Bases normales d'entiers et corps de classes de Hilbert.

par Abdelmejid BAYAD

Résumé. Soit $d \in \mathbb{Z}^* - \{1\}$ sans facteur carré. On pose $K = \mathbb{Q}(\sqrt{d})$. Pour $d < 0$ (resp. $d > 0$) vérifiant l'une des conditions suivantes: (i) composé, (ii) congru à 2 ou 3 mod 4, (iii) premier congru à 1 mod 4 et où le groupe des classes d'idéaux Cl_K de K n'est pas un 2-groupe (resp. (i) composé , (ii) premier congru à 3(mod 4)) on montre qu' il existe des extensions N/K abéliennes finies modérément ramifiées et sans base normale d'entiers. Lorsque $d < 0$ est composé ou premier congru à 2 ou 3 mod4 (resp. $d > 0$ et admettant un diviseur strict congru à 1 mod 4) on établit que H_K/K est sans base normale d'entiers et h_K est pair, où H_K est le corps de classes de Hilbert de K.

Normal integral bases and Hilbert class fields

Abstract. Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic number field. In some cases, we prove in this article that K admits a tame extension L/K without normal integral basis. In others cases, we show that the class number h_K of K is even. We recover some known results.

1. Introduction et résultats.

Si F est un corps de nombres, on note O_F son anneau d'entiers. Soit E/F une extension galoisienne finie de corps de nombres de groupe de Galois G; on dit que O_E possède une base normale sur O_F s'il existe un $\alpha \in O_E$ tel que $\{\alpha^\sigma\}_{\sigma \in G}$ constitue une base de O_E en tant que O_F-module.

Le résultat classique de Hilbert-Speiser classique nous assure que *toute extension $L/\mathbb{Q}$ abélienne finie et modérément ramifiée, admet une base normale. En d'autres termes, O_L est un $\mathbb{Z}[\ \mathrm{Gal}(L/\mathbb{Q})]$-module libre de rang* 1. Nous nous intéréssons à la situation relative abélienne. De façon plus précise, nous essayons d'apporter une réponse positive à la question suivante:

Question[(1)]. — *Soit $K/\mathbb{Q}$ une extension abélienne finie de degré ≥ 2. A-t-on une extension L/K abélienne finie et modérément ramifiée telle que: L/K est dépourvue de base normale d'entiers?.*

Cette question est motivée par les premières réponses partielles mais positives données dans les articles [1],[2],[3],[4],[5],[6],[7],[8] et [9].

Les résultats essentiels de ce travail sont les suivants

THÉORÈME A. — *Soit* $K = \mathbb{Q}(\sqrt{d})$ *où* d *est entier négatif non nul sans facteur carré. On suppose que* d *vérifie l'une des trois conditions suivantes: (i) composé , (ii) congru à* 2 *ou* 3 *mod* 4*, (iii) premier congru à* 1 *mod* 4 *avec* Cl_K *n'est pas un* 2*-groupe. Alors il existe une extension* L/K *abélienne finie modérément ramifiée ne possédant pas de base normale d'entiers.*

THÉORÈME B. — *Soit* $K = \mathbb{Q}(\sqrt{d})$ *où* d *est entier naturel non nul différent de* 1 *et sans facteur carré. On suppose que* $d = d_0.d_1$ *avec* $d_0 > 1$ *et* $d_1 > 1$ *(resp.* d *premier congru à* 3 *(mod* 4*)), alors l'extension*

$$K(\sqrt{d_i})/K \text{ ou } K(\sqrt{-d_i})/K \quad \Big(\text{resp. } K(\sqrt{-d})/K \Big)$$

est modérément ramifiée et dépourvue de base normale d'entiers.

