Bull. Aust. Math. Soc. **110** (2024), 72–76
doi:10.1017/S0004972723001119

ON A CONJECTURE OF LENNY JONES ABOUT CERTAIN MONOGENIC POLYNOMIALS

SUMANDEEP KAUR and SURENDER KUMAR

(Received 6 September 2023; accepted 27 September 2023; first published online 21 November 2023)

Abstract

Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with θ satisfying a monic irreducible polynomial $f(x)$ of degree n over $\mathbb{Q}$. The polynomial $f(x)$ is said to be monogenic if $\{1, \theta, \ldots, \theta^{n-1}\}$ is an integral basis of K. Deciding whether or not a monic irreducible polynomial is monogenic is an important problem in algebraic number theory. In an attempt to answer this problem for a certain family of polynomials, Jones ['A brief note on some infinite families of monogenic polynomials', *Bull. Aust. Math. Soc.* **100** (2019), 239–244] conjectured that if $n \geq 3$, $1 \leq m \leq n-1$, $\gcd(n, mB) = 1$ and A is a prime number, then the polynomial $x^n + A(Bx+1)^m \in \mathbb{Z}[x]$ is monogenic if and only if $n^n + (-1)^{n+m}B^n(n-m)^{n-m}m^mA$ is square-free. We prove that this conjecture is true.

2020 *Mathematics subject classification*: primary 11R04; secondary 11R09.

Keywords and phrases: discriminant, monogenic polynomial.

1. Introduction and statements of results

Let $K = \mathbb{Q}(\theta)$ be an algebraic number field and let $f(x)$ of degree n be the minimal polynomial of θ over $\mathbb{Q}$. The polynomial $f(x)$ is said to be monogenic if $\{1, \theta, \ldots, \theta^{n-1}\}$ is an integral basis of K.

Denote the ring of algebraic integers of K by $\mathbb{Z}_K$. The field K is said to be monogenic if there exists $\alpha \in \mathbb{Z}_K$ such that $\mathbb{Z}_K = \mathbb{Z}[\alpha]$. It is well known that if $f(x)$ is monogenic, then the number field K is monogenic but the converse is not always true (for example, $\mathbb{Q}(\sqrt{d})$, where $d \neq 1$ is a square-free integer congruent to 1 modulo 4).

The discriminant of a monic polynomial over a field $\mathbb{F}$ of degree n having roots $\theta_1, \ldots, \theta_n$ in the algebraic closure of $\mathbb{F}$ is $\Delta_f = \prod_{1\leq i<j\leq n}(\theta_i - \theta_j)^2$. It is a classical result in algebraic number theory that if $f(x)$ is the minimal polynomial of an algebraic integer θ over $\mathbb{Q}$, then the discriminant Δ_f of $f(x)$ and the discriminant d_K of $K = \mathbb{Q}(\theta)$ are related by the formula

The first author is grateful to the Council of Scientific and Industrial Research, New Delhi for providing financial support in the form of Senior Research Fellowship through Grant No. 09/135(0878)/2019-EMR-1. The second author is grateful to the University Grants Commission, New Delhi, for providing financial support in the form of Senior Research Fellowship through Ref No.1129/(CSIR-NET JUNE 2019).

$$\Delta_f = [\mathbb{Z}_K : \mathbb{Z}[\theta]]^2 d_K. \tag{1.1}$$

Clearly if Δ_f is square-free, then $f(x)$ is monogenic but the converse need not be true. Jones [4, 6] constructed infinite families of monogenic polynomials having non square-free discriminant. In [7], Jones showed that there exist infinitely many primes $p \geq 3$ and integers $t \geq 1$ coprime to p, such that $f(x) = x^p - 2ptx^{p-1} + p^2t^2x^{p-2} + 1$ is nonmonogenic and, in [5], he gave infinite families of monogenic polynomials using a new discriminant formula.

Throughout the paper, $f(x) = x^n + A(Bx+1)^m \in \mathbb{Z}[x]$ is an irreducible polynomial with $n \geq 3$ and $1 \leq m \leq n-1$, θ is a root of f, $K = \mathbb{Q}(\theta)$ is the corresponding algebraic number field, Δ_f denotes the discriminant of $f(x)$ and $\mathrm{Ind}_K(\theta)$ denotes the group index $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$. From [4, Theorem 3.1],

$$\Delta_f = (-1)^{n(n-1)/2} A^{n-1}[n^n + (-1)^{n+m} B^n (n-m)^{n-m} m^m A]. \tag{1.2}$$

