



HAL
open science

Index, the prime ideal factorization in simplest quartic fields and counting their discriminants

Abdelmejid Bayad, Mohammed Seddik

► **To cite this version:**

Abdelmejid Bayad, Mohammed Seddik. Index, the prime ideal factorization in simplest quartic fields and counting their discriminants. *Filomat*, 2020, 34 (2), pp.591-600. 10.2298/FIL2002591B . hal-04458821

HAL Id: hal-04458821

<https://hal.science/hal-04458821v1>

Submitted on 4 Apr 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

INDEX, PRIME IDEAL FACTORIZATION IN SIMPLEST QUARTIC FIELDS AND COUNTING THEIR DISCRIMINANTS.

MOHAMMED SEDDIK

ABSTRACT. We consider the simplest quartic number fields \mathbb{K}_m defined by the irreducible quartic polynomials

$$x^4 - mx^3 - 6x^2 + mx + 1,$$

where m runs over the positive rational integers such that the odd part of $m^2 + 16$ is squarefree. In this paper, we study the common index divisor $I(\mathbb{K}_m)$ and determine explicitly the prime ideal decomposition for any prime number in any simplest quartic number fields \mathbb{K}_m . On the other hand, we establish an asymptotic formula for the number of simplest quartic fields with discriminant $\leq x$ and given index.

1. INTRODUCTION AND PRELIMINARIES

Let \mathbb{K} be a number field. We start with given most important known results on the common factor of indices $I(\mathbb{K})$, the prime ideal factorization and the asymptotic formula for number fields with discriminant $\leq x$.

1.1. **Index $I(\mathbb{K})$ for number fields \mathbb{K} .** Let \mathbb{K} be a number field of degree n over \mathbb{Q} and let $\mathbb{O}_{\mathbb{K}}$ be its ring of integers. Denote by $\widehat{\mathbb{O}}_{\mathbb{K}}$ the set of primitive elements of $\mathbb{O}_{\mathbb{K}}$. For any $\theta \in \mathbb{O}_{\mathbb{K}}$ we denote $F_{\theta}(x)$ the characteristic polynomial of θ over \mathbb{Q} . Let $D_{\mathbb{K}}$ be the discriminant of \mathbb{K} . It is well known that if $\theta \in \widehat{\mathbb{O}}_{\mathbb{K}}$, the discriminant of $F_{\theta}(x)$ has the form

$$(1.1) \quad D(\theta) = I(\theta)^2 D_{\mathbb{K}},$$

where $I(\theta) = (\mathbb{O}_{\mathbb{K}} : \mathbb{Z}[\theta])$ is called the index of θ . Let

$$(1.2) \quad I(\mathbb{K}) = \gcd_{\theta \in \widehat{\mathbb{O}}_{\mathbb{K}}} I(\theta).$$

A prime number p is called a common factor of indices if $p \mid I(\mathbb{K})$.

The knowledge of the index $I(\mathbb{K})$ makes it possible to find the explicit decomposition of the prime numbers in the fields \mathbb{K} : If the prime number $p \nmid I(\mathbb{K})$, by equation (1.2) there exist a primitive integer θ where $p \nmid I(\theta)$ and by Dedekind's theorem [5, §18] we explicitly have the factorization of p using θ . However, if p is a common factor divisor, the prime ideal decomposition in $\mathbb{O}_{\mathbb{K}}$ is more difficult.

Date: January 15, 2018.

2000 Mathematics Subject Classification. Primary : 11R04, 11R33, 13F20.

Key words and phrases. Common factor of indices, common divisor of values of polynomials, prime ideal factorization, cyclic quartic fields, discriminant.

* *Corresponding Author:* Mohammed Seddik, mohammed.seddik@univ-evry.fr.

Let us recall the statement of Dedekind's theorem. Let $\mathbb{K} = \mathbb{Q}(\theta)$ be an algebraic number field with $\theta \in \mathbb{O}_{\mathbb{K}}$. Let p be a rational prime. Let

$$f(x) = \text{Irr}_{\mathbb{Q}}(x, \theta) \in \mathbb{Z}[x].$$

We consider the canonical surjection map $\mathbb{Z}[x] \rightarrow \mathbb{Z}/p\mathbb{Z}[x]$. We write

$$\bar{f}(x) = g_1(x)^{e_1} \cdots g_r(x)^{e_r},$$

where $g_1(x), \dots, g_r(x)$ are distinct monic irreducible polynomials in $\mathbb{Z}/p\mathbb{Z}[x]$ and e_1, \dots, e_r are positive integers.

