ACTA ARITHMETICA
181.3 (2017)

Discriminants of pure square-free degree number fields

by

Anuj Jakhar, Sudesh K. Khanduja and
Neeraj Sangwan (Mohali)

1. Introduction. The problem of computation of discriminants of algebraic number fields, especially of pure number fields, has been of interest to several mathematicians ([1], [3], [5], [6], [8], [11]). In 1897, Landsberg [8] was the first to give a formula for the discriminant of fields of the form $\mathbb{Q}(a^{1/p})$ having prime degree p over the field $\mathbb{Q}$ of rational numbers. In 1927, Berwick [1] described a (local) $\mathbb{Z}_{(p)}$-basis for the integral closure of the localization $\mathbb{Z}_{(p)}$ of $\mathbb{Z}$ at each prime p in number fields of the type $\mathbb{Q}(a^{1/n})$ having square-free degree n over the rationals. However, it seems too complicated to deduce a formula for the discriminant of $\mathbb{Q}(a^{1/n})$ from these local bases which are split into several cases.

In this paper, our aim is to give an explicit formula for the discriminants of such fields, involving only the primes dividing n and prime powers dividing a.

In what follows, $K = \mathbb{Q}(\theta)$ with θ a root of an irreducible polynomial $x^n - a$ belonging to $\mathbb{Z}[x]$ of square-free degree $n = \prod_{i=1}^{k} p_i$, where p_i's are primes and a is an *nth-power-free integer*, i.e., a is not divisible by the nth power of a prime number. For $1 \le i \le k$, n_i will stand for n/p_i, and d_i for the p_ith-power-free integer such that a/d_i is the p_ith power of a natural number. Corresponding to the prime p_i, we shall denote by r_i the integer $n - 2n_i$ or n according as p_i^2 divides $a^{p_i-1} - 1$ or not. For a prime number p and a non-zero integer b, $v_p(b)$ will denote the highest power of p dividing b. Whenever some p_i divides both a and $v_{p_i}(a)$, we shall denote $v_{p_i}(a)/p_i$ by c_i; in this situation u_i will stand for $(p_i - 1)\gcd(n_i, c_i) - \gcd(n_i, c_i(p_i - 1))$ or $n_i + (p_i - 1)\gcd(n_i, c_i)$ according as $d_i^{p_i-1} \equiv 1 \pmod{p_i^2}$ or not.

2010 *Mathematics Subject Classification*: 11R04, 11R29.
Key words and phrases: rings of algebraic integers, discriminant.
Received 8 May 2017; revised 16 September 2017.
Published online 30 November 2017.

DOI: 10.4064/aa170508-4-11

With the above notation, we prove:

THEOREM 1.1. *Let $K = \mathbb{Q}(\theta)$ be an algebraic number field where θ is a root of an irreducible polynomial $f(x) = x^n - a$ belonging to $\mathbb{Z}[x]$ of square-free degree n, and a is an nth-power-free integer. Let $n = \prod_{i=1}^{k} p_i$ and $|a| = \prod_{j=1}^{l} q_j^{t_j}$ be the prime factorizations of n and $|a|$, and let n_i, d_i, r_i, c_i, u_i be as above. Then the discriminant d_K of K is given by*

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

where v_i is r_i when $p_i \nmid a$, and in case $p_i \mid a$, v_i equals u_i or n according as $p_i \mid v_{p_i}(a)$ or not.

If $f(x), \theta, d_K$ are as above, A_K is the ring of algebraic integers of K, and $N_{K/\mathbb{Q}}$ denotes the norm map from K into $\mathbb{Q}$, then it is well known [10, Propositions 2.9, 2.13] that

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

Since $N_{K/\mathbb{Q}}(f'(\theta)) = N_{K/\mathbb{Q}}(n\theta^{n-1}) = n^n(-a)^{n-1}$, d_K is determined as soon as the exact power of each of the primes p_i, q_j which divides d_K or $[A_K : \mathbb{Z}[\theta]]$ is known. Besides algebraic number theory and basic valuation theory, in certain cases we also use a special case of the Theorem of Index of Ore (stated as Theorem 2.A below) to find these powers.

The following corollaries can be quickly deduced from the above theorem.

