

代数 2 H 课程讲义



Instructor: 余成龙
Notes Taker: 刘博文

Qiuuzhen College, Tsinghua University
2023 Spring

课程信息:

- ◇ 授课人: 余成龙.
- ◇ 办公室: 近春园西楼 260.
- ◇ 邮箱: yuchenglong@mail.tsinghua.edu.cn.
- ◇ 成绩分布: 作业 (20%) + 期中 (30%) + 期末 (50%).
- ◇ 参考书: M.Atiyah *Communicative algebra*, S.Lang *Algebra*.

内容大纲:

- ◇ 伽罗瓦理论.
- ◇ 同调代数.
- ◇ 交换代数.





目录

第一部分 伽罗瓦理论	3
第一章 域论回顾	4
1.1 域扩张	4
1.2 代数扩张	6
第二章 分裂域及其应用	8
2.1 分裂域	8
2.2 有限域	9
2.3 代数闭域与代数闭包	10
第三章 正规扩张与可分扩张	13
3.1 正规扩张	13
3.2 可分扩张	14
3.3 纯不可分扩张	17
第四章 伽罗瓦理论	19
4.1 伽罗瓦扩张	19
4.2 伽罗瓦对应	21
4.3 伽罗瓦群的计算	23
第五章 伽罗瓦理论的应用	28
5.1 尺规作图问题	28
5.2 代数基本定理的证明	30
5.3 根式可解问题	31
5.4 求根公式	35
5.5 Kummer 理论	37
5.6 正规基定理	40
第六章 伽罗瓦上同调与希尔伯特 90	41
6.1 范与迹	41
6.2 伽罗瓦上同调	43

第一部分

伽罗瓦理论



第一章 域论回顾

1.1 域扩张

在本课程中, 如不加特殊说明, 环 R 总是指含有单位元的交换环, 并且环同态是保持单位元的.

定义 1.1.1. 对于环 R , 总有环同态 $\rho: \mathbb{Z} \rightarrow R$, 如果记 $\ker \rho = (n)$, 那么 R 的**特征** (characteristic) 定义为 n , 记作 $\text{char } R$.

定义 1.1.2. 如果环 R 中任何非零元素都可逆, 那么环 R 被称为一个**域** (field).

命题 1.1.3. 域的特征是素数.

我们在学习环论时, 环的理想是一个非常重要的概念, 但是对域来说, 其只有平凡理想, 即只有零理想及自身. 这很大程度上限制了域之间的同态. 假设有非平凡的域同态 $\tau: E \rightarrow F$, 那么 τ 一定是单射, 从而我们可以将 E 视作包含在 F 中, 这引出了下面的概念.

定义 1.1.4. 给定域 E, F , 如果存在 (单) 同态 $\tau: F \rightarrow E$, 那么称 E 是域 F 的**扩张** (extension), 记作 E/F .

注记. 当我们用 (单) 同态 τ 表示域扩张 E/F 时, 我们不仅强调可以将 F 视作 E 的子域, 也强调映射 τ , 因为可能存在多种方式将 F 视作 E 的子域, 例如:

$$\begin{array}{ccc}
 \tau: \mathbb{R}[x]/(x^2 + 1) \rightarrow \mathbb{C} & & \tau': \mathbb{R}[x]/(x^2 + 1) \rightarrow \mathbb{C} \\
 x \mapsto \sqrt{-1} & & x \mapsto -\sqrt{-1}
 \end{array}$$

都给出了这样的映射.

定义 1.1.5. 给定域扩张 $\tau: F \rightarrow E, \tau': F \rightarrow E'$, **域扩张之间的态射** (morphism between field extension) 是指域之间的同态 $\varphi: E \rightarrow E'$, 使得如下的图交换

$$\begin{array}{ccc}
 & & E \\
 & \nearrow \tau & \downarrow \varphi \\
 F & \xrightarrow{\tau'} & E'
 \end{array}$$

记号 1.1.6. 给定域扩张 $E/F, E'/F$, 用 $\text{Hom}_F(E, E')$ 记域扩张之间的态射的全体.

定义 1.1.7. 给定域扩张 $E/F, E'/F$, 其被称为**同构的** (isomorphism), 如果两者间存在是同构的域扩张之间的态射.

定义 1.1.8. 给定域扩张 E/F , 扩张的**次数** (degree) 定义为 $[E : F] = \dim_F E$.

命题 1.1.9. 对于域扩张 $F \subseteq E \subseteq K$, 则 $[K : F] = [K : E][E : F]$.

定义 1.1.10. 一个域扩张被称为**有限的** (finite extension), 如果其扩张次数有限, 否则被称为**无限的** (infinite extension).

例子. \mathbb{C}/\mathbb{R} 是二次扩张, \mathbb{R}/\mathbb{Q} 是无穷扩张.

例子. $\mathbb{Q}(i) = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\}/\mathbb{Q}$ 是二次扩张.

定义 1.1.11. E/F 是域扩张, $S \subseteq K$ 是一个子集, 则 $F(S)$ 是 E 中包含 F, S 最小的子域. 特别地, 如果 $S = \{u\}$, $F(u)$ 叫做域 F 的一个**单扩张** (simple extension).

例子. 给定域 F , $F(u)$ 有如下的具体构造

$$F(u) = \left\{ \frac{f(u)}{g(u)} \mid f(x), g(x) \in F[x] \right\}$$

命题 1.1.12. 假设域 \mathbb{F} 的特征不为 2, 如果 E/F 是二次扩张, 那么 $E = F(\alpha)$, 其中 $\alpha^2 \in F$.

证明: 假设 $\{1, \beta\}$ 是 E 的一组 F -基, 那么 $\beta^2 = a + b\beta$, 其中 $a, b \in F$, 注意到

$$\left(\beta - \frac{1}{2}b\right)^2 = a + \frac{1}{4}b^2 \in F$$

那么 $\alpha = \beta - \frac{1}{2}b$ 即可. □

注记. 域的特征不为 2 用在了配方上, 这是一个不可缺少的条件.

问题 1.1.13. 特征 2 域上的二次扩张是什么样的?

研究域扩张的一个重要的好处就是可以帮助我们求解方程, 例如 $x^2 + 1 = 0$ 在 \mathbb{R} 上没有根, 但是我们可以在 \mathbb{R} 的域扩张 \mathbb{C} 中找到它的一个根, 实际上, 我们总可以通过域扩张的办法去寻找根.

命题 1.1.14. 给定域 F 以及多项式 $f(x) \in F[x]$, 存在域扩张 E/F 使得 $f(x)$ 在 E 中有根.

证明: 将 $f(x)$ 在 $F[x]$ 中写作不可约因子 $p_1(x) \dots p_k(x)$ 的乘积, 如果有一次因子, 那么 $f(x)$ 在 F 中就有根, 否则取某个不可约多项式 $p_1(x)$, 考虑

$$E = F[x]/(p_1(x))$$

那么 E/F 是一个域扩张, 并且 $f(x)$ 在 E 中有根 $x + (p_1(x))$. □

定义 1.1.15. 给定域扩张 $F \subseteq E \subseteq K$ 以及 $F \subseteq E' \subseteq K$, **域扩张的复合** (composition of field extension) 定义为 K 中包含 E, E' 的所有子域的交, 记作 EE' .

1.2 代数扩张

定义 1.2.1. 给定域扩张 E/F , $\alpha \in E$ 称为在 F 上**代数** (algebraic), 如果存在非零多项式 $p(x) \in F[x]$, 使得 $p(\alpha) = 0$, 否则则称 α 在 F 上**超越** (transcendental).

例子. $\sqrt{2}$ 在 \mathbb{Q} 上是代数元, e, π 在 \mathbb{R} 上是超越元.

定义 1.2.2. 给定域扩张 E/F , $\alpha \in E$ 在 F 上代数, $F[x]$ 中零化 α 的最低次数首一多项式被称为 α 的在 F 上的**极小多项式** (minimal polynomial), 记作 $P_{\alpha, F}$.

注记. 我们还可以如下刻画 α 是否在 F 上代数: 考虑赋值映射 $\theta_\alpha: F[x] \rightarrow F[\alpha]$, 则

1. α 在 F 上代数当且仅当 $\ker \theta_\alpha \neq 0$.
2. α 在 F 上超越当且仅当 $\ker \theta_\alpha = 0$, 即 θ_α 是一个同构.

命题 1.2.3. 给定域扩张 E/F , $\alpha \in E$ 在 F 上代数, 那么 $[F(\alpha) : F] = \deg P_{\alpha, F}(x)$.

证明: 注意到 $F(\alpha) \cong F[x]/(P_{\alpha, F}(x))$, 并且 $[F[x]/(P_{\alpha, F}(x)) : F] = \deg P_{\alpha, F}$. □

引理 1.2.4. 给定单扩张 $F(\alpha)/F$, 其中 α 在 F 上代数, 对于域扩张 E/F , 存在 F -嵌入 $\tau: F(\alpha) \hookrightarrow E$ 当且仅当 $P_{\alpha, F}$ 在 E 中有根.

证明: 假设 $p(x)$ 在 E 中有根 β , 那么考虑 F -映射

$$\begin{aligned} \varphi: F[x] &\rightarrow E \\ x &\mapsto \beta \end{aligned}$$

并且由于 $P_{\alpha, F}(\beta) = 0$, 从而 φ 给出了 $F[x]/(P_{\alpha, F}(x)) \cong F(\alpha)$ 到 E 的 F -嵌入. □

注记.

1. 上述引理还可以做如下的简单推广

引理 1.2.5. 给定单扩张 $F(\alpha)/F$, 其中 α 在 F 上代数. 考虑映射 $\varphi: F \rightarrow F'$ 以及域扩张 E/F' , 存在如下的交换图当且仅当 $\varphi(P_{\alpha, F}(x))$ 在 E 中有根.

$$\begin{array}{ccc} F(\alpha) & \xrightarrow{\tau} & E \\ \uparrow & & \uparrow \\ F & \xrightarrow{\varphi} & F' \end{array}$$

不难发现之前是取 $\varphi: F \rightarrow F$ 为恒等的情况.

2. 从证明中我们还可以看出, $P_{\alpha, F}(x)$ 在 E 中的不同的根给出了不同的 F -嵌入, 因此嵌入的个数小于等于 $\deg P_{\alpha, F}(x)$.

定义 1.2.6. 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, 否则称为**超越扩张** (transcendental extension).

例子. \mathbb{C}/\mathbb{R} 是代数扩张.

命题 1.2.7. 有限扩张是代数扩张.

证明: 假设 E/F 是有限扩张, 任取 $\alpha \in E$, 考虑 $1, \alpha, \alpha^2, \dots$, 由于 E/F 是有限扩张, 则存在足够大的 n 使得

$$\alpha^{n+1} = a_n \alpha^n + \dots + a_1 \alpha + a_0$$

从而 $\alpha \in E$ 在 F 上代数, 即 E/F 是代数扩张. □

注记. 反之并不成立, 即代数扩张不一定是有限扩张.

推论 1.2.8. 给定域扩张 E/F , E 中所有在 F 上代数的元素组成了 E 的一个子域.

证明: 即证明, 如果 $\alpha, \beta \in E$ 都在 F 上代数, 则 $\alpha \pm \beta, \alpha\beta, \alpha/\beta (\beta \neq 0)$ 都在 F 上代数. 由于 $\alpha, \beta \in E$ 都是代数的, 那么 $F(\alpha), F(\beta)$ 都是有限扩张, 从而 $F(\alpha, \beta)$ 也是有限扩张, 从而是代数扩张, 即 $\alpha \pm \beta, \alpha\beta, \alpha/\beta (\beta \neq 0)$ 都是代数的. □

命题 1.2.9. 给定代数扩张 $E/F, K/E$, 那么 K/F 也是代数扩张.

命题 1.2.10. 给定代数扩张 E/F , 则 $\text{Hom}_F(E, E) = \text{Aut}_F(E)$.

证明: 任取 $\varphi: E \rightarrow E$ 是域扩张之间的态射, 我们现在只需要说明其一定是满射即可. 任取 $\alpha \in K$, 我们用 S 记 $P_{\alpha, F}(x)$ 在 E 中的根的全体, 由于 φ 固定 F , 从而 φ 给出了 S 到自身的一个映射, 并且由于 φ 是单的, 以及 S 是有限集, 从而 φ 在 S 上是满射, 从而一定存在 E 中的元素被 φ 映射成 α , 即 φ 是满射. □

第二章 分裂域及其应用

2.1 分裂域

定义 2.1.1. 给定域扩张 E/F , 多项式 $f(x) \in F[x]$ 在 E 中分裂 (split), 如果 $f(x)$ 在 E 中可以写成

$$f(x) = c \prod_{i=1}^n (x - \alpha_i)$$

其中 $\alpha_i \in E$.

定义 2.1.2. 给定域扩张 E/F , E 被称作是 $f(x) \in F[x]$ 的分裂域 (splitting field), 如果 E 是包含 F 使得 $f(x)$ 分裂的最小的域.

注记. 如果 E 是 $f(x) \in F[x]$ 的分裂域, 那么 E/F 是代数扩张.

定理 2.1.3. 给定域 F , 多项式 $f(x) \in F[x]$ 的分裂域 E 存在且在同构意义下唯一, 并且 $[E : F] \leq n!$, 其中 $n = \deg f(x)$.