For $i = 1, 2, \dots, r$ denote by $f_i(x)$ any monic polynomial of $\mathbb{Z}[x]$ such that $\bar{f}_i = g_i$. We then set

$$P_i = \langle p, f_i(\theta) \rangle.$$

If $I(\theta) \not\equiv 0 \pmod{p}$ then we have P_1, \dots, P_r are distinct prime ideals of $\mathbb{O}_{\mathbb{K}}$ with

$$p\mathbb{O}_{\mathbb{K}} = P_1^{e_1} \cdots P_r^{e_r},$$

and

$$N(P_i) = p^{\deg(f_i)}.$$

In the following we review some known results on the computation of the index $I(\mathbb{K})$.

- If \mathbb{K} is a quadratic field ($n = 2$), by classical number theory on quadratic fields, one can show that $I(\mathbb{K}) = 1$.
- In case \mathbb{K} is a cubic field ($n = 3$), Engstrom [6] showed that $I(\mathbb{K}) = 1$ or 2. Llorente and Nart in [14, Theorem 1] determine the *type of decomposition* of the rational primes and in [14, Theorem 4] give a necessary and sufficient condition for the index of \mathbb{K} to be 2. Moreover, in the paper [19] Spearman and Williams give the *explicit prime ideal factorization* of 2 in cubic fields with index 2.
- In the case \mathbb{K} is a quartic field ($n = 4$), Engstrom [6] showed that

$$(1.3) \quad I(\mathbb{K}) = 1, 2, 3, 4, 6 \text{ or } 12.$$

- If the field \mathbb{K} is a cyclic quartic field, Spearman and Williams [20] showed that $I(\mathbb{K})$ assumes all of these values and they give necessary and sufficient conditions for each to occur and find an asymptotic formula for the number of cyclic quartic fields with discriminant $\leq x$ and $I(\mathbb{K}) = i$ for each $i \in \{1, 2, 3, 4, 6, 12\}$,

$$N(x; i) = \alpha_i x^{\frac{1}{2}} + O(x^{\frac{1}{3}} \log^3 x),$$

where

$$\begin{aligned} \alpha_1 &\approx 0.0970153, & \alpha_2 &\approx 0.0067627, & \alpha_3 &\approx 0.0101764, \\ \alpha_4 &\approx 0.0067627, & \alpha_6 &\approx 0.0006321, & \alpha_{12} &\approx 0.0006321. \end{aligned}$$

- Funakura [7, Theorem 5] showed that in the case of a pure quartic field, we have $I(\mathbb{K}) = 1, 2$.
- In the pure quartic field, Spearman and Williams [21] gives the explicit prime ideal factorization of 2 when the index is equal to 2.

1.2. **Counting discriminants with given index.** The general problem in algebraic number theory is that of counting the number of fields by discriminant. If we let $N_n(x)$ denote the number of fields of degree n over \mathbb{Q} whose discriminants do not exceed x in absolute value. Then there is a conjecture that

$$\lim_{x \rightarrow \infty} \frac{N_n(x)}{x}$$

exist and is non-zero. This conjecture is proved in many special cases:

- For quadratic field, the problem is simple we have

$$N_2(x) = \sum_{\substack{|d| \leq x \\ d \equiv 1 \pmod{4}}} 1 + \sum_{\substack{|d| \leq \frac{x}{4} \\ d \equiv 2,3 \pmod{4}}} 1 \sim \frac{6}{\pi^2} x.$$

- For cyclic cubic fields H. Cohn [4] and Cohen-Diaz y Diaz in [3, p.577, §3] showed that

$$N_3(x) \sim C_3 x^{1/2}$$

where

$$C_3 = \frac{11\sqrt{3}}{36\pi} \prod_{\substack{p \equiv 1 \pmod{6} \\ p \text{ prime}}} \left(1 - \frac{2}{p(p+1)}\right).$$

- For cyclic quartic fields Baily [2, p. 209, Theorem 9] and its revised form by many authors see [13], [18] and [3, p.580, §5] by different methods, as follows

$$N_4(x) \sim C_4 x^{1/2}$$

where

$$C_4 = \frac{3}{\pi^2} \left(\left(1 + \frac{\sqrt{2}}{24}\right) \prod_{\substack{p \equiv 1 \pmod{4} \\ p \text{ prime}}} \left(1 + \frac{2}{p^{3/2} + p^{1/2}}\right) - 1 \right).$$

1.3. **Summary of the paper.** In this paper, we investigate the family of the simplest quartic fields which are defined by adjunction to \mathbb{Q} of a root of the polynomial

$$P_m = x^4 - mx^3 - 6x^2 + mx + 1, \quad m \in \mathbb{Z}^+$$

where $m^2 + 16$ is not divisible by an odd square. It is easy to see that m may be specified greater than zero as P_m and P_{-m} generate the same extension.

