

代数 2 H 课程讲义



Instructor: 余成龙
Notes Taker: 刘博文

Qiuuzhen College, Tsinghua University
2022 Fall



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	5
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	16
第四章 伽罗瓦理论	18
4.1 伽罗瓦扩张	18

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 .

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), 并且显然对于域来说, 其特征为素数.

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, 假设有域同态 $\tau: E \rightarrow F$, 那么如果 τ 不是零映射, 那么 τ 一定是单射, 从而我们不妨将 E 视作包含在 F 中, 这引出了下面的概念.

定义 1.1.3. 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), 记做 E/F .

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

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

都给出了这样的映射.

定义 1.1.4. 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

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

记号 1.1.5. 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 1.1.6. 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 1.1.7. 给定域扩张 E/F , 扩张的**次数** (degree) 定义为 $[E : F] = \dim_F E$.

命题 1.1.8. 对于域扩张 $F \subseteq E \subseteq K$, 则 $[K : F] = [K : E][E : F]$.

定义 1.1.9. 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. $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}/\mathbb{Q}$ 是二次扩张.

定义 1.1.10. 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).

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 1.1.11. 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 1.1.12. 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 1.1.13. 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 $x + (p_1(x))$. □

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), 通常记做 $P_{\alpha,F}$.

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 α 在 F 上代数当且仅当 $\ker \theta_\alpha \neq 0$; 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 $[F(\alpha):F] = \deg p(x)$.

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, $p(x)$ 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 $\deg p(x)$.

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 , 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.

证明: 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. \square

注记. 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.

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. \square



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 $p(x)$ 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 1.1.13, 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

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

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做 \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 , 并且是 \mathbb{F}_p 的有限扩张, 如果扩张次数为 n 的话, \mathbb{F}_q 是 \mathbb{F}_p 上的 n 维线性空间, 并且 $q = p^n$.

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

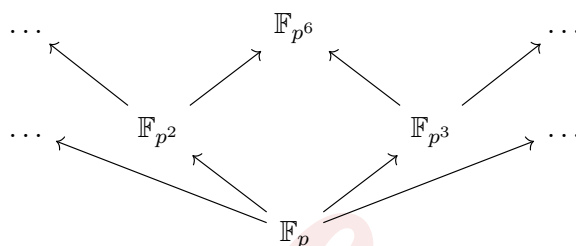
定义 2.3.3. 域扩张 E/F 中 E 被称为 F 的**代数闭包** (algebraic closure), 如果 E/F 是代数扩张, E 是代数闭域.

例子 ($\bar{\mathbb{Q}}$ 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 $\bar{\mathbb{Q}}$.

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



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

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 上的极小多项式记做 $P_{\alpha,F}$, 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 \bar{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

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

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 $f(x) = a_n x^n + \cdots + a_0 \in \bar{F}[x]$, 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 2.3.5 即可. \square

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, $\bar{F} = F(\sqrt{-1})$.

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. 二次扩张总是正规扩张.

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 $[E : F(\alpha_1)] < [E : F]$, 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 的根, 因此 $\tau(\alpha_i) \in E$, 即 $\tau(E) \subseteq E$.

□

推论 3.1.3. 给定域扩张 $F \subseteq E \subseteq K$, 如果 K/F 是正规扩张, 那么 K/E 也是正规扩张.

证明: 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.

□

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), 如果其在 \bar{F} 中不存在重根.

定义 3.2.7. 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 3.2.8. 域扩张 E/F 被称为**可分扩张** (separable 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 可分.
- (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.

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 上的极小多项式记做 $P_{\alpha, E}(x) = a_n x^n + \dots + a_0$. 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

命题 3.2.12. 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 3.2.13. 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 3.2.14. 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 3.2.15.

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

证明: (1) 和 (2) 根据命题3.2.12以及命题3.2.13即可. 对于 (3), 弗罗贝尼乌斯映射给出了 $F^p = F$. \square

命题 3.2.16. 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 3.2.17. 如果 $\text{char } F = 0$, 则任何代数扩张 E/F 是可分扩张.

推论 3.2.18. $\mathbb{F}_{p^n}/\mathbb{F}_p$ 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做 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** (pure 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** (pure 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. E/F 是有限扩张, 那么:

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

特别地, 等号取得当且仅当 E/F 是可分扩张.

证明: 首先我们证明有如下——对应:

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

通过 $\tau \mapsto \tau|_{K_s}$ 给出. 对应是满射可根据命题 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 $\tau(u^{p^m}) = \tau(u)^{p^m} = v \in \bar{F}$, 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 $|\text{Hom}_F(K, \bar{F})| = [K : F]$ 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 $\tau : F(u) \rightarrow \bar{F}$ 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, 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:

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

\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), 如果其是正规扩张, 且是可分扩张.

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 Galois 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 α_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, 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4.1.7, 即阿廷引理. \square

引理 4.1.6. 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 4.1.7 (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 $u \in K$, 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 是伽罗瓦扩张.

现在来证明 $[K:E] \leq |H|$: 只需要证明任取 $u_1, \dots, u_{n+1} \in K$, 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 $c_1, \dots, c_{n+1} \in K$, 且不全为零使得:

$$c_1 \begin{pmatrix} \tau_1(u_1) \\ \tau_2(u_1) \\ \vdots \\ \tau_n(u_1) \end{pmatrix} + c_2 \begin{pmatrix} \tau_1(u_2) \\ \tau_2(u_2) \\ \vdots \\ \tau_n(u_2) \end{pmatrix} + \dots + c_{n+1} \begin{pmatrix} \tau_1(u_{n+1}) \\ \tau_2(u_{n+1}) \\ \vdots \\ \tau_n(u_{n+1}) \end{pmatrix} = 0 \quad (4.1.3)$$



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:

$$u_1 + c_2 u_2 + \dots + c_r u_r = 0 \quad (4.1.4)$$

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

$$\tau_j(u_1) + \tau_j(c_2)\tau_j(u_2) + \dots + \tau_j(c_r)\tau_j(u_r) = 0 \quad (4.1.5)$$

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

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

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

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

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

$$\begin{cases} \xi_1 \tau_1(c_1 x_1) + \dots + \xi_n \tau_n(c_1 x_1) = 0 \\ \vdots \\ \xi_1 \tau_1(c_r x_r) + \dots + \xi_n \tau_n(c_r x_r) = 0 \end{cases}$$

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4.1.6可知 $\xi_i = 0$, 相矛盾! \square



索引

- Galois 闭包, Galois closure, 18
- 不可分次数, inseparable degree, 16, 17
- 代数, algebraic, 5
- 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, 18
- 分裂, split, 8
- 分裂域, splitting field, 8
- 单扩张, simple extension, 5
- 可分元, separable element, 14
- 可分多项式, separable polynomial, 14
- 可分扩张, separable extension, 15
- 可分次数, separable degree, 16, 17
- 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
- 域扩张的次数, degree of field extension, 4
- 完美域, perfect field, 16
- 弗罗贝尼乌斯映射, Frobenius map, 10
- 形式导数, formal derivative, 14
- 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
- 正规扩张, 13
- 特征, characteristic, 4
- 纯不可分, pure inseparable, 16
- 纯不可分扩张, pure inseparable extension, 16
- 超越, transcendental, 5
- 超越扩张, transcendental extension, 6