FROM PÓLYA FIELDS TO PÓLYA GROUPS
(II) NON-GALOISIAN NUMBER FIELDS

JEAN-LUC CHABERT

ABSTRACT. The Pólya group of a number field $K$ is the subgroup of the class group of $K$ generated by the classes of the products of the maximal ideals with same norm. A Pólya field is a number field whose Pólya group is trivial. Our purpose is to start with known assertions about Pólya fields to find results concerning Pólya groups. In this second paper we describe the Pólya group of some non-galoisian extensions of $\mathbb{Q}$.

1. Introduction

Notation. Let $K$ be a number field with ring of integers $\mathcal{O}_K$. For each positive integer $q$, let

$$\Pi_q(K) = \prod_{m \in \text{Max}(\mathcal{O}_K), |\mathcal{O}_K/m| = q} m.$$ 

If $q$ is not the norm of a maximal ideal of $\mathcal{O}_K$, then by convention $\Pi_q(K) = \mathcal{O}_K$.

The notion of Pólya fields goes back to Pólya [8] and Ostrowski [7] while its formal definition is given by Zantema [10]:

Definition 1.1. A Pólya field is a number field $K$ such that all the ideals $\Pi_q(K)$ are principal.

The notion of Pólya group of $K$ was introduced later in [2, §II.4] as a measure of the obstruction for $K$ to be a Pólya field.

Definition 1.2. The Pólya group of a number field $K$ is the subgroup $\mathcal{P}o(K)$ of the class group $\text{Cl}(K)$ generated by the classes of the ideals $\Pi_q(K)$.

Although the Pólya group of $K$ is also the subgroup of $\text{Cl}(K)$ generated by the classes of the factorials ideals of $K$ as defined by Bhargava [1] and that, following Pólya [8], a Pólya field is in fact a number field $K$ such that the $\mathcal{O}_K$-module $\{f \in K[X] : f(\mathcal{O}_K) \subseteq \mathcal{O}_K\}$ formed by the integer-valued polynomials on $K$ admits a basis formed by polynomials of each degree, we will not use these properties. Of course, the field $K$ is a Pólya field if and only if its Pólya group is trivial. So that, every result about Pólya group has a corollary which is a result about Pólya fields. Here we are going to make a reverse lecture of this fact: we make the conjecture that an assertion about Pólya fields is the evidence of a statement about Pólya groups.

Almost all the results about either Pólya fields or Pólya groups are obtained in the Galois case (see [3]) since this is the easier case thanks to the following remark due to Ostrowski [7]: if the extension $K/\mathbb{Q}$ is galoisian and if $p$ is not ramified in $K/\mathbb{Q}$, then the ideals $\Pi_{p^f}(K)$ are principal. Thus, in the Galois case, we just...
have to consider the finitely many ramified primes. On the other hand, in
the non-galoisian case, we have to consider a priori the ideals $P_{p,f}(K)$ for all primes $p$.

Among the few known results in the non-galoisian case, we have that the Hilbert
class field of every number field is a Pólya field [9 Corollary 3.2]. But the most
important result about Pólya fields that we want to translate into a result about
Pólya groups is the following one due to Zantema:

**Theorem 1.3.** [10 Thm 6.9] Let $K$ be a number field of degree $n \geq 3$ and let $G$ be
the Galois group of the normal closure of $K$ over $\mathbb{Q}$. If $G$ is either isomorphic to the
symmetric group $S_n$ where $n \neq 4$, or to the alternating group $A_n$ where $n \neq 3,5,$
or is a Frobenius group, then the following assertions are equivalent:

1. all the ideals $P_{p,f}(K)$ where $p$ is not ramified are principal,
2. $K$ is a Pólya field,
3. $h_K = 1$.

