*Proceedings of the Royal Society of Edinburgh*, **149**, 1421–1433, *2019*
DOI:10.1017/prm.2018.86

# Pólya $S_3$-extensions of $\mathbb{Q}$

**Abbas Maarefparvar and Ali Rajaei**
Department of Mathematics, Tarbiat Modares University,
Tehran 14115-134, Iran (a.maarefparvar@modares.ac.ir;
alirajaei@modares.ac.ir)

(MS received 10 May 2017; accepted 27 September 2017)

A number field $K$ with a ring of integers $\mathcal{O}_K$ is called a Pólya field, if the $\mathcal{O}_K$-module of integer-valued polynomials on $\mathcal{O}_K$ has a regular basis, or equivalently all its Bhargava factorial ideals are principal [**1**]. We generalize Leriche's criterion [**8**] for Pólya-ness of Galois closures of pure cubic fields, to general $S_3$-extensions of $\mathbb{Q}$. Also, we prove for a real (resp. imaginary) Pólya $S_3$-extension $L$ of $\mathbb{Q}$, at most four (resp. three) primes can be ramified. Moreover, depending on the solvability of unit norm equation over the quadratic subfield of $L$, we determine when these sharp upper bounds can occur.

*Keywords:* integer-valued polynomials; Pólya fields; non-Galois cubic fields; $S_3$-fields; $S_3$-extensions

2010 *Mathematics subject classification:* Primary 11R04; 11R16; 11R29; 11R37; 11R34; 13F20

**Notations.** Throughout this paper, $I(M)$, $P(M)$, $\mathcal{O}_M$, $Cl(M)$, $h(M)$, $U_M$, $\delta_M$ and $D_M$ denote the group of fractional ideals, group of principal fractional ideals, ring of integers, ideal class group, class number, unit group, different and discriminant of a number field $M$, respectively. For a finite extension $M/N$ of number fields, $\mathcal{N}_{M/N}$ denotes the ideal norm homomorphism $\mathcal{N}_{M/N} : I(M) \to I(N)$. Also for a prime ideal $\mathfrak{p}$ of $N$ and a prime ideal $\mathfrak{P}$ of $M$ above $\mathfrak{p}$, we denote the ramification index and residue class degree of $\mathfrak{P}$ over $\mathfrak{p}$ by $e(\mathfrak{P}/\mathfrak{p})$ and $f(\mathfrak{P}/\mathfrak{p})$, respectively. For an integer $n \geqslant 3$, $S_n$ and $A_n$ denote the symmetric and alternating group on $n$ symbols, respectively. $\rho$ is a primitive third root of unity.

## 1. Introduction

For every number field $K$ with a ring of integers $\mathcal{O}_K$, consider the ring of integer-valued polynomials on $\mathcal{O}_K$:

$$Int(\mathcal{O}_K) = \{f \in K[x] \mid f(\mathcal{O}_k) \subseteq \mathcal{O}_K\}.$$

$\mathrm{Int}(\mathcal{O}_K)$ is free as an $\mathcal{O}_K$-module, see [**14**, § 2]. But Pólya [**12**] and Ostrowski [**11**] tried to characterize the fields $K$ such that $\mathrm{Int}(\mathcal{O}_K)$ has a regular basis in the following sense:

Definition 1.1 [**14**]. A number field $K$ is called Pólya, if the $\mathcal{O}_K$-module $\text{Int}(\mathcal{O}_K)$ admits a regular basis, that is a basis $(f_n)_{n\geqslant 0}$ such that for every $n$, $deg(f_n) = n$.

Pólya [**12**, Satz I] showed that a number field $K$ is Pólya if and only if, for each positive integer $n$, the fractional ideal $\mathfrak{J}_n(K)$ of $K$ formed by 0 and leading coefficients of polynomials of degree $n$ in $\text{Int}(\mathcal{O}_K)$ is principal. He also proved that a quadratic field is Pólya if and only if all prime ideals above ramified primes are principal, see [**12**, Satz V].

Following Pólya [**12**], Ostrowski [**11**] proved that a number field $K$ is Pólya if and only if all the ideals

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

are principal. Therefore, for a Galois extension $K$ of $\mathbb{Q}$, the principality of $\Pi_q(K)$ needs to be checked only for ramified primes.

Obviously, every number field with class number 1 is a Pólya field, but not conversely. For example, the quadratic field $\mathbb{Q}(\sqrt{-4027})$ is Pólya, while it has class number 9.

For Galois number fields, we have:

Proposition 1.2 ([**14**, § 3, p. 163]). *Let $K/\mathbb{Q}$ be a Galois extension with Galois group $G$. For a prime number $p$, let $e(p)$ be the ramification index of $p$ in $K$. Then the following sequence is exact:*

$$\{0\} \longrightarrow H^1(G, U_K) \longrightarrow \bigoplus_{p\ prime} \mathbb{Z}/e(p)\mathbb{Z} \longrightarrow I(K)^G/P(K)^G \longrightarrow \{0\}. \tag{1.1}$$

Remark 1.3. Since

$$P(K)^G = I(K)^G \cap P(K),$$

the group of ambiguous ideals modulo principal ambiguous ideals, $I(K)^G/P(K)^G$, can be considered as a subgroup of $Cl(K)$ and $K$ is Pólya if and only if this subgroup is trivial, see [**14**, § 3, p. 164]. By exact sequence (1.1), the order of this group divides $\prod_{\text{p prime}} e(p)$, and since every ramification index $e(p)$ divides $[K : \mathbb{Q}]$, for any Galois number field $K$, if $[K : \mathbb{Q}]$ and $h(K)$ are relatively prime then $K$ is a Pólya field, but not conversely. For instance, as we will see, in Example (2.6), there is a Galois sextic Pólya number field with class number 3.

