COLLOQUIUM MATHEMATICUM

Online First version

ON THE DISCRIMINANT OF PURE NUMBER FIELDS

BY

ANUJ JAKHAR (Raipur), SUDESH K. KHANDUJA (SAS Nagar and Chandigarh) and NEERAJ SANGWAN (Mumbai)

Abstract. Let $K = \mathbb{Q}(\sqrt[n]{a})$ be an extension of degree n of the field $\mathbb{Q}$ of rational numbers, where the integer a is such that for each prime p dividing n either $p \nmid a$ or the highest power of p dividing a is coprime to p; this condition is clearly satisfied when a, n are coprime or a is squarefree. The paper contains an explicit formula for the discriminant of K involving only the prime powers dividing a, n.

1. Introduction and main results. Discriminant is one of the most basic invariants associated to an algebraic number field. The problem of its computation specially for pure algebraic number fields has attracted the attention of many mathematicians (cf. [B27], [D00], [F84], [HN15], [JKS17], [L97], [O82] [W10]). By a *pure number field* we mean an algebraic number field of the type $\mathbb{Q}(\sqrt[n]{a})$, where the polynomial $x^n - a$ with integer coefficients is irreducible over the field $\mathbb{Q}$ of rational numbers. In 1897, Landsberg [L97] gave a formula for the discriminant of pure prime degree number fields. In 1927, Berwick [B27] described a $\mathbb{Z}_{(p)}$-basis for the integral closure of the localization $\mathbb{Z}_{(p)}$ of $\mathbb{Z}$ at each prime p in $\mathbb{Q}(\sqrt[n]{a})$ having squarefree degree n. In 1982, Okutsu [O82] gave a formula for the discriminant of $\mathbb{Q}(\sqrt[n]{a})$ when a, n are coprime. In 1984, Funakura [F84] provided a formula for the discriminant of all pure quartic fields. In 2015, Hameed and Nakahara [HN15] found a formula for the discriminant of all those pure octic fields $\mathbb{Q}(\sqrt[8]{a})$ where a is a squarefree integer. In 2017, we gave a formula for the discriminant of pure number fields having squarefree degree (cf. [JKS17]).

In the present paper, our aim is to give a formula for the discriminant of nth degree fields of the type $\mathbb{Q}(\sqrt[n]{a})$ in terms of prime powers dividing a, n, where for each prime p dividing n either p does not divide a or the highest power of p dividing a (to be denoted by $v_p(a)$) is coprime to p. With this hypothesis, a formula for the discriminant of $\mathbb{Q}(\sqrt[n]{a})$ is given by Gassert [G17] using a method proposed by Montes and developed in [GMN11]–[GMN15],

2020 *Mathematics Subject Classification*: 11R04, 11R29.
Key words and phrases: rings of algebraic integers, discriminant, monogenic number fields.
Received 4 May 2020; revised 19 October 2020.
Published online 24 May 2021.

DOI: 10.4064/cm8257-11-2020

but our proof here is based on the classical theorem of Ore about Newton polygons and is more or less self-contained.

Precisely stated, we prove:

THEOREM 1.1. *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field with discriminant d_K, where θ is a root of an irreducible polynomial $f(x) = x^n - a$ belonging to $\mathbb{Z}[x]$. Let $\prod_{i=1}^{k} p_i^{s_i}, \prod_{j=1}^{l} q_j^{t_j}$ be the prime factorizations of $n, |a|$ respectively. Let m_j, n_i and r_i stand respectively for the integers $\gcd(n, t_j)$, $n/p_i^{s_i}$ and $v_{p_i}(a^{p_i-1} - 1) - 1$. Assume that for each i, either $v_{p_i}(a) = 0$ or $v_{p_i}(a)$ is coprime to p_i. Then*

$$d_K = (-1)^{(n-1)(n-2)/2} \operatorname{sgn}(a^{n-1}) \Big(\prod_{i=1}^{k} p_i^{v_i} \Big) \prod_{j=1}^{l} q_j^{n-m_j},$$

where v_i equals $ns_i - 2n_i \sum_{j=1}^{\min\{r_i, s_i\}} p_i^{s_i - j}$ or ns_i according as $r_i > 0$ or not.

