

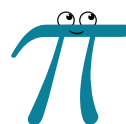
# Galois 理论 - 笔记

作者: 若水

邮箱: [ethanmxzhou@163.com](mailto:ethanmxzhou@163.com)

主页: [helloethanzhou.github.io](https://helloethanzhou.github.io)

时间: July 18, 2024





Après cela, il y aura, j'espère, des gens qui trouveront leur profit à déchiffrer tout ce gâchis.

— Evariste Galois

# 目录

<b>第一章 Galois 扩张</b>	<b>1</b>
1.1 Galois 对应 . . . . .	1
1.2 Artin 引理 . . . . .	3
1.3 Dedekind 无关性引理 . . . . .	4
1.4 有限 Galois 扩张 . . . . .	4
<b>第二章 Galois 理论基本定理</b>	<b>5</b>
<b>附录 A 群论</b>	<b>6</b>
<b>附录 B 环论</b>	<b>7</b>
<b>附录 C 域论</b>	<b>8</b>
C.1 基本概念 . . . . .	8

# 第一章 Galois 扩张

## 1.1 Galois 对应

### 定义 1.1.1 (域扩张)

对于域  $k$  与  $K$ , 称  $K/k$  为域扩张, 如果存在同态映射  $\varphi: k \rightarrow K$ .

### 定义 1.1.2 (中间域)

对于域扩张  $k \subset F \subset K$ , 称  $F$  为  $K/k$  的中间域。

### 定义 1.1.3 (自同构群)

定义域  $K$  的自同构群为

$$\text{Aut}(K) = \{\text{同构映射 } \varphi: K \rightarrow K\}$$

### 定义 1.1.4 ( $k$ -自同构群)

定义域扩张  $K/k$  的  $k$ -自同构群为

$$\text{Aut}_k(K) = \{\text{同构映射 } \varphi: K \rightarrow K \mid \varphi(x) = x, \forall x \in k\}$$

**证明** 我们来证明  $\text{Aut}_k(K)$  关于映射的复合构成群。

对于封闭性, 任取  $\varphi, \psi \in \text{Aut}_k(K)$ , 由于  $\varphi, \psi: K \rightarrow K$  为同构映射, 那么  $\varphi \circ \psi: K \rightarrow K$  为同构映射。由于  $\varphi|_k = \psi|_k = \mathbb{1}_k$ , 那么  $(\varphi \circ \psi)_k = \mathbb{1}_k$ , 进而  $\varphi \circ \psi \in \text{Aut}_k(K)$ 。

对于单位元, 显然  $\mathbb{1}_K \in \text{Aut}_k(K)$ , 且对于任意  $\varphi \in \text{Aut}_k(K)$ , 成立

$$\varphi \circ \mathbb{1}_K = \mathbb{1}_K \circ \varphi = \varphi$$

因此  $\mathbb{1}_K$  为  $\text{Aut}_k(K)$  的单位元。

对于逆元, 任取  $\varphi \in \text{Aut}_k(K)$ , 显然  $\varphi^{-1}: K \rightarrow K$  成立

$$\varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = \mathbb{1}_K$$

因此  $\varphi^{-1}$  为  $\varphi$  的逆元。

对于交换律, 这对映射的复合显然是成立的。

综上所述,  $\text{Aut}_k(K)$  关于映射的复合构成群。

### 定义 1.1.5 (不动域)

对于域扩张  $K/k$ , 定义子群  $G < \text{Aut}_k(K)$  的不动域为

$$\text{Inv}_K(G) = \{x \in K \mid \varphi(x) = x, \forall \varphi \in G\}$$

**证明** 我们来证明  $\text{Inv}_K(G)$  构成域。

显然  $\text{Aut}_k(K)$  对加法和乘法封闭, 这是因为  $\varphi(x+y) = \varphi(x) + \varphi(y)$  且  $\varphi(xy) = \varphi(x)\varphi(y)$ 。

显然  $K$  的加法单位元  $0$  和乘法单位元  $1$  分别为  $\text{Inv}_K(G)$  的加法单位元和乘法单位元, 这是因为  $0, 1 \in k$ 。

对于任意  $x \in K$ , 显然  $x$  在  $K$  中的加法逆元  $-x$  和乘法逆元  $x^{-1}$  (此时要求  $x \neq 0$ ) 分别为  $x$  在  $\text{Inv}_K(G)$  中的加法逆元和乘法逆元, 这是因为对于  $\varphi \in G$ ,  $\varphi(-x) = -x$  且  $\varphi(x^{-1}) = \varphi(x)^{-1}$ 。

