

## ON THE INDICES IN NUMBER FIELDS AND THEIR COMPUTATION FOR SMALL DEGREES.

*Abdelmejid Bayad\* and Mohammed Seddik*

Let  $\mathbb{K}$  be a number field. We investigate the indices  $I(\mathbb{K})$  and  $i(\mathbb{K})$  of  $\mathbb{K}$  introduced respectively by Dedekind and Gunji-McQuillan. Let  $n$  be a positif integer, we then prove that for any prime  $p \leq n$ , there exists  $\mathbb{K}$  a number field of degree  $n$  over  $\mathbb{Q}$  such that  $p$  divide  $i(\mathbb{K})$ . This result is an analogue to Bauer's one for  $i(\mathbb{K})$ . We compute  $I(\mathbb{K})$  and  $i(\mathbb{K})$  for cubic fields and infinite families of simplest number fields of degree less than 7. We solve questions and disprove the conjecture stated in [1].

### 1. INTRODUCTION

Let  $\mathbb{K}$  be a number field of degree  $n$  over  $\mathbb{Q}$  and let  $\mathbb{A}$  be its ring of integers. Denote by  $\hat{\mathbb{A}} = \{\theta \in \mathbb{A} \text{ such that } \mathbb{K} = \mathbb{Q}(\theta)\}$  the set of primitive elements of  $\mathbb{A}$ . For any  $\theta \in \mathbb{A}$  we denote  $F_\theta(x)$  the characteristic polynomial of  $\theta$  over  $\mathbb{Q}$ . Let  $D_{\mathbb{K}}$  be the discriminant of  $\mathbb{K}$ . It is well-known that if  $\theta \in \hat{\mathbb{A}}$ , the discriminant of  $F_\theta(x)$  has the form

$$(1) \quad D(\theta) = I(\theta)^2 D_{\mathbb{K}}$$

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

$$(2) \quad I(\mathbb{K}) = \gcd_{\theta \in \hat{\mathbb{A}}} I(\theta).$$

---

\*Corresponding author. Abdelmejid Bayad

2020 Mathematics Subject Classification: 11R04, 11R33, 12D05, 12E05,  
12E10, 12F05, 12F10, 13F20.

Keywords and Phrases: Common factor of indices, Common divisor of values of polynomials, Ramification, Polynomial, Discriminant.

A prime number  $p$  is called a common index divisor in  $\mathbb{A}$ , if  $p \mid I(\mathbb{K})$ . Dedekind was the first one to show the existence of common divisor of indices. He exhibited an example of a number field of degree 3 in which 2 is a common divisor of indices. Bauer [3] showed that if  $p < n$  then there exists a number field of degree  $n$  in which  $p$  is a common index divisor. Zylinski [26] showed the necessity of this condition, if  $p$  is common index divisor then  $p < n$ . Hensel [13] has given a necessary and sufficient condition on a prime  $p$  to be a common divisor of indices in a number field  $\mathbb{K}$ . This condition depends upon the splitting of the prime  $p$  in  $\mathbb{K}$ , which make Hensel's Theorem not easy to apply in general.

In 1926, Ore [21] conjectured that  $p$ -adic valuation  $v_p(I(\mathbb{K}))$  is not determined only by the splitting type of  $p$  in  $\mathbb{A}$ . Firstly, Engstrom [7] proved that if  $n \leq 7$ , then the splitting type determines the  $p$ -adic valuation  $v_p(I(\mathbb{K}))$ . On the other hand, he gave examples of number fields  $\mathbb{K}_1$  and  $\mathbb{K}_2$  of degree 8 in which the prime 3 has the same splitting type, but  $v_3(I(\mathbb{K}_1)) \neq v_3(I(\mathbb{K}_2))$ . Moreover, Śliwa [23] proved that if  $p$  is not ramified, then  $v_p(I(\mathbb{K}))$  is determined by the splitting type of  $p$  in  $\mathbb{K}$ .

Let  $\theta \in \mathbb{A}$  and  $i(\theta) = \gcd_{x \in \mathbb{Z}} F_\theta(x)$ . Gunji and McQuillan [11] defined the following integer

$$(3) \quad i(\mathbb{K}) = \operatorname{lcm}_{\theta \in \mathbb{A}} i(\theta),$$

and they showed that for  $m$  square free rational integer

$$i(\mathbb{Q}(\sqrt{m})) = \begin{cases} 2 & \text{if } m \equiv 1 \pmod{8}, \\ 1 & \text{otherwise.} \end{cases}$$

MacCluer [19] showed that  $i(\mathbb{K}) > 1$  if and only if there exists a prime number  $p \leq n$  having at least  $p$  distinct prime ideal factors in  $\mathbb{A}$ , each of these primes and only these primes are divisors of  $i(\mathbb{K})$ . Ayad and Kihel [1] prove that there exist a primitive integer  $\theta$  called a good element such that  $i(\mathbb{K}) = i(\theta)$  and an algorithm is given for the computation of such an integer and showed that if  $p$  is a common factor divisor then  $p \mid i(\mathbb{K})$ . The converse is shown to be false in general. However, the following result is proved. Suppose that  $\mathbb{K}$  is a Galois extension of degree  $n$  over  $\mathbb{Q}$ . Let  $1 \leq d < n$  be the greatest divisor of  $n$  and let  $p > d$  be a prime number,  $p \neq n$ , then  $p$  is a common index divisor if and only if  $p \mid i(\mathbb{K})$ . As a consequence, we obtain that if  $\mathbb{K}/\mathbb{Q}$  is cyclic of prime degree  $l$ , then a prime  $p \neq l$  is a common index divisor if and only if  $p \mid i(\mathbb{K})$ .

In [1] the authors ask the following question : suppose that the splitting of  $p$  in  $\mathbb{K}$  as a product of prime ideals is given by  $p\mathbb{A} = P_1^{e_1} \cdots P_r^{e_r}$ , where  $r \geq p$ . Let  $f_i$  be the inertial degree of the ideal  $P_i$ , for  $i = 1, \dots, r$ . Can one compute  $v_p(i(\mathbb{K}))$  in terms of integers  $r$ ,  $e_i$  and  $f_i$ . In other words, is  $v_p(i(\mathbb{K}))$  completely determined by splitting type of  $p$  ?

In this paper we prove that  $v_p(i(\mathbb{K}))$  is not completely determined by the splitting type of  $p$ . For  $\mathbb{K}_1 = \mathbb{Q}(\theta) : \theta^6 - 16\theta^5 - 55\theta^4 - 20\theta^3 + 40\theta^2 + 22\theta + 1 = 0$

and  $\mathbb{K}_2 = \mathbb{Q}(\theta) : \theta^6 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + \theta + 1 = 0$ , are number fields of degree 6, we prove that the prime 2 has the same splitting type  $P_1P_2$  in  $\mathbb{K}_i$ ,  $i = 1, 2$  and  $v_2(i(\mathbb{K}_1)) = 4$ ,  $v_2(i(\mathbb{K}_2)) = 3$  (see example 1).

They also showed that for  $\mathbb{K}_1$  and  $\mathbb{K}$  be number fields such that  $\mathbb{K}_1 \subseteq \mathbb{K}$  and  $m = [\mathbb{K} : \mathbb{K}_1]$ , then  $mv_p(i(\mathbb{K}_1)) \leq v_p(i(\mathbb{K}))$ . We show that the following statements are not equivalent (see example 2):

1.  $mv_p(i(\mathbb{K}_1)) = v_p(i(\mathbb{K}))$ ,
2. For any integer  $\beta$  of  $\mathbb{K}$ , if  $v_p(i(\beta)) = v_p(i(\mathbb{K}))$ , then there exists an integer  $\alpha$  of  $\mathbb{K}_1$  such that  $\beta \equiv \alpha \pmod{p}$ .

This gives answer to the question 2 in [1].

Let  $p$  be a prime number dividing  $i(\mathbb{K})$ , say  $\rho_{\mathbb{K}}(p)$  the number of  $\bar{\theta} \in \mathbb{A}/p\mathbb{A}$  such that  $p \mid i(\theta)$ . Ayad and Kihel prove the following result [1, Theorem 11]: let  $p$  be a prime number and let  $n \geq 2$  be an integer. Let  $\mathbb{K}_1$  and  $\mathbb{K}_2$  be two Galois extensions of  $\mathbb{Q}$  of the same degree  $n$ . Suppose that  $\rho_{\mathbb{K}_1}(p) = \rho_{\mathbb{K}_2}(p) \neq 0$  and the ramification indices of  $p$  in the two fields are the same. Then  $p$  has the same splitting type in  $\mathbb{K}_1$  and  $\mathbb{K}_2$ .