THÉORÈME C. — *Soit* $K = \mathbb{Q}(\sqrt{d})$ *un corps quadratique où* d *est un entier relatif non nul sans facteur carré. On suppose que* d *vérifie l'une des deux conditions suivantes: (i)* $d < 0$ *composé ou premier congru à* 2 *ou* 3 *mod* 4*, (ii)* $d > 0$ *et admettant un diviseur propre congru à* 1 *(mod* 4*). Alors* H_K/K *est sans base normale d'entiers et* h_K *est pair.*

2. Démonstration des résultats .

Démontrons les théorèmes A et B :

1). — Si d est composé, $d = d_0.d_1$ avec $|d_0| > 1$ et $|d_1| > 1$. Posons $K = \mathbb{Q}(\sqrt{d})$ et $N = K(\sqrt{|d_i|})$ si $|d_i| = 1 \pmod 4$, $i = 0$ ou 1 (resp. $N = K(\sqrt{-|d_i|})$ si $|d_i| = 3 \pmod 4$, $i = 0$ ou 1). Il est clair que N/K est quadratique non ramifiée partout (resp. N/K est quadratique non ramifiée partout si $d < 0$ et non ramifiée seulement en tout premier fini si $d > 0$). Supposons que N/K admet une base normale d'entiers $\{\omega_+, \omega_-\}$, il existe $(x, y) \in O_K \times O_K$ et $D \in O_K$:

$$O_{K(\sqrt{d_i})} = O_K\omega_+ + O_K\omega_-, \text{ où } \omega_\pm = \frac{x \pm y\sqrt{D}}{2}$$

On a $d_{K(\sqrt{d_i})/K}(\omega_+, \omega_-) = (xy)^2.D$. Comme $\{\omega_+, \omega_-\}$ est une base normale d'entiers de N/K alors $d_{K(\sqrt{d_i})/K}(\omega_+, \omega_-) = d_{K(\sqrt{d_i})/K}$ = le discriminant relatif de N/K. Or $N/\mathbb{Q}$ est biquadratique, alors on aurait D ou $-D$ élément de $(O_K^*)^2$. Ceci impliquerait que $K(\sqrt{d_i}) = K(\sqrt{-1})$ ou K. Ce qui est absurde. Donc, $K(\sqrt{d_i})/K$ n'admet pas de base normale d'entiers.

2). — $d = 3 \pmod 4$. Posons $K = \mathbb{Q}(\sqrt{d})$ et $N = K(\sqrt{-d})$. Donc N/K est une extension quadratique non ramifée en tout premier fini et comme

$$(d_{\mathbb{Q}(\sqrt{-d})}; d_{\mathbb{Q}(\sqrt{-1})}) = 1,$$

alors $O_{K(\sqrt{-d})} = \mathbb{Z}[i, \frac{1+\sqrt{-d}}{2}]$. supposons que N/K admet une base normale, alors il existe $(x, y) \in O_K \times O_K$ et $D \in O_K$ tels que :

$$O_{K(\sqrt{-d})} = O_K\omega_+ + O_K\omega_-, \text{ où } \omega_\pm = \frac{x \pm y\sqrt{D}}{2}$$

Donc, on a $d_{K(\sqrt{-d})/K}(\omega_+, \omega_-) = (xy)^2.D$. Comme précèdemment, on doit avoir x, y unités de K et D ou $-D$ élément de $(O_K^*)^2$. Donc, il existe $\epsilon \in O_K^*$ telle que $\{\frac{1+\epsilon i}{2}; \frac{1-\epsilon i}{2}\}$ est une base normale de $K(\sqrt{-d})/K$. Ceci est faux, car $\frac{1\pm\epsilon i}{2}$ n'est pas un entier algébrique. Ceci achève la démonstration du théorème B et une partie du théorème A, pour finir reste le cas suivant

3). — $d = -p$, p premier et $d = 1 \pmod 4$ avec Cl_K n'est pas un 2-groupe, ou encore $d = -2$ ou $d = -4$. Posons $K = \mathbb{Q}(\sqrt{d})$ et montrons que