显然  $\text{Aut}_k(K)$  对于加法和乘法满足交换律和结合律以及分配律, 这是因为  $K$  对于加法和乘法满足交换律和结合律以及分配律。

综上所述,  $\text{Inv}_K(G)$  构成域。

**定义 1.1.6 (Galois 对应)**

称域扩张  $K/k$  的 Galois 对应为

$$\begin{aligned} \{\text{域扩张 } K/k \text{ 的中间域}\} &\longleftrightarrow \{\text{自同构群 } \text{Aut}_k(K) \text{ 的子群}\} \\ F &\longmapsto \text{Aut}_F(K) \\ \text{Inv}_K(G) &\longleftarrow G \end{aligned}$$

**证明** 任取  $K/k$  的中间域  $F$ , 对于任意  $\sigma \in \text{Aut}_F(K)$ , 那么  $\sigma: K \rightarrow K$  为同构映射, 且  $\sigma|_F = 1_F$ 。由于  $k \subset F$ , 因此  $\sigma|_k = 1_k$ , 于是  $\sigma \in \text{Aut}_k(K)$ , 进而  $\text{Aut}_F(K) \subset \text{Aut}_k(K)$ 。由  $k$ -自同构群的定义 1.1.4,  $\text{Aut}_F(K)$  构成群, 进而  $\text{Aut}_F(K)$  为  $\text{Aut}_k(K)$  的子群。

任取  $\text{Aut}_k(K)$  的子群  $G$ , 由不动域的定义 1.1.5,  $\text{Aut}_F(K)$  构成  $K$  的子域。而由  $k$ -自同构群的定义 1.1.4,  $k \subset \text{Aut}_F(K)$ , 进而  $\text{Aut}_F(K)$  构成  $K/k$  的中间域。

**定义 1.1.7 (Galois 群)**

定义域扩张  $K/k$  关于中间域  $F$  的 Galois 群为

$$\text{Gal}(K/F) = \text{Aut}_F(K)$$

**注** 为了方便, 对于域扩张  $K/k$  的 Galois 对应, 引入记号

$$\mathcal{F} = \{\text{域扩张 } K/k \text{ 的中间域}\}, \quad \mathcal{G} = \{\text{自同构群 } \text{Aut}_k(K) \text{ 的子群}\}, \quad \text{Gal}(F) = \text{Gal}(K/F), \quad \text{Inv}(G) = \text{Inv}_K(G)$$

**引理 1.1.8**

对于域扩张  $K/k$ , Galois 对应  $\text{Gal}: \mathcal{F} \rightarrow \mathcal{G}$  与  $\text{Inv}: \mathcal{G} \rightarrow \mathcal{F}$  为反序映射, 换言之——

1. 对于  $F_1, F_2 \in \mathcal{F}$ , 如果  $F_1 \subset F_2$ , 那么  $\text{Gal}(F_1) \supset \text{Gal}(F_2)$ 。
2. 对于  $G_1, G_2 \in \mathcal{G}$ , 如果  $G_1 \subset G_2$ , 那么  $\text{Inv}(G_1) \supset \text{Inv}(G_2)$ 。

**证明** 对于 1, 任取  $F_1, F_2 \in \mathcal{F}$ , 使其成立  $F_1 \subset F_2$ 。任取  $\varphi \in \text{Gal}(F_2)$ , 那么  $\varphi: K \rightarrow K$  为同构映射, 且  $\varphi|_{F_2} = 1_{F_2}$ , 因此  $\varphi|_{F_1} = 1_{F_1}$ , 进而  $\varphi \in \text{Gal}(F_1)$ 。由  $\varphi$  的任意性,  $\text{Gal}(F_1) \supset \text{Gal}(F_2)$ 。

对于 2, 任取  $G_1, G_2 \in \mathcal{G}$ , 使其成立  $G_1 \subset G_2$ 。任取  $x \in \text{Inv}(G_2)$ , 那么对于任意  $\varphi \in G_2$ , 成立  $\varphi(x) = x$ , 因此对于任意  $\varphi \in G_1$ , 成立  $\varphi(x) = x$ , 进而  $x \in \text{Inv}(G_1)$ 。由  $x$  的任意性,  $\text{Inv}(G_1) \supset \text{Inv}(G_2)$ 。