Zantema found a criterion for Pólya-ness of cyclic number fields of prime power degree, see [**14**, proposition 3.2]. As a consequence, he gave a complete characterization of quadratic Pólya fields:

Proposition 1.4 ([**14**, example 3.3]). *A quadratic field $K = \mathbb{Q}(\sqrt{d})$ is a Pólya field if and only if $d$ has one of the following forms, where $p \equiv q (\text{mod}\, 4)$ denote two distinct odd prime numbers.*

(1) *$d = 2$, or $d = p$;*

https://doi.org/10.1017/prm.2018.86 Published online by Cambridge University Press

(2) *$d = -1$, or $d = -2$, or $d = -p$ where $p \equiv 3 (\mathrm{mod}\, 4)$;*

(3) *$d = 2p$, or $d = pq$, if $K$ has no units of norm $-1$.*

Following Zantema's results [**14**], Leriche [**8**] characterized cyclic cubic and cyclic quartic Pólya fields in terms of their equations, and she found a criterion for Pólya-ness of Galois closures of pure cubic fields.

For a non-Galois cubic field $K$, Zantema proved that Pólya-ness of $K$ is equivalent to $h(K) = 1$, see [**14**, Theorem 1.1]. Following Zantema, we restate the concept of a $G\text{-}field$:

Definition 1.5 [**14**]. For $G$ a transitive subgroup of $S_n$ $(n \geqslant 3)$, a field $K$ of degree $n$ over $\mathbb{Q}$ is called a $G$-field, if its Galois closure $L$ over $\mathbb{Q}$ has a Galois group isomorphic to $G$ and the action of $G$ on the $n$ embeddings of $K$ into $L$ corresponds to the action on the $n$ symbols.

More generally, Zantema gave a criterion for Pólya-ness of $S_n$-fields and $A_n$-fields as follows:

Proposition 1.6 ([**14**, theorem 1.1]). *Let $K$ be an $S_n$-field, for $n = 3$ or $n \geqslant 5$, or an $A_n$-field, for $n = 4$ or $n \geqslant 6$. Then $K$ is a Pólya field if and only if $h(K) = 1$.*

In this paper, we investigate Pólya-ness of Galois closures of non-Galois cubic fields, that is, Galois non-cyclic sextic fields.

Let $K$ be a non-Galois cubic number field. Denote the Galois closure of $K$ over $\mathbb{Q}$ by $L$ and denote by $E$ the unique quadratic subfield of $L$.

In § 2, we prove that if $h(K)$ is not divisible by 3 and $E$ is Pólya, then $L$ is a Pólya field. In particular, if $E$ and $K$ are Pólya then so is $L$, see corollary (2.5). We find a necessary but not sufficient condition for Pólya-ness of $L$, and prove that Pólya-ness of $L$ implies that its quadratic subfield $E$ is a Pólya field. (Note that for any pure cubic field $K = \mathbb{Q}(\sqrt[3]{m})$, the unique quadratic subfield $E = \mathbb{Q}(\sqrt{-3})$ of $L$ has class number one, hence is Pólya.) We also prove that if $L/E$ is unramified, Pólya-ness of $E$ and $L$ are equivalent, see corollary (2.10).

In § 3, with a cohomological interpretation, we give a sharp upper bound for the number of ramified primes in Pólya $S_3$-extensions of $\mathbb{Q}$. We prove that for a real Pólya $S_3$-extension $L$ of $\mathbb{Q}$ at most four primes ramify. We show that four ramified primes can occur if the norm equation $\mathcal{N}_{L/E}(u) = \xi$ has no solution $u \in U_L$, where $\xi$ is the fundamental unit of $E$. Also, we prove that for an imaginary Pólya $S_3$-extension $L$ of $\mathbb{Q}$ at most three primes can ramify, and this happens only for Galois closures of pure cubic fields. Indeed, three ramified primes can occur if $\rho \notin \mathcal{N}_{L/E}(U_L)$, where $\rho$ is a primitive third root of unity, see theorem (3.1).

In § 4, following Masley's article [**9**], we show that $h(K)$ divides $h(L)$, see corollary (4.3). Hence if $h(L) = 1$, then both subfields $E$ and $K$ are Pólya fields, see corollary (4.4).

## 2. Pólya $S_3$-extensions of $\mathbb{Q}$

Let $K$ be a non-Galois cubic number field with Galois closure $L$ whose unique quadratic subfield is $E = \mathbb{Q}(\sqrt{D_K})$.

https://doi.org/10.1017/prm.2018.86 Published online by Cambridge University Press

If a prime $p$ is unramified in $K/\mathbb{Q}$, it would also be unramified in all its Galois conjugates, hence in their compositum, namely $L/\mathbb{Q}$ (see the implications for $E$ in remark (2.2) below). Therefore, ramified primes in $K/\mathbb{Q}$ and $L/\mathbb{Q}$ coincide.

Now let $p$ be a ramified prime in $L/\mathbb{Q}$. Since $L/\mathbb{Q}$ is a Galois extension, all primes above $p$ have the same ramification index and residue class degree:

$$p\mathcal{O}_L = (\gamma_1\gamma_2\ldots\gamma_g)^{e(p)},$$

where the $\gamma_i$'s are the distinct prime ideals of $L$ above $p$ with residue class degree $f(p)$. Since $e(p)f(p)g = [L:\mathbb{Q}] = 6$, we have $e(p) = 2, 3$ or $6$.

LEMMA 2.1. *With the notations of this Section, let $p$ be a ramified prime in $L/\mathbb{Q}$.*

(a) *If $e(p) = 2$, then $p$ is ramified in $E/\mathbb{Q}$. Moreover,*

$$p\mathcal{O}_K = \beta_1\beta_2^2,$$
$$p\mathcal{O}_L = (\gamma_1\gamma_2\gamma_3)^2.$$

(b) *If $e(p) = 3$, then $p$ is totally ramified in $K/\mathbb{Q}$, but unramified in $E/\mathbb{Q}$. Moreover, depending on whether $p$ is split or inert in $E/\mathbb{Q}$, we have $p\mathcal{O}_L = (\gamma_1\gamma_2)^3$ or $p\mathcal{O}_L = \gamma^3$, respectively.*

(c) *If $e(p) = 6$, then $p = 3$ and ramifies totally in both $E/\mathbb{Q}$ and $K/\mathbb{Q}$.*