In other words, under the previous hypotheses, denoting by $P_o(K)_{nr}$ the sub-
group of $P_o(K)$ generated by the classes of the ideals $P_{p,f}(K)$ where $p$ is a not
ramified, one has the equivalences:

\[ P_o(K)_{nr} = \{1\} \Leftrightarrow P_o(K) = \{1\} \Leftrightarrow Cl(K) = \{1\}. \]

Note that $P_o(K)_{nr}$ is always trivial when $K/\mathbb{Q}$ is galoisian. Motivated by what we
did in the Galois case [3], we formulate the following unreasonable conjecture:

**Conjecture 4.** Each of the hypotheses of Theorem 1.3 implies the following equal-
ities:

\[ P_o(K)_{nr} = P_o(K) = Cl(K). \]

The aim of this paper is to give a proof of this conjecture (cf. Theorem 4.6). At
least at the beginning of this proof, the ideas that we will use follow closely that
given by Zantema for Theorem 1.3.

2. The Artin symbol $\left( \frac{H_K/K}{\Pi_{p,f}(K)} \right)$ for a non-ramified $p$

**Notations.** In the sequel, $K$ is a number field of degree $n \geq 3$. We denote by $O_K$ its
ring of integers, $\mathfrak{I}_K$ the group of its nonzero fractionary ideals, $P(K)$ the subgroup
of nonzero fractionary principal ideals, $Cl(K) = \mathfrak{I}_K/P_K$ its class group, $h_K$ its class
number, $P_q(K)$ the product of its prime ideals with norm $q$. Let $H_K$ be the Hilbert
class field of $K$, that is, the largest non-ramified abelian extension of $K$, and let
$N_H$ be the normal closure of $H_K$ over $\mathbb{Q}$. Finally, we denote the Galois groups in
the following way: $G = Gal(N_H/\mathbb{Q})$, $H = Gal(N_H/K)$, and $H_1 = Gal(N_H/H_K)$.

There exists an isomorphism of groups (see for instance [9 I §8])

\[ \gamma_K : Cl(K) \to Gal(H_K/K) = H/H_1. \]

To study the group $P_o(K)$, and more specifically the subgroup $P_o(K)_{nr}$, we will
use this isomorphism. Thus, let us describe $\gamma_K$. Recall that, if $L/K$ is a galoisian
extension and $\mathfrak{P}$ is a prime of $L$ non ramified in the extension $L/K$ and lying over
$p = \mathfrak{P} \cap K$, the Frobenius of $\mathfrak{P}$ in the extension $L/K$ is the element $\sigma$ of $Gal(L/K)$
characterized by:

\[ \forall a \in O_L \quad \sigma(a) \equiv a^q \pmod{\mathfrak{P}} \quad \text{where} \quad q = \text{Card}(O_K/p). \]

This Frobenius, that we denote by $(\mathfrak{P}, L/K)$, generates the decomposition group
of $\mathfrak{P}$ in the extension $L/K$, thus its order is $f_{\mathfrak{P}}(L/K) = [O_L/\mathfrak{P} : O_K/p]$. 
If the extension $L/K$ is abelian, the Frobenius of $\mathfrak{P}$ depends only on $\mathfrak{p} = \mathfrak{P} \cap K$, it is called the Artin symbol of $\mathfrak{p}$ and is denoted by $\left( \frac{L/K}{\mathfrak{p}} \right)$. By Chebotarev’s theorem, every element of $\text{Gal}(L/K)$ is the Artin symbol of a non-ramified prime $\mathfrak{p}$. More generally, the Artin symbol of an ideal $\mathfrak{a} = \prod_i \mathfrak{p}_i^{n_i}$ of $\mathcal{O}_K$ which is not contained in any ramified prime ideal of $\mathcal{O}_K$ is defined by linearity: $\left( \frac{L/K}{\mathfrak{a}} \right) = \prod_i \left( \frac{L/K}{\mathfrak{p}_i} \right)^{n_i}$.

