# THÈSE

**présentée à**

L'UNIVERSITÉ DES SCIENCES ET TECHNOLOGIES DE LILLE

**pour obtenir**

LE TITRE DE DOCTEUR DE L'UNIVERSITÉ

SPÉCIALITÉ : MATHÉMATIQUES PURES

par

**LO Nassirou**



## Etude du Niveau de Certains Corps

*Soutenue le : 26 Mars 1998 devant la Commission d'Examen :*

| | | | |
|---|---|---|---|
| Président du Jury | : | Professeur Jean Claude Douai | Université de Lille I. |
| Rapporteurs | : | Professeur Jean-Pierre Tignol | Université de Louvain-La-Neuve en Belgique. |
| | | Professeur David W. Lewis | Université de Belfield en Ireland. |
| Examinateurs | : | Professeur Pasquale Mammone | Université de Lens. |
| | | Maître de conférence Jérôme Burési | Université de Lens. |
| Directeur de thèse | : | Professeur Nicole Zinn-Justin | Université de Lille I. |

# Etude du Niveau de Certains Corps

LO Nassirou

A mes parents , ma famille...

# Table des matières


**1 Introduction** 6
- 1.1 Historique . . . 6
- 1.2 Etude du niveau de certains corps . . . 6
- 1.3 Remerciements . . . 7

**2 Etude du niveau d'extensions quartiques sur $\mathbb{Q}$ de polynôme minimal $X^4 + d$ , où $d \in \mathbb{Z}^*$.** 9
- 2.1 Introduction . . . 9
- 2.2 Résultat principal . . . 14

**3 Etude du niveau d'un corps de nombre $\mathbb{Q}(\alpha)$ dont le polynôme minimal de $\alpha$ sur $\mathbb{Q}$ est de la forme $X^n + d$ , où $d \in \mathbb{Q}$ et $n \in N^*$.** 17
- 3.1 introduction . . . 17
- 3.2 Résultat principal . . . 19

**4 Etude du niveau d'un corps de nombre $\mathbb{Q}(\alpha)$ dont le polynôme minimal de $\alpha$ sur $\mathbb{Q}$ est de la forme $X^4+aX^2+b$, où $a$ , $b \in \mathbb{Z}^*$.** 23
- 4.1 Résultat principal . . . 23

**5 Etude du niveau de $\mathbb{Q}_2(\xi_n)$ où $\xi_n$ est une racine primitive $n^{ième}$ de l'unité.** 32
- 5.1 Préliminaire . . . 32
- 5.2 Résultat principal . . . 33

**6 Etude du niveau de $\mathbb{Q}_p(\xi_n)$ , p premier impair où $\xi_n$ est une racine primitive $n^{ème}$ de l'unité.** 35
- 6.1 Contre-exemple . . . 36

**7 Etude du Niveau d'Extensions Kümmériennes** 39
- 7.1 Introduction . . . 39
- 7.2 Etude du niveau des extensions kümmériennes . . . 40

**8 Appendice** **42**

8.1 Algorithme pour déterminer l'ordre de la classe de 2 dans $(\mathbb{Z}/p\,\mathbb{Z})^*$ où $p \equiv 1 \bmod 8$. . . . . 42

8.2 Algorithme et Résultats pour $p \leq 30000$. . . . . 46

# Chapitre 1

# 1 Introduction

## 1.1 Historique

Les grecs s'intéressaient déjà à la notion de quantité proportionnelle dans leurs considérations géométriques (Théorème de Thalès , etc...). A cette époque où la philosophie imposait à l'homme l'idée d'une nature ordonnée et *rationnelle* dans sa structure profonde , on admettait mal que la longueur de l'hypoténuse d'un triangle rectangle déssiné sur le sable ne soit pas toujours un nombre rationnel. Pourtant le théorème de Pythagore est formel ! Cette idée que l'on ne puisse pas "attraper" certaines quantités "naturelles" par simple opérations arithmétiques sur $\mathbb{Q}$ est à relier à la notion de somme de carrés ( $x^2 + y^2 = z^2$ , intersections de cercles et de droites ). Dès lors beaucoup de mathématiciens se sont intéressés à étudier les quantités qui peuvent être obtenues comme somme de carrés dans un ensemble où ceci a un sens. Ce problème bien qu'étant facilement compréhensible est loin d'être facile , puisqu'il subsiste de nombreuses questions auxquelles on n'a pas encore de réponse. De très élégants et étonnants résultats ont étés obtenus par Albert Pfister sur l'identité des produits de $2^n$ carrés d'un corps K et le niveau d'un corps K.

## 1.2 Etude du niveau de certains corps

Les résultats généraux sur le niveau de corps de nombres sont obtenus vers les années 70 par un certain nombre d'auteurs. Cependant certains problèmes subsistent et nécéssitent un travail spécifique même pour obtenir certains résultats à partir de ce qui est déjà élaboré. Le but de cette thèse est d'essayer d'élucider certaines questions qui se posent à ce niveau. On sait depuis Pfister que le niveau d'un corps commutatif s'il est fini est une puissance de 2. Et le niveau d'un corps de nombre s'il est fini est 1,2 ou 4. Cependant la determination effective du niveau d'un corps quelconque pose problème. Dans la première partie de cette thèse on étudie le niveau

d'extensions quartiques ($[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$) , $\alpha \in \mathbb{C}$ où le polynôme minimal de $\alpha$ est de la forme $X^4 + d$ , $d \in \mathbb{Z}$. Dans la deuxième partie on détermine le niveau du corps de nombres K= $\mathbb{Q}(\alpha)$ où $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$ , $\alpha \in \mathbb{C}$ et le polynôme minimal de $\alpha$ est de la forme $X^n + d$ , où $d \in \mathbb{Q}$ et $n \in \mathbb{N}^*$. Dans la troisième partie on étudie le niveau d'un corps de nombre $\mathbb{Q}(\alpha)$ dont le polynôme minimal de $\alpha$ sur $\mathbb{Q}$ est de la forme $X^4 + aX^2 + b$, où $a$ , $b \in \mathbb{Z}^*$ . Ce qui généralise bien les théorèmes sur le niveau d'extensions quadratiques et quartiques. Dans la quatrième partie , on montre que si n est un entier ($n \geq 3$) que le niveau de $\mathbb{Q}_2(\xi_n)$ , où $\xi_n$ est une racine primitive $n^{ième}$ de l'unité dans une clôture algébrique $\overline{\mathbb{Q}_2}$ de $\mathbb{Q}_2$ est le même que celui du corps $\mathbb{Q}(e^{2i\pi/n})$. Mais le niveau de $\mathbb{Q}(e^{2i\pi/n})$ est bien connu à part le fait qu'il subsiste un problème quand n est premier congru à 1 modulo 8 cf.[11]. On donne ici en appendice un algorithme et le résultat obtenu à l'exécution (pour $p \leq 30000$ , mais en réalité le programme peut aller jusqu'à $p \leq 64000$ et une légère amélioration de ce programme permet d'aller jusqu'à $10^{31}$ ) qui donne l'ordre de la classe de 2 dans ( $\mathbb{Z}/p\,\mathbb{Z})^*$ pour $p \equiv 1 \bmod 8$ , p premier. L'avantage de cet algorithme réside sur le fait qu'on ne manipule que des nombres $\leq p$ alors que si on travaille directement avec des puissances de 2 on dépasse facilement p. La cinquième partie est consacrée à l'étude du niveau de $\mathbb{Q}_p(\xi_n)$ où p est un nombre premier impair et $\xi_n$ une racine primitive $n^{ième}$ de l'unité dans une clôture algébrique de $\mathbb{Q}_p$. On termine en donnant quelques résultats sur le niveau d'extension kümmérienne de $\mathbb{Q}(e^{\frac{2i\pi}{n}})$.

En guise de conclusion on peut dire que ce travail montre les difficultés auxquelles on est conffronté quand on étudie le niveau d'un corps de nombres. Pour les corps de nombres qui sont une extension galoisienne de $\mathbb{Q}$ ou une extension dont le polynôme minimal d'un élément primitif est résoluble par radicaux , on sait théoriquement trouver leurs niveaux avec un nombre fin d'opérations ( bien que ceci peut être très long et très compliqué ) . Par contre ce à quoi cette étude ne répond pas vraiment c'est quand l'extension n'est pas galoisienne et le polynôme minimal d'un élément primitif de l'extension n'est pas résoluble par radicaux .

## 1.3 Remerciements

Je voudrais bien remercier l'ensemble des membres du jury pour avoir

accepté de participer à la soutenance de ma thèse. Plus spécialement Jean Pierre Tignol et à David W. Lewis.
Je remercie particulièrement mon professeur en D.E.A. Pasquale Mammone de m'avoir demandé de répondre à certaines questions de David W. Lewis. Il a suivi mes travaux dans ces moindres détails. Qu'il trouve ici ma profonde gratitude. Je remercie également Jean Claude Douai , un professeur particulièrement remarquable ici à Lille I. Il m'a beaucoup apporté en voulant répondre à beaucoup de mes questions au moment où j'étais perdu dans les séminaires , ou bloqué dans mes recherches. Je remercie Jérôme Burési , Maître de conférence à l'Université de Lens , pour ces informations concernant les séminaires de Lens , il a suivi lui aussi mes travaux et ces suggestions ont été très fructueuses. Je remercie également le collègue Frédéric Guilbert , Informaticien Maître de conférence à la Faculté Libre des Sciences à l'Institut Catholique de Lille , qui m'a aidé à élaborer l'algorithme et la programmation à la fin de cette thèse , qu'il trouve ici ma profonde gratitude.

C'est en licence de mathématiques à l'option Algèbre et théorie des nombres que j'ai renconté pour la premiére fois le professeur Nicole Zinn-Justin. J'ai été tout de suite surpris par sa rapidité , sa lucidité , sa facilité et clarté d'exposé ( Qui démontre tout sans rien négliger ). Mon ami David Roussel actuellement professeur agrégé à l'université de Lens et moi même n'hésitions pas dans nos conversations d'étudiant à citer Nicole Zinn-Justin parmi les meilleurs professeurs ici à Lille I. C'est pourquoi David et moi n'avions pas hésité à suivre son cours de D.E.A. et de choisir sa spécialité comme sujet de recherche. On imagine facilement la chance et l'immence joie que j'ai eu en la retrouvant comme directeur de recherche. D'un niveau d'humanisme incomparable , toujours prête à m'écouter et à me soutenir , elle était là quand tout allait bien et surtout quand tout n'allait pas forcément bien ! C'est à son contact que j'ai appris le métier de la recherche. Je lui dois plus que les connaisances qu'elle m'a transmises , mais ces quelques lignes ne suffiraient pas à lui exprimer toute ma reconnaissance. Merci pour celle sans qui tout ceci n'aurait jamais vu le jour. Merci pour ses conseils ses renseignements et sa connaissance qu'elle m'a apportés. Merci à vous Nicole Zinn-Justin.

# Chapitre 2

## 2 Etude du niveau d'extensions quartiques sur $\mathbb{Q}$ de polynôme minimal $X^4 + d$ , où $d \in \mathbb{Z}^*$.

### 2.1 Introduction

Tout au long de ce chapitre $\mathbb{Q}_p$ désigne le complété p-adique de $\mathbb{Q}$ , où p est premier.

**Définition 2.1**
*Soit K un corps. Le niveau noté s(K) de K est le plus petit des entiers naturels n tels que -1 est somme de n carrés dans K. Si -1 n'est pas somme de carrés dans K , alors on pose par convention $s(K) = \infty$ , et on dit que K est formellement réel. Un corps non formellement réel est dit totalement complexe. Un corps contenu dans $\mathbb{R}$ est appelé corps réel. Il est évidemment de niveau infini.*

Nous allons rappeler quelques résultats qui seront utilisés par la suite.

**Théorème 2.1 (Pfister)** , [19] , *p 41.*
*Soit $L = K(\alpha)$ une extension algèbrique de corps et $P(X) = min(\alpha, K)$.On suppose que L n'est pas formellement réel (i.e totalement complexe) alors :-1 est somme de $2^{n-1}$ carrés dans L si et seulement si $P(X)$ est somme de $2^n$ carrés dans $K[X]$.*

**Corollaire 2.1**
*Soit K un corps , $L = K(\alpha)$ , $\alpha$ appartenant à une clôture algèbrique de K. Soit $\beta$ un conjugué de $\alpha$ et $L_1 = K(\beta)$ alors $s(L) = s(L_1)$.*

Démonstration
C'est une conséquence immédiate du théorème de Pfister , car -1 est somme

de $2^{n-1}$carrés dans L si et seulement si P est somme de $2^n$ carrés dans K(X) ce qui équivaut à -1 est somme de $2^{n-1}$ carrés dans $L_1$.On peut aussi remarquer que L est K-isomorphe à $L_1$ , ce qui signifie qu'ils ont même niveau.

**Théorème 2.2 (Springer)** , [19] , *p.42.*
*Soit L une extension du corps K avec* $[L : K] = n$ *impair*
*alors* $s(L) = s(K)$. *En particulier si* $K = \mathbb{Q}$ *et si L est une extension finie de* $\mathbb{Q}$ *de degré impair , alors* $s(L) = \infty$.

**Remarque 2.1**
Il existe des corps de nombres qui ne sont pas réels (de degré pair ou impair sur $\mathbb{Q}$) et de niveau infini (i.e formellement réels).
Pour $K = \mathbb{Q}(\sqrt{3}, \sqrt[3]{3}e^{2i\pi/3})$ , les polynômes $X^2-3$ et $X^3-3$ sont irréductibles sur $\mathbb{Q}$ comme leurs degrés sont premiers entre eux donc ce dernier polynôme est irréductible sur $\mathbb{Q}(\sqrt{3})$ qui est un corps réel. K est ainsi un corps non réel de degré pair sur $\mathbb{Q}$ et de niveau infini.

**Proposition 2.1**
*Soit K un corps ,* $d \in K^*$ *une somme de n carrés et non de n-1 carrés de K. Choisissons* $k \in \mathbb{N}$ *tel que :* $2^k \leq n < 2^{k+1}$ *et si un tel entier n n'existe pas on pose par convention que* $k = \infty$ *et* $2^k = \infty$ *alors :*
$s(K(\sqrt{-d})) = min(s(K), 2^k)$.

Démonstration
Si $s(K(\sqrt{-d})) = 2^h$ où $h \in \mathbb{N}$ fini alors :
Comme $s(K(\sqrt{-d})) \leq s(K)$ il suffit de prouver que si $s(K(\sqrt{-d})) < s(K)$ alors $h = k$ ; en effet $-(\sqrt{-d})^2 = d = d_1^2 + d_2^2 + \cdots + d_n^2$ où $d_i \in K$ en divisant par $(\sqrt{-d})^2$ on obtient que -1 est somme de n carrés dans $K(\sqrt{-d})$ comme le niveau est une puissance de 2 , $s(K(\sqrt{-d})) = 2^h \leq 2^k$ et $h \leq k$ d'une part. Comme $s(K(\sqrt{-d}))$ est fini tout élément de $K(\sqrt{-d})$ est somme de $2^h + 1$ carrés dans lui-même. Comme $2^{h+1} \geq 2^h + 1$ , la forme $\varphi = (2^{h+1}) < 1 >$ est isotrope donc $0 = d_1^2 + d_2^2 + \cdots + d_{2^{h+1}}^2$ où $d_i \in K(\sqrt{-d})$, donc $\forall$ i , $1 \leq i \leq 2^{h+1}$ . Posons $d_i = x_i + y_i\sqrt{-d}$ avec $x_i$ , $y_i \in K$. D'où $0 = \sum_{i=1}^{2^{h+1}} x_i^2 - d\sum_{i=1}^{2^{h+1}} y_i^2$ et $\sum_{i=1}^{2^{h+1}} x_i y_i = 0$.
Si tous les $y_i$ sont nuls.
Donc tous les $x_i$ ne sont pas nuls et $\sum_{i=1}^{2^{h+1}} x_i^2 = 0$ , on en déduit que $s(K) \leq 2^{h+1} - 1$. Comme le niveau de K est une puissance de 2 , on a : $s(K) \leq 2^h$ , ce qui contredit notre hypothèse.

Donc tous les $y_i$ ne sont pas nuls et $\sum_{i=1}^{2^{h+1}} y_i^2 \neq 0$ puisque sinon on obtient la même contradiction. On peut alors écrire que :

$$d = \frac{(\sum_{i=1}^{2^{h+1}} x_i^2)(\sum_{i=1}^{2^{h+1}} y_i^2)}{(\sum_{i=1}^{2^{h+1}} y_i^2)^2}$$

Or $(\sum_{i=1}^{2^{h+1}} x_i^2)(\sum_{i=1}^{2^{h+1}} y_i^2) = \sum_{i=1}^{2^{h+1}} \gamma_i^2$ , avec $\gamma_i \in K$ et
$\gamma_1 = \sum_{i=1}^{2^{h+1}} x_i y_i = 0$. D'où d est somme de $2^{h+1} - 1$ carrés dans K. Vu la condution sur n , $2^{h+1} - 1 \geq n \geq 2^k$. On en déduit que $2^{h+1} - 1 > 2^k$ par suite $2^{h+1} \geq 2^{k+1}$ et $h \geq k$ d'autre part. Finalement on conclut que h=k.
Si $s(K(\sqrt{-d})) = \infty$ alors s(K)=$\infty$ et d ne peut pas être somme de carrés d'éléments de K d'après ce qu'on vient de voir. Donc $k = \infty$ et le résultat est encore vrai.

**Corollaire 2.2 (Résultat bien connu d'une extension quadratique)**

*Soit* $d \in \mathbb{Z}^*$ *avec* $[\mathbb{Q}(\sqrt{-d}) : \mathbb{Q}] = 2$ *on a :*
$s(\mathbb{Q}(\sqrt{-d})) = \infty \Longleftrightarrow d < 0.$
$s(\mathbb{Q}(\sqrt{-d})) = 1 \Longleftrightarrow d = e^2$ *où* $e \in \mathbb{Z}^*$.
*On suppose* $d \in \mathbb{N}^*$ , $d = 4^a b$ *où* $a, b \in \mathbb{N}$ *et b n'est ni divisible par 4 , ni un carré dans* $\mathbb{Z}$ *alors :*
$s(\mathbb{Q}(\sqrt{-d})) = 2 \Longleftrightarrow b \not\equiv 7 \bmod 8.$
$s(\mathbb{Q}(\sqrt{-d})) = 4 \Longleftrightarrow b \equiv 7 \bmod 8.$

Démontration ( cf.[19] , théorème 3.2 , page 31 ).
Les deux premières équivalences sont triviales. On sait que d ($d > 0$) est une somme de trois carrés dans $\mathbb{Q}$ si et seulement si d est somme de trois carrés dans $\mathbb{Z}$ ce qui équivaut à ( d'après le théorème de Gauss) d n'est pas de la forme $4^{a_0}(8b_0 - 1)$ , en utilisant la proposition2.1 précédente , on a $s(\mathbb{Q}(\sqrt{-d})) \leq 2$ si et seulement si d est somme de trois carrés de $\mathbb{Q}$ et le résultat s'ensuit. Pour plus de détails cf.[21] , p. 159. On peut remarquer aussi qu'on peut démontrer ce résultat avec la méthode qui est employée pour la démontration du théorème 2.3.

On utilise les lemmes suivants:

**Lemme 2.1 (Propriété universelle de $K(\xi)$.)**
*Soit $\xi$ un élément algébrique sur K,de polynôme minimal P et soit $\varphi : K \longrightarrow M$ un homomorphisme de corps de K. Pour qu'il existe un homomorphisme de corps $\psi : K(\xi) \longrightarrow M$ , prolongeant $\varphi$ ,il faut et il suffit que M contienne une racine de $\varphi(P)$ ,et alors $\psi(\xi)$ est une racine de $\varphi(P)$.Le choix de cette racine détermine $\psi$. Il y a autant de prolongements $\psi$ que de racines de $\varphi(P)$ dans M.*

Démonstration
La condition est nécessaire.
On remarque d'abord que tout morphisme d'anneaux $\varphi : A \longrightarrow B$ peut être prolongé en un homomorphisme d'anneaux noté encore $\varphi$ ,
$\varphi : A[X] \longrightarrow B[X]$ qui à $P = \sum_{i=0}^{n} a_i X^i$ un élément de A[X] , on associe $\varphi(P) = \sum_{i=0}^{n} \varphi(a_i) X^i$. Soit $\psi : K(\xi) \longrightarrow M$ un tel prolongement. Puisque $P(\xi) = 0$ , on a : $\psi(P(\xi)) = 0$ , mais $\psi(P(\xi)) = (\psi(P))(\psi(\xi)) = \varphi(P)(\psi(\xi))$.
La condition est suffisante.
Supposons $P = X^n + a_{n-1}X^{n-1} + \cdots + a_0$.
Alors $\varphi(P) = X^n + \varphi(a_{n-1})X^{n-1} + \cdots + \varphi(a_0)$. Soit r une racine de $\varphi(P)$ dans M. On définit $\psi : K(\xi) \longrightarrow M$ , par $\psi(\xi) = r$ et $\psi(a) = \varphi(a)$
si $a \in K$. Chaque élément u de $K(\xi)$ s'écrit de manière unique :
$u = b_{n-1}\xi^{n-1} + b_{n-2}\xi^{n-2} + \cdots + b_0$ , avec les $b_i \in K$.
Soit $B = b_{n-1}X^{n-1} + b_{n-2}X^{n-2} + \cdots + b_0$ , alors $B \in K[X]$ et
$B(\xi) = u$. Alors $\psi(u) = \varphi(b_{n-1})r^{n-1} + \varphi(b_{n-2})r^{n-2} + \cdots + \varphi(b_0) = \varphi(B)(r)$.
Soit v un autre él'ement de $K(\xi)$. $v = C(\xi)$ avec $C \in K[X]$ et
$degC < n$. On a $u + v = B(\xi) + C(\xi) = (B + V)(\xi)$ et $deg(B + C) < n$ ,
donc $\psi(u + v) = \varphi(B + C)(\xi) = (\varphi(B) + \varphi(C))(\xi) = \psi(u) + \psi(v)$.
Pour le produit , il faut trouver une forme normale de uv , car le degré de B.C peut être de degré $\geq$ n.
K[X] est euclidien on a : B.C=PQ+R , avec $degR < n$ ,
Q,R sont dans K[X].
$B.C(\xi) = B(\xi).C(\xi) = P(\xi)Q(\xi) + R(\xi) = R(\xi)$ , puisque $P(\xi) = 0$. Et $\varphi(B.C) = \varphi(P)\varphi(Q) + \varphi(R)$.
$(\varphi(B.C))(r) = \varphi(P)(r)\varphi(Q)(r) + \varphi(R)(r) = \varphi(R)(r)$ car $\varphi(P)(r) = 0$.
D'où $\psi(u.v) = \psi[R(\xi)] = \varphi(R)(r)$ et $\psi(u)\psi(v) = \varphi(B)(r).\varphi(C)(r) = \psi(u.v)$
donc $\psi$ est bien un K-homomorpisme et il est bien déterminé par r.

