Etude du niveau de certains corps

Lo Nassirou

Résumé

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 nombres s'il est fini est 1, 2 ou 4. Cependant la détermination effective du niveau d'un corps quelconque reste un problème. Dans la première partie de cet exposé on étudie le niveau d'extensions quartiques ($[\mathbb{Q}(\alpha):\mathbb{Q}]=4$), $\alpha\in\mathbb{C}$ où le polynôme minimal de α est de la forme X^4+d, $d\in\mathbb{Z}$, ensuite on généralise ce résultat au corps de nombres K=$\mathbb{Q}(\alpha)$ où $[\mathbb{Q}(\alpha):\mathbb{Q}]=n$, $\alpha\in\mathbb{C}$ et le polynôme minimal de α est de la forme X^n+d, où $d\in\mathbb{Q}$ et $n\in\mathbb{N}^*$. Dans la deuxième partie, on montre que (si n est un entier, $n\geq 3$) le niveau de $\mathbb{Q}_2(\xi_n)$, où ξ_n est une racine primitive $n^{ième}$ de l'unité dans une clôture algébrique de $\mathbb{Q}_2$ est le même que celui du corps $\mathbb{Q}(e^{2i\pi/n})$ qui est bien connu à part le fait qu'il subsiste un problème quand n est premier congru à 1 modulo 8 cf.[8]. On donne ici un algorithme facilement programmable 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 dernière partie est consacrée à l'étude du niveau de $\mathbb{Q}_p(\xi_n)$ où p est un nombre premier impair et ξ_n une racine primitive $n^{ième}$ de l'unité dans une clôture algébrique de $\mathbb{Q}_p$.

Abstract

We know from Pfister Theorem that the level of commutative field when it is finite is a power of 2. And the level of an algebraic number field when it is finite is 1, 2 or 4. However it is not easy to determine exactly the level of a given field.

Our first aim is to determine the level of quartic extensions ($[\mathbb{Q}(\alpha):\mathbb{Q}]=4$), $\alpha\in\mathbb{C}$ where the minimal polynomial of α is of the form X^4+d, $d\in\mathbb{Z}$ and

Received by the editors May 1997.
Communicated by J. Van Geel.

we generalize this result to the number field K=$\mathbb{Q}(\alpha)$ where $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$, $\alpha \in \mathbb{C}$ and the minimal polynomial of α is of the form $X^n + d$, $d \in \mathbb{Q}$ and $n \in \mathbb{N}^*$. In the second part we show that (if n is an integer, $n \geq 3$) the level of $\mathbb{Q}_2(\xi_n)$, where ξ_n is a n-th primitive root of unity in the algebraic closure of $\mathbb{Q}_2$ is the same as for $\mathbb{Q}(e^{2i\pi/n})$ which is well-known except that it is more complicated when n is prime $n \equiv 1 \bmod 8$ see [8]. We give here an algorithm which enables us to calculate the order of the class of 2 in $(\mathbb{Z}/p\,\mathbb{Z})^*$ for $p \equiv 1 \bmod 8$, p prime. The interest of this program is that we work only with the numbers $\leq p$. In the last part we consider the level of $\mathbb{Q}_p(\xi_n)$, where p is an odd prime and ξ_n is a primitive root of unity in the algebraic closure of $\mathbb{Q}_p$.

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

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

Définition 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 1 (Pfister). [15], *p. 41.*
Soit $L = K(\alpha)$ une extension algébrique 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 1.
Soit K un corps, $L = K(\alpha)$, α appartenant à une clôture algébrique de K. Soit β un conjugué de α 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 par isomorphisme.

Théorème 2 (Springer). [15], *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 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 1. *cf.*[15], *p.43 (même méthode de démonstration que le théorème3.8). Soit K un corps. Soit $d \in K^*$, 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 $2^k = \infty$ et alors : $s(K(\sqrt{-d})) = min(s(K), 2^k)$.*

Corollaire 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 (esquisse, cf.[15], théorème 3.2, p.31.)
Les deux premières équivalences sont triviales. On sait que d ($d \geq 0$) 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 $4^{a_0}(8b_0 - 1)$, pour plus de détails cf.[16], p.159 , en utilisant la proposition1 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. On peut remarquer aussi qu'on peut démontrer ce résultat avec la méthode qui est employée pour la démontration du théorème 3 de cet article.

