域论与 Galois 理论基础笔记

整理自课程板书

2026 年 1 月 8 日

目录

1 域扩张的基本概念 (Field Extensions)

本章导读

本节介绍了代数结构层级（整环 vs 域），以及域扩张的基本术语。这是 Galois 理论研究大域与子域之间对称性结构的基石。

1.1 域与子域

定义 1.1 (域扩张). 设 k, L 为域。

- 若 $k \subseteq L$，称 k 是 L 的**子域** *(Subfield)*，L 是 k 的**扩域** *(Extension Field)*。
- 这种关系记作 L/k *(读作"L over k")*。
- 若存在 $k \subseteq E \subseteq L$，则称 E 为该扩张的**中间域** *(Intermediate Field)*。

例 1.2. 经典的数域扩张链：

$$\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

其中 $\mathbb{Z}$ 仅为整环（*Integral Domain*），而 $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ 均为域。

1.2 生成子域：$k[S]$ 与 $k(S)$ 的区别

设 L/k 为域扩张，$S \subseteq L$ 为子集。我们需要区分“环扩张”与“域扩张”：

- **环扩张** $k[S]$：
$$k[S] = \{f(s_1, \ldots, s_n) \mid s_i \in S, f \in k[x_1, \ldots, x_n]\}$$
这是包含 k 和 S 的最小**子环**。元素形式为多项式。
- **域扩张** $k(S)$：
$$k(S) = \left\{ \frac{f(s_1, \ldots, s_n)}{g(s_1, \ldots, s_n)} \;\middle|\; s_i \in S, g(\ldots) \neq 0 \right\}$$
这是包含 k 和 S 的最小**子域**。元素形式为有理函数（分式）。

直观理解：为什么要有圆括号和方括号之分？

方括号 $k[\alpha]$ 代表多项式环，运算只有加减乘；圆括号 $k(\alpha)$ 代表域，增加了除法运算（分式域）。在代数扩张中，它们经常相等，但在超越扩张中则截然不同。

2 代数元与单扩张 (Algebraic Elements & Simple Extensions)

2.1 代数元与超越元

设 L/k 为域扩张，取 $\alpha \in L$。

定义 2.1.

- **代数元 *(Algebraic)*：** 若存在非零多项式 $f(x) \in k[x]$ 使得 $f(\alpha) = 0$。
- **超越元 *(Transcendental)*：** 若 α 不是 k 上的代数元（即不满足任何整系数代数方程）。

例 2.2.

- $\sqrt{2}$ 在 $\mathbb{Q}$ 上是代数的（满足 $x^2 - 2 = 0$）。
- π, e 在 $\mathbb{Q}$ 上是超越的。

命题 2.3 (代数闭包). *L 中所有在 k 上代数的元素构成一个中间域，称为 k 在 L 中的* **代数闭包**。

2.2 单扩张的结构定理

考虑只添加一个元素生成的扩域 $k(\alpha)$，称为**单扩张**。

2.2.1 情况 1: α 是超越元

此时 α 表现得像一个变量 x。

$$k[\alpha] \cong k[x] \quad (\text{多项式环}), \qquad k(\alpha) \cong k(x) \quad (\text{有理函数域})$$

这是一个无限扩张。

2.2.2 情况 2: α 是代数元

此时存在唯一的首一不可约多项式 $f_0(x) \in k[x]$ 使得 $f_0(\alpha) = 0$，称为**极小多项式**。

定理 2.4 (代数单扩张结构). *若 α 在 k 上代数，则：*

1. **环即是域：** $k(\alpha) = k[\alpha]$。
2. **同构定理：** $k(\alpha) \cong k[x]/(f_0(x))$。

3. **维数：** $\dim_k k(\alpha) = \deg(f_0)$。

4. **基底：** $\{1, \alpha, \alpha^2, \ldots, \alpha^{d-1}\}$ 构成一组基。

直观理解：为什么环等于域？

在 $k[\alpha]$ 中，如何求逆元？利用 $f_0(x)$ 的不可约性。对任意 $\beta = g(\alpha) \neq 0$，由于 $f_0 \nmid g$，故 $\gcd(f_0, g) = 1$。根据裴蜀定理，存在 $u(x), v(x)$ 使得：

$$u(x)f_0(x) + v(x)g(x) = 1$$

代入 $x = \alpha$，得 $0 + v(\alpha)\beta = 1$。故 $\beta^{-1} = v(\alpha) \in k[\alpha]$。

3 扩张次数与塔公式 (Degree & Tower Law)

定义 3.1 (扩张次数). 域扩张 L/k 的次数定义为 L 作为 k-向量空间的维数：

$$[L : k] := \dim_k L$$

定理 3.2 (塔公式 / 乘法公式). 设 $k \subseteq E \subseteq L$。则：

$$[L : k] = [L : E] \cdot [E : k]$$

特别地，L/k 是有限扩张 $\iff$ L/E 和 E/k 均为有限扩张。

推论 3.3. 有限扩张一定是代数扩张。

4 分裂域与代数封闭 (Splitting Fields)

我们如何保证方程一定有解？答案是构造扩域。

4.1 Kronecker 定理

定理 4.1 (根的存在性). 设 k 为域，$f(x) \in k[x]$ 为非常数多项式。则存在扩域 L/k，使得 $f(x)$ 在 L 中至少有一个根。

证明. 设 $p(x)$ 是 $f(x)$ 的一个不可约因式。考虑商环 $L = k[x]/(p(x))$。

1. 由于 $p(x)$ 不可约，生成的理想 $(p(x))$ 是极大理想，故 L 是一个域。

2. 存在自然嵌入 $k \hookrightarrow L$，即将 $a \in k$ 映射为陪集 $a + (p(x))$。因此 L 可视为 k 的扩域。

3. 令 $\alpha = \bar{x} = x + (p(x))$。在 L 中计算 $f(\alpha)$，实际上等于 $f(x) \pmod{p(x)}$。因为 $p(x) \mid f(x)$，所以 $f(\alpha) = 0$。

即 α 是 $f(x)$ 在 L 中的一个根。 □

4.2 分裂域 (Splitting Fields)

定义 4.2. 设 $f(x) \in k[x]$。称域扩张 M/k 为 $f(x)$ 的**分裂域**，如果满足：

1. **全部分裂**：$f(x)$ 在 $M[x]$ 中可以分解为一次因式的乘积：

$$f(x) = c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n), \quad \alpha_i \in M$$

2. **极小性**：$M = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$。

4.2.1 存在性与唯一性证明

定理 4.3 (分裂域的存在性). 对任意 $f(x) \in k[x]$，存在 $f(x)$ 在 k 上的分裂域。

证明. 对 $f(x)$ 的次数 n 进行数学归纳。

- 当 $n = 1$ 时，$f(x)$ 已经在 k 中分裂，取 $M = k$ 即可。
- 假设对于次数小于 n 的多项式结论成立。
- 对次数为 n 的 $f(x)$，根据 Kronecker 定理，存在扩域 K_1，使得 $f(x)$ 在 K_1 中有一个根 α_1。
- 在 $K_1[x]$ 中，有 $f(x) = (x - \alpha_1)g(x)$，其中 $\deg(g) = n - 1$。
- 根据归纳假设，存在 $g(x)$ 在 K_1 上的分裂域 M。此时 $g(x)$ 的根 $\alpha_2, \ldots, \alpha_n$ 都在 M 中。
- 显然 $f(x)$ 的所有根 $\alpha_1, \ldots, \alpha_n$ 都在 M 中，且 M 由这些根生成。故 M 即为所求。

