=\{f:G\to A\mid \text{存在 } a\in A \text{ 使得} f(g)=ga-a\}$$

注记. 如果 $f:G\to A$ 是一个交错同态, 则有下面的观察:

(1)

$$f(1)=f(1)+1\cdot f(1)=2f(1)\implies f(1)=0$$

即 f 将 G 中的单位元映成 A 中的单位元.

[2]在同调代数中, 函子 $A\to A^G=\{a\in A\mid ga=a\}$ 是左正合函子, 则 $H^n(G,A)$ 被定义为这个函子的右导出函子.

(2)

$$f(g^2) = f(g) + g \cdot f(g) = (1+g) \cdot f(g)$$

归纳地可以得到:

$$f(g^n) = (1 + g + \cdots + g^{n-1}) f(g)$$

假设 G 是一个 n 阶循环群, 生成元为 g, 则

$$0 = f(1) = f(g^n) = (1 + g + \cdots + g^{n-1}) f(g)$$

反之, 如果 $x \in A$ 满足 $(1+g+\cdots+g^{n-1})x = 0$, 则 $f(g) := x$ 定义了交错同态 $f : G \to A$.

定理 4.2.3 (Hilbert 90)**.** *E/F 是有限 Galois 扩张, 则*

$$H^1(\mathrm{Gal}(E/F), E^\times) = 0$$
$$H^1(\mathrm{Gal}(E/F), E^+) = 0$$

前者称为乘法版本, 后者称为加法版本.

证明: 我们先来证明乘法版本: 令 $f : G \to E^\times$ 是交错同态, 那么任取 $\tau \in G, f(\tau) \neq 0$, 根据引理2.1.6可知 $\sum_{\tau\in G} f(\tau)\tau$ 是非零的, 即存在 $a \in E^\times$ 使得

$$\beta = \sum_{\tau\in G} f(\tau)\tau(a) \neq 0$$

因此

$$\begin{aligned}\sigma(\beta) &= \sum_{\tau\in G} \sigma f(\tau)(\sigma\tau)(\gamma) \\ &= \sum_{\tau\in G} f^{-1}(\sigma) f(\sigma\tau)(\sigma\tau)(\gamma) \\ &= f^{-1}(\sigma)\beta\end{aligned}$$

即 $f(\sigma) = \beta/\sigma(\beta)$. 令 $x = \beta^{=1}$, 则 $f(\sigma) = \sigma(x)/x$, 即任何交错同态都落在 $\mathrm{im}\,\mathrm{d}^0$ 中, 即上同调群平凡.

现在来证明加法版本: 令 $f : G \to E$ 是交错同态, 不妨假设 $f \neq 0$, 那么任取 $\tau \in G, f(\tau)$ 不全为零, 同样根据引理2.1.6有 $a \in E$ 使得

$$\beta = \sum_{\tau\in G} f(\tau)\tau(a) \neq 0$$

另外, 我们取 $b \in E^\times$ 满足 $\mathrm{Tr}_{E/F}(b) \neq 0$, 并且根据推论4.1.5, 这样的 b 是存在的. 令 $\mu = \sum_{\tau\in G} f(\tau)\tau$, 如果 $\mu(a+b) = 0$, 那么 $\mu(b) = -\mu(a) \neq 0$; 如果 $\mathrm{Tr}_{E/F}(a+b) = 0$, 那么 $\mathrm{Tr}_{E/F}(a) \neq 0$; 如果 $\mu(a+b) \neq 0$ 并且 $\mathrm{Tr}_{E/F}(a+b) \neq 0$, 那么我们用 $\mu(a+b)$ 代替 β. 如上分

析说明我们总可以找到 $a \in E^\times, \mu(a) \neq 0$ 并且 $\mathrm{Tr}_{E/F}(a) \neq 0$, 令 $\beta = \mu(a)$, 那么

$$\begin{aligned}\sigma(\beta) &= \sum_{\tau\in G} \sigma(f(\tau)\tau(a)) \\ &= \sum_{\tau\in G} \sigma(f(\tau))\sigma\tau(a) \\ &= \sum_{\tau\in G} (f(\sigma\tau) - f(\sigma))\sigma\tau(a) \\ &= \beta - f(\sigma)\sum_{\tau\in G} \sigma\tau(a) \\ &= \beta - f(\sigma)\,\mathrm{Tr}_{E/F}(a)\end{aligned}$$

