Bull. Aust. Math. Soc. (First published online 2024), page 1 of 12*
doi:10.1017/S0004972724000108
*Provisional—final page numbers to be inserted when paper edition is published

NON-PÓLYA FIELDS WITH LARGE PÓLYA GROUPS ARISING FROM LEHMER QUINTICS

NIMISH KUMAR MAHAPATRA and PREM PRAKASH PANDEY

(Received 26 December 2023; accepted 14 January 2024)

Abstract

We construct a new family of quintic non-Pólya fields with large Pólya groups. We show that the Pólya number of such a field never exceeds five times the size of its Pólya group. Finally, we show that these non-Pólya fields are nonmonogenic of field index one.

2020 *Mathematics subject classification*: primary 11R29; secondary 11R04, 11R20.

Keywords and phrases: Pólya field, Pólya group, Hilbert class field, genus field.

1. Introduction

Let K be an algebraic number field and $\mathcal{O}_K$ be its ring of integers. Let $Int(\mathcal{O}_K) = \{f \in K[X] \mid f(\mathcal{O}_K) \subseteq \mathcal{O}_K\}$ be the ring of integer-valued polynomials on $\mathcal{O}_K$. Then the number field K is said to be a Pólya field if the $\mathcal{O}_K$-module $Int(\mathcal{O}_K)$ has a regular basis, that is, a basis (f_n) such that for each $n \in \mathbb{N} \cup \{0\}$, degree $(f_n) = n$ (see [26]). For each $n \in \mathbb{N}$, the leading coefficients of the polynomials in $Int(\mathcal{O}_K)$ of degree n together with zero form a fractional ideal of $\mathcal{O}_K$, denoted by $\mathfrak{J}_n(K)$. The following result establishes a connection between $\mathfrak{J}_n(K)$ and the Pólya-ness of the number field K.

PROPOSITION 1.1 [1, Proposition II.1.4]. *A number field K is a Pólya field if and only if $\mathfrak{J}_n(K)$ is principal for every integer $n \geq 1$.*

It follows immediately from Proposition 1.1 that if the class number of K is one, then K is a Pólya field. However, the converse is not valid in general. That is, if the class number h_K of K is not one, then we cannot decide whether K is a Pólya field or not: for instance, every cyclotomic field is a Pólya field (see [26, Proposition 2.6]).

Let $Cl(K)$ denote the ideal class group of K. For each integer $n \geq 1$, let $[\mathfrak{J}_n(K)]$ be the ideal class in $Cl(K)$ corresponding to the fractional ideal $\mathfrak{J}_n(K)$. The Pólya group

N.K.M. would like to acknowledge financial support from the University Grants Commission (UGC), Government of India.

$Po(K)$ of K is defined to be the subgroup of $Cl(K)$ generated by the elements $[\mathfrak{I}_n(K)]$ in $Cl(K)$. Therefore, K is a Pólya field if and only if $Po(K) = \{1\}$.

It is an interesting problem to look for explicit families of number fields that are Pólya or non-Pólya (for example, see [9, 10, 19, 23]). The classification of Pólya fields of low degree is of significant interest. Towards this, Zantema [26] completely characterised quadratic Pólya fields.

PROPOSITION 1.2 [26, Example 3.3]. *Let p and q be two distinct odd primes. A quadratic field $\mathbb{Q}(\sqrt{d})$ is a Pólya field if and only if d is of one of the following forms:*

(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* $p \equiv 1 \pmod 4$.

REMARK 1.3. The classification of quadratic Pólya fields can also be obtained from Hilbert's theorems (see [13, Satz 105 and Satz 106]).

Leriche [17] completely classified Galois cubic Pólya fields. In the same article, Leriche also classified cyclic quartic and cyclic sextic Pólya fields. Moreover, she obtained similar classifications for some more families of bi-quadratic and sextic fields (see [17, Theorems 5.1 and 6.2]). Recently, there have been several attempts to provide families of Pólya and non-Pólya fields in the remaining cases of bi-quadratic extensions (see [9, 10, 19, 23]). In [3], the authors constructed a new family of totally real bi-quadratic fields with large Pólya groups.

