Werk

Titel: Sur la construction d'un corps de Hilbert.

Autor: Lbekkouri, Aboubakr

Jahr: 1989

PURL: https://resolver.sub.uni-goettingen.de/purl?365956996_0065|log20

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

manuscripta math. 65, 257 - 273 (1989)

manuscripta
mathematica
© Springer-Verlag 1989

SUR LA CONSTRUCTION D'UN CORPS DE HILBERT

Aboubakr LBEKKOURI

We are concerned with the following : If k is a quadratic field and N a cyclic unramified extension of degree q^n over k, q a prime number, determine N explicitely via a primitive element β, i.e., $N = k(\beta)$, in the spirit of Helmut Hasse [3] . We propose a method which determines these extensions, once we are able to specify the arithmetic of a certain field $k_{\overline{\chi}}$. To explicit our method, we construct the Hilbert fields of $\mathbb{Q}(\sqrt{226})$ and $\mathbb{Q}(\sqrt{646})$.

1. INTRODUCTION

La théorie du corps de classes permet de décrire les extensions abéliennes L d'un corps de nombres K, par leur groupe de Galois, à l'aide de groupes d'idéaux de K premiers aux idéaux ramifiés dans L; mais elle ne permet jamais de les construire, au moyen d'un polynôme par exemple.

Dans [4], Kerkour donne une méthode de construction explicite d'extensions N cycliques non ramifiées de degré q^n, q premier, d'un corps de nombres k. Cette méthode consiste à adjoindre à k une racine primitive q^n-ème de l'unité ω et à chercher parmi les extensions cycliques de degré q^n de $k(\omega)$ celles qui se décomposent en des extensions cycliques sur L , L un sous corps de $k(\omega)$ contenant k. Les générateurs des extensions de Kummer de degré q^n de $k(\omega)$ cherchées seront puisés dans un certain corps "plus petit" $k_{\overline{\chi}}$. En utilisant cette construction conjoitement avec la théorie du corps de classes, Kerkour détermine numériquement l'extension cyclique non ramifiée de degré 9 de $\mathbb{Q}(\sqrt{1129})$.

Dans ce travail on s'intéresse à la construction effective et numérique des extensions N cycliques non ramifiées de degré 2^n, d'un corps quadratique k et plus particulièrement à la détermination d'exemples numériques de telles extensions. Pour cela on utilise conjointement les résultats de [4] d'une part et l'algorithme de Gras d'autre part [2].

On résume maintenant les principaux résultats de [4] .
On désigne successivement par q un nombre premier, k_0 un corps de nombres et k une extension cyclique de k_0 de degré p, p premier ou égal à 1, divisant q(q-1). Soit $\mathcal{G}$ l e groupe de Galois de k sur k_0 engendré par $\mathcal{S}$. Pour tout entier m, m ≥ 1, on note $L^{(m)}$ le corps engendré par L et par une racine primitive q^m -ème de l'unité. Soient r un entier positif ou nul, n un entier, n ≥ 1, L un sous corps de $k^{(n+r)}$ cyclique de degré q^r sur k, $\mathbb{G}$ (resp. $\mathbb{G}'$, $\mathbb{G}''$) le groupe de Galois de $L^{(n)}$ sur L (resp. $L^{(n)}$ sur k, $L^{(n)}$ sur k_0). on définit l'entier i, i ≥ n, tel que $L^{(n)} = k^{(i)}$, et on distingue les deux cas suivants:

1^{er} cas : Pour les cas distincts du cas p = q, L = k et L/k_0 cyclique,
le corps L est le composé de k et d'un sous corps L_0 de $k_0^{(i)}$ cyclique de degré q^r sur k_0. Alors on définit ce qui suit. Soient $\mathfrak{X}$ le groupe des homomorphismes de $Gal(L^{(n)}/L_0)$ dans $(\mathbb{Z}/q^n\mathbb{Z})^*$, $\mathfrak{X}_0$ un sous groupe d'ordre p de $\mathfrak{X}$ dont les élements sont triviaux sur $\mathbb{G}$. Si q = 2 et n ≥ 3, $\mathfrak{X}_0(-1)$, $\mathfrak{X}_0(-1 + 2^{n-1})$ et $\mathfrak{X}_0(1 + 2^{n-1})$ désignent les 3 sous groupes $\mathfrak{X}_0$ possibles, qui sont respectivement définis par : $\chi(\mathcal{S}) = -1$, $\chi(\mathcal{S}) = -1 + 2^{n-1}$ et $\chi(\mathcal{S}) = 1 + 2^{n-1}$, χ étant un générateur du groupe $\mathfrak{X}_0$ correspondant. Soit ω une racine primitive q^n -ème de l'unité. Pour tout élément $\mathbb{S}$ de $\mathbb{G}'$ il existe un entier $r(\mathbb{S})$ mod q^n tel que $\omega^{r(\mathbb{S})} = \omega^{\mathbb{S}}$. On désigne par x^* l'élément de $\mathfrak{X}$ qui fait correspondre à tout $\mathbb{S}$ de $Gal(L^{(n)}/L_0)$ la classe mod q^n de $r(\mathbb{S})$. Pour tout élément χ de $\mathfrak{X}_0$ on appelle caractère reflet de χ l'élément $\chi^{-1}x^*$, noté $\overline{\chi}$ et on appelle $L_{\overline{\chi}}$ le corps fixe par $\ker\overline{\chi}$. Si la classe de -1 mod 2^n est dans l'image de $\mathbb{G}$ par x*, on appelle $\mathbb{S}_{-1}$ son unique antécédent. On appelle d le degré de $L^{(n)}$ sur L et on pose $d = hq^t$ avec h diviseur de (q - 1) et t un entier tel que : $0 \le t \le n-1$. Le lemme suivant définit mieux $L_{\overline{\chi}}$:

LEMME 1.1. *Soit χ un élément non trivial de $\mathfrak{X}_0$, on a :*

a) si $\ker\overline{\chi} \neq \{1\}$, alors $\ker\overline{\chi}$ est un sous groupe d'ordre p de $Gal(L^{(n)}/L_0)$ et $Gal(L_{\overline{\chi}}/L_0)$ est canoniquement isomorphe à $\mathbb{G}$ par restriction.

b) si $L \cap L_0^{(n)} = L_0$, on a :

$\ker\overline{\chi} = \{\mathcal{S}\mathbb{S}, \mathcal{S} \in \mathcal{G}$ et $\mathbb{S} \in \mathbb{G}$ tel que $\chi(\mathcal{S}) = x^*(\mathbb{S})\}$.

c) si q = 2 , si L est un sous corps de $L_0^{(n)}$ et si $\mathbb{S}$ et $\mathbb{S}_{-1}$ sont deux générateurs de $Gal(L^{(n)}/L_0)$, alors $\ker\overline{\chi} = \{1\}$ sauf dans les cas α) et β) suivants :

α) $\mathfrak{S}_{-1} \notin \mathfrak{G}$, en choisissant $\mathfrak{S}$ dans $\mathfrak{G}$ on a :

i) si $\mathfrak{X}_o = \mathfrak{X}_o(-1)$, alors $ker\overline{\chi} = \{1, \mathfrak{S}_{-1}\}$

ii) si $\mathfrak{X}_o = \mathfrak{X}_o(-1 + 2^{n-1})$, alors $ker\overline{\chi} = \{1, \mathfrak{S}^{2^{t-1}} \cdot \mathfrak{S}_{-1}\}$

β) $d = 2$ et $\mathfrak{S}_{-1} \in \mathfrak{G}$

i) si $\mathfrak{X}_o = \mathfrak{X}_o(1 + 2^{n-1})$, on a $ker\overline{\chi} = [1, \mathfrak{S}]$

ii) si $\mathfrak{X}_o = \mathfrak{X}_o(-1 + 2^{n-1})$, on a $ker\overline{\chi} = [1, \mathfrak{S}\mathfrak{S}_{-1}]$

$2^{ème}$cas : si $p = q$, L/k_o cyclique et $L \neq k$, alors $k^{(i)} = k_o^{(i)}$

Soit $\mathfrak{X}$ le groupe des homomorphismes de $\mathbb{G}''$ dans $(\mathbb{Z}/q^i\mathbb{Z})^*$, $\mathfrak{X}_o$ un sous groupe de $\mathfrak{X}$ d'ordre p dont les éléments sont triviaux sur $\mathbb{G}'$. En raisonnant mod q^i ou bien q^n on définit par analogie avec le 1^{er} cas, les éléments x^*, $\mathfrak{S}_{-1}$, $\overline{\chi}$ et $k_{\overline{\chi}}$. On posera $k_{\overline{\chi}} = L_{\overline{\chi}}$ et on désignera par $d=hq^t$ le degré de $L^{(n)}$ sur L.

