KUMMER EXTENSIONS AND PÔLYA FIELDS

GÉRARD KIENTEGA¹, THÉODORE TAPSOBA², CHARLES WEND-WAOGA TOUGMA³∗

ABSTRACT. A number field is called a Pólya field if the module of integer-valued polynomials over its ring of integers has a regular basis. Let \( a \in \mathbb{Z}, a \neq 0 \) and \( p \geq 3 \) be a prime number. In this paper, we characterize the number fields of the form \( \mathbb{Q}(\zeta_p, p\sqrt{a}) \) which are Pólya fields. We hence generalize results of [9]. New bounds for the number of ramified prime numbers in these fields are derived.

1. Introduction

1.1. Notations. Throughout this paper, if \( K \) is a number field, \( \mathbb{Z}_K \) is its ring of integers, \( U_K \) its units group and \( \mathcal{I}_K \) its group of fractional ideals. We denote by \( h_K \) the class number of \( K \). Let \( q \) be a prime number. \( \Pi_q(K) \) is the product of all maximal (prime) ideals of \( K \) with norm \( q^f, f \in \mathbb{N} \). If \( q^f \) is not a norm of an ideal, then \( \Pi_q(K) = \mathbb{Z}_K \). Finally, by \( (r,s) \) we mean the gcd of \( r \) and \( s \) with \( r,s \in \mathbb{Z} \). The same notation will be used for ideals. We note also \( r \mid s \) when \( r \) divides \( s \).

1.2. A result of Amandine Leriche. In the 1910’s, Pólya [11] and Ostrowski [10] had introduced the ring of integers valued polynomials on the ring \( \mathbb{Z}_K \) of integers of the number field \( K \):
\[
\text{Int}(\mathbb{Z}_K) = \{ P \in K[X], P(\mathbb{Z}_K) \subset \mathbb{Z}_K \}
\]
Pólya was interested by number fields \( K \) whose \( \mathbb{Z}_K \)-module \( \text{Int}(\mathbb{Z}_K) \) has a regular basis \( (f_n)_{n} \), which means that \( (f_n)_{n} \) is a basis of \( \text{Int}(\mathbb{Z}_K) \) such that \( \deg(f_n) = n \), for all \( n \in \mathbb{N} \). For each \( n \in \mathbb{N} \), the leading coefficients of the polynomials in \( \text{Int}(\mathbb{Z}_K) \) of degree \( n \) together with \( 0 \) form a fractional ideal denoted by \( \mathfrak{J}_n(K) \). Pólya proved that \( K \) has the above propriety if and only if \( \mathfrak{J}_n(K) \) is a principal ideal for each \( n \in \mathbb{N} \). Ostrowski showed just after Pólya that this propriety is satisfied if and only if the ideals \( \Pi_{q^f}, f \in \mathbb{N} \) are principal.
It is Zantema that in 1982, called these fields Pólya fields. In his 1982’s work [15], he gave a cohomological interpretation of Pólya fields that are Galois extension of \( \mathbb{Q} \) and showed that all cyclotomic fields are Pólya fields.
After Zantema’s results on cyclotomic fields, Kummer extensions seem like a
natural choice. In [9] and [8], Leriche gave a description of Pólya fields of the form $\mathbb{Q}(j, \sqrt{a})$ in terms of the subfield $\mathbb{Q}(\sqrt{a})$:

**Theorem 1.1** ([9], Theorem 6.2 or [8], Prop 3.7.). Let $a = bc^2$ where $a$ is an integer $\geq 2$, $b$ and $c$ square free and coprime. Let $M = \mathbb{Q}(j, \sqrt{a})$, $L = \mathbb{Q}(j)$ and $K = \mathbb{Q}(\sqrt{a})$. The field $M$ is a Pólya field if and only if:

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

**Corollary 1.2** ([9], Corollary 6.6 or [8], Cr. 3.10.). Let $q$ be a prime number. The field $\mathbb{Q}(j, \sqrt{q})$ is a Pólya field if and only if:

- either $q^2 \equiv 1 \mod 9$
- or there is an integer of $\mathbb{Q}(\sqrt{q})$ with norm $\pm 3$.

In this paper, we propose to generalize these results of Leriche to the fields $\mathbb{Q}(\zeta_p, \sqrt{a})$, $p \geq 3$, $a \in \mathbb{Z}$. We also improve the bounds of the ramified numbers in these fields and we apply them to refine Theorem 1.1.

2. Preliminaries

Let $K/F$ be an extension of number fields. If $\mathfrak{q}$ is a maximal ideal of $\mathbb{Z}_F$ and $\mathfrak{O}$ is a maximal ideal of $K$ lying over $\mathfrak{q}$, we denote by $e(\mathfrak{O}/\mathfrak{q})$ and $f(\mathfrak{O}/\mathfrak{q})$ the ramification index and the residue degree of $\mathfrak{O}$ over $\mathfrak{q}$. If $I \in \mathcal{I}_K \cap \mathbb{Z}_K$, $\text{Rac}(I)$ is the product of all prime ideals of $K$ dividing $I$.

Suppose now that $F$, $K$, $L$ and $M$ are number fields such that $F = K \cap L$ and $M = KL$. Let $\mathfrak{q}$, $\mathfrak{O}$, $\mathfrak{P}$ and $\mathfrak{M}$ be respectively prime ideals of $F$, $K$, $L$ and $M$ such that $\mathfrak{M} \cap K = \mathfrak{O}$, $\mathfrak{M} \cap L = \mathfrak{P}$, $\mathfrak{M} \cap F = \mathfrak{q}$ and $\mathfrak{M} \cap \mathbb{Q} = q\mathbb{Z}$.

\[
\begin{array}{ccc}
\mathfrak{O} & \longrightarrow & M = KL \\
\downarrow & & \downarrow \\
K & \longrightarrow & L \\
\downarrow & & \downarrow \\
F & \longrightarrow & \mathfrak{q} \\
\downarrow & & \downarrow \\
\mathbb{Q} & \longrightarrow & q\mathbb{Z}
\end{array}
\]  

(2.1)

Recall that $\mathcal{N}_{M/K}(\mathfrak{M}) = \mathfrak{O}^{(\mathfrak{M}/\mathfrak{O})}$ is the relative norm of $\mathfrak{M}$ over $K$. If $I \in \mathcal{I}_M$ then

\[
I = \prod_i \mathfrak{M}_i^{e_i}
\]

with $e_i \in \mathbb{Z}$ and $\mathfrak{M}_i$ prime ideals of $M$. As $\mathcal{I}_M$ is a multiplicative group generated by the prime ideals of $M$, if $\mathfrak{O}_i = \mathfrak{M}_i \cap K$ and $f_i = f(\mathfrak{M}_i/\mathfrak{O}_i)$ then

\[
\mathcal{N}_{M/K}(I) = \prod_i \mathfrak{O}_i^{e_if_i}
\]
Lemma 2.1. With the above notations,

1) \( e(M/q) \) is divisible by the least common multiple of \( e(\Omega/q) \) and \( e(\mathfrak{P}/q) \)
2) If \( K/Q \) or \( L/Q \) is galoisian, then \( e(M/q) \) divides \( e(\Omega/q) e(\mathfrak{P}/q) \)
3) If \( K/Q \) or \( L/Q \) is galoisian and if \( (e(\Omega/q), e(\mathfrak{P}/q)) = 1 \) then \( e(M/q) = e(\Omega/q) e(\mathfrak{P}/q) \)

Proof. See [8], Lemma 2.19, p.41.

