

关于分裂域的极小生成集和聚类塔群

SHUBHAM JAISWAL, P VANCHINATHAN

摘要. 聚类塔的概念由第二作者和 Krithika 在 [4] 中提出, 其中包含一个问题, 该问题由第一作者和 Bhagwat 在 [1] 中回答. 本文我们引入了分裂域的极小生成集概念, 并将其与聚类塔的概念联系起来. 我们证明存在无穷多个有理数上的不可约多项式, 其分裂域有两个极端极小生成集 (一个给定基数, 另一个最小基数), 并且对于这些多项式, 我们有两种极端的聚类塔 (一种给定长度, 另一种最短长度). 我们证明了与构造定理证明中所构建的极小生成集相关的聚类塔的一些有趣性质, 并且作为结果得到了即使在使用极小生成集时, 次数序列也取决于顺序的事实. 我们还建立了某个有理多项式族的极小极小生成集的一个等价条件, 并计算了总极小极小生成集的数量.

1. 介绍

假设不可约多项式 f 的次数为 n , 其伽罗瓦群是 $\mathfrak{S}_n$. 这意味着对其根的任何置换都会产生分裂域的一个自同构. 换句话说, 知道根子集上的一个自同构并不能完全决定该自同构. 在这种情况下, 我们可以粗略地说 f 的根之间没有相互关系. 当伽罗瓦群不是整个 $\mathfrak{S}_n$ 时, 这意味着根之间存在某种关系. 例如, 如果由 f 某个根子集生成的域包含其他一些根, 则显然伽罗瓦群是 $\mathfrak{S}_n$ 的真子群. 伽罗瓦的一个著名结果表明, 对于一个素数次多项式, 当伽罗瓦群可解时, 分裂域由两个根生成 (参考 §68 在 [2]). 在这篇论文中, 我们希望了解根的子集要多大或多小才能生成分裂域.

我们不感兴趣将分裂域 K_f 表示为某个原根 $\beta \in K_f$ 的 $K(\beta)$. 我们的兴趣是将其表示为 $K_f = K(\beta_1, \beta_2, \dots, \beta_m)$, 其中 $\{\beta_i\}_{i=1}^m$ 是 f 在 $\bar{K}$ 中的根的一个子集. 这样的子集称为多项式分裂域的生成集. 在此背景下, 研究属于由 f 的单一特定根生成的域中的 f 的子集是自然的. 受 Perlis 在 [6] 的工作启发, 第二作者和 Krithika 在其最近的 [4] 工作中将此类子集定义为根簇. 因此, 簇形成了 f 的根之间的明显等价关系中的等价类.

第二作者和 Krithika 还在 [4] 中引入了簇塔的概念. 在这项工作中, 他们提出了一个关于簇塔的度序列是否独立于根簇代表元素排序的问题. 这个问题由第一作者和 Bhagwat 在其最近关于根簇的工作 [1] 中通过构建反例来回答.

通过极小生成集, 我们意味着一个生成集, 其任何真子集都不是生成集. 在本文中, 我们证明了分裂域的极小生成集的一些基本性质. 然后我们继续建立定理 3.1, 该定理连接了极小生成集和簇塔的概念, 并有助于将关于极小生成集的结果重新表述为关于簇塔的结果.

一个警告: 在线性代数中, 我们有一个类似的极小生成集的概念. Steinitz 交换引理使我们能够得出所有这样的极小生成集具有相同的基数的结论, 因此我们有了向量空间维度的一个良好定义的概念. 本文的目标之一是证明以上述自然方式为分裂域定义的极小生成集不具备 Steinitz 交换性质. 相反, 我们将展示两个“基”, 其中一个的基数为 2, 另一个的基数为 $k > 2$.

Date: 2025 年 5 月 1 日.

2020 Mathematics Subject Classification. 11R32, 12F05, 12F10.

精确结果在定理 2.5 和定理 3.2 中确立，如下所示。

定理 1.1. 给定一个整数 $k > 2$ ，存在无限多个不可约多项式 f 在 $\mathbb{Q}$ 上，满足以下条件。

- (1) 分裂域 $\mathbb{Q}_f$ 有两个极小生成集：一个基数为 2，另一个基数为 k 。
- (2) 我们有两个极端的聚类塔楼：一个长度为 3，另一个长度为 $k + 1$ 。

定理 3.3 建立了与我们构造的基数 k 最小生成集相关的长度 $k + 1$ 聚类塔的一些有趣性质，该最小生成集是在证明定理 2.5 时构建的。由此我们可以得出，即使使用最小生成集，度数序列仍然依赖于集合中元素的顺序。

如下在定理 2.7 中建立。

定理 1.2. 令 $n > 2$ 为奇数。令 c 为一个正有理数，使得 $f = x^n - c$ 是在 $\mathbb{Q}$ 上的不可约多项式。固定 ζ 为 $\mathbb{Q}$ 中的一个本原 n 次单位根。令 $a = c^{1/n}$ 为正实根。那么我们有以下结论。

