

If I feel unhappy, I do mathematics to become happy.

If I am happy, I do mathematics to keep happy.

— Pál. Turán, *The Work of Alfred Renyi*

1. 理解关于对称多项式的基本理论。
2. 理解多项式的导数与可分之间的关联, 理解判别式的含义。
3. 学习使用 Dedekind 定理 (不要求其证明) 计算 Galois 群:

定理 1 (Dedekind). $P(X)$ 为首一的、整系数 n 次不可约多项式, L 是 P 在 \mathbb{Q} 上的分裂域, 通过在 P 的根上的作用, 将 $\text{Gal}(L/\mathbb{Q})$ 视为 \mathfrak{S}_n 的子群。假设存在素数 p , 使得 $\bar{P}(X)$ 是可分的, 其中 \bar{P} 是 P 在 $\mathbb{F}_p[X]$ 中的像。

令 $\bar{P}(X) = \bar{P}_1(X) \cdots \bar{P}_l(X)$ 为 \bar{P} 在 $\mathbb{F}_p[X]$ 中的不可约分解, 其中, 对 $i = 1, \dots, l$, $\deg(\bar{P}_i) = n_i$ 。那么, 存在 (n_1, \dots, n_l) -型的 $\sigma \in \text{Gal}(L/\mathbb{Q}) < \mathfrak{S}_n$ (把 σ 写成两两不交的循环之积)。

例子. 计算多项式 $P(X) = X^4 + 4X^3 + 2X^2 + 3X - 5$ 在 \mathbb{Q} 上的分裂域 L 的 Galois 群 $\text{Gal}(L/\mathbb{Q})$ 。

在 \mathbb{F}_2 中考虑, 我们有 $\bar{P}(X) = X^4 + X + 1$ 。容易看出, \bar{P} 在 \mathbb{F}_2 和 \mathbb{F}_4 中没有根, 从而, \bar{P} 是不可约的。据此, $\text{Gal}(L/\mathbb{Q})$ 中有 4-循环。

在 \mathbb{F}_3 中考虑, 我们有 $\bar{P}(X) = X^4 + X^3 + 2X^2 + 1$ 。容易看出, \bar{P} 在 \mathbb{F}_3 恰有一个根 -1 。从而,

$$\bar{P}(X) = (X + 1)(X^3 - X + 1).$$

并且 $X^3 - X + 1$ 是不可约的。据此, $\text{Gal}(L/\mathbb{Q})$ 中有 3-循环。

以上表明 $|\text{Gal}(L/\mathbb{Q})| \geq 3 \times 4 = 12$, 所以, $\text{Gal}(L/\mathbb{Q})$ 为 \mathfrak{S}_4 或者 \mathfrak{A}_4 。

在 \mathbb{F}_5 中考虑, 我们有 $\bar{P}(X) = X^4 - X^3 + 2X^2 - 2X$, 从而,

$$\bar{P}(X) = X(X - 1)(X^2 + 2).$$

此时, $X^2 + 2$ 在 $\mathbb{F}_5[X]$ 上不可约。据此, $\text{Gal}(L/\mathbb{Q})$ 中有对换。从而, $\text{Gal}(L/\mathbb{Q}) \neq \mathfrak{A}_4$ 。

综上所述, $\text{Gal}(L/\mathbb{Q}) \cong \mathfrak{S}_4$ 。

练习. 令 K 为 $P(X) = X^4 + 2X^2 + X + 3$ 在 \mathbb{Q} 上的分裂域, 计算 $\text{Gal}(K/\mathbb{Q})$ 。进一步, 不用计算给出 $P(X) = X^4 + 2X^2 - 59X - 27$ 在 \mathbb{Q} 上的分裂域的 Galois 群。

引理 2. G 是 \mathfrak{S}_n 的子群, 考虑 \mathfrak{S}_n 在 $\{1, \dots, n\}$ 上的自然作用并假设 G 的作用是传递的。如果 G 包含一个对换和一个 $(n-1)$ -循环, 那么 $G = \mathfrak{S}_n$

证明: 不妨设 $\sigma = (2, 3, \dots, n) \in G$ 以及 $(a, b) \in G$ 。由于 G 的作用传递, 通过选取 $g \in G$ 使得 $g(a) = 1$, 则 $g(a, b)g^{-1} = (1, g(b))$ 。所以, 我们不妨设 $(1, b) \in G$ 。据此,

$$\sigma^k(1, b)\sigma^{-k} = (\sigma^k(1), \sigma^k(b)) = (1, \sigma^k(b)).$$

所以, $(1, 2), (1, 3), \dots, (1, n) \in G$, 从而 $G = \mathfrak{S}_n$ 。 □

例子. 令 K 为 $P(X) = X^6 + 22X^5 + 6X^4 + 12X^3 - 52X^2 - 14X - 30$ 在 \mathbb{Q} 上的分裂域, 计算 $\text{Gal}(K/\mathbb{Q})$ 。

通过 mod 2 以及 Eisenstein 判别法, P 不可约。这表明 $\text{Gal}(K/\mathbb{Q})$ 是 \mathfrak{S}_6 的一个传递的子群。

在 $\mathbb{F}_3[X]$ 中, $P(X) = X^6 + X^5 - X^2 + X = X(X^5 + X^4 - X + 1)$ 。然而, 在 $\mathbb{F}_3[X]$ 中 $X^5 + X^4 - X + 1$ 不可约 (利用 $X^2 + 1, X^2 \pm X - 1$ 是唯一的二次不可约多项式), 从而 $\text{Gal}(K/\mathbb{Q})$ 包含 5-循环。

