Journal of Number Theory 133 (2013) 59–71

Contents lists available at SciVerse ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Cubic, quartic and sextic Pólya fields

Amandine Leriche

École Centrale de Lille, Cité Scientifique, 59650 Villeneuve d'Ascq, & Université de Picardie Jules Verne, 33, rue Saint-Leu 80039 Amiens, France

ARTICLE INFO

Article history:
Received 28 September 2011
Revised 27 June 2012
Accepted 28 June 2012
Available online 13 September 2012
Communicated by David Goss

Keywords:
Cubic fields
Quartic fields
Sextic fields
Pólya fields
Integer-valued polynomials

ABSTRACT

A Pólya field is a number field K, with ring of integers $\mathcal{O}_K$, such that the $\mathcal{O}_K$-module formed by the integer-valued polynomials on $\mathcal{O}_K$ has a regular basis. We are interested here by Pólya fields of small degree. We give a complete characterization of cyclic cubic, quartic and sextic Pólya fields (quadratic Pólya fields are known for a long time). Moreover, we prove that, with few exceptions, the compositum of two quadratic Pólya fields is a biquadratic Pólya field. Finally, we study sextic Pólya fields which are the Galoisian closure of pure cubic fields.

1. Introduction

We first recall the definition of a Pólya field and some basic characterizations. Let K be an algebraic number field and denote by $\mathcal{O}_K$ its ring of integers. We consider the ring of integer-valued polynomials on $\mathcal{O}_K$, that is

$$\operatorname{Int}(\mathcal{O}_K) = \left\{ P \in K[X] \;\middle|\; P(\mathcal{O}_K) \subseteq \mathcal{O}_K \right\}.$$

The $\mathcal{O}_K$-module $\operatorname{Int}(\mathcal{O}_K)$ is free [4, Remark II.3.7] but describing a basis often constitutes an arduous task. Thus, Pólya [13] and Ostrowski [12] tried to characterize the fields K such that $\operatorname{Int}(\mathcal{O}_K)$ admits a "regular basis" in the following sense:

Definition 1.1. (See Zantema [17].) A number field K is said to be a *Pólya field* if the $\mathcal{O}_K$-module $\operatorname{Int}(\mathcal{O}_K)$ admits a regular basis, that is, a basis $(f_n)_{n\in\mathbb{N}}$ such that, for each n, the polynomial f_n has degree n.

E-mail address: amandine.leriche@u-picardie.fr.

0022-314X/$ – see front matter
http://dx.doi.org/10.1016/j.jnt.2012.06.016

There are several ways to characterize Pólya fields. The first way is by considering the characteristic ideals. For each $n \in \mathbb{N}$, let $\mathfrak{I}_n(K)$ be the subset of K formed by 0 and the leading coefficients of the polynomials in $\mathrm{Int}(\mathcal{O}_K)$ with degree n. This is a fractional ideal of $\mathcal{O}_K$ called the *characteristic ideal of K of index n* [4, Proposition I.3.I]. The field K is a Pólya field if and only if the characteristic ideals $\mathfrak{I}_n(K)$ are principal [4, II.1.4]. Of course, a number field K with class number h_K equal to 1 is a Pólya field. But the converse does not hold: for instance, every cyclotomic field is a Pólya field (see [17]).

The second way is the study of the Pólya group of K which can be considered as a measure of the obstruction for a field K to be a Pólya field. Indeed, denote by $Cl(K)$ the class group of K, that is the quotient $Cl(K) = I(K)/P(K)$ of the group of fractional ideals $I(K)$ of K by the group $P(K)$ of nonzero principal ideals. The *Pólya group of K* is the subgroup $Po(K)$ of $Cl(K)$ generated by the classes of the characteristic ideals $\mathfrak{I}_n(K)$ of K. In fact, $Po(K)$ is also the subgroup of $Cl(K)$ generated by the classes of the ideals $\Pi_q(K)$ defined below [5, Proposition 2.2]:

Notation. For each $q \geqslant 2$, let $\Pi_q(K)$ be the product of all the maximal ideals of $\mathcal{O}_K$ with norm q:

$$\Pi_q(K) = \prod_{\substack{\mathfrak{m} \in Max(\mathcal{O}_K) \\ N(\mathfrak{m}) = q}} \mathfrak{m}.$$

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

We resume all these assertions in the following proposition:

Proposition 1.2. *The field K is a Pólya field if and only if one of the following assertions is satisfied*:

(1) $\mathrm{Int}(\mathcal{O}_K)$ *has a regular basis*;
(2) *for each $n \in \mathbb{N}$, the ideal $\mathfrak{I}_n(K)$ is principal*;
(3) *for each $q \geqslant 2$, the ideal $\Pi_q(K)$ is principal*;
(4) $Po(K) = \{1\}$.

Quadratic Pólya fields are completely characterized [17]:

Proposition 1.3. *A quadratic field $\mathbb{Q}[\sqrt{d}\,]$ is a Pólya field if and only if d is of one of the following forms where p and q denote two distinct odd prime numbers*:

(1) $d = 2$, *or* $d = -1$, *or* $d = -2$, *or* $d = -p$ *where* $p \equiv 3 \pmod 4$, *or* $d = p$,
(2) $d = 2p$, *or* $d = pq$ *where* $pq \equiv 1 \pmod 4$ *and, in both cases, the fundamental unit has norm* 1 *if* $p \equiv 1 \pmod 4$.

We believe this is the only characterization of Pólya fields of a given degree to be found in the literature. Here, we wish to characterize Galoisian Pólya fields with small degree, namely less than six. Indeed, several results about Pólya groups in Galoisian extensions stated in [5] suggest that such characterizations are obtained more easily for Galoisian fields. The simplicity of those characterizations depends on the properties of the Galois group $G(K/\mathbb{Q})$ and also on the ramification in the extension $K/\mathbb{Q}$.

This work has been undertaken in [11] for biquadratic fields through the following proposition that we will use later for our characterization.

Notation. For every finite extension L/K, denote by ϵ_K^L the natural morphism

$$\epsilon_K^L : \overline{\mathcal{I}} \in Cl(K) \mapsto \overline{\mathcal{I}\mathcal{O}_L} \in Cl(L).$$

Proposition 1.4. *(See [11, Proposition 4.2].) Let K, K_1 and K_2 be Galoisian extensions of $\mathbb{Q}$ such that $K_1 \cap K_2 = K$ and denote by $L = K_1K_2$ the compositum of K_1 and K_2. If, for each prime ideal $\mathfrak{p}$ of K, the ramification indices of $\mathfrak{p}$ in the extensions $K_1/\mathbb{Q}$ and $K_2/\mathbb{Q}$ are coprime, then*:

$$\epsilon_{K_1}^{L}\big(Po(K_1)\big).\epsilon_{K_2}^{L}\big(Po(K_2)\big) = Po(L).$$

In particular, if K_1 and K_2 are Pólya fields, then L is a Pólya field.

The first characterization is obtained when $G(K/\mathbb{Q})$ is cyclic and its order is an odd prime number: K is a Pólya field if and only if there is only one prime which is ramified in $K/\mathbb{Q}$. We describe in Section 3 all cyclic cubic Pólya fields.

If $G(K/\mathbb{Q})$ is still cyclic but if its order is not prime, Proposition 1.4 leads us to consider the case of cyclic Galois groups whose order is a prime power. We characterize in Section 4 cyclic quartic Pólya fields.

