*Indian J. Pure Appl. Math.*, **50**(2): 309-314, June 2019
 DOI: 10.1007/s13226-019-0326-7

# INTEGRAL BASIS OF PURE PRIME DEGREE NUMBER FIELDS[1]

Anuj Jakhar and Neeraj Sangwan

*Indian Institute of Science Education and Research (IISER), Mohali Sector*-81,
*S. A. S. Nagar* 140 306, *Punjab, India*
*e-mails: anujjakhar@iisermohali.ac.in; neerajsan@iisermohali.ac.in*

(*Received* 11 *June* 2017; *accepted* 28 *May* 2018)

Let $K = \mathbb{Q}(\theta)$ be an extension of the field $\mathbb{Q}$ of rational numbers where $\theta$ satisfies an irreducible polynomial $x^p - a$ of prime degree belonging to $\mathbb{Z}[x]$. In this paper, we give explicilty an integral basis for $K$ using only elementary algebraic number theory. Though an integral basis for such fields is already known (see [*Trans. Amer. Math. Soc*., **11** (1910), 388-392)], our description of integral basis is different and slightly simpler. We also give a short proof of the formula for discriminant of such fields.

**Key words** : Rings of algebraic integers; integral basis and discriminant.

## 1. INTRODUCTION

Computation of discriminant as well as integral basis of an algebraic number field has been one of the most challenging problems in algebraic number theory. In 1897, Landsberg [3] gave a formula for the discriminant of algebraic number fields of the type $\mathbb{Q}(a^{\frac{1}{p}})$ of prime degree $p$ over the field $\mathbb{Q}$ of rationals. In 1900, Dedekind [2] found explicitly an integral basis for all pure cubic fields. In 1910, Westlund [6] described an integral basis for all pure prime degree number fields. In this paper, we give a short proof of the formula for the discriminant of all such fields besides explicitly constructing an integral basis of these fields which is slightly simpler than the one given in [6]. Precisely stated, we prove:

***Theorem* 1.1** — *Let $p$ be a prime number and $K = \mathbb{Q}(\theta)$ be an algebraic number field with discriminant $d_K$, where $\theta$ is a root of an irreducible polynomial $F(x) = x^p - a$ belonging to $\mathbb{Z}[x]$.*

[1]The financial support from IISER Mohali is gratefully acknowledged by the authors.

*Assume that $a$ is not divisible by the $p^{th}$ power of any prime. Let $q$ run over all distinct primes dividing $a$. Then the following hold:*

*(i) When either $p|a$ or $p \nmid a$ and $p^2 \nmid (a^p - a)$, then* $d_K = (-1)^{\frac{(p-1)(p-2)}{2}} sgn(a^{p-1}) p^p \prod_{q|a} q^{p-1}$.

*(ii) When $p^2 \mid (a^{p-1} - 1)$, then* $d_K = (-1)^{\frac{(p-1)(p-2)}{2}} sgn(a^{p-1}) p^{p-2} \prod_{q|a} q^{p-1}$.

The following theorem describes an integral basis for $K$.

***Theorem* 1.2** — *Let $p,\ K = \mathbb{Q}(\theta),\ F(x)$ be as in the above theorem. Assume that $a$ is $p^{th}$ power-free which is expressed as $\prod_{i=1}^{p-1} a_i^i$ with each $a_i$ squarefree and $a_i$, $a_j$ coprime for $i \neq j$. Let $\gamma_i$ denote the element $\theta^i / \prod_{j=1}^{p-1} a_j^{l_{i,j}}$ of $K$, where $l_{i,j}$ stands for the largest integer not exceeding $\frac{ij}{p}$. Then the following hold:*

*(i) If $p^2 \nmid (a^{p-1} - 1)$, then the set $\{1, \gamma_1, \gamma_2, \cdots, \gamma_{p-1}\}$ is an integral basis of $K$.*

*(ii) If $p^2 \mid (a^{p-1} - 1)$, then $\{\gamma_0, \gamma_1, \cdots, \gamma_{p-1}\}$ is an integral basis of $K$, where $\gamma_0 = \frac{1}{p} \sum_{i=0}^{p-1} (a'\theta)^i$ and $a'$ is any integer so that $aa' \equiv 1\ (mod\ p^2)$.*