COROLLARY 1.2. *Let $a \neq \pm 1$ be a square-free integer and let $n = \prod_{i=1}^{k} p_i$ and r_i be as in Theorem* 1.1. *Let $K = \mathbb{Q}(\theta)$ with θ a root of $x^n - a$. Then the discriminant d_K of K is $(-1)^{(n-1)(n-2)/2} p_1^{v_1} \cdots p_k^{v_k} a^{n-1}$, where v_i is either n or r_i according as p_i divides a or not.*

COROLLARY 1.3. *Let $n = \prod_{i=1}^{k} p_i$ and $a = \pm \prod_{j=1}^{l} q_j^{t_j}$ be as in Theorem* 1.1. *Suppose that a is coprime to n, and the polynomial $x^n - a$ is irreducible over $\mathbb{Q}$ and has a root θ. Then the absolute value of the discriminant of $\mathbb{Q}(\theta)$ is $p_1^{r_1} \cdots p_k^{r_k} D$, where r_i's are as in Theorem* 1.1 *and $D = \prod_{j=1}^{l} q_j^{n-\gcd(n,t_j)}$.*

COROLLARY 1.4. *Let p_1 and p_2 be distinct prime numbers and a be a (p_1p_2)th-power-free integer such that $f(x) = x^{p_1p_2} - a$ is irreducible over $\mathbb{Q}$ and has a root θ. Let $\prod_{j=1}^{l} q_j^{t_j}$ be the factorization of $|a|$ into powers of distinct primes with $t_j > 0$. For $i = 1, 2$, let d_i and n_i be as in Theorem* 1.1 *and r_i denote the integer $p_1p_2 - 2n_i$ or p_1p_2 according as p_i^2 divides $a^{p_i-1} - 1$ or not. Let u_i stand for $p_i + n_i - 1$ when $d_i^{p_i-1} \not\equiv 1 \pmod{p_i^2}$, and in case*

$d_i^{p_i-1} \equiv 1 \pmod{p_i^2}$, *let* u_i *stand for* $p_i - n_i - 1$ *or* $p_i - 2$ *according as* n_i *divides* $p_i - 1$ *or not. Then the discriminant* d_K *of* $K = \mathbb{Q}(\theta)$ *is given by*

$$d_K = (-1)^{(p_1p_2-1)(p_1p_2-2)/2} \operatorname{sgn}(a^{p_1p_2-1}) \Big(\prod_{i=1}^{2} p_i^{v_i} \Big) \prod_{j=1}^{l} q_j^{p_1p_2-\gcd(p_1p_2,t_j)},$$

where v_i *is* r_i *when* $p_i \nmid a$, *and in case* $p_i \mid a$, v_i *equals* u_i *or* p_1p_2 *according as* $p_i \mid v_{p_i}(a)$ *or not.*

2. Preliminary results. Throughout, A_K denotes the ring of algebraic integers of an algebraic number field K, and d_K its discriminant. For a non-zero prime ideal $\wp$ of A_K, $v_\wp$ will stand for the $\wp$-adic valuation of K defined to be the highest power of $\wp$ dividing the ideal αA_K for any non-zero $\alpha \in A_K$. We shall denote by $\mathbb{F}_\wp$ the residue field of $v_\wp$. The canonical homomorphism from the valuation ring of $v_\wp$ onto its residue field $\mathbb{F}_\wp$ will be denoted by $\xi \mapsto \bar{\xi}$.

Definition. Let K and $\wp$ be as above. Let $g(x) = \sum_{j=0}^{n} a_j x^j$ be a polynomial over K with $a_0 a_n \neq 0$. To each non-zero term $a_i x^i$, we associate the point $(n - i, v_\wp(a_i))$ and form the set

$$S = \{(j, v_\wp(a_{n-j})) \mid 0 \leq j \leq n,\ a_{n-j} \neq 0\}.$$

As in [12, Chapter 5], the *Newton polygon* of $g(x)$ *with respect to* $v_\wp$ (also called the $\wp$*-Newton polygon* of $g(x)$) is the polygonal path formed by the lower edges along the convex hull of the points of S. The slopes of the edges are increasing when calculated from left to right.

