Bull. Aust. Math. Soc. **100** (2019), 239–244
doi:10.1017/S0004972719000182

A BRIEF NOTE ON SOME INFINITE FAMILIES OF MONOGENIC POLYNOMIALS

LENNY JONES

(Received 26 December 2018; accepted 6 January 2019; first published online 13 February 2019)

Abstract

Suppose that $f(x) = x^n + A(Bx + C)^m \in \mathbb{Z}[x]$, with $n \geq 3$ and $1 \leq m < n$, is irreducible over $\mathbb{Q}$. By explicitly calculating the discriminant of $f(x)$, we prove that, when $\gcd(n, mB) = C = 1$, there exist infinitely many values of A such that the set $\{1, \theta, \theta^2, \ldots, \theta^{n-1}\}$ is an integral basis for the ring of integers of $\mathbb{Q}(\theta)$, where $f(\theta) = 0$.

2010 *Mathematics subject classification*: primary 11R04; secondary 11R09, 12F05.

Keywords and phrases: discriminant, monogenic, irreducible.

1. Introduction

Throughout this note, when we say a polynomial $f(x) \in \mathbb{Z}[x]$ is 'irreducible', we mean irreducible over $\mathbb{Q}$. We let $\Delta(f)$ and $\Delta(K)$ denote the discriminants over $\mathbb{Q}$, respectively, of the polynomial $f(x)$ and the number field K. If $f(x)$ is irreducible, with $f(\theta) = 0$ and $K = \mathbb{Q}(\theta)$, then we have the well-known equation

$$\Delta(f) = [\mathbb{Z}_K : \mathbb{Z}[\theta]]^2 \Delta(K), \tag{1.1}$$

where $\mathbb{Z}_K$ is the ring of integers of K (see [3]). We say that $f(x)$ is *monogenic* if $\mathbb{Z}_K = \mathbb{Z}[\theta]$, or equivalently from (1.1), if $\Delta(f) = \Delta(K)$. The property that $f(x)$ is monogenic facilitates computations in $\mathbb{Z}_K$ as in, for example, the cyclotomic fields (see [12]). Because $\Delta(f)$ is expressed in terms of the coefficients and exponents of $f(x)$, we see by (1.1) that one possible approach to proving that a generic polynomial $f(x)$ of arbitrary degree is monogenic is to determine conditions on the coefficients and exponents of $f(x)$ for which $\Delta(f)$ is squarefree (that is, not divisible by the square of any integer greater than 1). This approach was used in [1, 8]. But $\Delta(f)$ being squarefree is not necessary for $f(x)$ to be monogenic, and so, in the most general setting, any square factors of $\Delta(f)$ must be shown to be factors of $\Delta(K)$. The first step in this procedure is to derive a workable formula for $\Delta(f)$, which is not always tractable. One notable exception is the family of trinomials $f(x) = x^n + ax^m + b \in \mathbb{Z}[x]$ with $0 < m < n$. In this case, the formula

$$\Delta(f) = (-1)^{n(n-1)/2} b^{m-1} (n^{n/d} b^{(n-m)/d} - (-1)^{n/d} (n-m)^{(n-m)/d} m^{m/d} a^{n/d})^d,$$

where $d = \gcd(n, m)$, is due to Swan [11]. For the special trinomial $f(x) = x^n - x - 1$, the authors of the fascinating paper [1] use a generalisation of Wieferich primes to give a detailed analysis of the possible primes p such that

$$\Delta(f) = n^n + (-1)^n (n-1)^{n-1} \equiv 0 \pmod{p^2}. \tag{1.2}$$

If we let δ denote the density of positive integers n such that $\Delta(f)$ in (1.2) is squarefree, it is still unresolved as to whether $\delta > 0$. Nevertheless, the authors of [1] provide plausible evidence to support their conjecture that $\delta \geq 0.9934466$.

In [8], a more algebraic number-theoretic approach was used to show that, for each $n \geq 2$, there exists an irreducible polynomial $f(x)$ with $\deg(f) = n$ such that $\Delta(f)$ is squarefree and the Galois group of $f(x)$ over $\mathbb{Q}$ is the symmetric group on n letters. This result also provides an affirmative answer to a question of Lagarias [9].

