Journal de Théorie des Nombres
de Bordeaux **10** (1998), 163–201

Anneaux d'entiers stablement libres sur $\mathbb{Z}[H_8 \times C_2]$

par Jean COUGNARD

RÉSUMÉ. Le groupe $H_8 \times C_2$ est le plus petit groupe pour lequel existent des modules stablement libres non libres. On montre que toutes les classes d'isomorphisme de tels modules peuvent être représentées une infinité de fois par des anneaux d'entiers. On applique un travail de classification de Swan, pour cela on doit construire explicitement des bases normales d'entiers d'extensions à groupe H_8; cela se fait en liant un critère de Martinet avec une construction de Witt.

ABSTRACT. The smallest group which posseses stably free and non free modules is $H_8 \times C_2$. In each isomorphism class of such modules one exhibits infinitely many rings of integers. To use the classification done by Swan, we need an explicit construction of normal integral bases for rings of integers of H_8 extensions of $\mathbb{Q}$. That is done by comparing Martinet's criterion and Witt's construction of such extensions.

Soit $N/\mathbb{Q}$ une extension galoisienne modérément ramifiée de groupe de Galois G, son anneau des entiers $\mathcal{O}_N$ est un $\mathbb{Z}[G]$-module projectif de rang 1 localement libre ; on lui associe sa classe $[\mathcal{O}_N]$ dans le groupe des classes projectives $C\ell(\mathbb{Z}[G])$. M.J. Taylor [T] montre que cette classe est d'ordre au plus 2, prouvant une conjecture de A. Fröhlich. Il en déduit, grâce à la description de $C\ell(\mathbb{Z}[G])$ donnée par A. Fröhlich [F3], une méthode de calcul de cet ordre via les constantes d'équations fonctionnelles des fonctions $\Lambda(s,\chi)$ d'Artin liées aux caractères symplectiques de G.

La classe $[\mathcal{O}_N]$ est élément neutre de $C\ell(\mathbb{Z}[G])$ si et seulement si $\mathcal{O}_N \oplus \mathbb{Z}[G] \simeq \mathbb{Z}[G] \oplus \mathbb{Z}[G]$. Pour certains groupes il est possible de «simplifier» ([J], [F2]) et d'en déduire l'isomorphisme de $\mathcal{O}_N$ et $\mathbb{Z}[G]$: $\mathcal{O}_N$ est alors un $\mathbb{Z}[G]$-module libre de rang 1, il possède une base sur $\mathbb{Z}$ formée des conjugués $g(a)$, $g \in G$ d'un élément a (une base normale).

La simplification des $\mathbb{Z}[G]$-modules n'est pas toujours possible : Swan [Sw2] a donné un exemple de module stablement libre et non libre pour un $\mathbb{Z}[H_{32}]$-module où H_{32} est le groupe des quaternions d'ordre 32. En dépit

Manuscrit reçu le 2 mai 1997.

de la spécificité des anneaux d'entiers mise en évidence par le théorème de Taylor on a donné un exemple d'anneau d'entiers stablement libre et non libre sur $\mathbb{Z}[H_{32}]$ [Co].

La question se pose de savoir si toutes les classes d'isomorphisme de $\mathbb{Z}[G]$-modules stablement isomorphes à $\mathbb{Z}[G]$ peuvent être représentées par des anneaux d'entiers.

Dans ce travail on étudie cette question lorsque le groupe G est le produit direct $H_8 \times C_2$ d'un groupe de quaternion d'ordre 8 et d'un groupe cyclique d'ordre 2 ; le choix de ce groupe au lieu du groupe H_{32} de [Co] est guidé par l'étude faite dans [Sw4] et des considération d'effectivité des calculs.

Dans [Sw4] (théorème IV, §15 et §16) il est montré que le groupe des classes projectives $C\ell(\mathbb{Z}[G])$ est isomorphe à $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et qu'il y a quarante classes d'isomorphisme de ces $\mathbb{Z}[G]$-modules de rang 1 dont quatre sont stablement libres. Il résulte du même article que tout groupe G d'ordre strictement inférieur à 16 possède la propriété de simplification. Le groupe que l'on considère est en quelque sorte minimal pour le problème. On se propose de démontrer :

Théorème 1. *Chacune des quatre classes d'isomorphisme de $\mathbb{Z}[H_8 \times C_2]$-module stablement libre peut être représentée par une infinité d'anneaux d'entiers.*

Le premier chapître donne les notations et les grandes lignes de la méthode suivie, utilisant à la fois les produits fibrés et les discriminants. On utilise une factorisation de discriminants basée sur une décomposition de la trace introduite dans [Ma1].

L'étude de l'anneau des entiers d'une extension galoisienne de $\mathbb{Q}$ de groupe $H_8 \times C_2$ nécessite de connaître précisément la structure galoisienne des idéaux ambiges de certains sous-corps.

Les chapitres II et III décrivent des bases normales d'idéaux ambiges dans des extensions de $\mathbb{Q}$ de groupe de Galois isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (dans toute extension galoisienne modérément ramifiée les idéaux ambiges sont des modules galoisiens projectifs [U] prop. I-3). On aurait pu utiliser le chapitre I, mais il a paru plus rapide de procéder directement.

Le chapitre IV reprend avec quelques modifications le travail de Witt [W] sur la construction des extensions galoisiennes de $\mathbb{Q}$ de groupe H_8. Ces résultats sont utiles pour produire des exemples et construire de manière explicite, lorsqu'elles existent, des bases normales de l'anneau de leurs entiers ou de certains idéaux ambiges.

Le chapitre V est consacré à la détermination de bases normales pour les idéaux ambiges des extensions construites au chapitre précédent. Pour l'essentiel le critère est celui de [Ma1], le chapitre précédent permet de le compléter par un algorithme.

Le chapitre VI donne la description du groupe des classes de $G = H_8 \times C_2$ et des classes d'isomorphisme des $\mathbb{Z}[G]$-modules de rang un stablement libres. Il s'agit d'un extrait des paragraphes 15 et 16 de [Sw4]. Il a paru nécessaire de rappeler ces résultats techniques car c'est sur eux que reposent en définitive les identifications.

Le chapitre VII applique les précédents aux anneaux d'entiers des extensions galoisiennes de $\mathbb{Q}$ de groupe de Galois $H_8 \times C_2$. On donne l'algorithme de détermination d'une classe et on en déduit que si une classe est représentée par un anneau d'entiers elle l'est une infinité de fois. On illustre la démarche en étudiant les anneaux des entiers des corps composés de deux corps quaternioniques purs (définition en IV-4) contenant $\mathbb{Q}(\sqrt{1001}, \sqrt{2805})$. Ces corps sont au nombre de 28, on constate que chaque structure est représentée par un anneau d'entiers : trois le sont six fois et une l'est dix fois, ce qui assure la démonstration du théorème en composant ces corps avec des corps quadratiques de discriminant premier à ppcm(1001, 2805).

Les calculs ont été effectués avec Pari [P].

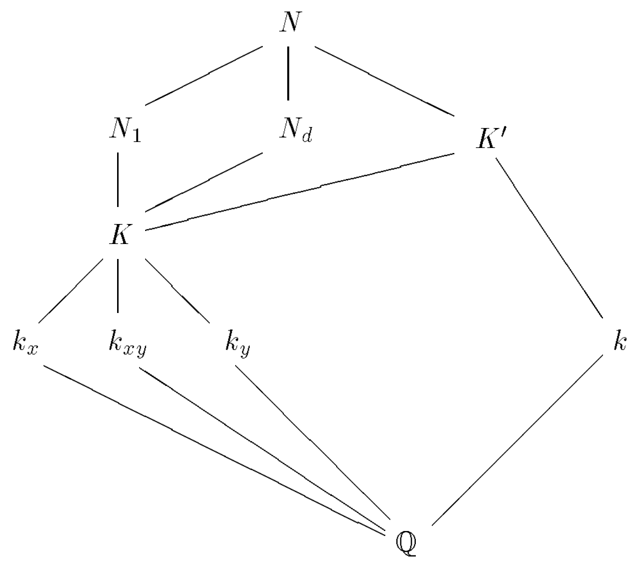
I. Généralités

I.1. **Groupes et extensions.** Le groupe C_2 est engendré par s, H_8 l'est par les éléments x, y vérifiant les relations $x^4 = e$, $x^2 = y^2$, $xyx^{-1} = y^{-1}$. Le centre de $G = H_8 \times C_2$ a pour générateurs x^2 et s, $\{e, x^2\}$ est le sous-groupe dérivé.

Soit $N/\mathbb{Q}$ une extension galoisienne de groupe $G = H_8 \times C_2$. Le sous-corps de N formé des invariants par H_8 est appelé k, il existe un entier d non divisible par un carré tel que $k = \mathbb{Q}(\sqrt{d})$. Le sous-corps des invariants par C_2 est noté N_1. Le sous-corps de N_1 invariant par x^2 est noté K, celui invariant par x (resp. y, xy) est k_x (resp. k_y, k_{xy}). Le corps N est une extension biquadratique bicyclique de K. On note K' le composé Kk, c'est la sous-extension abélienne maximale de $\mathbb{Q}$ incluse dans N son groupe de Galois sur $\mathbb{Q}$ est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$.

Le quotient de G par le sous-groupe distingué $\{e, sx^2\}$ est engendré par les classes de x et de y qui vérifient les mêmes relations que x et y, il est isomorphe au groupe H_8. Le sous-corps N_d de N quadratique sur K formé des éléments de N invariants par sx^2 est aussi une extension quaternionique de $\mathbb{Q}$.

Pour chaque corps de nombres L, on note $\mathcal{O}_L$ son anneau des entiers. Pour un réseau $\mathcal{L}$, muni d'une forme bilinéaire non dégénérée $\mathcal{T}$ on note $\Delta_{\mathcal{T}}$ son discriminant. Dans les cas particuliers de $\mathcal{O}_N$ (resp. $\mathcal{O}_{N_1}$, $\mathcal{O}_{N_d}$, $\mathcal{O}_K$), munis de la forme trace des corps correspondants, on note Δ (resp. Δ_1, Δ_d, Δ_K). Le diagramme des corps est indiqué ci-dessous :



Le groupe G est produit direct de deux groupes, ses représentations irréductibles sur $\mathbb{C}$ sont obtenues par tensorisation de celles de chacun des deux groupes. On obtient huit représentations de degré un qui sont celles de Gal($K'/\mathbb{Q}$), une représentation irréductible ψ_1 de degré 2 (soit χ_1 son caractère) qui se factorise par le groupe de Galois Gal($N_1/\mathbb{Q}$) et une représentation irréductible ψ_d de degré 2 (soit χ_d son caractère) qui se factorise par le groupe de Galois Gal($N_d/\mathbb{Q}$) : cette dernière est le produit tensoriel de ψ_1 avec la représentation irréductible non triviale de noyau Gal(N/k).

On suppose $N/\mathbb{Q}$ modérément ramifiée, son anneau des entiers $\mathcal{O}_N$ stablement libre. Cela implique que

$$\mathcal{O}_{N_1} \approx \Big(\mathbb{Z}[G]/(1-s)\Big) \otimes_{\mathbb{Z}[G]} \mathcal{O}_N \quad \text{et} \quad \mathcal{O}_{N_d} \approx \Big(\mathbb{Z}[G]/(1-sx^2)\Big) \otimes_{\mathbb{Z}[G]} \mathcal{O}_N$$

sont stablement libres, donc libres ([Ma1] Th. II-1). On sait que ces deux dernières conditions équivalent à $W(\chi_1) = W(\chi_d) = 1$ ($W(\chi_i)$ étant la constante de l'équation fonctionnelle de la fonction d'Artin étendue $\Lambda(\ ,\chi_i)$ associée à χ_i [F1]).
Réciproquement, si ces deux conditions sont vérifiées, la classe $[\mathcal{O}_N]$ est l'élément neutre de $C\ell(\mathbb{Z}[G])$ (voir [F4] Ch I §5 et 6 ou [T]).

On veut connaître les classes d'isomorphisme représentées par $\mathcal{O}_N$ dans la classe des modules stablement libres; celle de $\mathbb{Z}[G]$ s'obtient de manière évidente :

Il suffit de composer une extension galoisienne $N_1/\mathbb{Q}$ de groupe de Galois H_8 dont l'anneau des entiers est libre (J. Martinet montre comment le faire dans [Ma3]) avec une extension quadratique modérément ramifiée de discriminant premier à celui de $N_1/\mathbb{Q}$. On souhaite savoir si d'autres classes d'isomorphisme de $\mathbb{Z}[G]$-stablement libre de rang un sont ainsi représentées.

I.2. **Produits fibrés et classes d'isomorphisme.** Soit Γ un groupe fini et M un $\mathbb{Z}[\Gamma]$-module projectif stablement libre de rang 1 :

$$M \oplus \mathbb{Z}[\Gamma] \approx \mathbb{Z}[\Gamma] \oplus \mathbb{Z}[\Gamma].$$

Tous les groupes n'ont pas la propriété de simplification ([Sw2], [Sw3], [Sw4]). On peut déterminer dans un certain nombre de cas l'ensemble des classes d'isomorphisme de tels modules. On retrouve plusieurs fois la situation suivante : le centre de Γ contient un élément s d'ordre 2. Soit $H = \Gamma/\{1, s\}$. Les éléments $(1+s)$ et $(1-s)$ engendrent des idéaux bilatères de $\mathbb{Z}[\Gamma]$. L'algèbre quotient $\mathbb{Z}[\Gamma]/(1-s)$ est isomorphe à $\mathbb{Z}[H]$, on note $\mathcal{A}$ l'algèbre $\mathbb{Z}[\Gamma]/(1+s)$ d'où les diagrammes commutatifs :

$$\begin{array}{ccc} \mathbb{Z}[\Gamma] & \longrightarrow & \mathcal{A} \\ \downarrow & & \downarrow \\ \mathbb{Z}[H] & \longrightarrow & \mathbb{F}_2[H] \end{array} \qquad \begin{array}{ccc} M & \longrightarrow & M/(1+s)M \\ \downarrow & & \downarrow \\ M/(1-s)M & \longrightarrow & M/((1-s)M+(1+s)M) \end{array}$$

Le second se déduisant du premier en tensorisant par M.

Le module M est cohomologiquement trivial. En particulier le noyau de la trace $\mathrm{Tr} : m \mapsto (1+s)m$ est égal à $(1-s)M$ et donc $M/(1-s)M = M/\ker\Big(\mathrm{Tr}\Big)$ est isomorphe à l'image de la trace : $(1+s)M$. La nullité du groupe $H^0(\{1,s\}, M)$ dit que $(1+s)M$ est aussi $M^{\{1,s\}}$ (les éléments de M invariants par $< s >$); c'est un $\mathbb{Z}[H]$-module stablement libre de rang un.

D'autre part, comme s est dans le centre de Γ, $m \mapsto (1-s)m$ est un morphisme de $\mathbb{Z}[\Gamma]$-modules dont le noyau est formé des éléments invariants par s dont on vient de voir que c'est $(1+s)M$; on en déduit que $M/(1+s)M$ est isomorphe à $(1-s)M$. Le second diagramme devient :

$$\begin{array}{ccc} M & \longrightarrow & (1-s)M \\ \downarrow & & \downarrow \\ (1+s)M \approx M^{\{1,s\}} & \longrightarrow & M/(1-s),(1+s) \approx M^{\{1,s\}}/2 \end{array}$$

On suppose, ce qui est le cas dans les applications que nous avons en vue, que $M^{\{1,s\}}$ est $\mathbb{Z}[H]$-libre de rang un et que $(1-s)M$ est $\mathcal{A}$-libre de rang un. Ces deux modules ont donc des groupes d'automorphismes égaux respectivement à $\mathbb{Z}[H]^*$ et $\mathcal{A}^*$.

Réciproquement, étant donné un $\mathcal{A}$-module M_1 libre de rang un, M_2 un $\mathbb{Z}[H]$-module libre de rang un et un isomorphisme φ de $M_1/2$ sur $M_2/2$:

$$\begin{array}{ccc} & & M_2 \\ & & \downarrow \\ M_1 & \longrightarrow & M_1/2 \xrightarrow{\varphi} \approx M_2/2 \end{array}$$

La propriété de recollement de Milnor [M] montre qu'il est possible de compléter ce diagramme avec un $\mathbb{Z}[\Gamma]$-module localement libre de rang un : $M(M_1, M_2, \varphi)$. L'ensemble des classes d'isomorphisme des $\mathbb{Z}[\Gamma]$-modules de rang un vérifiant ces hypothèses est en bijection [Sw3] avec l'ensemble des doubles classes
$\mathrm{im}\Big(\mathbb{Z}[H]^*\Big)\backslash \mathbb{F}_2[H]^*/\ \mathrm{im}\Big(\mathcal{A}^*\Big)$ où im( ) désigne l'image dans $\mathbb{F}_2[H]^*$.

I.3. Un cas particulier. On conserve les notations et hypothèses de la seconde section et on suppose que $L/\mathbb{Q}$ est une extension galoisienne de groupe de Galois Γ. On note F le sous-corps de L formé des éléments invariants par s. On suppose que le module M est un idéal ambige $\mathcal{J}$ de $L/\mathbb{Q}$ (dont on connaît la décomposition en produit d'idéaux premiers) qui vérifie les mêmes hypothèses que dans la section précédente :

$$\begin{array}{ccc} \mathcal{I} & \longrightarrow & (1-s)\mathcal{I} \\ \downarrow & & \downarrow \\ \mathcal{I}^{\{1,s\}} & \longrightarrow & \mathcal{I}^{\{1,s\}}/2 \approx \mathbb{F}_2[H] \end{array}$$

Connaissant la décomposition en idéaux premiers de $\mathcal{J}$, il n'est pas difficile de déterminer $\mathcal{J}^{\{1,s\}}$.