- (i) $B = \{a\zeta^k, a\zeta^l\} | 0 \leq k < l \leq n - 1$ 是 $\mathbb{Q}_f$ 的最小生成集当且仅当 $\gcd(l - k, n) = 1$ 。
- (ii) 存在 $n\phi(n)/2$ 个最小生成集 $\mathbb{Q}_f$ ，其中 ϕ 是欧拉函数。

定理 2.8 建立了数域上具有给定基数的最小生成集的无穷多项式的存在性。

2. 多项式的分裂域的极小生成集

令 K 是一个完美域。我们固定一个代数闭包 $\bar{K}$ ，并始终与 K 上的不可约多项式以及包含在 $\bar{K}$ 中的 K 的有限扩张一起工作。令 $f \in K[t]$ 是一个次数为 n 的不可约多项式。由于 K 是完美的，因此 f 在 $\bar{K}$ 中有 n 个不同的根。我们用 $R = \{\alpha_1, \alpha_2, \dots, \alpha_n\}$ 表示 f 的根的集合。令 K_f 为 f 在 K 上的分裂域，并设 $G := \text{Gal}(K_f/K)$ 。设 $H = \text{Gal}(K_f/K(\alpha))$ 。我们有关于 f 的根簇的以下概念（详情见 [4] 的第 1 和第 2 节以及 [1] 的第 2.1 节）： f 的簇定义为属于由 f 在 K 上生成的域中的 f 的根的子集。结果表明，所有 f 的簇具有相同的基数，该基数被定义为 f 在 K 上的簇大小，表示为 $r_K(f)$ 。 f 在 K 上的簇的数量表示为 $s_K(f)$ 。

对于集合 $B = \{\beta_1, \beta_2, \dots, \beta_m\} \subset \bar{K}$ ，令 $K(B)$ 表示域 $K(\beta_1, \beta_2, \dots, \beta_m)$ 。

定义 2.1. 考虑一个在 K 上的不可约多项式 f 。集合 $B \subset R$ 被称为多项式 f 的分裂域的极小生成集，如果满足以下条件。

- (1) $K(B) = K_f$
- (2) 对于任何集合 $A \subsetneq B$ ，我们有 $K(A) \neq K_f$ 。

命题 2.2. 令 $B \subset R$ 为多项式 f 的分裂域的极小生成集。那么我们有如下内容

- (1) B 的所有元素都位于 f 的不同根簇中。因此 $|B| \leq s_K(f)$ 。
- (2) $B \subset B'$ 其中 B' 是 f 的根簇的完整代表集。

证明。

- (1) 如果 B 的两个元素，比如 β_1 和 β_2 位于同一个根簇中。那么 $K(\beta_1) = K(\beta_2)$ 。令 $A = B \setminus \{\beta_1\}$ 。然后 $A \subsetneq B$ 和 $K(A) = K_f$ 是一个矛盾。由于 $s_K(f)$ 是 f 的不同簇的数量，我们有 $|B| \leq s_K(f)$ 。

(2) 从部分 (1) 可以看出, B 的元素是 $|B|$ 多个 f 簇的代表。我们可以选择剩余 $s_K(f) - |B|$ 多个簇的代表, 并将该集合称为 B_0 。然后 $B' = B \sqcup B_0$ 满足我们的目的。

□

命题 2.3. 考虑 $B = \{\beta_1, \beta_2, \dots, \beta_m\} \subset R$ 。 B 是多项式 f 的分裂域的极小生成集, 当且仅当

- (1) $K(B) = K_f$ 和
- (2) 对于每一个 $1 \leq i \leq m$, 我们有 $\beta_i \notin K(B \setminus \{\beta_i\})$ 。

证明. 假设 B 是一个极小生成集。假设对于某个 i , 我们有 $\beta_i \in K(B \setminus \{\beta_i\})$ 。那么对于 $A = B \setminus \{\beta_i\} \subsetneq B$, 我们有 $K(A) = K(B) = K_f$, 这是一个矛盾。

反之, 假设对于某个 $A \subsetneq B$, $K(A) = K_f$ 。由于 $A \subsetneq B$, 我们有对于某个 i 的 $A \subset B \setminus \{\beta_i\}$ 。由于 $K(A) = K_f$ 。因此 $K(B \setminus \{\beta_i\}) = K_f$ 。因此 $\beta_i \in K(B \setminus \{\beta_i\})$, 这是一矛盾。 □

命题 2.4. 令 $C \subset R$ 是多项式 f 的分裂域的生成集, 即 $K(C) = K_f$ 。那么存在 $B \subset C$, 使得 B 是 f 的分裂域的极小生成集。