Then they make the following conjecture in [1] : let  $\mathbb{K}$  be a Galois number field and  $p$  a prime number such that  $p \mid i(\mathbb{K})$ . Then  $\rho_{\mathbb{K}}(p)$  determines the splitting type of  $p$  in  $\mathbb{K}$ . Unfortunately the statement of [1, Theorem 11] is false.

Also the conjecture stated above is not true. Thanks to the following example : we consider the two Galois number fields  $\mathbb{K}_1 = \mathbb{Q}(\sqrt{5}, \sqrt{-3})$  and  $\mathbb{K}_2 = \mathbb{Q}(\sqrt{17}, \sqrt{-7})$  where  $\rho_{\mathbb{K}_1}(2) = \rho_{\mathbb{K}_2}(2) = 6$ , the splitting type in  $\mathbb{K}_1$  is  $P_1P_2$  and in  $\mathbb{K}_2$  is  $P_1P_2P_3P_4$  (see example 3).

## 2. MAIN RESULTS

We now state the main results of this paper.

**Theorem 1.** *Let  $n$  be a positif integer and  $p$  a prime number.*

*If  $p \leq n$  then, there exists a number field  $\mathbb{K}$  of degree  $n$  in which  $p \mid i(\mathbb{K})$ .*

This result is the analogue for  $i(\mathbb{K})$  of Bauer's result [3].

Now we will compute  $i(\mathbb{K})$  for any cubic number fields. Let  $\mathbb{K}$  be a cubic field. We can suppose that  $\mathbb{K} = \mathbb{Q}(\theta)$ , where  $\theta$  is a root of an irreducible polynomial of the type

$$f(x) = x^3 - ax + b, \quad a, b \in \mathbb{Z}.$$

The discriminant of  $f(x)$  is  $\Delta = 4a^3 - 27b^2$ . If for any prime number  $p$  we have

$$v_p(a) \geq 2 \quad \text{and} \quad v_p(b) \geq 3$$

then  $\theta/p$  is an algebraic integer whose equation is  $x^3 - (a/p^2)x + b/p^3 = 0$ . Therefore, we can assume that for any prime number  $p$ ,

$$v_p(a) < 2 \quad \text{or} \quad v_p(b) < 3.$$

We denote by  $(P)$  the following property

$$(P) : \quad (a \equiv 3 \pmod{9}, b^2 \equiv a + 1 \pmod{27}, v_3(\Delta) > 6 \text{ even}, v_3(\Delta) \equiv 1 \pmod{3}) \\ \text{or } (a \equiv 1 \pmod{3}, 3 \mid b).$$

It is well-known that if  $\mathbb{K}$  is a cubic field, then  $I(\mathbb{K}) = 1$  or  $2$ . Llorente and Nart [16, Theorem 4] give a necessary and sufficient condition for which  $I(\mathbb{K}) = 2$ . Next, we state result which is an analogue of Llorente and Nart's theorem.

**Theorem 2.** *Let  $\mathbb{K}$  be a cubic field. Then we have*

$i(\mathbb{K})$	Splitting type of 2	Splitting type of 3
1	$P, P^3$	$P, P^3, PQ, PQ^2$
2	$PQ, PQ^2, PQR$	$P, P^3, PQ, PQ^2$
3	$P, P^3$	$PQR$
6	$PQ, PQ^2, PQR$	$PQR$

Basically, the above theorem is equivalent to

**Theorem 3.** *Let  $\mathbb{K} = \mathbb{Q}(\theta)$ ,  $\theta^3 - a\theta + b = 0$ , be a cubic field. Then  $i(\mathbb{K})$  is given by the formula*

$$i(\mathbb{K}) = 2^\alpha 3^\beta$$

where

$$\alpha = \begin{cases} 1 & \text{if } 1 = v_2(a) < v_2(b) \text{ or } a \not\equiv b \pmod{2}, \\ 0 & \text{else,} \end{cases}$$

$$\beta = \begin{cases} 1 & \text{if } (P) \text{ is true,} \\ 0 & \text{else.} \end{cases}$$

As a particular case of the above result, we get  $i(\mathbb{K})$  for any  $\mathbb{K}$  a pure cubic field.

**Corollary 1.** *Let  $\mathbb{Q}(\sqrt[3]{d})$  be an pure cubic field, then*

$$i(\mathbb{Q}(\sqrt[3]{d})) = \begin{cases} 2 & \text{if } d \text{ odd,} \\ 1 & \text{if } d \text{ even.} \end{cases}$$

Let us consider the family of cyclic cubic fields  $\mathbb{L}_m$  generated by some root of the polynomial  $l_m(x) = x^3 - mx^2 - (m+3)x - 1$ . This family was discussed by Shanks [24] and Jager [14, p 63-73], in order to study their class numbers and lower bounds for regulators. In the following we compute their indices  $I(\mathbb{L}_m)$  and  $i(\mathbb{L}_m)$ .

**Theorem 4.** *We have  $I(\mathbb{L}_m) = 1$  and*

$$i(\mathbb{L}_m) = \begin{cases} 3 & \text{if } m \equiv 39, 120, 201 \pmod{243}, \\ 1 & \text{otherwise.} \end{cases}$$

Now, we consider the family of cyclic quartic fields  $\mathbb{K}_m$ . For  $m \in \mathbb{Z}$  with  $m \notin \{0, \pm 3\}$  let  $P_m(x) = x^4 - mx^3 - 6x^2 + mx + 1$ . Let  $\theta$  be a root of  $P_m(x)$ , then each field in infinite parametric family of number fields  $\mathbb{K}_m = \mathbb{Q}(\theta)$  is called a simplest quartic field. If  $m \notin \{0, \pm 3\}$  then  $P_m(x)$  is irreducible over  $\mathbb{Q}$  and defined a totally real cyclic number field of degree 4, see [8, Proposition 6]. In that paper M. N. Gras give numerical type for the class numbers and found their units.

**Theorem 5.** *Assume that  $m \geq 1$  and that the odd part of  $\Delta_m = m^2 + 16$  is square-free. Then we have*

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

$$i(\mathbb{K}_m) = \begin{cases} 1 & \text{if } 1 \leq v_2(m) \leq 3, \\ 4 & \text{otherwise.} \end{cases}$$

Let us consider the family of quintic fields  $\mathbb{H}_m$  generated by some root of the polynomial  $h_m(x) = x^5 + m^2x^4 - (2m^3 + 6m^2 + 10m + 10)x^3 + (m^4 + 5m^3 + 11m^2 + 15m + 5)x^2 + (m^3 + 4m^2 + 10m + 10)x + 1$ . In [17], Emma Lehmer showed that the polynomial  $h_m(x)$  defines quintic cyclic real extension of  $\mathbb{Q}$  and constructed a parametric family of units of prime conductor  $p = m^4 + 5m^3 + 15m^2 + 25m + 25$ . Later R. Schoof and L. Washington [25] showed that these units are fundamental units of the quintic fields  $\mathbb{H}_m$ . Recently, H. Darmon [6] observed that the Lehmer's family comes from the covering of modular curves  $X_1(25) \rightarrow X_0(25)$ . In the following we compute their indices  $I(\mathbb{H}_m)$  and  $i(\mathbb{H}_m)$ .

**Theorem 6.** *(Lehmer's quintics) Let  $m \in \mathbb{Z}$  and suppose that  $p^2 \nmid m^4 + 5m^3 + 15m^2 + 25m + 25$  for any prime  $p \neq 5$ . Then we have  $I(\mathbb{H}_m) = 1$  and*

$$i(\mathbb{H}_m) = \begin{cases} 5 & \text{if } m \equiv 2 \pmod{5}, \\ 1 & \text{otherwise.} \end{cases}$$

Now, we consider the family of cyclic sextic fields  $\mathbb{S}_m$ . Assume that  $m \neq -8, -5, -3, 0$ . Let us consider the family of sextic cyclic fields  $\mathbb{S}_m$  generated by some root of the polynomial

$$s_m(x) = x^6 - 2mx^5 - (5m + 15)x^4 - 20x^3 + 5mx^2 + (2m + 6)x + 1.$$

This family of fields is called the simplest sextic fields, having a couple of nice properties, detailed in G. Lettl, A. Petho and P. Voutier [18]. Among others these

fields are totally real cyclic fields. These fields contained the simplest cubic fields  $\mathbb{L}_m$  defined by Shanks [24]. Recently, Gaal [9] found an explicit integral basis of  $\mathbb{S}_m$  and proved that  $\mathbb{S}_m$  are not monogenic except for a few values of  $m = -4, -2, -1, 1$ . In the following we give their indices  $I(\mathbb{S}_m)$  and  $i(\mathbb{S}_m)$ .

