RELATIVE PÓLYA GROUP AND PÓLYA DIHEDRAL EXTENSIONS OF $\mathbb{Q}$

ABBAS MAAREFPARVAR AND ALI RAJAEI*

Abstract. A number field with trivial Pólya group [3] is called a Pólya field. We define “relative Pólya group $Po(M/N)$” for $M/N$ a finite extension of number fields, generalizing the Pólya group. Using cohomological tools in [2], we compute some relative Pólya groups. As a consequence, we generalize Leriche’s results in [18] and prove the triviality of relative Pólya group for the Hilbert class field of $K$. Then we generalize our previous results [19] on Pólya $S_3$-extensions of $\mathbb{Q}$ to dihedral extensions of $\mathbb{Q}$ of order $2r$, for $r$ an odd prime. We also improve Leriche’s upper bound in [17] on the number of ramified primes in Pólya $D_r$-extensions of $\mathbb{Q}$ and prove that for a real (resp. imaginary) Pólya $D_r$-extension of $\mathbb{Q}$ at most 4 (resp. 2) primes ramify.

Keywords: integer valued polynomial, Bhargava factorial, Pólya field, Pólya group, relative Pólya group, dihedral extension.

Notations. Throughout this paper For a number field $M$, $I(M)$, $P(M)$, $Cl(M)$, $O_M$, $h(M)$, $U_M$, $w_M$, $H(M)$, $\Gamma(K)$ and $D_M$ denote the group of fractional ideals, group of principal fractional ideals, ideal class group, ring of integers, class number, group of units, Dirichlet rank of group of units, Hilbert class field, genus field and discriminant of $M$, respectively. For a finite extension $M/N$ of number fields, the maps $N_{M/N} : Cl(M) \rightarrow Cl(N)$ and $j_{M/N} : Cl(N) \rightarrow Cl(M)$ denote the ideal norm homomorphism and transfer of ideal classes, respectively. Also for a prime ideal $p$ of $N$ and a prime ideal $\mathfrak{p}$ of $M$ above $p$, denote the ramification index and residue class degree of $\mathfrak{p}$ over $p$ by $e(\mathfrak{p}/p)$ and $f(\mathfrak{p}/p)$, respectively. For a field $K$ and an irreducible polynomial $f(X) \in K[X]$ over $K$, denote the discriminant of $f(X)$ and the Galois group of the splitting field of $f(X)$ over $K$ by $\text{disc}(f(X))$ and $\text{Gal}(f/K)$, respectively. Also $r$ is an odd prime number, $C_r$ and $D_r$ denote the cyclic group of order $r$ and the dihedral group of order $2r$, respectively. $\zeta_n$ is a primitive $n$-th root of unity.

1. Introduction

Historically, the study of Pólya fields dates back to Pólya’s results on integer valued polynomials [24]. For a number field $K$, with ring of integers $O_K$, the ring of integer valued polynomials on $O_K$ is defined as follows:

$$\text{Int}(O_K) = \{ f \in K[x] \mid f(O_K) \subseteq O_K \}.$$  

For a nonnegative integer $n$, denote the subset of $K$ formed by 0 and the leading coefficients of integer valued polynomials of degree $n$ on $O_K$ by $\mathfrak{J}_n(K)$. This is a fractional ideal of $O_K$: $\mathfrak{J}_n(K) \subseteq (n!^{-1})O_K$, see [20] Section 2. One can show that

*Corresponding author.

2010 Mathematics Subject Classification. Primary 11R04, 11R29, 11R34, 11R37, 13F20.
\( \text{Int}(\mathcal{O}_K) \) is free as an \( \mathcal{O}_K \)-module and isomorphic to \( \bigoplus_{n=0}^{\infty} J_n(K) \), see [26, Section 2]. But an \( \mathcal{O}_K \)-basis for \( \text{Int}(\mathcal{O}_K) \) may be difficult to describe and Pólya [24] was interested in those fields \( K \) for which \( \text{Int}(\mathcal{O}_K) \) has an \( \mathcal{O}_K \) basis which exactly one member from each degree. Such basis, if it exists, is called a regular basis.

Pólya [24], proved that \( \text{Int}(\mathcal{O}_K) \) has a regular basis if and only if all the ideals \( J_n(K) \) are principal, see [24, Satz I]. Bhargava [1] generalized the factorial function to Dedekind domains and introduced the generalized factorial ideals. One can prove that \( n!_{\mathcal{O}_K} = J_n(K) - 1 \) in Bhargava’s notation, see [1, Theorem 12]. Hence \( \text{Int}(\mathcal{O}_K) \) has a regular basis if and only if all Bhargava factorial ideals \( n!_{\mathcal{O}_K} \) are principal.

Immediately after Pólya [24], Ostrowski [23] proved that \( \text{Int}(\mathcal{O}_K) \) has a regular basis if and only if all the ideals \( \Pi_q(K) := \prod_{\mathfrak{m} \in \text{Max}(\mathcal{O}_K)} \mathfrak{m}^{N_{K/\mathbb{Q}}(\mathfrak{m})=q} \) are principal. Hence for a Galois number field \( K \), existence of a regular basis for \( \text{Int}(\mathcal{O}_K) \) is equivalent to principality of \( \prod_{i=1}^{g} \mathfrak{P}_i \), where \( \mathfrak{P}_1, \mathfrak{P}_2, \cdots, \mathfrak{P}_g \) are all distinct prime ideals of \( K \) above a ramified prime \( p \), see [26, Section 1]. In a special case, Pólya [24, Satz V] proved this statement for quadratic fields.

Based on Pólya’s and Ostrowski’s results, Zantema [26] introduced the concept of Pólya fields:

**Definition 1.1.** [26] A number field \( K \) is called Pólya, if the \( \mathcal{O}_K \)-module \( \text{Int}(\mathcal{O}_K) \) admits a regular basis.

Now we recall the concept of the Pólya group:

**Definition 1.2.** [3, Definition II.3.8] For a number field \( K \), the Pólya-Ostrowski group or Pólya group of \( K \) is the subgroup \( \text{Po}(K) \) of \( \text{Cl}(K) \) generated by the classes of the ideals \( J_n(K) \). It is easy to see that this is same as the subgroup generated by the classes of the ideals \( \Pi_q(K) \) as well, see [3, Proposition II.3.9].

Hence a number field \( K \) is Pólya, if and only if \( \text{Po}(K) \) is trivial. Obviously every number field with class number 1 is a Pólya field, but not conversely. For example, the quadratic field \( \mathbb{Q}(\sqrt{-71}) \) is a Pólya field, while it has class number 7.

Now let \( K \) be a Galois extension of \( \mathbb{Q} \) with Galois group \( G \). One can show that the ideals \( \Pi_q(K) \) freely generate the ambiguous ideals \( I(K)^G \), see [2, Section 2]. Thus \( \text{Po}(K) \) coincides with the subgroup of the ambiguous ideals modulo the principal ambiguous ideals, i.e. the subgroup \( I(K)^G/P(K)^G \) of \( \text{Cl}(K) \). Therefore for Galois number fields, the Galois action on the ideal class group would determine the Pólya group. Hilbert in [9, §75, Theorem 106] completely characterized the structure of ambiguous ideal classes for quadratic number fields, which implies that in a Pólya quadratic field at most two primes ramify. Using Hilbert’s theorem 106, Pólya [24] gave the complete list of Pólya quadratic fields, restated by Zantema, see Proposition (1.5) below.

Brumer and Rosen showed that ramification in Pólya Galois number fields is very restricted, see [2] Section 2. Moreover, we have the following relation between Pólya group and ramification due to Zantema:

**Proposition 1.3.** [26, Section 3, page 9] Let \( K/\mathbb{Q} \) be a Galois extension with Galois group \( G \), and \( p \) be a prime number. Denote the ramification index of \( p \) in
relative Pólya group and Pólya dihedral extensions of \( \mathbb{Q} \)

By \( e_p \). Then the following sequence is exact:

\[
\{0\} \longrightarrow H^1(G, U_K) \longrightarrow \bigoplus_{p \text{ prime}} \mathbb{Z}/e_p \mathbb{Z} \longrightarrow I(K)^G/P(K)^G \longrightarrow \{0\}.
\]

Remark 1.4. By the above exact sequence, for a Galois number field \( K \), \( \#Po(K) \) divides \( \prod_{p \text{ prime}} e_p \), and every ramification index \( e_p \) divides \( [K : \mathbb{Q}] \). Thus for any Galois number field \( K \), if \( [K : \mathbb{Q}] \) and \( h(K) \) are relatively prime then \( K \) is Pólya, but not conversely. For instance, as we will see, in Example 1.10, there is a Pólya \( D_7 \)-extension of \( \mathbb{Q} \) with class number 7. We give a generalization of this statement, see Remark 2.3.

Zantema [26] also found a criterion for Pólya-ness of cyclic number fields of prime power degree, see [26, Proposition 3.2]. In particular, as stated, he reproved Pólya’s complete characterization of quadratic Pólya fields:

**Proposition 1.5.** [26, Example 3.3] A quadratic field \( K = \mathbb{Q}(\sqrt{d}) \) is a Pólya field if and only if \( d \) has one of the following forms, where \( p \equiv q \pmod{4} \) denote two distinct odd prime numbers.

1. \( d=2, \text{ or } d=p; \)
2. \( d=-1, \text{ or } d=-2, \text{ or } d=-p \) where \( p \equiv 3 \pmod{4}; \)
3. \( d=2p, \text{ or } d=pq, \text{ if } K \text{ has no units of norm } -1. \)

Following Zantema’s results [26], Leriche [17] characterized cyclic cubic and cyclic quartic Pólya fields, and found a criterion for Pólya-ness of Galois closures of pure cubic fields [17]. Using Zantema’s exact sequence (1.1) and Brumer-Rosen’s result [2], Leriche gave an upper bound for the number of ramified primes in Pólya Galois number fields depending only on their degree over \( \mathbb{Q} \), see [17, Proposition 2.5]. We vastly improve this upper bound for Pólya dihedral extensions of \( \mathbb{Q} \) in Section 5.

We recall the concepts of the “genus field” and the “Hilbert class field”:

**Definition 1.6.** [13, Chapter 4] The genus field \( \Gamma(K) \) of \( K \), is a composite of an absolute abelian number field with \( K \), which is abelian over \( K \) and is unramified at all finite places of \( K \), and is maximal with these properties.

**Definition 1.7.** [5, Chapter 6, Section 4] The Hilbert class field \( H(K) \) of \( K \), is the maximal unramified abelian extension of \( K \). Obviously \( \Gamma(K) \subseteq H(K) \).

**Remark 1.8.** One can show that \( \text{Gal}(H(K)/K) \simeq \text{Cl}(K) \), see [5, Chapter 6, Section 4]. Also the Principal Ideal Theorem states that: “every fractional ideal of \( K \) becomes principal in \( H(K) \)”, see [5, Theorem 4.2].

In [18], Leriche considered a new embedding problem: “Is every number field contained in a Pólya field?”. Using the Principal Ideal Theorem, Leriche proved that for a number field \( K \), the Hilbert class field \( H(K) \) of \( K \) is a Pólya field, hence every number field \( K \) is embedded in a Pólya field, see [18, Corollary 3.2]. Leriche also proved that when \( K \) is abelian, the genus field \( \Gamma(K) \) of \( K \) is Pólya, see [18, Theorem 3.8]. We shall generalize these results in Section 2.