On utilise les lemmes suivants :

Lemme 1. *cf.*[10] *(même démonstration que le lemme 3.9 p.60).*
Soit ξ 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 φ, 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 ψ. Il y a autant de prolongements ψ que de racines de $\varphi(P)$ dans M.

Lemme 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'algèbre 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 (esquisse)
L'équivalence de a) et b) découle du théorème 2.7 chap. 3 de [9] 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 [9]. Enfin a) équivaut à d) cf.[2] théorème 1.

Lemme 3.
Soit $K = \mathbb{Q}(\alpha)$ un corps de nombres totalement complexe où le polynôme minimal P de α 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 Ψ est injectif. On en déduit que $\mathbb{Q}_2$ contient un sous corps F isomorphe à $\mathbb{Q}(\alpha)$. D'où $4 \geq s(\mathbb{Q}(\alpha)) = s(F) \geq s(\mathbb{Q}_2) = 4$. Si P n'a pas de racine dans $\mathbb{Q}_2$, alors on sait que $\alpha \in K_\wp$, $\forall \wp$ divisant 2. Soit $T = min(\alpha, \mathbb{Q}_2)$: 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.

Corollaire 3.
Soit $K = \mathbb{Q}(\alpha), \alpha \in \mathbb{C}$ où le polynôme minimal de α sur $\mathbb{Q}$ est de la forme $X^4+d, d \in \mathbb{Z}^*$. Si $d = -1 + 2^5k$ avec $k \in \mathbb{N}^*$, alors $s(K) = 4$.

Démonstration
En effet en posant $P = X^4 + d$, on a, en dérivant $P' = 4X^3$, $P(1) = 2^5k$ et $|P(1)|_2 \leq \frac{1}{2^5} < |P'(1)|_2^2 = (\frac{1}{2^2})^2$ donc d'après le Lemme de Hensel cf.[3] p.49, P a une racine dans $\mathbb{Q}_2$ et $s(K) = 4$ d'après le Lemme 3 puisque $s(K) = s(\mathbb{Q}(\sqrt{\sqrt{-d}}))$.

Théorème 3.
Soit $K = \mathbb{Q}(\alpha)$ et $P = min(\alpha, \mathbb{Q}) = X^4+d$ le polynôme minimal de α 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.
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.[3] p.53 ou cf.[11].

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 1 (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 $i \in K$ et $i \notin \mathbb{Q}(\sqrt{-d})$ comme
$\mathbb{Q} \xrightarrow{2} \mathbb{Q}(\sqrt{-d}) \xrightarrow{2} \mathbb{Q}(\sqrt{-d})(i) \longrightarrow K$ et [K :$\mathbb{Q}$]=4 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 :
$\alpha^2 = \pm\sqrt{-d} = a_1^2 - b_1^2 + 2a_1 b_1 i \in \mathbb{Q}(\sqrt{-d})$ 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 cas où $b \equiv$ -1 mod 8.
a) Si a est impair. On sait que $\mathbb{Q}(\sqrt{\sqrt{-d}}) = \mathbb{Q}(\sqrt{2\sqrt{-b}})$. 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 $\mathbb{Q}_2$, $\pm 2\sqrt{-b}$ n'est pas un carré dans $\mathbb{Q}_2$ car 6 et 10 ne sont pas des carrés 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 ± 2, ni ± 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 $\mathbb{Q}_2[X]$ et $X^4 + b$ a une racine dans $\mathbb{Q}_2$ cf.corollaire 3. Si P a une racine dans $\mathbb{Q}_2$, alors 2 ou -2 est un carré dans $\mathbb{Q}_2$ car $\sqrt{-b}$ 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 $s(K) = s(\mathbb{Q}(\sqrt{\sqrt{-b}}))$.
<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 $a_2 = 0$ 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 3.
<u>cas 2</u> : Si $b \equiv$ -1 mod 16 et $b \not\equiv$ -1 mod 32.

