Journal de Théorie des Nombres
de Bordeaux **17** (2005), 767–778

Sur les corps de Hilbert-Speiser

par THOMAS HERRENG

RÉSUMÉ. On dit qu'un corps est de Hilbert-Speiser en un premier p si toute extension modérée abélienne finie de degré p admet une base normale entière. On dit qu'un corps est de Hilbert-Speiser s'il est de Hilbert-Speiser pour tout premier p. Il est bien connu que $\mathbb{Q}$ est un tel corps. Dans un article [3] de 1998, Greither, Replogle, Rubin et Srivastav ont montré que $\mathbb{Q}$ était le seul corps de Hilbert-Speiser. On donne ici une condition nécessaire et suffisante pour qu'un corps soit de Hilbert-Speiser en $p = 2$. On trouve par exemple que $\mathbb{Q}(\sqrt{p})$ est de Hilbert-Speiser en $p = 2$ si et seulement si son nombre de classes est un. On généralise ensuite un article de Conrad et Replogle [1], ce qui nous donne des premiers p pour lesquels un corps abélien imaginaire n'est pas de Hilbert-Speiser en p et on donne également une condition quand le corps est réel.

ABSTRACT. A number field is called a Hilbert-Speiser field for a prime number p if each tamely ramified finite abelian extension of degree p admits a normal integral basis. A number field is called a Hilbert-Speiser field if it's Hilbert-Speiser for all primes p. It's well known that $\mathbb{Q}$ is such a field. In an article [3] written in 1998, Greither, Replogle, Rubin et Srivastav showed that $\mathbb{Q}$ is the only Hilbert-Speiser field. We give here a necessary and sufficient condition for a field to be Hilbert-Speiser for $p = 2$. For example $\mathbb{Q}(\sqrt{p})$ is a Hilbert-Speiser field for $p = 2$ if and only if its class number is one. Then generalizing works of Conrad and Replogle [1] we obtain prime numbers p for which an imaginary abelian field is a Hilbert-Speiser field for p, and we also give a criterion for real abelian fields.

1. Introduction

Un des théorèmes essentiels de la théorie de Galois, bien connu depuis le dix-neuvième siècle, est le théorème de la base normale. Il affirme que si L/K est une extension galoisienne de corps de nombres de groupe de Galois G, alors L est un KG-module libre de rang un. Il est naturel de se demander s'il existe un équivalent arithmétique de cette proposition, c'est-à-dire si

Manuscrit reçu le 1er décembre 2003.

l'anneau des entiers algébriques $\mathcal{O}_L$ de L est un $\mathcal{O}_K G$-module libre. Dans ce cas, on dit que l'extension L/K admet une base normale entière. Les deux résultats classiques à ce sujet sont le théorème de Noether (1931) qui affirme qu'une extension de corps locaux admet une base normale entière si et seulement si l'extension est modérément ramifiée, et le théorème de Hilbert-Speiser (théorème 132 du *Zahlbericht* de Hilbert) qui affirme que toute extension modérée abélienne de $\mathbb{Q}$ admet une base normale entière. C'est ce dernier théorème que l'on cherche à généraliser. On dit qu'un corps de nombres K est de Hilbert-Speiser en un premier p si toute extension abélienne modérée de degré p de K admet une base normale entière. Un corps de Hilbert-Speiser est un corps de nombres qui a la propriété d'être de Hilbert-Speiser en tout premier p.

Pour caractériser de tels corps, on utilise les deux articles suivants :

- Tout d'abord un travail de H. B. Mann [5] qui dit que si $h_K \neq 1$, alors il existe des extensions quadratiques modérées L/K telles que $\mathcal{O}_L$ n'est pas $\mathcal{O}_K$-libre. A fortiori, L/Kn'admet pas de base normale entière.
- L'article fondamental [3] de Greither, Replogle, Rubin et Srivastav. Soit K un corps de nombres ; on suppose que $h_K = 1$. On définit pour n entier $V_n = (\mathcal{O}_K/n\mathcal{O}_K)^\times / Im(\mathcal{O}_K^\times)$. Si K est de Hilbert-Speiser en p, alors :
  - V_2 est trivial pour $p = 2$.
  - l'exposant de V_p divise $\frac{(p-1)^2}{2}$ pour p premier impair.

Ce dernier résultat [3] permet de montrer que $\mathbb{Q}$ est le seul corps de nombres de Hilbert-Speiser. On donne ici une condition nécessaire et suffisante pour qu'un corps de nombres K soit de Hilbert-Speiser en 2, puis on donne des exemples de nombres premiers p pour lesquels un corps donné ne soit pas de Hilbert-Speiser en p.

L'auteur tient particulièrement à remercier Bruno Anglès pour son aide précieuse ainsi que Cornelius Greither pour ses conseils toujours judicieux.

2. Cas $p = 2$

On donne dans ce paragraphe une condition nécessaire et suffisante pour qu'un corps soit de Hilbert-Speiser en 2, en utilisant le fait que l'on sait décrire les extensions quadratiques modérées d'un corps de nombres dont le nombre de classes est 1. Cette condition nous permettra de donner des exemples de corps de nombres qui sont de Hilbert-Speiser en 2.

On se sert de la caractérisation suivante (on pourra consulter [5] ou [4]) :

Lemme 2.1. *Soit K un corps de nombres de nombre de classes 1. Alors les extensions modérées de K sont données par $L = K(\sqrt{D})$ tel que D est sans facteur carré, D est premier à 2, et D est un carré modulo 4. On sait qu'alors D engendre le discriminant de L/K.*

Soit alors $\beta \in \mathcal{O}_K$ tel que $\beta^2 \equiv D \mod 4$. On vérifie alors facilement que $\{1, \frac{\beta+\sqrt{D}}{2}\}$ est une $\mathcal{O}_K$-base de $\mathcal{O}_L$.

