Bull. Aust. Math. Soc. **110** (2024), 460–467
doi:10.1017/S0004972724000182

CHARACTERISATION OF PRIMES DIVIDING THE INDEX OF A CLASS OF POLYNOMIALS AND ITS APPLICATIONS

ANUJ JAKHAR

(Received 16 January 2024; accepted 10 February 2024; first published online 1 April 2024)

Dedicated to Professor Sudesh Kaur Khanduja

Abstract

Let $\mathbb{Z}_K$ denote the ring of algebraic integers of an algebraic number field $K = \mathbb{Q}(\theta)$, where θ is a root of a monic irreducible polynomial $f(x) = x^n + a(bx + c)^m \in \mathbb{Z}[x]$, $1 \le m < n$. We say $f(x)$ is monogenic if $\{1, \theta, \ldots, \theta^{n-1}\}$ is a basis for $\mathbb{Z}_K$. We give necessary and sufficient conditions involving only a, b, c, m, n for $f(x)$ to be monogenic. Moreover, we characterise all the primes dividing the index of the subgroup $\mathbb{Z}[\theta]$ in $\mathbb{Z}_K$. As an application, we also provide a class of monogenic polynomials having non square-free discriminant and Galois group S_n, the symmetric group on n letters.

2020 *Mathematics subject classification*: primary 11R04; secondary 11R29, 11Y40.

Keywords and phrases: rings of algebraic integers, index of an algebraic integer, power basis.

1. Introduction and statements of results

Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with θ in the ring $\mathbb{Z}_K$ of algebraic integers of K and let $f(x)$ of degree n be the minimal polynomial of θ over the field $\mathbb{Q}$ of rational numbers. Let d_K denote the discriminant of K and D_f the discriminant of the polynomial $f(x)$. It is well known that d_K and D_f are related by the formula

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

We say that $f(x)$ is monogenic if $\mathbb{Z}_K = \mathbb{Z}[\theta]$, or equivalently, if $D_f = d_K$. In this case, $\{1, \theta, \ldots, \theta^{n-1}\}$ is an integral basis of K and K is a monogenic number field. A number field K is called monogenic if there exists some $\alpha \in \mathbb{Z}_K$ such that $\mathbb{Z}_K = \mathbb{Z}[\alpha]$.

The determination of monogenity of an algebraic number field is one of the classical and important problems in algebraic number theory. An arithmetic characterisation of monogenic number fields is a problem due to Hasse (see [6]). Gaál's book [5] provides some classifications of monogenity in lower degree number fields. Using Dedekind's Index Criterion, Jakhar *et al.* [8] gave necessary and sufficient conditions

The author is thankful to IIT Madras for NFIG grant RF/22-23/1035/MA/NFIG/009034.

© The Author(s), 2024. Published by Cambridge University Press on behalf of Australian Mathematical Publishing Association Inc.

https://doi.org/10.1017/S0004972724000182 Published online by Cambridge University Press

for $\mathbb{Z}_K = \mathbb{Z}[\theta]$ when θ is a root of an irreducible trinomial $x^n + ax^m + b \in \mathbb{Z}[x]$ having degree n, providing infinitely many monogenic trinomials. Jones [9] computed the discriminant of the polynomial $f(x) = x^n + a(bx + c)^m \in \mathbb{Z}[x]$ with $1 \le m < n$ and proved that when $\gcd(n, mb) = 1$, there exist infinitely many values of a such that $\mathbb{Z}_K = \mathbb{Z}[\theta]$ where $K = \mathbb{Q}(\theta)$ and θ has minimal polynomial $f(x)$. He also conjectured that if $\gcd(n, mb) = 1$ and a is a prime number, then the polynomial $x^n + a(bx + c)^m \in \mathbb{Z}[x]$ is monogenic if and only if $n^n + (-1)^{n+m} b^n (n - m)^{n-m} m^m a$ is square-free. Recently, Kaur and Kumar [12] proved that this conjecture is true. Jones [11] gave infinite families of number fields K generated by a root θ of an irreducible quadrinomial, quintinomial or sextinomial for which $\mathbb{Z}_K = \mathbb{Z}[\theta]$. He also proved in [10] that if θ is a root of an irreducible polynomial of the type $f(x) = x^p - 2ptx^{p-1} + p^2t^2x^{p-2} + 1 \in \mathbb{Z}[x]$ and p is an odd prime with $p \nmid t$, then $\mathbb{Z}_K \neq \mathbb{Z}[\theta]$.

