Bull. Aust. Math. Soc. **113** (2026), 81–89
doi:10.1017/S000497272500022X

MONOGENITY OF THE COMPOSITION OF POLYNOMIALS

SURENDER KUMAR

(Received 13 March 2025; accepted 17 March 2025; first published online 8 May 2025)

Abstract

One of the important problems in algebraic number theory is to study the monogenity of number fields. Monogenic number fields arise from the roots of monogenic polynomials. In this article, we deal with the problem of monogenity of the composition of two monic polynomials having integer coefficients. We provide necessary and sufficient conditions for the composition to be monogenic together with a further sufficient condition. At the end of the paper, we construct an infinite tower of monogenic number fields.

2020 *Mathematics subject classification*: primary 11R04; secondary 11R21.

Keywords and phrases: monogenity, discriminant, resultant.

1. Introduction and statement of results

An algebraic number field K having ring of integers $\mathbb{Z}_K$ is said to be monogenic if there exists an algebraic integer $\beta \in K$ such that $\mathbb{Z}_K = \mathbb{Z}[\beta]$. Monogenic number fields play a significant role in the study of algebraic number fields due to their simplified structure and computational advantages. One interesting problem in this direction is to study the monogenity of polynomials. A polynomial $f(x) \in \mathbb{Z}[x]$ having a root θ is said to be monogenic if it is irreducible over $\mathbb{Q}$ and the ring of algebraic integers of $\mathbb{Q}(\theta)$ is $\mathbb{Z}[\theta]$. Some known families of monogenic polynomials are $x^2 - a \in \mathbb{Z}[x]$, where $a \equiv 2, 3 \bmod 4$, $x^3 - b$, where $b \neq \pm 1$ is a squarefree integer, and cyclotomic polynomials. Determining infinite families of higher degree monogenic polynomials can be difficult and much research has been done to identify such families [4–7]. Despite the difficulty in determining higher degree monogenic polynomials, we are inspired by [2, 3, 8, 11] concerning the monogenity of the composition of polynomials.

Let $f(x)$ and $g(x)$ be two monic polynomials belonging to $\mathbb{Z}[x]$ such that $f(g(x))$ is irreducible over $\mathbb{Q}$. Let α be a root of $f(g(x))$. Then, we have a tower of fields

$$\mathbb{Q} \to \mathbb{Q}(\beta) \to \mathbb{Q}(\alpha),$$

where $\beta = g(\alpha)$. We focus on the monogenity of the number fields of this tower. We give necessary and sufficient conditions for the composition $f(g(x))$ to be monogenic

© The Author(s), 2025. Published by Cambridge University Press on behalf of Australian Mathematical Publishing Association Inc.

https://doi.org/10.1017/S000497272500022X Published online by Cambridge University Press

and a further sufficient condition. Finally, we construct some towers of monogenic number fields.

Throughout the paper, $D(f)$ and $(f \circ g)(x)$ will denote the discriminant of $f(x) \in \mathbb{Z}[x]$ and the composition of $f(x)$ and $g(x)$, respectively. The discriminant and the ring of integers of an algebraic number field K will be denoted by d_K and $\mathbb{Z}_K$, respectively. For a field extension K/F and $\gamma \in K$, the symbol $N_{K/F}(\gamma)$ denotes the norm of γ over F. The index of a monic irreducible polynomial $f(x) \in \mathbb{Z}[x]$ having root θ is the group index $[\mathbb{Z}_{\mathbb{Q}(\theta)} : \mathbb{Z}[\theta]]$.

THEOREM 1.1. *Let $f(x)$ and $g(x)$ belonging to $\mathbb{Z}[x]$ be two monic polynomials and α be a root of $(f \circ g)(x)$. Then, $(f \circ g)(x)$ is monogenic if and only if*

(1) *$f(x)$ is monogenic and*
(2) *$\mathbb{Z}_L = \mathbb{Z}_K[\alpha]$, where $L = \mathbb{Q}(\alpha)$ and $K = \mathbb{Q}(g(\alpha))$.*

Clearly, the theorem states that if $L = \mathbb{Q}(\alpha)$ and $K = \mathbb{Q}(\beta)$ with $\beta = g(\alpha)$, then $[\mathbb{Z}_L : \mathbb{Z}[\alpha]] = 1$ if and only if $[\mathbb{Z}_K : \mathbb{Z}[\beta]] = 1$ and $[\mathbb{Z}_L : \mathbb{Z}_K[\alpha]] = 1$. For the monogenity of $f \circ g$, the necessity of condition (2) is also mentioned in [1, Corollary 1.7].

