THÉORIE DES NOMBRES
BESANÇON

Années 1992/93-1993/94

Base normale dans un corps de classes de Hilbert

J. COUGNARD

BASE NORMALE DANS UN CORPS DE CLASSES DE HILBERT

par Jean COUGNARD

§1 Introduction - Exposé des motifs

Faisons l'hypothèse que l'on s'intéresse à la structure galoisienne des anneaux d'entiers. On sait que le cadre où l'on a les résultats les plus complets est le celui où N/K est une extension galoisienne modérément ramifiée de groupe de galois G. On peut alors affirmer que $\mathcal{O}_N$ est $\mathbb{Z}[G]$-projectif et le théorème de Taylor lie sa classe dans un groupe de Grothendieck aux valeurs des constantes de l'équation fonctionnelle des fonctions L d'Artin des caractères symplectiques de G. On renvoie à [F2] pour un exposé détaillé des résultats et des méthodes.

Dans le cas particulier où G est un groupe quaternionien H_{2^n} d'ordre 2^n avec $n > 3$, A. Fröhlich avait démontré auparavant [F1] que $\mathcal{O}_N$ est stablement libre, c'est à dire que :

$$\mathcal{O}_N \oplus \mathbb{Z}[G] \cong \mathbb{Z}[G] \oplus \mathbb{Z}[G]$$

Lorsque $n = 4$ ou $[K : \mathbb{Q}] \geq 2$ on peut simplifier :

$$\mathcal{O}_N \cong \mathbb{Z}[G]$$

ce qui assure l'existence d'une base normale de l'anneau des entier; il n'en va pas de même lorsque $K = \mathbb{Q}$ et $n > 4$ car l'on sait depuis Swan [Sw] qu'il existe des modules stablement libres non libres sur $\mathbb{Z}[H_{32}]$.

L'ordre des groupes de Grothendieck qui classent, à isomorphisme stable près, les modules projectifs sur $\mathbb{Z}[H_{2^n}]$ tend vers l'infini avec n et pourtant les anneaux d'entiers y occupent toujours une place privilégiée. On peut donc se poser la question de savoir si cette singularité va au-delà et s'il existe ou non des bases normales.

Il nous faut, pour cela, disposer d'extensions modérément ramifiées de $\mathbb{Q}$ à groupe de Galois quaternionien d'ordre 32. Une telle extension contient un corps quadratique réel $\mathbb{Q}(\sqrt{d})$ avec $d \equiv 1 \bmod 4$; ce corps se plonge d'une infinité de façon dans une extension diédrale de $\mathbb{Q}$ de degré 32, modérément ramifiée et d'une infinité de manière dans une extension cyclique de $\mathbb{Q}$ de degré 4, modérément ramifiée. On peut alors choisir une des extensions diédrales, la composer avec une des extensions cycliques de degré 4, le compositum contient une extension quaternionienne de degré 32. Réciproquement la composée de deux extensions, l'une quaternionienne de degré 32, l'autre cyclique de degré 4, contenant un même sous corps quadratique réel contient une extension cyclique de degré du même corps quadratique réel, diédrale su $\mathbb{Q}$. Les changement de corps diédraux et cycliques permettent de varier la ramification [DM].

Le but de ce travail est de réaliser la première étape en construisant une extension diédrale de $\mathbb{Q}$ de degré 32, modérément ramifiée et une base normale de son anneau des entiers. Il faut partir d'un corps quadratique réel $k = \mathbb{Q}(\sqrt{d})$ et chercher les groupes de classes généralisés possédant un quotient cyclique d'ordre 16, invariant par la conjugaison du corps quadratique. Mais pour un premier essai, il a paru plus facile de regarder dans les tables de groupes de classes de B. Oriat [Or] les $\mathbb{Q}(\sqrt{p_1 p_2})$ avec p_1 et $p_2 \equiv 1 \bmod 4$ ce qui assure que le 2-groupe des classes est cyclique. Le premier exemple est $\mathbb{Q}(\sqrt{5 \times 461})$ dont les nombres de classes au sens large et restreint sont égaux à 16. On construit le corps de classes de Hilbert de ce corps quadratique réel et une base normale de son anneau des entiers en utilisant la même technique que dans [C].

Ce travail a nécessité de nombreux calculs qu'il m'aurait été impossible de réaliser sans l'aide de PARI [P]. Une partie des programmes est donnée en annexe pour permettre la vérification des calculs et illustrer l'utilisation de PARI-GP. J'en profite pour remercier l'équipe qui le met au point.

§2 Remarques Préliminaires.

La première étape consiste bien sûr à construire le corps des genres de $\mathbb{Q}(\sqrt{2305})$ qui est le compositum de $\mathbb{Q}(\sqrt{5})$ et de $\mathbb{Q}(\sqrt{461})$ dont une base normale est engendrée par les conjugués de $\dfrac{1+\sqrt{5}}{2}.\dfrac{1+\sqrt{461}}{2}$.

On pose pour la suite $\omega = \dfrac{1+\sqrt{5}}{2}$ et $\omega_1 = 1 - \omega$. Le corps de classes de Hilbert de $K_0 = \mathbb{Q}(\sqrt{2305})$ est cyclique de degré 2^4 sur K_0.

On a donc la tour, abélienne non ramifiée maximale, de 2-extensions :

$$K_0 = \mathbb{Q}(\sqrt{2305}) \subset K_1 = \mathbb{Q}(\sqrt{5}, \sqrt{461}) \subset K_2 \subset K_3 \subset K_4$$

où K_i est diédrale de degré 2^{1+i} sur $\mathbf{Q}$. On remarque immédiatement que 2 est inerte dans $\mathbf{Q}(\sqrt{5})$ et décomposé dans $\mathbf{Q}(\sqrt{2305})$. Il en résulte que chacun des idéaux premiers au-dessus de 2 dans $\mathbf{Q}(\sqrt{2305})$ est inerte dans K_4/K_0 et par conséquent, la loi de réciprocité d'Artin nous dit que la classe de cet idéal engendre le groupe des classes de $\mathbf{Q}(\sqrt{2305})$.

Pour des raisons analogues, les idéaux premiers au-dessus de 461 et 5 dans K_0 sont d'ordre égal à 2 (les classes ambiges sont représentées par des idéaux ambiges [G]); il sont donc décomposés dans K_3/K_0.

Soit k un corps de nombres dont le 2-groupe des classes est cyclique et k_1/k l'extension quadratique non-ramifée de k. Si le 2-groupe des classes de k_1 n'est pas cyclique, ce corps possède deux extensions quadratiques k_2, k_2' non ramifiées distinctes. Si ces deux extensions sont galoisiennes (donc abéliennes) sur k, leur compositum vérifie encore cette propriété et l'on a construit une 2-extension abélienne, non cyclique, non ramifiée de k, ce qui est contraire à notre hypothèse. Si l'un des corps k_2 par exemple, n'est pas abélien sur k, sa clôture galoisienne sur k est diédrale de degré 8, non ramifiée et contient donc une extension biquadratique non ramifiée ce qui est toujours contraire à notre hypothèse de départ.

<u>Corollaire</u> : *Si le 2-groupe des classes d'un corps k est cyclique de degré 2^n $(n \geq 1)$ et $k = k_0 \subset k_1 \subset \ldots \subset k_n$ la tour d'extensions quadratiques non-ramifiées de k; le 2-nombre de classes de k_i est égal à 2^{n-i}.*

<u>*Démonstration*</u> : Le 2-groupe des classes de k_1 est cyclique d'après le paragraphe précédent l'énoncé. Il en est donc de même pour chacun des k_i et son 2-nombre des classes est supérieur ou égal à 2^{n-i}. S'il était strictement supérieur, le 2-nombre des classes de k_n serait au-moins égal à 2. Il existerait donc une unique extension quadratique non-ramifiée L/k_n, galoisienne sur k, forcément abélienne, ce qui est impossible.

Dès que l'on a construit un corps K_i, le corps K_{i+1} est l'unique extension quadratique non-ramifiée de K_i.

§3 Construction de K_2; Base normale; Principe de construction des K_i.

L'extension $K_2/\mathbf{Q}$ est diédrale de degré 8 et contient K_1 donc $L_1 = \mathbf{Q}(\omega)$. L'idéal (461) se décompose dans L_1 en deux idéaux de générateurs respectif $\omega + 21$, $-\omega + 22$ (que l'on détermine grâce aux fractions continues) ramifiés dans K_1/L_1 et non ramifiés dans K_2/K_1. Ils ont donc des groupes d'inertie d'ordre 2 dans K_2/L_1, conjugués par l'action de $\mathrm{Gal}(L_1/\mathbf{Q})$. L'extension K_2/L_1 contient deux sous-corps quadratiques sur L_1 ramifiés uniquement l'un en $(\omega + 21)$, l'autre en $(-\omega + 22)$. On remarque immédiatement que $\omega + 21 = \omega^2 + 20 \equiv \omega^2 \bmod 4$ et que $\omega + 21$ est totalement positif.

L'extension $L_2 = \mathbf{Q}(\sqrt{\omega + 21})$ est donc la seule extension quadratique de L_1 ramifiée uniquement en $\omega + 21$. Sa clôture galoisienne sur $\mathbf{Q}$ est donc K_2.

La méthode de construction de la base normale de l'anneau des entiers d'un corps quadratique $\mathbf{Q}(\sqrt{d})$ avec $d \equiv 1 \bmod 4$ s'applique ici.

<u>Lemme</u> : *Si M/k est une extension quadratique $M = \mathbf{Q}(\sqrt{\delta})$ avec δ entier de k, $\delta \equiv u^2 \bmod 4$ et u une unité de k, l'anneau des entiers de M possède une base normale relative sur k engendrée par $\frac{u+\sqrt{\delta}}{2}$.*

En particulier, l'anneau des entiers de L_2 possède une base normale sur $\mathbf{Z}[\omega]$ engendrée par $a = \dfrac{\omega + \sqrt{\omega + 21}}{2}$.

