N °d'ORDRE : 02/2016-D/MT

REPUBLIQUE ALGÉRIENNE DEMOCRATIQUE ET POPULAIRE
MINISTERE DE L'ENSEIGNEMENT SUPÉRIEURE ET
DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE DES SCIENCES ET DE LA TECHNOLOGIE
HOUARI BOUMEDIENE
Faculté de Mathématiques

THÈSE

Présentée pour l'obtention du grade de Docteur en Sciences

En : MATHÉMATIQUES

Spécialité : Algèbre et Théorie des Nombres

Par : **Rachid BOUCHENNA**

Intitulée

DENOMINATEURS DE NOMBRES ALGEBRIQUES ET INDICES

Soutenue publiquement le 12 avril 2016, devant le jury composé de :

Rachid BEBBOUCHI	Professeur à l'USTHB	Président
Mohamed AYAD	Maitre de Conférences HDR à l'Université du Littoral, Calais, France	Directeur de thèse
Mohammed AYADI	Professeur à l'Université Mohamed 1er, Oujda, Maroc	Examinateur
Boualem BENSEBAA	Maitre de Conférences/A à l'USTHB	Examinateur
Omar KIHEL	Professeur à Brock University, Canada	Examinateur
Toufik ZAIMI	Professeur à l'Université Larbi Ben M'hidi, Oum El Bouaghi	Examinateur

REMERCIEMENTS

Je tiens à remercier Mohamed Ayad, mon Directeur de Thèse, de m'avoir proposé ce sujet qui m'a tout de suite intéressé, d'avoir été très disponible et très impliqué, bref, d'avoir dirigé, au vrai sens du terme, ce travail.

J'adresse également un merci particulier à Omar Kihel avec qui j'ai également travaillé au même titre qu'avec Ayad et qui m'a énormément soutenu et encouragé pendant toute la durée de la réalisation de ce document.

Il faut dire que j'ai trouvé beaucoup de plaisir à étudier ce sujet avec Mohamed Ayad et Omar Kihel auprès desquels j'ai beaucoup appris.

Je remercie Rachid Bebbouchi d'avoir spontanément accepté de présider le jury et d'avoir tout fait pour permettre que cette soutenance ait lieu et dans un délai si court.

Mes remerciements vont aussi à Boualem Benseba qui a très naturellement accepté d'examiner ce travail et qui m'a été d'un grand soutien ainsi qu'à Mohammed Ayadi et Toufik Zaimi qui, après lecture du manuscrit, m'ont fait part de leurs précieuses remarques.

Je remercie aussi plusieurs autres collègues et amis pour l'aide, technique ou autre, qu'ils m'ont apportée, comme Amar Idris-Bey, Tarek Garici, Leila Cherchem, Ahmed Cherchem, Djamila Abchiche et Mourad Abchiche.

Et...merci, évidemment, à Melha, ma femme, et à Lylia, ma fille.

NOTATIONS

$\deg f(x)$: le degré du polynôme $f(x)$.

$Cont(f(x))$: le contenu du polynôme $f(x)$.

$Irr(\theta, K)$: le polynôme minimal de θ sur K.

$Irr(\theta, \mathbb{Z})$: le polynôme minimal de θ sur $\mathbb{Z}$.

$K(\theta)$: l'extension de K engendrée par θ.

$Aut(L)$: le groupe des automorphismes de L.

$Aut_K(L)$: le groupe des K-automorphismes de L, c'est-à-dire des automorphismes de L laissant fixes les éléments de K.

$Gal(L/K)$: le groupe de Galois de l'extension galoisienne L/K.

$A[x]$: l'anneau des polynômes en l'indéterminée x à coefficients dans l'anneau A.

$Disc_{K/\mathbb{Q}}(\theta_1, ..., \theta_n)$: le discriminant du uplet $(\theta_1, ..., \theta_n)$ relativement à l'extension $K/\mathbb{Q}$.

$Disc_{K/\mathbb{Q}}(\theta)$: le discriminant du uplet $(1, \theta, ..., \theta^{n-1})$ relativement à l'extension $K/\mathbb{Q}$, le corps de nombres K.

$| a |$: la valeur absolue de a si a représente un nombre réel.

$| E |$: le cardinal de E si E représente un ensemble.

v_p : la valuation p-adique.

$\gcd(a_0, ..., a_n)$: le plus grand commun diviseur des entiers rationnels a_i.

$s_j(\theta)$: la fonction symétrique élémentaire des racines d'indice j du polynôme minimal de θ, celui-ci étant un nombre algébrique.

$M_\theta(p, x)$: le polynôme minimal de congruence modulo p de θ, p étant un nombre premier et θ un entier algébrique.

$a \mid b$: l'élément a divise l'élément b, a et b étant deux éléments d'un anneau.

$p^n \parallel a$: p^n divise a et p^{n+1} ne divise pas a.

$\lceil a \rceil$: le plus petit entier rationnel $\geq a$, a étant un nombre réel.

A_r^n : le nombre d'arrangements à r éléments dans un ensemble ayant n éléments.

$N_p(f)$: le nombre des polynômes unitaires et irréductibles de degré f à coefficients dans le corps $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

$rad(f)$: le radical de f, autrement dit, le produit de tous les nombres premiers divisant f, f étant un entier rationnel ≥ 1.

Table des matières

Introduction

Cette thèse s'articule autour de la notion d'indice d'entier algébrique. Etant donné un corps de nombres K, l'ensemble A de ses entiers, c'est-à-dire de ses éléments dont les polynômes minimaux respectifs sont à coefficients dans l'anneau $\mathbb{Z}$ des entiers rationnels, possède une structure d'anneau, contenant $\mathbb{Z}$. Si le degré de K est n, A est un $\mathbb{Z}$-module libre de rang n. Par ailleurs, l'anneau A vérifie les 3 propriétés suivantes : il est *noethérien* (ses idéaux sont tous de type fini), *intégralement clos*, c'est-à-dire intègre et *intégralement fermé* dans son corps des fractions, ce qui veut dire que les seuls éléments de son corps des fractions qui soient racines de polynômes unitaires à coefficients dans A sont les éléments de A, et enfin, de *dimension de Krull* 0 ou 1, ce qui signifie que tous ses idéaux premiers non nuls sont maximaux. Ces trois dernières propriétés font de A un *anneau de Dedekind*.

Si K est un corps de nombres quadratique, donc engendré par une racine carrée d'un entier d, différent de 1 et sans facteur carré, il est bien connu que selon que l'on ait $d \equiv 2, 3 \pmod 4$ ou $d \equiv 1 \pmod 4$, l'anneau A est égal soit à $\mathbb{Z}\left[\sqrt{d}\right]$ soit à $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ (voir par exemple [22] ou [28]). Il existe par conséquent dans les deux cas un élément $\theta \in A$ tel que $A = \mathbb{Z}[\theta]$. Cependant, cette propriété n'est pas garantie lorsque K est un corps de nombres de degré ≥ 3. En fait, dans ce cas, il peut arriver que pour tout $\theta \in A$, $\mathbb{Z}[\theta]$ soit un sous-anneau propre de A. D'où l'intérêt de la notion d'*indice*. Par définition, l'indice d'un entier θ d'un corps de nombres K, noté $I(\theta)$, est tout simplement l'indice de $\mathbb{Z}[\theta]$ dans A en tant que groupes additifs si $K = \mathbb{Q}(\theta)$ et 0 si $K \neq \mathbb{Q}(\theta)$. On peut aussi le définir à partir de la notion de *discriminant* : si K est un corps de nombres de degré n sur $\mathbb{Q}$ et si D désigne le discriminant de K sur $\mathbb{Q}$, l'indice de θ est l'entier naturel $I(\theta)$ défini par l'égalité : $Disc_{K/\mathbb{Q}}(1, \theta, ..., \theta^{n-1}) = (I(\theta))^2 D$.

Le chapitre 1 constitue un rappel assez succinct des principales notions concernant les corps de nombres. Ce rappel concerne donc les extensions algébriques, en particulier les extensions algébriques finies, dont les corps de nombres, et la notion d'extension galoisienne

finie. Il concerne également les entiers d'un corps de nombres dont l'ensemble jouit de certaines propriétés grâce à ses structures de $\mathbb{Z}$-module libre et d'anneau de Dedekind. De même, nous évoquons la notion de discriminant d'une extension et ses différentes propriétés. Enfin, nous rappelons le théorème sur la décomposition d'un idéal en produit d'idéaux premiers dans les anneaux de Dedekind et les notions d'indice de ramification et de degré résiduel ainsi que la formule qui lie le degré du corps de nombres considéré aux idéaux premiers apparaissant dans la décomposition d'un nombre premier.

Le second chapitre est consacré à la notion de dénominateur de nombre algébrique ainsi qu'à celles de *petit indice* et de *grand indice* (on dira simplement indice au lieu de grand indice) dans les corps de nombres. Si γ est un nombre algébrique quelconque, l'ensemble de tous les entiers rationnels n tels que $n\gamma$ soit un entier algébrique est un idéal non nul de $\mathbb{Z}$. Par définition, le dénominateur de γ est le générateur positif de celui-ci. La seconde section traite de la notion de petit indice. Etant donné un corps de nombres K et un entier θ de K dont le polynôme minimal sur le corps des nombres rationnels est $g(x)$, on appelle *petit indice* de θ et on note $i(\theta)$ le plus grand commun diviseur de $g(x)$ lorsque x parcourt $\mathbb{Z}$. Gunji et McQuillan [14] définissent alors le *petit indice* de K, que l'on note $i(K)$, comme étant le plus petit multiple commun de l'ensemble des $i(\theta)$ lorsque θ parcourt l'ensemble des entiers primitifs de K. Enfin, dans la dernière section nous définissons ce qu'est l'indice (ou le grand indice s'il y a confusion) d'un entier algébrique, notion centrale à laquelle tout le reste du document est consacré. (Plus loin, à la fin du chapitre 4, nous verrons à travers un résultat dû à Ayad et Kihel [6], qu'une relation étroite existe entre les notions de petit et de grand indices).

Le troisième chapitre traite de la notion de *polynôme minimal de congruence* modulo un nombre premier. Soient K un corps de nombres, A son anneau des entiers, θ un élément quelconque de A de polynôme minimal $F(x) \in \mathbb{Z}[x]$ et p un nombre premier. On considère dans l'anneau principal $\mathbb{F}_p[x]$ l'ensemble E_θ de tous les polynômes qui s'annulent en $\overline{\theta} = \theta + pA$. C'est clairement un idéal et il est non nul. Il existe donc un polynôme unitaire $g_0(x)$ dans $\mathbb{F}_p[x]$ engendrant E_θ. Le polynôme minimal de congruence modulo p de θ est alors par définition un relèvement unitaire dans $\mathbb{Z}[x]$ de $g_0(x)$. Il est unique modulo p et est noté $M_\theta(p, x)$. Ce polynôme joue un rôle essentiel car il détermine si p est un diviseur ou pas de l'indice de θ. Dans le reste du chapitre, nous passons en revue un certain nombre de résultats qui consistent en des conditions, nécessaires ou suffisantes (ou nécessaires et suffisantes) pour

qu'un nombre premier soit un diviseur de l'indice d'un entier algébrique donné.

Le chapitre 4 est le prolongement naturel du chapitre 3. Un nombre premier p est dit *facteur commun d'indices*, f.c.i. en abrégé, dans un corps de nombres K, si p est un diviseur de $I(\theta)$ pour tout entier θ de K. Dans ce chapitre, nous étudions les conditions qui font qu'un nombre premier p est f.c.i. ou pas dans un corps donné. Nous rappelons certains résultats anciens comme celui de Zylinski : *tout facteur commun d'indices dans un corps de nombres donné est strictement plus petit que le degré de ce corps*, puis celui de Hensel qui offre, lui, une condition nécessaire et suffisante pour qu'un nombre premier soit f.c.i. dans un corps de nombres donné. Cette dernière condition repose sur la décomposition des nombres premiers en produit d'idéaux premiers dans les corps de nombres. Un autre résultat, dû à Ayad et Kihel, affirme que pour qu'un nombre premier soit un f.c.i. dans un corps de nombres K, il est nécessaire qu'il divise un certain invariant lié au corps de nombres K, le petit indice de K, déjà défini dans le chapitre 2.

Dans le cinquième et dernier chapitre nous introduisons une nouvelle fonction, notée μ_K, liée au corps de nombres K, qui permet de calculer pour un nombre premier p donné, le nombre, noté $\mu_K(p)$, des entiers de K incongrus modulo p dont l'indice est divisible par p. Une formule explicite de $\mu_K(p)$ est donnée. Cette valeur dépend uniquement de la décomposition de p dans K. La connaissance de la décomposition de p permet donc de déterminer la valeur de $\mu_K(p)$ et en particulier de savoir si p est f.c.i. ou pas dans K. Des tables donnant la valeur de $\mu_K(p)$, en fonction de la décomposition de p, sont établies pour les degrés $4, 5$ et 6. Réciproquement, la connaissance préalable de la valeur de $\mu_K(p)$ permet, dans certains cas, de déterminer le type de décomposition de p dans K.

Enfin, nous nous sommes intéressés à la situation où pour un nombre premier p donné, deux corps de nombres K et K' de même degré vérifient $\mu_K(p) = \mu_{K'}(p)$. Nous conjecturons que si p n'est pas f.c.i. dans K et K' et que si les décompositions de p dans K et K' sont *spéciales*, en particulier si les deux corps de nombres sont galoisiens, alors les *paramètres* de ces deux décompositions sont pareils. C'est l'objet du dernier théorème contenu dans ce document et qui consiste en la démonstration de cette conjecture, lorsque le nombre premier p est suffisamment grand.

Chapitre 1

Rappels sur les entiers algébriques

1.1 Extensions algébriques et extensions galoisiennes

Soient deux corps commutatifs L et K tels que $L \supseteq K$. On parle alors d'extension de L sur K et on écrit L/K. Un élément de L est dit algébrique sur K s'il est racine d'un polynôme non constant à coefficients dans K. On dit que l'extension L/K est algébrique si tous les éléments de L sont algébriques sur K et transcendante sinon. Si un élément θ de L est algébrique sur K, l'ensemble des polynômes de l'anneau principal $K[x]$ annulés par θ est un idéal de cet anneau. Il existe un polynôme unitaire unique de degré ≥ 1 dans $K[x]$ engendrant cet idéal. Il est irréductible sur K. Il est appelé le polynôme minimal de θ sur K et est noté $Irr(\theta, K)$. Le degré de θ sur K est par définition $\deg(Irr(\theta, K))$, c'est-à-dire le degré de son polynôme minimal sur K. C'est aussi la dimension du K-espace vectoriel $K(\theta)$, appelée également le degré de l'extension $K(\theta)/K$, $K(\theta)$ désignant le plus petit sous-corps de L contenant à la fois K et θ. Une extension est dite finie si elle est de degré fini. Toute extension L/K finie est algébrique. Si L/K est une extension quelconque, il arrive qu'il existe des éléments θ de L vérifiant $L = K(\theta)$. De tels éléments sont dits éléments primitifs de l'extension L/K.

Soit K un corps commutatif quelconque. Il existe un corps Ω contenant K tel que Ω soit algébrique sur K et algébriquement clos (c'est-à-dire dont les seuls polynômes irréductibles soient les polynômes de degré 1, ce qui veut dire aussi qu'elle est la seule extension algébrique d'elle-même). Ω est appelé clôture algébrique de K. On montre que la clôture algébrique d'un corps est unique à isomorphisme près. Si $P(x)$ est un polynôme quelconque de $K[x]$ de degré $n \geq 1$, $P(x)$ possède n racines dans Ω, chacune étant comptée avec son ordre de multiplicité.

Soit L/K une extension algébrique. Deux éléments θ et θ' de L sont dits conjugués s'ils ont le même polynôme minimal sur K. Si f est un homomorphisme de L dans un corps algébriquement clos quelconque Ω contenant L, laissant fixes les éléments de K, alors f transforme tout élément θ de L en l'un de ses conjugués sur K.

Soit L/K une extension finie. L'ensemble $Aut(L)$ de tous les automorphismes (de corps) de L est un groupe. De même pour l'ensemble de tous les automorphismes de L qui laissent fixes les éléments de K. Ce dernier, noté $Aut_K(L)$, est un sous-groupe de $Aut(L)$. Etant donné un sous-groupe H quelconque du groupe $G = Aut_K(L)$, l'ensemble de tous les éléments de L laissés fixes par tous les éléments de H est un sous-corps de L contenant K, appelé le sous-corps des invariants de H. Inversement, étant donné un sous-corps K' de L contenant K, l'ensemble de tous les éléments de G laissant fixes tous les éléments de K' est un sous-groupe de G. L'extension L/K est dite galoisienne (ou, le corps L est galoisien sur le corps K) si K coincide avec le sous-corps des invariants de $Aut_K(L)$. Dans ce cas, il existe, d'après le *théorème fondamental de Galois*, une correspondance biunivoque entre l'ensemble des sous-groupes de G et l'ensemble des sous-corps de L contenant K. Le groupe G est appelé dans ce cas le groupe de Galois de l'extension L/K et est noté $Gal(L/K)$. Il est fini et le nombre de ses éléments est égal au degré de l'extension L/K.

Si L/K est une extension galoisienne finie de degré n, il existe dans L des éléments primitifs. Si θ est l'un d'eux alors $L = K(\theta)$ et les éléments $\sigma_1, ..., \sigma_n$ du groupe de Galois $Gal(L/K)$ sont entièrement déterminés par $\sigma_1(\theta), ..., \sigma_n(\theta)$, c'est-à-dire par les images de θ par les σ_i.

1.2 Corps de nombres

Définissons d'abord ce que l'on entend par nombre algébrique.

Définition 1.2.1 *On appelle nombre algébrique tout nombre complexe, algébrique sur le corps $\mathbb{Q}$ des nombres rationnels, c'est-à-dire racine d'un polynôme non nul à coefficients dans ce corps.*

Définition 1.2.2 *On appelle corps de nombres tout sous-corps K de $\mathbb{C}$ tel que l'extension $K/\mathbb{Q}$ soit finie.*

Tout corps de nombres K admet des éléments primitifs. Si K est de degré n sur $\mathbb{Q}$, un élément quelconque θ de K est algébrique sur $\mathbb{Q}$ et de degré un diviseur de n. Un élément θ de K est un élément primitif de K si et seulement si son degré est égal à n. Si oui, la famille $\left\{1, \theta, ..., \theta^{n-1}\right\}$ est une base de K comme $\mathbb{Q}$-espace vectoriel.

Si K est un corps de nombres, pour tout θ dans K, le polynôme minimal $Irr(\theta, \mathbb{Q})$ n'a que des racines simples dans $\mathbb{C}$. On dit que l'extension $K/\mathbb{Q}$ est *séparable*. $K/\mathbb{Q}$ est galoisienne (on dit aussi le corps de nombres K est galoisien) si et seulement si elle est normale, c'est-à-dire que les conjugués sur $\mathbb{Q}$ de tout élément de K se trouvent dans K. Cela équivaut à dire que si θ est un élément quelconque de K, son polynôme minimal $Irr(\theta, \mathbb{Q})$ se "décompose complètement" dans $K[x]$, autrement dit, qu'il s'y écrit comme produit de facteurs de degré 1, ou encore, que tout plongement de K dans $\mathbb{C}$ est un automorphisme de K.

Soit K un corps de nombres de degré n. Il existe alors n plongements $\sigma_1, ..., \sigma_n$ de K dans $\mathbb{C}$, appelés aussi les *isomorphismes distincts* de K dans $\mathbb{C}$. Comme $\mathbb{Q}$ est un corps premier, ses éléments sont laissés fixes par chacun des σ_i. Si θ est un élément primitif quelconque de K, chacun des σ_i est entièrement déterminé par l'image dans $\mathbb{C}$ qu'il affecte à θ. De plus, un élément quelconque de K est primitif si et seulement si ses images par les σ_i sont deux à deux distinctes, et il est dans $\mathbb{Q}$ si et seulement s'il reste fixe par chacun des σ_i. Si K est galoisien (sur $\mathbb{Q}$), ces n isomorphismes distincts sont en fait des automorphismes de K et constituent le groupe de Galois $Gal(K/\mathbb{Q})$ de l'extension $K/\mathbb{Q}$.

1.3 Entiers algébriques, l'anneau des entiers d'un corps de nombres

Définition 1.3.1 *On appelle entier algébrique tout nombre complexe racine d'un polynôme unitaire à coefficients dans l'anneau des entiers rationnels $\mathbb{Z}$, autrement dit, tout nombre algébrique dont le polynôme minimal appartienne à $\mathbb{Z}[x]$.*

On montre que la somme et le produit d'un nombre fini d'entiers algébriques sont des entiers algébriques. Si K est un corps de nombres quelconque, l'ensemble A de tous les entiers algébriques contenus dans K est un sous-anneau de K, contenant $\mathbb{Z}$, appelé l'anneau des entiers de K. Si K est de degré n, A est un $\mathbb{Z}$-module libre de rang n.

Définition 1.3.2 *Soient K un corps de nombres et A son anneau des entiers. On appelle*

base de A (ou base des entiers de K) toute base du $\mathbb{Z}$-module libre A.

Si K est un corps de nombres de degré n sur $\mathbb{Q}$ et A son anneau des entiers, une base des entiers de K est donc une famille de n éléments $\omega_1, \omega_2, ..., \omega_n$ de A telle que tout élément θ de A peut être écrit et de manière unique sous la forme $\theta = a_1\omega_1 + a_2\omega_2 + ... + a_n\omega_n$ où les $a_i, i = 1, ..., n$, sont des entiers rationnels.

Remarque 1.3.1 *Soient K un corps de nombres et A son anneau des entiers. Par multiplication par un entier rationnel convenable, on peut toujours obtenir à partir d'un élément primitif donné de K sur $\mathbb{Q}$, un élément primitif θ qui soit un entier algébrique. La famille $\left\{1, \theta, ..., \theta^{n-1}\right\}$ est alors une base, formée d'entiers, de l'extension $K/\mathbb{Q}$. Ce n'est pas forcément une base des entiers de K. En fait, en tant que famille d'éléments de la $\mathbb{Z}$-algèbre A, elle engendre la sous-$\mathbb{Z}$-algèbre $\mathbb{Z}[\theta]$ et qui ne coincide pas toujours avec A.*

1.4 Discriminant d'un corps de nombres

Soient K un corps de nombres de degré n et $\sigma_1, ..., \sigma_n$ les n isomorphismes distincts de K dans $\mathbb{C}$.

Soit $(\theta_1, ..., \theta_n)$ un uplet quelconque d'éléments de K. Le discriminant, noté $Disc_{K/\mathbb{Q}}(\theta_1, ..., \theta_n)$, de ce uplet par rapport à l'extension $K/\mathbb{Q}$, est par définition le carré du déterminant de la matrice $(\sigma_i(\theta_j))_{i,j}$. C'est-à-dire :

$$Disc_{K/\mathbb{Q}}(\theta_1, ..., \theta_n) = |\sigma_i(\theta_j)|^2 = \begin{vmatrix} \sigma_1(\theta_1) & \sigma_1(\theta_2) & ... & \sigma_1(\theta_n) \\ \sigma_2(\theta_1) & \sigma_2(\theta_2) & ... & \sigma_2(\theta n) \\ ... & ... & ... & ... \\ \sigma_n(\theta_1) & \sigma_n(\theta_2) & ... & \sigma_n(\theta_n) \end{vmatrix}^2.$$

Le discriminant possède les propriétés données dans le résultat suivant.