2.1. Condition nécessaire et suffisante pour que K soit de Hilbert-Speiser en 2. Par définition, K est de Hilbert-Speiser en 2 si et seulement s'il existe $x = x_1 + x_2(\beta + \sqrt{D})/2 \in \mathcal{O}_L$ où $x_i \in \mathcal{O}_K$ tel que $\mathcal{O}_L = \mathcal{O}_K G.x$ avec $G = \mathbb{Z}/2\mathbb{Z} = \{1, \sigma\}$, ce qui est équivalent à l'existence d'un x dans $\mathcal{O}_L$ tel que $\operatorname{disc}(\mathcal{O}_K G.x) = D\mathcal{O}_K$, soit $(x^2 - \sigma(x^2))^2 \mathcal{O}_K = Dx_2^2(x_2\beta + 2x_1)^2 = D\mathcal{O}_K$.

Donc K est de Hilbert-Speiser en 2 si et seulement si $x_2 \in \mathcal{O}_K^\times$ et $(x_2\beta + 2x_1) \in \mathcal{O}_K^\times$. Or $(\beta + 2\frac{x_1}{x_2})^2 \equiv D \mod 4$. Donc D est congru au carré d'une unité modulo 4.

Réciproquement, si $D \equiv u^2 \in \mathcal{O}_K^\times \mod 4$, alors l'anneau des entiers de $K(\sqrt{D})$ est égal à $\mathcal{O}_K[\frac{u+\sqrt{D}}{2}]$ et l'élément $x = \frac{u+\sqrt{D}}{2}$ engendre une base normale entière.

On a donc montré le théorème :

Théorème 2.1. *Soit K un corps de nombres. Alors K est de Hilbert-Speiser en 2 si et seulement si $h_K = 1$ et pour tout $D \in \mathcal{O}_K$ tel que D est premier à 2, D est sans facteur carré et D est un carré modulo 4, alors D est congru au carré d'une unité modulo 4.*

Ce que l'on peut reformuler autrement en disant que tout carré dans $(\mathcal{O}_K/4\mathcal{O}_K)^\times$ est congru au carré d'une unité modulo 4. En particulier, cela implique que $V_4^2 = 1$ donc l'exposant de V_4 divise 2.

2.2. Quelques exemples.

2.2.1. *Cas de $\mathbb{Q}(i)$.* Appliquons le critère précédent. Soit $x \in \mathbb{Z}[i]$, avec x premier à 2. Cela se traduit par $x = a + ib$, avec $a, b \in \mathbb{Z}$ et $N(x) = a^2 + b^2 \not\equiv 0 \mod 2$. Ce qui signifie que a et b ne sont pas de même parité. On a $x^2 = a^2 - b^2 + 2iab$.

- Si a est pair, alors b est impair donc $x^2 \equiv -1 = i^2 \mod 4$.
- Si a est impair, alors b est pair donc $x^2 \equiv 1 = 1^2 \mod 4$.

Dans les deux cas, x^2 est congru au carré d'une unité de K modulo 4. On a donc montré que $\mathbb{Q}(i)$ est un corps de Hilbert-Speiser en 2.

2.2.2. *Cas de $\mathbb{Q}(j)$, où j est une racine troisième de l'unité.* On sait que 2 est non ramifié et premier dans $\mathbb{Z}[j]$ car le polynme $X^2 + X + 1$ est irréductible modulo 2. Notons $\mathfrak{P} = 2\mathbb{Z}[j]$. On a

$$(\mathcal{O}_K/4\mathcal{O}_K)^\times = (\mathcal{O}_K/\mathfrak{P}^2)^\times \twoheadrightarrow (\mathcal{O}_K/\mathfrak{P})^\times$$

le noyau de cette surjection étant $\frac{1+\mathfrak{P}}{1+\mathfrak{P}^2} \simeq \mathcal{O}_K/\mathfrak{P} \simeq \mathbb{F}_4$.

On a donc $(\mathcal{O}_K/4\mathcal{O}_K)^\times \simeq (\mathbb{F}_4)^\times \times \mathbb{F}_4$. Or j est d'ordre 3 et $1, j, j^2$ sont non congrus modulo 4 et sont tous les trois des carrés d'unités. Donc les

éléments de $(\mathcal{O}_K/4\mathcal{O}_K)^{\times 2} \simeq (\mathbb{F}_4)^\times$ sont tous représentés par des carrés, ce qui montre que $\mathbb{Q}(j)$ est un corps de Hilbert-Speiser en 2.

Remarque. On verra dans le paragraphe suivant des exemples de nombres premiers p pour lesquels $\mathbb{Q}(i)$ et $\mathbb{Q}(j)$ ne sont pas de Hilbert-Speiser en p.