*Proof.*

(a) Assume that $e(p) = 2$. Then $f(p) = 3$ or $f(p) = 1$. If $f(p) = 3$, then $p\mathcal{O}_L = \gamma^2$. Thus in this case, there exists only one prime ideal of $L$ above $p$, which means that there is only one prime ideal $\beta$ of $K$ above $p$. Since $p$ is also ramified in $K/\mathbb{Q}$, $p\mathcal{O}_K = \beta^3$, but the ramification index of $\beta$ above $p$ must divide $e(p)$ and we reach a contradiction. Hence if $e(p) = 2$, then $f(p) = 1$ and $p$ has the decomposition forms in $K$ and $L$ as follows:

$$p\mathcal{O}_K = \beta_1\beta_2^2,$$
$$p\mathcal{O}_L = (\gamma_1\gamma_2\gamma_3)^2,$$

respectively. Note that since $E$ is a Galois extension, we have:

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

where $\alpha$ is a prime ideal of $E$ above $p$ with $\alpha = \gamma_1 \cap E$. Since $e(\gamma_1/\alpha)$ divides $[L:E] = 3$, $p$ is ramified in $E/\mathbb{Q}$ and $\alpha$ stays unramified in the extension $L/E$.

(b) Assume that $e(p) = 3$. Hence $f(p) = 1$ or $f(p) = 2$. If $f(p) = 1$, then there exist two distinct prime ideals $\gamma_1$ and $\gamma_2$ of $L$ above $p$ with $p\mathcal{O}_L = (\gamma_1\gamma_2)^3$. Similarly, if $f(p) = 2$, then there exists only one prime ideal $\gamma_1$ of $L$ above $p$ with $p\mathcal{O}_L = \gamma_1^3$.

In both cases, since $p$ is ramified in $K/\mathbb{Q}$, for a prime ideal $\beta = \gamma_1 \cap K$ of $K$ above $p$, $e(\beta/p) > 1$. Since

$$3 = e(\gamma_1/p) = e(\gamma_1/\beta)e(\beta/p),$$

we have $e(\beta/p) = 3$. Hence if $e(p) = 3$, then $p$ is totally ramified in $K/\mathbb{Q}$.

https://doi.org/10.1017/prm.2018.86 Published online by Cambridge University Press

Now let $\alpha = \gamma_1 \cap E$ be a prime ideal of $E$ above $p$. Since

$$3 = e(\gamma_1/p) = e(\gamma_1/\alpha)e(\alpha/p),$$

and $e(\alpha/p) \leqslant 2$, we have $e(\alpha/p) = 1$ and $e(\gamma_1/\alpha) = 3$. This means that in the case $e(p) = 3$, $p$ is unramified in $E/\mathbb{Q}$. Indeed, we have:

$$f(p) = f(\gamma_1/p) = f(\gamma_1/\alpha)f(\alpha/p),$$

with $f(p) \leqslant 2$ and $f(\gamma_1/\alpha)|[L : E] = 3$. So if $e(p) = 3$, then $p$ is split (resp. inert) in $E/\mathbb{Q}$ if and only if $f(p) = 1$ (resp. $f(p) = 2$).

(c) For a ramified prime $p$ in $K/\mathbb{Q}$, either $p\mathcal{O}_K = \beta^3$ or $p\mathcal{O}_K = \beta_1\beta_2^2$. Then the $p$-part of $\delta_K$ would be $\beta^2$ or $\beta_2$, respectively, unless $p$ is wildly ramified, see [**13**, Chapter III, § 6, proposition 13]. Wild ramification can happen only for $3\mathcal{O}_K = \beta^3$ or $2\mathcal{O}_K = \beta_1\beta_2^2$.

If $2 \mid D_K$, one can show that either $2^2 \mid\mid D_K$ or $2^3 \mid\mid D_K$, and $2^3 \mid\mid D_K$ happens only when $2\mathcal{O}_K = \beta_1\beta_2^2$. Also if $3\mathcal{O}_K = \beta^3$, one has $3^t \mid\mid D_K$ for $t \in \{3, 4, 5\}$, see [**13**, Chapter III, § 6, remark 1 after proposition 13].

Hence one can write $D_K = s.f^2$, where $s$ is square-free and a prime number $p \neq 2, 3$ cannot divide both $s$ and $f$. Also for a prime number $p \neq 2$, one has $p \mid f$ if and only if $p\mathcal{O}_K = \beta^3$.

Now assume that $e(p) = 6$. Then $p$ is totally ramified in $L/\mathbb{Q}$, hence in all its subextensions. By the above argument this can only occur for $p = 2, 3$.

Suppose that $2\mathcal{O}_L = \gamma^6$. Since the order of the inertia group at 2 equals the ramification index $e(\gamma/2)$, the inertia group at 2 is the whole Galois group, see [**13**, Chapter I, § 7, corollary of proposition 21].

Localizing at 2 and denoting the $i$th ramification group by $G_i$, we have $G_1$ is a normal subgroup of $G_0 \simeq S_3$, see [**13**, Chapter IV, § 1, proposition 1]. By [**13**, Chapter IV, § 2, corollary 3] $G_1$ is a 2-group. Hence $G_1 = \{1\}$, but $G_0/G_1$ has to be cyclic which is impossible, see [**13**, Chapter IV, § 2, corollary 1]. Therefore 2 cannot totally ramify in $L/\mathbb{Q}$. This completes the proof. □

Remark 2.2. If $p$ ramifies in $E$, then it would ramify in $L$, hence also in $K$. Since $E = \mathbb{Q}(\sqrt{D_K})$, for $p \neq 2$ this is rather obvious. If 2 does not divide $D_K = s.f^2$, then it would be unramified in $E = \mathbb{Q}(\sqrt{s})$, hence $s \equiv 1 (\mathrm{mod}\, 4)$. Also if $D_K = 4t$ for some odd integer $t$, by the proof of part ($c$) above, it ramifies totally in $K$. Since 2 does not ramify totally in $L$, it is unramified in $E = \mathbb{Q}(\sqrt{t})$, which implies $t \equiv 1 (\mathrm{mod}\, 4)$.

