域扩张次数的计算

Aug 2025

1 基本概念

1.1 扩张次数

域扩张是域论的核心研究对象，甚至可以说是唯一研究对象。对于域论的其他话题，如其 Galois 群的计算和性质，以及其应用（如在方程根式可解问题等），甚至是后续课程中，如数论中对于理想论的研究事实上就是考察一个局部域的理想在扩张中的分歧与惯性行为。

一个**域扩张** K/F 指域 F 作为 K 的一个子域，K 称作 F 的**扩域**，而 F 称为**基域**。更进一步说，域 K 成为域 F 的一个线性空间，这是一个非常关键的观察和视角。于是**（域）扩张次数**（或度数）就自然地被定义为线性空间 K 在基域 F 上的维数，记作 $[K:F]$ 或 $\dim_F(K)$.

作为线性空间的维数，扩张次数当然也可以是无限的。若其是有限的，称 K/F 为一个**有限扩张**；反之则是一个**无限扩**张。本文指考虑有限扩张的情况。

Exercise 1. 复数域 $\mathbb{C}$ 为实数域 $\mathbb{R}$ 的一个有限扩张，由于 $\mathbb{C}$ 可以被看作为以 $\{1, \sqrt{-1}\}$ 为基的 $\mathbb{R}$ 线性空间。

Exercise 2. 实数域 $\mathbb{R}$ 为有理数域 $\mathbb{Q}$ 的一个无限扩张，因为显然这个线性空间的维数是无限的。

在处理相对复杂的域扩张时，直接计算器域扩张次数是比较复杂的。通常我们可以利用域扩张的**塔性质**将其拆解为一系列域扩张的合成：

塔律（Tower Law）
对于一个域扩张塔 $F \subseteq L \subseteq M$，那么其扩张次数满足：

$$[M:F] = [M:L] \cdot [L:F] \tag{1}$$

公式的证明并不复杂，只需要注意到若 $\{u_i\}_{1\le i\le d}$ 为 L 在 F 上的基（$d = [L:F]$），而 $\{w_j\}_{1\le j\le e}$ 为 M 在 L 上的基，那么可以证明 $\{u_i w_j\}_{1\le i\le d, 1\le j\le e}$ 构成了 M 在 F 上的基。

1.2 代数元与极小多项式

在域扩张 K/F 中，一个元素 $\alpha \in K$ 如果是某个系数在 F 中的多项式的根，则称为**代数的**；否则，称为**超越的**。

对于 F 上的代数元 α，一切以 α 为根的多项式构成 $F[x]$ 的一个理想，记为 $J_\alpha = \{f(x) \in F[x] : f(\alpha) = 0\}$。在这个理想中存在唯一的首一极小多项式，称为代数元 α 的**极小多项式**，记作 $m_{\alpha,F}(x)$。

包含 F 和 α 的最小域称为由 F 和 α 生成的域，记作 $F(\alpha)$。如果 α 是代数的，那么它同构于商环 $F[x]/(m_{\alpha,F}(\alpha))$，于是我们有公式：

单代数扩张的次数

$$[F(\alpha) : F] = \deg(m_{\alpha,F}(x)) \tag{2}$$

如果 K 的基都是代数元，则称为**代数（的）扩张**；否则，成为**超越扩张**；如果 K 的基都是超越元，则称为**纯超越扩张**。

Exercise 3. 域扩张 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ 是有限的代数扩张，$\sqrt{2}$ 是一个代数元，其极小多项式为 $x^2 - 2$，于是它的扩张次数为 2。

Exercise 4. 域扩张 $\mathbb{Q}(\pi)/\mathbb{Q}$ 是一个（纯）超越扩张，因为 π 为 $\mathbb{Q}$ 的超越元。事实上这个扩域同构于 $\mathbb{Q}$ 上的有理函数环 $\mathbb{Q}(x)$