The following corollary is an immediate application of the above theorem.

COROLLARY 1.2. *Let p be a prime number and $a \neq \pm 1$ be a squarefree integer. Let $K = \mathbb{Q}(\theta)$ with θ a root of $x^{p^s} - a$. Set $r = v_p(a^{p-1} - 1) - 1$. Then*

$$d_K = (-1)^{(p^s-1)(p^s-2)/2} p^{\nu} a^{p^s-1},$$

where ν equals $sp^s - 2\sum_{j=1}^{\min\{r,s\}} p^{s-j}$ or sp^s according as $r > 0$ or not.

It can be easily seen that in the special case when $p = 2$ and $s = 3$, the formula obtained in the above corollary for $K = \mathbb{Q}(\theta)$ can be restated in the following form as given in [HN15]:

$$d_K = \begin{cases} -2^{24} a^7 & \text{if } a \equiv 2, 3 \pmod 4, \\ -2^{16} a^7 & \text{if } a \equiv 5, 13 \pmod{16}, \\ -2^{12} a^7 & \text{if } a \equiv 9 \pmod{16}, \\ -2^{10} a^7 & \text{if } a \equiv 1 \pmod{16}. \end{cases}$$

The next corollary, which is partially proved in [G17], will be quickly deduced from Theorem 1.1.

COROLLARY 1.3. *Let $K = \mathbb{Q}(\theta)$ be an extension of $\mathbb{Q}$ with θ satisfying an irreducible polynomial $x^n - a$ over $\mathbb{Z}$. Then $\{1, \theta, \ldots, \theta^{n-1}\}$ is an integral basis of K if and only if a is squarefree and for each prime p dividing n, $p^2 \nmid (a^{p-1} - 1)$.*

2. Preliminary results. If $n = \prod_{i=1}^{k} p_i^{s_i}$, $|a| = \prod_{j=1}^{l} q_j^{t_j}$, $f(x) = x^n - a$, θ, d_K are as in Theorem 1.1, A_K denotes the ring of algebraic integers of K, and $N_{K/\mathbb{Q}}$ stands for the norm map, then by a basic result [N04,

Propositions 2.9, 2.13] we have

$$d_K[A_K : \mathbb{Z}[\theta]]^2 = (-1)^{\binom{n}{2}} N_{K/\mathbb{Q}}(f'(\theta)) = (-1)^{\binom{n}{2}} N_{K/\mathbb{Q}}(n\theta^{n-1})$$
$$= (-1)^{(n-1)(n-2)/2} n^n a^{n-1}.$$

So d_K is determined as soon as the exact power of each p_i, q_j which divides $[A_K : \mathbb{Z}[\theta]]$ is known. We first deal with the primes q_j dividing a because these are easier to handle. For primes p_i dividing n and not dividing a, $v_{p_i}([A_K : \mathbb{Z}[\theta]])$ is obtained essentially in two stages. The first stage deals with the situation when n is a prime power. Then we establish a relation between $v_{p_i}([A_K : \mathbb{Z}[\theta]])$ and $v_{p_i}([A_{K_i} : \mathbb{Z}[\theta_i]])$, where A_{K_i} is the ring of algebraic integers of $K_i = \mathbb{Q}(\theta_i)$, and $\theta_i = \theta^{n_i}$ is a root of the polynomial $x^{p_i^{s_i}} - a$. For calculating the prime powers dividing these indices, we use a particular case of the Theorem of Index of Ore (stated as Theorem 2.B) for which we need the notion of Newton polygon introduced below.

Throughout, $\mathbb{Z}_p$ denotes the ring of p-adic integers and $\mathbb{F}_p$ the field with p elements. For c in $\mathbb{Z}_p$, $v_p(c)$ stands for the p-adic valuation of c defined by $v_p(p) = 1$, and $\bar{c}$ for the image of c under the canonical homomorphism from $\mathbb{Z}_p$ onto $\mathbb{F}_p$.