The following result provides a sufficient condition for the composition to be nonmonogenic.

COROLLARY 1.2. *Let $f(x) \in \mathbb{Z}[x]$ be a monic polynomial. If there exists a prime p and an integer a such that $p \mid f'(a)$ and $p^2 \mid f(a)$, then $(f \circ g)(x)$ is nonmonogenic for each monic polynomial $g(x) \in \mathbb{Z}[x]$.*

Note that the prime factors of $f(0)$ and $f(a)$ can be different. So the primes different from the divisors of $f(0)$ satisfying the conditions of the above corollary cannot divide the index of $(f \circ g)(x)$. The particular case of the corollary with $a = 0$ and $f = g$ is proved in [11].

Applying Theorem 1.1 with mathematical induction gives the following result.

COROLLARY 1.3. *Let $F_n(x) = (f_1 \circ f_2 \circ \cdots \circ f_n)(x)$ be the composition of n monic polynomials $f_1, f_2, \ldots, f_n$ belonging to $\mathbb{Z}[x]$. If $F_n(x)$ is monogenic, then $F_i(x)$ is monogenic for all $i = 1, 2 \ldots, n$.*

In [3], Harrington and Jones characterised those binomials $f(x), g(x)$ which satisfy the condition that both $f(x)$ and $f(g(x))$ are monogenic. In general, it is not always true that $f(x)$ and $f(g(x))$ are both monogenic. An example of such polynomials is

$$f(x) = x^2 + x + 4 \quad \text{and} \quad g(x) = x^3.$$

Here, $f(x)$ is monogenic whereas $f(x^3)$ is nonmonogenic, because 2 divides the index of $f(x^3)$. We provide a sufficient condition under which both $f(x)$ and $(f \circ g)(x)$ are monogenic. First, we prove the following theorem that yields the prime divisors of the index of $(f \circ g)(x)$ when the composition is of a certain type.

https://doi.org/10.1017/S000497272500022X Published online by Cambridge University Press

THEOREM 1.4. *Let $f(x)$ and $g(x)$ be two monic polynomials in $\mathbb{Z}[x]$ of degree m and n, respectively, such that $(f \circ g)(x)$ is irreducible. Suppose α is a root of $(f \circ g)(x)$. If*

(1) *$f(x)$ is monogenic and*
(2) *$N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(g'(\alpha))/n^{mn}$ is a squarefree integer,*

then every prime divisor of the index of $(f \circ g)(x)$ will be a divisor of n.

From the theorem, we obtain the next two corollaries.

COROLLARY 1.5. *Let $f(x)$ and $g(x)$ be two monic polynomials belonging to $\mathbb{Z}[x]$ of degree m and n, respectively. Suppose $(f \circ g)(x)$ is an Eisenstein polynomial with respect to each prime divisor of n and has root α. If $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(g'(\alpha))/n^{mn}$ is a squarefree integer, then $f(x)$ is monogenic if and only if $(f \circ g)(x)$ is monogenic.*

The following corollary is useful in the construction of infinite towers of monogenic number fields. Some examples are given at the end of the paper.

COROLLARY 1.6. *Let $\{f_n\}$ be a sequence of monic polynomials belonging to $\mathbb{Z}[x]$ and let f_n have degree t_n. For each $n > 1$, assume that the polynomial $F_n(x) = (F_{n-1} \circ f_n)(x)$ is Eisenstein with respect to each prime divisor of t_n. Let α_n be a root of F_n and $K_n = \mathbb{Q}(\alpha_n)$. If $N_{K_n/\mathbb{Q}}(f_n'(\alpha_n))/t_n^{t_n \deg F_{n-1}}$ is a squarefree integer for each $n > 1$, then f_1 is monogenic if and only if F_n is monogenic.*

2. Preliminaries

THEOREM 2.1 (Capelli; see [12, page 288]). *Let F be a field. Let $f(x)$ and $g(x)$ be two monic polynomials belonging to $F[x]$ and β be a root of $f(x)$ in the algebraic closure of F. Then, the following statements are equivalent:*

(i) *$(f \circ g)(x)$ is irreducible over F;*
(ii) *$f(x)$ is irreducible over F and $g(x) - \beta$ is irreducible over $F(\beta)$.*

The following two results proved in [13] will be used in the proof of Lemma 2.4.