On obtient également des précisions sur $(1-s)\mathcal{J}$. Tout d'abord c'est un $\mathcal{O}_F$-module de rang un. Il existe un élément γ entier de F tel que $L = F\Big(\sqrt{\gamma}\Big)$. L'élément $\sqrt{\gamma}$ est un entier de L qui appartient au noyau de la trace de L sur F. De ceci résulte l'existence d'un idéal fractionnaire $\mathfrak{A}$ de F tel que $(1-s)\mathcal{J} = \mathfrak{A}\sqrt{\gamma}$. La détermination de $\mathfrak{A}$ est un pas important dans la connaissance de $(1-s)\mathcal{I}$. Elle est favorisée par la remarque suivante que l'on emprunte à [Ma1] :

On note $\mathcal{D}$ le discriminant de $L/\mathbb{Q}$, D celui de $F/\mathbb{Q}$. Soit T, T', T'' trois formes bilinéaires symétriques définies respectivement sur L, F, $(1-s)L$ par :

$$T(x,y) = \mathrm{Tr}_{L/\mathbb{Q}}(xy) \quad T'(x,y) = \mathrm{Tr}_{F/\mathbb{Q}}(xy) \quad T''(x,y) = \mathrm{Tr}_{F/\mathbb{Q}}(xy)$$

La dernière ayant un sens car si $x = (1-s)m$, $y = (1-s)n$ le produit xy invariant par s appartient à F. Les sous-espaces vectoriels F et $(1-s)L$ sont orthogonaux pour la forme T. On écrit $x = \dfrac{x+s(x)}{2} + \dfrac{x-s(x)}{2}$,

$y = \dfrac{y+s(y)}{2} + \dfrac{y-s(y)}{2}$ et on a :

$$\begin{aligned} T(xy) &= \frac{1}{4}\Big(T\Big((x+s(x))(y+s(y))\Big) + T\Big((x-s(x))(y-s(y))\Big)\Big) \\ &= \frac{1}{4}\Big(\mathrm{Tr}_{L/\mathbb{Q}}\Big((x+s(x))(y+s(y))\Big) + \mathrm{Tr}_{L/\mathbb{Q}}\Big((x-s(x))(y-s(y))\Big)\Big) \\ &= \frac{1}{2}\Big(\mathrm{Tr}_{F/\mathbb{Q}}\Big((x+s(x))(y+s(y))\Big) + \mathrm{Tr}_{F/\mathbb{Q}}\Big((x-s(x))(y-s(y))\Big)\Big) \end{aligned}$$

soit pour la décomposition orthogonale (relative à T) de $L = F \oplus (1-s)L$: $T = \frac{1}{2}\Big(T' \oplus T''\Big)$. Calculons l'indice dans $\mathcal{J}$ de $\mathcal{J}^{\{1,s\}} \oplus (1-s)\mathcal{J}$, la formule $x = \dfrac{x+s(x)}{2} + \dfrac{x-s(x)}{2}$ dit que c'est une puissance de 2. Localisons en 2, comme 2 n'est pas ramifié dans L/F cela entraîne que $\mathcal{J}_{(2)}$ possède une $\mathcal{O}_{F_{(2)}}[\{1,s\}]$-base normale formée d'un α et de son conjugué $s(\alpha)$: $\mathcal{J}_{(2)} = \mathcal{O}_{F_{(2)}}\alpha \oplus \mathcal{O}_{F_{(2)}}s(\alpha)$. On peut récrire cette décomposition : $\mathcal{O}_{F_{(2)}}(\alpha + s(\alpha)) \oplus \mathcal{O}_{F_{(2)}}\Big(\frac{(\alpha+s(\alpha))-(\alpha-s(\alpha))}{2}\Big)$ ce qui prouve que $\mathcal{J}^{\{1,s\}} \oplus (1-s)\mathcal{J}$ est d'indice $2^{[F:\mathbb{Q}]}$ dans $\mathcal{J}$. On a donc :

$$\begin{aligned} \Delta_T(\mathcal{J}) &= 2^{2[F:\mathbb{Q}]}\Delta_T(\mathcal{J}^{\{1,s\}} \oplus (1-s)\mathcal{J}) \\ &= 2^{2[F:\mathbb{Q}]}\frac{1}{2}^{[L/\mathbb{Q}]}\Delta_{T'\oplus T''}(\mathcal{J}^{\{1,s\}} \oplus (1-s)\mathcal{J}) \\ &= \Delta_{T'}(\mathcal{J}^{\{1,s\}})\Delta_{T''}((1-s)\mathcal{J}) \end{aligned}$$

On sait par ailleurs que $\Delta_T(\mathcal{J}) = N_{L/\mathbb{Q}}(\mathcal{J})^2\mathcal{D}$, et que $\Delta_{T'}(\mathcal{J}^{\{1,s\}}) = N_{F/\mathbb{Q}}\Big(\mathcal{J}^{\{1,s\}}\Big)^2 D$. D'où la formule :

$$N_{L/\mathbb{Q}}(\mathcal{J})^2\mathcal{D} = N_{F/\mathbb{Q}}\Big(\mathcal{J}^{\{1,s\}}\Big)^2 D\,\Delta_{T''}((1-s)\mathcal{J}) \tag{1}$$

qui donne $\Delta_{T''}((1-s)\mathcal{J})$ sur lequel nous avons d'autres informations dans chacun des cas envisagés.

II. Base normale d'un idéal ambige d'une extension quadratique

Soit $k = \mathbb{Q}(\sqrt{d})$, $d \equiv 1 \mod 4$ un corps quadratique modérément ramifié et $\mathcal{I}$ un idéal ambige de k. On écrit $d = \epsilon \displaystyle\prod_{i=1}^{s} p_i$, $\epsilon = \pm 1$, $p_i > 0$ et $\mathcal{I} = n \displaystyle\prod_{i \in T \subset [1,\ldots,s]} \mathfrak{p}_i$ avec $n \in \mathbb{Z}, \mathfrak{p}_i^2 = (p_i)$. On peut supposer $n = 1$. La structure, bien connue, des idéaux d'un corps quadratique permet d'énoncer :

Lemme 2. *L'idéal $\mathcal{I}$ admet une base normale dont un générateur est* $\omega_{\mathcal{I}} = \dfrac{\left(\prod_{i\in T} p_i\right) + \sqrt{d}}{2}$.

Preuve. Soit $\omega'_{\mathcal{I}} = \Big(\prod_{i\in T} p_i - \sqrt{d}\Big)/2$ et L le réseau $\mathbb{Z}\omega_{\mathcal{I}} + \mathbb{Z}\omega'_{\mathcal{I}}$. Ce réseau est un idéal entier de O_k : le produit des p_i ($i \in T$) étant impair, le réseau est constitué d'entiers algébriques. Il suffit de vérifier qu'il est stable par multiplication par $(1+\sqrt{d})/2$, pour cela :

$$\begin{aligned}
\frac{1+\sqrt{d}}{2}\omega_{\mathcal{I}} &= \Big(\prod_{i\in T} p_i + \prod_{i\in T} p_i\sqrt{d} + \sqrt{d} + \epsilon\prod_{i=1}^{s} p_i\Big)/4\\
&= \Big[\frac{1+\epsilon\prod_{\substack{j\in[1,\dots,s]\\ j\notin T}} p_j}{4}\Big](\omega_{\mathcal{I}} + \omega'_{\mathcal{I}}) + \Big[\frac{\prod_{i\in T} p_i + 1}{4}\Big](\omega_{\mathcal{I}} - \omega'_{\mathcal{I}})\\
&= \Big(\frac{1+\epsilon\prod_{\substack{j\in[1,\dots,s]\\ j\notin T}} p_j + 1 + \prod_{j\in T} p_j}{4}\Big)\omega_{\mathcal{I}}\\
&\quad + \Big(\frac{1+\epsilon\prod_{\substack{j\in[1,\dots s]\\ j\notin T}} p_j - 1 - \prod_{j\in T} p_j}{4}\Big)\omega'_{\mathcal{I}}
\end{aligned}$$

Le produit d de tous les p_i par ϵ étant congru à 1 mod 4, les deux produits partiels sont impairs congrus entre eux modulo 4. Les coefficients sont donc entiers. Il en va de même pour $\frac{1+\sqrt{d}}{2}\omega'_{\mathcal{I}}$. Le réseau L est un idéal. La construction du réseau montre à l'évidence qu'il est inclus dans $\mathcal{I}$; son discriminant pour la trace dans $k/\mathbb{Q}$ est :

$$\begin{vmatrix} \prod_{i\in T} p_i & \omega_{\mathcal{I}} \\ \prod_{i\in T} p_i & \omega'_{\mathcal{I}} \end{vmatrix}^2 = \epsilon\Big(\prod_{j\in T} p_j\Big)^2 d$$

égal à celui de $\mathcal{I}$ d'où l'égalité du réseau et de l'idéal. □

III. Idéal ambige d'une extension biquadratique bicyclique

Soit $K/\mathbb{Q}$ une extension biquadratique bicyclique de groupe $V_4 = \{e, x, y, xy\}$; pour chaque $g \neq e$ de V_4, on note k_g le sous-corps de K formé des éléments invariants par g. On suppose $K/\mathbb{Q}$ modérément ramifiée. Soit d_g l'entier non divisible par un carré tel que $k_g = \mathbb{Q}(\sqrt{d_g})$, les d_g sont des entiers congrus à 1 modulo 4. Si $\delta = \mathrm{pgcd}(d_x, d_y)$ on note $\delta_x = d_x/\delta$, $\delta_y = d_y/\delta$ et on a $d_{xy} = d_x d_y/\delta^2 = \delta_x\delta_y$.

Si le premier p divise δ_x, son groupe de ramification est $\mathrm{Gal}(K/k_y)$ et p n'est pas ramifié dans $k_y/\mathbb{Q}$.

Si le premier p divise δ_y, son groupe de ramification est $\mathrm{Gal}(K/k_x)$ et p n'est pas ramifié dans $k_x/\mathbb{Q}$.

Si le premier p divise δ, son groupe de ramification est $\mathrm{Gal}(K/k_{xy})$ et p n'est pas ramifié dans $k_{xy}/\mathbb{Q}$.
On note $\mathfrak{R}_x$ (resp. $\mathfrak{R}_y$, $\mathfrak{R}_{xy}$) l'ensemble des premiers p ramifiés dans K/k_x (resp. K/k_y, K/k_{xy}) ; ces ensembles sont disjoints. Un idéal ambige $\mathcal{I}$ de $K/\mathbb{Q}$ est de la forme :

$$\mathcal{I} = n\Big(\prod_{p_i\in T_x\subset\mathfrak{R}_x}\ \prod_{\mathfrak{P}_i|p_i}\mathfrak{P}_i\Big)\Big(\prod_{p_j\in T_y\subset\mathfrak{R}_y}\ \prod_{\mathfrak{P}_j|p_j}\mathfrak{P}_j\Big)\Big(\prod_{p_\ell\in T_{xy}\subset\mathfrak{R}_{xy}}\ \prod_{\mathfrak{P}_\ell|p_\ell}\mathfrak{P}_\ell\Big),\quad n\in\mathbb{Q}.$$

La ramification modérée de $K/\mathbb{Q}$ implique que ces idéaux ambiges sont des $\mathbb{Z}[V_4]$-modules projectifs ([U] prop. I-3). Le groupe des classes projectives de $\mathbb{Z}[V_4]$ est réduit à son élément neutre [S], les idéaux ambiges $\mathcal{I}$ ont donc des bases normales. On les construit en partant du cas où les $\mathfrak{R}_g$ sont vides (cas de l'anneau des entiers) de la façon suivante :

Si $\delta \equiv 1$ modulo 4, on construit le corps modérément ramifié $\mathbb{Q}(\sqrt{\delta_x}, \sqrt{\delta_y}, \sqrt{\delta})$, ce corps est le composé de trois sous-corps quadratiques de discriminants 2 à 2 premiers entre eux et congrus à 1 modulo 4. Son anneau des entiers admet une base normale $\dfrac{(1+\sqrt{\delta_x})(1+\sqrt{\delta_y})(1+\sqrt{\delta})}{8}$ dont la trace sur K donne $\omega = \dfrac{1+\sqrt{d_x}+\sqrt{d_y}+\sqrt{d_{xy}}}{4}$.

Si $d \equiv 3$ modulo 4, on remplace δ par $\delta' = -\delta$ et on pose $m = d_x/\delta'$, $n = d_y/\delta'$, on procède alors de la même manière et on obtient $\omega = \dfrac{1-\sqrt{d_x}-\sqrt{d_y}-\sqrt{d_{xy}}}{4}$, ω peut être remplacé par $\pm g(\omega)$, $g \in V_4$ (les $\pm g$ sont les seules unités de $\mathbb{Z}[V_4]$).

Soit $L/\mathbb{Q}$ une extension abélienne de groupe de Galois Γ. Pour chaque $\theta \in L$ et chaque caractère χ de Γ, on définit la résolvante de Lagrange de θ et χ dans $L/\mathbb{Q}$ par l'expression :

$$<\theta,\chi>_{L/\mathbb{Q}} = \sum_{\gamma\in\Gamma}\gamma(\theta)\chi(\gamma^{-1}).$$

Les calculs sont basés sur les propriétés élémentaires des résolvantes de Lagrange : la linéarité par rapport au premier argument, les relations $<g(\theta),\chi>_{L/\mathbb{Q}} = \chi(g) <\theta,\chi>_{L/\mathbb{Q}}$ et, si le noyau de χ contient le groupe de Galois de L/F, $<\theta,\chi>_{L/\mathbb{Q}} = <\mathrm{Tr}_{L/F(\theta)},\chi>_{F/\mathbb{Q}}$ (cette dernière résolvante étant calculée dans l'extension $F/\mathbb{Q}$ pour le caractère de $\mathrm{Gal}(F/\mathbb{Q})$ dont le relèvement à $\mathrm{Gal}(L/\mathbb{Q})$ donne χ).

Soit $\omega_{\mathcal{I}}$ une base normale de $\mathcal{I}$, on peut l'écrire : $\omega_{\mathcal{I}} = a_e\omega + a_x x(\omega) + a_y y(\omega) + a_{xy} xy(\omega)$ les $a_g \in \mathbb{Z}$. On va déterminer ces coefficients en calculant de deux façons différentes les résolvantes de Lagrange :

$$<\omega_{\mathcal{I}},\chi>_{K/\mathbb{Q}} = \omega_{\mathcal{I}}\chi(e) + x(\omega_{\mathcal{I}})\chi(x^{-1}) + y(\omega_{\mathcal{I}})\chi(y^{-1}) + xy(\omega_{\mathcal{I}})\chi((xy)^{-1})$$

de $\omega_{\mathcal{I}}$ associées aux caractères χ de V_4. Outre χ_0 (le caractère trivial) ces caractères sont : χ_x (resp. χ_y, resp. χ_{xy}) défini par $\chi_x(x) = 1$, $\chi_x(y) = -1$ (resp. $\chi_y(x) = -1$, $\chi_y(y) = 1$; resp. $\chi_{xy}(x) = -1$, $\chi_{xy}(y) = -1$).

Pour le caractère χ_0, on obtient : $< \omega_{\mathcal{I}}, \chi_0 >= \sum_{g\in V_4} a_g \operatorname{Tr}(\omega) = a_e + a_x + a_y + a_{xy}$. C'est la trace dans $K/\mathbb{Q}$ de $\omega_{\mathcal{I}}$ elle engendre $\mathcal{I}\cap\mathbb{Q}$ (car le $\mathbb{Z}[G]$-module $\mathcal{I}$ est cohomologiquement trivial) ce qui donne une relation :

$$(2) \quad a_e + a_x + a_y + a_{xy} = \pm\Big(\prod_{p_i\in T_x\subset\mathfrak{R}_x} p_i\Big)\Big(\prod_{p_j\in T_y\subset\mathfrak{R}_y} p_j\Big)\Big(\prod_{p_\ell\in T_{xy}\subset\mathfrak{R}_{xy}} p_\ell\Big).$$

On note π_0 le membre de droite. Pour le caractère χ_x, on obtient :

$$\begin{aligned} < \omega_{\mathcal{I}}, \chi_x >_{K/\mathbb{Q}} &= a_0 < \omega, \chi_x >_{K/\mathbb{Q}} + a_x < x(\omega), \chi_x >_{K/\mathbb{Q}} \\ &\qquad + a_y < y(\omega), \chi_x >_{K/\mathbb{Q}} + a_{xy} < xy(\omega), \chi_x >_{K/\mathbb{Q}} \\ &= (a_e + a_x - a_y - a_{xy}) < \omega, \chi_x >_{K/\mathbb{Q}} \end{aligned}$$

Le calcul de $< \omega, \chi_x >_{K/\mathbb{Q}}$, en remplaçant ω par son expression, donne $\sqrt{d_x}$ si $\delta \equiv 1 \bmod 4$, $-\sqrt{d_x}$ si $\delta \equiv 3 \bmod 4$. On obtient aussi : $< \omega_{\mathcal{I}}, \chi_x >_{K/\mathbb{Q}}= \Big(\omega_{\mathcal{I}} + x(\omega_{\mathcal{I}})\Big) - \Big(y(\omega_{\mathcal{I}}) + xy(\omega_{\mathcal{I}})\Big)$ or $\omega_{\mathcal{I}} + x(\omega_{\mathcal{I}})$ est une base normale de $\mathcal{I}\cap k_x = \operatorname{Tr}_{K/k_x}(\mathcal{I})$, idéal entier de k_x ambige dans $k_x/\mathbb{Q}$. Déterminons la décomposition de cet idéal en procédant localement.

Un idéal qui n'est pas dans $T_x \cup T_y \cup T_{xy}$ ne figure pas dans la trace.

Soit $\mathfrak{P}_i$ figurant dans la décomposition de $\mathcal{I}$, $(p_i) = \mathbb{Z}\cap\mathfrak{P}_i$ sous $\mathfrak{P}_i$ dans $\mathbb{Z}$ et $\mathfrak{p}_i = k_x \cap \mathfrak{P}_i$.

Si $\mathfrak{P}_i$ est ramifié dans dans K/k_x, sa trace sur k_x est $\mathfrak{p}_i$; si p_i est inerte dans $k_x/\mathbb{Q}$, $\mathfrak{p}_i = (p_i)$; si p_i est décomposé dans $k_x/\mathbb{Q}$, $y(\mathfrak{P}_i)$ divise $\mathcal{I}$ et $y(\mathfrak{p}_i)$ divise aussi $\operatorname{Tr}_{K/k_x}(\mathcal{I})$ dans les deux cas apparaît le facteur p_i.