On se propose de déterminer les extensions galoisiennes sur k_o, cycliques de degré q^{r+n} sur k et linéairement disjointes de $k^{(n+r)}$ sur L associées à un élément χ de $\mathfrak{X}_o$. La méthode consiste à chercher parmi les extensions de degré q^n de L linéairement disjointes de $L^{(n)}$ sur L celles qui sont cycliques sur k et galoisiennes sur k_o. On a besoin de :

PROPOSITION 1.2. *Pour tout élément $\mathfrak{S}$ de $\mathbb{G}''$ d'ordre r, il existe deux éléments $a_{\mathfrak{S}}$ et $m_{\mathfrak{S}}$ de $\mathbb{Z}$ et un élément $e_{\mathfrak{S}}$ de $\mathbb{Z}[\mathbb{G}'']$ tels que :*

1) $x^*(\mathfrak{S})$ est la classe résiduelle mod q^i de $a_{\mathfrak{S}}$.

2) $e_{\mathfrak{S}} = \sum_{i=1}^{r} a_{\mathfrak{S}}^{r-i}\,\mathfrak{S}^{i-1}$, $a_{\mathfrak{S}}^r = 1 + m_{\mathfrak{S}} q^n$ et $e_{\mathfrak{S}}(\mathfrak{S} - a_{\mathfrak{S}}) = -m_{\mathfrak{S}} q^n$

3) si $q = 2$ et $\mathfrak{S} = \mathfrak{S}_{-1}$, alors $m_{\mathfrak{S}_{-1}} = m2^{i-n+1}$ avec $m = 2^{i-1} - 1$

4) si $\mathfrak{S} \neq \mathfrak{S}_{-1}$, alors $m_{\mathfrak{S}} = m'q^{i-n}$; m' premier avec q.

On définit maintenant les ensembles suivants:

1^{er}cas : $L = k$

Soit χ un élément de $\mathfrak{X}_o$, le groupe de Galois de $k_{\overline{\chi}}$ sur k_o est de la forme $\overline{\mathbb{G}}x\overline{\mathfrak{g}}$ avec $\overline{\mathfrak{g}} = \mathfrak{g}$ ou $\overline{\mathfrak{g}} = \{1\}$ et $\overline{\mathbb{G}}$ un groupe canoniquement isomorphe à $\mathbb{G}$ ou bien $\overline{\mathbb{G}} = \mathbb{G}'$. A toute extension cyclique k de degré p de k_o et à tout élément χ de $\mathfrak{X}_o$ nous associons le sous groupe A_χ de $k_{\overline{\chi}}^*$ formé par les éléments α qui vérifient :

1) a) $\mathcal{G}$ *cyclique,* $\mathcal{S}_{-1} \notin \mathcal{G}$

$\forall\, \mathcal{S} \in \mathcal{G} \quad \exists\, b_{\mathcal{S}} \in k_{\overline{\chi}}\,;\ \alpha^{m_{\mathcal{S}}} = b_{\mathcal{S}}^{e_{\mathcal{S}}}$.

b) $\mathcal{G}$ *cyclique,* $\mathcal{S}_{-1} \notin \mathcal{G}$, *(necessairement* $q = 2$*)*

$\exists\, b_{\mathcal{S}_{-1}} \in k_{\overline{\chi}}\,;\ \alpha^{\mathcal{S}_{-1}-a_{\mathcal{S}_{-1}}} = b_{\mathcal{S}_{-1}}^{-2^n}$ et $\alpha^{m_{\mathcal{S}_{-1}}} = b_{\mathcal{S}_{-1}}^{e_{\mathcal{S}_{-1}}}$.

c) $\mathcal{G}$ *non cyclique* ($q = 2$ *et* $n > 2$)

Si $\mathcal{S}$ et $\mathcal{S}_{-1}$ engendrent $\mathcal{G}$, il existe $b_{\mathcal{S}}$ et $b_{\mathcal{S}_1}$ de $k_{\overline{\chi}}$ tels que :

$\alpha^{m_{\mathcal{S}}} = b_{\mathcal{S}}^{e_{\mathcal{S}}}$, $\alpha^{m_{\mathcal{S}_{-1}}} = b_{\mathcal{S}_{-1}}^{e_{\mathcal{S}_{-1}}}$ et $b_{\mathcal{S}}^{e_{\mathcal{S}_{-1}} - a_{\mathcal{S}_{-1}}} = b_{\mathcal{S}_{-1}}^{\mathcal{S}-a_{\mathcal{S}}}$

2) χ *non trivial et* $\ker\overline{\chi} = \{1\}$

$\forall\, \mathcal{S} \in \mathcal{G} \quad \exists\, b_{\mathcal{S}} \in k_{\overline{\chi}}\,;\ \alpha^{m_{\mathcal{S}}} = b_{\mathcal{S}}^{e_{\mathcal{S}}}$ avec de plus, si $q = 2$ et $\overline{\chi}(\mathcal{S}) = -1$,

$\alpha^{\mathcal{S}-a_{\mathcal{S}}} = b_{\mathcal{S}}^{-2^n}$ et $\forall\, \mathcal{S}' \in \mathcal{G}\ \ b_{\mathcal{S}}^{\mathcal{S}'-a_{\mathcal{S}'}} = b_{\mathcal{S}'}^{\mathcal{S}-a_{\mathcal{S}}}$.

2 éme cas : $L \neq k$

Soit ω une racine primitive q^n-ème de l'unité . On désigne par A_r l'ensemble des éléments α de $L_{\overline{\chi}}^*$ non puissance q-ème dans $k^{(n+r)}$ et vérifiant les conditions suivantes (on a deux cas) :

1) $L^{(n)} = k^{(n)}$

a) $\mathcal{G}'$ *cyclique,* $\mathcal{S}_{-1} \in \mathcal{G}'$

Il existe $b_{\mathcal{S}}$ de $L^{(n)}$ tel que $\alpha^{\mathcal{S}_{-1}-a_{\mathcal{S}_{-1}}} = b_{\mathcal{S}_{-1}}^{-2^n}$ et $\alpha^{m_{\mathcal{S}_{-1}}} = \omega b_{\mathcal{S}_{-1}}^{e_{\mathcal{S}_{-1}}}$

b) $\mathcal{G}'$ *cyclique,* $\mathcal{S}_{-1} \notin \mathcal{G}'$

$\forall\, \mathcal{S} \in \mathcal{G}'\ \exists\, b_{\mathcal{S}} \in L^{(n)*}\ ;\ \alpha^{m_{\mathcal{S}}} = \omega^{q^t} b_{\mathcal{S}}^{e_{\mathcal{S}}}$.

c) $\mathcal{G}'$ *non cyclique*

Soient $\mathcal{S}$ et $\mathcal{S}_{-1}$ deux générateurs de $\mathcal{G}'$ respectivement d'ordre 2^{r+t-1} et 2, il existe $b_{\mathcal{S}}$ et $b_{\mathcal{S}_{-1}}$ tels que (selon $\mathcal{G}$) :

i) $\mathcal{G} = \langle \mathcal{S}^{2^r}, \mathcal{S}_{-1} \rangle$

$\alpha^{m_{\mathcal{S}}} = \omega^{2^{t-1}} b_{\mathcal{S}}^{e_{\mathcal{S}}}$, $\alpha^{m_{\mathcal{S}_{-1}}} = b_{\mathcal{S}_{-1}}^{e_{\mathcal{S}_{-1}}}$ et $b_{\mathcal{S}}^{\mathcal{S}_{-1}-a_{\mathcal{S}_{-1}}} = b_{\mathcal{S}_{-1}}^{\mathcal{S}-a_{\mathcal{S}}}$.