Let $K = \mathbb{Q}(\theta)$ be an algebraic number field where θ has minimal polynomial $f(x) = x^n + a(bx + c)^m$ over $\mathbb{Q}$ with $1 \le m < n$. We characterise all the primes dividing the index of $\mathbb{Z}[\theta]$ in $\mathbb{Z}_K$. As an application, we provide necessary and sufficient conditions for $\mathbb{Z}_K = \mathbb{Z}[\theta]$. We also establish a more general result confirming [9, Conjecture 4.1]. Further, we give a class of monogenic polynomials of prime degree q having non square-free discriminant and Galois group isomorphic to the symmetric group S_q. In some examples, we determine the index $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ as well.

Throughout the paper, D_f will stand for the discriminant of $f(x) = x^n + a(bx + c)^m$ with $1 \le m < n$. Jones [9, Theorem 3.1] proved that the discriminant D_f is given by

$$D_f = (-1)^{\binom{n}{2}} c^{n(m-1)} a^{n-1} [c^{n-m} n^n + (-1)^{m+n} ab^n m^m (n - m)^{n-m}]. \tag{1.1}$$

We prove the following result.

Theorem 1.1. *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with θ in the ring $\mathbb{Z}_K$ of algebraic integers of K having minimal polynomial $f(x) = x^n + a(bx + c)^m$, $1 \le m < n$, over $\mathbb{Q}$. A prime factor p of the discriminant D_f of $f(x)$ does not divide $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ if and only if p satisfies one of the following conditions:*

(i) *when $p \mid a$, then $p^2 \nmid ac$;*
(ii) *when $p \nmid a$, $p \mid b$, $p \mid c$, then $m = 1$ and $p^2 \nmid c$;*
(iii) *when $p \nmid ac$ and $p \mid b$ with $j \ge 1$ as the highest power of p dividing n, then either $p \mid b_1$ and $p \nmid c_2$ or p does not divide $b_1[(ac^m)b_1^n + (-c_2)^n]$, where*

$$b_1 = \frac{mabc^{m-1}}{p}, \quad c_2 = \frac{1}{p}[ac^m + (-ac^m)^{p^j}];$$

(iv) *when p does not divide ab and $p \mid c$, then $m = 1$ and either $p \mid b_2$ with $p \nmid c_1$ or p does not divide $b_2[(ab)b_2^{n-1} + (-c_1)^{n-1}]$, where*

$$b_2 = \frac{1}{p}[ab + (-ab)^{p^l}], \quad c_1 = \frac{ac}{p} \quad \text{and} \quad n - 1 = p^l s', p \nmid s';$$

https://doi.org/10.1017/S0004972724000182 Published online by Cambridge University Press

(v) *when p does not divide abc and $p \mid m$ with $n = s'p^k,\ m = sp^k,\ p \nmid \gcd(s', s)$, then the polynomials*

$$x^{s'} + a(bx+c)^s \quad and \quad \frac{1}{p}\Big[pt(bx+c)^m - \sum_{j=1}^{p^k-1}\binom{p^k}{j}(x^{s'})^{p^k-j}(a(bx+c)^s)^j\Big]$$

are coprime modulo p, where $t \in \mathbb{Z}$ is an integer such that $a = a^{p^k} + pt$;

(vi) *when $p \nmid abcm$, then p^2 does not divide D_f.*

The following corollary is immediate. It extends the main results of [9].