The group $G(K/\mathbb{Q})$ may be Abelian but not cyclic. Proposition 1.4 leads us again to consider Abelian Galois groups whose order is a prime power. We study in Section 4 biquadratic fields obtained as a compositum of two quadratic Pólya fields.

Finally, we consider the case where $G(K/\mathbb{Q})$ is not Abelian. Such a case does not happen until degree 6 with a Galois group isomorphic to the symmetric group S_3. These sextic extensions are in fact the Galoisian closures of non-cyclic cubic fields. We characterize in Section 5 sextic extensions that are Galoisian closure of pure cubic fields, that is, fields of the form $\mathbb{Q}[j, \sqrt[3]{m}]$.

We begin this work with a general study on the number of primes that are ramified in a Galoisian Pólya field.

2. A bound for the number of ramified primes in a Pólya field

Let K be a number field which is a Galoisian extension of $\mathbb{Q}$. Denote by s_K the number of primes which are ramified in $K/\mathbb{Q}$, and, for each prime number p, denote by e_p the index of ramification of p in $K/\mathbb{Q}$. Recall a result from Zantema:

Proposition 2.1. *(See [17].) If $K/\mathbb{Q}$ is Galoisian with Galois group G, the following sequence of Abelian groups is exact*:

$$1 \to H^1\big(G, \mathcal{O}_K^{\times}\big) \to \oplus_{p\in\mathbb{P}}\mathbb{Z}/e_p\mathbb{Z} \to Po(K) \to 1.$$

In particular,

$$\big|Po(K)\big| \times \big|H^1\big(G, \mathcal{O}_K^{\times}\big)\big| = \prod_{p\in\mathbb{P}} e_p.$$

Thus, if $K/\mathbb{Q}$ is a Galoisian extension, K is a Pólya field if and only if $|H^1(G, \mathcal{O}_K^{\times})| = \prod_{p\in\mathbb{P}} e_p$. Moreover, since for cyclic extensions, the order of $H^1(G, \mathcal{O}_K^{\times})$ is known, we have:

Proposition 2.2. *(See [5, Corollary 3.11].) Assume that the extension $K/\mathbb{Q}$ is cyclic of degree n.*

(1) *If K is real and $N(\mathcal{O}_K^{\times}) = \{1\}$, then $|Po(K)| = \frac{1}{2n} \times \prod_p e_p$.*
(2) *In all other cases, $|Po(K)| = \frac{1}{n} \times \prod_p e_p$.*

One deduces easily the following property:

Proposition 2.3. *If $K/\mathbb{Q}$ is a cyclic extension whose degree is an odd prime number q, then $Po(K) = q^{s_K-1}$ where s_K denotes the number of primes which are ramified in $K/\mathbb{Q}$. In particular, K is a Pólya field if and only if there is exactly one prime which ramifies in $K/\mathbb{Q}$.*

Proof. A prime number which ramifies in a cyclic extension $K/\mathbb{Q}$ whose degree is a prime number is totally ramified in this extension. Thus, as $q \neq 2$ and as the cardinality of $Po(K)$ is an integer, following Proposition 2.2, $Po(K) = q^{s_K - 1}$. □

Remarks.

(1) Note that the case where $q = 2$ corresponds to quadratic number fields and the cardinality of $Po(K)$ was given by Hilbert [9, §75]:
- $|Po(K)| = 2^{s_K - 2}$ if K is real and $N(\mathcal{O}_K^\times) = \{1\}$ and
- $|Po(K)| = 2^{s_K - 1}$ in the other cases.

Consequently, for a quadratic Pólya field K, $s_K = 1$ or 2.

(2) If $K/\mathbb{Q}$ is not cyclic with an odd prime degree, not only s_K may be distinct from 1 but s_K may be arbitrarily large. Indeed, Proposition 1.4 enables us to construct Pólya fields that have a number of ramified prime numbers as large as we wish. For instance, the field $\mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_r}]$, where r is any positive integer and the p_i's are primes such that $p_i \equiv 1 \pmod 4$, is the compositum of r quadratic Pólya fields $K_1 = \mathbb{Q}[\sqrt{p_1}], \ldots, K_r = \mathbb{Q}[\sqrt{p_r}]$ (see Proposition 1.3). Since the ramification indices of the primes p_i in the extensions $K_i/\mathbb{Q}$ are coprime, by Proposition 1.4, we obtain that $L := \prod_{i=1}^r K_i = \mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_r}]$ is a Pólya field with r ramified primes. In this construction, in order to obtain r ramified prime numbers, we have to consider an extension of degree $\geqslant 2^r$.

On the other hand, if the degree n of $K/\mathbb{Q}$ is fixed, we may give an upper bound for s_K. For this purpose, we recall a result from Brumer and Rosen:

Proposition 2.4. *(See [3, Proposition 3.3].) Let $K/\mathbb{Q}$ be a Galoisian extension with group G and degree n. Let $n = \prod_p p^{v_p(n)}$ be a factorization of n into prime powers. Then $|H^1(G, \mathcal{O}_K^\times)|$ divides $\prod_{p|n} p^{R_p(n)}$ where*

$$R_p(n) = n\left(\frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^{v_p(n)}}\right) + v_p(n).$$

Proposition 2.5. *The number s_K of prime which are ramified in a Pólya field K which is a Galoisian extension of $\mathbb{Q}$ is bounded by a function which depends only on the degree n of the extension $K/\mathbb{Q}$. More precisely,*

$$s_K \leqslant \sum_{p|n} R_p(n) \quad \text{where } R_p(n) = n\left(\frac{1}{p} + \frac{1}{p^2} + \cdots + \frac{1}{p^{v_p(n)}}\right) + v_p(n).$$

Proof. Assume that $K/\mathbb{Q}$ is a Pólya field. Following Proposition 2.1, $|H^1(G, \mathcal{O}_K^\times)| = \prod_{p\in\mathbb{P}} e_p$, and the previous proposition shows that $\prod_{p\in\mathbb{P}} e_p \mid \prod_{p|n} p^{R_p(n)}$. The number of irreducible factors of $\prod_{p\in\mathbb{P}} e_p$ is $\geqslant s_K$, while the number of irreducible factors of $\prod_{p|n} p^{R_p(n)}$ is exactly $\sum_{p|n} R_p(n)$. Consequently, $s_K \leqslant \sum_{p|n} R_p(n)$. □

Application 1. Assume that K is a Pólya field which is a Galoisian extension of degree n. It follows from Proposition 2.5 that, if $n = 2$ (respectively 3, 4, 6), then $s_K \leqslant 2$ (respectively 2, 5, 7). The first bound agrees with the previous remark, the second bound is larger than the exact value 1 given by Proposition 2.3. We will see that the others are rough bounds.

3. Cyclic cubic Pólya fields

Let K be a cubic field. We denote by D_K the discriminant of K. One knows that K is a cyclic cubic field if and only if the discriminant D_K of K is a square in $\mathbb{Q}$. We recall the complete description of cyclic cubic fields that one may find in [6]:

Proposition 3.1. *(See [6, Lemma 6.4.5].) For any cyclic cubic field K, there exists a unique pair of integers e and u such that e is equal to a product of distinct primes congruent to 1 modulo 3, $u \equiv 2 \pmod 3$ and such that $K = \mathbb{Q}(\theta)$ where θ is a root of the polynomial $Q(X) = X^3 - 3eX - eu$. Moreover $e = \frac{u^2+3v^2}{4}$ where $v \in \mathbb{N}^*$. Conversely, a field K of the aforementioned type is a cyclic cubic field. Furthermore, if $3 \nmid v$ then $D_K = 81e^2$, and if $3|v$ then $D_K = e^2$.*

Proposition 3.2. *Let K be a cyclic cubic field. Then, K is a Pólya field if and only if $K = \mathbb{Q}(\theta)$ where θ is a root of a polynomial P such that*:

$$\text{either} \quad P = X^3 - 3X + 1,$$
$$\text{or} \quad P = X^3 - 3pX - pu$$

where p is a prime such that $p = \frac{u^2+27w^2}{4}$ with $u \equiv 2 \pmod 3$ and $w \in \mathbb{N}^*$.