In this article, we characterise the Pólya-ness of a special family of quintic fields arising from Lehmer qunitics. For each integer $n \in \mathbb{Z}$, the Lehmer quintic $f_n(x) \in \mathbb{Z}[x]$ is defined by

$$f_n(x) = x^5 + n^2x^4 - (2n^3 + 6n^2 + 10n + 10)x^3 + (n^4 + 5n^3 + 11n^2 + 15n + 5)x^2 \\ + (n^3 + 4n^2 + 10n + 10)x + 1.$$

Let $\theta_n \in \mathbb{C}$ be a root of $f_n(x) = 0$. If we set $K_n = \mathbb{Q}(\theta_n)$, then $[K_n : \mathbb{Q}] = 5$ and the fields K_n are called Lehmer quintic fields [16]. Our main theorem is the following result.

THEOREM 1.4. *Let $\{K_n\}$ be the family of Lehmer quintic fields. If $m_n = n^4 + 5n^3 + 15n^2 + 25n + 25$ is cube free, then:*

(1) *K_n is a Pólya field if and only if m_n is a prime or $m_n = 25$;*
(2) *$Po(K_n) \simeq (\mathbb{Z}/5\mathbb{Z})^{\omega(m_n)-1}$, where $\omega(t)$ is the number of distinct prime divisors of t.*

Moreover, there are infinitely many non-Pólya fields in the family $\{K_n\}$.

Let G be a finite group. If $m > 1$ is an integer, then the m-rank of G is the maximal integer r such that $(\mathbb{Z}/m\mathbb{Z})^r$ is a subgroup of G. The following folklore conjecture is widely believed to be true but it is still open.

https://doi.org/10.1017/S0004972724000108 Published online by Cambridge University Press

CONJECTURE 1.5 [5, Conjecture 1.1]. Let $d > 1$ and $m > 1$ be two integers. Then the m-rank of the class group of K is unbounded when K runs through the number fields of degree $[K : \mathbb{Q}] = d$.

It is known that when $m = d$, or more generally when $m \mid d$, this conjecture follows from class field theory (see [5, Conjecture 1.1]). The following corollary to Theorem 1.4 gives an alternative and elementary proof of the conjecture for the case $m = d = 5$.

COROLLARY 1.6. *The 5-ranks of the class groups of the non-Pólya Lehmer quintic fields K_n are unbounded.*

Recall the classical embedding problem: is every number field K contained in a field L with class number one? In 1964, Golod and Shafarevich [6] gave a negative answer to this question. The corresponding embedding problem for Pólya fields was confirmed affirmatively by Leriche [18]. Leriche proved that every number field is contained in a Pólya field, namely its Hilbert class field (see, [18, Theorem 3.3]).

A minimal Pólya field over K is a field extension L of K which is a Pólya field and such that no intermediate field $K \subseteq M \subsetneq L$ is a Pólya field.

DEFINITION 1.7. [18, Definition 6.1] The Pólya number of K is

$$po_K = \min\{[L : K] \mid K \subseteq L,\ L \text{ is a Pólya field}\}.$$

We study the Pólya number po_{K_n} of the non-Pólya field K_n and obtain an upper bound for po_{K_n} in terms of the size of the corresponding Pólya group $Po(K_n)$.

THEOREM 1.8. *Let K_n be the family of Lehmer quintic fields such that m_n is cube-free. Then $po_{K_n} \leq 5|Po(K_n)|$.*

Let K be a number field and $\theta \in \mathcal{O}_K$ be a primitive element. The index $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ is called the index of θ in K and is denoted by $I(\theta)$. The index of the number field K is defined by $I(K) = \gcd\{I(\theta) \mid \theta \in \mathcal{O}_K \text{ and } K = \mathbb{Q}(\theta)\}$. If $I(K) > 1$, then the number field K is not monogenic, that is, $\mathcal{O}_K \neq \mathbb{Z}[\theta]$ for any $\theta \in K$. However, the converse is not true in general. That is, there exist nonmonogenic number fields K with $I(K) = 1$. These are basically fields which are not monogenic, but not for a local reason (see [25] for more details). In this direction, we prove the following result.

THEOREM 1.9. *Let $\{K_n\}$ be the family of non-Pólya Lehmer quintic fields such that m_n is cube-free. Then K_n is not monogenic and $I(K_n) = 1$.*

In Section 2, we develop some preliminaries required to prove Theorem 1.4. Section 3 contains the proofs of Theorem 1.4 and Corollary 1.6. In Section 4, we study the Pólya numbers of Lehmer quintic fields and prove Theorem 1.8. In the same section, we also study the monogenicity of the non-Pólya number fields K_n and

https://doi.org/10.1017/S0004972724000108 Published online by Cambridge University Press

give the proof of Theorem 1.9. Finally, in Section 5, we present some computations performed with SageMath.