COROLLARY 1.2. *Let $K = \mathbb{Q}(\theta)$ and $f(x) = x^n + a(bx+c)^m$ be as in Theorem 1.1. Then $\mathbb{Z}_K = \mathbb{Z}[\theta]$ if and only if each prime p dividing D_f satisfies one of the conditions (i)–(vi) of Theorem 1.1.*

If we take $\gcd(n, mb) = 1$ and $c = 1$, then conditions (ii)–(v) of Theorem 1.1 are not possible. So in the special case when $c = 1$ and $\gcd(n, mb) = 1$, the above corollary provides the main result of [12] stated below. This gives infinite families of monogenic polynomials and establishes a more general form of [9, Conjecture 4.1].

COROLLARY 1.3 [12]. *Let $f(x) = x^n + a(bx+1)^m \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree n with $\gcd(n, mb) = 1$. Then $\mathbb{Z}_K = \mathbb{Z}[\theta]$ if and only if each prime p dividing D_f satisfies either (i) $p \mid a$ and $p^2 \nmid a$ or (ii) $p \nmid a$ and $p^2 \nmid D_f$.*

The following proposition follows readily from the proof of Theorem 1.1(vi) and is of independent interest.

PROPOSITION 1.4. *Let $f(x) = x^q + a(bx+c)^m \in \mathbb{Z}[x]$, $1 \le m < q$, be an irreducible polynomial of prime degree. If there exists a prime p such that p divides D_f and $p^2 \nmid D_f$ with $p \nmid abcm$, then the Galois group of $f(x)$ is S_q.*

The following result is an immediate consequence of Corollary 1.3 and Proposition 1.4. It provides a class of monogenic polynomials having non square-free discriminant and Galois group equal to a symmetric group.

COROLLARY 1.5. *Let m be a positive odd integer and $f(x) = x^q + a(bx+1)^m \in \mathbb{Z}[x]$ be a polynomial having prime degree $q \ge 3$ with $q \nmid b$. If $a \notin \{0, \pm 1\}$ and D_f/a^{q-1} are square-free numbers, then $f(x)$ is a monogenic polynomial having Galois group S_q.*

The following example is an application of Theorem 1.1, Corollary 1.3 and Proposition 1.4. In this example, $K = \mathbb{Q}(\theta)$ with θ a root of $f(x)$.

EXAMPLE 1.6. Let p be a prime number. Consider $f(x) = x^p + p(x+1)^{p-1}$. Note that $|D_f| = p^p(p^{p-1} - (p-1)^{p-1})$. Using Proposition 1.4, it is easy to check that the Galois group of $f(x)$ is S_p. By Corollary 1.3, $\mathbb{Z}_K = \mathbb{Z}[\theta]$ if and only if $p^{p-1} - (p-1)^{p-1}$ is square-free. We now compute $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ for $p < 20$. For $p = 2, 3, 7, 11, 17$, it can be verified that the number $p^{p-1} - (p-1)^{p-1}$ is square-free; and hence $\mathbb{Z}_K = \mathbb{Z}[\theta]$. Next we calculate the exact value of $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ corresponding to $p = 5, 13$ and 19.

https://doi.org/10.1017/S0004972724000182 Published online by Cambridge University Press

(i) For $p = 5$, it can be easily checked that $D_f = 5^5 \cdot 3^2 \cdot 41$. In view of Theorem 1.1(i), 5 does not divide $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$. Also, 3 divides $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ and 41 does not divide $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ by Theorem 1.1(vi). Since $D_f = [\mathbb{Z}_K : \mathbb{Z}[\theta]]^2 \cdot d_K$, where d_K is the discriminant of K, we see that $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ is 3 when $p = 5$.

(ii) Consider $p = 13$. One can verify that $D_f = 13^{13} \cdot 5^2 \cdot 7 \cdot 67 \cdot 109 \cdot 157 \cdot 229 \cdot 313$. By Theorem 1.1(i), 13 does not divide $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$. Also in view of Theorem 1.1(vi), 5 divides $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ and the primes 7, 67, 109, 157, 229, 313 do not divide $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$. Since the exact power of 5 dividing D_f is 2, $[\mathbb{Z}_K : \mathbb{Z}[\theta]] = 5$.