LEMMA 2.2. *An ideal $\mathfrak{M}$ of $\mathbb{Z}[x]$ containing a monic polynomial is maximal if and only if $\mathfrak{M} = \langle p, g(x) \rangle$ for some prime number p and a monic polynomial $g(x)$ belonging to $\mathbb{Z}[x]$ which is irreducible modulo p.*

THEOREM 2.3. *Let $K = \mathbb{Q}(\theta)$ with $\theta \in \mathbb{Z}_K$ having minimal polynomial $f(x)$ over $\mathbb{Q}$. Then, $\mathbb{Z}_K = \mathbb{Z}[\theta]$ if and only if $f(x)$ does not belong to $\mathfrak{M}^2$ for any maximal ideal $\mathfrak{M}$ of the polynomial ring $\mathbb{Z}[x]$.*

The following lemma will be used in the proof of Theorem 1.1.

LEMMA 2.4. *Let $f(x)$ and $g(x)$ be two monic polynomials belonging to $\mathbb{Z}[x]$ such that the composition $(f \circ g)(x)$ is irreducible over $\mathbb{Q}$. If $f(x)$ is nonmonogenic, then so is $(f \circ g)(x)$.*

https://doi.org/10.1017/S000497272500022X Published online by Cambridge University Press

PROOF. Suppose that $f(x)$ is reducible over $\mathbb{Q}$, so that $f(x) = a(x)b(x)$ for some nonconstant polynomials $a(x), b(x) \in \mathbb{Z}[x]$. Clearly, $f(g(x)) = a(g(x))b(g(x)) \in \mathbb{Z}[g(x)]$. As $\mathbb{Z}[g(x)] \subset \mathbb{Z}[x]$, we see that $f(g(x))$ is reducible over $\mathbb{Q}$. Thus, our supposition is wrong and $f(x)$ is irreducible over $\mathbb{Q}$. As $f(x)$ is nonmonogenic, by Theorem 2.3, there exists a maximal ideal $\mathfrak{M}$ of $\mathbb{Z}[x]$ such that $f(x) \in \mathfrak{M}^2$. By Lemma 2.2, there is a prime p and a monic polynomial $r(x) \in \mathbb{Z}[x]$ which is irreducible modulo p such that $\mathfrak{M} = \langle p, r(x)\rangle$. Since $f(x) \in \langle p, r(x)\rangle^2$, we can write

$$f(x) = p^2u(x) + p \cdot r(x) \cdot v(x) + r^2(x) \cdot w(x),$$

for suitable $u(x), v(x)$ and $w(x) \in \mathbb{Z}[x]$. By replacing x with $g(x)$ in the above equation, we see that

$$f(g(x)) = p^2u(g(x)) + p \cdot r(g(x)) \cdot v(g(x)) + r(g(x))^2 \cdot w(g(x)). \tag{2.1}$$

If $r(g(x)) \in \mathbb{Z}[x]$ is irreducible modulo p, then by Lemma 2.3, $f(g(x)) \in \langle p, r(g(x))\rangle^2$. Let $s(x) \in \mathbb{Z}[x]$ be a monic factor of $r(g(x))$ which is irreducible modulo p. Set $r(g(x)) = s(x)\alpha(x) + p\beta(x)$, for some $\alpha(x)$ and $\beta(x)$ belonging to $\mathbb{Z}[x]$. Substituting $r(g(x)) = s(x)\alpha(x) + p\beta(x)$ into (2.1) and simplifying the formula,

$$f(g(x)) = p^2c(x) + p \cdot s(x) \cdot d(x) + s(x)^2 \cdot t(x)$$

for some $c(x), d(x)$ and $t(x) \in \mathbb{Z}[x]$. Thus, by Lemma 2.2, $f(g(x))$ belongs to the square of the maximal ideal $\langle p, s(x)\rangle$. Hence, by Theorem 2.3, $f(g(x))$ is nonmonogenic. □