Definition. Let p be a prime number and $g(x) = \sum_{j=0}^{n} c_j x^j$ be a polynomial over $\mathbb{Z}_p$ with $c_0 c_n \neq 0$. To each non-zero term $c_i x^i$, we associate a point $(n - i, v_p(c_i))$ and form the set

$$P = \{(j, v_p(c_{n-j})) \mid 0 \leq j \leq n,\ c_{n-j} \neq 0\}.$$

The *Newton polygon* of $g(x)$ with respect to p (also called the *p-Newton polygon* of $g(x)$) is the polygonal path formed by the lower edges along the convex hull of points of P. Note that the slopes of the edges are increasing when calculated from left to right.

Definition. Let $g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial over $\mathbb{Z}_p$ such that the p-Newton polygon of $g(x)$ consists of a single edge having positive slope λ, i.e., $\min\{v_p(a_{n-i})/i \mid 1 \leq i \leq n\} = v_p(a_0)/n = \lambda$. Let e denote the smallest positive integer such that $e\lambda \in \mathbb{Z}$. We associate with $g(x)$ a polynomial $T(Y) \in \mathbb{F}_p[Y]$ not divisible by Y of degree $n/e = t$ (say) defined by

$$T(Y) = Y^t + \sum_{j=1}^{t} \frac{\overline{a_{n-ej}}}{p^{ej\lambda}} Y^{t-j}.$$

We shall call $T(Y)$ the *polynomial associated with $g(x)$ with respect to p.*

Example. Let $g(x) = (x + 5)^4 - 5$. One can easily check that the 2-Newton polygon of $g(x)$ consists of only one edge with slope $\lambda = 1/2$. With notations as in the above definition, we see that $e = 2$, $n = 4$, $t = 2$ and

the polynomial associated with $g(x)$ with respect to 2 is $T(Y) = Y^2 + Y + \bar{1}$ belonging to $\mathbb{F}_2[Y]$.

We shall use the following weaker versions of two theorems proved by Ore in a more general setup (cf. [O28], [MN92, pp. 322–325], [KK12, Theorem 1.1]). Their proofs are omitted.

THEOREM 2.A. *Let p be a prime number. Let $g(x) = \sum_{i=0}^{n} a_i x^i$, $a_0 \neq 0$, belonging to $\mathbb{Z}[x]$ be a monic polynomial such that $g(x) \equiv x^n \pmod{p}$. Suppose that the p-Newton polygon of $g(x)$ consists of k edges $S_1, \ldots, S_k$ having positive slopes $\lambda_1 < \cdots < \lambda_k$. Let l_i denote the length of the horizontal projection of S_i, and e_i be the smallest positive integer such that $e_i\lambda_i \in \mathbb{Z}$. Then $g(x) = g_1(x) \cdots g_k(x)$, where $g_i(x)$ is a monic polynomial over $\mathbb{Z}_p$ of degree l_i whose p-Newton polygon has a single edge which is a translate of S_i.*

THEOREM 2.B. *Let p, $g(x)$, S_i, λ_i, e_i, l_i and $g_i(x)$ be as in the above theorem for $1 \leq i \leq k$. Let $T_i(Y)$ denote the polynomial associated with $g_i(x)$ with respect to p. Assume that $g(x)$ is irreducible over $\mathbb{Q}$. Let β be a root of $g(x)$, and $K = \mathbb{Q}(\beta)$. If $T_i(Y)$ is a product of distinct monic irreducible polynomials over $\mathbb{F}_p$ for each i, then the highest power of p dividing the index $[A_K : \mathbb{Z}[\beta]]$ equals the number of points with positive integer coordinates lying on or below the p-Newton polygon of $g(x)$ away from the vertical line passing through the last vertex of this polygon.*

The following basic lemma to be used below is already known (cf. [DKM07, Problem 435]). We omit its proof. As usual, for a real number λ, $\lfloor \lambda \rfloor$ stands for the greatest integer not exceeding λ.

LEMMA 2.C. *Let t, n be positive integers with $\gcd(t, n) = m$. Let P denote the set of points in the plane with positive integer coordinates lying inside or on the triangle with vertices $(0, 0), (n, 0), (n, t)$ but not on the line $x = n$. Then*

$$\#P = \sum_{i=1}^{n-1} \left\lfloor \frac{it}{n} \right\rfloor = \frac{1}{2}[(n-1)(t-1) + m - 1].$$

With notations as in Theorem 1.1, using the above lemma and Theorem 2.B we now prove the following result which determines $v_{q_j}([A_K : \mathbb{Z}[\theta]])$.