ii) $\mathcal{G} = < \mathcal{S}^{2^{r-1}} \mathcal{S}_{-1} >$

$$\alpha^{m_{\mathcal{S}}} = \omega^{2^{t-1}} b_{\mathcal{S}}^{e_{\mathcal{S}}}, \quad \alpha^{m_{\mathcal{S}_{-1}}} = \omega b_{\mathcal{S}_{-1}}^{e_{\mathcal{S}_{-1}}} \quad \text{et} \quad b_{\mathcal{S}}^{\mathcal{S}_{-1} - a_{\mathcal{S}_{-1}}} = b_{\mathcal{S}_{-1}}^{\mathcal{S} - a_{\mathcal{S}}}.$$

iii) $\mathcal{G} = < \mathcal{S} >$ *(on a r = 1)*

$$\alpha^{m_{\mathcal{S}}} = b_{\mathcal{S}}^{e_{\mathcal{S}}}, \quad \alpha^{m_{\mathcal{S}_{-1}}} = \omega b_{\mathcal{S}_{-1}}^{e_{\mathcal{S}_{-1}}} \quad \text{et} \quad b_{\mathcal{S}}^{\mathcal{S}_{-1} - a_{\mathcal{S}_{-1}}} = b_{\mathcal{S}_{-1}}^{\mathcal{S} - a_{\mathcal{S}}}.$$

2) $L^{(n)} \neq k^{(n)}$

Les conditions relatives au cas $L^{(n)} = k^{(n)}$ restent valables pour chaque cas énuméré précédemment, de plus on devra avoir :

$$\alpha^{\mathcal{S} - a_{\mathcal{S}}} = b_{\mathcal{S}}^{-q^n} \quad \text{et} \quad \alpha^{\mathcal{S}_{-1} - a_{\mathcal{S}_{-1}}} = b_{\mathcal{S}_{-1}}^{-q^n}.$$

REMARQUE. Lorsque r = o i.e., L = k on pose $A_r = A_\chi$.

Pour tout χ de $\mathfrak{X}_0$, on désigne par $\mathcal{K}_\chi$ l'ensemble des extensions cycliques de degré q^{n+r} de k, linéairement disjointes de $k^{(n+r)}$ sur L et galoisiennes sur k_o à groupe de Galois du type : $\mathcal{S}\tau\mathcal{S}^{-1} = \tau^{\chi(\mathcal{S})}$, $\tau^{q^{n+r}} = \mathcal{S}^p = 1$

Soit $\mathcal{R}_\chi$ la relation d'équivalence définie sur $\mathcal{K}_\chi$ par : $N_1 \mathcal{R}_\chi N_2 \Leftrightarrow N_1^{(n)} = N_2^{(n)}$.
On a alors :

THEOREME 1.3. *Si χ est un élément de $\mathfrak{X}_0$ alors on a :*

1) Il existe une correspondance biunivoque entre les éléments de $\mathcal{K}_\chi / \mathcal{R}_\chi$ et ceux de A_χ.

2) Si $p \neq q$ et si χ est non trivial, alors il y a un élément de $\mathcal{K}_\chi$ et un seul par classe d'équivalence mod $\mathcal{R}_\chi$.

3) Toute classe mod $\mathcal{R}_\chi$ contient q^t éléments de $\mathcal{K}_\chi$ si :

($\mathfrak{X}_0 \neq \{1\}$ et $\chi = 1$) ou ($p = q$ et $q \neq 2$) ou ($q = 2$ et $\mathfrak{X}_0 = \mathfrak{X}_0(1 + 2^{n-1})$)

4)Toute classe mod $\mathcal{R}_\chi$ contient 4 éléments de $\mathcal{K}_\chi$ si

($q = 2$ et $\mathfrak{X}_0 = \mathfrak{X}_0(-1)$) ou ($q = 2$ et $\mathfrak{X}_0 = \mathfrak{X}_0(-1 + 2^{n-1})$).

Dénombrement des extensions N_i galoisiennes sur k_o.

$\mathcal{G}$ cyclique : chaque N_i est défini par un sous groupe $H_i = < \overline{\mathcal{S}}\tau^{iq^{n-t}} >$ avec $\overline{\mathcal{S}}$

le relèvement de $\mathfrak{S}$ défini par $\alpha'^{\overline{\mathfrak{S}} - a_{\mathfrak{S}}} = b_{\mathfrak{S}}^{- m_{\mathfrak{S}}}$, α' étant une racine q^n ème de α, $<\tau> = Gal(N^{(n)}/L^{(n)})$ et $1 \le i \le q^t$.

$\mathcal{G}$ non cyclique : chaque $N_{i,j}$ est défini par un sous groupe $H_{i,j} = <\overline{\mathfrak{S}}\tau^{i2^{n-t+1}}, \overline{\mathfrak{S}}_{-1}\tau^{j2^{n-1}}>$, $1 \le i \le 2^{t-1}$, $1 \le j \le 2$, $\overline{\mathfrak{S}}$ et $\overline{\mathfrak{S}}_{-1}$ étant les relèvements de $\mathfrak{S}$ et $\mathfrak{S}_{-1}$ définis par $(\alpha'^{m_{\mathfrak{S}}})^{\overline{\mathfrak{S}} - a_{\mathfrak{S}}} = b_{\mathfrak{S}}^{- m_{\mathfrak{S}}}$ et $(\alpha'^{m_{\mathfrak{S}_{-1}}})^{\overline{\mathfrak{S}}_{-1} - a_{\mathfrak{S}_{-1}}} = b_{\mathfrak{S}_{-1}}^{- m_{\mathfrak{S}_{-1}}}$.

PROPOSITION 1.4. *La trace de α' relative à H_i (ou $H_{i,j}$) est un élément primitif de N_i (ou $N_{i,j}$) sur L.*

On énonce maintenant un résultat concernant la ramification d'un idéal premier P_K de K (corps de nombres) dans une extension de Kummer cyclique M de degré q^n. On désigne par V_K la valuation discrète associée à P_K. On a alors :

PROPOSITION 1.5.*Soit $M = K(\sqrt[q^n]{\alpha})$ et ω une racine primitive q^n ème de 1*

1) si $V_K(q^n) = 0$ et $V_K(\alpha) \equiv 0 \mod q^n$, alors P_K est non ramifié.

2) si $V_K(\alpha) = 0$, P_K est non ramifié dans M si $t_n \ge q^{n-1}(nq - n + 1)V_K(1 - \omega)$, où t_n est l'entier maximum pour lequel la congruence $\alpha \equiv X^{q^n} \mod P_K^{t_n}$ est soluble dans K.

On garde les notations ci dessus et on introduit les suivantes

d : un élément de $\mathbb{Z}$ sans facteurs carrés.
$k=\mathbb{Q}(\sqrt{d})$ avec $k \cap \mathbb{Q}(\omega) = \mathbb{Q}$.
A_L : l'anneau des entiers du corps de nombres L.
$N_{L/K}$: la norme du corps L sur K.
G(L/K) : le groupe de Galois de L sur K.
H(L) : le groupe des classes au sens ordinaire de L.
H*(L) : le groupe des classes au sens réstreint de L.
$H_p(L)$: le p-sous groupe de H(L).
$e_{L/K}(P)$: l'indice de ramification du premier P dans L.
$f_{L/K}(P)$: le degré résiduel de P dans L.
EA(NR) : extension abélienne (non ramifiée)
EC(NR) : extension cyclique (non ramifiée)
LD : linéairement disjointe.
(O), (R) : sens ordinaire, sens réstreint réspectivement.
Rp(n) : racine primitive n-ème de l'unité.
ω : une racine primitive q^n-ème de l'unité.

2. ETUDE DE LA RAMIFICATION DANS k(ω)

PROPOSITION 2.1. *Soit P un premier de k divisant q , q ≠ 2,*

1) si q divise d , $e_{k(\omega)\,/\,k}(P) = \frac{q-1}{2} q^{n-1}$

2) si q ne divise pas d , P est totalement ramifié dans k(ω) .

PROPOSITION 2.2. *Soit P un premier de k divisant 2,*

1) si d ≡ 1 mod 4, P est totalement ramifié dans k(ω).