2. Preliminaries

In this section, we assume that the number field K is a finite Galois extension of $\mathbb{Q}$ and for any prime number p, we denote the ramification index of p in $K/\mathbb{Q}$ by e_p.

In [2], Chabert obtained a nice description for the cardinality of $Po(K)$ for cyclic extensions $K/\mathbb{Q}$.

PROPOSITION 2.1 [2, 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 $|Po(K)| = (\prod_p e_p)/(2n)$.*
(2) *In all other cases, $|Po(K)| = (\prod_p e_p)/n$.*

When K is a cyclic number field of odd degree, all ramification indices e_p are odd and case (1) of Proposition 2.1 does not occur. We record this in the following corollary.

COROLLARY 2.2. *If $K/\mathbb{Q}$ is a cyclic extension of degree n and n is odd, then $|Po(K)| = (\prod_p e_p)/n$.*

Zantema [26, Section 3] showed that $Po(K)$ is the subgroup of $Cl(K)$ generated by the classes of the ambiguous ideals of K. In other words,

$$Po(K) = \{[\mathfrak{a}] \in Cl(K) : \mathfrak{a}^\tau = \mathfrak{a} \text{ for all } \tau \in \mathrm{Gal}(K/\mathbb{Q})\}.$$

Next, we state some results on Lehmer quintics and their discriminants. In [22], Schoof and Washington showed that $f_n(x)$ is irreducible for all $n \in \mathbb{Z}$ and its discriminant is $(n^3 + 5n^2 + 10n + 7)^2(n^4 + 5n^3 + 15n^2 + 25n + 25)^4$. Let $\theta_n \in \mathbb{C}$ be a root of $f_n(x) = 0$. If we set $K_n = \mathbb{Q}(\theta_n)$, then K_n is a cyclic field for all $n \in \mathbb{Z}$ [22, Theorem 3.5]. We denote the ring of integers of K_n by $\mathcal{O}_{K_n}$. Now we recall some results of Jeannin [15] on the discriminant $d(K_n)$ of K_n.

LEMMA 2.3 [15, Lemme 2.1.1]. *All the prime divisors $p \neq 5$ of $n^4 + 5n^3 + 15n^2 + 25n + 25$ satisfy $p \equiv 1 \pmod 5$.*

LEMMA 2.4 [15, Théorème 2.2.1]. *The discriminant $d(K_n) = f(K_n)^4$, where the conductor $f(K_n)$ of K_n is given by*

$$f(K_n) = 5^b \prod_{\substack{p \equiv 1 \pmod 5 \\ v_p(n^4+5n^3+15n^2+25n+25) \not\equiv 0 \pmod 5}} p. \tag{2.1}$$

https://doi.org/10.1017/S0004972724000108 Published online by Cambridge University Press

Here $v_p(k)$ denotes the exponent of the highest power of the prime p dividing a nonzero integer k and

$$b = \begin{cases} 0 & \text{if } 5 \nmid n, \\ 2 & \text{if } 5 \mid n. \end{cases} \tag{2.2}$$

We quote the following result due to Erdős [4] which plays a crucial role in the proof of our main theorem.

THEOREM 2.5 [4, Section 1]. *Let $f(x)$ be a polynomial of degree $d \geq 3$ whose coefficients are integers with highest common factor 1 and whose leading coefficient is positive. Assume that $f(x)$ is not divisible by the $(d-1)$th power of a linear polynomial with integer coefficients. Then there are infinitely many positive integers n for which $f(n)$ is $(d-1)$th power free.*

Next we state a deep result on power-free values of polynomials (see [11, 12, 21]).

THEOREM 2.6 [21, Theorem 1]. *Let $f(x) \in \mathbb{Z}[x]$ be an irreducible polynomial of degree $d \geq 3$ and assume that f has no fixed $(d-1)$th power prime divisor. Define*

$$N'_f(X) = \#\{p \leq X : p \text{ prime}, f(p) \text{ is } (d-1)\text{-free}\}.$$

Then, for any $C > 1$,

$$N'_f(X) = c'_f \pi(X) + O_{C,f}\Big(\frac{X}{(\log X)^C}\Big),$$

as $x \to \infty$, where

$$c'_f = \prod_p \Big(1 - \frac{\rho'(p^{d-1})}{\phi(p^{d-1})}\Big)$$

and $\rho'(d) = \#\{n \ (\mathrm{mod}\ d) : (d,n) = 1, d \mid f(n)\}$.

