# Krull 拓扑与广义 Galois 对应

Aug 2025

## 1 Galois 理论拓扑方法的动机

有限域扩张的 Galois 理论取得了极大的成功，完全解决了根式可解性与尺规作图等问题，是二十世纪之前的代数学中最优美，最完整的理论（之一）。

但当考虑无限域扩张时，经典的 Galois 不足以对其给出一个完整的刻画，并且对于一些 Galois 群的子群，我们甚至无法找到对应的不动域。

Wolfgang Krull 在 1928 年正式引入了 Krull 拓扑的概念，为 Galois 群赋予了拓扑结构，重建了 Galois 的现代理论。

### 1.1 有限 Galois 对应的回顾

**有限 Galois 理论的基本定理**为有限 Galois 扩张 $L/K$ 建立了完整的对应关系。定理断言，在扩张 $L/K$ 的中间域 $E$ 的集合与 Galois 群 $G = \mathrm{Gal}(L/K)$ 的子群 $H$ 的集合之间，存在一个反向包含的**一一对应**。

该对应由两个互逆的映射给出：

1. **从中间域到子群的映射**：$E \mapsto \mathrm{Gal}(L/E)$，即 $G$ 中固定 $E$ 中所有元素的自同构组成的子群。
2. **从子群到中间域的映射**：$H \mapsto L^H$，即 $L$ 中被 $H$ 中所有自同构固定的元素组成的域，称为 $H$ 的固定域。

其中最重要的性质包括：

**有限 Galois 对应的性质**

- **次数与指数的关系**：$[E : K] = [G : \mathrm{Gal}(L/E)]$，同时也有 $[L : E] = |\mathrm{Gal}(L/E)|$。

- 正规扩张与正规子群的对应：中间域 $E$ 为 $K$ 的正规扩张（等价地，Galois 扩张）等且仅当其对应的子群 $\mathrm{Gal}(L/E)$ 是 $G$ 的正规子群。此时，商群 $G/\mathrm{Gal}(L/E)$ 同构于扩张 $E/K$ 的 Galois 群 $\mathrm{Gal}(E/K)$。

### 1.2 对应关系在无限扩张中的失效

当语境由有限转向无限时会发现，一个无限 Galois 扩张的 Galois 群所拥有的子群数量远远超过了中间域的数量，意味着这个对应关系不可能再是一一的，存在着多个子群可能拥有完全一致的固定域的情况。

**Exercise 1.** 我们将奇素数分成两组，其中 $P = \{p_i\}_{i\geq 1}, Q = \{q_j\}_{j\geq 1}$，$p_i$ 遍历所有 $4k+1$ 型素数，$q_j$ 遍历所有 $4k+3$ 型素数。

令 $K = \mathbb{Q}$，并令 $L = \mathbb{Q}(\sqrt{3}, \sqrt{5}, \cdots)$ 为通过添加一切奇素数的平方根生成的域。这是一个无限次的 Galois 扩张，其 Galois 群 $G = \mathrm{Gal}(L/\mathbb{Q})$ 同构于无限个二阶循环群的直积（读者可以亲自验证这一点）：

$$G \cong \prod_{p \text{ is prime}} \mathbb{Z}/2\mathbb{Z} \tag{1}$$

我们将构造两个子群，他们具有一致的固定域：考虑 $\tau_i$ 为这样一个自同构，它将 $\sqrt{p_i} \mapsto -\sqrt{p_i}$，同时 $\sqrt{q_i} \mapsto -\sqrt{q_i}$，并固定其他所有的 $\sqrt{p_j}$ 和 $\sqrt{q_j} (j \neq i)$。

令 $H_1 = \langle \tau_1, \tau_2, \cdots \rangle_{\text{代数生成}}, H_2 = \langle \rho_1, \rho_2, \cdots \rangle_{\text{代数生成}}$ 为两个子群，其中 $\rho_i = \tau_i \tau_{i+1}$，它们显然是不同的。

然而我们发现它们的固定域是相同的，均为 $C = \mathbb{Q}(\sqrt{p_1 q_1}, \sqrt{p_2 q_2}, \cdots)$。

这个例子已经表明，从子群到固定域的映射 $L \mapsto L^H$ 不再是单射，因此经典的 Galois 失效。

### 1.3 Krull 的观察

于是 Krull 提出要为 Galois 群 $G$ 赋予一个自然的拓扑结构。他的观察是，并非 $G$ 的所有子群都有完全等同的代数意义，那些能够通过取固定域，再取 Galois 群而恢复自守的良好子群，恰好成为这