证明. 如果 $C = \{\gamma_1, \gamma_2, \dots, \gamma_{m'}\}$ 本身是最小生成集, 则我们已经完成了。假设 C 不是最小生成集。那么根据命题 2.3, 对于某些 $1 \leq i \leq m', \gamma_i \in K(C \setminus \{\gamma_i\})$ 我们有结论。然后对于 $C' = C \setminus \{\gamma_i\}$, 我们有 $K(C') = K(C) = K_f$ 。现在如果 C' 是最小生成集, 那么我们就完成了。否则我们重复同样的过程直到得到一个子集 $B \subset C$, 它是最小的。 □

推论 2.4.1. 令 f 是定义在 K 上的不可约多项式。则存在一个生成集 B 为 K_f 的极小生成集。

证明. 设 $C = R$ 。因此 $K(C) = K_f$ 。现在由命题 2.4, 我们完成了证明。 □

备注 2.4.1. 对于多项式 f 的分裂域的最小生成集 B , $|B|$ 不必整除 f 的次数 n 。

考虑 $f = x^3 - 2$ 在 $\mathbb{Q}$ 上, 并令 ω 为原 3 次单位根。然后 $\{\sqrt[3]{2}, \sqrt[3]{2}\omega\}$ 是 f 的最小生成集, 但不是 $2 \nmid 3$ 。

备注 2.4.2. 假设 B_1 和 B_2 是多项式 f 的分裂域的两个不同的极小生成集。通过以下定理表明 B_1 和 B_2 的基数不一定相同。这也说明了线性代数中的施泰因茨交换引理对于极小生成集并不成立。

定理 2.5. 给定一个整数 $k > 2$, 存在无穷多个不可约多项式 f 在 $\mathbb{Q}$ 上, 其分裂域 $\mathbb{Q}_f$ 具有两个极小生成集: 其中一个的基数为 2, 另一个的基数为 k 。

证明. 令 $n = p_1 p_2 \cdots p_k$, 其中 p_i 的是不同的奇素数。固定 ζ 为 $\bar{\mathbb{Q}}$ 中的原 n 次单位根。令 c 是一个正有理数, 使得 $f = x^n - c$ 是在 $\mathbb{Q}$ 上的不可约多项式。令 $a = c^{1/n}$ 是其正实根。因此 $\mathbb{Q}_f = \mathbb{Q}(a, \zeta)$ 。显然 $B_1 = \{a, a\zeta\}$ 是 f 的最小生成集, 基数为 2。我们声称 $B_2 = \{a\zeta^{n/p_i}\}_{i=1}^k$ 是 f 的一个极小生成集, 其基数为 k 。

由于 n 是奇数, 根据 [3] 中的命题 1 和 [3] 中的定理 A, $\mathbb{Q}(a) \cap \mathbb{Q}(\zeta) = \mathbb{Q}$ 和 $\text{Gal}(\mathbb{Q}_f/\mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$ 。识别 $G = \text{Gal}(\mathbb{Q}_f/\mathbb{Q})$ 与 $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$ 我们有 $H = \text{Gal}(\mathbb{Q}_f/\mathbb{Q}(a)) = \{0\} \times (\mathbb{Z}/n\mathbb{Z})^\times \subseteq G$ 。现在 G 具有半直积群法则

$$(\alpha, u) \cdot (\beta, v) = (\alpha + u \cdot \beta, uv)$$

如在 [3] 中, $u \cdot \beta$ 是环 $\mathbb{Z}/n\mathbb{Z}$ 中的通常乘法 $u\beta$ 。 G 对 f 的根的作用由 $(\alpha, u) \cdot (a\zeta^j) = a\zeta^{(\alpha+uj)}$ 给出, 对于任意的 $1 \leq j \leq n$ 。因此我们观察到对于每个 j , $H_j = \{(j - vj, v) \mid v \in (\mathbb{Z}/n\mathbb{Z})^\times\}$ 是固定域 $\mathbb{Q}(a\zeta^j)$ 的 G 的子群。

考虑 $(\alpha, u) \in \cap_{i=1}^k H_{n/p_i}$ 。因此对于所有 $1 \leq i \leq k$, $\alpha = (1 - u)n/p_i$ 成立。所以对于每个 i , 有 $p_i \mid \alpha$ 。因此 $n \mid \alpha$, 这意味着 $\alpha = 0$ 。因此对于每个 i , $p_i \mid (1 - u)$ 。因此 $n \mid (1 - u)$, 这意味着 $u = 1$ 。因此我们已经证明了 $\cap_{i=1}^k H_{n/p_i} = 1$, 这意味着 $K(B_2) = \mathbb{Q}_f$ 。

现在对于任意的 $1 \leq l \leq k$, 考虑 $(\alpha, u) \in \cap_{i \neq l} H_{n/p_i}$ 。因此对于所有 $i \neq l$, 有 $\alpha = (1 - u)n/p_i$ 。从而对于每个 $1 \leq i \leq k$, 有 $p_i \mid \alpha$ 。因此 $\alpha = 0$ 。因此对于每个 $i \neq l$, $p_i \mid (1 - u)$ 。因此 $(n/p_l) \mid (1 - u)$ 。我们声称存在一个整数 $1 \leq z \leq (p_l - 1)$ 使得 $(n/p_l)z + 1 \in (\mathbb{Z}/n\mathbb{Z})^\times$ 。