THEOREM 2.5 [9, Theorem 1.19]. *If K/F is an extension of number fields of degree n and $\tau_1, \ldots, \tau_n$ are all F-isomorphisms of K into a normal extension of F containing K, then for every $\alpha \in K$, we have $N_{K/F}(\alpha) = \prod_{i=1}^{n} \tau_i(\alpha)$.*

For the discriminant formula of the composition of two nonzero polynomials belonging to $\mathbb{Z}[x]$, we need various results concerning the resultant of two polynomials. Let F be a field. Given two polynomials $f(x)$ and $g(x)$ belonging to the ring $F[x]$ with leading coefficients a and b, respectively, the resultant $R(f, g)$ of $f(x)$ and $g(x)$ is

$$R(f, g) = a^{\deg g} b^{\deg f} \prod_{\substack{1 \le i \le \deg f \\ 1 \le j \le \deg g}} (\lambda_i - \mu_j), \tag{2.2}$$

where $\lambda_1, \ldots, \lambda_{\deg f}$ and $\mu_1, \ldots, \mu_{\deg g}$ are the roots of f and g, respectively.

In the next lemma, we list some well-known properties of the resultant of two polynomials.

LEMMA 2.6. *Let $f(x) = a_m x^m + a_{m-1}x^{m-1} + \cdots + a_0$ and $g(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_0$ be two polynomials over a field F with $a_m b_n \neq 0$. If $\lambda_1, \ldots, \lambda_m$ and $\mu_1 \ldots, \mu_n$ are the roots of $f(x)$ and $g(x)$, respectively, then the following statements hold:*

(1) $R(f, g) = a_m^n \prod_{i=1}^{m} g(\lambda_i)$ *and* $R(f, g) = (-1)^{mn} b_n^m \prod_{j=1}^{n} f(\mu_j)$;
(2) $R(f, gh) = R(f, g)R(f, h)$ *for any* $h(x) \in \mathbb{Z}[x]$.

https://doi.org/10.1017/S000497272500022X Published online by Cambridge University Press

PROOF. (1) From (2.2),

$$R(f,g) = a_m^n b_n^m \prod_{\substack{1\le i\le m\\ 1\le j\le n}} (\lambda_i - \mu_j) = a_m^n \prod_{i=1}^{m} b_n^m \prod_{1\le j\le n} (\lambda_i - \mu_j).$$

Therefore, $R(f,g) = a_m^n \prod_{i=1}^m g(\lambda_i)$. The other identity can be proved similarly.

(2) Let $\deg h(x) = k$, $\gamma_1, \ldots, \gamma_k$ be the roots of $h(x)$ and c_k be the leading coefficient of $h(x)$. Then, by (2.2),

$$R(f,gh) = a_m^{n+k}(b_n c_k)^m \prod_{\substack{1\le i\le m\\ 1\le j\le n+k}} (\lambda_i - \alpha_j),$$

where $\alpha_j = \mu_j$ for $1 \le j \le m$ and $\alpha_j = \gamma_{j-m}$ for $m+1 \le j \le m+k$. This implies

$$R(f,gh) = a_m^n b_n^m \prod_{\substack{1\le i\le m\\ 1\le j\le n}} (\lambda_i - \mu_j) a_m^k c_k^m \prod_{\substack{1\le i\le m\\ 1\le j\le k}} (\lambda_i - \gamma_j).$$

Hence, $R(f,gh) = R(f,g)R(f,h)$. □

Let F be a field and $f(x) \in F[x]$ be a monic irreducible polynomial of degree m. Suppose $f(x)$ has a root α. From Lemma 2.6(1),

$$R(f,f') = \prod_{i=1}^{m} f'(\lambda_i),$$

where $f(\lambda_i) = 0$ for $1 \le i \le m$. Hence, using Theorem 2.5 and the fact that $D(f) = (-1)^{m(m-1)/2} \prod_{i=1}^m f'(\lambda_i)$, the discriminant of $f(x)$ is

$$D(f) = (-1)^{m(m-1)/2} R(f,f') = (-1)^{m(m-1)/2} N_{L/F}(f'(\alpha)), \tag{2.3}$$

where $L = F(\alpha)$.

The following lemma provides a formula for the discriminant of the composition of two monic polynomials belonging to $\mathbb{Z}[x]$.

