COMMON DIVISORS OF VALUES POLYNOMIALS AND COMMON FACTORS OF INDICES IN A NUMBER FIELD

MOHAMMED SEDDIK

ABSTRACT. Let \( K \) be a number field of degree \( n \) over \( \mathbb{Q} \). Let \( \hat{A} \) be the set of integers of \( K \) which are primitive over \( \mathbb{Q} \) and \( I(\hat{K}) \) be its index. Gunji and McQuillan defined the following integer
\[
i(\theta) = \gcd_{x \in \mathbb{Z}} F_\theta(x), \quad \text{where} \quad F_\theta(x) = \gcd_{x \in \mathbb{Z}} F_\theta(x),
\]
and \( I(\hat{K}) \) for families of simplest number fields of degree less than 7. We give also answers to questions one and two in [1].

1. INTRODUCTION AND STATEMENT OF MAIN RESULTS

Let \( K \) be a number field of degree \( n \) over \( \mathbb{Q} \) and let \( \hat{A} \) be its ring of integers. Denote by \( \hat{A} \) the set of primitive elements of \( A \). For any \( \theta \in \hat{A} \) we denote \( F_\theta(x) \) the characteristic polynomial of \( \theta \) over \( \mathbb{Q} \). Let \( D_K \) be the discriminant of \( K \). It is well known that if \( \theta \in \hat{A} \), the discriminant of \( F_\theta(x) \) has the form
\[
D(\theta) = I(\theta)^2 D_K
\]
where \( I(\theta) = [A : \mathbb{Z}[\theta]] \) is called the index of \( \theta \). Let
\[
I(\hat{K}) = \gcd_{\theta \in \hat{\mathbb{A}}} I(\theta).
\]
A prime number \( p \) is called a common divisor of indices in \( \hat{A} \) or sometimes a common index divisor, if \( p \mid I(\hat{K}) \). 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 [13, pp.183-184]. Bauer [2] showed that if \( p < n \) then there exists a number field of degree \( n \) in which \( p \) is a common index divisor. Zylinski [3] showed the necessity of this condition, if \( p \) is common index divisor then \( p < n \). Hensel [16] has given a necessary and sufficient condition on a prime \( p \) to be a common divisor of indices in a number field \( K \). This condition depends upon the splitting of the prime \( p \) in \( K \), which make Hensel’s Theorem not easy to apply in general.

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, splitting of prime numbers.
Let $\theta \in \mathbb{A}$ and $i(\theta) = \gcd_{x \in \mathbb{Z}} F_{\theta}(x)$. Gunji and McQuillan [4] defined the following integer

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

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

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

Mac Cluer [5] showed that $i(k) > 1$ 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 $i(k)$. Ayad and Kihel [1] gives two important theorems. It is shown that there exist a primitive integer $\theta$ called a good element such that $i(k) = i(\theta)$ and an algorithm is given for the computation of such an integer and showed that if $p$ is a common factor divisor then $p \mid i(k)$. The converse is shown to be false in general. However, the following result is proved. Suppose that $K$ is a Galois extension 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 $p \mid i(k)$. As a consequence, we obtain that if $K/\mathbb{Q}$ is cyclic of prime degree $l$, then $p \neq l$ is a common index divisor if and only if $p \mid i(k)$. Let $p$ be a prime number. Let $v_p(i(k))$ be the valuation of $p$ in $i(k)$.

In 1926, Ore [19] conjectured that $p$-adic valuation $v_p(I(k))$ is not determined only by the splitting type of $p$ in $\mathbb{A}$. Engstrom [6] proved that if $n \leq 7$, then the splitting type determines the $p$-adic valuation $v_p(I(k))$. He gave examples of number fields $K_1$ and $K_2$ of degree 8 in which the prime 3 has the same splitting type, but $v_3(I(K_1)) \neq v_3(I(K_2))$. Śliwa [7] proved that if $p$ is not ramified, then $v_p(I(K))$ is determined by the splitting type of $p$ in $K$. Similar to this conjecture of Ore, Ayad and Kihel [1] ask the following question,

Suppose that the splitting of $p$ in $K$ as a product of prime ideals is given by $pK = P_1^{f_1} \cdots P_r^{f_r}$, where $r \geq p$. Let $f_i$ be the inertial degree of the ideal $P_i$, for $i = 1, \ldots, r$. Can one compute $v_p(I(k))$ in terms of integers $r, e_i$ and $f_i$. In other words, is $v_p(i(k))$ completely determined by splitting type of $p$? We give answer of this question, we gives examples of number fields $K_1$ and $K_2$ of degree 6 in which the prime 3 has the same splitting type $P_1P_2$ but $v_3(I(K_1)) \neq v_3(I(K_2))$.