在 $\mathbb{F}_5[X]$ 中,

$$P(X) = X^6 + 2X^5 + X^4 + 2X^3 - 2X^2 + X = X(X-1)(X+1)(X+2)(X^2+2).$$

在 $\mathbb{F}_5[X]$ 中 $X^2 + 2$ 不可约, 从而 $\text{Gal}(K/\mathbb{Q})$ 包含一个对换。

根据上述引理, $\text{Gal}(K/\mathbb{Q}) \simeq \mathfrak{S}_6$ 。

4. A 是交换环, $\mathfrak{Nil}(A) = \{a \in A \mid \text{存在 } n \geq 1, \text{使得 } x^n = 0\}$, $\text{Spec}(A)$ 是 A 的所有素理想的集合。证明, $\mathfrak{Nil}(A) = \bigcap_{\mathfrak{p} \in \text{Spec}(A)} \mathfrak{p}$ 。
 5. A 和 B 是交换环, $\varphi : A \rightarrow B$ 是环同态。证明, 如果 $\mathfrak{q} \subset B$ 是素理想, $\varphi^{-1}(\mathfrak{q}) \subset A$ 也是素理想。进一步利用 $\mathbb{Z} \rightarrow \mathbb{Q}$ 的自然映射说明极大理想的逆像未必是极大的。
 6. A 是交换环, $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ 是素理想, I 是理想。证明, 若 $I \subset \bigcup_{i=1}^n \mathfrak{p}_i$, 则存在 i_0 , 使得 $I \subset \mathfrak{p}_{i_0}$ 。
 7. A 是环, I 和 J 是理想并且 I 与 J 互素 (即 $I + J = A$)。证明, 对任意的 $n \geq 1$, I^n 与 J^n 互素。
 8. L/K 是代数扩张, $\alpha, \beta \in L$ 并且其在 K 上的极小多项式分别为 $P(X), Q(X) \in K[X]$ 。证明, 如果 $\deg(P)$ 与 $\deg(Q)$ 互素, 那么, α 在 $K(\beta)$ 上的极小多项式也是 $P(X)$ 。据此, 计算 $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})/\mathbb{Q}$ 的次数。
 9. p 是奇素数, 试计算 $\mathbb{Q}(\cos(\frac{2\pi}{p}))/\mathbb{Q}$ 的扩张次数。
 10. 证明, $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5})$ 。(提示: 先计算 $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$)
 11. 给定域扩张 $\mathbb{Q} \subset K \subset \mathbb{C}$, K/\mathbb{Q} 是 Galois 扩张。证明, K 在复共轭下不变。
 12. 给定 Galois 扩张 L/K , M 为其中间域, N 为 M 在 L 中的正规闭包¹证明,
- $$\text{Gal}(L/N) = \bigcap_{\sigma \in \text{Gal}(L/K)} \sigma \cdot \text{Gal}(L/M) \cdot \sigma^{-1}.$$
- 13. 给定 Galois 扩张 L/\mathbb{K} , M 为其中间域, H 为其在 Galois 对应下所对应的 $\text{Gal}(L/K)$ 的子群, 即 $M = L^H$ 。令 $N_{\text{Gal}(L/K)}(H)$ 为 H 在 $\text{Gal}(L/K)$ 中的正规化子, $M_0 = L^{N_{\text{Gal}(L/K)}(H)}$ 。证明, M/M_0 为 Galois 扩张。进一步证明, 若 $M' \subset M$ 为 M/K 的中间域并且 M'/M 为 Galois 扩张, 则 $M' \supset M_0$ 。
- 14. K 是域, $P \in K[X]$ 是 n 次可分多项式, L 为 P 在 K 上的分裂域。通过对 P 的根的作用, 我们将 $\text{Gal}(L/K)$ 视为 \mathfrak{S}_n 的子群。证明,
- $$\text{Gal}(L/K) \subset \mathfrak{A}_n \Leftrightarrow \text{Disc}(P) \in K^2,$$
- 其中, $\text{Disc}(P) := \prod_{i < j} (x_i - x_j)^2$, 其中, $\{x_i\}$ 为 P 在 \overline{K} 中的根。进一步证明, 若 K 是域并且其特征不是 3, $\deg(P) = 3$, 则
- $$\text{Gal}(L/K) = \begin{cases} \mathfrak{A}_3, & \text{如果 } \text{Disc}(P) \text{ 是 } K \text{ 中的完全平方;} \\ \mathfrak{S}_3, & \text{如果 } \text{Disc}(P) \text{ 不是 } K \text{ 中的完全平方.} \end{cases}$$
- 15. L/K 是有限 Galois 扩张并且 $\text{Gal}(L/K) \simeq \mathfrak{S}_n$, 其中, $n \geq 5$ 。任意给定 $x \in L$, $P(X) \in K[X]$ 为其极小多项式。证明, 如果 $\deg(P) > 2$, 那么 $\deg(P) \geq n$ 。如果 $n = 4$, 是否有反例?
- 16. K 是域, $P(X) \in K[X]$ 为可分的不可约多项式, L 为 P 在 K 上的分裂域, 假设 $\text{Gal}(L/K)$ 为交换群, $x \in L$ 为 P 的一个根。证明, $L = K(x)$ 。
- 17. p_1, p_2, \dots, p_d 是 d 个不同的素数, $L = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_d})$ 。证明, L/\mathbb{Q} 是 Galois 扩张并计算其 Galois 群。据此证明, $\sqrt{15} \notin \mathbb{Q}(\sqrt{10}, \sqrt{42})$ 。

¹这是 L 中包含 M 并且在 K 上正轨的最小子域, 它由 K 添加上 M 中元素的在 K 上的极小多项式的所有根生成。

1. 理解关于对称多项式的基本理论。

对于环 A 上的多项式环 $A[X_1, \dots, X_n]$,

可以考虑 S_n 在 $A[X_1, \dots, X_n]$ 上的作用

$$S_n \times A[X_1, \dots, X_n] \longrightarrow A[X_1, \dots, X_n]$$

$$(g, P) \longmapsto (g \cdot P)(X_1, \dots, X_n) = P(X_{g(1)}, \dots, X_{g(n)})$$

若 $g \cdot P = P$, 则 P 是 对称多项式

$A[X_1, \dots, X_n]^{S_n}$ 为 $A[X_1, \dots, X_n]$ 中全部 A -系数对称多项式.