□

定理 4.4 (分裂域的唯一性). 设 $f(x) \in k[x]$。若 M 和 M' 都是 $f(x)$ 在 k 上的分裂域，则存在同构 $\sigma : M \to M'$ 使得 $\sigma|_k = \mathrm{id}_k$（即 M 与 M' 在 k-同构意义下唯一）。

证明思路. 这是一个更一般结论（同构延拓定理）的推论。

1. 设 $p(x)$ 是 $f(x)$ 在 k 上的一个不可约因式。
2. 设 $\alpha \in M$ 和 $\beta \in M'$ 分别是 $p(x)$ 的根。
3. 根据单扩张同构定理，存在同构 $\tau : k(\alpha) \to k(\beta)$，使得 $\tau(\alpha) = \beta$ 且 τ 在 k 上是恒等映射。
4. 将 $k(\alpha)$ 视为新的基域，重复上述过程。由于扩张次数有限，经过有限步后即可将同构延拓至整个分裂域 $M \to M'$。

□

5 特殊的扩张类型

5.1 二次扩张 (Quadratic Extensions)

定义：扩张次数为 $[L : k] = 2$ 的扩张。根据域的特征是否为 2，其结构有本质区别。

情形 1: $\mathrm{char}(k) \neq 2$ **(常规情形)**
此时 $2 \neq 0$,可以使用配方法 (Completing the Square)。任意二次方程 $x^2+a_1x+a_2 = 0$ 均可变形为 $(x + \frac{a_1}{2})^2 = \frac{a_1^2}{4} - a_2$。

- **结论：**扩张由添加平方根生成，即 $L = k(\sqrt{\Delta})$。
- **性质：**总是可分的 (Separable)。

情形 2: $\mathrm{char}(k) = 2$ **(特殊情形)**
此时 $1 + 1 = 0$，不可除以 2，配方法失效。二次扩张分为两类：

(a) **Artin-Schreier 扩张** (一次项系数 $a_1 \neq 0$)

$$x^2 + x + a = 0$$

- **判别：**形式导数 $f'(x) = 1 \neq 0$，故无重根。
- **根结构：**若 β 是根，则 $\beta + 1$ 也是根。

- **性质**：是**可分扩张**，Galois 群为 C_2。

(b) **纯不可分扩张** (一次项系数 $a_1 = 0$)

$$x^2 + a = 0 \iff x^2 = a$$

- **判别**：形式导数 $f'(x) = 2x = 0$，故必有重根。
- **根结构**：方程化为 $(x - \alpha)^2 = 0$，只有一个二重根 $\alpha = \sqrt{a}$。
- **性质**：是**不可分扩张** (Purely Inseparable)。

5.2 有限域 (Finite Fields)

- **基数**：有限域的大小必须是素数幂 $q = p^d$。
- **唯一性**：给定 q，同构意义下唯一的有限域记为 $\mathbb{F}_q$。
- **构造**：$\mathbb{F}_q$ 是多项式 $X^q - X$ 在 $\mathbb{F}_p$ 上的分裂域。

6 几何应用：尺规作图 (Ruler and Compass)

本章导读

本节将几何作图问题转化为代数域扩张问题，从而解决了古希腊三大难题。

6.1 基本操作的代数意义

尺规作图包含两种基本操作：

1. **作直线**（直尺）：求直线交点 $\Longrightarrow$ 解一次方程组 $\Longrightarrow$ 域内运算 $(+, -, \times, \div)$。
2. **作圆**（圆规）：求直线与圆或圆与圆交点 $\Longrightarrow$ 解二次方程 $\Longrightarrow$ 域扩张（开平方）。

6.2 可构造数与主定理

定义 6.1 (可构造数). *复数 α 是可构造的，若存在域塔：*

$$\mathbb{Q} = L_0 \subseteq L_1 \subseteq \cdots \subseteq L_r$$

其中 $\alpha \in L_r$，且每一步 $[L_i : L_{i-1}] = 2$。

定理 6.2 (判别准则). *若 α 是尺规可作的，则其代数度数 $[\mathbb{Q}(\alpha):\mathbb{Q}]$ 必须是 2 的幂次 (2^k)。*

注意 (NOTE): 应用：三大难题的否定

- **倍立方：**需要作 $\sqrt[3]{2}$。度数为 3。因为 $3 \neq 2^k$，故不可作。
- **三等分角：**需要解 $4x^3 - 3x - c = 0$。一般情况下度数为 3，故不可作。

本章导读

本笔记基于课程板书整理，涵盖了域扩张理论的核心内容。主要包括：

1. **分裂域与正规扩张**：定义、等价刻画及经典反例（$\mathbb{Q}(\sqrt[3]{2})$）。
2. **代数闭包**：定义、存在性证明（Artin 构造）及唯一性。
3. **分圆扩张**：单位根、分圆多项式及其不可约性。
4. **有限域**：结构定理、不可约多项式计数与莫比乌斯反演。

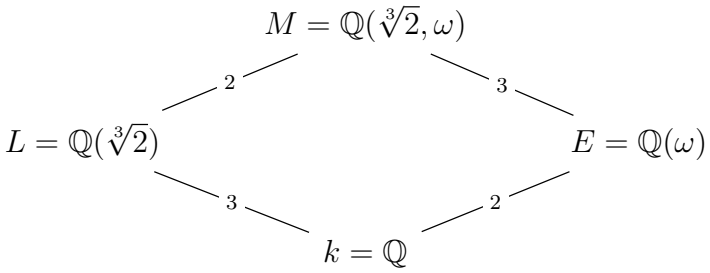
7 引例：分裂域与非正规扩张

我们从一个具体的例子出发，理解为何单纯添加一个根往往不够构成“完美”的扩域。

例 7.1 (经典反例). *考虑基域 $k=\mathbb{Q}$，多项式 $f(X)=X^3-2\in\mathbb{Q}[X]$。*

1. *令 $L=\mathbb{Q}(\sqrt[3]{2})\subseteq\mathbb{R}$。这是通过添加实根 $\sqrt[3]{2}$ 得到的扩域。*
2. *$f(X)$ 的根为 $\sqrt[3]{2},\sqrt[3]{2}\omega,\sqrt[3]{2}\omega^2$，其中 $\omega=\frac{-1+\sqrt{3}i}{2}$ 为三次单位根。*
3. *L 只包含了实根，缺了复根，因此 $f(X)$ 在 L 上不分裂。*
4. *分裂域 M 需要包含所有根，即 $M=\mathbb{Q}(\sqrt[3]{2},\omega)$。*