In the particular case of the extension $H_K/K$, this surjective morphism of groups $a \in \mathcal{I}_K \mapsto \left( \frac{H_K/K}{a} \right) \in \text{Gal}(H_K/K)$ induces the isomorphism $\gamma_K$:

$$\gamma_K : \mathfrak{p} \in \text{Cl}(K) \mapsto \left( \frac{H_K/K}{\mathfrak{p}} \right) \in \text{Gal}(H_K/K).$$

Let $\Omega$ be the set formed by the right cosets of $H$ in $G$. The group $G$ acts transitively on $\Omega$. As a permutation of $\Omega$, an element $g \in G$ is a product of $t$ disjoint cycles of orders $f_i$ ($1 \leq i \leq t$) (fixed points correspond to cycles of order one). For each $i$, let $s_i \in G$ be such that $Hs_i \in \Omega$ belongs to the orbit of the $i$-th cycle. Thus, $\Omega = \{Hs_ig^k \mid 1 \leq i \leq t, 0 \leq k < f_i\}$

**Proposition 2.1.** [10] Prop. 6.2| Assume that $p$ is not ramified in the extension $K/Q$. Let $\mathfrak{P}$ be a prime ideal of $N_H$ lying over $p$ and consider its Frobenius $g = (\mathfrak{P}, N_H/Q)$. With the previous notation ($t, f_i$ and $s_i$ for $g$), one has:

$$\left( \frac{H_K/K}{\mathfrak{P}^p'/(K)} \right) = \prod_{\{i \mid f_i = f\}} s_i g^f s_i^{-1} |_{H_K}. \tag{1}$$

**Proof.** Note that the fact that $p$ is not ramified in $K/Q$ implies that $\mathfrak{P}$ is not ramified in $N_H/Q$. By definition,

$$\left( \frac{H_K/K}{\mathfrak{P}^p'/(K)} \right) = \prod_{p \in \text{Max}(\mathcal{O}_K) \setminus N(\mathfrak{p}) = p^f} \left( \frac{H_K/K}{\mathfrak{p}} \right).$$

By Lemma [23] below,

$$\left( \frac{H_K/K}{\mathfrak{P}^p'/(K)} \right) = \prod_{\{i \mid f_i = f\}} \left( \frac{H_K/K}{s_i(\mathfrak{P}) \cap K} \right).$$

An Artin symbol is a Frobenius:

$$\left( \frac{H_K/K}{s_i(\mathfrak{P}) \cap K} \right) = (s_i(\mathfrak{P}) \cap H_K, H_K/K) = (s_i(\mathfrak{P}), H_K/K)|_{H_K}.$$

It follows from the properties of the Frobenius that

$$\langle s_i(\mathfrak{P}), N_H/K \rangle = \langle s_i(\mathfrak{P}), N_H/Q \rangle^{f_i} = \langle s_i(\mathfrak{P}, N_H/Q) s_i^{-1} \rangle^{f_i} = s_i g^{f_i} s_i^{-1}.$$  

Consequently,

$$\left( \frac{H_K/K}{s_i(\mathfrak{P}) \cap K} \right) = s_i g^{f_i} s_i^{-1} |_{H_K}. \quad \square$$

**Remarks 2.2.** With the hypotheses and notation of Proposition 2.1

(i) Note that, in Formula (1),
- for every $i$, $s_i g^{f_i} s_i^{-1} \in H$,
- to consider the restriction to $H_K$ is equivalent to consider the class modulo $H_1$,
- as the group $H/H_1$ is abelian, the product in (1) does not depend on the order.
Lemma 3.1. In the group \( H \) the class \( \text{mod} \ H_1 \) of the product \( \prod_{\{i|f_i=1\}} s_i g^{f_i} s_i^{-1} \)

does not depend on the choice of the \( s_i \)'s [10] p. 176.

Proposition 3.2. If the following equality holds

\[
1 = \gamma_K(pO_K) = \left( \frac{H_K/K}{pO_K} \right) = \prod_{1 \leq i \leq t} s_i g^{f_i} s_i^{-1} \mid_{H_K},
\]

which means that [10] Prop. 6.2

\[
\prod_{1 \leq i \leq t} s_i g^{f_i} s_i^{-1} \in H_1.
\]

Lemma 2.3. [5] III, Prop. 2.8] With the hypotheses and notation of Proposition

(i) the prime ideals of \( K \) lying over \( p \) are the \( t \) ideals \( s_i(\mathfrak{Q}) \cap K \ (1 \leq i \leq t) \),

(ii) the residual degree of \( s_i(\mathfrak{Q}) \cap K \) in the extension \( K/\mathbb{Q} \) is \( f_i \).