Le polynôme irréductible de $a = \dfrac{\omega + \sqrt{\omega + 21}}{2}$ sur $L_1 = \mathbf{Q}(\omega)$ est $X^2 - \omega X - 5$ et sur $\mathbf{Q}$:

$$X^4 - X^3 - 11X^2 + 5X + 25$$

de discriminant $5^4 * 461$ et de racines :

$$a = \frac{\omega + \sqrt{\omega + 21}}{2}$$

$$a_p = \frac{\omega - \sqrt{\omega + 21}}{2}$$

$$a_1 = \frac{\omega_1 + \sqrt{\omega_1 + 21}}{2}$$

$$a_{1p} = \frac{\omega_1 - \sqrt{\omega_1 + 21}}{2}$$

Lemme : [C]*Soit $N/K/L$ une tour d'extensions, N/L et K/L galoisiennes dont les anneaux d'entiers $\mathcal{O}_N$ (resp. $\mathcal{O}_K$) admettent une base normale b (resp. a) relativement à $\mathrm{Gal}(N/K)$ (resp. $\mathrm{Gal}(K/L)$) la base de $\mathcal{O}_N$ étant globalement invariante par les prolongements de $\mathrm{Gal}(K/L)$, alors ab est une base de $\mathcal{O}_N$ comme $\mathcal{O}_L[\mathrm{Gal}(N/L)]$ module.*

Corollaire : [C] *Soit M/k une extension quadratique dont l'anneau des entiers possède une base normale relative, N_1, N_2 deux extensions quadratiques de M distinctes, conjuguées sur k, de discriminants premiers entre eux et dont les anneaux d'entiers possèdent une base normale sur M; la clôture galoisienne N des N_i sur k est diédrale de degré 8 et son anneau des entiers possède une base normale sur k.*

Remarque 1 : Dans l'exemple qui nous intéresse, l'élément $\omega a\sigma(a)$ engendre, avec ses conjugués une base normale sur $\mathbf{Z}$ de l'anneau des entiers de K_3, son polynôme irréductible est :

$$X^8 + X^7 - 196X^6 + 165X^5 + 8525X^4 - 4125X^3 - 122500X^2 - 15625X + 390625$$

L'élément ωaa_1 engendre une base normale des entiers de $K_2/\mathbf{Q}$, construisons la matrice $M_{K_2} = g_i(g_j(\omega aa_1))$, i indice des lignes, j indice des colonnes, en prenant $g_1 = \mathrm{id}$, $g_2 = \sigma$, $g_3 = \sigma^2$, $g_4 = \sigma^3$, $g_5 = \tau$, $g_6 = \sigma\tau$, $g_7 = \sigma^2\tau$, $g_8 = \sigma^3\tau$. A tout élément $x = \sum_{i=1}^{8} x_i g_i(\omega aa_1)$ de K_2 associons le vecteur colonne $X = (x_i)$, le produit $M_{K_2}X$ est la matrice colonne formée des conjugués $g_j(x)$. Inversement, étant donné la matrice colonne Y des conjugués $g_j(y)$ d'un élément y de K_2, $M_{K_2}^{-1}Y$ est la matrice colonne des coordonnées $y_i \in \mathbf{Q}$ de y suivant la base $g_i(\omega aa_1)$.

L'extension K_3/L_1 est diédrale de degré 8, on va la construire de la même manière à partir d'une extension L_3 quadratique sur L_2. De même K_4 est diédrale de degré 8 sur L_2, on l'obtient comme la clôture galoisienne d'un corps L_4 quadratique sur L_3.

§4 Construction de K_3; Action du Groupe de Galois.

Effectuons quelques calculs dans L_2 : l'élément $-2 + 3\omega + 2a$ a pour norme -1 sur $L_1 = \mathbf{Q}(\omega)$ tandis que $-2 + 4\omega + (1+\omega)a$ a pour norme ω sur $L_1 = \mathbf{Q}(\omega)$;

La norme sur $L_1 = \mathbf{Q}(\omega)$ de $2 + a$ est égale à $-1 + 2\omega$, générateur dans ce corps d'un idéal premier au-dessus de 5. Comme cet idéal n'est pas ramifié dans $L_2/\mathbf{Q}(\omega)$, c'est qu'il y est décomposé et que l'on a mis en évidence des générateurs de ses facteurs premiers.

L'idéal $(-\omega + 22)$ au-dessus de 461 dans L_1 est ramifié dans K_1/L_1, décomposé dans K_2/K_1 et non ramifié dans L_2/L_1; il est donc décomposé dans L_2/L_1 en un produit de deux idéaux premiers $\mathcal{L}\mathcal{L}'$ ramifiés dans K_2/L_2. On peut donc raisonner pour la construction de K_3 à partir de L_2 comme on l'a fait pour obtenir K_2 à partir de L_1. Il faut et il suffit que l'on construise l'extension quadratique L_3 de L_2, ramifiée uniquement en $\mathcal{L}$; sa clôture galoisienne sur L_1 est diédrale de degré 8, contenant K_2 et non ramifiée sur K_2.

Cherchons tout d'abord une base sur $\mathbf{Z}[\omega]$ du réseau $\mathcal{L}$. Pour cela, réduisons modulo $(-\omega + 22)$ le polynôme irréductible de a sur L_1 : $X^2 - \omega X - 5$, on trouve qu'il admet comme racines les classes de 193 et 246 or
$193 \equiv -268 \equiv -268 + 12(-\omega + 22) = -12\omega - 4 \mod (-\omega + 22)$. Ce qui nous donne comme base $(-\omega + 22)$ et $-a + 12\omega + 4$. On calcule la norme sur $\mathbf{Q}$ de ce dernier élément et l'on obtient $2305 = 5 * 461$. Comme on a mis en évidence des générateurs des ideaux premiers de L_2 au-dessus de 5, on peut construire un élément de L_2 de norme sur $\mathbf{Q}$ égale à 461 soit : $15 + 7\omega + (1 - 5\omega)a$. On vérifie que ce générateur est positif ainsi que ses conjugués. Il reste à traîter la ramification en 2. En dressant une table des carrés modulo 4, on constate que :

$$15 + 7\omega + (1 - 5\omega)a \equiv 3 + 3\omega + (1 + 3\omega) \equiv (1 + (1+\omega)a)^2 \mod 4.$$

ceci nous montre que $L_3 = L_2(\sqrt{15 + 7\omega + (1 - 5\omega)a})$ et qu'une base de l'anneau des entiers de L_3 relativement à L_2 est formée de 1 et de

$$b = \frac{-1 - (1+\omega)a + \sqrt{15 + 7\omega + (1 - 5\omega)a}}{2}.$$

On construit une base des entiers de L_3 et la matrice M_{L_3} formée des conjugués des éléments de cette base. L'élément b a pour polynôme irréductible sur L_2 :

$$X^2 + (1 + (1+\omega)a)X - 1 + 2\omega + (1 + 3\omega)a$$

sur L_1 :

$$X^4 + (3 + 2\omega)X^3 + (-7 - 5\omega)X^2 + (-36 - 58\omega)X + (-40 - 65\omega)$$

et enfin sur $\mathbf{Q}$:

$X^8+8X^7-8X^6-181X^5-316X^4+255X^3+585X^2-25$. On constate alors que la trace sur L_1 de b est $-1-(1+\omega)a$ qui a pour norme sur L_1 $-8-13\omega$, c'est à dire une unité! Le lemme 2 dit que $\mathcal{O}_{K_3}$ a une $\mathbf{Z}[\omega]$ base normale et on peut l'expliciter. Avant de le faire, on va écrire les conjugués de b, à partir de ceux de a et ω. Ce sont bien évidemment les nombres :

$b=\dfrac{-1-(1+w)a+\sqrt{15+7w+(1-5w)a}}{2}$;

$b_t=-1-(1+w)a-b$;

$b_p=\dfrac{-1-(1+w)a_p+\sqrt{15+7w+(1-5w)a_p}}{2}$;

$b_{pt}=-1-(1+w)a_p-b_p$;

$b_1=\dfrac{-1-(1+w_1)a_1+\sqrt{15+7w_1+(1-5w_1)a_1}}{2}$;

$b_{1t}=-1-(1+w_1)a_1-b_1$;

$b_{1p}=\dfrac{-1-(1+w_1)a_{1p}+\sqrt{15+7w_1+(1-5w_1)a_{1p}}}{2}$;

$b_{1pt}=-1-(1+w_1)a_{1p}-b_{1p}$;

Il faut aussi préciser l'action sur eux du groupe de galois de $K_3/\mathbf{Q}$. Ce groupe est le groupe diédral d'ordre 16. Il possède deux générateurs, l'un d'ordre 8 relevant le générateur σ de $\mathrm{Gal}(K_2/K_0)$ et conservant le même nom, l'autre d'ordre 2 relevant le générateur τ de $\mathrm{Gal}(K_2/L_2)$ choisi égal au générateur du groupe de galois de K_3/L_3. Il suffit, en fait de connaître l'actions sur $\sqrt{15+7w_1+(1-5w_1)a_1}$ des puissances de σ car celle de τ sur les conjugués de b se déduit immédiatement de la relation de $\tau\sigma^i=\sigma^{-i}\tau$ et de l'invariance de b par τ. Puisque K_3/K_0 est cyclique d'ordre 8, quadratique sur K_2,

$$\sigma(\sqrt{15+7w_1+(1-5w_1)a_1})=u\sqrt{15+7w_1+(1-5w_1)a_1}$$

avec u élément de K_2, en élevant au carré $\sigma(15+7w_1+(1-5w_1)a_1)=u^2(15+7w_1+(1-5w_1)a_1)$. Déterminons cet élément u sachant, en outre, que $461u$ est un entier.

Nous connaissons $u^2=\sigma((15+7w_1+(1-5w_1)a_1))/(15+7w_1+(1-5w_1)a_1)$ et ses conjugués. Nous pouvons déterminer une approximation au signe près des conjugués $g_i(u)$ de u. On construit les vecteurs colonnes $\tilde{U}$ pour les différents choix de signes possibles, on calcule ensuite les produits $M_{K_2}^{-1}461\tilde{U}$, il n'y a que deux choix qui vont nous donner des matrices colonnes dont les cœfficients sont proches d'entiers. On choisit :

$u=-190a1\omega a+34a_p\omega_1a_1+140a_{1p}\omega a_p+1271a\omega_1a_{1p}+190a_{1p}\omega a+112a\omega_1a_1-140a_1\omega a_p+888a_p\omega_1a_{1p}$

En utilisant des valeurs approchées des conjugués de b et de u, on conclut que $\sigma(b)=b_1$, $\sigma^2(b)=b_p$, $\sigma^3(b)=b_{1pt}$, $\sigma^4(b)=b_t$, $\sigma^5(b)=b_{1t}$, $\sigma^6(b)=b_{pt}$, $\sigma^7(b)=b_{1p}$.

§5 Rappels sur les Résolvantes. Représentations.

Une notion de résolvante généralisant celle de Lagrange a été introduite par Speiser et développée par A.Fröhlich, pour plus de détails sur les propriétés nous renvoyons à l'ouvrage de A. Fröhlich [F2] et à sa bibliographie. Soit $K/\mathbf{Q}$ une extension galoisienne de groupe de galois G, une représentation ρ de G de caractère χ et θ un élément de K, on note $<\theta,\chi>$ la quantité $\det(\sum_{g\in G}g(\theta)\rho(g^{-1}))$. Supposons $K/\mathbf{Q}$ modérément ramifiée, pour que θ engendre avec ses conjugués une base normale de $K/\mathbf{Q}$, il faut et il suffit que pour χ caractère de la représentation régulière, on ait $<\theta,\chi>^2$ égal au discriminant de $K/\mathbf{Q}$. Ce calcul peut se simplifier grace à la propriété $<\theta,\chi+\chi'>=<\theta,\chi><\theta,\chi'>$ est additive par rapport aux caractères χ et que toute représentation se décompose en somme de représentations irréductibles.

La première propriété des éléments $<\theta,\chi>$ est d'être des entiers algébriques pour les représentations non virtuelles de G. Une représentation ρ se prolonge en un homomorphisme d'algèbre à $\mathbf{Z}[G]$ et pour tout $\lambda\in\mathbf{Z}[G]$ le déterminant $\det(\rho(\lambda))$ ne dépend que du caractère χ, on le note $\det_\chi(\lambda)$ et on a la formule ([F2], p. 30) :

$$<\lambda(\theta),\chi>=<\theta,\chi>\det{}_\chi(\lambda).$$

Soit $\omega\in\Omega_{\mathbf{Q}}$ (le groupe de Galois de la clôture algébrique de $\mathbf{Q}$) cet automorphisme change le caractère χ en un caractère χ^ω via son action sur les cœfficients de la représentation ρ, il a également une restriction à $\mathrm{Gal}(K/\mathbf{Q})$, encore notée ω et on a la formule ([F2] p. 32, prop 4.4) :

$$<\theta,\chi^{\omega^{-1}}>=<\theta,\chi>\det{}_\chi(\omega).$$

Enfin, on déduit de ([F2], Th.7, p. 42) que si $K/\mathbf{Q}$ est modérément ramifiée et si θ engendre avec ses conjugués une base normale des entiers de K, l'idéal engendré, pour tout caractère χ par $<\theta,\chi><\theta,\overline{\chi}>$ dans $\mathbf{Q}(<\theta,\chi><\theta,\overline{\chi}>)$ est égal à celui engendré par le conducteur d'Artin $\mathfrak{f}(K/\mathbf{Q},\chi)$ dans ce corps.

