New York Journal of Mathematics

New York J. Math. **28** (2022) 650–658.

Nonmonogenity of number fields defined by trinomials

Anuj Jakhar

Abstract. Let $f(x) = x^n - ax^m - b$ be a monic irreducible polynomial of degree n having integer coefficients. Let $K = \mathbf{Q}(\theta)$ be an algebraic number field with θ a root of $f(x)$. In this paper, we provide some explicit conditions involving only a, b, m, n for which K is not monogenic. Further, as an application, in a special case, we show that if p is a prime number of the form $32k + 1$, $k \in \mathbf{Z}$ and θ is a root of a monic polynomial $x^{32n} - 64ax^m - p$ with $2 \nmid n$, $p|a$, then $\mathbf{Q}(\theta)$ is not monogenic.

Contents

1. Introduction and statement of the result

For a given algebraic number field K, it is a classical problem in Algebraic Number Theory whether K is monogenic or not. There are many results in the literature for testing the monogenity of number fields using different approaches (cf. [1], [3], [5], [6], [7], [8], [9], [12], [16], [2]). Let $\mathbf{Z}_K$ denote the ring of algebraic integers of an algebraic number field $K = \mathbf{Q}(\theta)$ where θ is a root of a monic irreducible polynomial $f(x)$ of degree n having coefficients from the ring $\mathbf{Z}$ of integers. It is well-known that $\mathbf{Z}_K$ is a free abelian group of rank n. Let $\operatorname{ind}\theta$ denote the index of the subgroup $\mathbf{Z}[\theta]$ in $\mathbf{Z}_K$. The index $i(K)$ of the field K is defined as

$$i(K) = \gcd\{\operatorname{ind}\alpha \mid \alpha \in \mathbf{Z}_K \text{ generates the field extension } K/\mathbf{Q}\}.$$

A prime number p dividing $i(K)$ is called a prime common index divisor of K. A number field K is called monogenic if there exists an element $\alpha \in \mathbf{Z}_K$ such that $\{1, \alpha, \cdots, \alpha^{n-1}\}$ is an integral basis of K; if no such α exists, then we say that K is not monogenic. In 2016, Ahmad, Nakahara, and Husnine [1] proved that

Received October 1, 2021.
2010 *Mathematics Subject Classification.* 11R04.
Key words and phrases. Monogenity, non-monogenity, Newton polygon, power basis.
The author is supported by the SERB Start-up Research Grant SRG/2021/000393.

ISSN 1076-9803/2022

the sextic number field generated by $b^{\frac{1}{6}}$ is not monogenic if $b \equiv 1 \mod 4$ and $b \not\equiv \pm 1 \mod 9$. In 2017, Gaál and Remete [9] provided some new results on monogenity of number fields generated by $b^{\frac{1}{n}}$ with b a square free integer and $3 \leq n \leq 9$ by applying the explicit form of the index equation. In 2021, Yakkou and Fadil [2] studied the monogenity of number fields generated by $b^{\frac{1}{q^r}}$, where b is a square free integer and q be a prime number. In this paper, using the splitting of primes in $\mathbf{Z}_K$, we prove some results regarding the non-monogenity of a number field K defined by an irreducible trinomial of the type $x^n - ax^m - b$ having integer coefficients. As an application of our results, we provide a class of non-monogenic number fields defined by irreducible trinomials (see Example 1.3).

For a prime number q and a non-zero a belonging to the ring $\mathbf{Z}_q$ of q-adic integers, $v_q(a)$ will be the highest power of q dividing a and $v_q(a) = \infty$ when $a = 0$. Let $\mathbb{F}_q$ denote the field with q elements and $N(q, \ell)$ denote the number of irreducible polynomials of degree ℓ over $\mathbb{F}_q$. It is well known that

$$N(q, \ell) = \frac{1}{\ell} \sum_{k|\ell} \mu(k) q^{\frac{\ell}{k}},$$

where μ is the Möbius function. Observe that

$$N(q, 1) = q, \quad N(q, 2) = \frac{q(q-1)}{2}, \quad N(q, 3) = \frac{q(q^2-1)}{3}.$$

We now state our main result.