2) si d ≡ 3 mod 4, $e_{k(\omega)\,/\,k}(P) = 2^{n-2}$

3) si d ≡ 2 mod 4, $e_{k(\omega)\,/\,k}(P) = \begin{cases} 2^{n-2} & \text{pour } n > 2 \\ 2 & \text{pour } n = 2 \end{cases}$.

Preuve . On traitera le cas n = 3.

2) Soit $\pi = 1 - \omega$, $V_\pi(d) = o$, $d \equiv 1 + \pi^4 + \pi^6 = (1+\pi^2)^2 \mod \pi^8$, alors $e_{k(\omega)/k}(P) = 2$. $f_{k(\omega)/k}(P) = 2$ si $d \equiv 3 \mod 8$ car $d \equiv y^2 \mod \pi^9$ n'est pas soluble , $f_{k(\omega)/k}(P) = 1$ si $d \equiv 7 \mod 8$ car $1 + \pi^2$ est solution de la congruence ([2], Proposition 1.2).

3) Il suffit de remarquer que $\mathbb{Q}(\sqrt{\frac{d}{2}})$ est dans k(ω).

Pour n > 3, $\mathbb{Q}(\omega)$ contient les racines 8-èmes de l'unité.

3.EXTENSIONS ABELIENNES NON RAMIFIEES DE DEGRE 2^n

PROPOSITION 3.1. *Soit ω une Rp(*2^n *),*

1) si d ≡1 mod 4 , toute EANR de k est LD de k(ω) sur k.

2) si d ≡ 3 mod 4 , on a :

a) si k est réel, toute EANR(O) de k est LD de k(ω) sur k.

b) si $H_2^*(k)$ *est cyclique d'ordre* 2^n *, toute ECNR(R) de degré* 2^r *de k est LD de k(ω) sur k (*$\sqrt{-1}$*).*

3) si d ≡ 2 mod 4 , on a :

a) si $k \subset \mathbb{R}$ *et* $\frac{d}{2} \equiv 3 \mod 4$ *, toute EANR(O) est LD de k(ω) sur k .*

b) si $\frac{d}{2} \equiv 1 \mod 4$*, et si* $H_2(k)$ *(resp.* $H_2^*(k)$*) est cyclique d'ordre* 2^n*, toute ECNR(O) (resp. ECNR(R)) de degré* 2^r *est LD de k(ω) sur k(*$\sqrt{2}$*) pour n > 2.*

c) si $\frac{d}{2} \equiv 3 \mod 4$ *et si* $H_2^*(k)$ *est cyclique d'ordre* 2^n *toute ECNR(R) de degré* 2^r *de k est LD de k(ω) sur k(*$\sqrt{-2}$*).*

Preuve. D'après la Proposition 2.2 , $\mathbb{Q}(\sqrt{2}, \sqrt{d})$ et $\mathbb{Q}(\sqrt{d}, \sqrt{-2})$ sont ramifiés sur k et $\mathbb{Q}(\sqrt{d}, \sqrt{-1})$ est ramifiée aux places infinies de k.

3) si $\frac{d}{2} \equiv 1 \bmod 4$, $\mathbb{Q}(\sqrt{d}, \sqrt{-2})$ et $\mathbb{Q}(\sqrt{d}, \sqrt{-1})$ sont ramifiées sur k et $\mathbb{Q}(\sqrt{d}, \sqrt{2})$ est la seule sous extension non ramifiée de $k(\omega)$.

si $\frac{d}{2} \equiv 3 \bmod 4$, $k(\sqrt{2})$ et $k(\sqrt{-1})$ sont ramifiées sur k et $k(\sqrt{-2})$ est non ramifiée pour les places finies.

REMARQUE. Si $n = 2$ et $d \equiv 2 \bmod 4$, toute EANR de degré 2^r sur k est LD de $k(\sqrt{-1})$.Soit N une EC de degré 2^n sur k, $n > 3$, diédrale sur $\mathbb{Q}$ et LD de $k(\omega)$ sur L. Soit $\langle \mathcal{S} \rangle = \mathcal{G}$, à N est associé un élément χ de $\mathfrak{X}$ tel que $\chi(\mathcal{S}) = -1$. Le corps $L_{\overline{\chi}}$ associé est $\mathbb{Q}(\sqrt{-d}, \omega+\omega^{-1})$ si $L = k$ et $\mathbb{Q}(\sqrt{-d}, \omega^2 + \omega^{-2})$ si $L \neq k$.

Pour $n = 3$, on a les cas suivants pour $L_{\overline{\chi}}$:

$\mathbb{Q}(\sqrt{d}, \sqrt{-1})$ si $\sqrt{-1} \in L$, $\mathbb{Q}(\sqrt{-d}, \sqrt{2})$ si $L = k$ et $\mathbb{Q}(\sqrt{-d}, \sqrt{2})$ si $\sqrt{-1} \notin L$.

Pour $d < 0$, Les groupes des unités de $k(\sqrt{2})$ et $\mathbb{Q}(\sqrt{2})$ sont égaux.

Les lemmes suivants seront utiles par la suite.

LEMME 3.2. *Soit k un corps quadratique ; (q, H(k)) = 1 et k_o une extension quadratique de k, alors toute ECNR de degré q^n sur k , $n > 1$ si $q = 2$, est diédrale sur k.*

LEMME 3.3. *Soit ω une Rp(n) et N une EANR sur L , alors $N(\omega)$ est non ramifiée sur $L(\omega)$.*

Soit L_0 une EC de L de degré premier p telle que L_0 et $L(\omega)$ soient LD sur L.

PROPOSITION 3.4. *Soit $\alpha \in L_o(\omega)$ et $K = L_o(\omega)(\sqrt[q^n]{\alpha})$ une EC de $L_o(\omega)$, K se décompose en une EC de degré q^n sur L_o galoisienne sur L. Si $p \neq q$ et $\alpha A_{L_o(\omega)} = \mathbb{I}^{q^n}$, $\mathbb{I}$ idéal de $L_o(\omega)$, on peut choisir α et $\mathbb{I}$ dans $L_{o\overline{\chi}}$.*

Preuve. On peut choisir $\alpha \in L_{o\overline{\chi}}$ (Proposition 1.3). Comme $\alpha^p A_{L_{o\overline{\chi}}} = N_{L_o(\omega)/L_{o\overline{\chi}}}(\mathbb{I})^{q^n}$ (Lemme 1.1) et $(p,q) = 1$, α^p engendre K sur $L_0(\omega)$.

COROLLAIRE 3.5. *Si de plus le groupe des unités de $L_{o\overline{\chi}}$ est contenu dans $L(\omega)$, on peut choisir α et $\mathbb{I}$ dans $L_{o\overline{\chi}}$ avec la classe de $\mathbb{I}$ au sens ordinaire, d'ordre q^n .*

Preuve. Si $\mathbb{I}^{q^n} = \beta A_{L_o\overline{\chi}}$, $\beta \in L_{o\overline{\chi}}$ et $0 < i < n$, $\alpha = \beta^{q^{n-i}} u$. Or $\ker\overline{\chi} = G(L_o(\omega)/L_{o\overline{\chi}})$, d'où $u^{\mathbb{S}^j} = u^{\mathbb{S}^j} = u$. Comme $\alpha^{\mathbb{S}-a_{\mathbb{S}}} = v^{q^n}$, $v \in L_{o\overline{\chi}}$ (Proposition 1.2), $\alpha^{\mathbb{S}^j - a_{\mathbb{S}^j}} = (\beta^{\mathbb{S}^j - a_{\mathbb{S}^j}})^{q^{n-i}} u^{1-a_{\mathbb{S}^j}}$. $p \neq q$, donc $p \mid (q-1)$, d'où $a_{\mathbb{S}^j} \not\equiv 1 \bmod q$ et $(1 - a_{\mathbb{S}^j}, q) = 1$, donc α est une puissance de q dans $L_o(\omega)$.

PROPOSITION 3.6. *Soit ω une Rp(2^n), N une EC de degré 2^n de k, LD de $k(\omega)$ sur k, galoisienne sur $\mathbb{Q}$ et $\alpha \in k(\omega)$ tel que $N(\omega) = k(\omega)(\sqrt[2^n]{\alpha})$. Si $\alpha A_{k(\omega)} = \mathbb{I}^{2^n}$, $\mathbb{I}$ idéal de $k(\omega)$, on peut choisir $\mathbb{I}$ dans $k_{\overline{\chi}}$ dans les cas suivants :*

a) l'élément α n'est pas divisible par 2

b) l'extension $k(\omega) / k_{\overline{\chi}}$ est non ramifiée en 2.

