On the common Index divisors of an algebraic number field

Seddik Mohammed

Université d'Évry Val d'Essonne
Directeur de thèse Mr. Bayad Abdelemejid

abayad@maths.univ-evry.fr
mohammed.seddik@univ-evry.fr

1. Abstract

Let $\mathbb{K}$ be a number field of degree n over $\mathbb{Q}$. Let $\widehat{\mathbb{A}}$ be the set of integers of $\mathbb{K}$ which are primitive over $\mathbb{Q}$ and let $I(\mathbb{K})$ be its index. The prime factors of $I(\mathbb{K})$ are called common factors of indices. Bauer and Zylinsky show that if $p < n$ then there exists a number field of degree n in which p is a common index divisor and reciprocally, if p is common index divisor then $p < n$. Gunji and McQuillan as $i(\mathbb{K}) = \operatorname{lcm}_{\theta\in\widehat{A}} i(\theta)$, where $i(\theta) = \gcd_{x\in\mathbb{Z}} F_\theta(x)$ and $F_\theta(x)$ is the characteristic polynomial of θ over $\mathbb{Q}$. We will show that, if $p \mid i(\mathbb{K})$ then $p \leq n$. On the other hand, Ayad and Kihel show that, if $\mathbb{K}_1$ and $\mathbb{K}$ be number fields such that $\mathbb{K}_1 \subseteq \mathbb{K}$ and let $m = [\mathbb{K} : \mathbb{K}_1]$, then $i(\mathbb{K}_1)^m \mid i(\mathbb{K})$. We will give a necessary and sufficient condition for which $i(\mathbb{K}_1)^m = i(\mathbb{K})$. We suppose that $\mathbb{K}$ be a number field of degree 2 and 3, we calculate $i(\mathbb{K})$ in this cases.

2. 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 $\widehat{\mathbb{A}}$ the set of primitive elements of $\mathbb{A}$. For any $\theta \in \mathbb{A}$ we denote $F_\theta(x)$ the characteristic polynomial of θ over $\mathbb{Q}$. Let $D_{\mathbb{K}}$ be the absolute discriminant of $\mathbb{K}$. It is well known that if $\theta \in \widehat{\mathbb{A}}$, the discriminant of $F_\theta(x)$ has the form

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

where $I(\theta) = [\mathbb{A} : \mathbb{Z}[\theta]]$ is called the index of θ. Let $I(\mathbb{K}) = \gcd_{\theta\in\widehat{A}} I(\theta)$. A prime number p is called a common index divisor if $p \mid I(\mathbb{K})$. Bauer [2] showed that if $p < n$ then there exists a number field of degree n in which p is a common index divisor. Zylinsky [3] showed the necessity of this condition, if p is common index divisor then $p < n$. Let $\theta \in \mathbb{A}$ and $i(\theta) = \gcd_{x\in\mathbb{Z}} F_\theta(x)$. Gunji and McQuillan [4] defined the following integer

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

Mac Cluer [5] 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] showed that if p is a common index 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 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, then p is a common index divisor if and only if $p \mid i(\mathbb{K})$, and they show that there exists $\theta \in \widehat{\mathbb{A}}$ such that $i(\mathbb{K}) = i(\theta)$. they give an algorithm which one to find such elements.

3. Result

From Ayad and Kihel, we have, there exists an element $\theta \in \widehat{\mathbb{A}}$ whose characteristic polynomial

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

where $\binom{x}{k} = x(x-1)\cdots(x-(k-1)),\ k = 1, ..., n.$

satisfies

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

Then, we deduce that

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

We state our main results,

Theorem 1. *Let $\mathbb{K}$ be a number field of degree n over $\mathbb{Q}$ and p a prime number.*

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

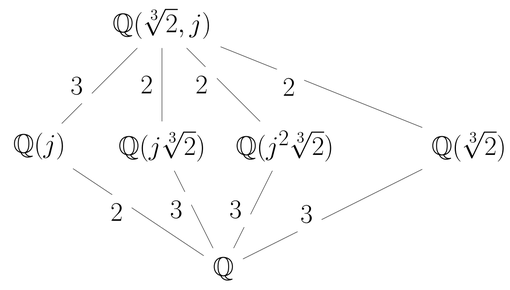
Theorem 2. *Let $\mathbb{K}_1$ and $\mathbb{K}$ be number fields such that $\mathbb{K}_1 \subseteq \mathbb{K}$ and let $m = [\mathbb{K} : \mathbb{K}_1]$. The two conditions are equivalent:*