**Theorem 7.** *For  $m \neq -8, -5, -3, 0$ , we have  $I(\mathbb{S}_m) = 1$  and  $i(\mathbb{S}_m) = 2^\alpha 3^\beta$  where*

$$\alpha = \begin{cases} 3 \text{ or } 4 & \text{if } m \equiv 0, 5, 8, 13, 16, 21 \pmod{24}, \\ 0 & \text{else,} \end{cases}$$

$$\beta = \begin{cases} 2 & \text{if } m \equiv 39, 120, 201 \pmod{243}, \\ 0 & \text{else.} \end{cases}$$

### 3. PROOF OF MAIN RESULTS:

Before proving our main results, we state some auxiliary results.

It is known that the polynomials  $\binom{x}{0} = 1$  and  $\binom{x}{k} = x(x-1)\cdots(x-(k-1))$  for  $k = 1, \dots, n$ , form a basis of the vector space over  $\mathbb{Q}$  whose elements are the polynomials of degree  $\leq n$ . This basis is useful for the enunciation of the following.

**Theorem 8** ([1]. Theorem 1). *There exists an element  $\theta \in \widehat{\mathbb{A}}$  whose characteristic polynomial*

$$F_\theta(x) = a_0 + a_1 \binom{x}{1} + \cdots + a_n \binom{x}{n}, \quad a_i \in \mathbb{Z}, a_n = 1,$$

satisfies

$$i(\mathbb{K}) = i(\theta) = \gcd_{j=0}^n (j!a_j).$$

**Corollary 2.** *We deduce from Theorem 8 that*

$$i(\mathbb{K}) \mid n!.$$

Now, we need to prove the following lemma.

**Lemma 1.** *Let  $n \in \mathbb{N}$  be a odd integer and  $p$  a prime number. The polynomial  $\binom{x}{n} + p$  is irreducible in  $\mathbb{Z}[x]$ .*

*Proof.* Assume that  $\binom{x}{n} + p$  is reducible in  $\mathbb{Z}[x]$ . Writing that  $\binom{x}{n} + p = Q(x)R(x)$  with  $1 \leq \deg(Q) \leq n-1$  and  $1 \leq \deg(R) \leq n-1$ . We then have  $|Q(i)||R(i)| = p$ ,  $\forall i = 0, \dots, n-1$ , this implies that  $(|Q(i)|, |R(i)|) = (1, p)$  or  $(p, 1)$ . The number of  $i$  such that  $(|Q(i)|, |R(i)|) = (1, p)$  (resp  $(|Q(i)|, |R(i)|) = (p, 1)$ ) is less than or equal to  $\min(\deg(Q), \deg(R))$ . So we have  $n \leq 2 \times \min(\deg(Q), \deg(R)) \leq \deg(Q) + \deg(R) = n$ . Hence  $\deg(Q) = \deg(R) = \frac{n}{2}$ , which is a contradiction with the fact that  $n$  is odd. Thus the claim is proved.  $\square$

*Proof of Theorem 1:* For  $p < n$ , according to Bauer [3] there exists a number field  $\mathbb{K}$  of degree  $n$  such that  $p \mid I(\mathbb{K})$ . On the other hand, by [1, Theorem 4] there exists a number field  $\mathbb{K}$  of degree  $n$  such that  $p \mid i(\mathbb{K})$ . If  $p = n$ , by Lemma 1 and Theorem 8 the following number field

$$\mathbb{K} = \mathbb{Q}(\theta), \theta(\theta - 1) \cdots (\theta - (p - 1)) + p = 0$$

satisfies  $i(\theta) = \gcd(p, p!) = p$ . Thanks to  $i(\mathbb{K}) = \text{lcm}_{\theta \in A} i(\theta)$ , we have  $p \mid i(\mathbb{K})$ .

**Lemma 2** ([22], Lemma 2.1). *Let  $\mathbb{K}$  be a cyclic cubic field. Let  $x^3 + ax + b$  be a defining polynomial for  $\mathbb{K}$  and suppose that  $v_2(a) < 2$  or  $v_2(b) < 3$ . Then*

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

*Proof of Theorem 3:* By Corollary 2 we have  $i(\mathbb{K}) \mid 6$ . So the possible values of  $i(\mathbb{K})$  are 1, 2, 3 or 6. Moreover, we have

1. By [16, Theorem 1], the condition :  $1 = v_2(a) < v_2(b)$  or  $a \not\equiv b \pmod{2}$  is equivalent to  $\langle 2 \rangle$  having a least 2 distinct prime ideal factors in  $\mathbb{A}$ . Hence, by MacCluer [19] we have  $2 \mid i(\mathbb{K})$ .
2. By [16, Theorem 1], the condition :  $(a \equiv 1 \pmod{3}, 3 \mid b)$  or  $(a \equiv 3 \pmod{9}, b^2 \equiv a + 1 \pmod{27}, s_3 > 6 \text{ even}, v_3(\Delta) \equiv 1 \pmod{3})$  is equivalent to  $\langle 3 \rangle$  is totally split [16, Theorem 1]. Hence, by MacCluer [19] we have  $3 \mid i(\mathbb{K})$ .

Thus complete the proof of Theorem 3.

*Proof of Corollary 1:* Immediate consequence of Theorem 3.

*Proof of Theorem 4:* Let  $\mathbb{L}_m = \mathbb{Q}(\theta)$  such that  $\theta^3 - A\theta + B = 0$ ,  $A = 3(9 + 3m + m^2)$  and  $B = -27 - 27m - 9m^2 - 2m^3$ . We can see that  $B \equiv 1 \pmod{2}$ , so by Lemma 2 we have  $I(\mathbb{L}_m) = 1$  and by Theorem 3, we obtain  $2 \nmid i(\mathbb{L}_m)$ . By [16, Theorem 1] we conclude that  $\langle 2 \rangle$  is inert in  $\mathbb{L}_m$ . On the other hand, we have

1. If  $3 \nmid m$ , we get  $3 \nmid B$ . By Theorem 3, we obtain  $i(\mathbb{L}_m) = 1$ .
2. If  $3 \mid m$ , put  $m = 3k$ , then  $\theta/3$  is an algebraic integer. Then the number field  $\mathbb{L}_m$  is defined by the equation  $x^3 - A'x + B' = 0$  where  $A' = 3(1 + k + k^2)$ ,  $B' = -(1 + 3k + 3k^2 + 2k^3)$  and  $\Delta = 3^4(k^2 + k + 1)^2$ . Moreover, we have
  - (a) If  $k \not\equiv 1 \pmod{3}$ , we have  $v_3(A') = 1$ ,  $v_3(B') = 0$  and  $v_3(\Delta) = 4$ , so by Theorem 3, we obtain  $i(\mathbb{L}_m) = 1$ .
  - (b) If  $k \equiv 1 \pmod{3}$ , put  $k = 3k' + 1$ , the equation of  $\mathbb{L}_m$  is given by  $\theta^3 - 3^2(3k'^2 + 3k' + 1)\theta - (54k'^3 + 81k'^2 + 45k' + 9) = 0$ . If  $k' \not\equiv 1 \pmod{3}$ , we have  $54k'^3 + 81k'^2 + 45k' + 9 \not\equiv 0 \pmod{27}$ . Then by Theorem 3, we get  $i(\mathbb{L}_m) = 1$ .

Now we suppose  $k' \equiv 1 \pmod{3}$ , we have  $v_3(3^2(3k'^2 + 3k' + 1)) = 2$  and  $v_3(54k'^3 + 81k'^2 + 45k' + 9) \geq 3$  :

- i. If  $k' \equiv 4, 13, 22 \pmod{27}$  ( $m \equiv 39, 120, 201 \pmod{243}$ ), we have  $54k'^3 + 81k'^2 + 45k' + 9 \equiv 0 \pmod{81}$ , so we get the equation of  $\mathbb{L}_m$  is given by

$$\theta^3 - (1 + 3k' + 3k'^2)\theta - \frac{54k'^3 + 81k'^2 + 45k' + 9}{27} = 0.$$

We note that  $1 + 3k' + 3k'^2 \equiv 1 \pmod{3}$ , and 3 divide  $(54k'^3 + 81k'^2 + 45k' + 9)/27$ . Then by Theorem 3, we get  $i(\mathbb{L}_m) = 3$ .