Si $\mathfrak{P}_i$ est ramifié dans dans K/k_g avec $g \neq x$, (p_i) est ramifié dans $k_x/\mathbb{Q}$; $\mathfrak{P}_i$ est soit inerte, soit décomposé dans K/k_x (mais alors son conjugué $x(\mathfrak{P}_i)$ et donc le produit $\mathfrak{P}_i x(\mathfrak{P}_i) = \mathfrak{p}_i$ figure dans $\mathcal{I}$) la trace de $\mathcal{I}$ est donc exactement divisible par $\operatorname{Tr}_{K/k_x}(\mathfrak{p}_i\mathcal{O}_K) = \mathfrak{p}_i$. On obtient ainsi :

$$\operatorname{Tr}_{K/k_x}(\mathcal{I}) = \prod_{p_i\in T_x} p_i \prod_{p_j\in T_y\cup T_{xy}} \mathfrak{p}_j .$$

Le lemme 1 nous donne une base normale de cet idéal :

$$\pm\Big(\prod_{p_i\in T_x} p_i\Big)\frac{\prod_{p_j\in T_y\cup T_{xy}} p_j \pm \sqrt{d_x}}{2}.$$

D'où la seconde expression de $< \omega_{\mathcal{I}}, \chi_x >_{K/\mathbb{Q}}= \pm\prod_{p_i\in T_x} p_i\sqrt{d_x}$ qui donne par comparaison avec la première :

$$(3) \qquad a_e + a_x - a_y - a_{xy} = \pm\prod_{p_i\in T_x} p_i .$$

On note π_x le membre de droite. De la même manière, on obtient avec χ_y et χ_{xy} :

$$(4) \qquad \begin{cases} a_e - a_x + a_y - a_{xy} & = \pm \prod_{p_j \in T_y} p_j \\ a_e - a_x - a_y + a_{xy} & = \pm \prod_{p_\ell \in T_{xy}} p_\ell \end{cases}$$

On note π_y (resp. π_{xy}) le premier (resp. second) membre de droite. Si on remplace $\omega_{\mathcal{I}}$ par son opposé, on change les seconds membres en leurs opposés. Si on remplace $\omega_{\mathcal{I}}$ par $y(\omega_{\mathcal{I}})$, on remplace $< \omega_{\mathcal{I}}, \chi_x >_{K/\mathbb{Q}}$ et $< \omega_{\mathcal{I}}, \chi_{xy} >_{K/\mathbb{Q}}$ par leurs opposés sans changer $< \omega_{\mathcal{I}}, \chi_0 >_{K/\mathbb{Q}}$ ni $< \omega_{\mathcal{I}}, \chi_y >_{K/\mathbb{Q}}$. Les nombres premiers intervenant dans les produits étant tous impairs, on peut supposer que π_0 et π_x sont congrus à 1 modulo 4 et il reste deux signes qui ne sont pas précisés. La solution du système obtenu est :

$$a_e = \frac{\pi_0 + \pi_x + \pi_y + \pi_{xy}}{4} \qquad a_x = \frac{\pi_0 + \pi_x - \pi_y - \pi_{xy}}{4}$$
$$a_y = \frac{\pi_0 - \pi_x + \pi_y - \pi_{xy}}{4} \qquad a_e = \frac{\pi_0 - \pi_x - \pi_y + \pi_{xy}}{4}$$

Comme a_y et a_{xy} doivent être entiers, il faut que $\pi_y \equiv \pi_{xy}$ modulo 4, ce qui laisse un choix, (correspondant à une éventuelle conjugaison par x, qui donc n'influerait ni sur π_0 ni sur π_x).

Si on reporte les expressions de a_e, a_x, a_y, a_{xy} dans $\omega_{\mathcal{I}}$ on obtient :

$$(5) \quad \omega_{\mathcal{I}} = \begin{cases} (\pi_0 + \pi_x\sqrt{d_x} + \pi_y\sqrt{d_y} + \pi_{xy}\sqrt{d_{xy}})/4 & \text{si } \delta \equiv 1 \mod 4 \\ (\pi_0 - \pi_x\sqrt{d_x} - \pi_y\sqrt{d_y} - \pi_{xy}\sqrt{d_{xy}})/4 & \text{si } \delta \equiv 3 \mod 4. \end{cases}$$

Notons que :

$$(6) \qquad \mathrm{Tr}_{K/\mathbb{Q}}(\omega_{\mathcal{I}}^2) = \frac{\pi_0^2 + \pi_x^2 d_x + \pi_y^2 d_y + \pi_{xy}^2 d_{xy}}{4}.$$

Exemples numériques :

On donne ici des bases normales d'idéaux utilisées dans la dernière partie. On considère le corps biquadratique $\mathbb{Q}(\sqrt{1001}, \sqrt{2805})$, on note $k_x = \mathbb{Q}(\sqrt{1001})$, $k_y = \mathbb{Q}(\sqrt{2805})$ et $k_{xy} = \mathbb{Q}(\sqrt{23205})$, soit $d_x = 1001 = 7.11.13$, $d_y = 2805 = 3.5.11.17$, $d_{xy} = 23205 = 3.5.7.13.17$. On a donc $\mathcal{R}_x = \{3, 5, 17\}$, $\mathcal{R}_y = \{7, 13\}$, $\mathcal{R}_{xy} = \{11\}$. Une base normale de $\mathcal{O}_K$ est engendrée par $\omega = (1 - \sqrt{d_x} - \sqrt{d_y} - \sqrt{d_{xy}})/4$. Avec les notations de cette section on obtient des bases normales suivantes pour les idéaux ambiges qui sont utilisés par la suite :

$\mathcal{I} = 5$,

d'où $\pi_e = 5$, $\pi_x = 5$, $\pi_y = 1$, $\pi_{xy} = 1$ ce qui donne $a_e = 3$, $a_x = 2$, $a_y = 0$, $a_{xy} = 0$.

$\mathcal{I} = 13$,

d'où $\pi_e = 13$, $\pi_x = 1$, $\pi_y = 13$, $\pi_{xy} = 1$ qui donne $a_e = 7$, $a_x = 0$, $a_y = 6$, $a_{xy} = 0$.
$\mathcal{I} = 17$,
d'où $\pi_e = 17$, $\pi_x = 17$, $\pi_y = 1$, $\pi_{xy} = 1$ qui donne $a_e = 9$, $a_x = 8$, $a_y = 0$, $a_{xy} = 0$.
$\mathcal{I} = 21 = 3.7$,
d'où $\pi_e = 21$, $\pi_x = -3$, $\pi_y = 7$, $\pi_{xy} = -1$ qui donne $a_e = 6$, $a_x = 3$, $a_y = 8$, $a_{xy} = 4$.
$\mathcal{I} = 65 = 5.13$,
d'où $\pi_e = 65$, $\pi_x = 5$, $\pi_y = 13$, $\pi_{xy} = 1$ qui donne $a_e = 21$, $a_x = 14$, $a_y = 18$, $a_{xy} = 12$.
$\mathcal{I} = 85 = 5.17$,
d'où $\pi_e = 85$, $\pi_x = 85$, $\pi_y = 1$, $\pi_{xy} = 1$ qui donne $a_e = 43$, $a_x = 42$, $a_y = 0$, $a_{xy} = 0$.
$\mathcal{I} = 105 = 3.5.7$,
d'où $\pi_e = 105$, $\pi_x = -15$, $\pi_y = -7$, $\pi_{xy} = 1$ qui donne $a_e = 21$, $a_x = 24$, $a_y = 28$, $a_{xy} = 32$.
$\mathcal{I} = 221 = 13.17$,
d'où $\pi_e = 221$, $\pi_x = 17$, $\pi_y = 13$, $\pi_{xy} = 1$ qui donne $a_e = 63$, $a_x = 56$, $a_y = 54$, $a_{xy} = 48$.
$\mathcal{I} = 273 = 3.7.13$,
d'où $\pi_e = 273$, $\pi_x = -3$, $\pi_y = 91$, $\pi_{xy} = -1$ qui donne $a_e = 90$, $a_x = 45$, $a_y = 92$, $a_{xy} = 46$.
$\mathcal{I} = 357 = 3.7.17$,
d'où $\pi_e = 357$, $\pi_x = -51$, $\pi_y = -7$, $\pi_{xy} = 1$ qui donne $a_e = 75$, $a_x = 78$, $a_y = 100$, $a_{xy} = 104$.
$\mathcal{I} = 1105 = 5.13.17$,
d'où $\pi_e = 1105$, $\pi_x = 85$, $\pi_y = 13$, $\pi_{xy} = 1$ qui donne $a_e = 301$, $a_x = 294$, $a_y = 258$, $a_{xy} = 252$.
$\mathcal{I} = 1365 = 3.5.7.13$,
d'où $\pi_e = 1365$, $\pi_x = -15$, $\pi_y = -91$, $\pi_{xy} = 1$ qui donne $a_e = 315$, $a_x = 360$, $a_y = 322$, $a_{xy} = 368$.
$\mathcal{I} = 1785 = 3.5.7.17$,
d'où $\pi_e = 1785$, $\pi_x = -255$, $\pi_y = -7$, $\pi_{xy} = 1$ qui donne $a_e = 381$, $a_x = 384$, $a_y = 508$, $a_{xy} = 512$.
$\mathcal{I} = 4641 = 3.7.13.17$,
d'où $\pi_e = 4641$, $\pi_x = -51$, $\pi_y = -91$, $\pi_{xy} = 1$ qui donne $a_e = 1125$, $a_x = 1170$, $a_y = 1150$, $a_{xy} = 1196$.

IV. Construction des extensions quaternioniques d'après [W]

Le groupe H_8 est extension du groupe de Klein V_4 par un groupe d'ordre 2. On note x, y deux générateurs du groupe de Klein et $\{\pm 1\}$ le groupe d'ordre 2. On a donc une suite exacte :

$$1 \longrightarrow \{\pm 1\} \longrightarrow H_8 \longrightarrow V_4 \longrightarrow 1. \tag{7}$$

Si on prend dans H_8 des représentants i_e, i_x, i_x, i_{xy} de e x, y, xy avec la convention $i_e = e$ le groupe est caractérisé par le système de facteurs bien connu $\zeta_{g,h}$ défini par :

$$i_g i_h = \zeta_{g,h} i_{gh} \qquad g, h \in V_4 \qquad \zeta_{g,h} \in \{\pm 1\}. \tag{8}$$

On se donne une extension biquadratique $K/\mathbb{Q}$ de groupe $V_4 = \{e, x, y, xy\}$, pour tout élément $g \neq e$ de V_4, on note k_g le sous-corps de K formé des éléments invariants par g. Dans k_x (resp. k_y) on choisit l'élément ξ_x, (resp. ξ_y) tel que $\xi_x^2 = \mathfrak{d}_x \in \mathbb{Z}$ (resp. $\xi_y^2 = \mathfrak{d}_y \in \mathbb{Q}$), entier non divisible par un carré. On pose $\xi_{xy} = \xi_x \xi_y$, $\mathfrak{d}_{xy} = \mathfrak{d}_x \mathfrak{d}_y$ (le changement de notations par rapport au chapitre III facilite l'écriture des formules).

La formule (8) définit un deux-cocycle de V_4 à valeurs dans le groupe $\{\pm 1\}$, qui s'injecte dans K^*, on obtient un 2-cocycle ζ de V_4 à valeurs dans K^* et on peut construire l'algèbre $\mathfrak{A}$, produit croisé de K par ce 2-cocycle : $\mathfrak{A} = (\zeta, K)$. L'existence d'un plongement de K dans une extension à groupe de Galois H_8 dépend de la décomposition de cette algèbre (cf. IV-1).

L'algèbre $\mathfrak{A}$ est un K-espace vectoriel de dimension 4 avec une base que l'on note par abus $i_e = 1$, i_x, i_y, i_{xy} et où le produit se déduit par $\mathbb{Q}$-linéarité des relations :

$$\forall g \, \forall h \in V_4, \quad i_g i_h = \zeta_{g,h} i_{gh}, \qquad \forall g \in V_4 \; \forall x \in K \quad i_g x = g(x) i_g. \tag{9}$$

Comme le cocycle est en fait à valeurs dans $\mathbb{Q}$, l'algèbre $\mathfrak{A}$ contient la $\mathbb{Q}$-algèbre de dimension 4 de même base et définie par les mêmes relations ; c'est l'algèbre des quaternions usuels $\left(\frac{-1, -1}{\mathbb{Q}}\right)$.

Posons $\xi_e = 1$ et construisons pour chaque g de V_4 l'élément $\xi_g i_g$ de $\mathfrak{A}$. Les relations (9) montrent que

$$\begin{aligned} (\xi_x i_x)^2 &= -\mathfrak{d}_x, & (\xi_y i_y)^2 &= -\mathfrak{d}_y, \\ (\xi_{xy} i_{xy})^2 &= -\mathfrak{d}_{xy}, & (\xi_x i_x)(\xi_y i_y) &= -(\xi_y i_y)(\xi_x i_x) \end{aligned}$$

ce qui prouve que l'algèbre $\mathfrak{A}$ contient aussi la $\mathbb{Q}$-algèbre $\mathfrak{D} = \left(\frac{-\mathfrak{d}_x, -\mathfrak{d}_y}{\mathbb{Q}}\right)$. On constate également par l'utilisation des relations (9) que les éléments de $\left(\frac{-1, -1}{\mathbb{Q}}\right)$ et $\mathfrak{D}$ commutent entre eux et qu'ils engendrent $\mathfrak{A}$, on a donc $\mathfrak{A} = \left(\frac{-1, -1}{\mathbb{Q}}\right) \times \mathfrak{D}$. La comparaison des dimensions montre que $\mathfrak{A}$ est isomorphe au produit tensoriel de ses deux sous-algèbres.

IV.1. **Un critère de plongement (d'après [M-N]).** Rappelons ce critère de plongement dans le contexte qui nous intéresse, on introduit les $\mathbb{F}_2$-espaces vectoriels $\Gamma_K = K^*/K^{*2}$, $\Gamma_{\mathbb{Q}} = \mathbb{Q}^*/\mathbb{Q}^{*2}$ sur lesquels opère V_4 ; la démonstration du lemme suivant est sans difficulté :

Lemme 3. *Les extensions de degré 2 de K, galoisiennes sur $\mathbb{Q}$, s'identifient aux droites du sous-espace vectoriel Γ_K^G des vecteurs de Γ_K laissés fixes par G.*

On a une application évidente de $\Gamma_{\mathbb{Q}}$ dans $\Gamma_K^{V_4}$ et deux suites exactes :

$$1 \longrightarrow K^{*2} \longrightarrow K^* \longrightarrow \Gamma_K \longrightarrow 1$$

$$1 \longrightarrow \{\pm 1\} \longrightarrow K^* \longrightarrow K^{*2} \longrightarrow 1$$

qui donnent les suites de cohomologie :

$$1 \longrightarrow \mathbb{Q}^* \cap K^{*2} \longrightarrow \mathbb{Q}^* \longrightarrow \Gamma_K^{V_4} \longrightarrow H^1(V_4, K^{*2}) \longrightarrow 1$$

$$1 \longrightarrow H^1(V_4, K^{*2}) \longrightarrow H^2(V_4, \{\pm 1\}) \longrightarrow H^2(V_4, K^*)$$

Ce qui conduit, par comparaison, à la suite exacte :

$$1 \longrightarrow \Gamma_K^{V_4} / \operatorname{im}(\Gamma_{\mathbb{Q}}) \simeq H^1(V_4, K^{*2}) \xrightarrow{\varphi} H^2(V_4, \{\pm 1\}) \xrightarrow{\psi} H^2(V_4, K^*)$$

où φ est un homomorphisme de connexion et ψ se déduit de l'inclusion naturelle $\{\pm 1\} \subset K^*$. On peut expliciter $\operatorname{im}(\varphi) = \ker(\psi)$: soit $a \in K^*$ représentant un élément de $\Gamma_K^{V_4}$, pour tout g de V_4, choisissons $\eta_g \in K^*$ tel que $a^{-1}\sigma(a) = \eta_g^2$, l'application de $V_4 \times V_4$ dans $\{\pm 1\}$ définie par $\zeta_{g,h} = \eta_{gh}^{-1}\eta_g g(\eta_h)$ est un 2-cocycle dont la classe dans $H^2(V_4, \{\pm 1\})$ dépend uniquement de la classe de a dans $\Gamma_K^{V_4}/\operatorname{im}(\Gamma_{\mathbb{Q}})$. On en déduit donc :

Proposition 4. *Le plongement de K dans une extension quaternionique de degré 8 a lieu si et seulement si l'algèbre $\mathfrak{A}$ est décomposée.*

IV.2. **Décomposition de l'algèbre $\mathfrak{A}$.** Comme les algèbres introduites dans 1 sont des algèbres de quaternions, leurs invariants locaux valent 1/2 ou 0 dans $\mathbb{Q}/\mathbb{Z}$; ces invariants locaux s'ajoutent par produit tensoriel d'algèbres. On en déduit que l'algèbre $\mathfrak{A} = \left(\frac{-1,-1}{\mathbb{Q}}\right) \times \mathfrak{D}$ est décomposée (c'est à dire isomorphe à $M_4(\mathbb{Q})$) si et seulement si $\mathfrak{D}$ est isomorphe à $\left(\frac{-1,-1}{\mathbb{Q}}\right)$, c'est ce qui conduit au critère de Witt [W] retouvé par A. Fröhlich [F1] et qui s'exprime ainsi :

Théorème 5. *Le plongement de K dans une extension quaternionique de degré 8 a lieu si et seulement si pour tout premier p divisant $\mathfrak{d}_x\mathfrak{d}_y$ on a l'égalité $(-1,\mathfrak{d}_x)_p(-1,\mathfrak{d}_y)_p(\mathfrak{d}_x,\mathfrak{d}_y)_p = 1$ où $(\ ,\ )_p$ désigne le symbole de Hilbert en p.*

Remarque 1. La formule du produit montre alors que l'on a la même relation pour la place à infini : les formes quadratiques $X^2 + Y^2 + Z^2$ et $\mathfrak{d}_x X^2 + \mathfrak{d}_y Y^2 + \mathfrak{d}_{xy} Z^2$ sont équivalentes sur $\mathbb{Q}$.

Rappelons un résultat classique extrait de [La] chapitre 3. Soit $A = \left(\dfrac{a,b}{\mathbb{Q}}\right)$ une algèbre de quaternions, comme $\mathbb{Q}$-espace vectoriel elle possède une base 1, i_a, i_b, i_{ab} et le produit est défini en étendant par linéarité les relations $i_a^2 = a$, $i_b^2 = b$, $i_a i_b = i_{ab} = -i_b i_a$. Sur cette algèbre il y a une anti-involution :

$$\overline{u + vi_a + wi_b + si_{ab}} = u - vi_a - wi_b - si_{ab},$$

on appelle quaternions purs et on note A_0 les éléments transformés en leur opposés par l'anti-involution. La norme réduite $\bar{c}c$ d'un élément c munit A d'une structure d'espace quadratique pour laquelle A_0 est orthogonal à $\mathbb{Q}$.

Proposition 6 ([La] Ch 3, prop 2.5). *Pour deux algèbres de quaternions* $A = \left(\dfrac{a,b}{\mathbb{Q}}\right)$, $A' = \left(\dfrac{a',b'}{\mathbb{Q}}\right)$ *les propriétés suivantes sont équivalentes :*

(i) A et A' sont isomorphes,

(ii) A et A' sont des espaces quadratiques isométriques,

(iii) les espaces quadratiques A_0 et A'_0 sont isométriques.