**Lemme 2.2**
*Soit* $K = \mathbb{Q}(\xi)$ *un corps de nombres totalement complexe.*
*Alors les propriétés suivantes sont équivalentes:*
*a)* $s(K) \leq 2$.
*b) L'algèbre de quaternion* $\left(\frac{-1,-1}{K}\right)$ *est isomorphe à l'algèbre de matrice* $\mathcal{M}_2(K)$.
*c)* $\forall \wp$ *idéal premier de l'anneau des entiers de K divisant 2 , et* $K_\wp$ *le complété* $\wp$*-adique de K.L'algébre de quaternion* $\left(\frac{-1,-1}{K_\wp}\right)$ *est isomorphe à* $\mathcal{M}_2(K_\wp)$.
*d)* $\forall \wp$ *idéal premier de l'anneau des entiers de K divisant 2 ,le degré* $[K_\wp : \mathbb{Q}_2]$ *est pair.*

Démonstration
L'équivalence de a) et b) découle du théorème 2.7 chap. 3 de [12] et du fait que $s(K) \leq 2$ est équivalent à la forme $\varphi =< 1,1,1,1 >$ est isotrope sur K. L'équivalence de b) et c) découle du principe de Hasse-Minkowski cf.théorème 3.7 chap.6 [12]. Enfin a) équivaut à d) cf. [2] théorème 1.

**Lemme 2.3**
*Soit* $K = \mathbb{Q}(\alpha)$ *un corps de nombres où le polynôme minimal P de* $\alpha$ *sur* $\mathbb{Q}$ *est de degré 4 , alors on a :* $s(K) \leq 2$ *si et seulement si P n'a pas de racine dans* $\mathbb{Q}_2$ *(complété 2-adique de* $\mathbb{Q}$ *).*

Démonstration
Si P a une racine dans $\mathbb{Q}_2$ , on a d'aprés le Lemme 1 un homomorphisme de corps $\Psi : \mathbb{Q}(\alpha) \longrightarrow \mathbb{Q}_2$ ,donc $\Psi$ est injectif.On en déduit que $\mathbb{Q}_2$ contient un sous corps F isomorphe à $\mathbb{Q}(\alpha)$. D'où $s(\mathbb{Q}(\alpha)) = s(F) \geq s(\mathbb{Q}_2) = 4$.
Si P n'a pas de racine dans $\mathbb{Q}_2$ ,alors on sait que $\alpha \in K_\wp$,$\forall \wp$ divisant 2. Soit $T = min(\alpha, \mathbb{Q}_2)$ , alors on a T divise P. Le degré de T n'est pas impair car sinon P=TR , et T ou R est de degré 1 i.e P aurait une racine dans $\mathbb{Q}_2$ ce qui est contraire à notre hypothèse. Donc le degré de T est pair et on en déduit que ,$\forall \wp$ divisant 2 : $[K_\wp : \mathbb{Q}_2] = [K_\wp : \mathbb{Q}_2(\alpha)][\mathbb{Q}_2(\alpha) : Q_2]$ est pair car $[\mathbb{Q}_2(\alpha) : Q_2] = degT$ est pair. Le résultat découle du Lemme 2.2.

**Corollaire 2.3**
*Soit* $K = \mathbb{Q}(\alpha), \alpha \in \mathbb{C}$ *où le polynôme minimal de* $\alpha$ *sur* $\mathbb{Q}$ *est de la forme* $X^4 + d, d \in \mathbb{Z}^*$. *Si* $d = -1 + 2^5 k$ *avec* $k \in \mathbb{N}^*$ *, alors* $s(K) = 4$.

Démonstration
En effet en posant $P = X^4 + d$ , on a en dérivant $P' = 4X^3$ , $P(1) = 2^5 k$ et

$|P(1)|_2 \leq \frac{1}{2^3} < |P'(1)|_2^2 = (\frac{1}{2^2})^2$ donc d'après le Lemme de Hensel cf.[4] , p.49. P a une racine dans $\mathbb{Q}_2$ et $s(K) = 4$ d'après le Lemme 2.3 puisque $s(K) = s(\mathbb{Q}(\sqrt{\sqrt{-d}}))$.

## 2.2 Résultat principal

**Théorème 2.3**
*Soit* $K = \mathbb{Q}(\alpha)$ *et* $P = min(\alpha, \mathbb{Q}) = X^4 + d$ *le polynôme minimal de* $\alpha$ *sur* $\mathbb{Q}$ ,$d \in \mathbb{Z}^*$ ,
*alors on a :* $s(K) = s(\mathbb{Q}(\sqrt{\sqrt{-d}}))$ ;( Deux corps conjugués ont même niveau ).
$s(K) = \infty \Longleftrightarrow d \in \mathbb{Z}^*_-$.
$s(K) = 1 \Longleftrightarrow d = e^2$ *où* $e \in \mathbb{Z}^*$.
*On suppose* $a, b \in \mathbb{N}^*$ , $d = 4^a b$ *où* $b$ *n'est ni un carré dans* $\mathbb{N}^*$ *ni divisible par 4 alors :*
$s(K) = 4 \Longleftrightarrow b \equiv$-*1mod 16 et a pair.*
$s(K) = 2 \Longleftrightarrow b \not\equiv$-*1mod 16 ou a impair.*

**Remarque 2.2**
Le dernier cas $s(K) = 2$ est décrit par :$b \not\equiv$-1 mod 8 ou $b = -1 + 8k$ avec k impair ou $b \equiv$ -1 mod 16 avec a impair.Et il n'a pas d'ambigüité à prendre $\alpha = \sqrt{\sqrt{-d}}$ , car deux corps conjugués ont même niveau et on rappelle que $\mathbb{Q}_2{}^* / \mathbb{Q}_2{}^{*2} = \{ 1 , 2 , 3 , 5 , 6 , 7 , 10 , 14 \}$ cf.[4] p.53 ou cf.[14] .

Démonstration
Supposons que $s(K) = \infty$ , si $d \in N^*$ alors $-1 = \underbrace{(\frac{1}{\alpha^2})^2 + \cdots + (\frac{1}{\alpha^2})^2}_{\text{d.fois}}$ ce qui est en contradiction avec notre hypothèse.
Réciproquement si $d < 0$ et $s(K) < \infty$ alors d'après le Théorème de Pfister comme $X^4 + d$ est somme de carrés dans K, P est somme de 8 carrés dans $\mathbb{Q}(X)$ ; en ne gardant que les termes constants , on a : d est somme de 8 carrés dans $\mathbb{Q}$ , donc $d \geq 0$ ,ce qui est en contradiction avec l'hypothèse. Ce qui montre que $s(K) = \infty$.
Supposons que $s(K) = 1$ i.e $i \in K$ , alors $i \notin \mathbb{Q}(\sqrt{-d})$ comme
$\mathbb{Q} \xrightarrow{2} \mathbb{Q}(\sqrt{-d}) \xrightarrow{2} \mathbb{Q}(\sqrt{-d})(i) \xrightarrow{2} K$
alors $\mathbb{Q}(\sqrt{-d})(i) = \mathbb{Q}(\alpha) = K$. Comme $\alpha^2 = \pm\sqrt{-d}$ en posant $\alpha = a_1 + b_1 i$ avec $a_1, b_1 \in \mathbb{Q}(\sqrt{-d})$ on a : $\alpha^2 = \pm\, \mathbb{Q}(\sqrt{-d}) = a_1^2 - b_1^2 + 2a_1 b_1 i \in \mathbb{Q}(\sqrt{-d})$

d'où $a_1^2 - b_1^2 = \pm\sqrt{-d}$ et $a_1 b_1 = 0$. Comme $b_1 \neq 0$ car sinon $a_1^2 = \alpha^2$ ce qui implique que $a_1 = \pm\alpha$ , ce qui est en contradiction avec $[K : \mathbb{Q}] = 4$.
D'où $a_1 = 0$.
$-b_1^2 = \pm\sqrt{-d} = \alpha^2$ ce qui implique en posant $b_1 = r + s\sqrt{-d}$ avec r et s appartenant à $\mathbb{Q}$. $-b_1^2 = -r^2 + ds^2 - 2rs\sqrt{-d} = \pm\sqrt{-d}$ équivaut à $r^2 - ds^2 = 0$ et $2rs = \pm 1$ ,par suite $-1 = \frac{\alpha^4}{d} = (\frac{\alpha^2}{(\frac{r}{s})})^2$ car $d = (\frac{r}{s})^2$ , ce qui est en contradiction avec $s(\mathbb{Q}(\sqrt{-d})) \neq 1$. La réciproque est évidente.
On suppose maintenant $d \in \mathbb{N}^*$ et d n'est pas un carré. On sait que le niveau de K est fini d'après ce qu'on vient de voir. On écrit $d = 4^a b$ où b n'est pas divisible par 4.
Donc si $b \not\equiv 7 \bmod 8$ alors $2 \geq s(\mathbb{Q}(\sqrt{-d})) \geq s(K) > 1 (car\ \mathbb{Q}(\sqrt{-d}) \subset K)$ et $s(K) = 2$.
Examinons le où $b \equiv$ -1 mod 8.
a) Si a est impair. On sait que $\mathbb{Q}(\sqrt{\sqrt{-d}}) = \mathbb{Q}(\sqrt{2\sqrt{-d}})$.Soit $c \in \mathbb{Z}_2$ tel que $c^2 = -b$ , $\mathbb{Z}_2$ est l'anneau de valuation de $\mathbb{Q}_2$. On a $|c|_2 = 1$. Alors :
$c = 1 + 2a_1 + 2^2 a_2 + 2^3 a_3 + 2^4 a_4 + 2^5 a_5 + 2^6 a_6 + 2^7 a_7 + \cdots + \cdots$ où $a_i \in \{0, 1\}$.
$c^2 = 1 + 2^3(a_2 + \frac{(a_1+1)a_1}{2}) + 2^4(a_3 + a_1 a_2 + a_2^2) + 2^5(a_4 + a_1 a_3) + 2^6(a_3^2 + a_5 + a_4 a_1 + a_2 a_3) + \cdots$
<u>cas 1</u> : $b \equiv$ -1 mod 8 et $b \not\equiv$ -1 mod 16.
$c^2 = -b = 1 - 8k$ , avec k impair , comme $-1 = 1 + 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + \cdots + \cdots$
$c^2 = 1 + 2^3 + 2^4 s$ où $s \in \mathbb{Z}_2$ , on a : ou bien $a_1 = 0$ et $a_2 = 1$ ou bien $a_1 = 1$ et $a_2 = 0$. $c = 5(1 + 8g)$ ou $c = 3(1 + 8h)$ où $g, h \in \mathbb{Z}_2$ comme 1+8g et 1+8h sont des carrés dans $\mathbb{Q}_2$ cf.[4] , p.53 , alors $\pm 2\sqrt{-b}$ n'est pas un carré dans $\mathbb{Q}_2$ ,d'où $s(K) = 2$.
<u>cas 2</u> : $b \equiv$-1 mod 16 et $b \not\equiv$-1mod 32. $c^2 = -b = 1 - 16k = 1 + 2^4 + 2^5 k_1$ où $k_1 \in \mathbb{Z}_2$, avec k impair. D'après ce qui précède , on a :
$a_1 = 0$ et $a_2 = 0$ ou bien $a_1 = 1$ et $a_2 = 1$ i.e c=1+8g ou bien c=7(1+8h) où $g, h \in \mathbb{Z}_2$.
On en déduit que , $\pm 2\sqrt{-b}$ n'est pas un carré dans $\mathbb{Q}_2$ , car ni $\pm 2$ , ni $\pm 14$ n'est un carré dans $\mathbb{Q}_2$ d'où $s(K) = 2$.
<u>cas 3</u> : $b \equiv$ -1 mod 32.
On sait que $P = X^4 + 4b = (X^2 + 2\sqrt{-b})(X^2 - 2\sqrt{-b})$ se factorise dans $\mathbb{Q}_2[X]$. Si P a une racine dans $\mathbb{Q}_2$ , alors 2 ou -2 est un carré dans $\mathbb{Q}_2$ car -b est un carré dans $\mathbb{Q}_2$. Ce qui est une contradiction. Donc P n'a pas de racine dans $\mathbb{Q}_2$ et $s(K) = 2$.
b) Si a est pair. Alors $s(K) = s(\mathbb{Q}(\sqrt{\sqrt{-b}}))$.

cas 1 : $b \equiv$ -1 mod 8 et $b \not\equiv$ -1 mod 16.
$c^2 = -b = 1-8k$ avec k impair comme $-1 = 1+2^1+2^2+2^3+2^4+2^5+\cdots+\cdots$
$c^2 = 1 + 2^3 + 2^4 s$ où $s \in \mathbb{Z}_2$ , on a ou bien $a_1 = 0$ et $a_2 = 1$ ou bien $a_1 = 1$ et $a_2 = 0$ i.e $c = 5(1 + 8g)$ ou $c = 3(1 + 8h)$ où $g, h \in \mathbb{Z}_2$ , comme 1+8g et 1+8h sont des carrés dans $\mathbb{Q}_2$ , $\pm\sqrt{-b}$ n'est pas un carré un carré dans $\mathbb{Q}_2$. Donc $s(K) = 2$ en utilisant le Lemme 2.3.
cas 2 : Si $b \equiv$ -1 mod 16 et $b \not\equiv$ -1 mod 32.
$c^2 = -b = 1 - 16k = 1 + 2^4 + 2^5 k_1$ où $k_1 \in Z_2$ , avec k impair. D'après ce qui précède ,on a :
$a_1 = 0$ et $a_2 = 0$ ou bien $a_1 = 1$ et $a_2 = 1$ i.e c=1+8g ou c=7(1+8h) où $g, h \in \mathbb{Z}_2$. On en déduit que , $\sqrt{-b}$ ou $-\sqrt{-b}$ est un carré dans $\mathbb{Q}_2$. Donc $s(K) = 4$.
cas 3 : Si b≡ -1 mod 32.
Le corollaire 2.3 permet de conclure que $s(K) = 4$.

**Exemple 2.1**
On sait que le polynôme $P = X^4 + 7$ est irréductible sur $\mathbb{Q}$ d'après le critère d'Eisenstein.
Soit $\alpha = \sqrt{\sqrt{-7}}$ une racine de P , $K = \mathbb{Q}(\alpha)$ ,on a $[K : \mathbb{Q}] = 4$ : on a $s(\mathbb{Q}(\sqrt{-7})) = 4$ car $7 \equiv 7$ mod 8.
Par contre $-\sqrt{-7} = (\frac{3}{2} - \frac{1}{2}\sqrt{-7})^2 + (\frac{1}{2} + \frac{1}{2}\sqrt{-7})^2 + 1^2$.
En effet $(\frac{3}{2})^2 + (\frac{1}{2})^2 + 1^2 - 7((\frac{1}{2})^2 + (\frac{1}{2})^2) - 2(\frac{3}{4} - \frac{1}{4})\sqrt{-7} = \frac{14}{4} - \frac{14}{4} - \sqrt{-7} = -\sqrt{-7}$.

$$-1 = (\frac{(\frac{3}{2} - \frac{1}{2}\sqrt{-7})}{\alpha})^2 + (\frac{(\frac{1}{2} + \frac{1}{2}\sqrt{-7})}{\alpha})^2 + (\frac{1}{\alpha})^2.$$

Or le niveau est une puissance de 2 , donc $s(K) = 2$ , car 7 n'est pas un carré dans $\mathbb{Q}$.
Cet exemple montre qu'on peut avoir $s(K) = 2$ , alors que $s(\mathbb{Q}(\sqrt{-d})) = 4$.

# Chapitre 3

## 3 Etude du niveau d'un corps de nombre $\mathbb{Q}(\alpha)$ dont le polynôme minimal de $\alpha$ sur $\mathbb{Q}$ est de la forme $X^n + d$ , où $d \in \mathbb{Q}$ et $n \in N^*$.

### 3.1 introduction

Tout au long de ce chapitre $\mathbb{Q}_2$ désigne le complété diadique de $\mathbb{Q}$ . Et $\mathbb{Z}_2$ désigne l'anneau de valuation de $\mathbb{Q}_2$. On sait que quand n est impair le théorème de Springer permet de dire que $s(\mathbb{Q}(\alpha)) = \infty$ , tout au long de ce chapitre on suppose n pair.