证明: 我们通过对 $p(x)$ 次数的归纳来证明存在唯一性, 当 $n = 1$ 的时候是显然的.

1. 存在性: 根据命题 1.1.14, 总可以找到域扩张 F'/F 使得 $p(x)$ 在 F' 中有根, 因此 $p(x)$ 在 $F'[x]$ 中可以写成:

$$f(x) = (x - u)f_1(x), \quad \deg f_1(x) = n - 1$$

因此利用归纳假设, 存在 $f_1(x)$ 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 $f(x)$ 在 F 上的另一个分裂域, 根据引理 1.2.4, 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 $E' \cong E$.

□

上述证明分裂域存在的方法虽然简洁, 但是我们实际上可以做的更精细一些, 计算出分裂域之间的同构的个数有多少个, 这主要依赖于注记 1.2.

定理 2.1.4. 给定域 F , E 是 $f(x) \in F[x]$ 的分裂域. 如果 $f(x)$ 在域扩张 L/F 中分裂, 那么存在 $\varphi \in \text{Hom}_F(E, L)$. 这样 φ 的个数小于等于 $[E : F]$, 并且等号取得当且仅当 $f(x)$ 没有重根.

证明: 假设 $\{\alpha_1, \dots, \alpha_n\}$ 是 $f(x)$ 的所有根, 我们归纳地考虑: 由于 $f(x)$ 在 L 中分裂, 那么根据引理 1.2.4 有如下的延拓:

$$\begin{array}{ccc}
 F(\alpha_1) & \xrightarrow{\varphi_1} & L \\
 \uparrow & & \uparrow \\
 F & \xrightarrow{\text{id}} & F
 \end{array}$$

此时延拓可以选择的个数小于等于 $[F(\alpha_1) : F]$. 利用注记1.2我们可以做如下的延拓:

$$\begin{array}{ccc}
 F(\alpha_1, \alpha_2) & \xrightarrow{\varphi_2} & L \\
 \uparrow & \nearrow \varphi_1 & \uparrow \\
 F(\alpha_1) & & \\
 \uparrow & & \uparrow \\
 F & \xrightarrow{\text{id}} & F
 \end{array}$$

这是因为 α_2 在 $F(\alpha_1)$ 上的极小多项式 $P_{\alpha_2, F(\alpha_1)}$ 是 f 的因子, 从而 $\varphi_1(P_{\alpha_2, F(\alpha_1)})$ 依然在 L 中分裂, 此时延拓的可以选择的个数小于等于 $[F(\alpha_1, \alpha_2) : F(\alpha_1)]$, 不断归纳即可得到 $\varphi \in \text{Hom}_F(E, L)$, 并且这样的 φ 的个数小于等于

$$[F(\alpha_1) : F][F(\alpha_1, \alpha_2) : F(\alpha_1)] \dots [F(\alpha_1, \dots, \alpha_n) : F(\alpha_1, \dots, \alpha_{n-1})] = [E : F]$$

并且等号取得当且仅当 $f(x)$ 没有重根. □

注记. 特别地, 如果取 L 就是 $f(x)$ 的分裂域 E , 那么 $\varphi \in \text{Hom}_F(E, E) = \text{Aut}_F(E)$ 的个数小于等于 $[E : F]$, 并且等号取得当且仅当 $f(x)$ 没有重根.

2.2 有限域

定义 2.2.1. 域 F 被称为**有限域** (finite field), 如果其元素个数 $|F| < \infty$.

记号 2.2.2. 有 q 个元素的有限域通常记作 \mathbb{F}_q .

注记. 根据定义, 显然有限域 \mathbb{F}_q 的特征一定是素数 p , 并且如果 \mathbb{F}_q 是 \mathbb{F}_p 的 n 次扩张, 则 $q = p^n$.

定理 2.2.3. 对任意 $n \in \mathbb{Z}_{\geq 0}$, 元素个数为 $q = p^n$ 的有限域存在且唯一, 其中 p 是素数.

证明: 存在性: 考虑 $p(x) = x^q - x \in \mathbb{F}_p[x]$, 通过直接验证, 即验证加减乘除的封闭性, 可以发现 $p(x)$ 的所有根恰好组成了一个域 E . 并且根据引理3.2.4计算可知 $p(x)$ 没有重根, 因此 $|E| = q$, 即给出了一个元素个数为 $q = p^n$ 的有限域.

唯一性: 假设 \mathbb{F}_q 是元素个数为 q 的有限域, 那么 $|F^\times| = q-1$, 即任取 $\alpha \in F^\times$, 有 $\alpha^{q-1} = 1$, 从而任取 $\alpha \in F$, 其满足

$$\alpha^q - \alpha = 0$$

并且由于上述方程至多有 q 个解, 从而 F 是 $x^q - x \in \mathbb{F}_p[x]$ 的分裂域, 因此是唯一的. □

引理 2.2.4. 给定域 F , 以及 F^\times 的有限子群 G , 那么 G 是循环群.

证明: 由于 G 是有限阿贝尔群, 如果记其最大的不变因子为 d_n , 那么任取 $\alpha \in G$, 有 $\alpha^{d_n} = 1$. 考虑 $x^{d_n} - 1 \in F[x]$, 其最多只有 d_n 个根, 那么 $d_n \geq |G|$. 而另一方面, $|G| \leq d_n$, 从而 $|G| = d_n$, 即 $G \cong \mathbb{Z}/d_n\mathbb{Z}$. □

推论 2.2.5. \mathbb{F}_q^\times 是 $q-1$ 阶循环群.

证明: 当 F 是有限域时, F^\times 自身就是 F^\times 的有限子群, 从而是循环群. \square

例子. 考虑 $x^3 - x - 1 \in \mathbb{F}_3[x]$, 其为 $\mathbb{F}_3[x]$ 上的不可约多项式, 那么

$$\mathbb{F}_3[x]/(x^3 - x - 1)$$

给出了一个 27 元域.

命题 2.2.6. 对任意的 $n \in \mathbb{Z}_{\geq 0}$, 都存在 $\mathbb{F}_q[x]$ 中的 n 次不可约多项式.

证明: 由于 \mathbb{F}_q^\times 是循环群, 取其生成元为 α , 那么 $\mathbb{F}_q[\alpha] = \mathbb{F}_{q^n}$, 从而 α 对应的极小多项式就是 $\mathbb{F}_q[x]$ 中的 n 次不可约多项式. \square

问题 2.2.7. 对任意的 $n \in \mathbb{Z}_{\geq 0}$, $\mathbb{F}_q[x]$ 中的首一 n 次不可约多项式有多少个呢?

定义 2.2.8. 给定有限域 \mathbb{F}_{p^n} , 如下映射

$$\begin{aligned} \text{Frob}: \mathbb{F}_{p^n} &\rightarrow \mathbb{F}_{p^n} \\ x &\mapsto x^p \end{aligned}$$

被称作**弗罗贝尼乌斯映射** (Frobenius map).

注记. 根据命题 1.2.10, 我们有 $\text{Frob} \in \text{Aut}_{\mathbb{F}_p}(\mathbb{F}_q)$, 并且直接计算可知 $\text{Frob}^n = \text{id}$.

命题 2.2.9. 给定有限域 \mathbb{F}_{p^n} , \mathbb{F}_{p^m} 是 \mathbb{F}_{p^n} 的子域当且仅当 $m \mid n$.

证明: 如果 \mathbb{F}_{p^m} 是 \mathbb{F}_{p^n} 的子域, 那么 \mathbb{F}_{p^n} 可以视作 \mathbb{F}_{p^m} 上的有限维线性空间, 不妨假设为 k 维, 那么 $p^n = (p^m)^k$, 即 $n = mk$. 另一方面, 如果 $m \mid n$, 那么考虑 $x^{n/m} - x \in \mathbb{F}_{p^m}[x]$, 其分裂域就是 \mathbb{F}_{p^n} . \square

注记. 由于 $\text{Frob}^n = \text{id}$, 因此 Frob 生成了一个 n 阶循环群 G , 并且注意到 G 的任何一个子群都是由 Frob^m 生成的, 其中 $m \mid n$. 注意到 $\{\alpha \in \mathbb{F}_{p^n} \mid \text{Frob}^m(\alpha) = \alpha\} = \mathbb{F}_{p^{n/m}}$, 这实际上给出了一个 G 的所有子群与 \mathbb{F}_{p^n} 的所有子域之间的一一对应. 上述的结果实际上已经展示了伽罗瓦理论的雏形.

2.3 代数闭域与代数闭包

定义 2.3.1. 域 F 被称为**代数闭域** (algebraic closed field), 如果其不存在真的代数扩张.

命题 2.3.2. 给定代数扩张 E/F , 如果任取 $f(x) \in F[x]$, 其在 E 上都分裂, 那么 E 是代数闭域.

证明: 任取 $\alpha \in E$, 使得其在 E 上代数, 即存在 $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in E[x]$, 使得 $f(\alpha) = 0$, 特别地, 我们有 α 在 $F(a_n, \dots, a_0)$ 上代数, 并且由于 E/F 上代数, 那么 $F(a_n, \dots, a_0)/F$ 也是代数扩张, 从而根据命题 1.2.9 可知 $F(\alpha)/F$ 是代数扩张, 因此存在多项式 $g(x) \in F[x]$ 使得 $g(\alpha) = 0$, 而由于 $g(x)$ 在 E 中分裂, 从而 $\alpha \in E$, 即证明了 E 是代数闭域. \square

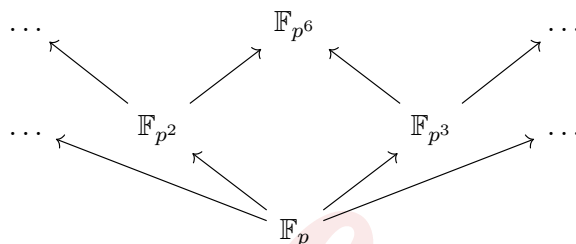
定义 2.3.3. 域扩张 E/F 中 E 被称为 F 的**代数闭包** (algebraic closure), 如果 E/F 是代数扩张, E 是代数闭域.

例子 ($\overline{\mathbb{Q}}$ 的构造). 注意到 $\mathbb{Q}[x]$ 是可数的, 不妨排序为 f_1, f_2, \dots , 那么我们令 E_1 是 f_1 在 \mathbb{Q} 上的分裂域, E_2 是 f_2 在 E_1 上的分裂域, 依次不断操作得到

$$\mathbb{Q} \subseteq E_1 \subseteq E_2 \subseteq \dots$$

考虑 $E = \bigcup_{i=1}^{\infty} E_i$, 则 E/\mathbb{Q} 是一个域扩张, 并且 \mathbb{Q} 上所有的多项式在 E 上都分裂, 并且根据命题 1.2.9 可知 E 是代数扩张, 从而 E 就是 $\overline{\mathbb{Q}}$.

例子 ($\overline{\mathbb{F}_p}$ 的构造). 对于素数 p , 我们有如下的包含关系



那么我们有 $\overline{\mathbb{F}_p} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$.

命题 2.3.4 (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 $F[\mathfrak{X}] \rightarrow F'$, 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

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

我们用 \bar{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 2.3.5. 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 $\tau': K \rightarrow E$. 特别地, 如果 K 是代数闭域, 那么 $\tau': K \rightarrow E$ 是同构.

证明: 任取 $u \in K$, α 在 F 上的极小多项式记作 $P_{\alpha,F}$, 由于 E 是代数闭域, 那么 $\tau(P_{\alpha,F})$ 在 E 中存在根 β , 那么根据引理 1.2.4 可知 σ 可以延拓到 $F(\alpha) \rightarrow E$. 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 1.2.4 可知 K' 就是 K . \square

定理 2.3.6. 域 F 的代数闭包 \overline{F} 存在且唯一 (在同构意义下).

证明: 存在性: 根据命题 2.3.4, 存在代数闭域 E 使得其是 F 的扩张, 定义

$$\overline{F} := \{\alpha \in E \mid \alpha \text{ 在 } F \text{ 上代数}\}$$

那么有 \overline{F} 是 F 的代数扩张. 并且 \overline{F} 是代数闭域, 因为任取 $f(x) = a_n x^n + \cdots + a_0 \in \overline{F}[x]$, 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 \overline{F} .

唯一性: 根据命题 2.3.5 即可. \square

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

第三章 正规扩张与可分扩张

3.1 正规扩张

定义 3.1.1. 代数扩张 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 E 中有一个根, 则其全部的根都在 E 中.

例子. 二次扩张是正规扩张.

定理 3.1.2. 下列叙述等价:

- (1) E/F 是正规扩张.
- (2) 任何 F -嵌入 $\tau: E \rightarrow \bar{F}$ 满足 $\tau(E) \subseteq E$.
- (3) $\text{Hom}_F(E, \bar{F}) = \text{Hom}_F(E, E)$.