Les représentations irréductibles de D_{2^n} pour $n \geq 3$ se décrivent aisément par la "méthode des petits groupes" de Wigner [Se1, ch 8]. Il y bien sûr 4 représentations de degré 1 correspondant à celles du groupe quotient isomorphe à V_4 et dont le conducteur d'Artin correspond au conducteur au sens de la théorie du corps de classes (ici le discriminant du corps quadratique invariant par le noyau de la représentation), puis des représentations de degré 2 qui sont induites par des représentations de degré 1 du sous groupe cyclique d'ordre 2^{n-1}; si la représentation de degré 1 est à valeurs dans les racines 2^{n-i}-èmes de l'unité ($1 \leq i \leq n-2$) la représentation induite peut être réalisée sur le sous-corps réel maximal de $\mathbf{Q}(\zeta_{2^{n-i}})$. Une façon de procéder est la suivante : σ opère sur $\mathbf{Q}(\zeta_{2^{n-i}})$ par la multiplication par $\zeta_{2^{n-i}}$ et τ opère comme l'automorphisme non-trivial de $\mathbf{Q}(\zeta_{2^{n-i}})/\mathbf{Q}(\zeta_{2^{n-i}})_+$. Matriciellement cela se traduit par :

$$\sigma \mapsto \begin{pmatrix} 0 & -1 \\ 1 & \zeta_{2^{n-i}}+\zeta_{2^{n-i}}^{-1} \end{pmatrix} \qquad \tau \mapsto \begin{pmatrix} 1 & \zeta_{2^{n-i}}+\zeta_{2^{n-i}}^{-1} \\ 0 & -1 \end{pmatrix}$$

Ce qui donne dans le cas de D_{32} :
La représentation ρ_2 de noyau $\mathrm{Gal}(K_4/K_2)$:

$$\sigma \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \tau \mapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

La représentation ρ_3 de noyau $\mathrm{Gal}(K_4/K_3)$:

$$\sigma \mapsto \begin{pmatrix} 0 & -1 \\ 1 & \sqrt{2} \end{pmatrix} \qquad \tau \mapsto \begin{pmatrix} 1 & \sqrt{2} \\ 0 & -1 \end{pmatrix}$$

et sa conjuguée par l'automorphisme de $\mathbf{Q}(\sqrt{2})/\mathbf{Q}$.
La représentation ρ_4 de noyau $\mathrm{Gal}(K_4/K_2)$:

$$\sigma \mapsto \begin{pmatrix} 0 & -1 \\ 1 & \sqrt{\frac{1+\sqrt{2}}{2}} \end{pmatrix} \qquad \tau \mapsto \begin{pmatrix} 1 & \sqrt{\frac{1+\sqrt{2}}{2}} \\ 0 & -1 \end{pmatrix}$$

et ses conjuguées par les automorphismes de $\mathbf{Q}(\sqrt{\frac{1+\sqrt{2}}{2}})/\mathbf{Q}$.

Le conducteur d'Artin $\mathfrak{f}(\chi_j)$ des caractères χ_j des représentations ρ_j ci-dessus, lorsque K_4/K_0 est non ramifiée est égal au discriminant de de $K_0/\mathbf{Q}$ ([Se2],ch VI §3).

En particulier, si θ n'engendre pas une base normale, en tenant compte des formules précédentes, on a l'égalité :

$$\prod_s (<\theta, s(\chi_j)><\theta, s(\overline{\chi_j})>) = \delta \mathfrak{f}(\chi_j)^{\Phi(2^j)/2}$$

avec $\delta \in \mathbf{Z}$, $\delta \neq \pm 1$ le produit étant pris pour $s \in \mathrm{Gal}(\mathbf{Q}(\zeta_{2^j})_+/\mathbf{Q})$.

§6 Base normale des entiers de K_3.

Choisissons un élément θ. Nous avons remarqué grâce aux calculs précédents et au lemme 2 que abb_p engendre avec ses L_1-conjugués une $\mathcal{O}_{L_1}$ base normale de $\mathcal{O}_{K_3}$, on connaît donc une base de l'anneau des entiers de $K_3/\mathbf{Q}$. Si un élément x de K_3 engendre avec ses conjugués une base normale des entiers de K_3, c'est un entier de trace ± 1. Comme la trace de abb_p sur L_1 est égale à ω^8, on est amené à tenter $\theta = \omega^{-7} abb_p$.

Parmi les représentations irréductibles de Gal $(K_3/\mathbf{Q})$, il est logique de s'intéresser en premier à celles qui sont fidèles. On sait qu'elles sont égales soit à :

$$\sigma \mapsto \begin{pmatrix} 0 & -1 \\ 1 & \sqrt{2} \end{pmatrix} \qquad \tau \mapsto \begin{pmatrix} 1 & \sqrt{2} \\ 0 & -1 \end{pmatrix}$$

soit à sa conjuguée sur $\mathbf{Q}$. Le conducteur d'Artin du caractère de cette représentation est égal à 2305. L'action des groupe de Galois de $K_3(\zeta_8)/\mathbf{Q}$ sur les résolvantes montre que $< \omega^{-7}abb_p, \chi >< \omega^{-7}abb_p, \overline{\chi} >$ appartient à $\mathbf{Q}$.

Les calculs effectués avec Pari donnent 2305 à 10^{-26} près. Par contre, si on essaye de calculer le discriminant du réseau engendré par le θ choisi et ses conjugués sur $\mathbf{Q}$, on voit apparaître un indice différent de 1. On sait, d'après les propriétés des résolvantes que $< \theta, \chi >$ avec χ caractère fidèle de degré 2 de $\mathrm{Gal}(K_3/\mathbf{Q})$ est nulle sur les éléments de K_2 et que, pour que θ engendre une base normale des entiers de K_3 sur $\mathbf{Z}$, il faut et il suffit qu'outre la propriété mise en évidence ci-dessus, sa trace sur K_2 engendre une base normale des entiers de K_2 sur $\mathbf{Z}$.

On va donc calculer la trace de θ sur K_2. Pour cela on va, comme précédemment, identifier les éléments de K_2 à la suite de leurs conjugués. On calcule donc les 8 conjugués de $\theta + \sigma^4(\theta)$. Ce sont les nombres : $\omega^{-7}a(bb_p + b_t b_{pt})$, $\omega_1^{-7}a_1(b_1 b_{1pt} + b_{1t} b_{1p})$, $\omega^{-7}a_p(b_p b_t + b_{pt} b)$, $\omega_1^{-7}a_{1p}(b_{1pt} b_{1t} + b_{1p} b_1)$, $\omega^{-7}a(bb_{pt} + b_t b_p)$, $\omega_1^{-7}a_1(b_1 b_{1p} + b_{1t} b_{1pt})$, $\omega^{-7}a_p(b_p b + b_{pt} b_t)$, $\omega_1^{-7}a_{1p}(b_{1pt} b_1 + b_{1p} b_{1t})$ puis on effectue le produit de l'inverse de la matrice M_{K_2} par le vecteur colonne dont les composantes sont les nombres ci-dessus. On obtient $[-1, 0, 0, 4, 2, -4, 0, 0]$ qui sont les coordonnées de la trace de θ suivant la base normale de l'anneau des entiers de K_2. Il en résulte que $\theta - 2\sigma^3(\omega a a_1) - \tau(\omega a a_1) + 2\sigma\tau(\omega a a_1)$ engendre avec ses conjugués sur $\mathbf{Q}$ une base normale de l'anneau des entiers de K_3 relativement à $\mathbf{Z}$.
Le polynôme irréductible de ce générateur est :
$X^{16} - X^{15} - 701X^{14} + 1051X^{13} + 186250X^{12} - 262469X^{11} - 24480961X^{10} + 25857884X^9 + 1702433571X^8 - 1027335580X^7 - 61736086525X^6 + 8421660125X^5 + 1081589475000X^4 + 212057393750X^3 - 8034404937500X^2 - 2047352421875X + 18765141015625$

Ayant ceci, on construit pour les calculs ultérieurs la matrice 16×16 des plongements dans $\mathbf{R}^{16}$ des éléments de cette base normale.

§7 Construction de K_4.

Commençons par un calcul annexe, celui de la norme de $\omega + b$, qui est égale à -5. L'idéal engendré par $\omega + b$ est donc un des idéaux premiers de L_3 au-dessus de 5. Un autre idéal premier au-dessus de 5 est donc engendré par $-1 - \omega - (1 + \omega)a - b$.

L'idéal $(15 + 7\omega + (1 - 5\omega)a)$ de $\mathbf{Q}(a)$ est ramifié dans $\mathbf{Q}(b)/\mathbf{Q}(a)$ et décomposé dans K_3/L_3. Son conjugué sur $\mathbf{Q}(\omega)$, engendré par $15 + 7\omega + (1 - 5\omega)(w - a) = 10 + 3\omega - (1 - 5\omega)a$ est donc décomposé dans L_3/L_2 et ses deux facteurs sont ramifiés dans K_3/L_3. Un raisonnement déjà utilisé montre que chacun des deux facteurs premiers de $(10 + 3\omega - (1 - 5\omega)a)$ dans L_3 est ramifié dans une des extensions quadratiques de L_3 contenues dans K_4 et différentes de K_3. On essaye de trouver des générateurs de ces idéaux premiers. Soit $\mathfrak{B}$, l'un de ces idéaux; $\omega \equiv 22 \bmod \mathfrak{B}$, comme $10 + 3\omega - (1 - 5\omega)a \in \mathfrak{B}$ on en déduit que $a \equiv 215 \bmod \mathfrak{B}$. Il s'ensuit que $\mathrm{Irr}(b, \mathbf{Q}(a), X)$ modulo $\mathfrak{B}$ est égal à $X^2 - 125X + 157$ qui a -248 et 373 pour racines, modulo 461. Si on écrit $248 = 215 + 44 - 11$, cela montre que $b + a + 2\omega - 11 \in \mathfrak{B}$ de même que $2b + 2a + 4\omega - 22 = 2b + 2a + 3\omega$ on vérifie que la norme de ce nombre sur $\mathbf{Q}$ est -2305. Le calcul suivant :

$$\frac{3\omega + 2a + 2b}{-1 - \omega - (1 + \omega)a - b} = \frac{(3\omega + 2a + 2b)(\omega + b)}{\omega(2 + a)} =$$

$$\frac{5 + 12\omega - (1 + 5\omega)a + (9 + 5\omega - (4 + \omega)a)b}{\omega}$$

montre que $x = 5 + 12\omega - (1 + 5\omega)a + (9 + 5\omega - (4 + \omega)a)b$ est un entier de L_3 de norme 461. On constate malheureusement que cet élément n'est pas totalement positif. On ne peut donc prendre sa racine carrée pour engendrer L_4. On est donc contraint de chercher des unités de L_3. On procéde de manière simpliste, puisque l'on a une base $1, \omega, a, a\omega, b, b\omega, ba, ba\omega$ de l'anneau des entiers de L_3 et les conjugués de ces éléments, on calcule les normes des entiers dont les cœfficients ont une valeur absolue inférieur ou égale à 3 et on trouve un grand nombre d'unités. Dans ce qui suit, on donne des unités par leurs coordonnées dans la base $1, \omega, a, a\omega, b, b\omega, ba, ba\omega$, on précise leurs signatures et on donne leurs polynômes irréductibles