(iii) When $p = 19$, then one can check that the prime factorisation of D_f is given by $19^{19} \cdot 7^3 \cdot r$ with r a square-free number. Arguing as above, 19 and each prime p dividing r do not divide $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ and 7 divides $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$. Therefore, $[\mathbb{Z}_K : \mathbb{Z}[\theta]] = 7$.

2. Proof of Theorem 1.1

In what follows, while dealing with a prime number p, for a polynomial $h(x)$ in $\mathbb{Z}[x]$, we shall denote by $\bar{h}(x)$ the polynomial over $\mathbb{Z}/p\mathbb{Z}$ obtained by interpreting each coefficient of $h(x)$ modulo p.

We first state the following well-known theorem. The equivalence of assertions (i) and (ii) of the theorem was proved by Dedekind (see [2, Theorem 6.1.4], [3]). A simple proof of the equivalence of assertions (ii) and (iii) is given in [7, Lemma 2.1].

THEOREM 2.1. *Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial having the factorisation $\bar{g}_1(x)^{e_1} \cdots \bar{g}_t(x)^{e_t}$ modulo a prime p 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 $K = \mathbb{Q}(\theta)$ with θ a root of $f(x)$. Then the following statements are equivalent:*

(i) *p does not divide $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$;*

(ii) *for each i, either $e_i = 1$ or $\bar{g}_i(x)$ does not divide $\overline{M}(x)$ where*

$$M(x) = \frac{1}{p}(f(x) - g_1(x)^{e_1} \cdots g_t(x)^{e_t});$$

(iii) *$f(x)$ does not belong to the ideal $\langle p, g_i(x)\rangle^2$ in $\mathbb{Z}[x]$ for any i, $1 \le i \le t$.*

The next lemma (see [7, Corollary 2.3]) is easily proved using the binomial theorem.

LEMMA 2.2. *Let $k \ge 1$ be the highest power of a prime p dividing a number $n = p^k s'$ and c be an integer not divisible by p. If $\bar{g}_1(x) \cdots \bar{g}_r(x)$ is the factorisation of $x^{s'} - \bar{c}$ into a product of distinct irreducible polynomials over $\mathbb{Z}/p\mathbb{Z}$ with each $g_i(x) \in \mathbb{Z}[x]$ monic, then*

$$x^n - c = (g_1(x) \cdots g_r(x) + pH(x))^{p^k} + pg_1(x) \cdots g_r(x)T(x) + p^2U(x) + c^{p^k} - c$$

for some polynomials $H(x), T(x), U(x) \in \mathbb{Z}[x]$.

PROOF OF THEOREM 1.1. Let p be a prime dividing D_f. In view of Theorem 2.1, p does not divide $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ if and only if $f(x) \notin \langle p, g(x)\rangle^2$ for any monic polynomial

https://doi.org/10.1017/S0004972724000182 Published online by Cambridge University Press

$g(x) \in \mathbb{Z}[x]$ which is irreducible modulo p. Note that $f(x) \notin \langle p, g(x)\rangle^2$ if $\bar{g}(x)$ is not a repeated factor of $\bar{f}(x)$. We prove the theorem case by case.

Case (i): $p \mid a$. In this case, $f(x) \equiv x^n \pmod{p}$. Clearly, $f(x) \in \langle p, x\rangle^2$ if and only if p^2 divides ac^m; consequently, $p \nmid [\mathbb{Z}_K : \mathbb{Z}[\theta]]$ if and only if $p^2 \nmid ac$.

Case (ii): *$p \nmid a$ and p divides both b and c*. In this situation, $f(x) \equiv x^n \pmod{p}$ and it is easy to see that $f(x) \in \langle p, x\rangle^2$ if and only if p^2 divides c^m. Therefore, $p \nmid [\mathbb{Z}_K : \mathbb{Z}[\theta]]$ if and only if $p^2 \nmid c^m$, that is, $m = 1$ and $p^2 \nmid c$.