子环

基本对称多项式

$$\left\{ \begin{array}{l} S_1 = \sum_i X_i \\ S_2 = \sum_{i < j} X_i X_j \\ \vdots \\ S_k = \sum_{i_1 < i_2 < \dots < i_k} X_{i_1} X_{i_2} \cdots X_{i_k} \\ \vdots \\ S_n = X_1 \cdots X_n \end{array} \right.$$

对于指标 $\mathbf{i} = (i_1, \dots, i_n)$, 考虑 $\text{Stab}(\mathbf{i})$

从而 $S_{\mathbf{i}} = \sum_{g \in S_n / \text{Stab}(\mathbf{i})} g \cdot (X^{i_1} X^{i_2} \cdots X^{i_n})$

注: 摸去 $\text{Stab}(\mathbf{i})$ 是因为要保证系数为 1.

命题

$$S_{\mathbf{i}} \in A[X_1, \dots, X_n]^{S_n}$$

命题

$$\forall P \in A[X_1, \dots, X_n] \quad \exists \text{有限个 } \mathbf{i}, \text{ 以及 } a_i \in A, \text{ s.t.}$$

$$P = \sum_{\text{有限}} a_i \cdot S_{\mathbf{i}}$$

3) 理

$$S_I \cdot S_J = S_{I+J} + \sum_{K < I+J} a_K S_K$$

定理

$$A[X_1, X_2, \dots, X_n]^{S_n} = A[\sigma_1, \dots, \sigma_n].$$

例子

$$K(X_1, \dots, X_n)^{S_n} = K(\sigma_1, \dots, \sigma_n)$$

例子

$$\Delta = \prod_{i < j} (X_i - X_j)$$

$$\text{那么有 } g \cdot \Delta = \varepsilon(g) \Delta \quad \varepsilon: S_n \rightarrow \{\pm 1\}$$

$$\Delta \in A[X_1, \dots, X_n]^{A_n}$$

$$disc = \Delta^2(b_1, \dots, b_n) = (-1)^{\frac{n(n-1)}{2}} Disc(P)$$

2. 理解多项式的导数与可分之间的关联，理解判别式的含义。

判别式的意义在于利用其来判断多项式是否有重根

判别式的意义在于利用它是否为零来断定 P 是否有重根。

注记 5.23 (判断多项式的可分性). 根据注记4.21, 多项式 P 可分等价于 $\text{Disc}(P) \neq 0$ 。另外, 由于 $\text{Disc}(P) := \text{Res}(P, P')$, 所以多项式 P 可分等价于 $(P, P') = 1$ 。

特别地, 若 $P \in K[X]$ 是不可约多项式, 则 P 可分等价于 $P' \neq 0$: 实际上, 若 P 可分, 则 $(P, P') = 1$, 这显然说明 $P' \neq 0$; 反之, $P' \neq 0$ 并且 $\deg(P') < \deg(P)$, 根据 P 不可约, 只能有 $(P, P') = 1$ 。

注记 5.24 (不可分的不可约多项式). 假设 $P \in K[X]$ 是不可约多项式, 记 $P(X) = a_n X^n + \dots + a_1 X + a_0$, 其中 $a_n \neq 0$ 。那么,

$$P'(X) = \sum_{k=1}^n k a_k X^{k-1} = n a_n X^{n-1} + \dots.$$

若 P 是不可分的, 则 $P' = 0$, 从而, $n \cdot a_n = 0$, 所以, 在 K 中 $n = 0$ 。这表明 $\text{Char}(K) = p$ 并且 $p \mid n$, 其中 p 是素数。

利用 $\text{Char}(K) = p$ 重新计算 $P'(X)$:

$$P'(X) = \sum_{p \nmid k} k a_k X^{k-1} = 0.$$

所以, 当 $p \nmid k$ 时, $a_k = 0$ 。这表明

$$P(X) = \sum_{p \mid k} a_k X^k = Q(X^p).$$

其中, $Q(X)$ 的定义如下:

$$Q(X) = \sum_{p \mid k} a_k X^{\frac{k}{p}}.$$

由于 P 不可约, 根据 $P(X) = Q(X^p)$, $Q(X)$ 也不可约。特别地, 如果 P 不可约并且不可分, 则 $\deg(P) \geq p$ 。

另外, 当 $\text{Char}(K) = p$ 时, 我们注意到形如 $Q(X^p)$ 的多项式的导数为 0。

注记 5.25. 在特征零情形下, 不可约多项式都是可分多项式。特别地, 如果 $\text{Char}(K) = 0$, 那么, 任意的代数扩张 L/K 均为可分扩张。

3. 讲义 P219

练习. 令 K 为 $P(X) = X^4 + 2X^2 + X + 3$ 在 \mathbb{Q} 上的分裂域, 计算 $\text{Gal}(K/\mathbb{Q})$ 。进一步, 不用计算给出 $P(X) = X^4 + 2X^2 - 59X - 27$ 在 \mathbb{Q} 上的分裂域的 Galois 群。

解: 在 \mathbb{F}_2 中, $\bar{P}(X) = X^4 + X + 1$ 不可约 有 4-循环

在 \mathbb{F}_3 中, $\bar{P}(X) = X^4 + 2X^2 + X = X \underbrace{(X^3 + 2X + 1)}_{\text{不可约}} \text{ 有 } 3\text{-循环}$

那么已知 $\text{Gal}(K/\mathbb{Q}) \cong S_4$

对于 $P(X) = X^4 + 2X^2 - 59X - 27$

有 \mathbb{F}_2 中 $\bar{P}(X) = X^4 + X + 1$

\mathbb{F}_3 中 $\bar{P}(X) = X^4 + 2X^2 + X$

与前一个多项式情况相同.

