Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Mohamed AYAD, Rachid BOUCHENNA et Omar KIHEL

Indices in a Number Field

Tome 29, n° 1 (2017), p. 201-216.

<http://jtnb.cedram.org/item?id=JTNB_2017__29_1_201_0>

Journal de Théorie des Nombres
de Bordeaux **29** (2017), 201–216

Indices in a Number Field

par Mohamed AYAD, Rachid BOUCHENNA et Omar KIHEL

Résumé. Soient K un corps de nombres, A son anneau des entiers et p un nombre premier. Nous définissons une fonction $\mu_K(p)$ qui compte le nombre de $\overline{\theta} \in A/pA$ d'indice multiple de p tout en en donnant une formule explicite. De plus, nous montrons que la valeur de $\mu_K(p)$ détermine dans certains cas le type de décomposition de p dans K.

Abstract. Let K be a number field, A be its ring of integers and p be a prime number. In this paper, we define a function $\mu_K(p)$ which counts the number of $\overline{\theta} \in A/pA$ such that the index of θ is divisible by p. We give as well an explicit formula for it. Moreover, we show that the value of $\mu_K(p)$ determines in some cases the splitting type of p in K.

1. Introduction

Let K be a number field of degree n over $\mathbb{Q}$ and let A be its ring of integers. Denote by $\hat{A}$ the set of the elements of A which are primitive. Let D_K be the absolute discriminant of K. Let $\theta \in A$ and $F_\theta(x)$ its characteristic polynomial. The discriminant of this polynomial has the form $D(\theta) = [I(\theta)]^2 D_K$, where $I(\theta)$ is 0 if $\theta \notin \hat{A}$ or a positive integer if $\theta \in \hat{A}$, called the index of θ. Let $I(K) = \gcd_{\theta\in\hat{A}} I(\theta)$. This integer is called the index of K.

A prime number p is called a common factor of indices in K (c.f.i. for short) if $p \mid I(K)$.

Zylinski ([10]) (see also [7]) has shown that if p is a c.f.i. in K, then $p < n$.

There are examples and criteria for some primes to be common factor of indices in certain abelian extensions of $\mathbb{Q}$ (see [2], [3]).

For number fields of low degree, namely cubics fields and quartic fields, one may consult [5], [8] and [9].

Manuscrit reçu le 12 mars 2015, accepté le 14 novembre 2015.
Mathematics Subject Classification. 11R04, 12Y05.
Mots-clefs. Dedekind theorem, Common factor of indices.
The third author was supported in part by NSERC.

In this paper, we define a function related to the field K and to the fixed prime p as follows:

$$\mu_K(p) = \left|\left\{\overline{\theta} \in A/pA, p \mid I(\theta)\right\}\right| \tag{1.1}$$

An explicit formula for this function $\mu_K(p)$ is given. Moreover, we show that its values determine in some cases the splitting type of p in A. In [1], a function $\rho_p(K)$, similar to $\mu_K(p)$, is defined.

We fix some notations.

- Let $F(x) \in \mathbb{Z}[x]$ and p a prime number. Then $\overline{F(x)}$ denotes the polynomial, with coefficients in $\mathbb{F}_p$, obtained by reducing modulo the prime p the coefficients of $F(x)$.
- Let a be an integer, $p^e \parallel a$ means p^e divides exactly a.
- If p (resp. $\mathcal{P}$) is a prime number (resp. a prime ideal), then ν_p (resp. $\nu_{\mathcal{P}}$) denotes the p-adic (resp. the $\mathcal{P}$-adic) valuation.
- If E is a set, we denote by $|E|$ its cardinality.
- If $\mathcal{P}$ is a prime ideal of a number field lying over some prime number p, we denote by $e_{\mathcal{P}}$ and $f_{\mathcal{P}}$ its ramification index and its residual degree over $p\mathbb{Z}$ respectively.
- If θ is an element of a number field K, we denote by $Irr(\theta, \mathbb{Q})$ and $F_\theta(x)$ its minimal polynomial and its characteristic polynomial over $\mathbb{Q}$ respectively.
- Recall that $F_\theta(x) = Irr(\theta, \mathbb{Q})^d$ where $d = [K : \mathbb{Q}[\theta]]$.
- Let p be a prime number and f be a positive integer. We denote by $N_p(f)$ the number of monic irreducible polynomials in $\mathbb{F}_p[x]$ of degree f.
- If n and k are two positive integers, A_k^n denotes 0 if $k > n$ and $\dfrac{n!}{(n-k)!}$ if $k \leq n$.
- Let n be a positive integer and $p_1, \ldots, p_r$ be its distinct prime divisors, then the product of these primes is called the radical of n and will be denoted by $\mathrm{rad}(n)$.

2. Preliminary results

Let K be a number field of degree n, A be its ring of integers and θ an element of A.

The following theorem, due to K. Hensel, is the most basic result on the common factor of indices in a number field (see [6]).

Theorem 2.1. *Let K be a number field, A be its ring of integers and p be a prime number. Then, p is a c.f.i. in K if and only if there exists a positive integer f such that the number of prime ideals of A lying over p of residual degree equal to f is greater than $N_p(f)$.*

Let $\overline{\theta} = \theta + pA$ be the class of θ modulo p. The ideal

$$E_\theta = \left\{ g(x) \in \mathbb{F}_p[x], g(\overline{\theta}) = 0 \right\}$$

is a nonzero principal ideal of $\mathbb{F}_p[x]$ generated by some monic polynomial $g_0(x) \in \mathbb{F}_p[x]$.

We introduce the following definition.

Definition 2.2. We call a monic lift $M_\theta(p, x)$ of $g_0(x)$ in $\mathbb{Z}[x]$ the minimal polynomial-congruence of θ modulo p.

$M_\theta(p, x)$ divides $Irr(\theta, \mathbb{Q})$ in $F_p[x]$. Let $m_K(p) = \max \deg M_\theta(p, x)$, where the maximum runs over the elements $\theta \in A$ such that $p \mid I(\theta)$.

For the next result, we need the following lemma.