Case (iii): *$p \nmid ac$ and $p \mid b$*. As $p \mid D_f$, it is clear from (1.1) that $p \mid n$. Write $n = p^j s'$, $p \nmid s'$. By the binomial theorem,

$$f(x) \equiv x^n + ac^m \equiv (x^{s'} + ac^m)^{p^j} \pmod{p}.$$

Let $\bar{g}_1(x)\cdots\bar{g}_t(x)$ be the factorisation of $h(x) = x^{s'} + ac^m$ over $\mathbb{Z}/p\mathbb{Z}$, where $g_i(x) \in \mathbb{Z}[x]$ are monic polynomials which are distinct and irreducible modulo p. Write $h(x)$ as $g_1(x)\cdots g_t(x) + pH(x)$ for some polynomial $H(x) \in \mathbb{Z}[x]$. Applying Lemma 2.2 to $h(x)$ and keeping in view that

$$f(x) = h(x^{p^j}) + a(bx)^m + \binom{m}{1} a(bx)^{m-1}c + \cdots + \binom{m}{m-1} a(bx)c^{m-1}$$

with $p \mid b$, we see that

$$f(x) = \Big(\prod_{i=1}^{t} g_i(x) + pH(x)\Big)^{p^j} + pT(x)\prod_{i=1}^{t} g_i(x) + p^2U(x) + ac^m + (-ac^m)^{p^j} + ma(bx)c^{m-1} \tag{2.1}$$

for some polynomials $T(x), U(x) \in \mathbb{Z}[x]$. As $j \ge 1$, the first three summands on the right-hand side of (2.1) belong to $\langle p, g_i(x)\rangle^2$ for each i, $1 \le i \le t$. So $f(x) \in \langle p, g_i(x)\rangle^2$ for some i, $1 \le i \le t$, if and only if $mabc^{m-1}x + ac^m + (-ac^m)^{p^j} = p(b_1x + c_2)$ does so. Clearly, $p(b_1x + c_2)$ belongs to $\langle p, g_i(x)\rangle^2$ for some i if and only if either p divides both b_1, c_2 or $p \nmid b_1$ and the polynomials $\bar{b}_1x + \bar{c}_2$, $x^n + \overline{ac^m}$ have a common root. One can easily check that the polynomials $\bar{b}_1x + \bar{c}_2$ and $x^n + \overline{ac^m}$ have a common root if and only if $(-\bar{c}_2/\bar{b}_1)^n = -\overline{ac^m}$, that is, if and only if $p \mid [(-ac^m)b_1^n - (-c_2)^n]$. Hence, $f(x) \notin \langle p, g_i(x)\rangle^2$ for any i if and only if either $p \mid b_1$ and $p \nmid c_2$ or p does not divide $b_1[(ac^m)b_1^n + (-c_2)^n]$. This proves the theorem in case (iii) by virtue of Theorem 2.1.

Case (iv): *$p \nmid ab$ and $p \mid c$*. In this case, $\overline{f}(x) = x^m(x^{n-m} + \overline{ab^m})$. If $m \ge 2$, then x is a repeated factor and it is easy to check that $f(x) \in \langle p, x\rangle^2$, that is, p always divides $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ by Theorem 2.1. So, assume now that $m = 1$. By (1.1), $p \mid (n-1)$, say $n - 1 = p^l s'$ with $p \nmid s'$. Write $x^{s'} + ab = g_1(x)\cdots g_t(x) + pH(x)$, where $g_1(x), \ldots, g_t(x)$ are monic polynomials which are distinct as well as irreducible modulo p and $H(x) \in \mathbb{Z}[x]$. Applying Lemma 2.2 to $h(x) = x^{s'} + ab$, we can write $f(x) = x(x^{n-1} + ab) + ac$ as

https://doi.org/10.1017/S0004972724000182 Published online by Cambridge University Press