Proposition 1.4.1 *Soit $(\theta_1, ..., \theta_n)$ un uplet d'éléments d'un corps de nombres K de degré n.*

(1) $Disc_{K/\mathbb{Q}}(\theta_1, ..., \theta_n)$ est invariant par permutation quelconque de l'ensemble $\{\theta_1, ..., \theta_n\}$.

(2) Si T désigne la fonction "trace" sur l'extension $K/\mathbb{Q}$, on a l'égalité suivante :

$$Disc_{K/\mathbb{Q}}(\theta_1, ..., \theta_n) = |T(\theta_i\theta_j)|$$

(3) $Disc_{K/\mathbb{Q}}(\theta_1, ..., \theta_n)$ *est invariant aux différents plongements* σ_i *de* K *dans* $\mathbb{C}$.
(4) $Disc_{K/\mathbb{Q}}(\theta_1, ..., \theta_n) = 0$ *si et seulement si* $\theta_1, ..., \theta_n$ *sont* K*-linéairement dépendants.*
(5) Si $(\alpha_1, ..., \alpha_n)$ *est une base des entiers de* K *et si pour tout* $i \in \{1, ..., n\}, \theta_i = \sum_{j=1}^{n} a_{ij}\alpha_j$, *alors :*

$$Disc_{K/\mathbb{Q}}(\theta_1, ..., \theta_n) = \det(a_{ij})^2 Disc_{K/\mathbb{Q}}(\alpha_1, ..., \alpha_n).$$

De la propriété (3) on déduit que $Disc_{K/\mathbb{Q}}(\theta_1, ..., \theta_n)$ est un élément de $\mathbb{Q}$. Si les θ_i sont des entiers de K, $Disc_{K/\mathbb{Q}}(\theta_1, ..., \theta_n)$ est un élément de $\mathbb{Z}$.

La propriété (5) implique, elle, que si $(\alpha, ..., \alpha_n)$ et $(\alpha'_1, ..., \alpha'_n)$ sont deux bases quelconques des entiers de K, alors leurs discriminants respectifs sont égaux. Cela permet de définir le discriminant d'un corps de nombres.

Définition 1.4.1 *Soit* K *un corps de nombres, on appelle discriminant de* K *(ou discriminant de* K *sur* $\mathbb{Q}$*), et on note* $Disc(K)$ *ou* $D(K)$*, le discriminant par rapport à l'extension* $K/\mathbb{Q}$ *de n'importe quelle base des entiers de* K.
Autrement dit, si $(\omega_1, ..., \omega_n)$ *est une base quelconque des entiers de* K, *on a*

$$Disc(K) = Disc_{K/\mathbb{Q}}(\omega_1, ..., \omega_n).$$

1.5 Décomposition d'un nombre premier dans un corps de nombres

Soient K un corps de nombres. On a rappelé dans la section 3 du présent chapitre la structure de $\mathbb{Z}$-module libre de A. Dans cette section, nous considérons A en sa qualité d' anneau de Dedekind.

On rappelle qu'un anneau A est dit noethérien si, dans cet anneau, l'une des trois conditions équivalentes suivantes est réalisée.

(a) Toute suite croissante d'idéaux de A est stationnaire.

(b) Toute famille non vide d'idéaux de A admet un élément maximal.

(c) Tout idéal de A est de type fini.

Un anneau A est dit intégralement clos s'il est intègre et si les seuls éléments de son corps des fractions qui soient entiers sur A, autrement dit, qui soient racines de polynômes unitaires à coefficients dans A, sont les éléments de A.

La définition d'un anneau de Dedekind est donnée dans ce qui suit.

Définition 1.5.1 *Un anneau est dit de Dedekind s'il est noethérien, intégralement clos et dont tous les idéaux premiers non nuls sont maximaux.*

Ainsi, les anneaux principaux, en particulier l'anneau $\mathbb{Z}$ des entiers rationnels, sont des anneaux de Dedekind. De même, on montre que, plus généralement, si A est un anneau de Dedekind de caractéristique 0 de corps des fractions K et si L est une extension finie de K, alors l'ensemble de tous les éléments de L entiers sur A (c'est-à-dire dont les polynômes minimaux respectifs sur K sont à coefficients dans A) est un anneau de Dedekind.

Théorème 1.5.1 *L'anneau des entiers d'un corps de nombres est un anneau de Dedekind.*

Un anneau de Dedekind étant intègre, l'idéal nul est un idéal premier. La propriété fondamentale vérifiée par un anneau de Dedekind est qu'un idéal quelconque peut s'écrire et de manière unique comme un produit fini d'idéaux premiers. En particulier, un idéal non nul a une écriture unique comme produit d'un nombre fini d'idéaux premiers non nuls, donc d'idéaux maximaux. C'est le résultat suivant.

Théorème 1.5.2 *Soit A un anneau de Dedekind. Tout idéal $\mathfrak{a}$ de A, non nul et différent de A, possède une écriture unique (à l'ordre près des termes) sous la forme :*

$$\mathfrak{a} = \mathcal{P}_1^{e_1} ... \mathcal{P}_r^{e_r}$$

où r et les e_i sont des entiers naturels ≥ 1 et les $\mathcal{P}_i$ des idéaux premiers non nuls (donc maximaux) de A.

Remarque 1.5.1 *La notion d'anneau de Dedekind est plus générale que celle d'anneau principal et l'unicité de la décomposition d'un élément comme produit d'éléments irréductibles (à la multiplication près par un élément inversible), valable dans les anneaux principaux, ne l'est pas toujours dans des anneaux de Dedekind quelconques. Celle-ci est remplacée par celle des idéaux comme produits d'idéaux premiers.*

Dans les anneaux noethériens, catégorie nettement plus large que celle des anneaux de Dedekind, il est une décomposition des idéaux qui soit garantie : la "décomposition primaire". Un idéal I d'un anneau A est dit primaire s'il est différent de A et si pour tous x et y dans A dont le produit xy soit dans I, l'élément x ou une puissance de l'élément y est dans I. Un résultat datant du début du XX-ème siècle, le "théorème de Lasker-Noether", affirme que tout idéal d'un anneau noethérien est intersection d'un nombre fini d'idéaux primaires. C'est cette décomposition primaire qui se transforme, dans le cas particulier des anneaux de Dedekind, en la décomposition en produit d'idéaux premiers. En effet, les idéaux primaires dans les anneaux de Dedekind sont en fait (0) et les puissances d'idéaux premiers non nuls, tandis qu' une intersection d'idéaux primaires, dont les radicaux sont distincts deux à deux, est égale à leur produit, étant donné que les idéaux puissances d'idéaux premiers non nuls, donc maximaux, sont étrangers deux à deux.

Remarque 1.5.2 *En réalité, le résultat énoncé dans le théorème 1.5.2 s'étend aux idéaux fractionnaires de A (on dit aussi de K) (Voir par exemple [22] ou [28]). Un idéal fractionnaire d'un anneau intègre quelconque A de corps des fractions K est par définition tout sous-A-module I de K formé d'éléments ayant un dénominateur commun dans A, c'est-à-dire tel qu'il existe un élément $d \in A$ vérifiant : $\forall x \in I, dx \in A$.*
Les idéaux de A sont des idéaux fractionnaires de A en prenant $d = 1$. Plus généralement, les sous-A-modules de type fini de K sont des idéaux fractionnaires de A.
L'ensemble des idéaux fractionnaires de K peut être muni de manière naturelle d'une multiplication qui en fait un monoïde dont l'élément neutre est A.
On montre que si A est un anneau de Dedekind, ce monoïde est un groupe et la décomposition des idéaux de A s'étend aux idéaux fractionnaires comme suit.

Tout idéal fractionnaire non nul $\mathfrak{b}$ de A, différent de A, peut s'écrire et de manière unique sous la forme :

$$\mathfrak{b} = \mathcal{P}_1^{e_1} ... \mathcal{P}_r^{e_r}$$

où $r \in \mathbb{N}^*$, les $e_i \in \mathbb{Z}^*$ et où les $\mathcal{P}_i$ sont des idéaux premiers non nuls de A.

Corollaire 1.5.1 *Soient K un corps de nombres et A son anneau des entiers. Alors tout*

idéal non nul $\mathfrak{a}$ *de* A *possède une écriture unique (à l'ordre près des termes) sous la forme :*

$$\mathfrak{a} = \mathcal{P}_1^{e_1} ... \mathcal{P}_r^{e_r}$$

où r *et les* e_i *sont des entiers naturels* ≥ 1 *et les* $\mathcal{P}_i$ *des idéaux premiers non nuls de* A*.*

Soient K un corps de nombres d'anneau des entiers A et p un nombre premier. L'idéal pA engendré par p dans A n'est pas forcément un idéal premier de A. C'est, d'après ce qui précède, un produit d'idéaux premiers de A. Les idéaux premiers qui interviennent dans la décomposition de pA sont exactement les idéaux premiers $\mathcal{P}$ de A vérifiant $\mathcal{P} \cap \mathbb{Z} = p\mathbb{Z}$. Ils sont en nombre fini et sont appelés les idéaux premiers de A (ou de K) au dessus de p. Si $\mathcal{P}$ est l'un d'eux, le corps $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ s'identifie à un sous-corps du corps $A/\mathcal{P}$. Ce dernier est donc une extension du corps premier $\mathbb{F}_p$. On montre que l'extension $(A/\mathcal{P})/\mathbb{F}_p$ est de degré fini $f_{\mathcal{P}}$. Cet entier $f_{\mathcal{P}}$ est alors appelé le degré résiduel de $\mathcal{P}$ sur p. Par ailleurs, l'exposant e, ou $e_{\mathcal{P}}$, avec lequel apparaît $\mathcal{P}$ dans la décomposition de pA est appelé l'indice de ramification de $\mathcal{P}$ sur p.

L'anneau quotient A/pA possède également une structure naturelle de $\mathbb{F}_p$-espace vectoriel. On montre qu'il est de dimension finie. Le résultat suivant donne une formule reliant cette dimension aux degrés résiduels et autres indices de ramification des idéaux premiers de A au dessus de p ainsi qu'au degré du corps de nombres considéré.

Théorème 1.5.3 *Soient* K *un corps de nombres de degré* n *sur* $\mathbb{Q}$ *et* A *son anneau des entiers. Soit* p *un nombre premier dont on suppose la décomposition en produit d'idéaux premiers donnée comme suit :*

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

où r *est un entier naturel non nul et où, pour tout* $i \in \{1, ..., r\}$*, le degré résiduel* $f_{\mathcal{P}_i}$ *de* $\mathcal{P}_i$ *est* f_i*.*
Alors on a l'égalité suivante :

$$\sum_{i=1}^{r} e_i f_i = [A/pA : \mathbb{F}_p] = n.$$

Le nombre premier p est dit inerte dans A (on dit aussi dans K) si l'idéal pA est un idéal premier de A, c'est-à-dire si dans la décomposition ci-dessus de pA, on a $r = e_1 = 1$ et donc $f = n$. Il est dit ramifié si l'un des e_i est ≥ 2 et complètement décomposé si $r = n$. Dans ce dernier cas on a alors $e_i = f_i = 1$ pour tout $i \in \{1, ..., n\}$.

Le résultat suivant précise les nombres premiers qui sont ramifiés dans un corps de nombres donné selon la valeur du discriminant de celui-ci.

Théorème 1.5.4 *Soit K un corps de nombres. Alors les nombres premiers qui se ramifient dans K sont ceux qui divisent le discriminant de K sur $\mathbb{Q}$. Ils sont de ce fait en nombre fini.*

Pour plus de détails sur les différentes notions contenues dans ce premier chapitre, on peut consulter [8], [22] et [28].

Chapitre 2

Dénominateurs de nombres algébriques et indices

2.1 Dénominateurs de nombres algébriques

Soient K un corps de nombres de degré $n \geq 2$ sur $\mathbb{Q}$, A son anneau des entiers et γ un élément primitif de K. Son polynôme minimal sur $\mathbb{Q}$ est alors un polynôme de degré n à coefficients rationnels. Par multiplication par un entier rationnel convenable, on peut toujours se ramener à un polynôme de degré n à coefficients entiers. On définit le polynôme minimal sur $\mathbb{Z}$ de γ de la manière suivante.

Définition 2.1.1 *On appelle polynôme minimal sur $\mathbb{Z}$ de γ et on note $Irr(\gamma, \mathbb{Z})$ l'unique polynôme $g(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in \mathbb{Z}[x]$ tel que $a_n \geq 1$ et $\gcd(a_0, ..., a_n) = 1$ annulé par γ.*

Remarque 2.1.1 *L'élément γ est un entier de K si et seulement si $Irr(\gamma, \mathbb{Q}) = Irr(\gamma, \mathbb{Z})$.*

Si l'on note par $c = c(\gamma)$ le coefficient dominant a_n de $Irr(\gamma, \mathbb{Z})$, il est clair que puisque $c\gamma^n + a_{n-1}\gamma + ... + a_1\gamma + a_0 = 0$, alors par multiplication par c^{n-1}, on a : $(c\gamma)^n + a_{n-1}(c\gamma)^{n-1} + ... + c^{n-2}a_1(c\gamma) + c^{n-1}a_0 = 0$. L'élément $c\gamma$ est donc racine du polynôme unitaire à coefficients dans $\mathbb{Z}$ défini par : $h(x) = x^n + a_{n-1}x^{n-1} + ... + c^{n-2}a_1 x + c^{n-1}a_0$. C'est donc un élément de A.

Dans la suite, on appellera, par abus de langage, coefficient dominant du nombre algébrique γ l'entier $c(\gamma)$ défini ci-dessus.

Posons $J(\gamma) = \{m \in \mathbb{N}, m\gamma \in A\}$. L'ensemble $J(\gamma)$ est clairement un idéal non nul de $\mathbb{Z}$. Il existe donc un entier $d(\gamma) \geq 1$ (unique) engendrant $J(\gamma)$. L'entier $d(\gamma)$ est appelé le dénominateur du nombre algébrique γ. Compte tenu de ce qui précède, il est évident que $d(\gamma)$ est plus petit ou égal à $c(\gamma)$ et même un diviseur (dans $\mathbb{Z}$) de $c(\gamma)$. (Voir [1], [2] ou [3]).

Etant donné un nombre algébrique γ, on n'a pas forcément l'égalité de $c(\gamma)$ et $d(\gamma)$. Par exemple, si γ est une racine (dans $\mathbb{C}$) du polynôme irréductible (sur $\mathbb{Q}$) $4x^2 + 2x + 1$, il est clair que $c(\gamma) = 4$ tandis que $d(\gamma) = 2$, étant donné que le nombre algébrique 2γ vérifie $(2\gamma)^2 + (2\gamma) + 1 = 0$.

Arno, Robinson et Wheeler [1] ont étudié la densité des nombres algébriques pour lesquels les dénominateur et coefficient dominant sont égaux. Plus précisément, en utilisant un résultat de J. E. Nymann sur la probabilité que k entiers strictement positifs soient premiers entre eux dans leur ensemble [25] et un calcul dû à Pólya et Szegő [27] du nombre de polynômes de $\mathbb{Z}[x]$ primitifs de degré donné et dont les coefficients sont en valeur absolue bornés par un certain entier donné, ils ont calculé la proportion des nombres algébriques γ de degré donné d tels que $d(\gamma) = c(\gamma)$. C'est le théorème suivant.

Théorème 2.1.1 *La densité des nombres algébriques γ de degré donné d tels que $d(\gamma) = c(\gamma)$ est égale à*

$$\prod_p \left(1 - \frac{1}{p^3} \frac{(1 - \frac{1}{p^{d-1}})}{(1 - \frac{1}{p^{d+1}})}\right)$$

où le produit porte sur tous les nombres premiers.
Il s'ensuit que cette densité tend vers $\dfrac{1}{\zeta(3)}$ lorsque d tend vers ∞.

Remarque 2.1.2 *Etant donnés un corps de nombres K, un élément γ de K de degré n et un nombre premier p, il est clair que si $k = v_p(c(\gamma))$, alors $v_p(d(\gamma))$ est comprise entre k et nk. Dans un récent article paru en 2015, Ayad, Bayad et Kihel ont étudié les valeurs possibles prises par $v_p(d(\gamma))$ lorsque γ parcourt K. Voir [2].*

Soient θ et θ' deux entiers algébriques primitifs d'un corps de nombres de degré n, p un nombre premier quelconque et k un entier rationnel ≥ 1. On suppose que p ne divise pas θ et que $\theta \equiv \theta' \pmod{p^k}$. On peut se poser la question suivante.

A-t-on l'égalité : $(*) : v_p(c(\frac{\theta}{p^k})) = v_p(c(\frac{\theta'}{p^k}))$?

On verra dans ce qui suit que dans le cas des corps de nombres quadratiques, la réponse est oui.

Notons par θ_i, $i = 1, ..., n$, les conjugués de θ et pour tout $m = 1, ..., n$, par $s_m(\theta)$, l'entier rationnel défini par $s_m(\theta) = \sum_{i_1<...<i_m} \theta_{i_1}\theta_{i_2}...\theta_{i_m}$. Alors
$Irr(\theta, \mathbb{Q}) = Irr(\theta, \mathbb{Z}) = f(x) = x^n - s_1(\theta)x^{n-1} + s_2(\theta)x^{n-2} - ... + (-1)^n s_n(\theta)$.
Dans ce cas, $Irr(\frac{\theta}{p^k}, \mathbb{Q})$ vérifie : $f(p^k x) = p^{nk} Irr(\frac{\theta}{p^k}, \mathbb{Q})$.
D'autre part, $f(p^k x) = Cont(f(p^k x)) \times Irr(\frac{\theta}{p^k}, \mathbb{Z})$. On en tire : $c(\frac{\theta}{p^k}) = \frac{p^{nk}}{Cont(f(p^k x))}$, en particulier, $v_p(c(\frac{\theta}{p^k})) = nk - v_p(Cont(f(p^k x))$.
De même, si $g(x) = Irr(\theta', \mathbb{Q}) = Irr(\theta', \mathbb{Z})$, on a : $v_p(c(\frac{\theta'}{p^k})) = nk - v_p(Cont(g(p^k x))$
Démontrer l'égalité $(*)$ revient donc à démontrer l'égalité suivante :

$$v_p(Cont(f(p^k x)) = v_p(Cont(g(p^k x))$$

Par hypothèse, $\theta' = \theta + p^k\alpha$ pour un certain entier algébrique $\alpha \in \mathbb{Q}(\theta) = \mathbb{Q}(\theta')$. Si l'on note par $\theta'_1, ..., \theta'_n$ les conjugués de θ' et par $\alpha_1, ..., \alpha_n$ ceux de α (numérotés de sorte que pour tout i, les éléments θ'_i et α_i correspondent respectivement à l'image de θ et à celle de α par le même $\mathbb{Q}$-isomorphisme de $\mathbb{Q}(\theta)$ dans $\mathbb{C}$), on a pour tout i : $\theta'_i = \theta_i + p^k\alpha_i$. Par conséquent, on a :
$g(x) = x^n - s_1(\theta')x^{n-1} + s_2(\theta')x^{n-2} - ... + (-1)^n s_n(\theta')$
$= x^n - s_1(\theta + p^k\alpha)x^{n-1} + s_2(\theta + p^k\alpha)x^{n-2} - ... + (-1)^n s_n(\theta + p^k\alpha)$
Mais,
$s_1(\theta + p^k\alpha) = s_1(\theta) + p^k s_1(\alpha)$, $s_2(\theta + p^k\alpha) = \sum_{i<j}(\theta_i + p^k\alpha_i)(\theta_j + p^k\alpha_j)$
$= \sum_{i<j}\left[\theta_i\theta_j + p^k(\alpha_i\theta_j + \alpha_j\theta_i) + p^{2k}(\alpha_i\alpha_j)\right] = s_2(\theta) + p^k(\sum_{i<j}(\alpha_i\theta_j + \alpha_j\theta_i)) + p^{2k}s_2(\alpha)$
...
$s_n(\theta + p^k\alpha) = \prod_i(\theta_i + p^k\alpha_i) = (\prod_i\theta_i) + p^k\left[\alpha_1(\prod_{i\neq 1}\theta_i) + ... + \alpha_n(\prod_{i\neq n}\theta_i)\right]$
$+p^{2k}\left[\alpha_1\alpha_2(\prod_{i\neq 1,2}\theta_i)) + ...\right] + ... + p^{nk}\prod_i\alpha_i = s_n(\theta) + p^k[...] + ... + p^{nk}s_n(\alpha)$
En fait, pour tout $i = 1, ..., n$, $s_i(\theta') = s_i(\theta) + p^k a_i$ pour un certain entier rationnel a_i. Donc,
$g(x) = x^n - \left[s_1(\theta) + p^k a_1\right]x^{n-1} + \left[s_2(\theta) + p^k a_2\right]x^{n-2} - ... + (-1)^n\left[s_n(\theta) + p^k a_n\right]$.

On a finalement :

$$f(p^k x) = p^{nk}x^n - p^{(n-1)k}s_1(\theta)x^{n-1} + ... + (-1)^{n-1}p^k s_{n-1}(\theta)x + (-1)^n s_n(\theta)$$

et

$$g(p^k x) = x^n - p^{(n-1)k}\left[s_1(\theta) + p^k a_1\right]x^{n-1} + ...$$

$$... + (-1)^{n-1}p^k\left[s_{n-1}(\theta) + p^k a_{n-1}\right]x + (-1)^n\left[s_n(\theta) + p^k a_n\right].$$

Lemme 2.1.1 *Si* $Cont(f(p^k x)) = p^t$ *avec* $t \leq k$ *alors* $v_p(Cont(f(p^k x)) = v_p(Cont(g(p^k x))$.

Démonstration. En effet, si $t \leq k$, alors d'après ce qui précède, p^t divise tous les coefficients de $g(p^k x)$. Par conséquent, $v_p(Cont(f(p^k x)) \leq v_p(Cont(g(p^k x))$. Mais θ et θ' jouant des rôles symétriques, on a aussi $v_p(Cont(g(p^k x)) \leq v_p(Cont(f(p^k x))$ d'où l'égalité. ■

Dans la suite, nous montrons que l'égalité $(*)$ est vraie dans le cas des corps quadratiques. Nous avons besoin pour cela du lemme suivant.