**Lemme 3.1**
*On suppose $b \in N^*$ , $b \equiv$-1mod $2^{n+1}$ où n est un entier naturel ($n \geq 2$). On pose $P_{2^n} = X^{2^n} + b$ , qu'on suppose irréductible sur $\mathbb{Q}$ et $\alpha$ une racine de $P_{2^n}$ dans $\mathbb{C}$ , $K = \mathbb{Q}(\alpha)$. Alors les propriétés suivantes sont équivalentes :*
*i) $s(K) \leq 2$.*
*ii) $P_{2^n}$ n'a pas de racine dans $\mathbb{Q}_2$.*
*iii) $b \not\equiv$ -1 mod $2^{n+2}$.*

Démonstration
On démontre ce lemme en procédant par récurrence sur n. Pour n=2 ce Lemme est vrai cf.théorème 2.3.
Supposons $n \geq 3$ et le lemme vrai au rang n-1.
i) $\Longrightarrow$ ii). Si $P_{2^n}$ a une racine dans $\mathbb{Q}_2$ alors K est isomorphe à un sous-corps de $\mathbb{Q}_2$ (d'après le lemme 2.1 ). On en déduit que $s(\mathbb{Q}_2) = 4 \leq s(K) \leq 4$ d'où s(K)=4.
ii) $\Longrightarrow$ iii). On suppose que b$\equiv$-1 mod $2^{n+2}$.
Posons $a = \sum_{i=0}^{\infty} 2^i a_i$ avec $a_i \in \{0,1\}$ et $a_0 = 1$. Alors on a :

$$a^2 = 1 + 2^3(a_2 + \frac{a_1(a_1+1)}{2}) + 2^4(a_2^2 + a_3 + a_1 a_2) + \cdots +$$
$$2^{2k+2}(\sum_{i=0}^{k} a_i a_{2k+1-i} + a_{k+1}^2) + 2^{2k+3}(\sum_{i=0}^{k} a_i a_{2k+2-i}) + \cdots .$$

En posant $-b = a^2$ , on trouve une racine $c_1$ de $X^2 + b$ dans $\mathbb{Z}_2$ telle que $c_1 \equiv 1 \bmod 2^{n+1}$ dans $\mathbb{Z}_2$ (On distingue les cas n pair ou n impair ; on fait le choix $a_1 = 0$ et on constate que tous les $a_i$ sont nuls pour $i = 1, \cdots, n-1$ ). On en déduit le résultat suivant :

$$\begin{array}{c}
\text{le polynôme } X^2 + b \text{ a une racine } c_1 \equiv 1 \bmod 2^{n+1} \text{ dans } \mathbb{Z}_2 . \\
\text{le polynôme } X^2 - c_1 \text{ a une racine } c_2 \equiv 1 \bmod 2^{n} \text{ dans } \mathbb{Z}_2 . \\
\vdots \\
\vdots \\
\text{le polynôme } X^2 - c_{n-3} \text{ a une racine } c_{n-2} \equiv 1 \bmod 2^{4} \text{ dans } \mathbb{Z}_2 . \\
\text{le polynôme } X^2 - c_{n-2} \text{ a une racine } c_{n-1} \equiv 1 \bmod 2^{3} \text{ dans } \mathbb{Z}_2 . \\
\text{le polynôme } X^2 - c_{n-1} \text{ a une racine } c_{n} \equiv 1 \bmod 2^{2} \text{ dans } \mathbb{Z}_2 .
\end{array}$$

On en déduit que -b=$c_1^2 = c_2^{2^2} = \cdots = c_{n-1}^{2^{n-1}} = c_n^{2^n}$. Et par suite le polynôme $P_{2^n} = X^{2^n} + b$ a une racine $\beta$ dans $\mathbb{Z}_2$ donc dans $\mathbb{Q}_2$ ce qui contredit ii).
Montrons que iii)$\Longrightarrow$i).
Comme b$\equiv$1 mod $2^{n+1}$ et b$\not\equiv$1 mod $2^{n+2}$. On a :

$$\begin{array}{c}
\text{le polynôme } X^2 + b \text{ a une racine } c_1 \equiv 1 \bmod 2^{n} \text{ dans } \mathbb{Z}_2 \text{ et } c_1 \not\equiv 1 \bmod 2^{n+1}. \\
\text{le polynôme } X^2 - c_1 \text{ a une racine } c_2 \equiv 1 \bmod 2^{n-1} \text{ dans } \mathbb{Z}_2 \text{ et } c_2 \not\equiv 1 \bmod 2^{n}. \\
\vdots \\
\vdots \\
\text{le polynôme } X^2 - c_{n-3} \text{ a une racine } c_{n-2} \equiv 1 \bmod 2^{3} \text{ dans } \mathbb{Z}_2 \text{ et } c_{n-2} \not\equiv 1 \bmod 2^{4}. \\
\text{le polynôme } X^2 - c_{n-2} \text{ a une racine } c_{n-1} \equiv 1 \bmod 2^{2} \text{ dans } \mathbb{Z}_2 \text{ et } c_{n-1} \not\equiv 1 \bmod 2^{3}.
\end{array}$$

Ce qu'on vient de faire montre que $P_{2^{n-1}} = X^{2^{n-1}} + b$ a une racine $\beta = c_{n-1}$ dans $\mathbb{Q}_2$ ; or $\beta$ n' est pas un carré dans $\mathbb{Q}_2$ , donc $X^2 - \beta$ est irréductible sur $\mathbb{Q}_2[X]$.

$$P_{2^n} = X^{2^n} + b = X^{2^n} - \beta^{2^{n-1}} = (X^{2^{n-1}} + \beta^{2^{n-2}})(X^{2^{n-1}} - \beta^{2^{n-2}}) =$$
$$= (X^{2^{n-1}} + \beta^{2^{n-2}})(X^{2^{n-2}} + \beta^{2^{n-2}}) \cdots (X^4 + \beta^2)(X^2 - \beta)$$

Soit $T = min(\alpha, \mathbb{Q}_2)$ le polynôme minimal de de $\alpha$ sur $\mathbb{Q}_2$. Si le degré de T est impair alors $\mathbb{Q}(\alpha)$ est isomorphe à un sous-corps de $\mathbb{Q}_2(\alpha)$ (cf.lemme 1[2]) et $s(\mathbb{Q}_2(\alpha)) = 4$ d'après le théorème de Springer car $[\mathbb{Q}_2(\alpha) : \mathbb{Q}_2]$ est impair parconcéquent $s(\mathbb{Q}(\alpha)) = 4$. Comme $\mathbb{Q}(\alpha)$ est isomorphe à $\mathbb{Q}(\sqrt{\beta})$

car $\alpha$ et $\beta$ ont le même polynôme minimal sur $\mathbb{Q}$. On a aussi $s(\mathbb{Q}(\sqrt{\beta})) = 4$.
En posant $L = \mathbb{Q}(\sqrt{\beta})$ , $\forall \wp$ idéal premier divisant 2 :
$[L_\wp : \mathbb{Q}_2] = [L_\wp : \mathbb{Q}_2(\sqrt{\beta})][\mathbb{Q}_2(\sqrt{\beta}) : \mathbb{Q}_2]$ , comme $[\mathbb{Q}_2(\sqrt{\beta})) : \mathbb{Q}_2] = 2$ alors d'après le principe de Hasse-Minskowski cf.lemme2.2 d) on a :
$s(\mathbb{Q}(\sqrt{\beta})) \leq 2$ , ce qui donne une contradiction. Donc l'hypothèse le degré de T impair est faux , donc le degré de T est pair. En utilisant de nouveau le principe de Hasse-Minskowski $\forall \wp$ ideal premier divisant 2 on a :
$[K_\wp : \mathbb{Q}_2] = [K_\wp : \mathbb{Q}_2(\alpha)][\mathbb{Q}_2(\alpha) : \mathbb{Q}_2]$ qui est pair car $[\mathbb{Q}_2(\alpha) : \mathbb{Q}_2] = degT$ est pair. On en déduit que $s(K) \leq 2$.Ce qui termine la démonstration du lemme.

**Remarque 3.1** On a montré que si $\beta$ est la racine de $P_{2^{n-1}} = X^{2^{n-1}} + b$ dans $\mathbb{Q}_2$ , construite dans démonstration du lemme1 , alors $P_{2^n}$ a une racine dans $\mathbb{Q}_2$ si et seulement si $\beta$ est un carré dans $\mathbb{Q}_2$.

## 3.2 Résultat principal

**Théorème 3.1**
*Soit $P = X^{2^n} + d \in \mathbb{Z}[X]$ un polynôme irréductible sur $\mathbb{Q}$ ($n \geq 2$) , $\alpha \in \mathbb{C}$ une racine de $P_{2^n}$ et $K = \mathbb{Q}(\alpha)$. Alors on a :*

- *$s(K) = \infty \Longleftrightarrow d < 0$.*

- *$s(K) = 1 \Longleftrightarrow d = e^2$ , $e \in \mathbb{Z}$.*

*On suppose maintenant $d \in \mathbb{N}^*$ , $d = 2^a b$ , où $a \in \mathbb{N}$ , $b$ n'est pas divisible par 2 et $d$ n'est pas un carré dans $\mathbb{Z}$. Alors on a :*

- *$s(K) = 2 \Longleftrightarrow b \not\equiv -1 \bmod 2^{n+2}$ ou $2^n$ ne divise pas $a$.*

- *$s(K) = 4 \Longleftrightarrow b \equiv -1 \bmod 2^{n+2}$ et $2^n$ divise $a$.*

Démonstration
Le théorème est vrai quand n=1 et n=2 cf.corollaire2.2 et théorème2.3. On suppose maintenant $n \geq 3$ et on raisonne par récurrence sur n.
Si $d < 0$ et $s(K) < \infty$ alors d'après le théorème de Pfister le polynôme $X^{2^n} + d$ est somme de 8 carrés dans $\mathbb{Q}(X)$ (donc dans $\mathbb{Q}[X]$ d'après le théorème de

Cassels . Et $X^{2^n}+d=P_1^2(X)+P_2^2(X)+\cdots+P_8^2(X)$. En faisant X=0 , on trouve d=$d_1^2+d_2^2+d_3^2+d_4^2+d_5^2+d_6^2+d_7^2+d_8^2$ où les $d_i \in \mathbb{Z}$. Ce qui montre que d est positif , ce qui est en contradiction avec notre hypothèse par suite $s(K)=\infty$.
Réciproquement si $s(K)=\infty$ et $d>0$ alors $-\alpha^{2^n}=\underbrace{1+\cdots+1}_{d.fois}$. Par conséquent on a :
$-1=\underbrace{(\frac{1}{\alpha^{2^{n-1}}})^2+\cdots+(\frac{1}{\alpha^{2^{n-1}}})^2}_{d.fois}$ et -1 est somme de carrés dans K ce qui contredit notre hypothèse donc $d<0$.
Si $d=e^2$ avec $e \in \mathbb{Z}^*$ alors $(\alpha^{2^{n-1}})^2=-d=-e^2$ , d'où -1=$(\frac{\alpha^{2^{n-1}}}{e})^2$ et s(K)=1.
Réciproquement si s(K)=1 alors comme $K=\mathbb{Q}(\alpha^2)(\sqrt{\alpha^2})$.
Si $s(\mathbb{Q}(\alpha^2))=1$ , le polynôme $X^{2^{n-1}}+d$ est irréductible sur $\mathbb{Q}$ (sinon $X^{2^n}+d$ ne serait pas irréductible sur $\mathbb{Q}$ ) et c'est le polynôme minimal de $\alpha^2$ sur $\mathbb{Q}$ , d'après l'hypothèse de récurrence sur n , le résultat est vrai au rang n-1 et d est un carré.
Si $s(\mathbb{Q}(\alpha^2)) \neq 1$ alors d'après la proposition 2.1 , $-\alpha^2$ est un carré dans $\mathbb{Q}(\alpha^2)$. Donc $\pm\sqrt{\alpha^4}=-\alpha^2=a_1^2$ avec $a_1 \in \mathbb{Q}(\alpha^2)$. Comme on peut écrire $\mathbb{Q}(\alpha^2)$ sous la forme $\mathbb{Q}(\alpha^2)=\mathbb{Q}(\alpha^4)(\sqrt{\alpha^4})$. On obtient :
$\pm\sqrt{\alpha^4}=-\alpha^2=a_1^2=(\alpha_0+\beta_0\sqrt{\alpha^4})^2=\alpha_0^2+\beta_0^2\alpha^4+2\alpha_0\beta_0\sqrt{\alpha^4}$ , d'où $\alpha_0^2+\beta_0^2\alpha^4=0$ et $2\alpha_0\beta_0=\pm 1$ par conséquent $-1=(\frac{\beta_0\alpha^2}{\alpha_0})^2$. Comme $\frac{\beta_0\alpha^2}{\alpha_0} \in \mathbb{Q}(\alpha^2)$ , on en déduit que $s(\mathbb{Q}(\alpha^2))=1$ ce qui est contradiction avec l'hypothèse.
On suppose maintenant $d \in \mathbb{N}^*$ , d=$2^a b$ , où $a \in \mathbb{N}$ , b n'est pas divisible par 2 et d n'est pas un carré dans $\mathbb{Z}$.
Supposons le théorème vrai au rang n-1.
Comme on sait que $P_{2^{n-1}}=min(\alpha^2, \mathbb{Q})=X^{2^{n-1}}+d$.
$s(\mathbb{Q}(\alpha^2))=2 \Longleftrightarrow$ b$\not\equiv$ -1 mod $2^{n+1}$ ou $2^{n-1}$ ne divise pas a.
$s(\mathbb{Q}(\alpha^2))=4 \Longleftrightarrow$ b$\equiv$ -1 mod $2^{n+1}$ et $2^{n-1}$ divise a.
Donc si b$\not\equiv$-1 mod $2^{n+1}$ ou $2^{n-1}$ ne divise pas a alors , comme $\mathbb{Q}(\alpha^2) \subset \mathbb{Q}(\alpha)$ , on a :
$1 \leq s(\mathbb{Q}(\alpha)) \leq s(\mathbb{Q}(\alpha^2))=2$ de plus $s(\mathbb{Q}(\alpha)) \neq 1$ d'après les hypothèses (d non carré ) on a : $s(\mathbb{Q}(\alpha))=2$. On peut supposer que b$\equiv$-1 mod $2^{n+1}$ et $2^{n-1}$ divise a. Si de plus $2^n$ ne divise pas a , alors on a : $a=2^{n-1}(1+2a_0)$

et $d=2^{2^{n-1}}.2^{2^n a_0}b$

le polynôme $X^2+d$ a une racine $d_1 = 2^{2^{n-2}}.2^{2^{n-1}a_0}a_1$ avec $a_1 \equiv 1 \bmod 2^n$ dans $\mathbb{Z}_2$ .
le polynôme $X^2-d_1$ a une racine $d_2 = 2^{2^{n-3}}.2^{2^{n-2}a_0}a_2$ avec $a_2 \equiv 1 \bmod 2^{n-1}$ dans $\mathbb{Z}_2$ .

$\vdots$

$\vdots$

le polynôme $X^2-d_{n-4}$ a une racine $d_{n-3} = 2^{2^2}.2^{2^3 a_0}a_{n-3}$ avec $a_{n-3} \equiv 1 \bmod 2^4$ dans $\mathbb{Z}_2$ .
le polynôme $X^2-d_{n-3}$ a une racine $d_{n-2} = 2^2.2^{2^2 a_0}a_{n-2}$ avec $a_{n-2} \equiv 1 \bmod 2^3$ dans $\mathbb{Z}_2$ .
le polynôme $X^2-d_{n-2}$ a une racine $d_{n-1} = 2.2^{2a_0}a_{n-1}$ avec $a_{n-1} \equiv 1 \bmod 2^2$ dans $\mathbb{Z}_2$ .

On en déduit que $d_{n-1}^{2^{n-1}} = -d$ et le polynôme $P_{2^{n-1}} = X^{2^{n-1}} + d$ a une racine $\beta = d_{n-1}$ dans $\mathbb{Q}_2$. La forme de $d_{n-1}$ , nous montre qu'il n'est pas un carré dans $\mathbb{Q}_2$. On en déduit d'après la remarque que le polynôme $P_{2^n}$ n'a pas de racine dans $\mathbb{Q}_2$. En utilisant le lemme3.1 on a : s(K)=2.
Si $2^n$ divise a et b$\not\equiv$-1 mod $2^{n+2}$ , quitte à multiplier $\alpha$ par un rationnel non nul , on peut supposer que $\min(\alpha, \mathbb{Q})=X^{2^n}+b$ (car $2^n$ divise a ) donc grâce au lemme1 $s(K) \leq 2$ et comme $s(K) \neq 1$ , s(K)=2.
Enfin si b$\equiv$ -1 mod $2^{n+2}$ et $2^n$ divise a , quitte à multiplier $\alpha$ par un rationnel non nul , on peut supposer que $\min(\alpha, \mathbb{Q})=X^{2^n}+b$ (car $2^n$ divise a ) donc grâce au lemme3.1 , $4 \geq s(K) > 2$
et $s(K) = 4$ , ce qui termine la démonstration du théorème.

**Corollaire 3.1**
*Soit $P = X^n + d \in \mathbb{Q}[X]$ où ($n \in \mathbb{N}$ , et $n \geq 2$) un polynôme irréductible sur $\mathbb{Q}$ , $\alpha$ une racine de $P$ dans $\mathbb{C}$ et $K = \mathbb{Q}(\alpha)$. Si $n$ est impair alors $s(K) = \infty$ . On suppose maintenant $n$ pair alors on a :*

- *$s(K)= \infty \Longleftrightarrow d < 0$.*

- *$s(K)=1 \Longleftrightarrow d= e^2$ , $e \in \mathbb{Q}$.*

*On peut supposer maintenant $d \in \mathbb{N}^*$ , $d=2^a b$ , où $a \in \mathbb{N}^*$ , $b$ n'est pas divisible par 2 et $d$ n'est pas un carré dans $\mathbb{Z}$ ($n = 2^k n_1$ avec $n_1$ impair). Alors on a :*

- *$s(K)=2 \Longleftrightarrow b \not\equiv$ -1 mod $2^{k+2}$ ou $2^k$ ne divise pas $a$.*

- *s(K)=4* $\Longleftrightarrow$ $b \equiv$ *-1 mod* $2^{k+2}$ *et* $2^k$ *divise a.*

Démonstration ( On suppose n pair car sinon on utilise théorème2.2 de Springer ).

On peut supposer d entier relatif en multipliant $\alpha$ par un élément non nul convenable de $\mathbb{Q}$. On considére la suite d'extensions
$\mathbb{Q} \longrightarrow \mathbb{Q}(\alpha^{n_1}) \longrightarrow \mathbb{Q}(\alpha)$ , or n=[ $\mathbb{Q}(\alpha)$ : $\mathbb{Q}$]=[ $\mathbb{Q}(\alpha)$ : $\mathbb{Q}(\alpha^{n_1})$][ $\mathbb{Q}(\alpha^{n_1})$: $\mathbb{Q}$] comme le polynôme minimal de $\alpha^{n_1}$ sur $\mathbb{Q}$ est min( $\alpha^{n_1}$ , $\mathbb{Q}$ )=$X^{2^k} + d$. On en déduit que [ $\mathbb{Q}(\alpha^{n_1})$: $\mathbb{Q}$]=$2^k$ et par suite [ $\mathbb{Q}(\alpha)$ : $\mathbb{Q}(\alpha^{n_1})$]=$n_1$. D'après le théorème de Springer , comme $n_1$ est impair , s(K)=s( $\mathbb{Q}(\alpha^{n_1})$). Le résultat s'ensuit en appliquant le théorème précédent au corps $\mathbb{Q}(\alpha^{n_1})$.

# Chapitre 4

## 4 Etude du niveau d'un corps de nombre $\mathbb{Q}(\alpha)$ dont le polynôme minimal de $\alpha$ sur $\mathbb{Q}$ est de la forme $X^4 + aX^2 + b$, où $a$ , $b \in \mathbb{Z}^*$.

### 4.1 Résultat principal

***Théorème 4.1***

*Soit $K = \mathbb{Q}(\xi)$ un corps de nombres, $\xi \in \mathbb{C}$ et $P = min(\xi , \mathbb{Q}) = X^4 + aX^2 + b$.*

*A)On suppose $a < 0$ , alors :*

*$s(K) = \infty \iff b < (\frac{a}{2})^2$ .*

*On suppose maintenant $b > (\frac{a}{2})^2$ donc $s(K) < \infty$.*

*1)Si $s(\mathbb{Q}(\sqrt{a^2 - 4b})) = 1$ alors $s(K) = 1$.*

*2)Si $s(\mathbb{Q}(\sqrt{a^2 - 4b})) = 2$ alors :*

s(K)=*1 $\iff$ ($b = {b_0}^2$ , $b_0 \in \mathbb{N}$) et ( $a + 2b_0$ est un carré dans $\mathbb{Z}$ ) .*

s(K)=*2 $\iff$ ($b \neq {b_0}^2$ , $\forall b_0 \in \mathbb{N}$) ou ($b = {b_0}^2$ , $b_0 \in \mathbb{N}$ et $a + 2b_0$ n'est pas un carré dans $\mathbb{Z}$) .*

*3)Si $s(\mathbb{Q}(\sqrt{a^2 - 4b})) = 4$ alors :*

*$s(K)$=1 $\iff$ ($b = {b_0}^2$ , $b_0 \in \mathbb{N}$) et ($a + 2b_0$ est un carré dans $\mathbb{Z}$ ).*

*On suppose maintenant que : ($b \neq {b_0}^2$ , $\forall b_0 \in \mathbb{N}$) ou*

*($b = {b_0}^2$ , $b_0 \in \mathbb{N}$ et $a + 2b_0$ n'est pas un carré dans $\mathbb{Z}$ ) ,*

*on a alors $2 \leq s(K) \leq 4$ .*

*On pose $4b - a^2 = 4^\alpha d$ avec $d \equiv$ -1 mod 8 et $-a = 2^\beta a_1$ , avec $a_1$ impair .*

*<u>Premier cas</u> : $\beta > \alpha$ :*

*Si $\alpha$ est pair alors : $s(K)$=2 .*

*Si $\alpha$ est impair alors :*

*Si ( $\beta \geq \alpha + 3$ ) ou ( $\beta = \alpha + 1$ et $a_1 \equiv 1 \ mod\ 4$ ) alors :*

$$\text{s(K)=} \begin{cases} 2 & \iff d \not\equiv -1 \ mod\ 16. \\ 4 & \iff d \equiv -1 \ mod\ 16. \end{cases}$$

*Si ( $\beta = \alpha + 2$ ) ou ($\beta = \alpha + 1$ et $a_1 \equiv 3 \ mod\ 4$) alors :*

$$\text{s(K)=} \begin{cases} 2 & \iff d \equiv -1 \ mod\ 16. \\ 4 & \iff d \not\equiv -1 \ mod\ 16. \end{cases}$$

*Deuxième cas* : $\beta < \alpha$ :
*Si* $\beta$ *est pair alors :* $s(K)=2$ .
*Si* $\alpha$ *est impair alors :*

$$\textit{Si } \alpha \geq \beta+3 \textit{ alors : } s(K) = \begin{cases} 2 & \Longleftrightarrow\ a_1 \not\equiv 1 \ mod\ 8. \\ 4 & \Longleftrightarrow\ a_1 \equiv 1 \ mod\ 8. \end{cases}$$

$$\textit{Si } \alpha = \beta+2 \textit{ alors : } s(K) = \begin{cases} 2 & \Longleftrightarrow\ a_1 \not\equiv 5 \ mod\ 8. \\ 4 & \Longleftrightarrow\ a_1 \equiv 5 \ mod\ 8. \end{cases}$$

$$\textit{Si } \alpha = \beta+1 \textit{ alors : } \mathrm{s(K)} = \begin{cases} 2 & \Longleftrightarrow\ a_1 \not\equiv -1 \ mod\ 8 \ \textit{et}\ a_1 \not\equiv 3 \ mod\ 8. \\ 4 & \Longleftrightarrow\ a_1 \equiv -1 \ mod\ 8 \ \textit{ou}\ a_1 \equiv 3 \ mod\ 8. \end{cases}$$