3. The set \( T \) formed by the elements of \( H \) with one fixed point

Let \( T \) be the set formed by the elements of \( H \) with only one fixed point, namely the class \( H \), in their action on \( \Omega \):

\[
T = \{ h \in H \mid \forall s \in G \setminus H \ Hsh \neq Hs \}.
\]

Lemma 3.1. In the group \( H/H_1 \), one has the containment:

\[
T \text{mod} \ H_1 \subseteq \left\{ \left( \frac{H_K/K}{\Pi_p(K)} \right) \mid p \in \mathbb{P} \text{ non-ramified in } K \right\}.
\]

Proof. Let \( g \in T \subseteq H \). By Cheborev’s density theorem, \( g \) is the Frobenius of a prime \( \mathfrak{Q} \) of \( N_H \) lying over a prime number \( p \) which is not ramified in \( K \). Following formula [11], \( \left( \frac{H_K/K}{\Pi_p(K)} \right) = \prod_{\{i|f_i=1\}} s_i g^{f_i} s_i^{-1} \mod H_1 \). As \( H \) is the unique fixed point of \( g \) in its action on \( \Omega \), there is exactly one \( f_i \) which is equal to 1 and we may choose \( s_i = 1 \). Consequently, \( \left( \frac{H_K/K}{\Pi_p(K)} \right) = g \mod H_1 \). \( \square \)

Recall that

\[
\mathcal{P}o(K) = \langle \Pi_q(K) \mid q \in \mathbb{N}^* \rangle
\]

and

\[
\mathcal{P}o(K)_{nr} = \langle \Pi_p(K) \mid f \in \mathbb{N}^*, p \in \mathbb{P} \text{ non-ramified in } K \rangle.
\]

Let also:

\[
\mathcal{P}o(K)_{nr1} = \langle \Pi_p(K) \mid p \in \mathbb{P} \text{ non-ramified in } K \rangle.
\]

Proposition 3.2. If the following equality holds

\[
H = \langle T, H_1 \rangle,
\]

then

\[
\mathcal{C}l(K) = \mathcal{P}o(K) = \mathcal{P}o(K)_{nr} = \mathcal{P}o(K)_{nr1}.
\]

Proof. We have to prove the containment \( \mathcal{C}l(K) \subseteq \mathcal{P}o(K)_{nr1} \). The hypothesis means that \( H/H_1 = \langle T \mod H_1 \rangle \). Applying the isomorphism \( \gamma^{-1}_K \) to both sides, the image of the left hand side is \( \gamma^{-1}_K(H/H_1) = \mathcal{C}l(K) \) while, by lemma [12] the image of the right hand side \( \gamma^{-1}_K(\langle T \mod H_1 \rangle) \) is contained in \( \mathcal{P}o(K)_{nr1} \). \( \square \)
Thus, we obtain the conclusion of the conjecture, but how can we know that the hypothesis is satisfied? In some cases, in particular if the hypotheses of Theorem 1.3 are satisfied, we may replace the normal closure of $H_K$ by those of $K$.

Let $N_K$ be the normal closure of $K$ over $\mathbb{Q}$. We let $G_0 = \text{Gal}(N_K/\mathbb{Q})$, $H_0 = \text{Gal}(N_K/K)$, and $H_2 = \text{Gal}(N_H/N_K)$. Of course, $H_2$ is the largest normal subgroup of $G$ contained in $H$. Thus,

$$H_2 = \cap_{g \in G} gHg^{-1}.$$

Analogously to that we considered with respect to $G$ and $H$, we introduce the set $\Omega_0$ formed by the right cosets of $H_0$ in $G_0$, and the set $T_0$ formed by the elements of $H_0$ with only one fixed point in their action on $\Omega_0$. Moreover, we consider the canonical surjection $\pi : G \to G/H_2 = G_0$.

**Lemma 3.3.** For every $h \in H$, $h \in T$ if and only if $\pi(h) \in T_0$. Moreover, if $T_0 \neq \emptyset$, then $H_2 \subseteq \langle T \rangle$.