Lemme 2.1.2 *Soit* θ *un entier algébrique primitif de polynôme minimal* $f(x)$ *d'un corps quadratique* $\mathbb{Q}(\sqrt{d})$, *où* $d \neq 1$ *et* d *sans facteur carré,* p *un nombre premier quelconque et* k *un entier* ≥ 1. *On suppose* θ *non congru à* $0 \pmod p$. *Alors :*

$$\begin{cases} v_2(Cont(f(2^k x))) \leq k+1 & si\ d \equiv 2,3 (\mathrm{mod}\, 4) \\ v_p(Cont(f(p^k x))) \leq k & si\ d \equiv 1 (\mathrm{mod}\, 4) \end{cases}$$

Démonstration. 1) Cas $d \equiv 2,3 \pmod 4$ θ s'écrit : $\theta = a + b\sqrt{d}$, a et b entiers rationnels non tous deux divisibles par p. Dans ce cas, $f(x) = x^2 - 2ax + a^2 - db^2$ et $f(p^k x) = p^{2k}x^2 - 2p^k ax + a^2 - db^2$. Supposons $p \neq 2$. Si $v_p(Cont(f(p^k x))) > k$, alors p^{k+1} divise $2p^k a$ et $a^2 - db^2$. Par conséquent, p divise a et p^2 divise $a^2 - db^2$. Mais comme p^2 divise a^2 alors il est diviseur de db^2 donc de b^2, d étant sans facteur carré. Finalement p divise à la fois a et b ce qui contredit l'hypothèse. Si $p = 2$, le même raisonnement permet d'affirmer que la

valuation 2-adique ne peut excéder $k+1$ strictement car sinon 2 diviserait à la fois a et b.
2) Cas $d \equiv 1 \pmod 4$ θ s'écrit : $\theta = a + b(\frac{1+\sqrt{d}}{2})$, a et b entiers rationnels non tous deux divisibles par p et on a : $f(x) = x^2 - (2a+b)x + a^2 + ab + b^2(\frac{1-d}{4})$ et $f(p^k x) = p^{2k}x^2 - 2p^k(2a+b)x + a^2 + ab + b^2(\frac{1-d}{4})$. Montrons que $v_p(Cont(f(p^k x))) \leq k \ \forall p$. En effet, si $p \neq 2$, $v_p(Cont(f(p^k x))) > k$ impliquerait que p^{k+1} divise $2a+b$ et $a^2+ab+b^2(\frac{1-d}{4})$ donc aussi $4(a^2+ab+b^2(\frac{1-d}{4})) = (2a+b)^2 - db^2$. Donc p divise $2a+b$, ce qui implique que p^2 divise $(2a+b)^2$ et donc aussi db^2. Donc, p divise forcément b donc aussi $2a$ donc a. Contradiction avec le fait que θ soit non congru à $0 \pmod p$. Si $p=2$, $v_2(Cont(f(2^k x))) > k$ impliquerait que 2 est diviseur de $2a+b$ et que 2^{k+1} est diviseur de $a^2+ab+b^2(\frac{1-d}{4})$. Donc, 2 divise b (puisqu'il divise $2a+b$ et $2a$) et 2^{k+3} divise $4(a^2+ab+b^2(\frac{1-d}{4})) = (2a+b)^2 - db^2$. k étant ≥ 1, 2^{k+3} est multiple de 16. Donc $(2a+b)^2 - db^2$ est multiple de 16. Or, modulo 16, $db^2 \equiv b^2$ (car $b^2 \equiv 0 (\mathrm{mod}\, 4)$ et $d \equiv 1 (\mathrm{mod}\, 4)$ donc, $(2a+b)^2 - db^2 \equiv (2a+b)^2 - b^2 = 4a(a+b) \equiv 0 (\mathrm{mod}\, 16)$. Et ceci n'est possible que si a est pair. Donc a et b sont tous les deux divisibles par 2, ce qui contredit l'hypothèse. ■

Proposition 2.1.1 *Soient θ et θ' deux entiers algébriques primitifs d'un corps quadratique, p un nombre premier quelconque et k un entier rationnel ≥ 1. On suppose que p ne divise pas θ et que $\theta \equiv \theta' (\mathrm{mod}\, p^k)$. Alors*

$$v_p(c(\frac{\theta}{p^k})) = v_p(c(\frac{\theta'}{p^k})).$$

Démonstration. D'après les deux lemmes précédents, l'égalité $(*)$ est vraie dans le cas des corps quadratiques $\mathbb{Q}(\sqrt{d})$ avec $d \equiv 1 (\mathrm{mod}\, 4)$ ainsi que dans celui des corps $\mathbb{Q}(\sqrt{d})$ avec $d \equiv 2, 3 (\mathrm{mod}\, 4)$ lorsque $p \neq 2$. Il reste donc seulement le cas $\mathbb{Q}(\sqrt{d})$ avec $d \equiv 2, 3 (\mathrm{mod}\, 4)$ lorsque $p = 2$. Dans ce cas, on a vu que $v_2(Cont(f(2^k x))) \leq k+1$. Or, $f(2^k x) = 2^{2k}x^2 - 2^{k+1}ax + a^2 - db^2$ et si $\theta' = \theta + 2^k\alpha = a + b\sqrt{d} + 2^k(c + e\sqrt{d})$, le polynôme minimal $g(x)$ sur $\mathbb{Q}$ (ou sur $\mathbb{Z}$) de θ' vérifie :
$g(2^k x) = 2^{2k}x^2 - 2^{k+1}(a+2^k c)x + 2^{2k}c^2 + 2^{k+1}ac + a^2 - (b^2 + 2^{k+1}be + 2^{2k}e^2)d$.
Montrons que si $(Cont(f(2^k x))) = 2^t$ avec $t \leq k+1$, alors 2^t divise les coefficients de $g(2^k x)$. Pour cela, il suffit de vérifier que 2^t divise les coefficients du polynôme :
$g(2^k x) - f(2^k x) = 2^{k+1}2^k cx + 2^{2k}c^2 + 2^{k+1}ac - (2^{k+1}be + 2^{2k}e^2)d$,
ce qui est manifestement le cas. ■

2.2 Petit indice d'un corps de nombres

Dans cette section, nous traitons de la notion de *petit indice* d'un corps de nombres, une notion définie par Gunji et McQuillan [14]. La section suivante traitera de la notion de *grand indice* (ou plus simplement *indice* s'il n'y a pas de risque de confusion). Au chapitre 4, nous verrons un lien entre les deux notions à travers un résultat de Ayad et Kihel [5].

Posons pour tout entier naturel k

$$\begin{pmatrix} x \\ k \end{pmatrix} = \begin{cases} 1 & \text{si } k = 0 \\ x(x-1)...(x-(k-1)) & \text{si } k \geq 1 \end{cases}$$

Pour tout k, $\begin{pmatrix} x \\ k \end{pmatrix}$ est un polynôme de degré k. Par conséquent, la famille des $\begin{pmatrix} x \\ k \end{pmatrix}$ pour k allant de 0 à n, est une base du $\mathbb{Q}$-espace vectoriel $\mathbb{Q}_n[x]$ des polynômes de degré $\leq n$ à coefficients dans $\mathbb{Q}$.

Soit un polynôme $F(x)$ appartenant à $\mathbb{Q}[x]$. Dans [24], Nagell rappelle que $F(x)$ représente des entiers pour toutes les valeurs entières de x si et seulement si $F(x)$ peut s'écrire sous la forme :

$$F(x) = a_0 + a_1 \begin{pmatrix} x \\ 1 \end{pmatrix} + ... + a_n \begin{pmatrix} x \\ n \end{pmatrix}$$

où pour tout $i = 0, ..., n$, $i!a_i \in \mathbb{Z}$.

En particulier, si $F(x)$ est à coefficients entiers rationnels et qu'il est unitaire, alors :

$$F(x) = a_0 + a_1 \begin{pmatrix} x \\ 1 \end{pmatrix} + ... + a_n \begin{pmatrix} x \\ n \end{pmatrix}$$

où pour tout $i = 0, ..., n$, $a_i \in \mathbb{Z}$ et $a_n = 1$.

En effet, si $F(x)$ s'écrit dans la base $\left(1, \begin{pmatrix} x \\ 1 \end{pmatrix}, ..., \begin{pmatrix} x \\ n \end{pmatrix}\right)$ sous la forme $F(x) = a_0 + a_1 \begin{pmatrix} x \\ 1 \end{pmatrix} + ... + a_n \begin{pmatrix} x \\ n \end{pmatrix}$ alors

$F(x) = a_0 + a_1 x + a_2 x(x-1) + ... + a_n x(x-1)...(x-(n-1))$

Il est clair que a_0 coincide avec le coefficient constant de $F(x)$ et a_n avec son coefficient dominant. Ils sont donc entiers et a_n vaut 1. Pour les autres coefficients, on peut remarquer

que pour tout $i = 1, ..., n-1$, le coefficient de x^i peut s'écrire sous la forme $a_i + f_i(a_{i+1}, ..., a_n)$ où f_i est une forme linéaire d'ordre $n - i$ (autrement dit, $f_i(a_{i+1}, ..., a_n)$ est de la forme $c_{i+1}a_{i+1} + ... + c_n a_n$ où les c_j sont dans $\mathbb{Z}$). On voit alors facilement que $a_{n-1} \in \mathbb{Z}$, puis de proche en proche que tous les $a_i \in \mathbb{Z}$.

Dans ce qui suit, on définit le *petit indice* d'un entier algébrique.

Définition 2.2.1 *Soit θ un entier algébrique de polynôme minimal $F(x)$ sur $\mathbb{Q}$. On appelle petit indice de θ et on note $i(\theta)$ le plus grand commun diviseur de l'ensemble $\{F(x), x \in \mathbb{Z}\}$, c'est-à-dire :*

$$i(\theta) = \underset{x \in \mathbb{Z}}{\gcd} F(x)$$

On montre facilement (voir par exemple [5]), que l'écriture d'un polynôme de degré n à coefficients dans $\mathbb{Z}$ dans la base des $\begin{pmatrix} x \\ k \end{pmatrix}$, $k = 0, ..., n$, permet de déterminer rapidement la valeur de son plus grand commun diviseur comme le montre la proposition ci-dessous.

Proposition 2.2.1 *Soit $F(x)$ un polynôme de $\mathbb{Z}[x]$ de degré n. On suppose que son écriture dans la base des $\begin{pmatrix} x \\ k \end{pmatrix}$, $k = 0, ..., n$, est la suivante :*

$$F(x) = a_0 + a_1 \begin{pmatrix} x \\ 1 \end{pmatrix} + ... + a_n \begin{pmatrix} x \\ n \end{pmatrix}$$

où les $a_i \in \mathbb{Z}$.

Alors :

$$\underset{x \in \mathbb{Z}}{\gcd} F(x) = \underset{j \in \{0,...,n\}}{\gcd} (j! a_j)$$

Corollaire 2.2.1 *Soient θ un entier algébrique de degré n sur $\mathbb{Q}$ et $F(x)$ son polynôme minimal. On suppose que $F(x)$ s'écrit :*

$$F(x) = a_0 + a_1 \begin{pmatrix} x \\ 1 \end{pmatrix} + ... + a_n \begin{pmatrix} x \\ n \end{pmatrix}.$$

Alors :

$$i(\theta) = \gcd_{j\in\{0,\dots,n\}} (j!a_j).$$

Remarque 2.2.1 *Avec les hypothèses de ce corollaire, on a* $a_n = 1$ *et, par conséquent,* $i(\theta)$ *est un diviseur de* $n!$ *et ceci pour tout* θ *entier de degré* n*. Ainsi, pour tout corps de nombres, l'indice de n'importe lequel de ses entiers primitifs est diviseur de la factorielle du degré de ce corps sur* $\mathbb{Q}$*.*

Cette remarque permet la définition suivante.

Définition 2.2.2 *Soient* K *un corps de nombres de degré* n *d'anneau des entiers* A*. On note par* A_n *l'ensemble des entiers primitifs de* K*. On appelle alors petit indice de* K *et on note* $i(K)$ *le plus petit multiple commun des* $i(\theta)$ *lorsque* θ *parcourt* A_n*. Autrement dit,*

$$i(K) = \operatorname*{lcm}_{\theta\in A_n} i(\theta)$$

Exemple 2.2.1 *Le cas des corps quadratiques.*
Il est clair d'après ce qui précède que pour tout entier algébrique de degré 2*, le petit indice ne peut être que* 1 *ou* 2*. Si* d *est un entier différent de* 1 *sans facteur carré, on a le résultat suivant (voir [23])*

$$i(\mathbb{Q}(\sqrt{d})) = \begin{cases} 2 & si\ d \equiv 1 \pmod 8 \\ 1 & sinon \end{cases}$$

On peut, ici, vérifier directement (sans utiliser le corollaire 2.2.1) que, par exemple, si $d \equiv 1 \pmod 8$ *alors* $i(\mathbb{Q}(\sqrt{d})) = 2$*. En effet, dans ce cas, un entier quelconque de degré* 2 *peut être écrit sous la forme* $a + b\dfrac{1+\sqrt{d}}{2}$ *avec* $b \neq 0$ *et son polynôme minimal est*

$$F(x) = x^2 - (2a+b)x + a^2 + ab + b^2\frac{1-d}{4}$$

Dire que $i(\mathbb{Q}(\sqrt{d})) = 2$ *équivaut à l'existence d'un entier dont le petit indice est* 2 *donc d'un*

couple (a,b) *tel que* 2 *divise* $F(x) = x^2 - (2a+b)x + a^2 + ab + b^2\dfrac{1-d}{4}$ *pour tout* $x \in \mathbb{Z}$. *Or, il suffit que* a *soit pair et* b *impair pour que cette expression soit un entier pair pour toute valeur de* x. *En effet,* d *étant congru à* $1 \pmod 8$, *l'entier* $\dfrac{1-d}{4}$ *est pair donc aussi* $a^2+ab+b^2\dfrac{1-d}{4}$ *puisque* a *est pair. Il reste à voir la parité de* $x^2-(2a+b)x$. *Or,* $x^2-(2a+b)x = x(x-2a-b)$ *et on voit que dans ce produit l'un des deux facteurs est forcément pair.*
On peut voir de la même manière que si $d \equiv 2$ *ou* $3 \pmod 4$, *alors* $i(\mathbb{Q}(\sqrt{d})) = 1$ *en montrant que tout entier est d'indice* 1 *(les entiers non primitifs, donc de degré* 1, *étant évidemment d'indice* 1 *puisque d'indice diviseur de* 1!*). En effet, dans ce cas, tout entier* θ *peut être écrit sous la forme* $a + b\sqrt{d}$ *et son polynôme minimal, si* $b \neq 0$, *est* $F(x) = x^2 - 2ax + a^2 - db^2$. *On voit alors clairement que quelle que soit la "valeur" du couple* (a,b), *la parité de* $F(x)$ *dépendra entièrement de celle de* x. 2 *n'est donc pas diviseur de* $F(x)$ *pour toute valeur de* x *et on a donc* $i(\mathbb{Q}(\sqrt{d})) = 1$.

On voit que dans le cas des corps de nombres quadratiques, il existe toujours un entier dont le petit indice est celui du corps. Le résultat suivant, dû à Gunji et McQuillan [14], généralise cette propriété à tous les corps de nombres.

Théorème 2.2.1 *Soit* K *un corps de nombres. Parmi les entiers de* K *qui sont primitifs, il en existe au moins un dont le petit indice est multiple de celui de chacun des autres.*

Etant donné un corps de nombres K de degré n sur $\mathbb{Q}$, son petit indice $i(K)$ est un diviseur de $n!$. MacCluer donne ci-après une condition nécessaire et suffisante pour qu'un nombre premier donné divise $i(K)$.

Théorème 2.2.2 *Soit* K *un corps de nombres de degré* n *d'anneau des entiers* A. *Alors* $i(K) > 1$ *si et seulement si pour un certain nombre premier* $p \leq n$, *le nombre d'idéaux premiers de* A *au-dessus de* p *est au moins égal à* p. *Si oui,* $i(K)$ *a exactement comme diviseurs premiers les nombres premiers vérifiant cette propriété.*

Remarque 2.2.2 *D'autres résultats sur les notions de dénominateur et de petit indice sont établis par Ayad, Bayad et Kihel [3], dont une généralisation du théorème de MacCluer.*

2.3 Indice (ou grand indice) d'un entier algébrique

Soit K un corps de nombres de degré n. On note par A l'anneau des entiers de K.

On suppose que $(\omega_1, ..., \omega_n)$ est une base des entiers de K, autrement dit une base du $\mathbb{Z}$-module libre A.

Soit D le discriminant de K, c'est-à-dire $D = Disc(K) = Disc_{K/\mathbb{Q}}(\omega_1, ..., \omega_n)$.

D'après les propriétés du discriminant, pour tout $\theta \in A$, on a :

$Disc_{K/\mathbb{Q}}(1, \theta, ..., \theta^{n-1}) = I(\theta)^2 D$ où $I(\theta)$ est défini par :

$$I(\theta) = \begin{cases} 0 & \text{si } K \neq \mathbb{Q}(\theta) \\ |\det(P)| & \text{si } K = \mathbb{Q}(\theta) \end{cases}$$

P étant la matrice de passage de la base $(\omega_1, ..., \omega_n)$ à la base $(1, \theta, ..., \theta^{n-1})$ (en tant que bases du corps de nombres K sur $\mathbb{Q}$).

Si θ est un entier primitif de K, le nombre $I(\theta)$ est un entier naturel non nul et il coincide avec l'indice du sous-groupe $\mathbb{Z}[\theta]$ dans le groupe A en tant que groupes additifs.

Définition 2.3.1 *Soient K un corps de nombres de degré n sur $\mathbb{Q}$ d'anneau des entiers A et θ un élément quelconque de A. On appelle indice de θ l'entier naturel $I(\theta)$ défini par*

$$Disc_{K/\mathbb{Q}}(1, \theta, ..., \theta^{n-1}) = I(\theta)^2 D(K)$$

De plus, $I(\theta)$ est non nul si et seulement si θ est un élément primitif de K et si oui, il est égal à l'indice de $\mathbb{Z}[\theta]$ dans A, en tant que groupes additifs.

Soit K un corps de nombres et A son anneau des entiers. On sait, il existe des éléments primitifs dans K et même des entiers primitifs, c'est-à-dire des éléments θ de A tels que $K = \mathbb{Q}(\theta)$. Mais, en dehors du cas où K est quadratique, il n'existe pas toujours d'élément θ de A dont les puissances engendrent le $\mathbb{Z}$-module A, autrement dit, il n'existe pas toujours d'élément $\theta \in A$ tel que $A = \mathbb{Z}[\theta]$.

Cependant, si θ est un entier primitif quelconque d'un corps de nombres K, le résultat suivant, utilisant les propriétés des modules sur les anneaux principaux, affirme l'existence d'une base privilégiée de l'anneau des entiers de K et qui, dans la pratique, rend d'énormes services.

Théorème 2.3.1 *Soit K un corps de nombres de degré n sur $\mathbb{Q}$, A son anneau des entiers et θ un entier primitif de K.*

Alors il existe une base de A de type :

$$(1, \frac{f_1(\theta)}{d_1}, ..., \frac{f_{n-1}(\theta)}{d_{n-1}})$$

où les d_i sont des entiers rationnels non nuls vérifiant $d_1 \mid d_2 \mid ... \mid d_{n-1}$ et où pour tout $i \in \{1, ..., n-1\}$, f_i est un polynôme unitaire à coefficients dans $\mathbb{Z}$ de degré i.
De plus, les d_i sont déterminés de manière unique et on a :

$$I(\theta) = d_1 d_2 ... d_{n-1}$$

Démonstration. Voir [22]. Pour la dernière égalité, il suffit d'utiliser la propriété 4) concernant le discriminant et de remarquer que le vecteur colonne

$$(\omega_1 = 1, \omega_2 = \frac{f_1(\theta)}{d_1}, ..., \omega_n = \frac{f_{n-1}(\theta)}{d_{n-1}})$$

est l'image par une matrice carrée triangulaire du vecteur colonne $(1, \theta, ..., \theta^{n-1})$ et dont les coefficients de la diagonale sont $1, \frac{1}{d_1}, ..., \frac{1}{d_{n-1}}$. ■

Nous avons vu dans la première section de ce chapitre les notions de coefficient dominant et de dénominateur d'un nombre algébrique, notions qui se confondent "souvent" grâce au résultat de Arno, Robinson et Wheeler [1]. Le résultat suivant, dont la démonstration utilise le théorème précédent, compare les coefficients dominants de deux nombres algébriques vérifiant certaines conditions.

Théorème 2.3.2 *Soient p un nombre premier, θ et θ' deux entiers d'un corps de nombres K tels que $\theta \equiv \theta' (mod\ p)$. On suppose θ primitif, non congru à 0 $(mod\ p)$ et que $p \nmid I(\theta)$.*
Alors θ' est aussi un élément primitif de K et on a l'égalité :

$$c(\frac{\theta}{p}) = c(\frac{\theta'}{p})$$

Démonstration. On suppose que K est de degré n sur $\mathbb{Q}$. θ' peut s'écrire $\theta' = \theta + p\gamma$ où γ est un certain entier de K. Notons par $\theta_1, \theta_2, ..., \theta_n$ et $\gamma_1, \gamma_2, ..., \gamma_n$ les n images de θ et γ respectivement par les n isomorphismes distincts de K dans $\mathbb{C}$. Les θ_i sont les racines du polynôme caractéristique de θ et qui, θ étant primitif, coincide avec son polynôme minimal

sur $\mathbb{Q}$ tandis que les γ_i sont les racines du polynôme caractéristique de γ (donc aussi racines de son polynôme minimal mais sans être forcément deux à deux distinctes). Les conjugués de θ' sur $\mathbb{Q}$ sont alors les entiers $\theta'_1 = \theta_1 + p\gamma_1, \theta'_2 = \theta_2 + p\gamma_2, ..., \theta'_n = \theta_n + p\gamma_n$. L'hypothèse "$\theta$ non congru à 0 (mod p)" signifie $c(\frac{\theta}{p}) = p^t$ avec $t \geq 1$. Ce t est le plus petit entier tel que $p^t \times Irr(\theta, \mathbb{Q}) \in \mathbb{Z}[x]$. Si pour tout entier α primitif, $s_1(\alpha), s_2(\alpha), ..., s_n(\alpha)$ désignent les fonctions élémentaires symétriques des racines de $Irr(\alpha, \mathbb{Q})$, cette hypothèse signifie que t est le plus petit entier tel que $p^t s_j(\frac{\theta}{p}) \in \mathbb{Z}$ pour tout $j = 1, ..., n$. On va montrer que si $c(\frac{\theta'}{p}) = p^{t'}$ alors $t \leq t'$. Cela impliquerait par symétrie que l'on a aussi $t' \leq t$ d'où l'égalité.

Il est clair que $s_j(\frac{\theta}{p}) = \frac{1}{p^j} s_j(\theta)$ et, de même, $s_j(\frac{\theta'}{p}) = \frac{1}{p^j} s_j(\theta')$. Par conséquent, t est le plus petit entier tel que $p^{t-j} s_j(\theta) \in \mathbb{Z}$, ce qui signifie aussi que t est le plus petit entier tel que $p^{j-t} \mid s_j(\theta)$ pour tout $j = 1, ..., n$. Pour montrer que $t \leq t'$ il suffit alors de montrer que p^{j-t} divise $s_j(\theta')$ pour tout $j = 1, ..., n$.