THEOREM 1.1. *Let A, B, n, m be integers with $1 \leq m \leq n-1, n > 2$ and $B \neq 0$. Assume that* $\gcd(n, mB) = 1$. *Then an irreducible polynomial of the type $f(x) = x^n + A(Bx+1)^m$ is monogenic if and only if both A and $n^n + (-1)^{n+m} B^n (n-m)^{n-m} m^m A$ are square-free.*

REMARK 1.2. In Theorem 1.1, the assumption that $\gcd(n, mB) = 1$ cannot be dropped. For example, consider the polynomial $f(x) = x^3 - 6(3x+1)$. Here $n = 3, m = 1, A = -6$ and $B = 3$. Note that $f(x)$ is irreducible over $\mathbb{Q}$. The polynomial $f(x)$ is monogenic and has discriminant $\Delta_f = 23.2^2.3^5$. However, $n^n + (-1)^{n+m} B^n (n-m)^{n-m} m^m A = 23.3^3$ is not square-free.

The following corollary is an immediate consequence of Theorem 1.1. It is conjectured by Jones in [4, Conjecture 4.1].

COROLLARY 1.3. *Let p be a prime number, and n, m and B be positive integers with $1 \leq m \leq n-1$, $n > 2$ and* $\gcd(n, mB) = 1$. *Then $f(x) = x^n + p(Bx+1)^m$ is monogenic if and only if $n^n + (-1)^{n+m} B^n (n-m)^{n-m} m^m p$ is square-free.*

EXAMPLE 1.4. Let p be an odd prime number and let a, b be positive integers with $n > 2$. Consider the polynomial $f(x) = x^n + ax^2 + bx + p$ with $b^2 = 4ap$. Note that $f(x)$ satisfies Eisenstein's criterion with respect to p, so it is irreducible over $\mathbb{Q}$. The polynomial $x^n + ax^2 + bx + p$ with $b^2 = 4ap$ can be reduced to the form $x^n + p(Bx+1)^2$ with $B = b/2p$. If $\gcd(n, 2B) = 1$, that is, $\gcd(n, b/p) = 1$, then Corollary 1.3 implies that $f(x)$ is monogenic if and only if $n^n + (-1)^n 4(b/2p)^n (n-2)^{n-2} p$ is square-free.

EXAMPLE 1.5. Let B be an integer not divisible by 3 with $|B| \geq 4$ and let $A \neq \pm 1$ be a nonzero square-free integer. Then the polynomial $f(x) = x^3 + A(Bx+1)^2$ is irreducible by Perron's criterion, which states that if $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ with $a_0 \neq 0$ and $|a_{n-1}| > 1 + |a_{n-2}| + \cdots + |a_0|$, then the polynomial $f(x)$ is irreducible over $\mathbb{Q}$. In view of Theorem 1.1, the polynomial $x^3 + A(Bx+1)^2$ is monogenic if and only if $4AB^3 - 27$ is square-free.

2. Preliminary results

In what follows, for a prime number p and a given polynomial $g(x) \in \mathbb{Z}[x]$, $\overline{g}(x)$ will denote the polynomial obtained by reducing each coefficient of $g(x)$ modulo p.

Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial having a root θ and let $L = \mathbb{Q}(\theta)$ be an algebraic number field. In 1878, Dedekind proved the following criterion which gives a necessary and sufficient condition to be satisfied by $f(x)$ so that p does not divide $\mathrm{Ind}_L(\theta)$.

THEOREM 2.1 (Dedekind's criterion, [2]; see also [1, Theorem 6.1.4]). *Let $L = \mathbb{Q}(\theta)$ be an algebraic number field and $f(x)$ the minimal polynomial of the algebraic integer θ over $\mathbb{Q}$. Let p be a prime and $\overline{f}(x) = \overline{g}_1(x)^{e_1} \cdots \overline{g}_t(x)^{e_t}$ be the factorisation of $\overline{f}(x)$ as a product of powers of distinct irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$, with each $g_i(x) \in \mathbb{Z}[x]$ monic. Let $M(x) = (f(x) - g_1(x)^{e_1} \cdots g_t(x)^{e_t})/p \in \mathbb{Z}[x]$. Then p does not divide $\mathrm{Ind}_L(\theta)$ if and only if, for each i, either $e_i = 1$ or $\overline{g}_i(x)$ does not divide $\overline{M}(x)$.*

With the notation as in Theorem 2.1, one can easily check that if $f(x)$ is monogenic, then for each prime p dividing Δ_f, either $e_i = 1$ or $\overline{g}_i(x)$ does not divide $\overline{M}(x)$ for each i.