个拓扑下的闭子群。

# 2 Krull 拓扑的定义

Krull 拓扑有两种等价的定义方式，一种基于邻域基的拓扑语言，另一种基于逆向极限的代数语言。这种等价性恰恰是无限 Galois 理论的精妙之处。

## 2.1 邻域基方法

设 $L/K$ 是一个 Galois 扩张，$G = \mathrm{Gal}(L/K)$ 为其 Galois 群。由于 $G$ 为一个群，其拓扑结构由单位元 $1 \in G$ 处的邻域基完全确定，其他元素处的邻域基可以通过平移得到。

**Krull 拓扑的直观定义**
Krull 拓扑在单位元 $1 \in G$ 处的开邻域基由所有形如 $\mathrm{Gal}(L/F)$ 的子群构成，其中 $F$ 遍历 $L/K$ 的所有**有限次**中间子扩张。

对于任意一个元素 $\sigma \in G$ 其一个开邻域基由所有形如 $\sigma \cdot \mathrm{Gal}(L/F)$ 的左陪集构成，其中 $F$ 同样遍历所有有限次中间子扩张。拓扑空间中的任意一个开集，就是这些陪集的并集。

## 2.2 逆向极限方法

一个无限 Galois 扩张 $L/K$ 可以看作是其所有有限 Galois 子扩张 $F_i/K$ 的并集（或合成域）。这些有限 Galois 子扩张在域的包含关系下构成一个有向集。

对于任意两个有限 Galois 子扩张 $F_i \subseteq F_j$，存在一个自然的限制同态：

$$\mathrm{res}_{j,i} : \mathrm{Gal}(F_j/K) \to \mathrm{Gal}(F_i/K) \tag{2}$$

定义为 $\sigma \mapsto \sigma|_{F_i}$。这些有限 Galois 群和它们之间的限制同态构成了一个群的**逆向系统**。

无限 Galois 群 $G = \mathrm{Gal}(L/K)$ 与这个逆向系统的**逆向极限**存在一个典范同构：

$$G \cong \varprojlim_{F_i/K \text{ finite Galois}} \mathrm{Gal}(F_i/K) \tag{3}$$

逆向极限的元素是一个协调的自同构序列 $\{\sigma_i\}_i$，其中每个 $\sigma_i \in \mathrm{Gal}(F_i/K)$，并且当 $F_i \subseteq F_j$ 时，满足协调性条件 $\mathrm{res}_{j,i}(\sigma_j) = \sigma_i$。

我们可以为这个逆向极限赋予一个自然的拓扑：

**Krull 拓扑的极限定义**

首先为每一个有限群 $\mathrm{Gal}(F_i)/K$ 赋予离散拓扑。

然后在其直积空间 $\prod_i \mathrm{Gal}(F_i/K)$ 上赋予乘积拓扑。

最后，逆向极限 $G$ 作为该直积空间的子空间，继承其子空间拓扑，这个拓扑被称为**逆向极限拓扑**。

再次声明一个核心的结论是，通过邻域基定义的 Krull 拓扑与通过逆向极限构造赋予的拓扑是完全等同的。邻域基定义中的基本开集 $\sigma \cdot \mathrm{Gal}(L/F)$ 在你继续视角下，恰好是那些在分量 $\mathrm{Gal}(F/K)$ 上的投影等于 $\sigma|_F$ 的元素。这正式乘积拓扑中基本开集在逆向极限上的诱导形式。

### 2.3 Galois 群作为一个拓扑群

Krull 拓扑的一个关键性质是它是的 $G = \mathrm{Gal}(L/K)$ 称为一个拓扑群。这意味着群的乘法和求逆运算都是连续的。

- **乘法连续型**：映射 $m : G \times G \to G, (\sigma, \tau) \mapsto \sigma\tau$ 连续。
- **求逆连续性**：映射 $i : G \to G, \sigma \mapsto \sigma^{-1}$ 连续。

可以使用邻域基的定义来证明之，以乘法映射为例。只要证明对于 $\sigma\tau$ 的任意一个邻域 $U = \sigma\tau \cdot \mathrm{Gal}(L/F)$，都存在 $\sigma$ 的邻域 $V = \sigma \cdot \mathrm{Gal}(L/F')$，$\tau$ 的邻域 $W = \tau \cdot \mathrm{Gal}(L/F'')$ 使得 $V \cdot W \subseteq U$。

这里关键在于，我们可以不是一般性假设 $F/K$ 是 Galois 扩张，这是因为任何有限扩张都包含在一个有限 Galois 扩张内。对于一个有限 Galois 扩张 $F/K$，其对应的子群 $\mathrm{Gal}(L/F)$ 在 $G$ 中是