LEMMA 2.1. *Let $f(x) = x^n - a, K = \mathbb{Q}(\theta)$, $|a| = \prod_{j=1}^{l} q_j^{t_j}$ and $m_j = \gcd(n, t_j)$ be as in Theorem 1.1. For a fixed prime q_j dividing a, suppose that q_j does not divide m_j. Then $v_{q_j}([A_K : \mathbb{Z}[\theta]]) = \frac{1}{2}[(n-1)(t_j-1)+m_j-1]$.*

Proof. Clearly, the q_j-Newton polygon of $f(x)$ consists of a single edge having slope t_j/n. It can be easily seen that the polynomial associated with $f(x)$ with respect to q_j is $T(Y) = Y^{m_j} - \overline{a/q_j^{t_j}}$ belonging to $\mathbb{F}_{q_j}[Y]$. By

hypothesis $q_j \nmid m_j$. So $T(Y)$ has no repeated roots. The desired equality now follows immediately from Theorem 2.B and Lemma 2.C. ∎

The following simple result is well known. For the reader's convenience, we prove it here.

LEMMA 2.D. *For any positive integer $u \le p^s$ with p a prime and $s > 0$ an integer, one has $v_p\big(\binom{p^s}{u}\big) = s - v_p(u)$.*

Proof. Since for any natural number m, $v_p(m!) = \sum_{j=1}^{\infty} \lfloor m/p^j \rfloor$, we see that

$$v_p\left(\binom{p^s}{u}\right) = v_p(p^s!) - v_p(u!) - v_p((p^s-u)!) = \sum_{j=1}^{s} p^{s-j} - \sum_{j=1}^{s} \left\lfloor \frac{u}{p^j} \right\rfloor - \sum_{j=1}^{s} \left\lfloor p^{s-j} - \frac{u}{p^j} \right\rfloor. \tag{2.1}$$

Keeping in mind that $\lfloor p^{s-j} - u/p^j \rfloor = p^{s-j} - u/p^j$ or $p^{s-j} - \lfloor u/p^j \rfloor - 1$ according as $j \le v_p(u)$ or not, the desired equality follows immediately from (2.1). ∎

Using the above lemma and Theorems 2.A, 2.B, we prove the following result which plays a significant role in the proof of Theorem 1.1.

LEMMA 2.2. *Let $L = \mathbb{Q}(\alpha)$ be an algebraic number field with α a root of an irreducible polynomial $x^{p^s} - a$ belonging to $\mathbb{Z}[x]$, where p is a prime number not dividing a, and s is a positive integer. Let A_L be the ring of algebraic integers of L. Set $r = v_p(a^{p-1} - 1) - 1$. Then the exact power of p dividing the index $[A_L : \mathbb{Z}[\alpha]]$ is $\sum_{i=1}^{\min\{r,s\}} p^{s-i}$ or 0 according as r is positive or not.*

Proof. Since $p \nmid a$, p divides $a^{p-1} - 1$ and hence $r \ge 0$. Set $\xi = \alpha - a$, so that ξ is a root of $g(x) = (x+a)^{p^s} - a$ and $\mathbb{Z}[\xi] = \mathbb{Z}[\alpha]$. Observe that $v_p(a^{p^s-1} - 1) = v_p(a^{p-1} - 1)$, which can be quickly verified keeping in mind that $p^s - 1 = (p-1)m$ with $m \equiv 1 \pmod p$ and $a^{p-1} \equiv 1 \pmod p$. If $r = 0$, then the lemma is trivially true because $g(x)$ is an Eisenstein polynomial with respect to p by the above observation and p does not divide $[A_L : \mathbb{Z}[\xi]]$ in view of [N04, Lemma 2.17]. From now on, it is assumed that $r \ge 1$.