For an integer \( n \geq 3 \) and a transitive subgroup \( G \) of symmetric group \( S_n \) on \( n \) symbols, a \( G \)-field is defined to be a field \( K \) of degree \( n \) over \( \mathbb{Q} \) for which \( G \) is the Galois group of the Galois closure \( L \) of \( K \) over \( \mathbb{Q} \), see [26, Section 1]. Zantema [26] proved that a \( D_r \)-field \( K \) is a Pólya field if and only if \( h(K) = 1 \), see [26, Theorem 6.9].
In this article, our main purpose is generalizing our previous results in [19] for Pólya $S_3$-extension of $\mathbb{Q}$ to Pólya $D_r$-extensions of $\mathbb{Q}$.

Let $K$ be a $D_r$-field with Galois closure $L$. Denote the unique quadratic subfield of $L$ by $E$. We describe an outline of this paper as follows:

In Section (2), we generalize the concept of the Pólya group and define the “relative Pólya group $\text{Po}(M/N)$” for a finite extension $M/N$ of number fields. For finite Galois extensions of number fields, using Brumer-Rosen’s method in [2], we give an exact sequence generalizing Zantema’s exact sequence (1.1). In some special cases, we determine the structure of the relative Pólya group. In particular, we generalize Leriche’s results in [18], and prove that for a number field $N$, the relative Pólya group of the Hilbert class field of $N$ is trivial. Also we give a counterexample for triviality of the relative Pólya group of the genus field of $N$, see Example (2.13).

In Section (3), using the results in Section (2), for $D_r$-extensions of $\mathbb{Q}$, we find a relation between the Pólya groups $\text{Po}(E)$, $\text{Po}(K)$ and $\text{Po}(L)$, see Theorem (3.3). Then we present some interesting consequences, see Corollaries (3.6), (3.7), (3.8), (3.9), (3.10) and (3.13). Also we generalize Honda’s result in [10] and give necessary and sufficient conditions for divisibility of $h(E)$ by $r$, see Lemma (3.11).

Finally, following Masley’s article [20], we show that $h(K)$ divides $h(L)$ and conclude that if $h(L) = 1$, then both subfields $E$ and $K$ are Pólya, see Corollary (3.16) and (3.17).

In Section (4), first we give some examples of Pólya and non-Pólya $S_3$-extensions of $\mathbb{Q}$ studied in [19]. Then following [14], for a monic polynomial $f(X) \in \mathbb{Z}[X]$ of degree $r$, we restate the necessary and sufficient conditions to $\text{Gal}(f/\mathbb{Q}) \cong D_r$, see Proposition (4.5). Using Brumer’s theorem and generic polynomials for $D_5$-extensions of $\mathbb{Q}$, we find some examples of Pólya and non-Pólya $D_5$-extensions of $\mathbb{Q}$, see Proposition (4.8). Following [15], we consider the special family of generic polynomials for $D_5$-extensions of $\mathbb{Q}$ whose splitting fields are unramified over their quadratic subfields, and determine when these types of $D_5$-extensions of $\mathbb{Q}$ are Pólya, see Proposition (4.12) and Corollary (4.13). Finally, following [14], for $r = 7, 13, 19$ we give some examples of Pólya $D_r$-extensions of $\mathbb{Q}$.

In Section (5), by a cohomological interpretation similar to [19], we decrease Leriche’s upper bound [17, Section 2], for the number of ramified primes in Pólya $D_r$-extensions of $\mathbb{Q}$. We prove that for $r > 3$ and a real (resp. imaginary) Pólya $D_r$-extension of $\mathbb{Q}$, at most four (resp. two) primes ramify, see Theorem (5.1). As a consequence, for special family of $D_r$-fields we improve Ishida’s result [12]. we prove that for $r > 3$ and a $D_r$-field $K$ with real (resp. imaginary) Galois closure $L$, if the quadratic subfield $E$ of $L$ is Pólya and at least three (resp. two) primes totally ramify in $K/\mathbb{Q}$, then $r \mid h(K)$. Also we prove a similar result for $S_3$-fields, see Corollaries (5.2) and (5.3).

2. Relative Pólya group

Using Brumer-Rosen’s method in [2], we can generalize Zantema’s result in [26, Section 3] to finite Galois extensions of number fields and find an exact sequence similar to (1.1). First we generalize concept of the Pólya group:

**Definition 2.1.** Let $M/N$ be a finite extension of number fields. The *relative Pólya group* of $M$ over $N$, is the subgroup of $\text{Cl}(M)$ generated by the set of all ideals $\Pi_{\mathfrak{P}^f}(M/N)$, where $\mathfrak{P}$ is a prime ideal of $N$, $f$ is a positive integer and $\Pi_{\mathfrak{P}^f}(M/N)$
is defined as follows:

\[ \Pi_{\mathfrak{P}}(M/N) = \prod_{\mathfrak{M} \in \text{Max}(O_M) \atop N_{M/N}(\mathfrak{M}) = \mathfrak{P}} \mathfrak{M}. \]

We denote the relative Pólya group of \( M \) over \( N \) by \( Po(M/N) \). In particular, \( Po(M/Q) = Po(M) \) and \( Po(M/M) = Cl(M) \).

Now let \( M/N \) be a Galois extension with Galois group \( G \). It is easily seen that the set of all ideals \( \Pi_{\mathfrak{P}}(M/N) \) is a set of free generators for the ambiguous ideals \( I(M)^G \), see [2, Proof of Proposition 2.2]. On the other hand \( P(M)^G = I(M)^G \cap P(M) \). Hence in this case \( Po(M/N) = I(M)^G/P(M)^G \). As in [26, Section 3], we define:

\[
\psi : I(M)^G \to \bigoplus_{\mathfrak{P} \text{ is a prime of } N} \mathbb{Z}/e_{\mathfrak{P}} \mathbb{Z}
\]

\[
\psi(\prod_{i=1}^m \Pi_{\mathfrak{P}_i}(M/N) t_i))_{\mathfrak{P}_i} := t_i(\text{mod } e_{\mathfrak{P}_i}),
\]

where \( m \) is a positive integer, \( t_i \)'s are integers numbers and \( e_{\mathfrak{P}} \) denotes the ramification index of \( \mathfrak{P} \) in \( M/N \). It is clear that \( \psi \) is a group epimorphism and one can show that \( \ker(\psi) = I(N) \). Hence we get the following exact sequence:

\[
\{0\} \to I(N) \to I(M)^G \to \bigoplus_{\mathfrak{P} \text{ is prime of } N} \mathbb{Z}/e_{\mathfrak{P}} \mathbb{Z} \to \{0\}.
\]

Now following Brumer-Rosen [2], Consider the following exact sequence:

\[
\{0\} \to U_M \to M^* \to P(M) \to \{0\}.
\]

Taking Cohomology and using Hilbert’s theorem 90, we obtain the exact sequence:

\[
\{0\} \to U_N \to N^* \to P(M)^G \to H^1(G, U_M) \to \{0\}.
\]

Equivalently, the following sequence is exact:

\[
\{0\} \to P(N) \to P(M)^G \to H^1(G, U_M) \to \{0\}.
\]

Now we can generalize Zantema’s result in [26, Section 3]:

**Theorem 2.2.** Let \( M/N \) be a finite Galois extension of number fields with Galois group \( G \). Then the following sequence is exact:

\[
\{0\} \to \ker(j_{M/N}) \to H^1(G, U_M) \to \bigoplus_{\mathfrak{P} \text{ is prime of } N} \mathbb{Z}/e_{\mathfrak{P}} \mathbb{Z} \to \frac{Po(M/N)}{Po(M/N)(Cl(N))} \to \{0\}.
\]
Proof. We have the following commutative diagram with exact rows of abelian groups:

\[
\begin{array}{cccccc}
\{0\} & \rightarrow & P(N) & \rightarrow & I(N) & \rightarrow \text{Cl}(N) & \rightarrow \{0\} \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\{0\} & \rightarrow & P(M)^G & \rightarrow & I(M)^G & \rightarrow & \text{I}(M)^G/\text{P}(M)^G & \rightarrow \{0\} \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & \text{\psi} \downarrow & \text{\oplus}_{\text{disc}(M/N)} \mathbb{Z}/e_{\mathbb{P}}\mathbb{Z} \\
H^1(G, U_M) & \rightarrow & 0 & \rightarrow & 0 & \rightarrow & 0 \\
\end{array}
\]

The first column is the exact sequence (2.3), and the second column is the exact sequence (2.2). Hence by the snake lemma, we find an exact sequence as follows:

\[
\{0\} \rightarrow \text{Ker}(j_{M/N}) \rightarrow H^1(G, U_M) \rightarrow \bigoplus_{\mathbb{P}\mid \text{disc}(M/N)} \mathbb{Z}/e_{\mathbb{P}}\mathbb{Z} \rightarrow \text{Coker}(j_{M/N}) \rightarrow \{0\}.
\]

Since \(M/N\) is a Galois extension, \(\text{Po}(M/N) = \text{I}(M)^G/\text{P}(M)^G\) and the statement is proved.

Rem

\textbf{Remark 2.3.} By the exact sequence in Theorem (2.2), the order of quotient group \(\text{Po}(M/N)\) divides a power of \([M : N]\). On the other hand, \(\text{Po}(M/N)\) is a subgroup of \(\text{Cl}(M)\). Hence if \(\gcd(h(M), [M : N]) = 1\), then \(\text{Po}(M/N) = j_{M/N}(\text{Cl}(N))\). Note that this statement is a generalization of Remark (1.4).

\textbf{Corollary 2.4.} Let \(M/N\) be a finite Galois extension of number fields with Galois group \(G\). If \(h(N)\) is relatively prime to \([M : N]\), then \(\text{Cl}(N)\) is embedded in \(\text{Po}(M/N)\). In particular, \(h(N)\) divides \(h(M)\). Moreover, we get a generalization of Zantema’s exact sequence (1.1) as follows:

\[
\{0\} \rightarrow H^1(G, U_M) \rightarrow \bigoplus_{\mathbb{P}\mid \text{disc}(M/N)} \mathbb{Z}/e_{\mathbb{P}}\mathbb{Z} \rightarrow \text{Po}(M/N)/\text{Cl}(N) \rightarrow \{0\}.
\]

Proof. Assume that \(h(N)\) is relatively prime to \([M : N]\). For every prime \(p\) dividing \(\#G\), denote the \(p\)-sylow subgroup of \(G\) by \(G_p\). Since the Restriction map, embeds the \(p\)-primary part of \(H^1(G, U_M)\) in \(H^1(G_p, U_M)\), see [22, Proposition 1.6.9], \(h(N)\) would be relatively prime to \(\#H^1(G, U_M)\). On the other hand, by exact sequence in Theorem (2.2), \(\#\text{Ker}(j_{M/N})\) divides \(\#H^1(G, U_M)\). Since \(\text{Ker}(j_{M/N})\) is a subgroup of \(\text{Cl}(N)\), \(\text{Ker}(j_{M/N}) = \{0\}\), i.e. \(j_{M/N}\) is injective and the statement follows from Theorem (2.2).

\textbf{Remark 2.5.} Note that when \(h(N)\) and \([M : N]\) are relatively prime, then \(h(N) / h(M)\), even for non-Galois extensions \(M/N\), see [21, Corollary 1 after Proposition 4.49].)
Corollary 2.6. Let \( M/N \) be a finite Galois extension of number fields with Galois group \( G \). If every ideal class of \( N \) extended to \( M \) is principal, then
\[
\{0\} \to \text{Cl}(N) \to H^1(G, U_M) \to \bigoplus_{\mathfrak{p} \text{ is prime of } N} \mathbb{Z}/\mathfrak{p}\mathbb{Z} \to \text{Po}(M/N) \to \{0\}
\]
is exact.

Proof. In this case, \( \text{Ker}(j_{M/N}) = \text{Cl}(N) \) and the statement follows from Theorem 2.2. Note that this generalizes Zantema’s exact sequence (1.1). \( \square \)

Corollary 2.7. Let \( M/N \) be a finite Galois extension of number fields with Galois group \( G \). If all finite places of \( N \) are unramified in \( M \), then \( H^1(G, U_M) \) is embedded in \( \text{Cl}(N) \) and \( \text{Po}(M/N) \simeq j_{M/N}(\text{Cl}(N)) \).