域塔结构如下：



其中 $[M:\mathbb{Q}]=6$。$L/\mathbb{Q}$ 不是正规扩张，而 $M/\mathbb{Q}$ 是正规扩张。

8 核心定义：分裂域与正规扩张

§5.3 - 5.5 定 义 与 性 质

8.1 分裂域 (Splitting Field)

定义 8.1. 设 k 是域，$S \subseteq k[x]$ 是多项式集合。L/k 称为关于 S 的**分裂域扩张**，如果满足：

1. **分裂性**：$\forall f \in S$，f 在 L 上完全分裂（即分解为一次因式的乘积）。
2. **极小性**：$L = k(R_S)$，其中 $R_S = \{\alpha \in L \mid \exists f \in S, f(\alpha) = 0\}$ 是所有根的集合。

8.2 正规扩张 (Normal Extension)

定义 8.2. 代数扩张 L/k 称为**正规扩张**，如果满足：对于任意不可约多项式 $f \in k[x]$，若 f 在 L 中有一个根，则 f 在 L 上完全分裂（即所有根都在 L 中）。

直观理解："全有或全无"性质

正规扩张体现了一种对称的完备性：不可约多项式的根是"一家人"，要么整整齐齐都在扩域里，要么一个都不在。$\mathbb{Q}(\sqrt[3]{2})$ 作为一个"半吊子"扩域（有根但不全），就是典型的非正规扩张。

例 8.3.

- **二次扩张**：若 $[L : k] = 2$，则 L/k 总是正规扩张。（证明：取 $\alpha \in L \setminus k$，其极小多项式为二次，由韦达定理，另一根也在 L 中）。
- **有限域扩张**：有限域的有限扩张总是正规扩张（见后文）。

补充证明：为什么二次扩张一定是正规的？

证明. 设 $[L : k] = 2$。取 $\alpha \in L \setminus k$。

1. α 在 k 上的极小多项式 $m_\alpha(x)$ 必然是二次的（因为 $[k(\alpha) : k]$ 必须整除 $[L : k] = 2$，且 $\alpha \notin k$）。
2. 设 $m_\alpha(x) = x^2 + bx + c$，其中 $b, c \in k$。
3. 设 $m_\alpha(x)$ 的两个根为 α 和 β。由韦达定理：
$$\alpha + \beta = -b \implies \beta = -b - \alpha$$
4. 由于 $b \in k \subseteq L$ 且 $\alpha \in L$，根据域的封闭性，$\beta \in L$。
5. 故 $m_\alpha(x)$ 的所有根都在 L 中。任何不可约多项式若有根在 L 中，必分裂。

□

9 正规扩张的等价刻画

这是域论中最重要的定理之一，连接了构造（分裂域）、性质（正规性）和变换（自同构）。

定理 9.1 (等价性定理). *设 L/k 是代数扩张，则以下命题等价：*

(i) 存在 $S \subseteq k[x]$，使得 L 是 S 在 k 上的分裂域。

(ii) L/k 是正规扩张。

(iii) 对于任意包含 L 的扩域 M 和任意 $\sigma \in \mathrm{Aut}(M/k)$，都有 $\sigma(L) = L$。

9.1 关键引理：根的传递性

为了证明上述定理及后续结论，我们需要以下关于嵌入延拓的引理。

引理 9.2 (根的传递性/嵌入延拓). *设 L 是 $f(x) \in k[x]$ 的分裂域，f 不可约。若 $\alpha, \beta \in L$ 均为 f 的根，则存在 $\sigma \in \mathrm{Aut}(L/k)$ 使得 $\sigma(\alpha) = \beta$。*

9.2 正规扩张等价性定理的完整证明

我们按照 $(i) \implies (iii) \implies (ii) \implies (i)$ 的顺序进行证明。

证明. **(i) $\implies$ (iii)：分裂域 $\implies$ 自同构不变性**

假设： L 是多项式集合 $S \subseteq k[x]$ 的分裂域。即 $L = k(R_S)$，其中 R_S 是 S 中多项式在 L 中的根集。
目标： 对于任意扩域 $M \supseteq L$ 和任意 $\sigma \in \mathrm{Aut}(M/k)$，证明 $\sigma(L) = L$。

1. 设 $\alpha \in L$。因为 $L = k(R_S)$，α 可以由 R_S 中的元素通过有限次加法和乘法生成。2. 考察 σ 对 R_S 的作用。设 $\gamma \in R_S$，则存在 $f \in S$ 使得 $f(\gamma) = 0$。3. 对等式两边作用 σ（利用 σ 固定 k 中系数的性质）：

$$f(\sigma(\gamma)) = \sigma(f(\gamma)) = \sigma(0) = 0$$

4. 这说明 $\sigma(\gamma)$ 也是 f 的一个根。5. 因为 f 在 L 中分裂（条件 i），f 的所有根都在 L 中。所以 $\sigma(\gamma) \in L$。更确切地说，σ 只是置换了集合 R_S 中的元素，即 $\sigma(R_S) \subseteq R_S$（对于代数扩张其实是相等）。6. 因为 σ 将 L 的生成元映射回 L，所以 $\sigma(L) \subseteq L$。7. 同

理，考虑 $\sigma^{-1} \in \mathrm{Aut}(M/k)$，我们有 $\sigma^{-1}(L) \subseteq L$，两边作用 σ 得 $L \subseteq \sigma(L)$。8. 综上，$\sigma(L) = L$。

(iii) $\Longrightarrow$ (ii)：自同构不变性 $\Longrightarrow$ 正规性

假设：对任意 $M \supseteq L$ 及 $\sigma \in \mathrm{Aut}(M/k)$，有 $\sigma(L) = L$。
目标：设不可约多项式 $f \in k[x]$ 在 L 中有一根 α，证明 f 的所有根都在 L 中。

1. 设 β 是 f 在某个代数闭包 $\Omega \supseteq L$ 中的任意另一个根。我们需要证明 $\beta \in L$。2. 因为 f 不可约且 α, β 都是根，根据**根的传递性引理**（或基底同构），存在 k-同构 $\tau : k(\alpha) \to k(\beta)$ 使得 $\tau(\alpha) = \beta$。3. 利用**嵌入延拓定理**，将 τ 延拓为 Ω 上的自同构 $\sigma \in \mathrm{Aut}(\Omega/k)$。4. 根据假设 (iii)（取 $M = \Omega$），我们有 $\sigma(L) = L$。5. 因为 $\alpha \in L$，所以 $\beta = \tau(\alpha) = \sigma(\alpha) \in \sigma(L) = L$。6. 这说明 f 的任意根 β 都在 L 中，即 f 在 L 上分裂。所以 L/k 是正规扩张。

