Journal de Théorie des Nombres
de Bordeaux **14** (2002), 87–102

Construction de bases normales pour les extensions galoisiennes absolues à groupe de Galois quaternionien d'ordre 12

par Jean COUGNARD et Jacques QUEYRUT

Résumé. On donne une caractérisation simple pour l'existence des bases normales pour les extensions modérément ramifiées à groupe de Galois quaternionien d'ordre 12. La preuve conduit à un algorithme que l'on illustre par un exemple.

Abstract. We give an easy caracterisation for the existence of normal integral bases for tame quaternionian extensions of degree 12 of the rationals. The proof gives an algorithm.

Soit G le groupe quaternionien d'ordre 12, on s'intéresse aux extensions galoisiennes de $\mathbb{Q}$, modérément ramifiées de groupe de Galois G. Ce travail reprend et complète celui de J. Queyrut paru en 1973 [Q]. Soit $N/\mathbb{Q}$ une telle extension, son anneau des entiers O_N est un $\mathbb{Z}[G]$-module projectif de rang un, étendu à un ordre maximal $\mathcal{M}$ de $\mathbb{Q}[G]$ contenant $\mathbb{Z}[G]$, il est $\mathcal{M}$-stablement libre [F1], le noyau de l'extension des scalaires de $Cl(\mathbb{Z}[G])$ dans $Cl(\mathcal{M})$ contient deux éléments [F2]. À chaque caractère ϕ de G on associe $\Lambda(s,\phi)$, la fonction L d'Artin étendue ; la classe de O_N est déterminée par la valeur $W(\psi)$ de la constante de l'équation fonctionnelle de $\Lambda(s,\psi)$ où ψ est l'unique caractère symplectique de G. Le $\mathbb{Z}[G]$-module O_N est stablement libre si et seulement si $W(\psi) = +1$ [F2]. On sait que les $\mathbb{Z}[G]$-module stablement-libres sont libres [S], on en déduit l'existence d'une base normale. On se propose, comme dans [Q], de reprendre la méthode de Martinet [M2] et de la pousser jusqu'à une construction explicite de la base normale.

Remarques. La construction peut s'appliquer au cas des extensions quaternioniennes modérées de degré 20 pour lesquelles les modules stablement libres sont libres [S] ainsi qu'à celles de degré 16 puisque l'on sait construire une base normale pour les extensions modérément ramifiées de $\mathbb{Q}$ à groupe de Galois D_4 [C] (leur existence est assurée dans ce dernier cas en appliquant

Manuscrit reçu le 27 mars 2001.

conjointement les résultats de [F3] et [S]). La même méthode permet de construire la base normale des entiers d'une extension modérée de $\mathbb{Q}$ dont le groupe de Galois est $D_3 \times C_2$.

1. Le groupe G et ses représentations

Le groupe G est le produit semi-direct d'un groupe cyclique d'ordre 3 et d'un groupe cyclique d'ordre 4, avec un centre d'ordre 2. Il admet la présentation suivante :

$$< \tau,\ \sigma |\ \tau^4 = e,\ \tau^2 = \sigma^3,\ \tau\sigma\tau^{-1} = \sigma^{-1} > .$$

Le centre de G est engendré par σ^3 et son corps N_1 des invariants est une extension à groupe $G/ < \tau^2 > \simeq S_3$ diédral d'ordre 6. Cette extension étant modérément ramifiée, O_{N_1} est $\mathbb{Z}[S_3]$-libre de rang un [M1]. L'unique sous-groupe d'ordre 3 de G est engendré par σ^2 et le groupe quotient $G/ < \sigma^2 >$ est cyclique d'ordre 4, on note E le corps qu'il laisse invariant et E_1 son sous-corps quadratique (E_1 est réel puisque plongeable dans une extension cyclique de degré 4). Le choix de τ comme élément d'ordre 4 détermine une extension cubique K de clôture galoisienne N_1. On se propose de démontrer :

Théorème. *O_N admet une base normale si et seulement si :*

$$\prod_{p, e_p = 3} p \quad \equiv 1 \quad \mathrm{mod}\ 3.$$

Remarque. Le critère montre que l'existence de la base normale tient aux propriétés de ramification dans N_1/E_1 et est indépendant du plongement de l'extension de degré 6 dans l'extension quaternionienne.

On connaît les représentations de G, d'abord celles qui sont relevées de ses quotients :
Les représentations de degré un :

$$\phi_0 \ :\ \sigma \mapsto 1, \quad \tau \mapsto 1$$
$$\phi_1 \ :\ \sigma \mapsto 1, \quad \tau \mapsto -1$$

associées à des facteurs simples de l'algèbre $\mathbb{Q}[G]$ isomorphes à $\mathbb{Q}$;

$$\phi_c \ :\ \sigma \mapsto -1, \quad \tau \mapsto i$$

et sa conjuguée correspondant au facteur simple de $\mathbb{Q}[G]$ isomorphe à $\mathbb{Q}[i]$;
la représentation de degré 2 du groupe S_3 :

$$\phi' \ : \sigma \mapsto \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \quad \tau \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

de caractère ψ' qui donne un facteur simple de $\mathbb{Q}[G]$ isomorphe à $M_2(\mathbb{Q})$.