- ii. If  $k' \equiv 1, 7, 10, 16, 19, 25 \pmod{27}$  ( $m \equiv 12, 66, 93, 150, 174, 228 \pmod{243}$ ), we have  $27 \parallel 54k'^3 + 81k'^2 + 45k' + 9$ , so we get  $\mathbb{L}_m$  by equation

$$\theta^3 - (1 + 3k' + 3k'^2)\theta - \frac{54k'^3 + 81k'^2 + 45k' + 9}{27} = 0,$$

and by Theorem 3, we get  $i(\mathbb{L}_m) = 1$ .

This completes the proof of Theorem 4.

Before proving Theorem 5 we need to recall next Lemmas.

**Lemma 3** ([8]. Proposition 8). *Assume that  $m \geq 1$  and that the odd part of  $\Delta_m = m^2 + 16$  is square-free. Let  $f_{\mathbb{K}_m}$  and  $f_{k_m}$  denote the conductors of the simplest quartic field  $\mathbb{K}_m$  and of its real quadratic subfield  $k_m$ . Then*

$$(f_{\mathbb{K}_m}, f_{k_m}) = \begin{cases} (\Delta_m, \Delta_m) & \text{if } m \equiv 1 \pmod{2}, \\ (\Delta_m, \Delta_m/4) & \text{if } m \equiv 2 \pmod{4}, \\ (\Delta_m/2, \Delta_m/4) & \text{if } m \equiv 4 \pmod{8}, \\ (\Delta_m/2, \Delta_m/16) & \text{if } m \equiv 0 \pmod{8}. \end{cases}$$

**Lemma 4** ([15]). *An integral basis of  $\mathbb{K}_m$  is given by as follows*

$$\mathbb{A} = \begin{cases} \mathbb{Z}[1, \theta, \theta^2, \frac{1+\theta^3}{2}] & \text{if } v_2(m) = 0, \\ \mathbb{Z}[1, \theta, \frac{1+\theta^2}{2}, \frac{\theta+\theta^3}{2}] & \text{if } v_2(m) = 1, \\ \mathbb{Z}[1, \theta, \frac{1+\theta^2}{2}, \frac{1+\theta+\theta^2+\theta^3}{4}] & \text{if } v_2(m) = 2, \\ \mathbb{Z}[1, \theta, \frac{1+2\theta-\theta^2}{4}, \frac{1+\theta+\theta^2+\theta^3}{4}] & \text{if } v_2(m) \geq 3. \end{cases}$$

*Proof of Theorem 5:* Let  $m \in \mathbb{Z}$  with  $m \neq 0, \pm 3$  and suppose the  $m^2 + 16$  is not divisible by an odd square. Consider a simplest quartic fields  $\mathbb{K}_m = \mathbb{Q}(\theta)$ ,  $\theta^4 - m\theta^3 - 6\theta^2 + m\theta + 1 = 0$ . We have  $D(\theta) = 4 \cdot \Delta_m^3$  where  $\Delta_m = m^2 + 16$ .

1. Let  $f_{\mathbb{K}_m}$  and  $f_{k_m}$  denote the conductors of the simplest quartic field  $\mathbb{K}_m$  and of its real quadratic subfield  $k_m$ . Then we have  $D(\mathbb{K}_m) = f_{k_m} \cdot f_{\mathbb{K}_m}^2$  and by Lemma 3 and by equation (1), we get  $3 \nmid I(\theta)$ . The Dedekind's theorem [4, §18] gives explicitly the factorization of 3 using  $\theta$ , namely  $P_m(x) = x^4 - mx^3 - 6x + 1$



the minimal polynomial of  $\theta$ , so we have

$$\begin{aligned} P_0(x) &\equiv (x^2 + x + 2)(x^2 + 2x + 2) \pmod{3}, \\ P_1(x) &\equiv x^4 + 2x^3 + x + 1 \pmod{3}, \\ P_2(x) &\equiv x^4 + x^3 + 2x + 1 \pmod{3}, \end{aligned}$$

so the possibilities of splitting type of  $\langle 3 \rangle$  are

$$\langle 3 \rangle = \begin{cases} \langle 3, \theta^2 + \theta^2 + 2 \rangle \langle 5, \theta^2 + 2\theta + 2 \rangle & \text{if } m \equiv 0 \pmod{3}, \\ \langle 3, \theta^4 + 2\theta^3 + \theta + 1 \rangle & \text{if } m \equiv 1 \pmod{3}, \\ \langle 3, \theta^4 + \theta^3 + 2\theta + 1 \rangle & \text{if } m \equiv 2 \pmod{3}. \end{cases}$$

So by Engstrom [7], we get  $v_3(I(\mathbb{K}_m)) = 0$  and by MacCluer [19], we have  $v_3(i(\mathbb{K}_m)) = 0$ .

2. If  $v_2(m) = 0$ , by Lemma 4 an integral basis of  $\mathbb{K}_m$  is given by  $\{1, \theta, \theta^2, \frac{1+\theta^3}{2}\}$ . We have  $D(1, \theta, \theta^2, \frac{1+\theta^3}{2}) = \frac{1}{4}D(1, \theta, \theta^2, \theta^3) = \frac{D(\theta)}{4} = \Delta_m^3$ . By Lemma 3, we have  $D(\mathbb{K}_m) = f_{k_m} \cdot f_{\mathbb{K}_m}^2 = \Delta_m^3$  and by equation (1), we get  $I(\theta) = 2$ . Denote  $k_m = \mathbb{Q}(\sqrt{\Delta_m})$  be a real quadratic subfield of  $\mathbb{K}_m$  of discriminant  $D(k_m) = \Delta_m \equiv 1 \pmod{8}$ . Then, the splitting type of 2 in  $k_m$  is  $P_1P_2$ . In this case, we have  $2 \nmid D(\mathbb{K}_m)$ , then the splitting type of 2 in  $\mathbb{K}_m$  are

$$P_1P_2 \text{ or } P_1P_2P_3P_4.$$

We claim that  $\langle 2 \rangle = P_1P_2$  in  $\mathbb{K}_m$ .

Suppose that the splitting of 2 is  $P_1P_2P_3P_4$ , so by Engstrom [7], we have  $I(\mathbb{K}_m) = 4$ . This gives contradiction with  $I(\theta) = 2$ . Then the splitting type of 2 in  $\mathbb{K}_m$  is  $P_1P_2$  and by Engstrom [7], we obtain  $I(\mathbb{K}_m) = 2$ .

By [11, 1] we get  $i(k_m) = 2$  and  $4 \mid i(\mathbb{K}_m)$ . Let us show that  $i(\mathbb{K}_m) = 4$ . Take  $\varphi = x_1 + x_2\theta + x_3\theta^2 + x_4\frac{1+\theta^3}{2}$  and the characteristic polynomials of  $\varphi$  can be written as follows

$$F_\varphi(x) = a_0 + a_1 \binom{x}{1} + a_2 \binom{x}{2} + a_3 \binom{x}{3} + \binom{x}{4}$$

By the algorithm [1, p.1187], we get  $(a_0, a_1, a_2, a_3) \not\equiv (0, 0, 0, 0) \pmod{8}$  for any  $x_i \in \{0, \dots, 7\}, i = 1, \dots, 4$ . Then we have  $8 \nmid i(\mathbb{K}_m)$ , and we deduce that  $i(\mathbb{K}_m) = 4$ .

