



HAL
open science

On fixed divisors of the values of the minimal polynomials over \mathbb{Z} of algebraic numbers

M Ayad, A Bayad, O Kihel

► **To cite this version:**

M Ayad, A Bayad, O Kihel. On fixed divisors of the values of the minimal polynomials over \mathbb{Z} of algebraic numbers. Hardy-Ramanujan Journal, 2023, Volume 45 - 2022, pp.57 – 73. 10.46298/hrj.2023.10748 . hal-03913479

HAL Id: hal-03913479

<https://hal.science/hal-03913479>

Submitted on 27 Dec 2022

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

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

On fixed divisors of the values of the minimal polynomials over \mathbb{Z} of algebraic numbers

M. Ayad, A. Bayad and O. Kihel

Abstract. Let K be a number field of degree n , A be its ring of integers, and A_n (resp. K_n) be the set of elements of A (resp. K) which are primitive over \mathbb{Q} . For any $\gamma \in K_n$, let $F_\gamma(x)$ be the unique irreducible polynomial in $\mathbb{Z}[x]$, such that its leading coefficient is positive and $F_\gamma(\gamma) = 0$. Let $i(\gamma) = \gcd_{x \in \mathbb{Z}} F_\gamma(x)$, $i(K) = \text{lcm}_{\theta \in A_n} i(\theta)$ and $\hat{i}(K) = \text{lcm}_{\gamma \in K_n} i(\gamma)$. For any $\gamma \in K_n$, there exists a unique pair (θ, d) , where $\theta \in A_n$ and d is a positive integer such that $\gamma = \theta/d$ and $\theta \not\equiv 0 \pmod{p}$ for any prime divisor p of d . In this paper, we study the possible values of $\nu_p(d)$ when $p|i(\gamma)$. We introduce and study a new invariant of K defined using $\nu_p(d)$, when γ describes K_n . In the last theorem of this paper, we establish a generalisation of a theorem of MacCluer.

Keywords. Values of polynomials, Denominators of algebraic numbers, Splitting of prime numbers.

2010 Mathematics Subject Classification. 11R04, 12Y05.

1. Introduction

Let K be a number field of degree $n \geq 2$ and A be its ring of integers. Denote by A_n (resp. K_n) be the set of elements of A (resp. K) which are primitive over \mathbb{Q} , that is those elements which generate K over \mathbb{Q} . For any primitive polynomial $g(x) \in \mathbb{Z}[x]$, we define the integer $i(g)$ by

$$i(g) = \gcd_{x \in \mathbb{Z}} g(x).$$

Let γ be an algebraic number. When we refer to the minimal polynomial of γ over \mathbb{Z} , we mean the unique polynomial $F_\gamma(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, irreducible such that $a_n > 0$ and $F_\gamma(\gamma) = 0$. The leading coefficient a_n will be denoted by $c(\gamma)$. We set $i(\gamma) = i(F_\gamma)$. In [GuMc70], Gunji and McQuillan defined the integer $i(K)$ by

$$i(K) = \text{lcm}_{\theta \in A_n} i(\theta).$$

MacCluer [Mac71] proved that a given prime p divides $i(K)$ if and only if the number of prime ideals of A lying over p is at least equal to p . In [GuMc70] or [AyKi11], it is proved that there exists $\theta \in A_n$ such that

$$i(K) = i(\theta).$$

The smallest positive integer d such that $d\gamma$ is an algebraic integer is called the denominator of γ and will be denoted by $d(\gamma)$.

Arno et al proved in [ARW96] that the density of the set of the algebraic numbers γ such that $c(\gamma) = d(\gamma)$ is equal to $1/\zeta(3) = 0.8319 \dots$. In [ABK15], for a fixed number field K , the set

$$T_p(k) = \{t \geq 1, \text{ there exists } \gamma \in K_n, \nu_p(d(\gamma)) = k \text{ and } \nu_p(c(\gamma)) = t\}$$

is connected to the splitting of the prime p in K .

In this paper, among other results, we study the possible values of $\nu_p(d)$ when $p \mid i(\gamma)$. After recalling some lemmas in section 2, it is proved in Theorem 3.1 that if $\theta \not\equiv 0 \pmod{pA}$ and $p \mid i(\theta/p^k)$, for some positive integer k , then the p -adic valuation of the leading coefficient of the minimal polynomial of θ/p^k belongs to the set $\{k, k+1, \dots, (n-p)k\}$. Furthermore any element of this set may occur. Section 4 shows that given $\theta \in A_n$ such that $\theta \not\equiv 0 \pmod{pA}$, it is possible to find explicitly the values of $k \in \mathbb{N}$, if any, such that $p \mid i(\theta/p^k)$. Fix $\theta \in A_n$ such that $\theta \not\equiv 0 \pmod{pA}$ and define the set $V_p(\theta) = \{k \in \mathbb{N} ; p \mid i(\theta/p^k)\}$. On the one hand it is shown that $|V_p(\theta)|$ for $\theta \in A_n$ is bounded by some constant depending on n and p . On the other hand the values of k are bounded by a constant depending on p and $\nu_p(N_{K/\mathbb{Q}}(\theta))$, where $\nu_p(a)$ denotes the p -adic valuation of a . Section 5 deals with this last bound. It is shown that, even if we fix the field K , the values of k may be greater than any given positive constant. In this section, we give examples of Galois number fields K of degree 4 (resp. 3) for which the set of the values of k , when θ runs in A_n is $\{0\}$ (resp. \mathbb{N}). Throughout this paper we denote by \mathbb{N} the set of nonnegative integers. The paper ends with remarks and open questions.

2. Indices and denominators of algebraic numbers

Let K be a number field of degree n , A its ring of integers, $\gamma \in K_n$ and let $g(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ be the unique primitive polynomial of degree n such that $a_n > 0$ and $g(\gamma) = 0$. We denote this polynomial $F_\gamma(x)$. This polynomial will be called the minimal polynomial of γ over \mathbb{Z} . The leading coefficient a_n will be denoted $c(\gamma)$.

Let

$$\mathfrak{J}(\gamma) = \{m \in \mathbb{Z}, m\gamma \in A\},$$

then $\mathfrak{J}(\gamma)$ is a nonzero ideal of \mathbb{Z} , hence a principal ideal generated by some positive integer denoted by $d(\gamma)$. The integer $d(\gamma)$ is called the denominator of γ . Since $c(\gamma) \in \mathfrak{J}(\gamma)$, then $d(\gamma) \mid c(\gamma)$. Write $\gamma = \frac{\theta}{d(\gamma)}$, where $\theta \in A_n$, then θ is unique and we call it the numerator of γ . Let $f(x)$ be the minimal polynomial of θ over \mathbb{Q} , then $g(x) = f(d(\gamma)x)/\text{cont}(f(d(\gamma)x)$, where the abbreviation $\text{cont}(h(x))$ denotes the content of the polynomial $h(x)$. From [ARW96] we have the following result:

Lemma 2.1. *For any prime p , we have*

$$\nu_p(d(\gamma)) = \max \left(0, \max_{j=0}^{n-1} \left\lceil \frac{\nu_p(a_n) - \nu_p(a_j)}{n-j} \right\rceil \right). \quad (2.1)$$

From Lemma 2.1 we see that any prime factor p of $c(\gamma)$ divides $d(\gamma)$.

Summarizing the relations between $c(\gamma)$ and $d(\gamma)$, we have:

Remark 2.1. *Let K be a number field of degree n and $\gamma \in K_n$, then $d(\gamma)$ and $c(\gamma)$ have the same prime factors and for any prime p , we have $\nu_p(d(\gamma)) \leq \nu_p(c(\gamma)) \leq n\nu_p(d(\gamma))$.*

For any $\theta \in A_n$, let $F_\theta(x)$ its minimal polynomial over \mathbb{Q} . Following [GuMc70], we define the integers

$$i(\theta) = \gcd_{x \in \mathbb{Z}} F_\theta(x) \text{ and } i(K) = \text{lcm}_{\theta \in A_n} i(\theta). \quad (2.2)$$

For the integers $i(\theta)$ and $i(K)$ we have the following results:

- i) C. R. MacCluer proved in [Mac71] that for a given prime number p , p divides $i(K)$ if and only if the number of prime ideals of A lying over p is at least equal to p .
- ii) In [GuMc70] and [AyKi11], it is proved that there exists $\theta \in A_n$ such that $i(K) = i(\theta)$, and that $i(K) = \text{lcm}_{\theta \in A} i(\theta)$.