Or,

$$s_j(\theta') = \sum_{1 \leq i_1 < ... < i_j \leq n} \theta'_{i_1} \theta'_{i_2} ... \theta'_{i_j} = \sum_{1 \leq i_1 < ... < i_j \leq n} (\theta_{i_1} + p\gamma_{i_1})(\theta_{i_2} + p\gamma_{i_2})...(\theta_{i_j} + p\gamma_{i_j})$$

et on a :

$$(\theta_{i_1} + p\gamma_{i_1})(\theta_{i_2} + p\gamma_{i_2})...(\theta_{i_j} + p\gamma_{i_j}) = \theta_{i_1}\theta_{i_2}...\theta_{i_j}$$
$$+p(\gamma_{i_1}\theta_{i_2}...\theta_{i_j} + \gamma_{i_2}\theta_{i_1}\theta_{i_3}...\theta_{i_j} + ... + \gamma_{i_j}\theta_{i_1}\theta_{i_2}...\theta_{i_{j-1}})$$
$$+p^2(\gamma_{i_1}\gamma_{i_2}\theta_{i_3}...\theta_{i_j} + \gamma_{i_1}\gamma_{i_3}\theta_{i_2}\theta_{i_4}...\theta_{i_j} + ...)$$
$$.....$$
$$+p^{j-1}(\gamma_{i_1}\gamma_{i_2}...\gamma_{i_{j-1}}\theta_{i_j} + ... + \gamma_{i_2}...\gamma_{i_j}\theta_{i_1}) + p^j\gamma_{i_1}\gamma_{i_2}...\gamma_{i_j}.$$

Par conséquent,

$$s_j(\theta') = s_j(\theta) + p \sum_{1 \leq i_1 < ... < i_j \leq n} (\gamma_{i_1}\theta_{i_2}...\theta_{i_j} + \gamma_{i_2}\theta_{i_1}\theta_{i_3}...\theta_{i_j} + ... + \gamma_{i_j}\theta_{i_1}\theta_{i_2}...\theta_{i_{j-1}})$$
$$+p^2 \sum_{1 \leq i_1 < ... < i_j \leq n} (\gamma_{i_1}\gamma_{i_2}\theta_{i_3}...\theta_{i_j} + \gamma_{i_1}\gamma_{i_3}\theta_{i_2}\theta_{i_4}...\theta_{i_j} + ... + \gamma_{i_{j-1}}\gamma_{i_j}\theta_{i_1}\theta_{i_2}...\theta_{i_{j-2}})$$
$$.....$$
$$+p^{j-1} \sum_{1 \leq i_1 < ... < i_j \leq n} (\gamma_{i_1}\gamma_{i_2}...\gamma_{i_{j-1}}\theta_{i_j} + ... + \gamma_{i_2}...\gamma_{i_j}\theta_{i_1})$$
$$+p^j\gamma_{i_1}\gamma_{i_2}...\gamma_{i_j}$$

La divisibilité par p^{j-t} de $s_j(\theta)$ et de $p^j s_j(\gamma)$ étant manifeste, prouvons que chacun des autres termes dans cette dernière expression de $s_j(\theta')$ est aussi divisible par p^{j-t}. C'est-à-dire que pour pour tout k entre 1 et $j-1$,

$$p^{j-t} \text{ divise } s_j^{(k)}(\theta') = p^k \sum_{1 \leq i_1 < ... < i_j \leq n} (\gamma_{i_1}\gamma_{i_2}...\gamma_{i_k}\theta_{i_{k+1}}...\theta_{i_j} + ... + \gamma_{i_{j-k+1}}...\gamma_{i_j}\theta_{i_1}...\theta_{i_{j-k}})$$

Autrement dit, que p^{j-t-k} divise $\sum_{1\leq i_1<...<i_j\leq n}(\gamma_{i_1}\gamma_{i_2}...\gamma_{i_k}\theta_{i_{k+1}}...\theta_{i_j}+...+\gamma_{i_{j-k+1}}...\gamma_{i_j}\theta_{i_1}...\theta_{i_{j-k}})$
$=\sum_{1\leq i_1<...<i_j\leq n}(\sum_{1\leq r_1<...<r_k\leq j}(\prod_{1\leq t\leq k}\gamma_{i_{r_t}}\times\prod_{1\leq s\leq j,s\neq r_1,...,r_k}\theta_{i_s}))$
Or, d'après le théorème précédent, il existe une base $(\omega_{0,...,}\omega_{n-1})$ de l'anneau des entiers de K de la forme :
$\omega_0=1,\omega_1=\frac{a_0^{(1)}+\theta}{d_1},...,\omega_{n-1}=\frac{a_0^{(n-1)}+...+a_{n-2}^{(n-1)}\theta^{n-2}+\theta^{n-1}}{d_{n-1}}$
où les coefficients $a_i^{(k)}$ et les d_i sont dans $\mathbb{Z}$ et vérifient $d_1\mid d_2\mid ...\mid d_{n-1}$ et $\prod d_i=I(\theta)$.

Par conséquent on peut écrire chaque γ_i, et de manière unique, sous la forme
$\gamma_i=\frac{b_0+b_1\theta_i+...+b_{n-1}\theta_i^{n-1}}{d}=\sum_{0\leq t\leq n-1}\frac{b_t}{d}\theta_i^t$ où les b_i sont dans $\mathbb{Z}$, ou, pour faire plus simple, $\gamma_i=a_0+a_1\theta_i+...+a_{n-1}\theta_i^{n-1}$ où les coefficients $a_1,...,a_{n-1}$ sont dans $\mathbb{Q}$ et, p n'étant pas diviseur de $I(\theta)=\prod d_i$, de valuation p-adique positive ou nulle.

Par conséquent,
$s_j^{(k)}(\theta')=\sum_{1\leq i_1<...<i_j\leq n}(\sum_{1\leq r_1<...<r_k\leq j}(\prod_{1\leq t\leq k}(a_0+a_1\theta_{i_{r_t}}+...+a_{n-1}\theta_{i_{r_t}}^{n-1})\times\prod_{1\leq s\leq j,s\neq r_1,...,r_k}\theta_{i_s})$
Pour montrer la divisibilité par p^{j-t-k} de $s_j^{(k)}(\theta')$, il suffit de montrer la divisibilité par p^{j-t-k} de toute expression de la forme
$s_{(j;h_1,...,h_k)}(\theta)=\sum_{1\leq i_1<...<i_j\leq n}(\sum_{1\leq r_1<...<r_k\leq j}(\prod_{1\leq t\leq k}\theta_{i_{r_t}}^{h_{i_{r_t}}}\times\prod_{1\leq s\leq j,s\neq r_1,...,r_k}\theta_{i_s})$
(en effet, $S_k(\theta')$ est une combinaison linéaire des $s_{(j,h_1,...,h_k)}(\theta)$ lorsque $(h_1,...,h_k)$ parcourt l'ensemble de tous les k-uplets à valeurs dans l'ensemble $\{0,...,n-1\}$. Plus précisément, $S_k(\theta')$ peut s'écrire sous la forme suivante :
$S_k(\theta')=$
$\sum_{1\leq i_1<...<i_j\leq n}(\sum_{1\leq r_1<...<r_k\leq j}(\sum_{0\leq h_i\leq n-1}a_{(h_1,...,h_k)}(\sum_{\sigma\in S_{\{1,...,k\}}}\theta_{i_{r_{\sigma(1)}}}^{h_1}\theta_{i_{r_{\sigma(2)}}}^{h_2}...\theta_{i_{r_{\sigma(k)}}}^{h_k}))\times\prod_{1\leq s\leq j,s\neq r_1,...,r_k}\theta_{i_s}))$
où les coefficients $a_{(h_1,...,h_k)}$ sont dans $\mathbb{Q}$ et de valuation p-adique positive)

Il suffit alors de montrer que pour un uplet $(h_1,...,h_k)$ fixé quelconque, la somme :
$s_{(j,h_1,...,h_k)}(\theta)=\sum_{1\leq i_1<...<i_j\leq n}(\sum_{1\leq r_1<...<r_k\leq j}(\sum_{\sigma\in S_{\{1,...,k\}}}\theta_{i_{r_{\sigma(1)}}}^{h_1}\theta_{i_{r_{\sigma(2)}}}^{h_2}...\theta_{i_{r_{\sigma(k)}}}^{h_k})\times\prod_{1\leq s\leq j,s\neq r_1,...,r_k}\theta_{i_s}))$
est divisible par p^{j-t-k}.

Nous allons démontrer cela d'abord dans les cas $k=1$ et $k=2$ puis passer au cas général.

Cas $k=1$.

On a $s_{(j;h)}=\sum_{1\leq r_1<...<r_k\leq n}\theta_{i_1}^h\theta_{i_2}...\theta_{i_j}+\theta_{i_1}\theta_{i_2}^h...\theta_{i_j}+...+\theta_{i_1}\theta_{i_2}...\theta_{i_j}^h$.
Selon les valeurs de h, on obtient facilement les résultats suivants :

$$s_{(j;h)}(\theta) = \begin{cases} (n-j+1)s_{j-1}(\theta) & \text{si } h=0 \\ js_j(\theta) & \text{si } h=1 \\ (\sum_{r=1}^{n}\theta_r^{h-1})s_j(\theta) - s_{(j+1;h-1)}(\theta) & \text{si } h\geq 2 \end{cases}$$

En effet, le résultat est évident pour $h=0$ ou 1 et si $h\geq 2$, on a

$s_{(j;h)}(\theta) = \sum_{1\leq i_1<...<i_j\leq n}(\theta_{i_1}^{h-1}+\theta_{i_2}^{h-1}+...+\theta_{i_j}^{h-1})\theta_{i_1}...\theta_{i_j}$

$= \sum_{1\leq i_1<...<i_j\leq n}\left[(\sum_{r=1}^{n}\theta_r^{h-1}) - (\sum_{r\neq i_1,...,i_j}\theta_r^{h-1})\right]\theta_{i_1}...\theta_{i_j}$

$= (\sum_{r=1}^{n}\theta_r^{h-1})\sum_{1\leq i_1<...<i_j\leq n}\theta_{i_1}...\theta_{i_j}$

$- \sum_{1\leq i_1<...<i_j<i_{j+1}\leq n}(\theta_{i_1}^{h-1}\theta_{i_2}...\theta_{i_j}+\theta_{i_1}\theta_{i_2}^{h-1}\theta_{i_3}...\theta_{i_j}+...)$

$= (\sum_{r=1}^{n}\theta_r^{h-1})s_j(\theta) - s_{(j+1;h-1)}(\theta)$

De même, s'agissant de $s_{(j+1;h-1)}(\theta)$, on a d'après ce qui précède

$$s_{(j+1;h-1)}(\theta) = \begin{cases} (n-j)s_j(\theta) & \text{si } h=1 \\ (j+1)s_{j+1}(\theta) & \text{si } h=2 \\ (\sum_{r=1}^{n}\theta_r^{h-2})s_{j+1}(\theta) - s_{(j+2;h-2)}(\theta) & \text{si } h\geq 3 \end{cases}$$

On voit ainsi que, de proche en proche, on peut écrire $s_{(j;h)}(\theta)$ comme une combinaison linéaire des $s_i(\theta)$ avec $i\in\{j-1,...,n\}$ et $s_{(j;h)}(\theta)$ est donc divisible par p^{j-t-1}.

Cas $k=2$.

On a : $s_{(j;h_1,h_2)}(\theta) = \sum_{1\leq i_1<...<i_j\leq n}\theta_{i_1}^{h_1}\theta_{i_2}^{h_2}...\theta_{i_j} + \theta_{i_1}^{h_1}\theta_{i_2}\theta_{i_3}^{h_2}...\theta_{i_j}+...$

Il est clair que si h_1 ou h_2 est nul (ou les deux), on se ramène à $s_{(j-1;h)}(\theta)$ ou à $s_{j-2}(\theta)$.

De même, si $(h_1,h_2)=(h,1)$ (ou $(1,h)$), $s_{(j;h_1,h_2)}(\theta) = s_{(j;h,1)}(\theta)$ est un multiple de $s_{(j;h)}(\theta)$ et on applique alors ce qui précède.

Supposons donc que les h_i soient tous les deux ≥ 2. Dans ce cas, on peut écrire :

$s_{(j;h_1,h_2)}(\theta) = \sum_{1\leq i_1<...<i_j\leq n}(\theta_{i_1}^{h_1-1}\theta_{i_2}^{h_2-1}+\theta_{i_1}^{h_2-1}\theta_{i_2}^{h_1-1}+...)\theta_{i_1}...\theta_{i_j}$

$= \sum_{1\leq i_1<...<i_j\leq n}\Bigg[\sum_{r\neq s}\theta_r^{h_1-1}\theta_s^{h_2-1} - \sum_{r\in\{i_1,...,i_j\},s\notin\{i_1,...,i_j\}}\theta_r^{h_1-1}\theta_s^{h_2-1}$

$- \sum_{r\notin\{i_1,...,i_j\},s\in\{i_1,...,i_j\}}\theta_r^{h_1-1}\theta_s^{h_2-1} - \sum_{r\neq s,r,s\notin\{i_1,...,i_j\}}\theta_r^{h_1-1}\theta_s^{h_2-1}\theta_{i_1}...\theta_{i_j}\Bigg]$

$$= \sum_{r\neq s} \theta_r^{h_1-1}\theta_s^{h_2-1} \sum_{1\leq i_1<...<i_j\leq n} \theta_{i_1}...\theta_{i_j}$$
$$- \sum_{1\leq i_1<...<i_j<i_{j+1}\leq n} (\theta_{i_1}^{h_1}\theta_{i_2}^{h_2-1}...\theta_{i_j}\theta_{i_{j+1}} + ...)$$
$$- \sum_{1\leq i_1<...<i_j<i_{j+1}\leq n} (\theta_{i_1}^{h_1-1}\theta_{i_2}^{h_2}...\theta_{i_j}\theta_{i_{j+1}} + ...)$$
$$- \sum_{1\leq i_1<...<i_j<i_{j+1}<i_{j+2}\leq n} (\theta_{i_1}^{h_1-1}\theta_{i_2}^{h_2-1}...\theta_{i_{j+2}} + ...)$$
$$= (\sum_{r\neq s,r,s\in\{1,...,n\}}^{n} \theta_r^{h_1-1}\theta_s^{h_2-1})s_j(\theta) - s_{(j+1;h_1,h_2-1)}(\theta) - s_{(j+1;h_1-1,h_2)}(\theta) - s_{(j+2;h_1-1,h_2-1)}(\theta).$$

Le même raisonnement que pour le cas $k = 1$ permet d'affirmer que $s_{(j;h_1,h_2)}$ est une combinaison linéaire (à coefficients dans $\mathbb{Z}$) des $s_i(\theta)$ avec $i \geq j-2$ et est par conséquent divisible par p^{j-t-2}.

Cas k quelconque entre 1 et $j-1$.

On a $s_{(j;h_1,...,h_k)}(\theta) = \sum_{1\leq i_1<...<i_j\leq n} \theta_{i_1}^{h_1}\theta_{i_2}^{h_2}...\theta_{i_k}^{h_k}\theta_{i_{k+1}}...\theta_{i_j} + ...$

On a les propriétés suivantes :

(a) $s_{(j;h_1,...,h_k)}(\theta) = s_{(j;h_{\sigma(1)},...,h_{\sigma(k)})}(\theta)$ pour toute permutation σ de l'ensemble $\{1,...,k\}$

(b) si $h_k = 0$, $s_{(j;h_1,...,h_k)}(\theta)$ est un multiple (par un entier rationnel) de $s_{(j-1;h_1,...,h_{k-1})}(\theta)$

(c) si $h_k = 1$, $s_{(j;h_1,...,h_k)}(\theta)$ est un multiple de $s_{(j;h_1,...,h_{k-1})}(\theta)$.

A partir de là, on peut supposer tous les $h_i \geq 2$. On a alors

$s_{(j;h_1,...,h_k)}(\theta) = \sum_{1\leq i_1<...<i_j\leq n} (\theta_{i_1}^{h_1-1}...\theta_{i_k}^{h_k-1} + ...)\theta_{i_1}...\theta_{i_j}$

Notons $A_k = \theta_{i_1}^{h_1-1}...\theta_{i_k}^{h_k-1} + ... = \sum_{\sigma\in S_k} \theta_{i_{\sigma(1)}}^{h_1-1}...\theta_{i_{\sigma(k)}}^{h_k-1}$

On a $A_k = \sum_{\{r_1,...,r_k\}\subset\{i_1,...,i_j\}} \theta_{r_1}^{h_1-1}...\theta_{r_k}^{h_k-1} = \sum_{\text{les } r_i\in\{1,...,n\}} \theta_{r_1}^{h_1-1}...\theta_{r_k}^{h_k-1}$

$- \sum_{\text{les } r_i\in\{i_1,...,i_j\} \text{ sauf } r_k} \theta_{r_1}^{h_1-1}...\theta_{r_k}^{h_k-1} - \sum_{\text{les } r_i\in\{i_1,...,i_j\} \text{ sauf } r_{k-1}} \theta_{r_1}^{h_1-1}...\theta_{r_k}^{h_k-1}$

...

$- \sum_{\text{les } r_i\in\{i_1,...,i_j\} \text{ sauf } r_1} \theta_{r_1}^{h_1-1}...\theta_{r_k}^{h_k-1}$

$- \sum_{\text{les } r_i\in\{i_1,...,i_j\} \text{ sauf } r_k \text{ et } r_{k-1}} \theta_{r_1}^{h_1-1}...\theta_{r_k}^{h_k-1}... - \sum_{\text{les } r_i\in\{i_1,...,i_j\} \text{ sauf } r_1 \text{ et } r_2} \theta_{r_1}^{h_1-1}...\theta_{r_k}^{h_k-1}$

...

...

$- \sum_{\text{les } r_i\notin\{i_1,...,i_j\}} \theta_{r_1}^{h_1-1}...\theta_{r_k}^{h_k-1}$

On en déduit :

$s_{(j;h_1,...,h_k)}(\theta) = (\sum_{\text{les } r_i\in\{1,...,n\}} \theta_{r_1}^{h_1-1}...\theta_{r_k}^{h_k-1})s_j(\theta)$

$-s_{(j+1;h_1,...,h_{k-1})}(\theta) - ... - s_{(j;h_1-1,...,h_k)}(\theta)$

$-s_{(j+2;h_1,...,h_{k-2},h_{k-1}-1,h_k-1)}(\theta) - ... - s_{(j;h_1-1,h_2-1,h_3,...,h_k)}(\theta)$

...

$-s_{(j+k;h_1-1,h_2-1,...,h_k-1)}(\theta)$.

Le même raisonnement que pour les cas $k = 1$ et $k = 2$ permet d'affirmer que quel que soit le uplet $(h_1, ..., h_k)$, on peut écrire $s_{(j;h_1,...,h_k)}(\theta)$ comme une combinaison linéaire à coefficients dans $\mathbb{Z}$ des $s_i(\theta)$ avec $i \geq j - k$. Ce qui assure sa divisibilité par p^{j-t-k}. ■

Chapitre 3

Le polynôme minimal de congruence modulo un nombre premier

3.1 Polynôme minimal de congruence

Soit K un corps de nombres de degré n sur $\mathbb{Q}$, A son anneau des entiers, θ un élément de A et p un nombre premier.

On note :

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

Il est facile de voir que E_θ est un idéal non nul de l'anneau principal $\mathbb{F}_p\left[x\right]$. Soit $g_0(x)$ l'unique polynôme unitaire engendrant E_θ.

On peut à présent donner la définition suivante.

Définition 3.1.1 *On appelle polynôme minimal de congruence modulo p de θ un polynôme $M_\theta(p,x) \in \mathbb{Z}\left[x\right]$ tel que :*

$$\begin{cases} M_\theta(p,x) = g_0(x) \pmod{p} \\ M_\theta(p,x) \text{ est unitaire} \end{cases}$$

Remarque 3.1.1 *Il n'existe pas forcément de polynôme irréductible engendrant l'idéal E_θ. En effet, l'anneau quotient A/pA n'est pas intègre sauf si p est inerte dans A, autrement dit, si pA est un idéal premier de A, donc aussi maximal et auquel cas cet anneau serait carrément un corps.*

Remarque 3.1.2 *$M_\theta(p,x)$ est de même degré que $g_0(x)$. Il est unique modulo p. C'est un diviseur modulo p du polynôme minimal $Irr(\theta,\mathbb{Q})$ de θ sur $\mathbb{Q}$.*

3.2 Polynôme minimal de congruence et nombres premiers diviseurs d'indices

Le degré de $M_\theta(p,x)$ a un lien avec le fait que le nombre premier p divise ou pas l'indice de θ comme le montre le résultat suivant.

Lemme 3.2.1 *Soit un corps de nombres K de degré n sur $\mathbb{Q}$, un nombre premier p et un entier quelconque θ de K. Alors on a l'équivalence :*

$$p \text{ divise } I(\theta) \Leftrightarrow \deg M_\theta(p,x) \leq n-1$$

Démonstration. Soient $(\omega_1,...,\omega_n)$ une base (ordonnée) des entiers de K et θ un entier quelconque.
Supposons que l'écriture des éléments $1,\theta,...,\theta^{n-1}$ dans cette base soit donnée par :

$$\theta^i = a_{1,i}\omega_1 + a_{2,i}\omega_2 + ... + a_{n,i}\omega_n$$

où $a_{j,i} \in \mathbb{Z}$ pour tout $(i,j) \in \{0,...,n-1\} \times \{1,...,n\}$.
Considérons alors la matrice P suivante :

$$P = \begin{pmatrix} a_{1,0} & a_{1,1} & ... & a_{1,n-1} \\ . & . & ... & . \\ . & . & ... & . \\ a_{n,0} & a_{n,1} & ... & a_{n,n-1} \end{pmatrix}.$$

P est en fait la matrice dont la première colonne est l'écriture dans la base $(\omega_1,...,\omega_n)$ de l'entier $1=\theta^0$, la deuxième colonne l'écriture dans la base $(\omega_1,...,\omega_n)$ de l'entier $\theta=\theta^1$,...etc.
Dans ce cas, on sait que l'indice de θ est égal à $|\det P|$.
Par conséquent, dire que le nombre premier p divise $I(\theta)$ équivaut à dire qu'il divise $\det(P)$.

Or, $p \mid \det P$ équivaut à la nullité modulo p de $\det(P)$, donc au fait que les n colonnes de la matrice P soient linéairement dépendantes modulo p. Ou encore à l'existence d'entiers $g_1, ..., g_n \in \mathbb{Z}$, pas tous multiples de p, tels que :

$$g_1 \begin{pmatrix} a_{1,0} \\ . \\ . \\ a_{n,0} \end{pmatrix} + g_2 \begin{pmatrix} a_{1,1} \\ . \\ . \\ a_{n,1} \end{pmatrix} + ... + g_n \begin{pmatrix} a_{1,n-1} \\ . \\ . \\ a_{n,n-1} \end{pmatrix} \equiv \begin{pmatrix} 0 \\ . \\ . \\ 0 \end{pmatrix} (\mathrm{mod}\, p).$$

Ce qui signifie que ces g_i vérifient : $g_1 + g_2\theta + ... + g_n\theta^{n-1} \equiv 0 \pmod{p}$ dans A ou que θ vérifie une équation de dépendance intégrale modulo p de degré $\leq n-1$. Par conséquent, p divise $I(\theta)$ si et seulement si $\deg M_\theta(p, x) \leq n-1$. ■

Etant donnés un corps de nombres K d'anneau des entiers A, un élément θ de A et un nombre premier p, le résultat suivant, dû à Dedekind, établit un lien entre la décomposition modulo p du polynôme minimal de θ en produit de facteurs unitaires irréductibles et celle de p dans K (en produit d'idéaux premiers de A), mais à la condition que p ne divise pas l'indice de θ.

Théorème 3.2.1 *Soient K un corps de nombres, A son anneau des entiers, θ un élément de A et p un nombre premier.*
On suppose que la décomposition de $F(x) = Irr(\theta, \mathbb{Q})$ en facteurs unitaires irréductibles modulo p est donnée par :

$$F(x) \equiv F_1^{e_1}(x)...F_r^{e_r}(x) \pmod{p}$$

où pour tout $i = 1, ..., r$, $e_i \geq 1$.
Si p ne divise pas l'indice $I(\theta)$ de θ, alors la décomposition de p en produit d'idéaux premiers de A est donnée par :

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

où pour tout $i = 1, ..., r$, $\mathcal{P}_i$ est l'idéal premier de A engendré par p et $F_i(\theta)$.