2.2.3. *Cas de $\mathbb{Q}(\sqrt{p})$, p premier.* Distinguons quatre sous-cas.
Si $p \equiv 1 \mod 8$, alors 2 est totalement décomposé donc on a :

$$(\mathcal{O}_K/4\mathcal{O}_K)^\times \simeq \mathbb{F}_2 \times \mathbb{F}_2.$$

Tous les carrés de $(\mathcal{O}_K/4\mathcal{O}_K)^\times$ sont triviaux donc $K = \mathbb{Q}(\sqrt{p})$ est de Hilbert-Speiser en 2 si $h_K = 1$.
Si $p \equiv 5 \mod 8$, alors 2 reste premier dans $\mathcal{O}_K$. On a alors $(\mathcal{O}_K/4\mathcal{O}_K)^\times \simeq (\mathbb{F}_4)^\times \times \mathbb{F}_4$, donc $((\mathcal{O}_K/4\mathcal{O}_K)^\times)^2 \simeq \mathbb{Z}/3\mathbb{Z}$. K est donc un corps de Hilbert-Speiser en 2 si et seulement si $h_K = 1$ et le carré de l'unité fondamentale n'est pas congru à 1 modulo 4. Soit ϵ l'unité fondamentale, $\epsilon = a + b\frac{1+\sqrt{p}}{2}$, avec $a, b \in \mathbb{Z}$. De plus, on a le critère suivant (cf. [2], corollaire 2 p.182) :

Rappel. Soit $K/\mathbb{Q}$ une extension quadratique, si le discriminant d_K n'a qu'un seul diviseur premier et que K est réel, alors la norme de l'unité fondamentale est -1.

Ce qui donne : $N(\epsilon) = a^2 + ab + b^2(\frac{1-p}{4}) = -1$.
Donc

$$\epsilon^2 \equiv 1 \mod 4 \iff (a^2+ab+b^2(\frac{p-1}{4})) + \frac{1+\sqrt{p}}{2}(2ab+b^2) \equiv 1 \mod 4$$

ce qui donne $2ab+b^2 \equiv 0 \mod 4$, c'est-à-dire b pair et $a^2+ab \equiv 1 \mod 4$. Or le calcul de la norme donne $a^2 + ab \equiv -1 \mod 4$, ce qui n'est pas possible. K est donc un corps de Hilbert-Speiser en 2 si son nombre de classes est 1.
Supposons à présent que p est congru à 3 modulo 4. Dans ce cas, 2 est ramifié puisque le discriminant est $4p$. Il existe donc un idéal premier $\mathfrak{P}$ de $\mathcal{O}_K$ tel que $2 = \mathfrak{P}^2$. On a donc :

$$(\mathcal{O}_K/4\mathcal{O}_K)^\times \simeq \mathbb{F}_2^\times \times \frac{1+\mathfrak{P}}{1+\mathfrak{P}^4}.$$

Or $\frac{1+\mathfrak{P}}{1+\mathfrak{P}^4}$ est un groupe abélien d'ordre 8 et d'exposant 4, c'est donc $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Ce qui donne en définitive, $((\mathcal{O}_K/4\mathcal{O}_K)^\times)^2 \simeq \mathbb{Z}/2\mathbb{Z}$. K est de Hilbert-Speiser en 2 si et seulement si le carré de l'unité fondamentale n'est pas congru à 1 modulo 4 et $h_K = 1$. Comme précédemment, nous utiliserons le critère (toujours extrait de [2], proposition 1.7 p.179) :

Rappel. Soit $K/\mathbb{Q}$ une extension quadratique, si le discriminant d_K est divisible par un premier congru à -1 modulo 4, alors la norme de l'unité fondamentale est 1.

Soit ϵ l'unité fondamentale, $\epsilon = a + b\sqrt{p}$, avec $a, b \in \mathbb{Z}$. Le calcul de la norme donne : $1 = N(\epsilon) = a^2 - pb^2 \equiv a^2 + b^2 \mod 4$, donc a et b ne sont pas de même parité. Et $\epsilon^2 = (a^2 + pb^2) + \sqrt{p}(2ab)$. On a donc

$$\epsilon^2 \equiv 1 \mod 4 \iff a^2 - b^2 \equiv 1 \mod 4$$

ce qui équivaut à a impair. Etudions ϵ plus en détails.

Etude de l'unité fondamentale. Montrons que pour p premier congru à 3 modulo 4, tous les corps $\mathbb{Q}(\sqrt{p})$ de nombre de classes 1 sont de Hilbert-Speiser en 2. Pour cela, il nous reste juste à montrer que l'unité fondamentale ϵ a une trace divisible par 4 (i.e. $\epsilon = a+b\sqrt{p}$, avec a pair). On se servira de la caractérisation de l'unité fondamentale suivante (voir [2], proposition 1.6, p.178) :

Rappel. L'unité fondamentale $\epsilon = a + b\sqrt{p}$ est caractérisée par : toute unité $\mu = c + d\sqrt{p}$ telle que $\mu > 1$ et $\mu \neq \epsilon$ vrifie $a < c$.

Supposons donc que l'on ait une unité $\epsilon = a+b\sqrt{p}$ avec a impair. Comme on sait que la norme de ϵ est 1, on a $a^2 - pb^2 = 1$, donc a et b n'ont pas même parité. On pose donc $a = (2h + 1)$ et $b = 2l$. Cela nous donne $\epsilon = (2h+1)+2l\sqrt{p}$. On écrit que la norme est 1, cela entraîne $h^2+h-pl^2 = 0$, soit

$$h(h + 1) = pl^2.$$

On en déduit que soit h est divisible par p et h/p, $(h + 1)$ sont des carrés, soit $(h+1)$ est divisible par p et $(h+1)/p$, h sont des carrés. On en déduit aussi que l est pair.

1^{er} *cas : h est un carré.* Posons $h = \eta^2$. On sait que cela implique que $\frac{\eta^2+1}{p}$ est un carré. Or $p \equiv -1 \mod 4$, ce qui donne une contradiction.