只要证明存在一个 $1 \leq z \leq (p_l - 1)$ 使得 $p_l \nmid ((n/p_l)z + 1)$ 即可。假设相反, 对于所有 $1 \leq z \leq (p_l - 1)$ 都有 $p_l \mid ((n/p_l)z + 1)$ 。因此 p_l 整除 $\sum_{z=1}^{(p_l-1)} ((n/p_l)z + 1) = (n/p_l)(\sum_{z=1}^{(p_l-1)} z) + (p_l - 1) = (n/p_l)(p_l(p_l - 1)/2 + (p_l - 1))$ 这是一个矛盾。

因此我们得到了一个非平凡的元素 $(0, (n/p_l)z + 1) \in \cap_{i \neq l} H_{n/p_i}$ 对于那个选择的 z 。从而对于任意的 $1 \leq l \leq k$, 我们有 $K(B_2 \setminus \{a\zeta^{n/p_l}\}) \neq \mathbb{Q}_f$ 。因此根据命题 2.3, 我们就完成了证明。由于我们对 $n = p_1 p_2 \cdots p_k$ 和 c 有无限的选择, 所以我们得到了具有该性质的无穷多项式。 $\square$

定义 2.6. $B \subset R$ 被称为多项式 f 的分裂域的极小生成集, 如果 B 是具有最小可能基数的极小生成集。

定理 2.7. 令 $n > 2$ 为奇数。固定 ζ 为 $\bar{\mathbb{Q}}$ 中的原 n 次单位根。令 c 是一个正有理数, 使得 $f = x^n - c$ 是在 $\mathbb{Q}$ 上的不可约多项式。设 $a = c^{1/n}$ 是其正实根。那么我们有如下结论。

- (1) $B = \{a\zeta^k, a\zeta^l\}$ 对于 $0 \leq k < l \leq n - 1$ 是 $\mathbb{Q}_f$ 的最小生成集当且仅当 $\gcd(l - k, n) = 1$ 。
- (2) 有 $n\phi(n)/2$ 个最小生成集的 $\mathbb{Q}_f$ 。

证明.

- (1) 现在是 $\mathbb{Q}_f = \mathbb{Q}(a, \zeta)$ 。如同定理 2.5 的证明, 我们有 $\text{Gal}(\mathbb{Q}_f/\mathbb{Q}) \cong \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$ 。我们将 $G = \text{Gal}(\mathbb{Q}_f/\mathbb{Q})$ 与 $\mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times$ 等同。现在我们有半直积群法则在 G 上, G 对 f 的根的作用以及每个 $0 \leq j \leq n - 1$ 的子群 H_j , 如同定理 2.5 的证明中所述。

现在 $\zeta^{l-k} \in K(B)$ 。假设 $\gcd(l - k, n) = 1$ 。因此 $\zeta \in K(B)$ 。从而 $a \in K(B)$ 。从而 B 是一个极小生成集的最小值。反之, 假设 $\gcd(l - k, n) = d \neq 1$ 。我们将证明 $K(B) \neq \mathbb{Q}_f$ 即 $H_k \cap H_l \neq 1$ 。

现在考虑 $(\alpha, u) \in H_k \cap H_l$ 。因此 $\alpha = (1 - u)k = (1 - u)l$ 。由此可知 $n \mid (l - k)(1 - u)$ 。我们声称存在一个 $1 \leq z \leq d - 1$ 使得 $-(n/d)zk, (n/d)z + 1$ 是 $H_k \cap H_l$ 中的一个非平凡元素。显然对于任何 z 都有 $(n/d)zk = (n/d)zl$, 因为 $d \mid (l - k)$ 。因此只需证明存在一个 $1 \leq z \leq d - 1$ 使得 $\gcd((n/d)z + 1, n) = 1$ 。

如果素数 $p \mid n$ 但 $p \nmid d$, 那么显然对于任意 z 我们有 $p \nmid ((n/d)z + 1)$ 。考虑 $P = \prod_{p \mid d} p$ 。假设对于所有 $1 \leq z \leq d - 1$ 都有 $P \mid ((n/d)z + 1)$ 。因此, P 整除 $\sum_{z=1}^{(d-1)} ((n/d)z + 1) = (n/d)(\sum_{z=1}^{(d-1)} z) + (d - 1) = (n/d)(d(d - 1)/2 + (d - 1))$ 这是一个矛盾。

(注意这里我们使用了 n 是奇数, 因此 d 也是奇数)。因此存在一个 z 使得 $P \nmid ((n/d)z + 1)$ 。通过那个选择的 z 我们就完成了。

- (2) 我们将计算满足条件的对数 (k, l) , 使得 $0 \leq k < l \leq n - 1$ 和 $\gcd(l - k, n) = 1$ 。由于 $n > 2$, $\phi(n)$ 是偶数。令 $e = \phi(n)$, 并令 e 个元素在 $(\mathbb{Z}/n\mathbb{Z})^\times$ 中为