**引理 1.1.9**

对于域扩张  $K/k$  的 Galois 对应  $\text{Gal}: \mathcal{F} \rightarrow \mathcal{G}$  与  $\text{Inv}: \mathcal{G} \rightarrow \mathcal{F}$ , 如果  $F \in \mathcal{F}$  且  $G \in \mathcal{G}$ , 那么

$$F \subset \text{Inv}(\text{Gal}(F)), \quad G \subset \text{Gal}(\text{Inv}(G))$$

**证明** 对于左式, 由于

$$\begin{aligned} x \in F &\implies (x \in K) \text{ 且 } (\forall \text{同构映射 } \varphi: K \rightarrow K \quad (\varphi|_F = 1_F \implies \varphi(x) = x)) \\ &\iff (x \in K) \text{ 且 } (\forall \varphi \in \text{Gal}(F), \varphi(x) = x) \\ &\iff x \in \text{Inv}(\text{Gal}(F)) \end{aligned}$$

那么  $F \subset \text{Inv}(\text{Gal}(F))$ 。

对于右式, 由于

$$\begin{aligned} \varphi \in G &\implies (\varphi: K \rightarrow K \text{ 为同构映射}) \text{ 且 } (\forall x \in K \quad ((\forall \psi \in G, \psi(x) = x) \implies \varphi(x) = x)) \\ &\iff (\varphi: K \rightarrow K \text{ 为同构映射}) \text{ 且 } (\forall x \in \text{Inv}(G), \varphi(x) = x) \\ &\iff \varphi \in \text{Gal}(\text{Inv}(G)) \end{aligned}$$

那么  $G \subset \text{Gal}(\text{Inv}(G))$ 。

## 引理 1.1.10

对于域扩张  $K/k$  的 Galois 对应  $\text{Gal}: \mathcal{F} \rightarrow \mathcal{G}$  与  $\text{Inv}: \mathcal{G} \rightarrow \mathcal{F}$ , 成立

$$\text{Gal} \circ \text{Inv} \circ \text{Gal} = \text{Gal}, \quad \text{Inv} \circ \text{Gal} \circ \text{Inv} = \text{Inv}$$



**证明** 对于左式, 任取  $F \in \mathcal{F}$ , 则  $\text{Gal}(F) \in \mathcal{G}$ 。一方面, 由引理 1.1.9,  $\text{Gal}(F) \subset \text{Gal}(\text{Inv}(\text{Gal}(F)))$ , 即  $\text{Gal}(F) \subset (\text{Gal} \circ \text{Inv} \circ \text{Gal})(F)$ 。另一方面, 由引理 1.1.9,  $F \subset \text{Inv}(\text{Gal}(F))$ 。又由引理 1.1.8,  $\text{Gal}F \supset \text{Gal}(\text{Inv}(\text{Gal}(F)))$ , 即  $\text{Gal}F \supset (\text{Gal} \circ \text{Inv} \circ \text{Gal})(F)$ 。综合两方面,  $\text{Gal}F = (\text{Gal} \circ \text{Inv} \circ \text{Gal})(F)$ 。由  $F$  的任意性,  $\text{Gal} \circ \text{Inv} \circ \text{Gal} = \text{Gal}$ 。

对于右式, 任取  $G \in \mathcal{G}$ , 则  $\text{Inv}(G) \in \mathcal{F}$ 。一方面, 由引理 1.1.9,  $\text{Inv}(G) \subset \text{Inv}(\text{Gal}(\text{Inv}(G)))$ , 即  $\text{Inv}(G) \subset (\text{Inv} \circ \text{Gal} \circ \text{Inv})(G)$ 。另一方面, 由引理 1.1.9,  $G \subset \text{Gal}(\text{Inv}(F))$ 。又由引理 1.1.8,  $\text{Inv}G \supset \text{Inv}(\text{Gal}(\text{Inv}(F)))$ , 即  $\text{Inv}(G) \supset (\text{Inv} \circ \text{Gal} \circ \text{Inv})(G)$ 。综合两方面,  $\text{Inv}(G) = (\text{Inv} \circ \text{Gal} \circ \text{Inv})(G)$ 。由  $G$  的任意性,  $\text{Inv} \circ \text{Gal} \circ \text{Inv} = \text{Inv}$ 。