Proof. If all finite places of \( N \) are unramified in \( M \), by exact sequence in Theorem 2.2, \( H^1(G, U_M) \simeq \text{Ker}(j_{M/N}) \) is a subgroup of \( \text{Cl}(N) \) and the quotient group \( j_{M/N}(\text{Cl}(N)) / \text{Po}(M/N) \) would be trivial. \( \square \)

Corollary 2.8. Let \( M/N \) be a finite Galois extension of number fields with Galois group \( G \). If every ideal class of \( N \) extended to \( M \) is principal and all finite places of \( N \) are unramified in \( M \), then \( \text{Cl}(N) \simeq H^1(G, U_M) \) and \( \text{Po}(M/N) = \{0\} \). In particular, the relative Połya group of the Hilbert class field \( H(N) \) of \( N \) (over \( N \)) is trivial.

Proof. Immediately follows from Corollaries 2.6 and 2.7. \( \square \)

Leriche in [15] proved that:

Proposition 2.9. [15] Section 3.1] Let \( M/N \) be a finite Galois extension of number fields such that every ideal class of \( N \) extended to \( M \) is principal. If all finite places are unramified in the extension \( M/N \), then \( M \) is a Połya field. In particular, the Hilbert class field \( H(N) \) of \( N \) is Połya.

Using the following lemma (for \( P = \mathbb{Q} \)), we conclude that Corollary 2.8 is a generalization of the above proposition:

Lemma 2.10. Let \( P \subseteq N \subseteq M \) be a tower of finite extensions of number fields. If \( M/N \) is a Galois extension, then \( j_{M/N}(\text{Po}(N/P)) \subseteq \text{Po}(M/P) \subseteq \text{Po}(M/N) \).

Proof. To prove the first inclusion, suppose that \( \Pi_{p^f}(N/P) = \prod_{i=1}^u n_i \), where \( p \) is a prime of \( P \) and \( f \) is a nonnegative integer. Since \( M/N \) is a Galois extension, for every \( i = 1, 2, \ldots, u \), all prime ideals of \( M \) above \( n_i \) have the same ramification index (over \( n_i \)), say \( e_i \), and the same ideal norm (over \( N \)), say \( n_i^{f_i} \). Hence one can write:
\[
j_{M/N}(n_i) = (m_1^{(i)} \cdots m_u^{(i)})^{e_i} = (\Pi_{i=1}^u n_i^{f_i} (M/N))^{e_i}.
\]

Since \( N_{P^{f_k}}(n_i) = p^f \), for every \( k = 1, \ldots, j \), we have \( N_{M/P}(m_k^{(i)}) = p^{f_k} \). Therefore
\[
j_{M/N}(\Pi_{p^f}(N/P)) = \prod_{i=1}^u (\Pi_{p^{f_k}}(M/P))^{e_i} \in \text{Po}(M/P).
\]

To prove the second inclusion, let
\[
p_{M} = m_1^{e_1'} m_2^{e_2'} \cdots m_u^{e_u'},
p_{N} = n_1^{e_1} n_2^{e_2} \cdots n_u^{e_u},
\]

where \( e_i' \) and \( e_i \) are the same for all \( i = 1, 2, \ldots, u \). Since \( P \subseteq N \subseteq M \), we have \( \Pi_{P^{f_k}}(N/P) = p^f \). Therefore, for every \( i = 1, 2, \ldots, j \),
\[
j_{M/N}(\Pi_{p^f}(N/P)) = \prod_{i=1}^u (\Pi_{p^{f_k}}(M/P))^{e_i} \in \text{Po}(M/P),
\]

and
\[
j_{M/N}(\Pi_{p^f}(N/P)) = \prod_{i=1}^u (\Pi_{p^{f_k}}(M/P))^{e_i} \in \text{Po}(M/P),
\]

hence
\[
j_{M/N}(\Pi_{p^f}(N/P)) = \prod_{i=1}^u (\Pi_{p^{f_k}}(M/P))^{e_i} \in \text{Po}(M/P).
\]

\( \square \)
be the decomposition forms of $p$ in $N/P$ and $M/P$, respectively. Let $\Pi_p f(M/P) = \prod_{j=1}^d m_j$, and $\{n_1, n_2, \cdots, n_l\} = \{m_j \cap N : j = 1, 2, \cdots, d\}$ be set of all the distinct prime ideals of $N$ below $m_j$’s. Also for every $i = 1, \ldots, l$, let $\{m_{i,1}, \cdots, m_{i,s_i}\}$ be the set of all the distinct prime ideals of $M$ above $n_i$. Since $M/N$ is a Galois extension, for every $i = 1, \ldots, l$, the ideals $m_{i,1}, m_{i,2}, \cdots, m_{i,s_i}$ have the same ideal norm (over $N$), say $n_{f_i}$. Hence

$$\Pi_p f(M/P) = \prod_{i=1}^l \Pi_{n_{f_i}}(M/N) \in Po(M/N).$$

\[\square\]

**Remark 2.11.** (i) Chabert in [4], for a finite extension $M/N$ of Galois number fields proved that $j_{M/N}(Po(N)) \subseteq Po(M)$. Hence Lemma (2.10), is a generalization of Chabert’s result.

(ii) By Corollary (2.8) and Lemma (2.10), we have $Po(H(H(N))/N)$ is trivial. Hence every number field in the tower of Hilbert class fields for $N$ has trivial relative Pólya group over $N$.

When $M$ and $N$ are Galois extensions of $\mathbb{Q}$, Leriche [18] proved the following:

**Proposition 2.12.** [18, Section 3.2] Let $M/N$ be a finite extension of Galois number fields. If all finite places of $N$ are unramified in $M$, and $j_{M/N}(Po(N))$ is trivial, then $M$ is Pólya. Moreover, if $N$ is an abelian number field, then the genus field $\Gamma(N)$ of $N$ is Pólya.

We want to generalize the above result. But before this, note that unlike the Hilbert class field, the relative Pólya group of the genus field, even for abelian number fields, is not necessarily trivial:

**Example 2.13.** For $N = \mathbb{Q}(\sqrt{-23})$, one can show that $\Gamma(N) = N$, see [13, Chapter 4, page 4]. Hence $Po(\Gamma(N)/N) = Cl(N) \simeq \mathbb{Z}/3\mathbb{Z}$.

Now we generalize Leriche’s result in Proposition (2.12):
exact rows of abelian groups:

\[
\begin{array}{ccccccc}
\{0\} & \rightarrow & H^1(T,U_N) & \oplus_{p|D_N} \mathbb{Z}/e_p\mathbb{Z} & \rightarrow & \text{Po}(N) & \rightarrow \{0\} \\
\downarrow & & \downarrow \text{Inf} & & \downarrow i & & \downarrow j_{M/N} \\
\{0\} & \rightarrow & H^1(G,U_M) & \oplus_{p|D_M} \mathbb{Z}/e(p)\mathbb{Z} & \rightarrow & \text{Po}(M) & \rightarrow \{0\} \\
\downarrow & & \downarrow \frac{H^1(G,U_M)}{H^1(T,U_N)} & & \downarrow \bigoplus_{\mathfrak{p}|\text{disc}(M/N)} \mathbb{Z}/e(\mathfrak{p})\mathbb{Z} & & \\
\{0\} & \rightarrow & \{0\} \\
\end{array}
\]

where \( i \) is the inclusion map, \( p \) is a prime number, \( e_\mathfrak{p} \) and \( e(p) \) are the ramification indices of \( p \) in \( N/\mathbb{Q} \) and \( M/\mathbb{Q} \), respectively. Also \( \mathfrak{p} \) is a prime of \( N \) and \( e(\mathfrak{p}) \) is the ramification index of \( \mathfrak{p} \) in \( M/N \).

Using the snake lemma, the statement is proved. \( \square \)

**Corollary 2.15.** Let \( M/N \) be a finite extension of Galois number fields with \( G = \text{Gal}(M/\mathbb{Q}) \) and \( T = \text{Gal}(N/\mathbb{Q}) \).

(i) If all finite places of \( N \) are unramified in \( M \), then \( \text{Po}(M) = j_{M/N}(\text{Po}(N)) \) and \( \text{Ker}(j_{M/N}|_{\text{Po}(N)}) \simeq \frac{H^1(G,U_M)}{H^1(T,U_N)} \).

(ii) If \( j_{M/N}(\text{Po}(N)) \) is trivial, then we get a generalization of Zantema’s exact sequence (1.1):

\[
\begin{equation}
(2.6) \quad \{0\} \rightarrow \text{Po}(N) \rightarrow \frac{H^1(G,U_M)}{H^1(T,U_N)} \rightarrow \bigoplus_{\mathfrak{p}|\text{disc}(M/N)} \mathbb{Z}/e(\mathfrak{p})\mathbb{Z} \rightarrow \text{Po}(M) \rightarrow \{0\}.
\end{equation}
\]

(iii) If \( j : \text{Po}(N) \rightarrow \text{Po}(M) \) is injective, then we find another generalization of Zantema’s exact sequence (1.1):

\[
\begin{equation}
(2.7) \quad \{0\} \rightarrow \frac{H^1(G,U_M)}{H^1(T,U_N)} \rightarrow \bigoplus_{\mathfrak{p}|\text{disc}(M/N)} \mathbb{Z}/e(\mathfrak{p})\mathbb{Z} \rightarrow \frac{\text{Po}(M)}{\text{Po}(N)} \rightarrow \{0\}.
\end{equation}
\]

**Proof.** Immediately follows from Theorem (2.14). \( \square \)

Now we are interested in finding some finite extension \( M/N \) of Galois number fields for which the map \( j_{M/N} : \text{Po}(N) \rightarrow \text{Po}(M) \) is injective. For this purpose, we can restrict the degrees of \( M \) and \( N \) over \( \mathbb{Q} \):

**Theorem 2.16.** Let \( M \) be a Galois extension of \( \mathbb{Q} \) of degree \( pq \), where \( p < q \) are prime numbers. Denote the subfield of \( M \) of degree \( p \) over \( \mathbb{Q} \) by \( N \). Then \( \text{Po}(N) \) is embedded in \( \text{Po}(M) \).

**Proof.** Assume that \( G = \text{Gal}(M/\mathbb{Q}) \) and denote the subgroup of \( G \) of index \( p \) by \( H \). Hence \( H \) is a normal subgroup of \( G \), and \( N \) would be Galois over \( \mathbb{Q} \). Since \( N/\mathbb{Q} \)
is a cyclic extension of prime degree $p$, every ramified prime number $p_0$ in $N/Q$ is totally ramified, i.e.:

$$p_0 \mathcal{O}_N = \mathfrak{P}^p = (\Pi_{p_0}(N))^p,$$

for some prime ideal $\mathfrak{P}$ of $N$.

Now consider the decomposition form of $p_0$ in $M/Q$. Let $\gamma$ be a prime ideal of $M$ above $p_0$. One has $p|e(\gamma/p_0)$ and $e(\gamma/p_0)|pq$. Hence three cases are possible:

Case (1) If $e(\gamma/p_0) = p$ and $f(\gamma/p_0) = q$, then $p_0 \mathcal{O}_M = (\Pi_{p_0}(M))^p$. Comparing with the decomposition form (2.8), we have $j_{M/N}(\Pi_{p_0}(N)) = \Pi_{q}(M)$. Now suppose that $\Pi_{p_0}(N) \in Ker(j_{M/N})$. Hence $\Pi_{p_0}(M)$ is principal and taking the relative ideal norm of $M$ over $N$, one has $\Pi_{p_0}(N)$ is principal.