例子. 令 K 为 $P(X) = X^6 + 22X^5 + 6X^4 + 12X^3 - 52X^2 - 14X - 30$ 在 \mathbb{Q} 上的分裂域, 计算 $\text{Gal}(K/\mathbb{Q})$ 。

解: 通过 Eisenstein 判别法知 $P(X)$ 不可约 $\pmod{2}$ 从而 $\text{Gal}(K/\mathbb{Q})$ 作用传递

\mathbb{F}_3 中 $\bar{P}(X) = X^6 + X^5 + 2X^4 + X^3 - 2X^2 + X = X(X^5 + X^4 + 2X^3 - 2X^2 + X + 1)$ 5-循环

$$(X-a)(X-b) \\ X^2 - (a+b)X + ab$$

$$\begin{array}{c} X^2 - \cancel{X} \\ X^2 + X \cancel{X} \\ X^2 \cancel{X} \end{array} \quad \left| \begin{array}{l} X^2 + X + 1 \\ X^2 - X + 1 \\ X^2 - 1 \end{array} \right.$$

\mathbb{F}_3 中的二次不可约多项式

\mathbb{F}_5 中

$$\bar{P}(X) = X^6 + 2X^5 + X^4 + 2X^3 - 2X^2 + X$$

$$= X(X^5 + 2X^4 + X^3 + 2X^2 - 2X + 1)$$

$$= X(X-1)(X+1)(X^3 + 2X^2 + 2X - 1)$$

$$= X(X-1)(X+1)(X+2)(X^2 + 2)$$

2-循环

由引理, $\text{Gal}(K/\mathbb{Q}) \cong S_6$

4. A 是交换环, $\text{Nil}(A) = \{a \in A \mid \text{存在 } n \geq 1, \text{ 使得 } a^n = 0\}$, $\text{Spec}(A)$ 是 A 的所有素理想的集合。证明, $\text{Nil}(A) = \bigcap_{\mathfrak{p} \in \text{Spec}(A)} \mathfrak{p}$

证: 一方面

$$\forall a \in \text{Nil}(A) \quad a^n = 0$$

$$\text{由于 } 0 \in P, \forall P \in \text{Spec}(A) \Rightarrow a \in P \Rightarrow a \in \bigcap_{P \in \text{Spec}(A)} P$$

另一方面

$$\forall a \in \bigcap_{P \in \text{Spec}(A)} P.$$

考虑所有与 $S = \{a^n \mid n \geq 1\}$ 相交为空的理想集合

$$I = \{q \mid q \text{ 为理想且 } q \cap S = \emptyset\}$$

若 $a \notin \text{Nil}(A)$, I 非空, 因为 $0 \in I$,

对于 I 中任意的链 $\{q_i\}_{i \in I}$, 定义 $q = \bigcup_{i \in I} q_i$, 则 q 为理想且 $q \in I$

从而 I 中链都有上界, 根据 Zorn 引理, I 有极大元 $m \supseteq q$
根据定义是极大理想

而 极大理想都是素理想, 从而 m 也是素理想, 但 $a \notin m$.

与 $a \in \bigcap_{P \in \text{Spec}(A)} P$ 矛盾! 从而 $a \in \text{Nil}(A)$.

$$\text{综上, } \text{Nil}(A) = \bigcap_{P \in \text{Spec}(A)} P$$

5. A 和 B 是交换环, $\varphi: A \rightarrow B$ 是环同态。证明, 如果 $\mathfrak{q} \subset B$ 是素理想, $\varphi^{-1}(\mathfrak{q}) \subset A$ 也是素理想。进一步利用 $\mathbb{Z} \rightarrow \mathbb{Q}$ 的自然映射说明极大理想的逆像未必是极大的。

证: 假设 $\mathfrak{q} \subset B$ 是素理想

从而 $\varphi^{-1}(\mathfrak{q}) \subset A$ 也是理想 (理想的原像是理想)

$$\forall a, b \in \varphi^{-1}(\mathfrak{q}), \quad \varphi(ab) = \varphi(a)\varphi(b) \in \mathfrak{q}$$

那么 $\varphi(a) \in \mathfrak{q}$ 或 $\varphi(b) \in \mathfrak{q}$

从而 $a \in \varphi^{-1}(\mathfrak{q})$ 或 $b \in \varphi^{-1}(\mathfrak{q})$.

$\Rightarrow \varphi^{-1}(\mathfrak{q}) \subset A$ 也是素理想

下面利用 $\mathbb{Z} \rightarrow \mathbb{Q}$ 的自然映射说明极大理想的逆像未必极大。

零理想 $(0) \subset \mathbb{Q}$ 且 (0) 极大

$$\text{而 } \varphi^{-1}(0) = (0) \subset \mathbb{Z}$$

这不是 \mathbb{Z} 的极大理想。

注: 理想的像不一定是理想

但若环同态是满射, 则能保持理想。

6. A 是交换环, $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ 是素理想, I 是理想。证明, 若 $I \subset \bigcup_{i=1}^n \mathfrak{p}_i$, 则存在 i_0 , 使得 $I \subset \mathfrak{p}_{i_0}$ 。

证: 使用数学归纳法。

当 $n=1$ 时, 命题显然成立。

假设当于 n 时, 命题都成立, 证明 n 时命题也成立。

若 $\exists 1 \leq k \leq n$, s.t. $I \subset \bigcup_{i=1, i \neq k}^n \mathfrak{p}_i$, 则由归纳假设得证。

若 $\forall 1 \leq k \leq n$, $I \not\subset \bigcup_{i=1, i \neq k}^n \mathfrak{p}_i$, 那么 $\forall 1 \leq k \leq n$, $\exists a_k \in I$
但 $a_k \notin \bigcup_{i=1, i \neq k}^n \mathfrak{p}_i$ 从而 $a_k \in \mathfrak{p}_k$ 。

定义 $a = a_1 a_2 \cdots a_{n-1} + a_n$

那么 $a \in I$. 一方面 $\forall 1 \leq k \leq n-1$, $a_k \notin \mathfrak{p}_n$, 所以 $a_1 a_2 \cdots a_{n-1} \notin \mathfrak{p}_n$

结合 $a_n \in \mathfrak{p}_n$, 有 $a \notin \mathfrak{p}_n$

另一方面 $\forall 1 \leq k \leq n-1$, $a_k \in \mathfrak{p}_n$, 从而 $a_1 a_2 \cdots a_{n-1} \in \mathfrak{p}_n$

但 $a_n \notin \mathfrak{p}_n$, 有 $a \notin \mathfrak{p}_n$

$\Rightarrow a \notin \bigcup_{i=1}^n \mathfrak{p}_i$, 与 $a \in I$ 矛盾。

这种情况不成立。

综上, 由归纳假设知 $\exists 1 \leq i_0 \leq n$, s.t. $I \subset \mathfrak{p}_{i_0}$ 。

7. A 是环, I 和 J 是理想并且 I 与 J 互素 (即 $I + J = A$)。证明, 对任意的 $n \geq 1$, I^n 与 J^n 互素。

证: 因为 $I + J = A$, $\exists a \in I, b \in J$, s.t. $a + b = 1$.