Now we give the main result as follows:

Theorem 2.3. *Let $K$ be a non-Galois cubic number field. Denote the Galois closure of $K$ over $\mathbb{Q}$ by $L$ and denote by $E$ the unique quadratic subfield of $L$. Then $L$ is a Pólya field if and only if for each ramified prime $p$ in $L/\mathbb{Q}$:*

(a) *if $e(p) = 2$, then the ideal $\Pi_p(E)$ is principal;*

https://doi.org/10.1017/prm.2018.86 Published online by Cambridge University Press

(b) *if* $e(p) = 3$*, then the ideal* $\Pi_p(K)$ *is principal;*

(c) *if* $e(p) = 6$*, then both of the ideals* $\Pi_p(E)$ *and* $\Pi_p(K)$ *are principal.*

*Proof.*

(a) Suppose that $e(p) = 2$. By part $(a)$ of lemma (2.1), we have:

$$p\mathcal{O}_E = \alpha^2 = (\Pi_p(E))^2,$$
$$p\mathcal{O}_K = \beta_1\beta_2^2,$$
$$p\mathcal{O}_L = (\gamma_1\gamma_2\gamma_3)^2 = (\Pi_p(L))^2.$$

By comparing the decomposition forms of $p$ in $E$ and $L$, we have $\Pi_p(E)\mathcal{O}_L = \Pi_p(L)$. Obviously if $\Pi_p(E)$ is principal, then $\Pi_p(L)$ is principal, too.

Conversely, if $\Pi_p(L)$ is principal, by taking norm we find:

$$\mathcal{N}_{L/E}(\Pi_p(L)) = \mathcal{N}_{L/E}(\gamma_1\gamma_2\gamma_3) = (\Pi_p(E))^3.$$

Hence $(\Pi_p(E))^3$ is principal, and so $\Pi_p(E)$ is principal if and only if $(\Pi_p(E))^2$ is principal. Since $p\mathcal{O}_E = (\Pi_p(E))^2$, the statement in part $(a)$ is proved.

(b) According to part $(b)$ of lemma (2.1), $p$ is totally ramified in $K$, say $p\mathcal{O}_K = \beta^3 = (\Pi_p(K))^3$. Depending on whether $p$ is split or inert in $E/\mathbb{Q}$, we have:

$$p\mathcal{O}_L = (\gamma_1\gamma_2)^3 = (\Pi_p(L))^3,$$
$$p\mathcal{O}_L = \gamma^3 = (\Pi_{p^2}(L))^3,$$

respectively.

Hence we have $\Pi_p(K)\mathcal{O}_L = \Pi_p(L)$ (resp. $\Pi_p(K)\mathcal{O}_L = \Pi_{p^2}(L)$). Therefore, if $\Pi_p(K)$ is principal, then $\Pi_p(L)$ (resp. $\Pi_{p^2}(L)$) is principal.
Conversely, if $\Pi_p(L)$ (resp. $\Pi_{p^2}(L)$) is principal, then

$$(\Pi_p(K))^2 = \mathcal{N}_{L/K}(\Pi_p(L))$$

(resp. $\mathcal{N}_{L/K}(\Pi_{p^2}(L))$) is principal, too. Since $(\Pi_p(K))^3 = p\mathcal{O}_K$, $\Pi_p(K)$ is principal.

(c) Finally, suppose that $e(p) = 6$, that is, $p$ is totally ramified in $L/\mathbb{Q}$. By part $(c)$ of lemma (2.1), $p = 3$ and ramifies totally in both $E/\mathbb{Q}$ and $K/\mathbb{Q}$. Let:

$$3\mathcal{O}_E = \alpha^2 = (\Pi_3(E))^2,$$
$$3\mathcal{O}_K = \beta^3 = (\Pi_3(K))^3,$$
$$3\mathcal{O}_L = \gamma^6 = (\Pi_3(L))^6.$$

Thus we have:

$$\Pi_3(E)\mathcal{O}_L = (\Pi_3(L))^3,$$
$$\Pi_3(K)\mathcal{O}_L = (\Pi_3(L))^2.$$

Hence if $\Pi_3(E)$ and $\Pi_3(K)$ are principal, then $(\Pi_3(L))^3$ and $(\Pi_3(L))^2$ are principal, which implies that $\Pi_3(L)$ is principal.

https://doi.org/10.1017/prm.2018.86 Published online by Cambridge University Press

Now let $\Pi_3(L)$ be principal. Taking norms, we get:

$$\Pi_3(E) = \mathcal{N}_{L/E}(\Pi_3(L))$$
$$\Pi_3(K) = \mathcal{N}_{L/K}(\Pi_3(L)).$$

Thus, $\Pi_3(E)$ and $\Pi_3(K)$ are principal. □

REMARK 2.4. For a pure cubic field $K = \mathbb{Q}(\sqrt[3]{m})$, where $m$ is a cube-free integer, with the Galois closure $L = \mathbb{Q}(\rho, \sqrt[3]{m})$, Leriche [**8**] proved that for a prime divisor $p \neq 3$ of $m$, $\Pi_p(K)$ is principal if and only if $\Pi_p(L)$ (or $\Pi_{p^2}(L)$) is principal, see [**8**, lemma 6.4]. (The use of [**8**, proposition 6.3] is not clear to us, since $[L : K] = n = 2$ there not 3.)