$[1, 0, -2, -3, -1, -2, 0, 0]$ a tous ses conjugués positifs sauf ceux lui-même et son image par σ^2
$X^8 - 12X^7 - 143X^6 + 496X^5 + 1899X^4 - 8601X^3 + 40587X^2 - 4233X + 1$

$[-1, 0, 1, 1, -1, 3, 3, 1]$ a tous ses conjugués sont négatifs sauf celui par σ
$X^8 + 187X^7 + 10615X^6 + 193352X^5 + 932801X^4 - 138070X^3 - 5438751X^2 - 29809X - 1$

$[-1, 1, 0, 0, 3, -1, -1, 1]$ a tous ses conjugués sont négatifs sauf celui par σ^2
$X^8 + 35X^7 + 362X^6 + 978X^5 - 1350X^4 - 7657X^3 - 6065X^2 - 354X - 1$

$[2,3,1,1,2,-1,-1,1]$ a tous ses conjugués positifs sauf celui par σ^3

$X^8 - 13X^7 + 49X^6 - 15X^5 - 251X^4 + 454X^3 - 235X^2 + 36X - 1$

$[-2,-3,2,3,-2,-1,1,1]$ a tous ses conjugués négatifs sauf celui par σ^5

$X^8 + 73X^7 + 1155X^6 + 5573X^5 + 3461X^4 - 22820X^3 - 34901X^2 - 13136X - 1$

$[-2,-2,1,1,3,-1,0,3]$ a tous ses conjugués sont négatifs sauf celui par σ^6

$X^8 + 193X^7 + 11909X^6 + 248870X^5 + 762914X^4 + 51271X^3 - 1135X^2 - 101X - 1$

$[0,1,0,1,2,-1,-1,1]$ a tous ses conjugués négatifs sauf celui par σ^7

$X^8 + 13X^7 + 49X^6 + 15X^5 - 251X^4 - 454X^3 - 235X^2 - 36X - 1$

$[2,0,0,1,0,1,0,0]$ a tous ses conjugués positifs sauf ceux par σ^4 et σ^6

$X^8 - 13X^7 + 37X^6 + 114X^5 - 606X^4 + 191X^3 + 1767X^2 - 1617X + 1$

Ceci, prouve que les unités de $\mathcal{O}_{L_3}$ peuvent avoir toutes les signatures possibles. Le générateur x que nous avons trouvé de polynôme irréductible :

$X^8 - 145X^7 - 2080X^6 - 1215X^5 + 34028X^4 + 33120X^3 - 31230X^2 - 11585X + 461.$

est négatif ainsi que ses images par σ^3, σ^6 et σ^7. Dans les unités que nous avons trouvées, il y en a une u_1 de coordonnées $[1,2,-1,0,3,-3,-1,1]$, de polynôme irréductible :

$X^8 - X^7 - 112X^6 + 7X^5 + 2339X^4 - 3103X^3 + 1353X^2 - 196X + 1$

et une autre u_2 de coordonnées $[3,2,0,0,-2,1,-1,1]$ et de polynôme irréductible :

$X^8 - 23X^7 + 22X^6 + 1045X^5 - 1274X^4 - 550X^3 + 9298X^2 - 2549X + 1$

telles que le produit $-u_1u_2$ a la même signature que x. Le générateur $-u_1u_2x$ est totalement positif. On peut calculer son polynôme irréductible sur $\mathbf{Q}$:

$X^8 + 601X^7 + 41452X^6 + 851338X^5 + 4024120X^4 + 2981117X^3 + 675962X^2 + 33929X + 461$

et en se servant de l'inverse de la matrice des conjugués des éléments de la base de $\mathcal{O}_{L_3}$, on obtient les coordonnées de $y = -u_1u_2x$ suivant la base que nous avions choisie : $[76,-38,20,-15,-24,13,-33,21]$ soit

$$y = 76 - 38\omega + (20 - 15\omega)a + (-24 + 13\omega + (-33 + 21\omega)a)b.$$

Si on prend la racine carrée de cet élément, on obtient une extension quadratique de L_3 non ramifiée à l'infini, ramifiée en un seul idéal au dessus de 461, il reste à vérifier qu'elle n'est pas ramifiée en 2; c'est à dire que cet élément est congru à un carré modulo 4. Si on regarde les carrés des éléments modulo 2, on constate qu'un tel élément aurait des coordonnées congrues au 8-uplet $[1,0,0,1,1,1,0,1]$, or parmi toutes les unités que nous avons calculées, il y en a une u_3 de coordonnées $[3,2,0,1,-3,3,2,-1]$ et de polynôme irréductible :

$X^8 - 13X^7 + 2X^6 + 420X^5 - 1294X^4 + 1255X^3 - 272X^2 - 99X + 1.$

On a donc démontré que L_4/L_3 possède une base normale d'entiers engendrée par :

$c = \frac{3+2\omega+\omega a+(-3+3\omega+(2-\omega)a)b+\sqrt{76-38\omega+(20-15\omega)a+(-24+13\omega+(-33+21\omega)a)b}}{2}$

et que, par conséquent, il en est de même pour K_4/L_2. On est donc en mesure de construire une base de l'anneau des entiers de K_4 et on va, pour la suite, avoir besoin de l'action du groupe de Galois de $K_4/\mathbf{Q}$ sur ces éléments.

§8 Base des entiers de K_4 et action du groupe de Galois.

Les conjugués de c sont les éléments :

$c = \frac{3+2\omega+\omega a+(-3+3\omega+(2-\omega)a)b+\sqrt{76-38\omega+(20-15\omega)a+(-24+13\omega+(-33+21\omega)a)b}}{2}$

$c_1 = \frac{3+2\omega_1+\omega_1 a_1+(-3+3\omega_1+(2-\omega_1)a_1)b_1+\sqrt{76-38\omega_1+(20-15\omega_1)a_1+(-24+13*\omega_1+(-33+21\omega_1)a_1)b_1}}{2};$

$c_p = \frac{3+2\omega+\omega a_p+(-3+3\omega+(2-\omega)a_p)b_p+\sqrt{76-38\omega+(20-15\omega)a_p+(-24+13\omega+(-33+21\omega)a_p)b_p)}}{2};$

$c_{1ptu} = \frac{3+2\omega_1+\omega_1 a_{1p}+(-3+3\omega_1+(2-\omega_1)a1p)b1pt-\sqrt{76-38\omega_1+(20-15\omega_1)a1p+(-24+13\omega_1+(-33+21\omega_1)a_{1p})b_{1pt})}}{2};$

$c_{tu} = \frac{3+2\omega+\omega a+(-3+3\omega+(2-\omega)a)b_t-\sqrt{76-38\omega+(20-15\omega)a+(-24+13\omega+(-33+21\omega)a)b_t)}}{2};$

$c_{1tu} = \frac{3+2\omega_1+\omega_1 a_1+(-3+3\omega_1+(2-\omega_1)a_1)b_{1t}-\sqrt{76-38\omega_1+(20-15\omega_1)a_1+(-24+13\omega_1+(-33+21\omega_1)a_1)b_{1t})}}{2};$

$c_{pt} = \frac{3+2\omega+\omega a_p+(-3+3\omega+(2-\omega)a_p)b_{pt}+\sqrt{76-38\omega+(20-15\omega)a_p+(-24+13\omega+(-33+21\omega)a_p)b_{pt})}}{2};$

$c_{1pu} = \frac{3+2\omega_1+\omega_1 a_{1p}+(-3+3\omega_1+(2-\omega_1)a_{1p})b_{1p}-\sqrt{76-38\omega_1+(20-15\omega_1)a_{1p}+(-24+13\omega_1+(-33+21\omega_1)a_{1p})b_{1p})}}{2};$

$c_u = \frac{3+2\omega+\omega a+(-3+3\omega+(2-\omega)a)b-\sqrt{76-38\omega+(20-15\omega)a+(-24+13\omega+(-33+21\omega)a)b)}}{2};$

$c_{1u} = \frac{3+2\omega_1+\omega_1 a_1+(-3+3\omega_1+(2-\omega_1)a_1)b_1-\sqrt{76-38\omega_1+(20-15\omega_1)a_1+(-24+13\omega_1+(-33+21\omega_1)a_1)b_1)}}{2};$

$$c_{pu} = \frac{3+2\omega+\omega a_p+(-3+3\omega+(2-\omega)a_p)b_p-\sqrt{76-38\omega+(20-15\omega)a_p+(-24+13\omega+(-33+21\omega)a_p)b_p)}}{2};$$
$$c_{1pt} = \frac{3+2\omega_1+\omega_1 a_{1p}+(-3+3\omega_1+(2-\omega_1)a_{1p})b_{1pt}+\sqrt{76-38\omega_1+(20-15\omega_1)a_{1p}+(-24+13\omega_1+(-33+21\omega 1)a_{1p})b1pt)}}{2};$$
$$c_t = \frac{3+2\omega+\omega a+(-3+3\omega+(2-\omega)a)b_t+\sqrt{76-38\omega+(20-15\omega)a+(-24+13\omega+(-33+21\omega)a)b_t)}}{2};$$
$$c_{1t} = \frac{3+2\omega_1+\omega_1 a_1+(-3+3\omega_1+(2-\omega_1)a_1)b_{1t}+\sqrt{76-38\omega_1+(20-15\omega_1)a_1+(-24+13\omega_1+(-33+21\omega_1)a_1)b_{1t})}}{2};$$
$$c_{ptu} = \frac{3+2\omega+\omega a_p+(-3+3\omega+(2-\omega)a_p)b_{pt}-\sqrt{76-38\omega+(20-15\omega)a_p+(-24+13\omega+(-33+21\omega)a_p)b_{pt})}}{2};$$
$$c_{1p} = \frac{3+2\omega_1+\omega_1 a_{1p}+(-3+3\omega_1+(2-\omega_1)a_{1p})b_{1p}+\sqrt{76-38\omega_1+(20-15\omega_1)a_{1p}+(-24+13\omega_1+(-33+21\omega_1)a_{1p})b_{1p})}}{2};$$

Pour connaître l'action de σ sur K_4, il suffit de la connaître sur les conjugués de $d = \sqrt{76 - 38\omega + (20 - 15\omega)a + (-24 + 13\omega + (-33 + 21\omega)a)b}$.