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

(2) 推 (1): 任取 $\alpha \in E$, 考虑其在 F 上的极小多项式 $P_{\alpha, F}$, 任取其另一个根 $\beta \in \bar{F}$, 则存在态射 $F(\alpha) \rightarrow \bar{F}, \alpha \mapsto \beta$, 因此根据引理 1.2.4 可以延拓成 $\tau: K \rightarrow \bar{F}$, 因此 $\tau(\alpha) = \beta \in E$, 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) 推 (4): 假设 E/F 是正规扩张, 任取 $\alpha_1 \in E \setminus F$, 记其在 F 上的极小多项式为 $P_{\alpha_1, F}$, 并且 $[E : F(u_1)] < [E : F]$, 再取 $\alpha_2 \in E \setminus F(\alpha_1)$, 由于扩张次数不断在减小, 因此有限次重复后一定有 $E = F(\alpha_1, \dots, \alpha_n)$, 令 $P = \prod_{i=1}^n P_{\alpha_i, F}$, 则 K 是 p 的分裂域.

(4) 推 (2): 如果 E 是 $P(x)$ 的分裂域, 其所有的根为 $\{\alpha_1, \dots, \alpha_n\}$, 则 $E = F(\alpha_1, \dots, \alpha_n)$, 考虑 F -嵌入 $\tau: F(\alpha_1, \dots, \alpha_n) \rightarrow \bar{F}$, 由于 $\tau(\alpha_i)$ 仍然是 $P(x)$ 的根, 因此 $\tau(\alpha_i) \in E$, 即 $\tau(E) \subseteq E$.

□

推论 3.1.3. 对于域扩张 $F \subseteq E \subseteq K$

- (1) 如果 K/F 是正规扩张, 那么 K/E 也是正规扩张.
- (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 $\alpha \in K$, 考虑其在 F, E 上的极小多项式, 分别为 $P_{\alpha, F}, P_{\alpha, E}$, 则 $P_{\alpha, E} \mid P_{\alpha, F}$. 由于 K/F 是正规扩张, 因此 $P_{\alpha, F}$ 的所有根都在 K 中, 因此 $P_{\alpha, E}$ 的所有根也在 K 中, 即 K/E 也是正规扩张.

(2). 给定嵌入 $\tau: EE' \rightarrow \bar{F}$, 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. \square

注记. K/F 是正规扩张并不意味着 E/F 是正规扩张, 例如考虑下面的例子:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi\sqrt{-1}}{3}})$$

注记. 如果 K/E 是正规扩张, E/F 是正规扩张, 但 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.

3.2 可分扩张

注记1.2还可以有如下的形式:

引理 3.2.1. 给定代数扩张 $E = F[\alpha_1, \dots, \alpha_n]/F$, 则

$$|\text{Hom}_F(E, \bar{F})| \leq [E : F]$$

等号取得当且仅当 α_i 在 F 上的极小多项式 $P_{\alpha_i, F}$ 没有重根.

因此我们关心在什么时候这些极小多项式没有重根.

定义 3.2.2. 给定域 F 以及 $f(x) = a_n x^n + \dots + a_1 x + a_0 \in F[x]$, 其**形式导数** (formal derivative) 定义为

$$f'(x) := na_n x^{n-1} + \dots + a_1$$

引理 3.2.3. 对于 $f(x), g(x) \in F[x]$, 有

1. $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$.
2. $(f(g(x)))' = f'(g(x))g'(x)$.

引理 3.2.4. 给定 $f(x) \in F[x]$, $p(x)$ 有重根当且仅当 $(f, f') \neq 1$.

证明: 在 $f(x)$ 的分裂域中将 $f(x)$ 写做 $f(x) = c \prod_{i=1}^n (x - \alpha_i)$, 则

$$f'(x) = c \sum_{i=1}^n (x - \alpha_1) \dots (x - \alpha_{i-1})(x - \alpha_{i+1}) \dots (x - \alpha_n)$$

如果 p 有重根, 不妨假设 $\alpha_1 = \alpha_2$, 则 $f'(\alpha_1) = 0$, 即 $(x - \alpha_1) \mid (f, f')$. 另一方面, 如果 $\alpha_i \neq \alpha_j$ 对任意 $i \neq j$ 成立, 则 $f'(\alpha_i) \neq 0$ 对任意 $1 \leq i \leq n$ 成立, 从而 $(f, f') = 1$. \square

推论 3.2.5. 如果 f 是不可约多项式, f 有重根等价于 $f' = 0$.

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

定义 3.2.6. 给定域 F , $p(x) \in F[x]$ 被称为**可分多项式** (seperable polynomial), 如果其不存在重根.

定义 3.2.7. 给定域扩张 E/F , $\alpha \in E$ 被称为 F 上的**可分元** (seperable element), 如果其在 F 上的极小多项式 $P_{\alpha, F}$ 是可分多项式.

定义 3.2.8. 代数扩张 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.

定理 3.2.9. 给定代数扩张 E/F , 如下叙述等价:

- (1) E/F 是可分扩张.
- (2) $E = F(\{\alpha_i\}_{i \in I})$, 其中 α_i 是 F 上的可分元.

如果 E/F 是有限扩张, 则上述两条还与下面的等价:

- (3) $|\text{Hom}_F(E, \bar{F})| = [E : F]$.

证明: (1) 推 (2) 是显然的, (2) 推 (3) 成立依赖于本节最初的引理3.2.1, 下面我们假设 E/F 是有限扩张来证明 (3) 推 (1): 由于 E/F 是有限扩张, 因此不妨假设 E 是 F 添加有限多个元素得到的, 即 $E = F(\alpha_1, \dots, \alpha_n)$, 任取 $\alpha \in E$, 我们不妨考虑 $E = F(\alpha, \alpha_1, \dots, \alpha_n)$, 因此根据引理3.2.1的取等条件可知 $\alpha, \alpha_1, \dots, \alpha_n$ 都是 F 上的可分元. 特别地, 有 α 是 F 上的可分元, 即 E/F 可分.

最后我们来证明 (2) 推 (1): 假设 $E = F(\{\alpha_i\}_{i \in I})$, 其中 α_i 是 F 上的可分元. 任取 $\alpha \in E$, 由于 E/F 代数, 从而存在 F 的某个有限扩张 $L = F(\alpha_1, \dots, \alpha_n)$ 使得 $\alpha \in L$, 因此利用有限扩张情形的 (2) 推 (3) 推 (1) 即可知 α 在 F 上可分. \square

推论 3.2.10. 可分多项式的分裂域是可分扩张.

证明: 可分多项式的分裂域可以视作是添加若干可分元得到的扩域. \square

推论 3.2.11. 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 $\alpha \in K$, 其在 E 上的极小多项式记作 $P_{\alpha, E}(x) = a_n x^n + \dots + a_0$. 考虑 $F \subseteq F(a_0, \dots, a_n) \subseteq E \subseteq E(u) \subseteq K$, 由于 E/F 是可分的, 从而 $F(a_0, \dots, a_n)/F$ 是可分的. 而 α 在 $F(a_0, \dots, a_n)$ 上的极小多项式也是 $P_{\alpha, E}$, 是一个可分多项式, 即 α 在 $F(a_0, \dots, a_n)$ 上可分, 从而根据定理3.2.9有 $F(u, a_0, \dots, a_n)/F$ 是可分的. 特别地, α 在 F 上是可分的. \square

推论 3.2.12. $E/F, E'/F$ 都是可分扩张, 则 EE'/F 也是可分扩张.

证明: 显然 EE' 中所有的元素都是 F 上的可分元, 从而根据定理3.2.9可知 EE'/F 是可分扩张. \square

命题 3.2.13. 如果 $\text{char } F = 0$, 则任何不可约多项式都是可分的.

证明: 当 $\text{char } F = 0$ 时, 任何非常数的多项式都有非零导数, 从而根据引理3.2.4即可. \square

例子. 当 $\text{char } F = p$ 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

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

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.

命题 3.2.14. 如果 $\text{char } F = p$, 则任何不可约多项式都是可分的当且仅当 $F = F^p$.

证明: 假设不可约 $f \in F[x]$ 不可分当且仅当 $f' = 0$, 这也当且仅当 f 可以写作

$$f = \sum_{k=0}^n a_k x^{kp}$$

假设 $F = F^p$, 那么对于任意 a_k , 总存在 b_k 使得 $b_k^p = a_k$, 从而

$$f = \sum_{k=0}^n b_k^p x^{kp} = \left(\sum_{k=0}^n b_k x^k \right)^p$$

与 f 不可约相矛盾. 另一方面, 假设 $F \neq F^p$, 那么存在 $t \in F$ 使得 $\sqrt[p]{t} \notin F$, 考虑 $x^p - t$ 便得到了一个不可约的不可分多项式. \square

定义 3.2.15. 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.

命题 3.2.16.

1. 如果 $\text{char } F = 0$, 则 F 是完美域.
2. 如果 $\text{char } F = p$, 域 F 是完美域当且仅当 $F^p = F$.
3. 任何有限域都是完美域.

证明: (1) 和 (2) 根据命题3.2.13以及命题3.2.14即可. 对于 (3), 弗罗贝尼乌斯映射给出了 $F^p = F$. \square

命题 3.2.17. 完美域的代数扩张都是可分扩张.

证明: 假设 F 是完美域, E/F 是代数扩张, 任取 $\alpha \in E$, 则其在 F 上的极小多项式是可分多项式, 从而 α 是 F 上的可分元, 即 E/F 是可分扩张. \square

推论 3.2.18. 如果 $\text{char } F = 0$, 则任何代数扩张 E/F 是可分扩张.

推论 3.2.19. $\mathbb{F}_{p^n}/\mathbb{F}_p$ 是可分扩张.

3.3 纯不可分扩张

在本节中, F 总是指特征为 p 的域. 给定一个不可约的不可分多项式 $P(x) \in F[x]$, 那么根据 $P'(x) = 0$ 可知存在 $P_1(x)$, 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.

定义 3.3.1. 对于不可约的不可分多项式 $P(x) \in F[x]$, $n_s := \deg P_e$, 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).

命题 3.3.2. 给定域扩张 E/F , F 上所有可分的元素组成的集合记作 E_s , 那么 E_s 是 E 的一个子域.

证明: 任取 $\alpha, \beta \in E$ 是可分元, 那么根据定理 3.2.9 可知 $F(\alpha, \beta)/F$ 是可分扩张, 从而可分元的加减乘除都在其中, 即 E_s 是 E 的一个子域. \square

定义 3.3.3. $u \in \bar{F}$ 被称为在 F 上**纯不可分** (purely inseperable), 如果 $u^{p^m} \in F$, 对某个正整数 m 成立.

定义 3.3.4. 代数扩张 E/F 被称为**纯不可分扩张** (purely inseperable extension), 如果 E 中的每个元素在 F 上都是纯不可分的.

命题 3.3.5. 给定域扩张 E/F , 则 E/E_s 是纯不可分扩张.

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

注记. 即给定域扩张 E/F , 其可以分解为可分扩张 E_s/F 和纯不可分扩张 E/E_s .

定义 3.3.6. 给定域扩张 E/F , 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 3.3.7.

- (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.

证明: (1). 由于 E/F 是纯不可分扩张, 从而 $\alpha \in E$ 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 , $\alpha \in E$ 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

$$[E : F] = [F(\alpha_1, \dots, \alpha_n) : F(\alpha_1, \dots, \alpha_{n-1})] \dots [F(\alpha_1) : F]$$

是 p 的幂次.

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

命题 3.3.8. 给定有限扩张 E/F , 则

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

特别地, 等号取得当且仅当 E/F 是可分扩张.

证明: 如果 E/F 是可分扩张, 则根据定理3.2.9可知

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

而当 E/F 不是可分扩张时, 我们断言有如下——对应:

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

通过 $\tau \mapsto \tau|_{K_s}$ 给出. 对应是满射可根据命题2.3.5; 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 $\tau(u^{p^m}) = \tau(u)^{p^m} = v \in \overline{F}$, 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. \square



第四章 伽罗瓦理论

4.1 伽罗瓦扩张

记号 4.1.1. 给定域扩张 E/F , 对于 $H < \text{Aut}_F(E)$, 记 $E^H = \{u \in E \mid \tau(u) = u, \forall \tau \in H\}$.

定义 4.1.2. 代数扩张 E/F 被称为伽罗瓦扩张 (Galois extension), 如果其是可分正规扩张.

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

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

其中 (1) 成立是根据定理 3.1.2, (2) 成立是根据定理 3.2.9.

命题 4.1.3. 对于域扩张 $F \subseteq E \subseteq K$, 如果 K/F 是伽罗瓦扩张, 则 K/E 也是.

证明: 根据推论 3.1.3 以及推论 3.2.11 即可. □

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

定义 4.1.4. 给定可分扩张 E/F , 则在 \bar{F} 中包含 E 的最小的伽罗瓦扩张被称为 E/F 的伽罗瓦闭包 (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 $F(\{\alpha_i\}_{i \in I})$, 其中 α_i 都是代数元. 对于每一个 α_i , 用 $P_{\alpha_i, F}$ 去记其在 F 上的极小多项式, 那么将这些 $P_{\alpha_i, F}$ 在 \bar{F} 中的所有根都添加到 F 中, 得到的域记作 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 α_i 都是可分元, 从而此时的 N/F 也是可分扩张, 从而 N/F 是 E/F 的 Galois 闭包. 更特别地, 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.