Ayad et Kihel [6] établissent le résultat suivant qui lie la décomposition du polynôme caractéristique $F(x)$ de θ à celle du nombre premier p dans le cas général où p peut être, éventuellement, un diviseur de l'indice de θ. Ils généralisent ainsi celui de Dedekind. De plus, par ce résultat, ils précisent l'écriture du polynôme de congruence $M_\theta(p,x)$ en fonction des facteurs unitaires irréductibles qui apparaissent dans la décomposition de $F(x)$.

Théorème 3.2.2 *Soit K un corps de nombres, θ un élément quelconque de son anneau des entiers A, $F(x)$ le polynôme caractéristique de θ sur $\mathbb{Q}$ et p un nombre premier.*
On suppose que la décomposition de p dans K et celle de $F(x)$ en produit de facteurs unitaires et irréductibles modulo p sont données respectivement par :

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

$$F(x) \equiv F_1(x)^{h_1}...F_s(x)^{h_s} (\mathrm{mod}\, p).$$

où les $e_i, i = 1,...,r$ et les $h_j, j = 1,...,s$ sont ≥ 1. Alors :
(1) Pour tout $j = 1,...,s$, il existe un idéal $\mathcal{P}$ parmi les $\mathcal{P}_i$ tel que $F_j(\theta) \equiv 0 \pmod{\mathcal{P}}$. De plus, $\deg(F_j(x))$ divise le degré résiduel $f_\mathcal{P}$ de $\mathcal{P}$.
(2) Pour tout $j \in \{1,...,s\}$, si $C_j = \{\mathcal{P} \in \{\mathcal{P}_1,...,\mathcal{P}_r\}, F_j(\theta) \equiv 0 \pmod{\mathcal{P}}\}$, alors :

$$M_\theta(p,x) \equiv \prod_{j=1}^{s} F_j(x)^{\lambda_j} (\mathrm{mod}\, p).$$

où pour tout j, on a : $\lambda_j = \max_{\mathcal{P}\in C_j} \lceil e_\mathcal{P}/\nu_\mathcal{P}(F_j(\theta))\rceil$.
De plus, on a $s \leq r, h_j = \sum_{\mathcal{P}\in C_j} e_\mathcal{P} \dfrac{f_j}{\deg(F_j(x))}$ et $pA + F_j(\theta)A = \prod_{\mathcal{P}\in C_j} \mathcal{P}^{\inf(\nu_\mathcal{P}(F_j(\theta)),\nu_\mathcal{P}(p))}$.

Le résultat suivant (voir [4]) donne des conditions nécessaires et suffisantes pour qu'un nombre premier p divise l'indice d'un entier donné d'un corps de nombres.

Théorème 3.2.3 *Soient K un corps de nombres, A son anneau des entiers, θ un élément de A et p un nombre premier.*
On suppose que la décomposition de p dans A est donnée par

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

où le degré résiduel de $\mathcal{P}_i$ est f_i pour $i = 1, ..., r$.

Alors $p \mid I(\theta)$ si et seulement si l'une des conditions suivantes est vérifiée :

(i) Il existe $i \in \{1, ..., r\}$ tel que $e_i \geq 2$ et si $G(x) = Irr(\theta + \mathcal{P}_i, \mathbb{F}_p)$, alors $G(x)$ vérifie $G(\theta) \equiv 0 (\text{mod } \mathcal{P}_i^2)$.

(ii) Il existe $i \in \{1, ..., r\}$ tel que $f_i \geq 2$ et $\deg Irr(\theta + \mathcal{P}_i, \mathbb{F}_p) < f_i$.

(iii) Il existe $i, j \in \{1, ..., r\}, i \neq j$, tels que $Irr(\theta + \mathcal{P}_i, \mathbb{F}_p) = Irr(\theta + \mathcal{P}_j, \mathbb{F}_p)$.

Démonstration. On suppose que p divise $I(\theta)$. On considère la factorisation de $M_\theta(p, x)$ modulo p que l'on suppose donnée par :

$$M_\theta(p, x) \equiv F_1(x)^{h_1} ... F_s(x)^{h_s} (\text{mod } p)$$

Puisque $p \mid I(\theta)$, d'après le lemme 3.2.1, $\deg M_\theta(p, x) \leq n - 1$. Supposons que (ii) et (iii) n'aient pas lieu, alors $s = r$ et pour tout $j \in \{1, ..., r\}$, il existe un unique $i = i(j)$ tel que $F(\theta) \equiv 0 (\text{mod } \mathcal{P}_j)$. Mais, étant donné que $\deg F_{i(j)} = f_{\mathcal{P}_j}$ et que $\deg M_\theta(p, x) \leq n - 1$, il existe j_0 tel que $h_{i(j_0)} < e_{j_0}$. Supposons que $\mathcal{P}_{j_0} \parallel F_{i(j_0)}(\theta)$, alors $\mathcal{P}_{j_0}^{h_{i(j_0)}} \parallel F_{i(j_0)}^{h_{i(j_0)}}(\theta)$ et qui est en contradiction avec le fait que $\mathcal{P}_{j_0}^{e_{j_0}} \mid M_\theta(p, x)$. Par conséquent, $\mathcal{P}_{j_0}^2 \mid F_{i(j_0)}(\theta)$ et (i) est vraie.

Démontrons la réciproque. Supposons que (ii) soit vraie et soit $F(x) = \prod_{j=1}^{r} F_j(x)^{e_j}$ où pour tout $j \in \{1, ..., r\}$, $F_j(x)$ est un relèvement unitaire dans $\mathbb{Z}[x]$ de $Irr(\theta + \mathcal{P}_j, \mathbb{F}_p)$. Puisque $\deg Irr(\theta + \mathcal{P}_i, \mathbb{F}_p) < f_i$ et $F(\theta) \equiv 0 (\text{mod } p)$, alors $\deg M_\theta(p, x) \leq n - 1$. Donc d'après le lemme 3.2.1, $p \mid I(\theta)$.

Supposons que (iii) soit vraie. Soit $F(x) = (F_i(x))^{\max(e_i, e_j)} \prod_{k \neq i,j} F_k(x)^{e_k}$, où $F_i(x)$ est un relèvement unitaire de $Irr(\theta + \mathcal{P}_i, \mathbb{F}_p)$ et où pour tout $k \neq i, j$, $F_k(x)$ est un relèvement unitaire de $Irr(\theta + \mathcal{P}_k, \mathbb{F}_p)$ dans $\mathbb{Z}[x]$. On a clairement $F(\theta) \equiv 0 \ (\text{mod } p)$ et $\deg F(x) \leq n - 1$. Donc $\deg M_\theta(p, x) \leq n - 1$. D'après le lemme 3.2.1, $p \mid I(\theta)$.

Supposons à présent que (i) soit vraie. Soit $F(x) = (F_i(x))^{(e_i + \epsilon)/2} \prod_{j \neq i} F_j(x)^{e_j}$ où $\epsilon = 0$ si e_i est pair et 1 sinon et où, comme précédemment, pour tout k, $F_k(x)$ est un relèvement unitaire de $Irr(\theta + \mathcal{P}_k, \mathbb{F}_p)$ dans $\mathbb{Z}[x]$. Alors on a, là encore, $F(\theta) \equiv 0 \ (\text{mod } p)$ et $\deg F(x) \leq n - 1$. D'où $\deg M_\theta(p, x) \leq n - 1$. Donc $p \mid I(\theta)$. ■

Le résultat suivant (voir [16]) offre une manière pratique de savoir si un nombre premier p divise ou pas l'indice d'un entier donné d'un corps de nombres sans passer par la

décomposition de p dans ce corps.

Théorème 3.2.4 *Soient K un corps de nombres, A son anneau des entiers, θ un entier primitif de K dont le polynôme minimal est $F(x)$ et p un nombre premier.*
On suppose que la factorisation en facteurs unitaires irréductibles modulo p de $F(x)$ est donnée par :

$$F(x) = \prod_{i=1}^{s} F_i(x)^{h_i} + pG(x)$$

où $G(x)$ est un polynôme de $\mathbb{Z}[x]$.
Alors, $p \mid I(\theta)$ si et seulement s'il existe un $i \in \{1, ..., s\}$ tel que $h_i \geq 2$ et que $F_i(x)$ divise $G(x)$ modulo p.

Exemple 3.2.1 *Soit le polynôme $F(x) = x^3 - x^2 - 2x - 8$.*
Il est irréductible sur $\mathbb{Q}$. Soit θ une racine quelconque de $F(x)$ dans $\mathbb{C}$. On sait depuis Dedekind que 2 divise $I(\theta)$. Vérifions que le théorème ci-dessus permet de retrouver ce résultat. En effet,

$$F(x) = x^2(x-1) + 2(-x-4)$$

et on voit bien que le facteur irréductible x est multiple et qu'il divise le polynôme $-x-4$ dans $\mathbb{F}_2[x]$. Donc 2 divise $I(\theta)$.

Exemple 3.2.2 *Soit K le corps cubique engendré sur $\mathbb{Q}$ par une racine θ (quelconque) du polynôme irréductible $F(x) = x^3 + x^2 + 2x + 4$.*
On a :

$$F(x) = x^2(x+1) + 2(x+2)$$

Ici, $s = 2, F_1(x) = x, h_1 = 2, F_2(x) = x + 1, h_2 = 1$ et $G(x) = x + 2$. Comme $F_1(x)$ divise $G(x)$ modulo 2, on en déduit que 2 divise $I(\theta)$.

Exemple 3.2.3 *Soit le corps de nombres biquadratique* $K = \mathbb{Q}(\sqrt{7}, \sqrt{10})$. *On sait (voir [22]) qu'il n'existe pas d'entier* θ *dans* K *tel que l'anneau* A *de* K *vérifie* $A = \mathbb{Z}[\theta]$. *Soit* $\theta = \sqrt{7} + \sqrt{10}$. θ *est un entier primitif de* K *dont le polynôme minimal est* $F(x) = x^4 - 34x^2 + 9$. *On va montrer, grâce au théorème ci-dessus, que* 2 *et* 3 *divisent* $I(\theta)$ *et que* 5 *ne le divise pas. On a :*

$$F(x) = (x+1)^4 + 2(-2x^3 - 20x^2 - 2x + 4).$$

Comme le facteur multiple $x + 1$ *divise le polynôme* $-2x^3 - 20x^2 - 2x + 4$ *modulo* 2, 2 *est donc diviseur de* $I(\theta)$.
Pour 3, *la factorisation modulo* 3 *de* $F(x)$ *donne :*

$$F(x) = x^2(x-1)(x+1) + 3(-11x^2 + 3).$$

Là aussi, le facteur multiple x *est diviseur de* $-11x^2 + 3$ *modulo* 3. *Par conséquent,* 3 *est diviseur de* $I(\sqrt{7} + \sqrt{10})$.
Par contre, pour le nombre premier 5, *on a :*

$$F(x) = (x^2 - 2)^2 + 5(-6x^2 + 1).$$

Le polynôme unitaire $x^2 - 2$ *est irréductible dans* $\mathbb{F}_5[x]$ *et est en même temps l'unique facteur multiple modulo* 5 *de* $F(x)$. *Comme il ne divise pas* $-6x^2 + 1$ *dans* $\mathbb{F}_5[x]$, *le nombre premier* 5 *n'est donc pas un diviseur de* $I(\sqrt{7} + \sqrt{10})$.

Chapitre 4

Facteurs communs d'indices

4.1 Introduction

Définition 4.1.1 *Soit K un corps de nombres. Un nombre premier p est dit facteur commun d'indices, ou f.c.i. en abrégé, dans K si p est un diviseur de $I(\theta)$ pour tout entier θ de K.*

Remarque 4.1.1 *Etant donné un corps de nombres quadratique K, il est toujours possible de trouver un entier θ de K qui engendre la $\mathbb{Z}$-algèbre A des entiers de K, c'est-à-dire tel que $A = \mathbb{Z}[\theta]$. Plus précisément, si $K = \mathbb{Q}\left(\sqrt{d}\right)$ où d est un entier (forcément autre que 1) sans facteur carré, alors si $d \equiv 2, 3 \pmod 4$, $A = \mathbb{Z}\left[\sqrt{d}\right]$ et si $d \equiv 1 \pmod 4$, $A = \mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right]$. Il ne peut donc exister de nombre premier facteur commun d'indices pour un corps quadratique. Par contre, pour un corps de nombres K de degré ≥ 3 sur $\mathbb{Q}$, l'existence d'un entier θ de K engendrant l'anneau des entiers n'est plus assurée. Par exemple, si K est le corps de nombres biquadratique $\mathbb{Q}(\sqrt{7}, \sqrt{10})$, on montre que $\left\{1, \sqrt{7}, \sqrt{10}, \dfrac{\sqrt{7}+\sqrt{70}}{2}\right\}$ est une base des entiers de K et pour tout θ dans l'anneau A des entiers de K, $\mathbb{Z}[\theta]$ est strictement inclus dans A [22].*

C'est Dedekind qui fut le premier à exhiber un corps de nombres admettant un facteur commun d'indices en montrant que si K est un corps engendré sur $\mathbb{Q}$ par une racine quelconque du polynôme irréductible $x^3 - x^2 - 2x - 8$, alors 2 est f.c.i. dans K [16].

Soit K un corps de nombres. Nous avons vu, à travers le lemme 3.2.1 que pour qu'un nombre premier p divise l'indice d'un entier donné de K, il est nécessaire et suffisant que le polynôme minimal de congruence modulo p de celui-ci soit de degré strictement plus petit que le degré de K sur $\mathbb{Q}$.

Comme conséquence de ce lemme, on a le résultat suivant.

Corollaire 4.1.1 *Soit K un corps de nombres. Pour qu'un nombre premier p soit f.c.i. dans K il est nécessaire et suffisant que pour tout entier θ de K, on ait :* $\deg M_\theta(p,x) < [K:\mathbb{Q}]$.

Cependant, vérifier si cette condition est satisfaite ou pas n'est pas toujours chose aisée. Le résultat suivant, dû à Zylinski [32], propose une condition nécessaire simple pour qu'un nombre premier soit un f.c.i. dans un corps de nombres. Celle-ci repose uniquement sur le degré du corps de nombres.

Théorème 4.1.1 *Pour qu'un nombre premier soit f.c.i. dans un corps de nombres K, il est nécessaire qu'il soit strictement plus petit que le degré de K.*

Ainsi, et comme on l'a vu dans la remarque ci-dessus, il n'y a pas de f.c.i. pour un corps de nombres quadratique. Seul le nombre premier 2 est susceptible d'être f.c.i. pour un corps de nombres cubique. De même, seuls les deux nombres premiers 2 et 3 peuvent l'être pour un corps de nombres de degré quatre ou cinq,...etc.

4.2 Une condition nécessaire et suffisante pour être facteur commun d'indices

Dans cette section, nous rappelons un résultat dû à Hensel (voir [16] ou [17] et [18]) et qui donne une condition nécessaire et suffisante pour qu'un nombre premier soit un facteur commun d'indices dans un corps de nombres donné. Il repose entièrement sur la décomposition de ce nombre premier en produit d'idéaux et sur le nombre de polynômes unitaires et irréductibles de degré donné à coefficients dans un corps fini.

4.2.1 Le nombre de polynômes unitaires et irréductibles à coefficients dans un corps fini de degré donné

Soit p un nombre premier. Il existe une formule, utilisant la fonction de Mobiüs, qui donne le nombre de tous les polynômes unitaires et irréductibles de degré donné à coefficients dans le corps fini $\mathbb{F}_p$.

Rappelons que la fonction de Mobiüs est la fonction μ définie sur l'ensemble $\mathbb{N}$ des entiers naturels par $\mu(n) = 0$ si n est divisible par le carré d'un nombre premier, 1 si n est le produit d'un nombre pair de nombres premiers distincts et -1 si n est le produit d'un nombre impair de nombres premiers distincts.

On a alors le résultat suivant.

Proposition 4.2.1 *Soient n un entier naturel non nul et p un nombre premier. Alors le nombre $N_p(n)$ des polynômes unitaires et irréductibles de degré n de $\mathbb{F}_p[x]$ vérifie :*

$$N_p(n) = \frac{1}{n}\sum_{d|n}\mu(d)p^{\frac{n}{d}}$$

Démonstration. Voir [16] ■

Ainsi, si n s'écrit : $n = l_1^{h_1}l_2^{h_2}...l_s^{h_s}$, où les l_i, $i = 1, ..., s$, sont des nombres premiers distincts deux à deux et les h_i des entiers ≥ 1, alors, compte tenu de la définition de la fonction μ, on a :

$nN_p(n) = \sum_{d|n}\mu(d)p^{\frac{n}{d}} = p^n - (p^{\frac{n}{l_1}} + p^{\frac{n}{l_2}} + ... + p^{\frac{n}{l_s}})$

$+(p^{\frac{n}{l_1l_2}} + p^{\frac{n}{l_1l_3}} + ... + p^{\frac{n}{l_{s-1}l_s}}) - ...$

....

$+(-1)^{s-1}(p^{\frac{n}{l_1...l_{s-1}}} + p^{\frac{n}{l_1...l_{s-2}l_s}} + ... + p^{\frac{n}{l_2...l_s}}) + (-1)^s p^{\frac{n}{l_1...l_s}}$

Par conséquent, en utilisant le symbôle "somme", on peut écrire :

$nN_p(n) = p^n - \sum_{1\leq i_1\leq s} p^{\frac{n}{l_{i_1}}} + \sum_{1\leq i_1<i_2\leq s} p^{\frac{n}{l_{i_1}l_{i_2}}} - ...$

$+(-1)^{s-1}\sum_{1\leq i_1<i_2<...<i_{s-1}\leq s} p^{\frac{n}{l_{i_1}...l_{i_{s-1}}}} + (-1)^s p^{\frac{n}{l_1...l_s}}.$

Finalement,

$$N_p(n) = \frac{1}{n}(p^n - \sum_{1\leq i_1\leq s} p^{\frac{n}{l_{i_1}}} + \sum_{1\leq i_1<i_2\leq s} p^{\frac{n}{l_{i_1}l_{i_2}}} - ... + (-1)^s p^{\frac{n}{l_1...l_s}}).$$

En particulier, si $n = l^h$ où l est un nombre premier et h un entier ≥ 1, alors :

$N_p(n) = N_p(l^h) = \frac{1}{l^h}(p^{l^h} - p^{l^{h-1}})$.

Remarque 4.2.1 *Pour tout entier naturel non nul n et tout nombre premier p, $nN_p(n)$ est un multiple de p, non nul.*

4.2.2 Le théorème de Hensel

Théorème 4.2.1 *Soient K un corps de nombres, A son anneau des entiers et p un nombre premier. Alors p est f.c.i. pour le corps K si et seulement s'il existe un entier naturel non nul f tel que le nombre d'idéaux premiers de A au dessus de p de degré f soit strictement plus grand que $N_p(f)$.*
Autrement dit, soit $pA = \mathcal{P}_1^{e_1}...\mathcal{P}_r^{e_r}$ la décomposition de l'idéal pA en produit d'idéaux premiers de A telle que chaque $\mathcal{P}_k$ soit de degré résiduel f_k. Alors p est un f.c.i. dans K si et seulement si pour l'un des f_k, le nombre t_k des idéaux $\mathcal{P}_i$ ayant pour degré résiduel f_k vérifie $t_k > N_p(f)$.

Remarque 4.2.2 *Le théorème de Hensel implique celui de Zylinski. En effet, si un nombre premier p pouvait être f.c.i. dans un corps de degré $n \leq p$, d'après le théorème de Hensel, il existerait un entier $f \geq 1$ tel que le nombre t des idéaux premiers au dessus de p vérifie $t > N_p(f)$. On aurait alors $p \geq n \geq tf > fNp(f)$. Donc au final, $p > fNp(f)$. Or, $fN_p(f)$ est un entier non nul et un multiple de p. Ce qui contredit cette dernière inégalité.*

4.3 Facteur commun d'indice et petit indice

Rappelons le résultat de MacCluer selon lequel, si K est un corps de nombres et p un nombre premier, alors p est diviseur de $i(K)$ si et seulement si le nombre d'idéaux premiers (de l'anneau des entiers de K) au-dessus de p est supérieur ou égal à p.

Ayad et Kihel [5] établissent le résultat suivant et qui relie les deux notions de petit et de grand indices.

Théorème 4.3.1 *Soient K un corps de nombres et p un nombre premier.*
Si p est un facteur commun d'indices dans K alors p divise $i(K)$.

Chapitre 5

La fonction μ_K

Etant donné un corps de nombres K, nous définissons dans [4] une nouvelle fonction liée à K, notée μ_K, définie sur l'ensemble des nombres premiers et à valeurs dans l'ensemble des entiers naturels. Elle permet de calculer pour un nombre premier p donné le nombre d'entiers de K incongrus modulo p, dont l'indice est divisible par p. Ce calcul repose sur le type de décomposition du nombre premier p dans K, plus précisément sur les indices de ramification et les degrés résiduels des idéaux premiers de K (en réalité de son anneau des entiers) au dessus de p. Réciproquement et dans certains cas, la connaissance préalable de la valeur de $\mu_K(p)$ peut renseigner, comme on va le voir au cours de ce chapitre, sur le type de décomposition dans K de ce nombre premier.

5.1 Le nombre de $\overline{\theta} \in A/pA$ tels que $p \mid I(\theta)$

Lemme 5.1.1 *Soient α et β deux éléments de A tels que $\alpha \equiv \beta \pmod{p}$. Si $p \mid I(\alpha)$, alors $p \mid I(\beta)$.*

Démonstration. On pose $\beta = \alpha + p\gamma$ où $\gamma \in A$. Soit $M(x) = M_\alpha(p, x)$ le polynôme minimal de congruence modulo p de α. Alors $M(\beta) = M(\alpha + p\gamma) \equiv M(\alpha) \pmod{p}$, donc $p \mid I(\beta)$ d'après le lemme 3.2.1. ■

Soient K un corps de nombres de degré n sur $\mathbb{Q}$ et A son anneau des entiers. Il est clair que l'ensemble des $\theta \in A$ tels que p divise $I(\theta)$ est infini. Mais, compte tenu du lemme ci-dessus, deux éléments quelconques d'une même classe modulo p sont d'indices ou bien tous les deux divisibles par p ou bien tous les deux non divisibles par p. Il est par conséquent

plus judicieux de raisonner par rapport aux classes, c'est-à-dire de considérer plutôt l'anneau quotient A/pA, qui est évidemment fini.
Nous définissons alors une fonction liée à K et notée μ_K sur l'ensemble des nombres premiers et à valeurs dans l'ensemble des entiers naturels $\mathbb{N}$ en posant :

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

On sait, A/pA est un espace vectoriel de dimension n sur $\mathbb{F}_p$. Par conséquent, pour un nombre premier donné p quelconque, on a $\mu_K(p) \leq p^n$ et l'égalité n'a lieu que si et seulement si p est un facteur commun d'indices dans K.

Le prochain théorème précise la valeur que prend cette fonction en un idéal premier p selon le type de décomposition de celui-ci dans K. Mais avant cela, nous avons besoin du lemme suivant.