Definition. Let $v_\wp$ be as above and let π be a fixed prime element of the valuation ring of $v_\wp$. Let $g(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with coefficients from the valuation ring of $v_\wp$ such that the $\wp$-Newton polygon of $g(x)$ consists of a single side with positive slope $\lambda = l/e$, where $\gcd(l, e) = 1$, so that n is divisible by e, say $n = et$, and $v_\wp(a_{n-i}) \geq i\lambda$, $1 \leq i \leq n - 1$. Corresponding to this Newton polygon, we associate with $g(x)$ a polynomial $T(Y) \in \mathbb{F}_\wp[Y]$ not divisible by Y defined by

$$T(Y) = Y^t + \sum_{j=1}^{t} \left(\frac{\overline{a_{n-ej}}}{\pi^{lj}} \right) Y^{t-j}.$$

Example. Let $g(x) = x^6 - 18$. One can easily check that the Newton polygon of $g(x)$ with respect to the 3-adic valuation of $\mathbb{Q}$ consists of only one edge with slope $\lambda = 1/3$, and the polynomial associated to $g(x)$ is $T(Y) = Y^2 - \bar{2} \in \mathbb{F}_3[Y]$.

Definition 2.1. Let $L = K(\beta)$ be an extension of an algebraic number field K of degree n with β an algebraic integer having minimal polynomial

$g(x)$ over K. Let $\wp$ be a non-zero prime ideal of A_K, and S be the integral closure in L of the valuation ring $R_\wp$ of $v_\wp$. Then S is a free $R_\wp$-module. We define the *$\wp$-index* of $g(x)$, denoted by $i_\wp(g)$, to be the $v_\wp$-valuation of the determinant of the transition matrix from an $R_\wp$-basis of S to $\{1, \beta, \ldots, \beta^{n-1}\}$.

REMARK 2.2. It can be easily seen that if $L = \mathbb{Q}(\beta)$ is an algebraic number field of degree n having an integral basis $\mathcal{B}$, and $\mathbb{Z}_{(p)}$ is the localization of $\mathbb{Z}$ at a non-zero prime ideal $p\mathbb{Z}$, then $\mathcal{B}$ is also a $\mathbb{Z}_{(p)}$-basis of the integral closure of $\mathbb{Z}_{(p)}$ in L; consequently, if $g(x)$ is the minimal polynomial of $\beta \in A_L$ over $\mathbb{Q}$, then $i_{p\mathbb{Z}}(g) = v_p([A_L : \mathbb{Z}[\beta]])$, because the absolute value of the determinant of the transition matrix from $\mathcal{B}$ to $\{1, \beta, \ldots, \beta^{n-1}\}$ equals $[A_L : \mathbb{Z}[\beta]]$ in view of a well known result which states that if N is a subgroup of a finitely generated free abelian group M having the same rank as M, then $[M : N]$ equals the absolute value of the determinant of the transition matrix from a basis of M to a basis of N [2, Chapter 2, §2, Theorem 2].

The result stated below is a weaker version of the Theorem of Index of Ore ([7, Theorem 1.4], [9, p. 325]). Its proof is omitted.

THEOREM 2.A. *Let $L = K(\beta)$, $g(x)$ and $\wp$ be as in Definition* 2.1. *Suppose that the $\wp$-Newton polygon of $g(x)$ consists of a single side with positive slope λ, and the polynomial $T(Y) \in \mathbb{F}_\wp[Y]$ associated with $g(x)$ corresponding to this Newton polygon has no repeated roots. Then $i_\wp(g)$ equals the number of points with integral coordinates lying on or below the $\wp$-Newton polygon of $g(x)$ away from the axes as well as from the vertical line passing through the last vertex of this polygon.*

The following simple lemma is already known [4, Problem 435]. We omit its proof. As usual, for a real number λ, $[\lambda]$ stands for the largest integer not exceeding λ.

LEMMA 2.B. *Let t and n be positive integers with $\gcd(t, n) = m$. Let S_1 denote the set of points in the plane with positive integer entries lying inside or on the triangle with vertices $(0, 0), (n, 0), (n, t)$ which do not lie on the line $x = n$. Then*

$$\#S_1 = \sum_{i=1}^{n-1} \left[\frac{it}{n}\right] = \frac{1}{2}[(n-1)(t-1) + m - 1].$$