有限扩张一定是代数扩张，但很容易构造出一个无限的代数扩张。

Exercise 5. 域扩张 $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \ldots, \sqrt{p_i}, \cdots)/\mathbb{Q}$ 为一个无限的代数扩张，其中 p_i 为第 i 个素数，基的每一个元素 $\sqrt{p_i}$ 都是 $\mathbb{Q}$ 上的代数元，极小多项式为 $x^2 - p_i$，但总的扩张次数为

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}, \ldots, \sqrt{p_i}, \cdots) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \cdot [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] \cdot \cdots = \infty \tag{3}$$

1.3 形式导数

对于一个任意交换环上的多项式 $f(x) = \sum_{0 \le i \le n} a_i x^i$，其**形式代数** $f'(x)$ 或 $\mathrm{D}(f(x))$ 定义为

$$f'(x) = \sum_{1 \le i \le n} i a_i x^{i-1} \tag{4}$$

这个公式并不依赖于微积分的极限等概念工具，只是一个“形式上的”表达。这种纯代数性质适用于任何特征域（只有在 Hausdorff 的局部紧群上才能建立极限理论）。

2 可分性与不可分性

2.1 可分与不可分多项式

多项式的根是刻画域结构的关键特征，在 Galois 理论以及分歧理论中有详尽的描述。

一个域 F 上的多项式 $f(x)$ 如果在其**分裂域**（包含其所有根的最小扩域）上是无重根的，则称为**可分的**；反之称为**不可分的**。

直接构造其分裂域来判断多项式的可分性极为困难且不具有性价比。幸而可以同构形式导数提供了一个清晰的判别准则，即：

形式导数对可分性的刻画
一个多项式 $f(x) \in F[x]$ 是可分的，当且仅当其与其形式导数 $f'(x)$ 在 F 中互素，也即 $\gcd(f, f') = 1$.

证明依旧是容易的，只需要对于 $f(x)$ 的一个重根 α，将 $f(x)$ 在某个扩域中写作 $f(x) = (x-\alpha)^k g(x)$，其中 $k \geq 2, g(\alpha) \neq 0$。

不可分是正特征现象
零特征的域上的非零数不可约多项式都是可分的。因为零特征域上的非常数多项式的形式导数必不为 0。

正特征的域上的不可约多项式不可分当且仅当其形式导数为 0。

Exercise 6. 在有理函数域 $F_p(t)$ 上的多项式 $f(x) = x^p - t$ 的形式导数为 0，于是其是不可分多项式。事实上也可以看出 $f(x)$ 有一个 p 重根 $t^{\frac{1}{p}}$。

2.2 完美域

有些域天然地排除了不可分的情形，即如果一个域 F 上的任何代数扩张都是可分扩张，那么域 F 称为完美域。

完美域并不多：

完美域的等价条件
一个域 F 是完美的，当且仅当下列条件之一成立:

1. 零特征。
2. 正特征 p，且 F 上的 Frobenius 自同态 $\phi : a \to a^p$ 是一个自同构。这意味着 ϕ 满射，也即 F 中任一元素可以开 p 次根：$F^p = F$。

Exercise 7. 一切零特征域和有限域都是完美域。对于有限域只要注意到有限集上的满射和单射是等同的。

完美域上的不可约多项式均可分
在完美域上，任何不可约多项式都是可分的。

对于正特征域，注意到若 $f(x)$ 是一个不可约的不可分多项式，那么 $f(x) = g(x^p) = g^p(x)$（Freshman's Dream），于是 $f(x)$ 可约，得到了一个矛盾。

2.3 可分元、不可分元与纯不可分扩张

基于多项式的可分性，我们可以同样对域扩张中的元素和扩张进行分类:

- 一个 F 上的代数元，如果其在 F 上的极小多项式可分，则称为可分元；反正，称为不可分元。
- 一个代数扩张 K/F 如果其中每一个元素 $\alpha \in K$ 都是 F 上的可分元，则称其为一个可分扩张。
- 一个代数扩张 K/F 如果其中每一个元素 $\alpha \in K \setminus F$ 都是 F 上的不可分元，则称其为一个纯不可分扩张。

