Bol. Soc. Paran. Mat.
©SPM –ISSN-2175-1188 ON LINE
SPM: www.spm.uem.br/bspm

(3s.) **v. 2024 (42)** : 1–7.
ISSN-0037-8712 IN PRESS
doi:10.5269/bspm.64902

On the Ideal Discriminant of Some Relative Pure Extensions

Mohammed. E. Charkani and Omar Boughaleb

ABSTRACT: Let $L = K(\alpha)$ be an extension of a number field K where α satisfies the monic irreducible polynomial $P(X) = X^p - a \in R[X]$ of prime degree p and such that a is p^{th} power free in $R := O_K$ (the ring of integers of K). The purpose of this paper is to give an explicit formula for the ideal discriminant $D_{L/K}$ of L over K involving only the prime ideals dividing the principal ideals aR and pR. As an illustration, we compute the discriminant $D_{L/K}$ of a family of septic and quintic pure fields over quadratic fields. Hence a slightly simpler computation of discriminant $D_{L/\mathbb{Q}}$ is obtained.

Key Words: Integral closure, discriminant, relative pure extensions.

Contents

1. Introduction

Computation of the discriminant of certain number fields is in general a difficult task and is related to the computation of integral bases which is a classical hard problem in algebraic number theory. Many works are available in this area (cf. [1], [7], [8], [11], [12], [13], [14], [22], [23], [25], and others). It is called a problem of Hasse to characterize whether the ring of integers in an algebraic number field has a power integral basis or does not. Let R be a Dedekind ring of characteristic zero and K its fraction field. Let L/K be a finite separable extension of degree n and let O_L denote the ring of the integral elements of L. We say that L/K is *monogenic* if L possesses a relative *monogenic* integral basis, or equivalently, $\{1, \alpha, \ \alpha^2, \ \ldots, \ \alpha^{n-1}\}$ is an integral basis of L/K for some α in O_L, in other words $O_L = R[\alpha]$ (In this case one may say that α is a power basis generator of L/K (see [10]). In 2010 Del Corso and Rossi [8] provided a formula for the discriminant of Kummer cyclic extension of number fields. For pure algebraic number fields Jakhar and Khanduja [13] gave a formula for the discriminant of pure number fields having square free degree. In 2020 the authors of [12] gave a formula for the discriminant of n-th degree fields of the type $\mathbb{Q}(\sqrt[n]{a})$ using Newton polygon techniques. Let L be a relative pure extension, in other word an algebraic field of the type $L = K(\sqrt[p]{a})$, where K is an algebraic number field and the polynomial $X^p - a$ of prime degree belonging to $K[X]$ is irreducible over the field K. In the present paper, our aim is to give an explicit formula for the relative discriminant $D_{L/K}$ of O_L the ring of integer of L in terms of the set of primes $\mathfrak{p}$ in O_K (denoted by $Spec(O_K)$) with $p\mathbb{Z} = \mathfrak{p} \cap O_K$ and such that $aO_K \subseteq \mathfrak{p}$. As a consequence, using the tower formula stated below (2.2), we compute the discriminant $D_{L/\mathbb{Q}}$ for two families of septic and quintic pure fields L, such that $[L : \mathbb{Q}] = 10$ and $[L : \mathbb{Q}] = 14$ respectively.

Let R be a Dedekind ring with finite residual fields and containing $\mathbb{Z}$. Let K be its fraction field. Let $\mathfrak{p}$ be a non zero prime ideal in R and $N_{\mathfrak{p}} = \mid R/\mathfrak{p} \mid$ be the cardinality of the residual field $R/\mathfrak{p}$. Let a be a non zero element in R. We will say that a is n^{th} power free in R if $\upsilon_{\mathfrak{p}}(a) \leq n-1$ for any non zero prime ideal $\mathfrak{p}$ in R, where $\upsilon_{\mathfrak{p}}$ is the $\mathfrak{p}$-adic discrete valuation associated to $\mathfrak{p}$. Let p be a prime number. We denote by $Fib_R(p)$ the set of all non zero primes ideals in R which lie above p. It is clear that $\mathfrak{p} \in Fib_R(p)$

2010 *Mathematics Subject Classification:* 13B22, 11R04, 13F10.
Submitted September 05, 2022. Published March 08, 2023

if and only if $char(R/\mathfrak{p}) = p$. We note also that if a non zero element a in K, is n^{th} power free in K then $a \notin K^p$. The converse is false. By theorem 9.1 [[17] p. 331], if K is a field, p is an odd prime and $a \in K - \{0\}$ then the polynomial $P = X^p - a$ is irreducible in $K[X]$ if and only if $a \notin K^p$. Hence if a is n^{th} power free in K then the polynomial $P = X^p - a$ is irreducible in $K[X]$. If further R is integrally closed and a is n^{th} power free in R then the polynomial $P = X^p - a$ is irreducible in $R[X]$.