(ii) $\Longrightarrow$ (i)：正规性 $\Longrightarrow$ 分裂域

假设：L/k 是正规扩张。
目标：构造一个多项式集合 S，使得 L 是 S 的分裂域。

1. 构造集合 $S = \{m_\alpha(x) \in k[x] \mid \alpha \in L\}$，即 L 中所有元素的极小多项式构成的集合。2. 显然 L 是由 S 中多项式的根生成的（因为 α 本身就是 m_α 的根），即 $L \subseteq \mathrm{SplittingField}(S)$。3. 根据正规扩张的定义：对于任意 $m_\alpha \in S$，因为它在 L 中有根 α，所以它在 L 中完全分裂。4. 这意味着 S 中所有多项式的所有根都在 L 中。5. 因此，L 恰好就是 S 的分裂域。

□

10 代数闭包 (Algebraic Closure)

10.1 定义与例子

定义 10.1. 域扩张 Ω/k 称为 k 的**代数闭包**，如果：

1. Ω/k 是代数扩张。
2. Ω 是代数封闭的（即 Ω 上所有非常数多项式都有根）。

例 10.2.
- $\mathbb{C}/\mathbb{R}$ 是代数闭包扩张（代数基本定理）。

- $\mathbb{C}$ 不是 $\mathbb{Q}$ 的代数闭包（因为含超越数）。$\mathbb{Q}$ 的代数闭包记为 $\overline{\mathbb{Q}}$，它是 $\mathbb{C}$ 中所有代数数的集合。

10.2 存在性证明 (Artin 构造)

定理 10.3. *任意域 k 都存在代数闭包。*

11 代数闭包存在性的完整证明 (Artin 构造)

定理 11.1. *任意域 k 都存在代数闭包。*

证明. 证明分为两步：首先构造一个扩域 k_1，使得 k 中所有非常数多项式在 k_1 中都有根；然后通过归纳构造域塔并取并集得到代数闭包。

第一步：构造扩域 k_1 (Artin 的单步构造)

令 S 为 $k[x]$ 中所有首一不可约多项式（次数 ≥ 1）构成的集合。对于每一个 $f \in S$，我们需要为它“制造”一个根。

1. **引入变量与多项式环：**对每个 $f \in S$，引入一个独立的变量 X_f。考虑基域 k 上由这些无穷多个变量生成的多项式环：

$$R = k[\{X_f\}_{f \in S}]$$

2. **构造理想：**我们希望 X_f 成为多项式 f 的根，即希望 $f(X_f) = 0$。为此，考虑由所有 $f(X_f)$ 生成的理想 $\mathfrak{a}$：

$$\mathfrak{a} = (\{f(X_f) \mid f \in S\}) \subseteq R$$

3. **关键引理：$\mathfrak{a}$ 是真理想 ($\mathfrak{a} \neq R$)。**

   反证法：假设 $\mathfrak{a} = R$，则 $1 \in \mathfrak{a}$。

   这意味着存在有限个多项式 $f_1, \ldots, f_n \in S$ 以及 R 中的元素 $g_1, \ldots, g_n$，使得：

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

   注意到这个等式只涉及有限个变量 $X_{f_1}, \ldots, X_{f_n}$。

设 E 是 $f_1 \dots f_n$ 在 k 上的分裂域（这是有限扩域，必然存在）。在 E 中，每个 f_i 都有一个根，记为 α_i。

定义求值同态 $\phi : R \to E$：

$$\phi(X_h) = \begin{cases} \alpha_i & \text{若} h = f_i \\ 0 & \text{若} h \in S \setminus \{f_1, \dots, f_n\} \end{cases}$$

对原等式两边作用 ϕ：

$$1 = \phi(1) = \sum_{i=1}^{n} \phi(g_i) \cdot f_i(\alpha_i)$$

由于 α_i 是 f_i 的根，故 $f_i(\alpha_i) = 0$。因此等式右边为 0，即 $1 = 0$。这在域 E 中是不可能的，导出矛盾。

结论： $\mathfrak{a} \neq R$。

4. **利用 Zorn 引理 (Krull 定理)：**因为 $\mathfrak{a}$ 是真理想，必然存在一个包含 $\mathfrak{a}$ 的极大理想 $\mathfrak{m} \subset R$。

5. **定义扩域 k_1：**令 $k_1 = R/\mathfrak{m}$。由于 $\mathfrak{m}$ 是极大的，k_1 是一个域。我们可以通过自然映射 $k \hookrightarrow R \twoheadrightarrow k_1$ 将 k 视为 k_1 的子域。对于任意 $f \in S$，设 $\bar{X}_f = X_f + \mathfrak{m} \in k_1$。在 k_1 中有：

$$f(\bar{X}_f) = f(X_f) + \mathfrak{m} = 0 + \mathfrak{m} = 0$$

(因为 $f(X_f) \in \mathfrak{a} \subseteq \mathfrak{m}$)。因此，$k$ **中所有不可约多项式在 k_1 中都至少有一个根**。

第二步：迭代构造与取并集

k_1 虽然解决了 k 上的多项式，但 k_1 系数的多项式未必有根。我们需要迭代：

- 令 $k_0 = k$。
- 利用第一步的方法，构造 k_1 使得 k_0 上多项式有根。
- 归纳地，构造 k_{n+1} 使得 k_n 上所有多项式在 k_{n+1} 中有根。
- 得到域塔：$k = k_0 \subseteq k_1 \subseteq k_2 \subseteq \dots$

令 $\Omega = \bigcup_{n=0}^{\infty} k_n$。

1. Ω **是域：**对于任意 $\alpha, \beta \in \Omega$，存在某个 n 使得 $\alpha, \beta \in k_n$，故其和、积、逆元都在 $k_n \subseteq \Omega$ 中。

2. Ω **是代数封闭的**：设 $F(x) \in \Omega[x]$ 是非常数多项式。由于 F 只有有限个系数，必定存在某个 N，使得 F 的所有系数都在 k_N 中。根据构造，k_N 上的多项式 F 在 k_{N+1} 中有根。因为 $k_{N+1} \subseteq \Omega$，所以 F 在 Ω 中有根。

3. Ω **是代数扩张**：Ω 中的每个元素都在某个 k_n 中，而 k_n/k 是代数扩张（由构造可知每一步都是代数扩张，代数扩张的传递性），所以 Ω/k 是代数扩张。

综上，Ω 即为 k 的代数闭包。 □

12 分圆扩张 (Cyclotomic Extension)

§5.3 分 圆 域

定义 12.1. $L = k(\mu_n)$ 称为分圆扩张，它是 $X^n - 1$ 在 k 上的分裂域。其中 $\mu_n = \{x \mid x^n = 1\}$ 是 n 次单位根集合。

对于 $k = \mathbb{Q}$，我们有以下重要结论：

- $\mathbb{Q}(\mu_n) = \mathbb{Q}(\xi_n)$，其中 $\xi_n = e^{2\pi i/n}$ 是本原单位根。
- **扩张次数**：$[\mathbb{Q}(\xi_n) : \mathbb{Q}] = \phi(n)$（欧拉函数）。
- **极小多项式**：ξ_n 的极小多项式是 **分圆多项式** $\Phi_n(X)$。

$$\Phi_n(X) = \prod_{1 \le k < n, (k,n)=1} (X - \xi_n^k) \in \mathbb{Z}[X]$$

- **不可约性**：$\Phi_n(X)$ 在 $\mathbb{Q}$ 上不可约（Eisenstein 判别法对 p 适用，一般情况需用 Gauss 证明）。