Lemme 5.1.2 *Soient $\mathcal{P}$ un idéal premier de A au dessus de p de degré résiduel d et $G(x) \in \mathbb{Z}[x]$ un polynôme unitaire irréductible sur $\mathbb{F}_p$ de degré d. Soient $\rho \in A$ tel que $G(\rho) \equiv 0 \pmod{\mathcal{P}}$ et e un entier ≥ 2. Alors, le nombre des éléments $\theta \in A$ incongrus modulo $\mathcal{P}^e$ et vérifiant :*

$$\theta \equiv \rho \pmod{\mathcal{P}} \text{ et } G(\theta) \notin \mathcal{P}^2 \tag{5.1}$$

est égal à $(p^d - 1)p^{d(e-2)}$.

Démonstration. Si $G(\rho) \in \mathcal{P}^2$, soit $\mu \in \mathcal{P}\backslash\mathcal{P}^2$ et $\tau = \rho + \mu$. Alors $\tau \equiv \rho \pmod{\mathcal{P}}$ et on a :

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

Puisque $G'(\rho) \notin \mathcal{P}$, car sinon ρ annulerait modulo P un polynôme non nul de degré strictement plus petit que d, alors $G(\tau) \notin \mathcal{P}^2$. Par conséquent, on peut supposer, sans perdre la généralité, que $G(\rho) \notin \mathcal{P}^2$.
a) Dans un premier temps, on va montrer que le nombre des éléments $\theta \in A$, incongrus modulo $\mathcal{P}^2$ et satisfaisant les conditions (5.1) est égal à $p^d - 1$. En fait, le nombre des éléments

θ incongrus modulo $\mathcal{P}^2$ et vérifiant $\theta \equiv \rho \pmod{\mathcal{P}}$ est égal à $\mid \mathcal{P}/\mathcal{P}^2 \mid = p^d$. On va montrer que :

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

On suppose que $A_0(\rho) + A_1(\rho)G(\rho) \equiv B_0(\rho) + B_1(\rho)G(\rho) \pmod{\mathcal{P}^2}$. Alors, $A_0(\rho) - B_0(\rho) + (A_1(\rho) - B_1(\rho))G(\rho) \equiv 0 \pmod{\mathcal{P}^2}$, d'où $A_0(\rho) - B_0(\rho) \equiv 0 \pmod{\mathcal{P}}$ et donc $A_0(x) = B_0(x)$. On en déduit que $A_1(\rho) - B_1(\rho) \equiv 0 \pmod{\mathcal{P}}$, d'où $A_1(x) = B_1(x)$. Le nombre des éléments ayant la forme ci-dessus étant p^{2d}, alors l'égalité des deux ensembles est établie.
Soit $\theta \in A/P^2, \theta = A_0(\rho) + A_1(\rho)G(\rho)$ tel que $\theta \equiv \rho \pmod{\mathcal{P}}$ et $G(\theta) \in \mathcal{P}^2$, alors $A_0(\rho) = \rho$ et on a :

$$G(\theta) = G(\rho + A_1(\rho)G(\rho))$$

$$= G(\rho) + A_1(\rho)G(\rho))\frac{G'(\rho)}{1!} + ... + [A_1(\rho)G(\rho)]^d \frac{G^{(d)}(\rho)}{d!} \equiv 0 \pmod{\mathcal{P}^2}$$

d'où, $G(\rho) + A_1(\rho)G(\rho)G'(\rho) \equiv 0 \pmod{\mathcal{P}^2}$.
On en déduit que $1 + A_1(\rho)G'(\rho) \equiv 0 \pmod{\mathcal{P}}$. Comme $G'(\rho) \notin \mathcal{P}$, alors $A_1(\rho)$ est déterminé de manière unique. Par conséquent, le nombre des éléments θ incongrus modulo $\mathcal{P}^2$ et vérifiant les conditions $\theta \equiv \rho \pmod{\mathcal{P}}$ et $G(\theta) \notin \mathcal{P}^2$ est égal à $p^d - 1$.
b) Soit $\theta_1 \in A$ vérifiant $\theta_1 \equiv \rho \pmod{\mathcal{P}}$ et $G(\theta_1) \notin \mathcal{P}^2$. Puisque $\mid \mathcal{P}^2/\mathcal{P}^e \mid = p^{d(e-2)}$, il existe $p^{d(e-2)}$ éléments $\gamma \in A$ incongrus modulo $\mathcal{P}^e$ et vérifiant $\gamma \equiv \theta_1 (\mathrm{mod}\, \mathcal{P}^2)$.
Il s'ensuit que le nombre des éléments $\theta \in A$ incongrus modulo $\mathcal{P}^e$ et vérifiant (5.1) est égal à $(p^d - 1)p^{d(e-2)}$. ■

Théorème 5.1.1 *Soient K un corps de nombres de degré n sur $\mathbb{Q}$, A son anneau des entiers et p un nombre premier. Soit $pA = \mathcal{P}_1^{e_1}...\mathcal{P}_r^{e_r}$ la décomposition de p comme produit d'idéaux premiers de A, où l'on suppose que le degré résiduel de $\mathcal{P}_i$ est $f_{\mathcal{P}_i} = f_i$. On suppose que $r = r_1 + ... + r_s$ où r_i est un entier strictement positif pour tout $i = 1, ..., s$ et que les idéaux $\mathcal{P}_i$ pour $i = 1, ..., r$, sont numérotés de façon que :*

$$f_1 = ... = f_{r_1} = f_1^*$$

$$f_{r_1+1} = ... = f_{r_1+r_2} = f_2^*$$

.....

$$f_{r_1+...+r_{s-1}+1} = ... = f_{r_1+...+r_s} = f_s^*.$$

Alors,

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

Démonstration. Il suffit de montrer que le nombre N des $\overline{\theta} \in A/pA$ tels que $p \nmid I(\theta)$ vérifie :

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

D'après le lemme (5.1.3), on peut définir une relation d'équivalence sur l'ensemble des éléments $\overline{\theta} \in A/pA$ tels que $p \nmid I(\theta)$ de la façon suivante :

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

si et seulement si pour tout $i = 1, ..., r, Irr(\theta + \mathcal{P}_i, F_p) = Irr(\alpha + \mathcal{P}_i, F_p)$.
Nous allons d'abord compter les éléments dans une classe d'équivalence puis compter le nombre des classes d'équivalence. En effet, les classes sont toutes de même cardinal. Une classe d'équivalence est définie par un certain uplet $(G_1(x), ..., G_r(x))$ de polynômes unitaires et irréductibles sur F_p tels que $\deg G_i = f_i$ pour $i = 1, ..., r$ et $G_i(x) \neq G_j(x)$ si $i \neq j$. D'après le lemme (5.1.3), le nombre des éléments $\overline{\theta} \in A/\mathcal{P}_i^e$ vérifiant $G_i(\theta) \equiv 0 \pmod{\mathcal{P}_i}$ et la condition $G_i(\theta) \notin \mathcal{P}_i^e$ est égal à f_i si $e_i = 1$ et égal à $f_i(p^{f_i} - 1)p^{f_i(e_i-2)}$ si $e_i \geq 2$.
Il s'ensuit que le nombre de uplets $(\theta_1 + \mathcal{P}_1^{e_1}, ..., \theta_1 + \mathcal{P}_r^{e_r}) \in A/\mathcal{P}_1^{e_1} \times ... \times A/\mathcal{P}_r^{e_r}$ satisfaisant les conditions $G_i(\theta_i) \equiv 0 \pmod{\mathcal{P}_i}$ pour $i = 1, ..., r$ et la condition $G_i(\theta_i) \notin \mathcal{P}_i^e$ pour tous les i tels que $e_i \geq 2$ est égal à

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

Nous comptons à présent le nombre des classes d'équivalence et qui correspond au nombre des uplets $(G_1(x), ..., G_r(x))$, $G_k(x)$ étant, pour tout $k \in \{1, ..., r\}$, un polynôme unitaire et

irréductible de $F_p[x]$ de degré f_k, tels que $G_i(x) \neq G_j(x)$ pour $i \neq j$.
Rappelons que les f_i sont numérotés de façon particulière dans le théorème (5.1.1). Il existe $A_{r_1}^{N_p(f_1^*)}$ manières de choisir $G_1(x), ..., G_{r_1}(x)$. Pour chacun de ces choix, il existe $A_{r_2}^{N_p(f_2^*)}$ manières de choisir les r_2 polynômes suivants, à savoir $G_{r_1+1}(x), ..., G_{r_1+r_2}(x)$,...etc. Donc, le nombre des classes d'équivalence est égal à $\prod_{j=1}^{s} A_{r_j}^{N_p(f_j^*)}$et par conséquent,

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

Ce qui achève la démonstration. ■

Proposition 5.1.1 *Soit s l'entier défini dans l'énoncé du théorème ci-dessus. Alors on a :*

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

Démonstration. Puisque pour tout $j = 1, ..., s$, $p \mid f_j^* N_p(f_j^*)$, alors la première assertion se déduit du théorème (5.1.1). Pour la seconde partie, on définit une relation d'équivalence dans A/pA comme suit : deux éléments $\overline{\alpha}$ et $\overline{\beta}$ de A/pA sont dits équivalents s'il existe $\lambda \in F_p^*$ tel que $\overline{\beta} = \lambda\overline{\alpha}$. Il est clair que si $\overline{\alpha}$ and $\overline{\beta}$ sont équivalents et si $p \mid I(\beta)$, alors $p \mid I(\alpha)$. Si la classe de 0 contient seulement un élément, chacune des autres en contient exactement $p-1$. Soit u le nombre de classes des éléments $\overline{\alpha}$ tels que $p \mid I(\alpha)$. Alors $\mu_K(p) = 1 + u(p-1)$, d'où le résultat. ■

Remarque 5.1.1 *A partir du théorème précédent, on retrouve celui de Hensel. En effet, avec les notations de la démonstration ci-dessus, le nombre premier p est f.c.i. dans K si et seulement si $N = 0$. Mais N s'annule si et seulement si pour un certain $j \in \{1, ..., s\}$, le nombre $A_{r_j}^{N_p(f_j^*)}$ est nul, ce qui équivaut à $r_j > N_p(f_j^*)$.*

Les trois corollaires à suivre sont parmi les conséquences immédiates de ce résultat. Ils affirment que pour certains types de décomposition du nombre premier p dans le corps de nombres K, on peut savoir si celui-ci est, ou n'est pas, un facteur commun d'indices dans K.

Corollaire 5.1.1 *Soit K un corps de nombres de degré n et A son anneau des entiers. Si un nombre premier $p < n$ se décompose complètement dans K, alors il est un facteur commun d'indices dans K.*

Démonstration. En effet, dans ce cas, ces n idéaux premiers distincts sont tous de degré $f_1^* = 1$. Par conséquent, on a $r = r_1 = n > N_p(f_1^*) = N_p(1) = p$. ■

Corollaire 5.1.2 *Soit K un corps de nombres et A son anneau des entiers. Si un nombre premier p est tel que l'idéal pA est un idéal premier de A (c'est-à-dire p inerte dans A) ou bien une puissance d'un idéal premier de A alors il n'est pas f.c.i. dans K.*

Démonstration. En effet, dans ce cas, avec les notations du théorème précédent, $r = r_1 = 1, s = 1$ et $f = f_1$. Donc $r_1 = 1 \leq N_p(f)$ quelle que soit la valeur de f. Le nombre premier p n'est donc pas f.c.i. dans K. ■

Corollaire 5.1.3 *Soit K un corps de nombres quartique.*
1) Pour que le nombre premier 2 soit f.c.i. dans K, il faut et il suffit qu'il ait l'un des trois types de décomposition suivants :
a) 2 est complètement décomposé, c'est-à-dire $2A = \mathcal{P}_1\mathcal{P}_1'\mathcal{P}_1''\mathcal{P}_1'''$;
b) $2A = \mathcal{P}_1\mathcal{P}_1'\mathcal{P}_1''^2$ (où les trois idéaux sont forcément de degré 1) ;
c) $2A$ est le produit de deux idéaux premiers distincts, tous les deux du second degré.
2) Pour que le nombre premier 3 soit f.c.i. dans K il faut et il suffit qu'il soit complètement décomposé.

Démonstration. Dans le cas du nombre premier 2, il est nécessaire et suffisant qu'il existe un f tel que $N_2(f) < r$, r étant le nombre d'idéaux premiers de degré f. Ce n'est pas le cas avec $f = 3$ ou 4. Il reste les valeurs possibles $f = 1$ ou 2. Si $f = 1$, on a $N_2(f) = N_2(1) = 2$, donc r doit être égal à 3 ou 4. Si $f = 2$, $N_2(f) = N_2(2) = 1$ et dans ce cas, r doit être égal à 2. Ce qui correspond bien aux trois décompositions de l'idéal $2A$ décrites.
Dans le cas du nombre premier 3, on a besoin, et c'est aussi suffisant, qu'un degré f vérifie $N_3(f) < r$. Comme $N_3(f) \geq 3$ quel que soit f, la seule valeur de r qui convienne éventuellement est 4. Et elle convient effectivement avec $f = 1$. Ce qui correspond à la décomposition de $3A$ comme produit de quatre idéaux premiers distincts du premier degré. ■

Définition 5.1.1 *Soient K un corps de nombres, A son anneau des entiers et p un nombre premier. On dit que p possède une décomposition spéciale dans K si tous les idéaux premiers de A au-dessus de p ont le même indice de ramification et le même degré résiduel sur p. Dans ce cas, si n est le degré de K sur $\mathbb{Q}$ et r le nombre des idéaux premiers de A au-dessus*

de p, on a : $n = efr$. Dans ce cas, e, f et r sont appelés les paramètres de la décomposition spéciale.

Remarque 5.1.2 *Si K est un corps de nombres galoisien, alors tout nombre premier possède dans K une décomposition spéciale.*

Le résultat suivant donne l'expression, considérablement simplifiée, de $\mu_K(p)$ lorsque p possède une décomposition spéciale dans K.

Corollaire 5.1.4 *Soit K un corps de nombres de degré n sur $\mathbb{Q}$ et p un nombre premier possèdant une décomposition spéciale dans K de paramètres e, f, r. Alors :*

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

Remarque 5.1.3 *Ce dernier corollaire implique qu'en particulier, si p se décompose complètement dans K, c'est-à-dire s'il s'écrit comme produit de n idéaux premiers distincts de l'anneau des entiers de K, forcément de degré résiduel 1, alors $\mu_K(p) = p^n - A_n^p$.*
Ce qui, dans le cas $p < n$, donne $\mu_K(p) = p^n$ et signifie que p est f.c.i. dans K.

5.2 Facteurs communs d'indices dans des corps de nombres de petits degrés

Il existe différents critères pour savoir si un nombre premier donné est facteur commun d'indices ou pas dans certains corps de nombres abéliens ainsi que dans des corps de nombres quelconques de degré trois ou quatre. On peut se référer aux travaux de Carlitz [9] [10], de Hall [15] et de Spearman et Williams [29] [30].

Dans ce qui suit, nous examinons les valeurs de la fonction μ_K lorsque K est un corps de nombres de degré quatre, cinq ou six. Nous déterminons les types de décomposition en produit d'idéaux premiers qui font d'un nombre premier donné un facteur commun d'indices dans le corps K. De plus, nous montrons comment, dans certains cas, la valeur de μ_K en un nombre premier p peut déterminer le type de décomposition de p dans K.

5.2.1 Le cas quartique

La table ci-dessous donne, en utilisant le théorème 5.1.1, la valeur de $\mu_K(p)$ lorsque K est un corps de nombres de degré 4 sur $\mathbb{Q}$ selon le type de décomposition de p dans K.

Table 1

La décomposition de p dans K	$\mu_K(p)$	$p, \mu_K(p) = p^4$
$\mathcal{P}_4$	p^2	–
$\mathcal{P}_1^4$	p^3	–
$\mathcal{P}_2^2$	$p^3 + p^2 - p$	–
$\mathcal{P}_1^3\mathcal{P}_1'$	$2p^3 - p^2$	–
$\mathcal{P}_2\mathcal{P}_2'$	$2p^3 + p^2 - 2p$	2
$\mathcal{P}_1\mathcal{P}_3$	p^2	–
$\mathcal{P}_1^2\mathcal{P}_2$	$2p^3 - p^2$	–
$\mathcal{P}_1^2\mathcal{P}_1'^2$	$3p^3 - 3p^2 + p$	–
$\mathcal{P}_1\mathcal{P}_1'\mathcal{P}_2$	$2p^3 - p^2$	–
$\mathcal{P}_1\mathcal{P}_1'\mathcal{P}_1''^2$	$4p^3 - 5p^2 + 2p$	2
$\mathcal{P}_1\mathcal{P}_1'\mathcal{P}_1''\mathcal{P}_1'''$	$6p^3 - 11p^2 + 6p$	2, 3

(L'indice de chaque idéal premier figurant dans cette table représentant son degré résiduel sur p.)

Remarque 5.2.1 *Cette table confirme, évidemment, les résultats du corollaire 5.1.3. En effet, les types de décomposition de l'idéal $2A$ qui font de 2 un f.c.i. dans K sont ceux pour lesquels $\mu_K(2) = 2^4 = 16$ et qui sont bien d'après cette table ceux prévus par le corollaire 5.1.3. De même, s'agissant du nombre premier 3, on constate bien que le seul cas où $\mu_K(3) = 3^4 = 81$ et qui fait donc de 3 un f.c.i. correspond à l'écriture de $3A$ comme produit de quatre idéaux premiers distincts, comme indiqué dans le même corollaire.*

Remarque 5.2.2 *Soit p un nombre premier, K un corps de nombres de degré n, A son anneau des entiers et $\omega_1, ..., \omega_n$ une base des entiers de K. Pour tout élement $\theta \in A$ écrit sous la forme $\theta = \sum_{i=1}^{n} x_i\omega_i$ où les $x_i \in \mathbb{Z}$ et $0 \leq x_i \leq p-1$, il est possible de déterminer*

si p divise $I(\theta)$ et donc de calculer $\mu_K(p)$ de cette manière. D'un autre côté, en utilisant la formule donnée dans le théorème 5.1.1, on peut déterminer toutes les valeurs possibles de $\mu_K(p)$ dans un corps de nombres de degré n selon le type de décomposition de p. En comparant la valeur trouvée selon le premier procédé à la table de toutes les valeurs, il est possible de déterminer, dans certains cas, le type de décomposition du nombre premier p dans le corps considéré. Par exemple, dans le cas d'un corps quartique K, si la valeur de $\mu_K(2)$ trouvée est $8, 10$ ou 14, alors, d'après la table ci-dessus, on peut en déduire le type de décomposition du nombre premier 2 dans le corps K.

5.2.2 Le cas quintique

Etant donnés un corps de nombres K de degré cinq et un nombre premier p, la table ci-après donne les valeurs de $\mu_K(p)$ selon le type de décomposition du nombre premier p dans K. De plus, elle détermine les types de décomposition qui font des deux nombres premiers 2 et 3 des facteurs communs d'indices dans K.

Table 2

La décomposition de p dans K	$\mu_K(p)$	$p, \mu_K(p) = p^5$
$\mathcal{P}_5^1$	p	–
$\mathcal{P}_1^5$	p^4	–
$\mathcal{P}_3\mathcal{P}_2'$	$p^4 + p^3 - p^2$	–
$\mathcal{P}_3\mathcal{P}_1'^2$	$p^4 + p^3 - p^2$	–
$\mathcal{P}_1^3\mathcal{P}_2'$	$p^4 + p^3 - p^2$	–
$\mathcal{P}_1^3\mathcal{P}_1'^2$	$3p^4 - 3p^3 + p^2$	–
$\mathcal{P}_4\mathcal{P}_1'$	p^3	–
$\mathcal{P}_1^4\mathcal{P}_1'$	$2p^4 - p^3$	–
$\mathcal{P}_3\mathcal{P}_1'\mathcal{P}_1''$	$p^4 + p^3 - p^2$	–
$\mathcal{P}_1^3\mathcal{P}_1'\mathcal{P}_1''$	$4p^4 - 5p^3 + 2p^2$	2
$\mathcal{P}_2\mathcal{P}_2'\mathcal{P}_1''$	$2p^4 + p^3 - 2p^2$	2
$\mathcal{P}_2\mathcal{P}_1'^2\mathcal{P}_1''$	$3p^4 - 3p^3 + p^2$	–
$\mathcal{P}_1^2\mathcal{P}_1'^2\mathcal{P}''$	$5p^4 - 9p^3 + 7p^2 - 2p$	2
$\mathcal{P}_2\mathcal{P}_1'\mathcal{P}_1''\mathcal{P}_1'''$	$4p^4 - 5p^3 + 2p^2$	2
$\mathcal{P}_1^2\mathcal{P}_1'\mathcal{P}_1''\mathcal{P}_1'''$	$7p^4 - 17p^3 + 17p^2 - 6p$	2, 3
$\mathcal{P}_1\mathcal{P}_1'\mathcal{P}_1''\mathcal{P}_1'''\mathcal{P}_1''''$	$10p^4 - 35p^3 + 50p^2 - 24p$	2, 3

Remarque 5.2.3 *Des* 16 *types de décomposition éventuels de nombres premiers dans un corps de nombres de degré cinq, seuls* 3 *d'entre-eux correspondent à des décompositions spéciales. Et seulement l'une de ces trois (la toute dernière dans la table ci-dessus) donne un* $\mu_K(p) = p^5$ *(pour* $p = 2$ *et pour* $p = 3$*). Les cinq autres décompositions donnant lieu à un f.c.i. (* 2 *ou* 3 *ou les deux) correspondent à des corps non galoisiens.*

5.2.3 Le cas sextique

Soit K un corps de nombres de degré 6 sur $\mathbb{Q}$. D'après Zylinski, trois nombres premiers peuvent éventuellement prétendre à la qualité de facteurs communs d'indices dans K. Il s'agit de 2, 3 et 5. Si l'on note par p l'un d'eux, pour qu'il le soit effectivement, il faut et il suffit, d'après le théorème de Hensel, ou le théorème 5.1.1, que la condition suivante soit vérifiée.

(*) Il existe un degré résiduel f commun à un nombre t d'idéaux premiers au dessus de p tel que $t > N_p(f)$.

Remarquons que cette condition est d'autant plus facile à satisfaire que $N_p(f)$ est "petit", ce qui équivaut, globalement, à p et f "petits". On obtient les résultats suivants.

(a) Si $p = 2$, alors pour $f = 1$, la condition (*) devient : $t > N_2(1) = 2$. Par conséquent 2 est f.c.i. pour tout type de décomposition de 2 où l'on a au moins trois idéaux premiers de degré 1. Pour $f = 2$, comme $N_2(2) = 1$, la condition est remplie pour tout type de décomposition de 2 où l'on a au moins deux idéaux premiers de degré 2.

(b) Si $p = 3$, on a $N_3(1) = 3$ et $N_3(f) \geq N_3(2) = 8$ pour tout $f \geq 2$. Par conséquent, compte tenu de la formule $6 = \sum e_i f_i$, la seule valeur de f pour laquelle la condition peut être satisfaite est $f = 1$. Et elle l'est pour les décompositions de 3 où l'on a au moins quatre idéaux premiers de degré 1.

(c) Si $p = 5$, un seul type de décomposition de 5 est "bon" : le type "complètement décomposé". En effet, comme $N_5(f) > 5$ pour tout $f > 1$, la seule valeur intéressante de f est $f = 1$. Comme $N_5(1) = 5$, la condition (*) est satisfaite si et seulement si 5 s'écrit comme le produit de six idéaux premiers (de degré 1).

Comme dans le cas des degrés 4 et 5, la table suivante donne les valeurs de $\mu_K(p)$ dans le cas où K est de degré 6.