Let L be a finite separable extension of K and O_L the integral closure of R in L. Let $\alpha \in O_L$ such that $L = K(\alpha)$. Assume that $charK = 0$ and $P = X^p - a \in R[X]$ is the monic minimal polynomial of α, where p is an odd prime number and a is p^{th} power free in R. The main result of this paper is Theorem 1.1 which gives the discriminant $D_{L/K}$ of a pure relative cyclic fields of prime degree. Precisely stated, we prove the following result:

Theorem 1.1. *With the above assumptions, if $\upsilon_{\mathfrak{p}}(a^{N_{\mathfrak{p}}} - a) = 1$, for all primes $\mathfrak{p} \in Fib_R(p)$, then*

$$D_{L/K} = p^p \ \mathfrak{a}^{p-1},$$

where $\mathfrak{a}$ is the ideal radical of aR.

Corollary 1.1. *With the above assumptions, if the ideal aR is square free and $\upsilon_{\mathfrak{p}}(a^{N_{\mathfrak{p}}} - a) = 1$, for all primes $\mathfrak{p} \in Fib_R(p)$, then α is a power basis generator of L/K.*

*Proof.*indeed if the ideal aR is square free then its radical is aR and hence $D_{L/K} = Disc_R P$.

Note the above corollary is approved by Theorem 6.1 in [21]. Indeed $\mathfrak{p}$ satisfies the Wieferich congruence if and only if $\upsilon_{\mathfrak{p}}(a^{N_{\mathfrak{p}}-1} - 1) \geq 2$ (see [6]).

2. Preliminary results

Throughout this article, unless specifically stated otherwise, R is a Dedekind ring of characteristic zero and K its fraction field. Let L/K be a finite separable extension of degree n, O_L the integral closure of R in L, and $L = K(\alpha)$ for some $\alpha \in O_L$. Let $P \in K[X]$ be the minimal irreducible polynomial of α over K. Since R is integrally closed, $P \in R[X]$ (see [15, p. 7]). Let $\mathrm{Disc}_R(P)$ be the principal ideal of R generated by $\mathrm{Res}(P, P')$, where $\mathrm{Res}(P, P')$ denotes the resultant of the two polynomials P and its derivative P', we let $D_{L/K}$ denote the discriminants over R of the number field L over K. The following Index-discriminant formula (2.1) and the tower formula (2.2) are well known (see [2], [5] or [9]).

$$\mathrm{Disc}_R(P) = \mathrm{Ind}_R(\alpha)^2 \, D_{L/K}, \tag{2.1}$$

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

where $N_{K/\mathbb{Q}}$ denotes the norm from K to $\mathbb{Q}$ (see [19, Corollary 10. 2] and [9]). We denote by $Spec(R)$, the set of the prime ideals of a commutative ring R. Recall that the closed sets of the Zariski topology on $Spec(R)$, are the sets:

$$V(I) = \{\mathfrak{p} \in Spec\,(R) \mid I \subseteq \mathfrak{p}\}$$

where I is an arbitrary ideal in R. Note also that for any non-zero prime ideal $\mathfrak{p}$ in R, we consider the set of prime ideals $\mathfrak{q}$ in O_L such that $\mathfrak{p} = \mathfrak{q} \cap R$. We call this set the fibre of $\mathfrak{p}$ in L and we will denote it by $Fib_L(\mathfrak{p})$.