Lemma 2.2. If \( M/Q \) is galoisian, then the following assertions are equivalent:

1) \( M \) is a Pólya field
2) For each prime number \( q \) and for each \( f \in \mathbb{N} \), \( \Pi_q f(M) \) is a principal ideal.
3) For each ramified prime number \( q \) and for each \( f \in \mathbb{N} \), \( \Pi_q f(M) \) is a principal ideal.
4) For each ramified prime number \( q \), \( \text{Rac}(q\mathbb{Z}_M) \) is a principal ideal.
5) For each ramified prime number \( q \), \( \text{Rac}(q\mathbb{Z}_M) \) is a principal ideal.

Proof. 1) \( \iff \) 2) is Ostrowski’s result\(^1\). Other equivalences are Ostrowski’s results in the galoisian case. Indeed, in a galoisian extension, all prime ideals lying over \( q \) have the same residue degree \( f = f(q) \). Hence \( \text{Rac}(q\mathbb{Z}_M) = \Pi_q f(M) \). This shows that assertions 2) and 4) are equivalent. If \( q \) is not ramified in \( M \), then \( \text{Rac}(q\mathbb{Z}_M) = \Pi_q f(M) = q\mathbb{Z}_M \) and hence \( \text{Rac}(q\mathbb{Z}_M) \) is a principal ideal showing that assertions 2), 3) and 5) are equivalent.

Remark 2.3. If \( M/Q \) is not galoisian, Lemma 2.2 is not necessary true.

From now on, throughout the paper \( p \geq 3 \) and \( q \geq 2 \) will be prime numbers; \( a > 1 \) a \( p \)-th power free integer, \( \zeta_p \) a \( p \)-th primitive root of unit, \( L = \mathbb{Q}(\zeta_p) \). The polynomial \( X^p - a \) has a unique real root. We denote this root by \( \sqrt[p]{a} \). We set \( K = \mathbb{Q}(\sqrt[p]{a}) \) and \( M = KL = \mathbb{Q}(\zeta_p, \sqrt[p]{a}) \) as in the following diagram

\[
\begin{array}{c}
K = \mathbb{Q}(\sqrt[p]{a}) \\
\mathbb{Q} \\
M = \mathbb{Q}(\zeta_p, \sqrt[p]{a}) \\
L = \mathbb{Q}(\zeta_p)
\end{array}
\]

Lemma 2.4. \( p \) is totally ramified in \( L \):

\[ p\mathbb{Z}_L = (1 - \zeta_p)^{p-1}\mathbb{Z}_L. \]

Proof. See [1], Lemma 3, p.87

It is well known that \( p \) is the only ramified prime number in \( L \) (see [12], p.90). The ramified prime numbers in \( K \) are those that divide \( pa \). Westlund’s following Theorem [14] gives their decomposition in \( K \).

\(^1\)See Introduction
Theorem 2.5 (Westlund). The integer $a$ may be expressed in one way only in the form $a = a_1a_2^2 \ldots a_{p-1}^{p-1}$ where $a_1, a_2, \ldots, a_{p-1}$ are relatively prime and are not divisible by the square of a prime number. Let $b = a_1a_2^2 \ldots a_{p-2}^{p-2} = \frac{a}{a_{p-1}^{p-1}}$ and $d = b^{p-1} - a_{p-1}^{p-1}$. Then

1) $qZ_K = \Omega^p$ if $q$ is a prime number such that $q \mid a$

2) If $(p, a) = 1$ then
   - $pZ_K = \Omega^p$ if $d \neq 0 \mod p^2$
   - $pZ_K = \Omega_1^{p-1} \Omega_2$ if $d \equiv 0 \mod p^2$.

Proof. [14], p.389-391.

Lemma 2.6. With the notations of the previous Theorem, the following assertions are equivalent.

1) $d \equiv 0 \mod p^2$
2) $a^{p-1} \equiv 1 \mod p^2$

Proof.
1) $\Rightarrow$ 2): $d \equiv 0 \mod p^2 \Rightarrow b^{p-1} - a_{p-1}^{p-1} \equiv 0 \mod p^2$. It is clear that $a_{p-1}^{p-1} \equiv 0 \mod p^2 \Rightarrow p \mid a_{p-1}$ since $p$ is an odd prime. Thus if we suppose that $a_{p-1}^{p-1} \equiv 0 \mod p^2$ then $p \nmid b$ since $a_1, a_2, \ldots, a_{p-1}$ are relatively primes. $(a_{p-1}^{p-1} \equiv 0 \mod p^2$ and $p \nmid b) \Rightarrow d = b^{p-1} - a_{p-1}^{p-1} \not\equiv 0 \mod p^2$ and this contradicts our hypothesis. So, we may assume that $a_{p-1}^{p-1} \not\equiv 0 \mod p^2$.

$d \equiv 0 \mod p^2 \Leftrightarrow a_{p-1}^{p-1} - a_{p-1}^{p(p-1)} \equiv 0 \mod p^2$ since the multiplicative group of $\mathbb{Z}/p^2\mathbb{Z}$ has order $p(p-1)$.

2) $\Rightarrow$ 1): We have $a_{p-1}^{p-1} \equiv 0 \mod p^2$ (this is equivalent to $p \nmid a_{p-1}$). In fact if $a_{p-1}^{p-1} \equiv 0 \mod p^2$ then $a \equiv 0 \mod p^2$ because $a_{p-1}^{p-1}$ divides $a$: which is absurd since by hypothesis $a_{p-1}^{p-1} \equiv 1 \mod p^2$. First, one has $d = b^{p-1} - a_{p-1}^{p-1} = \frac{a_{p-1}^{p-1}}{a_{p-1}^{(p-1)^2}}$.

Corollary 2.7. Under the hypothesis of Theorem 1.1, the following assertions are equivalent:

1) $b^2 \equiv c^2 \mod 9$
2) $a^2 \equiv 1 \mod 9$

Westlund[14] also found an integral basis of $K = \mathbb{Q}(\sqrt{a})$. 
Theorem 2.8 (Westlund). Let $\alpha_i = \sqrt[p]{\beta_i}$ where $\beta_i$ is the $p$-th power free part of $a^i$.
Let $b$ and $d$ be as in the Theorem 2.5 and $\gamma = \frac{\alpha_1^{p-1} + \alpha_1^{p-2}b + \cdots + \alpha_1b^{p-2} + 1}{p}$.