LEMME. — *Si $d \neq -4$, alors toute extension quadratique $K(\sqrt{m})/K$ non ramifiée en 2 admet une base normale d'entiers, pour $m \in \mathbb{Z}^*$ sans facteur carré.*

Démonstration. — Si $K(\sqrt{m})/K$ est non ramifiée en 2 alors $m = 1 \pmod 4$ car $d = 1 \bmod 4$. On peut imposer à m de vérifier: $(d, m) = 1$. Car si d divise m on remplace $\sqrt{m}$ par $\sqrt{\frac{m}{d}}$, on obtient $\frac{m}{d} = 1 \pmod 4$ et $(\frac{m}{d}, d) = 1$. Le fait, qu'on peut choisir m tels que: $(d, m) = 1$ et $m = 1 \pmod 4$, implique que

$$O_{K(\sqrt{m})} = O_K O_{\mathbb{Q}(\sqrt{m})} = O_K\left[\frac{1+\sqrt{m}}{2}\right]$$

D'où $\{\frac{1+\sqrt{m}}{2}; \frac{1-\sqrt{m}}{2}\}$ est une base normale pour $K(\sqrt{m})/K$. Donc, dans ce cas 3, pour trouver une extension N/K modérée sans base normale on est amener à considérer d'autres types d'extensions L/K. C'est ce que nous allons essayer de développer dans ce qui suit.

i) $h_K = 1$. — Ce sous cas est traité en détail dans le travail [8]. D'après ce travail, on sait pour $d = -2, -11, -43, -19, -67, -163$, qu'il existe une infinité d'idéaux premiers $\mathfrak{p}$ tels que: le coprs de classes de rayon $K(\mathfrak{p})/K$ est sans base normale d'entiers. D'après ce même ce travail, on sait pour $d = -3, -4, -7$ on peut construire des extensions de la forme $K(\mathfrak{p}\mathfrak{q})/K$ est sans base normale d'entiers, où $\mathfrak{p}$ et $\mathfrak{q}$ sont des premiers dans K.

ii) $h_K > 1$ et Cl_K n'est pas un 2-groupe. — On prend $L = H_K$ le corps de classes de Hilbert de K. On sait qu'il existe $\alpha \in \mathbb{C}$ telle que: $L = \mathbb{Q}(\alpha)$. L'extension $L/\mathbb{Q}(\alpha + \overline{\alpha})$ est quadratique imaginaire et bien sûr $\mathbb{Q}(\alpha + \overline{\alpha})/\mathbb{Q}$ est réelle. Donc, L/K est non ramifée abélienne et extensions de corps CM. On se ramène aux hypothèses du résultat de J.Brinkhuis [1]. On l'applique et on obtient que $K(1)/K$ est sans base normale d'entiers. Ce qui achève la *démonstration du théorème A.*

Remarque. — *Pour $d = p$ premier et congru à 1 (mod 4) ou $d = 2$, on pose $K = \mathbb{Q}(\sqrt{d})$. Alors, toute extension quadratique $K(\sqrt{m})/K$ non ramifiée en 2 admet une base normale d'entiers, où $m \in \mathbb{Z}^*$ sans facteur carré.*

Démonstration. — Soit $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique réel où $d = 1$ (mod 4), ou $K = \mathbb{Q}(\sqrt{2})$. Si $K(\sqrt{m})/K$ est non ramifée en 2 alors $m = 1$ (mod 4). De plus, on peut imposer à m de vérifier: $(d, m) = 1$. En effet, si d divise m on remplace $\sqrt{m}$ par $\sqrt{\frac{m}{d}}$, on obtient $\frac{m}{d} = 1$ (mod 4) et $(\frac{m}{d}, d) = 1$. Le fait, qu'on peut choisir $(d, m) = 1$ avec $m = 1$ (mod 4), implique que

$$O_{K(\sqrt{m})} = O_K O_{\mathbb{Q}(\sqrt{m})} = O_K\left[\frac{1+\sqrt{m}}{2}\right]$$

D'où $\{\frac{1+\sqrt{m}}{2}; \frac{1-\sqrt{m}}{2}\}$ est une base normale pour $K(\sqrt{m})/K$. Il serait intéréssant d'expliciter, si elle existe, une extension N/K modérée sans base normale d'entiers.