As a consequence of theorem (2.3), we have:

COROLLARY 2.5. *With the notations of theorem* (2.3)*, if $h(K)$ is not divisible by* 3 *and $E$ is Pólya, then $L$ is a Pólya field. In particular, if $E$ and $K$ are Pólya, then so is $L$.*

*Proof.* If $h(K)$ is not divisible by 3, then for every totally ramified prime $p$ in $K/\mathbb{Q}$, $\Pi_p(K)$ is principal. By theorem (2.3), the statement is proved. □

EXAMPLE 2.6. Let $K = \mathbb{Q}(\alpha)$ be a cubic number field where $\alpha$ is a root of $f(x) = x^3 - 25x + 19$. We have $D_K = 71.743$, hence $K$ is a non-Galois cubic field and the Galois closure $L$ of $K$ over $\mathbb{Q}$ is $L = K(\sqrt{D_K}) = K(\sqrt{71.743})$. Since $h(K) = 1$, $K$ is Pólya. Also, by proposition (1.4) the quadratic field $E = \mathbb{Q}(\sqrt{71.743})$ is Pólya. Therefore, by corollary (2.5), $L$ is a (real) Pólya field. Note that $h(L) = 3$, see remark (1.3).

REMARK 2.7. Let $K_1$ and $K_2$ be two Galois number fields with coprime degrees over $\mathbb{Q}$ and $L = K_1.K_2$. Zantema [**14**] proved that $K_1$ and $K_2$ are Pólya fields if and only if $L$ is a Pólya field, see [**14**, theorem 3.4]. The condition on relative primality of the degrees is necessary as was shown in [**3**, **4**] in the case of biquadratic fields. Also the condition on Galois-ness of both $K_1$ and $K_2$ is necessary: with the notations of theorem (2.3), for a ramified prime $p$ in the extension $L/\mathbb{Q}$ with $e(p) = 2$, $\Pi_p(K)$ can be principal (resp. non-principal), with $\Pi_p(L)$ non-principal (resp. principal). Hence one can say there exist Pólya (resp. non-Pólya) non-Galois cubic fields with non-Pólya (resp. Pólya) Galois closure, see example (2.8) (resp. example (2.9)). Hence the part 'only if' in Zantema's result [**14**, theorem 3.4] for Galois number fields does not necessarily hold if either $K_1$ or $K_2$ is not Galois. Note that even if $\Pi_p(K)$ is principal for every ramified prime $p$ in $K/\mathbb{Q}$, $K$ need not be Pólya, see example (2.14).

EXAMPLE 2.8. Let $K = \mathbb{Q}(\alpha)$ where $\alpha$ is a root of $f(x) = x^3 - 3x + 3$. The discriminant of $K$ is $D_K = -3^3.5$. Thus the Galois closure $L$ of $K$ over $\mathbb{Q}$ is the compositum of $K$ and the imaginary quadratic field $E = \mathbb{Q}(\sqrt{-15})$. We have $e(5) = 2$, and since $\Pi_5(E)$ is not principal, by part $(a)$ of theorem (2.3) the ideal $\Pi_5(L)$ is not principal. Hence $L$ is not a Pólya field, while $h(K) = 1$.

https://doi.org/10.1017/prm.2018.86 Published online by Cambridge University Press

EXAMPLE 2.9. Consider the pure cubic field $K = \mathbb{Q}(\sqrt[3]{19})$. The Galois closure of $K$ over $\mathbb{Q}$ is the sextic field $L = \mathbb{Q}(\rho, \sqrt[3]{19})$. The primes 3 and 19 are ramified in $L$. Since $e(3) = 2$, and the quadratic subfield $E = \mathbb{Q}(\sqrt{-3})$ of $L$ has class number one, by part $(a)$ of theorem (2.3) the ideal $\Pi_3(L)$ is principal. On the other hand, $e(19) = 3$, and since the ideal $\Pi_{19}(K)$ is principal, by part $(b)$ of theorem (2.3) the ideal $\Pi_{19}(L)$ is principal. Thus $L$ is a Pólya field, while $K$ is not Pólya, since $\Pi_3(K)$ is not principal.

As another consequence of theorem (2.3), we find a relation between Pólya-ness of $L$ and Pólya-ness of the quadratic subfield $E$:

COROLLARY 2.10. *With the notation of theorem* (2.3)*,*

(a) *if $L$ is Pólya, then $E$ is also Pólya;*

(b) *if $L/E$ is unramified and $E$ is Pólya, then $L$ is also Pólya.*

*Proof.*

(a) Suppose that $L$ is Pólya and $p$ is a ramified prime in $E/\mathbb{Q}$. Hence 2 divides $e(p)$, so $e(p) = 2$ or $e(p) = 6$. Following parts $(a)$ and $(c)$ of theorem (2.3), we conclude that the ideal $\Pi_p(E)$ is principal. Hence $E$ is Pólya.

(b) Let $L/E$ be unramified. For each ramified prime $p$ in $L/\mathbb{Q}$, by lemma (2.1), if $e(p) = 3$ or $e(p) = 6$, then there exists a prime ideal of $E$ above $p$ which is ramified in $L/E$. Hence if $L/E$ is unramified, for each ramified prime $p$ in $L/\mathbb{Q}$, we have $e(p) = 2$. Thus if $E$ is a Pólya field, by part $(a)$ of theorem (2.3), so is $L$.

□

REMARK 2.11. With the notation in theorem (2.3), if $L/E$ is unramified, by class field theory, $h(E)$ is divisible by 3. Following Honda [**6**], we restate an interesting result which gives a necessary and sufficient condition for divisibility of the class number of a quadratic field by 3:

PROPOSITION 2.12 ([**6**, proposition 10]). *If the class number of a quadratic field $N$ is a multiple of 3, then $N$ must be of the form $N = \mathbf{Q}(\sqrt{4a^3 - 27b^2})$, for some $a, b \in \mathbb{Z}$. Conversely, for arbitrary $a, b \in \mathbb{Z}$, if $gcd(a, 3b) = 1$, and if $a$ cannot be represented by a form $(b + h^3)h^{-1}$ with $h \in \mathbb{Z}$, then the class number of the quadratic field $\mathbb{Q}(\sqrt{4a^3 - 27b^2})$ is a multiple of 3.*

Hence using Honda's result above and corollary (2.10), we find a simple criterion for Pólya-ness of a special class of $S_3$-extensions of $\mathbb{Q}$ as follows:

COROLLARY 2.13. *With the notation of theorem* (2.3)*, let $L$ be the splitting field of $f(x) = x^3 + ax + b$ over $\mathbb{Q}$, with $a, b \in \mathbb{Z}$ . If $gcd(a, 3b) = 1$ and $E$ is a Pólya field, then $L$ is Pólya.*