Lemma 2.3. *Let K be a a number field of degree n, A be its ring of integers and p be a prime number. Then $p \mid I(\theta)$ if and only if $\deg M_\theta(p, x) \leq n - 1$.*

Proof. See [6]. □

Theorem 2.4. *Let $K/\mathbb{Q}$ be a number field, A be its ring of integers and p a prime number. Suppose that the splitting of p in A is given by*

$$pA = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}$$

where the residual degree of $\mathcal{P}_i$ is f_i for $1 \leq i \leq r$. Let $\theta \in A$, then $p \mid I(\theta)$ if and only if one of the following conditions holds:

(i) There exists $i \in \{1, \ldots, r\}$ such that $e_i \geq 2$ and if $G(x) = Irr(\theta + \mathcal{P}_i, \mathbb{F}_p)$, then $G(x)$ satisfies $G(\theta) \equiv 0 \pmod{\mathcal{P}_i^2}$.

(ii) There exists $i \in \{1, \ldots, r\}$ such that $f_i \geq 2$ and $\deg Irr(\theta + \mathcal{P}_i, \mathbb{F}_p) < f_i$.

(iii) There exists $1 \leq i \neq j \leq r$, such that $Irr(\theta + \mathcal{P}_i, \mathbb{F}_p) = Irr(\theta + \mathcal{P}_j, \mathbb{F}_p)$.

Proof. Suppose that $p \mid I(\theta)$. Consider the factorization of $M_\theta(p, x)$ modulo p to be:

$$M_\theta(p, x) \equiv F_1(x)^{h_1} \cdots F_s(x)^{h_s} \pmod{p}$$

Since $p \mid I(\theta)$, then Lemma 2.3 implies that $\deg M_\theta(p, x) \leq n - 1$. Suppose that (ii) and (iii) do not hold, then $s = r$ and for $j \in \{1, \ldots, r\}$, there exists a unique $i = i(j)$ such that $F_i(\theta) \equiv 0 \pmod{\mathcal{P}_j}$. Since $\deg F_{i(j)} = f_{\mathcal{P}_j}$ and $\deg M_\theta(p, x) \leq n - 1$, then there exists j_0 such that $h_{i(j_0)} < e_{j_0}$. Suppose that $\mathcal{P}_{j_0} || F_{i(j_0)}(\theta)$, then $\mathcal{P}_{j_0}^{h_{i(j_0)}} || F_{i(j_0)}^{h_{i(j_0)}}(\theta)$, which is a contradiction to $\mathcal{P}_{j_0}^{e_{j_0}} \mid M_\theta(p, \theta)$. Hence, $\mathcal{P}_{j_0}^2 \mid F_{i(j_0)}(\theta)$ and condition (i) holds.

We prove the converse. Suppose (ii) and let $F(x) = \prod_{j=1}^r F_j(x)^{e_j}$, where $F_j(x)$ is a monic lift in $\mathbb{Z}[x]$ of $Irr(\theta + \mathcal{P}_j, \mathbb{F}_p)$. Since $\deg Irr(\theta + \mathcal{P}_i, \mathbb{F}_p) < f_i$ and $F(\theta) \equiv 0 \pmod{p}$, then $\deg M_\theta(p, x) \leq n - 1$. Hence by Lemma 2.3, $p \mid I(\theta)$.

Suppose that (iii) holds. Let $F(x) = (F_i(x))^{\max(e_i, e_j)} \prod_{k \neq i,j} F_k(x)^{e_k}$, where $F_i(x)$ is a monic lift of $Irr(\theta + \mathcal{P}_i, \mathbb{F}_p)$ and $F_k(x)$ is a monic lift of $Irr(\theta+\mathcal{P}_k,\mathbb{F}_p)$ in $\mathbb{Z}[x]$. Clearly, $F(\theta)\equiv 0 \pmod p$ and $\deg F(x)\le n-1$. Therefore, $\deg M_\theta(p,x)\le n-1$. Hence, Lemma 2.3 implies that $p\mid I(\theta)$.

Suppose that (i) holds. Let $F(x)=(F_i(x))^{(e_i+\epsilon)/2}\prod_{j\neq i}F_j(x)^{e_j}$, where $\epsilon=\begin{cases}0 & \text{if } e_i \text{ is even}\\ 1 & \text{if } e_i \text{ is odd}\end{cases}$ and $F_k(x)$ is a monic lift of $Irr(\theta+\mathcal{P}_k,\mathbb{F}_p)$. As in the preceding case, we have $F(\theta)\equiv 0 \pmod p$ and $\deg F(x)\le n-1$. Hence $\deg M_\theta(p,x)\le n-1$ and Lemma 2.3 implies that $p\mid I(\theta)$. $\square$

3. The number of $\overline{\theta}\in A/pA$ such that $p\mid I(\theta)$

Let K be a number field and A its ring of integers. For the definition of a function related to p and to K, we need the following.

Lemma 3.1. *Let α and β be elements of A such that $\alpha\equiv\beta \pmod p$. If $p\mid I(\alpha)$, then $p\mid I(\beta)$.*

Proof. Set $\beta=\alpha+p\gamma$ where $\gamma\in A$ and let $M(x)$ be the minimal polynomial congruence modulo p of α. Then $M(\beta)=M(\alpha+p\gamma)\equiv M(\alpha) \pmod p$, hence $p\mid I(\beta)$ by Lemma 2.3. $\square$

Define the integer $\mu_K(p)=|\{\,\overline{\theta}\in A/pA,\ p\mid I(\theta)\}|$. If p is a c.f.i. in K, then $\mu_K(p)=p^n$. We have the following.

Theorem 3.2. *Let*

$$pA=\mathcal{P}_1^{e_1}\cdots\mathcal{P}_r^{e_r}$$

be the splitting of p as a product of prime ideals in A, where $f_{\mathcal{P}_i}=f_i$. Suppose that $r=r_1+\ldots+r_s$ where r_i is a positive integer for each $i=1,\ldots,s$ and that the ideals $\mathcal{P}_i$ for $i=1,\ldots,r$, are ordered such that

$$f_1=\ldots=f_{r_1}:=f_1^*$$
$$f_{r_1+1}=\ldots=f_{r_1+r_2}:=f_2^*$$
$$f_{r_1+\ldots+r_{s-1}+1}=\ldots=f_{r_1+\ldots+r_s}:=f_s^*$$

Then,

$$\mu_K(p)=p^n-\prod_{j=1}^{r}f_j\prod_{e_j\ge 2}(p^{f_j}-1)p^{\sum_{e_j\ge 2}f_j(e_j-2)}\prod_{j=1}^{s}A_{r_j}^{N_p(f_j^*)} \tag{3.1}$$

By Hensel's theorem, the result is true if p is a c.f.i. in K. Hence, for the proof of this theorem, we suppose that p is not a c.f.i. in K.