In view of the previous Index-Discriminant formula (2.1), the element α is a power basis generator (PBG for short) of L over K if and only if $\mathfrak{p}$ doesn't divide the index ideal $[O_L : R[\alpha]]_R$, for any non zero prime ideal $\mathfrak{p}$ in R, such that $\mathfrak{p}^2$ divides $\mathrm{Disc}_R(P)$. This fact leads us to introduce, for any irreducible polynomial P, the set S_P of prime ideals which square divides the ideal $Disc_R P$. Then:

$$S_P = \{ \mathfrak{p} \in specR \mid \mathfrak{p}^2 \ divides \ \mathrm{Disc}_R(P) \}.$$

It may pointed out that S_P is the set of non zero primes whose may divide the ideal $\mathrm{Ind}_R(\alpha)$. Finally recall that -with notation as above - for a polynomial P belonging to $R[X]$, $\overline{P}$ will stand for the polynomial over $k = R/\mathfrak{p}$ obtained on replacing each coefficient of P by its residue modulo $\mathfrak{p}$. Denote by $R_{\mathfrak{p}}$ the localization of R at the prime $\mathfrak{p}$.

The following lemma is an immediate consequence of the already known results [1, Proposition 5.12, p. 62]) and [2, property (2), p. 10]), its proof is omitted (cf. [[6], Lemma 3.4]).

Lemma 2.1. *Let R be a Dedekind ring, K its fraction field, L is a finite separable extension over K and O_L is the integral closure of R in L. Let $\alpha \in O_L$ be an algebraic integer over R such that $L = K(\alpha)$. Let $\mathfrak{p}$ be a non zero prime ideal in R and B the integral closure of $R_\mathfrak{p}$ in L. Then $\mathrm{Ind}_{R_\mathfrak{p}}(\alpha) = (\mathrm{Ind}_R(\alpha))_\mathfrak{p}$. In particular $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ if and only if $B = R_\mathfrak{p}[\alpha]$.*

Definition 2.1. *Let R be a Dedekind ring, K its fraction field and υ be a valuation on K. Let $P = a_0 + a_1X + ... + a_nX^n \in K[X]$, we put:*

$$\upsilon_G(P) = \inf\{\upsilon(a_i) \mid 0 \le i \le n\},$$

then υ_G is a valuation on $K[X]$ called the Gauss valuation on $K[X]$ relative to υ.

The well known Dedekind criterion permits us to decide whether a primitive element $\alpha \in O_L$ is a power basis generator of L over K (PBG for short or a monogenic element of L over K).

Theorem 2.2 (Dedekind Criterium)**.** *(see [20], [3], [18], [16], [4], [23]) With notations as above, let $P = Irrd(\alpha, R) \in R[X]$ be the monic irreducible polynomial of α. Let $\mathfrak{p}$ be a non zero prime ideal in R and $k := R/\mathfrak{p}$ its residual field. Let $\bar{P}$ be the image in $k[X]$ of P and assume that $\bar{P} = \Pi_{i=1}^r \bar{P_i}^{l_i}$ is the primary decomposition of $\bar{P}$ in $k[X]$ with $P_i \in R[X]$ a monic lift of the irreducible polynomial $\overline{P_i}$ for $1 \le i \le r$. Let $T \in R[X]$ satisfying $P = \prod_{i=1}^r P_i^{l_i} + \pi T$. Then α is a PBG of L over $R_\mathfrak{p}$ if and only if $gcd\left(\overline{P}_i, \overline{T}\right) = 1$ for all $i = 1, \cdots, r$ such that $l_i \ge 2$.*

Corollary 2.1. *With notations as in Theorem 2.2. Let $V_i \in R[X]$ be the remainder of Euclidean division of P by P_i. Let $\upsilon_\mathfrak{p}$ be the $\mathfrak{p}$-adic discrete valuation associated to $\mathfrak{p}$. Let υ_G be the Gauss valuation on $K[X]$ associated to $\upsilon_\mathfrak{p}$. Then $\mathfrak{p}$ doesn't divide the index ideal $\mathrm{Ind}_R(\alpha)$ if and only if $\upsilon_G(V_i) = 1$ for all $i = 1, \cdots, r$ such that $l_i \ge 2$.*

*Proof.*Let $T \in R[X]$ satisfying $P = \prod_{i=1}^r P_i^{l_i} + \pi T$. Then it can be easily verified that $gcd\left(\overline{P}_i, \overline{T}\right) = 1$ for all $i = 1, \cdots, r$ such that $l_i \ge 2$ if and only if $\upsilon_G(V_i) = 1$ for all $i = 1, \cdots, r$ such that $l_i \ge 2$, where $V_i \in R[X]$ is the remainder of Euclidean division of P by P_i.