Preuve. On peut choisir $\alpha \in k_{\overline{\chi}}$ (Théorème 1.3), si $\mathbb{I} = \prod_i \mathfrak{P}_i^{e_i}$ avec $\mathfrak{P}_i$ premier de $k(\omega)$ divisant P_i, idéal premier de $k_{\overline{\chi}}$, alors $N(\mathfrak{P}_i) = P_i^{f_i}$, comme $\alpha^2 A_{k_{\overline{\chi}}} = N_{k(\omega)/k_{\overline{\chi}}}(\mathbb{I})^{2^n} = \mathbb{I}^{2^{n+1}}$, $\prod_i \mathfrak{P}_i^{2^{n+1} e_i} = \prod_i (P_i A_{k(\omega)})^{2^n e_i f_i}$, vu la nature de $k_{\overline{\chi}}$, $k(\omega)/k_{\overline{\chi}}$ ne peut être ramifiée qu'en 2, or les $\mathfrak{P}_i$ sont non ramifiés dans $k(\omega)$, d'où $\alpha A_{k_{\overline{\chi}}} = (\prod_i P_i^{e_i})^{2^n}$.

COROLLAIRE 3.7. *On suppose de plus k réel et $n = 3$, alors la classe de $\mathbb{I}$ est d'ordre 8 dans $H_2(k_{\overline{\chi}})$.*

Preuve. Si $\mathbb{I}^{2^r} = \nu A_{k_{\overline{\chi}}}$, $\nu \in k_{\overline{\chi}}$ et $0 < r < 3$, $\alpha = \nu^{2^{3-r}} u$. Si $\langle\mathbb{S}\rangle = G(k(\omega)/k)$ $\alpha^{\mathbb{S}-5} = b_{\mathbb{S}}^{-8}$, $b_{\mathbb{S}} \in k_{\overline{\chi}}^*$ (Proposition 1.2), comme $\mathbb{S}(\sqrt{2}) = -\sqrt{2}$ et $u = (1+\sqrt{2})^m$ alors α est un carré dans $k_{\overline{\chi}}$.

4. CONSTRUCTION DES ECNR DE DEGRE q^n DE k

On se propose d'appliquer les étapes suivantes :

1ère étape : Choix de k.

Pour que N existe, H(k) doit posséder au moins une composante cyclique d'ordre q^n, on consultera [5]. Comme N est diédrale sur $\mathbb{Q}$ (Lemme3.2), on s'intéresse à:

2ème étape : Détermination des extensions diédrales.
On adjoint à N , ω . A N correspond χ ; $\chi(\mathcal{S}) = -1$, où $<\mathcal{S}> = G(k(\omega)/\mathbb{Q}(\omega))$. On a $k_{\bar{\chi}}$ ou $L_{\bar{\chi}}$ suivant que N est LD de $k(\omega)$ sur k ou pas, (Proposition 3.1). Comme $N(\omega)/k(\omega)$ est non ramifiée, on cherchera N parmi les extensions diédrales telles que $N(\omega)$ soit non ramifiée sur $k(\omega)$.

3 ème étape : Détermination de α tel que $N(\omega) = k(\omega)(\sqrt[q^n]{\alpha})$.

On choisit α dans k_{χ} (Théorème 1.3). Comme $N(\omega)/k(\omega)$ est non ramifiée, il faut déterminer tous les idéaux $\mathbb{I}$ de $k(\omega)$ d'ordre q^n tels que $\mathbb{I}^{q^n} = \alpha A_{k(\omega)}$. Si $q \neq 2$, Proposition 3.4 et Corollaire 3.5 permettent sous condition de choisir $\mathbb{I}$ dans $k_{\bar{\chi}}$. Pour $q = 2$, on a un résultat analogue pour les extensions de degré 8 (Proposition 3.6). On est amené à déterminer suivant les cas : $H_q(k_{\bar{\chi}})$ ou $H_q(k(\omega))$, à l'aide de l'algorithme de Gras [2]; une fois l'arithmétique de $k_{\bar{\chi}}$ (base d'entiers, groupe des unités) est connue; On précisera ensuite les idéaux d'ordre q^n et on récupérera α, qui doit vérifier les conditions de décomposition (Théoréme 1.3), ainsi que la non ramification de $N(\omega)/k(\omega)$ en q. Si pour toutes les unités u de $k_{\bar{\chi}}$ αu ne donne pas l'extension non ramifiée, on ira vers une autre classe d'ordre q^n.

4 ème étape : Détermination de l'extension N.
Les sous corps de $N(\omega)$ cycliques de degré q^n sur k et diédrales sur $\mathbb{Q}$ sont obtenus de la Proposition 1.4. Une fois N déterminée numériquement, on doit vérifier si elle est non ramifiée, si cela est impossible il faut rechercher un autre α.

On explicite la construction des ECNR de degré 8 d'un corps quadratique à l'aide d'un exemple. On consulte la table [5] et le premier corps qui répond à la 1ère étape est $\mathbb{Q}(\sqrt{226})$. La Proposition 3.1 montre que l'extension cherchée est LD de $k(\omega)$ sur $k(\sqrt{2})$, ω étant une Rp(8). On se ramène à la détermination d'une ECNR de degré 4 de $k(\sqrt{2})$ cyclique sur k.
Pour que la méthode de construction proposée soit plus explicite, on donnera un exemple d'extension LD de $k(\omega)$ sur k, de degré 8 sur k. Le premier corps qui répond est $\mathbb{Q}(\sqrt{646})$

5. DETERMINATION DU CORPS DE HILBERT DE $\mathbb{Q}(\sqrt{226})$

On pose : $k = \mathbb{Q}(\sqrt{226})$, $L = k(\sqrt{2})$, $L_0 = \mathbb{Q}(\sqrt{2})$, $\vec{k} = \mathbb{Q}(\sqrt{-113})$, $\omega^8 = 1$, $\omega^{\mathbb{S}_{-1}} = \omega^7$, $\omega^{\mathbb{S}} = \omega^5$, $K = k(\omega) = \mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{113})$, $\mathfrak{X}_0 = <\chi>$ avec $\chi(\mathbb{S}_{-1}) = 1$ et $\chi(\mathcal{S}) = -1$, $\ker\overline{\chi} = <\mathcal{S}\mathbb{S}_{-1}>$ et $L_{\overline{\chi}} = \mathbb{Q}(\sqrt{2}, \sqrt{-113})$.
On précise maintenant les différents groupes de Galois dans le tableau suivant :

G(K/k)	G(K/Q)	G(K/L)	G(K/L_0)	G(L/L_0)	G(L/k)	G($L_{\overline{\chi}}$/$\vec{k}$)
$<\mathbb{S}, \mathbb{S}_{-1}>$	$<\mathcal{S}, \mathbb{S}, \mathbb{S}_{-1}>$	$<\mathbb{S}_{-1}>$	$<\mathcal{S}, \mathbb{S}_{-1}>$	$<\mathcal{S}>$	$<\mathbb{S}>$	$<\mathbb{S}\mathbb{S}_{-1}>$

Les unités de $L_{\overline{\chi}}$ sont celles de $\mathbb{Q}(\sqrt{2})$, $e_{L_{\overline{\chi}}/\mathbb{Q}}(2) = 4$, $e_{L_{\overline{\chi}}/\mathbb{Q}}(113) = 2$ et $k(\omega)/L_{\overline{\chi}}$ est non ramifiée.

Le 2- groupe des classes de $L_{\overline{\chi}}$

On applique ([2], p.42) à $L_{\overline{\chi}}$. $|H(\vec{k})| = 8$ d'après [5], $3A_{\vec{k}} = P_3^{1-\mathbb{S}_{-1}}$ avec P_3 et $P_3^{\mathbb{S}_{-1}}$ définis par $\sqrt{-113} \equiv 1 \bmod P_3$ et $\sqrt{-113} \equiv -1 \bmod P_3^{\mathbb{S}_{-1}}$. On a $P_3^8 = (32 + 7\sqrt{-113})A_{\vec{k}}$, la classe de P_3 dans $\vec{k}$ engendre $H(\vec{k})$. D'après ([2], p.26), $|H_1| = |H(\vec{k})| = 8$.