对于正特征 p 域 F，域扩张 K/F 是纯不可分的当且仅当对任一 $\alpha \in K$，都存在一个非负整数 k 是的 $\alpha^{p^k} \in F$，此时 α 在 F 上的极小多项式必然具有 $x^{p^k} - a^{p^k}$ 形式。

3 扩张次数的结构

一般来讲域扩张的情况比较繁杂，但事实上任何一个域扩张都可以被唯一分解为一个可分部分和不可分部分。这个性质为计算提供了极大的方便。

3.1 可分闭包

对于任一代数扩张 K/f 可以证明一切在 K 中且在 F 上可分的元素构成一个域，这个域被称为 F 在 K 中的**可分闭包**，记作 F_{sep} 或 K_{s}。

可分闭包具有特殊的唯一性：

可分闭包的唯一性
可分闭包是 K/F 中唯一满足下列性质的中间域：

1. F_{sep}/F 为一个可分扩张。
2. K/F_{sep} 为一个纯不可分扩张。

这个定理意味着对于任何代数扩张 K/F 都可以通过插入合适的中间域 F_{sep} 被分解为一个标注的域扩张塔 $F \subseteq F_{\mathrm{sep}} \subseteq K$。它将扩张过程分解为两个概念上截然不同的阶段：首先是一个“行为良好”的可分扩张，引入所有不同的根（或等价地，所有不同的嵌入方式）；然后是一个纯不可分扩张，它不产生新的嵌入，而是通过开 p 次方根的方式“加厚”已有的结构。

3.2 可分次数与不可分次数

通过由可分闭包提供的标准分解，我们可以自然地定义可分次数与不可分次数：

- 扩张 K/F 的可分次数记作 $[K:F]_{\mathrm{s}}$ 定义为可分闭包相对于基域的次数：$[K:F]_{\mathrm{s}} = [F_{\mathrm{sep}}:F]$。
- 扩张 K/F 的不可分次数记作 $[K:F]_{\mathrm{i}}$ 定义为可分闭包相对于基域的次数：$[K:F]_{\mathrm{i}} = [K:F_{\mathrm{sep}}]$。

于是我们得到了域论中最经典的定理之一：

标准域塔的扩张次数

$$[K:F] = [K:F]_{\mathrm{s}} \cdot [K:F]_{\mathrm{i}} \tag{5}$$

事实上可分次数还有更为深刻的定义，这一定义与 Galois 理论相联系。对于一个有限扩张 K/F，其可分次数 $[K:F]_{\mathrm{s}}$ 为从 K 到 F 的某个固定代数闭包 $\overline{F}$ 的所有不同 F-同态个数。

一个 F-同态 $\sigma : K \to \overline{F}$ 将 K 嵌入到 $\overline{F}$ 中。一个可分扩张 K/F 拥有的最大嵌入方式个数即只有 $K:F$ 种；而一个纯不可分扩张则只有一种，即 $[K:F]_{\mathrm{s}} = 1$。

4 单扩张的计算

任何一个域扩张都可以逐步拆分为若干个单扩张，因此我们先提供一个单扩张 $F(\alpha)/F$ 的总次数，可分次数与不可分次数的计算方法。

4.1 确定极小多项式

首先找到 α 在 F 上的极小多项式 $m_{\alpha,F}(x)$，此时可以直接得到域扩张的总扩张次数：

$$[F(\alpha):F] = \deg(m_{\alpha,F}(x)) \tag{6}$$

4.2 分析极小多项式的可分性

接下来可以使用形式导数判断极小多项式的可分性。

1. 计算形式导数 $m'_{\alpha,F}(x)$。
2. 判断
    - 可分情形：若 F 零特征，或正特征且 $m'_{\alpha,F}(x) \neq 0$，则多项式 $m_{\alpha,F}(x)$ 可分。次数扩张 $F(\alpha)/F$ 是可分扩张，其次数为：