Proof. Following Proposition 2.3, K is a cyclic cubic Pólya field if and only if there is only one prime which ramifies in the extension $K/\mathbb{Q}$. Assume that 3 ramifies in $K/\mathbb{Q}$. Using notation of the previous proposition, the prime 3 is thus the only possible prime divisor of e. But $e \equiv 1 \pmod 3$ and as a consequence $e = 1$, $u = \pm 1$ and $v = 1$. Since $u \equiv 2 \pmod 3$ then $u = -1$ and $P = X^3 - 3X + 1$. Now, if 3 does not ramify in $K/\mathbb{Q}$, then we have $3|v$ and $D_K = e^2$. Thus $e = p$ where p is a prime number such that $p \equiv 1 \pmod 3$. We conclude that

$$P = X^3 - 3pX - pu$$

where p is a prime such that $p = \frac{u^2+27w^2}{4}$ with $u \equiv 2 \pmod 3$ and $w \in \mathbb{N}^*$. □

Example 3.3. For $p = 13$, $u = 5$ and $w = 1$, the previous proposition shows that the field $K = \mathbb{Q}(\theta)$ where θ is a root of $X^3 - 39X - 65$ is a cyclic cubic Pólya field.

4. Cyclic quartic Pólya fields

Next, we carry on the study with cyclic quartic fields. We find a complete description of cyclic quartic fields in [8] and their discriminants are computed in [16]. We first recall these properties.

Proposition 4.1. *A cyclic quartic extension $K/\mathbb{Q}$ can be expressed uniquely in the following form $K = \mathbb{Q}(\sqrt{A(D + B\sqrt{D})})$ where A, B, C and D are integers such that A is squarefree and odd, $D = B^2 + C^2$ is squarefree, $B > 0$, $C > 0$, $\gcd(A, D) = 1$.*

The discriminant D_K of such a field K is given by

$$D_K = \begin{cases} 2^8A^2D^3, & \text{if } D \equiv 0 \pmod 2, \\ 2^6A^2D^3, & \text{if } D \equiv 1 \pmod 2 \text{ and } B \equiv 1 \pmod 2, \\ 2^4A^2D^3, & \text{if } D \equiv 1 \pmod 2 \text{ and } B \equiv 0 \pmod 2,\ A + B \equiv 3 \pmod 4, \\ A^2D^3, & \text{if } D \equiv 1 \pmod 2 \text{ and } B \equiv 0 \pmod 2,\ A + B \equiv 1 \pmod 4. \end{cases}$$

Remark that $k = \mathbb{Q}(\sqrt{D})$ is the unique quadratic subfield of K. Moreover, K is totally real if $A > 0$ and totally imaginary if $A < 0$.

Notations. For each $n \in \mathbb{N}$, denote by $\omega(n)$ the number of distinct prime numbers dividing n. Let α_K be the integer defined by

$$\begin{cases} \alpha_K = 1 & \text{if } K \text{ is real and if } N(\mathcal{O}_K^\times) = \{1\}, \\ \alpha_K = 0 & \text{else.} \end{cases}$$

In order to study the ramification in a cyclic quartic extension $K/\mathbb{Q}$, we precise the notion of a minimal extension: a non-trivial extension M/K is said to be a *minimal extension* of K if, for each field L such that $K \subset L \subset M$, $L = M$ or $L = K$.

Lemma 4.2. *Let L/K be a Galoisian extension of number fields. A prime ideal $\mathfrak{p}$ of K is totally ramified in L/K if and only if it ramifies in every minimal extension of K contained in L.*

Proof. One assertion is obvious. We prove the other one. Assume that $\mathfrak{p}$ is not totally ramified in the extension L/K. Let $\mathfrak{P}$ be a prime ideal of L lying over $\mathfrak{p}$, the inertial group I of $\mathfrak{P}$ in L/K is a strict subgroup of the Galois group of L/K. Denote by L^I the subfield of L fixed by I. The prime ideal $\mathfrak{p}$ does not ramify in the extension L^I/K and L^I/K contains a minimal extension where $\mathfrak{p}$ does not ramify. □

Proposition 4.3. *Let $K = \mathbb{Q}(\sqrt{A(D + B\sqrt{D})})$ be a cyclic quartic field. The order $|Po(K)|$ of the Pólya group of K is given by*:

(1) $|Po(K)| = 4^{\omega(D)-1}2^{\omega(A)-\alpha_K}$ *if* $D \equiv 0 \pmod 2$ *or* $A + B \equiv 1 \pmod 4$.
(2) $|Po(K)| = 4^{\omega(D)-1}2^{\omega(A)-\alpha_K+1}$ *in the other cases.*

Proof. By Proposition 2.2,

$$\big|Po(K)\big| = \frac{1}{4} \times \frac{1}{2^{\alpha_K}} \times \prod_p e_p.$$

By Lemma 4.2, p is totally ramified in $K/\mathbb{Q}$ if and only if p is ramified in $k/\mathbb{Q}$, that is, $e_p = 4$ if and only if $p|D_k$. Consequently,

$$\prod_p e_p = 4^{\omega(D_k)} \times 2^{\omega(D_K)-\omega(D_k)}.$$

Since D is a sum of two squares, one has $D \equiv 1$ or $2 \pmod 4$, and hence, $\omega(D_k) = \omega(D)$. Since A is an odd number coprime to D, it follows from Proposition 4.1 that:

- if $D \equiv 0 \pmod 2$ or if $A + B \equiv 1 \pmod 4$, then $\omega(D_K) - \omega(D_k) = \omega(A)$,
- in the other cases, $\omega(D_K) - \omega(D_k) = \omega(A) + 1$. □

Theorem 4.4. *Let $K = \mathbb{Q}(\sqrt{A(D + B\sqrt{D})})$ be a cyclic quartic field where A, B, C, D are integers such that A is squarefree and odd, $D = B^2 + C^2$ is squarefree, $B > 0$, $C > 0$, $\gcd(A, D) = 1$. Then K is a Pólya field if and only if one of the following conditions is satisfied (p and q denote distinct odd prime numbers)*:

(1) $K = \mathbb{Q}(\sqrt{2 + \sqrt{2}})$ *or* $K = \mathbb{Q}(i\sqrt{2 + \sqrt{2}})$.
(2) $K = \mathbb{Q}(\sqrt{q(2 + \sqrt{2})})$ *with* $N(\mathcal{O}_K^\times) = \{1\}$.
(3) $K = \mathbb{Q}(\sqrt{p + B\sqrt{p}})$ *with* $p \equiv 1 \pmod 4$, $B \equiv 0 \pmod 4$ *and* $p = B^2 + C^2$.
(4) $K = \mathbb{Q}(i\sqrt{p + B\sqrt{p}})$ *with* $p \equiv 1 \pmod 4$, $B \equiv 2 \pmod 4$ *and* $p = B^2 + C^2$.
(5) $K = \mathbb{Q}(\sqrt{p + B\sqrt{p}})$ *with* $p \equiv 1 \pmod 4$, $B \equiv 1, 2, 3 \pmod 4$, $p = B^2 + C^2$ *and* $N(\mathcal{O}_K^\times) = \{1\}$.
(6) $K = \mathbb{Q}(\sqrt{q(p + B\sqrt{p})})$ *with* $p \equiv 1 \pmod 4$, $p = B^2 + C^2$, $q + B \equiv 1 \pmod 4$ *and* $N(\mathcal{O}_K^\times) = \{1\}$.