$c^2 = -b = 1-16k = 1+2^4+2^5k_1$ 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 3 permet de conclure que $s(K) = 4$.

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

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

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 $s(\mathbb{Q}(\sqrt{-d})) = 4$.

Etude du 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 α est de la forme $X^n + d$, où $d \in \mathbb{Q}$ et $n \in \mathbb{N}^*$.

Lemme 4.
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 α 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=1 ce Lemme est vrai cf.corollaire2 et n=2 cf.théorème3. 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 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≡-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 :

$$a^2 = 1 + 2^3(a_2 + \frac{a_1(a_1+1)}{2}) + 2^4(a_4 + a_1a_3) + \cdots + 2^{2k+2}(\sum_{i=0}^{k} a_i a_{2k+1-i} + a_{k+1}^2) + 2^{2k+3}(\sum_{i=0}^{k} a_i a_{2k+2-i}) + \cdots$$

En posant $-b = a^2$, on trouve une racine c_1 de $X^2 + b$ dans $\mathbb{Z}_2$ telle que $c_1 \equiv 1 \mod 2^{n+1}$ 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 successivement le résultat suivant :

$$\begin{gathered}
\text{le polynôme } \mathrm{X^2 + b} \text{ a une racine } \mathrm{c_1} \equiv 1 \mod 2^{\mathrm{n+1}} \text{ dans } \mathbb{Z}_2 \,. \\
\text{le polynôme } \mathrm{X^2 - c_1} \text{ a une racine } \mathrm{c_2} \equiv 1 \mod 2^{\mathrm{n}} \text{ dans } \mathbb{Z}_2 \,. \\
\vdots \\
\text{le polynôme } \mathrm{X^2 - c_{n-2}} \text{ a une racine } \mathrm{c_{n-1}} \equiv 1 \mod 2^3 \text{ dans } \mathbb{Z}_2 \,. \\
\text{le polynôme } \mathrm{X^2 - c_{n-1}} \text{ a une racine } \mathrm{c_n} \equiv 1 \mod 2^2 \text{ dans } \mathbb{Z}_2 \,.
\end{gathered}$$

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 β 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 :

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

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 β n' est pas un carré dans $\mathbb{Q}_2$, donc $X^2 - \beta$ est irréductible sur $\mathbb{Q}_2[X]$.

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

Soit $T = min(\alpha, \mathbb{Q}_2)$ le polynôme minimal de α 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. Comme $\mathbb{Q}(\alpha)$ est isomorphe à $\mathbb{Q}(\sqrt{\beta})$ car α et β 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 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 $[K_\wp : \mathbb{Q}_2] = [K_\wp : \mathbb{Q}_2(\alpha)][\mathbb{Q}_2(\alpha) : \mathbb{Q}_2]$ 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.
On a montré que si β 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 β est un carré dans $\mathbb{Q}_2$.

Théorème 4.
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 mod 2^{n+2} ou 2^n ne divise pas a.
s(K)=4 $\Longleftrightarrow$ b $\equiv$ -1 mod 2^{n+2} et 2^n divise a.

Démonstration
Le théorème est vrai quand n=1 et n=2, c'est le corollaire2 et le théorème 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'aprés 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 $d_i \in \mathbb{Q}$. 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 α^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 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 $a_1 \equiv 1 \mod 2^n$ 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 $a_2 \equiv 1 \mod 2^{n-1}$ dans $\mathbb{Z}_2$.
$\vdots$
le polynôme $X^2 - d_{n-3}$ a une racine $d_{n-2} = 2^2.2^{2^2 a_0}a_{n-2}$ avec $a_{n-2} \equiv 1 \mod 2^3$ 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 $a_{n-1} \equiv 1 \mod 2^2$ dans $\mathbb{Z}_2$.