3. If  $v_2(m) = 1$ , by Lemma 3, we have  $f_{\mathbb{K}_m} = \Delta_m$  and  $f_{k_m} = \Delta_m/4$  and  $D(\mathbb{K}_m) = f_{k_m} \cdot f_{\mathbb{K}_m}^2 = \Delta_m^3/4$ . By Lemma 4, an integral basis of  $\mathbb{K}_m$  is given by  $\{1, \theta, \frac{1+\theta^2}{2}, \frac{\theta+\theta^3}{2}\}$ . Take  $\varphi = \frac{1+\theta^2}{2} \in \mathbb{A}$ , we have  $D(\varphi) = \frac{m^4}{24}\Delta_m^3 \neq 0$ , so the characteristic polynomial of  $\varphi$  is given by

$$F_\varphi(x) = x^4 - \left(\frac{1}{2}m^2 + 8\right)x^3 + \left(\frac{5}{4}m^2 + 20\right)x^2 - (m^2 + 16)x + \frac{1}{4}m^2 + 4$$

is separable over  $\mathbb{Q}$  and then  $\varphi \in \widehat{\mathbb{A}}$ . By equation (1) we have  $I(\theta) = m^2/4$  and  $2 \nmid I(\theta)$ . Then the Dedekind's theorem [4, §18] gives the factorization of 2 in  $\mathbb{K}_m$ . We have  $F_\varphi(x) \equiv (x^2 + x + 1)^2 \pmod{2}$  and  $\langle 2 \rangle = P^2$ . Then by MacCluer [19], we get  $i(\mathbb{K}_m) = 1$  and by Engstrom [7], we obtain  $I(\mathbb{K}_m) = 1$ .

4. If  $v_2(m) = 2$ , put  $m = 4t$  with  $v_2(t) = 0$ , then by Lemma 3 we have  $f_{\mathbb{K}_m} = \Delta_m/2$ ,  $f_{k_m} = \Delta_m/4$  and  $D(\mathbb{K}_m) = f_{k_m} \cdot f_{\mathbb{K}_m}^2 = \Delta_m^3/16$ . By Lemma 4, an integral basis of  $\mathbb{K}_m$  is given by  $\{1, \theta, \frac{1+\theta^2}{2}, \frac{1+\theta+\theta^2+\theta^3}{4}\}$ . Take  $\varphi = \frac{5-\theta+5\theta^2-\theta^3}{4} \in \mathbb{A}$ , we have

$$D(\varphi) = \frac{1}{2^{20}}(m^2 + 5m - 32)^2(21m^4 - 220m^3 + 880m^2 - 1600m + 1088)^2\Delta_m^3 \neq 0$$

and the characteristic polynomial of  $\varphi$  is given by

$$\begin{aligned} F_\varphi(x) = & x^4 + \left(\frac{1}{4}m^3 - \frac{5}{4}m^2 + 4m - 20\right)x^3 + \left(108 - 25m + \frac{27}{4}m^2 - \frac{25}{16}m^3\right)x^2 \\ & + \left(\frac{49}{16}m^3 - \frac{25}{2}m^2 + 49m - 200\right)x - \frac{15}{8}m^3 + \frac{119}{16}m^2 - 30m + 119 \end{aligned}$$

is separable over  $\mathbb{Q}$  and then  $\varphi \in \widehat{\mathbb{A}}$ . By equation (1) we have

$$I(\theta) = (4t^2 + 5t - 8)(84t^4 - 220t^3 + 220t^2 - 100t + 17),$$

this gives  $2 \nmid I(\theta)$ . Then Dedekind's theorem [4, §18] gives explicitly the factorization of 2 in  $\mathbb{K}_m$ ,  $F_\varphi(x) \equiv x^4 \pmod{2}$  and  $\langle 2 \rangle = P^4$ . Then by MacCluer [19], we get  $i(\mathbb{K}_m) = 1$  and by Engstrom [7] we have  $I(\mathbb{K}_m) = 1$ .

5. If  $v_2(m) \geq 3$ , consider  $\varphi = \frac{2+7\theta+\theta^3}{4} \in \mathbb{A}$ , the minimal polynomial of  $\varphi$  is given by

$$\begin{aligned} P_\varphi(x) = & x^4 - \left(\frac{1}{4}m^3 + \frac{11}{2}m + 2\right)x^3 + \left(\frac{3}{8}m^3 - \frac{47}{16}m^2 + \frac{33}{4}m - 59\right)x^2 \\ & + \left(\frac{13}{16}m^3 + \frac{47}{16}m^2 + \frac{61}{4}m + 60\right)x - \frac{15}{32}m^3 + \frac{65}{64}m^2 - 9m + 18 \end{aligned}$$

with

$$D(\varphi) = \frac{1}{2^{16}}(64m^4 + 2135m^2 + 18032)^2(m^2 + 16)^3(m^2 + 18)^2 \neq 0.$$

By Lemma 3, we have  $D(\mathbb{K}_m) = \frac{\Delta_m^3}{2^6}$ . Then by the equation (1), we obtain

$$I(\varphi) = \frac{1}{2^5}(64m^4 + 2135m^2 + 18032)(m^2 + 18).$$

Therefore, we have

$$\frac{1}{2^5}(64m^4 + 2135m^2 + 18032)(m^2 + 18) \equiv 1 \pmod{2}.$$

This implies that  $\varphi$  is primitive integer and  $2 \nmid I(\varphi)$ . Dedekind's theorem [4, §18] gives explicitly the factorization of 2 using the minimal polynomial of  $\varphi$ . For that we consider two cases :

5.1. For  $v_2(m) = 3$ , we get  $P_\varphi(x) \equiv (x^2 + x + 1)^2 \pmod{2}$  and then we have

$$2\mathbb{A} = \langle 2, \varphi^2 + \varphi + 1 \rangle^2,$$

so by MacCluer [19], we get  $i(\mathbb{K}_m) = 1$  and by Engstrom [7], we have  $I(\mathbb{K}_m) = 1$ .

5.2. For  $v_2(m) \geq 4$ , we get  $P_\varphi(x) \equiv x^2(x+1)^2 \pmod{2}$  and

$$\begin{aligned} 2\mathbb{A} &= \langle 2, \varphi \rangle^2 \langle 2, \varphi + 1 \rangle^2, \\ 2\mathbb{A} &= \langle 2, \frac{2 + 7\theta + \theta^3}{4} \rangle^2 \langle 2, \frac{5 + 7\theta + \theta^3}{4} \rangle^2. \end{aligned}$$

Then we can write  $m = 16t$  with  $t \in \mathbb{Z}^*$ . Let us show that  $i(\mathbb{K}_m) = 4$ . For  $\psi = \frac{2+3\theta+\theta^3}{4} \in \mathbb{A}$ , we have  $D(\psi) = 1024(16t^2 + 1)^7(4096t^2 + 175)^2 \neq 0$  and it's characteristic polynomial is given by

$$\begin{aligned} F_\psi(x) &= x^4 - (1024t^3 + 72t + 2)x^3 + (1536t^3 - 432t^2 + 108t - 27)x^2 \\ &\quad + (256t^3 + 432t^2 + 12t + 38)x - 384t^3 - 60t^2 - 24t - 4 \end{aligned}$$

is separable over  $\mathbb{Q}$ . Therefore we have  $\psi \in \widehat{\mathbb{A}}$ . The characteristic polynomial of  $\psi$  can be written as follows

$$F_\psi(x) = a_0 + a_1 \binom{x}{1} + a_2 \binom{x}{2} + a_3 \binom{x}{3} + \binom{x}{4}$$

with

$$\begin{aligned} a_0 &= -384t^3 - 60t^2 - 24t - 4 \equiv 0 \pmod{4}, \\ a_1 &= -3328t^3 + 864t^2 - 240t + 80 \equiv 0 \pmod{4}, \\ 2a_2 &= 9216t^3 - 864t^2 + 648t - 100 \equiv 0 \pmod{4}, \\ 6a_3 &= -6144t^3 - 432t + 24 \equiv 0 \pmod{4}. \end{aligned}$$

This gives  $i(\psi) = \gcd(a_0, a_1, 2a_2, 6a_3, 24) = 4$ . On the other hand by taking  $\phi = x_1 + x_2\theta + x_3\frac{1+2\theta-\theta^2}{4} + x_4\frac{1+\theta+\theta^2+\theta^3}{4}$  where  $x_i \in \{0, \dots, 7\}, i = 1, \dots, 4$  with  $4 \mid i(\phi)$ . Thanks to the algorithm [1, p.1187], we get  $a_2 \equiv 4 \pmod{8}$ . Hence we obtain  $8 \nmid i(\phi)$ , then we get  $8 \nmid i(\mathbb{K}_m)$ . Hence  $i(\mathbb{K}_m) = i(\psi) = 4$ . This completes the proof of Theorem 5.