1. *$m v_p(i(\mathbb{K}_1)) = v_p(i(\mathbb{K})) = e$.*
2. *For any integer α of $\mathbb{K}_1$, if $v_p(i(\alpha)) = v_p(i(\mathbb{K}_1))$, then there exists a primitive integer β of $\mathbb{K}$ such that $\beta \equiv \alpha \ mod\ p^e$ and $i(\mathbb{K}) = i(\beta)$.*

Example 1. *Let $\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ be an biquadratique field. We show that $i(\mathbb{K}) = 1$, which implies that $I(\mathbb{K}) = 1$, in other words does not exist a common factor of indices.*

Example 2. *Let $\mathbb{K} = \mathbb{Q}(\sqrt{2}, \sqrt{-7})$ be an biquadratic field. We show that $i(\mathbb{K}) = 4$, which implies that $3 \nmid I(\mathbb{K})$, in other words 3 is not a common factor of indices.*

Example 3. *Let $\mathbb{K} = \mathbb{Q}(\sqrt[3]{2}, j)$ be an sextic where $j = \frac{-1+\sqrt{-3}}{2}$ the splitting field of $x^3 - 2$ over $\mathbb{Q}$. The possibilities of prime number divisors of $I(\mathbb{K})$ and $i(\mathbb{K})$ are $p = 2, 3, 5$.*



We show that $i(\mathbb{K}) = 1$, which implies that $I(\mathbb{K}) = 1$, in other words does not exist a common factor of indices.

4. An Algorithm

Now we will calculate $i(\mathbb{K})$ for quadratic and cubic number fields, for cubic number field we distinguish in two cases, cyclic and non-cyclic, finally we will treat the pure cubic field.

Theorem 3. *Let $m \neq 1$ square free rational integer, then*

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

Theorem 4. *Let $\mathbb{K} = \mathbb{Q}(\theta),\ \theta^3 + a\theta + b = 0$, be a cyclic cubic field. Then*

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

Theorem 5. *Let $\mathbb{K} = \mathbb{Q}(\theta),\ \theta^3 + a\theta + b = 0$, be a cubic field. Let*

$$\Delta = 4a^3 - 27b^2, \quad s_p = v_p(\Delta), \quad \Delta_p = \Delta/p^{s_p}$$

Namely ;
$3 \mid a,\ 3 \nmid b,\ a \equiv 3\ mod\ 9,\ b^2 \equiv a + 1\ mod\ 27,\ s_3 > 6$ *even*,
$\Delta_3 \equiv 1\ mod\ 3$ (1)
$3 \nmid a,\ a \equiv 1\ mod\ 3,\ 3 \mid b$ (2)

1. *If a, b even, then*
   - (a) *If $1 \leq v_2(b) \leq v_2(a)$, then*
     - i. *If (1) or (2) are satisfied, then $i(\mathbb{K}) = 3$.*
     - ii. *Else $i(\mathbb{K}) = 1$.*
   - (b) *If $1 = v_2(a) < v_2(b)$ then*
     - i. *If (1) or (2) are satisfied, then $i(\mathbb{K}) = 6$.*
     - ii. *Else $i(\mathbb{K}) = 2$.*
2. *If a, b of different parity, then*
   - (a) *If (1) or (2) are satisfied, then $i(\mathbb{K}) = 6$.*
   - (b) *Else $i(\mathbb{K}) = 2$.*
3. *If a, b odd, then*
   - (a) *If (1) or (2) are satisfied, then $i(\mathbb{K}) = 3$.*
   - (b) *Else $i(\mathbb{K}) = 1$.*

Theorem 6. *Let $\mathbb{Q}(\sqrt[3]{d})$ be an pure cubic field, then*

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

5. Discussion and comments

Theorem 7. *(Dedekind 1878)*
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

$$f(x) = irr_{\mathbb{Q}}(\theta) \in \mathbb{Z}[x].$$

Let denote the natural map $: \mathbb{Z}[x] \to \mathbb{Z}/p\mathbb{Z}[x]$. Let

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

where $g_1(x), \cdots, g_r(x)$ are distinct monic irreducible polynomials in $\mathbb{Z}/p\mathbb{Z}[x]$ and $e_1, \cdots, e_r$ are positive integers. For $i = 1, 2, \ldots, r$ let $f_i(x)$ be any monic polynomial of $\mathbb{Z}[x]$ such that $\bar{f}_i = g_i$. Set

$$P_i =< p, f_i(\theta) >, i = 1, 2, \ldots, r.$$

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

$$< p >= P_1^{e_1} \cdots P_r^{e_r},$$

and

$$N(P_i) = p^{deg f_i}, i = 1, 2, \ldots, r.$$

Comments :
Let p a prime number,

1. If $p \mid I(\mathbb{K})$ Then $\nexists\ \phi \in \widehat{\mathbb{A}}$ such that $p \nmid I(\phi)$ and we can not apply Theorem of Dedekind.
2. If $p \nmid I(\mathbb{K})$ then $\exists\ \phi \in \widehat{\mathbb{A}}$ such that $p \nmid I(\phi)$ and we can apply Theorem of Dedekind for decomposition of $< p >$ using the integer ϕ, but the difficulty is to find ϕ.