DEFINITION 2.2. A polynomial $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ in $\mathbb{Z}[x]$ with $a_n \neq 0$ is called an Eisenstein polynomial with respect to a prime p if $p \nmid a_n$, $p \mid a_i$ for $0 \leq i \leq n-1$ and $p^2 \nmid a_0$.

The following result is known as Eisenstein's criterion (see [3]). It will be used in the proof of Corollary 1.3.

THEOREM 2.3. *Let $g(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ with $n \geq 1$. If there is a prime number p such that $p \nmid a_n, p \mid a_{n-1}, \ldots, p \mid a_0$ and $p^2 \nmid a_0$, then $g(x)$ is irreducible over $\mathbb{Q}$.*

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

LEMMA 2.4 [8, Lemma 2.17]. *Let α be an algebraic integer and let $L = \mathbb{Q}(\alpha)$. If the minimal polynomial of α over $\mathbb{Q}$ is an Eisenstein polynomial with respect to the prime p, then $\mathrm{Ind}_L(\alpha)$ is not divisible by p.*

3. Proof of Theorem 1.1 and Corollary 1.3

PROOF OF THEOREM 1.1. Clearly $A \neq 0$. Suppose that θ is a root of $f(x)$ and $K = \mathbb{Q}(\theta)$. From (1.2),

$$\Delta_f = (-1)^{n(n-1)/2}A^{n-1}[n^n + (-1)^{n+m}B^n(n-m)^{n-m}m^mA].$$

First suppose that the polynomial $f(x)$ is monogenic. Then $\mathrm{Ind}_K(\theta) = 1$. Let p be a prime dividing Δ_f. The following cases arise.

Case 1: $p \mid A$. Then $f(x) \equiv x^n \bmod p$ and $M(x) = A(Bx+1)^m/p$. As $n \geq 3$, by Dedekind's criterion, we see that $\bar{x}$ should not divide $\overline{M}(x)$. This implies that $p^2 \nmid A$. Thus, A is square-free. Suppose that p^2 divides $(n^n + (-1)^{n+m}B^n(n-m)^{n-m}m^mA)$.

Then the hypothesis $p \mid A$ implies that $p \mid n$. Since $n \geq 3$ and A is square-free, we have $p \mid B^n(n-m)^{n-m}m^m$, that is, $p \mid m(n-m)B$, which is not true because $\gcd(n, mB) = 1$. It follows that p^2 cannot divide $(n^n + (-1)^{n+m}B^n(n-m)^{n-m}m^mA)$ and so $(n^n + (-1)^{n+m}B^n(n-m)^{n-m}m^mA)$ is square-free.

Case 2: $p \nmid A$. Then p will divide $(n^n + (-1)^{n+m}B^n(n-m)^{n-m}m^mA)$. Keeping in mind the hypothesis $\gcd(n, mB) = 1$, it is easy to see that $p \nmid n$ and so $p \nmid Bm(n-m)$. Let α be a repeated root of $\overline{f}(x) = x^n + \overline{A}(\overline{B}x + 1)^m$ in the algebraic closure of $\mathbb{Z}/p\mathbb{Z}$. Then

$$\alpha^n + A(B\alpha + 1)^m \equiv 0 \bmod p$$

and

$$n\alpha^{n-1} + mAB(B\alpha + 1)^{m-1} \equiv 0 \bmod p.$$

So $n\alpha^{n-1} \equiv -mAB(B\alpha + 1)^{m-1} \bmod p$. By substitution,

$$-\alpha mAB(B\alpha + 1)^{m-1} + nA(B\alpha + 1)^m \equiv 0 \bmod p,$$

that is,

$$(B\alpha + 1)^{m-1}(\alpha AB(n-m) + nA) \equiv 0 \bmod p.$$

If $B\alpha + 1 \equiv 0 \bmod p$, then $\alpha \equiv -1/B \bmod p$, which yields the contradiction $(-1)^n/\overline{B}^n = \overline{f}(-1//\overline{B}) = \overline{f}(\overline{\alpha}) = 0$. Thus, $\alpha AB(n-m) + nA \equiv 0 \bmod p$, so that

$$\alpha \equiv -\frac{nA}{AB(n-m)} \bmod p \tag{3.1}$$

is the unique repeated root of $\overline{f}(x)$ in $\mathbb{Z}/p\mathbb{Z}$ and it is easy to show that α has multiplicity 2. So, assuming that α is a positive integer satisfying (3.1), we can write