**Proof.** Let $h \in H$. Then, $h \notin T \iff \exists s \in G \setminus H \text{ s.t. } Hsh^{-1} = Hs \iff \exists s \in G \setminus H \text{ s.t. } shs^{-1} \in H \iff \exists s_0 \in G_0 \setminus H_0 \text{ s.t. } s_0\pi(h)s_0^{-1} \in H_0 \iff \pi(h) \notin T_0$.

Assume now that $T \neq \emptyset$ and fix some $t \in T$. Consider $h_2 \in H_2$. As $t \in T$, one has $\pi(th_2) = \pi(t) \in T_0$, and hence, $th_2 \in T$. Finally, $h_2 = t^{-1} \times th_2 \in \langle T \rangle$. □

Denoting by $H'_0$ the derived subgroup of $H_0$, we have:

**Lemma 3.4.** If $T_0 \neq \emptyset$ and $H_0 = \langle T_0, H'_0 \rangle$, then $H = \langle T, H_1 \rangle$.

**Proof.** It follows from Lemma 3.3 that $T_0 \neq \emptyset$ implies that $T \neq \emptyset$, and hence, that $H_2 \subseteq \langle T \rangle$. Clearly, $\pi(H') = H'_0$. Consequently,

$$\pi(\langle T, H' \rangle) = \langle \pi(T), \pi(H') \rangle = \langle T_0, H'_0 \rangle = H_0.$$

Since $H_2 \subseteq \langle T \rangle$, one has $H = \langle T, H' \rangle$, and since $H/H_1$ is abelian, one has $H' \subseteq H_1$. Finally,

$$H = \langle T, H' \rangle \subseteq \langle T, H_1 \rangle \subseteq H.$$ □
4. Conclusion

**Theorem 4.1.** Let $K$ be a number field of degree $n \geq 3$. Let $N_K$ be the normal closure of $K$ over $\mathbb{Q}$. Let $G = \text{Gal}(N_K/\mathbb{Q})$ and $H = \text{Gal}(N_K/K)$. Let $\Omega$ be the set formed by the right cosets of $H$ in $G$ and let $T$ be the set formed by the elements of $H$ which, in their action on $\Omega$, have only $H$ as fixed point. Assume that both following conditions are satisfied:

\[ T \neq \emptyset \quad \text{and} \quad H = \langle T, H' \rangle. \]

Then, the class group $\text{Cl}(K)$ of $K$ is generated by the classes of the ideals $\Pi_p(K)$ where $p \in \mathbb{P}$ is not ramified in $K$.

**Proof.** This is a straightforward consequence of Lemma 3.4 and Proposition 3.2. □

**Remark 4.2.** [10, Remark 6.5] If the action of $G$ on $\Omega$ is 2-transitive, then the action of $H$ on $\Omega \setminus \{H\}$ is transitive. Since $\text{Card}(\Omega \setminus \{H\}) = n - 1 \geq 2$, it follows from Burnside’s formula that $T \neq \emptyset$.

In the following applications of Theorem 4.1, $G := \text{Gal}(N_K/\mathbb{Q})$ is considered as isomorphic to a subgroup of the symmetric group $S_n$ since, if $K$ is generated by $x$, the elements of $G$ are permutations of the $n$ conjugates $x = x_1, x_2, \ldots, x_n$ of $x$ over $\mathbb{Q}$. Moreover, $H := \text{Gal}(N_K/K)$ is then the subgroup of $G$ which fixes $x$.

**Lemma 4.3.** Conditions (2) of Theorem 4.1 are satisfied if $G \cong S_n$ with $n = 3$ or $n \geq 5$, or if $G \cong A_n$ with $n = 4$ or $n \geq 6$.