We will use the following.

Lemma 3.3. *Let $\mathcal{P}$ be a prime ideal of A lying above p of residual degree d. Let $G(x)\in\mathbb{Z}[x]$ be monic and irreducible over $\mathbb{F}_p$ of degree d. Let $\rho\in A$ such that $G(\rho)\equiv 0 \pmod{\mathcal{P}}$ and let $e\ge 2$ be an integer. Then, the number of elements $\theta\in A$ incongruent modulo $\mathcal{P}^e$ and satisfying:*

$$\theta\equiv\rho \pmod{\mathcal{P}} \text{ and } G(\theta)\notin\mathcal{P}^2 \tag{3.2}$$

is equal to $(p^d-1)p^{d(e-2)}$.

Proof. If $G(\rho)\in\mathcal{P}^2$, let $\mu\in\mathcal{P}\backslash\mathcal{P}^2$ and $\tau=\rho+\mu$. Then, $\tau\equiv\rho\pmod{\mathcal{P}}$ and we have:

$$G(\tau)=G(\rho)+\mu G'(\rho)+\mu^2\frac{G''(\rho)}{2!}+...+\mu^d\frac{G^{(d)}(\rho)}{d!}$$

Since $G'(\rho)\notin\mathcal{P}$, then $G(\tau)\notin\mathcal{P}^2$. Hence, without loss of generality, we may suppose that $G(\rho)\notin\mathcal{P}^2$.

We first show that the number of elements $\theta\in A$ distinct modulo $\mathcal{P}^2$ and satisfying the condition (3.2) is equal to p^d-1.

In fact, the number of elements θ distinct modulo $\mathcal{P}^2$ and satisfying $\theta\equiv\rho\pmod{\mathcal{P}}$ is equal to $|\mathcal{P}/\mathcal{P}^2|=p^d$. We next show that:

$$A/\mathcal{P}^2=\{A_0(\rho)+A_1(\rho)G(\rho)\mid A_i(x)\in\mathbb{F}_p\left[x\right],\deg A_i\leq d-1 \text{ for } i=0,1\}$$

Suppose that $A_0(\rho)+A_1(\rho)G(\rho)\equiv B_0(\rho)+B_1(\rho)G(\rho)\pmod{\mathcal{P}^2}$. Then, $A_0(\rho)-B_0(\rho)+(A_1(\rho)-B_1(\rho))G(\rho)\equiv 0\pmod{\mathcal{P}^2}$, hence $A_0(\rho)-B_0(\rho)\equiv 0\pmod{\mathcal{P}}$ therefore $A_0(x)=B_0(x)$. We deduce that $A_1(\rho)-B_1(\rho)\equiv 0\pmod{\mathcal{P}}$, then $A_1(x)=B_1(x)$.

Since the number of elements having the above form is equal to p^{2d}, then we have proved the equality of the two sets.

Let $\theta\in A/\mathcal{P}^2,\theta=A_0(\rho)+A_1(\rho)G(\rho)$ such that $\theta\equiv\rho\pmod{\mathcal{P}}$ and $G(\theta)\in\mathcal{P}^2$, then $A_0(\rho)=\rho$ and we have:

$$\begin{aligned}G(\theta)&=G(\rho+A_1(\rho)G(\rho))\\&=G(\rho)+A_1(\rho)G(\rho))\frac{G'(\rho)}{1!}+...+\left[A_1(\rho)G(\rho)\right]^d\frac{G^{(d)}(\rho)}{d!}\\&\equiv 0\pmod{\mathcal{P}^2}\end{aligned}$$

Hence, $G(\rho)+A_1(\rho)G(\rho)G'(\rho)\equiv 0$ (mod)P^2. Then, we deduce that $1+A_1(\rho)G'(\rho)\equiv 0\pmod{\mathcal{P}}$. Since $G'(\rho)\notin\mathcal{P}$, then $A_1(\rho)$ is uniquely determined. Therefore, the number of elements θ distinct modulo $\mathcal{P}^2$ and satisfying the condition $\theta\equiv\rho\pmod{\mathcal{P}}$ and $G(\theta)\notin\mathcal{P}^2$ is equal to p^d-1.

Let $\theta_1\in A$ such that $\theta_1\equiv\rho\pmod{\mathcal{P}}$ and $G(\theta_1)\notin\mathcal{P}^2$. Since $|\mathcal{P}^e/\mathcal{P}^2|=p^{d(e-2)}$, there exists $p^{d(e-2)}$ elements $\gamma\in A$ incongruent modulo $\mathcal{P}^e$ satisfying $\gamma\equiv\theta_1\pmod{\mathcal{P}^2}$.

It follows that the number of elements $\theta\in A$ incongruent modulo $\mathcal{P}^e$ and satisfying the condition (3.2) is equal to $(p^d-1)p^{d(e-2)}$. □

Proof of Theorem 3.2. To prove Theorem 3.2, we count the number, say N, of $\overline{\theta}\in A/pA$ such that $p\nmid I(\theta)$ and then $\mu_K(p)=p^n-N$.

By Lemma 3.1, we may define an equivalence relation in the set of elements $\overline{\theta}\in A/pA$ such that $p\nmid I(\theta)$ as follows:

$$(\theta+\mathcal{P}_1^{e_1},...,\theta+\mathcal{P}_r^{e_r})\simeq(\alpha+\mathcal{P}_1^{e_1},...,\alpha+\mathcal{P}_r^{e_r})$$

if and only if for each number $i = 1, \ldots, r$,

$$Irr(\theta + \mathcal{P}_i, \mathbb{F}_p) = Irr(\alpha + \mathcal{P}_i, \mathbb{F}_p)$$

We first count the number of elements in each equivalence class and then the number of equivalence classes. Indeed we will see that all the classes have the same cardinality. According to Theorem 2.4 an equivalence class is defined by some given uplet $(G_1(x), ..., G_r(x))$ of monic irreducible polynomials over $\mathbb{F}_p$ such that $\deg G_i = f_i$ for $i = 1, ..., r$ and $G_i(x) \neq G_j(x)$ if $i \neq j$.