## 1.2 Artin 引理

## 引理 1.2.1 (Artin 引理)

对于域  $K$ , 如果  $G < \text{Aut}(K)$  且  $|G| < \infty$ , 那么

$$[K : \text{Inv}(G)] \leq |G|$$



**证明** 设  $|G| = n$ , 若要证明  $[K : \text{Inv}(G)] \leq n$ , 只需证明  $K$  中任意  $n+1$  个元素  $u_1, \dots, u_{n+1}$  必然  $\text{Inv}(G)$ -线性相关。记  $G = \{\varphi_1, \dots, \varphi_n\}$ , 其中  $\varphi_1 = \mathbb{1}_K$ 。考虑  $K$  上的齐次线性方程

$$\begin{pmatrix} \varphi_1(u_1) & \cdots & \varphi_1(u_{n+1}) \\ \vdots & \ddots & \vdots \\ \varphi_n(u_1) & \cdots & \varphi_n(u_{n+1}) \end{pmatrix} \begin{pmatrix} x_1 \\ \vdots \\ x_{n+1} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

由齐次线性方程解的判定, 该齐次线性方程存在非零解, 取其中非零分量数最少的非零解为  $(a_1, \dots, a_{n+1})$ 。必要时调换诸  $u_k$  与  $x_k$  的下标, 使得  $a_1 \neq 0$ ; 进而, 不妨  $a_1 = 1$ 。

断言: 诸  $a_k \in \text{Inv}(G)$ 。从而由线性方程的第一行

$$a_1 u_1 + \cdots a_{n+1} u_{n+1} = 0$$

可知  $u_1, \dots, u_{n+1}$  为  $\text{Inv}(G)$ -线性相关的。

如果此断言不成立, 不妨  $a_2 \notin \text{Inv}(G)$ , 则存在  $\varphi_t \in G$ , 使得成立  $\varphi_t(a_2) \neq a_2$ 。将  $\varphi_t$  作用于线性方程, 可得

$$\begin{pmatrix} (\varphi_t \circ \varphi_1)(u_1) & \cdots & (\varphi_t \circ \varphi_1)(u_{n+1}) \\ \vdots & \ddots & \vdots \\ (\varphi_t \circ \varphi_n)(u_1) & \cdots & (\varphi_t \circ \varphi_n)(u_{n+1}) \end{pmatrix} \begin{pmatrix} \varphi_t(x_1) \\ \vdots \\ \varphi_t(x_{n+1}) \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

由于  $G$  为群且诸  $\varphi_k: K \rightarrow K$  为同构映射, 因此  $\varphi_t \circ \varphi_1, \dots, \varphi_t \circ \varphi_n$  为  $\varphi_1, \dots, \varphi_n$  的置换, 从而  $(\varphi_t(a_1) = 1, \varphi_t(a_2), \dots, \varphi_t(a_{n+1}))$  亦为齐次线性方程的解。而  $(1, \dots, a_{n+1})$  为齐次线性方程的解, 因此

$$(0, a_2 - \varphi_t(a_2), \dots, a_{n+1} - \varphi_t(a_{n+1}))$$

亦为齐次线性方程的解。由  $\varphi_t(a_2) \neq a_2$ , 此为非零解, 且其非零分量数比  $(1, \dots, a_{n+1})$  的非零分量数要少, 这与  $(1, \dots, a_{n+1})$  的取法矛盾!

## 1.3 Dedekind 无关性引理

### 定义 1.3.1 ( $K$ -线性特征标)

对于群  $G$  与域  $K$ , 称群同态映射  $\chi: G \rightarrow K^\times$  为  $G$  的  $K$ -线性特征标。

### 引理 1.3.2 (Dedekind 无关性引理)

如果  $\chi_1, \dots, \chi_n$  为群  $G$  的互异  $K$ -线性特征标, 那么  $\chi_1, \dots, \chi_n$  在域  $K$  上线性无关; 换言之, 若存在  $c_1, \dots, c_n \in K$ , 使得成立  $\sum_{i=1}^n c_i \chi_i = 0$ , 那么  $c_1 = \dots = c_n = 0$ 。