Using the above two results, we prove

LEMMA 2.3. *Let $K = \mathbb{Q}(\theta)$ with θ a root of an irreducible polynomial $x^n - a$ belonging to $\mathbb{Z}[x]$ and let $\prod_{j=1}^{l} q_j^{t_j}$ be the prime factorization of $|a|$. For a fixed j, suppose that either $q_j \nmid n$ or $v_{q_j}(a)$ is coprime to q_j. Then $v_{q_j}([A_K : \mathbb{Z}[\theta]]) = \frac{1}{2}[(n-1)(t_j - 1) + \gcd(n, t_j) - 1]$.*

Proof. Set $m_j = \gcd(n, t_j)$. It is clear that the q_j-Newton polygon of $g(x) = x^n - a$ consists of only one side having slope t_j/n. The polynomial associated with $g(x)$ corresponding to this Newton polygon is $T(Y) = Y^{m_j} - \overline{a/q_j^{t_j}} \in \mathbb{F}_{q_j}[Y]$. Keeping in mind the hypothesis that either $q_j \nmid n$ or $v_{q_j}(a) = t_j$ is coprime to q_j, we see that $q_j \nmid m_j$. Hence $T(Y)$ has no repeated roots. On applying Theorem 2.A and Lemma 2.B, we see that $i_{q_j\mathbb{Z}}(g) = \frac{1}{2}[(n-1)(t_j-1) + m_j - 1]$. The desired equality now follows as $i_{q_j\mathbb{Z}}(g) = v_{q_j}([A_K : \mathbb{Z}[\theta]])$ in view of Remark 2.2. ∎

The following lemma is proved in [13]; for the reader's convenience, we recall the proof.

LEMMA 2.4. *Let $L = \mathbb{Q}(\xi)$ be an algebraic number field with ξ a root of an irreducible polynomial $F(x) = x^p - a \in \mathbb{Z}[x]$, where p is a prime not dividing a. Then:*

(i) *If $p^2 \nmid a^{p-1} - 1$, then $v_p(d_L) = p$ and $pA_L = \wp^p$, $\wp$ being a prime ideal of A_L.*

(ii) *If $p^2 \mid a^{p-1} - 1$, then $v_p(d_L) = p - 2$; further in this case, if p is odd or $p = 2$ with $a \equiv 1 \pmod 8$, then $pA_L = \wp_1\wp_2^{p-1}$, where $\wp_1$ and $\wp_2$ are distinct prime ideals of A_L.*

Proof. Set $\alpha = \xi - a$, so that α is a root of $F(x+a) = (x+a)^p - a$ and $\mathbb{Z}[\alpha] = \mathbb{Z}[\xi]$. If $p^2 \nmid a^{p-1} - 1$, then $F(x+a)$ is an Eisenstein polynomial in x with respect to p. So $p \nmid [A_L : \mathbb{Z}[\alpha]]$ and $pA_L = \wp^p$ for some prime ideal $\wp$ of A_L in view of [10, Lemma 2.17, Proposition 4.38]. Further applying formula (1) to $F(x) = x^p - a$ having ξ as a root and keeping in mind that $v_p(a) = v_p([A_L : \mathbb{Z}[\xi]]) = 0$, we see that $v_p(d_L) = p$.

Now we assume $p^2 \mid a^{p-1} - 1$. In this case, we need to prove (ii) when p is an odd prime, as the result is well known when $p = 2$ [10, Theorem 4.39]. We first show that a is a pth power in the ring $\mathbb{Z}_p$ of p-adic integers. By hypothesis $a^{p-1} = 1 + bp^2$ for some $b \in \mathbb{Z}$. Keeping in mind that $p > 2$, it can be easily seen that $1 + bp^2 \equiv (1+bp)^p \pmod{p^3}$. So $\frac{a^p}{a(1+bp)^p} \equiv 1 \pmod{p^3}$. Applying Hensel's lemma [2, Chapter 1, Section 5, Theorem 3], we see that $\frac{a^p}{a(1+bp)^p}$ is a pth power in $\mathbb{Z}_p$, and hence so is a, say $a = c^p$, $c \in \mathbb{Z}_p$.