By Lemma 3.3, the number of elements $\overline{\theta} \in A/\mathcal{P}_i^e$ satisfying $G_i(\theta) \equiv 0 \pmod{\mathcal{P}_i}$ and also the condition $G_i(\theta) \notin \mathcal{P}_i^e$ is equal to f_i if $e_i = 1$ and equal to $f_i(p^{f_i} - 1)p^{f_i(e_i - 2)}$ if $e_i \geq 2$.

It follows that the number of

$$(\theta_1 + \mathcal{P}_1^{e_1}, \ldots, \theta_r + \mathcal{P}_r^{e_r}) \in A/\mathcal{P}_1^{e_1} \times ... \times A/\mathcal{P}_r^{e_r}$$

satisfying the conditions $G_i(\theta_i) \equiv 0 \pmod{\mathcal{P}_i}$ for $i = 1, \ldots, r$ and the condition $G_i(\theta_i) \notin \mathcal{P}_i^e$ for all i such that $e_i \geq 2$ is equal to

$$\prod_{j=1}^{r} f_j \prod_{e_j \geq 2} f_j(p^{f_j} - 1)p^{f_j(e_j - 2)} = p^{\sum_{e_j \geq 2} f_j(e_j - 2)} \prod_{j=1}^{r} f_j \prod_{e_j \geq 2} (p^{f_j} - 1)$$

We now count the number of equivalence classes which means the number of $(G_1(x), ..., G_r(x))$ such that $G_i(x)$ is a monic irreducible polynomial in $\mathbb{F}_p[x]$ of degree f_i and such that $G_i(x) \neq G_j(x)$ for $i \neq j$. Recall that the f_i in Theorem 2.4 are labelled in a particular order.

For each $j = 1, ..., s$, there exists $A_{r_j}^{N_p(f_j^*)}$ possibilities. Then, the number of equivalence classes is equal to $\prod_{j=1}^{s} A_{r_j}^{N_p(f_j^*)}$, thus

$$N = p^{\sum_{e_j \geq 2} f_j(e_j - 2)} \prod_{j=1}^{r} f_j \prod_{e_j \geq 2} (p^{f_j} - 1) \prod_{j=1}^{s} A_{r_j}^{N_p(f_j^*)} \qquad \square$$

Proposition 3.4. *Let s be the integer defined in the above theorem, then*

$$p^s \mid \mu_K(p) \text{ and } \mu_K(p) \equiv 1 \pmod{p-1}$$

Proof. Since for any $j = 1, ..., s$, we have that $p \mid f_j^* N_p(f_j^*)$, then the first assertion follows from Equation (3.1). For the proof of the second part, we define an equivalence relation in A/pA as follows. The elements $\overline{\alpha}$ and $\overline{\beta}$ of A/pA are said to be equivalent if there exists $\lambda \in \mathbb{F}_p^*$ such that $\overline{\beta} = \lambda\overline{\alpha}$. It is clear that if $\overline{\alpha}$ and $\overline{\beta}$ are equivalent and if $p \mid I(\beta)$, then $p \mid I(\alpha)$. Except the class of 0 which contains only one element, all the others contains exactly $p - 1$ elements. Let u be the number of classes of the elements $\overline{\alpha}$ such that $p \mid I(\alpha)$. Then $\mu_K(p) = 1 + u(p - 1)$ and the result follows. $\square$

Definition 3.5. Let K be a number field, A be its ring of integers and p be a prime number. We say that p has a special splitting in K if all the prime ideals of A lying over $p\mathbb{Z}$ have the same ramification index e and also the same residual degree f. Let r be the number of these prime ideals, then $n = efr$. The elements e, f, r will be called the parameters of the special splitting.

Notice that for a Galois number field K, all prime numbers have special splittings in K.

Corollary 3.6. *Let K be a number field of degree n and p be a prime number having a special splitting in K with parameters e, f, r, then*

$$\mu_K(p) = \begin{cases} p^n - f^r A_r^{N_p(f)} & \text{if } e = 1 \\ p^n - f^r (p^f - 1)^r p^{rf(e-2)} A_r^{N_p(f)} & \text{if } e \geq 2 \end{cases}$$

The following table, computed by using Equation (3.1), lists the values of $\mu_K(p)$ for a quartic field K depending on the splitting type of p into a product of prime ideals.

The splitting of p in A	$\mu_K(p)$
$\mathcal{P}_4$	p^2
$\mathcal{P}_1^4$	p^3
$\mathcal{P}_2^2$	p^3+p^2-p
$\mathcal{P}_1^3\mathcal{P}_1'$	$2p^3-p^2$
$\mathcal{P}_2\mathcal{P}_2'$	$2p^3+p^2-2p$
$\mathcal{P}_1\mathcal{P}_3$	p^2
$\mathcal{P}_1^2\mathcal{P}_2$	$2p^3-p^2$
$\mathcal{P}_1^2\mathcal{P}_1'^2$	$3p^3-3p^2+p$
$\mathcal{P}_1\mathcal{P}_1'\mathcal{P}_2$	$2p^3-p^2$
$\mathcal{P}_1\mathcal{P}_1'\mathcal{P}_1''^2$	$4p^3-5p^2+2p$
$\mathcal{P}_1\mathcal{P}_1'\mathcal{P}_1''\mathcal{P}_1'''$	$6p^3-11p^2+6p$

TABLE 3.1.

The index of each prime ideal in Table 3.1 represents its residual degree over $p\mathbb{Z}$

Remark 3.7. Let p be a prime number, K be a number field of degree n, A be its ring of integers and $\omega_1, \ldots, \omega_n$ be an integral basis of K. For any element $\theta \in A$ of the form $\theta = \sum_{i=1}^n x_i\omega_i$ with $x_i \in \mathbb{Z}$ and $0 \leq x_i \leq p-1$ it is possible to determine if $p \mid I(\theta)$ or not. Therefore we may compute $\mu_K(p)$ this way. On the other hand, using Equation (3.1), we may compute the table of all the possible values of $\mu_K(p)$ in a number field of degree n

depending on the splitting of p. Comparing the value found by the first way with the values appearing in the table, it is possible to determine in some cases the precise splitting of p in the given field or in any case to exclude some type of splitting of p for the particular field we are considering. For example, if in a quartic field we have found that the value of $\mu_K(2)$ is equal to $8, 10$ or 14, then, looking at the above table, one may find how the prime 2 splits in the field K.