则 $f(\sigma) = \mathrm{Tr}_{E/F}(a)^{-1}(\beta - \sigma(\beta))$, 取 $x = \frac{-\beta}{\mathrm{Tr}_{E/F}(a)}$, 则有 $f(\sigma) = \sigma(x) - x$. □

定理 4.2.4 (Hilbert 90)**.** *E/F 是有限 Galois 扩张, 并且 $G = \mathrm{Gal}(E/F) = \langle\sigma\rangle$ 是 n 阶循环群, 则*

(1) *如果 $\alpha \in E^\times$ 满足范数为 1, 则 $\alpha = \frac{\sigma(\beta)}{\beta}, \beta \in E^\times$.*

(2) *如果 $\alpha \in E$ 满足迹为 0, 则 $\alpha = \sigma(\beta) - \beta, \beta \in E$.*

证明: 由于 (1) 和 (2) 的证明几乎完全一致, 在这里我们给出 (2) 的证明: 如果 $\alpha \in E$ 满足迹为零, 则

$$0 = \mathrm{Tr}_{K/F}(\alpha) = \sum_{\tau\in G} \tau\alpha = \sum_{i=0}^{n-1} \sigma^i\alpha$$

考虑 $f : G \to K$, 定义为 $\sigma^i \mapsto (1 + \sigma + \cdots + \sigma^{i-1})x$, 可以直接验证[3]其为一个是一个交错同态. 根据定理4.2.3可知存在 $\beta \in E$ 使得 $f(\sigma^k) = \sigma^k(\beta) - \beta$ 对任意的 $0 \leq k \leq n-1$ 成立. 特别地, $\alpha = f(\sigma) = \sigma(\beta) - \beta$. □

推论 4.2.5. *令 $a, b \in \mathbb{Q}$, 满足 $a^2 + b^2 = 1$, 则存在 $c, d \in \mathbb{Z}$ 使得*

$$a = \frac{c^2 - d^2}{c^2 - d^2}, \quad b = \frac{-2cd}{c^2 + d^2}$$

证明: 考虑 $\mathbb{Q}(i)/\mathbb{Q}$, 取 $a + bi \in \mathbb{Q}(i)$ 满足范数为 1, 则存在 $c + di$ 使得:

$$a + bi = \frac{c - di}{c + di}$$

实部虚部对应即可. □

4.2.1 高阶上同调

定义 4.2.6. $H < G$ 是子群, A 是 H 模, 则定义**诱导模** (induced module)如下:

$$\mathrm{Ind}_H^G A = \mathrm{Hom}_{\mathbb{Z}[H]}(\mathbb{Z}[G], A)$$

定理 4.2.7 (Shapiro)**.**

$$H^n(G, \mathrm{Ind}_H^G A) \cong H^n(H, A)$$

[3]这里用到了 α 的迹为零这个条件.

定理 4.2.8 (正规基定理). *K/F 是有限 Galois 扩张, 则存在 K/F 的一族正规基, 即存在 $\alpha \in K^\times$, 使得 $\{\sigma\alpha \mid \alpha \in G\}$ 构成了 K/F 的一族基.*

推论 4.2.9. *作为 G 模, 有同构:*

$$(K, +) \cong \mathrm{Ind}_{\{1\}}^{G} F$$

定理 4.2.10. *K/F 是有限 Galois 扩张, 则 $H^n(\mathrm{Gal}(K/F), K^+) = 0, n \geq 1$.*

证明:

$$H^n(\mathrm{Gal}(K/F), K^+) = H^n(\{1\}, F) = 0$$

□

注记. 一般来说, $H^2(\mathrm{Gal}(K/F), K^\times) \neq 0$. 有如下结果: $H^2(\mathrm{Gal}(F^{sep}/F), F^{sep})$ 可以建立起与 F 上的中心单代数的等价类的一一对应.

4.2.2 连续上同调

在本节中, G 是一个射有限群.

定义 4.2.11. *A 被称为**离散 G 模*** (discrete G-module), 如果满足下列等价条件中的某一条:

1. $A = \bigcup A^U$, 其中 U 跑遍 G 的所有开的正规子群.
2. $G \times A \to A$ 是连续的 (A 上赋予离散拓扑) .