$x_1 = 1 < x_2 < \cdots < x_e = (n-1)$ 。现在对于给定的 k ，我们必须有 $l = k + x_i$ 对于某些 $1 \leq i \leq e$ 使得条件得到满足。

当 $k = 0$ ，则 l 有 e 个选择。考虑 $0 \leq y \leq (e-2)$ 。对于 $(n - x_{e-y}) \leq k \leq (n - 1 - x_{e-y-1})$ 我们有 $e - y - 1$ 个选择来决定 l 。因此，总对数为 $e + \sum_{y=0}^{e-2} (x_{e-y} - x_{e-y-1})(e - y - 1) = ne - \sum_{i=1}^e x_i$ 。观察到对于所有 $1 \leq i \leq e/2$ 都有 $x_{e-i+1} = n - x_i$ ，我们得到 $\sum_{i=1}^e x_i = ne/2$ ，从而完成证明。 $\square$

备注 2.7.1. 如果 n 是定理 2.7 中的一个奇素数 p ，则 $\mathbb{Q}_f$ 的 $p\phi(p)/2 = {}^pC_2$ 个最小生成集 $\{a\zeta^k, a\zeta^l\}$ 对于 $0 \leq k < l \leq p-1$ 而言是分裂域 $\mathbb{Q}_f$ 的所有可能的极小生成集。

定理 2.8. 令 K 是一个数域。给定一个整数 $k > 1$ ，存在无穷多个不可约多项式在 K 上，其分裂域具有最小基数为 k 的极小生成集。

证明. 根据 [7] 在希尔伯特域上的结果，我们有 $\mathfrak{S}_{k+1}$ 可以被实现为在 K 上的无穷多个成对线性不相交的伽罗瓦扩张的伽罗瓦群。因此，根据珀里斯的最终命题 [5]，存在无穷多个不可约多项式 f ，在域 K 上，次数为 $k+1$ 且伽罗瓦群为 $\mathfrak{S}_{k+1}$ 。设 f 的根集为 $R = \{\alpha_i\}_{i=1}^{k+1} \subset \bar{K}$ 。设 $B_i = R \setminus \{\alpha_i\}$ 对于 $1 \leq i \leq k+1$ 。那么每个 B_i 是最小生成集，其基数为 k 。 $\square$

备注 2.8.1. 在上述证明中， $k+1$ 个 B_i 都是分裂域 f 的所有可能的极小生成集。

3. 极小生成集与聚类塔楼

在 [4] 中，引入了簇塔的概念。参见 [1] 的第 5.2 节以获取群论表述。

多项式的聚类塔: 令 f 是 K 上的一个不可约多项式。考虑 f 在 $\bar{K}$ 中根的簇的一组完全代表元。令 $(\beta_1, \beta_2, \dots, \beta_s)$ 为该集合的一种排序，其中 $s = s_K(f)$ 。现在考虑以下终止于分裂域 K_f 的字段簇塔。

$$K \subseteq K(\beta_1) \subseteq K(\beta_1, \beta_2) \subseteq \cdots \subseteq K(\beta_1, \beta_2, \dots, \beta_s) = K_f.$$

塔的长度是塔中不同域的数量，这些不同域关于 K 的次数构成次数序列。显然塔的长度 $\leq s+1$ 。

示例 5.1.3 在 [1] 中表明，度序列和塔的长度都依赖于 β_i 的顺序。

以下结果将最小生成集和簇塔的概念联系起来。

定理 3.1. 考虑 $B = \{\beta_1, \beta_2, \dots, \beta_m\} \subset R$ 。

(1) B 是多项式 f 的分裂域的一个极小生成集，当且仅当对于任意排列 $(i_1, i_2, \dots, i_m)(1, 2, \dots, m)$ ，

$$K \subseteq K(\beta_{i_1}) \subseteq K(\beta_{i_1}, \beta_{i_2}) \subseteq \cdots \subseteq K(\beta_{i_1}, \beta_{i_2}, \dots, \beta_{i_m})$$

是 f 的长度为 $m+1$ 的簇塔。

(2) 在上述情况下，所有的 $m!$ 个聚类塔都是不同的。换句话说， B 与之关联的有 $m!$ 个聚类塔。

(3) B 是一个多项式 f 的分裂域的极小生成集, 当且仅当

$$K \subseteq K(\beta_1) \subseteq K(\beta_1, \beta_2) \subseteq \cdots \subseteq K(\beta_1, \beta_2, \dots, \beta_m)$$

是 f 的一个簇塔, 并且长度为 $m+1$, 这是任何 f 的塔可能的最小长度。

证明.