Corollary 3.8. *Let K and K' be two finite extensions of $\mathbb{Q}$ of the same degree n, A and A' be their respective rings of integers. Let p be a prime number having special splittings in K and $K^{'}$ given by*

$$pA = \mathcal{P}_1^e \cdots \mathcal{P}_r^e \tag{3.3}$$

and

$$pA' = \mathcal{P}_1'^{e'} \cdots \mathcal{P}_{r'}'^{e'} \tag{3.4}$$

respectively, where the common degree of the $\mathcal{P}_i$ is f and the degree of the $\mathcal{P}_i'$ is f'. Suppose that $\mu_K(p) = \mu_{K'}(p)$ and p is not a c.f.i. in K. Then p is not a c.f.i. in K' and if $f = f'$, then $e = e'$ and $r = r'$.

Proof. The first assertion is trivial. For the second, suppose by contradiction that $r < r'$.

Case 1: e and $e' \geq 2$. We have

$$\begin{aligned} \mu_K(p) &= p^n - f^r(p^f-1)^r p^{rf(e-2)} A_r^{N_p(f)} \\ &= p^n - p^n\left(\frac{p^f-1}{p^f}\right)^r \prod_{k=0}^{r-1} \frac{f(N_p(f)-k)}{p^f} \end{aligned} \tag{3.5}$$

and

$$\mu_{K'}(p) = p^n - p^n\left(\frac{p^f-1}{p^f}\right)^{r'} \prod_{k=0}^{r'-1} \frac{f(N_p(f)-k)}{p^f} \tag{3.6}$$

Our aim is to order $\mu_K(p)$ and $\mu_{K'}(p)$, so we compare the number

$$a(p) = \left(\frac{p^f-1}{p^f}\right)^r \prod_{k=0}^{r-1} \frac{f(N_p(f)-k)}{p^f}$$

with

$$a'(p) = \left(\frac{p^f-1}{p^f}\right)^{r'} \prod_{k=0}^{r'-1} \frac{f(N_p(f)-k)}{p^f}$$

Because $r < r'$, then

$$\left(\frac{p^f-1}{p^f}\right)^r > \left(\frac{p^f-1}{p^f}\right)^{r'} \tag{3.7}$$

We have

$$\prod_{k=0}^{r'-1}\frac{f(N_p(f)-k)}{p^f}=\prod_{k=0}^{r-1}\frac{f(N_p(f)-k)}{p^f}\prod_{k=r}^{r'-1}\frac{f(N_p(f)-k)}{p^f}$$

Clearly, for any $k=r,\dots,r'-1$, we have

$$f(N_p(f)-k)<p^f$$

hence,

$$\prod_{k=r}^{r'-1}\frac{f(N_p(f)-k)}{p^f}<1$$

It follows that

$$\prod_{k=0}^{r'-1}\frac{f(N_p(f)-k)}{p^f}<\prod_{k=0}^{r-1}\frac{f(N_p(f)-k)}{p^f} \tag{3.8}$$

Now, Equations (3.7) and (3.8) yield $a'(p)<a(p)$. Therefore, by Equations (3.5) and (3.6), we conclude that $\mu_K(p)<\mu_{K'}(p)$ which is a contradiction.

Case 2: $e=1$ and $e'\geq 2$. In this case, $\mu_K(p)=\mu_{K'}(p)$ implies that

$$f^rA_r^{N_p(f)}=f^{r'}(p^f-1)^{r'}p^{r'f(e'-2)}A_{r'}^{N_p(f)}$$

where $r=e'r'$. Hence,

$$f^{r-\frac{r}{e'}}\prod_{k=\frac{r}{e'}}^{r-1}(N_p(f)-k)=(p^f-1)^{\frac{r}{e'}}p^{\frac{r}{e'}f(e'-2)} \tag{3.9}$$

On the other hand, we have

$$f^{r-\frac{r}{e'}}\prod_{k=\frac{r}{e'}}^{r-1}(N_p(f)-k)=\prod_{k=\frac{r}{e'}}^{r-1}[f(N_p(f)-k)]$$

Clearly, for every nonzero integer k, we have

$$f(N_p(f)-k)<f(N_p(f)<p^f-1$$

Then

$$f^{r-\frac{r}{e'}}\prod_{k=\frac{r}{e'}}^{r-1}(N_p(f)-k)<(p^f-1)^{r-\frac{r}{e'}} \tag{3.10}$$

On the other hand, we have

$$(p^f-1)^{\frac{r}{e'}}p^{\frac{r}{e'}f(e'-2)}\geq(p^f-1)^{\frac{r}{e'}}(p^f-1)^{\frac{r}{e'}(e'-2)}$$

hence,

$$(p^f-1)^{\frac{r}{e'}}p^{\frac{r}{e'}f(e'-2)}\geq p^f-1)^{\frac{r}{e'}(e'-1)}=(p^f-1)^{r-\frac{r}{e'}} \tag{3.11}$$

Now, Equations (3.11) and (3.10) are in contradiction with Equation (3.9). □

Remark 3.9. Let K and K' be two number fields of the same degree n and let p be a prime number having special splittings in K and $K^{'}$ with parameters e, f, r and e', f', r' respectively. Suppose that $\mu_K(p) = \mu_{K'}(p)$ and that p is not a c.f.i. in K. We are unable to prove that if $e = e'$ (resp. $r = r'$), then $f = f'$.

We propose the following.

Conjecture 3.10. *Suppose that $\mu_K(p) = \mu_{K'}(p)$ for two number fields of the same degree $n \geq 3$ and for a prime number p , not a c.f.i. in K and having special splittings in K and K', with parameters e, f, r and e', f', r' respectively. Then $e = e'$, $f = f'$ and $r = r'$.*

Theorem 3.12 below, shows that this conjecture is true for large primes. The following lemma, due to P. Erdős and J. Selfridge (see [4]), will be used in the proof of the next result.