*Proof of Theorem 6:* Let  $m \in \mathbb{Z}$ . Consider a simplest quintic fields generated by some root of the polynomial  $h_m(x) = x^5 + m^2x^4 - (2m^3 + 6m^2 + 10m + 10)x^3 +$

$(m^4 + 5m^3 + 11m^2 + 15m + 5)x^2 + (m^3 + 4m^2 + 10m + 10)x + 1$ . Suppose that  $p^2 \nmid m^4 + 5m^3 + 15m^2 + 25m + 25$  for any prime  $p \neq 5$ . We have

$$D(h_m) = (m^3 + 5m^2 + 10m + 7)^2(m^4 + 5m^3 + 15m^2 + 25m + 25)^4.$$

By [10], the discriminant of field  $\mathbb{H}_m$  is given by  $D_{\mathbb{H}_m} = (m^4 + 5m^3 + 15m^2 + 25m + 25)^4$ . Furthermore, by equation (1), we have  $I(\theta) = m^3 + 5m^2 + 10m + 7$ . We obtain

$m \bmod 2$	$I(\theta) \bmod 2$	$h_m(x) \bmod 2$	splitting type of 2
0	1	$x^5 + x^2 + 1$	inert
1	1	$x^5 + x^4 + x^2 + x + 1$	inert

$m \bmod 3$	$I(\theta) \bmod 3$	$h_m(x) \bmod 3$	splitting type of 3
0	1	$x^5 + 2x^3 + 2x^2 + x + 1$	inert
1	2	$x^5 + x^4 + 2x^3 + x^2 + x + 1$	inert
2	1	$x^5 + x^4 + 2x^3 + 1$	inert

$m \bmod 5$	$I(\theta) \bmod 5$	$h_m(x) \bmod 5$	splitting type of 5
0	2	$(x + 1)^5$	completely ramified
1	3	$x^5 + x^4 + 2x^3 + 2x^2 + x + 1$	inert
2	0	$(x + 1)(x + 2)(x + 3)(x + 4)^2$	split completely
3	4	$x^5 + 4x^4 + 2x^3 + 3x + 1$	inert
4	1	$x^5 + x^4 + x^3 + 2x^2 + 3x + 1$	inert

In the case  $m \equiv 2 \pmod 3$  we have  $I(\theta) \equiv 0 \pmod 5$ . Thus we can not apply Dedekind's theorem [4, §18]. To determine the splitting type of 5 we deduce that

$$P_1 P_2 P_3 P_4^2 \mid \langle 5 \rangle$$

where  $P_i = \langle 5, \theta + i \rangle$ ,  $i = 1, 2, 3, 4$ . Then we have 5 splits in  $\mathbb{H}_m$ , see [2, p. 251]. In the other hand, we have  $\mathbb{H}_m$  is cyclic number fields of degree 5. Then 5 splits completely in  $\mathbb{H}_m$ . Therefore, by Engstrom [7], we get  $I(\mathbb{H}_m) = 1$  and by MacCluer [19]

$$i(\mathbb{H}_m) = \begin{cases} 5 & \text{if } m \equiv 2 \pmod 5, \\ 1 & \text{otherwise.} \end{cases}$$

This completes the proof of Theorem 6.

*Proof of Theorem 7:*

Assume  $3 \nmid m$ ,  $m \neq -8, -5$ . Let us consider the family of sextic field  $\mathbb{S}_m$  generated by some root  $\theta$  of the polynomial

$$s_m(x) = x^6 - 2mx^5 - (5m + 15)x^4 - 20x^3 + 5mx^2 + (2m + 6)x + 1.$$

Among others these fields are totally real cyclic fields.

We have the simplest cubic fields  $\mathbb{L}_m$  and quadratic fields  $\mathbb{Q}(\sqrt{m^2 + 3m + 9})$  are subfields of  $\mathbb{S}_m$ . We have 2 is inert in  $\mathbb{L}_m$  (see the proof of Theorem 4), so the splitting type possibilities of 2 in  $\mathbb{S}_m$  are

$$\langle 2 \rangle = P, P^2 \text{ or } P_1P_2.$$

**The case where  $3 \nmid m$ .** For  $m \equiv 0, 5 \pmod{8}$  ( $m^2 + 3m + 9 \equiv 1 \pmod{8}$ ), we have  $i(\mathbb{Q}(\sqrt{m^2 + 3m + 9})) = 2$  and  $\langle 2 \rangle = P_1P_2$  in  $\mathbb{Q}(\sqrt{m^2 + 3m + 9})$ . Then we get  $\langle 2 \rangle = P_1P_2$  in  $\mathbb{S}_m$  if and only if  $m \equiv 0, 5 \pmod{8}$ . Moreover, we have  $i(\mathbb{S}_m) \mid 6!$  and by [1, Theorem 2], we obtain

$$v_2(i(\mathbb{S}_m)) = \begin{cases} 3 \text{ or } 4 & \text{if } m \equiv 5, 8, 13, 16 \pmod{24}, \\ 0 & \text{otherwise.} \end{cases}$$

**The case where  $3 \mid m$ .** Let  $m = 3k$ . For  $m \equiv 0, 21 \pmod{24}$  ( $k^2 + k + 1 \equiv 1 \pmod{8}$ ), we have  $i(\mathbb{Q}(\sqrt{k^2 + k + 1})) = 2$  and  $\langle 2 \rangle = P_1P_2$  in  $\mathbb{Q}(\sqrt{k^2 + k + 1})$ . Then we get  $\langle 2 \rangle = P_1P_2$  in  $\mathbb{S}_m$  if and only if  $m \equiv 0, 21 \pmod{24}$ . Since,  $i(\mathbb{S}_m) \mid 6!$  and by [1, Theorem 2], we obtain

$$v_2(i(\mathbb{S}_m)) = \begin{cases} 3 \text{ or } 4 & \text{if } m \equiv 0, 21 \pmod{24}, \\ 0 & \text{otherwise.} \end{cases}$$

In the other hand we have  $i(\mathbb{L}_m) = 3$  if and only if  $m \equiv 39, 120, 201 \pmod{243}$  (see Theorem 4). Moreover, we have  $i(\mathbb{S}_m) \mid 6!$  and by [1, Theorem 2], we obtain

$$v_3(i(\mathbb{S}_m)) = \begin{cases} 2 & \text{if } m \equiv 39, 120, 201 \pmod{243}, \\ 0 & \text{otherwise.} \end{cases}$$

In the case where  $m \equiv 39, 120, 201 \pmod{243}$  we have the splitting type of 3 in  $\mathbb{L}_m$  is  $P_1P_2P_3$ , so the splitting type possibilities of 3 in  $\mathbb{S}_m$  are

$$P_1P_2P_3, P_1^2P_2^2P_3^2 \text{ or } P_1P_2P_3P_4P_5P_6.$$

We claim that for  $m \equiv 39, 120, 201 \pmod{243}$  the splitting type of 3 is  $P_1^2P_2^2P_3^2$  in  $\mathbb{S}_m$ . Note that  $m = 3k$ , we have  $k \equiv 1 \pmod{3}$  and  $3 \mid k^2 + k + 1$ , so  $\langle 3 \rangle = \langle 3, \sqrt{k^2 + k + 1} \rangle^2$  in  $\mathbb{Q}(\sqrt{k^2 + k + 1})$ . Then by Engstrom [7], we get  $3 \nmid I(\mathbb{S}_m)$ .

Now we study the splitting type of 5 in  $\mathbb{S}_m$ . We have

$$D(s_m) = 2^6 3^6 (m^2 + 3m + 9)^5 = I(\theta)^2 D(\mathbb{S}_m).$$

We can see that  $5 \nmid m^2 + 3m + 9$ , so  $5 \nmid I(\theta)$ , so Dedekind's Theorem [4, §18] gives the factorization of 5 using the minimal polynomial of  $\theta$ ,

$$s_m(x) \equiv \begin{cases} (x^3 + 3x^2 + 4)(x^3 + 2x^2 + 4x + 4) \pmod{5} & \text{if } m \equiv 0 \pmod{5}, \\ (x^2 + x + 2)(x^2 + 3x + 3)(x^2 + 4x + 1) \pmod{5} & \text{if } m \equiv 1 \pmod{5}, \\ (x^3 + x^2 + 3x + 4)(x^3 + 2x + 4) \pmod{5} & \text{if } m \equiv 2 \pmod{5}, \\ x^6 + 4x^5 + 2x + 1 \pmod{5} & \text{if } m \equiv 3 \pmod{5}, \\ x^6 + 2x^5 + 4x + 1 \pmod{5} & \text{if } m \equiv 4 \pmod{5}, \end{cases}$$

so

$$\langle 5 \rangle = \begin{cases} \langle 5, \theta^3 + 3\theta^2 + 4 \rangle \langle 5, \theta^3 + 2\theta^2 + 4\theta + 4 \rangle & \text{if } m \equiv 0 \pmod{5}, \\ \langle 5, \theta^2 + \theta + 2 \rangle \langle 5, \theta^2 + 3\theta + 3 \rangle \langle 5, \theta^2 + 4\theta + 1 \rangle & \text{if } m \equiv 1 \pmod{5}, \\ \langle 5, \theta^3 + \theta^2 + 3\theta + 4 \rangle \langle 5, \theta^3 + 2\theta + 4 \rangle & \text{if } m \equiv 2 \pmod{5}, \\ \langle 5, \theta^6 + 4\theta^5 + 2\theta + 1 \rangle & \text{if } m \equiv 3 \pmod{5}, \\ \langle 5, \theta^6 + 2\theta^5 + 4\theta + 1 \rangle & \text{if } m \equiv 4 \pmod{5}, \end{cases}$$

hence by MacCluer [19], we have  $5 \nmid i(\mathbb{S}_m)$  and by Engstrom [7], we get  $5 \nmid I(\mathbb{S}_m)$ . This completes the proof of Theorem 7.