13 有限域 (Finite Fields)

有 限 域 的 结 构 与 计 数

13.1 结构定理

定理 13.1. *1. 有限域 $\mathbb{F}_q$ 的阶数 q 必为素数幂 p^r。*

2. $\mathbb{F}_q$ 恰好是多项式 $X^q - X$ 在 $\mathbb{F}_p$ 上的分裂域。

3. $\mathbb{F}_q/\mathbb{F}_p$ 是正规扩张。

13.2 子域判定

$\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^r} \iff d \mid r$。这意味着 $\mathbb{F}_{p^r}$ 包含了所有次数 d 整除 r 的不可约多项式的根。

14 有限域结构与子域判定的详细证明

14.1 结构定理的证明

定理 14.1 (有限域结构定理)**.** *设 $\mathbb{F}$ 是一个有限域。*

1. $\mathbb{F}$ 的特征必为素数 p，且 $|\mathbb{F}| = p^r$ $(r \geq 1)$。

2. $\mathbb{F}$ 是多项式 $X^{p^r} - X$ 在 $\mathbb{F}_p$ 上的分裂域。

3. $\mathbb{F}/\mathbb{F}_p$ 是正规扩张。

证明. **1. 证明阶数为素数幂**

- 因为 $\mathbb{F}$ 是有限的，其特征 $\mathrm{char}(\mathbb{F})$ 不能为 0（否则含 $\mathbb{Q}$，导致无限）。故 $\mathrm{char}(\mathbb{F}) = p$ 为素数，否则包含零因子。
- 因此 $\mathbb{F}$ 包含素域 $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$。
- $\mathbb{F}$ 可以看作是 $\mathbb{F}_p$ 上的向量空间。由于 $\mathbb{F}$ 有限，其维数必为有限值，设为 $r = [\mathbb{F} : \mathbb{F}_p]$。
- 作为向量空间，$\mathbb{F} \cong (\mathbb{F}_p)^r$。因此其元素个数为 $|\mathbb{F}| = p^r$。

2. 证明是分裂域令 $q = p^r$。

- 考虑 $\mathbb{F}$ 的乘法群 $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$。这是一个阶为 $q - 1$ 的有限群。
- 根据 Lagrange 定理，对任意 $\alpha \in \mathbb{F}^\times$，有 $\alpha^{q-1} = 1$。

- 等式两边同乘 α，得 $\alpha^q = \alpha$。
- 对于 $0 \in \mathbb{F}$，显然满足 $0^q = 0$。
- 因此，$\mathbb{F}$ 中的所有 q 个元素都是方程 $X^q - X = 0$ 的根。
- 由于多项式 $X^q - X$ 的次数为 q，它在任何域中最多有 q 个根。
- 结论：$\mathbb{F}$ 恰好由 $X^q - X$ 的所有根组成。因此 $\mathbb{F}$ 是该多项式在 $\mathbb{F}_p$ 上的分裂域。

3. 证明是正规扩张

- 根据定义，任何多项式的分裂域扩张都是正规扩张。
- 因为 $\mathbb{F}$ 是 $X^q - X$ 的分裂域，所以 $\mathbb{F}/\mathbb{F}_p$ 是正规扩张。

□

14.2 子域判定定理的证明

定理 14.2 (子域判定). *设 $\mathbb{F}_{p^r}$ 是具有 p^r 个元素的有限域。则 $\mathbb{F}_{p^d}$ 是 $\mathbb{F}_{p^r}$ 的子域当且仅当 $d \mid r$。*

证明. **必要性 ($\Rightarrow$)**：假设 $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^r}$。

- $\mathbb{F}_{p^r}$ 可以看作是 $\mathbb{F}_{p^d}$ 上的向量空间。设其维数为 m。
- 根据扩张次数的乘法公式：

$$[\mathbb{F}_{p^r} : \mathbb{F}_p] = [\mathbb{F}_{p^r} : \mathbb{F}_{p^d}] \cdot [\mathbb{F}_{p^d} : \mathbb{F}_p]$$

- 代入维数：$r = m \cdot d$。
- 显然 $d \mid r$。

充分性 ($\Leftarrow$)：假设 $d \mid r$。

- 此时 $r = kd$ ($k \in \mathbb{Z}^+$)。
- 我们利用代数恒等式：若 $a \mid b$，则 $X^a - 1 \mid X^b - 1$。
- 因为 $d \mid r$，所以 $p^d - 1 \mid p^r - 1$。

- 这意味着在整数环中，$p^r - 1 = k'(p^d - 1)$。
- 再次利用多项式除法性质：$X^{p^d-1} - 1$ 整除 $X^{p^r-1} - 1$。
- 两边同乘 X，得到：
$$X^{p^d} - X \mid X^{p^r} - X$$
- 设 $\mathbb{F}_{p^r}$ 是 $X^{p^r} - X$ 的分裂域（即根集）。因为 $X^{p^d} - X$ 是 $X^{p^r} - X$ 的因子，所以 $X^{p^d} - X$ 的所有根都包含在 $\mathbb{F}_{p^r}$ 中。
- $X^{p^d} - X$ 的所有根构成的集合恰好是唯一的有限域 $\mathbb{F}_{p^d}$。
- 因此 $\mathbb{F}_{p^d} \subseteq \mathbb{F}_{p^r}$。

□

14.3 不可约多项式计数与莫比乌斯反演

利用恒等式：
$$X^{p^r} - X = \prod_{d|r} \prod_{f \in P_d} f(X)$$
其中 P_d 是 $\mathbb{F}_p$ 上次数为 d 的首一不可约多项式集合。

比较两边次数，得 **高斯公式**：
$$p^r = \sum_{d|r} d \cdot N_d$$
其中 N_d 是次数为 d 的不可约多项式个数。

利用 **莫比乌斯反演公式**，可解得：
$$N_r = \frac{1}{r} \sum_{d|r} \mu(d) p^{r/d}$$

例 14.3 (计算 $\mathbb{F}_2$ 上 3 次不可约多项式个数). 取 $p = 2, r = 3$。
$$N_3 = \frac{1}{3} \sum_{d|3} \mu(d) 2^{3/d} = \frac{1}{3} \left(\mu(1) 2^3 + \mu(3) 2^1 \right)$$
$$= \frac{1}{3}(1 \cdot 8 + (-1) \cdot 2) = \frac{6}{3} = 2$$
这两个多项式为 $X^3 + X + 1$ 和 $X^3 + X^2 + 1$。

本章导读

本笔记涵盖了域扩张理论的两个核心概念：**正规扩张 (Normal Extension)** 与 **可分扩张 (Separable Extension)**。

- **正规扩张**：讨论了扩张的正规性在中间域、复合域下的遗传性，以及正规性不满足传递性的反例。
- **复合域性质**：给出了线性不相交性的初步结论（扩张次数的不等式）。
- **可分性**：从经典（极小多项式无重根）与现代（张量积无幂零元）两个角度定义可分性。讨论了特征 p 下不可分现象的本质（$P'(x)=0$）。
- **完美域**：定义及其性质，证明了有限域是完美域。
- **可分次数**：引入嵌入映射计数，建立了可分扩张的等价命题。