*Troisième cas* : $\beta = \alpha$ :
*On écrit :*
$a_1 = 1 + \sum_{i=1}^{i=k} 2^i n_i$ , *avec* $n_i \in \{0,1\}$.
$\sqrt{-d} = 1 + \sum_{i=1}^{i=\infty} 2^i m_i$ , *avec* $m_i \in \{0,1\}$.
*et* $-\sqrt{-d} = 1 + \sum_{i=1}^{i=\infty} 2^i m_i{}'$ , *avec* $m_i{}' \in \{0,1\}$.
*Soit* $i_0 = min\{i \geq k+1 \textit{ tel que } m_i = 0\}$
*Soit* $j_0 = min\{j \geq k+1 \textit{ tel que } m_j{}' = 0\}$
$a_1 + m = 2^\gamma q$ *avec* $q$ *impair où* $m = 1 + \sum_{i=1}^{i=i_0+2} 2^i m_i$.
$a_1 + m' = 2^{\gamma'} q'$ *avec* $q'$ *impair où* $m' = 1 + \sum_{i=1}^{i=j_0+2} 2^i m_i{}'$.
*Si* $\alpha+\gamma+1$ *et* $\alpha+\gamma'+1$ *sont impairs alors :* $s(K)=2$.
*Si* $\alpha+\gamma+1$ *et* $\alpha+\gamma'+1$ *sont pairs alors :*

$$\mathrm{s(K)} = \begin{cases} 2 & \Longleftrightarrow\ q \not\equiv 1 \ mod\ 8 \ \textit{et}\ q' \not\equiv 1 \ mod\ 8. \\ 4 & \Longleftrightarrow\ q \equiv 1 \ mod\ 8 \ \textit{ou}\ q' \equiv 1 \ mod\ 8. \end{cases}$$

$$\textit{Si } \alpha+\gamma+1 \textit{ est pair et } \alpha+\gamma'+1 \textit{ est impair alors : } \mathrm{s(K)} = \begin{cases} 2 & \Longleftrightarrow\ q \not\equiv 1 mod\ 8. \\ 4 & \Longleftrightarrow\ q \equiv 1 \ mod\ 8. \end{cases}$$

$$\textit{Si } \alpha+\gamma+1 \textit{ est impair et } \alpha+\gamma'+1 \textit{ est pair alors : } s(K) = \begin{cases} 2 & \Longleftrightarrow\ q' \not\equiv 1 \ mod\ 8. \\ 4 & \Longleftrightarrow\ q' \equiv 1 \ mod\ 8. \end{cases}$$

*B)On suppose* $a > 0$ , *alors :*
$\mathrm{s(K)} = \infty \Longleftrightarrow b < 0$ .
*On suppose maintenant* $b > 0$ *alors :* $s(K) < \infty$ .
*B-1) Si* $b > (\frac{a}{2})^2$ *alors :* $s(\ \mathbb{Q}(\sqrt{a^2-4b})) < \infty$.
*1)Si* $s(\ \mathbb{Q}(\sqrt{a^2-4b})) = 1$ *alors* $s(K) = 1$.
*2)Si* $s(\ \mathbb{Q}(\sqrt{a^2-4b})) = 2$ *alors :*
$\mathrm{s(K)}=1 \Longleftrightarrow (b = {b_0}^2 , b_0 \in \mathbb{N})$ *et* $(a + 2b_0$ *est un carré dans* $\mathbb{Z})$.
$\mathrm{s(K)}=2 \Longleftrightarrow (b \neq {b_0}^2 , \forall b_0 \in \mathbb{N})$ *ou* $(b = {b_0}^2 , b_0 \in \mathbb{N}$ *et* $a + 2b_0$ *n'est pas un carré dans* $\mathbb{Z}$ ) .
*3)Si* $s(\ \mathbb{Q}(\sqrt{a^2-4b})) = 4$ *alors :*

$s(K)$=*1* $\iff$ ($b = {b_0}^2$ , $b_0 \in$ $I\!N$) *et* ($a + 2b_0$ *est un carré dans* $Z\!\!Z$ ).
*On suppose maintenant :* ($b \neq {b_0}^2$ , $\forall b_0 \in$ $I\!N$) *ou* ($b = {b_0}^2$ ,
$b_0 \in$ $I\!N$ *et* $a + 2b_0$ *n'est pas un carré dans* $Z\!\!Z$ ).
*On pose* $4b - a^2 = 4^\alpha d$ *avec* $d \equiv$ *-1 mod 8 et* $a = 2^\beta a_1$ , *avec* $a_1$ *impair .*
*Premier cas :* $\beta > \alpha$ :
*Si* $\alpha$ *est pair alors :* $s(K)$=*2 .*
*Si* $\alpha$ *est impair alors :*
*Si* ( $\beta \geq \alpha + 3$ ) *ou* ( $\beta = \alpha + 1$ *et* $a_1 \equiv$ 3 *mod* 4 ) *alors :*

$$s(K) = \begin{cases} 2 & \iff d \not\equiv -1 \text{ mod } 16. \\ 4 & \iff d \equiv -1 \text{ mod } 16. \end{cases}$$

*Si* ( $\beta = \alpha + 2$ ) *ou* ( $\beta = \alpha + 1$ *et* $a_1 \equiv$ 1 *mod* 4 ) *alors :*

$$s(K) = \begin{cases} 2 & \iff d \equiv -1 \text{ mod } 16. \\ 4 & \iff d \not\equiv -1 \text{ mod } 16. \end{cases}$$

*Deuxième cas :* $\beta < \alpha$ :
*Si* $\beta$ *est pair alors* $s(K)$=*2 .*
*Si* $\alpha$ *est impair alors :*

*Si* $\alpha \geq \beta + 3$ *alors :* $s(K) = \begin{cases} 2 & \iff a_1 \not\equiv 1 \text{ mod } 8. \\ 4 & \iff a_1 \equiv 1 \text{ mod } 8. \end{cases}$

*Si* $\alpha = \beta + 2$ *alors :* $s(K) = \begin{cases} 2 & \iff a_1 \not\equiv -5 \text{ mod } 8. \\ 4 & \iff a_1 \equiv -5 \text{ mod } 8. \end{cases}$

*Si* $\alpha = \beta + 1$ *alors :* $s(K) = \begin{cases} 2 & \iff a_1 \not\equiv 1 \text{ mod } 8 \text{ et } a_1 \not\equiv -3 \text{ mod } 8. \\ 4 & \iff a_1 \equiv 1 \text{ mod } 8 \text{ ou } a_1 \equiv -3 \text{ mod } 8. \end{cases}$

*Troisième cas* : $\beta = \alpha$ :
*On écrit :*
$a_1$=*1*+$\sum_{i=1}^{i=k} 2^i n_i$ , *avec* $n_i \in \{0, 1\}$.
$\sqrt{-d}$=$1 + \sum_{i=1}^{i=\infty} 2^i m_i$ , *avec* $m_i \in \{0, 1\}$.
*et* $-\sqrt{-d}$=$1 + \sum_{i=1}^{i=\infty} 2^i {m_i}'$ , *avec* ${m_i}' \in \{0, 1\}$.
*Soit* $i_0$=$min\{i \geq k + 1$ *tel que* $m_i = 0\}$
*Soit* $j_0$=$min\{j \geq k + 1$ *tel que* ${m_i}' = 0\}$
$-a_1 + m = 2^\gamma q$ *avec* $q$ *impair où* $m$=$1 + \sum_{i=1}^{i=i_0+2} 2^i m_i$.
$-a_1 + m' = 2^{\gamma'} q'$ *avec* $q'$ *impair où* $m'$=$1 + \sum_{i=1}^{i=j_0+2} 2^i {m_i}'$.
*a) Si* $-a_1 + m \neq 0$ *et* $-a_1 + m' \neq 0$ *alors :*
*Si* $\alpha + \gamma + 1$ *et* $\alpha + \gamma' + 1$ *sont impairs alors : s(K)=2.*
*Si* $\alpha + \gamma + 1$ *et* $\alpha + \gamma' + 1$ *sont pairs alors :*

$$s(K) = \begin{cases} 2 & \iff q \not\equiv 1 \text{ mod } 8 \text{ et } q' \not\equiv 1 \text{ mod } 8. \\ 4 & \iff q \equiv 1 \text{ mod } 8 \text{ ou } q' \equiv 1 \text{ mod } 8. \end{cases}$$

*Si* $\alpha+\gamma+1$ *est pair et* $\alpha+\gamma'+1$ *est impair alors :* $s(K) = \begin{cases} 2 & \Longleftrightarrow q \not\equiv 1 \ mod\ 8. \\ 4 & \Longleftrightarrow q \equiv 1 mod\ 8. \end{cases}$

*Si* $\alpha+\gamma+1$ *est impair et* $\alpha+\gamma'+1$ *est pair alors :* $s(K) = \begin{cases} 2 & \Longleftrightarrow q' \not\equiv 1 \ mod\ 8. \\ 4 & \Longleftrightarrow q' \equiv 1 \ mod\ 8. \end{cases}$

*b) Si* $-a_1 + m = 0$ *alors* $-a_1 + m' \neq 0$ *et on a :*
*Soit* $k_0 = min\{k \geq i_0 + 3$ *tel que* $m_k = 1\}$
*Soit* $q_1 = 1 + 2m_{k_0+1} + 2^2 m_{k_0+2}$ .
*Si* $\alpha + k_0 + 1$ *et* $\alpha + \gamma' + 1$ *sont impairs alors : s(K)=2.*
*Si* $\alpha + k_0 + 1$ *et* $\alpha + \gamma' + 1$ *sont pairs alors :*
$s(K) = \begin{cases} 2 & \Longleftrightarrow q_1 \not\equiv 1 \ mod\ 8 \ et \ q' \not\equiv 1 \ mod\ 8. \\ 4 & \Longleftrightarrow q_1 \equiv 1 \ mod\ 8 \ ou \ q' \equiv 1 \ mod\ 8. \end{cases}$

*Si* $\alpha+k_0+1$ *est pair et* $\alpha+\gamma'+1$ *est impair alors :* $s(K) = \begin{cases} 2 & \Longleftrightarrow q_1 \not\equiv 1 \ mod\ 8. \\ 4 & \Longleftrightarrow q_1 \equiv 1 mod\ 8. \end{cases}$

*Si* $\alpha+\gamma+1$ *est impair et* $\alpha+\gamma'+1$ *est pair alors :* $s(K) = \begin{cases} 2 & \Longleftrightarrow q' \not\equiv 1 \ mod\ 8. \\ 4 & \Longleftrightarrow q' \equiv 1 \ mod\ 8. \end{cases}$

*c) Si* $-a_1 + m' = 0$ *alors* $-a_1 + m \neq 0$ *et on a :*
*Soit* $k'_0 = min\{k \geq j_0 + 3$ *tel que* $m_k = 1\}$
*Soit* $q_2 = 1 + 2m_{k'_0+1} + 2^2 m_{k'_0+2}$ .
*Si* $\alpha + \gamma + 1$ *et* $\alpha + k'_0 + 1$ *sont impairs alors : s(K)=2.*
*Si* $\alpha + \gamma + 1$ *et* $\alpha + k'_0 + 1$ *sont pairs alors :*
$s(K) = \begin{cases} 2 & \Longleftrightarrow q \not\equiv 1 \ mod\ 8 \ et \ q_2 \not\equiv 1 \ mod\ 8. \\ 4 & \Longleftrightarrow q \equiv 1 \ mod\ 8 \ ou \ q_2 \equiv 1 \ mod\ 8 . \end{cases}$

*Si* $\alpha+\gamma+1$ *est pair et* $\alpha+k'_0+1$ *est impair alors :* $s(K) = \begin{cases} 2 & \Longleftrightarrow q \not\equiv 1 \ mod\ 8. \\ 4 & \Longleftrightarrow q \equiv 1 mod\ 8. \end{cases}$

*Si* $\alpha+\gamma+1$ *est impair et* $\alpha+k'_0+1$ *est pair alors :* $s(K) = \begin{cases} 2 & \Longleftrightarrow q_2 \not\equiv 1 \ mod\ 8. \\ 4 & \Longleftrightarrow q_2 \equiv 1 \ mod\ 8. \end{cases}$

*B-2)Si* $0 < b < (\frac{a}{2})^2$ *alors* $s(\mathbb{Q}(\sqrt{a^2 - 4b})) = \infty$ .
$s(K)=1 \Longleftrightarrow (b = {b_0}^2$ , $b_0 \in \mathbb{N})$ *et* $(a + 2b_0$ *ou* $a - 2b_0$ *est un carré dans* $\mathbb{Z})$ .
*On suppose maintenant que :(* $b \neq {b_0}^2$ , $\forall b_0 \in \mathbb{N})$ *ou* $(b = {b_0}^2$ *et ni* $a + 2b_0$ *ni* $a - 2b_0$ *n'est un carré dans* $\mathbb{Z})$ , *on a :* $2 \leq s(K) \leq 4$ .
*Posons* $a^2 - 4b = 4^\alpha d$ *avec d non divisible par 4 et* $a = 2^\beta a_1$ *avec* $a_1$ *impair .*
*Si* $d \not\equiv 1 \ mod\ 8$ *alors* $s(K)=2$ .
*Si* $d \equiv 1 \ mod\ 8$ *alors :*
*Premier cas :* $\beta > \alpha$ :

*Si $\alpha$ est pair alors : $s(K)=2$ .*
*Si $\alpha$ est impair alors :*
*Si ( $\beta \geq \alpha+3$ ) ou ( $\beta=\alpha+1$ et $a_1 \equiv 3 \bmod 4$ ) alors :*

$$s(K)=\begin{cases} 2 & \Longleftrightarrow d \not\equiv 1 \bmod 16. \\ 4 & \Longleftrightarrow d \equiv 1 \bmod 16. \end{cases}$$

*Si ( $\beta=\alpha+2$ ) ou ( $\beta=\alpha+1$ et $a_1 \equiv 1 \bmod 4$ ) alors :*

$$s(K)=\begin{cases} 2 & \Longleftrightarrow d \equiv 1 \bmod 16. \\ 4 & \Longleftrightarrow d \not\equiv 1 \bmod 16. \end{cases}$$

*Deuxième cas : $\beta < \alpha$ :*
*Si $\beta$ est pair alors : $s(K)=2$ .*
*Si $\beta$ est impair alors :*

*Si $\alpha \geq \beta+3$ alors:* $s(K)=\begin{cases} 2 & \Longleftrightarrow a_1 \not\equiv -1 \bmod 8. \\ 4 & \Longleftrightarrow a_1 \equiv -1 \bmod 8. \end{cases}$

*Si $\alpha=\beta+2$ alors :* $s(K)=\begin{cases} 2 & \Longleftrightarrow a_1 \not\equiv -5 \bmod 8. \\ 4 & \Longleftrightarrow a_1 \equiv -5 \bmod 8. \end{cases}$

*Si $\alpha=\beta+1$ alors :* $s(K)=\begin{cases} 2 & \Longleftrightarrow a_1 \not\equiv 1 \bmod 8 \text{ et } a_1 \not\equiv -3 \bmod 8. \\ 4 & \Longleftrightarrow a_1 \equiv 1 \bmod 8 \text{ ou } a_1 \equiv -3 \bmod 8. \end{cases}$

*Troisième cas : $\beta=\alpha$ :*
*On écrit :*
$a_1=1+\sum_{i=1}^{i=k} 2^i n_i$ , *avec* $n_i \in \{0,1\}$.
$\sqrt{d}=1+\sum_{i=1}^{i=\infty} 2^i m_i$ , *avec* $m_i \in \{0,1\}$.
*et* $-\sqrt{d}=1+\sum_{i=1}^{i=\infty} 2^i m_i^{'}$ , *avec* $m_i^{'} \in \{0,1\}$.
*Soit* $i_0=min\{i \geq k+1$ *tel que* $m_i=0\}$
*Soit* $j_0=min\{j \geq k+1$ *tel que* $m_i^{'}=0\}$
$-a_1+m=2^{\gamma}q$ *avec* $q$ *impair où* $m=1+\sum_{i=1}^{i=i_0+2} 2^i m_i$.
$-a_1+m^{'}=2^{\gamma^{'}}q^{'}$ *avec* $q^{'}$ *impair où* $m^{'}=1+\sum_{i=1}^{i=j_0+2} 2^i m_i^{'}$.
*a) Si $-a_1+m \neq 0$ et $-a_1+m^{'} \neq 0$ alors :*
*Si $\alpha+\gamma+1$ et $\alpha+\gamma^{'}+1$ sont impairs alors : $s(K)=2$.*
*Si $\alpha+\gamma+1$ et $\alpha+\gamma^{'}+1$ sont pairs alors :*

$$s(K)=\begin{cases} 2 & \Longleftrightarrow q \not\equiv 1 \bmod 8 \text{ et } q^{'} \not\equiv 1 \bmod 8. \\ 4 & \Longleftrightarrow q \equiv 1 \bmod 8 \text{ ou } q^{'} \equiv 1 \bmod 8. \end{cases}$$

*Si $\alpha+\gamma+1$ est pair et $\alpha+\gamma^{'}+1$ est impair alors :* $s(K)=\begin{cases} 2 & \Longleftrightarrow q \not\equiv 1 \bmod 8. \\ 4 & \Longleftrightarrow q \equiv 1 \bmod 8. \end{cases}$

*Si $\alpha+\gamma+1$ est impair et $\alpha+\gamma^{'}+1$ est pair alors :* $s(K)=\begin{cases} 2 & \Longleftrightarrow q^{'} \not\equiv 1 \bmod 8. \\ 4 & \Longleftrightarrow q^{'} \equiv 1 \bmod 8. \end{cases}$

*b) Si $-a_1+m=0$ alors $-a_1+m^{'} \neq 0$ et on a :*

*Soit* $k_0$=$min\{k \geq i_0 + 3$ *tel que* $m_k = 1\}$
*Soit* $q_1 = 1 + 2m_{k_0+1} + 2^2 m_{k_0+2}$ .
*Si* $\alpha + k_0 + 1$ *et* $\alpha + \gamma' + 1$ *sont impairs alors :* $s(K)$=*2.*
*Si* $\alpha + k_0 + 1$ *et* $\alpha + \gamma' + 1$ *sont pairs alors :*

$$s(K) = \begin{cases} 2 & \Longleftrightarrow\ q_1 \not\equiv 1\ mod\ 8\ et\ q' \not\equiv 1\ mod\ 8. \\ 4 & \Longleftrightarrow\ q_1 \equiv 1\ mod\ 8\ ou\ q' \equiv 1\ mod\ 8. \end{cases}$$

*Si* $\alpha$+$k_0$+1 *est pair et* $\alpha$+$\gamma'$+1 *est impair alors :* $s(K) = \begin{cases} 2 & \Longleftrightarrow\ q_1 \not\equiv 1\ mod\ 8. \\ 4 & \Longleftrightarrow\ q_1 \equiv 1 mod\ 8. \end{cases}$

*Si* $\alpha$+$\gamma$+1 *est impair et* $\alpha$+$\gamma'$+1 *est pair alors :* $s(K) = \begin{cases} 2 & \Longleftrightarrow\ q' \not\equiv 1\ mod\ 8. \\ 4 & \Longleftrightarrow\ q' \equiv 1\ mod\ 8. \end{cases}$

*c) Si* $-a_1 + m' = 0$ *alors* $-a_1 + m \neq 0$ *et on a :*
*Soit* $k'_0$=$min\{k \geq j_0 + 3$ *tel que* $m_k = 1\}$
*Soit* $q_2 = 1 + 2m_{k'_0+1} + 2^2 m_{k'_0+2}$ .
*Si* $\alpha + \gamma + 1$ *et* $\alpha + k'_0 + 1$ *sont impairs alors :* $s(K) = 2$.
*Si* $\alpha + \gamma + 1$ *et* $\alpha + k'_0 + 1$ *sont pairs alors :*

$$s(K) = \begin{cases} 2 & \Longleftrightarrow\ q \not\equiv 1\ mod\ 8\ et\ q_2 \not\equiv 1\ mod\ 8. \\ 4 & \Longleftrightarrow\ q \equiv 1\ mod\ 8\ ou\ q_2 \equiv 1\ mod\ 8\ . \end{cases}$$

*Si* $\alpha$+$\gamma$+1 *est pair et* $\alpha$+$k'_0$+1 *est impair alors :* $s(K) = \begin{cases} 2 & \Longleftrightarrow\ q \not\equiv 1\ mod\ 8. \\ 4 & \Longleftrightarrow\ q \equiv 1 mod\ 8. \end{cases}$

*Si* $\alpha$+$\gamma$+1 *est impair et* $\alpha$+$k'_0$+1 *est pair alors :* $s(K) = \begin{cases} 2 & \Longleftrightarrow\ q_2 \not\equiv 1\ mod\ 8. \\ 4 & \Longleftrightarrow\ q_2 \equiv 1\ mod\ 8. \end{cases}$