$$\text{而 } (a+b)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} a^k b^{2n-k} = 1$$

因为 $\forall 0 \leq k \leq 2n$, $a^k b^{2n-k} \in I^n + J^n$ (对于 $0 \leq k \leq n$, $b^{2n-k} \in J^n$,
 $n < k \leq 2n$, $a^k \in I^n$)

从而 $1 \in I^n + J^n$. 即 I^n 与 J^n 互素。

8. L/K 是代数扩张, $\alpha, \beta \in L$ 并且其在 K 上的极小多项式分别为 $P(X), Q(X) \in K[X]$ 。证明, 如果 $\deg(P)$ 与 $\deg(Q)$ 互素, 那么, α 在 $K(\beta)$ 上的极小多项式也是 $P(X)$ 。据此, 计算 $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})/\mathbb{Q}$ 的次数。

证: 首先设 α 在 $K(\beta)$ 上的极小多项式为 $P'(X)$
那么 $P'(X) | P(X)$ 在 $K(\beta)$ 中, 因为 $P(X) \in K[X] \subset K(\beta)[X]$

$$\begin{array}{ccc} & K(\alpha, \beta) & \\ / & & \backslash \deg P' \\ K(\alpha) & & K(\beta) \\ \deg P \swarrow & K & \searrow \deg Q \end{array}$$

从而 $\deg P | [K(\alpha, \beta):K]$, $\deg Q | [K(\alpha, \beta):K]$

由 $\deg(P)$ 与 $\deg(Q)$ 互素, 知 $\deg(P) \cdot \deg(Q) | [K(\alpha, \beta):K]$
同时 $[K(\alpha, \beta):K] = \deg(P') \cdot \deg(Q) \leq \deg(P) \cdot \deg(Q)$

$\Rightarrow [K(\alpha, \beta):K] = \deg(P) \cdot \deg(Q)$. 上述不等式取到等号.

从而 $\deg P' = \deg P \Rightarrow P' = P$ #

具体地, $\sqrt{2}$ 的极小不等式为 $X^2 - 2$

$\sqrt[3]{2}$ 的极小不等式为 $X^3 - 2$ $(2, 3) = 1$

从而由以上推理知 $[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}): \mathbb{Q}] = 2 \times 3 = 6$

9. p 是奇素数, 试计算 $\mathbb{Q}(\cos(\frac{2\pi}{p}))/\mathbb{Q}$ 的扩张次数。

解: 考虑 $X^p - 1 = 0$ 的根 $\xi = e^{\frac{2\pi i}{p}}$ 那么 $\cos \frac{2\pi}{p} = \frac{1}{2}(\xi + \xi^{-1})$

$$\mathbb{Q}(\cos \frac{2\pi}{p}) \subset \mathbb{Q}(\xi)$$

记 $H = \text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q}(\cos \frac{2\pi}{p}))$ $G = \text{Gal}(\mathbb{Q}(\xi)/\mathbb{Q})$ 知 $= 2$.

$\mathbb{Q}(\xi)/\mathbb{Q}$ 是分圆扩张, 且 p 是质数, 从而 $G \cong C_{p-1}$

且有如下一一对应: $G \xrightarrow{\sim} C_{p-1} \cong (\mathbb{Z}/p\mathbb{Z})^\times$

$$g_k \mapsto \xi^k$$

$$\text{其中 } g(\xi) = \xi^k$$

其中仅有 $\underset{\substack{\parallel \\ 1}}{g_1}$ 与 g_{p-1} 保持 $\cos \frac{2\pi}{p}$ 不变, 从而 $H = \{1, g_{p-1}\}$

又 G 为交换群 $\Rightarrow H \trianglelefteq G \xrightarrow[\text{Galois}]{\text{Gal}(H)} \mathbb{Q}(\cos \frac{2\pi}{p})/\mathbb{Q}$ 是 Galois 扩张

$$\text{从而 } |\text{Gal}(\mathbb{Q}(\cos \frac{2\pi}{p})/\mathbb{Q})| = \frac{|G|}{|H|} = \frac{p-1}{2}$$

10. 证明, $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5})$ 。(提示: 先计算 $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$)

证: 考虑扩张列

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$$

类似 17 之证明可知 $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ $\sqrt{5} \notin \mathbb{Q}(\sqrt{2}, \sqrt{3})$

$$\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^3$$

具体构造为

$$\sigma_1 = \begin{cases} \sqrt{2} \mapsto -\sqrt{2}, \\ \sqrt{3} \mapsto \sqrt{3}, \\ \sqrt{5} \mapsto \sqrt{5} \end{cases}, \quad \sigma_2 = \begin{cases} \sqrt{2} \mapsto \sqrt{2}, \\ \sqrt{3} \mapsto -\sqrt{3}, \\ \sqrt{5} \mapsto \sqrt{5} \end{cases}, \quad \sigma_3 = \begin{cases} \sqrt{2} \mapsto \sqrt{2}, \\ \sqrt{3} \mapsto \sqrt{3}, \\ \sqrt{5} \mapsto -\sqrt{5} \end{cases}$$

$$\text{从而 } \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}) = \langle \sigma_1, \sigma_2, \sigma_3 \rangle$$

$$\exists \text{知 } \mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})$$

$$\text{考虑 } \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5})) \quad \forall \sigma \in \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$$

$$\sigma(\sqrt{2} + \sqrt{3} + \sqrt{5}) = -\sqrt{2} + \sqrt{3} + \sqrt{5} \neq$$

$$\sigma = \sigma_1^{i_1} \sigma_2^{i_2} \sigma_3^{i_3}, \quad i_k \in \{0, 1\}$$

$$\begin{aligned} \text{于是 } \sigma(\sqrt{2} + \sqrt{3} + \sqrt{5}) &= (\sigma_1^{i_1} \sigma_2^{i_2} \sigma_3^{i_3})(\sqrt{2} + \sqrt{3} + \sqrt{5}) \\ &= (-1)^{i_1} \sqrt{2} + (-1)^{i_2} \sqrt{3} + (-1)^{i_3} \sqrt{5} = \sqrt{2} + \sqrt{3} + \sqrt{5} \end{aligned}$$

$$\Rightarrow i_1 = i_2 = i_3 = 0 \Rightarrow \sigma = 1$$

$$\text{从而 } \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5})) = 1$$

$$\Rightarrow \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{2} + \sqrt{3} + \sqrt{5})$$