The next Theorem gives algorithm to calculate ϕ in cubic field.

Theorem 8. *Let $\mathbb{K} = \mathbb{Q}(\theta)$, $\theta^3 + a\theta + b = 0$ be a cubic field. Let $\phi = \frac{x+y\theta+z\theta^2}{I(\theta)} (x, y, z \in \mathbb{Z})$ be an element of $\mathbb{A}$. Then the two conditions are equivalent :*

1. $I(\phi) = m$,

2. There is an integral solution to $|y^3 + ayz^2 + bz^3| = I(\theta)^2 \times m$.

Remark 1. *The following Theorem gives a necessary and sufficient conditions in which a cubic number field $\mathbb{K}$ has a power integral basis.*

Remark 2. *It is well known that if $\mathbb{K}$ is a cubic field, then $I(\mathbb{K}) = 1$ or 2. In the case $I(\mathbb{K}) = 1$ we apply Theorem 8 and Theorem 7 for the factorization of the principal ideal $< p >$, but in the case $I(\mathbb{K}) = 1$, we can not apply Theorem 7 for the factorization of the principal ideal $< 2 >$. Alaca, Spearman and Williams [18] give the explicit factorization of the principal $< 2 >$ in cubic fields with index 2. Let $\mathbb{K} = \mathbb{Q}(\theta)$, $\theta^3 + a\theta + b = 0$ be a cubic field. If $a \equiv 1\ mod\ 4,\ b \equiv 0\ mod\ 4,\ \Delta_2 \equiv 1\ mod\ 8$, then*

$$< 2 >=< 2, \theta >< 2, \frac{2 + \theta + \theta^2}{2} >< 2, \frac{2 + 3\theta + \theta^2}{2} > .$$

If $a \equiv 3\ mod\ 4,\ b \equiv 2\ mod\ 4,\ s_2 \equiv 0\ mod\ 2,\ \Delta_2 \equiv 1\ mod\ 8$, then

$$< 2 >=< 2, \theta >< 2, \alpha >< 2, \theta + \alpha > .$$

where $\alpha = \frac{x+y\theta+\theta^2}{2^{m+1}},\ m = \frac{s_2-1}{2} \geq 1$, x and y are integers satisfies

$$3x \equiv -2a\ mod\ 2^{2m+3},\ ay \equiv \frac{3b}{2} + 2^m\ mod\ 2^{2m+3}$$

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, 11731194.

[2] N. Bauer. *Uber den ausserwesentlicher discriminamtenteiler algebraischer korper*, Math. Ann. 64, (1907), 573.

[3] E. Zylinski. *Zur Theorie der ausserwesentlicher discriminamtenteiler algebraischer korper* , 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] Mac. Cluer. *Common divisors of values of polynomials*, J. Number Theory 3, (1971), 33-34.

[6] K. Spearman. *Indices of Intergres in Cyclic Cubic Fields*,Int. Math, 3,2008, no, 32, 1595-1606.

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

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

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

[10] L. Carlitz. *A note on common index divisors*. Proc. Amer. Math. Soc. 3 (1952) 688-692.

[11] D. S. Dummit and H. Kisilevsky *indices in cyclic cubic fields, in Number Theory and Algebra, ed H. Zassenhaus* (Academic Press, New York, 1977), pp.29-42.

[12] M. Hall. *Indices in cubic fields*, Bull. Amer. Math. Soc. 43 (1937) 104-108.

[13] T. Nagell. *Quelques résultats sur les diviseurs fixes de l'index des nombres entiers d'un corps algébrique*, Ark. Mat. 6 (1965) 269-289.

[14] E. Nart. *On the index of a number field*, Trans. Amer. Math. Soc. 289 (1985) 171-183.

[15] J. Silwa. *On the nonessential discriminant divisor of an algebraic number field*, Acta Arith. 42 (1982) 57-72.

[16] B. K. Spearman and K. S. Williams *Cubic fields with index 2*, Monatsh. Math. 134, (2002), 331-336.

[17] B. K. Spearman and K. S. Williams *The index of a cyclic quartic field*, Monatsh. Math. 140, (2003), 19-70.

[18] S. Alaca, B. K. Spearman and K. S. Williams *The factorization of 2 in cubic fields with index 2* , (FJMS) 14 (2004), no. 3, 273-282.