LEMMA 2.7. *Let $f(x)$ and $g(x)$ be two nonzero monic polynomials belonging to $\mathbb{Z}[x]$ of degree m and n, respectively. If $(f\circ g)(x)$ is irreducible, then the discriminant of $(f\circ g)(x)$ is given by*

$$D(f\circ g) = (-1)^{mn[m(n+1)-2]/2} (D(f))^n N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(g'(\alpha)),$$

where α is a root of $(f\circ g)(x)$.

PROOF. Let α be a root of $F(x) := (f\circ g)(x)$. Then, using (2.3),

$$D(F) = (-1)^{mn(mn-1)/2} R(F,F') = (-1)^{mn(mn-1)/2} R(F(x), (f'\circ g)(x) g'(x)).$$

Applying Lemma 2.6(2),

$$D(F) = (-1)^{mn(mn-1)/2} R(F(x), (f'\circ g)(x)) R(F(x), g'(x)).$$

https://doi.org/10.1017/S000497272500022X Published online by Cambridge University Press

If $\delta_1, \ldots, \delta_{mn}$ and $\mu_1, \ldots, \mu_m$ are the roots of $F(x)$ and $f(x)$, respectively, then by Lemma 2.6(1),

$$D(F) = (-1)^{mn(mn-1)/2} \prod_{i=1}^{mn} f'(g(\delta_i))R(F(x), g'(x)).$$

For each j with $1 \le j \le n$, we can assume that $g(\delta_{i+j-1}) = \mu_j$ for $1 \le i \le m$, so that

$$D(F) = (-1)^{mn(mn-1)/2} \prod_{j=1}^{m} (f'(\mu_j))^n R(F(x), g'(x)).$$

Thus, by (2.3) and Lemma 2.6(1),

$$D(F) = (-1)^{mn[m(n+1)-2]/2} (D(f(x)))^n R(F(x), g'(x)).$$

Finally, Lemma 2.6(1) implies that

$$D(F) = (-1)^{mn[m(n+1)-2]/2} (D(f))^n N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(g'(\alpha)). \qquad \square$$

REMARK 2.8. With the notation of the above lemma, if $g(x) = x^n + a \in \mathbb{Z}[x]$, then

$$D(f \circ g) = (-1)^{mn[m(n+1)-2]/2} (D(f))^n n^{mn} f(a)^{n-1}.$$

The following lemmas are useful in the construction of a tower of monogenic number fields.

LEMMA 2.9 [10, Lemma 2.17]. *Let α be an algebraic integer and let $L = \mathbb{Q}(\alpha)$ be the field generated by it. If the minimal polynomial $f(x)$ of α over $\mathbb{Q}$ is an Eisenstein polynomial with respect to a prime p, that is, it has the form $x^n + a_{n-1}x^{n-1} + \cdots + a_0$, with $a_0, \ldots, a_{n-1}$ divisible by p and $p^2 \nmid a_0$, then the index of $f(x)$ is not divisible by p.*

LEMMA 2.10 [9, Corollary 7.10]. *If $\mathbb{Q} \subset K \subset L$ is a tower of number fields, then*

$$d_L = (d_K)^{[L:K]} N_{K/\mathbb{Q}}(d_{L/K}),$$

where $d_{L/K}$ denotes the discriminant of the extension L/K.

3. Proofs of Theorem 1.1, Corollary 1.2 and Theorem 1.4

PROOF OF THEOREM 1.1. Here, $L = \mathbb{Q}(\alpha)$ and $K = \mathbb{Q}(\beta)$, where $\beta = g(\alpha)$. First, assume that $(f \circ g)(x)$ is monogenic. Then, by Lemma 2.4, the polynomial $f(x)$ is monogenic. By Theorem 2.1, the polynomial $h(x) = g(x) - \beta$ belonging to $\mathbb{Z}_K[x]$ is irreducible over K. Now, we show that $\mathbb{Z}_K[\alpha] = \mathbb{Z}_L$. As both $f(x)$ and $(f \circ g)(x)$ are monogenic, we have $\mathbb{Z}_K = \mathbb{Z}[\beta]$ and $\mathbb{Z}_L = \mathbb{Z}[\alpha]$. Clearly,

$$\mathbb{Z}_K[\alpha] = (\mathbb{Z}[\beta])[\alpha] = \mathbb{Z}[\beta, \alpha] \subset \mathbb{Z}[\alpha] = \mathbb{Z}_L.$$

Also, $\mathbb{Z} \subset \mathbb{Z}_K$ and so $\mathbb{Z}[\alpha] \subset \mathbb{Z}_K[\alpha]$, that is, $\mathbb{Z}_L \subset \mathbb{Z}_K[\alpha]$. Hence, $\mathbb{Z}_L = \mathbb{Z}_K[\alpha]$.