例子. *K/F 是 Galois 扩张, $\mathrm{Gal}(K/F) \curvearrowright K$ 是离散模. 这是因为任取 $a \in K$, 存在 E/F 是有限 Galois 扩张, 使得 $a \in E$, 并且 $\mathrm{Gal}(K/E)$ 是固定 a 的 $\mathrm{Gal}(K/F)$ 的开集.*

引理 4.2.12. *A 是一个离散 G 模, 则*

$$C^n_{cont}(G, A) = \{f : G^n \to A \mid f \text{ 连续}\} = \varinjlim_{U \lhd G} C^n_{cont}(G/U, A)$$

证明: □

定义 4.2.13. 将定义4.2.2中的 $C^n(G, A)$ 换成 $C^n_{cont}(G, A)$, 则可以定义**连续上同调** (continous cohomology)$H^n_{cont}(G, A)$.

命题 4.2.14. *A 是离散 G 模, 则*

$$H^n_{cont}(G, A) = \varinjlim_{U \lhd G} H^n(G/U, A^U)$$

定理 4.2.15. *K/F 是 Galois 扩张, 则*

$$H^1(\mathrm{Gal}(K/F), K^\times) = 0$$

$$H^n(\mathrm{Gal}(K/F), K^+) = 0, \quad n \geq 1$$

4.3 Kummer 理论

在本节中[4], 域 F 总是满足如下两条假设:

(1) 包含 n 次本原单位根, 从而包含所有的 n 次单位根, 我们用 μ_n 记全体 n 次单位根组成的群.

(2) x^n-1 在 F 中有 n 个不同的根.

引理 4.3.1. *令 $a\in F^\times$, m 是 a 在 $F^\times/(F^\times)^n$ 中的阶数, 那么 x^n-a 的每个不可约因子都是 $x^m-b, b\in F$ 的形式.*

证明: 即证明, 如果 α 是 $P(x)=x^n-a$ 在 $\bar{F}$ 中的根, 则其极小多项式为 $x^m-b, b\in F$ 的形式: 首先, 由于 $a^m\in(F^\times)^n$, 因此存在 $b\in F^\times$, 使得 $a^m=b^n$, 而 $\alpha^n=a$, 因此 $\alpha^{nm}=b^n$, 因此 $(\alpha^m/b)^n=1\implies \alpha^m/b\in\mu_n$, 因此 $\alpha^m\in F^\times$, 因此 α 的极小多项式 $Q(x)\mid x^m-b$, 下面只需要证明 $\deg Q(x)=m$ 即可:

由于 $P(x)=\prod_{i=0}^{n-1}(x-\alpha\xi_n^i)$, 因此 $Q(x)=\prod_{i\in S}(x-\alpha\xi_n^i), |S|=\deg Q(x)$. 将 $Q(x)$ 展开, 考虑其常数项则有 $\alpha^{\deg q(x)}\xi_n^i\in F\implies \alpha^{\deg q(x)}\in F$, 不妨用 d 记 $\deg Q(x)$, 因此:

$$a^d=(\alpha^n)^d=(\alpha^d)^n\in(F^\times)^n$$

因此 $m\mid d$, 因此 $m=d$ □

命题 4.3.2. *$E=F(\alpha)$, 其中 $\alpha^n=a\in F^\times$, 则 E/F 是一个次数为 m 的循环 Galois 扩张, 其中 m 是 a 在 $F^\times/(F^\times)^n$ 中的阶数.*

证明: 首先引理4.3.1可知 E/F 的扩张次数就是 m. 由于 x^n-a 的所有根是 $\{\alpha\xi_n^i\mid 0\le i\le n-1\}$ 是不同的, 进而 α 的极小多项式也没有重根, 从而 α 是 F 上的可分元, 根据命题1.3.12可知 E/F 是可分扩张; 并且由于 E 是 x^n-a 的分裂域, 从而根据定理1.3.2可知 E 是正规扩张, 从而 E/F 是 Galois 扩张. 最后我们来证明其为循环扩张: 考虑映射

$$\begin{aligned}\varphi:\mathrm{Gal}(E/F)&\to\mu_n\\ \sigma&\mapsto\frac{\sigma(\alpha)}{\alpha}\end{aligned}$$

这定义了一个群同态, 因为:

$$\varphi(\sigma\tau)=\frac{\sigma\tau(\alpha)}{\alpha}=\frac{\sigma\varphi(\tau)}{\alpha}=\varphi(\tau)\frac{\sigma(\alpha)}{\alpha}=\varphi(\sigma)\varphi(\tau)$$

并且这是个嵌入, 因为如果 $\varphi(\sigma)=1$, 即 $\sigma(\alpha)=\alpha$, 这意味着 σ 固定 E, 从而根据定理2.2.1可知 $\sigma=\mathrm{id}$. 因此 $\mathrm{Gal}(E/F)$ 嵌入到循环群 μ_n 中, 也是一个循环群. □

Kummer 理论, 实际上给出了上述命题的逆命题.