We extend the definition of $i(\theta)$ and $i(K)$ to algebraic numbers as follows. Given any $\gamma \in K_n$, we define

$$i(\gamma) := \text{gcd}_{x \in \mathbb{Z}} F_\gamma(x) \text{ and } \hat{i}(K) = \text{lcm}_{\gamma \in K_n} i(\gamma).$$

We quote from [AyKi11] the following result.

Lemma 2.2. *Let $g(x) \in \mathbb{Z}[x]$. Write $g(x)$ in the form*

$$g(x) = b_n(x)_n + \cdots + b_1(x)_1 + b_0,$$

where $b_0, \dots, b_n \in \mathbb{Z}$,

$$(x)_0 = 1 \text{ and } (x)_j := x(x-1) \cdots (x-(j-1)), \text{ for } j \geq 1.$$

Then, we have the identity

$$i(g) = \text{gcd}_{j=0}^n (j!b_j).$$

Corollary 2.1. *The integers $i(\gamma)$, $i(K)$ and $\hat{i}(K)$ divide $n!$.*

Remark 2.2. *Clearly, from the definitions of $i(K)$ and $\hat{i}(K)$, we see that $i(K)$ divides $\hat{i}(K)$.*

3. Study of the denominators of some algebraic numbers

We prove the following lemma, which is useful for the rest of this paper:

Lemma 3.1. *Let p be a prime number, γ be an algebraic number and $d(\gamma)$ be its denominator. Write $d(\gamma)$ in the form $d(\gamma) = p^k \cdot q$, where $\text{gcd}(p, q) = 1$ and let $\mu = q\gamma$. Then we have*

$$d(\mu) = p^k, \nu_p(c(\mu)) = \nu_p(c(\gamma)) \text{ and } \nu_p(i(\gamma)) = \nu_p(i(\mu)).$$

Proof: Let $\gamma = \theta/pk_q$ where θ is an algebraic integer such that $\theta \not\equiv 0 \pmod{p}$ and $\theta \not\equiv 0 \pmod{l}$ for any prime factor l of q . Then $\mu = q\gamma = \theta/pk$, hence $d(\mu) = pk$. Let n be the degree of γ over \mathbb{Q} and let $g(x) = a_n x^n + \cdots + a_1 x + a_0$ be its minimal polynomial over \mathbb{Z} . Since $a_n = c(\gamma)$ and $d(\gamma) | c(\gamma)$, then $q | a_n$. This implies that the polynomial $h(x) = q^{n-1}g(x/q) = (a_n/q)x^n + a_{n-1}x^{n-1} + \cdots + a_1q^{n-2}x + a_0q^{n-1}$ has integral coefficients and vanishes for μ . Therefore, the minimal polynomial of μ over \mathbb{Z} is given by $f(x) = h(x)/\text{cont}(h)$. Write $\text{cont}(h)$ in the form $\text{cont}(h) = \text{gcd}(q, \text{cont}(h)) \cdot \lambda$, where λ is a positive integer. We show that $\lambda = 1$. Suppose that there exists a prime number $l | \lambda$, then $l | \text{cont}(h)$ and $l \nmid q$. Since $l | a_0q^{n-1}, a_1q^{n-2}, \dots, a_{n-1}, a_n | q$, then $l | a_0, \dots, a_n$ which is a contradiction, hence $\lambda = 1$. Therefore $\text{cont}(h) | q$. Since

$$c(\mu) = (a_n/q) / \text{cont}(h) = a_n / q \text{cont}(h) = c(\gamma) / q \text{cont}(h),$$

then $V_p(c(\mu)) = V_p(c(\gamma))$. We now prove the last statement. Suppose that $p^u | i(\gamma)$ for some positive integer u and $x_0 \in \mathbb{Z}$. Since $\gcd(p, q) = 1$, there exists $y_0 \in \mathbb{Z}$ such that the congruence $qy_0 \equiv x_0 \pmod{p^u}$ holds. In particular $g(y_0) \equiv 0 \pmod{p^u}$, so that we have, $f(x_0) = h(x_0)/\text{cont}(h) = q^{n-1}g(y_0)/\text{cont}(h) \equiv 0 \pmod{p^u}$. Since x_0 was arbitrary, then $p^u | i(\mu)$. Conversely, suppose that $p^u | i(\mu)$ and let x_0 and y_0 as above. Then $f(x_0) = 0 \pmod{p^u}$, hence $q^{n-1}g(y_0)/\text{cont}(h) \equiv 0 \pmod{p^u}$, thus $g(y_0) \equiv 0 \pmod{p^u}$. Therefore $p^u | i(\gamma)$.

We state the main result of this section.

Theorem 3.1. *Let K be a number field of degree n over \mathbb{Q} and p be a prime number, Let $\gamma \in K_n$ such that $p | i(\gamma)$, $c = c(\gamma)$, $d = d(\gamma)$ and $k = v_p(d) \geq 1$. Then $p < n$ and $k \leq v_p(c) \leq (n - p)k$.*

Proof: Set $d = p^k q$ with $\gcd(p, q) = 1$. Let $\mu = q\gamma$, then $d(\mu) = p^k$ and by Lemma 3.1, we have $v_p(c(\mu)) = v_p(c(\gamma))$ and $v_p i(\mu) = v_p i(\gamma) \geq 1$. Therefore, $p | i(\mu)$. The minimal polynomial of μ over \mathbb{Z} has the form:

$$g(x) = p^t(x)_n + b_{n-1}(x)_{n-1} + \cdots + b_1(x)_1 + b_0, \text{ with } k \leq t \leq nk.$$

By corollary 2.1, $p | n!$, hence $p \leq n$. If $p = n$, since $p | j! b_j$ for all $j = 0, \dots, n - 1$, then we conclude that $p | b_0, b_1, \dots, b_{n-1}$. Therefore $g(x)$ is reducible in $\mathbb{Z}[x]$, which is a contradiction, hence $p < n$. In this case, since $p | b_0, b_1, \dots, b_{p-1}$, then we may write $g(x)$ in the form

$$g(x) = x(x-1) \cdots (x-(p-1)) \left(p^t x^{n-p} + \tilde{a}_{n-p-1} x^{n-p-1} + \cdots + \tilde{a}_1 x + \tilde{a}_0 \right) \\ + p \left(c_{p-1} x^{p-1} + \cdots + c_1 x + c_0 \right)$$

where all the coefficients \tilde{a}_i, c_j are integral. Since $g(x)$ is irreducible in $\mathbb{Z}[x]$, there exists $j \in \{0, \dots, n - p - 1\}$ such that $p \nmid \tilde{a}_j$. Denote by j_o the greatest of these integers. Let $\theta \in A_n$ be the unique element such that $\gamma = \frac{\theta}{p^k}$. Then we have

$$\theta(\theta - p^k) \cdots (\theta - (p-1)p^k) \left(p^t \theta^{n-p} + p^k \tilde{a}_{n-p-1} \theta^{n-p-1} \right. \\ \left. + \cdots + p^{k(n-p-j_o)} \tilde{a}_{j_o} \theta^{j_o} + \cdots + p^{k(n-p-1)} \tilde{a}_1 \theta + p^{k(n-p)} \tilde{a}_0 \right) \\ + p \cdot p^{k(n-(p-1))} (c_{p-1} \theta^{p-1} + c_{p-2} p^k \theta^{p-2} + \cdots + c_0 p^{k(p-1)}) = 0.$$