Theorem 1.1. *Let $K = \mathbf{Q}(\theta)$ be an algebraic number field with θ a root of a monic irreducible polynomial $f(x) = x^n - ax^m - b$ of degree n having integer coefficients. Let q be a prime factor of n with $n = q^r u$, $q \nmid u$. Assume that q^{r+1} divides a and $q \nmid b$. Suppose $\phi(x)$ is a monic irreducible factor of degree ℓ of the polynomial $x^u - b$ over $\mathbb{F}_q$ and $N(q, \ell)$ is as above. If r_1 stands for the integer $v_q(b^{q-1} - 1)$, then in the following cases q divides $i(K)$.*

(1) $q \neq 2$ and $N(q, \ell) < r_1 \leq r$.
(2) $q = 2$ and $N(2, \ell) + 2 < r_1 \leq r$.
(3) $N(q, \ell) + 1 < r < r_1$.

In the special case when $\ell = 1$, the following corollary is an immediate consequence of the above theorem.

Corollary 1.2. *Let $K = \mathbf{Q}(\theta)$, $f(x) = x^n - ax^m - b$, r and r_1 be as in Theorem 1.1. If q^{r+1} divides a, $b \equiv 1 \mod q$ and $\min\{r, r_1\} > q + 2$, then K is not monogenic.*

It may be pointed out that if we have $b = 1$ in the above corollary, then K is not monogenic for $r > q + 2$.

As an application, we provide a class of non-monogenic number fields defined by irreducible trinomials.

Example 1.3. Let p be a prime number[1] of the form $32k + 1$ with $k \in \mathbf{Z}$. Consider a monic polynomial $f(x) = x^n - ax^m - p \in \mathbf{Z}[x]$ with $v_2(n) = 5$ and $64p$ divides a. Note that $f(x)$ is irreducible over $\mathbf{Q}$ as $f(x)$ satisfies Eisenstein criterion with respect to p. If θ is a root of $f(x)$ and $K = \mathbf{Q}(\theta)$, then as in the notations of Corollary 1.2, for $q = 2$ we have $r = 5$ and $r_1 \geq 5$. Therefore K is not monogenic in view of Corollary 1.2.

2. Preliminary results

Let $K = \mathbf{Q}(\theta)$ be an algebraic number field with θ a root of an irreducible polynomial $f(x)$ having integer coefficients and $\mathbf{Z}_K$ denote the ring of algebraic integers of K. Let q be a prime number. If q does not divide $\operatorname{ind}\theta$, then Dedekind [4] proved a significant theorem in 1878 which relates the decomposition of $f(x)$ modulo q with the factorization of $q\mathbf{Z}_K$ into a product of prime ideals of $\mathbf{Z}_K$. Precisely, he proved the following.

Dedekind Theorem. Let $K = \mathbb{Q}(\theta)$ be an algebraic number field of degree n with θ an algebraic integer. Let $f(x)$ be the minimal polynomial of θ over $\mathbb{Q}$ and q be a rational prime not dividing $\operatorname{ind}\theta$. Let $\overline{f}(x) = \overline{g}_1(x)^{e_1} \cdots \overline{g}_t(x)^{e_t}$ be the factorization of $\overline{f}(x)$ into powers of distinct irreducible polynomials over $\mathbb{Z}/q\mathbb{Z}$, where each $g_i(x) \in \mathbb{Z}[x]$ is monic. Then $\wp_i = \langle g_i(\theta), q\rangle$ for $1 \leq i \leq t$ are distinct prime ideals of $\mathbf{Z}_K$ and $q\mathbf{Z}_K = \wp_1^{e_1} \cdots \wp_t^{e_t}$; moreover the norm of $\wp_i$ is $q^{\deg g_i(x)}$ for $1 \leq i \leq t$.

The following lemma is an immediate consequence of Dedekind's theorem. It plays a key role in the proof of Theorem 1.1. We shall denote by $\mathbb{F}_q$ the field with q elements.

Lemma 2.1. *Let K be a number field and q be a prime number. For every positive integer f, let $N(q, f)$ denote the number of irreducible polynomials of $\mathbb{F}_q[x]$ of degree f and $P(q, f)$ denote the number of distinct prime ideals of $\mathbf{Z}_K$ lying above q having residual degree f. If $P(q, f) > N(q, f)$ for some f, then for every algebraic integer α generating the field extension $K/\mathbf{Q}$, the prime q divides* $\operatorname{ind}\alpha$.