定理 4.3.3. *E/F 是有限 Galois 扩张, 其 Galois 群为 n 阶循环群 $\langle\sigma\rangle$, 则 $E=F(\alpha), \alpha^n\in F^\times$.*

[4]对于一般的域也有 Kummer 理论, 但为了方便起见, 我们在这种域上考虑.

证明: 取 ξ_n 是一个 n 次本原单位根, 则

$$\mathrm{N}_{K/F}(\xi_n) = \xi_n^{[K:F]} = 1$$

因此根据定理4.2.4, 即希尔伯特 90 可知存在 $\alpha \in E^\times$, 使得 $\xi_n = \frac{\alpha(\sigma)}{\alpha}$, 因此:

$$\sigma(\alpha^n) = \xi_n^n \alpha^n = \alpha^n$$

因此 $\alpha^n \in F^\times$. 下面说明 $E = F(\alpha)$, 我们断言 $\mathrm{Gal}(E/F(\alpha)) = \{\mathrm{id}\}$: 如果存在 $\tau = \sigma^i \in \mathrm{Gal}(E/F(\alpha))$, 则 $\tau(\alpha) = \sigma^i(\alpha) = \xi_n^i \alpha$, 那么 $\xi_n^i = 1$, 而 ξ_n 是本原单位根, 因此 $i = n$, 因此 $\tau = \mathrm{id}$. □

推论 4.3.4. *我们有如下的一一对应:*

$$\{F \text{ 的 } \mathbb{Z}/n\mathbb{Z} \text{ 扩张}[5]\} \Longleftrightarrow \{a \in F^\times/(F^\times)^n, \text{其中 } a \text{ 的阶数为 } n\}$$

证明: 命题4.3.2给出了对应 $\Leftarrow$, 定理 4.3.3 说明这个方向的对应是满射. 假设 $F(\alpha) = F(\beta)$ 是 F 的 $\mathbb{Z}/n\mathbb{Z}$ 扩张, 其中 $\alpha^n = a \in F^\times, \beta^n = b \in F^\times$, 根据命题4.3.2的证明过程, 我们可以定义映射

$$\varphi_\alpha(\sigma) = \frac{\sigma(\alpha)}{\alpha}$$
$$\varphi_\beta(\sigma) = \frac{\sigma(\beta)}{\beta}$$

并且由于 $\mathrm{im}\,\varphi_\alpha = \mathrm{im}\,\varphi_\beta = \mu_n$ 可知 $\frac{\sigma(\alpha)}{\alpha}, \frac{\sigma(\beta)}{\beta}$ 都是 n 次本元单位根, 因此存在整数 k 满足 $(k, n) = 1$ 使得

$$\frac{\sigma(\alpha)}{\alpha} = (\frac{\sigma(\beta)}{\beta})^k$$

即 $\sigma(\alpha\beta^{-k}) = \alpha\beta^{-k}$, 这意味着 $\alpha\beta^{-k} \in F^\times$, 并且注意到 $ab^{-k} = (ab^{-k})^n \in (F^\times)^n$, 从而在 $F^\times/(F^\times)^n$ 中 $a = b^k$, 并且由于 $(k, n) = 1$ 可知 a, b 的阶数相同. □

定义 4.3.5. 扩张 E/F 被称为 **Kummer 扩张** (Kummer extension), 如果其为一个阿贝尔扩张, 并且其 Galois 群 $\mathrm{Gal}(E/F)$ 的指数[6]整除 n.

定理 4.3.6. *E/F 是 Kummer 扩张, 当且仅当 $E = F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r}), a_i \in F^\times$.*

证明: 一方面, $F(\sqrt[n]{a_1}, \ldots, \sqrt[n]{a_r})$ 是 $F(\sqrt[n]{a_i})$ 的复合, 因此:

$$\mathrm{Gal}(K/F) \hookrightarrow \prod_i \mathrm{Gal}(F(\sqrt[n]{a_i})/F)$$

是一个指数整除 n 的阿贝尔群. 另一方面, 考虑阿贝尔群的分解:

$$\mathrm{Gal}(E/F) \cong C_1 \times \cdots \times C_r$$

其中 C_r 是阶数乘除 n 的循环群, 令 $H_i = \prod_{j \neq i} H_j \times \{1\}$, 令 $K_j = K^{H_j}$, 那么 $\mathrm{Gal}(K_j/F) \cong C_i$, 因此 $K_j = F(\sqrt[n]{a_i})$, 下面只需要说明 $K = K_1 \ldots K_r$ 即可, 下面以一个引理的形式证明, 因为这对一般情况来说也是正确的. □

[6]exponent, 指群中所有元素阶的最小公倍数.