3. Proof of Theorem 1.1

Let R be a Dedekind ring containing $\mathbb{Z}$ and $P = X^p - a$ a monic irreducible polynomial in $R[X]$. Recall that the discriminant of P is equal to $Disc_R(P) = p^p\, a^{p-1}R$. As $p \ge 3$, then the set $S_P = Fib_R(p) \cup V(aR)$. Recall also if $\mathfrak{p}$ is a non zero prime ideal in R then $char(R/\mathfrak{p}) = p$ if and only if $\mathfrak{p} \in Fib_R(p)$.

To prove Theorem 1.1 we shall need the following lemmas:

Lemma 3.1. *Let R be a Dedekind ring with finite residual fields and K its fraction field. Assume that $charK = 0$ and $L = K(\alpha)$ is a finite separable extension of K. Let $P = X^p - a \in R[X]$ be the monic minimal polynomial of α, where p is an odd prime number. Let $\mathfrak{p}$ be a non zero prime of R and $\upsilon_\mathfrak{p}$ be the $\mathfrak{p}$-adic discrete valuation associated to $\mathfrak{p}$. Assume that $\mathfrak{p} \in V(aR) - Fib_R(p)$. Then $\upsilon_\mathfrak{p}(D_{L/K}) = p - 1$.*

*Proof.*Assume that $\mathfrak{p} \in V(aR) - Fib_R(p)$, by localization at $\mathfrak{p}$ the ring $R_\mathfrak{p}$ is a discrete valuation ring, putting $\mathfrak{p} = \pi R$ its maximal ideal, we obtain $P \equiv X^p \mod \pi R$, therefore it is immediate that the remainder of the Euclidean division of P by X is a. Hence if $\upsilon_\mathfrak{p}(a) = 1$, then by Dedekind Criterion (Theorem 2.2) α is a PBG of L over $R_\mathfrak{p}$. Now applying Lemma 2.1 we see that $\mathfrak{p}$ does not divide the index ideal $\mathrm{Ind}_R(\alpha)$ and hence by the index-discriminant formula (2.1) we have $\upsilon_\mathfrak{p}(D_{L/K}) = p - 1$. Set $\upsilon_\mathfrak{p}(a) = s$ and suppose that $s > 1$, let $1 < r < p$ such that $sr \equiv 1[p]$. Set $t = \frac{rs-1}{p}$, then the element $\beta = \frac{\alpha^r}{\pi^t}$ is an algebraic integer satisfies the polynomial $Q = X^p - b$ where $b = \frac{a^r}{\pi^{tp}}$. As the remainder of the Euclidean division of Q by X is b and $\upsilon_\mathfrak{p}(b) = rs - tp = 1$, we see that β is a PBG of L over $R_\mathfrak{p}$. Now by index-discriminant formula (2.1) we immediately conclude that

$$p^p b^{p-1} = \mathrm{Ind}_R(\beta)^2\, D_{L/K}.$$

Since in view of Lemma 2.1, $\mathfrak{p}$ does not divide the index $\mathrm{Ind}_R(\beta)$, the above equation shows that the exact power of $\mathfrak{p}$ dividing $D_{L/K}$ is $p - 1$.

Lemma 3.2. *With notations as in Lemma 3.1 assume that* $\mathfrak{p} \in Fib_R(p) - V(aR)$ *and* $\upsilon_{\mathfrak{p}}(a^{N_{\mathfrak{p}}} - a) = 1$. *Then* $\upsilon_{\mathfrak{p}}(D_{L/K}) = p\, e(\mathfrak{p}/p)$.

*Proof.*Let $\mathfrak{p} \in Fib_R(p) - V(aR)$ and assume that $\upsilon_{\mathfrak{p}}(a^{N_{\mathfrak{p}}} - a) = 1$, by localization at $\mathfrak{p}$ the ring $R_{\mathfrak{p}}$ is a discrete valution ring, set $\mathfrak{p} = \pi R$ its maximal ideal, we claim that $\lambda = \alpha - a^{\frac{N_{\mathfrak{p}}}{p}}$ is a PBG of L over $R_{\mathfrak{p}}$. Observe first that the element λ is an algebraic integer satisfying the polynomial

$$P_\lambda(X) = \left(X + a^{\frac{N_{\mathfrak{p}}}{p}}\right)^p - a = \sum_{k=1}^{p} \binom{p}{k} X^k \left(a^{\frac{N_{\mathfrak{p}}}{p}}\right)^{p-k} + a^{N_{\mathfrak{p}}} - a,$$