Démonstration
A)On suppose que : a<0 .
Pour $b < (\frac{a}{2})^2$ on a : $P = (X^2 + \frac{a}{2})^2 + \frac{4b-a^2}{4}$ .
Si s(K)< $\infty$ alors d'après le théorème 2.1 de Pfister P=$P_1^2 + P_2^2 + \cdots + P_n^2$ les $P_i \in \mathbb{Q}[X]$ et n$\in$ $\mathbb{N}^*$. Ceci signifie que pour tout x appartenant à $\mathbb{R}$ , P(x)$\geq$ 0 . Or $P(\pm\sqrt{\frac{a}{2}}) = \frac{4b-a^2}{4} < 0$ , ce qui est une contradiction .
Réciproquement supposons s(K)=$\infty$ . Si b> $(\frac{a}{2})^2$ alors :
$P = (X^2 + \frac{a}{2})^2 + \underbrace{(\frac{1}{2})^2 + (\frac{1}{2})^2 + \cdots + (\frac{1}{2})^2}_{(4b-a^2)fois}$ . On en déduit facilement que :
$-1 = (2\xi^2 + a)^2 + \underbrace{1^2 + 1^2 + \cdots + 1^2}_{(4b-a^2-1)fois}$ , contradiction avec s(K)=$\infty$ .
On suppose maintenant que b> $(\frac{a}{2})^2$ alors s(K)< $\infty$ .
On sait d'après le corollaire 2.1 et la proposition 2.1 que le corps

$\mathbb{Q}(\sqrt{a^2-4b})(\sqrt{-\frac{a+\sqrt{a^2-4b}}{2}})$ a le même niveau que K , on a alors : s(K)=1 si et seulement si $s(\mathbb{Q}(\sqrt{a^2-4b}))=1$ ou $\frac{a+\sqrt{a^2-4b}}{2}$ est un carré dans $\mathbb{Q}(\sqrt{a^2-4b})$.
Or $\frac{a+\sqrt{a^2-4b}}{2}$ est un carré dans $\mathbb{Q}(\sqrt{a^2-4b})$ si et seulement si $2a+2\sqrt{a^2-4b}=(x+y\sqrt{a^2-4b})^2$ avec x,y$\in \mathbb{Q}$. Ce qui donne après calcul que
$x^4-2ax^2+a^2-4b=0$ i.e x=$\sqrt{a+2\sqrt{b}} \in \mathbb{Q}$ ce qui signifie que :
$\sqrt{b} \in \mathbb{Q}$ et$\sqrt{a+2\sqrt{b}} \in \mathbb{Q}$. La première assertion est dès lors une évidence .
Il est évident que $\mathbb{Q}(\sqrt{-(4b-a^2)}) \subset K$ , les premières équivalences dans 2) et 3) s'ensuivent .
On suppose maintenant que : $(b \neq {b_0}^2$ , $\forall b_0 \in \mathbb{N})$ *ou* $(b={b_0}^2$ , $b_0 \in \mathbb{N}$ *et* $a+2b_0$ n'est pas un carré dans $\mathbb{Z}$ ) , on a alors $2 \leq s(K) \leq 4$ .
Posons E= $\mathbb{Q}_2^*/\ {\mathbb{Q}_2}^{*2}=\{1,2,3,5,6,7,10,14\}$
Premier cas : $\beta > \alpha$ :
Si $\alpha$ est pair alors $\alpha+1$ est impair et $2^{\beta+1}a_1 \pm 2^{\alpha+1}\sqrt{-d} \notin {\mathbb{Q}_2}^{*2}$ car pour tout nombre impair h appartenant à E , 2h$\in E\backslash\{1\}$ . En utilisant le Lemme2.3 on en déduit que : s(K)=2 .
Si $\alpha$ est impair alors $\alpha+1$ est pair et on a :
$\mathbb{Q}(\sqrt{2^{\beta+1}a_1+2^{\alpha+1}\sqrt{-d}}) = \mathbb{Q}(\sqrt{2^{\beta-\alpha}a_1+\sqrt{-d}})$.
On voit donc qu'en utilisant le lemme2.3 si $\beta \geq \alpha+3$ alors :
s(K)=2 $\Longleftrightarrow d \not\equiv$ -1 mod 16 , car $\sqrt{-d}=1+2+2^3d_1$ ou $1+2^2+2^3d_2$ avec $d_1, d_2 \in \mathbb{Z}_2$ si $d \not\equiv$ -1 mod 16 parconséquent $\pm\sqrt{2^{\beta+1}a_1 \pm 2^{\alpha+1}\sqrt{-d}} \notin \mathbb{Q}_2$ et P n'a pas de racine dans $\mathbb{Q}_2$.
Si $\beta=\alpha+2$ alors : s(K)=2 $\Longleftrightarrow d \equiv$ -1 mod 16 en effet $\sqrt{-d}=1+2+2^3d_1$ ou $1+2^2+2^3d_2$ avec $d_1, d_2 \in \mathbb{Z}_2$ si $d \not\equiv$-1 mod 16. $2^{\beta-\alpha}a_1+\sqrt{-d}=2^2+1+2+2^3d_1$ ou $2^{\beta-\alpha}a_1+\sqrt{-d}=2^2+1+2^2+2^3d_2$ ce dernier est dans ${\mathbb{Q}_2}^{*2}$.
Si d$\equiv$-1 mod 16 alors $\sqrt{-d}=1+2^3d_1$ ou $1+2+2^2+2^3d_2$ par conséquent $2^{\beta-\alpha}a_1+\sqrt{-d}=2^2+1+2^3d_1$ ou $2^{\beta-\alpha}a_1+\sqrt{-d}=2^2+1+2+2^2+2^3d_2$ aucune de ces deux quantités n'est dans ${\mathbb{Q}_2}^{*2}$ , on endéduit que :
$\pm\sqrt{2^{\beta+1}a_1 \pm 2^{\alpha+1}\sqrt{-d}} \notin \mathbb{Q}_2$ et s(K)=4 en appliquant le lemme2.3 .
Si $\beta=\alpha+1$ et $a_1 \equiv 3$ mod 4 alors : s(K)=2 $\Longleftrightarrow d \equiv$ -1 mod 16 en effet $\sqrt{-d}=1+2+2^3d_1$ ou $1+2^2+2^3d_2$ avec $d_1, d_2 \in \mathbb{Z}_2$ si $d \not\equiv$-1 mod 16. $2^{\beta-\alpha}a_1+\sqrt{-d}=2+2^2+1+2^2+2^3d_2$ ou $2^{\beta-\alpha}a_1+\sqrt{-d}=2+2^2+1+2+2^3d_1$ ce dernier est dans ${\mathbb{Q}_2}^{*2}$ on endéduit que s(K)=4 . Si d$\equiv$-1 mod 16 alors $\sqrt{-d}=1+2^3d_1$ ou $1+2+2^2+2^3d_2$ par conséquent $2^{\beta-\alpha}a_1+\sqrt{-d}=2+2^2+1+2^3d_1$ ou $2^{\beta-\alpha}a_1+\sqrt{-d}=2+2^2+1+2+2^2+2^3d_2$ , aucune de ces deux derniéres

quantités n'est dans $\mathbb{Q}_2{}^{*2}$ . On en déduit que $\pm\sqrt{2^{\beta+1}a_1 \pm 2^{\alpha+1}\sqrt{-d}} \notin \mathbb{Q}_2$ et s(K)=2 en appliquant le lemme2.3 .
Si $\beta = \alpha + 1$ et $a_1 \equiv 1 \bmod 4$ alors : s(K)=2 $\Longleftrightarrow$ $d \not\equiv$ -1 mod 16 en effet $\sqrt{-d} = 1 + 2 + 2^3 d_1$ ou $1 + 2^2 + 2^3 d_2$ avec $d_1, d_2 \in \mathbb{Z}_2$ si $d \not\equiv$-1 mod 16. $2^{\beta-\alpha}a_1 + \sqrt{-d} = 2 + 1 + 2 + 2^3 d_1$ ou $2^{\beta-\alpha}a_1 + \sqrt{-d} = 2 + 1 + 2^2 + 2^3 d_2$ aucune de ces deux derniéres quantités n'est dans $\mathbb{Q}_2{}^{*2}$. On endéduit que $\pm\sqrt{2^{\beta+1}a_1 \pm 2^{\alpha+1}\sqrt{-d}} \notin \mathbb{Q}_2$ et s(K)=2 en appliquant le lemme2.3 .
Si d$\equiv$-1 mod 16 alors $\sqrt{-d} = 1 + 2^3 d_1$ ou $1 + 2 + 2^2 + 2^3 d_2$ par conséquent $2^{\beta-\alpha}a_1 + \sqrt{-d} = 2 + 1 + 2^3 d_1$ ou $2^{\beta-\alpha}a_1 + \sqrt{-d} = 2 + 1 + 2 + 2^2 + 2^3 d_2$ ce dernier est dans $\mathbb{Q}_2{}^{*2}$ on en déduit que s(K)=4 .
Deuxième cas: $\beta < \alpha$ :
Si $\beta$ est pair alors $\beta$+1 est impair et $2^{\beta+1}a_1 \pm 2^{\alpha+1}\sqrt{-d} \notin \mathbb{Q}_2{}^{*2}$ car pour tout nombre impair h appartenant à E , 2h$\in E\backslash\{1\}$ . En utilisant le Lemme2.3 on en déduit que : s(K)=2 .
Si $\beta$ est impair alors $\beta$+1 est pair et $\mathbb{Q}(\sqrt{2^{\beta+1}a_1 + 2^{\alpha+1}\sqrt{-d}}) = \mathbb{Q}(\sqrt{a_1 + 2^{\beta-\alpha}\sqrt{-d}})$.
On voit donc qu'en utilisant le lemme2.3 si $\alpha \geq \beta + 3$ alors :
s(K)=2 $\Longleftrightarrow$ $a_1 \not\equiv 1 \bmod 16$ , car $a_1 \pm 2^{\alpha-\beta}\sqrt{-d} = a_1 + 2^3 d_1$ avec $d_1 \in \mathbb{Z}_2$ et par conséquent $a_1 \pm 2^{\alpha-\beta}\sqrt{-d} \in \mathbb{Q}_2$ si et seulement si $a_1 \equiv 1 \bmod 8$. on endéduit que : s(K)=4 $\Longleftrightarrow$ $a_1 \equiv 1 \bmod 8$ .
Si $\alpha = \beta + 2$ alors : s(K)=2 $\Longleftrightarrow$ $a_1 \not\equiv 5 \bmod 16$ en effet pour $a_1 \equiv 5 \bmod 8$ comme $\sqrt{-d} = 1 + 2 + 2^3 d_1$ ou $1 + 2^2 + 2^3 d_2$ avec $d_1, d_2 \in \mathbb{Z}_2$ si $d \not\equiv$-1 mod 16. $a_1 + 2^{\alpha-\beta}\sqrt{-d} = 1 + 2^2 + 2^2 + 2^3 d_1$ ou $a_1 + 2^{\alpha-\beta}\sqrt{-d} = 1 + 2^2 + 2^2 + 2^3 d_2$ ces derniers sont dans $\mathbb{Q}_2{}^{*2}$ donc s(K)=4.
Si d$\equiv$-1 mod 16 alors $\sqrt{-d} = 1 + 2^3 d_1$ ou $1 + 2 + 2^2 + 2^3 d_2$ par conséquent $a_1 + 2^{\alpha-\beta}\sqrt{-d} = a_1 + 2^2 + 2^3 d_1$ ou $a_1 + 2^{\alpha-\beta}\sqrt{-d} = a_1 + 2^2 + 2^3 d_2$ aucune de ces deux quantités n'est dans $\mathbb{Q}_2{}^{*2}$ si $a_1 \not\equiv 5 \bmod 8$ , on en déduit que $\pm\sqrt{2^{\beta+1}a_1 \pm 2^{\alpha+1}\sqrt{-d}} \notin \mathbb{Q}_2$ et s(K)=4 en appliquant le lemme2.3 .
Si $\alpha = \beta + 1$ alors : s(K)=2 $\Longleftrightarrow$ $a_1 \not\equiv$ -1 mod 8 et $a_1 \not\equiv$3 mod 8 en effet $\sqrt{-d} = 1 + 2 + 2^3 d_1$ ou $1 + 2^2 + 2^3 d_2$ avec $d_1, d_2 \in \mathbb{Z}_2$ si $d \not\equiv$-1 mod 16. $a_1 + 2^{\alpha-\beta}\sqrt{-d} = a_1 + 2 + 2^3 d_2$ ou $a_1 + 2^{\alpha-\beta}\sqrt{-d} = a_1 + 2 + 2^2 + 2^3 d_1$ une de ces deux quantités est dans $\mathbb{Q}_2{}^{*2}$ si et seulement si $a_1 \equiv$ -1 mod 8 ou $a_1 \equiv$3 mod 8 on en déduit le résultat . Si d$\equiv$-1 mod 16 alors $\sqrt{-d} = 1 + 2^3 d_1$ ou $1 + 2 + 2^2 + 2^3 d_2$ par conséquent $a_1 + 2^{\alpha-\beta}\sqrt{-d} = a_1 + 2 + 2^3 d_1$ ou $a_1 + 2^{\alpha-\beta}\sqrt{-d} = a_1 + 2 + 2^2 + 2^3 d_2$ une de ces deux quantités est dans $\mathbb{Q}_2{}^{*2}$ si et seulement si $a_1 \equiv$ -1 mod 8 ou $a_1 \equiv$3 mod 8 on endéduit le résultat .
Troisième cas : $\beta = \alpha$ :

Un raisonnement analogue permet de conclure , puisqu'ici il faudra chercher l'argument "plus loin" en utilisant bien sûr le lemme2.3.
Les parties B-1) et B-2) se déduisent de manière analogue de la partie A).
Enfin remarquons tout de même en posant :$\pm\sqrt{\pm d}=1+\sum_{i=1}^{i=\infty}2^i m_i$ , qu'à partir d'un certain rang tous les $m_i$ ne valent pas 0 car $\pm\sqrt{\pm d}\notin\mathbb{Q}$ . De maniére analogue on montre qu'à partir d'un certain rang tous les $m_i$ ne valent pas 1 car $-1=1+\sum_{i=1}^{i=\infty}2^i$ .

# Chapitre 5

## 5 Etude du niveau de $\mathbb{Q}_2(\xi_n)$ où $\xi_n$ est une racine primitive $n^{ième}$ de l'unité.

### 5.1 Préliminaire

Soit $S_n$ l'ensemble des solutions de l'équation $x^n - 1$ dans $\overline{\mathbb{Q}_p}$ la clôture algébrique de $\mathbb{Q}_p$ où p est premier quelconque. On sait que $S_n$ est un sous groupe fini du groupe multiplicatif du corps $\overline{\mathbb{Q}_p}$ , donc $S_n$ est cyclique en tant que groupe. Soit $\xi_n$ un générateur de $S_n$. $\mathbb{Q}(\xi_n)$ est un corps normal et le polynôme minimal de $\xi_n$ sur $\mathbb{Q}$ est le $n^{ième}$ polynôme cyclotomique. Il est évident que si 4 divise n alors $s(\mathbb{Q}_p(\xi_n)) = 1$. Car n=4k et ${\xi_n}^{2k} = -1$ (puisque $({\xi_n}^{2k} - 1)({\xi_n}^{2k} + 1) = 0 = {\xi_n}^n - 1$ ) et ${\xi_n}^{2k} \neq 1$ car l'ordre de la classe de $\xi_n$ dans $S_n$ est n ). Pour n=2h avec h impair alors $\mathbb{Q}_p(\xi_n) = \mathbb{Q}_p(\xi_h)$ en effet comme ${\xi_h}^n = ({\xi_h}^h)^2$, on en déduit que $S_h \subset S_n$ par suite $\mathbb{Q}_p(\xi_h) \subseteq \mathbb{Q}_p(\xi_n)$. Comme P.G.C.D.(h+1,n)=2 ,on en déduit que l'ordre de ${\xi_n}^{h+1}$ dans $S_n$ est n/2=h. donc ${\xi_n}^{h+1}$ engendre $S_h$ , mais $\xi_n = -(-\xi_n) = -{\xi_n}^{h+1}$ (car ${\xi_n}^h = -1$ d'où $\mathbb{Q}_p(\xi_n) \subseteq \mathbb{Q}_p(\xi_h)$ ). Quand n n'est pas divisible par 4 , on peut supposer n impair.

Dans le cas où n=2h , h impair , on sait que $\mathbb{Q}(\xi_n) = \mathbb{Q}(\xi_h)$. Rappelons quelques résultats bien connus :

**Proposition 5.1** [19] , *th.18.5 p.263.*
*Soit* $n \in \mathbb{N}^*$ , $n \geq 3$.
$s(\mathbb{Q}(\xi_n)) = 1 \Longleftrightarrow$ *4 divise n.*
*On peut supposer n impair quand il n'est pas divisible par 4 , alors en désignant par f l'ordre de la classe de 2 dans* $(\mathbb{Z}/n\mathbb{Z})^*$ *le groupe des unités de* $\mathbb{Z}/n\mathbb{Z}$ *on a :*
$s(\mathbb{Q}(\xi_n)) = 2 \Longleftrightarrow$ *f est pair.*
$s(\mathbb{Q}(\xi_n)) = 4 \Longleftrightarrow$ *f est impair.*

**Lemme 5.1** *( découle du lemme Chinois )*
*Soit n impair ,* $n \geq 3$;
$s(\ \mathbb{Q}(\xi_n)) = 4 \Longleftrightarrow \forall$ *p premier , p divisant n , l'ordre de la classe de 2 dans* $(\ \mathbb{Z}/p\ \mathbb{Z})^*$ *est impair.*
$s(\ \mathbb{Q}(\xi_n)) = 2 \Longleftrightarrow \exists$ *p premier , p divisant n , l'ordre de la classe de 2 dans* $(\ \mathbb{Z}/p\ \mathbb{Z})^*$ *est pair.*

**Théorème 5.1** [19] *corollaire 1 et 2 page 265.*
*On suppose p premier.*
*i)Si* $p \equiv 7\ mod\ 8$ *alors* $s(\ \mathbb{Q}(\xi_p)) = 4$.
*ii)Si* $p \equiv \pm\ 3\ mod\ 8$ *alors* $s(\ \mathbb{Q}(\xi_p)) = 2$.

**Remarque 5.1**
Le cas p≡ 1 mod 8 non envisagé dans le théorème est très compliqué , voir [11]. Par exemple pour p=73 on a : f=9 et $s(\ \mathbb{Q}(\xi_p)) = 4$ , alors que pour p=17 on a : f=8 et ainsi $s(\ \mathbb{Q}(\xi_p)) = 2$.
Il est donc très important de déterminer l'ordre de la classe de 2 dans $(\ \mathbb{Z}/p\ \mathbb{Z})^*$.
Nous donnons en appendice un algorithme permettant cette détermination.

## 5.2 Résultat principal

Passons à l'étude du niveau de $\mathbb{Q}_2(\xi_n)$.

**Proposition 5.2**
*Soit* $n \in \mathbb{N}^*$ , $n \geq 3$.
$s(\ \mathbb{Q}_2(\xi_n)) = 1 \Longleftrightarrow$ *4 divise n.*
*On peut supposer n impair quand n n'est pas divisible par 4 , alors en désignant par f l'ordre de la classe de 2 dans* $(\ \mathbb{Z}/n\ \mathbb{Z})^*$ *le groupe des unités de* $\mathbb{Z}/n\ \mathbb{Z}$ *on a :*
$s(\ \mathbb{Q}_2(\xi_n)) = 4 \Longleftrightarrow f$ *est impair.*
$s(\ \mathbb{Q}_2(\xi_n)) = 2 \Longleftrightarrow f$ *est pair.*

Démonstration
Si 4 divise n , il est évident que $s(\ \mathbb{Q}_2(\xi_n)) = 1$ d'après l'introduction. Réciproquement si $s(\ \mathbb{Q}_2(\xi_n)) = 1$ si n n'est pas divisible par 4 d'après ce

qui est dit dans l'introduction on peut supposer n impair.Comme l'extension $\mathbb{Q}_2 \longrightarrow \mathbb{Q}_2(\xi_n)$ est cyclique non ramifiée , alors d'après la proposition 16 § 4 de [5].La théorie de Galois dit que $\mathbb{Q}_2(\xi_n)$ contient une extension unique F de degré 2 sur $\mathbb{Q}_2$. La formule des indices de ramifications donne : $1 = e_{\mathbb{Q}_2(\xi_p)/\mathbb{Q}_2} = e_{\mathbb{Q}_2(\xi_p)/F}.e_{F/\mathbb{Q}_2}$ , on en déduit que $e_{F/\mathbb{Q}_2} = 1$,donc l'extension $\mathbb{Q}_2 \longrightarrow F$ est non ramifiée. Or la seule extension non ramifiée de $\mathbb{Q}_2$ est $\mathbb{Q}_2(\sqrt{5})$ cf.[4] , p. 133. On en déduit que $F = \mathbb{Q}_2(\sqrt{5})$. Comme $s(\mathbb{Q}_2(\xi_n)) = 1$, $\mathbb{Q}_2(\xi_n)$ contient $\mathbb{Q}_2(\sqrt{-1})$ qui est aussi de degré 2 sur $\mathbb{Q}_2$. Ceci est en contradiction avec l'unicité de F.
Donc on a bien 4 divise n.
On suppose maintenant n impair.
Comme on sait aussi que $[\mathbb{Q}_2(\xi_n) : \mathbb{Q}_2] = f$ où f est l'ordre de la classe de 2 dans $(\mathbb{Z}/n\mathbb{Z})^*$ d'après le corollaire 1 § 4 de[5].Donc si f est impair le théorème de Springer et le fait que $s(\mathbb{Q}_2) = 4$ permettent de dire que $s(\mathbb{Q}_2(\xi_n)) = 4$.Si f est pair alors $\mathbb{Q}_2(\xi_n)$ contient un sous-corps F de degré 2 sur $\mathbb{Q}_2$. Comme n n'est pas divisible par 4 , $F \neq \mathbb{Q}_2(\sqrt{-1})$.Et on sait bien que les autres extensions quadratiques de $\mathbb{Q}_2$ (i.e différentes de $\mathbb{Q}_2(\sqrt{-1})$ ) sont toutes de niveau 2 cf.[14] ( ce résultat se vérifie facilement à la"main" ).On en déduit que $s(\mathbb{Q}_2(\xi_n)) = 2$. Ce qui démontre les deux dernières équivalences.