M.N. Gras in [9] proved that those polynomials are reducibles precisely when $m^2 + 16$ is a square, which occurs only for excluded cases $m = 0, 3$, and show that the form $m^2 + 16$ represents infinitely many square-free integers. Olajos [17] proved that \mathbb{K}_m admits power integral bases only for $m = 2, 4$ and he gave all generators of power integral bases. Recently, Gaál and Pentrányi [8] compute the minimal index of the simplest quartic fields.

The purpose of this paper :

- We study the common indices $I(\mathbb{K}_m)$ and the prime ideal decomposition is determined explicitly,
- We establish an asymptotic formula for the number of the simplest quartic fields with given index and the discriminants less than x .

2. STATEMENT OF MAIN RESULTS

We state our main results.

2.1. Computation of the index $I(\mathbb{K}_m)$ and prime decomposition.

Theorem 2.1. Let $m \in \mathbb{Z}^+$, $m \neq 0, 3$ and $\mathbb{K}_m = \mathbb{Q}(\theta)$ where θ be a root of P_m . Then we have

(1)

$$I(\mathbb{K}_m) = \begin{cases} 2 & \text{if } m \text{ odd,} \\ 1 & \text{if } m \text{ even.} \end{cases}$$

(2) The prime ideal factorization of 2 in \mathbb{K}_m with index 2 is

$$2\mathbb{O}_{\mathbb{K}_m} = \left\langle 2, \frac{1 + \sqrt{m^2 + 16}}{2} \right\rangle \left\langle 2, \frac{1 - \sqrt{m^2 + 16}}{2} \right\rangle.$$

(3) The prime ideal factorization of 2 in \mathbb{K}_m with index 1 is as follows:

1) If $v_2(m) = 1$, then,

$$2\mathbb{O}_{\mathbb{K}_m} = \left\langle 2, \frac{m\theta^3 + 10\theta^2 - m\theta + 6}{4} \right\rangle^2.$$

2) If $v_2(m) = 2$, then,

$$2\mathbb{O}_{\mathbb{K}_m} = \left\langle 2, \frac{1 + \theta + \theta^2 + \theta^3}{4} \right\rangle^4.$$

3) If $v_2(m) = 3$, then,

$$2\mathbb{O}_{\mathbb{K}_m} = \left\langle 2, \frac{(m^3 + 25m + 4)\theta^3 + (5m^2 + 168)\theta^2 - (m^3 + 21m - 56)\theta - m^2 + 8}{16} \right\rangle^2.$$

4) If $v_2(m) \geq 4$, then,

$$2\mathbb{O}_{\mathbb{K}_m} = \left\langle 2, \frac{2 + 7\theta + \theta^3}{4} \right\rangle^2 \left\langle 2, \frac{5 + 7\theta + \theta^3}{4} \right\rangle^2.$$

Proposition 2.1. Let $m \in \mathbb{Z}^+$, $m \neq 0, 3$ and $\mathbb{K}_m = \mathbb{Q}(\theta)$ where θ be a root of P_m . Then

$$I(\theta) = \begin{cases} 2 & \text{if } v_2(m) = 0, \\ 2^2 & \text{if } v_2(m) = 1, \\ 2^3 & \text{if } v_2(m) = 2, \\ 2^4 & \text{if } v_2(m) \geq 3. \end{cases}$$

Remark. Note that we can show that for any p odd prime, we can give explicitly the factorization of p using θ . To do it, we need to factorize $P_m \pmod{p}$ and we use Dedekind's theorem.

2.2. Asymptotic number of simplest quartic fields with discriminant $\leq x$ and given index. Let $\mathbb{K}_m = \mathbb{Q}(\theta)$ where θ be a root of P_m (simplest quartic fields).

We define for a positive integer i

$$(2.1) \quad N(x, i) = \text{number of } \mathbb{K}_m \text{ with } D(\mathbb{K}_m) \leq x \text{ and } I(\mathbb{K}_m) = i.$$

We state our second main result.

Theorem 2.2. For $i = 1, 2, 3, 4, 6, 12$ we have

(1) $N(x, i) = 0$ for $i \neq 1, 2$.