Détermination de J_1. Le seul premier qui se ramifie dans $L_{\overline{\chi}}/\vec{k}$ est P_2 de $\vec{k}$ divisant 2, $P_2 = \mathfrak{P}_2^2$, $2A_{L_{\overline{\chi}}} = \mathfrak{P}_2^4$ et $\sqrt{2}\,A_{L_{\overline{\chi}}} = \mathfrak{P}_2^2$. P_3 engendre $H(\vec{k})$ et est inerte dans $L_{\overline{\chi}}$, donc $P_3 \in J_1$. On résoud $N_{L_{\overline{\chi}}/\vec{k}}(a) = -1$, on obtient : $a = (11 - 2\sqrt{2})(\sqrt{-113})^{-1}$, comme les premiers de $L_{\overline{\chi}}$ divisant $P_{113} = \sqrt{-113}\,A_{\vec{k}}$ sont définis par $\sqrt{2} \equiv 51 \bmod \mathfrak{P}_{113}$ et $\sqrt{2} \equiv -51 \bmod \mathfrak{P}_{113}^{\mathbb{S}\mathbb{S}_{-1}}$, on obtient : $aA_{L_{\overline{\chi}}} = \mathfrak{P}_{113}^{1-\mathbb{S}\mathbb{S}_{-1}}$, donc $J_1 = <\mathfrak{P}_2, \mathfrak{P}_3, \mathfrak{P}_{113}>$ avec $\mathfrak{P}_3 = P_3 A_{L_{\overline{\chi}}}$. Comme $\mathfrak{P}_2^2 =$

$\sqrt{2}A_{L_{\overline{\chi}}}$ et $\mathfrak{P}_3^4 = (-7 + \sqrt{-113})A_{L_{\overline{\chi}}}$ et que $\mathfrak{P}_2$ et $\mathfrak{P}_3^2$ ne sont pas équivalents, on a $H_1 = <\mathfrak{P}_3, \mathfrak{P}_2>$ d'où $|H_2| = 16$.

Détermination de J_2 . J_2 est engendré par J_1 et les idéaux $\mathbb{I}$ tels que $N(\mathbb{I}) = N(U) = aA_{\vec{k}}$ où $U \in J_1$ et a égal respectivement à 2, $32 + 7\sqrt{-113}$ et $\sqrt{-113}$. Il suffit de résoudre $N(\mathbb{I}) = N(\mathfrak{P}_{113}) = N(\pi) = \sqrt{-113}\, A_{\vec{k}}$, on obtient comme solution $\pi = 5(11 + \sqrt{-113} + 2\sqrt{2})(18 + \sqrt{-226})^{-1}$.

On précise les premiers divisant 2, 5, 11 et 113. Si p est un nombre premier, on désigne par P un premier de $\vec{k}$ divisant p, P' un premier de $\mathbb{Q}(\sqrt{2})$ divisant p, $\mathfrak{P}$ un premier de $L_{\overline{\chi}}$ divisant P et P', et $\mathbb{P}$ un premier de $\mathbb{Q}(\sqrt{-226})$ divisant p.

p	P	P'	$\mathfrak{P}$	$\mathbb{P}$
2	$2A_{\vec{k}} = P^2$	$\sqrt{2}\, A_{\mathbb{Q}(\sqrt{2})}$	$\mathfrak{P}^2 = \sqrt{2}\, A_{L_{\overline{\chi}}}$	$2A_{\mathbb{Q}(\sqrt{-226})} = \mathbb{P}_2^2$
5	$P = 5A_{\vec{k}}$	$P' = 5A_{\mathbb{Q}(\sqrt{2})}$	$\sqrt{-226} \equiv 2\ \mathfrak{P}_5$ $\sqrt{-226} \equiv -2\ \mathfrak{P}_5^{\mathfrak{S}\mathfrak{S}_{-1}}$	$\sqrt{-226} \equiv 2\ \mathbb{P}_5$ $\sqrt{-226} \equiv -2\ \mathbb{P}_5^{\mathfrak{S}\mathfrak{S}_{-1}}$
11	$P = 11A_{\vec{k}}$	$P' = 11A_{\mathbb{Q}(\sqrt{2})}$	$\sqrt{-226} \equiv 7\ \mathfrak{P}_{11}$ $\sqrt{-226} \equiv -7\ \mathfrak{P}_{11}^{\mathfrak{S}\mathfrak{S}_{-1}}$	$\sqrt{-226} \equiv 7\ \mathbb{P}_{11}$ $\sqrt{-226} \equiv -7\ \mathbb{P}_{11}^{\mathfrak{S}\mathfrak{S}_{-1}}$
113	$P = \sqrt{-113}\, A_{\vec{k}}$	$\sqrt{2} \equiv 5\ P'_{113}$ $\sqrt{2} \equiv -5\ P'^{\mathfrak{S}_{-1}}_{113}$	$\sqrt{2} \equiv 51\ \mathfrak{P}_{113}$ $\sqrt{2} \equiv -51\ \mathfrak{P}_{113}^{\mathfrak{S}\mathfrak{S}_{-1}}$	$113A_{\mathbb{Q}(\sqrt{-226})} = \mathbb{P}_{113}^2$

On a alors $\pi A_{L_{\bar{\chi}}} = (\mathfrak{P}_5^{-1}\mathfrak{P}_{11})^{1-\mathfrak{S}\mathfrak{S}_{-1}}\mathfrak{P}_{113}$, $\mathbb{I} = \mathfrak{P}_5^{-1}\mathfrak{P}_{11}$,

$J_2 = <\mathfrak{P}_2, \mathfrak{P}_3, \mathfrak{P}_{113}, \mathfrak{P}_5^{-1}\mathfrak{P}_{11}>$ et $H_2 = <\overline{\mathfrak{P}}_3, \overline{\mathfrak{P}_5^{-1}\mathfrak{P}_{11}}>$. $|H_3 / H_2| = 2$, d'où

$|H_3| = 32$.

Détermination de J_3. J_3 est engendré par J_2 et les idéaux $\mathbb{I}$ tels que $N(\mathbb{I})=N(U) = \frac{11}{5}A_k = N(c)$, on trouve $c = \frac{c_1}{c_2}$ avec $c_1 = (18+\sqrt{-226})(5\sqrt{2}+10)^{-1}$ et

$c_2 = \left[(2+\sqrt{-113}) + (\sqrt{2}+\sqrt{-226})\right](-5-\sqrt{2})^{-1}$.

Les idéaux divisant 23 sont définis par : $\sqrt{-226} \equiv 2\ P_{23}$ et $\sqrt{-226} \equiv -2\ P_{23}^{\mathfrak{S}\mathfrak{S}_{-1}}$.

A l'aide du Théorème de Kummer, une base d'entiers de $L_{\bar{\chi}}$ sur $\mathbb{Q}(\sqrt{-226})$ est $1, \frac{\sqrt{-226}+\sqrt{2}}{2}$ d'après [1]. On a $\mathfrak{P}_{23}^{\mathfrak{S}_{-1}} = <P_{23}^{\mathfrak{S}_{-1}}, 8+\frac{\sqrt{-226}+\sqrt{2}}{2}>$,

$\mathfrak{P}_{23}^{\mathfrak{S}\mathfrak{S}_{-1}} = <P_{23}^{\mathfrak{S}_{-1}}, 13+\frac{\sqrt{-226}+\sqrt{2}}{2}>$, $\mathfrak{P}_{23} = <P_{23}, 10+\frac{\sqrt{-226}+\sqrt{2}}{2}>$ et

$\mathfrak{P}_{23}^{\mathfrak{S}} = <P_{23}, 15+\frac{\sqrt{-226}+\sqrt{2}}{2}>$.