Beyond these cases, there are isolated situations where knowledge of the nature of the zeros of $f(x)$ is useful in calculating $\Delta(f)$ (see, for example, [2, 5, 6]). Even when a reasonably 'nice' formula is known for $\Delta(f)$, a second obstacle arises in determining when $\Delta(f)$ is squarefree or managing the factors of $\Delta(f)$ that are not squarefree.

In this note, we derive a formula for the discriminant of irreducible polynomials of the form $f(x) = x^n + A(Bx + C)^m \in \mathbb{Z}[x]$ and we use it to prove the following theorem.

Theorem 1.1. *Let n, m and B be positive integers with $n \geq 3$, $1 \leq m \leq n - 1$ and $\gcd(n, mB) = 1$. Then there exist infinitely many positive integers A such that the polynomial $f(x) = x^n + A(Bx + 1)^m$ is irreducible and monogenic.*

All computer computations were done using either MAGMA, Maple or Sage.

2. Preliminaries

Definition 2.1. Let p be a prime and suppose

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x].$$

We say $f(x)$ is *p-Eisenstein* if

$$a_n \not\equiv 0 \pmod{p}, \quad a_i \equiv 0 \pmod{p} \text{ for } 0 \leq i \leq n-1 \quad \text{and} \quad a_0 \not\equiv 0 \pmod{p^2}.$$

We present some known facts that are used to establish Theorem 1.1.

Theorem 2.2 (See [7], Eisenstein's criterion). *Let p be a prime and let $f(x) \in \mathbb{Z}[x]$ be p-Eisenstein. Then $f(x)$ is irreducible.*

Theorem 2.3 (See [7]). *Let $f(x) \in \mathbb{Z}[x]$ be monic and irreducible with $\deg(f) = n$. Let $f(\theta) = 0$ and $K = \mathbb{Q}(\theta)$. Then*

$$\Delta(f) = (-1)^{n(n-1)/2} N_{K/\mathbb{Q}}(f'(\theta)).$$

Theorem 2.4 (See [4]). *Let p be a prime and let $f(x) \in \mathbb{Z}[x]$ be a monic p-Eisenstein polynomial with $\deg(f) = n$. Let $K = \mathbb{Q}(\theta)$, where $f(\theta) = 0$. Then $p^{n-1} \parallel \Delta(K)$ if $n \not\equiv 0 \pmod{p}$.*

https://doi.org/10.1017/S0004972719000182 Published online by Cambridge University Press

LEMMA 2.5. *Suppose that $F(x) = ax + b$, where a and b are positive integers with* $\gcd(a, b) = 1$. *Then there exist infinitely many primes p such that $F(p)$ is squarefree.*

Although Lemma 2.5 is well-known among analytic number theorists, there seems to be no reference in the literature for a proof of this specific fact. Lemma 2.5 follows from the asymptotic formula

$$|\{p \le N : p \text{ prime and } F(p) \text{ is squarefree}\}| \sim \left(\frac{C_1}{C_2}\right)\frac{N}{\log(N)}, \tag{2.1}$$

where

$$C_1 = \prod_{p \text{ prime}} \left(1 - \frac{1}{p(p-1)}\right) \approx 0.374$$

is Artin's constant and

$$C_2 = \prod_{p \text{ prime},\, p|ab} \left(1 - \frac{1}{p(p-1)}\right).$$

Hector Pasten has pointed out to us in a private communication that Lemma 2.5 can be deduced from a generalisation of (2.1) that appears in [10]. In that generalisation, C_1/C_2 is replaced by

$$\prod_{p \text{ prime}} \left(1 - \frac{\rho_F(p^2)}{p(p-1)}\right),$$

where $\rho_F(p^2)$ is the number of integers a, with $1 \le a \le p^2$ and $\gcd(a, p^2) = 1$, such that $F(a) \equiv 0 \pmod{p^2}$. Pasten's result applies unconditionally (without the assumption of the *abc* conjecture) to any $F(x)$ that factors into irreducibles of degree $d \le 3$ with no repeated factor.