An integral basis of $K$ is
1) $(1, \alpha_1, \ldots, \alpha_{p-1})$ if $d \not\equiv 0 \pmod{p^2}$
2) $(\gamma, \alpha_1, \ldots, \alpha_{p-1})$ if $d \equiv 0 \pmod{p^2}$

Theorem 2.9 (Hilbert). Let $\mu \in L$ such that $X^p - \mu$ is irreducible over $L$. Assume that $\mathfrak{P}$ is a prime ideal of $L$ such that $\mathfrak{P} \mid p\mathbb{Z}_L$ and $(\mu, \mathfrak{P}) = 1$. Then in $M$,
1) $\mathfrak{P}$ splits completely into $p$ factors, $\mathfrak{P}\mathbb{Z}_M = \mathfrak{M}_1 \cdots \mathfrak{M}_p$ iff $\mu \equiv \xi^p \pmod{\mathfrak{P}^{p+1}}$
2) $\mathfrak{P}$ remains prime: $\mathfrak{P}\mathbb{Z}_M = \mathfrak{M}$ iff $\mu \not\equiv \xi^p \pmod{\mathfrak{P}^{p+1}}$ and $\mu \equiv \xi^p \pmod{\mathfrak{P}^p}$
3) $\mathfrak{P}$ becomes the $p$-th power of a prime ideal: $\mathfrak{P}\mathbb{Z}_M = \mathfrak{M}^p$ iff $\mu \not\equiv \xi^p \pmod{\mathfrak{P}^p}$

Proof. [13], Theorem 1.1, p.589.

Theorem 2.10. If $q\mathbb{Z}_K = \Omega^p$ then the following assertions are equivalent:
1) $\Omega = \text{Rac}(q\mathbb{Z}_K)$ is a principal ideal
2) $\text{Rac}(q\mathbb{Z}_M)$ is a principal ideal.

Proof. 1) $\implies$ 2): i) $q \not\equiv p$: $q$ is not ramified in $\mathbb{Z}_L$ since $p$ is the only ramified prime number in $L$. Hence by Lemma 2.1, $\Omega$ is not ramified in $\mathbb{Z}_M$. So we have $\text{Rac}(q\mathbb{Z}_M) = \text{Rac}(\Omega\mathbb{Z}_M) = \Omega\mathbb{Z}_M$. Thus if $\Omega$ is a principal ideal then $\text{Rac}(q\mathbb{Z}_M)$ is a principal ideal.

ii) $q = p$: By Lemma 2.4, $p\mathbb{Z}_L = (1 - \zeta_p)^{p-1}\mathbb{Z}_L$. Lemma 2.1, shows that there exists a prime ideal $\mathfrak{M}$ of $\mathbb{Z}_M$ such that $p\mathbb{Z}_M = \mathfrak{M}^{p^{p-1}}$. Hence we have $\text{Rac}(p\mathbb{Z}_M) = \mathfrak{M}$. It follows that $\Omega\mathbb{Z}_M = \mathfrak{M}^{p-1}$ and $(1 - \zeta_p)\mathbb{Z}_M = \mathfrak{M}^p$. So $\mathfrak{M}^{p-1}$ and $\mathfrak{M}^p$ are principal ideals. As $\mathfrak{M} = \mathfrak{M}^{p^{p-1}}$ then $\mathfrak{M}$ is a principal ideal.

2) $\implies$ 1): $M/K$ is galoisian since $M/Q$ is galoisian. Thus $\Omega\mathbb{Z}_M = (\mathfrak{M}_1 \cdots \mathfrak{M}_r)^e$ with $ref = [M : K] = (p - 1)$. Hence: $\Omega^{p-1} = \Omega^{ref} = N_{M/K}(\Omega\mathbb{Z}_M) = N_{M/K}((\text{Rac}(q\mathbb{Z}_M))^e) = N_{M/K}((\text{Rac}(q\mathbb{Z}_M))^e)\mathbb{Z}_K$. Thus $\Omega^{p-1}$ is a principal ideal because the relative norm of a principal ideal is a principal ideal. Since by hypothesis, $\Omega^p$ is a principal ideal, then $\Omega = \Omega^p (\Omega^{p-1})^{-1}$ is a principal ideal.

3. POLYA fields of the form $\mathbb{Q}(\zeta_p, \sqrt[p]{a})$

With the notations of the previous sections, the following result generalizes Theorem 1.1. Recall that $M = \mathbb{Q}(\zeta_p, \sqrt[p]{a})$ and $K = \mathbb{Q}(\sqrt[p]{a})$.

Theorem 3.1. $M$ is a Pólya field if and only if:

- when $a^{p-1} \not\equiv 1 \pmod{p^2}$, for each prime $q$ dividing $pa$, there is an algebraic integer $\omega \in K$ such that $N_{K/\mathbb{Q}}(\omega) = q$.
- when $a^{p-1} \equiv 1 \pmod{p^2}$, for each prime $q$ dividing $a$, there is an algebraic integer $\omega \in K$ such that $N_{K/\mathbb{Q}}(\omega) = q$.

Proof. We look at diagram 2.2: the ramified prime numbers in $M$ are those dividing $pa$. Indeed by Lemma 2.1, $q$ is ramified in $M$ iff it is ramified at least in
one of the extensions \( L \) or \( K \), thus \( q \) is ramified in \( M \) if and only if it is ramified in \( K \) since \( p \) is ramified in \( K \) and is the only ramified prime number in \( L \).

By Lemma 2.2, \( M \) is a Polya field iff for each ramified prime number \( q \), \( \text{Rac}(q\mathbb{Z}_M) \) is a principal ideal. By Theorem 2.5 and Lemma 2.6,

i) if \( a^{p-1} \not\equiv 1 \pmod{p^2} \) and \( q \mid pa \) then \( q\mathbb{Z}_K = \mathcal{O}_p \)

ii) if \( a^{p-1} \equiv 1 \pmod{p^2} \) then

\[
q\mathbb{Z}_K = \mathcal{O}_p \text{ if } q \mid a, \; q \not\equiv p \\
P\mathbb{Z}_K = \mathcal{O}_p^{1-\delta} \mathcal{O}_2.
\]

In case i), Theorem 2.10 implies that \( \mathcal{O} = \text{Rac}(q\mathbb{Z}_K) \) is a principal ideal if \( q \mid pa \). Hence there exists \( \omega \in \mathbb{Z}_K \) such that \( \mathcal{O} = \omega\mathbb{Z}_K \). Taking norm, it is equivalent to \( N_{K/Q}(\omega) = \pm q \). If \( N_{K/Q}(\omega) = -q \), one takes \( \omega' = -\omega \) and we then have \( N_{K/Q}(\omega') = q \) since \( p \) is odd.