Proof. Assume that K is a Pólya field. From Proposition 4.3, we deduce that $\omega(D)=1$ and $\omega(A)=0$ or 1. Since $D\equiv 1,2 \pmod 4$, one has $D=2$ or $D=p$ with $p\equiv 1 \pmod 4$.

Consider the case $D=2$. Thus $\omega(A)=\alpha_K$. For $\alpha_K=0$, one has $A=\pm 1$ and K is one of the following fields: $K=\mathbb{Q}(\sqrt{2+\sqrt{2}})$ and $K=\mathbb{Q}(i\sqrt{2+\sqrt{2}})$. Conversely, these two fields are Pólya fields since there is only one prime which ramifies, namely 2. If $\alpha_K=1$, then $A>0$, $\omega(A)=1$ and $A=q$, q being an odd prime number. We obtain the field $\mathbb{Q}(\sqrt{q(2+\sqrt{2})})$. Such a field is a Pólya field under the condition $N(\mathcal{O}_K^\times)=\{1\}$.

Now we consider the case $D=p\equiv 1 \pmod 4$. If $A+B\equiv 1 \pmod 4$, then $\omega(A)=\alpha_K$. Assume that $\alpha_K=0$, we have $A=\pm 1$ and we get the fields $K=\mathbb{Q}(\sqrt{p+B\sqrt{p}})$ $(A=1,\ B\equiv 0 \pmod 4)$ and $K=\mathbb{Q}(i\sqrt{p+B\sqrt{p}})$ $(A=-1$ and $B\equiv 2 \pmod 4)$. Conversely these two fields are Pólya fields since p is the only ramified prime. If $\alpha_K=1$, then $A>0$, $\omega(A)=1$. We deduce that $A=q$ where q is an odd prime number. Hence, we get the field $\mathbb{Q}(\sqrt{q(p+B\sqrt{p})})$. Such a field is a Pólya field under the condition $N(\mathcal{O}_K^\times)=\{1\}$.

Assume that $A+B\not\equiv 1 \pmod 4$, we have $\omega(A)=\alpha_K-1=0$. Thus $\alpha_K=1$ and $A=1$ $(B\not\equiv 0 \pmod 4)$. We get a field of the form $\mathbb{Q}(\sqrt{(p+B\sqrt{p})})$. Such a field is a Pólya field under the condition $N(\mathcal{O}_K^\times)=\{1\}$. □

Sometimes, one may specify the previous theorem about the norm of units thanks to the following proposition:

Proposition 4.5. *(See [7].) Let K be a real finite Galoisian extension. Suppose the conductor f of K is composite. Let M_f be the maximal real subfield of $\mathbb{Q}(e^{\frac{2i\pi}{f}})$. If $[M_f:K]$ is odd (i.e. if $\frac{\varphi(f)}{2[K:\mathbb{Q}]}$ is odd), then $N(\mathcal{O}_K^\times)=\{1\}$.*

Following [15], the conductor f of a cyclic quartic field $K=\mathbb{Q}(\sqrt{A(D+B\sqrt{D})})$ is

$$f=2^l|A|D$$

where

$$l=\begin{cases}3, & \text{if } D\equiv 2 \pmod 4 \text{ or } D\equiv 1 \pmod 4,\ B\equiv 1 \pmod 2,\\ 2, & \text{if } D\equiv 1 \pmod 4,\ B\equiv 0 \pmod 2,\ A+B\equiv 3 \pmod 4,\\ 0, & \text{if } D\equiv 1 \pmod 4,\ B\equiv 0 \pmod 2,\ A+B\equiv 1 \pmod 4.\end{cases}$$

Then, we can refine assertions (5) and (6) of Theorem 4.4

Corollary 4.6.

(1) *Let $K=\mathbb{Q}(\sqrt{p+B\sqrt{p}})$ be a cyclic quartic field such that $p\equiv 1 \pmod 4$, $B\equiv 2 \pmod 4$ and $p=B^2+C^2$. If $p\equiv 5 \pmod 8$, then K is a Pólya field.*
(2) *Let $K=\mathbb{Q}(\sqrt{q(p+B\sqrt{p})})$ be a cyclic quartic field such that $p\equiv 1 \pmod 4$, $B\equiv 0 \pmod 2$ and $p=B^2+C^2$, $q+B\equiv 1 \pmod 4$. If $p\equiv 5 \pmod 8$ and $q\equiv 3 \pmod 4$, then K is a Pólya field.*

Proof.

(1) The conductor f of K is equal to $f=2^2p$. If $p\equiv 5 \pmod 8$, then $\frac{\varphi(f)}{2[K:\mathbb{Q}]}=\frac{p-1}{4}$ is odd.
(2) The conductor f of K is equal to $f=qp$. If $p\equiv 5 \pmod 8$ and $q\equiv 3 \pmod 4$, then $\frac{\varphi(f)}{2[K:\mathbb{Q}]}=\frac{(p-1)(q-1)}{8}$ is odd. □

5. About biquadratic Pólya fields

In this section, we prove that, with few exceptions, biquadratic fields obtained by composition of two quadratic Pólya fields are Pólya fields. This study has been undertaken in [11] and we pursue it in this section. We prove the following result:

Theorem 5.1. *Let m and n be two squarefree integers such that $\mathbb{Q}[\sqrt{m}\,]$ and $\mathbb{Q}[\sqrt{n}\,]$ are quadratic Pólya fields. The biquadratic field $\mathbb{Q}[\sqrt{m}, \sqrt{n}\,]$ is a Pólya field except for the following fields, where p and q denote odd primes and $p \equiv 3 \pmod 4$:*

(1) $\mathbb{Q}[i\sqrt{2}, \sqrt{p}\,]$ *is not a Pólya field*;
(2) $\mathbb{Q}[i, \sqrt{2q}\,]$ *is not a Pólya field*;
(3) $\mathbb{Q}[\sqrt{p}, \sqrt{2q}\,]$ *is not always a Pólya field. If it is a Pólya field, then*:
   (a) *either* $p \equiv -1 \pmod 8$ *and* $q \equiv \pm 1 \pmod 8$,
   (b) *or* $p \equiv 3 \pmod 8$ *and* $q \equiv 1, 3 \pmod 8$.

But these necessary conditions are not sufficient.

Notations. Let m and n be two squarefree integers. We let $l = \gcd(m, n)$ and write $m = lm_1$, $n = ln_1$, so that $\gcd(m_1, n_1) = 1$.