$2^{ème}$ *cas.* On a montré pour le moment que si $\epsilon = a + b\sqrt{p}$ est une unité avec a impair, alors $h = (a - 1)/2$ vérifie $(h + 1)$ est un carré et h/p aussi. On veut montrer que cette unité ne peut pas être l'unité fondamentale en construisant une unité $\mu = c + d\sqrt{p}$ avec $c < a$. Il suffit donc de construire une unité $\mu = c + d\sqrt{p}$ avec $\mu^2 = \epsilon$.

Posons $h = \eta^2 - 1$. On sait que $\frac{\eta^2-1}{p}$ est un carré. La norme de ϵ est 1, ce qui se traduit, en posant $l = 2k$ par

$$\eta^2 \frac{\eta^2 - 1}{p} = 4k^2.$$

Si l'on pose $\mu = \eta + 2k/\eta\sqrt{p}$, on vérifie que $N(\mu) = 1$ et $\mu^2 = \epsilon$. Ce qui montre que ϵ n'était pas l'unité fondamentale, et prouve bien que $\mathbb{Q}(\sqrt{p})$ est de Hilbert-Speiser en 2.

Le cas $p = 2$ se traite exactement comme le précédent, puisque 2 se ramifie dans $\mathbb{Q}(\sqrt{2})$. On a donc $(\mathcal{O}_K/4\mathcal{O}_K)^\times \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Q}(\sqrt{2})$ est de Hilbert-Speiser en 2 si et seulement si le carré de l'unité fondamentale n'est pas congru à 1 modulo 4. Or l'unité fondamentale est $1 + \sqrt{2}$ dont le carré est $3 + 2\sqrt{2}$ qui n'est pas congru à 1 modulo 4, donc $\mathbb{Q}(\sqrt{2})$ est de Hilbert-Speiser en 2.

Résumons les résultats que l'on a obtenus :

Proposition 2.1. *Soit $K = \mathbb{Q}(\sqrt{p})$ avec p premier, alors K est de Hilbert-Speiser en 2 si et seulement si $h_K = 1$.*

Remarque. On remarque que les démonstrations effectuées se généralisent dans certains cas à $\mathbb{Q}(\sqrt{d})$ pour d non premier.

- Si $d \equiv 1 \mod 8$, alors le discriminant est d et 2 est totalement décomposé, donc on a de la même manière que $\mathbb{Q}(\sqrt{d})$ est de Hilbert-Speiser en 2 si $h_K = 1$.
- si $d \equiv 3 \mod 4$ ou $d \equiv 2 \mod 4$ et d est divisible par un premier $p \equiv 3 \mod 4$, alors le discriminant est $4d$, donc 2 est ramifié et la norme de l'unité fondamentale est 1. Alors K est de Hilbert-Speiser en 2 si et seulement si $h_K = 1$ et si la trace de l'unité fondamentale est divisible par 4. (c'est-à-dire si et seulement si l'unité fondamentale s'exprime $a + b\sqrt{d}$, avec a pair). Cette condition n'est pas toujours vérifiée si d n'est pas premier : par exemple $\mathbb{Q}(\sqrt{6})$ n'est pas de Hilbert-Speiser en 2 (l'unité fondamentale est $5 + 2\sqrt{6}$) et $\mathbb{Q}(\sqrt{39})$ non plus (l'unité fondamentale est $25 + 4\sqrt{39}$).
- Dans les autres cas, on ne connaît pas à priori la norme de l'unité fondamentale, et pour cette raison, on ne peut pas donner de résultats généraux.

On est donc assuré de l'existence d'extensions modérées abéliennes de $\mathbb{Q}(\sqrt{6})$ de degré 2 sans base normale entière (le nombre de classes de $\mathbb{Q}(\sqrt{6})$ est bien 1.) Pour trouver un exemple, on se sert de la caractérisation des extensions quadratiques modérées donnée au début de cette section. Les entiers de $\mathbb{Q}(\sqrt{6})$ s'écrivent $a + b\sqrt{6}$, avec $a, b \in \mathbb{Z}$. Les carrés modulo 4 sont donc congrus à $\{0, 2, 1, -1 + 2\sqrt{6}\}$. Posons $D = -1 + 2\sqrt{6}$. La norme de D est -23, donc D est premier (en particulier sans facteur carré et premier à 2.) Donc $\mathbb{Q}(\sqrt{6}, \sqrt{-1 + 2\sqrt{6}})/\mathbb{Q}(\sqrt{6})$ n'a pas de base normale entière.

3. Corps imaginaires

Si K est un corps totalement imaginaire, alors le théorème de Dirichlet implique que le rang des unités est égal à $n/2 - 1$ où $n = [K : \mathbb{Q}]$. Voyons comment appliquer cela pour les corps cyclotomiques et comment le généraliser au cas des corps galoisiens totalement imaginaires.

3.1. Cas des corps cyclotomiques. On rappelle l'argument de Conrad et Replogle (voir [1]) pour le corps $K = \mathbb{Q}(\zeta_p)$, où p est un nombre premier impair et ζ_p une racine primitive p-ième de l'unité. Notons $\mathfrak{P} = (1 - \zeta_p)$ l'idéal premier de $\mathcal{O}_K$ au-dessus de p. On a donc

$$(\mathcal{O}_K/p\mathcal{O}_K)^\times = (\mathcal{O}_K/\mathfrak{P}^{p-1})^\times \twoheadrightarrow (\mathcal{O}_K/\mathfrak{P})^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}.$$

Ce qui donne : $(\mathcal{O}_K/p\mathcal{O}_K)^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z} \times (\mathbb{Z}/p\mathbb{Z})^{p-2}$ en tant que groupes abéliens.