$$f(x) = x\Big[\Big(\prod_{i=1}^{t} g_i(x) + pH(x)\Big)^{p^l} + pT(x)\prod_{i=1}^{t} g_i(x) + p^2U(x) + ab + (-ab)^{p^l}\Big] + ac, \tag{2.2}$$

where $T(x), U(x)$ belong to $\mathbb{Z}[x]$. Note that $x, \bar{g}_1(x), \ldots, \bar{g}_t(x)$ are distinct irreducible factors of $\bar{f}(x)$. Since $l \geq 1$, the first three summands inside the square bracket on the right-hand side of (2.2) belong to $\langle p, g_i(x)\rangle^2$ for each i, $1 \leq i \leq t$. So $f(x) \in \langle p, g_i(x)\rangle^2$ for some i, $1 \leq i \leq t$, if and only if $(ab + (-ab)^{p^l})x + ac = p(b_2x + c_1)$ does so. Clearly, the polynomial $p(b_2x + c_1)$ belongs to $\langle p, g_i(x)\rangle^2$ for some i if and only if either p divides both b_2, c_1 or $p \nmid b_2$ and the polynomials $\bar{b}_2x + \bar{c}_1$, $x^{n-1} + \overline{ab}$ have a common root. The polynomials $\bar{b}_2x + \bar{c}_1$ and $x^{n-1} + \overline{ab}$ have a common root if and only if $(-\bar{c}_1/\bar{b}_2)^{n-1} = -\overline{ab}$. Thus, $f(x) \in \langle p, g_i(x)\rangle^2$ for some i if and only if either p divides both b_2, c_1 or $p \nmid b_2$ and $p \mid [(-ab)b_2^{n-1} - (-c_1)^{n-1}]$. So we conclude that p does not divide $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ if and only if $m = 1$ and either $p \mid b_2$ with $p \nmid c_1$ or p does not divide $b_2[(ab)b_2^{n-1} + (-c_1)^{n-1}]$. This proves the theorem in case (iv).

Case (v): *$p \nmid abc$ and $p \mid m$*. As $p \mid D_f$, p divides n in view of (1.1). Write $n = s'p^k$, $m = sp^k$ with $p \nmid \gcd(s', s)$ so that $f(x) = (x^{s'})^{p^k} + a(bx + c)^{sp^k}$. Set $h(x) = x^{s'} + a(bx + c)^s$. Let $t \in \mathbb{Z}$ be an integer such that $a = a^{p^k} + pt$. Then one can easily check that $f(x) \equiv h(x)^{p^k} \pmod p$. Let $h(x) \equiv g_1(x)^{d_1} \cdots g_t(x)^{d_t} \pmod p$ be the factorisation of $h(x)$ into a product of irreducible polynomials modulo p with $g_i(x) \in \mathbb{Z}[x]$ monic and $d_i > 0$. Write

$$f(x) = h(x)^{p^k} + pt(bx + c)^m - \sum_{j=1}^{p^k-1} \binom{p^k}{j} (x^{s'})^{p^k-j}(a(bx + c)^s)^j.$$

Now $f(x) = (g_1(x)^{d_1} \cdots g_t(x)^{d_t})^{p^k} + pM(x)$ for some $M(x) \in \mathbb{Z}[x]$. Since $k > 0$, by Theorem 2.1, p does not divide $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ if and only if $\overline{M}(x)$ is coprime to $\bar{h}(x)$, which holds if and only if the polynomial

$$\frac{1}{p}\Big[pt(bx + c)^m - \sum_{j=1}^{p^k-1} \binom{p^k}{j} (x^{s'})^{p^k-j}(a(bx + c)^s)^j\Big]$$

is coprime to $h(x)$ modulo p. This proves the theorem in case (v).