Conclusion : $\forall n \geq 3$ , $s(\mathbb{Q}_2(\xi_n)) = s(\mathbb{Q}(e^{\frac{2i\pi}{n}}))$.

# Chapitre 6

## 6 Etude du niveau de $\mathbb{Q}_p(\xi_n)$ , p premier impair où $\xi_n$ est une racine primitive $n^{ème}$ de l'unité.

Soit $\xi_n$ une racine primitive de l'unité dans une clôture algébrique de $\mathbb{Q}_p$ où p est premier impair.

Rappel : $s(\mathbb{Q}_p) = 1$ si $p \equiv 1 \bmod 4$ , $s(\mathbb{Q}_p) = 2$ si $p \equiv 3 \bmod 4$ cf.[19] , p.260. on en déduit que $s(\mathbb{Q}_p(\xi_n) \leq 2$.

Il est évident que si $p \equiv 1 \bmod 4$ alors $s(\mathbb{Q}_p(\xi_n) = 1$.
On peut dès lors supposer que $n \geq 3$ et $p \equiv 3 \bmod 4$.
On a vu à l'introduction du chapitre préc'edent que si n=2m avec m impair alors : $\mathbb{Q}_p(\xi_n) = \mathbb{Q}_p(\xi_m)$.
Cas 1 : p et n sont premiers entre eux.

**Proposition 6.1**
*Soit $n \in \mathbb{N}^*$ , $n \geq 3$ et n et p premiers entre eux.*
*Si 4 divise n alors $s(\mathbb{Q}_p(\xi_n)) = 1$.*
*On peut supposer n impair quand n n'est pas divisible par 4 , alors en désignant par f l'ordre de la classe de p dans $(\mathbb{Z}/n\mathbb{Z})^*$ le groupe multiplicatif de l'anneau $\mathbb{Z}/n\mathbb{Z}$ on a :*
$s(\mathbb{Q}_p(\xi_n)) = 1 \Longleftrightarrow$ *f est pair.*
$s(\mathbb{Q}_p(\xi_n)) = 2 \Longleftrightarrow$ *f est impair.*

Démonstration
La première affirmation est claire d'après l'introduction du chapitre précédent.
Si f est impair alors le théorème de Springer permet de dire que $s(\mathbb{Q}_p(\xi_n)) = s(\mathbb{Q}_p) = 2$. Soit $k_n$ le corps résiduel de $\mathbb{Q}_p(\xi_n)$ et $k = \mathbb{F}_p$ alors $[\mathbb{Q}_p(\xi_n) : \mathbb{Q}_p] = [k_n : \mathbb{F}_p] = f$ où f est l'ordre de la classe de p dans $(\mathbb{Z}/n\mathbb{Z})^*$ d'après le corollaire 1 § 4 de la proposition 16 [5]. Si f est pair

alors $s(k_n) = 1$ d'après le théorème 3.4 de [19]. L'équation P=$X^2 + 1$ a donc une solution dans $\mathbb{Q}_p(\xi_n)$ d'après le Lemme de Hensel cf.[4] , p.49 car $\exists \alpha \in \mathbb{Q}_p(\xi_n)$ tel que $|P(\alpha)|_2 < 1 = |P'(\alpha)|_2^2$ , d'où $s(\mathbb{Q}_p(\xi_n)) = 1$.

**Corollaire 6.1**
*Soit n impair , $n \geq 3$ ;*
$s(\mathbb{Q}_p(\xi_n)) = 2 \Longleftrightarrow \forall$ *q premier divisant n , l'ordre f de la classe de p dans* $(\mathbb{Z}/q\mathbb{Z})^*$ *est impair.*
$s(\mathbb{Q}_p(\xi_n)) = 1 \Longleftrightarrow \exists$ *q premier divisant n , l'ordre f de la classe de p dans* $(\mathbb{Z}/q\mathbb{Z})^*$ *est pair.*

Démonstration
Résulte du théorème Chinois et du fait bien connu que si $2^f \equiv 1$ mod p alors $2^f$=1+kp , et alors $2^{fp^{\alpha-1}} \equiv 1 \bmod p^\alpha$.

**Corollaire 6.2**
*On suppose $q \geq 3$ et q premier différent de p.*
*Si* $\left(\frac{p}{q}\right) = -1$ *où* ($\left(\frac{\cdot}{q}\right)$ *désigne le symbole de Legendre* ) *alors f est pair et par conséquent* $s(\mathbb{Q}_p(\xi_q)) = 1$.

Démonstration
Sinon f est impair et alors $p^{f+1} \equiv$ p mod q. Et p est un résidu quadratique modulo q.Ce qui est en contradiction avec notre hypothèse.

**Corollaire 6.3**
*On suppose $q \geq 3$ et q premier différent de p.*
*Si* $q \equiv 3 \bmod 4$ *et* $\left(\frac{p}{q}\right) = 1$ *alors* $s(\mathbb{Q}_p(\xi_q)) = 2$.

Démonstration
Car comme $p \equiv u^2$ mod q et $p^{\frac{q-1}{2}} \equiv u^{q-1} \equiv 1$ mod q et (q-1)/2 est impair le résultat s'ensuit.

## 6.1 Contre-exemple

**Exemple 6.1**
Pour p=23 et q=17 , On vérifie que $\left(\frac{p}{q}\right) = -1$. Et l'ordre de la classe de

p ( qui est différent de la classe de 1) dans ( $\mathbb{Z}/17\ \mathbb{Z})^*$ est pair car il divise 16. Ce qui signifie que $s(\ \mathbb{Q}_{23}(\xi_{17})) = 1$.
Pour q=73 , alors on sait que ( $\mathbb{Z}/73\ \mathbb{Z})^*$ est engendré par la classe de 5.Le théorème de Dirichlet dit que si a et b sont deux entiers naturels non nuls premiers entre eux il existe une infinité de nombre premiers de la forme a+bn où n est un entier naturel. Comme $(5^8 + 2 \times 73)$ et $73 \times 8$ sont premiers entre eux , on peut choisir un nombre premier p=$(5^8 + 2 \times 73)+73 \times 8$k , avec k entier naturel. On vérifie que ce p est congru à 3 mod 4 , q congru à 1 modulo 4 et $\left(\begin{array}{c} p \\ q \end{array}\right) = 1$. Mais l'ordre de la classe de p qui est l'ordre de la classe de $5^8$ dans ( $\mathbb{Z}/73\ \mathbb{Z})^*$ est 72/8=9 , donc impair. On en déduit que $s(\ \mathbb{Q}_p(\xi_{73})) = 2$. Il existe même une infinité de tels nombres premiers. En posant p=$(5 + 2 \times 73)+73 \times 8$k , on obtient par un raisonnemet analogue à ce qui précéde une infinité de nombres premiers p tels que $s(\ \mathbb{Q}_p(\xi_{73})) = 1$.
Cet exemple montre que si $p \equiv 3 \bmod 4$ , $q \equiv 1 \bmod 4$ et $\left(\begin{array}{c} p \\ q \end{array}\right) = 1$ alors $s(\ \mathbb{Q}_p(\xi_q))$ peut prendre les deux valeurs 1 ou 2.

Cas 2: n et p ne sont pas premiers entre eux.

**Proposition 6.2**
*Soit $n = p^\alpha m$ avec p premier ne divisant pas m , $\alpha \geq 1$.*
*Si 4 divise n alors $s(\ \mathbb{Q}_p(\xi_n)) = 1$.*
*Si m=1 alors $s(\ \mathbb{Q}_p(\xi_n)) = 2$.*
*On peut supposer n impair quand n n'est pas divisible par 4 et $m \geq 3$ , alors en désignant par f l'ordre de la classe de p dans ( $\mathbb{Z}/m\ \mathbb{Z})^*$ le groupe des unités de $\mathbb{Z}/m\ \mathbb{Z}$ on a :*
*$s(\ \mathbb{Q}_p(\xi_n)) = 1 \Longleftrightarrow$ f est pair.*
*$s(\ \mathbb{Q}_p(\xi_n)) = 2 \Longleftrightarrow$ f est impair.*

Démonstration
La première affirmation est claire.
L'extension $Q_p(\xi_{p^\alpha})/\ \mathbb{Q}_p$ est totalement ramifiée d'après la proposition 17 §4 de [22]. Donc si $k_{p^\alpha}$ désigne le corps résiduel de $Q_p(\xi_{p^\alpha})$ et $k = \mathbb{F}_p$ celui de $\mathbb{Q}_p$ alors $[k_{p^\alpha} : \mathbb{F}_p] = 1$. Donc $k_{p^\alpha} = \mathbb{F}_p$ et grâce au lemme de Hensel , on a facilement $s(\ \mathbb{Q}_p(\xi_{p^\alpha})) = s(k_{p^\alpha}) = s(\ \mathbb{F}_p) = 2$ , la deuxième assertion s'ensuit.
Or on a $\mathbb{Q}_p(\xi_{p^\alpha})(\xi_m) = \mathbb{Q}_p(\xi_n)$ , donc on peut appliquer la proposition 16 §

4 de [22] avec K= $\mathbb{Q}_p(\xi_{p^\alpha})$. On en déduit que $[\mathbb{Q}_p(\xi_{p^\alpha})(\xi_m) : \mathbb{Q}_p(\xi_{p^\alpha})] = f$ et si f est impair le théorème de Springer permet de dire que
$s(\mathbb{Q}_p(\xi_n)) = s(\mathbb{Q}_p(\xi_{p^\alpha})) = 2$.
Soit $k_n$ le corps résiduel de $\mathbb{Q}_p(\xi_n)$ et $k = \mathbb{F}_p$ alors : $[\mathbb{Q}_p(\xi_n) : \mathbb{Q}_p] = [k_n : \mathbb{F}_p] = f$ où f est l'ordre de la classe de p dans $(\mathbb{Z}/m\,\mathbb{Z})^*$ d'après le corollaire 1 §4 de [22].Si f est pair alors : $s(k_n) = 1$ d'après le théorème 3.4 [19]. L'équation $X^2 + 1$ a donc une solution dans $\mathbb{Q}_p(\xi_n)$ d'après le lemme de Hensel , d'où $s(\mathbb{Q}_p(\xi_n)) = 1$.

# Chapitre 7

# 7 Etude du Niveau d'Extensions Kümmériennes

## 7.1 Introduction

***Définition 7.1***
*Soit $n \geq 3$ , $K$ un corps de nombres contenant toutes les racines $n^{ième}$ de l'unité (donc $K$ contient une racine primitive $n^{ième}$ de l'unité).On dit qu'une extension $L$ de $K$ est une extension kümmérienne de $K$ s'il existe $\alpha \in \mathbb{C}$ tel que $L = K(\alpha)$ où le polynôme minimal de $\alpha$ sur $K$ est de la forme $X^n - a$ , $a \in K$.*

Propriétés :

a) Une extension kümmérienne de K est une extension cyclique de K (i.e. une extension galoisienne dont le groupe de Galois est cyclique).
b)Toute extension galoisienne cyclique de K de degré n est une extension kümmérienne de K.
c)Soit L une extension kümmérienne de K , $L = K(\alpha)$ où le polynôme minimal de $\alpha$ sur K est de la forme $X^n - a$. Pour qu'il existe $\beta \in L$ tel que $L = K(\beta)$ où $\beta$ est une racine de $X^n - b$ , avec $b \in K$ , il faut et il suffit qu'il existe $\gamma \in L$ tel que $c = \frac{a}{b} = \gamma^n = N_{L/K}(\gamma)$.
Démonstration
Si $L = K(\beta)$ où $\beta$ est une racine de $X^n - b$ , avec $b \in K$.
Soit $\gamma = \frac{\alpha}{\beta} \in L$ alors $\gamma^n = \frac{a}{b} = c \in K$ , en posant $\omega$ une racine primitive $n^{ième}$ de l'unité.

$$N_{L/K}(\gamma) = \gamma^n = \frac{\prod_{i=0}^{n-1}(\omega^i \alpha)}{\prod_{i=0}^{n-1}(\omega^i \beta)} = \frac{\alpha^n}{\beta^n} = \frac{a}{b} = c \in K.$$

Réciproqument , pour tout $\gamma \in L$ $(\gamma \neq 0)$ tel que $c = \gamma^n = N_{L/K}(\gamma) \in K$. En posant $\beta = \gamma\alpha$ alors $\beta^n = \gamma^n \alpha^n = ca = b$ et les conjugués de $\beta$ sont : $\omega^l \beta$ pour $l = 0, \cdots, n-1$ et ces éléments sont distincts deux à deux donc le

polynôme $X^n - b$ est irréductible sur K et par conséquent $L = K(\beta)$.

## 7.2 Etude du niveau des extensions kümmériennes

**Proposition 7.1**
*Soit L une extension kümmerienne de K i.e.*$L = K(\alpha)$ *où le polynôme minimal de* $\alpha$ *sur K est* $X^n - a$ *où* $n \geq 3$ , $a \in K$ *alors on a en posant* $K_n = \mathbb{Q}(e^{\frac{2i\pi}{n}})$ :
*Si 4 divise n alors* $s(L) = s(K) = s(K_n) = 1$.
*Si n est impair alors :* $s(L) = s(K) \leq s(K_n)$ , $(2 \leq s(K_n) \leq 4$ *).*
*Si n=2k avec k impair alors :* $L = K(\alpha^k)(\alpha^2)$ *; Si -a est somme de n carrés et non de n-1 carrés de K posons* $k \in N$ *tel que* $2^k \leq n < 2^{k+1}$ , *alors on a :* $s(L) = min(s(K), 2^k)$.

Démonstration
On remarque que les résultats énoncés dans le théorème ne dépendent pas de l'élément primitif $\alpha$ en effet , supposons que $L = K(\beta)$ avec le polynôme minimal de $\beta$ sur K égal à $X^n - b$. Il suffit de considérer le cas n=2k , avec k impair : d'après la remarque a) , en posant $\gamma = \frac{\alpha}{\beta}$ on a : $c = \frac{a}{b} = \gamma^n = N_{L/K}(\gamma)$.
Soit $\sigma \in Gal(L/K)$ le groupe de galois de L sur K tel que $\langle\sigma\rangle = Gal(L/K)$ puisque ce groupe est cyclique. On peut supposer que $\sigma(\gamma) = \gamma\omega^l$ , où $\omega$ est une racine primitive de l'unité et pour un certain $l \in \{0, \cdots, n-1\}$ , car $(\frac{\sigma(\gamma)}{\gamma})^n = \frac{\sigma(\gamma^n)}{\gamma^n} = \frac{\gamma^n}{\gamma^n} = 1$.
$\gamma^n = N_{L/K}(\gamma) = \prod_{j=1}^n \sigma^j(\gamma) = \gamma^n \prod_{j=1}^n \omega^{lj} = \gamma^n \omega^{l\frac{n(n+1)}{2}} \Longrightarrow \omega^{l\frac{n(n+1)}{2}} = 1$
donc n divise $l\frac{n(n+1)}{2} \Longrightarrow (n+1)l = 2h$ où $h \in N$ ce qui implique que 2 divise l , car n est pair et n+1 est impair. $\gamma^k = \sigma(\gamma^k)$ d'où $\gamma^k \in K$ ( car ceci est vrai $\forall\phi \in Gal(L/K)$ puisque $\phi = \sigma^j$ avec $j \in \{0, \cdots, n-1\}$ on a : $\phi(\gamma^k) = \gamma^k$ ) d'où $(\gamma^k)^2 = \gamma^n = c$ i.e. c est un carré dans K.
Comme b=ac le résultat s'ensuit.
On revient à la démonstration du théorème.
On suppose toujours que n=2k avec k impair , on a :
$K \xrightarrow{2} K(\alpha^k) \xrightarrow{k} K(\alpha^k)(\alpha^2) = L$ , le théorème de Springer implique que $s(L) = s(K(\alpha^k))$.
Or $Irr(\alpha^k, K) = X^2 - a$ et on détermine $s(K(\alpha^k))$ grâce à la proposition 2.1

et on en déduit le résultat énoncé.

**Corollaire 7.1**
*Dans le théoème 6.1 si* $K = K_n = \mathbb{Q}(e^{\frac{2i\pi}{n}})$ *et* $L = K(\alpha)$ *avec* $min(\alpha, K) = X^n - a$.
*Si -a est somme de n carrés et non de n-1 carrés dans K posons* $h \in N$ *tel que* $2^h \leq n < 2^{h+1}$ *, alors on a :* $s(L) = min(s(K), 2^h)$.

Remarque le problème de détermination de niveau d'une extension kümmérienne de K revient au probléme de détermination des carrés de K et des sommes de trois carrés dans K et des éléments de K qui ne sont pas somme de trois carrés de K. Ici a n'est pas dans $\mathbb{Q}$ puisque sinon n$\phi(n)$=n et $\phi(n)$=1 donc n=1 ou n=2 ce qui est écarté par $n \geq 3$.

Sachant comment calculer la norme dans $\mathbb{Q}_p(e^{\frac{2i\pi}{n}})$ , on obtient le résultat suivant sans difficulté en utilisant le théorème 16.10 page 236 de [20] et le lemme2.2 d).

**Corollaire 7.2**
*Si* $K=K_n=\mathbb{Q}(e^{\frac{2i\pi}{n}})$ *et* $L=K(\alpha)$ *avec* $min(\alpha\ ,\ K)=X^n-a$ .
$s(L)=1 \Longleftrightarrow$ *4 divise n ou -a est un carré dans K.*
*On suppose maitenant que -a n'est pas un carré dans K et 4 ne divise pas n , alors :*
*Si n est impair alors :* $s(L) = s(K)$ .
*Si n est pair en posant* $N_{\mathbb{Q}_2(e^{\frac{2i\pi}{n}})/\ \mathbb{Q}_2}(-a) = d = 4^\beta d_1$ *(car* $d \in \mathbb{Z}_2$ *) avec* $d_1$ *non divisible par 4 alors :*
$s(L)=2 \Longleftrightarrow$ $(s(K) = 4$ *et* $d \not\equiv 1 \bmod 8$ *)* *ou* $s(K) = 2$ .
$s(L)=4 \Longleftrightarrow$ $d \equiv 1 \bmod 8$ *et* $s(K) = 4$.

# Chapitre 8

# 8 Appendice

## 8.1 Algorithme pour déterminer l'ordre de la classe de 2 dans ( $\mathbb{Z}/p\,\mathbb{Z})^*$ où $p \equiv 1 \bmod 8$.

Ecrivons p-1=fg où f est l'ordre de la classe de 2 dans ( $\mathbb{Z}/n\,\mathbb{Z})^*$.

On va mettre en évidence un algorithme qui permet de calculer g au lieu de f.Car si on travaille directement avec des puissances de 2 , on risque de dépasser facilement p. L'avantage de cet algorithme c'est qu'on travaille avec des nombres inférieurs à p pour déterminer f. Les exemples à la fin montre que ceci peut se faire " à la main" bien sûr pour des p pas "trop grands ". Mais ceci est facilement programmable sur ordinateur.

Nous allons rappeler quelques théorèmes très importants que nous allons utiliser par la suite.