Since p divide $\binom{p}{k}$ for $1 \le k \le p-1$, then we see immediately that $P_\lambda \equiv X^p \mod \pi R$ and hence the remainder of the Euclidean division of P by X is $a^{N_{\mathfrak{p}}} - a$, this proves in view of Dedekind Criterion and the fact that $\upsilon_{\mathfrak{p}}(a^{N_{\mathfrak{p}}} - a) = 1$ that λ is a PBG of L over $R_{\mathfrak{p}}$, consequently in view of Lemma 2.1 $\mathfrak{p}$ does not divide the index $\mathrm{Ind}_R(\lambda) = \mathrm{Ind}_R(\alpha)$. Now by index-discriminant formula (2.1) one can write

$$\mathrm{Disc}_R(P_\lambda) = \mathrm{Disc}_R(P) = p^p a^{p-1} = \mathrm{Ind}_R(\alpha)^2\, D_{L/K},$$

the above equation shows that the exact power of $\mathfrak{p}$ dividing $D_{L/K}$ is $p-1$.

Proof of Theorem 1.1.

Indeed $pR = \prod_{\mathfrak{p}|p} \mathfrak{p}^{e(\mathfrak{p}/p)}$. Let $\mathfrak{c} := p^p\, \mathfrak{p}^{p-1}$. It suffices to show that $\upsilon_{\mathfrak{p}}(D_{L/K}) = \upsilon_{\mathfrak{p}}(\mathfrak{c})$ for all prime $\mathfrak{p} \in S_P$. Let $\mathfrak{p} \in S_P$. It is clear first that

$$\upsilon_{\mathfrak{p}}(\mathfrak{c}) = \upsilon_{\mathfrak{p}}(p) + (p-1)\upsilon_{\mathfrak{p}}(\mathfrak{p}) = \begin{cases} p\, e(\mathfrak{p}/p) + (p-1) & \text{if } \upsilon_{\mathfrak{p}}(a) \geqslant 1, \\ p\, e(\mathfrak{p}/p) & \text{if } \upsilon_{\mathfrak{p}}(a) = 0, \end{cases}$$

If $\upsilon_{\mathfrak{p}}(a) = 0$, then $\mathfrak{p} \in Fib_R(p)$ and hence in view of Lemma 3.2 $\upsilon_{\mathfrak{p}}(D_{L/K}) = p\, e(\mathfrak{p}/p)$. If $\upsilon_{\mathfrak{p}}(a) \geqslant 1$, then then there is two cases: If $\mathfrak{p} \notin Fib_R(p)$ then $e(\mathfrak{p}/p) = 0$ and in view of Lemma 3.2 $\upsilon_{\mathfrak{p}}(D_{L/K}) = \upsilon_{\mathfrak{p}}(\mathfrak{c}) = p-1$. If $\mathfrak{p} \in Fib_R(p)$ then $\upsilon_{\mathfrak{p}}(a) = 1$ as $\upsilon_{\mathfrak{p}}(a^{N_{\mathfrak{p}}} - a) = 1$ hence $\mathfrak{p}$ does not divide the index $\mathrm{Ind}_R(\alpha)$ and consequently $\upsilon_{\mathfrak{p}}(D_{L/K}) = \upsilon_{\mathfrak{p}}(\mathrm{Disc}_R(P)) = \upsilon_{\mathfrak{p}}(\mathfrak{c}) = p\, e(\mathfrak{p}/p) + p - 1$.

4. Illustration

4.1. Relative pure septic extension

Theorem 4.1. *Let* $K = \mathbb{Q}(\sqrt{35})$ *be a quadratic extension and* O_K *its ring of integer. Let* $L = K(\alpha)$ *be a septic extension of the field* K, *where* α *satisfies an irreducible polynomial* $P = X^7 - a_m$ *belonging to* $O_K[x]$ *such that* $a_m = \sqrt{35} + m$, $(m \in \mathbb{Z})$, *furthermore we assume that* $7 \nmid m$ *and* $m^6 \equiv 1 \mod 49$. *Then*

$$D_{L/K} = 7^7 \mathfrak{b}_m^6,$$

where $\mathfrak{b}_m$ *is the ideal radical of* $a_m R$.