These exceptions are due to the prime 2 which may not satisfy the hypothesis of Proposition 1.4. More precisely:

Proposition 5.2. *(See [11, Proposition 4.3].) If $K_1 = \mathbb{Q}[\sqrt{m}\,]$ and $K_2 = \mathbb{Q}[\sqrt{n}\,]$ are two distinct quadratic Pólya fields such that 2 is ramified in at most two of the three extensions $\mathbb{Q}[\sqrt{m}\,]/\mathbb{Q}$, $\mathbb{Q}[\sqrt{n}\,]/\mathbb{Q}$ and $\mathbb{Q}[\sqrt{m_1n_1}\,]/\mathbb{Q}$, then the field $\mathbb{Q}[\sqrt{m}, \sqrt{n}\,]$ is a Pólya field.*

Thus, when $\mathbb{Q}[\sqrt{m}\,]$ and $\mathbb{Q}[\sqrt{n}\,]$ are quadratic Pólya fields, $\mathbb{Q}[\sqrt{m}, \sqrt{n}\,]$ may not be a Pólya field only if 2 is ramified in each extension $\mathbb{Q}[\sqrt{m}\,]/\mathbb{Q}$, $\mathbb{Q}[\sqrt{n}\,]/\mathbb{Q}$ and $\mathbb{Q}[\sqrt{m_1n_1}\,]/\mathbb{Q}$.

Lemma 5.3. *The prime 2 is ramified in each quadratic extension $\mathbb{Q}[\sqrt{m}\,]/\mathbb{Q}$, $\mathbb{Q}[\sqrt{n}\,]/\mathbb{Q}$ and $\mathbb{Q}[\sqrt{m_1n_1}\,]/\mathbb{Q}$ if and only if two of the three integers m, n, m_1n_1 are congruent to 2 modulo 4 and the third is congruent to 3 modulo 4.*

Proof. The prime 2 ramifies in the three quadratic extensions $\mathbb{Q}[\sqrt{m}\,]/\mathbb{Q}$, $\mathbb{Q}[\sqrt{n}\,]/\mathbb{Q}$ and $\mathbb{Q}[\sqrt{m_1n_1}\,]/\mathbb{Q}$ if and only if m, n, $m_1n_1 \equiv 2, 3 \pmod 4$.

- If $m, n \equiv 3 \pmod 4$, then $mn \equiv 1 \pmod 4$, $m_1n_1 \equiv 1 \pmod 4$ and 2 is not ramified in $\mathbb{Q}[\sqrt{m_1n_1}\,]/\mathbb{Q}$.
- If $m, n \equiv 2 \pmod 4$, then $m_1n_1 \not\equiv 2 \pmod 4$ (otherwise 4 would divide m or n, but they are squarefree). The prime 2 is ramified in $\mathbb{Q}[\sqrt{m_1n_1}\,]/\mathbb{Q}$ if and only if $m_1n_1 \equiv 3 \pmod 4$.
- If $m \equiv 2 \pmod 4$ and $n \equiv 3 \pmod 4$, then $m_1n_1 \equiv 2 \pmod 4$. □

Then, using the characterization of quadratic Pólya fields (cf. Proposition 1.3), we state all the biquadratic fields obtained by composition of quadratic Pólya fields such that 2 is ramified in each quadratic subfield, and hence, which are not necessarily Pólya fields.

Lemma 5.4. *Let $\mathbb{Q}[\sqrt{m}\,]$ and $\mathbb{Q}[\sqrt{n}\,]$ be two quadratic Pólya fields. The prime 2 is ramified in each quadratic subextensions of $L = \mathbb{Q}[\sqrt{m}, \sqrt{n}\,]$ if and only if L is one of the five following fields: $\mathbb{Q}[i, \sqrt{2}\,]$, $\mathbb{Q}[i, \sqrt{2q}\,]$, $\mathbb{Q}[\sqrt{2}, \sqrt{p}\,]$, $\mathbb{Q}[\sqrt{-2}, \sqrt{p}\,]$, $\mathbb{Q}[\sqrt{p}, \sqrt{2q}\,]$ where p and q are two distinct odd prime numbers and $p \equiv 3 \pmod 4$.*

A biquadratic field $L=\mathbb{Q}[\sqrt{m},\sqrt{n}\,]$ among the five fields given in Lemma 5.4 is a Pólya field if and only if $\Pi_2(L)$ is principal. Lemma 4.2 shows that 2 is totally ramified in these biquadratic fields. Thus the ideal $\Pi_2(L)$ is principal if and only if L contains an integer with norm ± 2.

Lemma 5.5. *Let $L=\mathbb{Q}[\sqrt{m},\sqrt{n}\,]$ be one of the five biquadratic fields of Lemma 5.4. If L is a Pólya field, each one of the three quadratic subextensions of L contains an integer with norm ± 2.*

It is an easy consequence of the following lemma:

Lemma 5.6. *Let L and K be two number fields such that $K\subset L$. Let $\mathfrak{N}$ be a maximal ideal of $\mathcal{O}_L$ and $\mathfrak{M}=\mathfrak{N}\cap\mathcal{O}_K$. If $\mathfrak{N}$ is principal and if $e(\mathfrak{N}/\mathfrak{M})=[L:K]$, then $\mathfrak{M}$ is also principal.*

Indeed, consider the norm morphism [14, Chapter I. §5]:

$$N_L^K : I(L)\mapsto I(K)$$

which is determined by its value on the maximal ideals $\mathcal{N}$ of $\mathcal{O}_L$

$$N_L^K(\mathcal{N})=\mathcal{M}^{f_{\mathcal{N}}(L/K)}$$

where $\mathcal{M}=\mathcal{N}\cap\mathcal{O}_K$ and $f_{\mathcal{N}}(L/K)=[\mathcal{O}_L/\mathcal{N}:\mathcal{O}_K/\mathcal{M}]$. We know that the morphism N_L^K generalizes the norm $N_{L/K}(x)$ of an element x and the absolute norm of an ideal:

$$N_L^K(x\mathcal{O}_L)=N_{L/K}(x)\mathcal{O}_K \quad\text{and}\quad \left|N_K^{\mathbb{Q}}(I)\right|=Card(\mathcal{O}_K/I),$$

for every $x\in L$ and every entire ideal I of K.

We come back to the proof of the previous lemma: if $\mathfrak{N}=\alpha\mathcal{O}_L$ then $N_L^K(\mathfrak{N})=\mathfrak{M}=N_{L/K}(\alpha)\mathcal{O}_K$.

Now, we can check whether some fields considered in Lemma 5.4 are Pólya fields or not. First, the field $L=\mathbb{Q}[\sqrt{2},i\,]$ is a Pólya field because its class number is 1 (see [2]). Then, we consider the imaginary biquadratic fields $\mathbb{Q}[\sqrt{-2},\sqrt{p}\,]$ and $\mathbb{Q}[i,\sqrt{2q}\,]$.