In case ii), the previous approach is valid for all prime numbers \( q \) dividing \( a \). Now, look what happens to \( \text{Rac}(q\mathbb{Z}_K) \).

By Theorem 2.5, \( P\mathbb{Z}_K = \mathcal{O}_p^{1-\delta} \mathcal{O}_2 \). On the other hand, \( P\mathbb{Z}_L = (1 - \zeta_p)^{p-1}\mathbb{Z}_L \) by Lemma 2.4. Only the decomposition 1) of Theorem 2.9 must hold. Indeed, since \( P\mathbb{Z}_L = (1 - \zeta_p)^{p-1}\mathbb{Z}_L \), it suffices to factorize \( (1 - \zeta_p)\mathbb{Z}_L \) in \( M \). We have \( a^{p-1} \equiv 1 \pmod{p^2} \) hence \( (p, a) = 1 \). Thus \( ((1 - \zeta_p)\mathbb{Z}_L, a\mathbb{Z}_L) = 1 \) since \( (1 - \zeta_p)\mathbb{Z}_L \) divides \( P\mathbb{Z}_L \). So we can apply Theorem 2.9. In decomposition 2) and 3) of this Theorem, there is only one prime ideal of \( M \) lying over \( (1 - \zeta_p)\mathbb{Z}_L \) thus only one prime ideal of \( M \) lying over \( p \): this is impossible since by Theorem 2.5, there are already two primes ideals lying over \( p \) in \( K \subset M \). Hence it remains only the decomposition 1) of Theorem 2.9: \( (1 - \zeta_p)\mathbb{Z}_L \) splits completely in \( M \) and thus \( \text{Rac}(P\mathbb{Z}_M) = \text{Rac}((1 - \zeta_p)\mathbb{Z}_M) = (1 - \zeta_p)\mathbb{Z}_M \). \( \square \)

Remark 3.2. Lerche’s result (Theorem 1.1) deals with \( \omega \in K \) but her proof shows clearly that \( \omega \) must be an algebraic integer. We obtain this Theorem by taking \( p = 3 \) and \( a = bc^2 \). It follows from Corollary 2.7, that the assertions \( a^2 \equiv 1 \pmod{9} \) and \( b^2 \equiv c^2 \pmod{9} \) are equivalent.

It is well known that the norm form equation \( N_{K/Q}(\omega) = q \) in our previous Theorem is difficult to solve in general. Our following result gives simple necessary conditions for \( M \) to be a Polya field based only on congruence relations. Before, define the radical of \( a \) to be

\[
r(a) = \prod_{p\mid a} p
\]

ie, the product of all the prime numbers dividing \( a \), taken with multiplicity 1 (see [7], p.196).

Corollary 3.3. If \( M = \mathbb{Q}(\zeta_p, \sqrt[3]{a}) \) is a Polya field then:

- when \( a^{p-1} \not\equiv 1 \pmod{p^2} \), for each prime number \( q \) dividing \( pa \), we have \( q \equiv u^p \pmod{p^2} \) for each prime number \( q \) dividing \( a \), we have \( q \equiv u \pmod{p} \) with \( u \in \mathbb{Z} \)

Proof. Let \( \omega \in \mathbb{Z}_K \). By Theorem 2.8, we have:

- \( \omega = x_0 + x_1\alpha_1 + \cdots + x_{p-1}\alpha_{p-1} \) where \( x_i \in \mathbb{Z} \) if \( a^{p-1} \not\equiv 1 \pmod{p^2} \) (\( \Leftrightarrow d \neq 0 \pmod{p^2} \) by Lemma 2.6)
The converse is false, i.e.

\[ \omega = x_0 \gamma + x_1 \alpha_1 + \cdots + x_{p-1} \alpha_{p-1} \] where \( x_i \in \mathbb{Z} \) if \( a^{p-1} \equiv 1 \mod p^2 \).

Thus:

- \( \omega - x_0 = x_1 \alpha_1 + \cdots + x_{p-1} \alpha_{p-1} \) if \( a^{p-1} \not\equiv 1 \mod p^2 \)
- \( p\omega - x_0 = x_0 (a^{p-1} + b \alpha_1^{p-2} + \cdots + b^{p-2} \alpha_1) + p(x_1 \alpha_1 + \cdots + x_{p-1} \alpha_{p-1}) \) if \( a^{p-1} \equiv 1 \mod p^2 \)

If \( \sigma \) is an embedding of \( K \) in \( \mathbb{C} \) then

\[ \sigma(\alpha_i) = \sigma(\sqrt[p]{\beta_i}) = \zeta_p^i \sqrt[p]{\beta_i} \quad (K = \mathbb{Q}(\sqrt[p]{a}) = \mathbb{Q}(\sqrt[p]{\beta_i})). \]

Thus let:

- \( \theta = \omega \) if \( a^{p-1} \not\equiv 1 \mod p^2 \)
- \( \theta = p\omega \) if \( a^{p-1} \equiv 1 \mod p^2 \)

Then:

\[ N_{K/Q}(\theta) = x_0^p + r(a)z \quad \text{with} \quad z \in \mathbb{Z} \]

Indeed, we have:

\[ N_{K/Q}(\theta) - x_0^p \in (\alpha_1, \cdots, \alpha_{p-1}) \mathbb{Z}_M = \left( \sqrt[p]{\beta_1}, \cdots, \sqrt[p]{\beta_{p-1}} \right) \mathbb{Z}_M \]

As \( N_{K/Q}(\theta) - x_0^p \in \mathbb{Z} \) and \( (\sqrt[p]{\beta_i}) \mathbb{Z}_M \cap \mathbb{Z} = \beta_i \mathbb{Z} \) then

\[ N_{K/Q}(\theta) - x_0^p \in (\beta_1, \cdots, \beta_{p-1}) \mathbb{Z} \]

By definition of \( \beta_i \), it follows that \( r(a) \mid \beta_i \) for all \( i \). Hence we have:

\[ N_{K/Q}(\theta) - x_0^p \in r(a)\mathbb{Z} \]

- \( N_{K/Q}(\theta) = N_{K/Q}(\omega) \) if \( a^{p-1} \not\equiv 1 \mod p^2 \)
- \( N_{K/Q}(\theta) = p^u N_{K/Q}(\omega) \) if \( a^{p-1} \equiv 1 \mod p^2 \)

If \( a^{p-1} \equiv 1 \mod p^2 \) then \( p \nmid a \), so \( p^u \) is invertible modulo \( r(a) \). Thus

\[ N_{K/Q}(\omega) - u^p \mod r(a) \quad \text{with} \quad u \in \mathbb{Z} \]

The corollary now follows from Theorem 3.1.