*Proof.*First of all we note that $7O_K = \mathfrak{p}^2$, it is known that the cardinality of $O_K/\mathfrak{p}$ is 7 since the residual degree of $\mathfrak{p}$ is $f = 1$. We claim that $\upsilon_{\mathfrak{p}}(a_m^7 - a_m) = 1$. Observe first that

$$\begin{aligned} a_m^6 - 1 &= \sum_{k=0}^{6} \binom{6}{k} \left(\sqrt{35}\right)^k m^{6-k} - 1 \\ &= m^6 - 1 + 525m^4 + 18375m^2 + 42875 + \sqrt{35}\left(6m^5 + 700m^3 + 7350m\right). \end{aligned}$$

Now by property of dominance principle, and using the fact that $\upsilon_7(m) = 0$, it is easy to check that

$$\upsilon_{\mathfrak{p}}\left(6m^5 + 700m^3 + 7350m\right) = 0,$$

and

$$v_{\mathfrak{p}}\left(525m^4+18375m^2+42875\right)=2.$$

Keeping this in mind and using the fact that $m^6\equiv 1 \mod 49$, we see immediately that

$$v_{\mathfrak{p}}\left(a_m^6-1\right)=\min\left(v_{\mathfrak{p}}\left(525m^4+18375m^2+42875\right),v_{\mathfrak{p}}((m^6-1)),v_{\mathfrak{p}}(\sqrt{35})\right)=1$$

Now it is clear that $v_{\mathfrak{p}}(a_m^7-a_m)=1$, as $v_{\mathfrak{p}}(a_m)=0$ since $7\nmid m$. Satisfying the conditions of Theorem 1.1, so the discriminant of L over K is given by

$$D_{L/K}=7^7\mathfrak{b}_m^6,$$

where $\mathfrak{b}_m$ is the ideal radical of a_mR.

Corollary 4.1. *With notations as in Theorem 4.1, the discriminant $D_{L/\mathbb{Q}}$ is given by*

$$D_{L/\mathbb{Q}}=7^{21}\cdot 2^{14}\cdot 5^7\cdot N_{K/\mathbb{Q}}(\mathfrak{p}_m)^6.$$

Proof. *The proof immediately follows from the discriminant tower formula (2.2) and the fact that $D_{K/\mathbb{Q}}=2^2\cdot 5\cdot 7$.*

Exemples 4.1. *With notations as in Theorem 4.1, let $m=1$, then $L=\mathbb{Q}(\sqrt{35},\sqrt[7]{1+\sqrt{35}})$. Now using the facts that $N_{K/\mathbb{Q}}(\sqrt{35}+1)=2\times 17$, $x^2-35\equiv(x+1)^2 \mod 2$, $x^2-35\equiv(x+1)(x+16) \mod 17$, we see that $(\sqrt{35}+1)O_K=\mathfrak{p}_1^2\mathfrak{p}_2$ where $\mathfrak{p}_1=2O_K+(\sqrt{35}+1)O_K$ and $\mathfrak{p}_2\in Fib_{O_K}(17)$. Hence by Theorem 4.1 the discriminant of L over K is given by*

$$D_{L/K}=7^7(\mathfrak{p}_1\mathfrak{p}_2)^6,$$

Using now corollary 4.1 we see that

$$D_{L/\mathbb{Q}}=7^{21}\cdot 2^{14}\cdot 5^7\cdot N_{K/\mathbb{Q}}(\mathfrak{p}_1)^6N_{K/\mathbb{Q}}(\mathfrak{p}_2)^6=7^{21}\cdot 2^{20}\cdot 5^7\cdot 17^6.$$

4.2. Relative pure quintic extension

Theorem 4.2. *Let $K=\mathbb{Q}(\sqrt{3})$ be a quadratic extension and O_K its ring of integer. Let $L=K(\alpha)$ be a quintic extension of the field K where α satisfies an irreducible polynomial $P=X^5-a_m$ belonging to $O_K[x]$ such that $a_m=5^2m+\sqrt{3}$, $(m\in\mathbb{Z})$. Then*

$$D_{L/K}=5^5\mathfrak{b}_m^4,$$

where $\mathfrak{b}_m$ is the ideal radical of a_mR.