引理 4.3.7. *K/F 是有限 Galois 扩张, 其 Galois 群为 $G = G_1 \times \cdots \times G_r$, 则 $K = K_1 \dots K_r$, 其中 $K_j = K^{H_j}, H_j = \prod_{i \neq j} G_i \times \{1\}$*

证明: 根据归纳法, 只需要证明 $r = 2$ 的情况即可: 如果 $K_1/F, K_2/F$ 都是 Galois 扩张, 则 $[K_1K_2 : K_2] = [K_1 : K_1 \cap K_2]$, 而这里 $K_1 \cap K_2 = F$, 因此 $[K_1K_2 : F] = [K_1 : F][K_2 : F] = |H_1||H_2| = |G|$, 因此 $K = F_1F_2$. □

附录 A　拓扑

A.1　拓扑群回顾

定义 A.1.1. 其上带有拓扑的一个群 G 被称为**拓扑群** (topological group), 如果乘法运算 $G \times G \to G$ 和取逆运算 $G \to G$ 是连续函数.

例子. $(\mathbb{R}, +)$ 构成了一个拓扑群.

例子. 有限群上赋予离散拓扑, 构成了一个拓扑群.

命题 A.1.2. 左乘运算 $L_a : G \to G, L_a(g) = ag$ 定义了 $G \to G$ 的一个同胚.

证明: 考虑:

$$\begin{array}{ccccc} G & \hookrightarrow & G \times G & \longrightarrow & G \\ g & \mapsto & (a, g) & \mapsto & ag \end{array}$$

可知 L_a 作为连续函数的复合也是连续的. 同理, $L_{a^{-1}}$ 也是连续的, 并且 $L_a, L_{a^{-1}}$ 彼此互逆. 因此 L_a 是 $G \to G$ 的一个同胚. □

注记. 因此拓扑群有一种非常好的“齐性”: 其任意一处的局部的性质, 都可以通过在单位元 1 处的性质反应.

推论 A.1.3. 如果 $\mathcal{N}$ 是 $1 \in G$ 的一个邻域, 则 $a\mathcal{N}$ 是 $a \in G$ 的一个邻域.

引理 A.1.4. G 是拓扑群, $H < G$ 是其子群, 则

(1) H 上带有子空间拓扑, 构成了一个拓扑群.

(2) H 的闭包 $\bar{H}$ 也是 G 的子群, 并且如果 $H \triangleleft G$, 则 $\bar{H} \triangleleft G$

(3) G 是 *Hausdorff* 的当且仅当 $\{1\}$ 是闭集.

证明: (1). 显然.

(2). 首先验证乘法: 任取 $h_1, h_2 \in \bar{H}$, 取 U 使得 $h = h_1 h_2 \in U$, 根据乘法连续的定义, 存在 $h_1 \in V_1, h_2 \in V_2$ 满足 $V_1 V_2 \subseteq U$, 而 $V_1 \cap H \neq \varnothing, V_2 \cap H \neq \varnothing$, 因此 $V_1 V_2 \cap H \neq \varnothing$, 即 $h_1 h_2 \in \bar{H}$; 取逆运算同理验证. 并且注意到 $\bar{H}$ 是包含 H 的最小闭集, 而 $g\bar{H}g^{-1}$ 也是包含 H 的闭集, 因此 $\bar{H} \subseteq g\bar{H}g^{-1}$, 进而有两者相同.

(3). Hausdorff 空间的所有单点集都是闭的, 因此一方面是显然的. 另一方面, 任取 $g \neq h \in G$, 则 $\{g^{-1}h\}$ 是闭集, 取开集 $1 \in U \subseteq G \backslash \{g^{-1}h\}$, 并且考虑连续映射

$$\begin{aligned} G \times G &\to G \\ (g, h) &\mapsto gh^{-1} \end{aligned}$$

则存在 1 的邻域 V,W, 使得 $VW^{-1}\subseteq U$, 因此 $g^{-1}h\notin VW^{-1}$, 因此 $gV\cap hW=\varnothing$, 即 G 是 Hausdorff 的. □

引理 A.1.5. *G 是拓扑群, $H<G$ 是其子群, 则*

(1) *如果 H 是开集, 则 H 是闭集.*

(2) *如果 H 是指数有限的闭集, 则 H 是开集.*

(3) *如果 G 是紧群, 则闭 + 指数有限等价于开.*

证明: (1). 用 S 记 G/H 代表元组成的集合, 则

$$G=\coprod_{\sigma\in S}\sigma H$$

因此如果 H 是开集, 则 σH 也是开集, 则

$$G\backslash H=\coprod_{\substack{\sigma\neq 1\\ \sigma\in S}}\sigma H$$

是开集, 因此 H 是闭集.