When Dedekind's theorem fails, i.e., q divides $i(K)$, then Ore developed an alternative approach in 1928 for obtaining the prime ideal factorization of the rational primes in a number field K by using Newton polygons (cf. [14], [15]).

We now introduce the notion of Gauss valuation which is required for defining the ϕ-Newton polygon of a polynomial, where $\phi(x)$ belonging to $\mathbf{Z}_q[x]$ is a monic polynomial with $\bar{\phi}(x)$ irreducible over $\mathbb{F}_q$.

We shall denote by $v_{q,x}$ the Gauss valuation of the field $\mathbf{Q}_q(x)$ of rational functions in an indeterminate x which extends the valuation v_q of $\mathbf{Q}_q$ and is defined on $\mathbf{Q}_q[x]$ by

$$v_{q,x}(\sum_i b_i x^i) = \min_i\{v_q(b_i)\}, b_i \in \mathbf{Q}_q. \tag{2.1}$$

[1]It is known that there exists infinitely many primes of the form $32k + 1$, $k \in \mathbf{Z}$.

Now we define the notion of ϕ-Newton polygon with respect to some prime q.

Definition 2.2. Let q be a prime number and $\phi(x) \in \mathbf{Z}_q[x]$ be a monic polynomial which is irreducible modulo q. Let $f(x) \in \mathbf{Z}_q[x]$ be a monic polynomial not divisible by $\phi(x)$ with ϕ-expansion $\sum_{i=0}^{n} a_i(x)\phi(x)^i$, $\deg a_i(x) < \deg \phi(x)$, $a_n(x) \neq 0$ which is obtained on dividing $f(x)$ by successive powers of $\phi(x)$. To each non-zero term $a_k(x)\phi(x)^k$, we associate the point $(n-k, v_{q,x}(a_k(x)))$ and form the set

$$P = \{(k, v_{q,x}(a_{n-k}(x))) \mid 0 \leq k \leq n, a_{n-k}(x) \neq 0\}.$$

The ϕ-Newton polygon of $f(x)$ with respect to q is the polygonal path formed by the lower edges along the convex hull of the points of P. The slopes of the edges are increasing when calculated from left to right. The principal ϕ-Newton polygon of $f(x)$ with respect to q is the part of the ϕ-Newton polygon of $f(x)$, which is determined by joining all edges of positive slopes.

Example 2.3. Let $f(x) = (x+5)^4 - 5$. Here take $\phi(x) = x$. Then the x-Newton polygon of $f(x)$ with respect to prime 2 consists of only one edge joining the points $(0,0)$ and $(4,2)$ with the lattice point $(2,1)$ lying on it (see Figure 1).

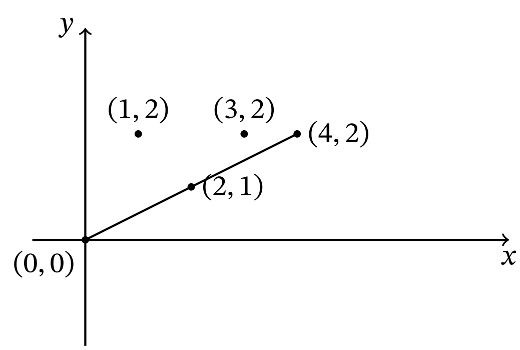

FIGURE 1. x-Newton polygon of $f(x)$ with respect to prime 2

Definition 2.4. Let q be a prime number and $\phi(x) \in \mathbf{Z}_q[x]$ be a monic polynomial which is irreducible modulo q having a root α in the algebraic closure $\widetilde{\mathbf{Q}}_q$ of $\mathbf{Q}_q$. Let $f(x) \in \mathbf{Z}_q[x]$ be a monic polynomial not divisible by $\phi(x)$ with ϕ-expansion $\phi(x)^n + a_{n-1}(x)\phi(x)^{n-1} + \cdots + a_0(x)$. Suppose that the ϕ-Newton polygon of $f(x)$ with respect to q consists of a single edge, say S having positive slope denoted by $\frac{d}{e}$ with d, e coprime, i.e.,