Il reste la représentation fidèle de degré 2 donnée par :

$$\phi \ : \sigma \mapsto \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix}, \quad \tau \mapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

où ζ est une racine primitive 6-ème de l'unité, de caractère ψ. Elle vient de ce que le groupe multiplicatif des quaternions de Hamilton ($\mathbb{H}(\mathbb{R}) = \mathbb{R}[i,j,k]$ de base $1, i, j, k$ avec les multiplications $i^2 = j^2 = -1$, $ij = -ji = k$) contient un sous-groupe isomorphe à G : on pose $\omega = \frac{1+j\sqrt{3}}{2}$, on a $\omega^3 = -1$, $i\omega(-i) = \omega^{-1}$. On déduit un morphisme d'algèbre de $\mathbb{Q}[G]$ dans $\mathbb{H}(\mathbb{R})$ dont l'image est la sous-algèbre de $\mathbb{H}(\mathbb{R})$ de dimension 4 sur $\mathbb{Q}$ de base $1, i, \omega, \omega i$ en envoyant σ sur ω et τ sur i. On peut calculer le discriminant de l'image de $\mathbb{Z}[G]$ dans cette algèbre à partir des traces réduites des éléments $e_t e_l$ de cette base, on obtient :

$$\begin{vmatrix} 2 & 0 & 1 & 0 \\ 0 & -2 & 0 & -1 \\ 1 & 0 & -1 & 0 \\ 0 & -1 & 0 & -2 \end{vmatrix} = -3^2.$$

Le nombre de places ramifiées dans l'algèbre est pair (loi de réciprocité de Hasse) et est strictement positif (la complétion à l'infini donne les quaternions usuels), l'algèbre ainsi construite est le corps de quaternions ramifié à l'infini et en 3 : $\mathbb{Q}_{(-1,-3)}$; c'est le facteur simple de $\mathbb{Q}[G]$ associé à ϕ. L'image $\Lambda_{(-1,-3)}$ de $\mathbb{Z}[G]$ dans ce corps est un ordre maximal (son discriminant est égal à celui de l'algèbre). On sait [V] que tous les modules sans torsion sur cet ordre sont libres. Pour un quaternion $a + bi + c\omega + d\omega i$, sa trace réduite et sa norme réduite sont données par :

$$\begin{aligned} &Tr(a + bi + c\omega + d\omega i) = 2a + c \\ (1) \qquad &Nr(a + bi + c\omega + d\omega i) = \left(a + \frac{c}{2}\right)^2 + \left(b + \frac{d}{2}\right)^2 + \frac{3}{4}c^2 + \frac{3}{4}d^2 \end{aligned}$$

Les représentations ci-dessus nous donnent des algèbres simples facteurs directs de l'algèbre $\mathbb{Q}[G]$. La comparaison des dimensions prouve l'isomorphisme :

$$\mathbb{Q}[G] \simeq \mathbb{Q} \times \mathbb{Q} \times M_2(\mathbb{Q}) \times \mathbb{Q}(i) \times \mathbb{Q}_{(-1,-3)}.$$

2. Ramification, discriminants

On utilise la formule de Hasse exprimant le discriminant comme produit de conducteurs. Pour chacune des extensions, cette formule nous donne :

$$
(2) \qquad
\begin{aligned}
\Delta_{E_1} &= \mathfrak{f}(\phi_1) \\
\Delta_E &= \mathfrak{f}(\phi_1)\mathfrak{f}(\phi_c)\mathfrak{f}(\overline{\phi_c}) = \mathfrak{f}(\phi_1)\mathfrak{f}(\phi_c)^2 \\
\Delta_{N_1} &= \mathfrak{f}(\phi_1)\mathfrak{f}(\psi')^2 \\
\Delta_N &= \mathfrak{f}(\phi_1)\mathfrak{f}(\phi_c)^2\mathfrak{f}(\psi')^2\mathfrak{f}(\psi)^2
\end{aligned}
$$

Les propriétés de ramification peuvent se déduire de [M1] (chapitre VI) et des propriétés générales de la ramification ([Se] Ch. IV). L'hypothèse de ramification modérée et les formules donnant le conducteur d'Artin d'une représentation induite ([Se] Ch. VI) conduisent aux formules suivantes pour les conducteurs :

$$
(2') \qquad
\begin{aligned}
\mathfrak{f}(\phi_1) &= \prod_{p \text{ ramifié dans } E_1/\mathbb{Q}} p \\
\mathfrak{f}(\phi_c) &= \prod_{p \text{ ramifié dans } E/\mathbb{Q}} p \\
\mathfrak{f}(\psi') &= \left(\prod_{p \text{ ramifié dans } E_1/\mathbb{Q}} p \right) \left(\prod_{p \text{ ramifié dans } N_1/E_1} p \right)^2 \\
\mathfrak{f}(\psi) &= \left(\prod_{p \text{ ramifié dans } N/\mathbb{Q}} p \right)^2 .
\end{aligned}
$$

Puisque l'extension est modérément ramifiée, 2 n'est pas ramifié dans $E/\mathbb{Q}$ et 3 ne l'est pas dans N/E (ni dans N_1/E_1), par contre 2 peut être ramifié dans N_1/E_1 (cf. [M-P]) et 3 l'être dans E/E_1 (mais pas dans $E_1/\mathbb{Q}$ plongeable dans une extension cyclique de degré 4).