Case (2) If $e(\gamma/p_0) = p$ and $f(\gamma/p_0) = 1$, then $p_0 \mathcal{O}_M = (\gamma_1 \gamma_2 \cdots \gamma_q)^p = (\Pi_{p_0}(M))^p$, which implies that $j_{M/N}(\Pi_{p_0}(N)) = (\Pi_{p_0}(M))$. Now if $\Pi_{p_0}(N)$ is principal, taking the relative ideal norm of $M$ over $N$, we find $(\Pi_{p_0}(N))^q$ is principal. Since $(\Pi_{p_0}(N))^p$ is principal, and $p$ and $q$ are distinct prime numbers, $\Pi_{p_0}(N)$ is principal.

Case (3) If $e(\gamma/p_0) = pq$, then $p_0 \mathcal{O}_M = (\Pi_{p_0}(M))^{pq}$ and so $j_{M/N}(\Pi_{p_0}(N)) = (\Pi_{p_0}(M))^q$. Hence if $\Pi_{p_0}(N) \in Ker(j_{M/N})$, then $(\Pi_{p_0}(M))^q$ would be principal. Therefore $N_{M/N}/(\Pi_{p_0}(M)) = \Pi_{p_0}(N)$ is principal. On the other hand, $\Pi_{p_0}(N)$ is principal and since $p$ and $q$ are distinct prime numbers, $\Pi_{p_0}(N)$ is principal.

Summing up the above arguments, we find $j_{M/N} : \mathcal{O}_N(M) \rightarrow \mathcal{O}_M(M)$ is injective and the statement is proved.

Remark 2.17. Using Galois cohomology, we can give another proof of Theorem (2.16), starting with the following:

Lemma 2.18. Let $M$ be a Galois extension of $\mathbb{Q}$ of degree $pq$, where $p < q$ are prime numbers. Denote the subfield of $M$ of degree $p$ over $\mathbb{Q}$ by $N$ and assume that $H = Gal(M/N)$. Then $H^1(H, U_M)$ has order $q^t$ for some $t \geq 0$.

Proof. Since $M/N$ is a cyclic extension, we can use the Herbrand quotient:

$$Q(H, U_M) = \frac{\# H^0(H, U_M)}{\# H^1(H, U_M)},$$

where

$$H^0(H, U_M) = \frac{U_M^H}{N_{M/N}(U_M)} = \frac{U_N}{N_{M/N}(U_M)}.$$

On the other hand, we have $Q(H, U_M) = \frac{q^s}{[M:N]}$, where $s$ is the number of infinite places of $N$ ramified in $M$, see [5] Proposition 5.10]. Hence:

$$\# H^1(H, U_M) = (U_N : N_{M/N}(U_M)) \cdot \frac{q^s}{2^t}.$$

Since $N_{M/N}(U_M)$ contains $U_N^s$, $(U_N : N_{M/N}(U_M))$ divides $U_N^s$. Denote the torsion subgroup of $U_N$ by $\mu(N)$. If $N$ is totally real, then $\mu(N) = \{\pm 1\}$ and since $q$ is an odd prime number, $(U_N : U_N^s) = q^{w_N}$, where $w_N$ is the Dirichlet rank of $U_N$.

Now assume that $N$ is totally imaginary and $\zeta_n \in \mu(N)$, for some positive integer $n$. Hence $\varphi(n)|p$, where $\varphi$ is the Euler’s $\varphi$ function. By an elementary calculation,
one can show that either $p = 2$ and $n \in \{2, 3, 4\}$, or $p$ is odd and $n = 2$. In both cases, we have $(\mu(N) : \mu(N)^r)|q$ and $(U_N : U_N^r)|q^{w_N+1}$.

By the above argument and using relation (2.10), we have

$$2^s \cdot \#H^1(H, U_M)|q^{w_N+2},$$

which implies that $s = 0$ and the statement is proved. □

Now we can give another proof of Theorem (2.16):

Proof. Assume that $G = Gal(M/Q)$, $H = Gal(M/N)$ and $T = Gal(N/Q)$. By exact sequence (2.14) in proof of Theorem (2.14) and Zantema’s exact sequence (1.1), we find the commutative diagram with exact rows as follows:

\[
\begin{array}{cccccc}
\{0\} & \rightarrow & H^1(T, U_N) & \rightarrow & H^1(G, U_M) & \rightarrow & H^1(G, U_M) \\
\{0\} & \rightarrow & \oplus_{a|D_N} \mathbb{Z}/e_a \mathbb{Z} & \rightarrow & \oplus_{b|D_M} \mathbb{Z}/e(b) \mathbb{Z} & \rightarrow & \oplus_{\mathfrak{p}|disc(M/N)} \mathbb{Z}/e(\mathfrak{p}) \mathbb{Z} & \rightarrow & \{0\} \\
\{0\} & \rightarrow & Po(N) & \rightarrow & Po(M) & \rightarrow & \{0\} \\
\{0\} & \rightarrow & \{0\} & \rightarrow & \{0\} & \rightarrow & \{0\} \\
\end{array}
\]

where $i$ is the inclusion map, $a$ is a prime number with the ramification index $e_a$ in $N$, $b$ is a prime number with the ramification index $e(b)$ in $M$, $\mathfrak{p}$ is a prime of $N$ with the ramification index $e(\mathfrak{p})$ in $M$, and $\theta$ is the map obtained in the exact sequence (2.4). Using the snake lemma, we get the following exact sequence:

\[(2.11) \quad \{0\} \rightarrow Ker(\theta) \rightarrow Po(N) \rightarrow Po(M) \rightarrow Coker(\theta) \rightarrow \{0\}.\]

By the exact sequence (2.15) $\text{Ker}(\theta)$ is a subgroup of $H^1(H, U_M)$ and by Lemma (2.18), $\#\text{Ker}(\theta)$ is a power of $q$. On the other hand, by the exact sequence (2.11), $Ker(\theta)$ is a subgroup of $Po(N)$ and by Zantema’s exact sequence (1.1), $\#\text{Po}(N)$ is a power of $[N : Q] = p$ which implies that $\#\text{Ker}(\theta)$ is also a power of $p$. Since $p$ and $q$ are distinct prime numbers, $Ker(\theta) = \{0\}$ and finally we find the following exact sequence:

\[(2.12) \quad \{0\} \rightarrow Po(N) \rightarrow Po(M) \rightarrow Coker(\theta) \rightarrow \{0\}.\]

Therefore $Po(N)$ is embedded in $Po(M)$. □

Remark 2.19. Theorem (2.16) doesn’t hold if $p = q$. For instance, for $N = \mathbb{Q}(\sqrt{-5})$ and $M = \mathbb{Q}(\sqrt{-1}, \sqrt{-5})$, $N$ is not Pólya, while $M$ is Pólya.

Combining Corollary (2.15) with Theorem (2.16), we have:
Corollary 2.20. Let $M$ be a Galois extension of $\mathbb{Q}$ of degree $pq$, where $p < q$ are prime numbers. Denote the subfield of $M$ of degree $p$ over $\mathbb{Q}$ by $N$. If all finite places of $N$ are unramified in $M$, then $H^1(Gal(M/\mathbb{Q}), U_M) \simeq H^1(Gal(N/\mathbb{Q}), U_N)$ and $Po(N) \simeq Po(M)$.

Remark 2.21. Note that with notations and hypotheses in Corollary (2.20), $M$ cannot be abelian over $\mathbb{Q}$. To prove this, suppose that $M/\mathbb{Q}$ is abelian and denote the subfield of $M$ of degree $q$ over $\mathbb{Q}$ by $F$. Hence $F$ is a Galois extension of $\mathbb{Q}$ and every ramified prime in $F/\mathbb{Q}$ has the ramification index $q$. Let $a$ be a ramified prime in $F/\mathbb{Q}$. Hence $q$ divides the ramification index of $a$ in $M/\mathbb{Q}$. Now let $\mathfrak{p}$ be a prime of $N$ above $a$. Since $[M : N] = p$, $\mathfrak{p}$ must be ramified in $M/N$ and we reach a contradiction.

3. Main Result

From now on, let $L$ be a Galois extension of $\mathbb{Q}$ with Galois group $Gal(L/\mathbb{Q}) \simeq D_r = \langle \sigma, \tau : \sigma^2 = 1, \tau \sigma = \sigma^{-1} \rangle$, and denote the fixed fields of $\sigma$ and $\tau$ by $E$ and $K$, respectively.

Suppose that $p$ is a ramified prime in $L/\mathbb{Q}$, and denote its decomposition in $L$ by $p\mathcal{O}_L = (\gamma_1 \gamma_2 \cdots \gamma_r)^{e(p)}$. Since $e(p)f(p)g = [L : \mathbb{Q}] = 2r$, we have $e(p) = 2$ or $e(p) = 2r$ or $e(p) = 2r$, where $f(p)$ is the residue class degree of $\gamma_i$'s over $p$.

With these notations, following [6] we restate the complete description of decomposition forms of ramified primes $p$ in $K/\mathbb{Q}$ and $L/\mathbb{Q}$:

Proposition 3.1. With the notations of this section, the following assertions hold:

1. If $e(p) = 2$, then $f(p) = 1$. Moreover, if

$$p\mathcal{O}_L = \gamma_1^2 \gamma_2^2 \cdots \gamma_r^2$$

is the decomposition of $p$ in $L/\mathbb{Q}$, then the decomposition of $p$ in $K/\mathbb{Q}$ has the form below:

$$p\mathcal{O}_K = \beta_1^2 \beta_2^2 \cdots \beta_r^2$$

2. If $e(p) = r$, then $f(p) = 1$ or $f(p) = 2$ and $p$ is totally ramified in $K/\mathbb{Q}$.
3. If $e(p) = 2r$, then $p = r$ and it is totally ramified in $K/\mathbb{Q}$.

Proof. A detailed analysis of ramification groups using [25] Chapter III yields the claims, for details see [6] Proposition 10.1.26].

Remark 3.2. Note that by Proposition (3.1), the set of ramified primes in the extensions $K/\mathbb{Q}$ and $L/\mathbb{Q}$ coincide. Also for a ramified prime $p$ in $L/\mathbb{Q}$ with $e(p) = 2$, let $\alpha = \gamma_1 \cap E$ be a prime ideal of $\mathcal{O}_E$ above $p$. We have:

$$2 = e(p) = e(\gamma_1/\alpha)e(\alpha/p).$$

Since $e(\gamma_1/\alpha)$ divides $[L : E] = r$, we have $e(\gamma_1/\alpha) = 1$ and hence $p$ is ramified in $E/\mathbb{Q}$. Thus $p\mathcal{O}_E = (\Pi_p(E))^2$ and

$$p\mathcal{O}_L = (\Pi_p(E)\mathcal{O}_L)^2 = (\gamma_1 \gamma_2 \cdots \gamma_r)^2 = (\Pi_p(L))^2,$$

which implies that

$$j_{L/E}(\Pi_p(E)) = \Pi_p(L).$$

Similarly, for $e(p) = r$ one can show that $p$ doesn’t ramify in $E/\mathbb{Q}$ and depending on whether $f(p) = 1$ or $f(p) = 2$, $p$ splits or remains inert in $E/\mathbb{Q}$, respectively.
Now we give the main result:

**Theorem 3.3.** With the notations in this section, there exists an exact sequence as follows:

\[ \{0\} \rightarrow Po(E) \rightarrow Po(L) \rightarrow Po(K). \]  

(3.5)

Moreover, the 2-torsion subgroup of Po(L) is isomorphic to Po(E) and the r-torsion subgroup of Po(L) is embedded in Po(K). Note that Po(L) is a 2r-torsion group.