## 2. Preliminary Results

For any algebraic number field $K$, $A_K$ will denote its ring of algebraic integers, $d_K$ its discriminant and for a maximal ideal $\wp$ of $A_K$, $N_{K/\mathbb{Q}}(\wp)$ will denote the absolute norm of $\wp$. If $\{\alpha_1, \cdots, \alpha_n\}$ is a vector space basis of $K/\mathbb{Q}$, then $D_{K/\mathbb{Q}}(\alpha_1, \cdots, \alpha_n)$ will stand for the determinant of the $n \times n$ matrix with $(i,j)$-th entry $Tr_{K/\mathbb{Q}}(\alpha_i \alpha_j)$, $Tr$ stands for the trace mapping. If $K = \mathbb{Q}(\alpha)$ with $\alpha$ an algebraic integer, then as is well known (cf. [5, Proposition 2.9])

$$D_{K/\mathbb{Q}}(1, \alpha, \cdots, \alpha^{n-1}) = d_K [A_K : \mathbb{Z}[\alpha]]^2; \tag{1}$$

further if $g(x)$ is the minimal polynomial of $\alpha$ over $\mathbb{Q}$, then one has

$$D_{K/\mathbb{Q}}(1, \alpha, \cdots, \alpha^{n-1}) = (-1)^{\frac{n(n-1)}{2}} N_{K/\mathbb{Q}}(g'(\alpha)). \tag{2}$$

The index $[A_K : \mathbb{Z}[\alpha]]$ will be denoted by $Ind(\alpha)$. We shall use the following basic lemma proved in [5, Lemma 2.17].

*Lemma* 2.A — Let $K = \mathbb{Q}(\alpha)$ be an algebraic number field with $\alpha$ an algebraic integer. If the minimal polynomial of $\alpha$ over $\mathbb{Q}$ is an Eisenstein polynomial with respect to a prime $p$, then $p$ does not divide $Ind(\alpha)$.

*Lemma* 2.1 — Let $F(x) = x^p - a,\ \theta$ and $K = \mathbb{Q}(\theta)$ be as in Theorem 1.2. For any prime $q \neq p$ dividing $a$, the exact power of $q$ dividing $d_K$ is $p-1$.

PROOF : Let $q \neq p$ be a prime dividing $a$. Then $q$ divides $a_j$ for exactly one $j$, $1 \leq j \leq p-1$. Choose a number $i$, $1 \leq i \leq p-1$, such that $ij \equiv 1\ (mod\ p)$. Set $k = \frac{ij-1}{p}$. It can be easily checked that the element $\frac{\theta^i}{a_j^k} = \xi$ (say) belonging to $K \backslash \mathbb{Q}$ satisfies the polynomial $x^p - b$ over $\mathbb{Z}$, where $b = a_j \prod_{m=1, m\neq j}^{p-1} a_m^{im}$. As $a_j$ is squarefree and $q$ divides $a_j$, the minimal polynomial $x^p - b$ of $\xi$ is an Eisenstein polynomial with respect to $q$. So by Lemma 2.A, $q$ does not divide $Ind(\xi)$. Keeping in mind (1) and (2), we see that

$$(Ind(\xi))^2 d_K = (-1)^{\frac{p(p-1)}{2}} N_{K/\mathbb{Q}}(p\xi^{p-1}) = \pm p^p b^{p-1}. \tag{3}$$

Since $q \nmid Ind(\xi)$, the above equation shows that the exact power of $q$ dividing $d_K$ is $p-1$. □

The following well known results will be used in the sequel (see [5, Proposition 6.1] for Theorem 2.B and [5, Theorem 4.24] for Theorem 2.C).

***Theorem* 2.B** — *Let $K = \mathbb{Q}(\alpha)$ with $\alpha \in A_K$ and $g(x)$ be the minimal polynomial of $\alpha$ over $\mathbb{Q}$. If for a prime $p$, $g(x)$ has the factorization $g_1(x) \cdots g_r(x)$ as a product of irreducible polynomials over the field $\mathbb{Q}_p$ of $p$-adic numbers, then $pA_K = \wp_1^{e_1} \cdots \wp_r^{e_r}$, where $\wp_i$'s are distinct prime ideals of $A_K$ with $N_{K/\mathbb{Q}}(\wp_i) = p^{f_i}$ and $e_i f_i = deg(g_i(x))$ for $1 \leq i \leq r$. Moreover the completion $K_{\wp_i} \cong \mathbb{Q}_p(\alpha_i)$ where $\alpha_i$ is a root of $g_i(x)$.*