Write this equation in the form:

$$p^t \theta^n + u_{n-1} \theta^{n-1} + \cdots + u_p \theta^p + \cdots + u_1 \theta + u_0 = 0.$$

Since θ is integral, it follows in particular that $p^t | u_j$ for $j = p, \dots, n - 1$. We can set

$$\theta(\theta - p^k) \cdots (\theta - (p-1)p^k) = \theta^p + \sigma_1 \theta^{p-1} + \cdots + \sigma_{p-1} \theta.$$

Then

$$\left\{ \begin{array}{l} \sigma_1 = -(p^k + \cdots + p^k(p-1)) = p^k \frac{p(p-1)}{2} \\ \sigma_2 = p^{2k} \sum_{\substack{i \neq j \\ i, j \in \{1, \dots, p-1\}}} ij \\ \dots \\ \sigma_{p-1} = (-1)^{p-1} p^{k(p-1)} (p-1)!. \end{array} \right.$$

We have

$$(x^p + \sigma_1 x^{p-1} + \dots + \sigma_{p-1} x) \left(p^t x^{n-p} + \dots + p^{k(n-p-j_0)} \tilde{a}_{j_0} x^{j_0} + \dots + \tilde{a}_0 p^{k(n-p)} \right) + p p^{k(n-(p-1))} \left(c_{p-1} x^{p-1} + \dots + c_1 x \right) = p^t x^n + u_{n-1} x^{n-1} + \dots + u_p x^p + \dots + u_1 x + u_0,$$

hence

$$\begin{cases} u_{n-1} &= p^k \tilde{a}_{n-p-1} + p^t \sigma_1 \\ u_{n-2} &= p^{2k} \tilde{a}_{n-p-2} + p^k \tilde{a}_{n-p-1} \sigma_1 + p^t \sigma_2 \\ &\dots \\ u_{j_0+p} &= \tilde{a}_{j_0} p^{k(n-p-j_0)} + \tilde{a}_{j_0+1} p^{k(n-p-(j_0+1))} \sigma_1 + \dots + \tilde{a}_{j_0+m} p^{k(n-p-(j_0+m))} \sigma_m \\ &+ \dots + p^t \sigma_{n-(j_0+p)} \end{cases}$$

The first equation implies that $p^t | p^k \tilde{a}_{n-p-1}$. Then the second implies that $p^t | p^{2k} \tilde{a}_{n-p-2}$. Iterating the process, the last equation gives $p^t | \tilde{a}_{j_0} p^{k(n-p-j_0)}$. Since $p \nmid \tilde{a}_{j_0}$, then

$$t \leq k(n-p-j_0) \leq k(n-p).$$

Theorem 3.2. *Let p be a prime number, n and k be positive integers, $p < n$. Then for any integer t , such that $k \leq t \leq (n-p)k$, there exist infinitely many algebraic numbers $\gamma \in \mathbb{C}$ of degree n such that $p | i(\gamma)$, $\nu_p(c(\gamma)) = t$ and $\nu_p(d(\gamma)) = k$.*

Proof: Dividing t by k , we have two possibilities:

$$t = (n-i)k + \alpha \text{ with } 0 < \alpha < k \text{ and } p < i \leq n-1 \tag{3.3}$$

$$t = (n-i)k \text{ with } p \leq i \leq n-1 \tag{3.4}$$

- First case: $t = (n-i)k + \alpha$ with $0 < \alpha < k$ and $p < i \leq n-1$. Then, we have

$$t > (n-i)\alpha + \alpha = \alpha(n-i+1), \text{ hence } \alpha < \frac{t}{n-(i+1)}.$$

On the other hand, choose integers a_0, \dots, a_n such that

$$\begin{cases} \gcd(a_0, \dots, a_n) = 1, \\ \nu_p(a_j) = t, \text{ for } j > i \\ \nu_p(a_i) = \alpha, \text{ (note that } \alpha \neq 0) \\ \nu_p(a_{i-1}) = 0 \\ \nu_p(a_j) = 1, \text{ for } j < i-1. \end{cases} \tag{3.5}$$

Consider the polynomials

$$f(x) = \sum_{j=0}^n a_j(x)_j = \sum_{j=0}^n \tilde{a}_j x^j$$

and

$$g(x) = \tilde{a}_n x^n + q^{e_{n-1}} \tilde{a}_{n-1} x^{n-1} + \dots + q^{e_1} \tilde{a}_1 x + q \tilde{a}_0 := \sum_{j=0}^n b_j x^j,$$

where q is a prime number such that $q \equiv 1 \pmod{p}$, $q \nmid \tilde{a}_0$ and the exponents e_j are arbitrary fixed positive integers. Clearly $g(x)$ is irreducible in $\mathbb{Z}[x]$ by Eisenstein's Theorem. Let γ be a root of $g(x)$. Since $p \leq i-1$, then by Lemma 2.2, we conclude that $p \mid i(\gamma)$ and since $g(x) \equiv f(x) \pmod{p}$ for any $x \in \mathbb{Z}$, then $p \mid i(\gamma)$. We look at the p -adic valuations of the \tilde{a}_j . Recall that $\tilde{a}_n = c(\gamma)$ and $\tilde{a}_0 = a_0$, hence $\nu_p(\tilde{a}_n) = t$ and $\nu_p(\tilde{a}_0) = 1$. We claim that

$$\begin{cases} \nu_p(\tilde{a}_j) \geq t, & \text{for } j > i \\ \nu_p(\tilde{a}_i) = \alpha, \\ \nu_p(\tilde{a}_{i-1}) = 0. \end{cases} \quad (3.6)$$

For any $j \geq 1$ we have $\tilde{a}_j = a_j + \sum_{l=j+1}^n a_l c_l$, where $c_l \in \mathbb{Z}$ for any l .

If $j > i$ then $\nu_p(a_j) = \nu_p(a_{j+1}) = \dots = \nu_p(a_l) = t$, hence $\nu_p(\tilde{a}_j) \geq t$.

For $j = i$ we have $\nu_p(a_j) = \alpha < t$ and $\nu_p(a_l) = t$ for $l = i+1, \dots, n$, hence $\nu_p(\tilde{a}_i) = \alpha$.

For $j = i-1$ we have $\nu_p(a_{i-1}) = 0$ and $\nu_p(a_l) \geq \alpha$ for $l = i, \dots, n$, hence $\nu_p(\tilde{a}_{i-1}) = 0$. Thus we obtain the desired claim.

To compute the p -adic valuation of the denominator of γ , we use Lemma 2.1. For $j > i$, we have

$$\frac{\nu_p(b_n) - \nu_p(b_j)}{n-j} = \frac{\nu_p(\tilde{a}_n) - \nu_p(\tilde{a}_j)}{n-j} = \frac{t - t_j}{n-j} \leq 0, \text{ because } t_j \geq t.$$

For $j = i$, we have

$$\frac{\nu_p(b_n) - \nu_p(b_i)}{n-i} = \frac{\nu_p(\tilde{a}_n) - \nu_p(\tilde{a}_i)}{n-i} = \frac{t - \alpha}{n-i} = k.$$

For $j < i$ we have

$$\frac{\nu_p(b_n) - \nu_p(b_j)}{n-j} = \frac{\nu_p(\tilde{a}_n) - \nu_p(\tilde{a}_j)}{n-j} = \frac{t - t_j}{n-j} \leq \frac{t}{n-(i-1)} \leq \frac{(n-i)k + \alpha}{n-(i-1)} < \frac{(n-i)k + k}{n-(i-1)} = k,$$

hence $\nu_p(d(\gamma)) = k$.