Let $f(x)$ be an irreducible polynomial with integral coefficients and $f(m) > 0$ for $m = 1, 2, \ldots$. Let $\omega(m)$ denote the number of distinct primes dividing m. For primes p, the following result due to Halberstam [8] determines the distribution of values of $\omega(f(p))$.

THEOREM 2.7 [8, Theorem 2]. *Let $f(X) \in \mathbb{Z}[X]$ be any nonconstant polynomial. For all but $o(X/\log X)$ primes $p \leq X$,*

$$\omega(f(p)) = (1 + o(1))\log\log X.$$

Now we state some results on the number of integral solutions of a Diophantine equation of the type

$$Y^m = f(X). \tag{2.3}$$

When $m = 2$ and $f(x)$ is a monic quartic polynomial, the following result due to Masser [20] gives a specific bound for integral points on the curve.

THEOREM 2.8 [20]. *Consider the Diophantine equation $Y^2 = f(X)$, where $f(X)$ is a polynomial of degree four with integer coefficients. Assume that $f(X)$ is monic and its discriminant is not a perfect square. Then any integer solution (x, y) of the equation satisfies $|x| \leq 26H(f)^3$, where $H(f)$ denotes the maximum of the absolute values of the coefficients of $f(X)$.*

3. Proof of Theorem 1.4

PROOF. We consider the set

$$\mathcal{P} = \{n \in \mathbb{Z} : m_n = n^4 + 5n^3 + 15n^2 + 25n + 25 \text{ is a cube-free integer}\}.$$

For $n \in \mathcal{P}$,

$$m_n = 5^b AB^2. \tag{3.1}$$

Here $b = 0$ if n is not divisible by 5 and $b = 2$ otherwise, and A, B are square-free natural numbers which are relatively prime and $5 \nmid AB$. From Lemma 2.3 and (2.1),

$$f(K_n) = 5^b AB \quad \text{and} \quad d(K_n) = (5^b AB)^4. \tag{3.2}$$

Since $K_n/\mathbb{Q}$ is Galois and of degree 5, we see that for any prime p, the ramification index e_p of p in K_n is given by

$$e_p = \begin{cases} 5 & \text{if } p \mid 5AB, \\ 1 & \text{otherwise.} \end{cases}$$

Thus,

$$\prod_p e_p = 5^{\omega(d(K_n))} = 5^{\omega(m_n)}. \tag{3.3}$$

Now from Corollary 2.2,

$$|Po(K_n)| = 5^{\omega(m_n)-1}. \tag{3.4}$$

Thus, for $n \in \mathcal{P}$, the Lehmer quintic field K_n is a Pólya field if and only if m_n is a prime or a square of a prime. We claim that m_n is a square of a prime if and only if $m_n = 25$. This claim will prove Theorem 1.4(1). To prove the claim, consider the curve

$$Y^2 = f(X) = X^4 + 5X^3 + 15X^2 + 25X + 25. \tag{3.5}$$

From Theorem 2.8, any integral solution (x, y) of (3.5) satisfies

$$|x| \leq 26 \times 25^3 = 406250.$$

Using a SageMath program, we find that for $x \in [-406250, 406250]$, the only integral point on the curve $Y^2 = f(X)$ is $(X, Y) = (0, 5)$. In other words, m_n is not a square for any nonzero integer n unless $m_n = 25$. This establishes the claim.

https://doi.org/10.1017/S0004972724000108 Published online by Cambridge University Press

We have $\mathrm{Gal}(K_n/\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z}$. Let σ be a generator of $\mathrm{Gal}(K_n/\mathbb{Q})$ and $[\mathfrak{I}] \neq [1]$ be an ambiguous ideal class in K_n. Then

$$[\mathfrak{I}]^5 = [\mathfrak{I}][\mathfrak{I}][\mathfrak{I}][\mathfrak{I}][\mathfrak{I}] = [\mathfrak{I}][\mathfrak{I}]^{\sigma}[\mathfrak{I}]^{\sigma^2}[\mathfrak{I}]^{\sigma^3}[\mathfrak{I}]^{\sigma^4} = [N(\mathfrak{I})] = [1],$$

where $N(\mathfrak{I}) \in \mathbb{Q}$ denotes the norm of the ideal $\mathfrak{I}$. We conclude that the order of any nontrivial ambiguous ideal class in the class group of K_n is 5. From the structure theorem for abelian groups,

$$Po(K_n) \simeq \left(\frac{\mathbb{Z}}{5\mathbb{Z}}\right)^{\omega(m_n)-1}.$$

This completes the proof of Theorem 1.4(2).