#### 4. FURTHER EXAMPLES

In this section, we give three important examples. In the example 1, we construct two sextic number fields  $\mathbb{S}_8$  and  $\mathbb{K}$  where the splitting type of 2 is  $P_1P_2$  and  $v_2(i(\mathbb{S}_8)) \neq v_2(i(\mathbb{K}))$ . It shows that  $v_p(i(\mathbb{K}))$  is not completely determined by the splitting type of  $p$ . The example 2 gives answer to the question 2 in [1]. The example 3 shows that the conjecture stated in [1] is false.

**Example 1.** Let  $\mathbb{S}_8 = \mathbb{Q}(\theta)$ ,  $\theta^6 - 16\theta^5 - 55\theta^4 - 20\theta^3 + 40\theta^2 + 22\theta + 1 = 0$  be a cyclic sextic field. We have the simplest cubic fields  $\mathbb{L}_8$  and quadratic fields  $\mathbb{Q}(\sqrt{97})$  are subfields of  $\mathbb{S}_8$  and the splitting type of 2 is  $P_1P_2$  in  $\mathbb{S}_8$  (see the proof of Theorem 7). Let  $\alpha = 3 + 2\varphi + \frac{1+\sqrt{97}}{2} + 6\frac{1+\sqrt{97}}{2}\varphi$  where  $\varphi$  is a generator of  $\mathbb{L}_8$ . The characteristic polynomial of  $\alpha$  is given by

$$F_\alpha(x) = x^6 - 503x^5 - 605467x^4 + 1669375x^3 + 459134890x^2 - 2719842464x + 2224769824$$

with  $D(F_\alpha) \neq 0$ , so  $\alpha$  is a primitive integer of  $\mathbb{S}_8$ . We can write  $F_\alpha(x)$  in the form

$$F_\alpha(x) = 2224769824 - 3172016160 \binom{x}{1} + 447489144 \binom{x}{2} + 5285832 \binom{x}{3} - 600762 \binom{x}{4} - 488 \binom{x}{5} + \binom{x}{6}.$$

So by Theorem 8, we obtain  $v_2(i(\mathbb{S}_8)) = v_2(i(\alpha)) = 4$ .

Let  $\mathbb{K} = \mathbb{Q}(\theta)$ ,  $\theta^6 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + \theta + 1 = 0$ , we have  $D(\mathbb{K}) = -7^5$  and  $I(\theta) = 1$ , so Dedekind's Theorem [4, §18] gives explicitly the factorization of 2 using the minimal polynomial of  $\theta$ , so we have

$$x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 \equiv (x^3 + x + 1)(x^3 + x^2 + 1) \pmod{2},$$

so  $\langle 2 \rangle = \langle 2, \theta^3 + \theta + 1 \rangle \langle 2, \theta^3 + \theta^2 + 1 \rangle$ . Take  $\beta = x_1 + x_2\theta + \dots + x_6\theta^5$  where  $x_i \in \mathbb{Z}, i = 1, \dots, 6$ . Apply the algorithm [1, p. 1187], we get there not exist

$x_i \in \{0, 1, \dots, 15\}$ ,  $i = 1, \dots, 6$ , such that  $v_2(i(\beta)) = 4$ . Take  $\gamma = \theta + \theta^2 + 3\theta^4 + 4\theta^5$ , we have the characteristic polynomial of  $\gamma$  is given by

$$F_\gamma(x) = x^6 + 9x^5 + 53x^4 + 71x^3 - 110x^2 - 1256x + 1576$$

with  $D(F_\gamma) = -12594220569828093952$ , so  $\gamma$  is primitive integer of  $\mathbb{K}$ . We can write  $F_\gamma(x)$  in the form

$$F_\gamma(x) = 1576 + 608\binom{x}{1} - 2824\binom{x}{2} + 1328\binom{x}{3} - 272\binom{x}{4} + 24\binom{x}{5} + \binom{x}{6}.$$

So by Theorem 8, we get  $v_2(i(\mathbb{K})) = v_2(i(\gamma)) = 3$ .

These examples show that there exist sextic number fields  $\mathbb{S}_8$  and  $\mathbb{K}$  where the splitting type of 2 is  $P_1P_2$  and  $v_2(i(\mathbb{S}_8)) \neq v_2(i(\mathbb{K}))$ . We conclude  $v_p(i(\mathbb{K}))$  is not completely determined by the splitting type of  $p$ .

**Example 2.** Let  $\mathbb{K}_1 = \mathbb{Q}(\theta)$ ,  $\theta^4 - \theta^3 - 6\theta^2 + \theta + 1 = 0$ . By Theorem 5, we have  $i(\mathbb{K}_1) = 4$ .  $\mathbb{K}_1$  contain the subfield  $k = \mathbb{Q}(\sqrt{17})$ . We have also  $i(k) = 2$ . An integral basis of  $\mathbb{K}_1$  is given by  $\omega_1 = 1, \omega_2 = \theta, \omega_3 = \theta^2, \omega_4 = \frac{1+\theta^3}{2}$ . Take  $\beta = \omega_2 + \omega_3$ . Table 1 shows that  $4 \mid i(\beta)$ , the minimal polynomial of  $\beta$  is given by  $x^4 - 14x^3 + 31x^2 - 10x - 4$  with discriminant 13284752, so  $\beta$  is primitive integer, so  $\beta$  does not element of  $\mathbb{Q}(\sqrt{17})$ . By Theorem 5, we have  $v_2(i(\mathbb{K}_1)) = v_2(i(\beta)) = 2$ , but there not exist any integer  $\alpha$  of  $k$  such that  $\beta \equiv \alpha \pmod 2$ .

Table 1: List of the elements  $\beta \in \mathbb{A}/4\mathbb{A}$  with their respective characteristic polynomial such that  $4 \mid i(\beta)$ .

$x_1$	$x_2$	$x_3$	$x_4$	$F(x)$
0	1	1	0	$x^4 - 14x^3 + 31x^2 - 10x - 4$
0	1	1	2	$x^4 - 34x^3 - 119x^2 + 476x - 272$
0	3	3	0	$x^4 - 42x^3 + 297x^2 - 270x - 324$
0	3	3	2	$x^4 - 62x^3 + 141x^2 + 192x - 64$
1	1	1	0	$x^4 - 18x^3 + 79x^2 - 118x + 52$
1	1	1	2	$x^4 - 38x^3 - 11x^2 + 608x - 832$
1	3	3	0	$x^4 - 64x^3 + 411x^2 - 958x + 268$
1	3	3	2	$x^4 - 66x^3 + 333x^2 - 280x - 52$
2	1	1	0	$x^4 - 22x^3 + 139x^2 - 334x + 268$
2	1	1	2	$x^4 - 42x^3 + 109x^2 + 512x - 1412$
2	3	3	0	$x^4 - 50x^3 + 555x^2 - 1922x + 1684$
2	3	3	2	$x^4 - 70x^3 + 537x^2 - 1148x + 628$
3	1	1	0	$x^4 - 26x^3 + 211x^2 - 682x + 764$
3	1	1	2	$x^4 - 46x^3 + 241x^2 + 164x - 1772$
3	3	3	0	$x^4 - 54x^3 + 711x^2 - 3186x + 4212$
3	3	3	2	$x^4 - 74x^3 + 753x^2 - 2436x + 2384$

This example shows that the following statements are not equivalent :

1.  $mv_p(i(\mathbb{K}_1)) = v_p(i(\mathbb{K}))$ ,
2. For any integer  $\beta$  of  $\mathbb{K}$ , if  $v_p(i(\beta)) = v_p(i(\mathbb{K}))$ , then there exists an integer  $\alpha$  of  $\mathbb{K}_1$  such that  $\beta \equiv \alpha \pmod{p}$ .