On 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 lemme 4 on a : s(K)=2.
Si 2^n divise a et b≢-1 mod 2^{n+2}, quitte à multiplier α par un rationnel non nul, on peut supposer que min(α,$\mathbb{Q}$)=$X^{2^n} + b$ (car 2^n divise a) donc grâce au lemme 4 $s(K) \leq 2$ et comme $s(K) \neq 1$, s(K)=2.
Enfin si b≡ -1 mod 2^{n+2} et 2^n divise a, quitte à multiplier α par un rationnel non nul, on peut supposer que min(α,$\mathbb{Q}$)=$X^{2^n} + b$ (car 2^n divise a) donc grâce au lemme 4, $4 \geq s(K) > 2$
et $s(K) = 4$, ce qui termine la démonstration du théorème.

Corollaire 4.
Soit $P = X^n + d \in \mathbb{Q}[X]$ où ($n \in \mathbb{N}^*$) un polynôme irréductible sur $\mathbb{Q}$, α une racine de P dans $\mathbb{C}$ et $K = \mathbb{Q}(\alpha)$. $s(K) = \infty$ si n est impair, si n est pair 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 $\mathbb{Z}$ ($n = 2^k n_1$ avec n_1 impair et $k \geq 1$). Alors on a :
s(K)=2 $\Longleftrightarrow$ b ≢ -1 mod 2^{k+2} ou 2^k ne divise pas a.
s(K)=4 $\Longleftrightarrow$ b ≡ -1 mod 2^{k+2} et 2^k divise a.

Démonstration (On suppose n pair car sinon on utilise théorème de Springer).
On peut supposer d entier relatif en multipliant α 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 α^{n_1} sur $\mathbb{Q}$ est min(α^{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 4 précédent au corps $\mathbb{Q}(\alpha^{n_1})$.

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

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

Proposition 2. [15], *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. *(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. [15] *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 4.
Le cas p≡ 1 mod 8 non envisagé dans le théorème est très compliqué, voir [8]. 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.

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

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 ξ_n un générateur de S_n.$\mathbb{Q}(\xi_n)$ est un corps normal et le polynôme minimal de ξ_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 ξ_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.

Proposition 3.
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 [17]. 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 : $e_{\mathbb{Q}_2(\xi_p)/\mathbb{Q}_2} = e_{\mathbb{Q}_2(\xi_p)/F}.e_{F/\mathbb{Q}_2}$ 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.[3], 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 [17]. Donc si f est impair le théorème2 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.[11] (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 : $\forall n \geq 3$, $s(\mathbb{Q}_2(\xi_n)) = s(\mathbb{Q}(e^{\frac{2i\pi}{n}}))$.

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

Soit ξ_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.[15], 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 de la deuxième partie 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 4.
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 de la deuxième partie.
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 [17]. Si f est pair alors $s(k_n) = 1$ d'après le théorème 3.4 de [15]. L'équation P=$X^2 + 1$ a donc une solution dans $\mathbb{Q}_p(\xi_n)$ d'après le Lemme de Hensel cf.[3], p49 car $\exists \alpha \in \mathbb{Q}_p(\xi_n)$ tel que $|P(\alpha)|_p < 1 = |P'(\alpha)|_p^2$, d'où $s(\mathbb{Q}_p(\xi_n)) = 1$.

Corollaire 5.
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.
On suppose $q \geq 3$ *et q premier différent de p.*
Si $\left(\begin{array}{c} p \\ q \end{array}\right) = -1$ *où* ($\left(\begin{array}{c} . \\ q \end{array}\right)$ *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 7.
On suppose $q \geq 3$ *et q premier différent de p.*
Si $q \equiv 3 \bmod 4$ *et* $\left(\begin{array}{c} p \\ q \end{array}\right) = 1$ *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.