15 正规扩张 (Normal Extension)

正规扩张的性质与遗传性

定义 15.1 (正规扩张). 域扩张 L/k 称为**正规扩张**，如果 L 是某族多项式 $S \subseteq k[x]$ 在 k 上的分裂域。

命题 15.2 (正规性的遗传性). 设 L/k 为域的代数扩张。

1. **向上遗传**：若 L/k 为正规扩张，且 $k \subseteq E \subseteq L$，则 L/E 也是正规扩张。
2. **提升/平移 *(Lifting)***：设 L/k 为正规扩张，固定 $k \subseteq L \subseteq \bar{k}$ 和 $E \subseteq \bar{k}$。令 $L \cdot E = L(E) = E(L) = k(L \cup E)$ 为 L 与 E 的复合域。则 $L \cdot E/E$ 也是正规扩张。

证明. **(1) 的证明**：因为 L/k 是正规扩张，故 L 是某多项式族 $S \subseteq k[x]$ 在 k 上的分裂域。由于 $k \subseteq E$，则 $S \subseteq E[x]$。显然 L 包含了 S 的所有根，且 L 由 k 和这些根生成，自然也由 E 和这些根生成（因为 E 已经在 L 中了，实际上 $L = E(L) = E(\text{roots})$）。故 L 是 S 关于 E 的分裂域，即 L/E 是正规扩张。

(2) 的证明：同样设 L 是 $S \subseteq k[x]$ 在 k 上的分裂域，设 R 为 S 在 $\bar{k}$ 中的根集，则 $L = k(R)$。考察复合域 $L \cdot E = E(L) = E(k(R)) = E(R)$。由于 $S \subseteq k[x] \subseteq E[x]$，且 $L \cdot E$ 是由 E 添加 S 的根集 R 生成的。因此 $L \cdot E$ 是 S 在 E 上的分裂域，故 $L \cdot E/E$ 是正规扩张。 □

注意 (NOTE): 正规扩张的非传递性

正规扩张**不满足**传递性。即：若 L/E 和 E/k 都是正规扩张，L/k 不一定是正规扩张。另外，若大扩张 L/k 是正规的，中间扩张 E/k 也不一定是正规的。
经典反例：考察塔 $k = \mathbb{Q} \subseteq E = \mathbb{Q}(\sqrt{2}) \subseteq L = \mathbb{Q}(\sqrt[4]{2})$。

- E/k 是正规的（$x^2 - 2$ 的分裂域）。
- L/E 是正规的（$x^2 - \sqrt{2}$ 的分裂域）。
- 但 L/k **不是**正规的。因为极小多项式 $x^4 - 2$ 在 L 中有根 $\sqrt[4]{2}$，但其复根 $i\sqrt[4]{2} \notin L$（$L \subseteq \mathbb{R}$）。

命题 15.3 (正规扩张的复合). *若 L/k 和 E/k 都是正规扩张，则复合域 $L \cdot E/k$ 也是正规扩张。*

证明. 设 L 是 $f(x) \in k[x]$ 的分裂域，E 是 $g(x) \in k[x]$ 的分裂域。则 $L \cdot E$ 显然是多项式 $f(x)g(x)$ 在 k 上的分裂域。故为正规扩张。 □

例题：分圆域的复合

考察分圆扩张 $E_1 = \mathbb{Q}(\zeta_m)$ 和 $E_2 = \mathbb{Q}(\zeta_n)$，其中 $\zeta_k = e^{2\pi i/k}$ 为 k 次本原单位根。

命题 15.4. *若 $\gcd(m, n) = 1$，则 $\mathbb{Q}(\zeta_{mn}) = \mathbb{Q}(\zeta_m) \cdot \mathbb{Q}(\zeta_n)$。*

证明. 我们需要证明两个方向的包含关系：

1. 证明 $\mathbb{Q}(\zeta_m) \cdot \mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_{mn})$

- 注意到 $\zeta_m = e^{2\pi i/m} = e^{2\pi in/mn} = (\zeta_{mn})^n$。这意味着 $\zeta_m \in \mathbb{Q}(\zeta_{mn})$。
- 同理 $\zeta_n = e^{2\pi i/n} = e^{2\pi im/mn} = (\zeta_{mn})^m$，意味着 $\zeta_n \in \mathbb{Q}(\zeta_{mn})$。
- 由于复合域 $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)$ 是包含 ζ_m 和 ζ_n 的最小域，故 $\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) \subseteq \mathbb{Q}(\zeta_{mn})$。
- *注：此步骤不需要 $\gcd(m, n) = 1$ 的条件。*

2. 证明 $\mathbb{Q}(\zeta_{mn}) \subseteq \mathbb{Q}(\zeta_m) \cdot \mathbb{Q}(\zeta_n)$

- 利用条件 $\gcd(m, n) = 1$。根据贝祖等式 (Bézout's Identity)，存在整数 $a, b \in \mathbb{Z}$ 使得：

$$am + bn = 1$$

- 等式两边同时除以 mn，得：

$$\frac{1}{mn} = \frac{am+bn}{mn} = \frac{a}{n} + \frac{b}{m}$$

- 将其应用到单位根的指数上：

$$\zeta_{mn} = e^{2\pi i \frac{1}{mn}} = e^{2\pi i(\frac{a}{n}+\frac{b}{m})} = e^{2\pi i \frac{a}{n}} \cdot e^{2\pi i \frac{b}{m}} = (\zeta_n)^a \cdot (\zeta_m)^b$$

- 这表明生成元 ζ_{mn} 可以写成 ζ_n 和 ζ_m 的乘积形式。
- 因此 $\zeta_{mn} \in \mathbb{Q}(\zeta_m, \zeta_n) = \mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n)$。

3. 扩张次数验证 (Consistency Check)

- 已知分圆扩张的次数公式：$[\mathbb{Q}(\zeta_k) : \mathbb{Q}] = \varphi(k)$。
- 复合域的扩张次数满足乘法公式：

$$[\mathbb{Q}(\zeta_m)\mathbb{Q}(\zeta_n) : \mathbb{Q}] \leq [\mathbb{Q}(\zeta_m) : \mathbb{Q}] \cdot [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(m)\varphi(n)$$

- 另一方面，$[\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}] = \varphi(mn)$。
- 当 $\gcd(m,n) = 1$ 时，由欧拉函数的积性可知 $\varphi(mn) = \varphi(m)\varphi(n)$。
- 扩张次数的相等进一步印证了 E_1 和 E_2 是**线性不相交 (Linearly Disjoint)** 的，且 $\mathbb{Q}(\zeta_{mn})$ 恰好等于两者的复合。

□

16 复合域的扩张次数 (Natural Irrationalities)