11. 给定域扩张 $\mathbb{Q} \subset K \subset \mathbb{C}$, K/\mathbb{Q} 是 Galois 扩张。证明, K 在复共轭下不变。

证:

$$\overline{\mathbb{Q}} = \{x \in \mathbb{C} \mid x \text{ 在 } \mathbb{Q} \text{ 上是代数的}\}$$

$$\Rightarrow K \subset \overline{\mathbb{Q}}$$

$\forall x \in K$, K/\mathbb{Q} 是 Galois 扩张, 从而 x 是代数的

$\Rightarrow \exists$ 不可约多项式 $P(x) \in \mathbb{Q}[x]$ s.t. $P(x) = 0$

可知 $P(x) \in \mathbb{R}[x] \Rightarrow P(\bar{x}) = \overline{P(x)} = 0$
 $\bar{P} = P$

K/\mathbb{Q} Gal 从而正规 $\Rightarrow \bar{x} \in K$

从而 K 在复共轭 $\sigma: y \mapsto \bar{y}$ 下不变. # 这于依赖 \mathbb{R} 的性质

注意到 \mathbb{C} 是代数封闭域

K/\mathbb{Q} 是 Galois 扩张, 从而正规,

由正规扩张的性质, 因为 复共轭 $\sigma \in \text{Hom}_k(K, \mathbb{C})$

从而 $\sigma(K) \subset K$

而 $\sigma^2(x) = x$, $\forall x \in \mathbb{C}$, 从而 $K \subset \sigma(\sigma(K)) \subset \sigma(K)$

$\Rightarrow K = \sigma(K)$, $\Rightarrow K$ 在 σ 下不变.

12. 给定 Galois 扩张 L/K , M 为其中间域, N 为 M 在 L 中的正规闭包¹证明,

$$\text{Gal}(L/N) = \bigcap_{\sigma \in \text{Gal}(L/K)} \sigma \cdot \text{Gal}(L/M) \cdot \sigma^{-1}.$$

证:

$$\begin{array}{c} L \dashv \vdash 1 \\ | \quad | \\ N \dashv \vdash H_1 \\ | \quad | \\ M \dashv \vdash H_2 \\ | \quad | \\ K \dashv \vdash G \end{array}$$

$$H_1 \triangleleft H_2 \quad \text{且 } H_1 \triangleleft G$$

$$\begin{array}{c} N \\ | \quad | \\ K \end{array} \text{ 正规. } \Rightarrow H_1 \triangleleft G$$

$$\Rightarrow N-M \text{ 正规} \Rightarrow H_1 \triangleleft H_2$$

$$\text{即证: } H_1 = \bigcap_{\sigma \in G} \sigma \cdot H_2 \cdot \sigma^{-1} := H$$

$$\sigma^{-1} H_1 \sigma = H_1 \subset H_2$$

$$\Rightarrow H_1 \subset \sigma H_2 \sigma^{-1}$$

$$\text{从而 } H_1 \subset \bigcap_{\sigma \in G} \sigma \cdot H_2 \cdot \sigma^{-1} = H$$

$$\text{另一方面. } H \subset \sigma H_2 \sigma^{-1}, \forall \sigma \in G$$

$$\sigma^{-1} H \sigma \subset H_2, \forall \sigma \in G$$

$$\sigma_1^{-1} H \sigma_1 \subset \sigma_2 H_2 \sigma_2^{-1}, \forall \sigma_1, \sigma_2 \in G$$

$$\Rightarrow \sigma_1^{-1} H \sigma_1 \subset \bigcap_{\sigma_2 \in \text{Gal}(L/K)} \sigma_2 H_2 \sigma_2^{-1} = H, \forall \sigma_1 \in G$$

$$\Rightarrow H \triangleleft H_2 \quad H \triangleleft N', \text{ 有}$$

$$\Rightarrow N'/M \text{ 正规} \xrightarrow{\text{正规闭包}} NCN'$$

$$\begin{array}{c} L \dashv \vdash 1 \\ | \quad | \\ N' \dashv \vdash H \\ | \quad | \\ N \dashv \vdash H_1 \\ | \quad | \\ M \dashv \vdash H_2 \end{array}$$

$$\text{从而 } H \subset H_1$$

$$\Rightarrow H = H \neq \emptyset.$$

一方面, 由于 N/K 正规, $\Rightarrow \text{Gal}(L/N) \subset \text{Gal}(L/K)$
 $\forall \sigma \in \text{Gal}(L/K), \sigma \cdot \text{Gal}(L/N) \cdot \sigma^{-1} = \text{Gal}(L/N)$
 $\text{由于 } \text{Gal}(L/M) \supset \text{Gal}(L/N)$
 $\Rightarrow \sigma \cdot \text{Gal}(L/M) \cdot \sigma^{-1} \supset \sigma \cdot \text{Gal}(L/N) \cdot \sigma^{-1} = \text{Gal}(L/N)$
 $\text{从而 } \text{Gal}(L/N) \subset \bigcap_{\sigma \in \text{Gal}(L/K)} \sigma \cdot \text{Gal}(L/N) \cdot \sigma^{-1}$

另一方面,

13. 给定 Galois 扩张 L/\mathbb{K} , M 为其中间域, H 为其在 Galois 对应下所对应的 $\text{Gal}(L/\mathbb{K})$ 的子群, 即 $M = L^H$ 。令 $N_{\text{Gal}(L/\mathbb{K})}(H)$ 为 H 在 $\text{Gal}(L/\mathbb{K})$ 中的正规化子, $M_0 = L^{N_{\text{Gal}(L/\mathbb{K})}(H)}$ 。证明, M/M_0 为 Galois 扩张。进一步证明, 若 $M' \subset M$ 为 M/\mathbb{K} 的中间域并且 M'/M' 为 Galois 扩张, 则 $M' \supset M_0$ 。