***Theorem* 2.C** — *Let $p$ be a prime number and $K$ an algebraic number field with $pA_K = \wp_1^{e_1} \cdots \wp_r^{e_r}$, where $\wp_1, \cdots, \wp_r$ are distinct prime ideals of $A_K$ and $N_{K/\mathbb{Q}}(\wp_i) = p^{f_i}$. If $(p, e_i) = 1$ for $1 \leq i \leq r$, then the exact power of $p$ dividing $d_K$ is $\sum_{i=1}^{r} f_i(e_i - 1)$.*

## 3. PROOF OF THEOREM 1.1

By hypothesis $a$ is $p^{th}$ power-free, so it can be written as $\prod_{i=1}^{p-1} a_i^i$ with each $a_i$ squarefree and $a_i, a_j$ coprime for $i \neq j$. Using (1) and (2), we see that

$$D_{K/\mathbb{Q}}(1, \theta, \cdots, \theta^{p-1}) = (-1)^{\frac{p(p-1)}{2}} N_{K/\mathbb{Q}}(F'(\theta)) = (-1)^{\frac{(p-1)(p-2)}{2}} p^p a^{p-1} = Ind(\theta)^2 d_K. \tag{4}$$

It follows from the above equation that

$$sgn(d_K) = (-1)^{\frac{(p-1)(p-2)}{2}} sgn(a^{p-1}). \tag{5}$$

Consider first the case when $p$ divides $a$. So $p | a_j$ for a unique $j$, $1 \leq j \leq p-1$. Fix a number $i$ such that $1 \leq i \leq p-1$ and $ij \equiv 1\ (mod\ p)$. Define $k = \frac{ij-1}{p}$ and $\xi = \frac{\theta^i}{a_j^k}$. Arguing exactly as in the

proof of Lemma 2.1, it can be seen that $p \nmid Ind(\xi)$ and (3) holds, which implies that the exact power of $p$ dividing $d_K$ is $2p-1$. It now follows from Lemma 2.1 that $d_K = sgn(d_K)p^{2p-1}\prod_{q|a, q\neq p} q^{p-1}$ and hence the theorem is proved in this case in view of (5).

Now consider the case when $p \nmid a$ and $p^2 \nmid (a^p - a)$. In this case $F(x+a)$ is an Eisenstein polynomial with respect to $p$. So by virtue of Lemma 2.A, $p$ does not divide $Ind(\theta - a) = Ind(\theta)$. Using Lemma 2.1 and (4), we conclude that $d_K = sgn(d_K)p^p \prod_{q|a} q^{p-1}$, which proves the theorem in the present case.

Finally consider the case when $p^2 \mid (a^{p-1} - 1)$. In this case, we prove the theorem when $p$ is an odd prime as the result is trivially true when $p = 2$. We first show that $a$ is a $p$-th power in the ring $\mathbb{Z}_p$ of $p$-adic integers. By hypothesis $a^{p-1} \equiv 1 + bp^2 \ (mod\ p^3)$ for some $b \in \mathbb{Z}$. Keeping in mind that $p > 2$, it can be easily seen that $1 + bp^2 \equiv (1+bp)^p \ (mod\ p^3)$. So $\frac{a^p}{a(1+bp)^p} \equiv 1 \ (mod\ p^3)$. Applying Hensel's Lemma [1, Chapter 1, Section 5, Theorem 3], we see that $\frac{a^p}{a(1+bp)^p}$ is a $p$-th power in $\mathbb{Z}_p$ and hence so is $a$, say $a = c^p$, $c \in \mathbb{Z}_p$. Then the polynomial $F(x+c) = (x+c)^p - c^p = xg(x)$, where $g(x) = x^{p-1} + c\binom{p}{1}x^{p-2} + c^2\binom{p}{2}x^{p-3} + \cdots + pc^{p-1}$. As $F(x+c) \equiv x^p \ (mod\ p)$ and the constant term $pc^{p-1}$ of $g(x)$ is not divisible by $p^2$, it follows that $g(x)$ is an Eisenstein polynomial with respect to $p$. Therefore for any root $\eta$ of $g(x)$, $\mathbb{Q}_p(\eta)$ is a totally ramified extension of the field $\mathbb{Q}_p$ of $p$-adic numbers having degree $p-1$ (cf. [5, Theorem 5.27]). Consequently the factorization $F(x) = (x-c)g(x-c)$ of $F(x)$ over $\mathbb{Z}_p$ shows that $pA_K = \wp_1\wp_2^{p-1}$ in view of Theorem 2.B, where $\wp_1, \wp_2$ are distinct prime ideals of $A_K$ with $N_{K/\mathbb{Q}}(\wp_i) = p$. It now follows from Theorem $2.C$ that $v_p(d_K) = p-2$. Hence $d_K = \pm p^{p-2}\prod_{q|a} q^{p-1}$ by virtue of Lemma 2.1. This completes the proof of the theorem in view of (5).