(2) For $i = 1, 2$, we have the asymptotic formulas

$$N(x, i) \sim C_i x^{\frac{1}{6}},$$

where

$$C_1 = \left(\frac{1}{4\sqrt[3]{4}} + \frac{1}{4\sqrt[3]{2}} + \frac{1}{4} \right) \prod_{\substack{p \equiv 1 \pmod{4} \\ p \text{ prime}}} \left(1 - \frac{2}{p^2} \right)$$

and

$$C_2 = \frac{1}{4} \prod_{\substack{p \equiv 1 \pmod{4} \\ p \text{ prime}}} \left(1 - \frac{2}{p^2} \right)$$

As corollary, from Theorem 2.2, the number $N(x)$ of simplest quartic fields \mathbb{K}_m with discriminant $D(\mathbb{K}_m) \leq x$ is given by

$$N(x) = N(x, 1) + N(x, 2) \sim \left(\frac{1}{4\sqrt[3]{4}} + \frac{1}{4\sqrt[3]{2}} + \frac{1}{2} \right) \prod_{\substack{p \equiv 1 \pmod{4} \\ p \text{ prime}}} \left(1 - \frac{2}{p^2} \right) x^{\frac{1}{6}}, \text{ as } x \rightarrow \infty$$

REFERENCES

- [1] F. V. Atkinson, L. Cherwell, *The mean-values of arithmetical functions*, Quart. J. Math. Oxford Ser. **20** (1949), 65-79.
- [2] A. Baily, *On the density of discriminants of quartic fields*, J. reine angew. Math. **315** (1980), 190-210.
- [3] H. Cohen, F. Diaz y Diaz, M. Olivier, *Counting discriminants of number fields*, Journal de Théorie des nombres de Bordeaux **18** (2006), 573-593.
- [4] H. Cohn, *The density of abelian cubic fields*, Proc. Amer. Math. Soc. **5** (1954), 476-477.
- [5] B. N. Delone, D. K. Faddeev, *The theory of irrationalities of the third degree*, Trans. Math. Monographs. vol. **10**. Amer. Math. Soc. Providence. R. I. 1964.
- [6] H. T. Engstrom, *On the common index divisors of an algebraic field*, Trans. Amer. Math. Soc. **32** (1930), 223-237.
- [7] T. Funakura, *On integral bases of pure quartic fields*, Math. J. Okayama Univ. **26** (1984), 27-41.
- [8] I. Gaál, G. Petrányi, *Calculating all elements of minimal index in the infinite parametric family of simplest quartic fields*, Czechoslovak math. Journal **64**(2014), 465-475.
- [9] M. N. Gras, *Table numérique du nombre de classe et des unités des extensions cycliques réelles de degré 4 de \mathbb{Q}* , Publ. Math. Fac. Besanon, fasc **2**, 1977/1978.
- [10] H. Gunji, D. L. McQuillan, *On a class of ideals in an algebraic number field*, J. Number Theory **2** (1970), 207-222.
- [11] H. K. Kim, J. S. Kim, *Computation of the different of the simplest quartic fields*, (Manuscript) 2003.
- [12] A. J. Lazarus, *On the class number and unit index of simplest quartic fields*, Nagoya Math. J. Vol. **121** (1991), 1-13.
- [13] S. Mäki, *On the density of abelian number fields*. Thesis, Helsinki, (1985).
- [14] P. Llorente, E. Nart, *Effective determination of the rational primes in a cubic field*, Proc. Amer. Math. Soc. **87** (1983), 579-585.
- [15] S. R. Louboutin, *The simplest quartic fields with ideal class groups of exponents less than or equal to 2*, J. Math. Soc. Japan **56** (2004), no. 3, 717-727.
- [16] C. R. MacCluer, *Common divisors of values of polynomials*, J. Number Theory **3** (1971), 33-34.
- [17] P. Olajos, *Power integral bases in the family of simplest quartic fields*, Experiment. Math. Vol. **14** (2005), no. 2, 129-132.
- [18] Z.M. Ou, K.S. Williams, *On the density of cyclic quartic fields*, Cand. Math. Bull. Vol. **44** (2001), no.1, 97-104.
- [19] B. K. Spearman, K. S. Williams, *Cubic fields with index 2*, Monatsh. Math. **134** (2002), 331-336.
- [20] _____, _____, *The index of a cyclic quartic field*, Monatsh Math. **140** (2003), 19-70.
- [21] _____, _____, *The prime ideal factorization of 2 in pure quartic fields with index 2*, Math. J. Okayama Univ. **48** (2006), 43-46.

MOHAMMED SEDDIK, UNIVERSITÉ D'ÉVRY VAL D'ESSONNE, LABORATOIRE DE MATHÉMATIQUES ET MODÉLISATION D'ÉVRY (UMR 8071), I.B.G.B.I., 23 BD. DE FRANCE, 91037 ÉVRY CEDEX, FRANCE,
E-mail address: mohammed.seddik@univ-evry.fr