Proposition 5.7. *For all primes p such that $p\equiv 3 \pmod 4$ and all odd primes q, the fields $\mathbb{Q}[\sqrt{-2},\sqrt{p}\,]$ and $\mathbb{Q}[i,\sqrt{2q}\,]$ are not Pólya fields.*

Proof. Denote by L the field $\mathbb{Q}[\sqrt{-2},\sqrt{p}\,]$ and K the subfield $\mathbb{Q}[\sqrt{-2p}\,]$. Following Lemma 5.6, if the ideal $\Pi_2(L)$ is principal, the ideal $\Pi_2(K)$ is principal too. Since the prime 2 is ramified in $K/\mathbb{Q}$, there exists an element of $\mathcal{O}_K$ with norm ± 2. However, the equation $a^2+2pb^2=\pm 2$ has no integer solutions. Similarly, since the equation $a+2qb^2=\pm 2$ has no integer solutions, there is no ideal with norm 2 in the subfield $K'=\mathbb{Q}[\sqrt{-2q}\,]$ of $L'=\mathbb{Q}[i,\sqrt{2q}\,]$. Consequently, for each odd prime q, the field $L'=\mathbb{Q}[i,\sqrt{2q}\,]$ is not a Pólya field. □

The case of the fields $L=\mathbb{Q}[\sqrt{2},\sqrt{p}\,]$ where $p\equiv 3 \pmod 4$ may be solved by [1, Theorem 1]. Indeed, Azizi and Mouhib are interested in real biquadratic fields K such that $K=\mathbb{Q}[\sqrt{m},\sqrt{d}\,]$ with $m=2$ or m is a prime number satisfying $m\equiv 1 \pmod 4$ and d is a squarefree integer. Recall the part of their theorem corresponding to $m=2$:

Proposition 5.8. *(See [1, Theorem 1].) Let $k=\mathbb{Q}(\sqrt{2}\,)$ and $K=k(\sqrt{d}\,)$ where d is a squarefree integer. Denote by r the number of primes ideals in $k=\mathbb{Q}[\sqrt{2}\,]$ which are ramified in K and let e be such that $2^e=[\mathcal{O}_k^{\times}:N_{K/k}(K^*)\cap\mathcal{O}_k^{\times}]$. Then,*

(1) *The rank of the 2-class group $Cl_2(K)$ of K is $r-1-e$.*
(2) *If there is an odd prime number q dividing d such that $q\equiv 3 \pmod 4$, then $e=1$ or $e=2$.*
(3) *The rank of $Cl_2(K)$ is $r-2$ if and only if, for each odd prime number q dividing d, $(\frac{2}{q})=1\Rightarrow(\frac{-1}{q})=1$.*

Corollary 5.9. *The biquadratic fields $L = \mathbb{Q}[\sqrt{2}, \sqrt{p}\,]$ where $p \equiv 3 \pmod 4$ are Pólya fields.*

Proof. We use the previous proposition with $d = p \equiv 3 \pmod 4$. Here, the rank of $Cl_2(K)$ is $r-2$ or $r-3$.

When $(\frac{2}{p}) = -1$, there are $r = 2$ prime ideals of $\mathbb{Q}[\sqrt{2}\,]$ which are ramified in the extension $L/\mathbb{Q}[\sqrt{2}\,]$: the prime ideals of $\mathbb{Q}[\sqrt{2}\,]$ lying over 2 and p. The rank of the 2-class group of L is zero, in other words, the 2-class group of L is trivial. Moreover, since $2\mathcal{O}_L = \Pi_2(L)^4$, $\Pi_2(L)$ is principal.

If $(\frac{2}{p}) = 1$, then there are exactly $r = 3$ prime ideals of $\mathbb{Q}[\sqrt{2}\,]$ ramified in $L/\mathbb{Q}[\sqrt{2}\,]$: two prime ideals in $\mathbb{Q}[\sqrt{2}\,]$ lying over the prime p and the prime ideal lying over the prime 2. Since $p \equiv 3 \pmod 4$, one has $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = -1$. Following the third assertion of the previous proposition, the rank of $Cl_2(K)$ is different from $r-2$, thus it is $r-3 = 0$. The 2-class group of L is also trivial. □

Finally, we consider the last field $L = \mathbb{Q}[\sqrt{2q}, \sqrt{p}\,]$ where p and q are two distinct primes and $p \equiv 3 \pmod 4$. If we take norm equations in $\mathbb{Q}(\sqrt{2pq}\,)$, we obtain the following proposition:

Proposition 5.10. *Let p and q be two distinct prime numbers such that $p \equiv 3 \pmod 4$. If $\mathbb{Q}[\sqrt{p}, \sqrt{2q}\,]$ is a Pólya field, then*:

(1) *either $p \equiv -1 \pmod 8$ and $q \equiv 1, -1 \pmod 8$,*
(2) *or $p \equiv 3 \pmod 8$ and $q \equiv 1, 3 \pmod 8$.*

Proof. Assume that $L = \mathbb{Q}[\sqrt{p}, \sqrt{2q}\,]$ is a Pólya field, then the ideal $\Pi_2(L)$ is principal. Following Lemma 5.6, in the field $K = \mathbb{Q}[\sqrt{2pq}\,]$, the ideal $\Pi_2(K)$ is principal too. Since the prime 2 is ramified in $K/\mathbb{Q}$, there is an element in $\mathcal{O}_K$ with norm ± 2: the equation $a^2 - 2pqb^2 = \pm 2$ has a solution $(a, b) \in \mathbb{Z}^2$. We obtain:

$$\left(\frac{2}{p}\right) = \left(\frac{2}{q}\right) = 1 \quad \text{or} \quad \left(\frac{-2}{p}\right) = \left(\frac{-2}{q}\right) = 1.$$

However, $p \equiv 3 \pmod 4$ and as a consequence $p \equiv -1 \pmod 8$ or $p \equiv 3 \pmod 8$. Considering the rules of calculus with the Legendre symbol, we obtain easily the conditions about q in the proposition. □

Remark 5.11. If $p, q \equiv 3 \pmod 8$, one may compute that, for $p, q < 100$, $\mathbb{Q}[\sqrt{p}, \sqrt{2q}\,]$ is always a Pólya field. In the other cases, however, the previous conditions are not sufficient since we have, for each aforementioned condition on p and q, a couple (p, q) such that $\mathbb{Q}[\sqrt{p}, \sqrt{2q}\,]$ is not a Pólya field. For example, the fields $\mathbb{Q}[\sqrt{7}, \sqrt{62}\,]$, $\mathbb{Q}[\sqrt{7}, \sqrt{82}\,]$ and $\mathbb{Q}[\sqrt{3}, \sqrt{34}\,]$ are not Pólya fields.

The question remains open to know whether there are biquadratic Pólya fields which are not obtained by composition of two quadratic Pólya fields.

6. Sextic Pólya fields

Let K be a number field such that $K/\mathbb{Q}$ is a Galoisian extension of degree 6. Then, the Galois group $G(K/\mathbb{Q})$ is either cyclic or isomorphic to S_3.

Proposition 6.1. *Cyclic sextic Pólya fields are exactly those which are obtained by composition of a quadratic Pólya field with a cyclic cubic Pólya field.*

Proof. A cyclic sextic field K contains two non-trivial subfields: a quadratic subfield K_1 and a cyclic cubic subfield K_2. Following Proposition 1.4, the field K is a Pólya field if and only if K_1 and K_2 are Pólya field. □

Now, we consider non-Abelian sextic number fields K. The group S_3 contains only one subgroup of order 3 and three subgroups of order 2. Thus, K has only one quadratic subfield $K_1 = \mathbb{Q}[\sqrt{d}\,]$ and three conjugate cubic subfields $K_{2,k}$ $(1 \leqslant k \leqslant 3)$ over $\mathbb{Q}$. The field K is composed with K_1 and any subfield among $K_{2,k}$. The sextic field K is also the Galoisian closure of these three non-cyclic cubic fields, and conversely, the Galoisian closure of every non-cyclic cubic field is a sextic field with a Galois group isomorphic to S_3.

Here, we restrict our study to sextic fields K which contain a pure cubic field. This happens if and only if the quadratic subfield K_1 of K is the field $\mathbb{Q}[j]$. In other words, we are going to characterize Pólya fields of the form $\mathbb{Q}[j, \sqrt[3]{m}\,]$.