  - 可分次数 $[F(\alpha):F]_{\mathrm{s}} = [F(\alpha):F] = \deg(m_{\alpha,F}(x))$
  - 不可分次数 $[F(\alpha):F]_{\mathrm{i}} = 1$
- 不可分情形：若 F 正特征且 $m'_{\alpha,F} = 0$，则极小多项式不可分，进行下一步分解。

4.3 不可分极小多项式的分解

通过之前的讨论我们指导 $m'_{\alpha,F}(x) = 0$ 时 $m_{\alpha,F}(x)$ 必然能够表为一个关于 x^p 的多项式。根据域论中的讨论指导，任何一个正特征 p 的域上的不可约多项式 $p(x)$，存在唯一的整数 $k \geq 0$ 和唯一不可分多项式 $p_{\mathrm{sep}}(x) \in F[x]$，使得

$$p(x) = p_{\mathrm{sep}}(x^{p^k}) \tag{7}$$

于是令 $p(x) = m_{\alpha,F}(x)$，我们可以寻找这个分解：

1. 若 $m_{\alpha,F}(x)$ 中所有指数都可被 p 整除，则令 $m_1(y) = m_{\alpha,F}(x)$，其中 $y = x^p$。
2. 对 m_1 重复过程。
3. 直至得到多项式 $m_k(z)$，其指数不全为 p 的倍数，这个 $m_k(z)$ 成为 $m_{\mathrm{sep}}(x)$，重复的次数 k 就是分解式中的次数。

4.4 从分解式计算次数

一旦完成这个极小多项式的分解 $m_{\alpha,F}(x) = m_{\mathrm{sep}}(x^{p^k})$，可分次数与不可分次数可以直接读出：

- 可分次数为可分部分的次数：$[F(\alpha):F]_{\mathrm{s}} = \deg(m_{\mathrm{sep}})$。
- 不可分次数为特征的幂次：$[F(\alpha):F]_{\mathrm{i}} = p^k$。

容易验证这个结果是相容的：

$$[F(\alpha):F] = \deg(m_{\alpha,F}(x)) = \deg(m_{\mathrm{sep}}) \cdot p^k = [F(\alpha):F]_{\mathrm{s}} \cdot [F(\alpha):F]_{\mathrm{i}} \tag{8}$$

在此情况下，可分闭包 F_{sep} 也已经具体确定。因为 α^{p^k} 为可分多项式 $m_{\text{sep}}(x)$ 的一个根，所以元素 α^{p^k} 可分，尤其生成的扩张是一个可分扩张。容易看到这就是 $F(\alpha)/F$ 的可分闭包，即

$$F_{\text{sep}} = F(\alpha^{p^k}) \tag{9}$$

5 一般的有限扩张

由多个元素生成的扩张或由多项式定义的扩张都可以通过单扩张分解和域塔规律计算。

5.1 塔律

总扩张次数在域塔 $F \subseteq L \subseteq M$ 中满足乘法规则 $[M:F] = [M:L] \cdot [L:F]$，一个深刻的结果是这个乘法性质同样适用于可分次数和不可分次数：

可分次数与不可分次数的塔律

$$[M:F]_{\text{s}} = [M:L]_{\text{s}} \cdot [L:F]_{\text{s}} \tag{10}$$

$$[M:F]_{\text{i}} = [M:L]_{\text{i}} \cdot [L:F]_{\text{i}} \tag{11}$$

可分次数的乘法规则可以通过同态计数得到证明，不可分次数的乘法规则将由总次数和可分次数得到。

5.2 将复杂扩张分解为单扩张塔

任何有限扩张 K/F 可以通过有限个生成元 $\alpha_1, \cdots, \alpha_n$ 得到，即 $K = F(\alpha_1, \cdots, \alpha_n)$，这样的扩张可以自然地表成一个单扩张塔：

$$F \subseteq F(\alpha_1) \subseteq \cdots \subseteq F(\alpha_1, \cdots, \alpha_n) = K \tag{12}$$