- Second case: $t = (n-i)k$ with $p \leq i \leq n-1$. Choose integers a_0, \dots, a_n such that $\gcd(a_0, \dots, a_n) = 1$ and

$$\begin{cases} \nu_p(a_j) \geq t, & \text{for } j > i, \\ \nu_p(a_i) = 0, \\ \nu_p(a_j) = 1, & \text{for } j < i, \\ \nu_p(a_n) = t. \end{cases} \quad (3.7)$$

Consider the polynomials

$$f(x) = \sum_{j=0}^n a_j(x)_j = \sum_{j=0}^n \tilde{a}_j x^j$$

and

$$g(x) = \tilde{a}_n x^n + q^{e_{n-1}} \tilde{a}_{n-1} x^{n-1} + \dots + q^{e_1} \tilde{a}_1 x + q \tilde{a}_0 := \sum_{j=0}^n b_j x^j,$$

where q and the e_j have the same meaning as in the preceding case. Clearly $g(x)$ is irreducible in $\mathbb{Z}[x]$ by Eisenstein's Theorem. Let γ be a root of $g(x)$. Since $p \leq i$, then by Lemma 2.2, we conclude that $p|i(f)$ and since $g(x) \equiv f(x) \pmod{p}$ for any $x \in \mathbb{Z}$, then $p|i(\gamma)$. We look at the p -adic valuations of the \tilde{a}_j . We have $\tilde{a}_n = a_n$ hence $\nu_p(\tilde{a}_n) = t$. For $j > i$, we have

$$\tilde{a}_j = a_j + \sum_{l=j+1}^n a_l c_l \text{ where } c_l \in \mathbb{Z} \text{ and we have } \nu_p(a_j) \geq t \text{ and } \nu_p(a_l) \geq t \text{ for } l \geq j + 1, \text{ hence } \nu_p(\tilde{a}_j) \geq t.$$

For $j = i$, we have $\nu_p(a_i) = 0$ and $\nu_p(a_l) = t, l \geq j + 1$, hence $\nu_p(\tilde{a}_i) = 0$.

For $j < i$, we have $\nu_p(\tilde{a}_j) \geq 0$.

For $j < i$, we have $\nu_p(\tilde{a}_j) \geq 0$.

We compute the p -adic valuation of the denominator of γ by using Lemma 2.1.

For $j > i$, we have

$$\frac{\nu_p(b_n) - \nu_p(b_j)}{n - j} = \frac{\nu_p(\tilde{a}_n) - \nu_p(\tilde{a}_j)}{n - j} = \frac{t - t_j}{n - j} \leq 0, \text{ because } t_j \geq t.$$

For $j = i$, we have

$$\frac{\nu_p(b_n) - \nu_p(b_i)}{n - i} = \frac{\nu_p(\tilde{a}_n) - \nu_p(\tilde{a}_i)}{n - i} = \frac{t}{n - i} = k.$$

For $j < i$ we have

$$\frac{\nu_p(b_n) - \nu_p(b_j)}{n - j} = \frac{\nu_p(\tilde{a}_n) - \nu_p(\tilde{a}_j)}{n - j} < \frac{t - t_j}{n - i} \leq \frac{t}{n - i} = k,$$

hence $\nu_p(d(\gamma)) = k$.

Since we can choose q and the e_j in an infinite number of ways, then the number of γ 's is infinite. \square

4. Upper bounds for the enumeration of the denominators of some algebraic numbers

Proposition 4.1. *Let $\theta \in A_n$, and $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$ its minimal polynomial over \mathbb{Q} . Suppose that $\theta \not\equiv 0 \pmod{pA}$. Construct the Newton polygon of $f(x)$ by plotting in the (x, y) plan the points A_i whose coordinates are $(i, \nu_p(a_i))$ for all $i \in \{0, \dots, n\}$ such that $a_i \neq 0$. Suppose that there exists $k \geq 1$ such that $p|i(\theta/p^k)$. Then there exists two integers m, M such that $1 \leq m < M \leq n - 1$ and the line joining the points A_m and A_M has the following equation*

$$y + kx - u = 0, \text{ where } kM \leq u < \nu_p(a_0) \text{ and } u = \nu_p(\text{cont}(f(p^k x))).$$

Moreover all the points A_i such that $i < m$ or $i > M$ belong to the domain of all points (x, y) such that $y + kx - u > 0$. If $m < i < M$, then we have $\nu_p(a_i) + ki - u \geq 0$.

Proof: The minimal polynomial over \mathbb{Z} of θ/p^k is given by

$$f(p^k x)/p^u = p^{nk-u}x^n + p^{(n-1)k-u}a_{n-1}x^{n-1} + \dots + p^{k-u}a_1x + p^{-u}a_0 := g(x),$$

where $u = \nu_p(\text{cont}(f(p^k x)))$. Let

$$I = \{i : 1 \leq i \leq n-1, a_i \neq 0 \text{ and } ik + \nu_p(a_i) - u = 0\}.$$

Since θ/p^k is not integral then $nk - u > 0$. Since $g(0) \equiv 0 \pmod{p}$, then $\nu_p(a_0) - u > 0$. Adding these two facts to the property that $g(x)$ is primitive implies that $I \neq \emptyset$. Furthermore $g(1) \equiv 0 \pmod{p}$, hence $|I| \geq 2$.

Let $m = \inf(I)$ and $M = \max(I)$. Clearly the equation of the line joining the points A_m and A_M is given by: $y + kx - u = 0$. Moreover a point $(i, \nu_p(a_i))$ of the Newton polygon belongs to this line if and only if $i \in I$. The definition of m and M implies the properties of the points A_i and of u . \square

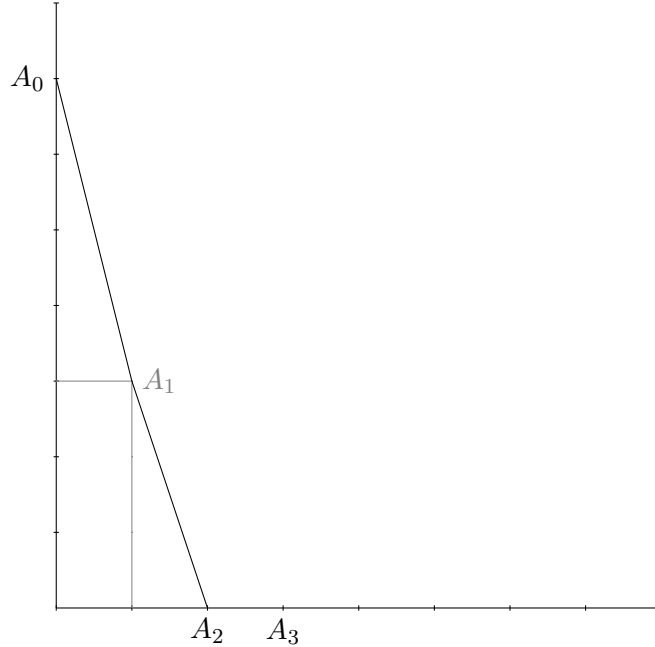
Remark 4.1. Proposition 4.1 shows that $-k$ is the slope of some line joining two points A_m and A_M . Moreover all the others points belong to the same side of the line (or on the line). Therefore, if we fix a prime p and an algebraic integer θ such that $\theta \not\equiv 0 \pmod{pA}$, it is possible to find explicitly all the values of k such that $p \mid i(\theta/p^k)$. This proposition shows also that the set of such nonnegative integers k is finite (may be empty).

Example 4.1. Let $t \geq 2$ be an integer, $f(x) = x^3 + x^2 + 2^t x + 2^{t+1}$ and θ_t be a root of $f(x)$. It is seen that $f(x)$ is irreducible over \mathbb{Q} : if not, it has a root a/b in \mathbb{Q} with $a, b \in \mathbb{Z}$ and $\gcd(a, b) = 1$. Substitution then yields

$$a^3 + a^2b + 2^t ab^2 + 2^{t+1}b^3 = 0,$$

implying $b \mid a^3$. Thus, $b = \pm 1$, and we then obtain $a \mid 2^{t+1}$. Letting $a = 2^i$, we obtain $2^{3i} + 2^{t+i} = 2^{2i} + 2^{t+1}$, implying that $t+i \leq t+1$ so $i = 1$ which is impossible.