(1) 假设 B 是一个极小生成集。考虑任意排列 $(i_1, i_2, \dots, i_m)$ 为 $(1, 2, \dots, m)$ 的情况。显然, 以下是一个簇塔, 终止于分裂域

$$K \subseteq K(\beta_{i_1}) \subseteq K(\beta_{i_1}, \beta_{i_2}) \subseteq \cdots \subseteq K(\beta_{i_1}, \beta_{i_2}, \dots, \beta_{i_m}) = K_f$$

, 因为 $K(B) = K_f$ 。

如果聚类塔的长度为 $< m+1$, 则存在 $2 \leq j \leq m$ 使得 $\beta_{i_j} \in K(\beta_{i_1}, \beta_{i_2}, \dots, \beta_{i_{j-1}})$ 。令 $A = B \setminus \{\beta_{i_j}\}$ 。我们有 $A \subsetneq B$ 与 $K(A) = K_f$, 这与 B 是最小生成集相矛盾。因此, 簇塔的长度是 $m+1$ 。

相反, 假设 B 不是最小生成集。

情况 1: $K(B) \neq K_f$ 。那么对于任何排列, 这座塔都不是聚类塔, 因为它不会在分裂域处终止。

情况 2: $K(B) = K_f$ 且存在 $A \subsetneq B$ 使得 $K(A) = K_f$ 。考虑一个排列 $(i_1, i_2, \dots, i_m)$ 的 $(1, 2, \dots, m)$, 使得 $A = \{\beta_{i_1}, \beta_{i_2}, \dots, \beta_{i_l}\}$ 其中 $l < m$ 。则聚类塔

$$K \subseteq K(\beta_{i_1}) \subseteq K(\beta_{i_1}, \beta_{i_2}) \subseteq \cdots \subseteq K(\beta_{i_1}, \beta_{i_2}, \dots, \beta_{i_m}) = K_f$$

的长度是 $\leq l+1 < m+1$ 。

(2) 假设 $(i_1, i_2, \dots, i_m)$ 和 $(j_1, j_2, \dots, j_m)$ 是 $(1, 2, \dots, m)$ 的两个不同的排列。考虑最小的 $1 \leq l \leq m-1$, 使得 $i_l \neq j_l$ 成立。我们声称 $K(\beta_{i_1}, \beta_{i_2}, \dots, \beta_{i_l}) \neq K(\beta_{j_1}, \beta_{j_2}, \dots, \beta_{j_l})$ 。

假设相反, $K(\beta_{i_1}, \beta_{i_2}, \dots, \beta_{i_l}) = K(\beta_{j_1}, \beta_{j_2}, \dots, \beta_{j_l})$ 。由于对于所有 $1 \leq k \leq l-1$ 都有 $i_k = j_k$ 。因此对于任意的 $1 \leq k \leq l$ 都有 $j_l \neq i_k$ 。这暗示了 $\beta_{j_l} \in K(B \setminus \{\beta_{j_l}\})$, 根据命题 2.3, 这是与 B 作为一个极小生成集相矛盾的。因此, 对应于这两个置换的簇塔是不同的。

(3) 假设

$$K \subseteq K(\beta_1) \subseteq K(\beta_1, \beta_2) \subseteq \cdots \subseteq K(\beta_1, \beta_2, \dots, \beta_m)$$

是 f 的一个簇塔, 其长度为 $m+1$, 这是任何 f 塔的最小可能长度。因此对于每个排列 $(i_1, i_2, \dots, i_m)$ 的 $(1, 2, \dots, m)$,

$$K \subseteq K(\beta_{i_1}) \subseteq K(\beta_{i_1}, \beta_{i_2}) \subseteq \cdots \subseteq K(\beta_{i_1}, \beta_{i_2}, \dots, \beta_{i_m})$$

是长度为 $m+1$ 的 f 的簇塔。由第 (1) 部分, B 是一个极小生成集。如果 B' 是任何其他极小生成集。然后根据第 (1) 部分, 对应的簇塔的长度将是 $|B'| + 1$ 。由于 $|B| + 1$ 是任何簇塔可能的最小长度对于 f 。因此 $|B| \leq |B'|$ 。因此 B 是最小生成集。

反之, 假设 B 是最小的生成集。那么根据第 (1) 部分, 由于 B 是最小生成集,

$$K \subseteq K(\beta_1) \subseteq K(\beta_1, \beta_2) \subseteq \cdots \subseteq K(\beta_1, \beta_2, \dots, \beta_m)$$

是 f 的长度为 $m+1$ 的簇塔。假设 $m+1$ 不是簇塔对于 f 的可能的最短长度。因此存在一个集合 $C = \{\gamma_1, \gamma_2, \dots, \gamma_{m'}\} \subset R$, 其中包含 $m' < m$, 使得

$$K \subseteq K(\gamma_1) \subseteq K(\gamma_1, \gamma_2) \subseteq \cdots \subseteq K(\gamma_1, \gamma_2, \dots, \gamma_{m'})$$