On regarde ensuite les unités de $\mathcal{O}_K$. Par le théorème de Dirichlet, $\mathcal{O}_K^\times \simeq < -\zeta_p > \times < \epsilon_1 > \times \cdots \times < \epsilon_{(p-3)/2} >$.

On considère V_p^{p-1}, de manière à supprimer la partie $\mathbb{Z}/(p-1)\mathbb{Z}$ dans $\mathcal{O}_K/p\mathcal{O}_K$. On sait que ζ_p n'est pas congru à 1 modulo p donc $-\zeta_p$ a une image non triviale dans un $\mathbb{Z}/p\mathbb{Z}$.

On obtient donc $V_p^{p-1} \simeq (\mathbb{Z}/p\mathbb{Z})^{p-2-j}$ pour un certain entier j avec $1 \leq j \leq (p-1)/2$.

On a donc obtenu le résultat suivant : V_p^{p-1} est un groupe d'exposant p si $p - 2 - j > 0$, c'est-à-dire dès que $p \geq 5$, l'exposant de V_p ne divise pas $(p-1)^2/2$ ce qui implique :

Proposition 3.1 (Conrad et Replogle). *Pour un nombre premier p supérieur ou égal à 5, $\mathbb{Q}(\zeta_p)$ n'est pas Hilbert-Speiser en p.*

3.2. Cas des corps galoisiens totalement imaginaires. Proposons dans cette section une généralisation de la démonstration précédente pour K corps de nombres totalement imaginaire galoisien sur $\mathbb{Q}$.

Si p est ramifié dans K, alors

$$(\mathcal{O}_K/p\mathcal{O}_K)^\times = \prod_{\mathfrak{P}/p} (\mathcal{O}_K/\mathfrak{P}^{e(\mathfrak{P}/p)}\mathcal{O}_K)^\times.$$

Fixons un premier $\mathfrak{P}|p$, et notons $e = e(\mathfrak{P}/p)$ et $f = f(\mathfrak{P}/p)$. En réappliquant l'argument utilisé dans le cas des corps cyclotomiques, on voit que $(\mathcal{O}_K/\mathfrak{P}^e\mathcal{O}_K)^\times \simeq (\mathcal{O}_K/\mathfrak{P}\mathcal{O}_K)^\times \times U(\mathfrak{P})$ où $U(\mathfrak{P}) = \frac{1+\mathfrak{P}}{1+\mathfrak{P}^e}$.

Etude de $U(\mathfrak{P})$. On sait que pour tout $n \geq 1$, $\frac{1+\mathfrak{P}^n}{1+\mathfrak{P}^{n+1}} \simeq \mathcal{O}_K/\mathfrak{P}$ donc $|U(\mathfrak{P})| = p^{f(e-1)}$.

Lemme 3.1. *L'exposant de $U(\mathfrak{P})$ est $p^{\lceil \frac{log(e)}{log(p)} \rceil}$ où $\lceil x \rceil$ désigne le plus petit entier supérieur ou égal à x.*

Démonstration. Notons $k = \lceil \frac{log(e)}{log(p)} \rceil$. Alors k est le plus petit entier tel que $p^k \geq e$.

- Soit $x \in 1 + \mathfrak{P}$, $x = 1 + z$ avec $z \in \mathfrak{P}$. On a $(1+z)^{p^k} \equiv 1 + z^{p^k} \equiv 1 \mod \mathfrak{P}^e$. L'exposant de $U(\mathfrak{P})$ divise donc p^k.

– Soit $x \in \mathfrak{P}\backslash\mathfrak{P}^2$. Alors on a $(1+x)^{p^n} = 1 + x^{p^n} \mod \mathfrak{P}^e$ pour tout n et donc l'ordre de $(1+x)$ dans $U(\mathfrak{P})$ est p^k.

□

Remarque. Dans le cas du p-ième corps cyclotomique, $U(\mathfrak{P})$ est un $\mathbb{F}_p$-espace vectoriel. C'est le cas si tout élément est d'ordre p, c'est-à-dire d'après le lemme précédent si $e(\mathfrak{P}/p) \leq p$.

Mais k n'est pas nécessairement égal à 1, on n'a donc plus un espace vectoriel. On est alors amené à définir le p-rang qui généralise la notion de dimension.

Définition. Soit A un groupe abélien fini. On définit le p-rang de A par : $d_p(A) = dim_{\mathbb{F}_p} A/A^p$.

Remarque. A peut s'écrire $A_1 \times A_p$ où A_p est le p-sous-groupe de Sylow. et $A_p \simeq \mathbb{Z}/p^{e_1} \times \cdots \times \mathbb{Z}/p^{e_t}$, avec $t \geq 0$. Par définition, $d_p(A) = t$. Si le p-rang de V_p est strictement positif, p divise l'exposant de V_p et donc K n'est pas un corps de Hilbert-Speiser en p.

On veut calculer $r = d_p(U(\mathfrak{P}))$. Pour cela, on remarque que par définition, $|(U(\mathfrak{P})/U(\mathfrak{P})^p)| = p^r$.

On a une surjection naturelle $U(\mathfrak{P}) \twoheadrightarrow U(\mathfrak{P})^p$, dont on veut calculer le cardinal du noyau. Soit $x \in 1 + \mathfrak{P}$ modulo $1 + \mathfrak{P}^e$. Alors x s'écrit $1 + \pi\delta$ avec $\pi \in \mathfrak{P}\backslash\mathfrak{P}^2$ une uniformisante et $\delta \in \mathfrak{P}$ défini modulo $\mathfrak{P}^{e-1}$ et on a des équivalences :

$$x^p \in 1 + \mathfrak{P}^e \iff \delta^p \in \mathfrak{P}^{e-p} \iff v_{\mathfrak{P}}(\delta) \geq \lceil \frac{e-p}{p} \rceil.$$

Le cardinal du noyau de la surjection est donc $p^{f(e-1-\lceil \frac{e-p}{p} \rceil)}$. Le p-rang de $U(\mathfrak{P})$ est donc $f(e-1-\lceil \frac{e-p}{p} \rceil)$.