We first prove the lemma when $r > s$. Using Lemma 2.D, it can be easily seen that the successive vertices of the p-Newton polygon of $g(x) = x^{p^s} + \binom{p^s}{1} a x^{p^s-1} + \cdots + \binom{p^s}{p^s-1} a^{p^s-1} x + a^{p^s} - a$ are $(0,0)$, $(p^s - p^{s-1}, 1)$, $(p^s - p^{s-2}, 2), \ldots, (p^s - 1, s)$, $(p^s, r+1)$. In this case the p-Newton polygon of $g(x)$ has $s+1$ edges with slopes $\lambda_i = 1/(p^{s-i+1} - p^{s-i})$ for $1 \le i \le s$ and $\lambda_{s+1} = r + 1 - s$. Applying Theorem 2.A, we see that $g(x) = \prod_{i=1}^{s+1} g_i(x)$, where $g_i(x) \in \mathbb{Z}_p[x]$ is a monic polynomial whose p-Newton polygon has a single edge with slope λ_i and $\deg(g_i(x)) = p^{s-i+1} - p^{s-i}$ for $1 \le i \le s$,

$\deg(g_{s+1}(x)) = 1$. Clearly the polynomial associated with $g_i(x)$ with respect to p is a monic linear polynomial in $\mathbb{F}_p[Y]$. Note that the number of points with positive integral entries which lie on or below the p-Newton polygon of $g(x)$ with ordinate i is p^{s-i} for $1 \leq i \leq s$. So it follows from Theorem 2.B that $v_p([A_L : \mathbb{Z}[\alpha]]) = v_p([A_L : \mathbb{Z}[\xi]]) = \sum_{i=1}^{s} p^{s-i}$.

We proceed to the case when $1 \leq r \leq s$ and p is odd. Using Lemma 2.D, one can quickly verify that the successive vertices of the p-Newton polygon of $g(x)$ are $(0,0)$, $(p^s - p^{s-1}, 1)$, $(p^s - p^{s-2}, 2), \ldots, (p^s - p^{s-r}, r)$, $(p^s, r+1)$. Note that in this case the p-Newton polygon of $g(x)$ has $r+1$ edges with slopes $\lambda_i = 1/(p^{s-i+1} - p^{s-i})$ for $1 \leq i \leq r$ and $\lambda_{r+1} = 1/p^{s-r}$. Applying Theorem 2.A, we see that $g(x)$ can be written as a product $\prod_{i=1}^{r+1} g_i(x)$ of monic polynomials belonging to $\mathbb{Z}_p[x]$, where the p-Newton polygon of $g_i(x)$ has a single edge with slope λ_i, and the polynomial associated with $g_i(x)$ with respect to p is a monic linear polynomial. Arguing as in the previous case, we see that $v_p([A_L : \mathbb{Z}[\xi]]) = \sum_{i=1}^{r} p^{s-i}$, which proves the lemma in this case.

Now we deal with the situation when $1 \leq r \leq s$ and $p = 2$. One can check that the successive vertices of the 2-Newton polygon of $g(x) = x^{2^s} + \binom{2^s}{1} a x^{2^s-1} + \cdots + \binom{2^s}{2^s-1} a^{2^s-1} x + a^{2^s} - a$ are $(0,0)$, $(2^s - 2^{s-1}, 1)$, $(2^s - 2^{s-2}, 2), \ldots, (2^s - 2^{s-r+1}, r-1)$, $(2^s, r+1)$. The 2-Newton polygon of $g(x)$ has r edges with slopes $\lambda_i = 1/(2^{s-i+1} - 2^{s-i})$ for $1 \leq i \leq r-1$ and $\lambda_r = 1/2^{s-r}$. It follows quickly from Theorem 2.A that $g(x) = \prod_{i=1}^{r} g_i(x)$ where $g_i(x)$ belonging to $\mathbb{Z}_2[x]$ is a monic polynomial which corresponds to the ith edge of the 2-Newton polygon of $g(x)$. Further the polynomial associated with $g_i(x)$ with respect to 2 is a monic linear polynomial for $1 \leq i \leq r-1$ and the polynomial associated with $g_r(x)$ with respect to 2 is a second degree polynomial, say $T_r(Y)$, belonging to $\mathbb{F}_2[Y]$. Keeping in mind that the 2-Newton polygon of $g_r(x)$ (being a translate of the last edge of the 2-Newton polygon of $g(x)$) has lattice points $(0,0), (2^{s-r}, 1), (2^{s-r+1}, 2)$ on it, we conclude that $T_r(Y) = Y^2 + Y + \bar{1}$. So Theorem 2.B is applicable to $g(x)$. Since the number of points with positive integral entries which lie on or below the 2-Newton polygon of $g(x)$ with ordinate i is 2^{s-i}, it follows that $v_2([A_L : \mathbb{Z}[\xi]]) = \sum_{i=1}^{r} 2^{s-i}$. This completes the proof of Lemma 2.2. ∎