Conversely, assume that $\mathbb{Z}_K = \mathbb{Z}[\beta]$ and $\mathbb{Z}_L = \mathbb{Z}_K[\alpha]$. Using Theorem 2.1, the irreducibility of $g(x) - \beta$ over K and irreducibility of $f(x)$ over $\mathbb{Q}$ imply that $(f \circ g)(x)$ is irreducible over $\mathbb{Q}$. To show that $(f \circ g)(x)$ is monogenic, we need to show that

https://doi.org/10.1017/S000497272500022X Published online by Cambridge University Press

$\mathbb{Z}_L = \mathbb{Z}[\alpha]$. Clearly, $\mathbb{Z}_L = \mathbb{Z}_K[\alpha] = \mathbb{Z}[\beta, \alpha] \subset \mathbb{Z}[\alpha]$. Since $\mathbb{Z}[\alpha] \subset \mathbb{Z}_L$, we have $\mathbb{Z}_L = \mathbb{Z}[\alpha]$. Hence, the proof is complete. □

PROOF OF COROLLARY 1.2. If $f(x)$ or $(f \circ g)(x)$ is reducible over $\mathbb{Q}$, then the result is obvious. Suppose that both $f(x)$ and $(f \circ g)(x)$ are irreducible over $\mathbb{Q}$. In view of Theorem 1.1, it is enough to prove that the polynomial $f(x)$ is nonmonogenic. Set $f(a) = p^2 b$ and $f'(a) = pc$ for some integers b and c. Write

$$f(x) = f(x - a + a) = \sum_{i=2}^{n} \frac{f^{(n+2-i)}(a)}{(n+2-i)!}(x-a)^{n+2-i} + f'(a)(x-a) + f(a),$$

where $f^{(i)}$ denotes the ith derivative of f. Consequently,

$$f(x) = (x-a)^2 h(x) + pc(x-a) + p^2 b,$$
$$\text{where } h(x) = \sum_{i=2}^{n} \frac{f^{(n+2-i)}(a)}{(n+2-i)!}(x-a)^{n-i} \in \mathbb{Z}[x].$$

This implies that $f(x) \in \langle x - a, p\rangle^2$. Since $x - a$ is irreducible modulo p, by Lemma 2.2 and Theorem 2.3, we see that $f(x)$ is nonmonogenic. □

PROOF OF THEOREM 1.4. Set $L = \mathbb{Q}(\alpha)$ and $K = \mathbb{Q}(\beta)$, where $\beta = g(\alpha)$. By Lemma 2.7, the discriminant of $f \circ g$ is

$$D(f \circ g) = \pm(D(f))^n N_{L/\mathbb{Q}}(g'(\alpha)). \tag{3.1}$$

Since $f(x)$ is monogenic, we have $d_K = D(f)$. Substituting the value of $D(f)$ into (3.1), we obtain $D(f \circ g) = \pm(d_K)^n N_{L/\mathbb{Q}}(g'(\alpha))$. If I denotes the index $[\mathbb{Z}_L : \mathbb{Z}[\alpha]]$, then using (1.4) and the well-known identity $D(f \circ g) = I^2 d_L$, we see that $I^2 d_L = d_K^n N_{L/\mathbb{Q}}(g'(\alpha))$, which gives

$$I^2 \frac{d_L}{d_K^n} = n^{mn} \frac{1}{n^{mn}} N_{L/\mathbb{Q}}(g'(\alpha)).$$

Since $d_L/d_K^n \in \mathbb{Z}$ and $N_{L/\mathbb{Q}}(g'(\alpha))/n^{mn}$ is a squarefree integer, we can easily see that the possible prime divisors of I are prime divisors of n. □

4. Infinite examples

In the following proposition, we construct an infinite tower of monogenic number fields. This construction follows from Corollary 1.6.