## 4. Proof of Theorem 1.2

The following simple lemma is already known (cf. [4, Problem 434]). For reader's convenience, we prove it here.

*Lemma* 4.A — Let $p$ be a prime number and $l_{i,j}$ denote the largest integer not exceeding $\frac{ij}{p}$, $1 \leq i, j \leq p-1$. Then

$$\sum_{j=1}^{p-1} l_{i,j} = \frac{(p-1)(i-1)}{2} \text{ for } 1 \leq i \leq p-1.$$

Proof : Let $S = \{(j,k) \in \mathbb{Z} \times \mathbb{Z} \mid 1 \leq j \leq p-1, 1 \leq k \leq i-1\}$. It is clear that the number of elements of $S$ (to be denoted by $\#S$) is $(p-1)(i-1)$. Now let $S_1 = \{(j,k) \in S | ij > pk\}$ and $S_2 = \{(j,k) \in S | ij < pk\}$. Since $(i,p) = 1$, there is no point of $S$ with integer coordinates on the

line $y = ix/p$, and hence $S_1 \cup S_2 = S$ and $S_1 \cap S_2 = \emptyset$. By symmetry we have $\#S_1 = \#S_2 = \frac{\#S}{2} = \frac{(p-1)(i-1)}{2}$. For a fixed integer $j$ chosen arbitrarily in the interval $[1, p-1]$, there are exactly $l_{i,j}$ points of $S$ with integer coordinates of abscissa $j$ located below the line $y = ix/p$. Therefore $\frac{(p-1)(i-1)}{2} = \#S_1 = \sum_{j=1}^{p-1} \sum_{1 \le k \le ij/p} 1 = \sum_{j=1}^{p-1} l_{i,j}$. □

PROOF OF THEOREM 1.2. : It can be easily checked that the element $\gamma_i = \frac{\theta^i}{\prod_{j=1}^{p-1} a_j^{l_{i,j}}}$ satisfies the polynomial $x^p - \prod_{j=1}^{p-1} a_j^{ij - pl_{i,j}}$ and hence is an algebraic integer because $ij \ge pl_{i,j}$.

First we consider the case when $p^2 \nmid (a^{p-1} - 1)$. In this case the transition matrix from $\{1, \gamma_1, \cdots, \gamma_{p-1}\}$ to $\{1, \theta, \cdots, \theta^{p-1}\}$ has determinant $\prod_{j=1}^{p-1} \prod_{i=1}^{p-1} a_i^{l_{i,j}}$ which is equal to $\prod_{i=1}^{p-1} a_i^{\frac{(p-1)(i-1)}{2}}$ by virtue of Lemma 4.A. Now using a basic result (cf. [5, Proposition 2.9]), we see that

$$D_{K/\mathbb{Q}}(1, \theta, \cdots, \theta^{p-1}) = \left( \prod_{i=1}^{p-1} |a_i|^{\frac{(p-1)(i-1)}{2}} \right)^2 D_{K/\mathbb{Q}}(1, \gamma_1, \cdots, \gamma_{p-1}).$$

Comparing the above equation with (4), we see that

$$D_{K/\mathbb{Q}}(1, \gamma_1, \cdots, \gamma_{p-1}) = \frac{(-1)^{\frac{(p-1)(p-2)}{2}} p^p a^{p-1}}{\prod_{i=1}^{p-1} |a_i|^{(p-1)(i-1)}}.$$

Keeping in mind that $a = sgn(a) \prod_{i=1}^{p-1} |a_i|^i$, a simple calculation shows that the above equation can be rewritten as

$$D_{K/\mathbb{Q}}(1, \gamma_1, \cdots, \gamma_{p-1}) = (-1)^{\frac{(p-1)(p-2)}{2}} sgn(a^{p-1}) p^p \prod_{i=1}^{p-1} |a_i|^{p-1}.$$

Since the right hand side of the last equation equals $d_K$ by Theorem 1.1(i), we conclude that the subset $\{1, \gamma_1, \cdots, \gamma_{p-1}\}$ of $A_K$ is an integral basis of $K$.