***Théorème 8.1*** *, [15] 8 , théorème4.14 p.167.*
*Soit $K = \mathbb{Q}(\xi_p)$ et $R_K$ l'anneau des entiers de K. Soit f l'ordre de la classe de 2 dans ( $\mathbb{Z}/p\,\mathbb{Z})^*$ , alors l'idéal engendré par 2 dans $R_K$ se décompose en produit d'idéaux premiers deux à deux distincts : $2R_K = \wp_1 \cdots \wp_g$ où fg=p-1.*

***Théorème 8.2*** *[16] , théorème2.17 chap.2.*
*Soit $K = \mathbb{Q}(\theta)$ , $\theta \in R_K$ (l'anneau des entiers de K ) et $f_\theta(X) \in \mathbb{Z}[X]$. le polynôme minimal de $\theta$. On suppose que $R_K = \mathbb{Z}[\theta]$. Soit $f_\theta(X) = \varphi_1^{e_1} \cdots \varphi_g(X)^{e_g} \bmod p$ , la décomposition de $f_\theta(X)$ mod p où chaque $\varphi_i(X) \in \mathbb{Z}[X]$ est unitaire et irréductible modulo p. Alors , $\wp_i = (p, \varphi_i(\theta))$ est un idéal premier et on a : $pR_K = \wp_1^{e_1} \cdots \wp_g^{e_g}$ avec le degré résiduel de $\wp_i$ est égal au degré de $\varphi_i$ où $1 \leq i \leq g$.*

*Soit $P = min(\xi_p, \mathbb{Q})$ ,alors P est le $p^{ième}$ polynôme cyclotomique. Soit $\mathbf{F} = \mathbb{F}_2 \simeq (\mathbb{Z}/2\,\mathbb{Z})$.*
*L'application $\mathbf{F}[X] \longrightarrow \mathbf{F}[X]$ , $T(X) \longmapsto T(X^2)$ est $\mathbf{F}$-linéaire , et elle envoie l'idéal $P\mathbf{F}[X]$ dans lui-même. Donc cette application passe au quotient par l'idéal $P\mathbf{F}[X]$, ce qui permet de définir un endomorphisme*
*$u \in Hom_F(\mathbf{F}[X]/P\mathbf{F}[X])$.*

***Théorème 8.3*** [1] , *p.106.*
*En posant* $A = \mathbf{F}[X]/P\mathbf{F}[X]$ , $N = Ker(u - id_A)$ , *alors on a :* $dim_F(N) = g$ *où (p-1)=fg et f l'ordre de la classe de 2 dans* ( $\mathbb{Z}/p\,\mathbb{Z}$)$^*$.

*Par abus de notation , on note encore X la classe de X modulo P. Une base de A sur* $\mathbf{F}$ *est :* $(X^i)_{0\leq i\leq p-2}$. *En pose* $e_i = (u - id_A)(X^i)$ *pour* $0 \leq i \leq p-2$*;on a* $e_0 = 0$*;*$e_i = X^{2i} - X^i$ *pour*
$1 \leq i \leq (p-3)/2$*;*$e_{(p-1)/2} = -1 - X - \cdots - X^{(p-3)/2} - 2X^{(p-1)/2} - X^{(p+1)/2} - \cdots - X^{(p-2)}$
$e_i = X^{2i-p} - X^i$ ,$(p+1)/2 \leq i \leq p-2$ *ou encore* $e_{(p-1)/2+i} = X^{2i-1} - X^{(p-1)/2+i}$ *pour* $1 \leq i \leq (p-3)/2$ ,

$$\sum_{i=0}^{p-2} \lambda_i e_i = \sum_{i=1}^{(p-1)/2} \lambda_i (X^{2i} - X^i) + \sum_{i=(p+1)/2}^{p-2} \lambda_i (X^{2i-p} - X^i) = 0$$

*avec* $\lambda_i \in \mathbf{F}$ , $\lambda_0$ *quelconque et* $\lambda_{(p-1)/2} = 0$

$$\sum_{i=1}^{(p-3)/2} \lambda_i X^i = \sum_{i=1}^{(p-5)/4} \lambda_{2i} X^{2i} + \sum_{i=1}^{(p-1)/4} \lambda_{2i-1} X^{2i-1}$$

$$\sum_{i=(p+1)/2}^{p-2} \lambda_i X^i = \sum_{i=(p+3)/4}^{(p-3)/2} \lambda_{2i} X^{2i} + \sum_{i=(p+3)/4}^{(p-1)/2} \lambda_{2i-1} X^{2i-1}$$

$$\sum_{i=(p+1)/2}^{(p-2)} \lambda_i X^{2i-p} = \sum_{i=1}^{(p-3)/2} \lambda_{(p-1)/2+i} X^{2i-1}$$

$$\sum_{i=1}^{(p-3)/2} \lambda_i X^{2i} - \sum_{i=1}^{(p-5)/4} \lambda_{2i} X^{2i} - \sum_{i=(p+3)/4}^{(p-3)/2} \lambda_{2i} X^{2i} = \sum_{i=1, i\neq(p-1)/4}^{(p-3)/2} (\lambda_i - \lambda_{2i}) X^{2i} + \lambda_{(p-1)/4} X^{(p-1)/2} = 0.$$

$$\sum_{i=(p+1)/2}^{p-2} \lambda_i X^{2i-p} - \sum_{i=1}^{(p-1)/4} \lambda_{2i-1} X^{2i-1} - \sum_{i=(p+3)/4}^{(p-1)/2} \lambda_{2i-1} X^{2i-1} =$$

$$\sum_{i=1}^{(p-3)/2} (\lambda_{(p-1)/2+i} X^{2i-1} - \sum_{i=1}^{(p-1)/4} \lambda_{2i-1} X^{2i-1} - \sum_{i=(p+3)/4}^{(p-1)/2} \lambda_{2i-1} X^{2i-1} =$$

$$\sum_{i=1}^{(p-3)/2} (\lambda_{(p-1)/2+i} - \lambda_{2i-1}) X^{2i-1} - \lambda_{p-2} X^{p-2} = 0.$$

*Ce qui conduit au système suivant :* $\begin{cases} \lambda_0 \text{ quelconque }, \lambda_{(p-1)/2} = \lambda_{(p-1)/4} = \lambda_{p-2} = 0 \\ \lambda_i = \lambda_{2i} \text{ avec } 1 \leq i \leq (p-3)/2 \\ \lambda_{(p-1)/2+j} = \lambda_{2j-1} \text{ avec } 1 \leq j \leq (p-3)/2 \end{cases}$

*Pour i pair* $i \leq (p-3)/2$*,on cherche les* $\lambda_j$ *tels que* $\lambda_j = \lambda_i$*. On cherche le nombre maximum de* $\lambda_i$ *pouvant être choisi arbitrairement : comme* $\lambda_{2i} = \lambda_i$ *on peut se limiter à i impair.*

*Ce qui conduit à l'algorithme suivant :*

*1 étape : On fait corespondre les 2i-1 aux (p-1)/2+i tels que* $\lambda_{(p-1)/2+i} = \lambda_{2i-1}$ *pour* $1 \leq i \leq (p-1)/4$ *et i pair. (cf. sur la figure 1 pour* $p = 41$ *).*

*2 étape : Pour* $1 \leq i \leq (p-1)/4$ *et i pair on factorise (p-1)/2+i sous la forme* $2^{\alpha}\gamma$ *avec* $\gamma$ *impair.*

*3 étape : On fait correspondre chaque 2i-1 au* $\gamma$ *ainsi trouvé ,sauf pour celui qui n'avait pas de correspondance pair ,on lui associe p-2.*

*4 étape :On calcule le nombre de classes. Chaque classe étant obtenue en partant d'un i*
*quelconque , on lui fait correspondre* $\gamma$ *puis à* $\gamma$ *on associe* $\gamma'$ *ainsi de suite jusqu'à retrouver i.*

***Exemple 8.1***

| *p=41 , 1ière étape.* | | | | |
|---|---|---|---|---|
| *1* | *21* | *31* | **36** | |
| *3* | **22** | | | |
| *5* | *23* | **32** | | |
| *7* | **24** | | | |
| *9* | *25* | *33* | *37* | *39* |
| *11* | **26** | | | |
| *13* | *27* | **34** | | |
| *15* | **28** | | | |
| *17* | *29* | *35* | **38** | |
| *19* | **30** | | | |

| *p=41 ,2ième étape.* | |
|---|---|
| *1* | *36=4× 9* |
| *3* | *22=2× 11* |
| *5* | *32=32× 1* |
| *7* | *24=8× 3* |
| *9* | 39 |
| *11* | *26=2×13* |
| *13* | *34=2×17* |
| *15* | *28=4×7* |
| *17* | *38=2×19* |
| *19* | *30=2×15* |

| *p=41 , 3ième étape.* | |
|---|---|
| *1* | *9* |
| *3* | *11* |
| *5* | *1* |
| *7* | *3* |
| *9* | 39 |
| *11* | *13* |
| *13* | *17* |
| *15* | *7* |
| *17* | *19* |
| *19* | *15* |
| *39* | *5* |

*On obtient deux classes :*

$1^{ère}$ *classe* $1 \longrightarrow 9 \longrightarrow 39 \longrightarrow 5 \longrightarrow 1$

$2^{ème}$ *classe* $3 \longrightarrow 11 \longrightarrow 13 \longrightarrow 17 \longrightarrow 19 \longrightarrow 15 \longrightarrow 7 \longrightarrow 3$

*Par conséquent g=2 et f=20 , donc* $s(\mathbb{Q}(\xi_{41})) = 2$.

***Exemple 8.2***

| $p=73$ , $1^{ière}$ étape. | | | | | |
|---|---|---|---|---|---|
| 1 | 37 | 55 | **64** | | |
| 3 | **38** | | | | |
| 5 | 39 | **56** | | | |
| 7 | **40** | | | | |
| 9 | 41 | 57 | 65 | 69 | 71 |
| 11 | **42** | | | | |
| 13 | 43 | **58** | | | |
| 15 | **44** | | | | |
| 17 | 45 | 59 | **66** | | |
| 19 | **46** | | | | |
| 21 | 47 | **60** | | | |
| 23 | **48** | | | | |
| 25 | 49 | 61 | 67 | **70** | |
| 27 | **50** | | | | |
| 29 | 51 | **62** | | | |
| 31 | **52** | | | | |
| 33 | 53 | 63 | **68** | | |
| 35 | **54** | | | | |

| $p=73$ , $2^{ième}$ étape. | |
|---|---|
| 1 | $64=64\times 1$ |
| 3 | $38=2\times 19$ |
| 5 | $56=8\times 7$ |
| 7 | $40=8\times 5$ |
| 9 | $71=71$ |
| 11 | $42=2\times 21$ |
| 13 | $58=2\times 29$ |
| 15 | $44=4\times 11$ |
| 17 | $66=2\times 33$ |
| 19 | $46=2\times 23$ |
| 21 | $60=4\times 15$ |
| 23 | $48=16\times 3$ |
| 25 | $70=2\times 35$ |
| 27 | $50=2\times 25$ |
| 29 | $62=2\times 31$ |
| 31 | $52=4\times 13$ |
| 33 | $68=4\times 17$ |
| 35 | $54=2\times 27$ |

| $p=73$ ,$3^{ème}$ étape. | |
|---|---|
| 1 | 1 |
| 3 | 19 |
| 5 | 7 |
| 7 | 5 |
| 9 | 71 |
| 11 | 21 |
| 13 | 29 |
| 15 | 11 |
| 17 | 33 |
| 19 | 23 |
| 21 | 15 |
| 23 | 3 |
| 25 | 35 |
| 27 | 25 |
| 29 | 31 |
| 31 | 13 |
| 33 | 17 |
| 35 | 27 |
| 71 | 9 |

*On obtient huit classes :*
$1^{ère}$ *classe* $1 \longrightarrow 1$.
$2^{ème}$ *classe* $3 \longrightarrow 19 \longrightarrow 23 \longrightarrow 3$.
$3^{ème}$ *classe* $5 \longrightarrow 7 \longrightarrow 5$.
$4^{ème}$ *classe* $9 \longrightarrow 71 \longrightarrow 9$.
$5^{ème}$ *classe* $11 \longrightarrow 21 \longrightarrow 15 \longrightarrow 11$.
$6^{ème}$ *classe* $13 \longrightarrow 13 \longrightarrow 29 \longrightarrow 31 \longrightarrow 13$.
$7^{ème}$ *classe* $17 \longrightarrow 33 \longrightarrow 17$.
$8^{ème}$ *classe* $25 \longrightarrow 35 \longrightarrow 27 \longrightarrow 25$.
*On obtient* $g=8$ *et* $f=9$ *, donc* $s(\mathbb{Q}(\xi_{73})) = 4$.
*Je dispose d'un tel algorithme programmé en Turbo Pascal pouvant chercher tous les nombres premiers p inférieurs ou égals à 64000 , congrus à*

*1 modulo 8 et affichant l'ordre de la classe de 2 dans* $(\mathbb{Z}/p\,\mathbb{Z})^*$. *Une légère amélioration de ce programme permet d'aller jusqu'à* $p \leq 10^{31}$.

## 8.2 Algorithme et Résultats pour $p \leq 30000$.

```
program nbprem;
uses crt;
const
  NN=64000;
type
 entier=1..NN;
 enr=record
       c1,c2:longint;
       c3:boolean;
      end;
 fichier=file of enr;
var
  crible:packed array[entier] of boolean;
  nombre:longint;
  nb,ii,kk:longint;
  sauve:text;
  f:fichier;
procedure classes(p:longint);
var
   t:enr;
   nbc,n,k,i:longint;
begin
  {Creation du fichier contenant les deux colonnes de nombres }
  rewrite(f);
  for i:=1 to trunc((p-1)/4) do
  begin
       t.c1:=2*i-1;
       t.c2:=trunc((p-1)/2)+i;
       t.c3:=tue;
       write(f,t);
  end;
 close(f);
```

```
 reset(f);
 k:=trunc((p/4)*3-3/4)+1);
 repeat
   read(f,t);
   if t.c2 mod2 <> 0 then
      begin
        seek(f,filepos(f)-1);
        t.c2:=k;
        write(f,t);
        inc(k);
      end;
   if eof(f) then seek(f,0);
 until (k>p-2);
 seek(f,0);
 for i:=1 to trunc((p-1)/4) do
     begin
       read(f,t);
       while t.c2 mod 2 = 0 do
         begin
           t.c2:=trunc(t.c2/2);
         end;
       seek(f,filepos(f)-1);
       write(f,t);
     end;
close(f);
  { Recherche du nombre de classes }
nbc:=1;
reset(f);
read(f,t);
  while t.c2<>p-2 do
     read(f,t);
repeat
 n:=t.c1;
 t.c3:=false;
 seek(f,filepos(f)-1);
 write(f,t);
 seek(f,0);
```

```
 while (not eof(f)) and (t.c2<>n) do
     read(f,t);
until t.c2<>n ;
repeat
 seek(f,0);
 read(f,t);
 while(not eof(f)) and (not t.c3) do
 if not eof(f) then
    begin
      nbc:=nbc+1;
      i:=t.c1;
      repeat
        n:=t.c2;
        t.c3:=false;
        seek(f,filepos(f)-1);
        write(f,t);
        seek(f,trunc(n/2));
        read(f,t);
      until n=i;
    end;
 until eof(f);
close(f);
writeln(p,' f=',trunc((p-1)/nbc));
append(sauve);{ Remplacer par rewrite(sauve) pour creer le fichier }
writeln(sauve,'Nb premier:',p,' Ordre f = ',trunc((p-1)/nbc));
close(sauve);
end;
begin
   assign(sauve,'c:\nbre\resultat.txt');
   assign(f,'nbp.lis');
   clrscr;
   for ii:=1 to nn do crible[ii]:=true;
   nombre:=2;
   nb:=nn-1;
   kk:=1;
   repeat
     while not(crible[nombre]) do
```

```
        nombre:=succ(nombre);
        if (nombre-1)/8=(nombre-1) div 8 then
        begin
          classes(nombre);
          inc(kk);
        end;
     ii:=nombre;
    while ii<=nn do
     begin
        if crible[ii] then
        begin
          crible[ii]:=false;
          nb:=nb-1;
       end;
      ii:=ii+nombre;
     end;
   until nb=0;
 readln;
end.
```

Résultat à l'exécution :(page suivante)

| p | ordre de $\bar{2}$ dans ( $\mathbb{Z}/p\,\mathbb{Z}$)*. | p | ordre de $\bar{2}$ dans ( $\mathbb{Z}/p\,\mathbb{Z}$)*. |
|---|---|---|---|
| 17 | 8 | 953 | 68 |
| 41 | 20 | 977 | 488 |
| 73 | 9 | 1009 | 504 |
| 89 | 11 | 1033 | 258 |
| 97 | 48 | 1049 | 262 |
| 113 | 28 | 1097 | 274 |
| 137 | 68 | 1129 | 564 |
| 193 | 96 | 1153 | 288 |
| 233 | 29 | 1193 | 298 |
| 241 | 24 | 1201 | 300 |
| 257 | 16 | 1217 | 152 |
| 281 | 70 | 1249 | 156 |
| 313 | 156 | 1289 | 161 |
| 337 | 21 | 1297 | 648 |
| 353 | 88 | 1321 | 60 |
| 401 | 200 | 1361 | 680 |
| 409 | 204 | 1409 | 704 |
| 433 | 72 | 1433 | 179 |
| 449 | 224 | 1481 | 370 |
| 457 | 76 | 1489 | 744 |
| 521 | 260 | 1553 | 194 |
| 569 | 284 | 1601 | 400 |
| 577 | 144 | 1609 | 201 |
| 593 | 148 | 1657 | 92 |
| 601 | 25 | 1697 | 848 |
| 617 | 154 | 1721 | 215 |
| 641 | 64 | 1753 | 146 |
| 673 | 48 | 1777 | 74 |
| 761 | 380 | 1801 | 25 |
| 769 | 384 | 1873 | 936 |
| 809 | 404 | 1889 | 472 |
| 857 | 428 | 1913 | 239 |
| 881 | 55 | 1993 | 996 |
| 929 | 464 | 2017 | 336 |
| 937 | 117 | 2081 | 1040 |

| p | ordre de $\bar{2}$ dans $(\mathbb{Z}/p\,\mathbb{Z})^*$. | p | ordre de $\bar{2}$ dans $(\mathbb{Z}/p\,\mathbb{Z})^*$. |
|---|---|---|---|
| 2089 | 29 | 3121 | 156 |
| 2113 | 44 | 3137 | 784 |
| 2129 | 532 | 3169 | 1584 |
| 2137 | 1068 | 3209 | 1604 |
| 2153 | 1076 | 3217 | 804 |
| 2161 | 1080 | 3257 | 407 |
| 2273 | 568 | 3313 | 828 |
| 2281 | 190 | 3329 | 1664 |
| 2297 | 1148 | 3361 | 168 |
| 2377 | 1188 | 3433 | 1716 |
| 2393 | 598 | 3449 | 431 |
| 2417 | 1208 | 3457 | 576 |
| 2441 | 305 | 3529 | 882 |
| 2473 | 618 | 3593 | 1796 |
| 2521 | 1260 | 3617 | 1808 |
| 2593 | 81 | 3673 | 918 |
| 2609 | 1304 | 3697 | 1848 |
| 2617 | 1308 | 3761 | 188 |
| 2633 | 1316 | 3769 | 1884 |
| 2657 | 166 | 3793 | 1896 |
| 2689 | 224 | 3833 | 958 |
| 2713 | 1356 | 3881 | 388 |
| 2729 | 1364 | 3889 | 648 |
| 2753 | 1376 | 3929 | 1964 |
| 2777 | 1388 | 4001 | 1000 |
| 2801 | 1400 | 4049 | 506 |
| 2833 | 118 | 4057 | 169 |
| 2857 | 102 | 4073 | 2036 |
| 2897 | 1448 | 4129 | 688 |
| 2953 | 492 | 4153 | 346 |
| 2969 | 371 | 4177 | 87 |
| 3001 | 1500 | 4201 | 525 |
| 3041 | 1520 | 4217 | 1054 |
| 3049 | 762 | 4241 | 2120 |
| 3089 | 772 | 4273 | 534 |

| p | ordre de $\bar{2}$ dans $(\mathbb{Z}/p\,\mathbb{Z})^*$. | p | ordre de $\bar{2}$ dans $(\mathbb{Z}/p\,\mathbb{Z})^*$. |
|---|---|---|---|
| 4289 | 1072 | 5569 | 464 |
| 4297 | 537 | 5641 | 564 |
| 4337 | 2168 | 5657 | 2828 |
| 4409 | 551 | 5689 | 711 |
| 4441 | 2220 | 5737 | 239 |
| 4457 | 1114 | 5801 | 2900 |
| 4481 | 560 | 5849 | 2924 |
| 4513 | 47 | 5857 | 2928 |
| 4561 | 2280 | 5881 | 1470 |
| 4649 | 2324 | 5897 | 2948 |
| 4657 | 388 | 5953 | 992 |
| 4673 | 2336 | 6073 | 3036 |
| 4721 | 295 | 6089 | 761 |
| 4729 | 788 | 6113 | 3056 |
| 4793 | 2396 | 6121 | 1530 |
| 4801 | 1200 | 6217 | 1036 |
| 4817 | 1204 | 6257 | 3128 |
| 4889 | 2444 | 6329 | 3164 |
| 4937 | 1234 | 6337 | 288 |
| 4969 | 2484 | 6353 | 397 |
| 4993 | 624 | 6361 | 53 |
| 5009 | 2504 | 6449 | 806 |
| 5081 | 635 | 6473 | 3236 |
| 5113 | 426 | 6481 | 810 |
| 5153 | 112 | 6521 | 1630 |
| 5209 | 217 | 6529 | 102 |
| 5233 | 1308 | 6553 | 117 |
| 5273 | 2636 | 6569 | 1642 |
| 5281 | 2640 | 6577 | 3288 |
| 5297 | 662 | 6673 | 1112 |
| 5393 | 1348 | 6689 | 836 |
| 5417 | 2708 | 6737 | 3368 |
| 5441 | 544 | 6761 | 1690 |
| 5449 | 908 | 6793 | 1698 |
| 5521 | 2760 | 6833 | 3416 |