**Example 3.** Let  $\mathbb{Q}(\sqrt{5}, \sqrt{-3})$  be a biquadratic field. The splitting type of 2 is  $P_1P_2$  in [20, Theorem 9]. An integral basis of this biquadratic field is given by  $\omega_1 = 1, \omega_2 = \frac{1+\sqrt{5}}{2}, \omega_3 = \frac{1+\sqrt{-3}}{2}, \omega_4 = \frac{1+\sqrt{5}+\sqrt{-3}+\sqrt{-15}}{4}$  [20, Theorem 2]. Take  $\beta = x_1\omega_1 + \dots + x_4\omega_4$  where  $x_i \in \mathbb{Z}$ .

Table 2: list of the elements  $\beta \in \mathbb{A}/2\mathbb{A}$  with their respective characteristic polynomial such that  $2 \mid i(\beta)$ .

$x_1$	$x_2$	$x_3$	$x_4$	$F(x)$
0	1	1	0	$x^4 - 4x^3 + 5x^2 - 2x + 4$
0	1	1	1	$x^4 - 5x^3 + 9x^2 + 10x + 4$
1	0	0	1	$x^4 - 5x^3 + 11x^2 - 10x + 4$
1	0	1	1	$x^4 - 7x^3 + 23x^2 - 32x + 16$
1	1	0	1	$x^4 - 7x^3 + 15x^2 - 4x + 4$
1	1	1	0	$x^4 - 8x^3 + 23x^2 - 28x + 16$

Let  $\mathbb{Q}(\sqrt{17}, \sqrt{-7})$  be a biquadratic field. The splitting type of 2 is  $P_1P_2P_3P_4$  [20, Theorem 9]. An integral basis of this biquadratic is given by  $\omega_1 = 1, \omega_2 = \frac{1+\sqrt{17}}{2}, \omega_3 = \frac{1+\sqrt{-7}}{2}, \omega_4 = \frac{1+\sqrt{17}+\sqrt{-7}+\sqrt{-119}}{4}$ . Take  $\beta = x_1\omega_1 + \dots + x_4\omega_4$  where  $x_i \in \mathbb{Z}$ .

Table 3: list of the elements  $\beta \in \mathbb{A}/2\mathbb{A}$  with their respective characteristic polynomial such that  $2 \mid i(\beta)$ .

$x_1$	$x_2$	$x_3$	$x_4$	$F(x)$
0	0	1	0	$x^4 - 2x^3 + 5x^2 - 4x + 4$
0	1	0	0	$x^4 - 2x^3 - 7x^2 + 8x + 16$
0	1	1	0	$x^4 - 4x^3 + x^2 + 6x + 32$
1	0	1	0	$x^4 - 6x^3 + 17x^2 - 24x + 16$
1	1	0	0	$x^4 - 6x^3 + 5x^2 + 12x + 4$
1	1	1	0	$x^4 - 8x^3 + 19x^2 - 12x - 32$

**Conclusion.** So we can see that  $\rho_{\mathbb{Q}(\sqrt{5}, \sqrt{-3})}(2) = \rho_{\mathbb{Q}(\sqrt{17}, \sqrt{-7})}(2) = 6$  and the ramification indices of 2 in the two fields are the same but 2 has not the same splitting type in  $\mathbb{Q}(\sqrt{5}, \sqrt{-3})$  and  $\mathbb{Q}(\sqrt{17}, \sqrt{-7})$ . This example shows that the conjecture stated in [1] is false.



## REFERENCES

1. M. AYAD, O. KIHTEL: *Common divisors of values of polynomials and common factors of indices in a number field*. Int. J. Number Theory **7** (2011), no. 5, 1173–1194.
2. S. ALACA, KENNETH S. WILLIAMS: *Introductory Algebraic Number Theory*. Cambridge University Press, 2012.
3. M. BAUER: *Über die außerwesentlichen Discriminantenteiler einer Gattung*. (German) Math. Ann. **64** (1907), no. 4, 573–576.
4. 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.
5. R. DEDEKIND: *Über die Theorie der ganzen algebraischen Zahlen*. XI Supplement to Dirichlet's "Vorlesungen über Zahlentheorie" 2nd ed. (1871), 3rd ed. (1879), 4th d. (1894). [Gesammelte mathematische Werke, vol. III, 1-314, Vieweg, 1932.]
6. H. DARMON: *Note on a polynomial of Emma Lehmer*. Math. Comput. **56** (1991), 795-800.
7. H. T. ENGSTROM: *On the common index divisors of an algebraic field*. Trans. Amer. Math. Soc. **32** (1930), 223-237.
8. 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. Sci. Besançon, (1977-1978), fasc 2, (1978).
9. I. GAAL, L. REMETE: *Integral bases and monogeneity of the simplest sextic fields*. Acta Arith. **183** (2018), no. 2, 173-183.
10. I. GAAL, M. POHST: *Power integral bases in a parametric family of totally real quintics*. Math. Comput. **66** (1997), 1689-1696.
11. H. GUNJI, D. L. MCQUILLAN: *On a class of ideals in an algebraic number field*. J. Number Theory **2** (1970), 207-222.
12. J. G. HUARD, B. K. SPEARMAN AND K. S WILLIAMS: *A short proof of the formula for the conductor of an abelian cubic field*. Norske Vid. Selsk. Skr. **2** (1994), 3-8.
13. K. HENSEL: *Theorie der algebraischen zahlen*. Leipzig 1908.
14. H. JAGER: *Number Theory Noordwijkerhout*. Springer Verlag, 1984.
15. H. K. KIM, J. S. KIM: *Computation of the different of the simplest quartic fields*. Manuscript, 2003.
16. P. LLORENTE, E. NART: *Effective determination of the rational primes in a cubic field*. Proc. Amer. Math. Soc. **87** (1983), 579-585.
17. E. LEHMER: *Connection between Gaussian periods and cyclic units*. Math. Comput. **50** (1988), 535-541.
18. G. LETTL, A. PETHO AND P. VOUTIER: *On the arithmetic of simplest sextic fields and related Thue equations*. Number theory (Eger, 1996), de Gruyter, Berlin, (1998), 331-348.
19. C. R. MACCLUER: *Common divisors of values of polynomials*. J. Number Theory **3** (1971), 33-34.
20. T. NAGELL: *Quelques résultats sur les diviseurs fixes de l'index des nombres entiers d'un corps algébrique*. Ark. Mat. **6** (1966), 269-289.

21. O. ORE: *Über den Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Körpern*. Math. Ann. **96** (1926), 313-352.
22. BLAIR K. SPEARMAN, KENNETH S. WILLIAMS: *Indices of Integers in Cyclic Cubic Fields*. International Mathematical Forum **3**, (2008), no. 32, 1595 - 1606.
23. J.ŚLIWA: *On the essential discriminant divisor of an algebraic number field*. Acta Arith. **42** (1983), 57-72.
24. D. SHANKS: *The simplest cubic fields*. Math. Comput. **28** (1974), 1137-1152.
25. R. SCHOOF, L. WASHINGTON: *Quintic polynomials and real cyclotomic fields with large class numbers*. Math. Comput. **50** (1988), 543-556.
26. E. ZYLINSKI: *Zur Theorie der ausserwesentlichen discriminantenteiler algebraischer korper*. Math. Ann. **73** (1913), 273-274.

**Abdelmejid Bayad**

Université Paris-Saclay,  
Laboratoire de Mathématiques et Modélisation d'Évry,  
(UMR 8071), I.B.G.B.I., 23 Bd. de France,  
91037 Évry Cedex, France,  
E-mails: [abdelmejid.bayad@univ-evry.fr](mailto:abdelmejid.bayad@univ-evry.fr)

(Received 25. 10. 2019.)

(Revised 22. 09. 2020.)

**Mohammed Seddik**

Université Paris-Saclay,  
Laboratoire de Mathématiques et Modélisation d'Évry,  
(UMR 8071), I.B.G.B.I., 23 Bd. de France,  
91037 Évry Cedex, France,  
E-mails: [seddik.mohamed2011@gmail.com](mailto:seddik.mohamed2011@gmail.com)