**Proof.** By Theorem (2.16), we find the following exact sequence:

\[ \{0\} \rightarrow Po(E) \rightarrow Po(L) \rightarrow \frac{Po(L)}{j_{L/E}(Po(E))} \rightarrow \{0\}. \]

(3.6)

Using Proposition (3.1) and Equation (3.4) in Remark (3.2), we have is isomorphic to the subgroup of Po(L) generated by all the ideals \( \Pi_{p_f}(L) \), where \( f \) is a positive integer and \( p \) is a ramified prime number in \( L/\mathbb{Q} \) with \( r|e(p) \). Equivalently \( \frac{Po(L)}{j_{L/E}(Po(E))} \) is isomorphic to the r-torsion subgroup of Po(L). Now we define:

\[ \varphi : \frac{Po(L)}{j_{L/E}(Po(E))} \rightarrow Po(K) \]

\[ \Pi_{p_f}(L) \mapsto N_{L/K}(\Pi_{p_f}(L)). \]

We show that \( \varphi \) is injective:

Let \( p \) be a ramified prime number in \( L/\mathbb{Q} \) such that \( r|e(p) \). By Proposition (3.1), \( p \) is totally ramified in \( K/\mathbb{Q} \). Now if \( e(p) = r \), by Remark (3.2), \( p \) is unramified in \( E/\mathbb{Q} \) and depending on whether it splits or remains inert in \( E \), \( p\mathcal{O}_E = (\gamma_1\gamma_2)^r \) or \( p\mathcal{O}_E = \gamma^r \), respectively. Hence for \( e(p) = r \), we have \( \Pi_{p_f}(K)\mathcal{O}_L = \Pi_{p_f}(L) \) (or \( \Pi_{p_f}(L) \)), which implies that if \( \Pi_{p}(K) = N_{L/K}(\Pi_{p_f}(L)) \) (resp. \( \Pi_{p}(K) = N_{L/K}(\Pi_{p_f}(L)) \)) is principal, then so is \( \Pi_{p_f}(L) \) (resp. \( \Pi_{p_f}(L) \)).

Now assume that \( e(p) = 2r \). By Proposition (3.1), \( p = r \) ramifies totally in \( L/\mathbb{Q} \) and so in all its subextensions. In this case we have \( \Pi_{r_f}(K)\mathcal{O}_L = (\Pi_{r_f}(L))^2 \). Hence if \( \Pi_{r_f}(K) = N_{L/K}(\Pi_{r_f}(L)) \) is principal, then \( \Pi_{r_f}(L) \) belongs to the 2-torsion subgroup of \( Po(L) \), i.e. belongs to \( j_{L/E}(Po(E)) \), since

\[ j_{L/E}(\Pi_{r_f}(E)) = \Pi_{r_f}(E)\mathcal{O}_L = (\Pi_{r_f}(L))^r = \Pi_{r_f}(L)(\Pi_{r_f}(L))^{r-1} = \Pi_{r_f}(L). \]

Therefore, \( \frac{Po(L)}{j_{L/E}(Po(E))} \) is embedded in \( Po(K) \) and we find the following exact sequence:

\[ \{0\} \rightarrow Po(E) \rightarrow Po(L) \rightarrow Po(K). \]

\[ \{0\} \rightarrow Po(E) \rightarrow Po(L) \rightarrow Coker(\theta) \rightarrow \{0\}. \]

(3.7)  

where \( \theta : H^1(Gal(L/\mathbb{Q})) \rightarrow \bigoplus_{\mathcal{P}|\mathcal{O}_L} \mathbb{Z}/e(\mathcal{P})\mathbb{Z} \), is the map obtained in the exact sequence (2.4). Hence by Theorem (3.3), we have \( \frac{Po(L)}{j_{L/E}(Po(E))} \simeq Coker(\theta) \). In particular, \( Coker(\theta) \) is embedded in \( Po(K) \).
Remark 3.5. Zantema [26], proved that for two finite Galois extensions $K_1$ and $K_2$ of $\mathbb{Q}$ with $M = K_1.K_2$, if for every prime number $p$, the ramification indices of $p$ in $K_1$ and $K_2$ are coprime, then Pólya-ness of $K_1$ and $K_2$ implies that $M$ is also Pólya. Conversely, if $gcd([K_1 : \mathbb{Q}], [K_2 : \mathbb{Q}]) = 1$ and $M$ is Pólya then $K_1$ and $K_2$ are Pólya, see [26] Theorem 3.4. Under these hypotheses, one can easily show that $j_{M/K_1}(Po(K_1))j_{M/K_2}(Po(K_2)) = Po(M)$, see [1]. The condition on relative primality of the degrees is necessary as was shown in [17] and [18] in the case of biquadratic fields. Also the condition on Galois-ness of both $K_1$ and $K_2$ is necessary. For instance, as we saw in Theorem (3.3), if either $K_1$ or $K_2$ is not Galois, this statement doesn’t hold, in general. Indeed, with the notations in this section, for every ramified prime $p$ in $L/\mathbb{Q}$ with $c(p) = 2$, by Proposition [14], $\Pi_p(K) = \beta_1\beta_2\cdots\beta_{r+1}$, and $j_{L/K}(\Pi_p(K)) = \gamma_1\Pi_p(L)$. Since $Gal(L/\mathbb{Q})$ acts transitively on the set $\{\gamma_1, \cdots, \gamma_r\}$, $\gamma_1$ is not ambiguous. Hence $j_{L/K}(Po(K)) \not\subseteq Po(L)$.

Unsing the results in Section (2) and Theorem (3.3), we find some interesting consequences:

Corollary 3.6. If $E$ is Pólya, then $Po(L)$ is embedded in $Po(K)$.

Proof. Immediately follows from Theorem (3.3).

Corollary 3.7. If $h(K)$ is not divisible by $r$, then $Po(L) \simeq Po(E)$. In particular, if $K$ is Pólya then $Po(L) \simeq Po(E)$.

Proof. If $h(K)$ is not divisible by $r$, then by the exact sequence in Theorem (3.3), the $r$-torsion subgroup of $Po(L)$ is trivial which implies that $Po(L)$ is a 2-torsion group isomorphic to $Po(E)$.

Corollary 3.8. If $L$ is Pólya, then $E$ is also Pólya and for every totally ramified prime $p$ in $K/\mathbb{Q}$, $\Pi_p(K)$ is principal.

Proof. Immediately follows from Theorem (3.3).

Corollary 3.9. If $E$ and $K$ are Pólya, then so is $L$.

Proof. Immediately follows from Theorem (3.3).

Now we can use Corollary (2.20) for $D_r$-extension $L$:

Corollary 3.10. If all finite places of $E$ are unramified in $L$, then $Po(L) \simeq Po(E)$ and $H^1(Gal(L/\mathbb{Q}), U_L) \simeq H^1(Gal(E/\mathbb{Q}), U_E)$.

With the notations of this section, if $L/E$ is unramified, by class field theory $h(E)$ is divisible by $r$. Now, by an argument completely similar to Honda’s reasoning [10] Proof of Proposition 10], we give necessary and sufficient conditions for divisibility of class number of a quadratic field by $r$:

Lemma 3.11. Suppose that $N$ is a quadratic field and $r|h(N)$. Then there exists a $D_r$-extension $M$ of $\mathbb{Q}$ such that $N$ is the quadratic subfield of $M$, and $M$ is unramified over $N$. Conversely, let $M$ be a $D_r$-extension of $\mathbb{Q}$ which is the splitting field of the irreducible polynomial

\[
(3.8) \quad f(X) = X^r + a_2X^{r-2} + a_3X^{r-3} + \cdots + a_{r-1}X + a_r, \quad a_i \in \mathbb{Z}
\]

over $\mathbb{Q}$. If $gcd(a_2, a_3, \cdots, a_{r-1}, ra_r) = 1$, then class number of the unique quadratic subfield of $M$ is divisible by $r$. 


Proof. Assume that $h(N)$ is divisible by $r$. Hence there exists an unramified abelian extension $M$ of degree $r$ over $N$. One can show that $M$ is a Galois extension of $Q$, thanks to Honda’s lemma [10, Lemma 3]. If $Gal(M/Q) \simeq C_{2r}$, denote the unique subfield of $M$ of degree $r$ over $Q$ by $F$. Hence $F$ is a cyclic extension of $Q$, and so every ramified prime $p$ in the extension $F/Q$, is totally ramified. Therefore, $p$ has the remification index $r$ or $2r$ in the extension $M/Q$. In both cases, there exists a prime ideal of $N$, above $p$ which ramifies in the extension $M/N$ and we reach a contradiction. Thus $M$ is not abelian over $Q$, i.e. $Gal(M/Q) \simeq D_r$.

Conversely, let $M$ be a $D_r$-extension of $Q$. Let $N$ be the unique quadratic subfield of $M$ and denote a subfield of $M$ of degree $r$ over $Q$ by $F$. Let $p$ be a prime ideal of $N$ ramified in $M$. Hence for $p = p \cap Q$, its ramification index is divisible by $r$. By Proposition (3.1), $p$ totally ramifies in $F/Q$ which implies that there exists $f(X) \in Z[X]$ with

$$f(X) \equiv (X - h)^r \pmod{p},$$

where $h \in Z$ and $M$ is the splitting field of $f(X)$. From this congruence equation, we have either

$$p = r, \quad r \mid gcd(a_2, a_3, \cdots, a_{r-1}),$$

or

$$p \mid gcd(a_2, a_3, \cdots, a_{r-1}, a_r).$$

Thus $p$ divides $gcd(a_2, a_3, \cdots, a_{r-1}, a_r)$. On the other hand, if there exists no totally ramified prime in the extension $F/Q$, by Proposition (3.1) every ramified prime in $M/Q$ has ramification index 2, which implies that $M/N$ is unramified. \qed

Remark 3.12. For $N = Q(\sqrt{-23})$, as mentioned in Example (2.13), $\Gamma(N) = N$. One can also see this, using the above lemma:

Since $h(N) = 3$, by the above lemma, there exists a $S_3$-extension $M$ of $Q$ such that $N$ is the unique quadratic subfield of $M$. Indeed $M = H(N)$, and since $Gal(M/Q) \simeq S_3$, but any compositum of $N$ and a cyclic cubic extension of $Q$ is abelian. So $M$ cannot be $\Gamma(N)$, hence $\Gamma(N) = N$.

Using Corollary (3.10) and Lemma (3.11), we obtain:

Corollary 3.13. With the notations of this section, let $L$ be the splitting field of an irreducible polynomial

$$f(X) = X^r + a_2 X^{r-2} + a_3 X^{r-3} + \cdots + a_{r-1} X + a_r, \quad a_i \in Z$$

over $Q$. If $gcd(a_2, a_3, \cdots, a_{r-1}, r, a_r) = 1$, then $Po(E) \simeq Po(L)$.

We conclude this section with a result on divisibility of class numbers. Following Masley [20], we define:

Definition 3.14. (See [20]) We call an extension $M/N$ of number fields totally ramified if no subextension of $M/N$ except $N$ itself is unramified over $N$.

Proposition 3.15. [20] Corollary 2.3 Suppose an extension $M/N$ of number fields is totally ramified. Then $h(N)$ divides $h(M)$.

In a special case, if $[M : N]$ is a prime number and $M/N$ is not unramified, then $M/N$ is a totally ramified extension. Now, we have:

Corollary 3.16. With the notations of this section, $h(K)$ divides $h(L)$.
Proof. Let \( p \) be a ramified prime in the extension \( E/\mathbb{Q} \). Hence \( 2 \mid e(p) \). If \( e(p) = 2 \), by Proposition \((3.1)\), \( p \) has the decomposition form in \( K/\mathbb{Q} \) as follows:

\[
\sigma \mathcal{O}_K = \beta_1 \beta_2 \cdots \beta_r,
\]

which implies that \( \beta_1 \) ramifies in \( L/K \). Similarly, if \( e(p) = 2r \), then by Proposition \((3.1)\), \( p = r \) and in this case the only prime ideal \( \beta \) of \( K \) above \( r \) is ramified in \( L/K \). Hence in both cases \( L/K \) is a totally ramified extension, and by Proposition \((3.15)\) the statement is proved. \( \square \)

Now we can say in a special case, the converse of Corollary \((3.9)\) holds:

**Corollary 3.17.** With the notations of this section, if \( h(L) = 1 \), then both subfields \( E \) and \( K \) are \( \text{Pólya} \).