命题 4.1.5. 对于有限扩张 E/F , 如下叙述等价:

- (1) E/F 是伽罗瓦扩张.
- (2) E 是可分多项式 $f \in F[x]$ 的分裂域.
- (3) $F = E^{\text{Gal}(E/F)}$.
- (4) 存在 $\text{Aut}_F(E)$ 的有限子群 H 使得 $F = E^H$.

证明: (1) 和 (2) 等价是根据定理3.1.2和推论3.2.10即可. (1) 推 (3): 首先显然 $F \subseteq E^{\text{Gal}(E/F)}$; 另一方面, 任取 $\alpha \in E^{\text{Gal}(E/F)}$, 考虑 α 在 F 上的极小多项式 $P_{\alpha,F}$, 任取 $P_{\alpha,F}$ 的一个根 β , 定义嵌入 $F(\alpha) \hookrightarrow \bar{F}$ 为 $\alpha \mapsto \beta$, 根据命题2.3.5可以将其延拓成 $\tau: E \rightarrow \bar{F}$, 而根据 E 是正规扩张, 可知 $\tau(E) = E$, 即 $\tau \in \text{Gal}(E/F)$. 由于 $\alpha \in E^{\text{Gal}(E/F)}$, 因此 $\beta = \tau(\alpha) = \alpha$, 即 $P_{\alpha,F}(x) = x - \alpha$, 即 $\alpha \in F$. (3) 推 (4) 是显然的, 取 $H = \text{Aut}_F(K)$ 即可. (4) 推 (1) 是下面将要证明的引理4.1.8, 即阿廷引理. \square

记号 4.1.6. 如果伽罗瓦扩张 E/F 是多项式 $f(x) \in F[x]$ 的分裂域, 那么此时记伽罗瓦群为 G_f .

引理 4.1.7. K 是域, $H = \{\tau_1, \dots, \tau_n\}$ 是 $\text{Aut}(K)$ 的有限子集 (不必要是子群). 如果存在 $c_i \in K$ 使得

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

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

$$c_1\tau_1(x) + \dots + c_r\tau_r(x) = 0 \quad (4.1.1)$$

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

$$c_1\tau_1(a)\tau_1(x) + \dots + c_r\tau_r(a)\tau_r(x) = 0 \quad (4.1.2)$$

(4.1.2) 减 (4.1.1) 乘 $\tau_r(a)$ 则有

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

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. \square

引理 4.1.8 (阿廷引理). K 是域, $H = \{\tau_1, \dots, \tau_n\}, \tau_1 = \text{id}$ 是 $\text{Aut}(K)$ 的有限子群, 记 $E = K^H$, 则 K/E 是伽罗瓦扩张, 并且扩张次数 $[K:E] = |H|$.

证明: 我们首先证明 K/E 是伽罗瓦扩张: 任取 $\alpha \in K$, 记 α 在 E 上的极小多项式为 p , 令 \mathcal{O} 是 α 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 $\alpha \in \mathcal{O}$, 即 $q(\alpha) = 0$, 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 是伽罗瓦扩张.

现在来证明 $[K:E] \leq |H|$: 只需要证明任取 $\alpha_1, \dots, \alpha_{n+1} \in K$, 它们是 E -线性相关即可: 考虑矩阵 $(\tau_i(\alpha_j)) \in M_{n \times (n+1)}(K)$, 则其 $n+1$ 列 K -线性相关, 即存在 $c_1, \dots, c_{n+1} \in K$, 且不全为零使得:

$$c_1 \begin{pmatrix} \tau_1(\alpha_1) \\ \tau_2(\alpha_1) \\ \vdots \\ \tau_n(\alpha_1) \end{pmatrix} + c_2 \begin{pmatrix} \tau_1(\alpha_2) \\ \tau_2(\alpha_2) \\ \vdots \\ \tau_n(\alpha_2) \end{pmatrix} + \dots + c_{n+1} \begin{pmatrix} \tau_1(\alpha_{n+1}) \\ \tau_2(\alpha_{n+1}) \\ \vdots \\ \tau_n(\alpha_{n+1}) \end{pmatrix} = 0 \quad (4.1.3)$$

不妨假设 $c_1, \dots, c_r \neq 0, c_{r+1} = \dots = c_{n+1} = 0$, 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:

$$\alpha_1 + c_2\alpha_2 + \dots + c_r\alpha_r = 0 \quad (4.1.4)$$

我们断言 $c_2, \dots, c_n \in E$, 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 (4.1.4) 可得

$$\tau_j(\alpha_1) + \tau_j(c_2)\tau_j(\alpha_2) + \dots + \tau_j(c_r)\tau_j(\alpha_r) = 0 \quad (4.1.5)$$

用 (4.1.5) 分别与 (4.1.3) 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 $\{x_1, \dots, x_r\}$ 是 K 在 E 上的一组基, 那么任取 $y \in K$, 将其写成

$$y = c_1x_1 + \dots + c_rx_r$$

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

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

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

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

因此 $\xi_1\tau_1(y) + \dots + \xi_n\tau_n(y) = 0$ 对任意的 $y \in K$ 成立, 根据引理4.1.7可知 $\xi_i = 0$, 相矛盾! \square

4.2 伽罗瓦对应

定理 4.2.1 (伽罗瓦主定理). 给定有限伽罗瓦扩张 K/F , 则

(1) 存在如下的一一对应:

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

对应法则为 $H \mapsto K^H$ 与 $E \mapsto \text{Gal}(K/E)$.

(2) E/F 是伽罗瓦扩张当且仅当 $\text{Gal}(K/E)$ 是 $\text{Gal}(K/F)$ 的正规子群, 并且:

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

证明: (1). 根据命题4.2.4的 (3) 可知

$$E \rightarrow \text{Gal}(K/E) \rightarrow K^{\text{Gal}(K/E)} = E$$

现在只需要证明下面的对应成立:

$$H \rightarrow K^H \rightarrow \text{Gal}(K/K^H) = H$$

一方面 $H \subseteq \text{Gal}(K/K^H)$ 是显然的, 而根据引理4.1.8:

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

即两者相同.

(2). 根据推论3.2.11可知 E/F 是可分扩张, 从而 E/F 是伽罗瓦扩张当且仅当 E/F 是正规扩张, 即 $\tau(E) = E$. 任取 $\tau \in \text{Gal}(K/F)$, 可以直接验证:

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

因此 E/F 是伽罗瓦扩张当且仅当 $\tau(E) = E$ 当且仅当 $\text{Gal}(K/E)$ 是正规子群. \square

推论 4.2.2. 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4.1可知其 Galois 闭包 K/F 也是有限扩张, 从而根据伽罗瓦对应 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. \square

推论 4.2.3 (本原元定理). 如果 E/F 是有限可分扩张, 则 $E = F(\alpha)$, $\alpha \in E$.

证明: 如果 F 是有限域, 则不妨假设 $F = \mathbb{F}_p$, $E = \mathbb{F}_q$, $q = p^m$, 根据推论2.2.5可知 \mathbb{F}_q^\times 是循环群, 不妨记其生成元为 ξ , 则 $\mathbb{F}_q = \mathbb{F}_p(\xi)$; 如果 F 是无限域, 不妨假设 $E = F(\alpha_1, \alpha_2)$, 一般情况归纳即可: 任取 $r \in F$, 考虑 $F \subseteq F(\alpha_1 + r\alpha_2) \subseteq E$, 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:

$$F(\alpha_1 + r_1\alpha_2) = F(\alpha_1 + r_2\alpha_2)$$

考虑 $\alpha = \alpha_1 + r_1\alpha_2$, 我们断言 $F(\alpha) = F(\alpha_1, \alpha_2)$: 显然 $F(\alpha) \subseteq F(\alpha_1, \alpha_2)$; 另一方面, 由于 $\alpha = \alpha_1 + r_1\alpha_2 = \alpha_1 + r_2\alpha_2$, 并且 $r_1 \neq r_2$, 从而 $(r_1 - r_2)\alpha_2 \in F(\alpha)$, 即 $\alpha_2 \in F(\alpha)$, 从而 $\alpha_1 \in F(\alpha)$, 即 $F(\alpha) = F(\alpha_1, \alpha_2)$. \square

命题 4.2.4. 如果 $E/F, K/F$ 都是有限伽罗瓦扩张, 则 EK/F 也是伽罗瓦扩张, 并且

(1)

$$\varphi: \text{Gal}(EK/K) \rightarrow \text{Gal}(E/E \cap K)$$

$$\tau \mapsto \tau|_E$$

是同构.

(2)

$$\psi: \text{Gal}(EK/F) \rightarrow \text{Gal}(E/F) \times \text{Gal}(K/F)$$

$$\tau \mapsto (\tau|_E, \tau|_K)$$

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3.1.3可知 EK/F 是正规扩张. 根据推论3.2.12可知 EK/F 是可分扩张, 从而 EK/F 是伽罗瓦扩张, 并且由于 $E/F, K/F$ 都是有限的, 从而 EK/F 也是有限伽罗瓦扩张, 因此 EK/E 也是有限伽罗瓦扩张.

(1). 任取 $\tau \in \text{Gal}(EK/K)$, 考虑 $\tau|_E: E \rightarrow EK \hookrightarrow \bar{F}$, 由于 E/F 是正规的, 从而根据定理3.1.2有 $\tau(E) \subseteq E$, 即 $\tau|_E \in \text{Gal}(E/E \cap K)$. 如果 $\tau|_E = \text{id}_E$, 那么由于 $\tau|_F = \text{id}_F$ 有 $\tau = \text{id}_{EK}$,

即 φ 是单射. 另一方面, $\text{im } \varphi$ 是 $\text{Gal}(E/E \cap K)$ 的子群, 并且 $E^{\text{im } \varphi} = (EK)^{\text{Gal}(EK/K)} \cap E = K \cap E$, 从而 $\text{im } \varphi = \text{Gal}(E/E \cap K)$.

(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 $(\sigma_1, \sigma_2) \in \text{Gal}(E/F) \times \text{Gal}(K/F)$, 根据 (1) 有 σ_1, σ_2 可以被延拓成 $\sigma'_1 \in \text{Gal}(EK/K)$ 和 $\sigma'_2 \in \text{Gal}(EK/E)$. 令 $\tau = \sigma'_2 \circ \sigma'_1 \in \text{Gal}(EK/F)$, 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. \square

定义 4.2.5. 伽罗瓦扩张被称为**阿贝尔扩张** (abelian extension), 如果其伽罗瓦群是阿贝尔群.

定义 4.2.6. 伽罗瓦扩张被称为**循环扩张** (cyclic extension), 如果其伽罗瓦群是循环群.

推论 4.2.7. 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.

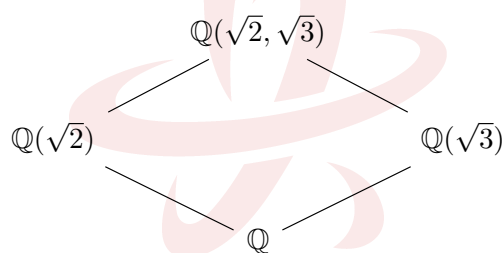
证明: 注意到阿贝尔群 (循环群) 的子群还是阿贝尔群 (循环群). \square

4.3 伽罗瓦群的计算

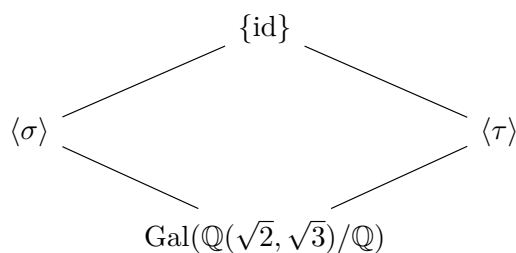
4.3.1 简单多项式的分裂域

通过伽罗瓦对应, 我们可以计算一些常见的扩张的伽罗瓦群, 例如下面的两个例子.

例子. 考虑伽罗瓦扩张 $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$, 我们有如下的中间域:



其对应到子群



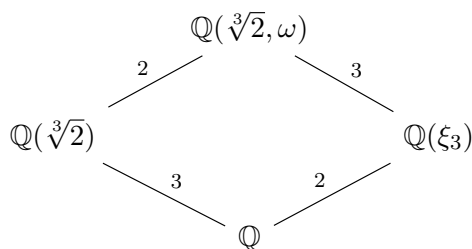
其中

$$\sigma: \begin{cases} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{cases} \quad \tau: \begin{cases} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{cases}$$

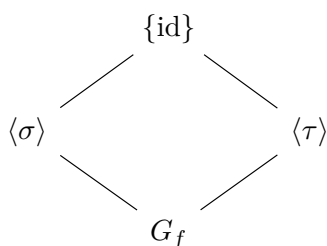
由于 $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ 是一个四阶群, 并且我们已经找到了其两个二阶子群 $\langle \sigma \rangle, \langle \tau \rangle$, 并且 $\sigma\tau = \tau\sigma$, 从而可知 $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \mathbb{Z}_2 \times \mathbb{Z}_2$.

注记. 注意到 $\mathbb{Z}_2 \times \mathbb{Z}_2$ 还有一个二阶子群 $\langle \tau\sigma \rangle$, 其对应到的不变子域为 $\mathbb{Q}(\sqrt{6})$.