Dans notre cas, soit φ un isomorphisme entre les algèbres de quaternions $\left(\dfrac{-1,-1}{\mathbb{Q}}\right)$ et $\mathfrak{D}$. Posons $v_x = \varphi(\xi_x i_x)$, $v_y = \varphi(\xi_y i_y)$, $v_{xy} = \varphi(\xi_{xy} i_{xy})$ ce sont des images de quaternions purs, donc des quaternions purs. On peut écrire :

$$\begin{aligned} v_x &= p_{x,x} i_x + p_{x,y} i_y + p_{x,xy} i_{xy}, \\ v_y &= p_{y,x} i_x + p_{y,y} i_y + p_{y,xy} i_{xy}, \\ v_{xy} &= p_{xy,x} i_x + p_{xy,y} i_y + p_{xy,xy} i_{xy}. \end{aligned}$$

On obtient ainsi une matrice $M = (p_{g,h})_{g,h \in V_4 - \{e\}}$ de passage de la base i_x, i_y, i_{xy} à v_x, v_y, v_{xy}. Puisque les $\xi_x i_x$, $\xi_y i_y$, $\xi_{xy} i_{xy}$ forment une base orthogonale, il en est de même de la nouvelle. La matrice de la forme quadratique norme réduite dans cette base est la matrice diagonale $(\mathfrak{d}_x, \mathfrak{d}_y, \mathfrak{d}_{xy})$; puisque φ est un isomorphisme d'algèbre $v_{xy} = v_x v_y$ et la nouvelle base est de même sens que i_x, i_y, i_{xy}. La matrice M a donc pour déterminant $\mathfrak{d}_x \mathfrak{d}_y$.

Montrons que l'on peut apporter une précision sur les coefficients $p_{g,h}$, à priori dans $\mathbb{Q}$. L'algèbre $\mathfrak{D}$ est construite à partir des entiers $\mathfrak{d}_x$, $\mathfrak{d}_y$, en particulier le $\mathbb{Z}$-module :

$$\mathbb{Z} + \mathbb{Z}(\xi_x i_x) + \mathbb{Z}(\xi_y i_y) + \mathbb{Z}(\xi_{xy} i_{xy})$$

est un ordre de cette algèbre. Son image par φ est un ordre de $\left(\dfrac{-1,-1}{\mathbb{Q}}\right)$ inclus dans un ordre maximal. Or on sait que les idéaux à gauche de l'ordre de Hurwitz (ordre maximal) sont tous principaux. Il en résulte que tous les ordres maximaux sont conjugués ([Che],[E]) ; on peut donc, quite à composer φ avec un automorphisme intérieur de $\left(\frac{-1,-1}{\mathbb{Q}}\right)$, supposer que les coefficients de la matrice M sont des entiers. On les obtient en remarquant que :

$$M^t M = \begin{pmatrix} \mathfrak{d}_x & 0 & 0 \\ 0 & \mathfrak{d}_y & 0 \\ 0 & 0 & \mathfrak{d}_{xy} \end{pmatrix}$$

ce qui revient à décomposer $\mathfrak{d}_x$ et $\mathfrak{d}_y$ en sommes de trois carrés d'entiers formant des vecteurs orthogonaux de $\mathbb{R}^3$ et à prendre comme troisième colonne le produit vectoriel des deux premières, nous procédons désormais de cette façon. Il reste un certain arbitraire dans le signe et l'ordre des coefficients de v_x et v_y ; on reviendra sur cette question en IV-4.

IV.3. **Construction du plongement.** On suit les calculs de [W] (une interprétation et une généralisation en sont donnés dans [Cr] en termes d'algèbres de Clifford).

On construit une nouvelle algèbre $K \otimes \left(\frac{-1,-1}{\mathbb{Q}}\right) = \left(\frac{-1,-1}{K}\right)$. Soit, dans cette algèbre, les éléments

$j_1 = 1$, $j_x = v_x/\xi_x$, $j_y = v_y/\xi_y$, $j_{xy} = v_{xy}/\xi_{xy}$.

On a les relations :

$j_x^2 = j_y^2 = j_{xy}^2 = -1$, $j_x j_y = j_{xy} = -j_x j_y$

Les éléments j_1, j_x, j_y, j_{xy} forment une K-base de $\left(\frac{-1,-1}{K}\right)$ avec le même système de facteurs que 1, i_x, i_y, i_{xy}.

La réalisation du plongement de K dans une extension quaternionique repose sur les propriétés de l'élément $C = \frac{1}{2}(1 + i_x^{-1} j_x + i_y^{-1} j_y + i_{xy}^{-1} j_{xy})$; on le développe en exprimant les j_h suivant la base 1, i_x, i_y, i_{xy}

$$C = \frac{1}{2}\Big(1+p_{x,x}/\xi_x+p_{y,y}/\xi_y+p_{xy,xy}/\xi_{xy}\Big) + \frac{1}{2}\Big(p_{xy,y}/\xi_{xy} - p_{y,xy}/\xi_y\Big) i_x + \frac{1}{2}\Big(p_{x,xy}/\xi_x - p_{xy,y}/\xi_{xy}\Big) i_y + \frac{1}{2}\Big(p_{y,x}/\xi_y - p_{x,y}/\xi_x\Big) i_{xy} \tag{10}$$

De la définition de C résulte immédiatement que :

$$\begin{aligned} i_h^{-1} C j_h &= \frac{1}{2}(i_h^{-1} j_h + i_h^{-1} i_x^{-1} j_x j_h + i_h^{-1} i_y^{-1} j_y j_h + i_h^{-1} i_{xy}^{-1} j_{xy} j_h) \\ &= \frac{1}{2}(i_h^{-1} j_h + (i_x i_h)^{-1} j_x j_h + (i_y i_h)^{-1} j_x j_h + (i_{xy} i_h)^{-1} j_{xy} j_h) \end{aligned}$$

Soit, puisque les systèmes de facteurs sont les mêmes :

$$i_h^{-1} C j_h = C. \tag{11}$$

On désigne par $\overline{C}$ le transformé de C par l'anti-involution ; la norme réduite $N(C) = C\overline{C} \in K$, la trace réduite $\mathrm{Tr}(C) = C + \overline{C} \in K$: comme $C\overline{C} \in K$ on a $N(C) = C\overline{C} = \dfrac{1}{2}\mathrm{Tr}(C\overline{C})$. De la définition des j_h résulte que $N(j_h) = 1$, $\mathrm{Tr}(j_h) = 0$ et donc $\overline{j}_h = j_h^{-1} = -j_h$, comme pour les i_h. Puisque la conjugaison est une anti-involution : $N(C) = \frac{1}{4}\mathrm{Tr}(C\sum_h j_h^{-1} i_h)$ mais d'après (11) $Cj_h^{-1} = i_h^{-1}C$, ce qui donne $N(C) = \frac{1}{4}\mathrm{Tr}(\sum_h i_h^{-1} C i_h) = \mathrm{Tr}(C)$ car la trace réduite est invariante par conjugaison.

Si on note $\gamma = N(C)$, on obtient d'après (10) :

$$\gamma = 1 + p_{x,x}/\xi_x + p_{y,y}/\xi_y + p_{xy,xy}/\xi_{xy} \neq 0 \tag{12}$$

car les éléments 1, $1/\xi_x$, $1/\xi_y$, $1/\xi_{xy}$ forment une $\mathbb{Q}$-base de $K/\mathbb{Q}$. L'élément C est donc inversible dans l'algèbre $\left(\dfrac{-1,-1}{K}\right)$ et la relation (11) se récrit :

$$C j_h C^{-1} = i_h. \tag{13}$$

Le groupe $\mathrm{Gal}(K/\mathbb{Q})$ opère sur l'algèbre $\left(\dfrac{-1,-1}{K}\right)$ par conjugaison des coefficients de 1, i_x, i_y, i_{xy}. Transformons le membre de gauche de (13) en remplaçant C par $i_g C^g$, on obtient $i_g C^g j_h \Big(C^g\Big)^{-1} i_g^{-1}$.

Si $g = h$, $j_g = v_g/\xi_g$, ξ_g et les coefficients de v_g (dans $\mathbb{Q}$) sont invariants par g, on a $j_g^g = j_g$ ce qui donne :

$$i_g C^g j_g^g \Big(C^{-1}\Big)^g i_g^{-1} = i_g \Big(C j_g C^{-1}\Big)^g i_g^{-1} = i_g i_g^g i_g^{-1} = i_g$$

Si $g \neq h$, $j_h = v_h/\xi_h$, les coefficients de v_h sont dans $\mathbb{Q}$, invariants par g alors que ξ_h est transformé en son opposé on a donc $j_h^g = -j_h$ ce qui donne

$$\begin{aligned} i_g C^g j_h \Big(C^{-1}\Big)^g i_g^{-1} &= -i_g C^g j_h^g \Big(C^{-1}\Big)^g i_g^{-1} = -i_g \Big(C j_h C^{-1}\Big)^g i_g^{-1} \\ &= -i_g i_h^g i_g^{-1} = -i_g i_h i_g^{-1} = i_h i_g i_g^{-1} = i_h. \end{aligned}$$

Il en résulte que les automorphismes intérieurs associés à $\Big(i_g C^g\Big)^{-1} C$ laissent invariants 1, j_x, j_y, j_{xy} ; il existe donc des éléments $\delta_g \in K$ tels que $i_g C^g = \delta_g C$, les relations (10) et (12) permettent de calculer explicitement les δ_g.

Nous avons l'identité :

$$\Big(CC^{-g}\Big)\Big(CC^{-h}\Big)^g\Big(CC^{-gh}\Big)^{-1} = 1 \quad \forall g\ \forall h \in V_4$$

qui devient

$$1 = \delta_g^{-1} i_g \Big(\delta_h^{-1} i_h\Big)^g (\delta_{gh}^{-1} i_{gh})^{-1} = \delta_g^{-1}\delta_h^{-g}\zeta_{g,h}\delta_{gh}$$

soit

$$\delta_g \delta_h^g = \zeta_{g,h}\delta_{g,h}. \tag{14}$$

Si on revient à la définition de $\gamma = N(C)$ et que l'on prend la norme réduite des relations $C^g C^{-1} = i_g^{-1}\delta_g$, on obtient $\gamma^{g-1} = \delta_g^2$ ce qui avec la relation (14) montre que le corps $N_1 = K(\sqrt{\gamma})$ est une extension quaternionique.

Modifions l'écriture de γ :

$$\begin{aligned}\gamma &= 1 + p_{x,x}/\xi_x + p_{y,y}/\xi_y + p_{xy,xy}/\xi_{xy}\\ &= 1 + p_{x,x}\xi_x/\mathfrak{d}_x + p_{y,y}\xi_y/\mathfrak{d}_y + p_{xy,xy}\xi_{xy}/\mathfrak{d}_x\mathfrak{d}_y\\ &= \frac{1}{\mathfrak{d}_x\mathfrak{d}_y}\Big(\mathfrak{d}_x\mathfrak{d}_y + p_{x,x}\mathfrak{d}_y\xi_x + p_{y,y}\mathfrak{d}_x\xi_y + p_{xy,xy}\xi_{xy}\Big)\end{aligned}$$

Comme $\mathfrak{d}_x\mathfrak{d}_y$ est un carré dans K, on peut remplacer γ par l'entier algébrique :

$$\gamma_1 = \mathfrak{d}_x\mathfrak{d}_y + p_{x,x}\mathfrak{d}_y\xi_x + p_{y,y}\mathfrak{d}_x\xi_y + p_{xy,xy}\xi_{xy}. \tag{15}$$

IV.4. **Quelques remarques pratiques.** L'extension biquadratique K de $\mathbb{Q}$ étant donnée et plongeable dans un corps quaternionique, il existe des corps quaternioniques particuliers que A. Fröhlich ([F1]) appelle «purs» : ceux tels que si p est ramifié dans $N_1/\mathbb{Q}$, il l'est déjà dans $K/\mathbb{Q}$. On sait que si $N_1 = K(\sqrt{\gamma})$ est un tel corps, tous les autres sont de la forme $N_1^t = K(\sqrt{\gamma t})$ avec $t \in \mathbb{Z}$ (voir la démonstration donnée dans [Ma3] au début du paragraphe 2). De tels corps ne sont pas uniques et on peut en déterminer le nombre (voir [F1], Th. 4 et le corollaire). La construction de Witt en donne rapidement. En particulier, si $\mathfrak{d}_x$ et $\mathfrak{d}_y$ ne sont pas premiers entre eux il est pratique de remplacer γ_1 par $\gamma_1/\operatorname{pgcd}(\mathfrak{d}_x, \mathfrak{d}_y)$.

Comme on l'a laissé entendre plus haut, l'ordre et le signe des coefficients de v_x et de v_y n'est pas entièrement imposé. Voyons les conséquences qu'entraînent ces modifications.

Si on remplace $p_{x,x}$ par son opposé, cela impose de remplacer aussi $p_{y,x}$ par son opposé mais alors $p_{xy,xy}$ l'est aussi de manière automatique et γ devient $y(\gamma)$, l'extension reste la même.

Si on remplace $p_{x,y}$ par son opposé, cela impose de remplacer aussi $p_{y,y}$ par son opposé mais alors $p_{xy,xy}$ l'est aussi de manière automatique et γ devient $x(\gamma)$, l'extension reste la même.

Si on remplace $p_{x,xy}$ par son opposé, cela impose de remplacer aussi $p_{y,xy}$ par son opposé alors $p_{xy,xy}$ et γ ne changent pas.

Si on effectue une permutation des coefficients v_x, on effectue la même sur ceux de v_y, on obtient de nouveaux vecteurs orthogonaux v'_x, v'_y, v'_{xy} : nous avons construit un nouvel isomorphisme φ' de $\mathfrak{D}$ sur $\left(\dfrac{-1,-1}{\mathbb{Q}}\right)$, le théorème de Skolem-Nœther nous dit qu'il existe un élément ρ de $\left(\dfrac{-1,-1}{\mathbb{Q}}\right)$ (quitte à le multiplier par un entier, on peut le supposer dans l'ordre de Hurwitz) tel que pour tout c de $\mathfrak{D}$ $\varphi'(c) = \rho\varphi(c)\rho^{-1}$. On poursuit la construction par l'introduction de j'_x, j'_y, j'_{xy} puis de C' inversible vérifiant une relation (11′) :

$i_h^{-1}C'j_h' = C'$ pour tout h de V_4, et on pose $\gamma' = N(C')$. L'automorphisme intérieur de $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ s'étend à $\left(\frac{-1,-1}{k}\right)$ et transforme les j_h en les j_h'. Si on compare les relations (11) et (11′) on obtient $(C'^{-1}C)j_h(C^{-1}C') = j_h'$. La conjugaison intérieure par $C'^{-1}C$ dans $\left(\frac{-1,-1}{k}\right)$ a le même effet que celle par ρ. Il existe donc $\mu \in k$ tel que $C'^{-1}C = \mu\rho$ et en prenant la norme réduite $\gamma = \gamma'\mu^2 N(\rho)$. Le facteur μ^2 ne change pas l'extension. Comme $N(\rho)$ est un entier rationnel les corps quaternioniques construits à partir de γ et de $\gamma'/N(\rho)$ sont les mêmes. On peut préciser des choix d'éléments ρ associés à certaines des permutations :
$\rho = i + j$ $(i \mapsto j,\ j \mapsto i,\ k \mapsto -k)$; $\rho = j + k$ $(i \mapsto -i,\ j \mapsto k,\ k \mapsto j)$;
$\rho = 1 - i - j - k$ $(i \mapsto k, j \mapsto i,\ k \mapsto j)$ qui sont des éléments de normes réduites respectives 2, 2, 4.

V. Bases normales d'un idéal ambige d'une extension quadratique quaternionique

Soit $N_1/\mathbb{Q}$ une extension galoisienne de groupe de Galois isomorphe à H_8. On conserve les notations de I pour le groupe de Galois et les sous-corps de N_1. On suppose cette extension modérément ramifiée, ses idéaux ambiges sont donc des $\mathbb{Z}[H_8]$-modules projectifs. La caractérisation de [Ma1] qui permet de dire si l'anneau des entiers est ou non stablement libre se transpose aux idéaux ambiges ce qui, couplé avec la construction des extensions quaternioniennes rappelée dans IV, permet de construire explicitement les bases normales lorsqu'elles existent.

On note $\mathfrak{R}_x$ (resp. $\mathfrak{R}_y$, $\mathfrak{R}_{xy}$) l'ensemble des premiers p_i totalement ramifiés dans N_1/k_x (resp. N_1/k_y, N_1/k_{xy}) et $\mathfrak{R}'$ l'ensemble des premiers p_i ramifiés seulement dans N_1/K. Un idéal ambige $\mathcal{U}$ de $N_1/\mathbb{Q}$ est de la forme :
(16)

$$\mathcal{U} = n\Big(\prod_{\substack{\mathfrak{P}_i|p_i\\ p_i\in T_x\subset\mathfrak{R}_x}} \mathfrak{P}_i^{r_{p_i}}\Big)\Big(\prod_{\substack{\mathfrak{P}_j|p_j\\ p_j\in T_y\subset\mathfrak{R}_y}} \mathfrak{P}_j^{r_{p_j}}\Big)\Big(\prod_{\substack{\mathfrak{P}_\ell|p_\ell\\ p_\ell\in T_{xy}\subset\mathfrak{R}_{xy}}} \mathfrak{P}_\ell^{r_{p_\ell}}\Big)\Big(\prod_{\substack{\mathfrak{P}_u|p_u\\ p_u\in T'\subset\mathfrak{R}'}} \mathfrak{P}_u\Big),$$

les exposants appartenant à l'ensemble $\{1, 2, 3\}$ et $n \in \mathbb{Q}$. Le facteur n peut être supposé égal à 1. Ce que l'on fait dans ce qui suit.

Donnons quelques calculs auxiliaires utiles. Soit p un idéal ramifié dans $N_1/\mathbb{Q}$, $\mathfrak{P}$ un idéal premier de $\mathcal{O}_{N_1}$ au-dessus de p divisant (ainsi que ses conjugués) avec l'exposant r l'idéal ambige $\mathcal{U}$. On distingue plusieurs cas suivant l'indice de ramification et le degré résiduel de p. On a besoin de connaître l'intersection de $\mathcal{U}$ avec K (égale à la trace de $\mathcal{U}$ sur K) et les normes sur $\mathbb{Q}$ des différents idéaux premiers au-dessus de p.