On va procéder comme pour le prolongement de K_2 à K_3 de σ : $461\sigma(d)/d$ est un élément entier de K_2 dont on connaît les conjugués du carré. Les conjugués de $461\sigma(d)/d$ sont donc connus au signe près. Il faut donc trouver la combinaison telle que le produit de l'inverse de M_{K_3} par ce vecteur colonne soit un vecteur à coordonnées entières. Le nombre de signes à étudier peut être réduit par les remarques suivantes : on peut imposer un des signes, ensuite $\tau\sigma^i(\sigma(d)/d) = \sigma^{-i-1}(d)/\sigma^{-i}(d)$ est l'inverse de $\sigma^{16-i}(d)/\sigma^{16-i-1}(d)$. Il reste 2^7 cas à étudier. Celui qui convient est indiqué en annexe à la suite de la construction de la matrice M_{K_3}. On remarque que la précision demandée au début des calculs a du être augmentée, le logiciel signalant la perte de validité des résultats avec 28 décimales. Les coordonnées de $461\sigma(d)/d$ obtenues sont, suivant la base normale : -42784, 27895, 18491, -45064, 56582, -24919, -10874, 51800, 11436, 39478, -48595, 42437, 5192, -33767, 54808, -38959. Ceci acquis, on a $\sigma(c) = c_1$, $\sigma^2(c) = c_p$, $\sigma^3(c) = c_{1ptu}$, $\sigma^4(c) = c_{tu}$, $\sigma^5(c) = c_{1tu}$, $\sigma^6(c) = c_{pt}$, $\sigma^7(c) = c_{1pu}$, $\sigma^8(c) = c_u$, $\sigma^9(c) = c_{1u}$, $\sigma^{10}(c) = c_{pu}$, $\sigma^{11}(c) = c_{1pt}$, $\sigma^{12}(c) = c_t$, $\sigma^{13}(c) = c_{1t}$, $\sigma^{14}(c) = c_{ptu}$, $\sigma^{15}(c) = c_{1p}$. On construit maintenant la $\mathcal{O}_{L_2}$-base normale de $\mathcal{O}_{K_4}$: $c\sigma^4(c)b$, $\sigma^4(c)\sigma^8(c)b_t$, $\sigma^8(c)\sigma^{12}(c)b$, $\sigma^{12}(c)cb_t$, $c\sigma^{12}(c)b$, $\sigma^4(c)cb_t$, $\sigma^8(c)\sigma^4(c)b$, $\sigma^{12}(c)\sigma^8(c)b_t$ puis la base sur $\mathbf{Z}$ de $\mathcal{O}_{K_4}$ obtenue en multipliant successivement les éléments de cette base par $a\omega$, $a_p\omega$, $a\omega_1$, $a_p\omega_1$ on en déduit la matrice M_{K_4} des conjugués pour pouvoir effectuer les calculs dans le corps K_4.

§9 Base Normale des entiers de K_4.

On connaît une base des entiers de K_4 ainsi que l'action du groupe de Galois sur ses éléments et une base normale de $\mathcal{O}_{K_3}$. Le groupe quotient $\mathcal{O}_{K_4}/\mathcal{O}_{K_3}$ est un module sur $\mathbf{Z}[D_{32}]/(1+\sigma^8)$ qui est un ordre de l'algèbre des matrices 2×2 sur l'anneau des entiers de $\mathbf{Q}(\zeta_{16})_+$, l'identification étant obtenue au moyen de la representation ρ_3 décrite plus haut : Il n'est pas aisé, à première vue de calculer dans ce module quotient. C'est maintenant que l'on re-utiliser la démarche qui avait été celle J. Martinet dans [M]. Il y a un autre $\mathbf{Z}[D_{32}]/(1+\sigma^8)$-module qui se met facilement en évidence : c'est le noyau de la trace dans l'extension K_4/K_3. Une base sur $\mathbf{Z}$ de ce module est facile à écrire puisque K_4/K_3 est modérément ramifiée $\mathrm{Ker}(\mathrm{Tr}_{K_4/K_3}(\mathcal{O}_{K_4})) = (1-\sigma^8)\mathcal{O}_{K_4}$. La construction de la base des entiers de K_4 que nous avons donnée est particulièrement bien adaptée à cette situation puisqu'elle fait intervenir des éléments conjugués par σ^8. De surcroit, J. Martinet a noté qu'une structure euclidienne apparaît naturellement sur le noyau de la trace : $(x, y) \mapsto \mathrm{Tr}_{K_3/\mathbf{Q}}(xy)$ puisque $xy \in K_3$ et que K_4 est, ici, totalement réelle. On connaît une base du réseau euclidien de dimension 16 $\mathrm{Ker}(\mathrm{Tr}_{K_4/K_3}(\mathcal{O}_{K_4}))$; on construit la matrice de Gram correspondante et on lui applique ensuite l'algorithme LLL qui en donne une base "aussi orthogonale que possible". La suite des instructions Pari qui effectuent ces calculs sont indiquées en annexe (base du noyau de la trace...). On obtient une nouvelle base dont les vecteurs ont pour coordonnées par rapport à l'ancienne

$v_1 = [132, 66, 62, 33, -159, -85, -76, -55, -84, -36, -20, 4, -165, -75, -37, -2]$
$v_2 = [38, 20, 30, 18, 43, 21, 19, 9, 51, 26, 20, 12, -4, 0, 16, 13]$
$v_3 = [159, 85, 76, 55, 132, 66, 62, 33, 165, 75, 37, 2, -84, -36, -20, 4]$
$v_4 = [43, 21, 19, 9, -38, -20, -30, -18, -4, 0, 16, 13, -51, -26, -20, -12]$
$v_5 = [42, 18, 18, 2, 153, 77, 66, 37, 155, 78, 62, 35, 23, 9, 12, 0]$
$v_6 = [-157, -77, -65, -31, -25, -6, 7, 20, -98, -54, -53, -41, 121, 55, 28, 2]$
$v_7 = [23, 9, 12, 0, 155, 78, 62, 35, 153, 77, 66, 37, 42, 18, 18, 2]$
$v_8 = [-51, -26, -20, -12, -4, 0, 16, 13, -38, -20, -30, -18, 43, 21, 19, 9]$
$v_9 = [8, 14, 34, 43, -84, -44, -49, -31, -73, -40, -29, -25, -14, 1, 19, 30]$
$v_{10} = [146, 71, 55, 25, 136, 72, 71, 48, 169, 80, 51, 17, -87, -46, -40, -28]$
$v_{11} = [84, 36, 20, -4, -165, -75, -37, -2, -132, -66, -62, -33, -159, -85, -76, -55]$
$v_{12} = [-77, -36, -40, -15, -153, -81, -72, -50, -164, -80, -64, -30, 7, 8, 0, 12]$

$v_{13} = [-4, 0, 16, 13, 51, 26, 20, 12, 43, 21, 19, 9, 38, 20, 30, 18]$
$v_{14} = [-84, -44, -49, -31, -8, -14, -34, -43, -14, 1, 19, 30, 73, 40, 29, 25]$
$v_{15} = [-178, -90, -89, -50, -7, -6, -11, -12, -68, -32, -22, -7, 146, 71, 39, 17]$
$v_{16} = [199, 99, 74, 39, 25, 15, 6, 10, 105, 49, 43, 14, -179, -91, -82, -48]$

Ces vecteurs, sont images par $1 - \sigma^8$ d'éléments de $\mathcal{O}_{K_4}$ définis à addition près par un élément de $\mathcal{O}_{K_3}$. On choisit $a_i u$ comme représentant de $a_i(1 - \sigma^8)(u)$. On obtient ainsi 16 entiers dont les images par $(1 - \sigma^8)$ forment une base de $\mathrm{Ker}(\mathrm{Tr}_{K_4/K_3}(\mathcal{O}_{K_4}))$. Pour chacun de ces entiers, on calcule ses conjugués (annexe Calcul des conjugués) puis les résolvantes de Speiser associées aux caractères fidèles de degré 2 de D_{32} (annexe Calcul de la norme des résolvantes). Si pour chacun de ces caractères et de ces entiers θ, on calcule $< \theta, \chi >< \theta, \overline{\chi} >$ on va retrouver un élément multiple entier d'un générateur du conducteur d'Artin situé dans le centre du facteur simple associé à la représentation. En faisant le produit on obtient un multiple de la norme sur $\mathbf{Q}$ du conducteur d'Artin, soit un multiple de 2305^4. Il se trouve que dans chaque cas le calcul est particulièrement agréable puisqu' après division par 2305^4 on obtient 0 pour v_1, 0 pour v_2, 0 pour v_3, 0 pour v_4, 1 pour v_5, 1 pour v_6, 1 pour v_7, 0 pour v_8, 1 pour v_9, 4 pour v_{10}, 0 pour v_{11}, 1 pour v_{12}, 0 pour v_{13}, 1 pour v_{14}, 1 pour v_{15}, 16 pour v_{16}. C'est dire que les vecteurs v_5, v_6, v_7, v_9, v_{12}, v_{14}, v_{15} se comportent comme le ferait un générateur de la base normale pour les caractères associés aux représentations fidèles de D_{32}. Intéressons-nous au premier de ces vecteurs.

On se base sur une remarque qui a déjà été faite. L'élément v_5 satisfait une condition nécessaire puisque les résolvantes associées aux représentations fidèles de D_{32}, ont, à une unité près, les valeurs voulues. Il suffirait donc que sa trace sur K_3 engendre une base normale de $\mathcal{O}_{K_3}$. On procède comme dans le §6 pour calculer la trace de v_5 sur K_3. On obtient les coordonnées :
$[-345, 571, -268, -67, 506, -53, 332, 118, 505, -64, -258, 558, -353, 137, 331, -541]$
Le calcul des résolvantes pour la trace de v_5 et les caractères de D_{16}, montre que cet élément n'est pas une base normale.

On a déjà dit que v_5 n'est défini qu'à un entier de K_3 près, sa trace l'est donc modulo $2\mathcal{O}_{K_3}$, on peut remplacer les cœfficients de la trace de v_5 par des entiers qui leurs sont congrus modulo 2. On choisit l'élément de coordonnées $[-1, 1, 0, -1, 0, 1, 0, 0, 1, 0, 0, 0, -1, 1, 1, -1]$. Puis on calcule le discriminant du module galoisien engendré par cet élément, on trouve le discriminant de $K_3/\mathbf{Q}$ muliplié par $3^2 5^2 7^2$. On a dit que la modification de la trace revenait à ajouter à v_5 un élément v de $\mathcal{O}_{K_3}$; on connaît les coordonnées de v, on peut donc donner une valeur approchée de ses conjugués au moyen de la matrice M_{K_3}, puis au moyen de l'inverse de M_{K_4} les coordonnées de v dans la base de $\mathcal{O}_{K_4}$.