NOTATION 2.E. If $K = \mathbb{Q}(\alpha)$ with α an algebraic integer, then the index $[A_K : \mathbb{Z}[\alpha]]$ will be denoted by $\mathrm{Ind}(\alpha)$. For a relative extension L/K of algebraic number fields, $d_{L/K}$ will stand for the relative discriminant. We shall use the following formula (see [N04, Theorem 4.15]):

$$d_L = \pm d_K^{[L:K]} N_{K/\mathbb{Q}}(d_{L/K}). \tag{2.2}$$

If $\{\alpha_1, \ldots, \alpha_n\}$ is a vector space basis of L/K, then $D_{L/K}(\alpha_1, \ldots, \alpha_n)$ will denote the determinant of the $n \times n$ matrix with (i,j)th entry $\mathrm{Tr}_{L/K}(\alpha_i \alpha_j)$,

where Tr stands for the trace map. If $L = K(\alpha)$, $\alpha \in A_L$ with $g(x)$ as the minimal polynomial of α over K, then as in [N04, Proposition 2.9], it can be easily seen that

$$D_{L/K}(1, \alpha, \ldots, \alpha^{n-1}) = (-1)^{n(n-1)/2} N_{L/K}(g'(\alpha)). \tag{2.3}$$

With the above notation, we prove the following lemma which extends Lemma 2.2 to general n.

LEMMA 2.3. *Let $K = \mathbb{Q}(\theta)$ where θ is a root of an irreducible polynomial $x^n - a$ belonging to $\mathbb{Z}[x]$. Let $\prod_{i=1}^{k} p_i^{s_i}$ be the prime factorization of n. Suppose $p_i \nmid a$ for some i. If r_i, n_i denote the integers $v_{p_i}(a^{p_i-1} - 1) - 1, n/p_i^{s_i}$ respectively, then the exact power of p_i dividing $\operatorname{Ind}(\theta)$ is $\sum_{j=1}^{\min\{r_i,s_i\}} n_i p_i^{s_i-j}$ or 0 according as r_i is positive or not.*

Proof. Set $\theta_i = \theta^{n_i}$ and $K_i = \mathbb{Q}(\theta_i)$. Note that $[K : K_i] = n_i$. By (2.2), we have

$$d_K = \pm d_{K_i}^{n_i} N_{K_i/\mathbb{Q}}(d_{K/K_i}). \tag{2.4}$$

A claim is that p_i does not divide $N_{K_i/\mathbb{Q}}(d_{K/K_i})$. Note that the minimal polynomial of θ over K_i is $g(x) = x^{n_i} - \theta_i$. By [N04, Theorem 4.16], d_{K/K_i} divides the ideal $N_{K/K_i}(g'(\theta))A_{K_i}$. So $N_{K_i/\mathbb{Q}}(d_{K/K_i})$ divides $N_{K/\mathbb{Q}}(g'(\theta)) = \pm n_i^n a^{n_i-1}$, which proves the claim in view of the fact that $p_i \nmid n_i a$. It is immediate from (2.4) and the claim that

$$v_{p_i}(d_K) = n_i v_{p_i}(d_{K_i}). \tag{2.5}$$

Using (2.3), we see that

$$D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{n-1}) = \pm n^n a^{n-1}, \quad D_{K_i/\mathbb{Q}}(1, \theta_i, \ldots, \theta_i^{p_i^{s_i}-1}) = \pm p_i^{s_i p_i^{s_i}} a^{p_i^{s_i}-1}. \tag{2.6}$$