Then $F(x+c) = (x+c)^p - c^p = xg(x)$, where $g(x) = x^{p-1} + c\binom{p}{1}x^{p-2} + c^2\binom{p}{2}x^{p-3} + \cdots + c^{p-1}\binom{p}{p-1}$. Clearly $g(x)$ is an Eisenstein polynomial with respect to p. Therefore for any root η of $g(x)$, $\mathbb{Q}_p(\eta)$ is a totally ramified extension of the field $\mathbb{Q}_p$ of p-adic numbers having degree $p-1$ [10, Theorem 5.27]. Consequently, the factorization $F(x) = (x-c)g(x-c)$ over $\mathbb{Z}_p$ shows that $pA_L = \wp_1\wp_2^{p-1}$ in view of [10, Proposition 6.1], where $\wp_1$ and $\wp_2$ are distinct prime ideals of A_K with $N_{L/\mathbb{Q}}(\wp_i) = p$. Now [10, Theorem 4.24] yields $v_p(d_L) = p - 2$. ∎

NOTATION AND BASIC FORMULAS. For a non-zero ideal I of A_K, we let $N_{K/\mathbb{Q}}(I) = [A_K : I]$ denote the (absolute) norm of I. 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 [10, Proposition 4.15]:

$$d_L = \pm d_K^{[L:K]} N_{K/\mathbb{Q}}(d_{L/K}). \tag{2}$$

Further, if $L = K(\beta)$ and $g(x)$ is the minimal polynomial of the algebraic integer β over K, and if $\wp$ is a non-zero prime ideal of A_K and $i_\wp(g)$ is as in Definition 2.1, then as is well known,

$$v_\wp(\mathrm{discr}(g)) = v_\wp(d_{L/K}) + 2i_\wp(g). \tag{3}$$

With the above notation, we prove

LEMMA 2.5. *Let $K = \mathbb{Q}(\theta)$ where θ is a root of an irreducible polynomial $x^n - a$ belonging to $\mathbb{Z}[x]$, and let $\prod_{i=1}^k p_i^{s_i}$ be the prime factorization of n. Let n_i denote the integer $n/p_i^{s_i}$ and K_i the field $\mathbb{Q}(\theta_i)$ with $\theta_i = \theta^{n_i}$. Suppose that $p_i \nmid a$ for some i. Then $v_{p_i}(d_K) = n_i v_{p_i}(d_{K_i})$.*

Proof. Since $[K : K_i] = n_i$, using (2) we have $d_K = \pm d_{K_i}^{n_i} N_{K_i/\mathbb{Q}}(d_{K/K_i})$. So the lemma is proved once we show that $p_i \nmid N_{K_i/\mathbb{Q}}(d_{K/K_i})$. Note that the minimal polynomial of θ over K_i is $g(x) = x^{n_i} - \theta_i$. By a basic result [10, 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 desired assertion in view of the fact that $p_i \nmid n_i a$. ∎

With n_i as in Theorem 1.1, the following corollary can be quickly deduced from the above lemma and Lemma 2.4 applied to the field $L = \mathbb{Q}(\theta^{n_i})$ of degree p_i over $\mathbb{Q}$.

COROLLARY 2.6. *Let $f(x) = x^n - a$, $K = \mathbb{Q}(\theta)$ and r_i be as in Theorem* 1.1. *Suppose that $p_i \nmid a$ for some i. Then $v_{p_i}(d_K) = r_i$.*

We now prove

LEMMA 2.7. *Let $K = \mathbb{Q}(\theta)$, a, p_i, d_i, c_i and u_i be as in Theorem* 1.1. *Suppose that p_i divides both a and $v_{p_i}(a)$ for some fixed i. Then $v_{p_i}(d_K) = u_i + n - p_i \gcd(n_i, c_i)$.*

Proof. In view of the hypothesis, we can write a as $p_i^{p_i c_i} b_i^{p_i} d_i$, where the integers b_i and d_i are not divisible by p_i. As a is nth-power-free, we have $1 \le c_i \le n_i - 1$. Since $(\theta^{n_i})^{p_i} = a = p_i^{p_i c_i} b_i^{p_i} d_i$, there exists a root α_i of $x^{p_i} - d_i$ such that $\theta^{n_i} = p_i^{c_i} b_i \alpha_i$. Set $K_0 = \mathbb{Q}(\alpha_i)$. Note that the minimal polynomial of θ over K_0 is $g(x) = x^{n_i} - p_i^{c_i} b_i \alpha_i$. Hence

$$N_{K/K_0}(g'(\theta)) = \pm n_i^{n_i} (p_i^{c_i} b_i \alpha_i)^{n_i - 1}. \tag{4}$$

The proof is split into three cases.