Case (vi): *$p \nmid abcm$*. Since $p \mid D_f$ and $p \nmid abcm$, it follows from (1.1) that $p \nmid n(n - m)$. Let β be a repeated root of $\bar{f}(x) = x^n + \bar{a}(\bar{b}x + \bar{c})^m$ in the algebraic closure of $\mathbb{Z}/p\mathbb{Z}$. Then

$$\bar{f}(\beta) = \beta^n + \bar{a}(\bar{b}\beta + \bar{c})^m = \bar{0}; \quad \bar{f}'(\beta) = \bar{n}\beta^{n-1} + \bar{m}\bar{a}\bar{b}(\bar{b}\beta + \bar{c})^{m-1} = \bar{0}. \tag{2.3}$$

On substituting $\bar{n}\beta^{n-1} = -\bar{m}\bar{a}\bar{b}(\bar{b}\beta + \bar{c})^{m-1}$ in the first equation of (2.3), we see that

$$(b\beta + c)^{m-1}(ab(n - m)\beta + nac) \equiv 0 \pmod p.$$

https://doi.org/10.1017/S0004972724000182 Published online by Cambridge University Press

Observe that $(b\beta + c) \not\equiv 0 \pmod p$, otherwise $\beta = \bar{0}$ in view of the first equation of (2.3) which is not possible as $p \nmid ac$. Therefore, keeping in mind that $p \nmid abcn(n-m)$,

$$\beta \equiv -\frac{nc}{b(n-m)} \pmod p \tag{2.4}$$

is the unique repeated root of $\bar{f}(x)$ in $\mathbb{Z}/p\mathbb{Z}$ and it can be easily checked that β has multiplicity 2. Assuming that β is a positive integer satisfying (2.4), we can write

$$\begin{aligned} f(x) &= (x-\beta+\beta)^n + a(b(x-\beta+\beta)+c)^m, \\ &= \sum_{k=0}^{n}\binom{n}{k}\beta^{n-k}(x-\beta)^k + a\bigg(\sum_{k=0}^{m}\binom{m}{k}(b\beta+c)^{m-k}b^k(x-\beta)^k\bigg), \\ &= (x-\beta)^2 g(x) + f'(\beta)(x-\beta) + f(\beta), \end{aligned}$$

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

$$g(x) = \sum_{k=2}^{n}\binom{n}{k}\beta^{n-k}(x-\beta)^{k-2} + a\bigg(\sum_{k=2}^{m}\binom{m}{k}(b\beta+c)^{m-k}b^k(x-\beta)^{k-2}\bigg)$$

is in $\mathbb{Z}[x]$. Then

$$\bar{f}(x) = (x-\beta)^2\bar{g}(x), \tag{2.5}$$

where $\bar{g}(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ is separable. Write $g(x) = g_1(x)\cdots g_t(x) + ph(x)$, where $g_1(x), \ldots, g_t(x)$ are monic polynomials which are distinct as well as irreducible modulo p and $h(x) \in \mathbb{Z}[x]$ monic. Therefore, we can write

$$f(x) = (x-\beta)^2\bigg(\prod_{i=1}^{t} g_i(x) + ph(x)\bigg) + f'(\beta)(x-\beta) + f(\beta).$$

So, by Theorem 2.1, p does not divide $[\mathbb{Z}_K : \mathbb{Z}[\theta]]$ if and only if $\overline{M}(x)$ is coprime to $x-\beta$, where

$$M(x) = \frac{1}{p}[p(x-\beta)^2h(x) + (x-\beta)f'(\beta) + f(\beta)],$$

that is, $f(\beta) \not\equiv 0 \pmod{p}^2$. By (2.4), since $p \nmid abcmn(n-m)$, we see that $f(\beta) \not\equiv 0 \pmod{p}^2$ if and only if $(n^nc^{n-m} + (-1)^{n+m}b^n(n-m)^{n-m}m^ma) \not\equiv 0 \pmod{p}^2$. This final case completes the proof of the theorem. □

3. Proof of Proposition 1.4

The following two results on Galois groups will be used in the proof of Proposition 1.4.