*Proof.* We show that $L/E$ is unramified and the assertion would follow from corollary (2.10). For a contradiction, assume that $\alpha$ is a prime of $E$, ramified in $L$. By

https://doi.org/10.1017/prm.2018.86 Published online by Cambridge University Press

lemma (2.1), $p = \alpha \cap \mathbb{Q}$ totally ramifies in $K/\mathbb{Q}$, which implies that $p \mid gcd(a, 3b)$, the details can be found in [**6**, Proof of Proposition 10]. □

EXAMPLE 2.14. Let $K = \mathbb{Q}(\alpha)$ where $\alpha$ is a root of $f(x) = x^3 + 10x + 1$. Denote the Galois closure of $K$ over $\mathbb{Q}$ by $L$. Here the discriminant of $f(x)$ is $-4027$, and hence the unique quadratic subfield of $L$ is $E = \mathbb{Q}(\sqrt{-4027})$, which is a Pólya field by proposition (1.4). Since $gcd(10, 3) = 1$, by corollary (2.13), $L$ is a Pólya field. Note that $h(K) = 6$, hence by proposition (1.6), $K$ is not Pólya. While for the only ramified prime 4027 in $K$, the ideal $\Pi_{4027}(K)$ is principal. (By Ostrowski's theorem [**11**] this can only happen for non-Galois number fields).

## 3. Maximum number of ramified primes

For a number field $M$, denote the number of ramified primes in $M/\mathbb{Q}$ by $s_M$. In [**8**], Leriche for any Galois Pólya number field $M$, gave an upper bound for $s_M$ which only depends on the degree of $M$ over $\mathbb{Q}$, see [**8**, proposition 2.5]. For example, for Pólya quadratic fields this upper bound is 2, which is sharp by proposition (1.4). For a cyclic Pólya number field of an odd prime power degree, the sharp upper bound is 1, see [**14**, proposition 3.2]. For biquadratic extensions of $\mathbb{Q}$ this upper bound is 5, proved to be sharp in [**5**]. For cyclic sextic Pólya number fields, by Zantema's results [**14**, proposition 3.2 and theorem 3.4] this upper bound drops to 3. For $S_3$-extensions of $\mathbb{Q}$, we prove:

THEOREM 3.1. *Let $K$ be a non-Galois cubic field with Galois closure $L$. Denote by $E$ the unique quadratic subfield of $L$. If $L$ is Pólya, then:*

(a) *for $L$ real, $s_L \leqslant 4$ and this is sharp. Moreover, if $\xi \in \mathcal{N}_{L/E}(U_L)$ where $\xi$ is the fundamental unit of $E$, then $s_L \leqslant 3$.*

(b) *for $L$ imaginary:*
   (i) *for non-pure $K$, $s_L \leqslant 2$ and this is sharp;*

   (ii) *for pure $K$, $s_L \leqslant 3$ and this is sharp. Moreover, if $\rho \in \mathcal{N}_{L/E}(U_L)$ where $\rho$ is a primitive third root of unity, then $s_L \leqslant 2$.*

*Proof.* Let $G = Gal(L/\mathbb{Q})$. Since $L$ is a Pólya Galois number field, by the exact sequence in proposition (1.2) and remark (1.3), we have:

$$\#H^1(G, U_L) = \prod_{p \mid D_L} e(p). \qquad (3.1)$$

Hence to find an upper bound for $s_L$, we give an upper bound for the order of $H^1(G, U_L)$. Let $G_2 = Gal(L/K)$ and $G_3 = Gal(L/E)$. The restriction maps

$$res : H^1(G, U_L) \to H^1(G_2, U_L),$$

and

$$res : H^1(G, U_L) \to H^1(G_3, U_L),$$

that are injective on the 2-primary and 3-primary part of $H^1(G, U_L)$, respectively, see [**10**, proposition 1.6.9]. By equality (3.1), $\#H^1(G, U_L)$ has only 2-primary and

https://doi.org/10.1017/prm.2018.86 Published online by Cambridge University Press

3-primary part. Hence:

$$\#H^1(G, U_L) \mid \#H^1(G_2, U_L).\#H^1(G_3, U_L). \tag{3.2}$$

Now for the cyclic extensions $L/K$ and $L/E$, we can use the Herbrand quotient:

$$Q(G_2, U_L) = \frac{\#\hat{H}^0(G_2, U_L)}{\#H^1(G_2, U_L)}, \quad Q(G_3, U_L) = \frac{\#\hat{H}^0(G_3, U_L)}{\#H^1(G_3, U_L)}, \tag{3.3}$$

where

$$\hat{H}^0(G_2, U_L) = U_L^{G_2}/\mathcal{N}_{L/K}(U_L) = U_K/\mathcal{N}_{L/K}(U_L),$$
$$\hat{H}^0(G_3, U_L) = U_L^{G_3}/\mathcal{N}_{L/E}(U_L) = U_E/\mathcal{N}_{L/E}(U_L).$$

On the other hand, the Herbrand quotients $Q(G_2, U_L)$ and $Q(G_3, U_L)$ are given by [**2**, proposition 5.10]:

$$Q(G_2, U_L) = \frac{2^s}{[L:K]} = 2^{s-1},$$
$$Q(G_3, U_L) = \frac{2^t}{[L:E]} = \frac{2^t}{3},$$

where $s$ (resp. $t$) is the number of infinite places of $K$ (resp. $E$) ramified in $L$. Hence

$$Q(G_2, U_L) = \begin{cases} \frac{1}{2} & : \text{L is real,} \\ 1 & : \text{L is imaginary,} \end{cases} \tag{3.4}$$

$$Q(G_3, U_L) = \frac{1}{3}. \tag{3.5}$$

Since $\mathcal{N}_{L/K}(U_L)$ (resp. $\mathcal{N}_{L/E}(U_L)$) contains $U_K^2$ (resp. $U_E^3$), Dirichlet Unit Theorem gives an upper bound for $(U_K : \mathcal{N}_{L/K}(U_L))$ and $(U_E : \mathcal{N}_{L/E}(U_L))$:

- for $L$ real, $(U_K : U_K^2) = 2^3$ and $(U_E : U_E^3) = 3$, so $(U_K : \mathcal{N}_{L/K}(U_L)) \mid 2^3$ and $(U_E : \mathcal{N}_{L/E}(U_L)) \mid 3$;
- for $L$ imaginary, $(U_K : U_K^2) = 2^2$ and $(U_E : U_E^3) \mid 3$, so $(U_K : \mathcal{N}_{L/K}(U_L))$ divides $2^2$ and $(U_E : \mathcal{N}_{L/E}(U_L)) \mid 3$.