CASE 1: $d_i^{p_i-1} \not\equiv 1 \pmod{p_i^2}$. Applying Lemma 2.4(i), we see that $p_i A_{K_0} = \wp_i^{p_i}$ with $N_{K_0/\mathbb{Q}}(\wp_i) = p_i$, where $\wp_i$ is a prime ideal of A_{K_0}. One can easily check that the $\wp_i$-Newton polygon of $g(x)$ consists of one side having slope $c_i p_i/n_i$. Since n_i is coprime to p_i, we see that $\gcd(c_i p_i, n_i) = k_i$ (say) is not divisible by p_i. So the polynomial associated to $g(x)$ is $T(Y) = Y^{k_i} - \bar{\beta}_i \in \mathbb{F}_{\wp_i}[Y] = \mathbb{F}_{p_i}[Y]$ and has no repeated roots, where $\beta_i = b_i \alpha_i p_i^{c_i}/\pi_i^{p_i c_i}$, π_i being a prime element of the valuation ring of $v_{\wp_i}$. By Theorem 2.A, $i_{\wp_i}(g)$ equals the number of points with positive integral entries which lie on or below the $\wp_i$-Newton polygon of $g(x)$. This number equals $\frac{1}{2}[(n_i-1)(c_i p_i - 1) + \gcd(n_i, c_i p_i) - 1]$ by Lemma 2.B. Consequently, using (3), (4) and the fact that $p_i A_{K_0} = \wp_i^{p_i}$, we see that

$$\begin{aligned} v_{\wp_i}(d_{K/K_0}) &= v_{\wp_i}\big(N_{K/K_0}(g'(\theta))\big) - 2i_{\wp_i}(g) \\ &= c_i p_i(n_i-1) - (c_i p_i - 1)(n_i - 1) - \gcd(n_i, c_i p_i) + 1 \\ &= n_i - \gcd(n_i, c_i p_i) = n_i - \gcd(n_i, c_i). \end{aligned}$$

As $\wp_i$ is the only prime ideal of K_0 lying over p_i and $N_{K_0/\mathbb{Q}}(\wp_i) = p_i$, we conclude from the last displayed equation that $v_{p_i}(N_{K_0/\mathbb{Q}}(d_{K/K_0})) = n_i - \gcd(n_i, c_i)$. By Lemma 2.4(i), $v_{p_i}(d_{K_0}) = p_i$. Therefore applying (2), we have

$$\begin{aligned} v_{p_i}(d_K) &= n_i v_{p_i}(d_{K_0}) + v_{p_i}(N_{K_0/\mathbb{Q}}(d_{K/K_0})) = n_i p_i + n_i - \gcd(n_i, c_i) \\ &= n + n_i - \gcd(n_i, c_i). \end{aligned}$$

CASE 2: Either p_i is odd with $d_i^{p_i-1} \equiv 1 \pmod{p_i^2}$ or $p_i = 2$ with $d_i \equiv 1 \pmod 8$. Applying Lemma 2.4(ii), we see that $p_i A_{K_0} = \wp_i^{p_i-1}\wp_i'$ with $N_{K_0/\mathbb{Q}}(\wp_i) = p_i = N_{K_0/\mathbb{Q}}(\wp_i')$, where $\wp_i$ and $\wp_i'$ are distinct prime ideals of A_{K_0}. In this case the $\wp_i$-Newton polygon of $g(x)$ contains exactly one side with slope $(p_i-1)c_i/n_i$. Note that the polynomial $T(Y) \in \mathbb{F}_{\wp_i}[Y] = \mathbb{F}_{p_i}[Y]$ associated to $g(x)$ (with respect to this Newton polygon) has degree $\gcd(n_i, c_i(p_i-1)) = k_i'$ (say), which is not divisible by the prime p_i. So $T(Y) = Y^{k_i'} - \bar{\gamma}_i$ has no repeated roots, where $\gamma_i = b_i \alpha_i p_i^{c_i}/\pi_i^{(p_i-1)c_i}$, π_i being a prime element of the valuation ring of $v_{\wp_i}$. Applying Theorem 2.A and Lemma 2.B, we have