Table 3

La décomposition de p dans K	$\mu_K(p)$	$p, \mu_K(p) = p^6$
$\mathcal{P}_6$	$p^3 + p^2 - p$	–
$\mathcal{P}_3^2$	$p^4 + p^3 - p$	–
$\mathcal{P}_2^3$	$p^5 + p^4 - p^3$	–
$\mathcal{P}_1^6$	p^5	–
$\mathcal{P}_5\mathcal{P}_1'$	p^2	–
$\mathcal{P}_4\mathcal{P}_2'$	$p^5 + p^4 - p^3$	–
$\mathcal{P}_4\mathcal{P}_1'^2$	$p^5 + p^4 - p^3$	–
$\mathcal{P}_3\mathcal{P}_3'$	$2p^4 + 3p^3 - p^2 - 3p$	–
$\mathcal{P}_3\mathcal{P}_1'^3$	$p^5 + p^4 - p^3$	–
$\mathcal{P}_2^2\mathcal{P}_2'$	$2p^5 + 2p^4 - 4p^3 - p^2 + 2p$	2
$\mathcal{P}_2^2\mathcal{P}_1'^2$	$2p^5 - 2p^3 + p^2$	–
$\mathcal{P}_2\mathcal{P}_1'^4$	$2p^5 - p^4$	–
$\mathcal{P}_1^5\mathcal{P}_1'$	$2p^5 - p^4$	–
$\mathcal{P}_1^4\mathcal{P}_1'^2$	$3p^5 - 3p^4 + p^3$	–
$\mathcal{P}_1^3\mathcal{P}_1'^3$	$3p^5 - 3p^4 + p^3$	–
$\mathcal{P}_4\mathcal{P}_1'\mathcal{P}_1''$	$p^5 + p^4 - p^3$	–
$\mathcal{P}_3\mathcal{P}_2'\mathcal{P}_1''$	$p^5 + p^4 - p^3$	–
$\mathcal{P}_3\mathcal{P}_1'^2\mathcal{P}_1''$	$2p^5 - 2p^3 + p^2$	–
$\mathcal{P}_2^2\mathcal{P}_1'\mathcal{P}_1''$	$2p^5 - 2p^3 + p^2$	–
$\mathcal{P}_2\mathcal{P}_2'\mathcal{P}_2''$	$3p^5 + 3p^4 - 11p^3 - 2p^2 + 8p$	2
$\mathcal{P}_2\mathcal{P}_2'\mathcal{P}_1''^2$	$3p^5 - p^4 - 3p^3 + 2p^2$	2
$\mathcal{P}_2\mathcal{P}_1'^2\mathcal{P}_1''^2$	$4p^5 - 6p^4 + 4p^3 - p^2$	–
$\mathcal{P}_2\mathcal{P}_1'^3\mathcal{P}_1''$	$3p^5 - 3p^4 + p^3$	–
$\mathcal{P}_1^4\mathcal{P}_1'\mathcal{P}_1''$	$4p^5 - 5p^4 + 2p^3$	2
$\mathcal{P}_1^3\mathcal{P}_1'^2\mathcal{P}_1''$	$5p^5 - 9p^4 + 7p^3 - 2p^2$	2
$\mathcal{P}_1^2\mathcal{P}_1'^2\mathcal{P}_1''^2$	$6p^5 - 14p^4 + 16p^3 - 9p^2 + 2p$	2
$\mathcal{P}_3\mathcal{P}_1'\mathcal{P}_1''\mathcal{P}_1'''$	$3p^5 - p^4 - 3p^3 + 2p^2$	2
$\mathcal{P}_2\mathcal{P}_2'\mathcal{P}_1''\mathcal{P}_1'''$	$3p^5 - p^4 - 3p^3 + 2p^2$	2
$\mathcal{P}_2\mathcal{P}_1'^2\mathcal{P}_1''\mathcal{P}_1'''$	$5p^5 - 9p^4 + 7p^3 - 2p^2$	2
$\mathcal{P}_1^3\mathcal{P}_1'\mathcal{P}_1''\mathcal{P}_1'''$	$7p^5 - 17p^4 + 17p^3 - 6p^2$	2, 3

$\mathcal{P}_1^2\mathcal{P}_1'^2\mathcal{P}_1''\mathcal{P}_1'''$	$8p^5 - 24p^4 + 34p^3 - 23p^2 + 6p$	$2, 3$
$\mathcal{P}_2\mathcal{P}_1'\mathcal{P}_1''\mathcal{P}_1'''\mathcal{P}_1''''$	$7p^5 - 17p^4 + 17p^3 - 6p^2$	$2, 3$
$\mathcal{P}_1^2\mathcal{P}_1'\mathcal{P}_1''\mathcal{P}_1'''\mathcal{P}_1''''$	$11p^5 - 45p^4 + 85p^3 - 74p^2 + 24p$	$2, 3$
$\mathcal{P}_1\mathcal{P}_1'\mathcal{P}_1''\mathcal{P}_1'''\mathcal{P}_1''''\mathcal{P}_1'''''$	$15p^5 - 85p^4 + 225p^3 - 274p^2 + 120p$	$2, 3, 5$

Remarque 5.2.4 *Sachant que $\mu_K(p)$ est multiple de p, non nul, et qu'il est au plus égal à p^6, il est clair que pour $p = 2$, $\mu_K(2)$ est un entier pair entre 2 et 64 et que par conséquent, plusieurs types de décomposition parmi les 34 possibles peuvent donner la même valeur de $\mu_K(2)$. Cependant, certaines valeurs sont obtenues pour un seul type de décomposition. Il s'agit des suivantes : $4, 10, 22, 32, 46$ et 60. Ainsi, chacune de ces valeurs de $\mu_K(2)$ implique un type de décomposition précis de 2 dans K.*

5.3 Exemples explicites de corps de nombres admettant un nombre premier donné comme facteur commun d'indices

Etant donné un nombre premier p, d'après le théorème de Zylinski, p ne peut être facteur commun d'indices dans les corps de nombres de degré $\leq p$. Et il ne l'est pas forcément dans un corps donné quelconque K de degré $> p$. La condition, nécessaire et suffisante, pour que p le soit, étant que p possède dans ce corps un type de décomposition qui fasse que $\mu_K(p) = p^n$, n étant le degré de K sur $\mathbb{Q}$, c'est-à-dire, que cette décomposition de p vérifie la condition de Hensel. La question qui se pose alors est : étant donnés un entier n et un nombre premier p tel que $n > p$, existe-t-il forcément un corps K de degré n où p est f.c.i. ?

La réponse à cette question est donnée par le résultat suivant, dû à Bauer [7].

Théorème 5.3.1 *Soient p un nombre premier et n un entier strictement plus grand que p. Alors il existe un corps de nombres de degré n dans lequel p est facteur commun d'indices.*

Ce résultat rend légitime la question suivante : étant donnés un nombre premier p et un entier $n > p$, quels sont les corps de nombres de degré n admettant p comme facteur commun d'indices ? C'est l'objet de la prochaine section.

5.3.1 Corps de nombres cubiques admettant 2 comme facteur commun d'indices

Dans la recherche d'exemples de corps de nombres cubiques admettant 2 comme facteur commun d'indices, Nagell [24] utilise un résultat de Levi [21] sur l'existence d'une correspondance entre corps de nombres cubiques et formes binaires du troisième degré.

Dans ce qui suit, nous rappelons certains résultats sur les formes binaires et la correspondance qui existe entres les formes binaires du troisième degré et les corps de nombres cubiques.

Une forme binaire de degré $n \geq 2$ est toute expression de type

$$F(x,y) = a_0x^n + a_1x^{n-1}y + ... + a_{n-1}xy^{n-1} + a_ny^n$$

où les coefficients a_i sont des entiers rationnels.

Une telle forme est notée, comme dans [24], plus simplement $((a_0, a_1, ..., a_{n-1}, a_n))$. Elle est dite primitive si les a_i sont premiers entre eux dans leur ensemble, c'est-à-dire si $\gcd(a_1, ..., a_n) = 1$.

On appelle diviseur fixe d'une forme binaire $((a_0, a_1, ..., a_{n-1}, a_n))$ tout élément de $\mathbb{Z}$ divisant $F(x,y) = a_0x^n + a_1x^{n-1}y + ... + a_{n-1}xy^{n-1} + a_ny^n$ pour toute "valeur" du couple (x,y) dans $\mathbb{Z}^2$.

Il est clair que 1 est diviseur fixe de toute forme binaire et que si $\delta \in \mathbb{Z}$ est diviseur fixe d'une forme binaire donnée, son opposé $-\delta$ aussi. Par conséquent, par diviseur fixe on entendra dorénavent diviseur fixe ≥ 2.

Nagell montre dans [24] que tout diviseur fixe d'une forme binaire primitive de degré n divise $(n-1)!$.

Soient deux formes binaires $F(x,y) = ((a_0, a_1, ..., a_n))$ et $G(x,y) = ((b_0, b_1, ..., b_n))$. Elles sont dites équivalentes s'il existe une matrice carrée P d'ordre 2 à coefficients dans $\mathbb{Z}$ inversible (donc de déterminant ± 1) telle que

$$G(x,y) = F\left({}^tP\begin{pmatrix} x \\ y \end{pmatrix}\right)$$

Soient $((a_0, a_1, ..., a_{n-1}, a_n))$ et $((b_0, b_1, ..., b_{n-1}, b_n))$ deux formes binaires équivalentes de même degré. Alors, si l'une d'elles est primitive, l'autre aussi. De plus, elles ont les mêmes

diviseurs fixes.

Enfin, si $((a_0, a_1, ..., a_{n-1}, a_n)) = F(x, y)$ est une forme binaire irréductible et si θ est une racine dans $\mathbb{C}$ du polynôme $F(x, 1) = a_0x^n + a_1x^{n-1} + ... + a_n$, on dit que le corps de nombres $K = \mathbb{Q}(\theta)$ est engendré par la forme binaire $((a_0, a_1, ..., a_{n-1}, a_n))$, ou que celle-ci est construite sur le corps de nombres K.

D'après un résultat de Voronoï, pour tout corps de nombres cubique K, il existe une base des entiers de la forme $\{1, \alpha, \beta\}$ telle que α et β vérifient les relations suivantes :

$$\alpha^3 - b\alpha^2 + ac\alpha - a^2d = 0 \text{ et } \alpha\beta = ad$$

où a, b, c et d sont des entiers rationnels. De plus, on a forcément a et d non nuls puisque sinon, les entiers α et β vérifieraient, chacun, une équation de dépendance intégrale de degré 2 ce qui serait absurde.

En fait, les deux relations ci-dessus en impliquent une troisième :

$$\beta^3 - c\beta^2 + bd\beta - ad^2 = 0$$

On peut maintenant préciser la correspondance entre corps de nombres cubiques et formes binaires de degré 3 à travers le théorème suivant, dû à Levi [21].

Théorème 5.3.2 *Soit K un corps de nombres cubique et $\{1, \alpha, \beta\}$ et $\{1, \alpha', \beta'\}$ deux bases des entiers de K vérifiant :*

$$\begin{aligned} \alpha^3 - b\alpha^2 + ac\alpha - a^2d &= 0, \alpha\beta = ad; \\ \alpha'^3 - b'\alpha'^2 + a'c'\alpha' - a'^2d' &= 0, \alpha'\beta' = a'd' \end{aligned}$$

Alors les formes binaires du $3^{ème}$ degré $((a, b, c, d))$ et $((a', b', c', d'))$ sont irréductibles, primitives et équivalentes. De plus, elles ont pour discriminant celui de K.

Ainsi, à tout corps de nombres cubique correspond une et une seule forme binaire de degré 3, à équivalence près, et celle-ci est irréductible et primitive ; le corps et la forme binaire ont le même discriminant.

Soit donc un corps cubique K. Nous savons que le seul nombre premier susceptible d'être un facteur commun d'indices dans K est 2. Dans la suite nous allons voir, en suivant Nagell, que 2 est un f.c.i. dans K si et seulement si 2 est un diviseur fixe de la forme binaire de degré 3 associée à K. Du reste, 2 est le seul diviseur fixe éventuel d'une forme binaire primitive de degré 3.

En effet, on sait d'après ce qui précède qu'il existe une base $\{1, \alpha, \beta\}$ des entiers de K telle que α et β vérifient les relations :

$$\alpha^3 - b\alpha^2 + ac\alpha - a^2 d = 0 \text{ et } \alpha\beta = ad$$

Etant donné un entier θ quelconque de K, on peut l'écrire, et de manière unique, sous la forme :

$$\theta = x\alpha - y\beta + z$$

où x, y et z sont dans $\mathbb{Z}$.

Dans ce cas, l'écriture de θ^2 dans la base $\{1, \alpha, \beta\}$ est donnée comme suit :

$$\theta^2 = (bx^2 + dy^2 + 2xz)\alpha + (ax^2 + cy^2 - 2yz)\beta + z'$$

où $z' \in \mathbb{Z}$. (On verra dans la suite que la valeur de z' n'influe en rien sur l'indice de l'entier θ.)

On en déduit que l'indice de θ, soit $I(\theta)$, vérifie

$$(I(\theta))^2 = (\det(P))^2$$

où P est la matrice suivante :

$$P = \begin{pmatrix} 1 & z & z' \\ 0 & x & bx^2 + dy^2 + 2xz \\ 0 & -y & ax^2 + cy^2 - 2yz \end{pmatrix}$$

Or, $\det(P) = x(ax^2 + cy^2 - 2yz) + y(bx^2 + dy^2 + 2xz) = ax^3 + bx^2y + cxy^2 + dy^3$.

Il s'ensuit que les diviseurs de $I(\theta)$ sont exactement ceux de la forme binaire $((a, b, c, d))$. En particulier, 2 est facteur commun d'indices dans K si et seulement si 2 est un diviseur fixe de la forme binaire $((a, b, c, d))$.

Le résultat suivant précise les formes binaires primitives dont 2 est diviseur fixe.

Lemme 5.3.1 *Soit $((a,b,c,d))$ une forme binaire primitive de degré 3 quelconque. Alors, 2 en est un diviseur fixe si et seulement si a et d sont pairs et b et c sont impairs.*

Démonstration. En effet, écrivons $((a,b,c,d)) = F(x,y) = ax^3+bx^2y+cxy^2+dy^3$. Si 2 est diviseur fixe de $F(x,y)$, alors 2 divise $F(1,0)$ et $F(0,1)$, c'est-à-dire a et d. Il divise donc aussi $G(x,y) = F(x,y)-(ax^3+dy^3) = bx^2y+cxy^2$ pour tous $x,y \in \mathbb{Z}$. Mais, $G(x,y) = xy(bx+cy)$ et pour x et y impairs, on voit que 2 divise $G(x,y)$ si et seulement si b et c sont de même parité. Par ailleurs, comme a et d sont pairs et que la forme binaire est primitive, on voit que b et c sont nécessairement impairs. Réciproquement, il est clair que si ces conditions sont vérifiées, 2 est diviseur fixe de la forme binaire. ■

On peut donc énoncer le résultat suivant.

Théorème 5.3.3 *Soit K un corps de nombres cubique. Alors K est engendré sur $\mathbb{Q}$ par une racine d'un polynôme irréductible de la forme*

$$f(x) = x^3 - bx^2 + acx - a^2d$$

où les coefficients a,b,c et d sont dans $\mathbb{Z}$.
Dans ce cas, le nombre premier 2 est facteur commun d'indices dans K si et seulement si a et d sont pairs et que b et c sont impairs.

Dans la suite, nous allons montrer comment on peut construire une infinité de polynômes irréductibles dont les corps engendrés respectifs possèdent le nombre premier 2 comme facteur commun d'indices.

Plus précisément, en prenant un triplet (a,b,c) quelconque vérifiant les conditions a pair et b et c impairs, il est possible, et d'une infinité de manières, de choisir un entier pair d de façon que le polynôme $f(x) = x^3 - bx^2 + acx - a^2d$ soit irréductible, c'est-à-dire qu'il n'ait pas de racine parmi les diviseurs de a^2d.

Exemple 5.3.1 *Soient les entiers $a = 2, b = c = 1$ et $d = 2p$ où p est un nombre premier différent de 2. On considère le polynôme $f(x) = x^3 - x^2 + 2x - 8p$. Nous allons montrer que si p est suffisamment grand, ce polynôme est irréductible. En effet, les diviseurs de $8p$ étant les $\pm 2^k p^l$ où $k \in \{0,...,3\}$ et $l \in \{0,1\}$, il suffit de choisir p de façon que $f(\pm 2^k p^l) \neq 0$ pour tout couple $(k,l) \in \{0,...,3\} \times \{0,1\}$.*
Or, $f(\pm 2^k p^l) = \pm 2^{3k} p^{3l} - 2^{2k} p^{2l} \pm 2^{k+1} p^l - 2^3 p$.

On distingue les deux cas suivants :
Si $l = 0$, $f(\pm 2^k p^l) = f(\pm 2^k) = \pm 2^{3k} - 2^{2k} \pm 2^{k+1} - 2^3 p < 2^9 + 2^4 - 2^3 p = 2^3(2^6 + 2 - p)$,
ce qui, pour p *suffisamment grand (il suffit en fait que* $p \geq 67$*), est strictement négatif.*
Si $l = 1$, $f(\pm 2^k p^l) = f(\pm 2^k p) = \pm 2^{3k} p^3 - 2^{2k} p^2 \pm 2^{k+1} p - 2^3 p$.
Pour éviter que cette quantité s'annule, il suffit que p^3 *soit supérieur à la valeur absolue de* $-2^{2k} p^2 \pm 2^{k+1} p - 2^3 p$. *Ce qui est le cas dès que l'on prend* $p > 2^6$.

En conclusion, pour tout nombre premier $p \geq 67$, le polynôme $f(x) = x^3 - x^2 + 2x - 8p$ est irréductible et si θ en est une racine quelconque dans $\mathbb{C}$, le corps de nombres cubique $\mathbb{Q}(\theta)$ admet 2 comme facteur commun d'indices.

5.3.2 Corps de nombres de degré supérieur à 3 admettant un nombre premier donné comme facteur commun d'indices

D'après le corollaire 5.1.3 (ou la table 1), le nombre premier 2 est facteur commun d'indices dans un corps de nombres quartique si et seulement s'il se décompose dans ce corps sous l'une des trois formes suivantes : $\mathcal{P}_1\mathcal{P}_1'\mathcal{P}_1''\mathcal{P}_1'''$, $\mathcal{P}_1\mathcal{P}_1'\mathcal{P}_1''^2$ ou $\mathcal{P}_2\mathcal{P}_2'$. Quant à 3, il n'est facteur commun d'indices dans ce corps que si et seulement s'il est complètement décomposé.

Des exemples de corps quartiques admettant l'un des deux nombres premiers 2 et 3 ou les deux à la fois sont donnés par Nagell (voir [24]). A titre d'exemple, il montre que si l'on prend un corps biquadratique $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2})$ où d_1 et d_2 sont deux entiers sans facteur carré tels que leur produit $d_1 d_2$ n'est pas un carré, alors :

a) 2 est f.c.i. de la première catégorie (c'est-à-dire en se décomposant complètement dans K) si et seulement si $d_1 \equiv d_2 \equiv 1 \pmod 8$.

b) 2 est f.c.i. de la troisième catégorie (c'est-à-dire en ayant une décomposition de type $\mathcal{P}_2\mathcal{P}_2'$) si et seulement si $d_1 \equiv d_2 \equiv 1 \pmod 4$ et que d_1 ou d_2 ne soit pas congru à 1 (mod 8).

c) 3 est f.c.i. dans K si et seulement si $d_1 \equiv d_2 \equiv 1 \pmod 3$.

Pour des corps de nombres de degré plus grand, le résultat suivant, dû à Varmon [31], permet de dégager toute une classe de corps de nombres de différents degrés admettant un nombre premier donné comme facteur commun d'indices.

Proposition 5.3.1 *Soient* $d_1, d_2, ..., d_n$ $(n \geq 2)$ *des entiers rationnels tels que le corps* $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, ..., \sqrt{d_n})$ *soit de degré* 2^n *sur* $\mathbb{Q}$.

a) Si pour tout $i = 1, ..., n$, on a $d_i \equiv 1 \pmod 8$, alors 2 est complètement décomposé dans K.

b) Si p est un nombre premier impair et que d_i est résidu quadratique modulo p pour tout $i = 1, ..., n$, alors p est complètement décomposé dans K.

Démonstration. Voir [31] ■

Il faut remarquer que la condition "K de degré 2^n" est satisfaite si par exemple les d_i sont des nombres premiers deux à deux distincts.

On déduit de ce résultat que 2 est f.c.i. dans le cas a) et p, avec $2 < p < 2^n$ est f.c.i. dans le cas b).

Il est clair que ce résultat offre alors une classe infinie de corps de nombres admettant un nombre premier donné comme facteur commun d'indices.

Si $n = 2$, on retrouve l'un des résultats de Nagell, cités plus haut, concernant les corps quartiques.

5.4 Corps de nombres K et K' tels que $\mu_K(p) = \mu_{K'}(p)$

Dans cette section, étant donné un nombre premier p, on s'intéressera aux corps de nombres de même degré où p possède une décomposition spéciale. On sait, dans un corps de nombres galoisien, n'importe quel nombre premier possède une décomposition spéciale. Les deux résultats suivants s'appliquent donc en particulier à ces corps.

Théorème 5.4.1 *Soient K et K' deux corps de nombres de même degré sur $\mathbb{Q}$ et p un nombre premier ayant des décompositions spéciales dans K et K' et de paramètres e, f, r et e', f', r' respectivement. On suppose que $\mu_K(p) = \mu_{K'}(p)$ et que p n'est pas f.c.i. dans K (ni donc dans K').*
Si $f = f'$ alors $e = e'$ et $r = r'$.

Démonstration. La première assertion est triviale. Pour la seconde, raisonnons par l'absurde et supposons $r < r'$.

Cas 1 : si e et $e' \geq 2$. Nous avons dans ce cas :

$$\mu_K(p) = p^n - f^r(p^f - 1)^r p^{rf(e-2)} A_r^{N_p(f)} = p^n - p^n\left(\frac{p^f - 1}{p^f}\right)^r \prod_{k=0}^{r-1} \frac{f(N_p(f) - k)}{p^f} \tag{5.2}$$

et

$$\mu_{K'}(p) = p^n - p^n(\frac{p^f-1}{p^f})^{r'}\prod_{k=0}^{r'-1}\frac{f(N_p(f)-k)}{p^f}. \tag{5.3}$$

L'égalité $\mu_K(p) = \mu_{K'}(p)$ équivaut donc à la suivante :

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

Puisque $r < r'$, alors

$$(\frac{p^f-1}{p^f})^{r} > (\frac{p^f-1}{p^f})^{r'}. \tag{5.4}$$

Nous pouvons écrire :

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

Manifestement, pour tout $k = r, ..., r'-1$, on a $f(N_p(f)-k) < p^f$
d'où

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

Il s'ensuit que

$$\prod_{k=0}^{r'-1}\frac{f(N_p(f)-k)}{p^f} < \prod_{k=0}^{r-1}\frac{f(N_p(f)-k)}{p^f}. \tag{5.5}$$

De (5.4) et (5.5) on tire $a'(p) < a(p)$. Par conséquent, de (5.2) et (5.3), on déduit que $\mu_K(p) < \mu_{K'}(p)$, ce qui est absurde.