Proposition 3.2. *Soit K un corps de nombres et p un nombre premier. Alors*

$$\begin{aligned} d_p((\mathcal{O}_K/p\mathcal{O}_K)^\times) &= \sum_{\mathfrak{P}|p} f(\mathfrak{P}/p)(e(\mathfrak{P}/p) - 1 - \lceil \frac{e(\mathfrak{P}/p) - p}{p} \rceil) \\ &= [K:\mathbb{Q}] - \sum_{\mathfrak{P}|p} f(\mathfrak{P}/p)(1 + \lceil \frac{e(\mathfrak{P}/p) - p}{p} \rceil) \end{aligned}$$

d'où l'on déduit

$$d_p((\mathcal{O}_K/p\mathcal{O}_K)^\times) \geq \frac{p-1}{p}[K:\mathbb{Q}] - \sum_{\mathfrak{P}|p} f(\mathfrak{P}/p).$$

Regardons à présent le p-rang de $Im((\mathcal{O}_K)^\times)$. Si K est un corps de nombres, le théorème de Dirichlet nous dit que $(\mathcal{O}_K)^\times =< \zeta_n > \times \mathbb{Z}^{rang\mathcal{O}_K^\times}$.

Si $\mu_p \not\subset K$, où μ_p désigne le groupe des racines p-ièmes de l'unité, alors ζ_n est d'ordre premier à p. On obtient donc le résultat suivant :

$$d_p(Im\mathcal{O}_K^\times) \leq rg(\mathcal{O}_K^\times) + \epsilon \text{ avec } \epsilon = \begin{cases} 1 & \text{si } \mu_p \subset K \\ 0 & \text{sinon} \end{cases}$$

d'où l'on déduit le lemme :

Lemme 3.2. *avec les notations précédentes, on a*

$$d_p(V_p) \geq \frac{p-1}{p}[K:\mathbb{Q}] - \sum_{\mathfrak{P}|p} f(\mathfrak{P}/p) - rg(\mathcal{O}_K^\times) - \epsilon.$$

Supposons de plus K galoisien totalement imaginaire, le théorème de Dirichlet affirme que le rang de $\mathcal{O}_K^\times$ est $n/2-1$. Il faut alors envisager deux cas :

1^{er} *cas :* $\mu_p \subset K$, *i.e.* $\epsilon = 1$. Le lemme précédent implique alors $d_p(V_p) \geq n(1/2 - 1/p - 1/e)$ où e est l'indice de ramification de p. Donc $d_p(V_p) > 0$ si $e > \frac{2p}{p-2}$. De plus, on a supposé que $\mu_p \subset K$ ce qui entraîne $e \geq p-1$. On a donc le résultat suivant :

Proposition 3.3. *Soit K un corps de nombres galoisien totalement imaginaire, et soit p un nombre premier ≥ 5. Alors si $\mu_p \subset K$, K n'est pas de Hilbert-Speiser en p.*

On remarque que cette proposition généralise bien le résultat de Conrad et Replogle que l'on avait énoncé pour les corps cyclotomiques.

$2^{ième}$ *cas :* $\mu_p \not\subset K$, *i.e.* $\epsilon = 0$. En appliquant la même méthode, on trouve que $d_p(V_p) > 0$ si $1/2 - 1/e - 1/p > -1/n$ ou encore $e > \frac{2np}{np+2p-2n}$. Mais on n'a plus comme précédemment que $e > p-1$

- Supposons $p > n$, alors $2p - 2n > 0$ donc $\frac{2np}{np+2p-2n} < 2$: il suffit donc que $e \geq 2$, c'est-à-dire que p soit ramifié.
- Si on ne suppose pas $p > n$, on peut toujours écrire : $np + 2p - 2n > np - 2n$ donc $\frac{2np}{np+2p-2p} < \frac{2p}{p-2}$. Il suffit donc que $e > \frac{2p}{p-2}$. En particulier, si $p \geq 7$, il suffit que $e \geq 3$.

Ce qui prouve la proposition suivante :

Proposition 3.4. *Soit K un corps de nombres galoisien totalement imaginaire et p un nombre premier. Alors si $p > [K:\mathbb{Q}]$ et p ramifié ou si $p \geq 7$ et le degré de ramification de p est ≥ 3, alors K n'est pas de Hilbert-Speiser en p.*

3.3. Deux cas particuliers.

Cas de $\mathbb{Q}(j)$. On a vu au début de cette section que pour p premier ≥ 5, le corps $\mathbb{Q}(\zeta_p)$ n'est pas de Hilbert-Speiser en p. Cherchons des premiers p impairs pour lesquels $\mathbb{Q}(j)$ ne soit pas de Hilbert-Speiser en p. On sait que dans ce cas, $\mathcal{O}_K^\times = \mathcal{C}$ où $\mathcal{C}$ désigne les unités cyclotomiques qui sont engendrées par $(-\zeta_3)$. Si $p \equiv 2 \mod 3$, alors $X^2 + X + 1$ est irréductible modulo p, donc p reste premier dans $\mathcal{O}_K$ et

$$|(\mathbb{Z}[j]/p\mathbb{Z}[j])^\times| = p^2 - 1.$$

De plus, $\mathbb{Z}[j]^\times$ est l'ensemble μ_6 des racines sixièmes de l'unité, donc $\mathbb{Z}[j]^\times$ s'injecte dans $(\mathbb{Z}[j]/p\mathbb{Z}[j])^\times$ car $p \notin \{2, 3\}$.