They also showed that, if $K_1$ and $K$ be number fields such that $K_1 \subseteq K$ and let $m = [K : K_1]$, then $mv_p(i(K_1)) \leq v_p(i(K))$. Answer the question 2 in [1], we show that the following statements are not equivalent,

1. $mv_p(i(K_1)) = v_p(i(K))$.
2. For any integer $\beta$ of $K$, if $v_p(i(\beta)) = v_p(i(K))$, then there exists an integer $\alpha$ of $K_1$ such that $\beta \equiv \alpha \mod p$.

We now state the main result of this paper.

**Theorem 1.1.** Let $K$ be a number field of degree $n$ over $\mathbb{Q}$ and $p$ a prime number.

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


Now we will calculate $i(\mathbb{K})$ for 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

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

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

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

Let,

$$s_3 = v_3(\Delta), \quad \Delta_3 = \Delta/3^{s_3}.$$  

It is well known that if $\mathbb{K}$ is a cubic field, then $I(\mathbb{K}) = 1$ or 2 and

$$I(\mathbb{K}) = 2 \iff a \text{ odd}, b \text{ even}, s_2 \text{ even and } \Delta_2 \equiv 1 \mod 8.$$  

see [8, Theorem 4].

**Theorem 1.2.** Let $\mathbb{K} = \mathbb{Q}(\theta)$, $\theta^3 - a\theta + b = 0$, be a cubic field. Then the common divisors of values polynomials is given by

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

where

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

$$\beta = \begin{cases} 1 & \text{if } (a \equiv 3 \mod 9, b^2 \equiv a + 1 \mod 27, s_3 > 6 \text{ even, } \Delta_3 \equiv 1 \mod 3) \\ 0 & \text{else.} \end{cases}$$

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

**Corollary 1.1.** 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 a root of the polynomial

$$l_m(x) = x^3 - mx^2 - (m + 3)x - 1.$$  

This family were discussed by Shanks [14] and Jager [28, p 63-73].

**Theorem 1.3.** Let a simplest cubic fields given by $\mathbb{L}_m$ generated by a root of the polynomial $l_m$. Then

$$I(\mathbb{L}_m) = 1.$$  

$$i(\mathbb{L}_m) = \begin{cases} 3 & \text{if } m \equiv 39, 120, 201 \mod 243, \\ 1 & \text{otherwise.} \end{cases}$$
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 $K_m = \mathbb{Q}(\theta)$ 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 [21, Proposition 6]. Note that $K_m = \mathbb{Q}(\theta) = \mathbb{K}_m = \mathbb{Q}(-\theta)$, that is we can assume that $m > 0$ and $m \neq 3$.

**Theorem 1.4.** Let $m > 0$ and $m \neq 3$. Suppose the $m^2 + 16$ is not divisible by an odd square. Consider a simplest quartic fields generated by a root of the polynomial $P_m$. Then

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

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

Let us consider the family of sextic field $\mathbb{H}_m$ generated by a root of the polynomial $h_m(x) = x^6 - 2mx^5 - (2m^3 + 6m^2 + 10m + 10)x^3 + (m^4 + 5m^3 + 11m^2 + 15m + 5)x^2 + (m^3 + 4m^2 + 10m + 10)x + 1$. This polynomial were discussed by Emma Lehmer [24]. The fields $\mathbb{H}_m$ were also investigated by R. Schoof and L. Washington [25] and H. Darmon [26] for prime conductors $m^4 + 5m^3 + 15m^2 + 25m + 25$.

**Theorem 1.5.** (Lehmer’s quintics)
Let $m \in \mathbb{N}$ and suppose that $p^2 \nmid m^4 + 5m^3 + 15m^2 + 25m + 25$ for any prime $p \neq 5$. Consider a simplest quintic fields given by $\mathbb{H}_m$ generated by a root of the polynomial $h_m(x)$. Then

$$I(\mathbb{H}_m) = 1,$$

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

Assume $m \notin \{-8, -5, -3, 0\}$. Let us consider the family of sextic cyclic fields $S_m$ generated by a root of the polynomial

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

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 [27].