**Proof.** If \( h(L) = 1 \), by Corollary \((3.10)\) one has \( h(K) = 1 \), which implies that \( K \) is a \( \text{Pólya} \) field. \( \text{Pólya} \)-ness of \( E \) is obtained by Corollary \((3.8)\). \( \square \)

### 4. Generic Polynomials and Some Examples

In this Section, for some small values of \( r \), we give some examples of \( D_r \)-extensions of \( \mathbb{Q} \) and investigate their \( \text{Pólya} \)-ness.

#### 4.1. \( S_3 \)-extensions of \( \mathbb{Q} \)

In \([19]\) we generalized Leriche’s results in \([17]\) for \( \text{Pólya} \)-ness of Galois closures of pure cubic fields to general \( S_3 \)-extensions of \( \mathbb{Q} \) and gave some examples of \( \text{Pólya} \) and non-\( \text{Pólya} \) \( S_3 \)-extensions of \( \mathbb{Q} \). Here we give some other examples.

We recall that for a monic irreducible cubic polynomial \( f(X) \in \mathbb{Z}[X] \), \( \text{disc}(f(X)) \) is not a perfect square if and only if \( \text{Gal}(f/\mathbb{Q}) \simeq S_3 \) with \( E = \mathbb{Q}(\sqrt{\text{disc}(f(X))}) \) the unique quadratic subfield of the splitting field of \( f(X) \) over \( \mathbb{Q} \), see \([14\text{, Theorem 2.1.1}]\). (For arbitrary \( D_r \)-extensions of \( \mathbb{Q} \) see Remark \((4.7)\) below.)

**Example 4.1.** Let \( K = \mathbb{Q}(\alpha) \), where \( \alpha \) is a root of \( f(X) = X^3 - 2X + 2 \). The discriminant of \( f(X) \) is \( \text{disc}(f(X)) = -2^2 \cdot 5 \cdot 7 \). Thus the Galois closure \( L \) of \( K \) over \( \mathbb{Q} \) is the compositum of \( K \) and the imaginary quadratic field \( E = \mathbb{Q}(\sqrt{-35}) \). We have \( h(K) = 1 \), \( h(E) = 2 \) and by Proposition \((1.5)\) \( E \) is not \( \text{Pólya} \). Using Corollary \((3.7)\) we find \( \text{Po}(L) \simeq \text{Po}(E) \simeq C_2 \).

**Example 4.2.** Let \( K = \mathbb{Q}(\alpha) \), where \( \alpha \) is a root of \( f(X) = X^3 + 2X - 11 \). The discriminant of \( K \) is \( D_K = \text{disc}(f(X)) = -3299 \), hence the Galois closure of \( K \) over \( \mathbb{Q} \) is the sextic field \( L = K(\sqrt{-3299}) \). By Proposition \((1.5)\), the quadratic subfield \( E = \mathbb{Q}(\sqrt{-3299}) \) of \( L \) is \( \text{Pólya} \). Since \( \text{gcd}(2,33) = 1 \) by Corollary \((3.13)\), \( L \) is a \( \text{Pólya} \) field. But since \( h(K) = 3 \), by \([26\text{, Theorem 6.9}]\) \( K \) is not \( \text{Pólya} \), while \( \Pi_{3299}(K) \) is principal, and by Ostrowski’s Theorem \([22]\) this can only happen for non-Galois number fields. See Remark \((6.5)\).

**Example 4.3.** Let \( K = \mathbb{Q}(\alpha) \), where \( \alpha \) is a root of \( f(X) = X^3 - 19X + 6 \). We have \( D_K = 2^3 \cdot 827 \), hence the Galois closure of \( K \) over \( \mathbb{Q} \) is the real sextic field \( L = K(\sqrt{2.827}) \). By Proposition \((1.5)\), the quadratic field \( E = \mathbb{Q}(\sqrt{2.827}) \) is \( \text{Pólya} \). Also \( h(K) = 1 \), and so by Corollary \((3.9)\), \( L \) is a \( \text{Pólya} \) field.

For some examples of \( D_r \)-extensions of \( \mathbb{Q} \), following \([14]\), we restate some results characterizing dihedral polynomials. First, we recall the concept of “parametric” or “generic” polynomial:
**Definition 4.4.** [14] Definition 0.1.1 Let $K$ be a field, $G$ be a finite group, $P(t, X)$ be a monic polynomial in $K(t)[X]$, where $t = (t_1, \ldots, t_n)$ and $X$ are indeterminates, and $M$ be the splitting field of $P(t, X)$ over $K(t)$. Suppose that $P(t, X)$ satisfies the following conditions:

(i) $M/K(t)$ is Galois with Galois group $\text{Gal}(M/K(t)) \simeq G$, and

(ii) every Galois extension $M/K$ with $\text{Gal}(M/K) \simeq G$ is the splitting field of a polynomial $P(a, X)$ for some $a = (a_1, \ldots, a_n) \in K^n$.

Then we say that $P(t, X)$ parametrizes $G$-extensions of $K$, and call $P(t, X)$ a parametric polynomial. The parametric polynomial $P(t, X)$ is said to be generic, if it satisfies the following additional condition:

(iii) $P(t, X)$ is parametric for $G$-extensions over any field containing $K$.

One can show that for any odd integer $n \geq 3$, generic polynomials for $D_n$-extensions over $\mathbb{Q}$ exist, see [14] Section 5.5.

Now let $f(X) \in \mathbb{Z}[X]$ be a monic irreducible polynomial (over $\mathbb{Q}$) of degree $r$, and let $\alpha_1, \alpha_2, \ldots, \alpha_r$ be $r$ roots of $f(X)$. Then the $r_2 = \binom{r}{2}$ elements $\alpha_i + \alpha_j$, $1 \leq i < j \leq r$ are all distinct, see [14] Chapter 7. Let $P_{r_2}(X)$ be the linear resolvent polynomial of $f(X)$:

\[(4.1) \quad P_{r_2}(X) = \prod_{1 \leq i < j \leq r} (X - (\alpha_i + \alpha_j)) \in \mathbb{Z}[X].\]

**Proposition 4.5.** [14] Theorem 7.1.3] With the notations of this Section, assume that $\text{Gal}(f/\mathbb{Q}) \not\simeq C_r$. Then $\text{Gal}(f/\mathbb{Q}) \simeq \mathbb{D}_r$, if and only if the resolvent polynomial $P_{r_2}(X)$ decomposes into the product of at least $\frac{r-1}{2}$ distinct irreducible polynomials of degree $r$ over $\mathbb{Q}$.

**Remark 4.6.** There is a generalization of Proposition 1.5 to dihedral extensions of degree $2n$, for any odd integer $n \geq 3$, see [14] Theorem 7.1.4.

**Remark 4.7.** With the notations of this Section, it is well known that the discriminant $\text{disc}(f(X))$ of $f(X)$ is a perfect square if and only if $\text{Gal}(f/\mathbb{Q})$ is contained in $A_r$, where $A_r$ is the alternating group on $r$ symbols, see [14] Chapter 2, page 29. On the other hand, one can show that $D_r \subseteq A_r$ if and only if $r \equiv 1(\text{mod } 4)$, see [14] Chapter 7, page 170.

Thus for $r \equiv 3(\text{mod } 4)$, if $\text{Gal}(f/\mathbb{Q}) \simeq D_r$, then the unique quadratic subfield of the splitting of $f(X)$ over $\mathbb{Q}$ is given by $E = \mathbb{Q}(\sqrt{\text{disc}(f(X))})$.

### 4.2. $D_5$-extensions of $\mathbb{Q}$

Brumer’s theorem gives a generic polynomial for $D_5$-extensions over $\mathbb{Q}$:

**Proposition 4.8.** [14] Theorem 2.3.5 and Remark after it] Let $M$ be an arbitrary field. The polynomial

\[(4.2) \quad f(s, t, X) = X^5 + (t - 3)X^4 + (s - t + 3)X^3 + (t^2 - t - 2s - 1)X^2 + sX + t \]

in $M(s, t)[X]$ is then generic for $D_5$-extensions over $M$.

Also the quadratic subextension (in characteristic $\neq 2$) of the splitting field of the polynomial $f(s, t, X)$ is obtained by adjoining to $M(s, t)$ a square root of $-(4t^5 - 4t^4 - 24st^3 - 40s^3 - s^2t^2 + 34st^2 + 91t^2 + 30s^2t + 14st - 4t - s^2 + 4s^3)$.

Now we can use the generic polynomial in Proposition 4.8, and find some examples of Pólya (resp. non-Pólya) $D_5$-extensions of $\mathbb{Q}$. 
Example 4.9. With the notations of Proposition (1.8), let \( s = -4, t = -1 \) and \( K = \mathbb{Q}(\theta) \), where \( \theta \) is a root of the polynomial

\[
    f(X) = X^5 - 4X^4 + 9X^2 - 4X - 1.
\]

We have \( D_K = 19^2\cdot43^2 \), and by Proposition (1.8), the Galois closure \( L \) of \( K \) is a \( D_5 \)-extension of \( \mathbb{Q} \), with the unique quadratic subfield \( E = \mathbb{Q}(\sqrt{19\cdot43}) \). By Proposition (1.5), \( E \) is Pólya. Since \( h(K) = 1 \), by Corollary (3.10), \( L \) is a (real) Pólya \( D_5 \)-extension of \( \mathbb{Q} \).

Example 4.10. Using Proposition (1.8), we find for \( s = -5 \) and \( t = 3 \) the splitting field \( L \) of the polynomial

\[
    f(X) = X^5 - 5X^3 + 15X^2 - 5X + 3.
\]

over \( \mathbb{Q} \) is a \( D_5 \)-extension with the unique quadratic subfield \( E = \mathbb{Q}(\sqrt{-15}) \). We have \( D_K = 3^2\cdot5^6 \), \( h(K) = 1 \), \( h(E) = 2 \), where \( K = \mathbb{Q}(\theta) \) for some root \( \theta \) of \( f(X) \). By Proposition (1.5), \( E \) is not Pólya, which implies that \( Po(E) \simeq C_2 \). By Corollary (3.9), \( Po(L) \simeq C_2 \), see Remark (3.5).

Example 4.11. With the notations of Proposition (1.8), let \( s = 5 \) and \( t = 1 \) and \( K = \mathbb{Q}(\theta) \) where \( \theta \) is a root of the polynomial

\[
    f(X) = X^5 - 2X^4 + 7X^3 - 11X^2 + 5X + 1.
\]

We have \( D_K = 1367^2 \) and \( K \) is a \( D_5 \)-field. Denote the Galois closure of \( K \) over \( \mathbb{Q} \) by \( L \). By Proposition (1.8), \( E = \mathbb{Q}(\sqrt{-1367}) \) is the unique quadratic subfield of \( L \) and by Proposition (1.5), \( E \) is Pólya. Since \( h(K) = 4 \), By Corollary (3.9), \( L \) is a Pólya \( D_5 \)-extension of \( \mathbb{Q} \). While by [26, Theorem 6.9] \( K \) is not Pólya, see Remark (3.5).