For any nonnegative integer, let $\gamma_{t,k} = \theta_t/2^k$. We show that $V_2(\theta_t) = \{0, t\}$. Clearly, $2 \mid i(\theta_t)$, hence $0 \in V_2(\theta_t)$. The Newton diagram for $p = 2$ has the following shape:



The possible edges of the convex hull which may give rise to values of $k \in V_2(\theta_t)$, $k \geq 1$, are $[A_0A_1]$ and $[A_1A_2]$. Their slopes are equal to $-t - 1$ and t respectively. Thus, $k = t + 1$ or $k = t$.

If $k = t + 1$, the minimal polynomial of $\gamma_{t,k}$ over \mathbb{Z} is given by $g(x) = 2^{t+2}x^3 + 2x^2 + x + 1$. This shows that $2 \nmid i(g(x))$, hence $t + 1 \notin V_2(\theta_t)$.

If $k = t$, the minimal polynomial of $\gamma_{t,k}$ over \mathbb{Z} is given by $h(x) = 2x^3 + x^2 + x + 2$. This shows that $2 \mid i(h(x))$, hence $t \in V_2(\theta_t)$. Thus, $V_2(\theta_t) = \{0, t\}$.

We state now our main result on the upper bounds for the enumeration of the denominators of algebraic numbers γ such that $p \mid i(\gamma)$.

Theorem 4.1. *Let θ be a root of $f(x) \in \mathbb{Z}[x]$, monic irreducible, p a prime number such that $\theta \not\equiv 0 \pmod{p}$ and let $a_0 = f(0)$. We set*

$$V_p(\theta) = \left\{ k \geq 0; p \mid i(\theta/p^k) \right\}.$$

Suppose that $V_p(\theta) \neq \emptyset$ then we have

$$|V_p(\theta)| \leq \frac{n-1}{p-1}, \tag{4.8}$$

$$\sum_{k \in V_p(\theta)} k < \frac{\nu_p(a_0)}{p}. \tag{4.9}$$

For the proof of this theorem, we need the following lemma.

Lemma 4.1. *Let p be a prime number and $g(x) = a_Mx^M + \dots + a_mx^m$, $M > m > 0$ such that $p \nmid a_M$. If $p \mid i(g)$, then $M - m \geq p - 1$.*

Proof: Suppose that $p \mid i(g)$, then clearly $p \mid i(xg_1)$, where $g_1(x) = a_Mx^{M-m} + \dots + a_m$. Write xg_1 in the form

$$xg_1(x) = a_M(x)_{M-m+1} + \sum_{j < M-m+1} b_j(x)_j,$$

then by Lemma 2.2 $p \mid (M - m + 1)!a_M$, hence $p \mid (M - m + 1)!$. Therefore $p \leq M - m + 1$. \square

Proof of Theorem 4.1. Suppose that the complete list of elements of $V_p(\theta)$ is given by $k_1 < k_2 < \dots < k_z$. We have $k_1 = 0$ if and only if $p \mid i(\theta)$. Set $f(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$. For each $j = 1, \dots, z$, let $g_j(x)$ be the minimal polynomial of θ/p^{k_j} over \mathbb{Z} .

Set $g_j(x) = p^{t_j}x^n + b_{n-1}^{(j)}x^{n-1} + \dots + b_1^{(j)}x + b_0^{(j)}$, we have

$$g_1(x) = \begin{cases} f(x) & \text{if } k_1 = 0 \\ f(p^{k_1}x)p^{-u_1} & \text{if } k_1 \geq 1 \end{cases} \tag{4.10}$$

and $g_{j+1}(x) = g_j(p^{k_{j+1}-k_j}x)p^{-u_{j+1}}$ for $j = 1, \dots, z - 1$ and u_1, \dots, u_z are positive integers.

For any $j = 1, \dots, z$, let $I_j = \{i \in \{1, \dots, n - 1\}, \nu_p(b_i^{(j)}) = 0\}$. Since $t_j > 0$, $\nu_p(b_0^{(j)}) > 0$ and $g_j(x)$ is irreducible in $\mathbb{Z}[x]$, then it follows that $I_j \neq \emptyset$. Let $m_j = \inf(I_j)$ and $M_j = \sup(I_j)$. Since $g_j(1) \equiv 0 \pmod{p}$ then $|I_j| \geq 2$ and $m_j < M_j$. Clearly $m_j \geq 1$ and $M_j \leq n - 1$. We claim that:

- $M_j - m_j \geq p - 1$ for $j = 1, \dots, z$.

- $u_1 \geq k_1 M_1$ and $u_j \geq (k_j - k_{j-1})M_j$ for $j = 2, \dots, z$.
- $n \geq M_1 > m_1 \geq M_2 > m_2 \geq \dots \geq M_z > m_z \geq 1$.

The first claim follows from Lemma 4.1. If $k_1 = 0$, then from (4.10) we have $u_1 = 0 = k_1 M_1$. From the definition of M_1 and the definition of the interval I_1 , it follows that

$$\nu_p(b_{M_1}^{(1)}) = 0.$$

Therefore, if $k_1 \geq 1$, equation (10) and the above equality imply that

$$0 = \nu_p(b_{M_1}^{(1)}) = \nu_p(a_{M_1}) + k_1 M_1 - u_1,$$

hence $u_1 \geq k_1 M_1$. Similarly for $j = 2, \dots, z$, we have

$$0 = \nu_p(b_{M_j}^{(j)}) = \nu_p(b_{M_j}^{(j-1)}) + (k_j - k_{j-1})M_j - u_j,$$

hence $u_j \geq (k_j - k_{j-1})M_j$, which proves the second part of the claim. For the last part of the claim it is sufficient to prove that $m_j \geq M_{j+1}$ for $j = 1, \dots, z-1$. For, suppose that $m_j < M_{j+1}$ for some $j \in \{1, \dots, z-1\}$. We have $0 = \nu_p(b_{m_j}^{(j)})$, hence

$$\nu_p(b_{m_j}^{(j+1)}) = \nu_p(b_{m_j}^{(j)} \cdot p^{(k_{j+1}-k_j)m_j} \cdot p^{-u_{j+1}}) = (k_{j+1} - k_j)m_j - u_{j+1}.$$

We deduce that $(k_{j+1} - k_j)m_j \geq u_{j+1}$ and then $(k_{j+1} - k_j)M_{j+1} > u_{j+1}$. It follows that

$$\nu_p(b_{M_{j+1}}^{(j+1)}) = \nu_p(b_{M_{j+1}}^{(j)}) + (k_{j+1} - k_j)M_{j+1} - u_{j+1} > 0,$$

which contradicts the definition of M_{j+1} and completes the proof of the claim.

We now come back to the proof of Theorem 4.1.

Completion of proof of Theorem 4.1: We use the first and the third points of the claim. We have

$$n \geq M_1 > M_2 > \dots > M_{z-1} > M_z \geq p > 1.$$

Using the claim, we obtain

$$n - p \geq M_1 - M_z = (M_1 - M_2) + \dots + (M_{z-1} - M_z) \geq (p-1)(z-1)$$

hence

$$z \leq \frac{n-p}{p-1} + 1 = \frac{n-1}{p-1}.$$

Therefore (4.8) is proved.