**Theorem 1.6.** Let $S_m$ be a simplest sextic field. Then

$$I(S_m) = 1,$$

$$i(S_m) = 2^\alpha 3^\beta,$$

where

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

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

[1] M. Ayad and O. Kihel. 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] N. Bauer. Über den ausserwesentlicher discriminantenteiler algebraischer körper, Math. Ann. 64 (1907), 573.

[3] E. Zylinski. Zur Theorie der ausserwesentlicher discriminantenteiler algebraischer körper, Math. Ann. 73 (1913) 273-274.

[4] H. Gunji, D. L. McQuillan. On a class of ideals in an algebraic number field, J. Number Theory 2 (1970), 207-222.

[5] C. R. MacCluer. Common divisors of values of polynomials, J. Number Theory 3 (1971), 33-34.

[6] H. T. Engstrom. On the common index divisors of an algebraic field. Trans. Amer. Math. Soc. 32 (1930), 223-237.

[7] J. Śliwa. On the essential discriminant divisor of an algebraic number field. Acta Arith. 42 (1983). 57-72.

[8] P. Llorente, & E. Nart. Effective determination of the rational primes in a cubic field, Proc. Amer. Math. Soc. 87 (1983), 579-585.

[9] J. W. S. Cassels. Local fields. Cambridge University Press, 1986.

[10] H. Hass. Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage. Math. Zeit. 31 (1930), 565-582.

[11] W. Narkiewicz. Elementary and Analytic Theory of Algebraic Numbers. Second edition. Springer-Verlag, Berlin, 1990.

[12] B. N. Delone and D. K. Faddeev. The theory of irrationalities of the third degree. Trans. Math. Monographs. vol 10. Amer. Math. Soc. Providence. R. I. 1964.

[13] S. Alaca, K. S. Williams, Introductory Algebraic Number Theory, Cambridge University Press, 2004.

[14] D. Shanks. The simplest cubic fields. Mathematics of computation, 28 (1974), 1137-1152.

[15] T. Nagell. Quelques resultat sur les diviseurs fixes de l’index des nombres entiers d’un corps algébrique. Ark. Mat. 6 (1965) 269-289.

[16] K. Hensel. Theorie der algebraischen zahlen. Leipzig 1908.

[17] K. S Williams. Integers of biquadratic fields. Canad. Math. Bull. Vol. 13 (4), 1970.

[18] D. C. Mayer, Multiplicities of dihedral discriminant, Math. Comp. 58 (1992) 831-847.

[19] O. Ore, ber den Zusammenhang zwischen den definierenden Gleichungen und der Idealtheorie in algebraischen Krpern, Math. Ann. 69 (1926) 313-352.

[20] H. K. Kim and J. S. Kim, Computation of the different of the simplest quartic fields, Manuscript, 2003.

[21] M. N. Gras, Table numérique du nombre de classe et des units des extensions cycliques relles de degré 4 de Q. Publ. Math. Fac. Besançon, fasc 2, 1977-1978.

[22] I. Gaal and M. Pohst, Power integral bases in a parametric family of totally real quintics, Math. Comput., 66 (1997), 1689-1696.

[23] T. Funakura, On integral bases of pure quartic fields, Math. J. Okayama Univ. 26 (1984), 27-41.

[24] E. Lehmer, Connection between Gaussian periods and cyclic units, Math. Comput. 50 (1988), 535-541.

[25] R. Schoof and L. Washington, Quintic polynomials and real cyclotomic fields with large class numbers, Math. Comput., 50 (1988), 543-556.

[26] H. Darmon, Note on a polynomial of Emma Lehmer, Math. Comput. 56 (1991), 795-800.

[27] G. Lettl, A. Petho, P. Voutier On the arithmetic of simplest sextic fields and related Thue equations, in "Number Theory", ed. by K. Gyory, A Petho, y.T. S6s, Walter de Gruyter, Berlin-New York, 1998, pp. 331-348.

[28] H. Jager, Number Theory Noordwijkerhout, Springer Verlag, 1984.

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