因此对于一个复杂扩张 K/F, 我们可以通过将其分解为单扩张塔, 并计算每一步扩张的总次数, 可分次数和不可分次数。最后使用乘法规则组合成为整体扩张 K/F 的次数。

对于由一个多项式 $f(x)$ 定义的域扩张 K/F，即 K 为 $f(x) \in F[x]$ 在 F 上的分裂域。其计算遵循相同的规则，只需要设 $f(x)$ 的根为 $\alpha_1, \cdots, \alpha_n$，之后可以进行完全类似的计算。

6 一些例子

陈列一些计算的例子。

Exercise 8 (可分扩张 $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$)**.** 这是一个零特征域上的扩张，因此必定可分，这一点可以通过计算验证。

考虑域扩张塔 $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$。

对于第一步 $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$，其极小多项式为 $m(x) = x^2 - 2$，故总次数 $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$。

在形式上 $m'(x) = 2x \neq 0$，于是可分次数 $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]_{\mathrm{s}} = 2$，不可分次数 $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]_{\mathrm{i}} = 1$。

对于第二步 $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}(\sqrt{2})$，其化零多项式为 $p(x) = x^2 - 3$。当然对于 $p(x)$ 是极小多项式这一点还需要证明其是不可约的，这需要一些声明，但本文直接承认。于是扩张总次数 $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$。

又因为零特征，扩张必定可分，于是可分次数 $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})]_{\mathrm{s}} = 2$，不可分次数 $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})]_{\mathrm{i}} = 1$。

最后应用塔律，得到总扩张次数 $[\mathbb{Q}(\sqrt{2}, \sqrt{3} : \mathbb{Q})] = 4$，可分次数 $[\mathbb{Q}(\sqrt{2}, \sqrt{3} : \mathbb{Q})]_{\mathrm{s}} = 4$，不可分次数 $[\mathbb{Q}(\sqrt{2}, \sqrt{3} : \mathbb{Q})]_{\mathrm{i}} = 1$。

结果表明这是一个次数为 4 的可分扩张。

Exercise 9 (纯不可分扩张 $\mathbb{F}_p(t^{\frac{1}{p}})/\mathbb{F}_p(t)$)**.** 这是一个典型的纯不可分扩张，令 $F = \mathbb{F}_p(t)$，$K = F(t^{\frac{1}{p}})$，生成元 $\alpha = t^{\frac{1}{p}}$。

其极小多项式为 $m(x) = x^p - t$, 利用 Eisenstein 判别法知道这是不可约的。因此总次数 $[K : F] = p$。

对于极小多项式的形式导数有 $m'(x) = 0$，是不可分的，并且可以分解为 $m(x) = m_{\text{sep}}(x^p)$，其中 $m_{\text{sep}}(y) = y - t$，这里 $k = 1$。

于是得到可分次数 $[K : F]_{\text{s}} = \deg(m_{\text{sep}}) = 1$，不可分次数 $[K : F]_{\text{i}} = p^1 = p$。

Exercise 10 (混合扩张)**.** 考虑一个同时包含可分域不可分部分的扩张。设基域 $F = \mathbb{F}_p(t)$，扩域 $K = F(\alpha, \beta)$，其中 α 为 $x^p - t$ 的根，β 为某个 F 上次数为 d 的不可约多项式 $q(y)$ 的根。

将其分解为域塔 $F \subseteq F(\alpha) \subseteq F(\alpha, \beta) = K$。

对于第一步，根据上一个例子，这是一个纯不可分扩张，各次数参考上例。

对于第二步，我们需要确定 β 在 $F(\alpha)$ 上的极小多项式。需要指出的一个定理是，一个在基域上的不可约可分多项式，在一个纯不可分扩张 E/F 上仍然保持不可约。于是这是一个可分扩张。

最后应用塔律就有总次数 $[K : F] = pd$，可分次数 $[K : F]_{\text{s}} = d$，不可分次数 $[K : F]_{\text{i}} = p$。