Proof. Observe first that $O_K=\mathbb{Z}[\sqrt{3}]$ and $5O_K=\mathfrak{p}$ is prime in O_K. We claim that $v_{\mathfrak{p}}(a_m^{25}-a_m)=1$. It is clear that

$$\begin{aligned}a_m^{24}-1&=\sum_{k=0}^{24}\binom{24}{k}\left(\sqrt{3}\right)^k(5^2m)^{24-k}-1,\\&=\left(\sqrt{3}\right)^{24}-1+\sum_{k=0}^{23}\binom{24}{k}\left(\sqrt{3}\right)^k(5^2m)^{24-k}.\end{aligned}$$

Now using the fact that for any $0\leqslant k\leqslant 23$, we have

$$v_{\mathfrak{p}}(5^2m)^{24-k}=(24-k)(v_{\mathfrak{p}}(m)+2).$$

It is easy to check that

$$v_{\mathfrak{p}}\left(\sum_{k=0}^{23}\binom{24}{k}\left(\sqrt{3}\right)^k(5^2m)^{24-k}\right)>1.$$

Now since $\upsilon_{\mathfrak{p}}((\sqrt{3})^{24} - 1) = 1$, then by property of dominance principle, it is easy to check that

$$\upsilon_{\mathfrak{p}}(a_m^{24} - 1) = \min\left(\upsilon_{\mathfrak{p}}((\sqrt{3})^{24} - 1), \upsilon_{\mathfrak{p}}\left(\sum_{k=0}^{23}\binom{24}{k}\left(\sqrt{3}\right)^k (5^2m)^{24-k}\right)\right) = 1.$$

To complete the proof. It is clearly enough to show that $\upsilon_{\mathfrak{p}}(a_m) = 0$. Suppose to the contrary that 5 divides a_m, now since 5 divides 5^2m, then 5 divides $\sqrt{3}$ which is impossible as $\upsilon_5(\sqrt{3}) = 0$, this proves that $\upsilon_{\mathfrak{p}}(a_m) = \upsilon_5(a_m) = 0$. Satisfying the conditions of Theorem 1.1, so the discriminant of L over K is given by

$$D_{L/K} = 5^5\mathfrak{b}_m^4,$$

where $\mathfrak{b}_m$ is the ideal radical of a_mR.

Corollary 4.2. *With previous conditions in Theorem 4.2. The discriminant $D_{L/\mathbb{Q}}$ is given by:*

$$D_{L/\mathbb{Q}} = 5^{10} \cdot 2^{10} \cdot 3^5 N_{K/\mathbb{Q}}(\mathfrak{p}_m)^4.$$

Proof. *The proof follows immediately from the fact that Since $D_{K/\mathbb{Q}} = 2^2.3$ and the discriminant tower formula (2.2).*

Exemples 4.2. *Assume that $m = 2$, then $L = \mathbb{Q}(\sqrt{3}, \sqrt[5]{50+\sqrt{3}})$ Now using the facts that $N_{K/\mathbb{Q}}(50+\sqrt{3}) = 11.277$ and $x^2 - 3 \equiv \mod (x+5)(x+6) \mod 11$, $x^2 - 3 \equiv \mod (x+130)(x+147) \mod 277$, we see that $(50+\sqrt{3})O_K = \mathfrak{p}_1\mathfrak{p}_2$ where $\mathfrak{p}_1 \in Fib_{O_K}(11)$. and $\mathfrak{p}_2 \in Fib_{O_K}(277)$. Hence by Theorem 4.2 we see that*

$$D_{L/K} = 5^5(\mathfrak{p}_1\mathfrak{p}_2)^4.$$

Now using corollary 4.2 we see that the discriminant of L over $\mathbb{Q}$ is given by

$$D_{L/\mathbb{Q}} = 5^{10} \cdot 2^{10} \cdot 3^5 N_{K/\mathbb{Q}}(\mathfrak{p}_1)^4 N_{K/\mathbb{Q}}(\mathfrak{p}_2)^4 = 5^{10} \cdot 2^{10} \cdot 3^5 \cdot 11^4 \cdot 277^4.$$

Acknowledgments

The author is very grateful to the anonymous referee for his careful checking.