是长度为 $m'+1 < m+1$ 的 f 的簇塔。因此 $K(C) = K_f$ 。因此, 根据命题 2.4, 存在 $B' \subset C$, 使得 B' 是 f 的分裂域的一个极小生成集。从而 $|B'| \leq |C| < m$ 。这与 B 是一个最小极小生成集相矛盾。

□

推论 3.1.1. 令 f 是在 K 上的不可约多项式, α 是 f 在 $\bar{K}$ 中的一个根。那么 f 恰有一个簇塔当且仅当 $K(\alpha)/K$ 是伽罗瓦的。

证明. 如果 $K(\alpha)/K$ 是伽罗瓦的, 那么 $K \subseteq K(\alpha) = K_f$ 是 f 的唯一簇塔。反之假设 $K(\alpha)/K$ 不是伽罗瓦的。那么 K_f 的任何最小生成集都具有基数 ≥ 2 。由定理 3.1(2), f 至少有 2 个不同的聚类塔。 □

备注 3.1.1. 在上述情况下, 塔的长度是 2, 度序列是 $(\deg(f))$, 且有 $\deg(f)$ 个单元素最小生成集, 因此也是最小的最小生成集。

鉴于定理 3.1(1), 我们将集群塔的定理 2.5 重新表述如下。

定理 3.2. 给定一个整数 $k > 2$, 存在无限多个不可约多项式 f 在 $\mathbb{Q}$ 上, 其中我们有两个极端的簇塔: 一个长度为 3, 另一个长度为 $k+1$ 。

定理 3.3. 考虑具有基数 k 的最小生成集 $B_2 = \{a\zeta^{n/p_i}\}_{i=1}^k$, 如定理 2.5 的证明中所述。考虑与之相关的长度为 $k+1$ 的聚类塔。

$$\mathbb{Q} \subseteq L_1 \subseteq L_2 \subseteq \cdots \subseteq L_k = \mathbb{Q}_f$$

其中 $L_i = \mathbb{Q}(a\zeta^{n/p_1}, a\zeta^{n/p_2}, \dots, a\zeta^{n/p_i})$ 对于 $1 \leq i \leq k$ 。然后我们有以下内容。

- (1) $L_i = \mathbb{Q}(a, \zeta^{n/(p_1 p_2 \cdots p_i)})$ 对所有 $i \geq 2$ 。
- (2) 聚类塔的度数序列是 $(n, n\phi(p_1 p_2), n\phi(p_1 p_2 p_3), \dots, n\phi(p_1 p_2 \cdots p_{k-1}), n\phi(n))$ 。
- (3) 关于 a 的 L_i 的根容量 (以 $\mathbb{Q}$ 为基域), 即: 对于 $i \geq 2$ 和 $\rho_{\mathbb{Q}}(L_1, a) = 1$ 的 $\rho_{\mathbb{Q}}(L_i, a) = p_1 p_2 \cdots p_i$ 。(参见 [1] 的第 6.2 节以获取根容量的定义)。

证明.

- (1) 我们有 $i \geq 2$ 。现在对于每个 $1 \leq j \leq i$, 我们有 $a\zeta^{n/p_j} = (a)(\zeta^{n/(p_1 p_2 \cdots p_i)})^{(p_1 p_2 \cdots p_i)/p_j}$ 。因此 $L_i \subset \mathbb{Q}(a, \zeta^{n/(p_1 p_2 \cdots p_i)})$ 。不失一般性地假设 p_1 是 $p_1, p_2, \dots, p_i$ 中最大的素数。现在我们观察到

$$\gcd(n, (n/p_2 - n/p_1), (n/p_3 - n/p_1), \dots, (n/p_i - n/p_1)) = n/(p_1 p_2 \cdots p_i).$$

因此我们有整数 $y, x_2, x_3, \dots, x_i$ 使得 $yn + \sum_{j=2}^i x_j(n/p_j - n/p_1) = n/(p_1 p_2 \cdots p_i)$ 。令 $x_1 = -\sum_{j=1}^i x_j$ 。因此 $\prod_{j=1}^i (a\zeta^{n/p_j})^{x_j} = \zeta^{n/(p_1 p_2 \cdots p_i)}$ 。从而 $\zeta^{n/(p_1 p_2 \cdots p_i)} \in L_i$ 。因此 $a \in L_i$ 。这样我们就完成了。

(2) 现在 $\mathbb{Q}(a) \cap \mathbb{Q}(\zeta) = \mathbb{Q}$ 。因此 $\mathbb{Q}(a) \cap \mathbb{Q}(\zeta^{n/(p_1 p_2 \cdots p_i)}) = \mathbb{Q}$ 。由此 $[\mathbb{Q}(a, \zeta^{n/(p_1 p_2 \cdots p_i)}) : \mathbb{Q}] = [\mathbb{Q}(a) : \mathbb{Q}][\mathbb{Q}(\zeta^{n/(p_1 p_2 \cdots p_i)}) : \mathbb{Q}]$ 。因此对于 $i \geq 2$, $[L_i : \mathbb{Q}] = n\phi(p_1 p_2 \cdots p_i)$ 。