正规的。这是因为对于任意 $\tau \in G, \tau(F)$ 为 $F$ 在 $L$ 中的一个共轭域。由于 $F/K$ 是正规的，于是 $\tau(F) = F$。由此可知 $\tau \mathrm{Gal}(L/F)\tau^{-1} = \mathrm{Gal}(L/\tau(F)) = \mathrm{Gal}(L/F)$。

最后我们可以选择 $F = F' = F''$，则

$$(\sigma\cdot\mathrm{Gal}(L/F))\cdot(\tau\cdot\mathrm{Gal}(L/F)) = \sigma(\mathrm{Gal}(L/F)\tau)\mathrm{Gal}(L/F) = \sigma(\tau\mathrm{Gal}(L/F))\mathrm{Gal}(L/F) = \sigma\tau\cdot\mathrm{Gal}(L/F)$$

这表明乘法是连续的。类似可以证明求逆同样连续。

# 3 Galois 群的投射有限性质

赋予了 Krull 拓扑的 Galois 群 $G = \mathrm{Gal}(L/K)$ 有三个经典的性质：**紧性**，**Hausdorff 性**和**完全不连通性**。这三个性质恰好是射影有限群的拓扑学定义。这一结论是无限 Galois 理论中最重要的结构性成果，也是本节的主题。

## 3.1 紧性

**紧性**

赋予 Krull 拓扑的 Galois 群 $G$ 是一个紧拓扑空间。

通过逆向极限可以得到一个简洁的证明。

首先在逆向极限的构造中，每一个有限群 $\mathrm{Gal}(F_i/K)$ 都被赋予了离散拓扑，这必然是紧空间。根据拓扑学中的 Tychonoff 定理，任意多个紧空间的乘积空间在其乘积拓扑下也是紧空间。因此直积空间 $\prod_i \mathrm{Gal}(F_i/K)$ 是一个紧空间。

逆向极限 $G \cong \varprojlim \mathrm{Gal}(F_i/K)$ 是直积空间的一个子空间。容易证明这个子空间是闭的，因为逆向极限定义中的条件 $\mathrm{res}_{j,i}(\sigma_j) = \sigma_i$ 可以看作两个连续映射的等化子，而 Hausdorff 空间中的等化子是闭集。故又因紧空间的闭子集是紧的，$G$ 自身也是紧的。

此外还可以使用超滤子，通过将定义在有限子扩张上的“局部”同态“粘合”起来，构造出超滤子的极限点，从而证明空间的紧性。

### 3.2 Hausdorff 性

**Hausdorff 性**
赋予了 Krull 拓扑的 Galois 群 $G$ 是一个 Hausdorff 空间（T2 空间）

我们取任意两个不同元素 $\sigma \neq \tau \in G$。根据定义，他们作为自同构是不同的，因此必然存在某个元素 $\alpha \in L$ 使得它们的像不同。

元素 $\alpha$ 为 $K$ 上的代数元，因此它属于某个 $L/K$ 的有限次子扩张，如 $F = K(\alpha)$。考虑两个基本开邻域：$U = \sigma \cdot \mathrm{Gal}(L/F)$ 和 $V = \tau \cdot \mathrm{Gal}(L/F)$。

邻域 $U$ 中所有元素在 $F$ 上的作用都与 $\sigma$ 一致，而邻域 $V$ 中所有元素在 $F$ 上的作用都与 $\tau$ 一致，但由 $\alpha$ 的取法我们知道 $\sigma|_F \neq \tau|_F$ 故它们属于两个不相交的陪集。

### 3.3 完全不连通性

赋予 Krull 拓扑的 Galois 群 $G$ 是一个完全不连通空间。

在一个拓扑群中，任何一个开子集也是闭子集。

任何一个不等于单位元的元素 $\sigma \in G$ 必定会移动 $L$ 中的某个元素 $\alpha$。这个元素属于某个有限扩张 $F = K(\alpha)$，因此 $\sigma \notin \mathrm{Gal}(L/F)$。这意味着所有形如 $\mathrm{Gal}(L/K)$ 的开子群的交集只有单位元：

$$\{1\} = \bigcap_{F/K \text{ finite}} \mathrm{Gal}(L/F) \tag{4}$$

若 $C$ 为一个包含单位元的连通分支，对于任何一个开（同时闭）子群 $H_F$，集合 $C$ 必须完全包含于 $H_F$ 内部。否则 $C \cap H_F$ 和 $C \setminus H_F$ 将成为一个非平凡分割。