例子. 考虑 $f(x) = x^3 - 2 \in \mathbb{Q}[x]$ 的分裂域 $\mathbb{Q}(\sqrt[3]{2}, \xi_3)/\mathbb{Q}$, 其中 $\xi_3 = e^{\frac{2\pi\sqrt{-1}}{3}}$, 我们有如下的中间域:



对应到子群



其中

$$\sigma: \begin{cases} \omega \mapsto \xi_3^2 \\ \sqrt[3]{2} \mapsto \sqrt[3]{2} \end{cases} \quad \tau: \begin{cases} \xi_3 \mapsto \xi_3 \\ \sqrt[3]{2} \mapsto \sqrt[3]{2}\xi_3 \\ \sqrt[3]{2}\xi_3 \mapsto \sqrt[3]{2}\xi_3^2 \end{cases}$$

并且直接计算可知

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

从而可知 $G_f = S_3$.

练习. 写出 S_3 的其他子群, 与其对应的不变子域.

命题 4.3.1. 令 E 是不可约多项式 $f(x) \in F[x]$ 的分裂域, $\alpha_1, \dots, \alpha_n$ 是 $f(x)$ 的根, 那么 $\text{Gal}(E/F)$ 在 $\{\alpha_1, \dots, \alpha_n\}$ 上忠实地¹ (faithfully), 可递地 (transitively) 作用, 并且 n 整除 $|\text{Gal}(E/F)|$.

证明: 任取 $\sigma \in \text{Gal}(E/F)$, 其完全被 $\sigma(\alpha_i)$ 所决定, 因此 $G_f \hookrightarrow S_n$. 并且是可递的, 因为可以定义

$$\sigma': \alpha_i \rightarrow \alpha_j$$

再将其延拓成 $\text{Gal}(E/F)$ 中的元素. 注意到 $\mathbb{Q} \subseteq \mathbb{Q}(\alpha_1) \subseteq E$, 由于 $[\mathbb{Q}(\alpha_1) : \mathbb{Q}]$ 的扩张次数是 n , 因此 n 整除 $|\text{Gal}(E/F)|$. \square

注记. 根据上述命题, 不难直接看出 $x^3 - 2$ 的伽罗瓦群就是 S_3 .

4.3.2 有限域上的伽罗瓦扩张

定理 4.3.2. $q = p^m, m > 0$, 则 $\mathbb{F}_{q^d}/\mathbb{F}_q$ 是伽罗瓦扩张, 并且 $\text{Gal}(\mathbb{F}_{q^d}/\mathbb{F}_q) = \mathbb{Z}/d\mathbb{Z}$, 由弗罗贝尼乌斯同构 $\sigma: x \mapsto x^q$ 生成.

¹即有单嵌入 $\text{Gal}(E/F) \rightarrow S_n$.

4.3.3 模 p 方法

给定 n 次首一多项式 $f(x) \in \mathbb{Z}[x]$, 其判别式定义为 $D(f) = \prod_{i < j} (\alpha_i - \alpha_j)^2 \in \mathbb{Z}$, 其中 α_i 是 $f(x)$ 的根. 如果记 $f_p(x) \equiv f(x) \pmod{p}$, 那么 $D(f_p) \neq 0$ 当且仅当素数 p 不整除 $D(f)$.

定理 4.3.3 (Dedekind). $f(x) \in \mathbb{Z}[x]$ 是 n 次首一多项式, p 是使得 $f_p(x)$ 可分的素数, 假设 $f_p(x)$ 在 $(\mathbb{Z}/p\mathbb{Z})[x]$ 中分解成次数分别是 n_1, \dots, n_r 的不可约多项式的乘积, 那么 G_f 中包含一个类型为 (n_1, \dots, n_r) 的置换.

证明: 假设 K 是 f 的分裂域, $f(x)$ 在 K 中分裂为 $(x - \alpha_1) \dots (x - \alpha_n)$. 考虑 $R = \mathbb{Z}[\alpha_1, \dots, \alpha_n] \subseteq K$, 由于 $\alpha_1, \dots, \alpha_n$ 都是代数整数, 从而 R 中所有的元素都是代数整数. 由 p 生成的主理想 $pR \neq R$, 否则 $1/p \in R$ 导致 $1/p \in R \cap \mathbb{Q} = \mathbb{Z}$, 相矛盾. 取包含 pR 的一个极大理想 P , 因为 \mathbb{Z} 可以自然的嵌入到 R 中, 我们有映射 $\mathbb{Z} \rightarrow R/P$, 并且 $p\mathbb{Z}$ 包含在映射的核里, 再由于 $p\mathbb{Z}$ 是 \mathbb{Z} 的极大理想可知映射的核就是 $p\mathbb{Z}$, 即 R/P 是 \mathbb{F}_p 的一个域扩张. 假设

$$f(x) \equiv (x - \bar{\alpha}_1) \dots (x - \bar{\alpha}_n) \pmod{P}$$

从而 $f(x)$ 在 R/P 中分裂, 并且 R/P 由 $\bar{\alpha}_1, \dots, \bar{\alpha}_n$ 生成, 因此 R/P 是 $f_p(x)$ 的分裂域.

因为 $\text{Gal}(K/\mathbb{Q})$ 可以作用在 $\{\alpha_1, \dots, \alpha_n\}$ 上, 从而 $\text{Gal}(K/\mathbb{Q})$ 可以作用在 R 上. 令 $D_P = \{\sigma \in \text{Gal}(K/\mathbb{Q}) \mid \sigma P = P\}$, 从而有映射

$$\begin{aligned} \varphi: D_P &\mapsto \text{Aut}(R/P) \\ \sigma &\mapsto \sigma|_R \end{aligned}$$

□

引理 4.3.4. $G < S_n$ 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: 我们不妨取 $(n-1)$ -轮换 $\tau = (23 \dots n)$, 因为任何 $(n-1)$ -轮换都可以生成它. 并且我们可以取 $\sigma = (1a)$, 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 G 的可递性取 σ' 满足 $\sigma'(i) = 1$ 即可. 考虑如下 τ^k 在 $(1a)$ 上的作用

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

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

引理 4.3.5. p 是素数, $G < S_p$, 并且 G 包含一个对换和 p -轮换, 则 $G = S_p$.

例子. 考虑 $f(x) = x^5 - x - 1$, 首先模 5 可知 $f_5(x) = x^5 - x - 1$ 是不可约的, 从而 G_f 中包含一个 5-轮换. 模 2 可知 $f_2(x) = (x^2 + x + 1)(x^3 + x^2 + 1)$, 从而 G_f 包含一个对换, 从而可知 $G_f = S_5$.

例子. 考虑 $f(x) = x^6 + 22x^5 + 21x^4 + 12x^3 - 36x^2 - 29x - 15$, 首先模 2 可知 $f_2(x) = x^6 + x^4 + x^2 + x + 1$, 分析其不可约性可知其不可约, 从而 G_f 中包含一个 6-轮换, 即 G_f 是 S_6 的可递子群. 模 3 可知 $f_3(x) = x(x^5 + x^4 - x + 1)$, 从而 G_f 包含一个 5-轮换. 最后考虑模 5 得到 $f_5(x) = x(x-1)(x+1)(x+2)(x^2+2)$, 从而 G_f 包含 2-轮换, 从而根据引理 4.3.4 可知 $G_f = S_6$.

4.3.4 分圆扩张

定义 4.3.6. 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.

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

定义 4.3.7. n 次分圆多项式 (n -th cyclotomic polynomial) 被定义为:

$$\Phi_n(x) = \prod_{(n,k)=1} (x - \xi_n^k)$$

定理 4.3.8. $\mathbb{Q}(\xi_n)/\mathbb{Q}$ 是伽罗瓦扩张, 并且 $\text{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$.

证明: $\mathbb{Q}(\xi_n)/\mathbb{Q}$ 是伽罗瓦扩张, 因为是特征零域上的 $x^n - 1$ 的分裂域. 任取 $\tau \in \text{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$, 其一定形如 $\tau(\xi_n) = \xi_n^k$, 并且如果假设其逆映射为 $\tau^{-1}(\xi_n) = \xi_n^l$, 则

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

即 $kl \equiv 1 \pmod{n}$, 即 $k \in (\mathbb{Z}/n\mathbb{Z})^\times$, 因此有单射 $\text{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$. 为了证明满射, 只需要证明任取素数 $p \nmid n$, 存在 $\tau \in \text{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q})$ 使得 $\tau(\xi_n) = \xi_n^p$. 令 $R = \mathbb{Z}[\xi_n]$ 以及 P 是包含 pR 的极大理想, 那么根据模 p 方法的证明过程可知 R/P 是 $\Phi_n(x) \pmod{p}$ 的分裂域. 假设 $\sigma \in D_P$ 使得 $\sigma|_R$ 上给出了 $\text{Gal}((R/P)/\mathbb{F}_p)$ 的弗罗贝尼乌斯映射, 即

$$\sigma(\overline{\xi_n}) = \overline{\xi_n^p} = \overline{\xi_n^p}$$

假设 $\sigma(\xi_n) = \xi_n^i$, 那么 $\overline{\xi_n^i} = \overline{\xi_n^p}$. 由于 $\Phi_n(x) \mid x^n - 1$, 以及 $x^n - 1 \pmod{p}$ 无重根, 从而 $\Phi_n(x) \pmod{p}$ 无重根, 因此 $\xi_n^i = \xi_n^p$, 证毕. \square

推论 4.3.9. $\Phi_n(x)$ 是不可约多项式.

推论 4.3.10.

$$\Phi_n(x) \in \mathbb{Z}[x]$$

证明: 任取 $\tau \in \text{Gal}(\mathbb{Q}(\xi_n)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$, 有

$$\begin{aligned} \tau(\Phi_n(x)) &= \tau\left(\prod_{(n,k)=1} (x - \xi_n^k)\right) \\ &= \prod_{(n,k)=1} (x - \xi_n^k) \\ &= \Phi_n(x) \end{aligned}$$

从而 $\Phi_n(x) \in \mathbb{Q}[x]$. 并且注意到 $\Phi_n(x)$ 的系数都是本原单位根的组合, 从而是代数整数, 因此 $\Phi_n(x) \in \mathbb{Z}[x]$. \square

推论 4.3.11. 对于 $\mathbb{Q} \subseteq E \subseteq \mathbb{Q}(\xi_n)$, E/\mathbb{Q} 是阿贝尔扩张.

定理 4.3.12 (Kronecker-Weber). 如果 E/\mathbb{Q} 是有限阿贝尔扩张, 则存在 n 使得 $\mathbb{Q} \subseteq E \subseteq \mathbb{Q}(\xi_n)$.

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

命题 4.3.13. 如果 $n = p_1^{k_1} \dots p_r^{k_r}$, 则我们有:

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

命题 4.3.14. 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.

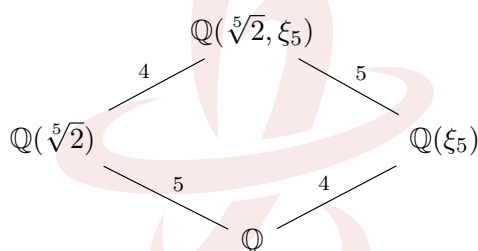
命题 4.3.15. 当 $p = 2, k \geq 4$ 时, 我们有:

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

不是循环群.

例子. 多项式 $f(x) = x^5 - 2$ 的伽罗瓦群 G_f 为 $\mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$.

证明: 考虑下图



由于 $|G_f| = 20$, 以及找到了其两个子群 $\mathbb{Z}/5\mathbb{Z} = \text{Gal}(\mathbb{Q}(\sqrt[5]{2}, \xi_5)/\mathbb{Q}(\xi_5))$ 以及 $\mathbb{Z}/4\mathbb{Z} = \text{Gal}(\mathbb{Q}(\sqrt[5]{2}, \xi_5)/\mathbb{Q}(\sqrt[5]{2}))$, 其中前者还是正规子群, 并且 $\mathbb{Q}(\sqrt[5]{2}) \cap \mathbb{Q}(\xi_5) = \mathbb{Q}$ 意味着这两个子群的交平凡, 从而

$$G_f \cong \mathbb{Z}/5\mathbb{Z} \rtimes \mathbb{Z}/4\mathbb{Z}$$

□

注记. 对于素数 p , 我们有 $x^p - 2$ 的伽罗瓦群 $G_f \cong \mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/(p-1)\mathbb{Z}$.

练习. 对于素数 p , 证明 $f(x) = x^p - 2$ 的伽罗瓦群 G_f 同构于

$$\left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in (\mathbb{Z}/p\mathbb{Z})^\times, b \in \mathbb{Z}/p\mathbb{Z} \right\} \subset \text{GL}(2, \mathbb{Z}/p\mathbb{Z})$$

第五章 伽罗瓦理论的应用

5.1 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 5.1.1. $(a, b) \in \mathbb{R}^2$ 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 5.1.2. (a, b) 可构造当且仅当 $(a, 0), (b, 0)$ 可构造.

定义 5.1.3. $c \in \mathbb{R}$ 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 5.1.4. 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 5.1.5. $K \subseteq \mathbb{R}$ 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 5.1.6. 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 $K(\sqrt{\alpha}), \alpha \in K$ 中的点.
- (3) 两个 K 中的圆的交点要么是空集, 要么是 $K(\sqrt{\alpha}), \alpha \in K$ 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 5.1.7. $c \in \mathcal{C}$ 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 $K_{i+1} = K_i(\sqrt{\alpha_i})$, 其中 $\alpha_i > 0 \in K_i$.