证明

### 命题 1.3.3

如果  $K/k$  为有限扩张, 那么  $|\text{Gal}(K/k)| \leq [K:k]$ 。

证明

## 1.4 有限 Galois 扩张

### 定义 1.4.1 (Galois 扩张)

称域扩张  $K/k$  为 Galois 扩张, 如果  $K/k$  为可分且正规的域扩张。

### 定理 1.4.2 (有限 Galois 扩张)

如下命题等价。

1.  $K/k$  为有限、可分、正规的域扩张。
2. 存在  $k$  上的可分多项式  $f(x)$ , 使得  $K$  为  $f(x)$  在  $k$  上的分裂域。
3.  $K/k$  为有限扩张, 且  $|\text{Gal}(K/k)| = [K:k]$ 。
4.  $\text{Gal}(K/k)$  为有限群, 且  $\text{Inv}_K(\text{Gal}(K/k)) = k$ 。

## 第二章 Galois 理论基本定理

### 定义 2.0.1 (共轭子群)

称群  $G$  的子群  $H$  与  $H'$  互为共轭子群, 如果存在  $g \in G$ , 使得成立  $H' = gHg^{-1}$ 。

### 定义 2.0.2 (共轭中间域)

称域扩张  $K/k$  的中间域  $F$  与  $F'$  互为共轭中间域, 如果存在  $\varphi \in \text{Gal}(K/k)$ , 使得成立  $F' = \varphi(F)$ 。

### 定理 2.0.3 (Galois 理论基本定理)

如果域扩张  $K/k$  为有限 Galois 扩张, 那么成立如下命题。

1. Galois 对应  $\text{Gal}: \mathcal{F} \rightarrow \mathcal{G}$  与  $\text{Inv}: \mathcal{G} \rightarrow \mathcal{F}$  为互逆且反序的映射, 换言之——

$$\text{Inv} \circ \text{Gal} = \mathbb{1}_{\mathcal{F}}, \quad \text{Gal} \circ \text{Inv} = \mathbb{1}_{\mathcal{G}}$$

2.  $\text{Gal}(K/k)$  的子群  $G$  与  $G'$  互为共轭子群  $\iff K/k$  的中间域  $\text{Inv}_K(G)$  与  $\text{Inv}_K(G')$  互为共轭中间域
3.  $K/k$  的中间域  $F$  与  $F'$  互为共轭中间域  $\iff \text{Gal}(K/k)$  的子群  $\text{Gal}(K/F)$  与  $\text{Gal}(K/F')$  互为共轭子群
4.  $\text{Gal}(K/k)$  的子群  $G$  为正规子群  $\iff \text{Inv}_K(G)/k$  为正规扩张, 此时  $\text{Gal}(\text{Inv}_K(G)/k) \cong \text{Gal}(K/k)/G$
5. 对于域扩张  $K/k$  的中间域  $F$ ,  $K/F$  为正规扩张  $\iff \text{Gal}(K/F)$  为  $\text{Gal}(K/k)$  的正规子群。



## 附录 A 群论

## 附录 B 环论

## 附录 C 域论

### C.1 基本概念

#### 定义 C.1.1 (域)

称代数系统  $(F, +, \cdot)$  为域, 如果加法运算  $+: F \times F \rightarrow F$  和乘法运算  $\cdot: F \times F \rightarrow F$  成立如下命题。

1. 加法单位元:

$$\exists 0 \in F, \forall x \in F, \quad 0 + x = x + 0 = x$$

2. 乘法单位元:

$$\exists 1 \in F \setminus \{0\}, \forall x \in F, \quad 1x = x1 = x$$

3. 加法逆元:

$$\forall x \in F, \exists -x \in F, \quad x + (-x) = (-x) + x = 0$$

4. 乘法逆元:

$$\forall x \in F \setminus \{0\}, \exists x^{-1} \in F, \quad xx^{-1} = x^{-1}x = 1$$

5. 加法交换律:

$$\forall x, y \in F, \quad x + y = y + x$$

6. 乘法交换律:

$$\forall x, y \in F, \quad xy = yx$$

7. 加法结合律:

$$\forall x, y, z \in F, \quad (x + y) + z = x + (y + z)$$

8. 乘法结合律:

$$\forall x, y, z \in F, \quad (xy)z = x(yz)$$

9. 分配律:

$$\forall x, y, z \in F, \quad (x + y)z = xz + yz$$

$$\forall x, y, z \in F, \quad x(y + z) = xy + xz$$

#### 定义 C.1.2 (同态映射)

对于域  $F$  与  $K$ , 称映射  $\varphi: F \rightarrow K$  为同态映射, 如果对于任意  $x, y \in F$ , 成立

$$\varphi(x + y) = \varphi(x) + \varphi(y), \quad \varphi(xy) = \varphi(x)\varphi(y)$$