扩 张 次 数 的 缩 减

命题 16.1. *设 $L, E/k$ 为有限扩张，且 L, E 包含在同一个大域中。*

1. $[L \cdot E : E] \leq [L : k]$。
2. $[L \cdot E : k] \leq [L : k] \cdot [E : k]$。

证明. **情形 1：单扩张** $L = k(\alpha)$

- $[L : k] = \deg P_{k,\alpha}$，其中 $P_{k,\alpha}$ 是 α 在 k 上的极小多项式。
- $L \cdot E = E(\alpha)$，故 $[L \cdot E : E] = \deg P_{E,\alpha}$，其中 $P_{E,\alpha}$ 是 α 在 E 上的极小多项式。
- 由于 $k \subseteq E$，故 $P_{k,\alpha}(x) \in E[x]$ 且 α 是其根。根据极小多项式的性质，$P_{E,\alpha} \mid P_{k,\alpha}$。
- 因此 $\deg P_{E,\alpha} \leq \deg P_{k,\alpha}$，即 $[L \cdot E : E] \leq [L : k]$。

情形 2：一般有限扩张设 $L = k(\alpha_1, \ldots, \alpha_n)$。构造塔 $L_0 = k, L_i = L_{i-1}(\alpha_i)$。应用归纳法和乘法公式（Tower Law）：

$$[L \cdot E : E] = \prod_{i=1}^{n} [L_i E : L_{i-1} E] \leq \prod_{i=1}^{n} [L_i : L_{i-1}] = [L : k]$$

结论 (2) 由 $[L \cdot E : k] = [L \cdot E : E][E : k]$ 直接得出。 □

例 16.2. n 次多项式的分裂域扩张次数 $\leq n!$。*(证明思路：每次添加一个根，扩张次数最多为当前多项式的次数，即 $n \times (n-1) \times \cdots \times 1$)*。

17 可分性 (Separability)

可 分 性 的 定 义 与 判 据

17.1 定义的层级

定义 17.1 (可分多项式). $P(x) \in k[x]$ 称为**可分多项式**，如果 $P(x)$ 的每一个**不可约因子**都无重根。

直观理解：判据

不可约多项式 $\pi(x)$ 无重根 $\iff \pi'(x) \neq 0$。

定义 17.2 (可分代数元). $\alpha \in L$ 是 k 上的**可分代数元**，如果 α 在 k 上的极小多项式 $P_\alpha(x)$ 无重根。

定义 17.3 (可分扩张). 代数扩张 L/k 称为**可分扩张**，如果 L 中所有元素都是 k 上的可分代数元。

17.2 现代代数视角（张量积）

定义 17.4 (可分代数 - Modern Definition). 设 A 为 k-代数。A 在 k 上可分，如果 $A_{\bar{k}} = A \otimes_k \bar{k}$ 是 ***reduced*** 的（即没有非零幂零元）。

注.
- 对于域扩张 L/k，上述定义等价于 L/k 是可分扩张。
- 直观理解：$L \otimes_k \bar{k} \cong \prod \bar{k}[x]/(x-\alpha_i)^{e_i}$。若存在重根 ($e_i > 1$)，则存在幂零元 $(x-\alpha_i)$，使得 $(x-\alpha_i)^{e_i} = 0$ 但本身非零。
- 例：$k[x], k(x)$ 都是 k 上的可分代数。

17.3 不可分现象与特征 p

命题 17.5 (不可分的充要条件). 若 α 不是可分代数元（即 $P_\alpha(X)$ 有重根），则必须同时满足：

1. $\mathrm{char}(k) = p > 0$。（特征 *0* 上一切皆可分）。
2. $P'_\alpha(X) = 0$。
3. 存在不可约多项式 $Q \in k[X]$，使得 $P_\alpha(X) = Q(X^p)$。

命题 17.6 (不可分性的充要条件). 设 α 是域 k 上的代数元，$P_\alpha(X)$ 是其极小多项式。以下命题等价：

1. α 是不可分代数元（即 $P_\alpha(X)$ 在 $\bar{k}$ 中有重根）。
2. $P'_\alpha(X) = 0$（这蕴含 $\mathrm{char}(k) = p > 0$ 且 $P_\alpha(X) = Q(X^p)$）。
3. $L \otimes_k \bar{k}$ 含有非零幂零元（即不是 *reduced* 的）。

证明. 我们分两个方向证明上述等价性。

方向一：(1) $\Longrightarrow$ (2)（不可分 $\Longrightarrow$ 导数为 0）

- 假设 α 不可分，即 $P_\alpha(X)$ 在 $\bar{k}$ 中有重根。
- 多项式有重根的充要条件是 $P_\alpha(X)$ 与其形式导数 $P'_\alpha(X)$ 互不互素，即 $\gcd(P_\alpha, P'_\alpha) \neq 1$。
- 由于 $P_\alpha(X)$ 是**不可约**多项式，其因式只有常数和它自身。因此 $\gcd(P_\alpha, P'_\alpha)$ 必须是 $P_\alpha(X)$（相差一个常数因子）。

- 这意味着 $P_\alpha(X) \mid P'_\alpha(X)$。
- 然而，导数的次数总是严格小于原多项式次数 ($\deg P'_\alpha < \deg P_\alpha$)。要让高次多项式整除低次多项式，唯一的可能性是低次多项式恒为零。
- 故 $P'_\alpha(X) = 0$。
- 注：在特征 0 中，非常数多项式的导数不可能为 0，故此情况只在 $\mathrm{char}(k) = p$ 时发生。此时 $P_\alpha(X)$ 中 X 的指数必须都是 p 的倍数，即 $P_\alpha(X) = Q(X^p)$。

方向二：(2) $\Longrightarrow$ (3) $\Longrightarrow$ (1) **（导数为 0 $\Longrightarrow$ 幂零元 $\Longrightarrow$ 不可分）**

- 若 $P'_\alpha(X) = 0$，则 $P_\alpha(X)$ 具有形式 $Q(X^p) = \sum a_i (X^p)^i$。
- 在代数闭包 $\bar{k}$ 中，系数可以开 p 次方，设 $a_i = b_i^p$。利用 Frobenius 性质 $(A+B)^p = A^p + B^p$：
$$P_\alpha(X) = \sum b_i^p (X^i)^p = \left(\sum b_i X^i\right)^p = (H(X))^p$$
其中 $H(X) \in \bar{k}[X]$。
- 考察张量积结构：
$$L \otimes_k \bar{k} \cong \bar{k}[X]/(P_\alpha(X)) = \bar{k}[X]/(H(X)^p)$$
- 在这个商环中，元素 $[H(X)]$ 本身非零（因为 $\deg H < \deg P_\alpha$），但其 p 次方 $[H(X)]^p = [P_\alpha(X)] = 0$。
- 故 $[H(X)]$ 是一个**非零幂零元**，说明 $L \otimes_k \bar{k}$ 不是 reduced 的。
- 同时，$P_\alpha(X) = (H(X))^p$ 说明 $P_\alpha(X)$ 的每一个根的重数至少为 $p \geq 2$，即 $P_\alpha(X)$ 有重根，故 α 不可分。