证:

$$\begin{array}{ccc} L & \xrightarrow{\quad} & 1 \\ | & & | \\ M & \xrightarrow{\quad} & H \\ | & & | \\ M_0 & \xrightarrow{\quad} & N_{\text{Gal}(\mathbb{K})}(H) \\ | & & | \\ K & \xrightarrow{\quad} & \text{Gal}(\mathbb{K}) \end{array}$$

有 $H \triangleleft N_{\text{Gal}(\mathbb{K})}(H)$, 并且 M_0 也是 Galois 扩张,
从而 M_0 是 Galois 扩张

$$\begin{array}{ccc} L & \xrightarrow{\quad} & 1 \\ | & & | \\ M & \xrightarrow{\quad} & H \\ | & & | \\ M' & \xrightarrow{\quad} & H' \\ | & & | \\ M_0 & \xrightarrow{\quad} & N_{\text{Gal}(\mathbb{K})}(H) \\ | & & | \\ K & \xrightarrow{\quad} & \text{Gal}(\mathbb{K}) \end{array}$$

M/M' Galois 从而 $H \triangleleft H'$
从而 $H' \triangleleft N_{\text{Gal}(\mathbb{K})}(H)$
从而 $M' \supset M_0$.

14. K 是域, $P \in K[X]$ 是 n 次可分多项式, L 为 P 在 K 上的分裂域。通过对 P 的根的作用, 我们将 $\text{Gal}(L/K)$ 视为 S_n 的子群。证明,

$$\text{Gal}(L/K) < A_n \Leftrightarrow \text{Disc}(P) \in K^2,$$

其中, $\text{Disc}(P) := \prod_{i < j} (x_i - x_j)^2$, 其中, $\{x_i\}$ 为 P 在 \bar{K} 中的根。进一步证明, 若 K 是域并且其特征不是 3, $\deg(P) = 3$, 则

$$\text{Gal}(L/K) = \begin{cases} A_3, & \text{如果 } \text{Disc}(P) \text{ 是 } K \text{ 中的完全平方;} \\ S_3, & \text{如果 } \text{Disc}(P) \text{ 不是 } K \text{ 中的完全平方.} \end{cases}$$

证:

启发:

$$\begin{array}{ccc} L & \dashrightarrow & 1 \\ | & & \Delta \\ K(\sqrt{\text{Disc}(P)}) & \dashrightarrow & A_n \\ | & & \Delta \\ K & \dashrightarrow & S_n \end{array}$$

若 $\text{Gal}(L/K) < A_n$, 那么 $\Delta = \sqrt{\text{Disc}(P)} = \prod_{i < j} (x_i - x_j)$
在 $\text{Gal}(L/K)$ 作用下不变。

$$\Rightarrow \Delta \in K, \text{ 从而 } \text{Disc}(P) = \Delta^2 \in K^2$$

若 $\text{Disc}(P) \in K^2$, 那么 $\Delta \in K \Rightarrow \Delta$ 在 $\text{Gal}(L/K)$ 作用下不变。
而 Δ 只在偶置换下不变, 从而 $\text{Gal}(L/K) < A_n$

进一步, 当 $\text{Char}(K) \neq 3$, $\deg(P) = 3$ 时. 此时 P 在 K 中可分,
从而 $\text{Disc}(P) \neq 0$
 $[L : K]$ 只可能为 3 或 6.

已知 $\text{Gal}(L/K) < S_3$, 而 S_3 的 3 阶子群只有 A_3

从而 由 $\text{Gal}(L/K) < A_3 \Leftrightarrow \text{Disc}(P) \in K^2$

$$\text{知 } \text{Gal}(L/K) = \begin{cases} A_3, & \text{Disc}(P) \in K^2 \\ S_3, & \text{Disc}(P) \notin K^2. \end{cases}$$

15. L/K 是有限 Galois 扩张并且 $\text{Gal}(L/K) \cong S_n$, 其中, $n \geq 5$ 。任意给定 $x \in L$, $P(X) \in K[X]$ 为其极小多项式。证明, 如果 $\deg(P) > 2$, 那么 $\deg(P) \geq n$ 。如果 $n = 4$, 是否有反例?

证: A_n 单群 $1 \triangleleft A_n \triangleleft S_n$
 $n \geq 5$

$$K(x) \cong \frac{K[x]}{(P(x))} \subset L$$

根据 Galois 对应.

$$\begin{array}{ccc} L & \xrightarrow{\quad} & 1 \\ \uparrow & & \downarrow \\ K(x) & \xrightarrow{\quad} & H \\ \uparrow & & \downarrow \\ K & \xrightarrow{\quad} & S_n \end{array}$$

且 $|H| = \frac{|S_n|}{[K(x):K]} = \frac{|S_n|}{\deg P}$

(注: 根据 Galois 对应定理的证明
 $|H| = [L:L^H] = \frac{[L:K]}{[L^H:K]} = \frac{|S_n|}{[K(x):K]}$)

$$\Rightarrow \deg P = \frac{|S_n|}{|H|} = [S_n : H]$$

回忆作业 2 B5). 由 $\deg P > 2$ 知 $H \neq A_n, S_n$
 从而 $\deg P \geq n$.

如果 $n=4$, S_4 有一个 8 阶子群

$$D_4 = \{1, (12)(34), (14)(23), (24), (13), (1234), (13)(24), (1432)\}$$

$\begin{matrix} \parallel & & \parallel \\ S & & Y \end{matrix}$

$$\begin{aligned} D_4 &= \{1, (1234), (13)(24), (1432), (24), (14)(23), (13), (14)(23)\} \\ &= \{1, r, r^2, r^3, s, sr, sr^2, sr^3\} \end{aligned}$$

$$\text{于是 } \exists M/K \text{ 的中间域 } M, [M:K] = \frac{|S_4|}{|D_4|} = 3$$

从而 M 中元素 x 的极小多项式 $P(x)$ 满足 $\deg P = 3$.