Montrons le théorème C: Pour $d < 0$ non premier, on pose $d = d_0.d_1$, $K = \mathbb{Q}(\sqrt{d})$ avec $|d_0|$ et $|d_1| > 1$, et $N = K(\sqrt{d_i})$ si $d_i = 1$ (mod 4), pour un $i = 0$ ou 1 (resp. $N = K(\sqrt{-d_i})$ si $d_i = 3$ (mod 4), pour un $i = 0$ ou 1) et lorsque $d < 0$ est premier congru à 3 mod 4 on pose $N = K(\sqrt{-1})$ (resp. si $d = -2$ on pose $N = K(\sqrt{2}), K = \mathbb{Q}(\sqrt{-2})$). D'après **1).-**, on a N/K est une quadratique réelle non ramifiée en tout premier fini. De même, si $d > 0$ non premier et admettant un diviseur propre $d_i > 0$ congru à 1 (mod 4) alors l'extension $N = K(\sqrt{d_i})/K$ pour $K = \mathbb{Q}(\sqrt{d})$ est une quadratique réelle non ramifiée en tout premier fini. Donc, finalement dans les deux cas on a une extension N/K abélienne non ramifiée partout. Comme H_K est la plus grande extension abélienne non ramifiée partout de K, alors $N \subset H_K$. Dans la démonstration des théorèmes A et B on montre que ces mêmes extensions N/K sont sans base normale d'entiers. Donc, H_K/K est sans base normale d'entiers et de degré pair.

Bibliographie

[1] J.Brinkhuis. — *Normal integral bases and complex conjugation*, J.Reine Angew. Math **375** (1987), 157–166.

[2] J.Cougnard. — *Une remarque sur l'anneau des entiers du corps des racines septièmes de l'unité*, Séminaire de théorie de nombres de Besançon, 1983.

[3] J.Cougnard. — *La non existence de base normale relative dans le corps des racines 11-èmes de l'unité*, Séminaire de théorie de nombres de Bordeaux, 1984.

[4] J.Cougnard. — *Quelques extensions modérément ramifiées sans bases normales*, J.London.Math.Soc **32** (1985), 200–204.

[5] J.Cougnard. — *Bases normales relatives dans certaines extensions cyclotomiques*, J.Number Theory **23** (1986), 336–346.

[6] E.J.Gómez-Ayala. — *Bases normales d'entiers dans les extensions de Kummer de degré premier*, J.de théorie de nombres Bordeaux **6** (1994), 95–116.

[7] E.J.Gómez-Ayala. — *Normal bases for quadratic extensions inside cyclotomic fields* , Archiv.Math **Vol 66** (1996), 123–125.

[8] E.J.Gómez-Ayala, R.Schertz. — *Eine Bemerkung zur Galoismodulstruktur in Strahlklasenkörpern über imaginär-Quadratischen Zahlkörpern*, J.Number Theory **44** (1993), 41–46.

[9] C.Greither. — *On normal integral bases in ray class fields over imaginary quadratic fields*, Acta Arithmetica **Vol.78** (1997), 315–329.

[10] S.Lang. — *Algebraic number theory*, Addison-Wesley, 1973.

[11] A.Srivastav and S.Venkataraman. — *Unramified Quadratic Extensions of Real Quadratic Fields, Normal integral Bases, and 2-adic L-Functions*, J.Number Theory **67** (1997), 139–145.

– ◇ –

Abdelmejid BAYAD
Université d'Evry Val d'Essonne
Département de Mathématiques
Boulevard des Coquibus
91025 EVRY Cedex (France)
bayad@lami.univ-evry.fr