Theorem 6.2. *Let $m = ab^2$ where m is an integer $\geqslant 2$, a and b are squarefree and coprime. Let $L = \mathbb{Q}[j, \sqrt[3]{m}\,]$, $K_1 = \mathbb{Q}[j]$ and $K = \mathbb{Q}[\sqrt[3]{m}\,]$. The field L is a Pólya field if and only if*

- *when $a^2 \not\equiv b^2 \pmod 9$, for each prime p dividing $3m$, there is an element $\alpha \in K$ such that $N_{K/\mathbb{Q}}(\alpha) = \pm p$,*
- *when $a^2 \equiv b^2 \pmod 9$, for each prime p dividing m, there is an element $\alpha \in K$ such that $N_{K/\mathbb{Q}}(\alpha) = \pm p$.*

We begin with some useful lemmas and first give a general result:

Proposition 6.3. *Let L/K be an extension of number fields of degree n and denote by $Cl(K)_{\hat{n}}$ the subgroup of $Cl(K)$ formed by the elements whose order is coprime to n. The restriction of the morphism $\epsilon_K^L : \bar{I} \in Cl(K) \mapsto \overline{I\mathcal{O}_L} \in Cl(L)$ to the subgroup $Cl(K)_{\hat{n}}$ is injective.*

Proof. The morphism N_L^K defined in Section 5 induces the morphism:

$$\nu_L^K : \bar{\mathcal{I}} \in Cl(L) \mapsto \overline{N_L^K(\mathcal{I})} \in Cl(K).$$

The following composed application is injective:

$$\nu_L^K \circ \epsilon_{K|Cl(K)_{\hat{n}}}^L : \bar{I} \in Cl(K)_{\hat{n}} \mapsto \overline{I^n} \in Cl(K). \qquad \square$$

Lemma 6.4. *Let m be a cubefree integer $\geqslant 2$, $K = \mathbb{Q}[\sqrt[3]{m}\,]$ and $L = \mathbb{Q}[j, \sqrt[3]{m}\,]$. For every prime p dividing m, $p \neq 3$, we have*:

(1) *$\Pi_p(K)\mathcal{O}_L = \Pi_p(L)$ or $\Pi_{p^2}(L)$,*
(2) *$\Pi_p(K)$ is principal if and only if $\Pi_p(L)$ (respectively $\Pi_{p^2}(L)$) is principal.*

Proof. Let $K_1 = \mathbb{Q}[j]$. Following the decomposition of a prime number in a cyclotomic field [10, Proposition 6.4.8], we have:

- If $p \equiv 1 \pmod 3$ then $p\mathcal{O}_{K_1} = \mathfrak{m}_1\mathfrak{m}_2$ and $N(\mathfrak{m}_1) = N(\mathfrak{m}_2) = p$.
- If $p \equiv 2 \pmod 3$ then $p\mathcal{O}_{K_1} = \mathfrak{m}$ and $N(\mathfrak{m}) = p^2$.

If $p \mid m$ and $p \neq 3$, then, according to the decomposition in a pure cubic field [6, Theorem 6.4.16], p is totally ramified in $K/\mathbb{Q}$: $p\mathcal{O}_K = \mathfrak{p}^3$ and $N(\mathfrak{p}) = p$.

Thus,

- if $p \equiv 1 \pmod 3$, then $p\mathcal{O}_L = \Pi_p(L)^3$,
- if $p \equiv 2 \pmod 3$, then $p\mathcal{O}_L = \Pi_{p^2}(L)^3$.

If $p \mid m$, $p \neq 3$ and $p \equiv 1 \pmod 3$ (respectively $p \equiv 2 \pmod 3$), we obtain the equality $\Pi_p(K)\mathcal{O}_L = \Pi_p(L)$ (respectively $\Pi_p(K)\mathcal{O}_L = \Pi_{p^2}(L)$). Consequently, if the ideals $\Pi_p(K)$ are principal, the ideals

$\Pi_p(L)$ (respectively $\Pi_{p^2}(L)$) are also principal. Conversely, if the ideals $\Pi_p(L)$ (respectively $\Pi_{p^2}(L)$) are principal, using the norm morphism N_L^K, one has, if $p \equiv 1 \pmod 3$:

$$N_L^K\big(\Pi_p(L)\big) = \Pi_p(K)^2.$$

Similarly, if $p \equiv 2 \pmod 3$, then $N_L^K(\Pi_{p^2}(L)) = \Pi_p(K)^2$. In both cases, $\Pi_p(K)^2$ is principal. This means that the image of $\Pi_p(K)$ is in the subgroup $Cl(K)_{\hat{3}}$ of $Cl(K)$ formed by the elements whose order is coprime to 3. Following Proposition 6.3, we obtain that $\Pi_p(K)$ is principal. □

Lemma 6.5. *Let $m = ab^2$ be a cubefree integer $\geqslant 2$ where a and b are coprime, $K = \mathbb{Q}[\sqrt[3]{m}]$ and $L = \mathbb{Q}[j, \sqrt[3]{m}]$.*

(1) *If $a^2 \equiv b^2 \pmod 9$, the ideal $\Pi_3(L)$ is principal.*
(2) *Otherwise, $\Pi_3(K)$ is principal if and only if $\Pi_3(L)$ is principal.*

Proof. One knows that there is only one maximal ideal $\mathfrak{m}$ of $K_1 = \mathbb{Q}[j]$ with norm 3 such that $3\mathcal{O}_{K_1} = \mathfrak{m}^2 = \Pi_3(K_1)^2$. First, assume that $3\mathcal{O}_K = \mathfrak{m}_1\mathfrak{m}_2^2$ where $N(\mathfrak{m}_i) = 3$. Following [6, Theorem 6.4.16], this happens if and only if $a^2 \equiv b^2 \pmod 9$. The extension $L/\mathbb{Q}$ is a Galoisian sextic extension, the only possible decomposition of the prime 3 in L is the following one:

$$3\mathcal{O}_L = (\mathfrak{n}_1\mathfrak{n}_2\mathfrak{n}_3)^2 \quad \text{where } N(\mathfrak{n}_i) = 3.$$

Since the extension L/K_1 is Galoisian, one has

$$\mathfrak{m}\mathcal{O}_L = \Pi_3(K_1)\mathcal{O}_L = \Pi_3(L) = \mathfrak{n}_1\mathfrak{n}_2\mathfrak{n}_3.$$

Since K_1 is a cyclotomic field, K_1 is a Pólya field (see [17]). As a consequence, $\Pi_3(K_1)$ is principal and $\Pi_3(L)$ too.