From (3.1), we see that m_n cannot be a prime whenever $5 \mid n$. Thus, K_n is a non-Pólya field whenever $n \neq 0, 5 \mid n$ and $n \in \mathcal{P}$. Next we show that there are infinitely many such n. To do this, we show that there are infinitely many k such that m_{5k} is cube-free. Note that

$$\begin{aligned} m_{5k} &= (5k)^4 + 5(5k)^3 + 15(5k)^2 + 25(5k) + 25 \\ &= 25(25k^4 + 25k^3 + 15k^2 + 5k + 1) = 25g(k). \end{aligned} \tag{3.6}$$

If $h(k) = ak + b$ is a linear polynomial such that $h(k)^3 \mid g(k)$, then for $t = -b/a \in \mathbb{Q}$,

$$g(t) = 0 \implies 25t^4 + 25t^3 + 15t^2 + 5t + 1 = 0, \tag{3.7}$$

$$g'(t) = 0 \implies 100t^3 + 75t^2 + 30t + 5 = 0, \tag{3.8}$$

$$g''(t) = 0 \implies 300t^2 + 150t + 30 = 0. \tag{3.9}$$

This contradicts the fact that $t \in \mathbb{Q}$. Thus, from Theorem 2.5, it follows that $g(k)$ is cube-free for infinitely many k. Since $5 \nmid g(k)$ for all k, it follows that m_{5k} is cube-free for infinitely many integers k. This proves that $\mathcal{P}$ is an infinite set and completes the proof of the theorem. □

REMARK 3.1. From the proof of Theorem 1.4, it follows that for any $n \neq 0$, the Lehmer quintic field K_{5n} is non-Pólya whenever m_{5n} is cube-free. However, there are non-Pólya fields K_{5n} with m_{5n} not being cube-free (see the entry for $n = -53$ in Table 1).

Conjecturally, there are infinitely many $n \in \mathbb{Z}$ such that m_n is prime and thus the family $\{K_n\}$ should have infinitely many Pólya fields. Under the assumption that m_n is cube-free, Theorem 1.4 asserts that there are infinitely many Pólya fields in the family K_n only if there are infinitely many primes of the form m_n.

PROOF OF COROLLARY 1.6. From the above remark, it is enough to find integers n such that m_{5n} is cube-free and $\omega(m_{5n})$ goes to infinity as n goes to infinity. Let $g(k) = (25k^4 + 25k^3 + 15k^2 + 5k + 1)$. From Theorem 2.6, for a positive proportion of primes p, we see that $g(p)$ is cube-free. Consequently, m_{5p} is cube-free for a positive proportion of prime numbers p. Now, we only consider those primes p such that m_{5p} is cube-free. There is a positive constant c such that for any large real number X, there are at least $cX/\log X$ many primes. From Theorem 2.7, it follows that $\omega(m_{5p})$ goes to infinity as p goes to infinity. □

https://doi.org/10.1017/S0004972724000108 Published online by Cambridge University Press

TABLE 1. Family of non-Pólya fields.

n	m_{5n}	$C_{m_{5n}}$	$\#Po(K_{5n})$
−60	7966342525	1	5^2
−59	7446286775	1	5^2
−58	6952119275	1	5^2
−57	6482966275	1	5^2
−56	6037969025	1	5^3
−55	5616283775	1	5^2
−54	5217081775	1	5^3
−53	**4839549275**	**1331**	$\mathbf{5^2}$
−52	4482887525	1	5^3
−51	4146312775	1	5^4
−50	3829056275	1	5^3
−49	3530364275	1	5^2
−48	3249498025	1	5^1
−47	2985733775	1	5^3
−46	2738362775	1	5^2
−45	2506691275	1	5^2
−44	2290040525	1	5^2
−43	2087746775	1	5^2
−42	1899161275	1	5^2
−41	1723650275	1	5^2
−40	1560595025	1	5^4
−39	1409391775	1	5^2
−38	1269451775	1	5^2
−37	1140201275	1	5^1
−36	1021081525	1	5^2
−35	911548775	1	5^2
−34	811074275	1	5^2
−33	719144275	1	5^1
−32	635260025	1	5^1
−31	558937775	1	5^3
−30	489708775	1	5^2
−29	427119275	1	5^3
−28	370730525	1	5^2
−27	320118775	1	5^2
−26	274875275	1	5^2
−25	234606275	1	5^1
−24	198933025	1	5^3
−23	167491775	1	5^3
−22	139933775	1	5^1