**Remark 3.4.** The necessary conditions of Corollary 3.3 holds if \( K \) is a Pólya field since if \( K \) is a Pólya field then \( M \) is also a Pólya field. Indeed, it follows from Theorem 2.5 that \( \Pi_q(K) = \text{Rac}(q \mathbb{Z}_K) \) if \( q \mid p^2 \). Thus by Ostrowski’s result, \( \text{Rac}(q \mathbb{Z}_K) \) must be a principal ideal if \( q \mid p^2 \) since \( K \) is a Pólya field. The proof of the Theorem 3.1 shows that if \( a^{p-1} \not\equiv 1 \mod p^2 \) and \( q \mid p^2 \) then the assertions \( (\text{Rac}(q \mathbb{Z}_K) \) is a principal ideal) and \( \text{there is } \omega \in \mathbb{Z}_K \text{ such that } N_{K/Q}(\omega) = q \) are equivalent.

*The converse is false, i.e \( M \) must be a Pólya field whithout \( K \): let \( K = \mathbb{Q}(\sqrt[p]{\Pi}) \) and \( M = \mathbb{Q}(j, \sqrt[p]{\Pi}) \). We have \( 11^2 \not\equiv 1 \mod 9, N_{K/Q}(\sqrt[p]{\Pi}) = 11 \), and \( N_{K/Q}(\sqrt[p]{\Pi}) = 11 \) and \( N_{K/Q}(\sqrt[p]{\Pi}) = 3 \). Thus, by Theorem 3.1, \( M \) is a Pólya field. According to Zantema, \( K \) is a Pólya field iff \( h_K = 1 \) since \( K \) is a \( S_3 \)-field (see [15], Theorem 1.1). But table from [6] shows that \( h_K = 2 \).

**Corollary 3.5.** If \( \mathbb{Q}(\zeta_p, \sqrt[p]{q}) \) is a Pólya field then:

- either \( q^{p-1} \equiv 1 \mod p^2 \)
- or \( p \equiv u^p \mod q \) with \( u \in \mathbb{Z} \)

**Proof.** A direct application of the previous Corollary on \( \mathbb{Q}(\zeta_p, \sqrt[p]{q}) \).
We now give some sufficient conditions for $M$ to be a Pólya field.

**Corollary 3.6.** If $p \nmid h_K$ then $M$ is Pólya field.

**Proof.** For each case of Theorem 3.1, we have $q\mathbb{Z}_K = Q^p$ by Theorem 2.6 and hence $N_{K/Q}(\omega) = q \iff \omega\mathbb{Z}_K = \Omega$. So it is enough to prove that $\Omega$ is a principal ideal. $Q^p$ is a principal ideal since $Q^p = q\mathbb{Z}_K$. On the other hand $Q^{hk}$ is a principal ideal. Since $p \nmid h_K$ then by Bezout’s Theorem, there exits $u,v \in \mathbb{Z}$ such that $up + vh_K = 1$. Thus $\Omega = (Q^p)^u \times (Q^{hk})^v$ is a principal ideal. $\square$

**Corollary 3.7.** Let $K = \mathbb{Q}(\sqrt{a})$. Then $M = \mathbb{Q}(\zeta_p, \sqrt{a})$ is a Pólya field if and only if:

- either $q^{p-1} \equiv 1 \mod p^2$
- or there exists $\omega \in \mathbb{Z}_K$ such that $N_{K/Q}(\omega) = p$.

In particular, $\mathbb{Q}(\zeta_p, \sqrt{p})$ is a Pólya field since $N_{K/Q}(\sqrt{p}) = p$.

**Proof.** Recall that $p \geq 3$ and $q \geq 2$ are prime numbers. Take $a = q$. Then $q$ is the only prime dividing $a$. By Theorem 3.1, $M = \mathbb{Q}(\zeta_p, \sqrt{a})$ is a Pólya field if and only if one of the following assertion is satisfied:

- $q^{p-1} \equiv 1 \mod p^2$ and there exists $\omega \in \mathbb{Z}_K$ such that $N_{K/Q}(\omega) = q$.
- $q^{p-1} \not\equiv 1 \mod p^2$ and there exists $\omega, \omega' \in \mathbb{Z}_K$ such that $N_{K/Q}(\omega) = q$ and $N_{K/Q}(\omega') = p$.

Since $\sqrt{a} \in K$ and $N_{K/Q}(\sqrt{a}) = q$, the two above assertions are equivalent to those of the Corollary 3.7. $\square$

**Example 3.8.** Let $n$ be a positive integer and $p$ a prime number such that $p \mid n$. If $n^2 + 1$ is a prime number then $\mathbb{Q}(\zeta_p, \sqrt{n^2 + 1})$ is a Pólya field. Indeed we have $q = n^2 + 1 \equiv 1 \mod n^2 \equiv 1 \equiv 1 \mod p^2$ so $q^{p-1} \equiv 1 \mod p^2$.

Recall that $p$ is a Wieferich’s prime number if and only if

$$2^{p-1} \equiv 1 \mod p^2$$

If $p$ is a Wieferich’s prime number then $\mathbb{Q}(\zeta_p, \sqrt{2})$ is a Pólya field. It is enough to take $q = 2$ in Corollary 3.7.

4. **Ramification in the Pólya fields $K = \mathbb{Q}(\sqrt{a})$ and $M = \mathbb{Q}(\zeta_p, \sqrt{a})$**

Recall that the ramified prime numbers in $M$ are those dividing $pa$. With the notations of the previous section, we have the following result.

**Theorem 4.1.** If $M$ is a Pólya field, let $n_M$ be the number of ramified prime numbers in $M$. Then $n_M \leq \frac{p-1}{2} + 2$. Precisely let $n_a$ be the number of prime divisors of $a$. Then

- $n_a \leq \frac{p-1}{2} + 1$ if $a^{p-1} \equiv 1 \mod p^2$ or $p \mid a$
- $n_a \leq \frac{p-1}{2}$ if $a^{p-1} \not\equiv 1 \mod p^2$ and $p \nmid a$
Remark 4.2. By Remark 3.4, necessary conditions of the previous Theorem holds if we replace $M$ by $K$.

General upperbounds exist for $n_M$ in [8] and [15]. By Corollary 2.43 of [8], we have $n_M \leq p - 1 + \frac{p(p-1)}{2} + cp$ with $c_p \geq 0$. It follows from Proposition 5.5 of [15] that $n_M \leq p$. Therefore Theorem 4.1 is sharper than these bounds.

To prove Theorem 4.1, we need some lemmas.

Lemma 4.3. The following are equivalent:

1) $\beta \notin \mathbb{Q}_p$
2) $X^p - \beta$ is irreductible in $\mathbb{Q}$.
3) $X^p - \beta$ has no roots in $\mathbb{Q}$.