On en déduit que $V_p = (\mathbb{Z}[j]/p\mathbb{Z}[j])^\times / \mathrm{Im}(\mathbb{Z}[j]^\times)$ est de cardinal $\frac{p^2-1}{6}$, or V_p est quotient du groupe multiplicatif d'un corps fini donc est cyclique. Son exposant est donc égal à $\frac{p^2-1}{6}$. Le critère issu de [3] entraîne que $\mathbb{Q}(\zeta_3)$ n'est pas de Hilbert-Speiser en p si $\frac{p^2-1}{6}$ ne divise pas $\frac{(p-1)^2}{2}$. Or $\frac{p^2-1}{6}$ divise $\frac{(p-1)^2}{2}$ si et seulement si $\frac{p+1}{3}$ divise $(p-1)$. Comme les seuls diviseurs communs à $(p+1)$ et $(p-1)$ sont 1 et 2, la divisibilité implique que $\frac{p+1}{3} = 1$ ou 2 et donc $p = 5$.

Proposition 3.5. *Soit un nombre premier impair p. Si p est congru à* 2 *modulo* 3 *et p différent de* 5, *alors* $\mathbb{Q}(\zeta_3)$ *n'est pas de Hilbert-Speiser en p.*

Remarque. Ce raisonnement ne donne aucune précision dans le cas de premiers totalement décomposés.

Cas de $\mathbb{Q}(i)$. On peut faire exactement la même chose pour $\mathbb{Q}(i)$. le discriminant de $\mathbb{Q}(i)$ est -4. On suppose $p \neq 2$. Si p est congru à 3 modulo 4, on a de même que pour $\mathbb{Q}(\zeta_3)$, p est premier dans $\mathbb{Z}[i]$ donc $|(\mathcal{O}_K/p\mathcal{O}_K)^\times| = p^2 - 1$. De plus, les unités de $\mathbb{Q}(i)$ sont engendrées par i qui est d'ordre 4.

Le même raisonnement que précédemment conduit à $\mathbb{Q}(i)$ n'est pas de Hilbert-Speiser en p si $\frac{p^2-1}{4}$ ne divise pas $\frac{(p-1)^2}{2}$, soit $p \neq 3$.

Proposition 3.6. *Soit un nombre premier impair p. Si p est congru à* 3 *modulo* 4 *et p différent de* 3, *alors* $\mathbb{Q}(i)$ *n'est pas de Hilbert-Speiser en p.*

4. Corps réels

Dans ce paragraphe, on veut étudier les corps totalement réels. Il est plus difficile de déterminer dans quels cas V_p est trivial pour un corps totalement réel que pour un corps imaginaire à cause du théorème de Dirichlet sur les unités.

On se limitera au cas où $K = \mathbb{Q}(\zeta_p)^+$ avec p premier, et on se demandera dans quel cas $\mathbb{Q}(\zeta_p)^+$ est de Hilbert-Speiser en p. Dans ce cas, on connaît une partie des unités, à savoir les unités cyclotomiques.

En répétant l'argument exposé pour les corps cyclotomiques, on trouve : $(\mathcal{O}_K/p\mathcal{O}_K)^\times = \mathbb{F}_p^\times \times \mathbb{F}_p^{\frac{p-3}{2}}$. De plus, le théorème des unités de Dirichlet nous dit que $\mathcal{O}_K^\times = \{\pm 1\} \times \mathbb{Z}^{(p-3)/2}$. La question est donc de savoir dans quel cas $\dim_{\mathbb{F}_p} \mathrm{Im}(\mathcal{O}_K^\times) < \frac{p-3}{2}$.

Unités cyclotomiques. Notons C_K^+ les unités cyclotomiques de $K = \mathbb{Q}(\zeta_p)^+$. G désignera dans la suite le groupe de Galois $\mathrm{Gal}(\mathbb{Q}(\zeta_p)^+/\mathbb{Q}) \simeq \mathbb{Z}/(\frac{p-1}{2})\mathbb{Z}$ et ζ une racine p-ième primitive de l'unité que l'on se fixe une fois pour toute.

Rappel. (voir [6] théorème 8.2) L'indice des unités cyclotomiques dans les unités est donné par : $[\mathcal{O}_K^\times : C_K^+] = h_p^+$ où h_p^+ est le nombre de classes de $\mathbb{Q}(\zeta_p)^+$.

Comme d'habitude, on regarde V_p^{p-1} de manière à éliminer le terme $\mathbb{F}_p^\times$ dans $(\mathcal{O}_K/p\mathcal{O}_K)^\times$. On note $\mathcal{C} = Im(C_K^+)^{p-1}$. Du théorème précédent, on déduit que si $p \nmid h_p^+$ (i. e. si la conjecture de Vandiver est vérifiée), alors $\mathcal{C} = Im(\mathcal{O}_K^\times)^{p-1}$.