$$\min\{\frac{v_{q,x}(a_{n-i}(x))}{i} \mid 1 \leq i \leq n\} = \frac{v_{q,x}(a_0(x))}{n} = \frac{d}{e}$$

so that n is divisible by e, say $n = et$ and $v_{q,x}(a_{n-ej}(x)) \geq dj$ for $1 \leq j \leq t$. Thus the polynomial $\frac{a_{n-ej}(x)}{q^{dj}} = b_j(x)$ (say) has coefficients in $\mathbf{Z}_q$ and hence

$b_j(\alpha) \in \mathbf{Z}_q[\alpha]$ for $1 \leq j \leq t$. The polynomial $T(y)$ in an indeterminate y defined by $T(y) = y^t + \sum_{j=1}^{t} \overline{b_j}(\overline{\alpha})y^{t-j}$ having coefficients in $\mathbb{F}_q[\overline{\alpha}]$ is said to be the polynomial associated to $f(x)$ with respect to (ϕ, S); here the field $\mathbb{F}_q[\bar{\alpha}]$ is isomorphic to the field $\frac{\mathbb{F}_q[x]}{\langle\bar{\phi}(x)\rangle}$.

Example 2.5. Consider $f(x) = (x + 5)^4 - 5$. Then, as in Example 2.3, the x-Newton polygon of $f(x)$ with respect to prime 2 consists of only one edge joining the points $(0, 0)$ and $(4, 2)$ with the lattice point $(2, 1)$ lying on it. With notations as in the above definition, we see that $e = 2$, $d = 1$ and the polynomial associated to $f(x)$ with respect to (x, S) is $T(y) = y^2 + y + \overline{1}$ belonging to $\mathbb{F}_2[y]$.

We now state a weaker version of Theorem 1.2 of [13].

Theorem 2.6. *Let $L = \mathbf{Q}(\eta)$ be an algebraic number field with η satisfying a monic irreducible polynomial $g(x) \in \mathbf{Z}[x]$ and q be a prime number. Let $\bar{\phi}_1(x)^{e_1} \cdots \bar{\phi}_r(x)^{e_r}$ be the factorization of $g(x)$ modulo q into a product of powers of distinct irreducible polynomials over $\mathbb{F}_q$ with each $\phi_i(x) \neq g(x)$ belonging to $\mathbf{Z}[x]$ monic. Assume that, for a fixed i, the ϕ_i-Newton polygon of $g(x)$ has k edges, say S_j having positive slopes $\lambda_j = \frac{d_j}{e_j}$ with $\gcd(d_j, e_j) = 1$ for $1 \leq j \leq k$. If the polynomial $T_j(y)$ associated to $f(x)$ with respect to (ϕ_i, S_j) is linear for k_1 edges with $1 \leq j \leq k_1 \leq k$, then there are at least k_1 distinct prime ideals of $\mathbf{Z}_L$ having residual degree $\deg \phi_i(x)$.*

In [10], Guàrdia, Montes, and Nart introduced the notion of ϕ-admissible expansion, which is used in order to treat some special cases when the ϕ-expansion of a polynomial $g(x)$ is not obvious.

Let q be a prime number and $f(x) \in \mathbf{Z}_q[x]$ be a monic polynomial not divisible by $\phi(x)$ with $\phi(x)$-development $\sum_{j=0}^{n} a'_j(x)\phi(x)^j$, $a'_j(x) \in \mathbf{Z}_q[x]$; here $\deg a'_j(x)$ can be greater than or equal to $\deg \phi(x)$. Analogous to the definition of ϕ-Newton polygon of $f(x)$ with respect to q, to each non-zero term $a'_k(x)\phi(x)^k$, we associate the point $(n-k, v_{q,x}(a'_k(x)))$ and the polygonal path formed by the lower edges along the convex hull of the points of $\{(k, v_{q,x}(a'_{n-k}(x))) \mid 0 \leq k \leq n, a'_{n-k}(x) \neq 0\}$ defines the ϕ-development Newton polygon of $f(x)$ with respect to q in this case. Now as in Definition 2.4, suppose that the ϕ-development Newton polygon of $f(x)$ with respect to q consists of a single edge, say S' having positive slope denoted by $\frac{d}{e}$ with d, e coprime, i.e.,