Si on suppose l'indice de ramification de p dans N_1 égal à 4, soit :

$$\begin{cases} \text{cas (a)} & p\mathcal{O}_K = \mathfrak{p}^2, \qquad p\mathcal{O}_{N_1} = \mathfrak{P}^4 \\ \text{cas (b)} & p\mathcal{O}_K = \mathfrak{p}^2\mathfrak{p}'^2, \qquad p\mathcal{O}_{N_1} = \mathfrak{P}^4\mathfrak{P}'^4. \end{cases}$$

Dans le cas (a), nous avons :
$r = 1$: $\mathfrak{P} \cap K = \mathfrak{p}$, $r = 2$: $\mathfrak{P}^2 \cap K = \mathfrak{p} \cap K = \mathfrak{p}$, $r = 3$: $\mathfrak{P}^3 \cap K = \mathfrak{p}\mathfrak{P} \cap K = \mathfrak{p}^2 = (p)$;
de plus $N_{N_1/\mathbb{Q}}(\mathfrak{P}) = p^2 = N_{K/\mathbb{Q}}(\mathfrak{p})$.
Dans le cas (b), nous avons :
$r = 1$: $\mathfrak{P}\mathfrak{P}' \cap K = \mathfrak{p}\mathfrak{p}'$, $r = 2$: $\mathfrak{P}^2\mathfrak{P}'^2 \cap K = \mathfrak{p}\mathfrak{p}' \cap K = \mathfrak{p}\mathfrak{p}'$,
$r = 3$: $\mathfrak{P}^3\mathfrak{P}'^3 \cap K = \mathfrak{p}\mathfrak{p}'\mathfrak{P}\mathfrak{P}' \cap K = \mathfrak{p}^2\mathfrak{p}'^2 = (p)$;
de plus $N_{N_1/\mathbb{Q}}(\mathfrak{P}) = p$, $N_{N_1/\mathbb{Q}}(\mathfrak{P}\mathfrak{P}') = p^2$, $N_{K/\mathbb{Q}}(\mathfrak{p}) = p$, $N_{K/\mathbb{Q}}(\mathfrak{p}\mathfrak{p}') = p^2$.
Dans chacun des cas, $N_{N_1/\mathbb{Q}}(\mathcal{U})$ est divisible exactement par p^{2r}.
Dans les cas (a) et (b) si $r = 1, 2$ $N_{K/\mathbb{Q}}\Big(\mathrm{Tr}_{N_1/K}(\mathcal{U})\Big)$ est divisible exactement par p^2, et si $r = 3$ par p^4 .

Supposons l'indice de ramification de p dans N_1 égal à 2. Nous avons :

$$\begin{cases} \text{cas (c)} & p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}', \qquad p\mathcal{O}_{N_1} = \mathfrak{P}^2\mathfrak{P}'^2 \\ \text{cas (d)} & p\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4, \qquad p\mathcal{O}_{N_1} = \mathfrak{P}_1^2\mathfrak{P}_2^2\mathfrak{P}_3^2\mathfrak{P}_4^2. \end{cases}$$

Dans le cas (c), nous avons :
$\mathfrak{P} \cap K = \mathfrak{p}$, $\mathfrak{P}' \cap K = \mathfrak{p}'$, $\mathfrak{P}\mathfrak{P}' \cap K = \mathfrak{p}\mathfrak{p}' = (p)$,
de plus $N_{N_1/\mathbb{Q}}(\mathfrak{P}) = p^2 = N_{K/\mathbb{Q}}(\mathfrak{p})$, $N_{N_1/\mathbb{Q}}(\mathfrak{P}\mathfrak{P}') = p^4 = N_{K/\mathbb{Q}}(\mathfrak{p}\mathfrak{p}')$.
Dans le cas (d), nous avons :
$\mathfrak{P}_i \cap K = \mathfrak{p}_i$, $\Big(\prod_i \mathfrak{P}_i\Big) \cap K = \prod_i \mathfrak{p}_i = (p)$;
de plus $N_{N_1/\mathbb{Q}}(\mathfrak{P}) = p = N_{K/\mathbb{Q}}(\mathfrak{p})$, $N_{N_1/\mathbb{Q}}(\prod_i \mathfrak{P}_i) = p^4 = N_{K/\mathbb{Q}}(\prod_i \mathfrak{p}_i)$
Dans chacun des cas (c) et (d) $N_{N_1/\mathbb{Q}}(\mathcal{U})$ et $N_{K/\mathbb{Q}}\Big(\mathrm{Tr}_{N_1/K}(\mathcal{U})\Big)$ sont divisible exactement par p^4.

V.1. **Critère de base normale [Ma1].** La détermination de la structure de $\mathbb{Z}[H_8]$-module de $\mathcal{U}$ et, s'il est libre la construction de sa base normale, s'appuient sur le produit fibré suivant (cf. I-§2) et III.

$$(17) \qquad \begin{array}{ccc} \mathcal{U} & \longrightarrow & (1-x^2)\mathcal{U} \\ \big\downarrow & & \big\downarrow \\ \mathcal{U} \cap K & \longrightarrow & (\mathcal{U} \cap K)/2 \approx \mathbb{F}_2[V_4] \end{array}$$

La propriété de recollement de Milnor montre que $\mathcal{U}$ est $\mathbb{Z}[H_8]$-libre s'il est possible de trouver une base de $\mathcal{U} \cap K$ et une base de $(1 - x^2)\mathcal{U}$ qui ont même image dans $\mathbb{F}_2[V_4]$; on note $\mathcal{H}$ l'algèbre $\mathbb{Z}[H_8]/(1 + x^2)$, isomorphe à l'anneau des quaternions entiers. On trouve immédiatement ici que les classes d'isomorphisme sont représentées par les classes de $\mathbb{F}_2[V_4]^*/V_4$ qui sont celles de 1 et de $1+x+y$. C'est la caractérisation de [Ma1]. On détermine aisément $\mathcal{U}\cap K$ et on a vu dans le chapitre III comment en construire une base φ comme $\mathbb{Z}[V_4]$-module libre de rang un.

Si on connaît une base ψ de $(1-x^2)\mathcal{U}$ comme $\mathcal{H}$-module libre de rang un, la propriété de recollement revient à dire que si on peut la modifier de sorte que $\varphi\equiv\psi$ modulo 2, alors $\dfrac{\varphi-\psi}{2}$ est une base de $\mathcal{U}$ comme $\mathbb{Z}[H_8]$-module libre de rang un.

On reprend la formule (1) dans le cas où $L=N_1$, $F=K$ avec $\Gamma=H_8$, $s=x^2$; ceci détermine $\Delta_{T''}((1-x^2)\mathcal{U})$. Le $\mathcal{H}$-module $(1-x^2)\mathcal{U}$ est libre de rang un ce qui conduit à une autre expression de ce discriminant :

Soit $\mathcal{L}$ un $\mathcal{H}$-module libre de rang un inclus dans $(1-x^2)N$. Il possède une $\mathcal{H}$-base μ d'où l'on déduit une $\mathbb{Z}$-base : μ, $x(\mu)$, $y(\mu)$, $xy(\mu)$. On constate alors que si $g(\mu)$ et $h(\mu)$ sont deux éléments distincts de cette base $\mathrm{Tr}_{K/\mathbb{Q}}(g(\mu)h(\mu))=0$ et que les $\mathrm{Tr}_{K/\mathbb{Q}}(g(\mu^2))$ sont égaux à $\mathrm{Tr}_{K/\mathbb{Q}}(\mu^2)$. On a donc $\Delta_{T''}(\mathcal{L})=\mathrm{Tr}_{K/\mathbb{Q}}(\mu^2)^4$. La formule (1) nous donne $\mathrm{Tr}_{K/\mathbb{Q}}(\mu^2)$, au signe près.

Remarque 2. On connaît la valeur absolue de $\mathrm{Tr}_{K/\mathbb{Q}}(\mu^2)$. On connaît également son signe : si N_1 est réel μ^2 est totalement positif, il en est de même pour $\mathrm{Tr}_{K/\mathbb{Q}}(\mu^2)$; si N_1 est complexe la conjugaison complexe égale à x^2, transforme μ en son opposé : μ est imaginaire pur pour chaque plongement complexe et $\mathrm{Tr}_{K/\mathbb{Q}}(\mu^2)$ est négatif.

Lemme 7 ([Ma1]). *Si* $\mathcal{U}=\mathcal{O}_{N_1}$ *on a* $\mathrm{Tr}_{K/\mathbb{Q}}(\psi^2)=\epsilon\prod_{p\mid\Delta_1}p \mod 4$ *où* $\epsilon=1$ *si* N_1 *est réel,* -1 *sinon.*

Remarque 3. Ceci permet de calculer $\Delta_{T''}((1-x^2)\mathcal{U})$ et l'indice $[(1-x^2)\mathcal{O}_{N_1}:(1-x^2)\mathcal{U}]$.

Théorème 8. *L'idéal ambige* $\mathcal{U}$ *possède une* $\mathbb{Z}[H_8]$*-base normale si et seulement si* $\mathrm{Tr}_{K/\mathbb{Q}}(\varphi^2)\equiv\mathrm{Tr}_{K/\mathbb{Q}}(\psi^2)$ *modulo* 4.

Preuve. S'il y a une base normale on a $\varphi\equiv\psi$ modulo 2 ce qui implique $\varphi^2\equiv\psi^2$ modulo 4. Cette congruence est vérifiée par conjugaison et donc pour les traces.

S'il n'y a pas de base normale on peut supposer que l'on a $\psi\equiv\varphi+x(\varphi)+y(\varphi)$ modulo 2 ce que l'on peut encore écrire : $\psi\equiv\varphi+x(\varphi)+y(\varphi)+xy(\varphi)-xy(\varphi)=\tau-xy(\varphi)$; où τ, trace de φ, est un générateur de $\mathcal{U}\cap\mathbb{Q}=\mathrm{Tr}_{N_1/\mathbb{Q}}(\mathcal{U})$, c'est un entier impair. En élevant au carré on obtient $\psi^2\equiv\tau^2+xy(\varphi^2)-2\tau xy(\varphi)$ modulo 4. La congruence reste valable quand on prend la trace dans $K/\mathbb{Q}$ soit :

$$\begin{aligned}\operatorname{Tr}_{K/\mathbb{Q}}(\psi^2) &\equiv 4\tau^2 + \operatorname{Tr}_{K/\mathbb{Q}}(\varphi^2) - 2\tau^2 \equiv \operatorname{Tr}_{K/\mathbb{Q}}(\varphi^2) - 2\tau^2 \\ &\equiv -\operatorname{Tr}_{K/\mathbb{Q}}(\varphi^2) \ \text{ modulo } 4.\end{aligned}$$

□

Rappelons ce que donne ce critère dans le cas où $\mathcal{U}$ est l'anneau des entiers, en utilisant le lemme précédent et la formule (6).

Théorème 9 ([Ma1]). *L'anneau des entiers possède une base normale si et seulement si*

$$(1 + d_x + d_y + d_{xy})/4 \equiv \epsilon \prod_{p|\Delta_1} p \bmod 4,$$

où $\epsilon = 1$ *si* N_1 *est réel,* -1 *sinon.*

V.2. **Construction de ψ.** Il faut maintenant construire une base ψ de $(1-x^2)\mathcal{U}$ comme $\mathcal{H}$-module de rang 1. Commençons par le cas où $\mathcal{U} = \mathcal{O}_{N_1}$

On connaît, par la construction de l'extension quaternionique, un élément γ_1 tel que $N_1 = K(\sqrt{\gamma_1})$. Cet élément est un entier algébrique et il est de trace nulle sur K : il appartient à $(1 - x^2)\mathcal{O}_{N_1}$.

Considérons le $\mathcal{H}$-module libre $\mathcal{L}$ de base $\sqrt{\gamma_1}$. On sait que le discriminant de $\mathcal{L}$ pour T'' est égal à $\operatorname{Tr}_{K/\mathbb{Q}}(\gamma_1)^4$ que l'on connaît explicitement. On a l'inclusion de $\mathcal{L}$ dans $(1 - x^2)\mathcal{O}_{N_1}$ qui est aussi un $\mathcal{H}$-module libre. Soit ψ une $\mathcal{H}$-base de $(1 - x^2)\mathcal{O}_{N_1}$, on peut écrire $\sqrt{\gamma_1} = \lambda\psi$ avec $\lambda \in \mathcal{H}$, le discriminant de ce module pour T'' est égal à $\operatorname{Tr}_{K/\mathbb{Q}}(\psi^2)$ qui nous est connu par le lemme 7. Le quotient $\Delta_{T''}(\mathcal{L})/\Delta_{T''}((1 - x^2)\mathcal{O}_{N_1})$ est connu et il est égal au carré de l'indice de $\mathcal{L}$ dans $(1 - x^2)\mathcal{O}_{N_1}$, c'est à dire au carré de la norme de λ dans $\mathcal{H}$. On connaît par conséquent la norme réduite n de λ dans $\mathcal{H}$. La norme réduite dans $\mathcal{H}$ est une forme quadratique définie positive à coefficients entiers pour des valeurs entières des variables. Il n'y a qu'un nombre fini de possibilités pour λ. On teste les $\lambda^{-1}\sqrt{\gamma_1} = \overline{\lambda}/n\sqrt{\gamma_1}$; l'un d'entre eux doit être entier, notons le ψ. Le module $\mathcal{H}\psi$ est formé d'entiers, il est inclus dans $(1 - x^2)\mathcal{O}_{N_1}$ et a même discriminant que lui pour T'' : ils coïncident.

En pratique, on pose $\overline{\lambda} = \alpha + \beta i + \eta j + \mu ij$ $(\alpha^2 + \beta^2 + \eta^2 + \mu^2 = n)$, en prenant la même notation pour x, y et un de leurs prolongements $\overline{\lambda}\sqrt{\gamma_1} = \alpha\sqrt{\gamma_1} + \beta x(\sqrt{\gamma_1}) + \eta y(\sqrt{\gamma_1}) + \mu xy(\sqrt{\gamma_1})$. Le calcul de $g(\sqrt{\gamma_1})$ nécessite donc de trouver les $r_g \in K$ tels que $g(\gamma_1) = r_g^2\gamma_1$ (on peut alors contrôler que l'on a bien construit une extension quaternionique en vérifiant que r_x (resp. r_y, r_{xy}) est de norme -1 sur k_x (resp k_y, k_{xy})).

On considère les éléments $\left(\dfrac{\alpha + \beta r_x + \eta r_y + \mu r_{xy}}{n}\right)^2\gamma_1$ de K, cette détermination se faisant à conjugaison près, pour une décomposition donnée on peut fixer α et son signe. Ceci étant précisé, un et un seul quadruplet $(\alpha, \beta, \eta, \mu)$ convient. On a donc ψ^2; pour obtenir la base normale, il suffit de savoir à quel conjugué de ω est congru (modulo 2) ψ (où ω est le générateur de la base normale de $\mathcal{O}_K$ défini dans la section III). Une méthode rapide consiste à construire les polynôme irréductibles des $(g(\omega) - \psi)/2$.

Remarque 4. Lorsque $N/\mathbb{Q}$ est sauvagement ramifiée, son anneau des entiers est libre sur son ordre associé [Ma2]. Les méthodes mises en évidence ici s'appliquent de la même manière pour en construire une base.

Revenons à $(1 - x^2)\mathcal{U}$; c'est, tout comme $(1 - x^2)\mathcal{O}_{N_1}$, un $\mathcal{H}$-module projectif de rang un, donc libre; soit ϕ une base. L'inclusion de $\mathcal{U}$ dans $\mathcal{O}_{N_1}$ implique $(1 - x^2)\mathcal{U} \subset (1 - x^2)\mathcal{O}_{N_1}$, il existe $\rho \in \mathcal{H}$ tel que $\phi = \rho\psi$.

Le quotient des discriminants $\Delta_{T''}((1 - x^2)\mathcal{U})/\Delta_{T''}((1 - x^2)\mathcal{O}_{N_1})$ est le carré de l'indice de $(1-x^2)\mathcal{U}$ dans $(1-x^2)\mathcal{O}_{N_1}$ comme ces deux réseaux ont une structure de $\mathcal{H}$-module cet indice est égal à $N(\rho)$ où N est la norme dans $\mathcal{H}$. Comme précédemment cela détermine un nombre fini de choix pour ρ.

Pour chaque choix possible de ρ, on construit les éléments $\rho\psi$, $x(\rho\psi)$, $y(\rho\psi)$, $xy(\rho\psi)$ qui forment une $\mathbb{Z}$-base de $\mathcal{H}\rho\psi$. Si ce $\mathcal{H}$-module est inclus dans $(1-x^2)\mathcal{U}$, les calculs de discriminants montrent comme ci-dessus qu'il y a égalité.

Il faut et il suffit que l'on vérifie que chacun de ces éléments ν est dans $(1-x^2)\mathcal{U}$. Un tel ν est de la forme $u - x^2(u)$, $u \in \mathcal{U}$ si et seulement si il existe $v \in \ \mathrm{Tr}_{N_1/K}(\mathcal{U})$ tel que $\dfrac{v+\nu}{2} \in \mathcal{U}$. Les idéaux premiers $\mathfrak{P}$ divisant $\mathcal{U}$ étant ramifiés dans N_1/K, il faut et il suffit que $N_{N_1/K}\Big(\dfrac{v+\nu}{2}\Big) = \dfrac{v^2-\nu^2}{4} \in \mathcal{U} \cap K$. Cette propriété ne dépend que de la classe de $v \in K \cap \mathcal{U}$ modulo 2, une $\mathbb{Z}$-base de $K \cap \mathcal{U}$ est connue, un nombre fini de vérifications permet donc de répondre à la question de l'appartenance des ν à $(1 - x^2)\mathcal{U}$.

VI. Classes d'isomorphismes et groupes des classes pour $H_8 \times C_2$

Soit maintenant $G = H_8 \times C_2$. Appliquons la technique du chapître I avec G et le sous-groupe d'ordre 2 du centre engendré par s. Reprenons les diagrammes commutatifs du chapitre I avec M un $\mathbb{Z}[G]$-module localement libre de rang un :

(18)

$$\begin{array}{ccccccc}
\mathbb{Z}[H_8 \times C_2] & \longrightarrow & \mathbb{Z}[H_8] & \quad & M & \longrightarrow & (1-s)M \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\mathbb{Z}[H_8] & \longrightarrow & \mathbb{F}_2[H_8] & & M^{\{1,s\}} & \longrightarrow & M/(1-s),(1+s) \approx M^{\{1,s\}}/2
\end{array}$$

Les modules $(1-s)M$ et $M^{\{1,s\}}$ sont des $\mathbb{Z}[H_8]$-modules localement libres, donc libres [Ma1]. Leurs automorphismes forment un groupe isomorphe au groupe des éléments inversibles de $\mathbb{Z}[H_8]$ donc aux éléments $\{\pm g \mid g \in H_8\}$ ([Ma1] Th I-2 b) ; $M^{\{1,s\}}/2M^{\{1,s\}} \approx (1-s)M/2(1-s)M$ est isomorphe à $\mathbb{F}_2[H_8]$.