(a) Let $E$ be real, and denote the fundamental unit of $E$ by $\xi$. By the above argument, depending on whether $\xi \in \mathcal{N}_{L/E}(U_L)$ or not, $(U_E : \mathcal{N}_{L/E}(U_L)) = 1$ or $(U_E : \mathcal{N}_{L/E}(U_L)) = 3$, respectively. Thus in this case, $\#H^1(G_2, U_L) \mid 2^4$ and depending on whether $\xi \in \mathcal{N}_{L/E}(U_L)$ or not, $\#H^1(G_3, U_L) = 3$ or $\#H^1(G_3, U_L) = 3^2$, respectively.

Now since $L$ is Pólya, by corollary (2.10), $E$ is also Pólya. By lemma (2.1), for each ramified prime $p$ in $E/\mathbb{Q}$, $e(p) = 2$ or $e(p) = 6$. On the other hand, by proposition (1.4), at most two primes ramify in $E/\mathbb{Q}$. Hence, using relation (3.2) and these arguments, we find:

https://doi.org/10.1017/prm.2018.86 Published online by Cambridge University Press

- for $L$ real and $\xi \in \mathcal{N}_{L/E}(U_L)$,

$$\#H^1(G, U_L) \mid 2^2.3^1; \tag{3.6}$$

- for $L$ real and $\xi \notin \mathcal{N}_{L/E}(U_L)$,

$$\#H^1(G, U_L) \mid 2^2.3^2. \tag{3.7}$$

By relations (3.1), (3.6) and (3.7), we find that for $\xi \in \mathcal{N}_{L/E}(U_L)$ (resp. $\xi \notin \mathcal{N}_{L/E}(U_L)$), $s_L \leqslant 3$ (resp. $s_L \leqslant 4$). Example (3.3) below shows that this upper bound is sharp and the statement in part $(a)$ is proved.

(b) Let $L$ be imaginary and Pólya. By corollary (2.10), $E$ is an imaginary quadratic Pólya field. Hence by proposition (1.4), there is only one ramified prime $p$ in $E/\mathbb{Q}$, and by lemma (2.1), $e(p) = 2$ or $e(p) = 6$, which implies that 2-primary part of $H^1(G, U_L)$ has order 2. Also, one can show that for $E = \mathbb{Q}(\sqrt{d})$, $U_E = \{\pm 1\}$, except for $d = -1, -3$ where $U_E = \{\pm 1 \pm i\}$ and $U_E = \{\pm 1 \pm \rho, \pm \rho^2\}$, respectively.

(i) If $K$ is not pure, then $E \neq \mathbb{Q}(\sqrt{-3})$ and $U_E = \mathcal{N}_{L/E}(U_L)$, since $\mathcal{N}_{L/E}(-1) = -1$ and for $E = \mathbb{Q}(\sqrt{-1})$, $\mathcal{N}_{L/E}(-i) = i$. Hence $\#\hat{H}^0(G_3, U_L) = 1$. Using relation (3.5), we have $\#H^1(G_3, U_L) = 3$. Therefore, in this case, we have

$$\#H^1(G, U_L) \mid 2^1.3^1,$$

and using relation (3.1), we find that for $K$ non-pure, $s_L \leqslant 2$.

To show that $s_L = 2$ occurs, let $p$ be an odd prime number such that $q = 4p + 27$ is also prime. Let $K = \mathbb{Q}(\theta)$ where $\theta$ is a root of $f(x) = x^3 + px + p$. By Eisenstein's Criterion $f(x)$ is irreducible over $\mathbb{Q}$, and discriminant of $f(x)$ is $d_f = -p^2(4p + 27)$. Hence $K$ is non-Galois and since $q > 3$, it is not pure either. Only $p$ can totally ramify in $K/\mathbb{Q}$ and this happens if $D_K = d_f$, see the argument in the beginning of § 2. Moreover, let $\Pi_p(K)$ be principal, for instance, we can assume $h(K)$ is not divisible by 3. Also by proposition (1.4), the unique quadratic subfield $E = \mathbb{Q}(\sqrt{-q})$ of $L$ is Pólya. With these assumptions and using theorem (2.3), $L$ is a Pólya $S_3$-extension of $\mathbb{Q}$ with $s_L = 2$. All these requirements are satisfied if for example $p = 5, 11, 41, 59, 71, 83, 89$.

(ii) Let $K$ be pure. Hence $E = \mathbb{Q}(\sqrt{-3})$. In this case, depending on whether $\rho \in \mathcal{N}_{L/E}(U_L)$ or not, $(U_E : \mathcal{N}_{L/E}(U_L)) = 1$ or $(U_E : \mathcal{N}_{L/E}(U_L)) = 3$, respectively. Using an argument similar to part $(i)$, we find:

- if $\rho \in \mathcal{N}_{L/E}(U_L)$, then

$$\#H^1(G, U_L) \mid 2^1.3^1; \tag{3.8}$$

- if $\rho \notin \mathcal{N}_{L/E}(U_L)$, then

$$\#H^1(G, U_L) \mid 2^1.3^2; \tag{3.9}$$

By relations (3.1), (3.8) and (3.9), the statement is proved.