Exemple 2.
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 73×8 sont premiers entre eux, on peut choisir un nombre premier p=$(5^8 + 2 \times 73)$+73×8k, 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=$(5^2 + 2 \times 73)$+73×8k, 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 $p \equiv 3$ mod 4, $q \equiv 1$ mod 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 5.
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 $\mathbb{Q}_p(\xi_{p^\alpha})/\mathbb{Q}_p$ est totalement ramifiée d'après la proposition 17 §4 de [17]. Donc si k_{p^α} désigne le corps résiduel de $\mathbb{Q}_p(\xi_{p^\alpha})$ 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 [17] 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 [17]. Si f est pair alors : $s(k_n) = 1$ d'après le théorème 3.4 [9]. L'équation $X^2 + 1$ a donc une solution dans $\mathbb{Q}_p(\xi_n)$ d'après le lemme de Hensel , d'où $s(\mathbb{Q}_p(\xi_n)) = 1$.

Appendice

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 6. [12], *th.4.14 p167.*
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 p-1=fg.

Théorème 7. [13], *th.2.17 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 θ. On suppose que $R_K = \mathbb{Z}[\theta]$. Soit $f_\theta(X) = \varphi_1^{e_1} \cdots \varphi_g(X)^{e_g}$ mod 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 φ_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. [1], *p106.*
*En posant A=F(**F**[X]/P**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 **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
$1 \leq i \leq (p-3)/2$; $e_{(p-1)/2} = -1 - X - \cdots - X^{(p-3)/2} - 2X^{(p-1)/2} - X^{(p+1)/2} - \ldots - X^{(p-2)}$
$e_i = X^{2i-p} - X^i$,$(p+1)/2 \leq i \leq p-2$ 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 $\lambda_i \in \mathbf{F}$, λ_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 : $\begin{cases} \lambda_0 \; quelconque \, , \lambda_{(p-1)/2} = \lambda_{(p-1)/4} = \lambda_{p-2} = 0 \\ \lambda_i = \lambda_{2i} \; avec \; 1 \leq i \leq (p-3)/2 \\ \lambda_{(p-1)/2+j} = \lambda_{2j-1} \; avec \; 1 \leq j \leq (p-3)/2 \end{cases}$
Pour i pair $i \leq (p-3)/2$,on cherche les λ_j tels que $\lambda_j = \lambda_i$. On cherche le nombre maximum de λ_i pouvant être choisi arbitrairement : comme $\lambda_{2i} = \lambda_i$ on peut se limiter à i impair.
Ce qui conduit à l'algorithme suivant :

1ère : 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 pour $p = 41$).
2ème : Pour $1 \leq i \leq (p-1)/4$ et i pair on factorise (p-1)/2+i sous la forme $2^{\alpha}\gamma$ avec γ impair.
3ème : On fait correspondre chaque 2i-1 au γ ainsi trouvé, sauf pour celui qui n'avait pas de correspondance pair, on lui associe p-2.
4ème : On calcule le nombre de classes. Chaque classe étant obtenue en partant d'un i
quelconque, on lui fait correspondre γ puis à γ on associe γ' ainsi de suite jusqu'à retrouver i.

Exemple 3.

p=41, 1ère 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, 2ème 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, 3ème 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 :
1ère *classe* $1 \longrightarrow 9 \longrightarrow 39 \longrightarrow 5 \longrightarrow 1$
2ème *classe* $3 \longrightarrow 11 \longrightarrow 13 \longrightarrow 17 \longrightarrow 19 \longrightarrow 15 \longrightarrow 7 \longrightarrow 3$
Par conséquent g=2 et f=20, donc $s(\mathbb{Q}(\xi_{41})) = 2$.

Je dispose d'un tel algorithme programmé en Turbo Pascal pouvant chercher tous les nombres premiers p inférieurs ou égaux 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 $p \leq 10^{31}$.

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

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

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

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

[7] 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 .

[8] 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.

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

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

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

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

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

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

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

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

[17] Serre, Jean-Pierre, *Corps locaux*, Hermann, Paris (962).

UFR de Mathématiques de l'Université
des Sciences et Technologies de Lille
59655 VILLENNEUVE D'ASCQ Cedex
e-mail : nlo@gat. univ-lille1. fr