3. The proof of Theorem 1.1

The following discriminant formula, which is needed for the proof of Theorem 1.1, is of some interest in its own right.

THEOREM 3.1. *Let $f(x) = x^n + A(Bx + C)^m \in \mathbb{Z}[x]$, where $n \ge 3$ and $1 \le m < n$. If $f(x)$ is irreducible, then*

$$\Delta(f) = (-1)^{n(n-1)/2} C^{n(m-1)} A^{n-1} (n^n C^{n-m} + (-1)^{n+m} B^n (n-m)^{n-m} m^m A).$$

PROOF. Suppose that $f(x)$ is irreducible and that $f(\theta) = 0$. Then, a straightforward manipulation yields

$$n\theta^{n-1} = \frac{-nA(B\theta + C)^m}{\theta}.$$

Since $f'(x) = nx^{n-1} + AmB(Bx + C)^{m-1}$, it follows that

$$\theta f'(\theta) = -A(B\theta + C)^{m-1}((n-m)B\theta + nC). \tag{3.1}$$

https://doi.org/10.1017/S0004972719000182 Published online by Cambridge University Press

We write simply $\mathcal{N}$ for the norm $\mathcal{N}_{K/\mathbb{Q}}$, where $K = \mathbb{Q}(\theta)$. Since $\mathcal{N}(\theta) = (-1)^n AC^m$, taking the norm of both sides of (3.1) yields

$$(-1)^n AC^m \mathcal{N}(f'(\theta)) = (-1)^n A^n \mathcal{N}(B\theta + C)^{m-1} \mathcal{N}((n-m)B\theta + nC). \tag{3.2}$$

To calculate $\mathcal{N}(B\theta + C)$, let $z = B\theta + C$ so that $\theta = (z - C)/B$. Then

$$0 = \left(\frac{z-C}{B}\right)^n + A\left(B\left(\frac{z-C}{B}\right) + C\right)^m = \frac{(z-C)^n + AB^n z^m}{B^n},$$

from which we deduce that the minimal polynomial of z is $g(x) = (x - C)^n + AB^n x^m$. Thus,

$$\mathcal{N}(B\theta + C) = (-1)^n g(0) = C^n. \tag{3.3}$$

Similarly, if we let $z = (n - m)B\theta + nC$, then

$$\begin{aligned} 0 &= \left(\frac{z-nC}{(n-m)B}\right)^n + A\left(B\left(\frac{z-nC}{(n-m)B}\right) + C\right)^m \\ &= \frac{(z-nC)^n + AB^n(n-m)^{n-m}(z-mC)^m}{(n-m)^n B^n}. \end{aligned}$$

Hence, the minimal polynomial for z in this case is

$$g(x) = (x - nC)^n + AB^n(n-m)^{n-m}(x - mC)^m.$$

Thus,

$$\begin{aligned} \mathcal{N}((n-m)B\theta + nC) &= (-1)^n g(0) \\ &= n^n C^n + AB^n(n-m)^{n-m}(-1)^{n+m} m^m C^m. \end{aligned} \tag{3.4}$$

Therefore, the theorem follows from Theorem 2.3, (3.2), (3.3) and (3.4). □

Proof of Theorem 1.1. Since $\gcd(n, mB) = 1$, it follows that

$$\gcd(n^n, (-1)^{n+m} B^n (n-m)^{n-m} m^m) = 1.$$

Thus, by Lemma 2.5, there exist infinitely many primes p such that

$$n^n + (-1)^{n+m} B^n (n-m)^{n-m} m^m p \quad \text{is squarefree.} \tag{3.5}$$

For any such prime p with $p > n$, let $A = p$. Then $f(x)$ is irreducible since $f(x)$ is p-Eisenstein, and hence

$$\Delta(f) = (-1)^{n(n-1)/2} p^{n-1} (n^n + (-1)^{n+m} B^n (n-m)^{n-m} m^m p), \tag{3.6}$$

by Theorem 3.1. Also, since $p > n$, we have $n \not\equiv 0 \pmod{p}$ and we conclude from Theorem 2.4 that $p^{n-1} \parallel \Delta(K)$. Therefore, from (1.1), (3.5) and (3.6), it follows that $f(x)$ is monogenic. □

https://doi.org/10.1017/S0004972719000182 Published online by Cambridge University Press

TABLE 1. Number of degree-11 monogenics and nonmonogenics.