n	m_{5n}	$C_{m_{5n}}$	$\#Po(K_{5n})$
1	1775	1	5^1
2	16775	1	5^2
3	71275	1	5^1
4	206525	1	5^2
5	478775	1	5^2
6	959275	1	5^1
7	1734275	1	5^1
8	2905025	1	5^1
9	4587775	1	5^1
10	6913775	1	5^3
11	10029275	1	5^2
12	14095525	1	5^1
13	19288775	1	5^2
14	25800275	1	5^2
15	33836275	1	5^3
16	43618025	1	5^2
17	55381775	1	5^3
18	69378775	1	5^2
19	85875275	1	5^1
20	105152525	1	5^1
21	127506775	1	5^3
22	153249275	1	5^2
23	182706275	1	5^1
24	216219025	1	5^2
25	254143775	1	5^3
26	296851775	1	5^2
27	344729275	1	5^3
28	398177525	1	5^2
29	457612775	1	5^1
30	523466275	1	5^2
31	596184275	1	5^2
32	676228025	1	5^2
33	764073775	1	5^1
34	860212775	1	5^2
35	965151275	1	5^3
36	1079410525	1	5^2
37	1203526775	1	5^2
38	1338051275	1	5^3
39	1483550275	1	5^2

Continued

https://doi.org/10.1017/S0004972724000108 Published online by Cambridge University Press

TABLE 1. Continued.

n	m_{5n}	$C_{m_{5n}}$	$Po(K_{5n})$	n	m_{5n}	$C_{m_{5n}}$	$Po(K_{5n})$
−21	115925275	1	5^3	40	1640605025	1	5^2
−20	95147525	1	5^3	41	1809811775	1	5^2
−19	77296775	1	5^2	42	1991781775	1	5^3
−18	62084275	1	5^3	43	2187141275	1	5^4
−17	49236275	1	5^2	44	2396531525	1	5^1
−16	38494025	1	5^2	45	2620608775	1	5^2
−15	29613775	1	5^1	46	2860044275	1	5^2
−14	22366775	1	5^2	47	3115524275	1	5^3
−13	16539275	1	5^2	48	3387750025	1	5^3
−12	11932525	1	5^2	49	3677437775	1	5^4
−11	8362775	1	5^1	50	3985318775	1	5^1
−10	5661275	1	5^1	51	4312139275	1	5^1
−9	3674275	1	5^3	52	4658660525	1	5^2
−8	2263025	1	5^2	53	5025658775	1	5^2
−7	1303775	1	5^2	54	5413925275	1	5^2
−6	687775	1	5^3	55	5824266275	1	5^3
−5	321275	1	5^2	56	6257503025	1	5^3
−4	125525	1	5^1	57	6714471775	1	5^3
−3	36775	1	5^1	58	7196023775	1	5^2
−2	6275	1	5^1	59	7703025275	1	5^3
−1	275	1	5^1	60	8236357525	1	5^2

4. Pólya numbers and monogenicity of Lehmer quintic fields

The genus field (respectively, genus field in the narrow sense) of K is the maximal abelian extension Γ_K (respectively, Γ'_K) of K which is a compositum of K with an absolute abelian number field and is unramified over K at all places (respectively, all finite places) of K. The genus number of K is defined to be the degree $g_K = [\Gamma_K : K]$. If K is abelian, then Leriche showed that the genus field Γ_K is Pólya and hence

$$po_K \leq g_K, \tag{4.1}$$

where po_K denotes the Pólya number of K. However, Zantema proved that both the cyclotomic and real cyclotomic fields are Pólya fields [26]. Thus, for abelian number fields K, if f is the conductor of K and $\phi(f)$ is the value of the Euler totient function, then

$$po_K \leq \frac{\phi(f)}{[K:\mathbb{Q}]} \quad \text{and} \quad po_K \leq \frac{\phi(f)}{2[K:\mathbb{Q}]} \quad \text{if } K \text{ is real.} \tag{4.2}$$

https://doi.org/10.1017/S0004972724000108 Published online by Cambridge University Press

For the general case, when K is a Galois number field (not necessarily abelian) with class number h_K,

$$po_K \leq h_K. \tag{4.3}$$

To prove Theorem 1.8, we need the following result due to Ishida [14] on the genus number of a cyclic number field of prime degree.