因此，$C$ 必须包含于一切开子群之交，那么只能有 $C = \{1\}$。由由于拓扑群是齐性空间，所以每个点的连通分支都只是该点本身，因此完全不连通。

这三个性质共同定义了一个**射影有限空间**。由于 $G$ 同时还是一个拓扑群，因此它是一个射影有限群。这一结论意义重大，它将无限 Galois 群的研究与一个更广泛的代数领域联系起来。诸如数论中的绝对 Galois 群 $\mathrm{Gal}(\overline{\mathbb{Q}}, \mathbb{Q})$、p-adic 整数群 $\mathbb{Z}_p$ 以及代数几何中的 étale 基本群等核心研究对象，

都属于射影有限群。Krull 拓扑不仅修复了 Galois 对应，更重要的是，它揭示了无限 Galois 群的普适结构，使得我们可以将射影有限群理论中的强大工具（如 Sylow 理论、上同调理论等）直接应用于无限域扩张的研究。

# 4 无限 Galois 群基本定理

在为 Galois 群赋予了 Krull 拓扑之后，我们终于得以陈述无限 Galois 理论的基本定理。

## 4.1 定理的陈述

**无限 Galois 群基本定理**
设 $L/K$ 为一个 Galois 扩张，令 $G = \mathrm{Gal}(L/K)$ 为其赋予了 Krull 拓扑的 Galois 群，则存在一个反向包含的一一对应关系，介于：

- $L/K$ 的所有**中间域** $M$ 的集合。
- $G$ 的所有**闭子群** $H$ 的集合

这个双射由两个互逆的映射给出：

- **从域到群**：$M \mapsto \mathrm{Gal}(L/M)$
- **从群到域** $H \mapsto L^H$

我们在此不提供该定理的证明，只指出证明的框架：

1. $\mathrm{Gal}(L/M)$ 为一个闭子群。
2. $L^{\mathrm{Gal}(L/M)} = M$。
3. 对于闭子群 $H$，有 $\mathrm{Gal}(L, L^H) = H$。

### 4.2 对应关系的细化

这个基本定理还可以进一步喜欢，将中间域的代数性质与对应闭子群的拓扑和代数性质联系起来，足矣推广有限情况下的结论。

- 有限扩张 $\leftrightarrow$ 开子群

  一个中间扩张 $M/K$ 是有限次的，当且仅当 $\mathrm{Gal}(L/M)$ 是 $G$ 中的开子群。

  如果 $M/K$ 有限次，那么 $\mathrm{Gal}(L/M)$ 本身就是单位元的一个基本邻域，因此是开集。

  反之，若一个子群 $H$ 是开的，它必定包含一个基本邻域 $\mathrm{Gal}(L/F)$。因此 $L^H \subseteq F$，故 $L^H/K$ 为有限扩张。

- 次数-指数关系

  如果 $M/K$ 为一个有限扩张，那么扩张次数 $[M : K]$ 等于对应子群 $\mathrm{Gal}(L/M)$ 在群 $G$ 中的指数 $[G : \mathrm{Gal}(L/M)]$。这与有限 Galois 理论中的情况是一致的。

- 正规扩张 $\leftrightarrow$ 正规子群

  一个中间扩张 $M/K$ 是正规扩张当且仅当其对应的闭子群 $\mathrm{Gal}(L/M)$ 是 $G$ 的正规子群。

  此时存在一个典范的拓扑群同构：

  $$\mathrm{Gal}(M/K) \cong G/\mathrm{Gal}(L/M) \tag{5}$$

  该映射由限制映射 $G \to \mathrm{Gal}(M/K)$ 诱导，其核恰好是 $\mathrm{Gal}(L/M)$。

## 5 经典的例子：有限域的绝对 Galois 群

本节将应用基本定理，分析一个典型例子：有限域 $\mathbb{F}_p$ 的代数闭包 $\overline{\mathbb{F}_p}$ 对 $\mathbb{F}_p$ 的 Galois 理论。这个例子是数论中极少见的已经具有清晰结构的绝对 Galois 群的例子，与之相对的整体情形下，有理数域 $\mathbb{Q}$ 的绝对 Galois 理论至今仍未得到阐明。

### 5.1 域扩张 $\overline{\mathbb{F}_p}/\mathbb{F}_p$

正特征 $p$ 的有限域 $\mathbb{F}_p$ 的代数闭包 $\overline{\mathbb{F}_p}$ 可以看作是一切有限域 $\mathbb{F}_{p^n}(n \geq 1)$ 的并集。

$$\overline{\mathbb{F}_p} = \bigcup_{n \geq 1} \mathbb{F}_{p^n} \tag{6}$$

这是一个无限次的 Galois 扩张。由于有限域是完美域，所有代数扩张都是可分的。同时又因为这是所有以 $\mathbb{F}_p$ 为系数的多项式的分裂域的并集，它也是正规的。于是这是一个 Galois 扩张。