Proof. See [7], Theorem 9.1, p.297. □

Lemma 4.4. Let $Tor(K^*/\mathbb{Q}^*) = \{x\mathbb{Q}^*, \exists n \in \mathbb{N}^*, x^n \in \mathbb{Q}\}$. Then

$Tor(K^*/\mathbb{Q}^*) = \{1\mathbb{Q}^*, \sqrt[p]{a}\mathbb{Q}^*, \cdots, (\sqrt[p]{a})^{p-1}\mathbb{Q}^*\}$


Corollary 4.5. Let $b, c \in \mathbb{Q}$. Then $\mathbb{Q}(\sqrt[p]{b}) = \mathbb{Q}(\sqrt[p]{c})$ if and only if $c = b^\alpha u^p$ with $u \in \mathbb{Q}$ and $0 \leq \alpha \leq p - 1$.

Proof. $\mathbb{Q}(\sqrt[p]{b}) = \mathbb{Q}(\sqrt[p]{c}) \Rightarrow Tor(\mathbb{Q}(\sqrt[p]{b})^*/\mathbb{Q}) = Tor(\mathbb{Q}(\sqrt[p]{c})^*/\mathbb{Q})$. Hence by Lemma 4.4, $\sqrt[p]{c} = \left(\sqrt[p]{b}\right)^\alpha u$ with $0 \leq \alpha \leq p - 1$ and $u \in \mathbb{Q}$ ie $c = b^\alpha u^p$. The converse is obvious. □

Lemma 4.6. Let $q$ be a prime number. If $q\mathbb{Z}_K = \mathbb{Q}_p$ then there is an equivalence between the following assertions:

1) There is $\omega \in \mathbb{Z}_K$ such that $N_{K/\mathbb{Q}}(\omega) = q$
2) There is $\varepsilon \in U_K$ such that the equation $\omega^p = \varepsilon N_{K/\mathbb{Q}}(\omega)$ has a solution $\omega \in \mathbb{Z}_K$ with $N_{K/\mathbb{Q}}(\omega) = q$

Proof. 1) $\Rightarrow$ 2): $N_{K/\mathbb{Q}}(\omega \mathbb{Z}_K) = q$. Hence $\omega \mathbb{Z}_K$ is a prime ideal lying over $q$. Thus $\omega \mathbb{Z}_K = \mathbb{Q}$ since $\mathbb{Q}$ is the only prime ideal over $q$ in $K$. We then have $\omega^p \mathbb{Z}_K = q\mathbb{Z}_K$ and hence there is $\varepsilon \in U_K$ such that $\omega^p = \varepsilon q$.

2) $\Rightarrow$ 1) is trivial. □

Proof of Theorem 4.1. Let $r$ be the number of fundamentals units in $K$. By Dirichlet's units Theorem, $U_K = \{\pm 1\} \times V_K$ where $V_K$ is a free $\mathbb{Z}$-module of rank $r$ since the only roots of units in $K$ are $\pm 1$. Suppose $M$ is a Pòlya. Let $s$ be the number of totally ramified prime numbers $q_i$ in $K$ ie $q_i\mathbb{Z}_K = \mathbb{Q}_p$. We will show that $s \leq r + 1$. Suppose $s \geq r + 2$. It follows from Theorem 3.1 and Lemma 4.6
that there are (at least) \( r + 2 \) elements \( \omega_i \in \mathbb{Z}_K \) and \( \varepsilon_i \in V_K^2 \) such that

\[
\begin{align*}
\omega_1^p &= \varepsilon_1 q_1 \\
\vdots & \quad \vdots \\
\omega_r^p &= \varepsilon_r q_r \\
\omega_{r+1}^p &= \varepsilon_{r+1} q_{r+1} \\
\omega_{r+2}^p &= \varepsilon_{r+2} q_{r+2}
\end{align*}
\] (4.1)

Let us first consider \( r \) and \( r + 1 \). Since the rank of the \( \mathbb{Z} \)-module \( V_K \) is \( r \) then there exist \( k_1, \ldots, k_r, k_{r+1} \in \mathbb{Z} \) such that

\[
\varepsilon_1^{k_1} \times \cdots \times \varepsilon_r^{k_r} \times \varepsilon_{r+1}^{k_{r+1}} = 1
\] (4.2)

There exists \( \ell \in \{1, \ldots, r, r + 1\} \) such that \( p \mid k_\ell \) even if we need to replace \( k_i, \ i \in \{1, \ldots, r, r + 1\} \) by \( k_i' = \frac{k_i}{p^\alpha} \) with \( \alpha = v_p(\gcd(k_1, \ldots, k_r, k_{r+1})) \). Indeed \( k_i' \in \mathbb{Z} \) and \( p \nmid \gcd(k_1', \ldots, k_r', k_{r+1}') \) since \( p^\alpha \) is the most power of \( p \) that divides \( \gcd(k_1, \ldots, k_r, k_{r+1}) \). From (4.2), we have

\[
\left( \varepsilon_1^{k_1} \times \cdots \times \varepsilon_r^{k_r} \times \varepsilon_{r+1}^{k_{r+1}} \right)^{\frac{1}{p^\alpha}} = \sqrt[p^\alpha]{1}. But 1 is the only \( p^{\alpha} \)-root of unit in \( K \) since \( p \) is odd. So \( \varepsilon_1^{k_1} \times \cdots \times \varepsilon_r^{k_r} \times \varepsilon_{r+1}^{k_{r+1}} = 1 \) and hence the relation (4.2) does not also change. We can assume that \( \ell = r + 1 \) is \( p \nmid k_{r+1} \) even if we must reorder \( \{k_1, \ldots, k_r, k_{r+1}\} \).

It follows from (4.1) and (4.2) that

\[
\left( \omega_1^{k_1} \times \cdots \times \omega_r^{k_r} \times \omega_{r+1}^{k_{r+1}} \right)^p = q_1^{k_1} \times \cdots \times q_r^{k_r} \times q_{r+1}^{k_{r+1}}
\] (4.3)

As \( p \nmid k_{r+1} \) and the \( q_i \) are relatively prime then \( q_1^{k_1} \times \cdots \times q_r^{k_r} \times q_{r+1}^{k_{r+1}} \notin \mathbb{Q}^p \). Hence by (4.3) and Lemma 4.3, we have

\[
\mathbb{Q} \left( \sqrt[p]{q_1^{k_1} \cdots q_r^{k_r} q_{r+1}^{k_{r+1}}} \right) = \mathbb{Q} \left( \omega_1^{k_1} \cdots \omega_r^{k_r} \omega_{r+1}^{k_{r+1}} \right), \quad \mathbb{Q} \left( \sqrt[p]{q_1^{k_1} \cdots q_r^{k_r} q_{r+1}^{k_{r+1}}} : \mathbb{Q} \right) = p
\]