THEOREM 4.1 [14, Theorem 5]. *Let K be a cyclic number field of degree q, where q is an odd prime. If t is the number of primes p such that p is totally ramified in K, then the genus number g_K of K is*

$$g_K = \begin{cases} q^t & \text{if } q \text{ is totally ramified in } K, \\ q^{t-1} & \text{otherwise.} \end{cases}$$

PROOF OF THEOREM 1.8. We have already seen in the proof of Theorem 1.4 that the number of primes p such that p is totally ramified in K_n is $\omega(m_n)$. Now applying Theorem 4.1 to the family of number fields K_n,

$$g_{K_n} = 5^{\omega(m_n)} \implies po_{K_n} \leq 5^{\omega(m_n)}. \tag{4.4}$$

Substituting (3.4) in (4.4),

$$po_{K_n} \leq 5|Po(K_n)|.$$

□

REMARK 4.2. Generally, po_K and $Po(K)$ are mutually independent, but here in the case of non-Pólya Lehmer quintic fields, we have an unexpected relation.

To prove Theorem 1.9, we need the following result of Gras [7] on the monogenicity of cyclic number fields of prime degree.

PROPOSITION 4.3 [7, Section 5]. *If K is a cyclic number field of prime degree $p \geq 5$, then K is monogenic only if $2p + 1$ is prime and it is the maximal real subfield of the cyclotomic field $\mathbb{Q}(\zeta_{2p+1})$.*

Lastly, we recall a result of von Zylinski [24].

PROPOSITION 4.4 [24]. *If K is a number field of degree n, then $I(K)$ has only prime divisors p satisfying $p < n$.*

PROOF OF THEOREM 1.9. Let K_n be the family of non-Pólya Lehmer quintic fields. We know that $\mathrm{Gal}(K_n/\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z}$. From Theorem 1.4,

$$|Po(K_n)| \geq 5. \tag{4.5}$$

Since real cyclotomic fields are Pólya fields, K_n never occurs as the maximal real subfield of a cyclotomic field. From Proposition 4.3, it follows that K_n is not monogenic.

https://doi.org/10.1017/S0004972724000108 Published online by Cambridge University Press

Next, we aim to show $I(K_n) = 1$ for all nonzero n for which K_n is non-Pólya. We recall the relation

$$d(\theta_n) = [I(\theta_n)]^2 d(K_n). \tag{4.6}$$

As mentioned earlier,

$$d(\theta_n) = (n^3 + 5n^2 + 10n + 7)^2 (n^4 + 5n^3 + 15n^2 + 25n + 25)^4.$$

From Lemma 2.3, $(n^4 + 5n^3 + 15n^2 + 25n + 25)$ is not divisible by 2 or 3. It is easily seen that $(n^3 + 5n^2 + 10n + 7)$ is also not divisible by 2 or 3. Consequently, we conclude that $I(\theta_n)$ is not divisible by 2 or 3. Now, from the result of Zylinski, it follows that $I(\theta_n) = 1$. □

5. Computation

The computations summarised in Table 1 show that there are many non-Pólya fields in the family K_{5n}. For $n \in \{-60, -59, \ldots, 59, 60\}$, we see that m_{5n} is cube-free with the only exception occurring at $n = -53$. For all n in this range, the Pólya group is nontrivial. In fact, for $n = -53$, m_{5n} is not cube-free but the field K_{5n} is non-Pólya. In Table 1, $C_{m_{5n}}$ denotes the cube part of m_{5n}. We performed the computations using the SageMath software. The program can be obtained by writing to the authors.

Acknowledgements

The author is grateful to the anonymous referee for careful reading and valuable comments which have helped to improve this article. The authors also express their sincere gratitude to the Indian Institute of Science Education and Research, Berhampur, for providing facilities to carry out this work.