PROPOSITION 4.1. *If $m \equiv 2 \bmod 4$ is a squarefree integer and n is a positive integer, then*

$$\mathbb{Q} \to \mathbb{Q}(\sqrt{m}) \to \mathbb{Q}(\sqrt[2^2]{m}) \to \cdots \to \mathbb{Q}(\sqrt[2^n]{m}) \to \cdots$$

is an infinite tower of monogenic number fields.

https://doi.org/10.1017/S000497272500022X Published online by Cambridge University Press

PROOF. Clearly, $x^{2^n} - m$ is an Eisenstein polynomial with respect to 2, so it is irreducible. Thus, we have a tower of number fields

$$\mathbb{Q} \to L_1 \to L_2 \to \cdots \to L_n \to L_{n+1} \to \cdots,$$

where $L_n = \mathbb{Q}(\sqrt[2^n]{m})$. Clearly, $f_1(x) = x^2 - m$ is monogenic, that is, $L_1 = \mathbb{Q}(\sqrt[2]{m})$ is monogenic. To prove the monogenity of L_n, we shall use induction on n. Let $f_2(x) = x^2$ and $L_2 = \mathbb{Q}(\sqrt[2^2]{m})$, then

$$N_{L_2/\mathbb{Q}}(2\sqrt[2^2]{m}) = \pm 2^{2^2} m.$$

Applying Theorem 1.4, we observe that the only prime that can divide the group index $[\mathbb{Z}_{L_2} : \mathbb{Z}[\sqrt[2^2]{m}]]$ is 2. However, $(f_1 \circ f_2)(x) = x^{2^2} - m$ is an Eisenstein polynomial with respect to 2, so using Lemma 2.9, we see that the field $L_2 = \mathbb{Q}(\sqrt[2^2]{m})$ is monogenic. Suppose that $f_{n-1}(x) = x^{2^{n-1}} - m$ is monogenic and $g(x) = x^2$. Then, $L_n = \mathbb{Q}(\sqrt[2^n]{m})$, which is generated by a root $\sqrt[2^n]{m}$ of $(f_{n-1} \circ g)(x)$. As $N_{L_n/\mathbb{Q}}(2\sqrt[2^n]{m})/2^{2^n} = \pm m$ is a squarefree integer, by Theorem 1.4, $[\mathbb{Z}_{L_n} : \mathbb{Z}[\sqrt[2^n]{m}]] = 2^s$ for some nonnegative integer s. Furthermore, by Lemma 2.9, $\mathbb{Z}_{L_n} = \mathbb{Z}[\sqrt[2^n]{m}]$, that is, L_n is monogenic. □

If $m \neq 0, 1$ is a squarefree integer, then the polynomial $f(x) = x^m - m$ is irreducible and has discriminant $D(f) = m^{2m-1}$. Let $K = \mathbb{Q}(\theta)$, where $f(\theta) = 0$. Keeping in mind Lemma 2.9 and the fact that $D(f) = [\mathbb{Z}_K : \mathbb{Z}[\theta]]^2 d_K$, we observe that the polynomial is monogenic. Using Remark 2.8 together with Lemma 2.9, we easily get the infinite tower of monogenic number fields

$$\mathbb{Q} \to \mathbb{Q}(\sqrt[m]{m}) \to \mathbb{Q}(\sqrt[m^2]{m}) \to \cdots \to \mathbb{Q}(\sqrt[m^n]{m}) \to \cdots.$$

EXAMPLE 4.2. Let a be an even squarefree integer. Let $f(x) = x^n - a^{n-1}x + a + a^n$ and $g(x) = x^2 + a$ be polynomials belonging to $\mathbb{Z}[x]$. Here,

$$(f \circ g)(x) = (x^2 + a)^n - a^{n-1}x^2 + a.$$

Clearly, $(f \circ g)(x)$ is an Eisenstein polynomial with respect to 2. So $(f \circ g)(x)$ is an irreducible polynomial. If α is a root of $(f \circ g)(x)$, then

$$N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(g'(\alpha)) = \pm 2^{2n} N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(\alpha) = \pm 2^{2n} a.$$

This implies that $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}(g'(\alpha))/4^n = \pm a$ is squarefree. Since $f(g(x))$ is an Eisenstein polynomial with respect to 2, by Corollary 1.5, it follows that $f(x)$ is monogenic if and only if $f(g(x))$ is monogenic.