Consider now the case when $p^2 \mid (a^{p-1} - 1)$. We shall soon prove that $\gamma_0$ is an algebraic integer. Using Lemma 4.A, we see that the transition matrix from $\{\gamma_0, \gamma_1, \cdots, \gamma_{p-1}\}$ to $\{1, \theta, \cdots, \theta^{p-1}\}$ has determinant $p \prod_{i=1}^{p-1} a_i^{\frac{(p-1)(i-1)}{2}}$. Now arguing exactly as in the previous case, it can be shown that

$$D_{K/\mathbb{Q}}(\gamma_0, \gamma_1, \cdots, \gamma_{p-1}) = (-1)^{\frac{(p-1)(p-2)}{2}} sgn(a^{p-1}) p^{p-2} \prod_{i=1}^{p-1} |a_i|^{p-1}.$$

By Theorem 1.1(ii), the right hand side of the above equation equals $d_K$. So the theorem is proved once we show that $\gamma_0$ is an algebraic integer. Denote $p\gamma_0$ by $\eta = \sum_{i=0}^{p-1} (a'\theta)^i$; multiplying this equality

by $(a'\theta - 1)$ on both sides and using the fact that $\theta^p = a$, we see that

$$a'\theta\eta = \eta + aa'^p - 1.$$

Now taking $p^{th}$ power on both sides and again using $\theta^p = a$, we obtain

$$aa'^p\eta^p = \sum_{r=0}^{p} \binom{p}{r} \eta^{p-r}(aa'^p - 1)^r,$$

which can be rewritten as

$$(aa'^p - 1)\eta^p = \sum_{r=1}^{p} \binom{p}{r} \eta^{p-r}(aa'^p - 1)^r. \tag{6}$$

Note that $aa'^p \neq 1$ because the equality $aa'^p = 1$ implies $a = \pm 1$ when $p$ is odd and $a = 1$ when $p = 2$, which is impossible in view of the irreducibility of $x^p - a$ over $\mathbb{Q}$. On dividing (6) by $aa'^p - 1$, we have

$$\eta^p = \sum_{r=1}^{p} \binom{p}{r} \eta^{p-r}(aa'^p - 1)^{r-1}.$$

Thus $\eta$ satisfies the polynomial $x^p - \sum_{r=1}^{p} \binom{p}{r} x^{p-r}(aa'^p - 1)^{r-1}$ and hence $\frac{\eta}{p} = \gamma_0$ satisfies the polynomial $x^p - \sum_{r=1}^{p} \frac{\binom{p}{r}}{p} x^{p-r} \left(\frac{aa'^p - 1}{p}\right)^{r-1} = g(x)$ (say). It only remains to verify that $g(x) \in \mathbb{Z}[x]$. For this it is enough to show that $aa'^p \equiv 1 \ (mod\ p^2)$. The last congruence quickly follows from the hypothesis $(aa')^p \equiv 1 \ (mod\ p^2)$ and $a^p \equiv a \ (mod\ p^2)$. This proves that $\gamma_0$ is an algebraic integer and hence the theorem. □

## REFERENCES


1. Z. I. Borevich and I. R. Shafarevich, *Number theory*, Academic Press, 1966.
2. R. Dedekind, Über die Anzahl der Idealklassen in reinen kubischen Zahlkörpern, *Journal für die reine und angewandte Mathematik*, **121** (1900), 40-123.
3. G. Landsberg, Ueber das Fundamental system und die Discriminante der Gattungen algebraischer Zahlen, welche aus Wurzelgrössen gebildet sind, *Journal für die reine und angewandte Mathematik*, **117** (1897), 140-147.
4. J. M. de Koninck and A. Mercier, 1001 Problems in classical number theory, *American Mathematical Society*, Providence Rhode Island, 2007.
5. W. Narkewicz, *Elementary and analytic theory of algebraic numbers*, Springer-Verlag, Berlin Heidelberg, 2004.
6. J. Westlund, On the fundamental number of the algebraic number field $k(\sqrt[p]{m})$, *Trans. Amer. Math. Soc.*, **11** (1910), 388-392.