$$\min\{\frac{v_{q,x}(a'_{n-i}(x))}{i} \mid 1 \leq i \leq n\} = \frac{v_{q,x}(a'_0(x))}{n} = \frac{d}{e}$$

so that n is divisible by e, say $n = et$ and $v_{q,x}(a'_{n-ej}(x)) \geq dj$ for $1 \leq j \leq t$. Let $\frac{a'_{n-ej}(x)}{q^{dj}}$ is denoted by $b'_j(x)$. We define the polynomial $T'(y)$ in an indeterminate y by $T'(y) = y^t + \sum_{j=1}^{t} \overline{b'_j}(\overline{\alpha})y^{t-j}$ having coefficients in $\frac{\mathbb{F}_q[x]}{\langle\bar{\phi}(x)\rangle}(\cong \mathbb{F}_q[\overline{\alpha}])$. $T'(y)$ is said to be the polynomial associated to $f(x)$ with respect to (ϕ, S'). We say that a ϕ-development of $f(x)$ is called admissible with respect to (ϕ, S') if and only if $\bar{\phi}$ does not divide $\bar{b'}_j(x)$ for each j. If the ϕ-development Newton polygon of a polynomial $f(x)$ has ℓ many egdes S_i having positive slopes, then ϕ-development of $f(x)$ is called admissible when ϕ-development of $f(x)$ is admissible with respect to (ϕ, S_i) for each i, $1 \leq i \leq \ell$. It is proved in [10] that if a ϕ-development of $f(x)$ is admissible, then the principal ϕ-Newton polygon of $f(x)$ with respect to q will be the same as ϕ-development Newton polygon of $f(x)$ with respect to prime q for edges having positive slopes; in particular, for any edge S having positive slope of the ϕ-Newton polygon of $f(x)$, we have $T(y) = T'(y)$.

3. Proof of Theorem 1.1

Proof of Theorem 1.1. Keeping in mind that $q^r - 1 = (q-1)m$ with $m \equiv 1 \mod q$ and $b^{q-1} \equiv 1 \mod q$, one can quickly verify that $v_q(b^{q^r-1} - 1) = v_q(b^{q-1} - 1) = r_1$.

Since $q|a$ and $q \nmid b$, we have $f(x) \equiv x^n - b \mod q$. Using Fermat's little theorem and the fact that $n = q^r u$, $q \nmid u$, it follows that $f(x) \equiv (x^u - b)^{q^r} \mod q$. Since q does not divide ub, the monic polynomial $x^u - b$ is separable in $\mathbb{F}_q[x]$. Let $\phi_1(x) \cdots \phi_t(x)$ be the factorization of $x^u - b$ into a product of monic irreducible polynomials in $\mathbb{F}_q[x]$, then $f(x) \equiv (\phi_1(x) \cdots \phi_t(x))^{q^r} \mod q$. Now we fix an irreducible factor $\bar{\phi}_i(x) = \bar{\phi}(x)$ of the polynomial $\bar{f}(x)$ in $\mathbb{F}_q[x]$. Write $x^u - b = \phi_1(x) \cdots \phi_t(x) + q^{k_1}h_1(x) = \phi(x)g_1(x) + q^{k_1}h_1(x)$, where $g_1(x) = \prod_{j=1, j\neq i}^{t} \phi_j(x)$, $h_1(x) \in \mathbf{Z}[x]$ and $k_1 \geq 1$ is an integer such that $\bar{h}_1(x) \neq \bar{0}$. Note that $\bar{\phi}(x) \nmid \bar{g}_1(x)$. Now we observe that there exists $g(x)$ and $h(x)$ such that $\bar{\phi}(x) \nmid \bar{g}(x)\bar{h}(x)$ and $x^u - b = \phi(x)g(x) + q^k h(x)$ for some $k \geq 1$. Because if $\bar{\phi}(x)$ divides $\bar{h}_1(x)$, we can write $\bar{h}_1(x) = \bar{\phi}(x)^e \bar{g}_2(x)$ such that $e \geq 1$ and $\bar{\phi}(x) \nmid \bar{g}_2(x)$. So we have $h_1(x) = \phi(x)^e g_2(x) + q^{k_2}h_2(x)$ and k_2 is a positive integer such that $\bar{h}_2(x) \neq \bar{0}$. If $\bar{\phi}(x) \nmid \bar{h}_2(x)$, then we set $g(x) = g_1(x) + q^{k_2}\phi(x)^{e-1}g_2(x)$ and $h(x) = h_2(x)$ with $k = k_1 + k_2$. If $\bar{\phi}(x)$ divides $\bar{h}_2(x)$, then we can repeat this process. Therefore, let $g(x), h(x) \in \mathbf{Z}[x]$ be such that