$$\begin{aligned} f(x) &= (x - \alpha + \alpha)^n + A(B(x - \alpha + \alpha) + 1)^m, \\ &= \sum_{k=0}^{n} \binom{n}{k} \alpha^{n-k}(x-\alpha)^k + A\bigg(\sum_{k=0}^{m} \binom{m}{k} (B\alpha + 1)^{m-k}B^k(x-\alpha)^k\bigg), \\ &= (x-\alpha)^2 h(x) + f'(\alpha)(x-\alpha) + f(\alpha), \end{aligned}$$

where $f'(x)$ is the derivative of $f(x)$ and

$$h(x) = \sum_{k=2}^{n} \binom{n}{k} \alpha^{n-k}(x-\alpha)^{k-2} + A\bigg(\sum_{k=2}^{m} \binom{m}{k} (B\alpha + 1)^{m-k}B^k(x-\alpha)^{k-2}\bigg)$$

is in $\mathbb{Z}[x]$. Then $\overline{f}(x) = (x - \overline{\alpha})^2\overline{h}(x)$, where $\overline{h}(x) \in \mathbb{Z}[x]$ is separable. Let $\prod_{i=1}^{t} \overline{h}_i(x)$ be the factorisation of $\overline{h}(x)$ into a product of distinct irreducible polynomials $\overline{h}_i(x) \in \mathbb{Z}/p\mathbb{Z}[x]$ with each $h_i(x) \in \mathbb{Z}[x]$ monic. Then we can write

$$f(x) = (x-\alpha)^2\bigg(\prod_{i=1}^{t} h_i(x) + pg(x)\bigg) + f'(\alpha)(x-\alpha) + f(\alpha),$$

for some polynomial $g(x) \in \mathbb{Z}[x]$. This implies that

$$M(x) = \frac{1}{p}[p(x-\alpha)^2 g(x) + (x-\alpha)f'(\alpha) + f(\alpha)].$$

In view of Dedekind's criterion and the hypothesis that $f(x)$ is monogenic, we see that $f(\alpha) \not\equiv 0 \bmod p^2$. Equivalently,

$$(n^n + (-1)^{n+m}(n-m)^{n-m}m^m B^n A) \not\equiv 0 \bmod p^2.$$

Hence, $(n^n + (-1)^{n+m}(n-m)^{n-m}m^m B^n A)$ is square-free.

Conversely, suppose A and $(n^n + (-1)^{n+m}(n-m)^{n-m}m^m B^n A)$ are square-free. If $A = \pm 1$, then using (1.1), we see that $\mathrm{Ind}_K(\theta) = 1$, that is, $f(x)$ is monogenic. If p be a prime divisor of A, then $f(x)$ is an Eisenstein polynomial with respect to the prime p. Therefore, by Lemma 2.4, $p \nmid \mathrm{Ind}_K(\theta)$. Hence, by (1.1), $f(x)$ is monogenic. This completes the proof of the theorem. □

PROOF OF COROLLARY 1.3. It is easy to verify that $f(x)$ satisfies Eisenstein's criterion with respect to the prime p. So $f(x)$ is an irreducible polynomial. Hence, the result follows from Theorem 1.1. □

References

[1] H. Cohen, *A Course in Computational Algebraic Number Theory* (Springer-Verlag, Berlin, Heidelberg, 1993).

[2] R. Dedekind, 'Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen', *Götttingen Abh.* **23** (1878), 1–23.

[3] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd edn, Graduate Texts in Mathematics, 84 (Springer, New York, 1990).

[4] L. Jones, 'A brief note on some infinite families of monogenic polynomials', *Bull. Aust. Math. Soc.* **100** (2019), 239–244.

[5] L. Jones, 'Generating infinite families of monogenic polynomials using a new discriminant formula', *Albanian J. Math.* **14** (2020), 37–45.

[6] L. Jones, 'Some new infinite families of monogenic polynomials with non-squarefree discriminant', *Acta Arith.* **197** (2021), 213–219.

[7] L. Jones, 'On necessary and sufficient conditions for the monogeneity of a certain class of polynomials', *Math. Slovaca* **72**(3) (2022), 591–600.

[8] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd edn, Springer Monographs in Mathematics (Springer-Verlag, Berlin, 2004).

SUMANDEEP KAUR, Department of Mathematics,
Panjab University, Chandigarh, India
e-mail: sumandhunay@gmail.com

SURENDER KUMAR, Department of Mathematics,
Indian Institute of Technology (IIT), Bhilai, India
e-mail: surenderk@iitbhilai.ac.in