$$i_{\wp_i}(g) = \tfrac{1}{2}[(n_i-1)(c_i(p_i-1)-1) + \gcd(n_i, c_i(p_i-1)) - 1]; \tag{5}$$

consequently, using (3)–(5) together with the fact that $v_{\wp_i}(p_i A_{K_0}) = p_i - 1$, a simple calculation shows that

$$v_{\wp_i}(d_{K/K_0}) = n_i - \gcd(n_i, c_i(p_i-1)). \tag{6}$$

To calculate $v_{\wp_i'}(d_{K/K_0})$, note that the $\wp_i'$-Newton polygon of $g(x)$ has exactly one side having slope c_i/n_i. As $\gcd(n_i, c_i)$ is not divisible by p_i,

the polynomial associated to $g(x)$ corresponding to this Newton polygon is $T(Y) = Y^{\gcd(n_i,c_i)} - \bar{\gamma}_i' \in \mathbb{F}_{p_i}[Y]$ and has no repeated roots for $\gamma_i' = b_i\alpha_i p_i^{c_i}/\pi_i^{c_i}$, π_i being prime element of the valuation ring of $v_{\wp_i'}$. By Theorem 2.A and Lemma 2.B, we have $i_{\wp_i'}(g) = \frac{1}{2}[(n_i-1)(c_i-1)+\gcd(n_i,c_i)-1]$. Therefore using (3), (4) and the fact that $v_{\wp_i'}(p_iA_{K_0}) = 1$, we see that

$$v_{\wp_i'}(d_{K/K_0}) = n_i - \gcd(n_i, c_i). \tag{7}$$

Keeping in mind that $p_iA_{K_0} = \wp_i^{p_i-1}\wp_i'$ with $N_{K_0/\mathbb{Q}}(\wp_i) = p_i = N_{K_0/\mathbb{Q}}(\wp_i')$, we immediately deduce from (6) and (7) that

$$v_{p_i}(N_{K_0/\mathbb{Q}}(d_{K/K_0})) = 2n_i - \gcd(n_i, c_i(p_i-1)) - \gcd(n_i, c_i).$$

Since $v_{p_i}(d_{K_0}) = p_i - 2$ by Lemma 2.4(ii), it now follows from the above equation and (2) that

$$\begin{aligned} v_{p_i}(d_K) &= n_i(p_i-2) + 2n_i - \gcd(n_i, c_i(p_i-1)) - \gcd(n_i, c_i). \\ &= n - \gcd(n_i, c_i(p_i-1)) - \gcd(n_i, c_i). \end{aligned}$$

Case 3: $p_i = 2$ and $d_i \equiv 5 \pmod 8$. As is well known, $2A_{K_0} = \wp_i$ with $N_{K_0/\mathbb{Q}}(\wp_i) = 2^2$, where $\wp_i$ is a prime ideal of A_{K_0} [10, Theorem 4.39]. The $\wp_i$-Newton polygon of $g(x)$ consists of one side with slope c_i/n_i, and one can see that the polynomial associated to $g(x)$ is $T(Y) = Y^{\gcd(n_i,c_i)} - \overline{b_i\alpha_i}$ with coefficients in $\mathbb{F}_{\wp_i}$, which has no repeated roots. Applying Theorem 2.A and Lemma 2.B, we obtain $i_{\wp_i}(g) = \frac{1}{2}[(n_i-1)(c_i-1)+\gcd(n_i,c_i)-1]$. Arguing as in the previous cases, one can check that $v_{\wp_i}(d_{K/K_0}) = n_i - \gcd(n_i, c_i)$; consequently, using the fact that $v_2(d_{K_0}) = 0$, we conclude that $v_2(d_K) = 2n_i - 2\gcd(n_i, c_i) = n - 2\gcd(n_i, c_i)$.

This completes the proof of Lemma 2.7. ∎

3. Proof of Theorem 1.1. Set $m_j = \gcd(n, t_j)$. By (1), we have

$$d_K[A_K : \mathbb{Z}[\theta]]^2 = (-1)^{(n-1)(n-2)/2} n^n a^{n-1}. \tag{8}$$

Recall that by Lemma 2.3, whenever either $q_j \nmid n$ or $v_{q_j}(a) = t_j$ is coprime to q_j, we have

$$v_{q_j}([A_K : \mathbb{Z}[\theta]]) = \tfrac{1}{2}[(n-1)(t_j-1) + m_j - 1];$$

consequently, it follows from (8) and the above equation that $v_{q_j}(d_K) = n - m_j$ or $2n - m_j$ according as $q_j \notin \{p_1, \ldots, p_k\}$ or $q_j \in \{p_1, \ldots, p_k\}$ with t_j coprime to q_j. The proof of the theorem is now complete as $v_p(d_K)$ is given by Corollary 2.6 and Lemma 2.7 for the other primes p dividing the right hand side of (8).