We prove the inequality (4.9) of Theorem 4.1. We have $b_0^{(1)} = a_0 p^{-u_1}$, $b_0^{(j+1)} = b_0^{(j)} p^{-u_{j+1}}$ for $j = 1, \dots, z-1$ and since $g_z(0) \equiv 0 \pmod{p}$, then $\nu_p(b_0^{(z)}) > 0$. Hence $u_1 + u_2 + \dots + u_z < \nu_p(a_0)$. On the other hand, using the first and the second parts of the claim, we obtain

$$\begin{aligned} u_1 + u_2 + \dots + u_z &\geq k_1 M_1 + (k_2 - k_1)M_2 + \dots + (k_z - k_{z-1})M_z \\ &\geq k_1 z p + (k_2 - k_1)(z-1)p + \dots + (k_z - k_{z-1})p \\ &= p(k_1 z + k_2 z - k_1 z - k_2 + k_1 + k_3 z - k_2 z - 2k_3 + 2k_2 + \dots + k_z - k_{z-1}) \\ &= p((k_1 + k_2 + \dots + k_z)). \end{aligned}$$

Therefore, we have

$$\nu_p(a_0) > \sum_{j=1}^z u_j \geq p \sum_{j=1}^z k_j,$$

hence

$$\sum_{j=1}^z k_j < \nu_p(a_0)/p.$$

Remark 4.2. *Theorem 4.1, shows that if $\nu_p(a_0) \leq p$, then $V_p(\theta) = \{0\}$ or $V_p(\theta) = \emptyset$.*

The following result shows that the bound (4.8) in Theorem 4.1 is the best possible. More precisely, we have

Proposition 4.2. *Let p and q be distinct prime numbers such that $q \equiv 1 \pmod{p}$, θ be a root of*

$$f(x) = x^n + \sum_{i=1}^N a_i x^{n-i(p-1)} + qp^\lambda,$$

where $N = \lfloor (n-1)/(p-1) \rfloor$, $a_i = (-1)^i qp^{(p-1)i(i-1)/2}$, for $i = 1, \dots, N$ and

$$\lambda > \frac{2n(N-1) - (p-1)((N-1)^2 + N-1)}{2}.$$

Then

$$|V_p(\theta)| = \left\lfloor \frac{n-1}{p-1} \right\rfloor.$$

Proof: Clearly, by Eisenstein's criterion, $f(x)$ is irreducible over \mathbb{Q} . The coefficient of $x^{n-(p-1)}$ is coprime to p , hence $\theta \not\equiv 0 \pmod{pA}$. By Theorem 4.1, we have

$$|V_p(\theta)| \leq \left\lfloor \frac{n-1}{p-1} \right\rfloor.$$

We show that the integers $0, 1, \dots, \left\lfloor \frac{n-1}{p-1} \right\rfloor - 1$ belong to $V_p(\theta)$ and this will complete the proof of Proposition 4.2. Since $f(x) \equiv x^n - qx^{n-(p-1)} \pmod{p\mathbb{Z}[x]}$ and $q \equiv 1 \pmod{p}$, then $f(x) \equiv x^{n-(p-1)}(x^p - 1) \pmod{p\mathbb{Z}[x]}$. Thus, $p \mid i(f)$ and $0 \in V_p(\theta)$. Set $a_0 = 1$ and fix $k \in \left\{1, \dots, \left\lfloor \frac{n-1}{p-1} \right\rfloor - 1\right\}$. We have

$$f(p^k x) = p^{nk} x^n + \sum_{i=1}^N a_i p^{nk-i(p-1)k} x^{n-i(p-1)} + qp^\lambda.$$

We claim, omitting the proofs that

$$\nu_p(a_k p^{nk-k(p-1)k}) = \nu_p(a_{k+1} p^{nk-k(p-1)(k+1)}) = \frac{2nk - (p-1)(k^2 + k)}{2}$$

and

$$\nu_p(a_i p^{nk-i(p-1)k}) > \frac{2nk - (p-1)(k^2 + k)}{2} \text{ if } i \neq k, k+1.$$

Moreover, since the function $x \mapsto \psi(x) = 2nx - (p-1)(x^2 + x)$ is increasing in $[0, N-1]$ and since $\lambda > \frac{2n(N-1) - (p-1)(N-1)^2 + N-1}{2}$, then $\lambda > \frac{2nk - (p-1)(k^2 + k)}{2}$. It follows that $\text{cont}(f(p^k x)) = \frac{2nk - (p-1)(k^2 + k)}{2}$ and the minimal polynomial over \mathbb{Z} of $\gamma_k = \frac{\theta}{p^k}$ is given by

$$g_k(x) = f(p^k x) p^{-(2nk - (p-1)k^2 + k)/2}.$$

From the above it is seen that

$$g_k(x) \equiv (-1)^k x^{n-k(p-1)} + (-1)^{k+1} x^{n-(k+1)(p-1)} \pmod{p} \equiv (-1)^k x^{n-(k+1)(p-1)} (x^{p-1} - 1) \pmod{p},$$

hence $p \mid i(\gamma_k)$, thus $k \in V_p(\theta)$. \square

Corollary 4.1. *Let p be a prime number, and θ be a root of*

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x],$$

irreducible over \mathbb{Q} . Suppose that there exists $i \in \{0, \dots, \min(p, n) - 1\}$ such that $\nu_p(a_i) = 0$. Then

$$\theta \not\equiv 0 \pmod{pA} \text{ and } V_p(\theta) = \emptyset \text{ or } V_p(\theta) = \{0\}.$$

Moreover if $p > n$, then $V_p(\theta) = \emptyset$.

Proof: Let α be an algebraic integer and $g(x) = x^n + b_{n-1}x^{n-1} + \cdots + b_0$ be its minimal polynomial over \mathbb{Q} . It is easy to prove that $\alpha \equiv 0 \pmod{p}$ if and only if $\nu_p(b_i) \geq n - i$ for $i = 0, \dots, n - 1$. Our assumption then implies that $\theta \not\equiv 0 \pmod{pA}$. Suppose that $V_p(\theta) \neq \emptyset$ and let $k \in V_p(\theta)$. Assume that $k \geq 1$ and let $\gamma = \theta/p^k$ and $u = \text{cont}(f(p^k x))$. Then the minimal polynomial of γ over \mathbb{Z} is given by

$$g(x) = f(p^k x) p^{-u} = p^{nk-u} x^n + p^{(n-1)k-u} a_{n-1} x^{n-1} + \cdots + p^{-u} a_0.$$

As in Theorem 4.1, let

$$I = \{j \in \{1, \dots, n-1\}; \nu_p(a_j) + kj - u = 0\}, m = \inf(I), M = \sup(I).$$

Suppose first that $m \leq i$. We have $ik - u = \nu_p(a_i) + ik - u \geq 0$. Since $M - m \geq p - 1$, then $M > i$ which implies $\nu_p(a_M) + Mk - u \geq Mk - u > ik - u \geq 0$, a contradiction. We deduce that $m > i$ and then $\nu_p(a_m) + km - u \geq km - u > ki - u = \nu_p(a_i) + ki - u \geq 0$, a contradiction again. Therefore $V_p(\theta) = \{0\}$. \square

5. A new invariant of number fields and a generalisation of MacCluer's Theorem

Let p be a fixed prime integer. We have shown that for any algebraic integer θ such that $\theta \not\equiv 0 \pmod{pA}$, $p \mid i(\theta/p^k)$ for some $k \geq 1$, then $k < \nu_p(N_{\mathbb{Q}(\theta)/\mathbb{Q}}(\theta))/p$. Does there exist some constant $c > 0$ such that if $\theta \in \overline{\mathbb{Q}}$, $\theta \not\equiv 0 \pmod{pA}$ and $p \mid i(\theta/p^k)$ then $k < c$?

Even if we fix the degree n of θ and suppose that the constant c depends on n , the answer is negative as it is shown by the following result.

Proposition 5.1. *Let n, N be positive integers and p be a prime number such that $p < n$. Then there exists an integer $k > N$ and an algebraic integer θ of degree n such that*

$$\theta \not\equiv 0 \pmod{pA} \text{ and } p \mid i(\theta/p^k).$$

Proof: Let F be a number field of degree $n - 1$ such that $p \mid i(F)$. In particular, we can take F such that p completely splits in F , so that $p \mid i(F)$ by MacCluer's Theorem. Such a field F exists by Tchebotarev's theorem [Neu99]. Let α be a primitive element of F/\mathbb{Q} . Suppose that α is integral and $p \mid i(\alpha)$. Let $F_\alpha(x)$ be the minimal polynomial of α over \mathbb{Q} . Let q be a prime number such that

$$q \neq p \text{ and } q \nmid N_{F/\mathbb{Q}}(\alpha).$$

Let t be an integer such that $t > nN$ and let $g(x) = p^t x^n + qF_\alpha(x)$. Then Eisenstein's criterion shows that $g(x)$ is irreducible over \mathbb{Q} . Obviously $g(x)$ is primitive, hence it is irreducible in $\mathbb{Z}[x]$. Let γ be a root of $g(x)$, then clearly $p \mid i(\gamma)$ and $d(\gamma) = p^k$ for some positive integer k such that $k \leq t \leq nk$, hence $k \geq t/n > N$. The algebraic integer $\theta = p^k \gamma$ satisfies all the conditions of the proposition and the proof is complete. \square

Let K be a number field of degree n over \mathbb{Q} and A be its ring of integers. We define the integer $v_p(K)$ as follows.