$$x^u - b = \phi(x)g(x) + q^k h(x) \text{ with } k \geq 1,\ \bar{\phi}(x) \nmid \bar{g}(x)\bar{h}(x). \tag{3.1}$$

Applying the binomial theorem, we see that

$$f(x) = (x^u - b + b)^{q^r} - ax^m - b = (\phi(x)g(x) + q^k h(x) + b)^{q^r} - ax^m - b$$

can be written as

$$f(x)=\sum_{j=1}^{q^r}\binom{q^r}{j}(q^kh(x)+b)^{q^r-j}g(x)^j\phi(x)^j+(q^kh(x)+b)^{q^r}-ax^m-b.$$

Let $d(x)\in\mathbf{Z}[x]$ be a polynomial such that

$$(q^kh(x)+b)^{q^r}-b^{q^r}=q^{r+k}d(x).$$

Then

$$d(x)=b^{q^r-1}h(x)+\frac{1}{q^{r+k}}\sum_{j=0}^{q^r-2}\binom{q^r}{j}b^j(q^kh(x))^{q^r-j}.$$

It follows that

$$\begin{aligned} f(x) &= (\phi(x)g(x))^{q^r} \\ &+\sum_{j=1}^{q^r-1}\binom{q^r}{j}(q^kh(x)+b)^{q^r-j}g(x)^j\phi(x)^j+q^{r+k}d(x)-ax^m+b^{q^r}-b. \end{aligned} \tag{3.2}$$

Thus $f(x)=\sum_{j=0}^{q^r}a'_j(x)\phi(x)^j$ is the ϕ-development of $f(x)$, where

$$a'_0(x)=q^{r+k}d(x)-ax^m+b^{q^r}-b.$$

$$a'_i(x)=\sum_{j=1}^{q^r}\binom{q^r}{j}(q^kh(x)+b)^{q^r-j}g(x)^j.$$

Note that

$$v_{q,x}(\binom{q^r}{j}(q^kh(x)+b)^{q^r-j}g(x)^j)=v_q(\binom{q^r}{j})\text{ for every } j=1,2,\cdots,q^r. \tag{3.3}$$

We now divide our proof into two cases.