The following examples are quick applications of Corollary 1.4.

EXAMPLE 1. Let $a \neq \pm 1$ be a cube-free integer divisible by 15. Then the polynomial $f(x) = x^{15} - a$ is irreducible over $\mathbb{Q}$ in view of the Dumas irreducibility criterion ([1]). Let $K = \mathbb{Q}(\theta)$ with θ a root of $f(x)$. Then $d_K = -15^{15} \prod_{q|a} q^{14}$ where q runs over all primes dividing a.

EXAMPLE 2. Let a be a sixth-power-free even integer not divisible by 4 and such that $a \equiv \pm 1 \pmod 9$. Let $K = \mathbb{Q}(\theta)$ with θ a root of $x^6 - a$ and let $\prod_{j=1}^{l} q_j^{t_j}$ be the prime factorization of $|a|$. Then $d_K = \operatorname{sgn}(a) 2^6 3^2 \prod_{j=1}^{l} q_j^{6-\gcd(6,t_j)}$.

EXAMPLE 3. Let $p > 3$ be any prime and θ be a root of $x^{2p} - 12$. Then the discriminant of $K = \mathbb{Q}(\theta)$ is $2^{3p-1}3^{2p-1}p^{2p-4}$ or $2^{3p-1}3^{2p-1}p^{2p}$ according as $12^{p-1} \equiv 1 \pmod{p^2}$ or not.

Acknowledgements. The financial support from IISER Mohali is gratefully acknowledged by the first and third authors. The second author is grateful to Indian National Science Academy for senior scientistship.

References

[1] W. E. H. Berwick, *Integral Bases*, Cambridge Univ. Press, London, 1927.
[2] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, 1966.
[3] R. Dedekind, *Ueber die Anzahl der Idealklassen in reinen kubischen Zahlkörpern*, J. Reine Angew. Math. 121 (1900), 40–123.
[4] J.-M. De Koninck and A. Mercier, *1001 Problems in Classical Number Theory*, Amer. Math. Soc., Providence, RI, 2007.
[5] T. Funakura, *On integral bases of pure quartic fields*, Math. J. Okayama Univ. 26 (1984), 27–41.
[6] 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.
[7] S. K. Khanduja and S. Kumar, *A generalization of a theorem of Ore*, J. Pure Appl. Algebra 218 (2014), 1206–1218.
[8] 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.
[9] J. Montes and E. Nart, *On a theorem of Ore*, J. Algebra 146 (1992), 318–334.
[10] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd ed., Springer, Berlin, 2004.
[11] K. Okutsu, *Integral basis of the field* $\mathbb{Q}(\sqrt[n]{a})$, Proc. Japan Acad. 58 (1982), 219–222.
[12] P. Ribenboim, *The Theory of Classical Valuations*, Springer, New York, 1999.

([1]) DUMAS IRREDUCIBILITY CRITERION. Let $g(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ be a polynomial with coefficients in $\mathbb{Z}$. Suppose there exists a prime p such that $v_p(a_n) = 0$, $v_p(a_i)/(n-i) \geq v_p(a_0)/n$ for $0 \leq i \leq n-1$ and $v_p(a_0), n$ are coprime. Then $g(x)$ is irreducible over $\mathbb{Q}$.

[13] U. Wegner, *Zur Theorie der auflösbaren Gleichungen von Primzahlgrad. I,* J. Reine Angew. Math. 168 (1932), 176–192.

Anuj Jakhar, Sudesh K. Khanduja (corresponding author), Neeraj Sangwan
Indian Institute of Science Education and Research (IISER), Mohali
Sector 81, S. A. S. Nagar 140306, Punjab, India
E-mail: anujjakhar@iisermohali.ac.in
skhanduja@iisermohali.ac.in
neerajsan@iisermohali.ac.in