References

1. Atiyah. M. F, Macdonald. I. G., *Introduction to Commutative Algebra*. Addison- Wesley, Massachusetts, (1969).
2. Cassels. J. W. S, Fröhlich. A., *Algebraic Number Theory*, Academic Press, London and New york, 1967.
3. M. E. Charkani, O. Lahlou, *On Dedekind's criterion and monogenicity over Dedekind rings*. Int. J. of Math. and Math. Sci. (2003) (7) (2003) 4455–4464. Zbl 1066.11046, https://doi.org/10.1155/S0161171203211534.
4. M. E. Charkani, A. Deajim, *Generating a power basis over a Dedekind Ring*. J. Number Theory 132, No. 10, 2267-2276, (2012).Zbl 1293.11101, https://doi.org/10.1016/j.jnt.2012.04.006.
5. M. E. Charkani, A. Deajim, *Relative index extensions of Dedekind rings*. JP J. Algebra, Number Theory and Appl **27**, 73–84 (2012). Zbl 1368.11111.
6. M. Sahmoudi, M. E. Charkani, *Relative monogenity of pure cyclic fields of degree an odd prime number*. Mathematica Bohemica, pp. 1-12, (2022).
7. Cohen. H., *A Course in Computational Algebraic Number Theory*, GTM Vol. 138, Springer Verlag, Berlin, 1996.
8. I. Corso, L. Rossi, *Normal integral bases for cyclic Kummer extensions*. Journal of Pure and Applied Algebra, 214(2010) 385391. Zbl 1203.11074, https://doi.org/10.1016/j.jpaa.2009.06.019.
9. Fröhlich. A, Taylor. M. J., *Algebraic Number Theory*, Combridge Studies in Advenced Mathematics, **27**, Cambridge University Press, (1993).
10. I.Gaál, *Diphantine equations and power integral bases*, Theory and algorithms. 2nd edition, Birkhäuser,2019.
11. A. Hameed, T. Nakahara, *Integral bases and relative monogenity of pure octic fields*. Bull. Math. Soc. Sci. Math. Roumanie Tome, 58(106) No. 4, 2015, 419-433. Zbl 1363.11094.
12. A. Jakhar, S. K. Khanduja, N.Sanagwan, *On integral basis of pure number fields*. Mathematika 67 (2021) 187–195.

13. A. Jakhar, N. Sangwan, *Integral basis of pure prime degree number fields.* Indian Journal of Pure andd Applied Mathematics, volume 50, pages 309-314 (2019). Zbl 1455.11141.

14. A. Jakhar, S. K. Khanduja, N. Sangwan, *Discriminant of pure square free degree number fields.* Acta Arith., 181, 2017, 287-296, DOI: 10.4064/aa170508-4-11.

15. Janusz.G.J., *Algebric Number Fields*, Academic Press, New York, Second Edition (1995).

16. M. Kumar, S. K. Khanduja, *A Generalization of Dedekind criterion.* Communication in Algebra, **35**, 1479-1486 (2007). Zbl 1145.11078, https://doi.org/10.1080/00927870601168897.

17. Lang. S., *Algebra*, Second Edition, Addison-Wesley, (1984).

18. J. Montes, E. Nart, *On a theorem of Ore. Journal of Algebra.* Vol. 146, (1992) 318-334. Zbl 0762.11045

19. Neukirch.J., *Algebraic Number theory. Springer Publication*, (1999).

20. P. Schmid, *On criteria by Dedekind and Ore for integral ring extensions.* Arch. Math. **84** (2005) 304–310. Zbl 1072.13004.

21. H. Smith, *The monogeneity of radical extensions.* Acta Arithmetica, 198 (2021), 313-327.

22. B. K. Spearman, K. S. Williams, *Relative integral bases for quartic fields over quadratic subfields.* Acta Math. Hungar., 70 ,185-192, (1996). Zbl 0864.11051.

23. A. Soullami, M. Sahmoudi, O. Boughaleb, *On relative power integral basis of a family of numbers fields.* Rocky Mountain J. Math. 51(4): 1443-1452 (2021). Zbl 1469.11414, DOI: 10.1216/rmj.2021.51.1443.

24. S.-L. Tan, D.-Q. Zhang, *The determination of integral closures and geometric applications*, Adv. in Math. **185** (2004) 215–245, DOI:10.1016/S0001-8708(03)00210-X.

25. K. Uchida, *When is $\mathbb{Z}[\alpha]$ the ring of the integers?*, Osaka J. Math. **14** (1977), 155–157.

Omar Boughaleb,
Department of Mathematics,
Sidi Mohamed Ben Abdellah University,
Morocco.
E-mail address: boughaleb01omar@gmail.com

and

Mohammed. E. Charkani,
Department of Mathematics,
Sidi Mohamed Ben Abdellah University,
Morocco.
E-mail address: mcharkani@gmail.com