16. K 是域, $P(X) \in K[X]$ 为可分的不可约多项式, L 为 P 在 K 上的分裂域, 假设 $\text{Gal}(L/K)$ 为交换群, $x \in L$ 为 P 的一个根。证明, $L = K(x)$ 。

证: 由于 P 不可约, $\text{Gal}(L/K)$ 在其根上的作用是传递的。

现证明 $\text{Gal}(L_{K(x)}) = 1$

而对于 $g \in \text{Gal}(L_{K(x)})$, $g(x) = x$

$\forall y \in L$ 为 P 的根 $\exists h \in \text{Gal}(L/K)$ s.t. $h(y) = x$

那么 $g(x) = g(h(y)) = h(g(y)) = h(y) = x$

$$\Rightarrow g = 1, \Rightarrow \text{Gal}(L_{K(x)}) = 1$$

那么 $L = K(x)$,

17. p_1, p_2, \dots, p_d 是 d 个不同的素数, $L = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_d})$ 。证明, L/\mathbb{Q} 是 Galois 扩张并计算其 Galois 群。据此证明, $\sqrt{15} \notin \mathbb{Q}(\sqrt{10}, \sqrt{42})$ 。

证明: L/\mathbb{Q} 可分由 $\text{Char}(\mathbb{Q})=0$ 得到

而 $\pm\sqrt{p_i}$ 都在 L 中, 故 L 是多项式族 $(X^2 - p_i)_{i=1}^d$ 在 \mathbb{Q} 上的分裂域
从而 L/\mathbb{Q} 正规

于是 L/\mathbb{Q} 是 Galois 扩张。

$$\text{首先 } [L:\mathbb{Q}] = 2^d$$

$$\text{因为 } L = L_d$$

$$L_d = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_{d-1}})$$

$$\begin{array}{c} | \\ L_1 = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}) \\ | \\ \vdots \\ L_2 = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}) \end{array}$$

$$L_1 = \mathbb{Q}(\sqrt{p_1})$$

$$\text{只需证明 } [L_{k+1}:L_k] = 2$$

归纳地证明, $k=0$ 时, $[L_1:\mathbb{Q}] = 2$
若小于 k 时, 结论都成立, 对于 k 时

反证: 若 $L_{k+1} = L_k$

$$\text{那么 } \sqrt{p_{k+1}} \in \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_k}) = L_k$$

由归纳假设知 L_k 的一组基为

$$\{1, \sqrt{p_1}, \dots, \sqrt{p_k}, \sqrt{p_1 p_2}, \dots, \sqrt{p_1 p_k}, \dots, \sqrt{p_1 \dots p_k}\}$$

$$\text{从而 } \sqrt{p_{k+1}} = a_1 + a_2 \sqrt{p_1} + \dots + a_{2^k} \sqrt{p_1 \dots p_k}, a_i \in \mathbb{Q}$$

$$\text{改写为 } \sqrt{p_{k+1}} = b_1 + b_2 \sqrt{p_k}, b_1, b_2 \in L_{k-1}$$

$$\text{两边平方得 } p_{k+1} = b_1^2 + b_2^2 p_k + 2b_1 b_2 \sqrt{p_k}, \text{ 可知 } 2b_1 b_2 = 0$$

$$\text{若 } b_1 = 0, \Rightarrow p_{k+1} = b_2^2 p_k, \text{ 如果 } b_2 \neq 0, \text{ 则 } b_2^2 \in \mathbb{Q} \Rightarrow p_k | p_{k+1}, \text{ 与 } p_k \text{ 为不同素数矛盾} \\ \Rightarrow b_2 = 0$$

$$\text{若 } b_2 = 0, \Rightarrow p_{k+1} = b_1^2 \in L_{k-1}, \text{ 于是由归纳假设, 可知矛盾}$$

(p_{k+1} 与 p_k 地位相同, 若 $[L_k:L_{k-1}] = 2^k$, 则 $[L_{k-1}(\sqrt{p_{k+1}}):L_{k-1}] = 2$ 也成立)

两种情况都导出 $p_{k+1} = 0$, 矛盾, 于是 $\sqrt{p_{k+1}} \notin L_k$. 那么 $[L_k(\sqrt{p_{k+1}}):L_k] = 2$.

再考虑自同构: $\sigma_i: \sqrt{p_i} \mapsto -\sqrt{p_i} \quad \sqrt{p_j} \mapsto \sqrt{p_j} \ (j \neq i)$

通过上述证明中 $\{1, \sqrt{p_1}, \dots, \sqrt{p_d}, \sqrt{p_1 p_2}, \dots, \sqrt{p_{d-1} p_1}, \dots, \sqrt{p_1 \dots p_d}\}$
是 L 的一组基, 可知 σ_i 良定义

$$\text{并且 } \forall i, j. \quad \sigma_i \sigma_j = \sigma_j \sigma_i$$

从而 $\forall \sigma = \sigma_1^{i_1} \sigma_2^{i_2} \cdots \sigma_d^{i_d} \quad i_k \in \{0, 1\}$ 都有 $\sigma \in \text{Gal}(L/\mathbb{Q})$
共有 2^d 个, 结合 $[L:\mathbb{Q}] = 2^d$, 知

$$\text{Gal}(L/\mathbb{Q}) = \{\sigma \mid \sigma = \sigma_1^{i_1} \sigma_2^{i_2} \cdots \sigma_d^{i_d}, i_k \in \{0, 1\}\}$$

$\mathbb{Q}(\sqrt{5})$ 和 $\mathbb{Q}(\sqrt{10}, \sqrt{42})$ 都是 $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7})$ 的中间域

考虑 σ :
 $\sqrt{2} \mapsto -\sqrt{2}$
 $\sqrt{3} \mapsto \sqrt{3}$
 $\sqrt{5} \mapsto -\sqrt{5}$
 $\sqrt{7} \mapsto -\sqrt{7}$

$\sigma \notin \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}) / \mathbb{Q}(\sqrt{5}))$ 但 $\sigma \in \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}) / \mathbb{Q}(\sqrt{10}, \sqrt{42}))$

那么 $\mathbb{Q}(\sqrt{5}) \not\subset \mathbb{Q}(\sqrt{10}, \sqrt{42})$

从而 $\sqrt{5} \notin \mathbb{Q}(\sqrt{10}, \sqrt{42})$