On a maintenant un élément u qui possède les mêmes propriétés que v_5 pour les résolvantes associées aux représentations fidèles de D_{32} et dont la trace sur K_3 se déduit de la base normale par multiplication par l'élément $-1 + \sigma - \sigma^3 + \sigma^5 + \tau - \sigma^4\tau + \sigma^5\tau + \sigma^6\tau - \sigma^7\tau$ de $\mathbf{Z}[D_{16}]$. Or cet élément est la projection sur $\mathbf{Z}[D_{16}]$ de $g = -1 + \sigma - \sigma^3 + \sigma^5 + \tau - \sigma^4\tau + \sigma^5\tau + \sigma^6\tau - \sigma^7\tau$ de $\mathbf{Z}[D_{32}]$. qui vérifie $\det_{\chi_4} = -1$, $\det_{\chi_3} = 7$, $\det_{\chi_2} = 5$, $\det_{V_4} = -3$ (ces propriétés se vérifient à l'aide des instructions regroupées dans *normes réduites*. La première de ces valeurs nous dit que l'image g est inversible dans l'ordre $\mathbf{Z}[D_{32}]/(1 + \sigma^8)$

On sait qu'il existe une base normale de $\mathcal{O}_{K_4}$, appelons-la φ, et $u = h\varphi$ avec $h \in \mathbf{Z}[D_{32}]$. Par comparaison, on doit avoir, à une unité près de $\mathbf{Z}[D_{32}]$: $h = g$. On calcule donc l'inverse de g dans $\mathbf{Q}[D_{32}]$, puis $g^{-1}u_1$ par l'intermédiaire de ses conjugués. On obtient alors son polynôme irréductible sur $\mathbf{Q}$, ses coordonnées sur la base initiale de $\mathcal{O}_{K_4}$. On vérifie par le calcul des résolvantes que c'est bien une base normale (Le calcul de l'inverse de g se fait avec l'utilisation de la représentation régulière de D_{32}). Les coordonnées sur la base des entiers de K_4 sont :
$[-32, 1, 60, 74, -87, -53, -90, -66, 41, 4, -53, -69, 91, 53, 70, 56, -89, -45, -19, -12, 61, 47, 92, 90, 80, 40, 12, 7,$
$-70, -52, -99, -95]$
et le polynôme irréductible est :
$X^{32} - X^{31} - 753X^{30} + 485X^{29} + 238854X^{28} - 29693X^{27} - 41887945X^{26} - 22629751X^{25} + 4474092010X^{24} +$
$5895786985X^{23} - 301539880402X^{22} - 653222045618X^{21} + 12798456585980X^{20} + 39203063155695X^{19}$
$-329628816303025X^{18} - 1344212963181859X^{17} + 4704638681394808X^{16} + 26359186074882722X^{15}$
$-27908421136071560X^{14} - 28492844678644 6670X^{13} - 633991361016184 99X^{12} + 1593274593453648068X^{11}$
$+1349948649938636629X^{10} - 4647130106491430080X^{9} - 5190594201276392235X^{8} + 7580672125641418004X^{7} +$
$8444933800958352349X^{6} - 7288105010153196062X^{5} - 5814065681993512876X^{4} + 3771785591758605540X^{3}$
$+1100528757405736775X^{2} - 521402089524256000X - 60534510651775625$

RÉFÉRENCES

[C] -J. COUGNARD- *Bases normales pour des extensions diedrales de degré 8*
Séminaire de Théorie des nombres de Caen 1992-93

[DM] - P. DAMEY J. MARTINET - *Plongement d'une extension quadratique dans une extension quaternionienne.*
J. für die Reine und Ang. Math. vol 262-263 1973 p. 323 - 338.

[F1] - A. FRÖHLICH - *Galois Module Structure and Rootnumbers for QuaternionExtension of degree* 2^n.
J. Number Theory vol. 12, n°4 1980 p. 499 - 518

[F2] - A. FRÖHLICH - *Galois Module Structure of Algebraic Integers.*
Ergebnisse der Math. vol. 1 Springer Verlag Berlin 1983

[G] - G. GRAS - *Nombre de φ-Classes Invariantes Application aux Classes des Corps Abéliens.*
Bull. Soc. Math. France 106 (1978), p. 337-364.

[M] - J.MARTINET - *Modules sur l'Algèbre de groupe Quaternionien.*
Ann. scient. Éc. Norm. Sup. 4^e dérie t.4, 1971, p. 399 à 408.

[Or] - B. ORIAT *Groupes des Classes des Corps Quadratiques Réels* $\mathbf{Q}(\sqrt{d}, d < 10000)$.
Tables numériques Faculté des Sciences de Besançon F.25030 Besançon Cedex

[P] -*User's Guide to PARI-GP* version 1.37.2
pari@ceremab.u-bordeaux.fr

[Se1] - J.-P. SERRE -*Représentations Linéaires des Groupes Finis.*
Collection Méthodes, seconde édition , Hermann Paris 1971.

[Se1] - J.-P. SERRE -*Corps Locaux.*
Actualités Scientifiques et Industrielles seconde édition, Hermann Paris 1967.

[Sw] - R.G. SWAN -*Projective Modules over Group Rings and Maximal Orders.*
Annals of Math. vol. 76, n°1 1962 p. 55 - 61.

ANNEXE

Instruction PARI, utilisées dans Gp pour les calculs de ce travail.

Bases normales des entiers de certaines extensions à groupe D8

```
w=(1+sqrt(5))/2;
w1=1-w;
a=(w+sqrt(w+21))/2;
ap=(w-sqrt(w+21))/2;
a1=(w1+sqrt(w1+21))/2;
a1p=(w1-sqrt(w1+21))/2;
(x-a)*(x-a1)*(x-ap)*(x-a1p)
round(%)
\w basesnormales
aa=[a,a1,ap,a1p,a,a1,ap,a1p];
aa1=[a1,ap,a1p,a,a1p,a,a1,ap];
om=[w,w1,w,w1,w,w1,w,w1];
nib=vector(8,ind,aa[ind]*aa1[ind]*om[ind]);
polynome=prod(1,ind=1,8,x-nib[ind]);
round(%)
\w basesnormales
nulle4=matrix(4,4,x,y,0);
v=concat(matrix(4,4,x,y,if((x-y-1)%4,0,1)),nulle4);
w=concat(nulle4,matrix(4,4,x,y,if((x-y-1)%4,0,1)));
s=concat(v~ ,w~ )~ ;
u=concat(nulle4,matrix(4,4,x,y,if((x+y-2)%4,0,1)))~ ; u1=concat(matrix(4,4,x,y,if((x+y-2)%4,0,1)),nulle4)~ ;
t=concat(u,u1)~ ;
sum(matrix(8,8,x,y,0),ind=1,4,nib[ind]*s^ (5-ind));
sum(%,ind=1,4,nib[ind+4]*s^ (ind-1)*t);
sqrt(round(det(%)))
\w basesnormales
```

Prolongement de σ de K_2 à K_3 : Programme Hilbert

```
w=(1+sqrt(5))/2;
w1=1-w;
a=(w+sqrt(w+21))/2;
ap=w-a;
a1=(w1+sqrt(w1+21))/2;
a1p=w1-a1;
mat([a*a1*w,a1*ap*w1, ap*a1p*w,a1p*a*w1, a*a1p*w, a1*a*w1, ap*a1*w, a1p*ap*w1]~ );
concat(% ,mat([a1*ap*w1, ap*a1p*w, a1p*a*w1, a*a1*w, a1p*ap*w1, a*a1p*w,a1*a*w1, ap*a1* w]~ ));
concat(% ,mat([ap*a1p*w, a1p*a*w1, a*a1*w, a1*ap*w1, ap*a1*w, a1p*ap*w1, a*a1p*w, a1*a*w 1]~ ));
concat(% ,mat([a1p*a*w1, a*a1*w, a1*ap*w1, ap*a1p*w, a1*a*w1, ap*a1*w, a1p*ap*w1, a*a1p* w]~ ));
concat(% ,mat( [a*a1p*w, a1*a*w1, ap*a1*w, a1p*ap*w1, a*a1*w, a1*ap*w1, ap*a1p*w, a1p*a*w 1]~ ));
concat(% ,mat( [a1*a*w1, ap*a1*w, a1p*ap*w1, a*a1p*w, a1p*a*w1, a*a1*w, a1*ap*w1, ap*a1p* w]~ ));
concat(% ,mat( [ap*a1*w, a1p*ap*w1, a*a1p*w, a1*a*w1, ap*a1p*w, a1p*a*w1, a*a1*w, a1*ap*w 1]~ ));
concat(% ,mat([a1p*ap*w1, a*a1p*w, a1*a*w1, ap*a1*w, a1*ap*w1, ap*a1p*w, a1p*a*w1 ,a*a1* w]~ ));
tableau=% ;
matsize(tableau) det(tableau);
factor(round(% ))
u= sqrt((15+7*w1+(1-5*w1)*a1)/(15+7*w+(1-5*w)*a))
su=sqrt( (15+7*w+(1-5*w)*ap)/(15+7*w1+(1-5*w1)*a1))
s2u=sqrt(( 15+7*w1+(1-5*w1)*a1p)/(15+7*w+(1-5*w)*ap))
s3u=sqrt((15+7*w+(1-5*w)*a)/( 15+7*w1+(1-5*w1)*a1p))
tu=sqrt(( 15+7*w1+(1-5*w1)*a1p)/(15+7*w+(1-5*w)*a))
```

```
stu=sqrt((15+7*w+(1-5*w)*a)/(15+7*w1+(1-5*w1)*a1))
s2tu=sqrt((15+7*w1+(1-5*w1)*a1)/(15+7*w+(1-5*w)*ap))
s3tu=sqrt((15+7*w+(1-5*w)*ap)/( 15+7*w1+(1-5*w1)*a1p))
v=461*[u,su,-s2u,s3u,tu,stu,s2tu,-s3tu]~ ;
matinvr(tableau)*v;
round(% );
```

Calcul de Résolvante dans K_2, Programme ResokiD16

```
\r Hilbert
\e
b=(-1-(1+w)*a+sqrt(15+7*w+(1-5*w)*a))/2;
bt=-1-(1+w)*a-b;
bp=(-1-(1+w)*ap+sqrt(15+7*w+(1-5*w)*ap))/2;
bpt=-1-(1+w)*ap-bp;
b1=(-1-(1+w1)*a1+sqrt(15+7*w1+(1-5*w1)*a1))/2;
b1t=-1-(1+w1)*a1-b1;
b1p=(-1-(1+w1)*a1p+sqrt(15+7*w1+(1-5*w1)*a1p))/2;
b1pt=-1-(1+w1)*a1p-b1p;
om=[w^(-7), w1^ (-7) ,w^ (-7), w1^ (-7), w^ (-7), w1^ (-7), w^ (-7) ,w1^ (-7), w^ (-7), w1^ (-7), w^ (-7), w1^ (-7),
w^ (-7), w1^ (-7), w^ (-7), w1^ (-7)];
AA=[a,a1,ap,a1p,a,a1,ap,a1p,a,a1,ap,a1p,a,a1,ap,a1p];
BB=[b,b1,bp,b1pt,bt,b1t,bpt,b1p,b,b1,bp,b1pt,bt,b1t,bpt,b1p];
CC=[bp,b1pt,bt,b1t,bpt,b1p,b,b1,bpt,b1p,b,b1,bp,b1pt,bt,b1t];
esp= vector(16,id,om[id]*AA[id]*BB[id]*CC[id]);
nulle2=[0,0;0,0];
tau=[1,sqrt(2);0,-1];
sygm=[0,-1;1,sqrt(2)];
sum(nulle2,id=1,8,compo(esp,id)*(sygm^ (9-id)));
sum(% ,id=1,8,compo(esp,id+8)*(sygm^ (id-1))*tau);
r1=det(% );
tau=[1,-sqrt(2);0,-1];
sygm=[0,-1;1,-sqrt(2)];
sum(nulle2,id=1,8,compo(esp,id)*(sygm^ (9-id)));
sum(% ,id=1,8,compo(esp,id+8)*(sygm^ (id-1))*tau);
r2=det(% );
r1*r2
round(% )
```

Un calcul de norme

w=quadgen(5)

$a = \mathrm{mod}(x, x^2 - \omega * x - 5)$;

$\mathrm{norm}(((2 * \omega - 1 - (1 + \omega) * a)^2 - (15 + 7 * \omega + (1 - 5 * \omega) * a))/4)$

norm(%)

$\mathrm{norm}((-1 + 3 * \omega + (1 - \omega) * a)^2 - (15 + 7 * \omega + (1 - 5 * \omega) * a))$

norm(%)