Recall that $n = n_i p_i^{s_i}$ and $p_i \nmid a n_i$. So it is clear from (2.6) that

$$v_{p_i}(D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{n-1})) = n_i v_{p_i}(D_{K_i/\mathbb{Q}}(1, \theta_i, \ldots, \theta_i^{p_i^{s_i}-1})). \tag{2.7}$$

Also by [N04, Proposition 2.13], $D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{n-1}) = d_K \operatorname{Ind}(\theta)^2$; consequently,

$$v_{p_i}(D_{K/\mathbb{Q}}(1, \theta, \ldots, \theta^{n-1})) = v_{p_i}(d_K) + 2v_{p_i}(\operatorname{Ind}(\theta)). \tag{2.8}$$

Substituting (2.5) and (2.7) in (2.8), we get

$$n_i v_{p_i}(D_{K_i/\mathbb{Q}}(1, \theta_i, \ldots, \theta_i^{p_i^{s_i}-1})) = n_i v_{p_i}(d_{K_i}) + 2v_{p_i}(\operatorname{Ind}(\theta)). \tag{2.9}$$

Keeping in mind that $D_{K_i/\mathbb{Q}}(1, \theta_i, \ldots, \theta_i^{p_i^{s_i}-1}) = d_{K_i} \operatorname{Ind}(\theta_i)^2$, we conclude from (2.9) that $v_{p_i}(\operatorname{Ind}(\theta)) = n_i v_{p_i}(\operatorname{Ind}(\theta_i))$. So the desired equality now follows from Lemma 2.2. ∎

3. Proofs of Theorem 1.1 and Corollary 1.3

Proof of Theorem 1.1. Recall that

$$D_{K/\mathbb{Q}}(1,\theta,\dots,\theta^{n-1}) = \mathrm{Ind}(\theta)^2 d_K = (-1)^{\binom{n}{2}} N_{K/\mathbb{Q}}(n\theta^{n-1}) = (-1)^{(n-1)(n-2)/2} n^n a^{n-1}. \tag{3.1}$$

So any prime dividing $\mathrm{Ind}(\theta)$ must divide an. It follows from Lemmas 2.1 and 2.3 that

$$\mathrm{Ind}(\theta) = \prod_{i=1}^{k} p_i^{u_i} \prod_{j=1}^{l} q_j^{[(n-1)(t_j-1)+m_j-1]/2},$$

where u_i equals $n_i \sum_{j=1}^{\min\{r_i,s_i\}} p_i^{s_i-j}$ or 0 according as $r_i > 0$ or not. Substituting for $\mathrm{Ind}(\theta)$ from the above equation and $n = \prod_{i=1}^{k} p_i^{s_i}$, $|a| = \prod_{j=1}^{l} q_j^{t_j}$ in (3.1), we immediately obtain the desired formula for d_K. ∎

Proof of Corollary 1.3. Assume first that $A_K = \mathbb{Z}[\theta]$. Suppose to the contrary that a is not a squarefree integer, say $a = bc^2$ with $c \geq 2$. The equality $\theta^n = a = bc^2$ shows that θ^n divides $(bc)^n$ in A_K and hence θ divides bc, which implies that $\theta^{n-1}/c = bc/\theta$ is an algebraic integer. Consequently, c will divide the index $[A_K : \mathbb{Z}[\theta]]$. This contradiction proves that a is squarefree.

When a is squarefree, writing the prime factorization of n as $\prod_{i=1}^{k} p_i^{s_i}$ and taking r_i, v_i as in Theorem 1.1, we see that the discriminant d_K of K is

$$d_K = (-1)^{(n-1)(n-2)/2} \operatorname{sgn}(a^{n-1}) \Big(\prod_{i=1}^{k} p_i^{v_i} \Big) |a|^{n-1}.$$

As shown in (3.1),

$$D_{K/\mathbb{Q}}(1,\theta,\theta^2,\dots,\theta^{n-1}) = \mathrm{Ind}(\theta)^2 d_K = (-1)^{(n-1)(n-2)/2} n^n a^{n-1}.$$

In view of the above two equations, $\{1,\theta,\theta^2,\dots,\theta^{n-1}\}$ is an integral basis of K if and only if $n^n = \prod_{i=1}^{k} p_i^{v_i}$, i.e., if and only if $\prod_{i=1}^{k} p_i^{ns_i} = \prod_{i=1}^{k} p_i^{v_i}$. Keeping in mind the definition of v_i, the last equality holds if and only if for $1 \leq i \leq k$, we have $r_i \leq 0$, i.e., $p_i^2 \nmid (a^{p_i-1} - 1)$. ∎

Acknowledgements. The financial support from the respective institutions is gratefully acknowledged by the authors. The second author is also thankful to Indian National Science Academy, New Delhi, for financial assistance through INSA Senior Scientistship.