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 $c \in \mathcal{C}$, 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 5.1.6 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 5.1.4, 如果 α, β 可构造, 那么 $\alpha \pm \beta, \alpha\beta$ 都可构造. 由于 a, b 是 1 和 $\sqrt{\alpha_{n-2}}$ 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 $\sqrt{\alpha_{n-3}}$ 的到. 因此问题归结于在 K_{n-2} 上构造 $\sqrt{\alpha_{n-2}}$. 由于 $(\sqrt{\alpha_{n-2}}, 0)$ 是 $x^2 + y^2 = \alpha_{n-2}$ 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. □

5.1.1 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.

5.1.2 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 .

5.1.3 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.

5.1.4 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 5.1.8. 尺规可作正 n 边形等价于 $[\mathbb{Q}(\xi_n) : \mathbb{Q}] = 2^n$.

证明: 令 $\xi_n = \cos \theta_n + \sqrt{-1} \sin \theta_n$, 只需要注意到:

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

即可. □

定理 5.1.9. 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

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

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.

5.2 代数基本定理的证明

命题 5.2.1. 对于任何 p -群 G , 都存在 G_i 使得

$$G \supset G_1 \supset G_2 \supset \dots \supset G_n = \{e\}$$

满足 $|G_i/G_{i+1}| = p$.

定理 5.2.2. 任何 $f(x) \in \mathbb{C}[x]$ 在 \mathbb{C} 中都有根.

证明: 考虑 $f(x)\overline{f(x)} \in \mathbb{R}[x]$, 如果 $f(x)\overline{f(x)}$ 有复根 α , 那么 α 或 $\bar{\alpha}$ 是 $f(x)$ 的一个复根, 从而我们不妨从一开始就假设 $f(x) \in \mathbb{R}[x]$. 记 $|G_f| = n$, 考虑 G_f 的西罗 2-子群 H , 那么 $[G_f : H]$ 是奇数, 从而根据伽罗瓦主定理对应到 \mathbb{R} 的一个奇数次扩域 L , 然而任何奇数次多项式 $f(x) \in \mathbb{R}[x]$ 在 \mathbb{R} 中都有根, 从而 $L = \mathbb{R}$, 再根据伽罗瓦主定理有 $G_f = H$, 即 $|G_f| = 2^n$.

根据命题 5.2.1 可知存在 G_i 使得

$$G_f \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{e\}$$

使得 $|G_i/G_{i+1}| = 2$. 注意到 \mathbb{R} 的任何二次扩张都同构于 \mathbb{C} , 从而 G_1 对应的 \mathbb{R} 的扩域就是 \mathbb{C} , 但是 \mathbb{C} 没有非平凡的二次扩域, 从而 $K_2 = \cdots = K_n = \mathbb{C}$, 从而 $f(x)$ 的分裂域就是 \mathbb{C} , 即 $f(x)$ 有复根. \square

5.3 根式可解问题

在本节中, 所有的域的特征都是 0.

5.3.1 根式扩张与根式可解

定义 5.3.1. 有限扩张 E/F 被称为**根式扩张** (radical extension), 如果存在 $\alpha_1, \dots, \alpha_n \in E, m_1, \dots, m_n \in \mathbb{N}$, 使得:

1. $E = F(\alpha_1, \dots, \alpha_n)$
2. $\alpha_1^{m_1} \in F$, 并且对 $2 \leq i \leq n$ 有 $\alpha_i^{m_i} \in F(\alpha_1, \dots, \alpha_{i-1})$.

即:

$$F \subseteq F(\alpha_1) \subseteq \cdots \subseteq F(\alpha_1, \dots, \alpha_n)$$

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

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

定义 5.3.2. $f(x) \in F[x]$ 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.

命题 5.3.3.

- (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.
- (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, 则其伽罗瓦闭包 K/F 也是根式扩张.

证明: (1). 如果 K/F 是根式扩张, 那么有 $K = F(\alpha_1, \dots, \alpha_n)$, 其中 $\alpha_1, \dots, \alpha_n$ 满足定义里的要求, 那么自然有 $K = E(\alpha_1, \dots, \alpha_n)$, 即 K/E 也是根式扩张.

(2). 如果 $E = F(\alpha_1, \dots, \alpha_n), K = E(\alpha_{n+1}, \dots, \alpha_m)$, 那么 $K = F(\alpha_1, \dots, \alpha_m)$, 即 K/F 是根式扩张.

¹这条性质与正规扩张类似.

(3). 假设 $E = F(\alpha_1, \dots, \alpha_n)$, 那么 $EE' = E'(\alpha_1, \dots, \alpha_n)$, 并且 $\alpha_i^{m_i} \in F(\alpha_1, \dots, \alpha_{i-1}) \subseteq E'(\alpha_1, \dots, \alpha_{i-1})$, 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 $E = F(\alpha_1, \dots, \alpha_n)$, 其中 $\alpha_i^{m_i} \in F(\alpha_1, \dots, \alpha_{i-1})$, 那么 Galois 闭包 K 由所有 $P_{\alpha_i, F}$ 的根生成. 令 $G = \text{Gal}(K/F)$, 任取 $\tau \in G$, 那么 $\tau(E) = F(\tau(\alpha_1), \dots, \tau(\alpha_n))$ 在 F 上也是根式扩张, 因为 $\tau(\alpha_i)^{m_i} = \tau(\alpha_i^{m_i}) \in \tau(F(\alpha_1, \dots, \alpha_{i-1})) = F(\tau(\alpha_1), \dots, \tau(\alpha_{i-1}))$. 从而根据 (3) 有 $K = \prod_{\tau} \tau(E)$ 是根式扩张. \square

5.3.2 可解群及其性质

本节中的群 G 都是有限群.

定义 5.3.4. 群 G 的换位子群 (commutator group), 定义为由形如 $ghg^{-1}h^{-1}$, 其中 $g, h \in G$ 生成的子群, 记作 $[G, G]$.

记号 5.3.5. 给定群 G , 记 $G^{(1)} = [G, G]$, 以及 $G^{(i)} := [G^{(i-1)}, G^{(i-1)}], i \geq 2$.

命题 5.3.6. 给定群 G , 有

1. $[G, G]$ 是 G 的正规子群.
2. $G/[G, G]$ 是阿贝尔群.
3. 对于群同态 $\varphi: G \rightarrow H$, 如果 H 是阿贝尔群, 那么 $[G, G] \subseteq \ker \varphi$.

定义 5.3.7. 群 G 被称为可解群 (solvable group), 如果 $G^{(n)} = \{e\}$ 对某个 $n \in \mathbb{Z}_{>0}$ 成立.

命题 5.3.8. 如果 G 是非交换的单群, 则 G 不是可解群.

证明: 注意到 $G = G^{(1)} = \dots = G^{(n)}$ 对任意 $n \in \mathbb{Z}_{>0}$ 成立, 从而 G 不是可解群. \square

推论 5.3.9. $A_n, n \geq 5$ 时不是可解群.

命题 5.3.10. 如下叙述等价:

1. 群 G 可解.
2. 如果 G 存在一个子群链 $G = G_0 \supset G_1 \supset \dots \supset G_n = \{e\}$, 满足 $G_{i+1} \triangleleft G_i$, 并且 G_i/G_{i+1} 是阿贝尔群.
3. 如果 G 存在一个子群链 $G = G_0 \supset G_1 \supset \dots \supset G_n = \{e\}$, 满足 $G_{i+1} \triangleleft G_i$, 并且 G_i/G_{i+1} 是素数阶循环群.

推论 5.3.11. p -群是可解群.

证明: 根据命题 5.2.1 即可. \square

命题 5.3.12.

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 .

5.3.3 根式可解与可解群

命题 5.3.13. E/F 是有限伽罗瓦根式扩张, 则 $\text{Gal}(E/F)$ 是可解群.

证明: 假设 $E = F(\alpha_1, \dots, \alpha_n)$, 其中 $\alpha_i^{m_i} \in F(\alpha_1, \dots, \alpha_{i-1})$, 我们对 n 做归纳法. 当 $n = 1$ 时, $E = F(\alpha_1)$, 并且 $\alpha_1^{m_1} \in F$, 注意到 $E \subseteq F(\alpha_1, \xi_{m_1})$, 从而根据命题 5.3.12 的 (1) 可知只需要证明 $\text{Gal}(F(\alpha_1, \xi_{m_1})/F)$ 是可解群即可. 考虑下图

$$\begin{array}{c}
 F(\alpha_1, \xi_{m_1}) \\
 \downarrow \\
 F(\xi_{m_1}) \\
 \downarrow \\
 F
 \end{array}$$

由于 $F(\xi_{m_1})$ 是 m_1 次本元多项式的分裂域, 从而 $F(\xi_{m_1})/F$ 是伽罗瓦扩张. 根据伽罗瓦对应, $\text{Gal}(F(\alpha_1, \xi_{m_1})/F(\xi_{m_1}))$ 是 $\text{Gal}(F(\alpha_1, \xi_{m_1})/F)$ 的正规子群, 并且

$$\text{Gal}(F(\xi_{m_1})/F) \cong \text{Gal}(F(\alpha_1, \xi_{m_1})/F) / \text{Gal}(F(\alpha_1, \xi_{m_1})/F(\xi_{m_1}))$$

那么根据命题 5.3.12 的 (3), 我们只需要证明 $\text{Gal}(F(\xi_{m_1})/F)$ 和 $\text{Gal}(F(\alpha_1, \xi_{m_1})/F(\xi_{m_1}))$ 是可解群即可. 考虑如下图

$$\begin{array}{ccc}
 & F(\xi_{m_1}) & \\
 \swarrow & & \searrow \\
 \mathbb{Q}(\xi_{m_1}) & & F \\
 \swarrow & & \searrow \\
 & \mathbb{Q} &
 \end{array}$$

我们有嵌入 $\text{Gal}(F(\xi_{m_1})/F) \hookrightarrow \text{Gal}(\mathbb{Q}(\xi_{m_1})/\mathbb{Q}) \cong (\mathbb{Z}/m_1\mathbb{Z})^\times$, 从而 $\text{Gal}(F(\xi_{m_1})/F)$ 是阿贝尔群, 从而是可解群. 另一方面, 任取 $\tau \in \text{Gal}(F(\alpha_1, \xi_{m_1})/F(\xi_{m_1}))$, τ 完全由其在 α_1 上的值决定, 由于 $x^{m_1} - \alpha_1^{m_1}$ 的所有根是 $\alpha_1 \xi_{m_1}^k$, 其中 $0 \leq k \leq m_1 - 1$, 因此 $\tau(\alpha_1) = \alpha_1 \xi_{m_1}^k$, 并且由于 $\tau(\xi_{m_1}) = \xi_{m_1}$, 从而可知 $\text{Gal}(F(\alpha_1, \xi_{m_1})/F(\xi_{m_1}))$ 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

$$\begin{array}{ccc}
 E = F(\alpha_1)(u_2, \dots, \alpha_n) & \xrightarrow{\quad} & E(\xi_{m_1}) \\
 \downarrow & & \downarrow \\
 F(\alpha_1) & \xrightarrow{\quad} & F(\alpha_1, \xi_{m_1}) \\
 \downarrow & \nearrow & \\
 F & &
 \end{array}$$

首先我们有 $\text{Gal}(F(\alpha_1, \xi_{m_1})/F)$ 是可解群, 并且根据归纳假设 $\text{Gal}(E(\xi_{m_1})/F(\alpha_1, \xi_{m_1}))$ 是可解群, 根据命题 5.3.12 的 (3) 有 $\text{Gal}(E(\xi_{m_1})/F)$ 是可解群, 再根据命题 5.3.12 的 (1) 有 $\text{Gal}(E/F)$ 是可解群. \square

引理 5.3.14 (Kummer). 假设域 F 包含 p 次单位根 ξ_p , 其中 p 是素数. 域扩张 E/F 是 p 次伽罗瓦扩张当且仅当 $E = F(\alpha)$, 其中 $\alpha \notin F, \alpha^p \in F$.