EXAMPLE 4.3. Let $L = \mathbb{Q}(\alpha)$ be an algebraic number field, where α is a root of

$$F(x) = x^{27} - 18x^{24} + 144x^{21} - 672x^{18} + 2016x^{15} - 4032x^{12} + 5376x^9 + 4608x^6 + 2304x^3 - 1.$$

Note that $F(x + 1)$ is an Eisenstein polynomial with respect to the prime 3; therefore, $F(x)$ is an irreducible polynomial. Take $f(x) = x^9 + 511$ and $g(x) = x^3 - 2$, so that

https://doi.org/10.1017/S000497272500022X Published online by Cambridge University Press

$F(x) = (f \circ g)(x)$. Now,

$$N_{L/\mathbb{Q}}(g'(\alpha)) = 3^{27} N_{L/\mathbb{Q}}(\alpha)^2 = 3^{27}.$$

Clearly, $N_{L/\mathbb{Q}}(g'(\alpha))/3^{27}$ is squarefree. If $f(x)$ is monogenic, then using Theorem 1.4, we can see that $[\mathbb{Z}_L : \mathbb{Z}[\alpha]] = 3^t$ for some nonnegative integer t. As $F(x+1)$ is an Eisenstein polynomial with respect to 3, it follows that $t = 0$ in view of Lemma 2.9. Hence, $F(x)$ is monogenic. Thus, we have the 3-tower of monogenic number fields

$$\mathbb{Q} \subset \mathbb{Q}(\alpha^3) \subset \mathbb{Q}(\alpha).$$

Now, we prove that $f(x) = x^9 + 511$ is monogenic. Here, $D(f) = \pm 9^9 7^8 73^8$. For each prime divisor p of 511, the polynomial $f(x)$ is Eisenstein. So using Lemma 2.9, p does not divide the index of $f(x)$. Also, $f(x-1)$ is an Eisenstein polynomial with respect to 3, so 3 does not divide the index of $f(x)$. In view of the identity $D(f) = [\mathbb{Z}_L : \mathbb{Z}[\alpha]]^2 d_L$, we see that the polynomial $f(x)$ is monogenic.

References

[1] I. Gaál, *Diophantine Equations and Power Integral Bases* (Birkhäuser, Boston, MA, 2002).
[2] I. Gaál, 'On the monogenity of certain binomial compositions', *JP J. Algebra Number Theory Appl.* **57** (2022), 1–16.
[3] J. Harrington and L. Jones, 'Monogenic binomial composition', *Taiwanese J. Math.* **24** (2020), Article no. 10731090.
[4] B. Jhorar and S. K. Khanduja, 'When is $R[\theta]$ integrally closed?', *J. Algebra Appl.* **15**(5) (2016), Article no. 1650091, 7 pages.
[5] L. Jones, 'A brief note on some infinite families of monogenic polynomials', *Bull. Aust. Math. Soc.* **100** (2019), 239–244.
[6] L. Jones, 'Some new infinite families of monogenic polynomials with non-square free discriminant', *Acta Arith.* **197**(2) (2021), 213–219.
[7] S. Kaur and S. Kumar, 'On a conjecture of Lenny Jones about certain monogenic polynomials', *Bull. Aust. Math. Soc.* **110** (2024), 72–76.
[8] S. Kaur, S. Kumar and L. Remete, 'On the index of power compositional polynommials', Preprint, 2024, arXiv.2404.17351.
[9] S. K. Khanduja, *A Textbook of Algebraic Number Theory*, Unitext, 135 (Springer, Singapore, 2022).
[10] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd edn (Springer, Berlin–Heidelberg, 2004).
[11] H. Sharma, R. Sharma and S. Laishram, 'Monogenity of iterates of polynomials', *Arch. Math.* **122** (2024), 295–305.
[12] N. G. Tschebotaröw, *Grundzüge der Galois'schen Theorie* (Noordhoff, Groningen, 1950); translated from Russian by H. Schwerdtfeger.
[13] K. Uchida, 'When is $\mathbb{Z}[\theta]$ the ring of integers?', *Osaka J. Math.* **14** (1977), 155–157.

SURENDER KUMAR
e-mail: surenderk@iitbhilai.ac.in

https://doi.org/10.1017/S000497272500022X Published online by Cambridge University Press