	Idéal P de $\vec{k}$ divisant 23	Idéal P' de $\mathbb{Q}(\sqrt{2})$ divisant 23	Idéal de $L_{\bar{\chi}}$ divisant P et P'
23	$\sqrt{-113} \equiv 28\ P_{23}$	$\sqrt{2} \equiv 5\ P'_{23}$	$\mathfrak{P}_{23}$
		$\sqrt{2} \equiv -5\ P'^{\mathfrak{S}\mathfrak{S}_{-1}}_{23}$	$\mathfrak{P}_{23}^{\mathfrak{S}\mathfrak{S}_{-1}}$
23	$\sqrt{-113} \equiv -28\ P_{23}^{\mathfrak{S}_{-1}}$	$\sqrt{2} \equiv 5\ P'^{\mathfrak{S}_{-1}}_{23}$	$\mathfrak{P}_{23}^{\mathfrak{S}_{-1}}$
		$\sqrt{2} \equiv -5\ P'^{\mathfrak{S}}_{23}$	$\mathfrak{P}_{23}^{\mathfrak{S}}$

On a $cA_{L_{\bar{\chi}}} = \mathfrak{P}_5^{1-2\mathfrak{S}\mathfrak{S}_{-1}} \mathfrak{P}_{11}^{\mathfrak{S}\mathfrak{S}_{-1}} \mathfrak{P}_{23}^{\mathfrak{S}-\mathfrak{S}_{-1}}$ or $N(cA_{L_{\bar{\chi}}}) = N(\mathfrak{P}_5^{-1}\mathfrak{P}_{11})$ d'où

$cA_{L_{\bar{\chi}}} = \mathfrak{P}_5^{-1}\mathfrak{P}_{11}\mathbb{I}^{1-\mathfrak{S}\mathfrak{S}_{-1}}$ avec $\mathbb{I} = \mathfrak{P}_5^2\mathfrak{P}_{11}^{-1}\mathfrak{P}_{23}^{\mathfrak{S}}$, donc on obtient

$J_3 = <\mathfrak{P}_2, \mathfrak{P}_3, \mathfrak{P}_{113}, \mathfrak{P}_5^{-1}\mathfrak{P}_{11}, \mathfrak{P}_5^2\mathfrak{P}_{11}^{-1}\mathfrak{P}_{23}>$ et $H_3 = <\overline{\mathfrak{P}}_3, \overline{\mathfrak{P}_5\mathfrak{P}_{23}^{\mathfrak{S}}}>$. On a $|H_4/H_3| = 1$ d'où $H_4 = H_3$ et $H(L_{\bar{\chi}}) = <\overline{\mathfrak{P}}_3, \overline{\mathfrak{P}_5\mathfrak{P}_{23}^{\mathfrak{S}}}>$ donc $\left|H(L_{\bar{\chi}})\right| = 32$.

Détermination de l'extension CNR de degré 8 de k.

On trouve que α est un générateur à une unité près de $(\mathfrak{P}_3^2\mathfrak{P}_5)^4$; c'est à dire

$\alpha = \frac{(-7+\sqrt{-113})^2}{2}(16\sqrt{2}+\sqrt{-113})u$ avec $u = (1+\sqrt{2})^n$. Pour $u = 1$, α convient et vérifie : $\alpha^6 = \omega' b_{\mathfrak{S}}^{5+\mathfrak{S}}$, $\alpha^{\mathfrak{S}_{-1}-3} = b_{\mathfrak{S}_{-1}}^{-4}$ et $\alpha^2 = b_{\mathfrak{S}_{-1}}^{3+\mathfrak{S}_{-1}}$

avec ω' une Rp(4) et $b_{\mathfrak{S}}$, $b_{\mathfrak{S}_{-1}}$ dans $L_{\bar{\chi}}$. On a aussi $b_{\mathfrak{S}_{-1}} = \frac{\alpha}{45}$ et $b_{\mathfrak{S}} = \frac{\alpha(-7+\sqrt{-113})}{9\omega\sqrt{2}}$. Donc $N(\omega) = L(\omega)(\sqrt[4]{\alpha})$ est décomposée sur k.

L'extension $N(\omega)/L(\omega)$ est non ramifiée car $\alpha A_{L(\omega)}$ et $2A_{L(\omega)}$ étant premiers entre eux, tout premier de $L(\omega)$ premier avec 2 est non ramifié dans $N(\omega)$ (Proposition 1.5). On a $2A_{\mathbb{Q}(\omega)} = (1-\omega)^4$ et $(1-\omega)A_{k(\omega)} = (\mathfrak{P}_2)^{1+\mathfrak{S}}$ donc $2A_{k(\omega)} = \mathfrak{P}^{4+4\mathfrak{S}}$. Le complété de $L(\omega)$ pour la valuation discrète associée à $\mathfrak{P}_2$ est égal au complété de $\mathbb{Q}(\omega)$ pour la valuation discrète associée à $(1-\omega)$. Comme $V_{\mathfrak{P}_2}(\alpha) = 0$, on résoud $\alpha \equiv y^4 \bmod (1-\omega)^{12}$, en choisissant π pour uniformisante, $(1-\pi)$ est solution et $\mathfrak{P}_2$ est non ramifié.

Soit α' une racine 4-ème de α, (Proposition 1.4) donne $H_1 = <\overline{\mathfrak{S}}_{-1}\tau^2>$, $H_2 = <\overline{\mathfrak{S}}_{-1}>$, $Tr_{H_1}(\alpha') = \alpha' - \frac{45}{\alpha'} = \beta_1$ et $Tr_{H_2}(\alpha') = \alpha' + \frac{45}{\alpha'} = \beta_2$. Les deux EC de degré 4 sont $L(\beta_1)$ et $L(\beta_2)$. On doit prendre celle qui est non ramifiée sur L. On considère le sous corps M de $N_1 = L(\beta_1)$ (resp. $N_2 = L(\beta_2)$) invariant par τ^2, $M = L(\sqrt{\alpha} + \sqrt{\overline{\alpha}}) = L(\sqrt{25-16\sqrt{2}})$. On a $(25-16\sqrt{2})A_{L_{\bar{\chi}}} = \mathfrak{P}_{113}^2$

Comme $(-16\sqrt{2} + 25) \equiv y^2 \mod (\sqrt{2})^6$ est vérifiée pour $y = 1$, M est non ramifiée sur L. On a $N_2 = L(\alpha' + \frac{45}{\alpha'}) = M(\sqrt{c})$ où $c = -\sqrt{113}\sqrt{-16\sqrt{2} + 25}\,(8\sqrt{2} - 16) + 45(-16\sqrt{2} + 25)$, comme $c \equiv 1 \mod (\sqrt{2})^4$, N_2 est non ramifiée sur k.

Le corps cherché est $N = k\left(\sqrt{\frac{\sqrt{113}\,(16\sqrt{2} - 32) + 90\sqrt{25 - 16\sqrt{2}}}{\sqrt{25 - 16\sqrt{2}}}}\right)$

ayant pour polynôme minimal sur k :

$X^8 - 360X^6 + 8644264X^4 + 1561799520X^2 + 354726128.$

6. DETERMINATION DU CORPS DE HILBERT DE $k = \mathbb{Q}(\sqrt{646})$

On a $k_\chi = \mathbb{Q}(\sqrt{2}, \sqrt{-646})$ (Paragraphe 3), d'après [6] $H(k_\chi)$ contient deux classes d'ordre 8 et $|H(k_\chi)| = 32$.

Détermination du 2- groupe des classes ambiges H_1.

On applique [2] à $k_\chi / \mathbb{Q}(\sqrt{-646})$. $|H(\mathbb{Q}(\sqrt{-646}))| = 16$ d'après [5],

$H(\mathbb{Q}(\sqrt{-646})) = <\overline{P}_5, \overline{P}_{17}>$, P_5 et P_{17} étant définis par $\sqrt{-646} \equiv 2 \mod P_5$ et $P_{17}^2 = 17A_{\mathbb{Q}(\sqrt{-646})}$. Comme 2 est inerte dans $\mathbb{Q}(\sqrt{-323})$ et $k_\chi / \mathbb{Q}(\sqrt{-646})$ est non ramifiée, $|H_1| = 8$ et H_1 est engendré par les idéaux de $\mathbb{Q}(\sqrt{-646})$ étendus à k_χ ; d'où $H_1 = <\overline{\mathfrak{P}}_5, \overline{P_{17}A_{k_\chi}}>$ où $\mathfrak{P}_5^8 = (-591 + 8\sqrt{-646})A_{k_\chi}$, $P_{17}A_{k_\chi} = \mathfrak{P}_{17}\mathfrak{P}'_{17}$ où $\sqrt{2} \equiv -6 \mod \mathfrak{P}_{17}^2$ et $\sqrt{2} \equiv 6 \mod \mathfrak{P}_{17}'^2$, $\mathfrak{P}_5$ (resp. $\mathfrak{P}_{17}$) est d'ordre 8 (resp. 2), H_1 est alors engendré par $\mathfrak{P}_5$ et par suite les seuls sous groupes d'ordre 8 de $H(k_\chi)$ sont $<\overline{\mathfrak{P}}_5>$ et $<\overline{\mathfrak{P}_5\mathfrak{P}_{17}}>$. Donc α provient d'un générateur de $\mathfrak{P}_5^8$ ou de $(\mathfrak{P}_{17}\mathfrak{P}_5)^8$.