Assume that $3\mathcal{O}_K = \mathfrak{p}^3 = \Pi_3(K)^3$. Following [6, Theorem 6.4.16], this happens if and only if $a^2 \not\equiv b^2 \pmod 9$. In this case, $3\mathcal{O}_L = \mathfrak{n}^6$. Since the extensions L/K and L/K_1 are Galoisian, we have:

$$\mathfrak{m}\mathcal{O}_L = \Pi_3(K_1)\mathcal{O}_L = \Pi_3(L)^3 = \mathfrak{n}^3,$$
$$\mathfrak{p}\mathcal{O}_L = \Pi_3(K)\mathcal{O}_L = \Pi_3(L)^2 = \mathfrak{n}^2.$$

Since $\Pi_3(K_1)$ is principal, $\Pi_3(L)^3$ is also principal. Thus, $\Pi_3(L)$ is principal if and only if $\Pi_3(L)^2$ is principal. But, if $\Pi_3(K)$ is principal, since $\Pi_3(K)\mathcal{O}_L = \Pi_3(L)^2$, the ideal $\Pi_3(L)^2$ is principal too. Conversely, suppose that $\Pi_3(L)^2$ is principal, then the ideal $N_L^K(\Pi_3(L)^2) = N_L^K(\Pi_3(K)\mathcal{O}_L) = \Pi_3(K)^2$ is principal, the equality $3\mathcal{O}_K = \Pi_3(K)^3$ implies that $\Pi_3(K)$ is also principal. Thus, $\Pi_3(L)^2$ is principal if and only if $\Pi_3(K)$ is principal. □

Proof of Theorem 6.2. The only prime which ramifies in $K_1/\mathbb{Q}$ is 3, the primes which are ramified in $K_2/\mathbb{Q}$ are 3 and the prime divisors of m. Their decompositions are studied in the two previous lemmas. The prime numbers distinct from 3 and from the divisors of m are not ramified in $K_1/\mathbb{Q}$, nor in $K_2/\mathbb{Q}$, nor, a fortiori [11, Lemma 4.1], in $L = K_1K_2$. Since the extension $L/\mathbb{Q}$ is Galoisian, the ideals $\Pi_q(L)$ lying over these primes are principal (see [5, Proposition 3.1]). □

Corollary 6.6. *Let p be a prime number. The field $\mathbb{Q}[j, \sqrt[3]{p}]$ is a Pólya field if and only if*

- *either $p^2 \equiv 1 \pmod 9$,*
- *or there is an integer of $\mathbb{Q}[\sqrt[3]{p}]$ with norm ± 3.*

Proof. The prime p is totally ramified in $\mathbb{Q}[\sqrt[3]{p}]/\mathbb{Q}$ and:

- if $p \equiv 1 \pmod 3$, then $p\mathcal{O}_L = \Pi_p(L)^3$ and $\Pi_p(L) = \sqrt[3]{p}\mathcal{O}_L$,
- if $p \equiv 2 \pmod 3$, then $p\mathcal{O}_L = \Pi_{p^2}(L)^3$ and $\Pi_{p^2}(L) = \sqrt[3]{p}\mathcal{O}_L$.

Thus $\mathbb{Q}[j, \sqrt[3]{p}]$ is a Pólya field if and only if when $p^2 \not\equiv 1 \pmod 9$, the ideal $\Pi_3(K_2)$ is principal, that is equivalent with the existence of an integer of $\mathbb{Q}[\sqrt[3]{p}]$ with norm ± 3. □

Recall that we know bases of the ring of integers of a pure cubic field:

Proposition 6.7. *(See [6, Theorem 6.4.13].) Let $K = \mathbb{Q}[\sqrt[3]{m}]$ be a pure cubic field, where $m \geqslant 2$ is a cubefree integer. Write $m = ab^2$ where a, b are squarefree and coprime and let $\theta = \sqrt[3]{m}$.*

(1) *If $a^2 \not\equiv b^2 \pmod 9$, then $(1, \theta, \frac{\theta^2}{b})$ is a basis of $\mathcal{O}_K$.*
(2) *If $a^2 \equiv b^2 \pmod 9$, then $(1, \theta, \frac{\theta^2 + m\theta + b^2}{3b})$ is a basis of $\mathcal{O}_K$.*

If $m = p$ where p is a prime number and $p^2 \not\equiv 1 \pmod 9$, a basis of the ring of integer of $\mathbb{Q}[\sqrt[3]{p}]$ is $(1, \sqrt[3]{p}, (\sqrt[3]{p})^2)$. An integer $\alpha = a + b\sqrt[3]{p} + c(\sqrt[3]{p})^2$ has norm $N(\alpha) = a^3 + p(b^3 + pc^3 - 3abc)$. Thus, if $\mathcal{O}_K$ has an element with norm 3, then 3 is a cube modulo p.

Example 6.8. For $p = 7$, we easily check that ± 3 is not a cube modulo 7. Consequently $\Pi_3(K_2)$ is not principal. Moreover, $K = \mathbb{Q}[\sqrt[3]{7}]$ has a class number 3. Thus $Po(K) = Cl(K) \simeq \mathbb{Z}/3\mathbb{Z}$ and the Pólya group of $\mathbb{Q}[j, \sqrt[3]{7}]$ is isomorphic to $\mathbb{Z}/3\mathbb{Z}$.

Example 6.9. For $p = 17$, $17^2 \equiv 1 \pmod 9$, the field $\mathbb{Q}[j, \sqrt[3]{17}]$ is a Pólya field.

References

[1] A. Azizi, A. Mouhib, Sur le rang du 2-groupe de classes de $\mathbb{Q}[\sqrt{m}, \sqrt{n}]$ où $m = 2$ ou un premier $p \equiv 1 \pmod 4$, Trans. Amer. Math. Soc. 353 (2001) 2741–2752.
[2] E. Brown, C.J. Parry, The imaginary bicyclic biquadratic fields with class-number 1, J. Reine Angew. Math. 266 (1974) 118–120.
[3] A. Brumer, M. Rosen, Class number and ramification in number fields, Nagoya Math. J. 23 (1963) 97–101.
[4] P.J. Cahen, J.L. Chabert, Integer-Valued Polynomials, Math. Surveys Monogr., vol. 48, Amer. Math. Soc., Providence, 1997.
[5] J.L. Chabert, Factorial groups and Pólya groups in Galoisian extensions of $\mathbb{Q}$, in: Commutative Ring Theory and Applications, in: Lect. Notes Pure Appl. Math., vol. 231, Dekker, New York, 2003, pp. 77–86.
[6] H. Cohen, A Course in Computational Algebraic Number Theory, Springer, 2000.
[7] D.A. Garbanati, Units with norm -1 and signatures of units, J. Reine Angew. Math. 283/284 (1976) 164–175.
[8] K. Hardy, R.H. Hudson, D. Richman, K.S. Williams, N.M. Holtz, Calculation of class numbers of imaginary cyclic quartic fields, Carleton-Ottawa Math. Lecture Note Ser. 7 (1986), 201 pp.
[9] D. Hilbert, Die Theorie der algebraischen Zahlkörper, Jahresber. Deutsch. Math.-Verein. 4 (1894–95) 175–546.
[10] H. Koch, Number Theory, Grad. Stud. Math., A.M.S., 2000.
[11] A. Leriche, Pólya fields, Pólya groups and Pólya extensions: A question of capitulation, J. Theor. Nombres Bordeaux 23 (2011) 235–249.
[12] A. Ostrowski, Über ganzwertige Polynome in algebraischen Zahlkörpern, J. Reine Angew. Math. 149 (1919) 117–124.
[13] G. Pólya, Über ganzwertige Polynome in algebraischen Zahlkörpern, J. Reine Angew. Math. 149 (1919) 97–116.
[14] J.P. Serre, Corps Locaux, Hermann, Paris, 1962.
[15] B.K. Spearman, K.S. Williams, The conductor of a cyclic quartic field using Gauss sums, Czechoslovak Math. J. 47 (1997) 453–462.
[16] K.S. Williams, Integers of biquadratic fields, Canad. Math. Bull. 13 (1970) 519–526.
[17] H. Zantema, Integer valued polynomials over a number field, Manuscripta Math. 40 (1982) 155–203.