证明: 假设 E/F 是 p 次伽罗瓦扩张, 即 $\text{Gal}(E/F) = \langle \sigma \rangle$ 是一个 p 阶循环群. 将 E 视作 p 维 F -线性空间, $\sigma: E \rightarrow E$ 是 F -线性变换, 满足 $\sigma^p = 1$. 由于 F 含有 ξ_p , 从而 σ 可对角化, 并且特征值为 $\{1, \xi_p, \dots, \xi_p^{p-1}\}$, 考虑 ξ_p 对应的特征向量 α , 那么

$$\sigma(\alpha^i) = \sigma(\alpha)^i = (\xi_p \alpha)^i = \xi_p^i \alpha^i$$

对任意 $0 \leq i \leq p-1$ 成立, 从而 $\{1, \alpha, \dots, \alpha^{p-1}\}$ 构成了一组 E/F 的基, 并且 $\alpha^p \in F$, 从而 α 对应的极小多项式为 $x^p - \alpha^p$, 从而 $E = F(\alpha)$. 另一方面, 假设 $E = F(\alpha)$, $\alpha \notin F$, $\alpha^p \in F$, 那么 E 是 $x^p - \alpha^p$ 的分裂域, 下面只需证明 $[E:F] = p$ 即可: 考虑 $\sigma \in \text{Gal}(E/F)$, 其中 $\sigma(\alpha) = \xi_p \alpha$, 可知 $\text{Gal}(E/F)$ 在 $\{\alpha, \xi_p \alpha, \dots, \xi_p^{p-1} \alpha\}$ 上的作用是可递的, 从而 $x^p - \alpha^p$ 是 α 的极小多项式, 从而 $[E:F] = p$. \square

定理 5.3.15. K/F 是有限伽罗瓦扩张, 并且 $\text{Gal}(K/F)$ 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 $[K:F] \leq n-1, n \geq 2$ 时成立, 考虑如下图

$$\begin{array}{ccccc}
 K & \xrightarrow{\quad} & K(\xi_p) & \xrightarrow{\quad} & L \\
 | & & \downarrow & \nearrow & \\
 F & \xrightarrow{\quad} & F(\xi_p) & &
 \end{array}$$

由于 $\text{Gal}(K/F)$ 是可解群, 根据命题 5.3.12 的 (4) 可知其存在一个指数是素数 p 的正规子群, 我们将 p 次本原单位根 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 $\text{Gal}(K/F)$ 指数为 p 的正规子群. 考虑下图

$$\begin{array}{ccc}
 K(\xi_p) & \xrightarrow{\quad} & L \\
 | & \nearrow & \\
 E & & \\
 | & & \\
 F(\xi_p) & &
 \end{array}$$

由于 H 是正规子群, 从而 $E/F(\xi_p)$ 是次数为 p 的伽罗瓦扩张, 那么根据引理 5.3.14 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. \square

定理 5.3.16. $f(x) \in F[x]$ 根式可解当且仅当 G_f 是可解群.

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 是伽罗瓦的, 因为根据命题 5.3.3 的 (4) 根式扩张的伽罗瓦闭包依然是根式扩张. 根据命

题5.3.13有 $\text{Gal}(K/F)$ 是可解群, 则 $G_f = \text{Gal}(E/F) \hookrightarrow \text{Gal}(K/F)$, 也是一个可解群. 另一方面, 根据定理5.3.15即可. \square

5.4 求根公式

5.4.1 五次及以上方程无求根公式

给定环 R , S_n 在 $R[x_1, \dots, x_n]$ 上有如下的作用

$$\sigma \cdot f(x_1, \dots, x_n) := f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$$

考虑在 S_n 作用下不变的子环 $R[x_1, \dots, x_n]^{S_n}$, 其中的元素称为 R 系数的**对称多项式** (symmetric polynomial).

例子 (初等对称多项式).

$$\begin{aligned} s_1 &= \sum_{i=1}^n x_i \\ s_2 &= \sum_{1 \leq i < j \leq n} x_i x_j \\ &\vdots \\ s_n &= x_1 \cdots x_n \end{aligned}$$

定理 5.4.1 (对称多项式基本定理).

$$\begin{aligned} \varphi: R[y_1, \dots, y_n] &\rightarrow R[x_1, \dots, x_n]^{S_n} \\ g(y_1, \dots, y_n) &\mapsto g(s_1, \dots, s_n) \end{aligned}$$

则 φ 是环同构.

证明: φ 是满射: 任取 $f \in R[x_1, \dots, x_n]^{S_n}$, 那么 $f(x_1, \dots, x_{n-1}, 0) \in R[x_1, \dots, x_{n-1}]^{S_{n-1}}$, 根据归纳假设存在 $n-1$ 元多项式 g 使得

$$f(x_1, \dots, x_{n-1}, 0) = g(x_1, \dots, x_{n-1})$$

令 $h(x_1, \dots, x_n) = f(x_1, \dots, x_n) - g(s_1, \dots, s_{n-1})$, 如果 $h \equiv 0$, 那么证明结束. 如果 $h \neq 0$, 根据构造有 $h(x_1, \dots, x_{n-1}, 0) = 0$, 即 x_n 整除 $h(x_1, \dots, x_n)$, 并且注意到 $h(x_1, \dots, x_n)$ 是 S_n 不变的, 从而任取 $1 \leq i \leq n$, 都有 $x_i \mid h(x_1, \dots, x_n)$, 因此不妨假设

$$h(x_1, \dots, x_n) = x_1 \cdots x_n H(x_1, \dots, x_n)$$

此时 $\deg H < \deg h$, 再对次数做归纳则可知 $H(x_1, \dots, x_n)$ 是初等对称多项式的组合, 从而 $h(x_1, \dots, x_n)$ 也是.

φ 是单射: 假设 $\varphi(g) = 0$, 即 $g(s_1, \dots, s_n) = 0$, 特别地有 $g(s_1, \dots, s_{n-1}, 0) = 0$. 根据归纳假设有 $g(y_1, \dots, y_{n-1}, 0) = 0$, 从而 $y_n \mid g(y_1, \dots, y_n)$, 不妨假设

$$g(y_1, \dots, y_n) = y_n h(y_1, \dots, y_n)$$

利用 $\varphi(g) = 0$ 有

$$x_1 \dots x_n \varphi(h) = 0$$

即 $\varphi(h) = 0$, 并且 $\deg h < \deg g$, 再对次数做归纳即可. \square

推论 5.4.2.

$$F(y_1, \dots, y_n) \cong F(x_1, \dots, x_n)^{S_n}$$

是域同构.

证明: 首先 $\varphi: F[x_1, \dots, x_n] \rightarrow F[x_1, \dots, x_n]^{S_n}$ 给出了分式域之间的同态

$$\begin{aligned} \varphi: F(y_1, \dots, y_n) &\rightarrow F(x_1, \dots, x_n)^{S_n} \\ \frac{f(y_1, \dots, y_n)}{g(y_1, \dots, y_n)} &\mapsto \frac{f(s_1, \dots, s_n)}{g(s_1, \dots, s_n)} \end{aligned}$$

下面只需要证明是满射: 任取 $\tau = \frac{f(x_1, \dots, x_n)}{g(x_1, \dots, x_n)} \in F(x_1, \dots, x_n)^{S_n}$, 考虑

$$r = \frac{f(x_1, \dots, x_n) \prod_{\sigma \in S_n \setminus \{\text{id}\}} \sigma g}{\prod_{\sigma \in S_n} \sigma g}$$

由于 $\prod_{\sigma \in S_n} \sigma g$ 以及 r 都在 $F(x_1, \dots, x_n)^{S_n}$ 中, 从而

$$r \prod_{\sigma \in S_n} \sigma g \in F[x_1, \dots, x_n] \cap F(x_1, \dots, x_n)^{S_n} = F[x_1, \dots, x_n]^{S_n}$$

\square

令 $K = F(x_1, \dots, x_n)$ 以及 $S_n \subset \text{Aut}_F(K)$, 那么 $K^{S_n} = F(s_1, \dots, s_n)$ 并且 K/K^{S_n} 是伽罗瓦扩张, 并且实际上 K 是

$$x^n - s_1 x^{n-1} + \dots + (-1)^n s_n = 0$$

的分裂域. 即我们找到了一个多项式 $f(x)$, 使得其伽罗瓦群 $G_f = S_n$. 由于我们知道 A_n 在 $n \geq 5$ 的时候不可解, 从而 S_n 在 $n \geq 5$ 的时候不可解, 即不存在五次及以上的多项式的求根公式.

注记. 对于素数 p , 伽罗瓦群为 S_p 的多项式的存在性更容易一些.

定理 5.4.3. p 是素数, f 是 \mathbb{Q} 上恰有两个虚根的不可约 p 次多项式, 则 $G_f \cong S_p$.

证明: 首先复共轭 $c: a + b\sqrt{-1} \mapsto a - b\sqrt{-1}$ 属于 G_f , 对应于一个对换. 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. 根据引理 4.3.5 可知 $G_f \cong S_p$. \square

5.4.2 低次方程求根公式

给定三次多项式 $x^3 - s_1x^2 + s_2x - s_3$, 有伽罗瓦对应如下

$$\begin{array}{ccc}
 K = F(x_1, x_2, x_3) & & \{\text{id}\} \\
 | & & | \\
 L & & A_3 \\
 | & & | \\
 E = F(s_1, s_2, s_3) & & S_3
 \end{array}$$

即 L 是 K 的 A_3 不变子域. 令

$$D = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$$

注意到 D 在 A_3 下不变, 并且 $[E(\sqrt{D}) : E] = [L : E] = 2$, 从而有 $L = E(\sqrt{D})$. 取 $\sigma \in A_3 = \text{Gal}(K/L)$, 其中

$$\sigma(x_1) = x_2$$

$$\sigma(x_2) = x_3$$

$$\sigma(x_3) = x_1$$

假设 F 中有三次单位根 ξ_3 , 考虑

$$t_1 = x_1 + \xi_3 x_2 + \xi_3^2 x_3$$

$$t_2 = x_2 + \xi_3 x_3 + \xi_3^2 x_1$$

直接验证则有 $t_1^3, t_2^3 \in E(\sqrt{D})$, 如果我们将 t_1^3, t_2^3 用 \sqrt{D} 以及 s_1, s_2, s_3 表示出来, 并注意到 \sqrt{D} 可以写成 s_1, s_2, s_3 的组合, 因此我们可以给出三次方程的求根公式.

注记. 四次方程的求根公式也可由上述步骤给出.

5.5 Kummer 理论

在本节中², 域 F 总是满足如下两条假设:

- (1) F 包含 n 次本原单位根 ξ_n , 并用 μ_n 表示全体单位根组成的群.
- (2) $x^n - 1$ 在 F 中有 n 个不同的根.

引理 5.5.1. 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 $P_{\alpha, F} = x^m - b, b \in F$ 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 $\alpha^{nm} = b^n$, 即 $a^m/b \in \mu_n \subseteq F$. 由于 $b \in F^\times$ 我们有 $\alpha^m \in F^\times$, 因此 $P_{\alpha, F} \mid x^m - b$, 下面只需要证明 $\deg P_{\alpha, F} = m$ 即可. 不妨记 $\deg P_{\alpha, F} = d$, 由于 $P(x) = \prod_{i=0}^{n-1} (x - \alpha \xi_n^i)$, 因此 $P_{\alpha, F} = \prod_{i \in S} (x - \alpha \xi_n^i)$, 其中 $|S| = d$. 将 $P_{\alpha, F}$ 展开, 考虑其常数项则有 $\alpha^d \xi_n^i \in F \implies \alpha^d \in F$. 因此:

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

²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.

因此 $m \mid d$, 再加上 $d \leq m$, 从而有 $m = d$. □

命题 5.5.2. $E = F(\alpha)$, 其中 $\alpha^n = a \in F^\times$, 则 E/F 是 m 次循环扩张, 其中 m 是 a 在 $F^\times/(F^\times)^n$ 中的阶数.

证明: 首先引理 5.5.1 可知 E/F 的扩张次数就是 m . 由于 $x^n - a$ 的所有根是 $\{\alpha \xi_n^i \mid 0 \leq i \leq n-1\}$ 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, 根据定理 3.2.9 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 3.1.2 可知 E 是正规扩张, 从而 E/F 是伽罗瓦扩张. 最后我们来证明其为循环扩张: 考虑映射

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

这定义了一个群同态, 因为:

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

并且是单射, 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 4.2.1, 即伽罗瓦对应可知 $\sigma = \text{id}$. 因此 $\text{Gal}(E/F)$ 嵌入到循环群 μ_n 中, 也是一个循环群. □

引理 5.5.3 (Dedekind). 给定群 G 以及域 F , 互不相同的群同态 $\sigma_1, \dots, \sigma_n: G \rightarrow F^\times$ 是 E -线性无关的, 即如果 $a_1, \dots, a_n \in E$ 使得

$$\sum_{i=1}^n a_i \sigma_i = 0$$

则 $a_1 = \dots = a_n = 0$.

证明: 我们对 n 做归纳. $\sigma_1 \neq \sigma_2$ 意味着存在 $h \in G$ 使得 $\sigma_1(h) \neq \sigma_2(h)$. 由 $\sum_{i=1}^n a_i \sigma_i = 0$ 可知

$$\sum_{i=1}^n a_i \sigma_i(h) \sigma_i(g) = 0$$

对任意的 $g \in G$ 成立, 即 $\sum_{i=1}^n a_i \sigma_i(h) \sigma_i = 0$, 则

$$\begin{aligned} 0 &= \sigma_1(h) \sum_{i=1}^n a_i \sigma_i - \sum_{i=1}^n a_i \sigma_i(h) \sigma_i \\ &= \sum_{i=2}^n a_i (\sigma_1(h) - \sigma_i(h)) \sigma_i \end{aligned}$$

根据归纳假设有 $a_i (\sigma_1(h) - \sigma_i(h)) = 0$ 对任意的 $2 \leq i \leq n$ 成立, 根据 h 的选取有 $a_2 = 0$, 再利用归纳假设即可. □

定理 5.5.4 (Kummer). 给定有限伽罗瓦扩张 E/F , 其伽罗瓦群为 n 阶循环群 $\langle \sigma \rangle$, 则 $E = F(\alpha)$, $\alpha^n \in F^\times$.