Extensions $N(\omega) = k(\omega)(\sqrt[8]{\alpha})$ décomposées sur k.

On a $G(k(\omega)/k) = <\mathbb{S}, \mathbb{S}_{-1}>$ avec $\mathbb{S}(\omega) = \omega^5$ et $\mathbb{S}_{-1}(\omega) = \omega^7$.

α doit vérifier : $\alpha^{\mathbb{S}-a_{\mathbb{S}}} = b_{\mathbb{S}}^{-8}$, $\alpha^{\mathbb{S}_{-1}-a_{\mathbb{S}_{-1}}} = b_{\mathbb{S}_{-1}}^{8}$ et $b_{\mathbb{S}_{-1}}^{\mathbb{S}-a_{\mathbb{S}}} = b_{\mathbb{S}}^{\mathbb{S}_{-1}-a_{\mathbb{S}_{-1}}}$.

On trouve que α doit provenir de $(\mathfrak{P}_{17}\mathfrak{P}_5)^8$, en effet

$\alpha = (5 - 2\sqrt{2})^4(-591 + 8\sqrt{-646})$, $b_{\mathbb{S}_{-1}}^{-1} = 5(5 - 2\sqrt{2})\alpha^{-1}$ et

$b_{\mathbb{S}}^{-1} = (5 - 2\sqrt{2})(17 + 4\sqrt{-646})\alpha^{-1}$.

Comme la congruence $\alpha \equiv y^8 \bmod (1 - \omega)^{16}$ est vérifiée pour

$y = \sqrt{-1}(3 + 3\sqrt{2})(1 + \sqrt{-646})$, $N(\omega)$ est non ramifiée sur $k(\omega)$.

L'extension cyclique non ramifiée de degré 8 de k.

Soit $\mathbb{S}$ (resp. $\mathbb{S}_{-1}$) le relèvement de $\mathbb{S}$ (resp. $\mathbb{S}_{-1}$) défini par

$\mathbb{S}(\alpha') = \dfrac{(5 - 2\sqrt{2})(17 + 4\sqrt{-646})}{(\alpha')^3}$, $\mathbb{S}_{-1}(\alpha') = \dfrac{5(5 - 2\sqrt{2})}{\alpha'}$ où α' est une racine 8-ème de α. Chaque extension $N_{i,j}$ est définie par un sous groupe $H_{i,j} = \langle \mathbb{S}\tau^{4i}, \mathbb{S}_{-1}\tau^{4j} \rangle$ avec $\langle \tau \rangle = G(k(\omega)(\alpha')/k(\omega))$ où $0 < i < 3$ et $0 < j < 3$.

On pose $\beta = Tr_{H_{2,2}}(\alpha')$ on a $\beta^2 = (5 + \sqrt{17})(5 + \sqrt{\dfrac{25 + \sqrt{17}}{2}})$ et

$\beta^2 + \tau^2(\beta^2) = 20(5 + \sqrt{17})$, on pose alors $L = k(\sqrt{17})$. Comme $17 \equiv 1 \bmod 16$, L/k est non ramifiée, on a aussi $2A_k = P_2^2$ et $\mathfrak{P}_2$ et $\mathfrak{P}'_2$ qui divisent P_2 dans L sont définis par $\sqrt{17} \equiv 1 \bmod \mathfrak{P}_2^2$ et $\sqrt{17} \equiv -1 \bmod \mathfrak{P}_2'^2$. On pose $M = k(\beta^2) = L(\sqrt{\dfrac{25 + \sqrt{17}}{2}})$. Soit $\mathfrak{P}'_{19}$ le premier de L divisant 19 défini par $\sqrt{17} \equiv -6 \bmod \mathfrak{P}_{19}'^2$, alors $\dfrac{(25 + \sqrt{17})}{2}A_L = \mathfrak{P}_2'^6\mathfrak{P}_{19}'^6$. Comme M/L est galoisienne, il suffit d'étudier la ramification pour $\mathfrak{P}_2$ par exemple. On a $\dfrac{25 + \sqrt{17}}{2} \equiv 1 \bmod \mathfrak{P}_2^6$, donc M/L est non ramifiée et $\mathfrak{P}_2$ se décompose complètement. Les idéaux $\mathbb{P}_2$ et $\mathbb{P}'_2$ de M qui le relèvent son définis par $\dfrac{25 + \sqrt{17}}{2} \equiv 1 \bmod \mathbb{P}_2^6$ et $\dfrac{25 + \sqrt{17}}{2} \equiv -1$

mod $\mathbb{P}_2^{'6}$. On vérifie que $\frac{(5+\sqrt{17})}{2}(5+\sqrt{\frac{25+\sqrt{17}}{2}})\frac{1}{2}$ est premier avec $\mathbb{P}_2$ et que $\frac{5+\sqrt{17}}{2}$ et $(5+\sqrt{\frac{25+\sqrt{17}}{2}})\frac{1}{2}$ sont congrus à 3 modulo $\mathbb{P}_2^4$.

On en déduit que $k(\beta)$ est non ramifiée sur M. Comme les sous corps de $k(\beta)$ sont

$$k \longrightarrow L = k(\beta^2 + \tau^2(\beta^2)) \longrightarrow M = k(\beta^2) \longrightarrow k(\beta)$$

on en déduit que $k(\beta)$ est non ramifiée sur k pour toutes les places. Le polynôme minimal de β sur k est : $X^8 - 100X^6 + 1660X^4 - 8640X^2 + 9728$
et que l'extension cherchée est :

$$N = k(\sqrt{(5+\sqrt{17})(5+\sqrt{\frac{25+\sqrt{17}}{2}})}) .$$

REMERCIEMENTS. Je tiens à remercier A.Kerkour pour les conseils qu'il m'a prodigués, P.Ribenboim et P.Roquette qui m'ont encouragé à soumettre mon travail à manuscripta mathematica et le Referee pour ses remarques .

BIBLIOGRAPHIE

[1] BIRD, R., PARRY, C. : Integral bases for bicyclic biquadratic fields over quadratic subfields. Pac. J. 66, 1, 29-36 (1976)

[2] GRAS, G. : Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l. Ann. Inst. Fourier, Grenoble. 23, 3, 1-48 (1973)

[3] HASSE, H. : Uber den Klassenkörper zum quadratischen Zahlkörper mit der Diskriminante - 47. Acta Arith. XVI, 419-434 (1964)

[4] KERKOUR, A. : Sur les extensions cycliques de degré l^n, l premier, galoisiennes sur certains sous corps du corps de base.Doctorat d'état. Université de Franche-Comté, Besançon. 131 (1978)

[5] ORIAT, B.: Table des groupes des classes des corps quadratiques réels $\mathbb{Q}(\sqrt{d})$ et imaginaires $\mathbb{Q}(\sqrt{-d})$, $d < 10^4$. Faculté des Sciences de Besançon. (1974-1975)

[6] ORIAT, B. : 2,4,8 rang du groupe des classes d'idéaux de $\mathbb{Q}(\sqrt{2},\sqrt{d})$ $|d| < 1000$. Séminaire de théorie des nombres. Besançon. 1-22 (1976)

Aboubakr Lbekkouri
Département de Mathématiques
Faculté des Sciences de Rabat
Avenue Ibn Battouta
Rabat, MAROKKO

(Reçu le 18 mars 1988;
la version révisée le 25 juillet 1989)