Case (1). Suppose $r_1\leq r$. Keeping in mind that q^{r+1} divides a, one can easily verify that the successive vertices of the ϕ-development Newton polygon of $f(x)$ with respect to an odd prime q is given by the set $\{(0,0),(q^r-q^{r-1},1),\cdots,(q^r-q^{r-r_1+1},r_1-1),(q^r,r_1)\}$ having r_1 edges S'_i with slopes $\lambda_i=\frac{1}{q^{r-i+1}-q^{r-i}}$ for $1\leq i\leq r_1-1$ and $\lambda_{r_1}=\frac{1}{q^{r-r_1+1}}$. Since $q\nmid b$ and $\bar{\phi}(x)\nmid\bar{g}(x)\bar{h}(x)$, one can see that the ϕ-development of $f(x)$ is admissible with respect to (ϕ,S'_i) for each i, and hence ϕ-development of $f(x)$ is admissible. Further, the polynomial associated to $f(x)$ with respect to (ϕ,S'_i) is linear for $1\leq i\leq r_1$. Therefore, the ϕ-Newton polygon of $f(x)$ has r_1 edges and the polynomials associated to $f(x)$ with respect to these edges are linear. Hence by Theorem 2.6, there are at least r_1 distinct prime ideals of $\mathbf{Z}_K$ lying above q having residual degree $\deg\phi(x)(=\ell)$. It is known [11] that the number of monic irreducible polynomials of degree ℓ over $\mathbb{F}_q$ are $N(q,\ell)$. Therefore, if $r_1>N(q,\ell)$, then applying Lemma 2.1 it follows that q divides $i(K)$. We now consider the situation when $q=2$. In this situation, the successive vertices of the ϕ-development Newton polygon of $f(x)$ with respect to 2 is given by the set $\{(0,0),(2^r-2^{r-1},1),\cdots,(2^r-2^{r-r_1+2},r_1-2),(2^r,r_1)\}$ having r_1-1 edges S'_i with slopes $\lambda_i=\frac{1}{2^{r-i+1}-2^{r-i}}$ for $1\le i\le r_1-2$ and $\lambda_{r_1-1}=\frac{1}{2^{r-r_1+1}}$. The polynomial associated to $f(x)$ with respect to (ϕ,S'_i) is linear for $1\le i\le r_1-2$ and the polynomial associated to $f(x)$ with respect to (ϕ,S'_{r_1-1}) is a second degree irreducible polynomial $y^2+y+\bar{1}$ over $\mathbb{F}_2$. Since $q\nmid b$ and $\bar{\phi}(x)\nmid\bar{g}(x)\bar{h}(x)$, ϕ-development of $f(x)$ is admissible. Hence, the ϕ-Newton polygon of $f(x)$ has r_1-2 edges such that the polynomials associated to $f(x)$ with respect to these edges are linear. Therefore, by Theorem 2.6, there are at least r_1-2 distinct prime ideals of $\mathbf{Z}_K$ lying above 2 having residual degree ℓ. So, if $r_1-2>N(2,\ell)$, then applying Lemma 2.1 it follows that 2 divides $i(K)$.

Case (2). Suppose $r_1>r$. Keeping in mind that q^{r+1} divides a, one can easily verify that the successive vertices of the ϕ-development Newton polygon of $f(x)$ with respect to an odd prime q are given by the set $\{(0,0),(q^r-q^{r-1},1),\cdots,(q^r-q,r-1),(q^r-1,r),(q^r,z)\}$ having $r+1$ edges S'_i with $z\ge r+1$ and slopes $\lambda_i=\frac{1}{q^{r-i+1}-q^{r-i}}$ for $1\le i\le r$, $\lambda_{r+1}=z-r$. Also, if $v_{q,x}(a'_0(x))=r+1$, then the successive vertices of the ϕ-development Newton polygon of $f(x)$ with respect to 2 is given by the set $\{(0,0),(2^r-2^{r-1},1),\cdots,(2^r-2,r-1),(2^r,r+1)\}$ having r edges S'_i with slopes $\lambda_i=\frac{1}{q^{r-i+1}-q^{r-i}}$ for $1\le i\le r-1$ and $\lambda_r=1$. Arguing exactly as in the above case, we see that there are at least $r-1$ distinct prime ideals of $\mathbf{Z}_K$ lying above q having residual degree ℓ. So, if $r-1>N(q,\ell)$, then applying Lemma 2.1 we see that q divides $i(K)$. This completes the proof of the theorem. □

Acknowledgement. The author is grateful to the anonymous referee for the detailed report which has substantially improved the readability of the paper.

References

[1] Ahmad, Shahzad; Nakahara, Toru; Hameed, Abdul. On certain pure sextic fields related to a problem of Hasse. *Internat. J. Algebra Comput.* **26** (2016), no. 3, 577–583. MR3506350, Zbl 1404.11124, doi: 10.1142/S0218196716500259. 650

[2] Ben Yakkou, Hamid; El Fadil, Lhoussain. On monogenity of certain pure number fields defined by $x^{p^r}-m$. *Int. J. Number Theory* **17** (2021), no. 10, 2235–2242. MR4322831, Zbl 07410931, doi: 10.1142/S1793042121500858. 650, 651

[3] Bilu, Yuri; Gaál, István; Győry, Kálmán. Index form equations in sextic fields: a hard computation. *Acta Arith.* **115** (2004), no. 1, 85–96. MR2102808, Zbl 1064.11084, doi: 10.4064/aa115-1-7. 650