这个扩张的中间域结构非常简单：对于每一个正整数 $n$，存在唯一一个阶为 $p^n$ 的子域 $\mathbb{F}_{p^n}$。它们构成了 $\overline{\mathbb{F}_p}/\mathbb{F}_p$ 的所有有限次中间域。其格结构是一个由整除关系定义的线序之并：$\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$ 当且仅当 $m|n$。

### 5.2 Galois 群 $G = \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$

考虑 Frobenius 自同构：$\phi : x \mapsto x^p$ 是一个（有限域上的）域自同构，于是有 $\phi \in G$

对于任何有限子扩张 $\mathbb{F}_{p^n}/\mathbb{F}_p$，其 Galois 群是 $n$ 阶循环群，由 $\phi$ 在 $\mathbb{F}_{p^n}$ 上限制生成。因此 $G$ 为这些有些循环群的逆向极限：

$$G = \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) \cong \varprojlim_n \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \varprojlim_n (\mathbb{Z}/n\mathbb{Z}) \tag{7}$$

这个逆向极限正是射影有限整数群（profinite integers）的定义，记作 $\hat{\mathbb{Z}}$。因此我们得到了一个核心同构：

$$G \cong \hat{\mathbb{Z}} \tag{8}$$

$\hat{\mathbb{Z}}$ 也可以同构中国剩余定理看作一切 p-adic 整数环 $\mathbb{Z}_p$ 的直积：

$$\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p \tag{9}$$

Frobenius 自同构 $\phi$ 并不是 $G$ 的一个生成元，因为 $G \cong \hat{\mathbb{Z}}$ 是一个不可数群，而由 $\phi$ 生成的循环子群注定可数。然而这个子群 $\langle\phi\rangle$ 在 $G$ 的 Krull 拓扑下的稠密的。因此 $\phi$ 是 $G$ 的一个**拓扑生成元**。

### 5.3 Galois 对应

现在我们可以将 $\overline{\mathbb{F}_p}/\mathbb{F}_p$ 的中间域格域 $\hat{\mathbb{Z}}$ 的闭子群格进行明确的对应：

- $\hat{\mathbb{Z}}$ 的闭子群：$\hat{\mathbb{Z}}$ 的开子群恰好是所有形如 $n\hat{\mathbb{Z}}$ 的子群，其中 $n$ 为一个正整数。这些子群的指数为 $n$。此外 $\hat{\mathbb{Z}}$ 还有其他的非空闭子群，但据 Galois 对应，只有开子群才对应于有限扩张。
- 双射关系

  根据定理，有限次中间域 $\mathbb{F}_{p^n}$ 对应于 $G$ 的一个开子群，即 $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$。

  一个自同构 $\sigma \in G$ 固定 $\mathbb{F}_{p^n}$ 当且仅当 $\sigma(x) = x$ 对一切 $x \in \mathbb{F}_{p^n}$ 成立。这等价于 $\sigma$ 的作用是 Frobenius 自同构的 $n$ 次幂的某个幂次。

  因此 $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ 是由 $\phi^n$ 拓扑生成的闭子群。在 $G \cong \hat{\mathbb{Z}}$ 的同构移一下，$\phi$ 对应于 $1 \in \hat{\mathbb{Z}}$，所以 $\phi^n$ 对应于 $b \in \hat{\mathbb{Z}}$。由 $n$ 拓扑生成的子群恰是 $n\hat{\mathbb{Z}}$。

  于是我们有一个完整对应：

$$\mathbb{F}_{p^n} \longleftrightarrow n\hat{\mathbb{Z}} \subseteq \hat{\mathbb{Z}} \tag{10}$$

- 我们可以与之前的理论进行检验，如：

  有限 $\leftrightarrow$ 开：$\mathbb{F}_{p^n}/\mathbb{F}_p$ 是有限扩张，其对应的子群 $n\hat{\mathbb{Z}}$ 是 $\hat{\mathbb{Z}}$ 的开子群。

  次数 $\leftrightarrow$ 指数：扩张次数 $[\mathbb{F}_{p^n}/\mathbb{F}_p] = n$。对应地，子群的指数 $[\hat{\mathbb{Z}} : n\hat{\mathbb{Z}}] = n$。

  正规 $\leftrightarrow$ 正规：所有中间扩张 $\mathbb{F}_{p^n}/\mathbb{F}_p$ 都是 Galois 扩张。对应地，$\hat{\mathbb{Z}}$ 是一个阿贝尔群（射影循环群），因此其所有子群均是正规的。