| p | ordre de $\bar{2}$ dans $(\mathbb{Z}/p\,\mathbb{Z})^*$. | p | ordre de $\bar{2}$ dans $(\mathbb{Z}/p\,\mathbb{Z})^*$. |
|---|---|---|---|
| 6841 | 1710 | 8081 | 1010 |
| 6857 | 857 | 8089 | 4044 |
| 6961 | 1160 | 8161 | 408 |
| 6977 | 3488 | 8209 | 2052 |
| 7001 | 500 | 8233 | 2058 |
| 7057 | 392 | 8273 | 2068 |
| 7121 | 890 | 8297 | 4148 |
| 7129 | 1782 | 8329 | 4164 |
| 7177 | 3588 | 8353 | 464 |
| 7193 | 3596 | 8369 | 2092 |
| 7297 | 3648 | 8377 | 1396 |
| 7321 | 1220 | 8513 | 4256 |
| 7369 | 1228 | 8521 | 4260 |
| 7393 | 264 | 8537 | 2134 |
| 7417 | 3708 | 8609 | 1076 |
| 7433 | 3716 | 8641 | 4320 |
| 7457 | 3728 | 8681 | 124 |
| 7481 | 1870 | 8689 | 4344 |
| 7489 | 468 | 8713 | 363 |
| 7529 | 941 | 8737 | 4368 |
| 7537 | 1256 | 8753 | 4376 |
| 7561 | 3780 | 8761 | 365 |
| 7577 | 1894 | 8849 | 4424 |
| 7649 | 3824 | 8929 | 496 |
| 7673 | 3836 | 8969 | 1121 |
| 7681 | 3840 | 9001 | 2250 |
| 7753 | 323 | 9041 | 904 |
| 7793 | 1948 | 9049 | 4524 |
| 7817 | 1954 | 9137 | 1142 |
| 7841 | 1960 | 9161 | 4580 |
| 7873 | 1312 | 9209 | 2302 |
| 7937 | 3968 | 9241 | 2310 |
| 7993 | 999 | 9257 | 4628 |
| 8009 | 4004 | 9281 | 1160 |
| 8017 | 4008 | 9337 | 2334 |

| p | ordre de $\bar{2}$ dans $(\mathbb{Z}/p\,\mathbb{Z})^*$. | p | ordre de $\bar{2}$ dans $(\mathbb{Z}/p\,\mathbb{Z})^*$. |
|---|---|---|---|
| 9377 | 2344 | 10993 | 2748 |
| 9433 | 4716 | 11057 | 2764 |
| 9473 | 2368 | 11113 | 463 |
| 9497 | 4748 | 11161 | 310 |
| 9521 | 476 | 11177 | 1397 |
| 9601 | 2400 | 11257 | 1407 |
| 9649 | 402 | 11273 | 5636 |
| 9689 | 4844 | 11321 | 2830 |
| 9697 | 2424 | 11329 | 472 |
| 9721 | 810 | 11353 | 5676 |
| 9769 | 1221 | 11369 | 5684 |
| 9817 | 1636 | 11393 | 5696 |
| 9833 | 4916 | 11489 | 5744 |
| 9857 | 4928 | 11497 | 5748 |
| 9929 | 292 | 11593 | 5796 |
| 10009 | 1668 | 11617 | 1452 |
| 10169 | 164 | 11633 | 1454 |
| 10177 | 636 | 11657 | 1457 |
| 10193 | 5096 | 11681 | 5840 |
| 10273 | 5136 | 11689 | 5844 |
| 10289 | 5144 | 11777 | 2944 |
| 10313 | 5156 | 11801 | 1475 |
| 10321 | 5160 | 11833 | 5916 |
| 10337 | 1292 | 11897 | 5948 |
| 10369 | 1296 | 11953 | 664 |
| 10433 | 1304 | 11969 | 2992 |
| 10457 | 2614 | 12041 | 1505 |
| 10513 | 2628 | 12049 | 753 |
| 10529 | 5264 | 12073 | 1509 |
| 10601 | 5300 | 12097 | 6048 |
| 10657 | 333 | 12113 | 6056 |
| 10729 | 5364 | 12161 | 3040 |
| 10753 | 1792 | 12241 | 510 |
| 10889 | 2722 | 12281 | 6140 |
| 10937 | 1367 | 12289 | 6144 |

| p | ordre de $\bar{2}$ dans $(\mathbb{Z}/p\,\mathbb{Z})^*$. | p | ordre de $\bar{2}$ dans $(\mathbb{Z}/p\,\mathbb{Z})^*$. |
|---|---|---|---|
| 12329 | 3082 | 13457 | 6728 |
| 12377 | 3094 | 13513 | 6756 |
| 12401 | 6200 | 13537 | 6768 |
| 12409 | 1551 | 13553 | 616 |
| 12433 | 6216 | 13577 | 6788 |
| 12457 | 1557 | 13633 | 1704 |
| 12473 | 3118 | 13649 | 6824 |
| 12497 | 3124 | 13681 | 6840 |
| 12553 | 3138 | 13697 | 6848 |
| 12569 | 3142 | 13721 | 6860 |
| 12577 | 1572 | 13729 | 6864 |
| 12601 | 6300 | 13841 | 3460 |
| 12641 | 395 | 13873 | 6936 |
| 12689 | 6344 | 13913 | 3478 |
| 12697 | 3174 | 13921 | 3480 |
| 12713 | 3178 | 14009 | 7004 |
| 12721 | 1272 | 14033 | 7016 |
| 12809 | 6404 | 14057 | 7028 |
| 12841 | 535 | 14081 | 7040 |
| 12889 | 6444 | 14153 | 7076 |
| 12953 | 6476 | 14177 | 7088 |
| 13001 | 6500 | 14249 | 3562 |
| 13009 | 2168 | 14281 | 2380 |
| 13033 | 6516 | 14321 | 1790 |
| 13049 | 1631 | 14369 | 3592 |
| 13121 | 328 | 14401 | 3600 |
| 13177 | 2196 | 14449 | 84 |
| 13217 | 3304 | 14489 | 7244 |
| 13241 | 6620 | 14537 | 1817 |
| 13249 | 6624 | 14561 | 7280 |
| 13297 | 2216 | 14593 | 1216 |
| 13313 | 6656 | 14633 | 1829 |
| 13337 | 1667 | 14657 | 7328 |
| 13417 | 1677 | 14713 | 3678 |
| 13441 | 1680 | 14737 | 3684 |

| p | ordre de $\bar{2}$ dans $(\mathbb{Z}/p\,\mathbb{Z})^*$. | p | ordre de $\bar{2}$ dans $(\mathbb{Z}/p\,\mathbb{Z})^*$. |
|---|---|---|---|
| 14753 | 1844 | 16057 | 2676 |
| 14897 | 931 | 16073 | 1148 |
| 14929 | 3732 | 16097 | 8048 |
| 14969 | 1871 | 16193 | 4048 |
| 15017 | 1877 | 16217 | 8108 |
| 15073 | 314 | 16249 | 2031 |
| 15121 | 270 | 16273 | 8136 |
| 15137 | 7568 | 16361 | 2045 |
| 15161 | 7580 | 16369 | 2728 |
| 15193 | 211 | 16417 | 2052 |
| 15217 | 3804 | 16433 | 2054 |
| 15233 | 1088 | 16481 | 8240 |
| 15241 | 381 | 16529 | 8264 |
| 15289 | 637 | 16553 | 4138 |
| 15313 | 3828 | 16561 | 2760 |
| 15329 | 7664 | 16633 | 2079 |
| 15361 | 3840 | 16649 | 4162 |
| 15377 | 7688 | 16657 | 2776 |
| 15401 | 7700 | 16673 | 2084 |
| 15473 | 7736 | 16729 | 697 |
| 15497 | 7748 | 16889 | 8444 |
| 15569 | 1946 | 16921 | 2820 |
| 15601 | 2600 | 16937 | 8468 |
| 15641 | 7820 | 16993 | 8496 |
| 15649 | 7824 | 17033 | 4258 |
| 15737 | 7868 | 17041 | 2840 |
| 15761 | 3940 | 17137 | 2142 |
| 15809 | 247 | 17209 | 2151 |
| 15817 | 7908 | 17257 | 8628 |
| 15881 | 3970 | 17321 | 4330 |
| 15889 | 2648 | 17377 | 4344 |
| 15913 | 2652 | 17393 | 8696 |
| 15937 | 2656 | 17401 | 580 |
| 16001 | 8000 | 17417 | 4354 |
| 16033 | 8016 | 17449 | 8724 |

| p | ordre de $\bar{2}$ dans $(\mathbb{Z}/p\,\mathbb{Z})^*$. | p | ordre de $\bar{2}$ dans $(\mathbb{Z}/p\,\mathbb{Z})^*$. |
|---|---|---|---|
| 17489 | 8744 | 18713 | 4678 |
| 17497 | 4374 | 18793 | 3132 |
| 17569 | 8784 | 18913 | 9456 |
| 17609 | 4402 | 19001 | 9500 |
| 17657 | 8828 | 19009 | 9504 |
| 17681 | 1768 | 19073 | 9536 |
| 17713 | 8856 | 19081 | 3180 |
| 17729 | 4432 | 19121 | 4780 |
| 17737 | 2217 | 19249 | 1203 |
| 17761 | 2960 | 19273 | 3212 |
| 17881 | 2235 | 19289 | 2411 |
| 17921 | 8960 | 19417 | 1618 |
| 17929 | 4482 | 19433 | 4858 |
| 17977 | 8988 | 19441 | 4860 |
| 18041 | 451 | 19457 | 4864 |
| 18049 | 3008 | 19489 | 9744 |
| 18089 | 9044 | 19553 | 9776 |
| 18097 | 9048 | 19577 | 4894 |
| 18121 | 151 | 19609 | 9804 |
| 18169 | 4542 | 19681 | 3280 |
| 18217 | 828 | 19697 | 9848 |
| 18233 | 4558 | 19753 | 3292 |
| 18257 | 2282 | 19777 | 1648 |
| 18289 | 4572 | 19793 | 2474 |
| 18313 | 9156 | 19801 | 9900 |
| 18329 | 9164 | 19841 | 4960 |
| 18353 | 4588 | 19889 | 9944 |
| 18401 | 1840 | 19913 | 9956 |
| 18433 | 2304 | 19937 | 9968 |
| 18457 | 9228 | 19961 | 9980 |
| 18481 | 2310 | 19993 | 4998 |
| 18521 | 2315 | 20089 | 5022 |
| 18553 | 9276 | 20113 | 2514 |
| 18593 | 1162 | 20129 | 10064 |
| 18617 | 2327 | 20161 | 10080 |

| p | ordre de $\bar{2}$ dans $(\mathbb{Z}/p\,\mathbb{Z})^*$. | p | ordre de $\bar{2}$ dans $(\mathbb{Z}/p\,\mathbb{Z})^*$. |
|---|---|---|---|
| 20177 | 5044 | 21577 | 1798 |
| 20201 | 10100 | 21601 | 1080 |
| 20233 | 10116 | 21617 | 10808 |
| 20249 | 10124 | 21649 | 10824 |
| 20297 | 2537 | 21673 | 2709 |
| 20353 | 2544 | 21713 | 1357 |
| 20369 | 5092 | 21737 | 10868 |
| 20393 | 10196 | 21817 | 10908 |
| 20441 | 1460 | 21841 | 156 |
| 20521 | 2565 | 21881 | 10940 |
| 20593 | 3432 | 21929 | 10964 |
| 20641 | 5160 | 21937 | 10968 |
| 20681 | 10340 | 21961 | 5490 |
| 20753 | 10376 | 21977 | 2747 |
| 20809 | 2601 | 22073 | 11036 |
| 20849 | 10424 | 22129 | 3688 |
| 20857 | 66 | 22153 | 11076 |
| 20873 | 5218 | 22193 | 11096 |
| 20897 | 5224 | 22273 | 11136 |
| 20921 | 2615 | 22369 | 11184 |
| 20929 | 10464 | 22409 | 11204 |
| 21001 | 3500 | 22433 | 11216 |
| 21017 | 2627 | 22441 | 1870 |
| 21089 | 5272 | 22481 | 11240 |
| 21121 | 10560 | 22697 | 2837 |
| 21169 | 504 | 22721 | 5680 |
| 21193 | 1766 | 22769 | 11384 |
| 21313 | 5328 | 22777 | 949 |
| 21377 | 10688 | 22817 | 11408 |
| 21401 | 2140 | 22921 | 11460 |
| 21433 | 2679 | 22937 | 11468 |
| 21481 | 895 | 22961 | 11480 |
| 21521 | 5380 | 22993 | 11496 |
| 21529 | 1794 | 23017 | 959 |
| 21569 | 674 | 23041 | 480 |

| p | ordre de $\bar{2}$ dans $(\mathbb{Z}/p\,\mathbb{Z})^*$. | p | ordre de $\bar{2}$ dans $(\mathbb{Z}/p\,\mathbb{Z})^*$. |
|---|---|---|---|
| 23057 | 2882 | 24473 | 3059 |
| 23081 | 11540 | 24481 | 12240 |
| 23201 | 11600 | 24593 | 12296 |
| 23209 | 967 | 24697 | 12348 |
| 23297 | 11648 | 24793 | 12396 |
| 23321 | 11660 | 24809 | 12404 |
| 23369 | 2921 | 24841 | 6210 |
| 23417 | 5854 | 24889 | 4148 |
| 23473 | 1956 | 24953 | 3119 |
| 23497 | 11748 | 24977 | 6244 |
| 23537 | 5884 | 25033 | 6258 |
| 23561 | 5890 | 25057 | 6264 |
| 23593 | 11796 | 25073 | 12536 |
| 23609 | 5902 | 25097 | 12548 |
| 23633 | 5908 | 25121 | 1570 |
| 23689 | 11844 | 25153 | 12576 |
| 23753 | 11876 | 25169 | 3146 |
| 23761 | 594 | 25321 | 12660 |
| 23801 | 2975 | 25409 | 1588 |
| 23833 | 993 | 25457 | 6364 |
| 23857 | 2982 | 25537 | 1596 |
| 23873 | 5968 | 25561 | 2556 |
| 23929 | 3988 | 25577 | 12788 |
| 23977 | 1998 | 25601 | 400 |
| 23993 | 5998 | 25609 | 582 |
| 24001 | 12000 | 25633 | 6408 |
| 24049 | 12024 | 25657 | 4276 |
| 24097 | 12048 | 25673 | 6418 |
| 24113 | 12056 | 25793 | 1612 |
| 24121 | 3015 | 25801 | 12900 |
| 24137 | 12068 | 25841 | 12920 |
| 24169 | 12084 | 25849 | 3231 |
| 24281 | 6070 | 25873 | 12936 |
| 24329 | 3041 | 25889 | 3236 |
| 24337 | 4056 | 25913 | 3239 |

| p | ordre de $\bar{2}$ dans ( $\mathbb{Z}/p\,\mathbb{Z}$)*. | p | ordre de $\bar{2}$ dans ( $\mathbb{Z}/p\,\mathbb{Z}$)*. |
|---|---|---|---|
| 25969 | 6492 | 27281 | 3410 |
| 26017 | 13008 | 27329 | 6832 |
| 26041 | 930 | 27337 | 13668 |
| 26113 | 13056 | 27361 | 304 |
| 26153 | 13076 | 27409 | 571 |
| 26161 | 4360 | 27449 | 6862 |
| 26177 | 3272 | 27457 | 6864 |
| 26209 | 2184 | 27481 | 6870 |
| 26249 | 3281 | 27529 | 13764 |
| 26297 | 6574 | 27617 | 13808 |
| 26321 | 13160 | 27673 | 2306 |
| 26393 | 13196 | 27689 | 13844 |
| 26417 | 508 | 27697 | 4616 |
| 26449 | 13224 | 27737 | 13868 |
| 26489 | 13244 | 27793 | 13896 |
| 26497 | 2208 | 27809 | 1738 |
| 26513 | 6628 | 27817 | 4636 |
| 26561 | 3320 | 27953 | 6988 |
| 26633 | 3329 | 27961 | 466 |
| 26641 | 13320 | 28001 | 500 |
| 26681 | 13340 | 28057 | 4676 |
| 26713 | 13356 | 28081 | 14040 |
| 26729 | 13364 | 28097 | 14048 |
| 26737 | 13368 | 28201 | 7050 |
| 26777 | 3347 | 28289 | 14144 |
| 26801 | 13400 | 28297 | 1179 |
| 26833 | 13416 | 28393 | 1183 |
| 26849 | 839 | 28409 | 7102 |
| 26881 | 960 | 28433 | 7108 |
| 26921 | 2692 | 28513 | 7128 |
| 26953 | 6738 | 28537 | 2378 |
| 26993 | 3374 | 28649 | 14324 |
| 27017 | 13508 | 28657 | 1791 |
| 27073 | 6768 | 28697 | 3587 |
| 27241 | 13620 | 28729 | 3591 |

| p | ordre de $\hat{2}$ dans ( $\mathbb{Z}/p\,\mathbb{Z}$)*. |
|---|---|
| 28753 | 7188 |
| 28793 | 14396 |
| 28817 | 1801 |
| 28921 | 14460 |
| 28961 | 14480 |
| 29009 | 14504 |
| 29017 | 2418 |
| 29033 | 3629 |
| 29129 | 14564 |
| 29137 | 7284 |
| 29153 | 3644 |
| 29201 | 3650 |
| 29209 | 3651 |
| 29297 | 14648 |
| 29401 | 14700 |
| 29473 | 14736 |
| 29537 | 14768 |
| 29569 | 1232 |
| 29633 | 14816 |
| 29641 | 14820 |
| 29753 | 14876 |
| 29761 | 744 |
| 29833 | 3729 |
| 29873 | 14936 |
| 29881 | 14940 |
| 29921 | 14960 |

# Références


[1] **Arnaudiès Jean-Marie et Bertin José** , *Groupes Algébres et Géométrie (Tome 1)* , Ellipse , Paris ( 1993 ).

[2] **Barnes F.W.** , *On the Stufe of an algebraic number field* , J.Number theory **4**( 1972 ) , 474-478.

[3] **Burnside W.S. and Penton A.W.** , *"The theory of Equations"* , Vol.I , 10th ed. , Chand , Delhi , 1954.

[4] **Cassels J.W.S.** , *Local Fields* , Cambridge University Press ( 1986 ).

[5] **Cassels J.W.** , *On the representation of rational functions as sums of squares* , Acta.Arith. , **9**(1964) , 79-82.

[6] **Cassels J.W. , Ellsion W.J and Pfister A.** , *On sums of squares and elliptic cuves over function fields* , J.No.Th. , **3**(1971) , 125-144.

[7] **Chowla P.** , *On the representation of -1 as a sum of squares in a cyclotomic field* , J. Number Theory **1** (1969) , 208-210.

[8] **Chowla P. and Chowla S.** , *Determination of the Stufe of certain cyclotomic fields* , J.Number Theory **2** (1970) , 271-272.

[9] **Connell I.** , *The Stufe of number fields* , Math.Zeit , **124** (1972) , 20-22.

[10] **Fein Burton & Basil , Gordon & Smith , John H.** , *On the representation of -1 as a sum of two squares in algebraic number Field* , Journal of number Theory **3**(1971) , 310-315 .

[11] **Hasse H.** , *Der $2^n$-te Potenzcharackter von 2 im Körper der $2^n$-ten Einheitswurzeln* , Rend. Circ.Mat.Palermo(2) 7 (1958) , 185-244.

[12] **Lam T.Y.** , *"The Algebraic theory of quadratic forms"* , Benjamin , New York ( 1973 ).

[13] **Malliavin M.-P.** , *Algèbre commutative Applications en géométrie et théorie des nombres* , Masson , Paris ( 1984 ).

[14] **Moser Claude** , *Représentation de -1 comme somme de carrés dans un corps cyclotomique , quelconque* , J.Number Theory , **5**(1973) , 139-141.

[15] **Narkiewicz Wladyslaw** , *Elementary and Analytic Theory of Algebraic Numbers* , WARSZAWA , Poland ( 1974 ).

[16] **Ono Takashi** , *An Introduction to Algebraic Number Theory* , Plenum Press , New York ( 1990 ).

[17] **Parnami J.C. , Agrawal M.K. , and Rajwade A.R.** , *On the Stufe of Quadratic Fields* , J.Number Theory **38** , 106-109 (1991).

[18] **Pfister A.** , *Darstellung von -1 als Summe von Quadratic fields* , Indian J.Pure Appl. Math. **6** (1975),725-726.

[19] **Rajwade A.R.** , *Squares* , London Mathematical Society , Lecture Note Series 171 , Cambridge University Press ( 1993 ).

[20] **Rajwade A.R.** , *A note on the stufe of quadratic fields* , Indian J.Pure Appl. Math. **6** (1975) , 725-726.

[21] **Rose H.E.** , *A Course in Number Theory* , Clarendon Press , Oxford ( 1988 ).

[22] **Serre Jean-Pierre** , *Corps locaux* , Hermann , Paris ( 1962 ).

[23] **Risman L.J.** , *A new proof of the 3-square theorem* , J.Number theory **6** (1974) , 282-283.

[24] **Small C.** , *Sum of 3 squares and levels of quadratic number fields* , Amer. Math. Monthly **93**( 1986 ) , 276-279.