THEOREM 3.1 [1, Theorem 2.1]. *Let $f(x) \in \mathbb{Z}[x]$ be a monic irreducible polynomial of degree n, having a root θ. Let p be a rational prime which is ramified in $\mathbb{Q}(\theta)$. Suppose that $f(x) \equiv (x-c)^2\phi_2(x)\cdots\phi_r(x) \pmod p$, where $(x-c), \phi_2(x), \ldots, \phi_r(x)$ are monic polynomials over $\mathbb{Z}$ which are distinct and irreducible modulo p. Then the Galois group*

https://doi.org/10.1017/S0004972724000182 Published online by Cambridge University Press

of $f(x)$ over $\mathbb{Q}$ contains a nontrivial automorphism which keeps $n-2$ roots of $f(x)$ fixed.

LEMMA 3.2 [4, Lemma 2]. *Let $f(x)$ be an irreducible polynomial of degree $n \geq 2$. If the Galois group of $f(x)$ over $\mathbb{Q}$ contains a transposition and a p-cycle for some prime $p > n/2$, then the Galois group is S_n.*

PROOF OF PROPOSITION 1.4. Let α be any root of $f(x)$, so that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = q$. By the fundamental theorem of Galois theory, the Galois group of $f(x)$, say G_f, contains a subgroup whose index is q. By Lagrange's theorem, q divides the order of G_f. So, by Cauchy's theorem, G_f has an element of order q. Hence, G_f contains a q-cycle. Now we show that G_f contains a transposition. By hypothesis, there exists a prime p such that $p \mid D_f$ and $p \nmid abcm$. As in (2.5) in the proof of Theorem 1.1(vi), $f(x) \equiv (x-\beta)^2 g_1(x) \cdots g_t(x) \pmod{p}$, where $x-\beta, g_1(x), \ldots, g_t(x)$ are monic polynomials over $\mathbb{Z}$ which are distinct and irreducible modulo p. Also, if $K = \mathbb{Q}(\theta)$ with θ a root of $f(x)$, then keeping in mind the hypothesis $p^2 \nmid D_f$ and the relation $D_f = [\mathbb{Z}_K : \mathbb{Z}[\theta]]^2 d_K$, we see that $p \mid d_K$. Hence, p is ramified in K. Therefore, by Theorem 3.1, the Galois group of $f(x)$ contains a transposition. Hence, by Lemma 3.2, the Galois group is S_q. □

References

[1] A. Bishnoi and S. K. Khanduja, 'A class of trinomials with Galois group S_n', *Algebra Colloq.* **19**(1) (2012), 905–911.

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

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

[4] M. Filaseta and R. Moy, 'On the Galois group over $\mathbb{Q}$ of a truncated binomial expansion', *Colloq. Math.* **154** (2018), 295–308.

[5] I. Gaál, *Diophantine Equations and Power Integral Bases: Theory and Algorithms*, 2nd edn (Birkhäuser/Springer, Cham, 2019).

[6] H. Hasse, *Zahlentheorie* (Akademie-Verlag, Berlin, 1963).

[7] A. Jakhar, S. K. Khanduja and N. Sangwan, 'On prime divisors of the index of an algebraic integer', *J. Number Theory* **166** (2016), 47–61.

[8] A. Jakhar, S. K. Khanduja and N. Sangwan, 'Characterisation of primes dividing the index of a trinomial', *Int. J. Number Theory* **13**(10) (2017), 2505–2514.

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

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

[11] L. Jones, 'Infinite families of monogenic quadrinomials, quintinomials and sextinomials', *Colloq. Math.* **169** (2022), 1–10.

[12] S. Kaur and S. Kumar, 'On a conjecture of Lenny Jones about certain monogenic polynomials', *Bull. Aust. Math. Soc.*, to appear. Published online (21 November 2023).

ANUJ JAKHAR, Department of Mathematics,
Indian Institute of Technology (IIT) Madras, Chennai, India
e-mail: anujjakhar@iitm.ac.in, anujiisermohali@gmail.com

https://doi.org/10.1017/S0004972724000182 Published online by Cambridge University Press