Réciproquement, si on se donne deux $\mathbb{Z}[H_8]$-modules libres M_1 et M_2 de rang un et un isomorphisme φ de $M_1/2M_1$ sur $M_2/2M_2$ le diagramme :

$$\begin{array}{ccc} & & M_1 \\ & & \downarrow \\ M_2 & \longrightarrow & M_1/2M_1 \overset{\varphi}{\approx} M_2/2M_2 \end{array}$$

permet de construire un $\mathbb{Z}[G]$-module localement libre $M(M_1, M_2, \varphi)$ par la propriété de recollement de Milnor ([M] §2, [Sw2] §4). On en déduit ([Sw4] lemme 16-1) :

Lemme 10. *L'ensemble des classes d'isomorphismes des $\mathbb{Z}[G]$-modules M projectifs de rang 1 tels que $M^{\{1,s\}}$, $(1-s)M$ sont des $\mathbb{Z}[H_8]$-modules libres est en bijection avec l'ensemble $H_8 \backslash \mathbb{F}_2[H_8]^*/H_8$. Cet ensemble admet pour représentants les* 10 *éléments suivants de $\mathbb{F}_2[H_8]$:*

(a) les 8 éléments $1+(x^2+1)(ax+by+cxy)$ *a, b, $c \in \mathbb{F}_2$,*

(b) $1+x+y$, $1+x+y+(x^2+1)xy$.

Le diagramme de gauche de (18) conduit également à une suite de Mayer-Vietoris ([M]§3)

$$\begin{aligned} K_1(\mathbb{Z}[G]) \to K_1(\mathbb{Z}[H_8]) \oplus K_1(\mathbb{Z}[H_8]) \to K_1(\mathbb{F}_2[H_8]) \xrightarrow{\partial} K_0(\mathbb{Z}[G]) \to \\ \to K_0(\mathbb{Z}[H_8]) \oplus K_0(\mathbb{Z}[H_8]) \to K_0(\mathbb{F}_2[H_8]) \end{aligned}$$

Comme $\mathbb{F}_2[H_8]$ est un anneau local $K_0(\mathbb{F}_2[H_8])$ est isomorphe à $\mathbb{Z}$, pour les autres $K_0(\ )$ le rang donne un isomorphisme entre $K_0(\ )$ et $\mathbb{Z} \oplus C\ell(\ )$ ce qui conduit à la suite exacte :

$$\begin{aligned} K_1(\mathbb{Z}[G]) \to K_1(\mathbb{Z}[H_8]) \oplus K_1(\mathbb{Z}[H_8]) \to K_1(\mathbb{F}_2[H_8]) \xrightarrow{\partial} C\ell(\mathbb{Z}[G]) \to \\ \to C\ell(\mathbb{Z}[H_8]) \oplus C\ell(\mathbb{Z}[H_8]) \to 0. \end{aligned}$$

On peut préciser la plupart des termes de cette suite exacte : $C\ell(\mathbb{Z}[H_8])$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ ([Ma1] th I-1 et II-1), on a rappelé dans le chapitre précédent pourquoi il y avait deux classes d'isomorphisme de $\mathbb{Z}[H_8]$-modules localement libres de rang un, le théorème II-1 de [Ma1] montre comment stablement isomorphe implique isomorphe (on pourrait aussi conclure par un calcul direct du groupe des classes utilisant les formules de [F2] ou de [F3]), l'anneau $\mathbb{F}_2[H_8]$ est local et la théorie des déterminants de Dieudonné montre que $K_1(\mathbb{F}_2[H_8])$ est isomorphe à $\mathbb{F}_2[H_8]^*_{ab}$, Keating a prouvé [K] que

le groupe $K_1(\mathbb{Z}[H_8])$ est isomorphe à H_{8ab}; enfin, en utilisant les formules de Fröhlich [F2], Swan [Sw4] montre que $C\ell(\mathbb{Z}[G])$ est isomorphe à :
$\mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ ce qui ramène à :

$$H_{8ab} \oplus H_{8ab} \to \mathbb{F}_2[H_8]^*_{ab} \xrightarrow{\partial} \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \to 0$$

qui devient

$$\mathbb{F}_2[H_8]^*_{ab}/\mathrm{image}(H_8) \xrightarrow{\partial} \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \to 0$$

Swan calcule $\mathbb{F}_2[H_8]^*_{ab}/\mathrm{image}(H_8)$ qu'il montre être isomorphe à $\mathbb{Z}/4\mathbb{Z}$, engendré par la classe de $1 + x + y$ ([Sw4] lemme 16-6). La comparaison des ordres montre que ce groupe s'injecte dans $C\ell(\mathbb{Z}[G])$ et est le noyau du morphisme suivant. Nous rappelons la démonstration car elle explicite les identifications qu'il faut faire ensuite.

Preuve. L'anneau $\mathbb{F}_2[H_8]$ est local, de cardinal 2^8, de corps résiduel $\mathbb{F}_2$; son groupe multiplicatif est donc d'ordre 2^7. Soit $V_4 = H_8/ < x^2 >$, pour les mêmes raisons $\mathbb{F}_2[V_4]^*$ est d'ordre 2^3, ses éléments sont tous d'ordre 2, il est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$ et engendré par les images de x, y, $1 + x + y$.

Le morphisme de $\mathbb{F}_2[H_8]^*$ dans $\mathbb{F}_2[V_4]^*$ est surjectif. Les éléments de $1 + (1 + x^2)\mathbb{F}_2[H_8]$ au nombre de 2^4 sont dans le noyau. Ils le décrivent en entier et ils sont tous d'ordre 2. Ce noyau est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^4$, ses éléments dans le centre de $\mathbb{F}_2[H_8]^*$ car ils commutent avec les éléments de H_8. Le quotient étant abélien, le noyau contient le sous-groupe dérivé.

Un commutateur $[a, b]$ ne dépend que des classes de a et b modulo le centre du groupe. On a la relation $a[b, c]a^{-1}[a, c] = [ab, c]$, les commutateurs étant dans le centre, elle devient $[a, c][b, c] = [ab, c]$. De ces deux remarques, on conclu que $[\ ,\ ]$ définit une forme bilinéaire de $\mathbb{F}_2[V_4]^* \times \mathbb{F}_2[V_4]^*$ dans $1 + (1 + x^2)\mathbb{F}_2[H_8]$. Par ailleurs, on connaît une base de $\mathbb{F}_2[V_4]^*$ comme $\mathbb{F}_2$-espace vectoriel : x, y, $1 + x + y$ l'ensemble des commutateurs se calcule, il est égal à $\{1 + (1 + x^2)(a + bx + cy + dxy)\ |b + c + d = 0\}$. C'est un sous-groupe d'ordre 8 de $1 + (1 + x^2)\mathbb{F}_2[H_8]$. On a donc :

$$1 \to \mathbb{Z}/2\mathbb{Z} \approx \frac{(1 + (1 + x^2)\mathbb{F}_2[H_8])}{[\mathbb{F}_2[H_8]^*, \mathbb{F}_2[H_8]^*]} \to \mathbb{F}_2[H_8]^*_{ab} \to \mathbb{F}_2[V_4]^* \to 1$$

Le groupe $\mathbb{F}_2[H_8]^*_{ab}$ est donc d'ordre 16. L'image de H_8 dans ce groupe est V_4 et reste V_4 dans $\mathbb{F}_2[V_4]^*$. Le quotient $\mathbb{F}_2[H_8]^*_{ab}/\mathrm{im}(H_8)$ est donc d'ordre 4. L'élément $(1 + x + y)^2 = 1 + (1 + x^2)xy$ ne s'écrit pas comme un commutateur, sa classe dans $\mathbb{F}_2[H_8]^*_{ab}$ est un carré non trivial. Le groupe est donc cyclique d'ordre 4 et l'image de $1 + x + y$ en est un générateur. □

On note $LL_1(\mathbb{Z}[G])$ (resp. $LL_1(\mathbb{Z}[H_8])$) l'ensemble des classes d'isomorphisme des $\mathbb{Z}[G]$ (resp. $\mathbb{Z}[H_8]$) modules localement libres de rang 1. À chaque module localement libre de rang 1, on associe sa classe dans le groupe des classes projectives. Le diagramme (18) conduit à :

$$\begin{array}{ccccc} LL_1(\mathbb{Z}[G]) & \longrightarrow & LL_1(\mathbb{Z}[H_8]) & \times & LL_1(\mathbb{Z}[H_8]) \\ \downarrow & & \downarrow & & \downarrow \\ C\ell(\mathbb{Z}[G]) & \longrightarrow & C\ell(\mathbb{Z}[H_8]) & \times & C\ell(\mathbb{Z}[H_8]) \end{array}$$

Soit M un $\mathbb{Z}[G]$-module stablement libre de rang 1. Ses images M_1 et M_2 sont libres. Il est représenté dans $\mathrm{Im}(H_8)\backslash\mathbb{F}_2[H_8]^*/\mathrm{Im}(H_8)$ par les éléments décrits dans le lemme 10.
Ceux de la forme $1+(1+x^2)(ax+by+cxy)$ avec $a+b+c=0$ sont des commutateurs de $\mathbb{F}_2[H_8]^*$ leur image dans $C\ell(\mathbb{Z}[G])$ est nulle.
L'élément $1+x+y$ a pour image un générateur du noyau du morphisme de $C\ell(\mathbb{Z}[G])$ dans le produit $C\ell(\mathbb{Z}[H_8])\times C\ell(\mathbb{Z}[H_8])$.
Comme $(1+x+y)^2 = 1+(x^2+1)xy$ ce dernier représente l'élément d'ordre 2 du noyau. Les relations du type $(1+(1+x^2)xy)(1+(1+x^2)(xy+x) = 1+(1+x^2)x$ montrent que les 4 éléments $1+(1+x^2)(ax+by+cxy)$ avec $a+b+c=1$ représentent également la classe d'ordre 2 dans le noyau.
L'identité $(1+x+y)^3 = 1+x+y+(1+x^2)(x+y+xy) = (1+x+y+(1+x^2)xy)(1+(x^2+1)(x+y))$ prouve que le dernier élément décrit dans le lemme 1 est au-dessus du second générateur du noyau.

Cette classification et le procédé de recollement de Milnor montrent que :

Proposition 11. *Il y a 4 classes d'isomorphismes de $\mathbb{Z}[G]$-modules de rang 1 stablement libres : elles sont représentés dans $\mathbb{F}_2[H_8]^*$ par les doubles classes modulo H_8 des éléments $1+(1+x^2)(ax+by+cxy)$ avec $a+b+c=0$.*

VII. Anneau des entiers de N/$\mathbb{Q}$

On suppose que le module M de la section précédente est l'anneau des entiers d'une extension galoisienne $N/\mathbb{Q}$ modérément ramifiée de groupe de Galois $H_8\times C_2$. Le diagramme commutatif de la partie droite de (18) devient :

$$\begin{array}{ccc} \mathcal{O}_N & \longrightarrow & (1-s)\mathcal{O}_N \\ \downarrow & & \downarrow \\ \mathcal{O}_{N_1} & \longrightarrow & \mathcal{O}_{N_1}/2\mathcal{O}_{N_1} \approx \mathbb{F}_2[H_8] \end{array} \tag{19}$$

On sait exprimer que $\mathcal{O}_{N_1}$ est stablement libre, on trouve dans [Ma3] comment construire de telles extensions.

Le dernier isomorphisme vient de ce que sous nos hypothèses $\mathcal{O}_{N_1}$ est isomorphe à $\mathbb{Z}[H_8]$, s opérant trivialement sur N_1, $1-s=2$. Soit θ une base normale de $\mathcal{O}_{N_1}$, d'où une $\mathbb{F}_2[H_8]$-base de $\mathcal{O}_{N_1}/2\mathcal{O}_{N_1}$, Il faut lui comparer l'image d'une base normale ρ de $(1-s)\mathcal{O}_N$ et en déduire son représentant dans $\mathrm{im}(H_8)\backslash\mathbb{F}_2[H_8]^*/\mathrm{im}(H_8)$. On peut alors conclure en suivant la discussion du chapitre précédent.

Puisque $\mathcal{O}_{N_1}$ est invariant par s, $(1-s)\mathcal{O}_N$ est un $\mathcal{O}_{N_1}$-module, son rang est égal à un ; s étant dans le centre de G c'est aussi un $\mathbb{Z}[G]$-module, donc un $\mathbb{Z}[H_8]$-module. Si on note d l'entier non divisible par un facteur carré tel que $k = \mathbb{Q}(\sqrt{d})$, il est évident que $\sqrt{d}$ est dans $(1-s)\mathcal{O}_N$. Il en résulte que $(1-s)\mathcal{O}_N$ contient $\mathcal{O}_{N_1}\sqrt{d}$. Il existe un idéal fractionnaire $\mathcal{U}$ de N_1 qui est un $\mathbb{Z}[G]$-module (donc un idéal ambige entier $\mathcal{U}$ de $\mathcal{O}_{N_1}$ car $\sqrt{d}$ est invariant par H_8) tel que $(1-s)\mathcal{O}_N = \mathcal{U}\sqrt{d}$. L'idéal $\mathcal{U}$ possède une base normale φ qui s'exprime comme une combinaison linéaire à coefficients rationnels des conjugués de θ. D'après le diagramme de droite de (19), la flèche verticale droite de (18) est le passage au quotient de $(1-s)\mathcal{O}_N$ à $(1-s)\mathcal{O}_N/(1-s)^2\mathcal{O}_N = (1-s)\mathcal{O}_N/2(1-s)\mathcal{O}_N$ qui a pour base l'image modulo 2 de φ, c'est ce qui donne le représentant cherché.

La construction d'une $\mathbb{Z}[H_8]$-base de $(1-s)\mathcal{O}_N$ conduit à considérer $(1+x^2)(1-s)\mathcal{O}_N$ et $(1-x^2)(1-s)\mathcal{O}_N$ (diagramme 17). Pour ce dernier, on remarque que $(1-x^2)(1-s) = 1 - x^2 - s + sx^2 = (1-x^2)(1+sx^2)$ et donc $(1-x^2)(1-s)\mathcal{O}_N = (1-x^2)T_{N/N_d}(\mathcal{O}_N) = (1-x^2)\mathcal{O}_{N_d}$ c'est un $\mathcal{H}$-module libre de rang un dont une base est obtenue avec les méthode du chapitre V.

Plus précisément, le corps N est le composé de N_1 et de $\mathbb{Q}(\sqrt{d})$ avec d entier non divisible par un carré et congru à 1 modulo 4, le corps N_d est donc égal à $K(\sqrt{d\gamma_1})$. La méthode du chapitre V montre que $(1-x^2)\mathcal{O}_{N_d}$ est un $\mathcal{H}$ module libre de base $f_d\psi_1\sqrt{d}$ où f_d peut être construit explicitement.

L'autre module, $(1+x^2)(1-s)\mathcal{O}_N$ est égal à $\mathrm{Tr}_{N_1/K}(\mathcal{U})\sqrt{d}$; on voit apparaître un $\mathbb{Z}[V_4]$-module libre de rang un dont on peut construire une base avec les méthodes de la section III. Il reste à déterminer $\mathcal{U}$ puis sa trace sur K.

VII.1. **Calculs de discriminants.** La formule (1) appliquée à $\mathcal{O}_N$ nous donne $\Delta_{T''}((1-s)\mathcal{O}_N)$. L'indice de $\mathcal{O}_{N_1}\sqrt{d}$ dans $(1-s)\mathcal{O}_N$ est la racine carrée de $\Delta_{T''}(\mathcal{O}_{N_1}\sqrt{d})/\Delta_{T''}((1-s)\mathcal{O}_N)$ c'est aussi la norme de $\mathcal{U}$ ce qui permet de déterminer $\mathcal{U}$. Calculons $\Delta_{T''}(\mathcal{O}_{N_1}\sqrt{d})$. Soit θ une base normale de $N_1/\mathbb{Q}$, une $\mathbb{Z}$ base de $\mathcal{O}_{N_1}\sqrt{d}$ est formée des $g(\theta)\sqrt{d}$. Le déterminant de la matrice $\Big(\mathrm{Tr}_{N_1/\mathbb{Q}}(g(\theta)\sqrt{d}h(\theta)\sqrt{d})\Big)_{g,h\in H_8}$ est égal à $d^8\Delta_1$.

La formule (1) devient :

$$\begin{aligned}
\Delta &= \Delta_1\Delta_{T''}((1-s)\mathcal{O}_N)\\
&= \Delta_1\Delta_{T''}(\mathcal{U}\sqrt{d})\\
&= \Delta_1 d^8\Delta_{T'}(\mathcal{U})\\
&= \Delta_1^2 d^8 N_{N_1/\mathbb{Q}}(\mathcal{U})^2
\end{aligned}$$

L'extension $N/\mathbb{Q}$ est modérément ramifiée, les groupes d'inertie sont cycliques donc d'ordre 4 ou 2.
Les sous-groupes d'ordre 4 sont au nombre de 6 engendrés respectivement par :

x, y, xy, sx, sy, sxy (ce qui donne 12 éléments d'ordre 4), ces groupes sont distingués dans G.
Ceux d'ordre 2 sont engendrés par :

s, x^2, sx^2 (avec l'élément neutre on a la liste des éléments de G). On note au passage que tous les sous-groupes d'ordre 4 contiennent le sous-groupe $<x^2>$.

Soit p un premier dont l'indice de ramification est égal à 4 et $\mathcal{T}(p)$ son groupe d'inertie. L'intersection de $\mathcal{T}(p)$ avec $< s >$ est triviale, donc p a un groupe d'inertie dans $N_1/\mathbb{Q}$ d'ordre 4. On en déduit que Δ_1 est divisible exactement par p^6 et Δ par p^{12} : p n'apparaît pas dans $d^8 N_{N_1/\mathbb{Q}}(\mathcal{U})^2$, on a donc deux cas :

• si p ne divise pas d, la valuation en p de $N_{N_1/\mathbb{Q}}(\mathcal{U})^2$ est nulle et les idéaux au-dessus de p n'apparaissent pas dans la décomposition de $\mathcal{U}$.

• si p divise d, p^{-4} est la contribution de p à $N_{N_1/\mathbb{Q}}(\mathcal{U})$ et $\mathcal{U} = \prod_{\mathfrak{P}|p} \mathfrak{P}^{-2}\mathcal{U}_p$ avec $\mathcal{U}_p$ premier à p.

Si l'indice de ramification est 2 et le groupe d'inertie $\mathcal{T}(p)$ égal à $<s>$, p est ramifié dans $k/\mathbb{Q}$ mais ni dans N/k ni dans $N_1/\mathbb{Q}$. On en déduit que p^8 divise Δ et d^8 mais que Δ_1 est premier à p. Il en est donc de même pour $N_{N_1/\mathbb{Q}}(\mathcal{U})$ et pour $\mathcal{U}$.

Si l'indice de ramification est 2 et le groupe d'inertie $\mathcal{T}(p)$ égal à $<x^2>$, p n'est pas ramifié dans $k/\mathbb{Q}$ et est ramifié uniquement dans $N_1/\mathbb{Q}$. Il en résulte que p^4 divise exactement Δ_1, p^8 divise exactement Δ, que p ne divise pas d et donc ne figure ni dans $N_{N_1/\mathbb{Q}}(\mathcal{U})$ ni dans $\mathcal{U}$.