Calcul de la trace de θ dans K_3/K_2

```
\r hilbert
\e
b=(-1-(1+w)*a+sqrt(15+7*w+(1-5*w)*a))/2;
bt=-1-(1+w)*a-b;
bp=(-1-(1+w)*ap+sqrt(15+7*w+(1-5*w)*ap))/2;
bpt=-1-(1+w)*ap-bp;
b1=(-1-(1+w1)*a1+sqrt(15+7*w1+(1-5*w1)*a1))/2;
b1t=-1-(1+w1)*a1-b1;
b1p=(-1-(1+w1)*a1p+sqrt(15+7*w1+(1-5*w1)*a1p))/2;
b1pt=-1-(1+w1)*a1p-b1p;
[ w^ (-7)*a*(b*bp+bt*bpt), w1^ (-7)*a1*(b1*b1pt+b1t*b1p), w^ (-7)*ap*(bp*bt+bpt*b),
w1^ (-7)*a1p*(b1pt*b1t+b1p*b1), w^ (-7)*a*(b*bpt+bt*bp), w1^ (-7)*a1*(b1*b1p+b1t*b1pt),
w^ (-7)*ap*(bp*b+bpt*bt), w1^ (-7)*a1p*(b1pt*b1+b1p*b1t)]~ ;
matinvr(tableau)*% round(%)
```

Unités dans L3 et générateur d'ideal

```
    w=(1+sqrt(5))/2;
w1=1-w;
a=(w+sqrt(w+21))/2;
ap=w-a;
a1=(w1+sqrt(w1+21))/2;
a1p=w1-a1;
b=(-1-(1+w)*a+sqrt(15+7*w+(1-5*w)*a))/2;
b1=(-1-(1+w1)*a1+sqrt(15+7*w1+(1-5*w1)*a1))/2;
bp=(-1-(1+w)*ap+sqrt(15+7*w+(1-5*w)*ap))/2;
bt=-1-(1+w)*a-b;
bpt=-1-(1+w)*ap-bp;
b1t=-1-(1+w1)*a1-b1;
b1p=(-1-(1+w1)*a1p+sqrt(15+7*w1+(1-5*w1)*a1p))/2;
b1pt=-1-(1+w1)*a1p-b1p;
mat([1,1,1,1,1,1,1,1]~ );
concat(% ,mat([w,w1,w,w1,w,w1,w,w1]~ ));
concat(% ,mat([a,a1,ap,a1p,a,a1,ap,a1p]~ ));
concat(% ,mat([w*a,w1*a1,w*ap,w1*a1p,w*a,w1*a1,w*ap,w1*a1p]~ ));
concat(% ,mat([b,b1,bp,b1pt,bt,b1t,bpt,b1p]~ ));
concat(% ,mat([w*b,w1*b1,w*bp,w1*b1pt,w*bt,w1*b1t,w*bpt,w1*b1p]~ ));
concat(% ,mat([a*b,a1*b1,ap*bp, a1p*b1pt, a*bt, a1*b1t, ap*bpt, a1p*b1p]~ ));
concat(% ,mat([w*a*b, w1*a1*b1, w*ap*bp, w1*a1p*b1pt, w*a*bt, w1*a1*b1t,
w*ap*bpt, w1*a1p*b1p]~ ));
N=% ;
elem=N*[5,12,-1,-5,9,5,-4,-1]~
prod(1,id=1,8,x-elem[id])
round(% ) u1=N*[1,2,-1,0,3,-3,-1,1]~ ;
prod(1,id=1,8,x-u1[id])
round(% )
u2=N*[3,2,0,0,-2,1,-1,1]~ ;
prod(1,id=1,8,x-u2[id])
round(% )
prod(1,id=1,8,x-u1[id]*u2[id])
```

```
round(% )
vvector(8,id,-elem[id]*u1[id]*u2[id]);
z=% ;
\b
prod(1,id=1,8,x+z[id])
round(% )
gen=matinvr(N)*z
round(% )
u3=N*[3,2,0,1,-3,3,2,-1]~ ;
prod(1,id=1,8,x-u3[id])
round(% )
vvector(8,id,u3[id]^ 2);
matinvr(n)*%
round(% )
epsilon=%
(round(gen)-epsilon)/4
```

Base Normale de K_3 Prolongement de σ, NIBK3

```
\e
\precision =80
w=(1+sqrt(5))/2;
w1=1-w;
a=(w+sqrt(w+21))/2;
ap=w-a;
a1=(w1+sqrt(w1+21))/2;
a1p=w1-a1;
b=(-1-(1+w)*a+sqrt(15+7*w+(1-5*w)*a))/2;
bt=-1-(1+w)*a-b;
bp=(-1-(1+w)*ap+sqrt(15+7*w+(1-5*w)*ap))/2;
bpt=-1-(1+w)*ap-bp;
b1=(-1-(1+w1)*a1+sqrt(15+7*w1+(1-5*w1)*a1))/2;
b1t=-1-(1+w1)*a1-b1;
b1p=(-1-(1+w1)*a1p+sqrt(15+7*w1+(1-5*w1)*a1p))/2;
b1pt=-1-(1+w1)*a1p-b1p;
om=[w^ (-7), w1^ (-7), w^ (-7), w1^ (-7), w^ (-7) , w1^ (-7),w^ (-7), w1^ (-7), w^ (-7), w1^ (-7), w^ (-7), w1^
(-7), w^ (-7),w1^ (-7),w^ (-7),w1^ (-7)];
nulle=matrix(16,16,x,y,0);
AA=[a,a1,ap,a1p,a,a1,ap,a1p,a,a1,ap,a1p,a,a1,ap,a1p];
AA1=(1/2)*[a1,ap,a1p,a,a1,ap,a1p,a,a1p,a,a1,ap,a1p,a,a1,ap];
BB2=[b,b1,bp,b1pt,bt,b1t,bpt,b1p,b,b1,bp,b1pt,bt,b1t,bpt,b1p];
CC2=[bp,b1pt,bt,b1t,bpt,b1p,b,b1,bpt,b1p,b,b1,bp,b1pt,bt,b1t];
sygalph=2*[w1*a1p*a, w*a*a1, w1*a1*ap, w*ap*a1p, w1*a1p*a, w*a*a1, w1*a1*ap, w*ap*a1p, w1*a1*a,
w*ap*a1, w1*a1p*ap, w*a*a1p, w1*a1*a, w*ap*a1, w1*a1p*ap, w*a*a1p];
taualph=[w*a*a1p, w1*a1*a, w*ap*a1, w1*a1p*ap, w*a*a1p, w1*a1*a, w*ap*a1, w1*a1p*ap, w*a*a1, w1*a1*ap
, w*ap*a1p, w1*a1p*a, w*a*a1, w1*a1*ap, w*ap*a1p, w1*a1p*a];
sygtoalph=2*[w1*a1*a, w*ap*a1, w1*a1p*ap, w*a*a1p, w1*a1*a, w*ap*a1, w1*a1p*ap, w*a*a1p,
w1*a1p*a, w*a*a1, w1*a1*ap, w*ap*a1p, w1*a1p*a, w*a*a1, w1*a1*ap, w*ap*a1p];
esp=matrix(16,1,x,y, compo(om,x)*compo(aa,x)*compo(bb2,x)*compo(cc2,x) -compo(sygalph,x)
-compo(taualph,x)+compo(sygtoalph,x));
matrix( 16,1,x,y, if(x<9, if((x+1)%8 !=0,esp[(x+1)%8,1],esp[8,1]), if((x-1)%8 !=0,esp[8+(x-1)%8,1],esp[16,1])) );
tableau=concat(esp,%);
matrix(16,1,x,y,if(x < 9, if((x+2)%8 !=0,esp[(x+2)%8,1],esp[8,1]), if((x-2)%8 !=0,esp[8+(x-2)%8,1],esp[16,1])) );
concat(tableau,%);
```

```
tableau=%;
matrix(16,1,x,y,if(x<9, if((x+3)%8 !=0,esp[(x+3)%8,1],esp[8,1]), if((x-3)%8 !=0,esp[8+(x-3)%8,1],esp[16,1])) );
concat(tableau,%);
tableau=%;
matrix(16,1,x,y,if(x<9, if((x+4)%8 !=0,esp[(x+4)%8,1],esp[8,1]), if((x-4)%8 !=0,esp[8+(x-4)%8,1],esp[16,1])) );
concat(tableau,%);
tableau=%;
matrix(16,1,x,y,if(x<9, if((x+5)%8 !=0,esp[(x+5)%8,1],esp[8,1]), if((x-5)%8 !=0,esp[8+(x-5)%8,1],esp[16,1])) );
concat(tableau,%);
tableau=%;
matrix(16,1,x,y,if(x<9, if((x+6)%8 !=0,esp[(x+6)%8,1],esp[8,1]), if((x-6)%8 !=0,esp[8+(x-6)%8,1],esp[16,1])) );
concat(tableau,%);
tableau=%;
matrix(16,1,x,y,if(x<9, if((x+7)%8 !=0,esp[(x+7)%8,1],esp[8,1]), if((x-7)%8!=0,esp[8+(x-7)%8,1],esp[16,1])) );
concat(tableau,%);
tableau=%;
esp1=matrix(16,1,x,y,if(x<9,esp[x+8,1] , esp[x-8,1]));
concat(tableau,%);
tableau=%;
matrix( 16,1,x,y, if(x<9, if((x+1)%8!=0,esp1[(x+1)%8,1], esp1[8,1]), if((x-1)%8 !=0,esp1[8+(x-1)%8,1],
esp1[16,1])) );
tableau=concat(tableau,%);
matrix(16,1,x,y,if(x<9, if((x+2)%8!=0,esp1[(x+2)%8,1],esp1[8,1]), if((x-2)%8 !=0,esp1[8+(x-2)%8,1],
esp1[16,1])) );
concat(tableau,%);
tableau=%;
matrix(16,1,x,y,if(x<9, if((x+3)%8!=0,esp1[(x+3)%8,1],esp1[8,1]), if((x-3)%8 !=0,esp1[8+(x-3)%8,1],
esp1[16,1])) );
concat(tableau,%);
tableau=%;
matrix(16,1,x,y,if(x<9, if((x+4)%8!=0,esp1[(x+4)%8,1],esp1[8,1]), if((x-4)%8 !=0,esp1[8+(x-4)%8,1],
esp1[16,1])) );
concat(tableau,%);
tableau=%;
matrix(16,1,x,y,if(x<9, if((x+5)%8!=0,esp1[(x+5)%8,1], esp1[8,1]), if((x-5)%8 !=0,esp1[8+(x-5)%8,1],
esp1[16,1])) );
concat(tableau,%);
tableau=%;
matrix(16,1,x,y,if(x<9, if((x+6)%8 !=0,esp1[(x+6)%8,1],esp1[8,1]), if((x-6)%8 !=0,esp1[8+(x-6)%8,1],
esp1[16,1])) );
concat(tableau,%);
tableau=%;
matrix(16,1,x,y,if(x<9, if((x+7)%8 !=0,esp1[(x+7)%8,1],esp1[8,1]), if((x-7)%8 !=0,esp1[8+(x-7)%8,1],
esp1[16,1])) );
concat(tableau,%);
tableau=%;
d=76-38*w+(20-15*w)*a+(-24+13*w+(-33+21*w)*a)*b;
d1=76-38*w1+(20-15*w1)*a1+(-24+13*w1+(-33+21*w1)*a1)*b1;
dp=76-38*w+(20-15*w)*ap+(-24+13*w+(-33+21*w)*ap)*bp;
d1pt=76-38*w1+(20-15*w1)*a1p+(-24+13*w1+(-33+21*w1)*a1p)*b1pt;
dt=76-38*w+(20-15*w)*a+(-24+13*w+(-33+21*w)*a)*bt;
d1t=76-38*w1+(20-15*w1)*a1+(-24+13*w1+(-33+21*w1)*a1)*b1t;
dpt=76-38*w+(20-15*w)*ap+(-24+13*w+(-33+21*w)*ap)*bpt;
```

```
d1p=76-38*w1+(20-15*w1)*a1p+(-24+13*w1+(-33+21*w1)*a1p)*b1p;
s=sqrt(d1/d);
s1=sqrt(dp/d1);
s2=sqrt(d1pt/dp);
s3=sqrt(dt/d1pt);
s4=sqrt(d1t/dt);
s5=sqrt(dpt/d1t);
s6=sqrt(d1p/dpt);
s7=sqrt(d/d1p);
wec=[s,s1,s2,s3,s4,s5,s6,s7];
messign=[1,1,-1,1,1,-1,-1,1];
rac=vector(8,ind,wec[ind]*messign[ind]);
suite=[1/rac[8],1/rac[1],1/rac[2],1/rac[3],1/rac[4],1/rac[5],1/rac[6],1/rac[7]];
syst=461*concat(rac,suite);
sum(0,ind=1,16,syst[ind])
sum(0,ind=1,16,syst[ind]^ 3)
prod(1,ind=1,16,x-syst[ind])
matinvr(tableau)*trans(syst)
round(%);
```