证明: 根据引理5.5.3存在 $\gamma \in F^\times$ 使得

$$\alpha := \sum_{i=0}^{n-1} \xi_n^i \sigma_i(\gamma) \neq 0$$

从而 $\sigma(\alpha) = \xi_n^{-1} \alpha$, 进而 $\sigma(\alpha^n) = \alpha^n$. 下面说明 $E = F(\alpha)$, 只需要证明 $\text{Gal}(E/F(\alpha)) = \{\text{id}\}$. 如果存在 $\tau = \sigma^k \in \text{Gal}(E/F(\alpha))$, 则 $\tau(\alpha) = \sigma^k(\alpha) = \xi_n^k \alpha$, 那么 $\xi_n^k = 1$, 而 ξ_n 是本原单位根, 因此 $k = n$, 因此 $\tau = \text{id}$. \square

推论 5.5.5.

$$\{F \text{ 的 } \mathbb{Z}/n\mathbb{Z} \text{ 扩张}\} \xrightarrow{1-1} \{a \in F^\times / (F^\times)^n, \text{ 其中 } a \text{ 的阶数为 } n\}$$

证明: 命题5.5.2给出了从左往右的对应, 定理 5.5.4 说明这个对应是满射, 现在只需证明对应是单射: 假设 $F(\alpha) = F(\beta)$ 是 F 的两个 $\mathbb{Z}/n\mathbb{Z}$ 扩张, 其中 $\alpha^n = a \in F^\times, \beta^n = b \in F^\times$, 我们要证明 a, b 在 $F^\times / (F^\times)^n$ 中的阶数相同. 根据命题5.5.2的证明过程, 我们可以定义映射:

$$\begin{aligned}\varphi_\alpha(\sigma) &= \frac{\sigma(\alpha)}{\alpha} \\ \varphi_\beta(\sigma) &= \frac{\sigma(\beta)}{\beta}\end{aligned}$$

并且由构造可知 $\frac{\sigma(\alpha)}{\alpha}, \frac{\sigma(\beta)}{\beta}$ 都是 n 次本原单位根, 因此存在整数 k 满足 $(k, n) = 1$ 使得

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

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

定义 5.5.6. n 次扩张 E/F 被称为 **Kummer 扩张** (Kummer extension), 如果其为一个阿贝尔扩张, 并且其伽罗瓦群 $\text{Gal}(E/F)$ 的指数³整除 n .

定理 5.5.7. E/F 是 Kummer 扩张, 当且仅当 $E = F(\sqrt[n]{a_1}, \dots, \sqrt[n]{a_r}), a_i \in F^\times$.

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

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

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:

$$\text{Gal}(E/F) \cong C_1 \times \dots \times C_r$$

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 $\text{Gal}(K_j/F) \cong C_i$, 因此 $K_j = F(\sqrt[n]{a_i})$, 下面只需要说明 $K = K_1 \dots K_r$ 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. \square

³exponent, 指群中所有元素阶的最小公倍数.

引理 5.5.8. K/F 是有限伽罗瓦扩张, 其伽罗瓦群为 $G = G_1 \times \cdots \times G_r$, 则 $K = K_1 \cdots K_r$, 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 $K_1/F, K_2/F$ 都是伽罗瓦扩张, 则 $[K_1 K_2 : K_2] = [K_1 : K_1 \cap K_2]$, 而这里 $K_1 \cap K_2 = F$, 因此 $[K_1 K_2 : F] = [K_1 : F][K_2 : F] = |H_1||H_2| = |G|$, 因此 $K = F_1 F_2$. \square

5.6 正规基定理

定理 5.6.1 (正规基定理). 给定有限伽罗瓦扩张 E/F , 则存在 E/F 的一族正规基, 即存在 $\alpha \in E^\times$, 使得 $\{\sigma(\alpha) \mid \sigma \in \text{Gal}(E/F)\}$ 构成了 E/F 的一族基.

证明: \square



第六章 伽罗瓦上同调与希尔伯特 90

6.1 范与迹

定义 6.1.1. 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

$$N_{E/F}(\alpha) = \det(m_\alpha)$$

其**迹** (trace) 定义为

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

命题 6.1.2.

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

$$N_{E/F}(\alpha) = \alpha^{[E:F]}$$

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

证明: 线性代数. □

引理 6.1.3. 如果 $F \subseteq E \subseteq K, \alpha \in E$, 则

$$N_{K/F}(\alpha) = N_{E/F}(\alpha)^{[K:E]}$$

$$\text{Tr}_{K/F}(\alpha) = [K:E] \text{Tr}_{E/F}(\alpha)$$

证明: 假设 $\{x_1, \dots, x_n\}$ 是 E/F 的一组基, $\{y_1, \dots, y_n\}$ 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

$$\alpha \begin{pmatrix} x_1 y_1 \\ x_2 y_1 \\ \vdots \\ x_n y_1 \\ x_1 y_2 \\ x_2 y_2 \\ \vdots \\ x_n y_2 \\ \vdots \\ x_n y_m \end{pmatrix} = \begin{pmatrix} A & & \\ & A & \\ & & \ddots \\ & & & A \end{pmatrix} \begin{pmatrix} x_1 y_1 \\ x_2 y_1 \\ \vdots \\ x_n y_1 \\ x_1 y_2 \\ x_2 y_2 \\ \vdots \\ x_n y_2 \\ \vdots \\ x_n y_m \end{pmatrix}$$

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

注记. 实际上, 上述引理是如下传递性的特殊情况.

$$N_{K/F} = N_{K/E} \circ N_{E/F}$$

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

引理 6.1.4. 给定 $E = F(\alpha)$, 如果 $P_{\alpha,F}(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, 则

$$N_{E/F}(\alpha) = (-1)^n a_0$$

$$\text{Tr}_{E/F}(\alpha) = -a_{n-1}$$

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

命题 6.1.5. 如果 E/F 是有限扩张, 任取 $\alpha \in K$, 则

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

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

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6.1.3有:

$$N_{E/F}(\alpha) = N_{F(\alpha)/F}(\alpha)^{[E:F(\alpha)]}$$

而考虑满射:

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

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

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

¹见定义3.3.6.

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

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

即单扩张的情形, 而根据引理6.1.4直接可以得到想要的结果. \square

推论 6.1.6. E/F 是有限扩张, 则 E/F 可分当且仅当 $\text{Tr}_{E/F}$ 是满射, 这也当且仅当 $\text{Tr}_{E/F}$ 是非零映射.

证明: 根据线性代数的知识, $\text{Tr}_{E/F}$ 非零当且仅当其为满射是显然的. 如果 E/F 不可分, 假设 $\text{char } F = p$, 则根据命题6.1.5可知 $\text{Tr}_{E/F}(\alpha)$ 中含有 $[K : F]_i$ 作为因子, 然而其为 p 的幂次, 因此 $\text{Tr}_{E/F}(\alpha)$ 恒为零映射. 另一方面, 如果 E/F 是可分的, 需要证明 $\text{Tr}_{E/F}$ 不是零映射, 这只需要寻找 α 使得:

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

\square

命题 6.1.7. E/F 是有限域上的有限扩张, 则 $N_{E/F}, \text{Tr}_{E/F}$ 都是满射.

证明: 不妨记 $E = \mathbb{F}_{q^d}, F = \mathbb{F}_q$. 根据推论6.1.6可知 $\text{Tr}_{E/F}$ 是满射, 因为有限域上的扩张都是可分的. 另一方面, 注意到 $N_{E/F}$ 是可乘的, 并且 E^\times 是循环群, 因此我们只需要考虑 $N_{E/F}$ 在 x 上的取值即可:

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

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 $N_{E/F}$ 也是满射. \square

注记. 希尔伯特 90 问题断言: 如果 $\text{Gal}(E/F) = \langle \sigma \rangle$ 是一个循环群, $\alpha \in E$ 满足其范数为 1, 则 $\alpha = \frac{\sigma(\beta)}{\beta}$, 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6.1.7中的记号, 如果 $\alpha = x^k$ 满足范数为 1, 则由于可乘性:

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

因此 $q-1 \mid k$, 不妨记作 $k = (q-1)r$, 则

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

6.2 伽罗瓦上同调

定义 6.2.1. 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 $\mu: G \times A \rightarrow A$ 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, 但这并不关键. 之后可能会根据情况需要而调整, 请读者留心.

例子. 给定有限伽罗瓦扩张 E/F , 令 $G = \text{Gal}(E/F)$, 则 $G \curvearrowright (E, +), G \curvearrowright (E^\times, \times)$ 都是 G 模.

定义 6.2.2. 给定有限群 G 和群 A , 定义

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

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

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

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:

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

例子. 当 $n = 0$ 时, $H^0(G, A) = \ker d^0$. 若 $a \in \ker d^0$, 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:

$$d^1 f(g_1, g_2) = g_1 f(g_2) - f(g_1 g_2) + f(g_2)$$

因此:

$$\ker d^1 = \{f: G \rightarrow A \mid f(g_1 g_2) = f(g_1) + g_1 f(g_2)\}$$

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

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

注记. 如果 $f: G \rightarrow A$ 是一个交错同态, 则下面的观察:

(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 $A \rightarrow A^G = \{a \in A \mid ga = a\}$ 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 $f: G \rightarrow A$.

定理 6.2.3 (Hilbert 90). 给定有限伽罗瓦扩张 E/F , 则

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

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

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 $f: G \rightarrow E^\times$ 是交错同态, 那么任取 $\tau \in G, f(\tau) \neq 0$, 根据引理 4.1.7 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 $\text{im } d^0$ 中, 即上同调群平凡.

现在来证明加法版本: 令 $f: G \rightarrow E$ 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 4.1.7 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 $\text{Tr}_{E/F}(b) \neq 0$, 并且根据推论 6.1.6, 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 $\text{Tr}_{E/F}(a + b) = 0$, 那么 $\text{Tr}_{E/F}(a) \neq 0$; 如果 $\mu(a + b) \neq 0$ 并且 $\text{Tr}_{E/F}(a + b) \neq 0$, 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 $\text{Tr}_{E/F}(a) \neq 0$, 令 $\beta = \mu(a)$, 那么

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

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

定理 6.2.4 (Hilbert 90). 给定有限伽罗瓦扩张 E/F , 并且 $G = \text{Gal}(E/F) = \langle \sigma \rangle$ 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

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

考虑 $f: G \rightarrow K$, 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 6.2.3 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 6.2.5. 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 $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$, 取 $a + b\sqrt{-1} \in \mathbb{Q}(\sqrt{-1})$ 满足范数为 1, 则存在 $c + d\sqrt{-1}$ 使得:

$$a + b\sqrt{-1} = \frac{c - d\sqrt{-1}}{c + d\sqrt{-1}}$$

实部虚部对应即可. □

³这里用到了 α 的迹为零这个条件.



索引

- K 中的圆, circle of K , 28
- K 中的平面, plane of K , 28
- K 中的直线, line of K , 28
- n 次分圆多项式, n -th cyclotomic polynomial, 26
- n 次本原单位根, n -th primitive root of unity, 26
- Galois 闭包, Galois closure, 19
- Kummer 扩张, Kummer extension, 39
- 不可分次数, inseparable degree, 17
- 交错同态, crossed homomorphism, 44
- 代数, algebraic, 6
- 代数扩张, algebraic extension, 6
- 代数闭包, algebraic closure, 11
- 代数闭域, algebraic closed field, 10
- 伽罗瓦扩张, Galois extension, 19
- 分裂, split, 8
- 分裂域, splitting field, 8
- 单扩张, simple extension, 5
- 单根式扩张, simple radical extension, 31
- 可分元, separable element, 15
- 可分多项式, separable polynomial, 15
- 可分扩张, separable extension, 15
- 可分次数, separable degree, 17
- 可构造的, constructable, 28
- 可解群, solvable group, 32
- 可递地, transitively, 24
- 域, field, 4
- 域扩张, field extension, 4
- 域扩张之间的同构, isomorphism between field extensions, 4
- 域扩张之间的态射, morphism between field extensions, 4
- 域扩张的复合, composition of field extension, 5
- 域扩张的次数, degree of field extension, 5
- 完美域, perfect field, 16
- 对称多项式, symmetric polynomial, 35
- 弗罗贝尼乌斯映射, Frobenius map, 10
- 形式导数, formal derivative, 14
- 循环扩张, cyclic extension, 23
- 忠实地, faithfully, 24
- 态射, morphism, 44
- 换位子群, commutator group, 32
- 无限扩张, infinite extension, 5
- 有限域, finite field, 9
- 有限扩张, finite extension, 5
- 极小多项式, minimal polynomial, 6
- 根式可解, solvable by radical, 31
- 根式扩张, radical extension, 31
- 模, module, 43
- 正规扩张, 13
- 特征, characteristic, 4
- 纯不可分, purely inseparable, 17
- 纯不可分扩张, purely inseparable extension, 17
- 群的上同调, group cohomology, 44
- 范数, norm, 41

超越, transcendental, 6

迹, trace, 41

超越扩张, transcendental extension, 6

阿贝尔扩张, abelian extension, 23