Si l'indice de ramification est 2 et le groupe d'inertie $\mathcal{T}(p)$ égal à $<sx^2>$, p est ramifié dans N_1/K et dans $k/\mathbb{Q}$. On a donc p^4 divise exactement Δ_1, p^8 divise exactement Δ, p divise d. Il en résulte que la contribution de p dans $N_{N_1/\mathbb{Q}}(\mathcal{U})$ est p^{-4} et, comme $\mathcal{U}$ est ambige et que l'indice de ramification dans $N_1/\mathbb{Q}$ est 2, que $\mathcal{U} = \prod_{\mathfrak{P}|p} \mathfrak{P}^{-1}\mathcal{U}_p$ avec $\mathcal{U}_p$ premier à p.

Finalement :

$$\begin{aligned} \mathcal{U} &= \prod_{\substack{p|\Delta_1 \text{ et } p|d \\ e(p)=4}} \Big(\prod_{\mathfrak{P}|p} \mathfrak{P}^{-2}\Big) \prod_{\substack{p|\Delta_1 \text{ et } p|d \\ e(p)=2}} \Big(\prod_{\mathfrak{P}|p} \mathfrak{P}^{-1}\Big) \\ &= \prod_{\substack{p|\Delta_1 \text{ et } p|d \\ e(p)=4}} \Big(\frac{1}{p}\prod_{\mathfrak{P}|p} \mathfrak{P}^{2}\Big) \prod_{\substack{p|\Delta_1 \text{ et } p|d \\ e(p)=2}} \Big(\frac{1}{p}\prod_{\mathfrak{P}|p} \mathfrak{P}\Big) \end{aligned}$$

Calculons maintenant la trace de $\mathrm{Tr}_{N_1/K}(\mathcal{U})$, on procède localement.

Si p divise Δ_1 et d avec $e(p) = 2$ soit $\mathfrak{P}$ au-dessus de p dans N_1, il y a un seul idéal premier $\mathfrak{p}$ dans K sous $\mathfrak{P}$ et $\mathrm{Tr}_{N_1/K}(\mathfrak{P}) = \mathfrak{p}$, quand on prend le produit sur les $\mathfrak{P}$ divisant p cette contribution disparaît avec le dénominateur.

Si p divise Δ_1 et d avec $e(p) = 4$, $\mathfrak{P}^2 = (\mathfrak{P} \cap K)\mathcal{O}_{N_1}$, en notant $\mathfrak{p} = (\mathfrak{P} \cap K)$ on obtient $\mathrm{Tr}_{N_1/K}(\mathfrak{P}^2) = \mathfrak{p}$ soit finalement :

$$\mathrm{Tr}_{N_1/K}(\mathcal{U}) = \prod_{\substack{p|\Delta_1 \text{ et } p|d \\ e(p)=4}} \Big(\frac{1}{p} \prod_{\mathfrak{p}|p} \mathfrak{p}\Big)$$

L' introduction de ce chapitre donne une base de $\mathcal{H}$-module de $(1-x^2)(1-s)\mathcal{O}_N$: $f_d\psi_1\sqrt{d}$, on peut calculer le générateur de base normale de $\mathrm{Tr}_{N_1/K}(\mathcal{U})$ qui multiplié par $\sqrt{d}$ lui est congru modulo 2. La demi-différence ρ de ces éléments est une $\mathbb{Z}[H_8]$-base de $(1-s)\mathcal{O}_N$ qui s'écrit :

$$\Big(\frac{\alpha\omega + \beta x(\omega) + \eta y(\omega) + \mu xy(\omega) - f_d\psi_1}{2}\Big)\sqrt{d}$$

On remarque que les ensembles $\{g(1+(1+x^2)(ax+by+cxy)) \mid g \in H_8,\ a+b+c \equiv 0 \bmod 2\}$ et $\{(1+(1+x^2)(ax+by+cxy))g \mid g \in H_8,\ a+b+c \equiv 0 \bmod 2\}$ pour a, b, c fixés sont identiques.

Une fois construite une base ρ du $\mathbb{Z}[H_8]$-module $(1-s)\mathcal{O}_N$ on doit trouver lequel des éléments
$g(1+(1+x^2)(a+bx+by+cxy))(\theta)$ lui est congru modulo 2.

La réponse est donnée par le calcul, pour $a+b+c \equiv 0$ modulo 2 et $g \in H_8$, des polynômes irréductibles des différences

$$\frac{g(1+(1+x^2)(ax+by+cxy))(\theta) - \rho}{2}.$$

On obtient ainsi la classe de $\mathcal{O}_N$.

VII.2. **Une amélioration du test.** Partons des éléments de la forme :

$$g(1-(1+x^2)(ax+by+cxy))(\theta) - \Big(\frac{\alpha\omega + \beta x(\omega) + \eta y(\omega) + \mu xy(\omega) - f_d\psi_1}{2}\Big)\sqrt{d}$$

Dans cette expression $g(1-(1+x^2)(ax+by+cxy))(\theta)$ et $\sqrt{d}$ sont entiers, le second étant premier à 2. On en déduit que

$$\Big(\frac{\alpha\omega + \beta x(\omega) + \eta y(\omega) + \mu xy(\omega) - f_d\psi_1}{2}\Big)$$

est un entier. Comme d est un entier congru à 1 modulo 4, on transforme le nombre considéré en :

$$g(1-(1+x^2)(ax+by+cxy))(\theta) - \Big(\frac{\alpha\omega + \beta x(\omega) + \eta y(\omega) + \mu xy(\omega) - f_d\psi_1}{2}\Big)\Big(2\frac{1+\sqrt{d}}{2} - 1\Big).$$

On fait ainsi apparaître un un entier divisible par 2 :

$$2\Big(\frac{\alpha\omega+\beta x(\omega)+\eta y(\omega)+\mu xy(\omega)-f_d\psi_1}{2}\Big)\Big(\frac{1+\sqrt{d}}{2}\Big)$$

On est donc ramené à étudier la divisibilité par 2 de l'entier :

$$g(1-(1+x^2)(ax+by+cxy))(\theta_1)+\Big(\frac{\alpha\omega+\beta x(\omega)+\eta y(\omega)+\mu xy(\omega)-f_d\psi_1}{2}\Big)$$

Sachant qu'il existe $g\in H_8$, $\Big\{a,b,c\in\{0,1\}\ |a+b+c=2\Big\}$ tels qu'il en soit ainsi, on les obtient en écrivant

$$\Big(\frac{\alpha\omega+\beta x(\omega)+\eta y(\omega)+\mu xy(\omega)-f_d\psi_1}{2}\Big) \tag{20}$$

dans la base normale de $\mathcal{O}_{N_1}$. Supposons donné K, $N_1/\mathbb{Q}$ une extension quaternionienne ayant une base normale ; on pose $N_1=K(\psi_1)$ où $\mathcal{H}\psi_1=(1-x^2)\mathcal{O}_{N_1}$. On compose N_1 avec $\mathbb{Q}(\sqrt{d})$ où d est un entier congru à 1 modulo 4. On note N_d le second corps quaternionique contenu dans $N_1(\sqrt{d})$ et on suppose que $\mathcal{O}_{N_d}$ possède une base normale. On pose $(1-x^2)\mathcal{O}_{N_d}=\mathcal{H}\psi_d$. Les constructions du chapitre montrent qu'il existe $f_d\in K$ tel que $\psi_d=f_d\psi_1\sqrt{d}$ et $\mathrm{Tr}(f_d^2\psi_1^2d)=\epsilon\prod_{p|\Delta_d}p$ avec Δ_d le discriminant de $N_d/\mathbb{Q}$.

Supposons que l'on remplace $\mathbb{Q}(\sqrt{d})$ par $\mathbb{Q}(\sqrt{d\delta})$ où δ est un entier congru à 1 modulo 4, non divisible par un carré et premier à Δ_1. En reprenant la construction précédente, on obtient un corps $N_{d\delta}=K(f_d\psi_1\sqrt{d\delta})$. Un calcul rapide de discriminant montre que $\mathrm{Tr}(f_d^2\psi_1^2d\delta)=\epsilon\prod_{p|\Delta_{d\delta}}p$ avec $\Delta_{d\delta}$ le discriminant de $N_{d\delta}/\mathbb{Q}$, c'est donc que $(1-x^2)\mathcal{O}_{N_{d\delta}}=\mathcal{H}\psi_{d\delta}$ avec $\psi_{d\delta}=f_d\psi_1\sqrt{d\delta}$. La formule (20) reste la même pour les corps $N_1(\sqrt{d})$ et $N_1(\sqrt{d\delta})$; de même la formule du théorème 8 montre que $\mathcal{O}_{N_{d\delta}}$ possède une base normale. On en déduit :

Corollaire 12. *Si une classe d'isomorphisme de $\mathbb{Z}[H_8\times C_2]$-module stablement libre est représentée par un anneau d'entiers $N/\mathbb{Q}$ elle l'est pour une infinité d'anneaux d'entiers.*

VIII. Exemples numériques

Corps quadratiques purs contenant $K=\mathbb{Q}(\sqrt{1001},\sqrt{2805})$

On vérifie par le calcul des symboles de Hilbert que K est plongeable dans un corps quaternionique de degré 8.

Le théorème 9 montre qu'un corps quaternionique pur N_1 contenant K, modérément ramifié possède une base normale si et seulement si c'est un corps complexe.

Il y a six nombres premiers ramifiés dans $K/\mathbb{Q}$, la 2-extension élémentaire contenant K, non ramifiée sur K aux places finies, maximale est de degré 2^6 sur $\mathbb{Q}$ donc de degré 2^4 sur K. Certains des nombres premiers ramifiés dans

$K/\mathbb{Q}$ étant congrus à 3 modulo 4, ce corps est complexe. Les extensions quadratiques de K, abéliennes sur $\mathbb{Q}$ et non ramifiées sur K sont donc au nombre de 8. Par composition avec N_1 on obtient 8 corps quaternioniques purs complexes dont l'anneau des entiers possède une base normale.

Construisons tout d'abord un premier plongement. Pour cela prenons une décomposition en somme de trois carrés des nombres $1001 = 2^2 + 6^2 + 31^2$, $2805 = 1^2 + 10^2 + 52^2$ qui donne une matrice $M = \begin{pmatrix} 31 & 10 & 110 \\ 2 & 1 & -1672 \\ -6 & 52 & 11 \end{pmatrix}$.
Ceci conduit à prendre, dans la formule (15) $p_x = 31$, $p_y = 1$ $p_{xy} = 11$.

Remarque 5. Le choix n'est pas unique : en tenant compte des permutations, et des différentes décomposition de d_x et d_y en sommes de trois carrés, on a testé 90 matrices. Il fallait en choisir une qui donne (au signe près) la bonne trace, on a choisi celle où les coefficients p_x, p_y, p_{xy} sont les plus petits.

On écrit cet élément sur la base normale des entiers de K, on divise les coefficients par leur pgcd. On obtient ainsi :

$$61812\omega + 61863x(\omega) + 65770y(\omega) + 65810xy(\omega)$$

dont la trace (somme des nouveaux coefficients dans la base normale) est 255255 cet élément est congru, modulo 4 à $-\Big(3x(\omega) + 2y(\omega) + 2xy(\omega)\Big)^2$.
On en conclu que le corps

$$K\left(\sqrt{-\Big(61812\omega + 61863x(\omega) + 65770y(\omega) + 65810xy(\omega)\Big)}\right)$$

est un corps quaternionique pur, complexe, donc ayant une base normale.
On note

$\gamma_1 = -\Big(61812\omega + 61863x(\omega) + 65770y(\omega) + 65810xy(\omega)\Big)$ et ψ_1 une de ses racines carrées. Pour obtenir la base normale, il suffit de savoir à quel conjugué de ω est congru (modulo 2) ψ_1. On construit les polynôme irréductibles des $g(\omega) - \psi_1$. On obtient ainsi comme générateur d'une base normale

$$\theta_1 = \frac{\omega - \psi_1}{2} = \frac{\omega - \sqrt{-\Big(61812\omega + 61863x(\omega) + 65770y(\omega) + 65810xy(\omega)\Big)}}{2}$$

dont le polynôme minimal est :

$$\begin{aligned} x^8 - x^7 + 62126x^6 - 565081x^5 + 1060385071x^4 - 16366741325x^3 \\ + 465279400700x^2 + 7092550941085x + 160472449673155. \end{aligned}$$

On note N_1 ce corps, les autres corps quaternioniques purs ramifiés à l'infini sont obtenus comme le second sous-corps quaternionique du composé de N_1 avec chacun des corps quadratiques réels $\mathbb{Q}(\sqrt{d})$ avec $d \in \{5, 5\times 13, 5\times 17, 3\times 7, 13, 17, 13\times 17\}$. Dans la partie numérique qui suit, chacun de ces corps quaternioniques purs est désigné par N_d. Les autres corps quaternioniques complexes sont les $K(\sqrt{d\gamma_1})$. Pour construire une base normale de l'anneau des entiers, comme dans discussion de la section précédente, il faut remplacer ce radicande en le multipliant par le carré d'un nombre de K de telle sorte que l'on obtienne un entier de trace -255255.

On note $\hat{\gamma} = d\gamma_1$ et $\hat{\psi} = \sqrt{\hat{\gamma}}$. La discussion de V-2 montre qu'il faut trouver les quaternions entiers ρ de norme réduite d et que le radicande cherché est l'un des $\left(\frac{\rho\hat{\psi}}{d}\right)^2$.

Si $\rho = \alpha+\beta i+\eta j+\mu ij$, $\rho\hat{\gamma} = \alpha\hat{\psi}+\beta x(\hat{\psi})+\eta y(\hat{\psi})+\mu xy(\hat{\psi})$ (en prenant la même notation pour x, y et un de leurs prolongements). Le calcul de $g(\hat{\psi})$ implique celui des $r_g \in K$ tels que $g(\gamma_1) = r_g^2\gamma_1$. Les calculs conduisent à :

$$\begin{aligned}
r_x &= \frac{39}{101}\omega + \frac{40}{101}x(\omega) + \frac{38}{101}y(\omega) + \frac{36}{101}xy(\omega)\\
r_y &= -\frac{613}{101}\omega - \frac{608}{101}x(\omega) - \frac{2888}{505}y(\omega) - \frac{2837}{505}xy(\omega)\\
r_{xy} &= -\frac{223}{101}\omega - \frac{208}{101}x(\omega) - \frac{1089}{505}y(\omega) - \frac{936}{505}xy(\omega)
\end{aligned}$$

On peut vérifier que r_x (resp. r_y, r_{xy}) est de norme -1 sur k_x (resp k_y, k_{xy}).

Il faut maintenant utiliser les décomposition $d = \alpha^2+\beta^2+\eta^2+\mu^2$ de d en sommes de quatre carrés d'entiers, leur associer les quaternions $\alpha+\beta i+\eta j+\mu ij$ puis les éléments $\left(\frac{\alpha+\beta r_x+\eta r_y+\mu r_{xy}}{d}\right)^2\hat{\gamma}$ de K, cette détermination se faisant à conjugaison près, pour une décomposition donnée on peut fixer α et son signe. Ceci étant précisé, un et un seul quadruplet $(\alpha, \beta, \eta, \mu)$ donne un entier $\gamma_d = f_d^2\gamma_1 d$ de K dont la racine carrée ψ_d permet de construire une base normale. Pour chacune des valeurs de d on donne les coefficients α, β, η, μ, les coordonnées de f_d puis celles de γ_d dans la base normale de K, le conjugué $g(\omega)$ auquel ψ_d est congru modulo 2 et enfin le polynôme irréductible de $\frac{g(\omega)-\psi_d}{2}$.

- $d = 5$ $\quad \alpha = 2$, $\beta = -1$, $\eta = 0$, $\mu = 0$

$f_5 = \left[\frac{163}{505}, \frac{162}{505}, \frac{164}{505}, \frac{166}{505}\right]$, $\quad \gamma_5 = \left[-63103, -60572, -66390, -65190\right]$, $\quad x(\omega)$

$$x^8 - x^7 + 62126x^6 - 3117631x^5 + 465640921x^4 - 8688670925x^3 + 227961169550x^2 - 8096607143015x + 78615823872205$$

- $d = 65 \quad \alpha = 6,\ \beta = 2,\ \eta = -5,\ \mu = 0$

$$f_{65} = \Big[\frac{3749}{6565}, \frac{3726}{6565}, \frac{714}{1313}, \frac{703}{1313}\Big], \quad \gamma_{65} = \Big[-63234, -64266, -63620, -64135\Big], \quad y(\omega)$$

$$x^8 - x^7 + 62126x^6 + 455939x^5 + 1403958301x^4 + 12074281285x^3 + 13695081726440x^2 + 96273652090225x + 450976570358370 25$$

- $d = 85 \quad \alpha = 7,\ \beta = 4,\ \eta = -2,\ \mu = 4$

$$f_{85} = \Big[\frac{1197}{8585}, \frac{1251}{8585}, \frac{1143}{8585}, \frac{1237}{8585}\Big], \quad \gamma_{85} = \Big[-61564, -64151, -63834, -65706\Big], \quad \omega$$

$$x^8 - x^7 + 62126x^6 - 2096611x^5 + 913358191x^4 - 20639199515x^3 + 1748113943690x^2 + 13349986875835x + 938956719025945$$

- $d = 21 \quad \alpha = 4,\ \beta = -1,\ \eta = -2,\ \mu = 0$

$$f_{21} = \Big[\frac{1591}{2121}, \frac{1580}{2121}, \frac{7606}{10605}, \frac{7514}{10605}\Big], \quad \gamma_{21} = \Big[-63423, -62292, -64978, -64562\Big], \quad x(\omega)$$

$$x^8 - x^7 + 62126x^6 - 1586101x^5 + 1278883351x^4 - 30555856265x^3 + 10693466710040x^2 - 157578154508165x + 31010272581373705$$

- $d = 13 \quad \alpha = 2,\ \beta = 2,\ \eta = -2,\ \mu = -1$

$$f_{13} = \Big[\frac{133}{101}, \frac{1706}{1313}, \frac{127}{101}, +\frac{1596}{1313}\Big], \quad \gamma_{13} = \Big[-63214, -64286, -64095, -63660\Big], \quad xy(\omega)$$

$$x^8 - x^7 + 62126x^6 - 2096611x^5 + 1084889551x^4 - 67412125715x^3 + 4827203957690x^2 - 123415137229775x + 950259835680775$$

- $d = 17 \quad \alpha = 3,\ \beta = 0,\ \eta = -2,\ \mu = -2$

$f_{17} = \Big[\frac{1975}{1717}, \frac{1935}{1717}, \frac{557}{505}, \frac{533}{505}\Big], \quad \gamma_{17} = \Big[-64404, -63351, -64634, -62866\Big], \quad \omega$

$$x^8 - x^7 + 62126x^6 - 565081x^5 + 1219664191x^4 - 19648299605x^3 + 8370234738980x^2 - 262621669734815x + 4861757903277895$$

- $d = 221 \quad \alpha = 12,\ \beta = 6,\ \eta = -4,\ \mu = 5$

$f_{221} = \Big[\frac{2783}{22321}, \frac{2844}{22321}, \frac{13307}{111605}, \frac{13808}{111605}\Big], \quad \gamma_{221} = \Big[-61482, -63978, -64007, -65788\Big],$
$xy(\omega)$

$$x^8 - x^7 + 62126x^6 + -54571x^5 + 813298231x^4 + 24859493725x^3 + 1797896836850x^2 + 130052349272455x + 2392810236402205$$

Remarque 6. On constate que les coordonnées des γ sont du même ordre de grandeur.