(2). 由于 H 指数有限, 因此 S 是有限集, 有限个闭集的并仍然是闭集, 因此根据 (1) 的论断可知 H 是开集.

(3). 由于 G 是紧群, 则 $G=\coprod_{\sigma\in S}\sigma H$ 这个开覆盖一定存在一个有限子覆盖, 但是对于不同的 σ, σH 之间没有交集, 因此 S 是有限集, 即紧群的开子群的指数一定有限. □

附录 B 代数

B.1 逆极限与射有限群

定义 B.1.1. $\{G_i\}_{i\in I}$ 是一族群, I 是一个正向集[1], 以及任取 $i,j\in I, i\le j$, 存在群同态 $P_{ij}: G_j\to G_i$, 满足 $P_{ij}\circ P_{jk}=P_{ik}$, **逆极限** (inverse limit)定义如下:

$$\varprojlim_{i\in I} G_i=\{(g_i)_{i\in I}\in\prod_{i\in I}G_i\mid P_{ij}(g_j)=g_i,\forall i\le j\}$$

例子. 令 $I=\mathbb{N}$, 以及 $G_i=\mathbb{Z}/p^i\mathbb{Z}$, P_{ij} 是自然的商映射, 则

$$\varprojlim_{i\in I} G_i\mathbb{Z}/p^i\mathbb{Z}=\{(x_i)_{i\in I}\mid x_i\equiv x_{i-1}\pmod{p^{i-1}}\}$$

即如果 $x_i=a_0+a_1p+\cdots+a_{i-2}p^{i-2}+a_{i-1}p^{i-1}$, 则 $x_{i-1}=a_0+a_1x+\cdots+a_{i-2}p^{i-2}$, 因此这个逆极限也通常写成如下的形式:

$$\varprojlim_{i\in I}\mathbb{Z}/p^i\mathbb{Z}\cong\{\sum_{i\ge0}a_ip^i,\quad 0\le a_i\le p-1\}$$

称作 p-adic 数, 通常也记作 $\mathbb{Z}_p$

定义 B.1.2. 一族带有离散拓扑的有限群的逆极限被称为**射有限群** (profinite group)

引理 B.1.3. 射有限群是紧的, Hausdorff, 以及完全不连通的[2].

证明: (1). 根据 Tychonoff 定理, 我们只需要证明 $\varprojlim G_i$ 在 $\prod_{i\in I}$ 中是闭集即可, 任取 $\{g_i\}_{i\in I}\notin\varprojlim G_i$, 存在 $i\le j$, 使得 $P_{ij}(g_j)\ne g_i$, 选择开邻域:

$$U=\prod_{k\ne i,j}G_k\times\{g_i\}\times\{g_j\}\subseteq\prod_{i\in I}G_i$$

因此 $U\cap\varprojlim G_i=\varnothing$, 因此 $\prod_{i\in I}G_i\backslash\varprojlim G_i$ 是开集.

(2). 只需要证明单点集 $\{(e_i)_{i\in I}\}$ 是闭集, 考虑如下开子群邻域:

$$U_i=\prod_{i\ne j}G_i\times\{e_i\}\subseteq\prod_i G_i$$

[1]即 I 是一个偏序集, 并且任取 $i,j\in I$, 存在 $k\in I$ 使得 $i,j\le k$

[2]空间 X 是完全不连通的, 如果任取 $x\in X$, 其连通分支就是单点 x, 即所有包含 x 的既开又闭的集合的交就是单点 x.

对于拓扑群来说, 每个开子群也是闭的. 考虑

$$\bigcap_{i\in I} U_i = \{(e_i)_{i\in I}\}$$

因此 $\{e_i\}_{i\in I}$ 是闭集.

(3). 由于拓扑群每点的性质都相同, 因此不妨选取 $x = \{(e_i)_{i\in I}\}$, 考虑 (2) 中的开邻域 U_i 即可. □

索引