Lemma 3.11. *The diophantine equation*

$$(x+1)\cdots(x+m) = y^k \tag{3.12}$$

with k and $m \geq 2$ has no solutions in nonnegative integers x and y.

Theorem 3.12. *Let K and K' be two number fields of the same degree $n \geq 3$ and p be a prime having special splittings in K and $K^{'}$ with parameters e, f, r and e', f', r' respectively. Suppose that p is not a c.f.i. in K, $\mu_K(p) = \mu_{K'}(p)$ and $p > 2(\frac{n}{4})^{\frac{n}{2}-1}$. Then $f = f'$, $e = e'$ and $r = r'$.*

Proof. We distinguish three cases: e and $e' \geq 2$ or $e = e^{'} = 1$ or $e = 1$ and $e' \geq 2$.

Case 1: e and $e' \geq 2$

The equality $\mu_K(p) = \mu_{K'}(p)$ is equivalent to:

$$f^r(p^f-1)^r p^{rf(e-2)} A_r^{N_p(f)} = f'^{r'}(p^{f'}-1)^{r'} p^{r'f'(e'-2)} A_{r'}^{N_p(f')} \tag{3.13}$$

Equating the p-adic valuations of the two sides of Equation (3.13), we obtain:

$$rf(e-2) + \frac{f}{\mathrm{rad}(f)} = r'f'(e'-2) + \frac{f'}{\mathrm{rad}(f')}$$

Since $efr = e'f'r'$, then

$$2(rf - r'f') = \frac{f}{\mathrm{rad}(f)} - \frac{f'}{\mathrm{rad}(f')} \tag{3.14}$$

On the other hand, after dividing in Equation (3.13), by $p^{\nu_p(\mu_K(p))}$ which is equal to $p^{\nu_p(\mu_{K'}(p))}$, we obtain:

$$\begin{aligned}(3.15)\quad & f^r(p^f-1)^r\frac{N_p(f)}{p^{\frac{f}{\mathrm{rad}(f)}}}(N_p(f)-1)\dots(N_p(f)-(r-1))\\ &= f'^{r'}(p^{f'}-1)^{r'}\frac{N_p(f')}{p^{\frac{f'}{\mathrm{rad}(f')}}}(N_p(f')-1)\dots(N_p(f')-(r'-1))\end{aligned}$$

Since $N_p(f)=\big(p^f-\sum p^{f/l}+\sum p^{f/l_1l_2}-\ldots\pm p^{f/\mathrm{rad}(f)}\big)/f$, where the k-th sum runs over selections of k distinct prime factors of f, then

$$\begin{aligned}&N_p(f)/p^{f/\mathrm{rad}(f)}\\ &\quad=\Big(p^{f-f/\mathrm{rad}(f)}-\sum p^{f/l-f/\mathrm{rad}(f)}+\sum p^{f/l_1l_2-f/\mathrm{rad}(f)}-\ldots\pm 1\Big)/f\\ &\quad\equiv(\pm1)/f\pmod p\end{aligned}$$

Similarly, we have $N_p(f')/p^{f'/\mathrm{rad}(f')}\equiv(\pm1)/f'\pmod p$. Reducing Equation (3.15) modulo p and using the preceding congruences, we obtain:

$$\epsilon f^{r-1}(r-1)!\equiv\epsilon' f'^{r'-1}(r'-1)!\pmod p$$

where ϵ and $\epsilon'\in\{1,-1\}$. We deduce that

$$f^{r-1}(r-1)!\equiv\pm f'^{r'-1}(r'-1)!\pmod p \tag{3.16}$$

Since $e\geq 2$, then $fr\leq n/2$, hence

$$\begin{aligned}f^{r-1}(r-1)!&\leq f^{r-1}(\frac{(1+(r-1))}{2})^{r-1}\\ &=(\frac{fr}{2})^{r-1}\leq(\frac{n}{4})^{r-1}\leq(\frac{n}{4})^{n/2-1}\end{aligned}$$

Similarly, we have $f'^{r'-1}(r'-1)!\leq(\frac{n}{4})^{\frac{n}{2}-1}$. The assumption on the magnitude of p, shows that we have the sign $+$ in Equation (3.16) and then

$$f^{r-1}(r-1)!=f'^{r'-1}(r'-1)! \tag{3.17}$$

Without loss of generality, we may suppose that $f'\leq f$, which in turn, by Equation (3.17), implies $r\leq r'$. Let $\lambda=\frac{(r'-1)!}{(r-1)!}$ and let q be a prime factor of f', then writing Equation (3.17) in the form $f^{r-1}=\lambda f'^{r'-1}$, we get

$$\nu_q(\lambda)+(r'-1)\nu_q(f')=(r-1)\nu_q(f)\leq(r'-1)\nu_q(f)$$

hence $\nu_q(f')\leq\nu_q(f)$. Using Equation (3.14), we show that, here in fact, we have equality. Let $t=\nu_q(f')$. Suppose that $\nu_q(f)>t$, then

$$\nu_q(2(rf-r'f'))\geq t,\text{ while }\nu_q\Big(\frac{f}{\mathrm{rad}(f)}-\frac{f'}{\mathrm{rad}(f')}\Big)=t-1$$

contradicting Equation (3.14). We conclude that for any prime factor of f' (if any), we have $\nu_q(f') = \nu_q(f)$.

Suppose that $f' > 1$ and let q be a prime factor of f'. If $r < r'$, then

$$\nu_q(f^{r-1}(r-1)!) = (r-1)\nu_q(f) + \nu_q((r-1)!) < (r'-1)\nu_q(f') + \nu_q((r'-1)!)$$

contradicting Equation (3.17). It follows that $r = r'$ and then $f = f'$ by Equation (3.17) and the proof is complete in this case.

Suppose that $f' = 1$. In this case Equations (3.14) and (3.17) take the form

$$2(rf - r') = \frac{f}{\operatorname{rad}(f)} - 1 \tag{3.18}$$

and

$$f^{r-1}(r-1)! = (r'-1)! \tag{3.19}$$

respectively.