□

18 完美域 (Perfect Field)

完 美 域 与 有 限 域

定义 18.1 (完美域). 域 k 称为**完美域**，如果满足以下条件之一：

1. $\mathrm{char}(k) = 0$。

2. $\mathrm{char}(k) = p > 0$，且 *Frobenius* 映射 $\sigma : x \mapsto x^p$ 是满射（即 $k^p = k$）。

定理 18.2 (完美域的性质). *若 k 是完美域，则：*

- *k 上所有不可约多项式都是可分的。*
- *k 的任何代数扩张都是可分扩张。*

证明. 特征 0 时显然。设 $\mathrm{char}(k) = p$ 且 k 完美。反证法：若不可约多项式 $\pi(x)$ 不可分，则 $\pi(x) = Q(x^p) = \sum a_i x^{ip}$。因 k 完美，存在 $b_i \in k$ 使 $a_i = b_i^p$。则 $\pi(x) = \sum b_i^p x^{ip} = (\sum b_i x^i)^p$。这意味着 $\pi(x)$ 可约，矛盾。 □

例 18.3 (有限域). *有限域 $\mathbb{F}_q$ $(q = p^d)$ 是完美域。*

- *$\mathbb{F}_q$ 是 $x^q - x$ 的分裂域。*
- *$f(x) = x^q - x$。求导得 $f'(x) = qx^{q-1} - 1 = -1 \neq 0$（因 q 是 p 的幂，在模 p 下为 0）。*
- *故 $f(x)$ 无重根，$\mathbb{F}_q$ 的扩张总是可分的。*

19 可分次数 (Separable Degree)

同态计数与等价命题

定义 19.1 (可分次数). *设 L/k 为有限扩张，定义 L/k 的**可分次数** $[L : k]_s$ 为保持 k 不变的嵌入映射的个数：*

$$[L : k]_s = \#\{\phi : L \to \bar{k} \mid \phi|_k = \mathrm{id}\}$$

19.1 单扩张的计算

设 $L = k(\alpha)$，极小多项式为 $P_\alpha(X)$，$\deg P_\alpha = n$。嵌入映射 ϕ 由 $\phi(\alpha)$ 唯一确定，且 $\phi(\alpha)$ 必须是 $P_\alpha(X)$ 的根。

- **情形 1：P_α 可分**（如 $\mathrm{char}(k) = 0$）。P_α 有 n 个互不相同的根。$\Longrightarrow$ $[L : k]_s = n = [L : k]$。

- **情形 2：P_α 不可分**（$\mathrm{char}(k)=p$）。$P_\alpha(X)=Q(X^{p^e})$，其中 Q 可分，$e\geq 1$。P_α 的根数为 n，但**几何上互异的根**只有 $d=\deg Q=n/p^e$ 个。每个根的重数为 p^e。$\Longrightarrow$ $[L:k]_s=d<n$。这里 p^e 称为不可分度 (Inseparable Degree)，记为 $[L:k]_i$。

$$[L:k]=[L:k]_s\cdot[L:k]_i$$

19.2 可分扩张的等价命题

定理 19.2 (主要定理). *以下关于有限扩张 L/k 的命题是等价的：*

1. *L/k 是可分有限扩张（所有元素可分）。*
2. *L 是可分代数生成的，即 $L=k(\alpha_1,\dots,\alpha_l)$，且 α_i 均为可分代数元。*
3. *$[L:k]_s=[L:k]$。*

证明. 我们按照循环蕴含的顺序进行证明：(1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (1)。

1. (1) $\Rightarrow$ (2)

- 假设 L/k 是可分有限扩张。
- 由于 L/k 是有限扩张，作为 k-向量空间，L 是有限维的。因此存在有限的一组基 $\{\alpha_1,\dots,\alpha_l\}$ 使得 $L=k(\alpha_1,\dots,\alpha_l)$。
- 根据定义 (1)，L 中**所有**元素都是 k 上的可分代数元。
- 特别地，生成元 $\alpha_1,\dots,\alpha_l$ 都是可分代数元。故 (2) 成立。

2. (2) $\Rightarrow$ (3)

- 假设 $L=k(\alpha_1,\dots,\alpha_l)$，且每个 α_i 在 k 上可分。
- 构造扩张塔：令 $L_0=k$，并定义 $L_i=L_{i-1}(\alpha_i)$ (对于 $i=1,\dots,l$)，于是有一串单扩张：

$$k=L_0\subseteq L_1\subseteq L_2\subseteq\cdots\subseteq L_l=L$$

- **关键引理**：若 α 在 k 上可分，则 α 在任何包含 k 的中间域 F 上也可分。
  - *引理证明*：设 α 在 k 上的极小多项式为 $f(x)$，在 F 上的极小多项式为 $g(x)$。由于 $f(x)\in k[x]\subseteq F[x]$ 且 $f(\alpha)=0$，故 $g(x)\mid f(x)$。因为 α 在 k 上可分，即 $f(x)$ 无重根，所以其因子 $g(x)$ 也无重根。故 α 在 F 上可分。

- 应用上述引理，因为 α_i 在 k 上可分，所以 α_i 在中间域 L_{i-1} 上也是可分的。
- 对于每一步单扩张 L_i/L_{i-1}，由于它是可分代数元生成的，我们有：

$$[L_i : L_{i-1}]_s = [L_i : L_{i-1}]$$

- 利用扩张次数和可分次数的乘法公式（Tower Law）：

$$[L : k]_s = \prod_{i=1}^{l} [L_i : L_{i-1}]_s = \prod_{i=1}^{l} [L_i : L_{i-1}] = [L : k]$$

- 故 (3) 成立。

3. (3) $\Rightarrow$ (1)

- 假设 $[L : k]_s = [L : k]$。
- 任取 $\alpha \in L$。我们需要证明 α 是可分代数元。
- 考虑中间域 $k(\alpha)$，利用积性公式：

$$[L : k] = [L : k(\alpha)] \cdot [k(\alpha) : k]$$

$$[L : k]_s = [L : k(\alpha)]_s \cdot [k(\alpha) : k]_s$$

- 我们已知一般不等式：对任意有限扩张 F/E，恒有 $[F : E]_s \leq [F : E]$。
- 若 α 不可分，则对于单扩张 $k(\alpha)/k$，必有 $[k(\alpha) : k]_s < [k(\alpha) : k]$。
- 结合 $[L : k(\alpha)]_s \leq [L : k(\alpha)]$，这将导致：

$$[L : k]_s = [L : k(\alpha)]_s [k(\alpha) : k]_s < [L : k(\alpha)][k(\alpha) : k] = [L : k]$$

  即 $[L : k]_s < [L : k]$，这与假设矛盾。
- 因此，必须有 $[k(\alpha) : k]_s = [k(\alpha) : k]$，这意味着 α 的极小多项式无重根，即 α 是可分的。
- 由于 α 是任意选取的，故 L 中所有元素皆为可分元，(1) 成立。

□