Cas 2 : $e = 1$ **et** $e' \geq 2$. Dans ce cas, $\mu_K(p) = \mu_{K'}(p)$ implique l'égalité

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

où $r = e'r'$. D'où,

$$f^{r-\frac{r}{e'}} \prod_{k=\frac{r}{e'}}^{r-1} (N_p(f)-k) = (p^f-1)^{\frac{r}{e'}} p^{\frac{r}{e'}f(e'-2)}. \tag{5.6}$$

Par ailleurs, on a d'une part :

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

et donc, pour tout entier non nul k, on a

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

d'où

$$f^{r-\frac{r}{e'}} \prod_{k=\frac{r}{e'}}^{r-1} (N_p(f)-k) < (p^f-1)^{r-\frac{r}{e'}}. \tag{5.7}$$

D'autre part, on a

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

d'où

$$(p^f-1)^{\frac{r}{e'}} p^{\frac{r}{e'}f(e'-2)} \geq p^f-1)^{\frac{r}{e'}(e'-1)} = (p^f-1)^{r-\frac{r}{e'}}. \tag{5.8}$$

On voit bien que (5.8) et (5.7) sont en contradiction avec l'équation (5.6). ■

Conjecture 5.4.2 *Soient K et K' deux corps de nombres de même degré strictement plus grand que 2 sur $\mathbb{Q}$ et p un nombre premier admettant dans chacun d'eux une décomposition*

spéciale. On suppose que $\mu_K(p) = \mu_{K'}(p)$ *et que* p *n'est pas f.c.i. dans* K*. Alors* $e = e'$*,* $f = f'$ *et* $r = r'$*.*

Le prochain et dernier théorème est une réponse partielle à cette conjecture. Il affirme que celle-ci est vraie pour des nombres premiers assez grands. Pour sa démonstration, nous aurons besoin du résultat qui suit, dû à Erdős et Selfridge [13].

Lemme 5.4.1 *Si* k *et* m *sont deux entiers quelconques* ≥ 2*, l'équation diophantienne*

$$(x+1)...(x+m) = y^k$$

n'a aucun couple solution (x, y) *avec* x *et* y *strictement positifs.*

Théorème 5.4.3 *Soient* K *et* K' *deux corps de nombres de même degré* $n \geq 3$ *sur* $\mathbb{Q}$ *et* p *un nombre premier ayant des décompositions spéciales dans* K *et* K' *et de paramètres* e, f, r *et* e', f', r' *respectivement. On suppose que* $\mu_K(p) = \mu_{K'}(p)$ *et que* $p > 2(\frac{n}{4})^{\frac{n}{2}-1}$*.*
Alors $f = f'$*,* $e = e'$ *et* $r = r'$*.*

Démonstration. On raisonne par rapport aux valeurs de e et de e'.
Cas 1 : $e \geq 2, e' \geq 2$
Alors l'égalité $\mu_K(p) = \mu_{K'}(p)$ équivaut à :

$$f^r(p^f - 1)^r p^{rf(e-2)} A_r^{N_p(f)} = f'^{r'}(p^{f'} - 1)^{r'} p^{r'f'(e'-2)} A_{r'}^{N_p(f')}. \tag{5.9}$$

En considérant la valuation p-adique de chacun des deux membres de (5.9), on obtient :

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

Comme $rfe = r'f'e'$, il vient :

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

ou encore :

$$2(rf - r'f') = \frac{f}{rad(f)} - \frac{f'}{rad(f')}. \tag{5.10}$$

D'autre part, après simplification par $p^{v_p(\mu_K(p))} = p^{v_p(\mu_{K'}(p))}$ des deux membres de (5.9), on tire :

$$f^r(p^f - 1)^r \frac{N_p(f)}{p^{\frac{f}{rad(f)}}}(N_p(f) - 1)...(N_p(f) - (r-1))$$

$$= f'^r(p^{f'} - 1)^r \frac{N_p(f')}{p^{\frac{f'}{rad(f')}}}(N_p(f) - 1)...(N_p(f) - (r-1)).$$

Or,

$$\frac{N_p(f)}{p^{\frac{f}{rad(f)}}} = \frac{1}{f}(p^{f - \frac{f}{rad(f)}} - p^{()} + ... \pm 1)$$

de même,

$$\frac{N_p(f')}{p^{\frac{f'}{rad(f')}}} = \frac{1}{f'}(p^{f' - \frac{f'}{rad(f')}} - p^{()} + ... \pm 1).$$

Donc, en considérant les restes modulo p, on a :

$$f^{r-1} \times (-1)^r \times (\pm 1) \times (-1) \times ... \times (-(r-1))$$

$$\equiv f'^{r'-1} \times (-1)^{r'} \times (\pm 1) \times (-1) \times ... \times (-(r'-1)) \ (mod\ p)$$

c'est-à-dire :

$$f^{r-1} \times (-1)^r \times (\pm 1) \times (-1)^{r-1} \times ((r-1)!)$$

$$\equiv f'^{r'-1} \times (-1)^{r'} \times (\pm 1) \times (-1)^{r'-1} \times ((r'-1)!) \ (mod\ p).$$

Comme $e \geq 2$, on a $rf \leq \frac{n}{2}$, donc :

$$\left| f^{r-1} \times (-1)^r \times (\pm 1) \times (-1)^{r-1} \times ((r-1)!) \right| = f^{r-1}(r-1)!$$

$$= f^{r-1} \times 1 \times 2 \times ... \times (r-1) \leq f^{r-1} \times (\frac{1+(r-1)}{2})^{r-1}$$

$$= (\frac{rf}{2})^{r-1} \leq (\frac{n}{4})^{r-1} \leq (\frac{n}{4})^{\frac{n}{2}-1}.$$

De même, on a :

$$\left| f'^{r'-1} \times (-1)^{r'} \times (\pm 1) \times (-1)^{r'-1} \times ((r'-1)!) \right| = f'^{r'-1}(r'-1)! \leq (\frac{n}{4})^{\frac{n}{2}-1}.$$

L'hypothèse sur p implique alors l'égalité :

$$f^{r-1}(r-1)! = f'^{r'-1}(r'-1)! \tag{5.11}$$

On suppose $f' \leq f$. Alors, $r \leq r'$. Par conséquent, en simplifiant dans (5.11) par division des deux membres par $(r-1)!$, on voit que $f'^{r'-1}$ divise f^{r-1}, donc que f' divise f.
Montrons qu'en fait, pour tout diviseur premier éventuel q de f', on a $v_q(f') = v_q(f)$. En effet, si q est un nombre premier divisant f', posons $v_q(f') = t$ et montrons que $v_q(f) = t$. Par l'absurde, si tel n'était pas le cas, comme f' divise f, on aurait $v_q(f) > t$. Donc
$v_q(2(rf - r'f')) \geq t$ tandis que $v_q(\frac{f'}{rad(f')}) = t-1$, $v_q(\frac{f}{rad(f)}) \geq t$ et donc
$v_q(\frac{f}{rad(f)} - \frac{f'}{rad(f')}) = t-1$, ce qui contredit (5.10).
Montrons à présent que l'on a forcément $r = r'$ et $f = f'$.

On distinguera deux sous-cas : $f' > 1$ et $f' = 1$.

$\underline{f' > 1}$

Supposons $r < r'$. Soit q un diviseur premier de f'. On aurait :

$$v_q(f^{r-1} \times (r-1)!) = v_q(f^{r-1}) + v_q((r-1)!) = (r-1)v_q(f) + v_q((r-1)!)$$

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

Ce qui contredit (5.11). Donc $r = r'$ et par suite $f = f'$.

$\underline{f' = 1}$

Dans ce cas, (5.10) devient :

$$\frac{f}{rad(f)} - 1 = 2(rf - r'). \tag{5.12}$$

De même, (5.11) devient :

$$f^{r-1}(r-1)! = (r'-1)!. \tag{5.13}$$

On déduit de (5.12) que $\dfrac{f}{rad(f)}$ est impair. f n'est donc pas multiple de 4.
On raisonne par rapport à r.

a) Si $r > 1$

En divisant les deux membres de (5.13) par $(r-1)!$, on obtient :

$$\begin{cases} f^{r-1} = 1 & \text{si } r = r' \\ f^{r-1} = r \times ... \times (r'-1) & \text{si } r < r' \end{cases}. \tag{5.14}$$

Montrons que la situation ($r < r'$ et $f^{r-1} = r \times ... \times (r'-1)$) ne peut avoir lieu.

En effet, on a deux situations.

Ou bien $r = 2$ et alors $f = (r'-1)!$. Par conséquent, $r' - 1 < 4$ car sinon f serait multiple de 4. Donc $r' = 3$ ou 4. Dans les deux cas, cela contredit (5.12).

Ou bien $r \geq 3$ et dans ce cas, d'après le lemme précédent, $r' = r + 1$ et $f^{r-1} = r$. Donc

$f \neq 1$. *Soit* q un nombre premier divisant f. On a alors $v_q(f^{r-1}) = (r-1)v_q(f) \geq r-1$ tandis que $v_q(r) \leq \frac{r}{q} < r-1$.

b) Si $r = 1$

(5.13) devient $f^0 \times 0! = (r'-1)!$ d'où $r' = 1$ ou 2.

Si $r' = 1$, (5.12) donne $2(f-1) = \frac{f}{rad(f)} - 1$ c'est-à-dire $f(2 - \frac{1}{rad(f)}) = 1$ d'où $f = 1$.

Si $r' = 2$, (5.12) donne $2(f-2) = \frac{f}{rad(f)} - 1$ c'est-à-dire $f(2 - \frac{1}{rad(f)}) = 3$ ce qui est impossible.

Conclusion : Si e et e' sont ≥ 2, les équations (5.12) et (5.13) impliquent $f = f'$ et $r = r'$.

Cas 2 : $e = e' = 1$

Dans ce cas, l'égalité $\mu_K(p) = \mu_{K'}(p)$ entraîne :

$$f^r A_r^{N_p(f)} = f'^{r'} A_{r'}^{N_p(f')}. \tag{5.15}$$

Comme dans le cas 1, en égalisant les valuations p-adiques des deux membres de (5.15) puis les restes modulo p après les avoir divisés par la plus grande puissance de p les divisant, on obtient les équations :

$$\frac{f}{rad(f)} = \frac{f'}{rad(f')} \tag{5.16}$$

$$f^{r-1}(r-1)! = f'^{r'-1}(r'-1)!. \tag{5.17}$$

On va montrer que forcément $r = r'$ (ce qui entrainerait $f = f'$).

Par l'absurde, supposons $r < r'$. Par division par $(r-1)!$ des deux membres de (5.17), on obtient :

$$f^{r-1} = f'^{r'-1}\frac{(r'-1)!}{(r-1)!}. \tag{5.18}$$

Mais $\frac{(r'-1)!}{(r-1)!}$ vaut 1 si $(r, r') = (1, 2)$ et vaut $r \times ... \times (r'-1)$ dans tous les autres cas.

Si $(r, r') = (1, 2)$, l'égalité (5.18) donne $1 = f'$. Donc $n = 2$, ce qui est exclu par hypothèse.

Si $(r, r') \neq (1, 2)$, l'égalité (5.18) entraîne :

$$f^{r-1} = f'^{r'-1} \times r \times ... \times (r' - 1). \tag{5.19}$$

r ne peut valoir 1 car alors r' vaudrait au moins 3 et on aurait
$1 = f'^{r'-1} \times (r' - 1)! \geq f'^{r'-1} \times 2!$ ce qui serait absurde. Donc $r \geq 2$. On en déduit que $f'^{r'-1}$ divise f^{r-1} donc que f' divise f.
Comme précédemment, on montre que si un nombre premier q divise f', alors $v_q(f) = v_q(f')$. En effet, si $v_q(f') = t < v_q(f)$, alors $v_q(\frac{f'}{rad(f')}) = t - 1$ tandis que $v_q(\frac{f}{rad(f)}) \geq t$ ce qui contredit (5.16).
Raisonnons alors selon les valeurs de f'. Si $f' \neq 1$, soit q un nombre premier divisant f', on a :

$$v_q(f^{r-1}) = (r - 1)v_q(f) = (r - 1)v_q(f')$$

$$< (r' - 1)v_q(f') = v_q(f'^{r'-1}) \leq v_q(f'^{r'-1} \times r \times ... \times (r' - 1)).$$

ce qui contredit (5.19).
Si $f' = 1$, comme $e = e' = 1$, on a alors $rf = r'$. D'autre part, (5.19) implique : $f^{r-1} = r \times ... \times (r' - 1)$. On sait que $r \geq 2$.
Si $r > 2$, d'après [13] on a forcément $r' - 1 = r$ d'où $r' = r + 1$, donc $f^{r-1} = r$. L'entier f étant différent de 1, en considérant un nombre premier q divisant f, on aboutit à une absurdité car alors

$$v_q(f^{r-1}) = (r - 1)v_q(f) \geq r - 1 > \frac{r}{q} \geq v_q(r).$$

Si $r = 2$, alors $r' = 2f$ et en même temps $f = 2 \times ... \times (r' - 1)$ ce qui est impossible.
Conclusion : si $e = e' = 1$, alors $r = r'$ et $f = f'$.

Cas 3 : $e = 1, e' \geq 2$

On obtient les deux égalités suivantes :

$$\frac{f}{rad(f)} = \frac{f'}{rad(f')} + r'f'(e'-2) \tag{5.20}$$

$$f^{r-1}(r-1)! = f'^{r'-1}(r'-1)!. \tag{5.21}$$

Nous allons aboutir à une absurdité.

Supposons $r = r'$. Alors, $f = e'f'$ d'où, en simplifiant dans (5.21), on obtient $f^{r-1} = f'^{r-1}$ ou encore $(e'f')^{r-1} = f'^{r-1}$ et finalement $e'^{r-1} = 1$. Mais comme $e' > 1$, alors $r = r' = 1$. L'égalité (5.20) devient alors :

$$\frac{f}{rad(f)} = \frac{f'}{rad(f')} + f'(e'-2). \tag{5.22}$$

Nous allons d'abord montrer que e' et f' sont forcément premiers entre eux. En effet, si q est un nombre premier divisant e' et f', alors, $v_q(f) = v_q(e'f') = v_q(e') + v_q(f') > v_q(f')$. Mais, $v_q(\frac{f}{rad(f)}) = v_q(f) - 1$ (dans ce cas), donc $v_q(\frac{f}{rad(f)}) \geq v_q(f')$.

D'un autre côté, $v_q(\frac{f'}{rad(f')}) < v_q(f'(e'-2))$ donc

$v_q(\frac{f'}{rad(f')} + f'(e'-2)) = v_q(\frac{f'}{rad(f')}) < v_q(f') \leq v_q(\frac{f}{rad(f)})$ et l'égalité (5.22) serait fausse.

A partir de là, l'égalité $\mu_K(p) = \mu_{K'}(p)$ équivaut à :

$$fN_p(f) = (p^{f'} - 1)p^{f'(e'-2)}f'N_p(f'). \tag{5.23}$$

Mais,

$$fN_p(f) = \sum_{d|f} \mu(\frac{f}{d})p^d = \sum_{d|f'} \mu(\frac{f}{d})p^d + \sum_{d|f, d\nmid f'} \mu(\frac{f}{d})p^d$$

$$= \sum_{d|f'} \mu(e')\mu(\frac{f'}{d})p^d + \sum_{d|f, d\nmid f'} \mu(\frac{f}{d})p^d = \mu(e')f'N_p(f') + \sum_{d|f, d\nmid f'} \mu(\frac{f}{d})p^d.$$

Calculons à présent $\sum_{d|f, d\nmid f'} \mu(\frac{f}{d})p^d$.

Tout d divisant f sans diviser f' peut s'écrire $d = d'd''$ où d' est un diviseur de e' autre que 1 et d'' un diviseur quelconque de f'. Donc,

$$\sum_{d|f,d\nmid f'} \mu(\frac{f}{d})p^d = \sum_{1\neq d'|e',d''|f'} \mu(\frac{e'}{d'})\mu(\frac{f'}{d''})p^{d'd''}. \tag{5.24}$$

Pour égaliser les valuations p-adiques dans (5.23), on a besoin d'expliciter celle de

$$\sum_{1\neq d'|e',d''|f'} \mu(\frac{e'}{d'})\mu(\frac{f'}{d''})p^{d'd''}.$$

C'est la plus petite valeur du produit $d'd''$ pour laquelle on a $\mu(\frac{e'}{d'})\mu(\frac{f'}{d''}) \neq 0$. Cette plus petite valeur est obtenue pour $d'' = \dfrac{f'}{rad(f')}$ et $d' = \dfrac{e'}{rad(e')}$ si e' admet un facteur carré et $d' = \dfrac{e'}{rad(e')} \times q = q$ où q est le plus petit nombre premier divisant e' sinon. En clair,

$$v_p(\sum_{1\neq d'|e',d''|f'} \mu(\frac{e'}{d'})\mu(\frac{f'}{d''})p^{d'd''})$$

$$= \begin{cases} \dfrac{f'}{rad(f')}\dfrac{e'}{rad(e')} = \dfrac{f}{rad(f)} & \text{si } e' \text{ possède un facteur carré} \\ \dfrac{f'}{rad(f')} \times q = \dfrac{f}{rad(f)} \times q & \text{sinon} \end{cases}.$$

Egalisons à présent les valuations p-adiques des deux membres de (5.23)
On a

$$v_p((p^{f'}-1)p^{f'(e'-2)}f'N_p(f')) = f'(e'-2) + \frac{f'}{rad(f')}$$

tandis que

$$v_p(fN_p(f)) = v_p(\mu(e')f'N_p(f') + \sum_{d|f,d\nmid f'} \mu(\frac{f}{d})p^d).$$

Nous distinguons les deux cas : e' sans facteur carré et e' avec un facteur carré.
1er cas : e' est sans facteur carré.

Dans ce cas,

$$v_p((\mu(e')f'N_p(f')) = v_p(f'N_p(f')) = \frac{f'}{rad(f')} \tag{5.25}$$

et

$$v_p(\sum_{d|f,d\nmid f'} \mu(\frac{f}{d})p^d) = \frac{f}{rad(f)} \times q > \frac{f'}{rad(f')}.$$

Par conséquent, $v_p(fN_p(f)) = \frac{f'}{rad(f')}$.
L'égalisation des valuations p-adiques des deux membres de l'égalité (5.23) implique donc : $\frac{f'}{rad(f')} = \frac{f'}{rad(f')} + f'(e'-2)$ ce qui nécessite que $e' = 2$. Mais alors, $f = 2f'$ et l'égalité (5.23) devient :

$$fN_p(f) = \mu(e')f'N_p(f') + \sum_{d|f'}\mu(\frac{f}{2d})p^{2d}$$

$$= -f'N_p(f') + \sum_{d|f'}\mu(\frac{f'}{d})p^{2d} = (p^{f'}-1)f'N_p(f').$$

D'où, en simplifiant,

$$\sum_{d|f'}\mu(\frac{f'}{d})p^{2d} = p^{f'}f'N_p(f')$$

Or,

$$v_p(\sum_{d|f'}\mu(\frac{f'}{d})p^{2d}) = 2\frac{f'}{rad(f')} \neq f' + \frac{f'}{rad(f')} = v_p(p^{f'}f'N_p(f'))$$

(car $rad(f') \neq 1$ puisque $f' \neq 1$). Donc l'hypothèse selon laquelle $\mu_K(p)$ et $\mu_{K'}(p)$ seraient égaux est fausse.

2ème cas : e' admet un facteur carré.

En égalisant les valuations p-adiques des deux membres de (5.23) cela donne :

$$\frac{f}{rad(f)} = \frac{f'}{rad(f')} + f'(e' - 2). \tag{5.26}$$

Mais, e' admettant un facteur carré (autre que 1), on a forcément $e' \geq 4$ d'où $e' - 2 \geq \frac{e'}{2}$. On a alors :

$$\frac{f}{2} \geq \frac{f}{rad(f)} = \frac{f'}{rad(f')} + f'(e' - 2) \geq \frac{f'}{rad(f')} + \frac{f'e'}{2} > \frac{f'e'}{2} = \frac{n}{2}$$

ce qui implique $f > n$ et qui est absurde. ■

Bibliographie

[1] S. Arno, M. L. Robinson, and F. S. Wheeler, On Denominators of Algebraic Numbers and Integer Polynomials, J. Number theory 57 (1996), 292-302.

[2] M. Ayad, A. Bayad, O. Kihel, Denominators of algebraic numbers in a number field, Inter. J. Number Theory 149, (2015), 1-14.

[3] M. Ayad, A. Bayad, O. Kihel, Common divisors of the values of polynomials and denominators in a number field, preprint.

[4] M. Ayad, R. Bouchenna, O. Kihel, Indices in a number field, Journal de Théorie des Nombres de Bordeaux, à paraitre.

[5] M. Ayad, O. Kihel, Common Divisors of values of Polynomials and Common Factors of Indices in a Number Field, J. Number Theory 7, (2011), 1173-1194.

[6] M. Ayad, O. Kihel, Indices des entiers dans les corps de nombres, preprint.

[7] N. Bauer, Uber den aussewescentlicher Discriminantenteiler algebraischer Korper, Math. Ann. 64, (1907), 573.

[8] N. Bourbaki, Eléments de Mathématiques, Chapitre 5 (Corps commutatifs), troisième édition, (1973).

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

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

[11] I. Del Corso, Factorization of prime ideal extensions in a number rings, Math. of Computations, 58, (1992), 849-853.

[12] H. T. Engstrom, On the common index divisors of an algebraic field, Trans. A. M. S. 32, (1930), 223-237.

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

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

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

[16] H. Hancock, Foundations of the Theory of Algebraic Numbers, Vol. 2, Dover Pub. (1964).

[17] K. Hensel, Theorie der algebraischen Zahlen, Leipzig, (1908).

[18] K. Hensel, Arithmetische Untersuchungen uber die gemeinsamen ausserwesentlichen Diskriminantenteiler einer Gattung. Journ. f. Math. Bd. 113, (1894).

[19] S. K. Khandudja, M. Kumar, On a theorem of Dedekind, Int. J. Number Theory 4, (2008), 1019-1025.

[20] S. K. Khandudja, M. Kumar, Prolongation of valuations to finite extensions, Manus. Math. 131, (2010), 323-334.

[21] F. Levi, Kubische Zahlkorper und binare kubische Formenklassen, Berichte d. Sachsischen Ges. d. Wiss.,Math. Phys. Klasse, Bd. 66, Leipzig (1914).

[22] D. A. Marcus, Number Fields, Springer Verlag, New-York, (1977).

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

[24] T. Nagell, Quelques résultats sur les diviseurs fixes de l'index des nombres entiers d'un corps algébrique, Arkiv for Mat. 6, (1965).

[25] J. E. Nymann, On the probability that k positive integers are relatively prime, J. Number Theory 4 (1972), 469-473.

[26] O. Ore, Uber der Zusammenhang zwischen dendefinienderenden Gleichungen und der idealtheorie in algebraischen Korper, Math. Ann. 96 (1926), 313-352.

[27] G. Pólya, G. Szegő, Problems and Theorems in Analysis II, Springer-Verlag, New York, (1976).

[28] P. Samuel, Théorie algébrique des nombres, Hermann, Paris, (1971).

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

[30] B. K. Spearman, K. S. Williams, The index of a Cyclic Quartic field, Monatsh. Math. 140, (2003), 19-70.

[31] J. Varmon, Uber Abelsche Korper, deren alle Gruppeninvarianten aus einer Primzahl l bestehen und uber Abelsche Korper als Kreiskorper. Akademische Abhandlung. Lund (1925).

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