• Suppose that $f' = 1$ and $r \geq 3$. If $r' = r+1$, then , by Equation (3.19), $f^{r-1} = r$, hence a contradiction. If $r' \geq r+2$, then from Equation (3.19), we get the following $f^{r-1} = (r'-1)(r'-2)\cdots r$. According to Lemma 3.11, this equation has no solution. Therefore, Theorem 3.12 is proved in this case.

• Suppose that $f' = 1$ and $r = 2$. From Equation (3.18), we conclude that $f/\operatorname{rad}(f)$ is odd, hence $f \not\equiv 0 \pmod 4$, thus $r' \leq 3$ by Equation (3.19). We may reject the possibility $r = 2$ and $r' = 3$, since in this case Equations (3.18) and (3.19) are contradictory. Therefore $r' = r = 2$ and then $f = 1$ by Equation (3.19) and the proof is complete in this case.

• Suppose that $f' = 1$ and $r = 1$. Equation (3.19) implies $r' \in \{1, 2\}$. If $r' = 2$, then from Equation (3.18), we get

$$f/\operatorname{rad}(f) = 2f - 3 \tag{3.20}$$

Set $f = \alpha\beta$, where α and β are coprime positive integers such that α is squarefree and β satisfies the condition: for any prime factor l of β, we have $\nu_l(\beta) \geq 2$. Set $\beta = \prod l^h$. Then Equation (3.20) reads: $\prod l^{h-1} = 2\alpha\beta - 3$. We conclude that $\beta = 1$ or $\beta = 3^2$. In the first case, Equation (3.20) becomes $1 = 2f - 3$, that is $f = 2$. Straightforward computations, using Corollary 3.6, shows that we cannot have $\mu_K(p) = \mu_{K'}(p)$ if $r = 1$, $f = 2$ and $r' = 2$, $f' = 1$. We conclude that $r' = 1 = r$. Equation (3.18) takes the form $f/\operatorname{rad}(f) = 2f - 1$. Using the representation of f as above, we obtain $\prod l^{h-1} = 2\alpha\beta - 1$. It follows that $\beta = 1$ and then $2\alpha = 2$, thus $f = \alpha = 1 = f'$ and the theorem is proved in this case.

Case 2: $e = e' = 1$

In this case, the condition $\mu_K(p) = \mu_{K'}(p)$ implies:

$$f^r A_r^{N_p(f)} = f'^{r'} A_{r'}^{N_p(f')} \tag{3.21}$$

Here also, we may assume that $f' \leq f$ and $r \leq r'$. As in case 1, equating the p-adic valuations of the two sides of Equation (3.21) and reducing modulo p these sides after dividing them by the greatest power of p dividing them, we obtain the following equations:

$$\frac{f}{\mathrm{rad}(f)} = \frac{f'}{\mathrm{rad}(f')} \tag{3.22}$$

$$f^{r-1}(r-1)! = f'^{r'-1}(r'-1)! \tag{3.23}$$

As above write f and f' in the forms $f = \alpha\beta$ and $f' = \alpha'\beta'$. Equation (3.22) implies $\beta = \beta'$. Equation (3.23) takes the form:

$$\alpha^{r-1}\beta^{r-1} = \alpha'^{r'-1}\beta^{r'-1}(r'-1)\cdots r \tag{3.24}$$

Suppose that $r < r'$, then Equation (3.24) implies that $\beta = 1$. It follows that

$$\alpha^{r-1} = \alpha'^{r'-1}(r'-1)\cdots r \tag{3.25}$$

Since α and α' are squarefree, then $\alpha' = 1$, thus $f' = 1$ and Equation (3.25) becomes

$$\alpha^{r-1} = (r'-1)\cdots r \tag{3.26}$$

We may exclude the case $r = 1$, otherwise we have $r' = 2$ by Equation (3.26) and then $n = e'f'r' = 2$, which is rejected by assumption. If $r = 2$, then by Equation (3.26), $\alpha = (r'-1)\cdots r$. Since α is squarefree, then $r' = 3$ or $r' = 4$. If $r' = 3$, then $efr = 4$ and $e'f'r' = 3$, which is a contradiction. The same arguments may reject the case $r = 2$ and $r' = 4$. It remains to consider the case $r' > r > 2$. If $r' \geq r + 2$, then, according to Lemma 3.11, already used above, Equation (3.26) has no nonnegative integral solutions. So we reject this possibility. If $r' = r + 1$, then $r = f^{r-1}$ by Equation (3.26). We deduce that $efr = f^r$ and $e'f'r' = r+1 = f^{r-1}+1$, which is a contradiction. We conclude that $r = r'$ and then obviously $f = f'$.

Case 3: $e = 1$ *and* $e' \geq 2$

By the same reasonning as in cases 1 and 2, the equation $\mu_K(p) = \mu_{K'}(p)$ implies the following two

$$\frac{f}{\mathrm{rad}(f)} = \frac{f'}{\mathrm{rad}(f')} + r'f'(e'-2) \tag{3.27}$$

$$f^{r-1}(r-1)! = f'^{r'-1}(r'-1)! \tag{3.28}$$

Since $e' \geq 2$ and $efr = e'f'r'$, then $fr \geq 2f'r'$, so $fr > f'r'$. This implies $r > r'$ or $f > f'$.

• Suppose that $r > r'$. If $f = 1$, then from Equation (3.28), we get

$$f'^{r'-1} = (r-1)\cdots r' \tag{3.29}$$

If moreover $r = r'+1$, then $r' = f'^{r'-1}$ by Equation (3.29). We deduce that $efr = r = r'+1 = f'^{r'-1}+1$ and $e'f'r' \geq 2f'^{r'}$, which is a contradiction. So we may suppose that $r \geq r'+2$. By Lemma 3.11, applied to Equation (3.29), we conclude that $r' = 2$ and

$$f' = (r-1)! \tag{3.30}$$

Since $f = 1$, then by Equation (3.27), f' is squarefree and $e' = 2$. Since $r \geq r'+2$, then $r \geq 4$. Equation (3.30) implies that $r = 4$ and then $f' = 6$. It follows that $efr = 4$ and $e'f'r' = 24$ which is a contradiction. Suppose now that $f \geq 2$. From Equation (3.28), we deduce that

$$f'^{r'-1} = f^{r-1}(r-1)\cdots r' \tag{3.31}$$

It follows that $f^{r-1} \mid f'^{r'-1}$. Let q be a prime factor of f, then $(r-1)\nu_q(f) \leq (r'-1)\nu_q(f') < (r-1)\nu_q(f')$, thus $\nu_q(f) < \nu_q(f')$. We deduce that $f \mid f'$ and $\dfrac{f}{\operatorname{rad}(f)} < \dfrac{f'}{\operatorname{rad}(f')}$, contradicting Equation (3.27).