Now we show that if $\rho \notin \mathcal{N}_{L/E}(U_L)$, the $s_L$ can be 3. Let $K = \mathbb{Q}(\sqrt[3]{n})$, where $n$ is a cube free integer. Following Honda [7], let $n = pq$ where $p$ and $q$ are prime

https://doi.org/10.1017/prm.2018.86 Published online by Cambridge University Press

numbers such that $p \equiv 2 (\bmod 9)$ and $q \equiv 5 (\bmod 9)$. We have $D_K = -3p^2q^2$, hence $e(p) = e(q) = 3$ and $e(3) = 2$, see [7]. One can show that $h(K)$ is not divisible by 3, see [7, theorem, page 8]. Hence $\Pi_p(K)$ and $\Pi_q(K)$ are principal, and by theorem (2.3), $\Pi_p(L)$ and $\Pi_q(L)$ are principal. Also $E = \mathbb{Q}(\sqrt{-3})$ is Pólya, hence again by theorem (2.3), $\Pi_3(L)$ is principal. Therefore $L = \mathbb{Q}(\rho, \sqrt[3]{pq})$ is a Pólya $S_3$-extension of $\mathbb{Q}$ with $s_L = 3$. □

Remark 3.2. One can find some examples of real Pólya $S_3$-extensions of $\mathbb{Q}$ with four ramified primes:

Example 3.3. Let $K$ be $\mathbb{Q}(\theta)$, where $\theta$ is a root of $f(x) = x^3 - 20x - 30$. We have $D_K = 2^2.5^2.7.11$, and so $K$ is a non-Galois cubic field. As before, denote the Galois closure of $K$ over $\mathbb{Q}$ by $L$, and denote by $E$ the unique quadratic subfield of $L$. Hence $E = \mathbb{Q}(\sqrt{77})$, which is a real quadratic Pólya field by proposition (1.4). Also, $h(K) = 1$, and hence $K$ is a Pólya field. Thus by corollary (2.5), $L$ is a real Pólya $S_3$-extension of $\mathbb{Q}$ with $s_L = 4$.

## 4. On divisibility of Class numbers

Following Masley [9], we define:

Definition 4.1 (See [9]). We call an extension $M/N$ totally ramified if no subextension of $M/N$ except $N$ itself is unramified over $N$.

Proposition 4.2 ([9, corollary 2.3]). *Suppose an extension $M/N$ of number fields is totally ramified. Then $h(N)$ divides $h(M)$.*

In the special case that $[M : N]$ is a prime number and $M/N$ is ramified, $M/N$ is a totally ramified extension. Therefore:

Corollary 4.3. *Let $K$ be a non-Galois cubic number field. Let $L$ be the Galois closure of $K$ over $\mathbb{Q}$. Then $h(K)$ divides $h(L)$.*

*Proof.* Denote by $E$ the unique quadratic subfield of $L$, and let $p$ be a ramified prime in $E/\mathbb{Q}$. By lemma (2.1), two cases are possible:

Case 1) $e(p) = 2$. By lemma (2.1), we have:

$$p\mathcal{O}_K = \beta_1\beta_2^2,$$
$$p\mathcal{O}_L = (\gamma_1\gamma_2\gamma_3)^2.$$

Hence $\beta_1$ is ramified in the extension $L/K$.

Case 2) $e(p) = 6$. By lemma (2.1), $p = 3$ and ramifies totally in $L/\mathbb{Q}$ and $K/\mathbb{Q}$, say $3\mathcal{O}_L = \gamma^6$ and $3\mathcal{O}_K = \beta^3$. Thus we have $\beta\mathcal{O}_L = \gamma^2$, which implies that $\beta$ is ramified in the extension $L/K$.

Thus $L/K$ is a totally ramified extension and the statement follows from proposition (4.2). □

https://doi.org/10.1017/prm.2018.86 Published online by Cambridge University Press

As a consequence, we find that in a special case, the converse of the corollary (2.5) holds:

Corollary 4.4. *Let $K$ be a non-Galois cubic number field. Denote the Galois closure of $K$ over $\mathbb{Q}$ by $L$, and denote by $E$ the unique quadratic subfield of $L$. If $h_L = 1$, then both subfields $E$ and $K$ of $L$ are Pólya.*

*Proof.* If $h_L = 1$ by corollary (4.3), $h_K = 1$. Hence $K$ is a Pólya field. Pólya-ness of $E$ follows from part $(a)$ of the corollary (2.10). □


## Acknowledgements

The authors would like to thank the anonymous referee for corrections and comments that significantly improved the original draft. The second author's research was in part supported by a grant from IPM (No. 95110131).


## References


1 M. Bhargava. $P$-orderings and polynomial functions on arbitrary subsets of Dedekind rings. *J. Reine Angew. Math.* **490** (1997), 101–127.

2 N. Childress. *Class field theory* (New York: Springer, 2009).

3 B. Heidaryan and A. Rajaei. Biquadratic Pólya fields with only one quadratic Pólya subfield. *J. Number Theory* **143** (2014), 279–285.

4 B. Heidaryan and A. Rajaei. Some non-Pólya biquadratic fields with low ramification. To appear in Rev. Mat. Iberoam.

5 B. Heidaryan and A. Rajaei. Biquadratic Pólya fields with no quadratic Pólya subfields and maximum ramification. Preprint.

6 T. Honda. Isogenies, rational points and section points of group varieties. *Japan. J. Math.* **30** (1960), 84–101.

7 T. Honda. Pure cubic fields whose class numbers are multiples of three. *J. Number Theory* **3** (1971), 7–12.

8 A. Leriche. Cubic, quartic and sextic Pólya fields. *J. Number Theory* **133** (2013), 59–71.

9 J. M. Masley. Class numbers of real cyclic number fields with small conductor. *Compositio Math.* **37** (1978), 297–319.

10 J. Neukirch, A. Schmidt and K. Wingberg. *Cohomology of number fields* (Berlin: Springer-Verlag, 2008).

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

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

13 J. P. Serre. *Local fields* (New York-Berlin: Springer-Verlag, 1979).

14 H. Zantema. Integer valued polynomials over a number field. *Manuscripta Math.* **40** (1982), 155–203.