Ceci étant, comme on doit considérer les composés deux à deux de ces corps, il est utile de connaître les nombres $f_{d,d'}$ de K tels que $\gamma_{d'} = f_{d,d'}^2 \gamma_d \dfrac{dd'}{\mathrm{pgcd}(d,d')^2}$ pour les couples autres que ceux qui viennent d'être considérés. Ce calcul peut être conduit à partir de la connaissance des f_d, $f_{d'}$. Donnons les valeurs obtenues par leurs coordonnées suivant la base normale des entiers de K.
Pour composer N_5 avec :

$$\begin{aligned}
N_{65} &: f_{5,65} = \Big[-\frac{706}{13}, -53, -\frac{672}{13}, -49\Big]\\
N_{85} &: f_{5,85} = \Big[\frac{146}{17}, \frac{143}{17}, \frac{696}{85}, \frac{664}{85}\Big]\\
N_{21} &: f_{5,21} = \Big[-\frac{1327}{105}, -\frac{37}{3}, -\frac{421}{35}, -\frac{57}{5}\Big]\\
N_{13} &: f_{5,13} = \Big[-\frac{2138}{65}, -\frac{2087}{65}, -\frac{407}{13}, -\frac{386}{13}\Big]\\
N_{17} &: f_{5,17} = \Big[-\frac{2658}{85}, -\frac{519}{17}, -\frac{506}{17}, -\frac{480}{17}\Big]\\
N_{221} &: f_{5,221} = \Big[-\frac{18}{85}, -\frac{45}{221}, -\frac{1}{5}, -\frac{12}{65}\Big]
\end{aligned}$$

Pour composer N_{65} avec :

$$N_{85} \ : \ f_{65,85} = \left[\frac{992}{22321}, \frac{5087}{111605}, \frac{25341}{558025}, \frac{26084}{558025}\right]$$
$$N_{21} \ : \ f_{65,21} = \left[\frac{20849}{689325}, \frac{20464}{689325}, \frac{21193}{689325}, \frac{21032}{689325}\right]$$
$$N_{13} \ : \ f_{65,13} = \left[\frac{164}{505}, \frac{166}{505}, \frac{163}{505}, \frac{162}{505}\right]$$
$$N_{17} \ : \ f_{65,17} = \left[\frac{16756}{558025}, \frac{16411}{558025}, \frac{16979}{558025}, \frac{16596}{558025}\right]$$
$$N_{221} \ : \ f_{65,221} = \left[\frac{3506}{42925}, \frac{3566}{42925}, \frac{3577}{42925}, \frac{3648}{42925}\right]$$

Pour composer N_{85} avec :

$$N_{21} \ : \ f_{85,21} = \left[\frac{7901}{934745}, \frac{7484}{934745}, \frac{30148}{2804235}, \frac{32582}{2804235}\right]$$
$$N_{13} \ : \ f_{85,13} = \left[\frac{-92381}{1735955}, \frac{-89094}{1735955}, \frac{-1021}{20423}, \frac{-952}{20423}\right]$$
$$N_{17} \ : \ f_{85,17} = \left[-\frac{4699}{7855}, -\frac{4621}{7855}, -\frac{4159}{7855}, -\frac{3821}{7855}\right]$$
$$N_{221} \ : \ f_{85,221} = \left[\frac{9433}{102115}, \frac{9472}{102115}, \frac{9703}{102115}, \frac{9872}{102115}\right]$$

Pour composer N_{21} avec :

$$N_{13} \ : \ f_{21,13} = \left[\frac{184586}{2850393}, \frac{26677}{407199}, \frac{61291}{950131}, \frac{8688}{135733}\right]$$
$$N_{17} \ : \ f_{21,17} = \left[\frac{206408}{3727437}, \frac{204805}{3727437}, \frac{206032}{3727437}, \frac{201356}{3727437}\right]$$
$$N_{221} \ : \ f_{21,221} = \left[\frac{620050}{48456681}, \frac{640109}{48456681}, \frac{632747}{48456681}, \frac{650362}{48456681}\right]$$

Pour composer N_{13} avec :

$$N_{17} \ : \ f_{13,17} = \left[-\frac{2086}{1105}, -\frac{1977}{1105}, -\frac{10968}{5525}, -\frac{10707}{5525}\right]$$
$$N_{221} \ : \ f_{13,221} = \left[-\frac{49}{17}, -\frac{231}{85}, -\frac{1293}{425}, -\frac{1257}{425}\right]$$

Pour composer N_{17} avec :

$$N_{221} \ : \ f_{17,221} = \left[\frac{25403}{39637}, \frac{26066}{39637}, \frac{24413}{39637}, \frac{25466}{39637}\right].$$

Remarque 7. Là encore les coordonnées de chaque f suivant la base normale de K sont du même ordre de grandeur.

On détermine la classe d'isomorphisme de l'anneau des entiers de chacun des corps N composés de N_d et de $N_{d'}$. On donne la liste par classes.

Le chapitre précédent et les calculs antérieurs donnent une base de $(1-x^2)(1-s)\mathcal{O}_N$, on peut calculer le générateur de base normale de $\mathrm{Tr}_{N_1/K}(\mathcal{U})$ auquel le précédent est congru modulo 2. La demi-somme φ de ces éléments est une base de $(1-s)\mathcal{O}_N$, comme $\mathbb{Z}\Big[H_8\Big]$-module.

1. Bases normales $(a=b=c=0)$.
$N_1N_5 = N_1(\sqrt{5})$ base :

$$\frac{1}{2}\Big\{x^2(\theta_1)-2\omega+3x(\omega)-f_5\psi_1 2\sqrt{5}\Big\}$$

$N_1N_{221} = N_1(\sqrt{221})$ base :

$$\frac{1}{2}\Big\{xy^3(\theta_1)-\frac{48\omega+54x(\omega)+56y(\omega)+63xy(\omega)-f_{221}\psi_1}{2}\sqrt{221}\Big\}$$

$N_5N_{221} = N_5(\sqrt{1105})$ base :

$$\frac{1}{2}\Big\{y(\theta_5)-\frac{252\omega+258x(\omega)+294y(\omega)+301xy(\omega)-f_{5,221}\psi_5}{2}\sqrt{1105}\Big\}$$

$N_{65}N_{21} = N_{65}(\sqrt{1365})$ base :

$$\frac{1}{2}\Big\{xy(\theta_{65})-\frac{360\omega+315x(\omega)+368y(\omega)+322xy(\omega)-f_{65,21}\psi_{65}}{2}\sqrt{1365}\Big\}$$

$N_{65}N_{13} = N_{65}(\sqrt{5})$ base :

$$\frac{1}{2}\Big\{x^3(\theta_{65})-\frac{2y(\omega)+3xy(\omega)-f_{65,13}\psi_{65}}{2}\sqrt{5}\Big\}$$

$N_{21}N_{13} = N_{21}(\sqrt{273})$ base :

$$\frac{1}{2}\Big\{xy(\theta_{65})-\frac{92\omega+46x(\omega)+90y(\omega)+45xy(\omega)-f_{65,21}\psi_{21}}{2}\sqrt{273}\Big\}$$

2. Classe $(a=0,\ b=1,\ c=1)$.
$N_1N_{17} = N_1(\sqrt{17})$ relation :

$$\frac{1}{2}\Big\{x(1+(1+x^2)(y+xy))(\theta_1)-\frac{9\omega+8x(\omega)-f_{17}\psi_1}{2}\sqrt{17}\Big\}$$

$N_5N_{17} = N_5(\sqrt{85})$ relation :

$$\frac{1}{2}\Big\{x^2(1+(1+x^2)(y+xy))(\theta_5)-\frac{43\omega+42x(\omega)-f_{5,17}\psi_5}{2}\sqrt{85}\Big\}$$

$N_{65}N_{85} = N_{65}(\sqrt{221})$ relation :

$$\frac{1}{2}\Big\{y(1+(1+x^2)(y+xy))(\theta_{65})-\frac{63\omega+56x(\omega)+54y(\omega)+48xy(\omega)-f_{65,85}\psi_1}{2}\sqrt{221}\Big\}$$

$N_{85}N_{21} = N_{85}(\sqrt{1785})$ relation :

$$\frac{1}{2}\Big\{x(1+(1+x^2)(y+xy))(\theta_{85})-\frac{384\omega+381x(\omega)+512y(\omega)+508xy(\omega)-f_{65,21}\psi_{85}}{2}\sqrt{1785}\Big\}$$

$N_{85}N_{13} = N_{85}(\sqrt{1105})$ relation :

$$\frac{1}{2}\Big\{xy(1+(1+x^2)(y+xy))(\theta_{85})-\frac{252\omega+258x(\omega)+294y(\omega)+301xy(\omega)-f_{85,13}\psi_{85}}{2}\sqrt{1105}\Big\}$$

$N_{17}N_{221} = N_{17}(\sqrt{13})$ relation :

$$\frac{1}{2}\Big\{xy(1+(1+x^2)(y+xy))(\theta_{17})-\frac{6x(\omega)+7xy(\omega)-f_{17,221}\psi_{17}}{2}\sqrt{13}\Big\}$$

3. Classe $(a=1,\ b=0,\ c=1)$.

$N_1N_{65} = N_1(\sqrt{65})$ relation :

$$\frac{1}{2}\Big\{y^3(1+(1+x^2)(x+xy))(\theta_1)-\frac{18\omega+12x(\omega)+21y(\omega)+14xy(\omega)-f_{65}\psi_1}{2}\sqrt{65}\Big\}$$

$N_1N_{21} = N_1(\sqrt{21})$ relation :

$$\frac{1}{2}\Big\{x^2(1+(1+x^2)(x+xy))(\theta_1)-\frac{6\omega+3x(\omega)+8y(\omega)+4xy(\omega)-f_{21}\psi_1}{2}\sqrt{21}\Big\}$$

$N_1N_{13} = N_1(\sqrt{13})$ relation :

$$\frac{1}{2}\Big\{xy(1+(1+x^2)(x+xy))(\theta_1)-\frac{6x(\omega)+7xy(\omega)-f_{13}\psi_1}{2}\sqrt{13}\Big\}$$

$N_5N_{65} = N_5(\sqrt{13})$ relation :

$$\frac{1}{2}\Big\{xy^3(1+(1+x^2)(x+xy))(\theta_5)-\frac{6\omega+7y(\omega)-f_{5,65}\psi_5}{2}\sqrt{13}\Big\}$$

$N_5N_{21} = N_5(\sqrt{105})$ relation :

$$\frac{1}{2}\Big\{(1+(1+x^2)(x+xy))(\theta_5)-\frac{24\omega+21x(\omega)+32y(\omega)+28xy(\omega)-f_{5,21}\psi_5}{2}\sqrt{105}\Big\}$$

$N_5N_{13} = N_5(\sqrt{65})$ relation :

$$\frac{1}{2}\Big\{y^3(1+(1+x^2)(x+xy))(\theta_5)-\frac{12\omega+18x(\omega)+14y(\omega)+21xy(\omega)-f_{5,13}\psi_5}{2}\sqrt{65}\Big\}$$

$N_{65}N_{221} = N_{65}(\sqrt{85})$ relation :

$$\frac{1}{2}\Big\{x^2(1+(1+x^2)(x+xy))(\theta_{65})-\frac{42y(\omega)+43xy(\omega)-f_{65,221}\psi_{65}}{2}\sqrt{85}\Big\}$$

$N_{85}N_{17} = N_{85}(\sqrt{5})$ relation :

$$\frac{1}{2}\Big\{x(1+(1+x^2)(x+xy))(\theta_{85})-\frac{3\omega+2x(\omega)-f_{85,17}\psi_{85}}{2}\sqrt{5}\Big\}$$

$N_{21}N_{221} = N_{21}(\sqrt{4641})$ relation :

$$\frac{1}{2}\Big\{y(1+(1+x^2)(x+xy))(\theta_{21})-\frac{1196\omega+1150x(\omega)+1170y(\omega)+1125xy(\omega)-f_{21,221}\psi_{21}}{2}\sqrt{4641}\Big\}$$

$N_{13}N_{221} = N_{13}(\sqrt{17})$ relation :

$$\frac{1}{2}\Big\{x(1+(1+x^2)(x+xy))(\theta_{13}) - \frac{8y(\omega)+9xy(\omega)-f_{13,221}\psi_{13}}{2}\sqrt{17}\Big\}$$

4. Classe $(a=1,\ b=1,\ c=0)$.

$N_1N_{85} = N_1(\sqrt{85})$ relation :

$$\frac{1}{2}\Big\{(1+(1+x^2)(x+y))(\theta_1) - \frac{43\omega+42x(\omega)-f_{85}\psi_1}{2}\sqrt{85}\Big\}$$

$N_5N_{85} = N_5(\sqrt{17})$ relation :

$$\frac{1}{2}\Big\{x^3(1+(1+x^2)(x+y))(\theta_5) - \frac{9\omega+8x(\omega)-f_{5,85}\psi_5}{2}\sqrt{17}\Big\}$$

$N_{65}N_{17} = N_{65}(\sqrt{1105})$ relation :

$$\frac{1}{2}\Big\{y^3(1+(1+x^2)(x+y))(\theta_{65}) - \frac{301\omega+294x(\omega)+258y(\omega)+252xy(\omega)-f_{65,17}\psi_{65}}{2}\sqrt{1105}\Big\}$$

$N_{85}N_{221} = N_{85}(\sqrt{1105})$ relation :

$$\frac{1}{2}\Big\{xy^3(1+(1+x^2)(x+y))(\theta_{85}) - \frac{252\omega+258x(\omega)+294y(\omega)+301xy(\omega)-f_{85,221}\psi_{85}}{2}\sqrt{1105}\Big\}$$

$N_{21}N_{17} = N_{21}(\sqrt{357})$ relation :

$$\frac{1}{2}\Big\{x^2(1+(1+x^2)(x+y))(\theta_{21}) - \frac{75\omega+78x(\omega)+100y(\omega)+104xy(\omega)-f_{21,17}\psi_{21}}{2}\sqrt{357}\Big\}$$

$N_{13}N_{17} = N_{13}(\sqrt{221})$ relation :

$$\frac{1}{2}\Big\{xy^3(1+(1+x^2)(x+y))(\theta_{13}) - \frac{63\omega+56x(\omega)+54y(\omega)+48xy(\omega)-f_{13,17}\psi_{13}}{2}\sqrt{221}\Big\}.$$

Bibliographie

[Che] C. Chevalley, *Sur certains idéaux dans une algèbre simple*, Abh. Math. Sem. Univ. Hamburg **10** (1934), 83–105.

[Co] J. Cougnard, *Un anneau d'entiers stablement libre et non libre*, Experimental Mathematics **3** n°2 (1994), 129–136.

[Cr] T.Crespo, *explicit construction of $\tilde{A}_n$ Type fields*, J. of Algebra **127 n° 2** (1989), 452–461.

[E] M. Eichler, *Über die Idealklassenzahl in gewissen normalen einfachen Algebren*, Math. Zeit. **43** (1938), 481–494.

[F1] A. Fröhlich, *Artin-Root Numbers and Normal Integral Bases for Quaternion fields*, Inventiones Math. **17** (1972), 143–166.

[F2] A. Fröhlich, *Locally free modules over arithmetic orders*, J. reine angew. Math **274/75** (1975), 112–138.

[F3] A. Fröhlich, *Arithmetic and Galois module structure for tame extensions*, J. reine angew. Math **286/287** (1976), 380–440.

[F4] A. Fröhlich, *Galois module structure of agebraic integers*, Springer Verlag (1983).

[J] H. Jacobinski, *Genera and decomposition of lattices over orders*, Acta Math **121** (1968), 1–29.

[K] M.E. Keating, *On the K-theory of the quaternion group*, Mathematika **20** (1973), 59–62.

[La] T.Y. Lam, The algebraic theory of quadratic forms, seconde édition, Benjamin (1980).

[Ma1] J. Martinet, *Modules sur l'algèbre du groupe quaternionien*, Annales Sci. de l'Ec. normale sup **4** série fasc. 3 (1971), 399–408.

[Ma2] J. Martinet, *Sur les extensions à groupe de Galois quaternionien*, C.R. Acad. Sc. Paris t. **274** (1972), 933–935.

[Ma3] J. Martinet, $H8$, Algebraic Number Fields, 525–538 édité par A. Fröhlich, Academic Press 1977.

[M] J. Milnor, Introduction to algebraic K-Theory, Annals of Math. Studies **72** (1971).

[M-N] R. Massy, T. Nuyen Quang Do, *Plongement d'une extension de degré p^2 dans une surextension non abélienne de degré p^3 : étude locale-globale*, J. für die reine und angew. Math. t. **291** (1977), 149–161.

[P] C. Batut, D. Bernardi, H. Cohen, M. Olivier, User's Guide to Pari-GP, version 1.39-12 (1995).

[S] J-P. Serre, *Modules projectifs et espaces fibrés à fibres vectorielles*, Séminaire Dubreil exposé n°23 (1968), 23.01–23.18.

[Sw1] R.G. Swan, *Induced representations and projective modules*, Ann. of Math. **71** (1960), 552–578.

[Sw2] R.G. Swan, *Projective modules over group rings and maximal orders*, Ann. of Math. **76** (1962), 55–61.

[Sw3] R.G. Swan, *Strong approximation theorem and locally free modules*, dans Ring Theory and Algebra III ed. (1980).

[Sw4] R.G. Swan, *Projective modules over binary polyhedral groups*, J. reine angew. Math. **342** (1983), 66–172.

[T] M.J. Taylor, *On Fröhlich's conjecture for rings of integers of tame extensions*, Invent. Math. **63** (1981), 41–79.

[U] S. Ullom, *Normal bases in Galois extensions of number fields*, Nagoya Math. J. **34** (1969), 153-167.

[W] E. Witt, *Konstruktion von Körpern zu vorgegebener gruppe der ordnung p^f*, J. reine angew. Math. **174** (1936), 237–245.

Jean COUGNARD
ESA 6081 du CNRS
Structures Discrètes et Analyse Diophantienne
Esplanade de la Paix
F–14032 CAEN cedex
E-mail : `cougnard@math.unicaen.fr`