[4] Dedekind, Richard. Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen. *Abh. der Kónigl. Ges. der Wissenschaften zu Göttingen* **23** (1878), 1–23. Also as Paper XV in Gesazmelte mathematische Werke, Bd. I, pp. 202–232. *Chelsea Publishing Co., New York*, 1968. MR0237282, JFM 56.0024.05. 652

[5] El Fadil, Lhoussain. On integral bases and monogeneity of pure sextic number fields with non-squarefree coefficients. *J. Number Theory* **228** (2021), 375–389. MR4276481, Zbl 07377291, doi: 10.1016/j.jnt.2021.03.025. 650

[6] Gaál, István. Power integer bases in algebraic number fields. *Ann. Univ. Sci. Budapest. Sect. Comput.* **18** (1999), 61—87. MR2118246, Zbl 0936.11072. 650

[7] GAÁL, ISTVÁN. Diophantine equations and power integral bases. Theory and algorithms. Second edition. *Birkhäuser/Springer, Cham*, 2019. xxii+326 pp. ISBN: 978-3-030-23864-3; 978-3-030-23865-0. MR3970246, Zbl 1465.11090, doi: 10.1007/978-3-030-23865-0. 650

[8] GAÁL, ISTVÁN; OLAJOS, PÉTER; POHST, MICHAEL. Power integral bases in orders of composite fields. *Experiment. Math.* **11** (2002), no. 1, 87–90. MR1960303, Zbl 1020.11064, doi: 10.1080/10586458.2002.10504471. 650

[9] GAÁL, ISTVÁN; REMETE, LÁSZLÓ. Integral bases and monogenity of pure fields. *J. Number Theory* **173** (2017), 129–146. MR3581912, Zbl 1419.11118, doi: 10.1016/j.jnt.2016.09.009. 650, 651

[10] GUÀRDIA, JORDI; MONTES, JESÚS; NART, ENRIC. Newton polygons of higher order in algebraic number theory. *Trans. Amer. Math. Soc.* **364** (2012), no. 1, 361–416. MR2833586, Zbl 1252.11091. doi: 10.1090/S0002-9947-2011-05442-5. 654, 655

[11] JACOBSON, NATHAN. Basic Algebra I, Second edition. *W. H. Freeman and Company, New York*, 1985. xviii+499 pp. ISBN: 0-7167-1480-9. MR0780184, Zbl 0557.16001. *Dover Publications*, 2009. 656

[12] JAKHAR, ANUJ; KUMAR, SURENDER. On nonmonogenic number fields defined by x^6+ax+b. Preprint, 2021. To appear in *Canadian Math. Bulletin*. doi: 10.4153/S0008439521000825. 650

[13] KHANDUJA, SUDESH KAUR; KUMAR, SANJEEV. On prolongations of valuations via Newton polygons and liftings of polynomials. *J. Pure Appl. Algebra* **216** (2012), no. 12, 2648–2656. MR2943747, Zbl 1267.12004, doi: 10.1016/j.jpaa.2012.03.034. 654

[14] MONTES, JESÚS; NART, ENRIC. On a theorem of Ore. *J. Algebra* **146** (1992), no. 2, 318–334. MR1152908, Zbl 0762.11045, doi: 10.1016/0021-8693(92)90071-S. 652

[15] ORE, ÖYESTEIN. Newtonsche Polygone in der Theorie der algebraischen Körper. *Math. Ann.* **99** (1928), no. 1, 84–117. MR1512440, JFM 54.0191.02, doi: 10.1007/BF01459087. 652

[16] PETHŐ, ATTILA; POHST, MICHAEL. On the indices of multiquadratic number fields. *Acta Arith.* **153** (2012), no. 4, 393–414. MR2925379, Zbl 1255.11052, doi: 10.4064/aa153-4-4. 650

(Anuj Jakhar) DEPARTMENT OF MATHEMATICS, INDIAN INSTITUTE OF TECHNOLOGY (IIT) BHILAI, CHHATTISGARH 492015, INDIA
anujjakhar@iitbhilai.ac.in; anujiisermohali@gmail.com

This paper is available via http://nyjm.albany.edu/j/2022/28-26.html.