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 $\alpha$ 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 $D_{L/Q}$ is obtained.

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

Contents

1 Introduction .......................... 1

2 Preliminary results ...................... 2

3 Proof of Theorem 1.1 ..................... 3

4 Illustration .............................. 4

4.1 Relative pure septic extension .......... 4

4.2 Relative pure quintic extension ........ 5

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 $\alpha$ in $O_L$, in other words $O_L = R[\alpha]$ (In this case one may say that $\alpha$ 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 $L = K(\sqrt[n]{a})$, 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 $p$ in $O_K$ (denoted by Spec($O_K$)) with $p\mathbb{Z} = p \cap O_K$ and such that $aO_K \subseteq p$. As a consequence, using the tower formula stated below (2.2), we compute the discriminant $D_{L/Q}$ 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 $p$ be a non zero prime ideal in $R$ and $N_p = | R/p |$ be the cardinality of the residual field $R/p$. Let $a$ be a non zero element in $R$. We will say that $a$ is $n$th power free in $R$ if $v_p(a) \leq n - 1$ for any non zero prime ideal $p$ in $R$, where $v_p$ is the $p$-adic discrete valuation associated to $p$. Let $p$ be a prime number. We denote by $\text{Fib}_R(p)$ the set of all non zero primes ideals in $R$ which lie above $p$. It is clear that $p \in \text{Fib}_R(p)$
if and only if $\text{char}(R/p) = p$. 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 $a \in K \setminus \{0\}$ 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 $\text{char}K = 0$ and $P = X^p - a \in R[X]$ is the monic minimal polynomial of $\alpha$, 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 $v_p(a^{N_p} - a) = 1$, for all primes $p \in \text{Fib}_R(p)$, then

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

where $a$ is the ideal radical of $aR$.

**Corollary 1.1.** With the above assumptions, if the ideal $aR$ is square free and $v_p(a^{N_p} - a) = 1$, for all primes $p \in \text{Fib}_R(p)$, then $\alpha$ is a power basis generator of $L/K$.

**Proof.** Indeed if the ideal $aR$ is square free then its radical is $aR$ and hence $D_{L/K} = \text{Disc}_R P$.

Note the above corollary is approved by Theorem 6.1 in [21]. Indeed $p$ satisfies the Wieferich congruence if and only if $v_p(a^{N_p-1} - 1) \geq 2$ (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 $\alpha$ over $K$. Since $R$ is integrally closed, $P \in R[X]$ (see [15, p. 7]). Let $\text{Disc}_R(P)$ be the principal ideal of $R$ generated by $\text{Res}(P, P')$, where $\text{Res}(P, P')$ 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]).

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

(2.1)

$$D_{L/Q} = N_{K/Q}(D_{L/K}) \cdot (D_{K/Q})^{[L:K]},$$

(2.2)

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

$$V(I) = \{p \in S_{\text{spec}}(R) \mid I \subseteq p\}$$

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

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

$$S_P = \{p \in S_{\text{spec}}(R) \mid p^2 \text{ divides } \text{Disc}_R(P)\}.$$

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

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 $\text{Ind}_{R_{\mathfrak{p}}}(\alpha) = (\text{Ind}_R(\alpha))_{\mathfrak{p}}$. In particular $\mathfrak{p}$ doesn’t divide the index ideal $\text{Ind}_R(\alpha)$ if and only if $B = R_{\mathfrak{p}}[\alpha]$.

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

$$\nu_G(P) = \inf\{\nu(a_i) \mid 0 \leq i \leq n\},$$

then $\nu_G$ is a valuation on $K[X]$ called the Gauss valuation on $K[X]$ relative to $\nu$.

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 Criterion). (see [20], [3], [18], [16], [4], [23]) With notations as above, let $P = \text{Irrd}(\alpha, R) \in R[X]$ be the monic irreducible polynomial of $\alpha$. 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 $\bar{P} = \prod_{i=1}^r \bar{P}_i^{l_i}$ is the primary decomposition of $P$ in $k[X]$ with $P_i \in R[X]$ a monic lift of the irreducible polynomial $\bar{P}_i$ for $1 \leq i \leq r$. Let $T \in R[X]$ satisfying $\bar{P} = \prod_{i=1}^r P_i^{l_i} + \pi T$. Then $\alpha$ is a PBG of $L$ over $R_{\mathfrak{p}}$ if and only if $\text{gcd}(\bar{P}_i, T) = 1$ for all $i = 1, \ldots, r$ such that $l_i \geq 2$.

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 $\nu_\mathfrak{p}$ be the $\mathfrak{p}$-adic discrete valuation associated to $\mathfrak{p}$. Let $\nu_G$ be the Gauss valuation on $K[X]$ associated to $\nu_\mathfrak{p}$. Then $\mathfrak{p}$ doesn’t divide the index ideal $\text{Ind}_R(\alpha)$ if and only if $\nu_G(V_i) = 1$ for all $i = 1, \ldots, r$ such that $l_i \geq 2$.