REFERENCES

[B27] W. E. H. Berwick, *Integral Bases*, Cambridge Univ. Press, London, 1927.

[D00] R. Dedekind, *Ueber die Anzahl der Idealklassen in reinen kubischen Zahlkörpern*, J. Reine Angew. Math. 121 (1900), 40–123.

[DKM07] J.-M. De Koninck and A. Mercier, *1001 Problems in Classical Number Theory*, Amer. Math. Soc., Providence, RI, 2007.

[F84] T. Funakura, *On integral bases of pure quartic fields*, Math. J. Okayama Univ. 26 (1984), 27–41.

[G17] T. A. Gassert, *A note on the monogeneity of power maps*, Albanian J. Math. 11 (2017), 3–12.

[GMN11] J. Guàrdia, J. Montes and E. Nart, *Higher Newton polygons in the computation of discriminants and prime ideal decomposition in number fields*, J. Théor. Nombres Bordeaux 23 (2011), 667–696.

[GMN12] J. Guàrdia, J. Montes and E. Nart, *Newton polygons of higher order in algebraic number theory*, Trans. Amer. Math. Soc. 364 (2012), 361–416.

[GMN13] J. Guàrdia, J. Montes and E. Nart, *A new computational approach to ideal theory in number fields*, Found. Comput. Math. 13 (2013), 729–762.

[GMN15] J. Guàrdia, J. Montes and E. Nart, *Higher Newton polygons and integral bases*, J. Number Theory 147 (2015), 549–589.

[HN15] A. Hameed and T. Nakahara, *Integral bases and relative monogenity of pure octic fields*, Bull. Math. Soc. Sci. Math. Roumanie 58 (106) (2015), 419–433.

[JKS17] A. Jakhar, S. K. Khanduja and N. Sangwan, *Discriminants of pure square-free degree number fields*, Acta Arith. 181 (2017), 287–296.

[KK12] S. K. Khanduja and S. Kumar, *On prolongations of valuations via Newton polygons and liftings of polynomials*, J. Pure Appl. Algebra 216 (2012), 2648–2656.

[L97] G. Landsberg, *Ueber das Fundamentalsystem und die Discriminante der Gattungen algebraischer Zahlen, welche aus Wurzelgrössen gebildet sind*, J. Reine Angew. Math. 117 (1897), 140–147.

[MN92] J. Montes and E. Nart, *On a theorem of Ore*, J. Algebra 146 (1992), 318–334.

[N04] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd ed., Springer, Berlin, 2004.

[O82] K. Okutsu, *Integral basis of the field* $\mathbb{Q}(\sqrt[n]{a})$, Proc. Japan Acad. Ser. A Math. Sci. 58 (1982), 219–222.

[O28] Ö. Ore, *Newtonsche Polygone in der Theorie der algebraischen Körper*, Math. Ann. 99 (1928), 84–117.

[W10] J. Westlund, *On the fundamental number of the algebraic number-field* $k(\sqrt[p]{m})$, Trans. Amer. Math. Soc. 11 (1910), 388–392.

Anuj Jakhar
Department of Mathematics
Indian Institute of Technology Bhilai
Raipur, 492015, India
E-mail: anujjakhar@iitbhilai.ac.in

Neeraj Sangwan
Department of Mathematics
Indian Institute of Technology (IIT) Bombay
Mumbai 400076, India
E-mail: neerajsan@math.iitb.ac.in

Sudesh K. Khanduja
Indian Institute of
Science Education and Research Mohali
Sector 81, Knowledge City
SAS Nagar, Punjab 140306, India
and
Department of Mathematics
Panjab University
Chandigarh 160014, India
E-mail: skhanduja@iisermohali.ac.in