So

\[
\mathbb{Q} \left( \sqrt[p]{a} \right) = K = \mathbb{Q} \left( \sqrt[p]{q_1^{k_1} \cdots q_r^{k_r} q_{r+1}^{k_{r+1}}} \right)
\]

since \( \omega_i \in K \) and \([K : \mathbb{Q}] = p \). Thus, by Corollary 4.5, we have

\[
q_1^{k_1} \cdots q_r^{k_r} q_{r+1}^{k_{r+1}} = a^\alpha u^p \text{ with } 1 \leq \alpha \leq p - 1 \text{ and } u \in \mathbb{Q}
\]

It follows that the set of prime divisors of \( a \) is contained in \( \{q_1, \ldots, q_r, q_{r+1}\} \). Indeed let \( \pi \) be a prime divisor of \( a \). Then

\[
v_\pi \left( q_1^{k_1} \cdots q_r^{k_r} q_{r+1}^{k_{r+1}} \right) = v_\pi (a^\alpha u^p) = v_\pi (a^\alpha) + v_\pi (u^p);
\]

if

\[
v_\pi \left( q_1^{k_1} \cdots q_r^{k_r} q_{r+1}^{k_{r+1}} \right) = 0 \text{ then } v_\pi (a^\alpha) = -v_\pi (u^p), \text{ which is absurd since } p \mid v_\pi (u^p) \text{ and } 3 \ p \nmid v_\pi (a^\alpha). \text{ Moreover } q_{r+1} \mid a. \text{ Indeed } k_{r+1} =
\]

\[
v_{q_{r+1}} \left( q_1^{k_1} \cdots q_r^{k_r} q_{r+1}^{k_{r+1}} \right) = k_{r+1} (a^\alpha u^p) = v_{q_{r+1}} (a^\alpha) + v_{q_{r+1}} (u^p); \text{ hence } v_{q_{r+1}} (a^\alpha) \neq 0 \text{ since } p \nmid k_{r+1} \text{ and } p \mid v_{q_{r+1}} (u^p), \text{ so } v_{q_{r+1}} (a) \neq 0.
\]

\[\text{2} \omega^p = q \varepsilon \Leftrightarrow (-\omega)^p = q \varepsilon. \text{ Since } U_K = \pm V_K, \text{ it's enough to take } \varepsilon \text{ in } V_K \text{ instead of in } U_K.
\]

\[\text{3} \quad u^p \text{ is a } p\text{-th power and } a^\alpha \text{ is } p\text{-th power free since } a \text{ is } p\text{-th power free and } 0 \leq \alpha \leq p - 1.
\]
With the same idea, we can show that the set of prime divisors of \( a \) is contained in \( \{q_1, \ldots, q_r, q_{r+2}\} \). Thus we obtain a contradiction since \( q_{r+1} \mid a \) and \( q_{r+1} \notin \{q_1, \ldots, q_r, q_{r+2}\} \).

It follows from the previous that if \( M \) is a Pólya field then the number \( s \) of totally ramified prime numbers in \( K \) satisfied \( s \leq r + 1 \). Since \( r \) is the number of fundamental units in \( K \) and the signature of \( K \) is \( (1, \frac{p-1}{2}) \) then \( r = \frac{p-1}{2} \).

Now let \( n_a \) be the number of prime divisors of \( a \). Then by Theorem 2.5 and Lemma 2.6,

\[
s = \begin{cases} n_a & \text{if } a^{p-1} \equiv 1 \mod p^2 \text{ or } p \mid a \\ n_a + 1 & \text{if } a^{p-1} \not\equiv 1 \mod p^2 \text{ and } p \nmid a \end{cases}
\]

Hence we have

\[
\begin{align*}
n_a & \leq \frac{p-1}{2} + 1 \quad \text{if } a^{p-1} \equiv 1 \mod p^2 \text{ or } p \mid a \\
n_a & \leq \frac{p-1}{2} \quad \text{if } a^{p-1} \not\equiv 1 \mod p^2 \text{ and } p \nmid a
\end{align*}
\]

since \( s \leq r + 1 \) and \( r = \frac{p-1}{2} \). \( \square \)

**Remark 4.7.** We will give an application of the previous Theorem on Theorem 1.1. Suppose \( a \) cubefree. Let \( n_a \) be the number of prime divisors of \( a \). Suppose that \( K = \mathbb{Q}(\sqrt[3]{a}) \) or \( M = \mathbb{Q}(j, \sqrt[3]{a}) \) is a Pólya field. By Theorem 4.1 and Remark 4.2, we have:

- \( n_a \leq 2 \) if \( a^2 \equiv 1 \mod 9 \) or \( 3 \mid a \)
- \( n_a \leq 1 \) if \( a^2 \not\equiv 1 \mod 9 \) and \( 3 \nmid a \)

Since \( \mathbb{Q}(\sqrt[3]{a}) = \mathbb{Q}(\sqrt[3]{a^2}) \), we can also suppose that \( a \) is not a square. More generally, for \( b, c \in \mathbb{N} \), we have \( \mathbb{Q}(\sqrt[3]{bc^2}) = \mathbb{Q}(\sqrt[3]{b^2c}) \). Moreover if \( 3 \mid a \) then \( a^2 \not\equiv 1 \mod 9 \). Hence

- if \( a^2 \equiv 1 \mod 9 \) then \( a = q \) or \( a = q_1q_2 \) or \( a = q_1^2q_2 \)
- if \( a^2 \not\equiv 1 \mod 9 \) then \( a = q \) or \( a = 3q \) or \( a = 3q^2 \)

where \( q, q_1, q_2 \) are prime numbers. Thus a Pólya field of the form \( \mathbb{Q}(\sqrt[3]{a}) \) or \( \mathbb{Q}(j, \sqrt[3]{a}) \) must be in one of the sets of the following Definition except when \( a = 3 \).

**Definition 4.8.** Let

- \( E_1 \) be the set of fields \( K = \mathbb{Q}(\sqrt[3]{a}) \) and \( M = \mathbb{Q}(j, \sqrt[3]{a}) \) such that \( a \) is a prime number and \( a^2 \equiv 1 \mod 9 \).
- \( E_2 \) be the set of fields \( K = \mathbb{Q}(\sqrt[3]{a}) \) and \( M = \mathbb{Q}(j, \sqrt[3]{a}) \) such that \( a^2 \equiv 1 \mod 9 \) and there exist two prime numbers \( q_1, q_2 \) such that \( a = q_1q_2 \) or \( a = q_1^2q_2 \).
- \( E_3 \) be the set of fields \( K = \mathbb{Q}(\sqrt[3]{a}) \) and \( M = \mathbb{Q}(j, \sqrt[3]{a}) \) such that \( a^2 \not\equiv 1 \mod 9 \) and there exists a prime number \( q \), \( q \not= 3 \) such that \( a = q \) or \( a = 3q \) or \( a = 3q^2 \).