References

[1] P. J. Cahen and J. L. Chabert, *Integer-Valued Polynomials*, Mathematical Surveys and Monographs, 48 (American Mathematical Society, Providence, RI, 1997).

[2] J. L. Chabert, 'Factorial groups and Pólya groups in Galoisian extensions of $\mathbb{Q}$', in: *Commutative Ring Theory and Applications*, Lecture Notes in Pure and Applied Mathematics, 231 (eds. M. Fontana, S.-E. Kabbaj and S. Wiegand) (Dekker, New York, 2003), 77–86.

[3] J. Chattopadhyay and A. Saikia, 'Totally real bi-quadratic fields with large Pólya groups', *Res. Number Theory* **8** (2022), Article no. 30.

[4] P. Erdős, 'Arithmetical properties of polynomials', *J. Lond. Math. Soc. (2)* **28** (1953), 416–425.

[5] J. Gillibert and A. Levin, 'A geometric approach to large class groups: A survey', in: *Class Groups of Number Fields and Related Topics* (eds. K. Chakraborty, A. Hoque and P. Pandey) (Springer, Singapore, 2020).

[6] E. S. Golod and I. R. Shafarevich, 'On the class field tower', *Izv. Akad. Nauk* **28** (1964), 261–272.

[7] M.-N. Gras, 'Non monogénéité de l'anneau des entires des extensions cycliques de $\mathbb{Q}$ de degré premier $l \geq 5$', *J. Number Theory* **23** (1986), 347–353.

[8] H. Halberstam, 'On the distribution of additive number-theoretic functions. III', *J. Lond. Math. Soc. (2)* **31** (1956), 14–27.

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

[10] B. Heidaryan and A. Rajaei, 'Some non-Pólya biquadratic fields with low ramification', *Rev. Mat. Iberoam.* **33** (2017), 1037–1044.

[11] H. Helfgott, 'Power-free values, large deviations and integer points on irrational curves', *J. Théor. Nombres Bordeaux* **19** (2007), 433–472.

[12] H. Helfgott, 'Power-free values repulsion between points, differing beliefs and the existence of error', in: *Anatomy of Integers*, CRM Proceedings and Lecture Notes, 46 (eds. J.-M. De Koninck, A. Granville and F. Luca) (American Mathematical Society, Providence, RI, 2008), 81–88.

[13] D. Hilbert, 'Die Theorie der algebraischen Zahlkörper', *Jahresber. Dtsch. Math.-Ver.* **4** (1894–1895), 175–546.

[14] M. Ishida, *The Genus Fields of Algebraic Number Fields* (Springer, Cham, 1976).

[15] S. Jeannin, 'Nombre de classes et unités des corps de nombres cycliques quintiques d'E. Lehmer', *J. Théor. Nombres Bordeaux* **8** (1996), 75–92.

[16] E. Lehmer, 'Connection between Gaussian periods and cyclic units', *Math. Comp.* **50** (1988), 535–541.

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

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

[19] A. Maarefparvar, 'Pólya group in some real biquadratic fields', *J. Number Theory* **228** (2021), 1–7.

[20] D. W. Masser, 'Polynomial bounds for Diophantine equations', *Amer. Math. Monthly* **93** (1986), 486–488.

[21] T. Reuss, 'Power-free values of polynomials', *Bull. Lond. Math. Soc.* **47** (2015), 270–284.

[22] R. Schoof and L. C. Washington, 'Quintic polynomials and real cyclotomic fields with large class numbers', *Math. Comp.* **50** (1988), 543–556.

[23] C. W.-W. Tougma, 'Some questions on biquadratic Pólya fields', *J. Number Theory* **229** (2021), 386–398.

[24] E. von Zylinski, 'Zur Theorie der außerwesentlichen Diskriminantenteiler algebraischer Körper', *Math. Ann.* **73**(2) (1913), 273–274.

[25] Z. Wolske, *Number Fields with Large Minimal Index*. Thesis, University of Toronto, 2018.

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

NIMISH KUMAR MAHAPATRA, Department of Mathematical Sciences,
Indian Institute of Science Education and Research, Berhampur, India
e-mail: nimishkm18@iiserbpr.ac.in

PREM PRAKASH PANDEY, Department of Mathematical Sciences,
Indian Institute of Science Education and Research, Berhampur, India
e-mail: premp@iiserbpr.ac.in