Definition 5.1. *Let*

$$V_p(K) = \left\{ k \geq 0, \text{ there exists } \theta \in A_n, \theta \not\equiv 0 \pmod{pA}, \text{ and } p \mid i(\theta/p^k) \right\},$$

and we define

$$v_p(K) = \begin{cases} -\infty & \text{if } V_p(K) = \emptyset, \\ \infty & \text{if } V_p(K) \text{ is infinite,} \\ \max(V_p(K)) & \text{if } V_p(K) \text{ is finite.} \end{cases}$$

Remark 5.1. *By Theorem 3.1, we have $v_p(K) = -\infty$ if and only if $p \nmid i(K)$. So there is no need to give examples illustrating this fact. Theorem 3.1 again shows that if the degree of the number field K is a prime p then $v_p(K) = 0$ if $p \mid i(K)$ and $v_p(K) = -\infty$ if $p \nmid i(K)$.*

In the following we compute explicitly $v_2(K)$ for some number fields of degree 3 or 4 over \mathbb{Q} .

Proposition 5.2. (Galois field of degree 4) *Let K/\mathbb{Q} be a Galois number field of degree 4 in which the prime 2 splits into a product of two prime ideals having their residual degree equal to 2. Then we have $v_2(K) = 0$.*

Proof: By MacCluer's theorem, $2 \mid i(K)$, hence $0 \in V_p(K)$. Let \mathfrak{p} and \mathfrak{p}' be the conjugate prime ideals of A lying over 2 and having their residual degree equal to 2. Suppose that $2 \mid i(\theta/2^k)$ for some $k \geq 1$ and $\theta \in A_n$ such that $\theta \not\equiv 0 \pmod{2A}$. Since $N_{K/\mathbb{Q}}(\theta) \equiv 0 \pmod{2}$, then we may suppose that $\mathfrak{p}^e \parallel \theta$ and $\mathfrak{p}' \nmid \theta$ for some $e \geq 1$. We suppose that the conjugates $\theta_1 = \theta, \theta_2, \theta_3, \theta_4$ of θ satisfy the following conditions:

$$\mathfrak{p}^e \parallel \theta_1, \mathfrak{p}^e \parallel \theta_3, \mathfrak{p}' \nmid \theta_1 \theta_3, \mathfrak{p}'^e \parallel \theta_2, \mathfrak{p}'^e \parallel \theta_4, \mathfrak{p} \nmid \theta_2 \theta_4.$$

Let $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$ be the minimal polynomial of θ over \mathbb{Q} . Let $g(x) \in \mathbb{Z}[x]$ be the minimal polynomial of $\gamma = \theta/2^k$ over \mathbb{Z} , then

$$g(x) = f(2^kx) \cdot 2^{-u} = 2^{4k-u}x^4 + 2^{3k-u}a_3x^3 + 2^{2k-u}a_2x^2 + 2^{k-u}a_1x + 2^{-u}a_0,$$

where u is the content of $f(2^kx)$. Using the elementary symmetric functions of the θ_j and our assumption on their \mathfrak{p} -adic and \mathfrak{p}' -adic valuations, we get

$$\nu_2(a_0) = 2e, \nu_2(a_1) \geq e \text{ and } \nu_2(a_2) = 0.$$

If $k \geq e$, then $\nu_2(2^{4k-u}) \geq 4e - u$, $\nu_2(2^{3k-u}a_3) \geq 3e - u$, $\nu_2(2^{2k-u}a_2) = 2k - u \geq 2e - u$, $\nu_2(2^{k-u}a_1) \geq 2e - u$, $\nu_2(2^{-u}a_0) = 2e - u$. Since these five 2-adic valuations must be nonnegative, then $u \leq 2e$. Furthermore one (at least) of these valuations must be 0, hence $u = 2e$. In this case, $g(0) \not\equiv 0 \pmod{2}$ which is a contradiction to $2|i(\gamma)$. If $k < e$, then $\nu_2(2^{4k-u}) = 4k - u$, $\nu_2(2^{3k-u}a_3) \geq 3k - u$, $\nu_2(2^{2k-u}a_2) = 2k - u$, $\nu_2(2^{k-u}a_1) > 2k - u$, $\nu_2(2^{-u}a_0) > 2k - u$. Using similar arguments as in the preceding case, we obtain $u = 2k$. We conclude that all the coefficients of $g(x)$ have their 2-adic valuations positive except the coefficient of x^2 which has a 2-adic valuation equal to 0. In this case also we reach a contradiction since $g(1) \not\equiv 0 \pmod{2}$. It follows that $V_2(K) = \{0\}$ and $\nu_2(K) = 0$. \square

For the proof of the next proposition, we will need the following lemma.

Lemma 5.1. (Engstrom) *Let K be a number field, A be its ring of integers and p be a prime integer. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ be distinct prime ideals of A lying over p and let $\Phi_1(x), \dots, \Phi_s(x)$ be monic irreducible polynomials over \mathbb{F}_p not necessarily distincts of degree d_1, \dots, d_s respectively, where d_i divides the residual degree of \mathfrak{p}_i . Let h_1, \dots, h_s be positive integers. Then there exists a primitive element $\theta \in A$ such that $\mathfrak{p}_i^{h_i} \parallel \Phi_i(\theta)$ for $i = 1, \dots, s$*

Proof: see [Eng30]. \square

Proposition 5.3. (Cubic Galois) *Let K/\mathbb{Q} be a Galois number field of degree 3 in which the prime 2 splits completely. Then $V_2(K) = \mathbb{N}$.*

Proof: Let k and e be positive integers such that $e > k$. Let $\mathfrak{p}_1, \mathfrak{p}_2$ and \mathfrak{p}_3 be the prime ideals of A lying over 2. By Lemma 5.1 there exists $\theta \in A_n$ such that

$$\mathfrak{p}_1^e \parallel \theta, \mathfrak{p}_2^k \parallel \theta \text{ and } \mathfrak{p}_3 \nmid \theta.$$

Assume that the conjugates of θ , $\theta_1 = \theta, \theta_2, \theta_3$ are labelled in order to satisfy the following conditions:

$$\begin{aligned} \mathfrak{p}_2^e \parallel \theta_2, \mathfrak{p}_3^k \parallel \theta_2, \mathfrak{p}_1 \nmid \theta_2, \\ \mathfrak{p}_3^e \parallel \theta_3, \mathfrak{p}_1^k \parallel \theta_3, \mathfrak{p}_2 \nmid \theta_3. \end{aligned}$$

Let $f(x) = x^3 + a_2x^2 + a_1x + a_0 \in \mathbb{Z}[x]$ be the minimal polynomial of θ over \mathbb{Q} . Expressing a_0, a_1 and a_2 in terms of $\theta_1, \theta_2, \theta_3$, we get

$$\nu_2(a_0) = e + k, \nu_2(a_1) = k \text{ and } \nu_2(a_2) = 0.$$

We have

$$f(2^k x) = 2^{3k} x^3 + 2^{2k} a_2 x^2 + 2^k a_1 x + a_0.$$

Set

$$b_3 = 2^{3k}, b_2 = 2^{2k} a_2, b_1 = 2^k a_1, b_0 = a_0.$$

Using the 2-adic valuation of a_0, a_1, a_2 we obtain

$$\nu_2(b_1) = \nu_2(b_2) = 2k, \nu_2(b_0) = e + k > 2k, \nu_2(b_3) = 3k > 2k.$$

Therefore $\text{cont}(f(2^{2k}x)) = 2^{2k}$ and the minimal polynomial of $\theta/2^k$ is given by

$$g(x) = f(2^k x) \cdot 2^{-2k}.$$

Clearly we have $g(0) \equiv g(1) \equiv 0 \pmod{2}$ hence $2|i(\theta/p^k)$. Since the prime 2 splits completely in K , then $0 \in V_2(K)$. Therefore $V_2(K) = \mathbb{N}$ and $\nu_2(K) = \infty$. \square

Remark 5.2. *Our result in the sequel can be viewed as a generalization of MacCluer's theorem which establishes a relation between the number of prime ideals of A lying over p and the property of p to be a divisor of $i(K)$.*

Fix a prime number p and define, for any primitive element $\theta \in A$ of K , the integer $j_p(\theta)$ as follows.