A	# of monogenics	# of nonmonogenics
2	88	12
3	96	4
5	92	8
7	92	8
13	84	16
17	91	9
19	92	8
23	86	14
29	93	7

4. Final remarks

Under the restrictions that A is prime and $\gcd(A, n) = \gcd(n, mB) = 1$, computer evidence suggests that most polynomials $f(x) = x^n + A(Bx + 1)^m \in \mathbb{Z}[x]$, with $n \geq 3$ and $1 \leq m \leq n - 1$, are monogenic. The data are given in Table 1 for $n = 11$, $1 \leq m \leq 10$, $1 \leq B \leq 10$ and A prime with $2 \leq A \leq 29$, $A \neq 11$. In this situation, for each value of A there is a total of 100 polynomials to consider.

A further analysis of the numerical data suggests the following conjecture.

CONJECTURE 4.1. Let A be prime, and n, m and B be positive integers with $n \geq 3$, $1 \leq m \leq n - 1$ and $\gcd(n, mB) = 1$. Then $f(x) = x^n + A(Bx + 1)^m$ is monogenic if and only if $n^n + (-1)^{n+m} B^n (n - m)^{n-m} m^m A$ is squarefree.

REMARK 4.2. The data in Table 1 and the evidence supporting Conjecture 4.1 were generated by Maple programs. The source code for these programs will be provided upon an email request to the author.

Acknowledgement

The author thanks the anonymous referee for helpful comments.

References

[1] D. W. Boyd, G. Martin and M. Thom, 'Squarefree values of trinomial discriminants', *LMS J. Comput. Math.* **18**(1) (2015), 148–169.

[2] M. Cipu and F. Luca, 'On the Galois group of the generalized Fibonacci polynomial', *An. Ştiinţ. Univ. Ovidius Constanţa Ser. Mat.* **9**(1) (2001), 27–38.

[3] H. Cohen, *A Course in Computational Algebraic Number Theory* (Springer, Berlin–Heidelberg, 2000).

[4] K. Conrad, 'Totally ramified primes and Eisenstein polynomials', Preprint, http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/totram.pdf.

[5] K. Dilcher and K. B. Stolarsky, 'Resultants and discriminants of Chebyshev and related polynomials', *Trans. Amer. Math. Soc.* **357**(3) (2005), 965–981.

[6] T. A. Gassert, 'Chebyshev action on finite fields', *Discrete Math.* **315** (2014), 83–94.
[7] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd edn, Graduate Texts in Mathematics, 84 (Springer, New York, 1990).
[8] K. Kedlaya, 'A construction of polynomials with squarefree discriminants', *Proc. Amer. Math. Soc.* **140**(9) (2012), 3025–3033; English summary.
[9] J. Lagarias, 'Problem 99:10', in: *Western Number Theory Problems, 16 & 19 Dec 1999, Asilomar, CA* (ed. G. Myerson), http://www.math.colostate.edu/~achter/wntc/problems/problems2000.pdf.
[10] H. Pasten, 'The ABC conjecture, arithmetic progressions of primes and squarefree values of polynomials at prime arguments', *Int. J. Number Theory* **11**(3) (2015), 721–737.
[11] R. Swan, 'Factorization of polynomials over finite fields', *Pacific J. Math.* **12** (1962), 1099–1106.
[12] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd edn, Graduate Texts in Mathematics, 83 (Springer, New York, 1997).

LENNY JONES, Department of Mathematics,
Shippensburg University, Shippensburg, PA 17257, USA
e-mail: lkjone@ship.edu

https://doi.org/10.1017/S0004972719000182 Published online by Cambridge University Press