We recall that for a \( D_t \)-extension \( L \) of \( \mathbb{Q} \) with quadratic subfield \( E \), if \( L/E \) is unramified then Pólya groups of \( E \) and \( L \) are isomorphic, see Corollary (5.10). As we see in the last example for \( t = 1 \), \( L/E \) is unramified. More generally (for \( t = 1 \)):

Proposition 4.12. [15, Section 2] Let \( s \in \mathbb{Z} \) and \( f_s(X) \) is given by

\[
    f_s(X) = X^5 - 2X^4 + (s + 2)X^3 - (2s + 1)X^2 + sX + 1.
\]

Then, \( f_s(X) \) is irreducible over \( \mathbb{Q} \), \( disc(f_s(X)) = (4s^3 + 28s^2 + 24s + 47)^2 \) and if \(-4s^3 + 28s^2 + 24s + 47 \) is not a square, then \( Gal(f(X)) \simeq D_5 \). Moreover, for \( Gal(f(X)) \simeq D_5 \) the splitting field of \( f(X) \) (over \( \mathbb{Q} \)) is unramified over its unique quadratic subfield, namely over \( \mathbb{Q}(\sqrt{-4s^3 - 28s^2 - 24s - 47}) \).

Now with the notations of Proposition (4.12), we can characterize all Pólya splitting fields of \( f_s(X) \):

Corollary 4.13. With the assumptions in Proposition (4.12), let \( L \) be the splitting field of a polynomial \( f_s(X) \) over \( \mathbb{Q} \), for some integer \( s \) with \( Gal(L/\mathbb{Q}) \simeq D_5 \). Then \( Po(L) \simeq Po(\mathbb{Q}(\sqrt{d})) \), where \( d = -4s^3 - 28s^2 - 24s - 47 \).

Proof. Denote the quadratic subfield of \( L \) by \( E \). By Proposition (4.12), \( L/E \) is unramified, and using Corollary (5.10), the statement is proved. \( \square \)

Example 4.14. Let \( f_s(X) \) be given by equation (1.3). Using Corollary (4.13) one can easily check that the splitting field of \( f_s(X) \) for

\[
    s \in \{ \pm 6, \pm 5, \pm 2, \pm 1, 0, 8, 12, 13, 19 \}
\]

is a Pólya \( D_5 \)-extension of \( \mathbb{Q} \), while for \( s \in \{ \pm 17, \pm 16, \pm 4, -3, 7, 9, 10 \} \) is not.
4.3. $D_7$-extensions of $\mathbb{Q}$. Let $K$ be a field of characteristic 0. Following [14], we restate a criterion for characterizing irreducible septimic polynomials $f(X) \in K[X]$ with $Gal(f/\mathbb{Q})) \simeq D_7$:

**Proposition 4.15.** [14] Lemma 2.5.1 and Theorem 2.5.3] Let $K$ be a field of characteristic 0, $f(X) \in K[X]$ be an irreducible polynomial of degree 7, and $\alpha_1, \alpha_2, \ldots, \alpha_7$ be roots of $f(X)$ in its splitting field over $K$. Then the resolvent polynomial

$$P_{35}(X) := \prod_{1 \leq i < j < k \leq 7} (X - (\alpha_i + \alpha_j + \alpha_k))$$

has distinct roots, and $Gal(f/\mathbb{Q})) \simeq D_7$ if and only if $P_{35}(X)$ factors into a product of four distinct irreducible polynomials of degrees 14, 7, 7 and 7 over $K$.

**Example 4.16.** Let $K = \mathbb{Q}(\alpha)$ where $\alpha$ is a root of

$$f(X) = X^7 - 7X^6 - 7X^5 - 7X^4 - 1.$$ 

Then $f(X)$ is irreducible over $\mathbb{Q}$ and $Gal(f/\mathbb{Q}) \simeq D_7$, see [14] Section 5.2, Example 5, page 54. Denote the Galois closure of $K$ over $\mathbb{Q}$ by $L$. We have $disc(f(X)) = -3^97^3$, hence $E = \mathbb{Q}(\sqrt{-7})$ is the quadratic subfield of $L$, which is Pólya by Proposition (4.1). Also $h(K) = 1$, and by Corollary (3.9) $L$ is Pólya. Note that $h(L) = 7$, see Remark (1.4).

**Example 4.17.** Let

$$f(X) = X^7 - X^6 - X^5 + X^4 - X^3 - X^2 + 2X + 1.$$ 

Then $f(X)$ is irreducible over $\mathbb{Q}$ and $Gal(f/\mathbb{Q}) \simeq D_7$, see [14] Chapter 7, Example 2, page 172]. Denote the splitting field of $f(X)$ over $\mathbb{Q}$ by $L$. We have $disc(f(X)) = -71^3$, hence $E = \mathbb{Q}(\sqrt{-71})$ is the unique quadratic subfield of $L$, which is Pólya by Proposition (1.5). By Proposition (5.1), we have $e(71) = 2$ and by Theorem (6.3), $L$ is also Pólya.

4.4. **Some Examples of $D_7$-extensions of higher degrees.** In [14], by considering Hilbert class field theory of an imaginary quadratic number field $N$ and using singular values of certain modular functions, a method for finding dihedral extensions of $\mathbb{Q}$ and some algorithms for constructing the Hilbert class field of $N$ are given, see [14] Section 7.3. Following [14], we restate two examples of $D_{13}$ and $D_{19}$-extension of $\mathbb{Q}$:

**Example 4.18.** Let $L$ be the splitting field of the polynomial

$$X^{13} - 6X^{12} + 10X^{11} - 16X^{10} + 22X^9 - 19X^8 + 11X^7 - 5X^6 - X^5 + 5X^4 - 4X^3 + 2X - 1$$

over $\mathbb{Q}$. Then $Gal(L/\mathbb{Q}) \simeq D_{13}$, $E = \mathbb{Q}(\sqrt{-191})$ is the unique quadratic subfield of $L$, and $L$ is the Hilbert class field of $E$, see [14] Section 7.3, Example 3, page 184]. By Proposition (1.5), $E$ is Pólya and by Corollary (3.10), so is $L$.

**Example 4.19.** Let $L$ be the splitting field of the polynomial

$$X^{19} - 14X^{18} + 59X^{17} - 113X^{16} + 91X^{15} + 19X^{14} - 90X^{13} + 51X^{12} + 2X^{11} - 5X^{10} + 9X^9 - 30X^8 + 22X^7 + 7X^6 - 14X^5 + 3X^4 + 2X^3 - 2X^2 + 2X - 1$$

over $\mathbb{Q}$. Then $Gal(L/\mathbb{Q}) \simeq D_{19}$, $E = \mathbb{Q}(\sqrt{-359})$ is the unique quadratic subfield of $L$, and $L$ is the Hilbert class field of $E$, see [14] Section 7.3, Example 3, page 184]. By an argument similar to Example (4.18), $L$ is Pólya.
Remark 4.20. Since \( L \) is the Hilbert class field of \( E \) in both Examples (4.18) and Example (4.19), by Leriche’s result too, \( L \) is Pólya.

5. Upper bound for the number of ramification

For a number field \( M \), denote the number of ramified primes in \( M/\mathbb{Q} \) by \( s_M \). Leriche in [17], for any Galois Pólya number field \( M \) gave an upper bound for \( s_M \) which only depends on the degree of \( M \) over \( \mathbb{Q} \), see [17] Proposition 2.5. In particular, for a Pólya Galois number field \( M \) of degree \( 2r \), this upper bound is given by \( s_M \leq r + 4 \).

In [26], Zantema proved that a cyclic number field \( M \) of degree \( r > 3 \) is Pólya if and only if \( M/\mathbb{Q} \) is ramified at only one prime, and in a Pólya quadratic field at most two primes are ramified, see [26] Proposition 3.2. He also proved that for two Galois number fields \( K_1 \) and \( K_2 \) of coprime degrees over \( \mathbb{Q} \), their compositum is Pólya if and only if \( K_1 \) and \( K_2 \) are Pólya, see [26] Theorem 3.4. Hence for a cyclic number field \( M \) of degree \( 2r \), using Zantema’s results the upper bound can be made sharp by \( s_M \leq 3 \).

In [19], we proved that for a non-Galois cubic field \( K \) with Galois closure \( L \), if \( L \) is Pólya depending on whether \( D_K > 0 \), \( D_K < 0 \) and \( K \) pure, or \( D_K < 0 \) and \( K \) non-pure, then \( s_L \leq 4 \), \( s_L \leq 3 \) or \( s_L \leq 2 \), respectively. Also by giving some examples, we showed that these upper bounds are actually sharp, see [19] Section 3.

In this section, by using the same methods in [19], for a Pólya \( D_r \)-extension \( L \) of \( \mathbb{Q} \) we give an upper bound for \( s_L \) which is much smaller than \( r + 4 \).

Theorem 5.1. Let \( K \) be a non-Galois number field of degree \( r > 3 \). Let \( L \) be the Galois closure of \( K \) over \( \mathbb{Q} \) with \( \text{Gal}(L/\mathbb{Q}) \simeq D_r \). Denote the unique quadratic subfield of \( L \) by \( E \). If \( L \) is Pólya, then:

(i) For \( L \) real, depending on whether the fundamental unit of \( E \) belongs to \( \mathcal{N}_{L/E}(U_L) \) or not, \( s_L \leq 3 \) or \( s_L \leq 4 \), respectively.

(ii) For \( L \) imaginary, \( s_L \leq 2 \).

Proof. Let \( G = \text{Gal}(L/\mathbb{Q}) \simeq D_r \). As before, for a ramified prime \( p \) in \( L/\mathbb{Q} \), denote its ramification index by \( e(p) \). Since \( L \) is a Pólya field, by exact sequence [1.1], we have

\[
\#H^1(G, U_L) = \prod_{p|D_L} e(p),
\]

which implies that \( \#H^1(G, U_L) \) is a divisor of a power of \( 2r \). Now consider the cyclic extensions \( L/K \) and \( L/E \). Let \( G_2 = \text{Gal}(L/K) \) and \( G_r = \text{Gal}(L/E) \) and use the Herbrand quotients:

\[
Q(G_2, U_L) = \frac{\#\hat{H}^0(G_2, U_L)}{\#H^1(G_2, U_L)}, \quad Q(G_r, U_L) = \frac{\#\hat{H}^0(G_r, U_L)}{\#H^1(G_r, U_L)}
\]

where

\[
\hat{H}^0(G_2, U_L) = U_L^{G_2} / \mathcal{N}_{L/K}(U_L) = U_K / \mathcal{N}_{L/K}(U_L),
\]

\[
\hat{H}^0(G_r, U_L) = U_L^{G_r} / \mathcal{N}_{L/E}(U_L) = U_E / \mathcal{N}_{L/E}(U_L).
\]
On the other hand, the Herbrand quotients \( Q(G_2, U_L) \) and \( Q(G_r, U_L) \) are given by [3 Proposition 5.10]:

\[
Q(G_2, U_L) = \frac{2^s}{[L : K]} = 2^{s-1},
\]

\[
Q(G_r, U_L) = \frac{2^t}{[L : E]} = \frac{2^t}{r},
\]

where \( s \) (resp. \( t \)) is the number of infinite places of \( K \) (resp. \( E \)) ramified in \( L \). For \( L \) real (resp. imaginary), the signature of \( K \) is \( (r,0) \) (resp. \( (1,\frac{r-1}{2}) \)), see [6 Theorem 9.2.6]. Hence

\[
(5.3) \quad Q(G_2, U_L) = \begin{cases} \frac{1}{2} : L \text{ is real,} \\ 1 : L \text{ is imaginary,} \end{cases}
\]

\[
(5.4) \quad Q(G_r, U_L) = \frac{1}{r}. 
\]

For the cyclic extension \( L/K \), since \( \mathcal{N}_{L/K}(U_L) \) contains \( U_K^2 \) and \( (U_K : U_K^2) \) divides \( 2^{w_K+1} \), \( (U_K : \mathcal{N}_{L/K}(U_L)) \) divides \( 2^{w_K+1} \).