Definition 5.2. *Let $F_\theta(x)$ be the minimal polynomial of θ over \mathbb{Q} . Let $j_p(\theta)$ be the largest integer y , if it exists, $1 \leq y \leq p$ such that $F_\theta(1) \equiv F_\theta(2) \equiv \dots \equiv F_\theta(y) \equiv 0 \pmod{p}$. If not set $j_p(\theta) = 0$. We define also $j_p(K) = \max_{\theta \in A_n} j_p(\theta)$.*

Theorem 5.1. *Let r be the number of prime ideals of A lying over p . Then*

$$j_p(K) = \inf(r, p).$$

Moreover

$$p|i(K) \iff j_p(K) = p.$$

Proof: Suppose first that $r \leq p$ and let $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ be the distinct prime ideals of A lying over p . By Lemma 5.1 there exists $\theta \in A_n$ such that $\theta \equiv i \pmod{p}$ for $i = 1, \dots, r$. It follows that the minimal polynomial $F_\theta(x)$ of θ satisfies the condition

$$F_\theta(x) \equiv (x-1)(x-2) \cdots (x-r)g(x) \pmod{p}$$

hence $j_p(\theta) \geq r$ which implies that $j_p(K) \geq r$. On the other hand, let $\theta \in A_n$ such that

$$j_p(K) = j_p(\theta) := t,$$

then

$$F_\theta(x) \equiv (x-1)(x-2) \cdots (x-t)g(x) \pmod{p}$$

hence, by Hensel's Lemma, we deduce that $F_\theta(x)$ has at least t irreducible factors over \mathbb{Z}_p , the ring of p -adic integers. Again by Theorem 5.1 of chap. 2 of [Jan96], we have $t \leq r$. We conclude that

$j_p(K) = r = \inf(p, r)$.

Suppose now that $r > p$. By Lemma 5.1, let $\theta \in A_n$ such that $\theta \equiv i \pmod{p}$ for $i = 1, \dots, p$. Then

$$F_\theta(x) \equiv (x-1)(x-2)\cdots(x-p)g(x) \pmod{p}.$$

therefore we have $j_p(\theta) \geq p$ which implies $j_p(K) \geq p$. From the definition we have $j_p(K) \leq p$, hence $j_p(K) = p = \inf(r, p)$.

We now prove the last statement of the proposition. We have

$$p|i(K) \iff r \geq p \text{ (by MacCluer's theorem)} \iff \inf(r, p) = p \iff j_p(K) = p. \quad \square$$

6. Concluding remarks

Questions Let K be a number field of degree n . If $[K : \mathbb{Q}] = 2$, then by Corollary 2.1, $i(K)$ and $\hat{i}(K)$ are equal to 1 or 2. Theorem 3.1 shows that $2 \nmid i(\gamma)$ if $\gamma \notin A_n$, hence $i(K) = \hat{i}(K) \in \{1, 2\}$.

If $[K : \mathbb{Q}] = 3$, then $i(K)$ and $\hat{i}(K) \in \{1, 2, 3, 6\}$. Moreover, Theorem 3.1 shows that $3 \mid \hat{i}(K)$ if and only if $3 \mid i(K)$.

Suppose that there exists $\gamma = \theta/2^k$ with $k \geq 1$, $k \leq t \leq 3k$ and $\theta \not\equiv 0 \pmod{p}$ such that $2 \mid i(\gamma)$. Let $g(x) = 2^t x^3 + b_2 x^2 + b_1 x + b_0$ be the minimal polynomial of γ over \mathbb{Z} . Since $g(0) \equiv 0 \pmod{2}$, then $b_0 \equiv 0 \pmod{2}$. Since $g(1) \equiv 0 \pmod{2}$, then $b_1 + b_2 \equiv 0 \pmod{2}$, thus $b_1 \equiv b_2 \pmod{2}$. Moreover, since $g(x)$ is primitive, then $b_1 \equiv b_2 \equiv 1 \pmod{2}$. By Theorem 3.1, $t \leq k$. Since $k \leq t$, then $k = t$. The minimal polynomial of θ is then given by

$$f(x) = x^3 + b_2 x^2 + b_1 2^t x + b_0 2^{2t}.$$

This shows that $2 \mid i(f)$ and then $2 \mid i(\theta)$, thus $2 \mid i(K)$. We conclude that $i(K) = \hat{i}(K)$.

Let K be a number field of degree n and let $\gamma \in K_n \setminus A_n$. Set $\gamma = \theta/d$, where d is an integer at least equal to 2 such that $\theta \not\equiv 0 \pmod{p}$ for any prime divisor p of d . It is proved in Lemma 3.1 that if $d = p^k q$ with $\gcd(p, q) = 1$ and $k \geq 1$, then $p \mid i(\gamma)$ if and only if $p \mid i(\theta/p^k)$. We ask that following: Is it true that if $p \mid i(\theta/p^k)$ with $k \geq 1$ and $\theta \not\equiv 0 \pmod{p}$, then $p \mid i(K)$? Do we have $\hat{i}(K) = i(K)$?

Recall that $\nu_p(K)$ is the greatest element of the set $V_p(K)$, when this set is finite. Do we have $\{0, 1, \dots, \nu_p(K)\} = V_p(K)$? The example given in section 4 shows that $V_p(\theta_t) = \{0, t\} \neq \{0, 1, \dots, t\}$. We may ask a similar question when $V_p(K)$ is infinite. Do we have $V_p(K) = \mathbb{N}$?

Acknowledgements. The authors express their gratitude to the anonymous referee for constructive suggestions which improved the quality of the paper. The third author was supported in part by NSERC.

References

- [ARW96] S. Arno, M. L. Robinson, and F. S. Wheeler, *On denominators of algebraic numbers and integer Polynomials*, J. Number theory **57** (1996), 292–302.
- [AyKi11] 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), 1173–1194.
- [ABK15] M. Ayad, A. Bayad, and O. Kihel, *Denominators of Algebraic Numbers in a Number Field*, J. Number Theory **149** (2015), 1–14.

- [Eng30] H. T. Engstrom, *On the common index divisors of an algebraic field*, Trans. A.M.S **32** (1930), 223–237.
- [GuMc70] H. Gunji, D. L. McQuillan, *On a class of ideals in an algebraic number field*, J. Number Theory **2** (1970), 207–222.
- [Jan96] G. J. Janusz, *Algebraic Number Fields, Graduate Studies in Math*, A.M.S. (1996).
- [Mac71] C. R. MacCluer, *Common divisors of values of polynomials*, J. Number Theory **3** (1971), 33–34.
- [Neu99] O. Neukirch, *Algebraic Number Theory*, Springer (1999).

Mohamed Ayad

Laboratoire de Mathématiques Pures et Appliquées
Université du Littoral, F-62228 Calais, France
e-mail: ayad@impa.univ-littoral.fr

Abdelmejid Bayad

Laboratoire de Mathématiques et Modélisation d'Évry (LAMME)
Université Paris-Saclay, CNRS (UMR 8071)
Bâtiment I.B.G.B.I., 23 Boulevard de France,
CEDEX, 91037 Evry, France
e-mail: abdelmejid.bayad@univ-evry.fr and
e-mail: abayad@maths.univ-evry.fr

Omar Kihel

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