**Proof.** (a) Assume that $G := \text{Gal}(N_K/\mathbb{Q}) \cong S_n$. Then, $H := \text{Gal}(N_K/K) \cong S_{n-1}$, $H' \cong A_{n-1}$, and $\Omega = \{S_{n-1}\sigma_i \mid 1 \leq i \leq n\}$ where $\sigma_i \in S_n$ satisfies $\sigma_i(i) = n$. As $H/H' \cong S_{n-1}/A_{n-1} \cong \mathbb{Z}/2\mathbb{Z}$, both conditions (2) will surely be satisfied if there exists some $\tau \in S_{n-1}\setminus A_{n-1}$ which does not fix any symbol. We obtain such a $\tau$ by considering any cycle of length $n - 1 \geq 2$ in $S_{n-1}$ if $n$ is odd (which leads to the constraint $n \geq 3$), and, if $n$ is even, by considering the product of two disjoint cycles of length $r \geq 2$ and $s \geq 2$ respectively such that $r + s = n - 1$ (which leads to the constraint $n \geq 5$).

(b) Assume now that $G := \text{Gal}(N_K/\mathbb{Q}) \cong A_n$. Then, $H := \text{Gal}(N_K/K) \cong A_{n-1}$. $A_{n-1}$ acts transitively on the $n$ right cosets of $A_n$ modulo $A_{n-1}$ as soon as $n \geq 4$. It then follows from Remark 4.2 that $T \neq \emptyset$. Moreover, as $H' \cong A_{n-1}$ for $n-1 \geq 5$, conditions (2) are satisfied for $n \geq 6$. And also for $n = 4$ since $\{1\} \subset T \subset A_3$. □

Frobenius groups lead also to similar conclusions. Recall:

**Definition 4.4.** A Frobenius group is a permutation group $G$ which acts transitively on a finite set $X$ such that every $g \in G \setminus \{1\}$ does not fix more than one point and that there exists at least one $g \in G \setminus \{1\}$ which fix an $x \in X$.

**Lemma 4.5.** Conditions (2) of Theorem 4.1 are satisfied if $G$ is a Frobenius group.

**Proof.** By transitivity the stabilizer of every element is not trivial, and hence, $H \neq \{1\}$. It follows then from the definition that $T = H \setminus \{1\} \neq \emptyset$. □

Now we can conclude:

**Theorem 4.6.** Let $K$ be a number field of degree $n \geq 3$. If the Galois group of the normal closure of $K$ is either isomorphic to $S_n$ ($n \neq 4$) or to $A_n$ ($n \neq 3, 5$), or is a Frobenius group, then

\[ \text{Cl}(K) = \mathcal{P}o(K) = \mathcal{P}o(K)_{nr} = \mathcal{P}o(K)_{nr1}. \]
For instance, the Pólya group $\mathcal{P}o(K)$ of a non-galoisian cubic number field $K$ is always equal to the class group $\mathcal{C}l(K)$ of $K$.

References

[1] M. Bhargava, Generalized Factorials and Fixed Divisors over Subsets of a Dedekind Domain, *J. Number Theory* **72** (1998), 67–75.

[2] P.-J. Cahen and J.-L. Chabert, *Integer-Valued Polynomials*, Mathematical Surveys and Monographs, Vol. 48, Amer. Math. Soc., Providence, 1997.

[3] J.-L. Chabert, From Pólya fields to Pólya groups, (I) Galoisian extensions. https://arxiv.org/pdf/1805.11585.pdf

[4] J.-L. Chabert, From Pólya fields to Pólya groups, Conference on *Rings and Factorizations*, Graz, February 2018. https://imsc.uni-graz.at/rings2018/slides/chabert.pdf

[5] G.J. Janusz, *Algebraic number fields*, Academic Press, 1973.

[6] A. Leriche, About the embedding of a number field in a Pólya field, *J. Number Theory* **145** (2014), 210–229.

[7] A. Ostrowski, Über ganzwertige Polynome in algebraischen Zahlkörpern, *J. reine angew. Math.* **149** (1919), 117–124.

[8] G. Pólya, Über ganzwertige Polynome in algebraischen Zahlkörpern, *J. reine angew. Math.* **149** (1919), 97–116.

[9] J.-P. Serre, *Corps locaux*, Hermann, Paris, 1962.

[10] H. Zantema, Integer valued polynomials over a number field, *Manuscr. Math.* **40** (1982), 155–203.

LAMFA (UMR-CNRS 7352), Université de Picardie, 33 rue Saint Leu, 80039 Amiens, France

E-mail address: jean-luc.chabert@u-picardie.fr