Construction de la base des entiers de K_4 et de la matrice associée

```
\r nibk3
c=(3+2*w+w*a+(-3+3*w+(2-w)*a)*b+sqrt(76-38*w+(20-15*w)*a+(-24+13*w+(-33+21*w)*a)*b))/2;
c1=(3+2*w1+w1*a1+(-3+3*w1+(2-w1)*a1)*b1+sqrt(76-38*w1+(20-15*w1)*a1+
(-24+13*w1+(-33+21*w1)*a1)*b1))/2;
cp=(3+2*w+w*ap+(-3+3*w+(2-w)*ap)*bp+sqrt(76-38*w+(20-15*w)*ap+
(-24+13*w+(-33+21*w)*ap)*bp))/2;
c1ptu=(3+2*w1+w1*a1p+(-3+3*w1+(2-w1)*a1p)*b1pt-sqrt(76-38*w1+(20-15*w1)*a1p+
(-24+13*w1+(-33+21*w1)*a1p)*b1pt))/2;
ctu=(3+2*w+w*a+(-3+3*w+(2-w)*a)*bt-sqrt(76-38*w+(20-15*w)*a+
(-24+13*w+(-33+21*w)*a)*bt))/2;
c1tu=(3+2*w1+w1*a1+(-3+3*w1+(2-w1)*a1)*b1t-sqrt(76-38*w1+(20-15*w1)*a1+
(-24+13*w1+(-33+21*w1)*a1)*b1t))/2;
cpt=(3+2*w+w*ap+(-3+3*w+(2-w)*ap)*bpt+sqrt(76-38*w+(20-15*w)*ap+
(-24+13*w+(-33+21*w)*ap)*bpt))/2;
c1pu=(3+2*w1+w1*a1p+(-3+3*w1+(2-w1)*a1p)*b1p-sqrt(76-38*w1+(20-15*w1)*a1p+
(-24+13*w1+(-33+21*w1)*a1p)*b1p))/2;
cu=(3+2*w+w*a+(-3+3*w+(2-w)*a)*b-sqrt(76-38*w+(20-15*w)*a+(-24+13*w+(-33+21*w)*a)*b))/2;
c1u=(3+2*w1+w1*a1+(-3+3*w1+(2-w1)*a1)*b1-sqrt(76-38*w1+(20-15*w1)*a1+
(-24+13*w1+(-33+21*w1)*a1)*b1))/2;
cpu=(3+2*w+w*ap+(-3+3*w+(2-w)*ap)*bp-sqrt(76-38*w+(20-15*w)*ap+
(-24+13*w+(-33+21*w)*ap)*bp))/2;
c1pt=(3+2*w1+w1*a1p+(-3+3*w1+(2-w1)*a1p)*b1pt+sqrt(76-38*w1+(20-15*w1)*a1p+
(-24+13*w1+(-33+21*w1)*a1p)*b1pt))/2;
ct=(3+2*w+w*a+(-3+3*w+(2-w)*a)*bt+sqrt(76-38*w+(20-15*w)*a+(-24+13*w+(-33+21*w)*a)*bt))/2;
c1t=(3+2*w1+w1*a1+(-3+3*w1+(2-w1)*a1)*b1t+sqrt(76-38*w1+(20-15*w1)*a1+
(-24+13*w1+(-33+21*w1)*a1)*b1t))/2;
cptu=(3+2*w+w*ap+(-3+3*w+(2-w)*ap)*bpt-sqrt(76-38*w+(20-15*w)*ap+
(-24+13*w+(-33+21*w)*ap)*bpt))/2;
c1p=(3+2*w1+w1*a1p+(-3+3*w1+(2-w1)*a1p)*b1p+sqrt(76-38*w1+(20-15*w1)*a1p+
(-24+13*w1+(-33+21*w1)*a1p)*b1p))/2;
\\ w et ses conjugues om=[w,w1,w,w1,w,w1,w,w1,w,w1,w,w1,w,w1,w,w1];
omun=om;
omK4=concat(om,omun);
```

```
\\ w1 et ses conjugues
sigom=[w1,w,w1,w,w1,w,w1,w,w1,w,w1,w,w1,w,w1,w];
sigomun=sigom;
sigomK4=concat(sigomun,sigom);
\\a et ses conjugues veca=[a,a1,ap,a1p,a,a1,ap,a1p,a,a1,ap,a1p,a,a1,ap,a1p];
aun=veca;
vecK4a=concat(veca,aun);
\\ap et ses conjugues vecap=[ap,a1p,a,a1,ap,a1p,a,a1,ap,a1p,a,a1,ap,a1p,a,a1];
veca1p=vecap;
vecK4ap=concat(vecap,veca1p);
\\b et ses conjugues BB1=[b,b1,bp,b1pt,bt,b1t,bpt,b1p,b,b1,bp,b1pt,bt,b1t,bpt,b1p];
BB2=BB1;
BB=concat(BB1,BB2);
\\s4(b) et ses conjugues
s4BB1=[bt,b1t,bpt,b1p,b,b1,bp,b1pt,bt,b1t,bpt,b1p,b,b1,bp,b1pt];
s4BB2=s4bb1;
s4BB=concat(s4bb1,s4bb2);
conj1c=[c,c1,cp,c1ptu,ctu,c1tu,cpt,c1pu,cu,c1u,cpu,c1pt,ct,c1t,cptu,c1p];
conj2c=conj1c;
conjc=concat(conj1c,conj2c);
conjs4c1=[ctu,c1tu,cpt,c1pu,cu,c1u,cpu,c1pt,ct,c1t,cptu,c1p,c,c1,cp,c1ptu];
conjs4c2=[ct,c1t,cptu,c1p,c,c1,cp,c1ptu,ctu,c1tu,cpt,c1pu,cu,c1u,cpu,c1pt];
conjs4c=concat(conjs4c1,conjs4c2);
conjs8c1=[cu,c1u,cpu,c1pt,ct,c1t,cptu,c1p,c,c1,cp,c1ptu,ctu,c1tu,cpt,c1pu];
conjs8c2=conjs8c1;
conjs8c=concat(conjs8c1,conjs8c2);
conjs12c1=[ct,c1t,cptu,c1p,c,c1,cp,c1ptu,ctu,c1tu,cpt,c1pu,cu,c1u,cpu,c1pt];
conjs12c2=[ctu,c1tu,cpt,c1pu,cu,c1u,cpu,c1pt,ct,c1t,cptu,c1p,c,c1,cp,c1ptu];
conjs12c=concat(conjs12c1,conjs12c2);
\\construction-d'une-base-sur-Z-de-OK4
awu=mat(vvector(32,ind,conjc[ind]*conjs4c[ind]*bb[ind]*vecK4a[ind]*omK4[ind]));
apwu=mat(vvector(32,ind,conjc[ind]*conjs4c[ind]*bb[ind]*vecK4ap[ind]*omK4[ind]));
aw1u=mat(vvector(32,ind,conjc[ind]*conjs4c[ind]*bb[ind]*vecK4a[ind]*sigomK4[ind]));
apw1u=mat(vvector(32,ind,conjc[ind]*conjs4c[ind]*bb[ind]*vecK4ap[ind]*sigomK4[ind]));
aws4u=mat(vvector(32,ind,conjs4c[ind]*conjs8c[ind]*s4bb[ind]*vecK4a[ind]*omK4[ind]));
apws4u=mat(vvector(32,ind,conjs4c[ind]*conjs8c[ind]*s4bb[ind]*vecK4ap[ind]*omK4[ind]));
aw1s4u=mat(vvector(32,ind,conjs4c[ind]*conjs8c[ind]*s4bb[ind]*vecK4a[ind]*sigomK4[ind]));
apw1s4u=mat(vvector(32,ind,conjs4c[ind]*conjs8c[ind]*s4bb[ind]*vecK4ap[ind]*sigomK4[ind]));
aws8u=mat(vvector(32,ind,conjs8c[ind]*conjs12c[ind]*bb[ind]*vecK4a[ind]*omK4[ind]));
apws8u=mat(vvector(32,ind,conjs8c[ind]*conjs12c[ind]*bb[ind]*vecK4ap[ind]*omK4[ind]));
aw1s8u=mat(vvector(32,ind,conjs8c[ind]*conjs12c[ind]*bb[ind]*vecK4a[ind]*sigomK4[ind]));
apw1s8u=mat(vvector(32,ind,conjs8c[ind]*conjs12c[ind]*bb[ind]*vecK4ap[ind]*sigomK4[ind]));
aws12u=mat(vvector(32,ind,conjs12c[ind]*conjc[ind]*s4bb[ind]*vecK4a[ind]*omK4[ind]));
apws12u=mat(vvector(32,ind,conjs12c[ind]*conjc[ind]*s4bb[ind]*vecK4ap[ind]*omK4[ind]));
aw1s12u=mat(vvector(32,ind,conjs12c[ind]*conjc[ind]*s4bb[ind]*vecK4a[ind]*sigomK4[ind]));
apw1s12u=mat(vvector(32,ind,conjs12c[ind]*conjc[ind]*s4bb[ind]*vecK4ap[ind]*sigomK4[ind]));
awtauu=mat(vvector(32,ind,conjc[ind]*conjs12c[ind]*bb[ind]*vecK4a[ind]*omK4[ind]));
apwtauu=mat(vvector(32,ind,conjc[ind]*conjs12c[ind]*bb[ind]*vecK4ap[ind]*omK4[ind]));
aw1tauu=mat(vvector(32,ind,conjc[ind]*conjs12c[ind]*bb[ind]*vecK4a[ind]*sigomK4[ind]));
apw1tauu=mat(vvector(32,ind,conjc[ind]*conjs12c[ind]*bb[ind]*vecK4ap[ind]*sigomK4[ind]));
aws4tauu=mat(vvector(32,ind,conjc[ind]*conjs4c[ind]*s4bb[ind]*vecK4a[ind]*omK4[ind]));
apws4tauu=mat(vvector(32,ind,conjc[ind]*conjs4c[ind]*s4bb[ind]*vecK4ap[ind]*omK4[ind]));
aw1s4tauu=mat(vvector(32,ind,conjc[ind]*conjs4c[ind]*s4bb[ind]*vecK4a[ind]*sigomK4[ind]));
```