D'autre part, G agit sur $\mathcal{C}$ donc $\mathcal{C}$ est un $\mathbb{F}_pG$-module (attention, ici l'action du corps $\mathbb{F}_p$ est une action exponentielle). Comme p est premier à l'ordre de G, on peut considérer les idempotents associés aux caractères $e_\chi \in \mathbb{F}_pG$ (on peut voir les caractères χ comme des morphismes de G dans $\mathbb{F}_p^\times$). On décompose alors $\mathcal{C}$ suivant ces idempotents, en remarquant que $e_{\chi_0}\mathcal{C} = 0$. On a

$$\mathcal{C} = \bigoplus_{\chi \neq \chi_0} e_\chi \mathcal{C}$$

donc $\dim_{\mathbb{F}_p} \mathcal{C} = \sum_{\chi \neq \chi_0} \dim_{\mathbb{F}_p} e_\chi \mathcal{C}$, chaque $e_\chi\mathcal{C}$ étant de dimension 0 ou 1. On a donc l'équivalence entre $\dim_{\mathbb{F}_p} C < (p-3)/2$ (ce qui implique $\mathbb{Q}(\zeta_p)^+$ n'est pas de Hilbert-Speiser en p) et l'existence d'un χ non trivial dans $\widehat{G}$ tel que $\dim_{\mathbb{F}_p} e_\chi\mathcal{C} = 0$.

Remarque. On peut voir $G = Gal(\mathbb{Q}(\zeta_p)^+/\mathbb{Q})$ comme un sous-groupe de $H = Gal(\mathbb{Q}(\zeta)/\mathbb{Q})$. Les caractères de G correspondent alors aux caractères pairs de H, autrement dit aux caractères ayant la conjugaison complexe dans leur noyau.

Fonctions L p-adiques. Soit g une racine primitive modulo p. On sait (voir [6], chapitre 8) que $\theta = (\zeta^{(1-g)/2}\frac{1-\zeta^g}{1-\zeta})^{p-1}$ engendre $\mathcal{C}$ comme $\mathbb{Z}G$-module. D'où l'équivalence entre $e_\chi\mathcal{C} = 0$ et $e_\chi\theta \equiv 1 \mod p$ dans $\mathbb{Q}_p(\zeta_p)$, ce qui est encore équivalent à $\log_p(e_\chi\theta) \equiv 0 \mod p$ où $\log_p$ est le logarithme p-adique.

$$\log_p e_\chi\theta = (\chi(g) - 1)\left(\sum_{a=1}^{p-1} \chi(a)^{-1} log_p(1-\zeta^a)\right)(p-1).$$

On a donc :

$$\log_p e_\chi\theta = -(p-1)(\chi(g)-1)\frac{p}{\tau(\chi)}L_p(1,\chi)$$

où $\tau(\chi)$ désigne la somme de Gauss $\sum_{i=1}^{p}\chi(i)\zeta^i$. Or, on a :
- $\chi(g) \not\equiv 1 \mod p$, donc $v_p(\chi(g)-1) = 0$.
- $|\tau(\chi)| = \sqrt{p}$ donc, $0 < v_p(\frac{p}{\tau(\chi)}) < 1$.
- $v_p(1,\chi) \in \mathbb{Z}_p$.

De là on déduit que

$$\log_p(e_\chi\theta) \equiv 0 \mod p \iff v_p(\log_p(e_\chi\theta)) > 0 \iff L_p(1,\chi) \equiv 0 \mod p.$$

On utilise ensuite le fait que $L_p(1,\chi) \equiv L_p(0,\chi) \mod p$. Enfin, en écrivant l'expression de L_p au moyen des nombres de Bernoulli, on trouve :

$$\log_p(e_\chi\theta) \equiv 0 \mod p \iff B_{1,\chi\omega^{-1}} \equiv 0 \mod p$$

où ω est le caractère de Teichmüller. Or on sait que ω est un générateur du groupe des caractères de $Gal(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, donc il existe i pair tel que $\chi = \omega^i$, et on a donc obtenu le résultat suivant :

$$\text{si } \chi = \omega^i,\ log_p(e_\chi\theta) \equiv 0 \mod p \iff B_i \equiv 0 \mod p.$$

L'indice d'irrégularité de p indique le nombre de i pairs compris entre 1 et $p-3$ tels que $B_i \equiv 0 \mod p$. Ainsi, nous avons démontré :

Théorème 4.1. *Si l'indice d'irrégularité de p est strictement supérieur à 1, c'est-à-dire si $p|h_p$, et si $p \not| h_p^+$, alors $\mathbb{Q}(\zeta_p)^+$ n'est pas de Hilbert-Speiser en p.*

On a donc montré que $\mathbb{Q}(\zeta_p)^+$ n'était pas de Hilbert-Speiser en p pour $p = 37, 59, 67, 101, 103, 131, 149, 157, ...$

Bibliographie

[1] M. CONRAD. D. R. REPLOGLE, *Nontrivial Galois Module Structure of cycloyomic Fields.* Mathematic of computation **72** (2003), no. 242, 891–899.

[2] A. FRHLICH, M. J. TAYLOR, *Algebraic Number Theory.* Cambridge University Press, 1991.

[3] C. GREITHER. D. R. REPLOGLE. K. RUBIN, A. SRIVASTAV, *Swan Modules and Hilbert-Speiser number fields.* J. of Number theory **79** (1999), 164–173.

[4] L. R. MCCULLOH, *A Stickelberger condition on Galois module structure for Kummer extensions of prime degree.* Dans Algebraic Number Fields Proceedings of the Durham Symposium 1975, Academic press, London, 1977.

[5] H. B. MANN, *On integral Basis.* Proc. Amer. Math. Soc. **9** (1958), 119–149.

[6] L.C. WASHINGTON, *Introduction to Cyclotomic Fields.* Springer-Verlag, New-York, 1982.

Thomas HERRENG
LMNO, BP 5186
Université de Caen
14032 Caen Cedex, France
E-mail : Thomas.Herreng@math.unicaen.fr