Similarly, for the cyclic extension \( L/E \), \( (U_E : \mathcal{N}_{L/E}(U_L)) \) divides \( r^{w_E+1} \). But for \( E = \mathbb{Q}(\sqrt{d}) \) imaginary, for \( d \not\in \{-1,-3\} \), \( d = -1 \) or \( d = -3 \) we have \( U_E = \{\pm 1\} \), \( U_E = \{\pm 1, \pm i\} \) or \( U_E = \{\pm 1, \pm \zeta_3, \pm \zeta_3^2\} \), respectively. Thus for \( E \) imaginary, since \( (U_E : \mathcal{N}_{L/E}(U_L)) \) divides \( \#U_E \) and \( \gcd(\#U_E, r) = 1 \), \( (U_E : \mathcal{N}_{L/E}(U_L)) = 1 \).

Now let \( E \) be real, and \( \xi \) be the fundamental unit of \( E \). By Dirichlet Unit Theorem we have \( U_E \cong C_2 \oplus \mathbb{Z} \). Hence depending on whether \( \xi \in \mathcal{N}_{L/E}(U_L) \) or not, \( (U_E : \mathcal{N}_{L/E}(U_L)) = 1 \) or \( (U_E : \mathcal{N}_{L/E}(U_L)) = r \), respectively.

Summing up the above arguments, and using relations (5.2), (5.3) and (5.4), we find:

- for \( L \) real, \( \#H^1(G_2, U_L) | 2^{r+1} \) and depending on whether the fundamental unit of \( E \) belongs to \( \mathcal{N}_{L/E}(U_L) \) or not, \( \#H^1(G_r, U_L) = r \) or \( \#H^1(G_r, U_L) = r^2 \), respectively.
- for \( L \) imaginary, \( \#H^1(G_2, U_L) | 2^{\frac{r+1}{2}} \) and \( \#H^1(G_r, U_L) = r \).

On the other hand, the restriction maps

\[
\text{res} : H^1(G, U_L) \to H^1(G_2, U_L),
\]

and

\[
\text{res} : H^1(G, U_L) \to H^1(G_r, U_L),
\]

are injective on the 2-primary and \( r \)-primary part of \( H^1(G, U_L) \), respectively, see [22 Proposition 1.6.9]. Thus:

\[
(5.5) \quad \#H^1(G, U_L) | \#H^1(G_2, U_L) \cdot \#H^1(G_r, U_L).
\]

Therefore,

- for \( L \) real, depending on whether the fundamental unit of \( E \) belongs to \( \mathcal{N}_{L/E}(U_L) \) or not,

\[
(5.6) \quad \#H^1(G, U_L) | 2^{r+1} \cdot 1 \quad \text{or} \quad \#H^1(G, U_L) | 2^{r+1} \cdot r^2,
\]

respectively.
- for \( L \) imaginary,

\[
(5.7) \quad \#H^1(G, U_L) | 2^{\frac{r+1}{2}} \cdot r^1.
\]
Now since $L$ is Pólya by Corollary (5.8), $E$ is also Pólya. On the other hand, by Proposition (1.5), for real (resp. imaginary) Pólya field $E$, $s_E \leq 2$ (resp. $s_E = 1$). Hence by Theorem (5.3), the 2-torsion subgroup of $Po(L)$ has at most 2 (resp. 1) cyclic factor. Using the relations (5.10) and (5.7) we find:

- for real Pólya $D_r$-extension $L$ of $Q$, depending on whether the fundamental unit of $E$ belongs to $N_{L/E}(U_L)$ or not,
  \begin{align*}
  \#H^1(G, U_L) & \mid 2^2.3^1 \quad \text{or} \quad \#H^1(G, U_L) \mid 2^1.3^2,
  \end{align*}
  \hspace{1cm} \text{respectively.}

- for imaginary Pólya $D_r$-extension $L$ of $Q$,
  \begin{align*}
  \#H^1(G, U_L) & \mid 2^1.3^1.
  \end{align*}

Finally using relations (5.8), (5.9) and (5.10), the statement in theorem is proved. \hfill \Box

In [12], Ishida proved that for a non-pure number field $M$ of degree $r$, if number of the totally ramified primes in $M/Q$ is more than the rank of the unit group $w_M$, then $r \mid h(M)$, see [12, Theorem 2]. The method used to prove Theorem (5.1), can yield Ishida-type results:

**Corollary 5.2.** Let $K$ be a non-Galois cubic field, $L$ be its the Galois closure over $Q$ and denote the unique quadratic subfield of $L$ by $E$. Denote the number of totally ramified primes in $K/Q$ by $t_K$. Then:

(i) for $D_K > 0$, if $E$ is Pólya and $t_K \geq 3$, then $3 \mid h(K)$;
(ii) for $D_K < 0$ and $K$ non-pure, if $E$ is Pólya and $t_K \geq 2$, then $3 \mid h(K)$;
(iii) for $D_K < 0$ and $K$ pure, if $t_K \geq 3$, then $3 \mid h(K)$.

**Proof.** In [19], we proved that if $L$ is Pólya, depending on whether $D_K > 0$, $D_K < 0$ with $K$ pure, or $D_K < 0$ with $K$ non-pure, then
\begin{align*}
\#H^1(G, U_L) & \mid 2^2.3^2, \quad \#H^1(G, U_L) \mid 2^1.3^2, \quad \text{or} \quad \#H^1(G, U_L) \mid 2^1.3^1,
\end{align*}
respectively, see [19, proof of Theorem 3.1].

(i) Assume that $D_K > 0$, $E$ is Pólya and at least three distinct primes totally ramify in $K/Q$. Hence by Proposition (5.1), $3^3$ divides $\prod_{p \mid D_L} e(p)$ and by Zantema's exact sequence (5.2), $L$ cannot be Pólya. Since $E$ is Pólya, by Theorem (5.3), $Po(L)$ is a nontrivial 3-group embedded in $Po(K)$ which implies that $3 \mid h(K)$.

Parts (ii) and (iii) can be proved similarly. Note that for pure $K$, we have $E = Q(\sqrt{-3})$ is Pólya. \hfill \Box

For $D_r$-fields $K$ with $r > 3$, one can find a lower bound, independent of $[K: Q]$, for $t_K$ making $h(K)$ divisible by $r$.

**Corollary 5.3.** Let $K$ be a non-Galois number field of degree $r > 3$, and $L$ be its Galois closure over $Q$ with $\text{Gal}(L/Q) \simeq D_r$. Denote the unique quadratic subfield of $L$ by $E$ and suppose that $E$ is Pólya. Also denote the number of totally ramified primes in $K/Q$ by $t_K$. Then:

(i) for $L$ real, if $t_K \geq 3$, then $r \mid h(K)$.
(ii) for $L$ imaginary, if $t_K \geq 2$, then $r \mid h(K)$.

**Proof.** By an argument similar to proof of Corollary (5.2), and using relations (5.8) and (5.9), the statements are proved. \hfill \Box
Remark 5.4. Indeed, one has $D_K = (D_E)^{2r-1} f^{r-1}$, where $f$ is the conductor of $L$ over $E$. Moreover, a prime number $p$ is totally ramified in $K/Q$ if and only if $p | f$ and also for $p | \gcd(D_E, f)$, we have $p = r$, see [6, Proposition 10.1.28]. Hence, for instance, for a pure cubic field $K = \mathbb{Q}(\sqrt[3]{m})$ if the conductor of $L = \mathbb{Q}(\sqrt[3]{m}, \zeta_3)$ over $E = \mathbb{Q}(\sqrt{-3})$ has more than two distinct prime divisors, then $3 | h(K)$.

References

1. M. Bhargava, $P$-orderings and polynomial functions on arbitrary subsets of Dedekind rings. J. Reine Angew. Math. 490 (1997), 101-127.
2. A. Brumer, M. Rosen, Class number and ramification in number fields. Nagoya Math. J. 23 (1963), 97-101.
3. P. J. Cahen, J. L. Chabert Integer-valued polynomials. Mathematical Surveys and Monographs 48, Amer. Math. Soc., Providence, 1997.
4. J. L. Chabert, Factorial groups and Pólya groups in Galoisian extension of $\mathbb{Q}$. Commutative ring theory and applications (Fez 2001), 77-86, Lecture Notes in Pure and Appl. Math., 231, Dekker, New York, 2003.
5. N. Childress, Class field theory. Springer, New York, 2009.
6. H. Cohen, Advanced topics in computational number theory. Springer-Verlag, New York, 2000.
7. B. Heidaryan, A. Rajaei, Biquadratic Pólya fields with only one quadratic Pólya subfield. J. Number Theory 143 (2014), 279-285.
8. B. Heidaryan, A. Rajaei, Some non-Pólya biquadratic fields with low ramification. Rev. Mat. Iberoam. 33 (2017), 1037-1044.
9. D. Hilbert, The theory of algebraic number fields. (English summary) Translated from the German and with a preface by Iain T. Adamson. With an introduction by Franz Lemmermeyer and Norbert Schappacher. Springer-Verlag, Berlin, 1998.
10. T. Honda, Isogenies, rational points and section points of group varieties. Japan. J. Math. 30 (1960), 84-101.
11. T. Honda, Pure cubic fields whose class numbers are multiples of three. J. Number Theory 3 (1971), 7-12.
12. M. Ishida, A note on class numbers of algebraic number fields. J. Number Theory 1 (1969) 65-69.
13. M. Ishida, The genus fields of algebraic number fields. Lecture Notes in Mathematics, Vol. 555, Springer-Verlag, Berlin-New York, 1976.
14. C. U. Jensen, A. Ledet, N. Yui, Generic polynomials. Constructive aspects of the inverse Galois problem. Cambridge University Press, 2002.
15. M. J. Lavallee, B. K. Spearman, K. S. Williams, Q. Yang, Dihedral quintic fields with a power basis. Math. J. Okayama Univ. 47 (2005), 75-79.
16. A. Leriche, Pólya fields, Pólya groups and Pólya extensions: a question of capitulation. J. Théor. Nombres Bordeaux 23 (2011), 235-249.
17. A. Leriche, Cubic, quartic and sextic Pólya fields. J. Number Theory 133 (2013) 59-71.
18. A. Leriche, About the embedding of a number field in a Pólya field. J. Number Theory 45 (2014), 210-229.
19. A. Maarefparvar, A. Rajaei, Pólya $S_3$-extensions of $Q$. To appear in Proc. Roy. Soc. Edinburgh Sect. A.

20. J. M. Masley, Class numbers of real cyclic number fields with small conductor. Compositio Math. 37 (1978), 279-319.

21. W. Narkiewicz, Elementary and analytic theory of algebraic numbers., Springer-Verlag, Berlin, 2004.

22. J. Neukirch, A. Schmidt, K. Wingberg, Cohomology of number fields. Springer-Verlag, Berlin, 2008.

23. A. Ostrowski, Über ganzwertige Polynome in algebraischen Zahlkörpern. J. Reine Angew. Math. 149 (1919) 117-124.

24. G. Pólya, Über ganzwertige Polynome in algebraischen Zahlkörpern. J. Reine Angew. Math. 149 (1919), 97-116.

25. J. P. Serre, Local fields. Translated from the French by Marvin Jay Greenberg. Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979.

26. H. Zantema, Integer valued polynomials over a number field. Manuscripta Math. 40 (1982), 155-203.

Department of Mathematics, Tarbiat Modares University, 14115-134, Tehran, Iran
E-mail address: a.maarefparvar@modares.ac.ir

Department of Mathematics, Tarbiat Modares University, 14115-134, Tehran, Iran
E-mail address: alirajaei@modares.ac.ir