• Suppose that $f > f'$. Since we have considered the case $r > r'$, we may suppose that $r \leq r'$. If $r = r'$, then by Equation (3.28), $f = f'$, which is a contradiction. So we suppose that $r < r'$. From Equation (3.28), we obtain

$$f^{r-1} = f'^{r'-1}(r'-1)\cdots r \tag{3.32}$$

Suppose first that $f' = 1$, then $f^{r-1} = (r'-1)\cdots r$. If morover $r' = r+1$, then $r = f^{r-1}$ and $r' = f^{r-1}+1$. In this situation Equation (3.27) takes the form

$$\frac{f}{\operatorname{rad}(f)} = 1 + (f^{r-1}+1)(e'-2) \tag{3.33}$$

This equation has no solution except possibly if $e' = 2$ or $r = 1$. In the first case, we have $efr = f^r$ and $e'f'r' = 2(f^{r-1}+1)$, which is impossible. In the second case, we have $efr = f$ and $e'f'r' = 2e'$, hence $2e' = f$. On the other hand, by Equation (3.33), we get $f/\operatorname{rad}(f) = 2e'-3$. We deduce that $f/\operatorname{rad}(f) = f-3$. Using the representation $f = \alpha\beta$, it is seen that this equation has no solution. We conclude that $r' \geq r+2$. Lemma 3.11 applied to Equation (3.31) implies $r = 2$ and $f = (r'-1)\cdots r$. Since $efr = r(r'-1)\cdots r$ and r is even, then so are efr and $e'f'r'$. It follows that e' is even or r' is even. In any case Equation (3.27) implies that $f/\operatorname{rad}(f)$ is odd. We deduce that $f \not\equiv 0 \pmod 4$. From the identity $f = (r'-1)\cdots r$ and the condition $r' \geq r+2$, we conclude that $r' = 4$ and $f = 6$. Hence $e' = 2$ by Equation (3.27) and then $efr = 12$, $e'f'r' = 8$, which is a contradiction. It remains to consider the case $f > f' \geq 2$ and $r < r'$. From

Equation (3.31), we conclude that ${f'}^{r'-1} \mid f^{r-1}$. Let q be a prime factor of f', then $(r'-1)\nu_q(f') \leq (r-1)\nu_q(f) < (r'-1)\nu_q(f)$, thus

$$\nu_q(f') < \nu_q(f) \tag{3.34}$$

Since $f' \geq 2$, then f' has a prime factor say q_0. Let $h = \nu_{q_0}(f')$, then

$$\nu_{q_0}(r'f'(e'-2)) \geq h \,\text{and}\, \nu_{q_0}(f'/\operatorname{rad}(f')) = h-1$$

hence

$$\nu_{q_0}(r'f'(e'-2)) + f'/\operatorname{rad}(f')) = h-1$$

By Equation (3.27), we conclude that $\nu_{q_0}(f/\operatorname{rad}(f)) = h-1$, hence $\nu_{q_0}(f) = h = \nu_{q_0}(f')$, contradicting Equation (3.34) and the proof of Theorem 3.12 is complete. □

Remark 3.13. It is not possible to remove the condition $n \geq 3$ in Theorem 3.12, since for any quadratic number field K, and any prime p, whatever is its splitting, we have $\mu_K(p) = p$.

In the same theorem, the condition, p is not a c.f.i. in K is necessary only for small n. Because if $n \geq 7$, then $n \leq 2(\frac{n}{4})^{\frac{n}{2}-1}$, so that, according to Zylinsky's result, any prime number larger than or equal to this last number is not a c.f.i. in K.

It is seen, through Equation (3.1), that $\mu_K(p)$ is a polynomial in p with integral coefficients. These polynomials are computed for quartic fields (see Table 3.1). Theorem 3.12 implies that if restrict ourselves to primes having special splittings, then the list of polynomials which are obtained, are all distinct.

References

[1] M. Ayad & O. Kihel, "Common Divisors of values of Polynomials and Common Factors of Indices in a Number Field", *Inter. J. Number Theory* **7** (2011), no. 5, p. 1173-1194.

[2] L. Carlitz, "On abelian fields", *Trans. Amer. Math. Soc.* **35** (1933), p. 505-517.

[3] ———, "A note on common index divisors", *Proc. Amer. Math. Soc.* **3** (1952), p. 688-692.

[4] P. Erdős & J. Selfridge, "The product of consecutive integers is never a power", *Illinois, J. Math.* **19** (1975), p. 292-301.

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

[6] H. Hancock, *Foundations of the theory of algebraic numbers. Vol. II.: The general theory.*, Dover Publications, 1964, xxvi+654 pages.

[7] T. Nagell, "Quelques résultats sur les diviseurs fixes de l'index des nombres entiers d'un corps algébrique", *Ark. Mat.* **6** (1966), p. 269-289.

[8] B. K. Spearman & K. S. Williams, "Cubic fields with index 2", *Monatsh. Math.* **134** (2002), no. 4, p. 331-336.

[9] ———, "The index of a Cyclic Quartic field", *Monatsh. Math.* **140** (2003), no. 1, p. 19-70.

[10] E. Von Zylinski, "Zur Theorie der aussewescentlicher Discriminantenteiler algebraischer Korper", *Math. Ann.* **73** (1913), p. 273-274.

Mohamed Ayad
Laboratoire de Mathématiques Pures et Appliquées
Université du Littoral
62228 Calais, France
E-mail: ayad@lmpa.univ-littoral.fr

Rachid Bouchenna
Laboratoire d'Arithmétique, Codage et Combinatoire
Université des Sciences et Technologies Houari Boumediène 16324
El Alia, Alger, Algeria
E-mail: rbouchenna@usthb.dz

Omar Kihel
Department of Mathematics
Brock University
Ontario, Canada L2S 3A1, Canada
E-mail: okihel@brocku.ca