The following Theorem is a refinement of Theorem 1.1.

**Theorem 4.9.** \( M = \mathbb{Q}(j, \sqrt[3]{a}) \) is a Pólya field if and only if one of the following is satisfied
1) $M = \mathbb{Q}(j, \sqrt[3]{3})$
2) $M \in E_1$
3) $M \in E_2$ and there is an algebraic integer $\omega \in K$ and a prime $q$ such that $N_{K/\mathbb{Q}}(\omega) = q$.
4) $M \in E_3$ and there is an algebraic integer $\omega \in K$ such that $N_{K/\mathbb{Q}}(\omega) = 3$.

Proof. The necessity follows naturally from Remark 4.7 and Theorem 3.1. By Corollary 3.7, 1) and 2) are sufficient. Let us now look at the sufficiency of 3) and 4). Suppose $M \in E_2$ and $a = q_1q_2$ where $q_1$ and $q_2$ are prime numbers. Suppose that there exists $\omega \in \mathbb{Z}_K$ such that $N_{K/\mathbb{Q}}(\omega) = q_1$. We will show that there exists $\omega' \in \mathbb{Z}_K$ such that $N_{K/\mathbb{Q}}(\omega') = q_2$ and by Theorem 4.1, we can conclude that $M$ is a Pólya field. $a\mathbb{Z}_K = q_1q_2\mathbb{Z}_K = \omega^3q_2\mathbb{Z}_K$. Hence $q_2\mathbb{Z}_K = (\omega^{-1}\sqrt[3]{a})^3\mathbb{Z}_K$. So $\omega^{-1}\sqrt[3]{a} \in \mathbb{Z}_K$ and $N_{K/\mathbb{Q}}(\omega^{-1}\sqrt[3]{a}) = q_2$. Thus $\omega' = \omega^{-1}\sqrt[3]{a}$.

The condition 3) is then sufficient when $a = q_1q_2$. With the same idea we get the sufficiency of the cases ($M \in E_2$ and $a = q_1^2q_2$), ($M \in E_3$ and $a = 3q$ or $3q^2$). Finally let $M \in E_3$ such that $a$ is a prime number and there exists $\omega \in \mathbb{Z}_K$ such that $N_{K/\mathbb{Q}}(\omega) = 3$. By Theorem 3.1, $M$ is a Pólya field since the only prime divisors of $3a$ are 3 and $a$, $a^2 \not\equiv 1 \mod 9$, $N_{K/\mathbb{Q}}(\omega) = 3$ and $N_{K/\mathbb{Q}}(\sqrt[3]{a}) = a$. Therefore we can conclude that all conditions of the Theorem are sufficient.□

Remark 4.10. Let us show why Theorem 4.9 is a refinement of Theorem 1.1. By Remark 3.2, the condition $(b^2 \equiv c^2 \mod 9)$ of Theorem 1.1 is equivalent to $(a^2 \equiv 1 \mod 9)$. By Theorem 1.1, to know a Pólya field $\mathbb{Q}(j, \sqrt[3]{a})$, we must solve the norm form equations $N_{K/\mathbb{Q}}(\omega) = q$, $\omega \in \mathbb{Z}_K$ for all prime divisors of $a$ or $3a$ (depending on whether we have $a^2 \equiv 1 \mod 9$ or not). Each of these equations is difficult to solve in general. Theorem 4.9 shows that this resolution is not necessary if the number $n_a$ of prime divisors of $a$ satisfies

- $n_a > 2$ and $(a^2 \equiv 1 \mod 9$ or $3 \mid a$)
- $n_a > 1$ and $(a^2 \not\equiv 1 \mod 9$ and $3 \nmid a$)

since in this case Theorem 4.9 shows clearly that $M$ is not a Pólya field. For example $\mathbb{Q}(j, \sqrt[3]{30})$ is not a Pólya field since $n_{30} = 3 > 2$. Similarly $\mathbb{Q}(j, \sqrt[3]{77})$ is not since $n_{77} = 2 > 1$, $77^2 \equiv (-4)^2 \equiv -2 \not\equiv 1 \mod 9$ and $3 \nmid 77$.

Moreover even if we need to solve norm form equation $N_{K/\mathbb{Q}}(\omega) = q$, only one is necessary in the Theorem 4.9 whereas in Theorem 1.1 it must be solved for all prime divisors of $a$. For example, suppose $3 \nmid a$ and $a$ cubefree. If the Thue equation $x^3 + ay^3 = 3$ has a solution $x, y \in \mathbb{Z}$ then the field $M = \mathbb{Q}(j, \sqrt[3]{a}) = K(j)$ is a Pólya field if and only if $a$ is a prime number or a square of a prime. Indeed $x^3, y^3 \equiv \{-1, 0, 1\} \mod 9$. Hence $a \equiv \pm\{4, 3, 2\} \mod 9$, so $a^2 \not\equiv 1 \mod 9$. Thus $M \not\in E_1$ and $M \not\in E_2$. Hence, by Theorem 4.9, if $M$ is a Pólya field field then $M \in E_3$. Since $3 \nmid a$ and $\mathbb{Q}(\sqrt[3]{a}) = \mathbb{Q}(\sqrt[3]{a^2})$, $a$ must be a prime number or a square of a prime number. The conclusion follows since $N_{K/\mathbb{Q}}(x + y\sqrt[3]{a}) = x^3 + ay^3 = 3$ gives us one solution of norm form equation. In particular let $x \in \mathbb{Z}$ such that $3 \nmid x$ and $3 + x^3$ cubefree. Then $\mathbb{Q}(j, \sqrt[3]{3 + x^3})$ is a Pólya field if and only if $3 + x^3$ is a prime number or $a = 4$. Indeed it follows from [5] that $3 + x^3$ is a square of an integer if and only if $x = 1$. 


References


1 Laboratoire de Théorie des Nombres, Algèbre, Géométrie Algébrique et Topologie Algébrique (TNAGATA), UFR. Sciences Exactes et Appliquées, 03 BP 7021 Ouaga 03, Ouagadougou, Burkina Faso
Email address: kientdia@yahoo.fr

2 Laboratoire d’Algèbre, de Mathématiques Discrètes et d’Informatique (LAMDI), Université Nazi Boni, 01 BP 1091 Bobo Dioulasso 01, Burkina Faso.
Email address: tmytapsoba@yahoo.fr

3 Laboratoire de Théorie des Nombres, Algèbre, Géométrie Algébrique et Topologie Algébrique (TNAGATA), UFR. Sciences Exactes et Appliquées, 03 BP 7021 Ouaga 03, Ouagadougou, Burkina Faso
Email address: tougmacarles@yahoo.fr