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 $\text{gcd}(\bar{P}_i, T) = 1$ for all $i = 1, \ldots, r$ such that $l_i \geq 2$ if and only if $\nu_G(V_i) = 1$ for all $i = 1, \ldots, r$ such that $l_i \geq 2$, 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 $\text{Disc}_R(P) = p^p \cdot a^{p-1}R$. As $p \geq 3$, then the set $S_p = \text{Fib}_R(p) \cup V(aR)$. Recall also if $p$ is a non zero prime ideal in $R$ then $\text{char}(R/\mathfrak{p}) = p$ if and only if $\mathfrak{p} \in \text{Fib}_R(p)$.

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 $\text{char}K = 0$ 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 $\alpha$, where $p$ is an odd prime number. Let $\mathfrak{p}$ be a non zero prime of $R$ and $\nu_\mathfrak{p}$ be the $\mathfrak{p}$-adic discrete valuation associated to $\mathfrak{p}$. Assume that $\mathfrak{p} \in V(aR) - \text{Fib}_R(p)$. Then $\nu_\mathfrak{p}(D_{L/K}) = p - 1$.

Proof. Assume that $\mathfrak{p} \in V(aR) - \text{Fib}_R(p)$, 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 $\nu_\mathfrak{p}(a) = 1$, then by Dedekind Criterion (Theorem 2.2) $\alpha$ 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 $\text{Ind}_R(\alpha)$ and hence by the index-discriminant formula (2.1) we have $\nu_\mathfrak{p}(D_{L/K}) = p - 1$. Set $\nu_\mathfrak{p}(a) = s$ and suppose that $s > 1$, let $1 < r < p$ such that $sr \equiv 1[p]$. Set $t = \frac{sr - 1}{p}$, then the element $\beta = a^r - b \in \mathfrak{p}$ is an algebraic integer satisfies the polynomial $Q = X^p - b$ where $b = \frac{a^r}{\pi^rp}$. As the remainder of the Euclidean division of $Q$ by $X$ is $b$ and $\nu_\mathfrak{p}(b) = rs - tp = 1$, we see that $\beta$ is a PBG of $L$ over $R_{\mathfrak{p}}$. Now by index-discriminant formula (2.1) we immediately conclude that $\nu_\mathfrak{p}(b)^{p-1} = \text{Ind}_R(\beta)^2 D_{L/K}$.

Since in view of Lemma 2.1, $\mathfrak{p}$ does not divide the index $\text{Ind}_R(\beta)$, 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 $p \in \text{Fib}_R(p) - V(aR)$ and $v_p(a^N - a) = 1$. Then $v_p(D_{L/K}) = pe(p/p)$.

Proof. Let $p \in \text{Fib}_R(p) - V(aR)$ and assume that $v_p(a^N - a) = 1$, by localization at $p$ the ring $R_p$ is a discrete valuation ring, set $p = \pi R$ its maximal ideal, we claim that $\lambda = \alpha - a a^N/\pi$ is a PBG of $L$ over $R_p$. Observe first that the element $\lambda$ is an algebraic integer satisfying the polynomial

$$P_\lambda(X) = \left(X + a a^N/\pi\right)^p - a = \sum_{k=1}^{p} \binom{p}{k} X^k \left(a a^N/\pi\right)^{p-k} + a a^N - a,$$

Since $p$ divide $\binom{p}{k}$ for $1 \leq k \leq p - 1$, 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 $a a^N - a$, this proves in view of Dedekind Criterion and the fact that $v_p(a a^N - a) = 1$ that $\lambda$ is a PBG of $L$ over $R_p$, consequently in view of Lemma 2.1 $p$ does not divide the index $\text{Ind}_R(\lambda) = \text{Ind}_K(\alpha)$. Now by index-discriminant formula (2.1) one can write

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

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

Proof of Theorem 1.1.

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

$$v_p(e) = v_p(p) + (p - 1)v_p(p) = \begin{cases} pe(p/p) + (p - 1) & \text{if } v_p(a) \geq 1, \\ pe(p/p) & \text{if } v_p(a) = 0, \end{cases}$$

If $v_p(a) = 0$, then $p \in \text{Fib}_R(p)$ and hence in view of Lemma 3.2 $v_p(D_{L/K}) = pe(p/p)$. If $v_p(a) \geq 1$, then then there is two cases: If $p \notin \text{Fib}_R(p)$ then $e(p/p) = 0$ and in view of Lemma 3.2 $v_p(D_{L/K}) = v_p(e) = p - 1$. If $p \in \text{Fib}_R(p)$ then $v_p(a) = 1$ as $v_p(a a^N - a) = 1$ hence $p$ does not divide the index $\text{Ind}_R(\alpha)$ and consequently $v_p(D_{L/K}) = v_p(\text{Disc}_R(P)) = v_p(e) = pe(p/p) + p - 1$.

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 integers. Let $L = K(\alpha)$ be a septic extension of the field $K$, where $\alpha$ 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 $m^8 \equiv 1 \mod 49$. Then

$$D_{L/K} = 7^7 b_m^6,$$

where $b_m$ is the ideal radical of $a_m R$.