(3) 由于域 $\mathbb{Q}(a)$ 包含 $f = x^n - c$ 的单根 a , 因为 n 是奇数。因此, 与 $\mathbb{Q}(a)$ 同构的域 $\mathbb{Q}(a\zeta^{n/p_1})$ 也包含 f 的单个根 $a\zeta^{n/p_1}$ 。从而 $\rho_{\mathbb{Q}}(L_1, a) = 1$ 。另外由于 $L_k = L_f$ 。因此 $\rho_{\mathbb{Q}}(L_k, a) = n = p_1 p_2 \cdots p_k$ 。

现在令 $2 \leq i \leq k-1$ 。显然, $p_1 p_2 \cdots p_i$ 个根 $\{a\zeta^{yn/(p_1 p_2 \cdots p_i)}\}_{y=0}^{(p_1 p_2 \cdots p_i)-1}$ 属于 f 位于 L_i 中。我们将证明这些是唯一位于 L_i 中的根。假设 f 的另一个根 $a\zeta^j$ 也位于 L_i 中。因此存在一个 $i+1 \leq l \leq k$, 使得 $p_l \nmid j$ 。

由于 $L_i = \mathbb{Q}(a\zeta^{n/p_1}, a\zeta^{n/p_2}, \dots, a\zeta^{n/p_i})$ 。因此固定 L_i 的 G 的子群是 $\cap_{w=1}^i H_{n/p_w}$ 。由于 $\mathbb{Q}(a\zeta^j) \subset L_i$ 。因此 $\cap_{w=1}^i H_{n/p_w} \subset H_j$ 。因此, $k-1$ 子群的交集是 $\cap_{w \neq l} H_{n/p_w} \subset H_j$ 。现在在定理 2.5 的证明的最后一段中, 我们得到了某个 $1 \leq z \leq p_l - 1$ 的非平凡元素 $(0, (n/p_l)z + 1) \in \cap_{w \neq l} H_{n/p_w}$ 。从而 $(0, (n/p_l)z + 1) \in H_j$ 。因此 $n \mid ((n/p_l)zj)$ 。但由于 $p_l \nmid ((n/p_l)zj)$, 我们得到了矛盾。

□

备注 3.3.1. 可以观察到, 定理 3.3 的第 (1) 和 (2) 部分的证明中的论点通过使用定理 3.1 (1), 给出了 B_2 是最小生成集的一个替代证明。

备注 3.3.2. 在定理 3.3 中, 如果我们考虑与排列 $(1, 3, 2, 4, \dots, k)$ 对应的簇塔 $(1, 2, 3, 4, \dots, k)$, 我们得到度数序列为

$(n, n\phi(p_1 p_3), n\phi(p_1 p_2 p_3), \dots, n\phi(p_1 p_2 \cdots p_{k-1}), n\phi(n))$ 。现在 $\phi(p_1 p_3) \neq \phi(p_1 p_2)$ 。因此这两个簇塔的度数序列是不同的。这表明即使使用最小生成集, 度数序列仍然取决于集合中元素的顺序。

示例 3.4. 考虑定理 2.7 中的情况。然后根据定理 3.1(3), 共有 n 多种不同的簇塔 f , 其长度是最小可能的长度。对于每个塔, 其长度是 3, 度数序列是 $(n, n\phi(n))$ 。如果 n 是一个奇素数 p , 那么总共有 p 个不同的聚类塔 f 。

示例 3.5. 考虑定理 2.8 的证明情况。通过类似于定理 3.1 (2) 中的论证, 我们可以证明总共有 $(k+1)!/2$ 个不同的簇塔 f 。

References

- [1] Chandrasheel Bhagwat and Shubham Jaiswal. Cluster Magnification, Root Capacity, Unique Chains, Base Change and Ascending Index. Accepted for publication in Proceedings Mathematical Sciences (2025). <https://arxiv.org/abs/2405.06825>, 2024.
- [2] Harold M Edwards. Galois theory, GTM 101. New York: Springer-Verlag, 1984.
- [3] Eliot T Jacobson and William Y Vélez. The Galois group of a radical extension of the rationals. Manuscripta Mathematica, 67:271–284, 1990.
- [4] M Krithika and P Vanchinathan. An elementary problem in Galois theory about the roots of irreducible polynomials. Proc. Indian Acad. Sci. (Math. Sci.) (2024) 134:28, 2024.

- [5] Alexander R Perlis. Roots appear in quanta: exercise solutions.
<https://www.math.lsu.edu/~aperlis/publications/rootsinquanta/>, 2003.
- [6] Alexander R Perlis. Roots appear in quanta. The American Mathematical Monthly, 111(1):61–63, 2004.
- [7] Helmut Völklein. Groups as Galois groups: an introduction. Number 53. Cambridge University Press, 1996.

Email address: `jaiswal.shubham@students.iiserpune.ac.in`, `vanchinathan@gmail.com`