Proof. First of all we note that $7O_K = p^2$, it is known that the cardinality of $O_K/p$ is 7 since the residual degree of $p$ is $f = 1$. We claim that $v_p(a_7^m - a_m) = 1$. Observe first that

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

Now by property of dominance principle, and using the fact that $v_7(m) = 0$, it is easy to check that

$$v_p \left(6m^5 + 700m^3 + 7350m\right) = 0,$$
2.2 we see that

\[ v_p (525m^4 + 18375m^2 + 42875) = 2. \]

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

\[ v_p (a_m^6 - 1) = \min \left( v_p (525m^4 + 18375m^2 + 42875), v_p((m^6 - 1)), v_p(\sqrt[3]{35}) \right) = 1 \]

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

\[ D_{L/K} = 7^7 b_m^6, \]

where \( b_m \) is the ideal radical of \( a_m R \).

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

\[ D_{L/Q} = 7^{21} \cdot 2^{14} \cdot 5^7 \cdot N_{K/Q}(p_m)^6. \]

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

**Examples 4.1.** With notations as in Theorem 4.1, let \( m = 1 \), then \( L = \mathbb{Q}(\sqrt[3]{35}, \sqrt[3]{1 + \sqrt[3]{35}}) \). Now using the facts that \( N_{K/Q}(\sqrt[3]{35} + 1) = 2 \times 17, x^2 - 35 \equiv (x + 1)^2 \mod 2, x^2 - 35 \equiv (x + 1)(x + 16) \mod 17 \), we see that \( (\sqrt[3]{35} + 1)O_K = p_1^2 p_2^2 \) where \( p_1 = 2O_K + (\sqrt[3]{35} + 1)O_K \) and \( p_2 \in \text{Fib}_{O_K}(17) \). Hence by Theorem 4.1 the discriminant of \( L \) over \( K \) is given by

\[ D_{L/K} = 7^7 (p_1 p_2)^6, \]

Using now corollary 4.1 we see that

\[ D_{L/Q} = 7^{21} \cdot 2^{14} \cdot 5^7 \cdot N_{K/Q}(p_1)^6 N_{K/Q}(p_2)^6 = 7^{21} \cdot 2^{20} \cdot 5^7 \cdot 17^6. \]

**4.2. Relative pure quintic extension**

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

\[ D_{L/K} = 5^5 b_m^4, \]

where \( b_m \) is the ideal radical of \( a_m R \).

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

\[ a_{m}^{24} - 1 = \sum_{k=0}^{24} \binom{24}{k} (\sqrt[3]{3})^k (5^2 m)^{24-k} - 1, \]

\[ = (\sqrt[3]{3})^{24} - 1 + \sum_{k=0}^{23} \binom{24}{k} (\sqrt[3]{3})^k (5^2 m)^{24-k}. \]

Now using the fact that for any \( 0 \leq k \leq 23 \), we have

\[ v_p(5^2 m)^{24-k} = (24 - k)(v_p(m) + 2). \]

It is easy to check that

\[ v_p \left( \sum_{k=0}^{23} \binom{24}{k} (\sqrt[3]{3})^k (5^2 m)^{24-k} \right) > 1. \]
Now since $v_p((\sqrt{3})^{24} - 1) = 1$, then by property of dominance principle, it is easy to check that

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

To complete the proof. It is clearly enough to show that $v_p(\lambda) = 0$. Suppose to the contrary that 5 divides $\lambda$, now since 5 divides $5^2 m$, then 5 divides $\sqrt{3}$ which is impossible as $v_5(\sqrt{3}) = 0$, this proves that $v_p(\lambda) = v_5(\lambda) = 0$. Satisfying the conditions of Theorem 1.1, so the discriminant of $L$ over $K$ is given by

$$D_{L/K} = 5^5 b_m^4,$$

where $b_m$ is the ideal radical of $a_m R$.

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

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

Proof. The proof follows immediately from the fact that since $D_{K/Q} = 2^2 \cdot 3$ and the discriminant tower formula (2.2).

**Examples 4.2.** Assume that $m = 2$, then $L = \mathbb{Q}(\sqrt{3}, \sqrt{50 + \sqrt{3}})$ Now using the facts that $N_{K/Q}(50 + \sqrt{3}) = 11.277$ and $x^2 - 3 \equiv \mod (x+5)(x+6) \mod 11$, we see that $(50 + \sqrt{3})O_K = p_1 p_2$ where $p_1 \in \text{Fib}_{O_K}(11)$, and $p_2 \in \text{Fib}_{O_K}(277)$. Hence by Theorem 4.2 we see that

$$D_{L/K} = 5^5 (p_1 p_2)^4.$$

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

$$D_{L/Q} = 5^{10} \cdot 2^{10} \cdot 3^5 N_{K/Q}(p_1)^4 N_{K/Q}(p_2)^4 = 5^{10} \cdot 2^{10} \cdot 3^5 \cdot 11^4 \cdot 277^4.$$ 

**Acknowledgments**

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

**References**


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