Soit $L/M/\mathbb{Q}$ une tour de corps de nombres $L/\mathbb{Q}$ et L/M galoisisiennes ($\mathrm{Gal}(L/\mathbb{Q}) = \Gamma$ et $\mathrm{Gal}(L/M) = H$), L/M cyclique modérément ramifiée de degré premier p ; on note s un générateur de $\mathrm{Gal}(L/M)$. On note $\mathcal{L}$ un $\mathbb{Z}[\Gamma]$-module projectif inclus dans L, $\mathcal{M} = \mathcal{L}^H$ et $\mathcal{T}$ la trace dans L/M, on a $\mathcal{T}(\mathcal{L}) = \mathcal{M}$, $\ker(\mathcal{T})_{|\mathcal{L}} = (1-s)\mathcal{L}$.

Lemme 1. *La suite :*

$$0 \longrightarrow (1-s)\mathcal{L} \oplus \mathcal{M} \longrightarrow \mathcal{L} \xrightarrow{\overline{\mathcal{T}}} \mathcal{M}/p\mathcal{M} \longrightarrow 0$$

où $\overline{\mathcal{T}}$ se déduit de la trace est exacte.

Démonstration. La trace $\mathcal{T}$ est une surjection de $\mathcal{L}$ sur $\mathcal{M}$, soit $y = pu \in p\mathcal{M}$, il existe $c \in \mathcal{L}$ tel que $\mathcal{T}(c) = y = \mathcal{T}(u)$ ce qui veut dire que $z =$

$c - u \in \ker(\mathcal{T})_{|\mathcal{L}} = (1-s)\mathcal{L}$, soit $c = z + u$. L'intersection de $(1-s)\mathcal{L}$ et $\mathcal{M}$ est égale à $\{0\}$. $\square$

On en déduit une relation entre les discriminants de ces modules, relativement à la forme trace $T = T_{L/\mathbb{Q}}$:

$$\Delta_T(\mathcal{L}) = \Delta_T((1-s)\mathcal{L})\Delta_T(\mathcal{M})p^{-2\dim_{\mathbb{Z}}(\mathcal{M})}$$

Comme $\mathcal{M} \subset M$, on a une forme trace T' liée à la trace $T_{M/\mathbb{Q}}$ dans $M/\mathbb{Q}$ et $\Delta_T(\mathcal{M}) = p^{\dim_{\mathbb{Z}}(\mathcal{M})}\Delta_{T'}(\mathcal{M})$ qui transforme la formule précédente en :

$$\Delta_T(\mathcal{L}) = \Delta_T((1-s)\mathcal{L})\Delta_{T'}(\mathcal{M})p^{-\dim_{\mathbb{Z}}(\mathcal{M})}. \tag{3}$$

On applique ceci dans diverses situations. Tout d'abord dans N/N_1 où l'on a une propriété supplémentaire due au degré. En effet si $x, y \in (1-\tau^2)O_N$, $xy \in O_{N_1}$ et $\mathrm{T}_{N/\mathbb{Q}}(xy) = 2\mathrm{T}_{N_1/\mathbb{Q}}(xy)$ ce qui donne :

$$\Delta_N = \Delta_{N_1}\Delta_{\mathrm{T}_{N_1/\mathbb{Q}}}((1-\tau^2)O_N) \tag{3'}$$

et de la même manière dans E/E_1 où l'on obtient :

$$\Delta_E = \Delta_{E_1}\Delta_{\mathrm{T}_{E_1/\mathbb{Q}}}((1-\tau^2)O_E). \tag{3''}$$

On sait que O_E possède une base normale engendrée par un élément v, défini à conjugaison et à multiplication par -1 près. On sait alors que $(1-\tau^2)O_E$ est un $\mathbb{Z}[i]$-module libre de base $\alpha = v - \tau^2 v$ et de $\mathbb{Z}$ base $\{\alpha, \tau(\alpha)\}$. On calcule $\Delta_{\mathrm{T}_{E_1/\mathbb{Q}}}((1-\tau^2)O_E)$ égal à :

$$\begin{vmatrix} \alpha^2 + \tau(\alpha^2) & \alpha\tau(\alpha) + \tau(\alpha)\tau^2(\alpha) \\ \tau(\alpha)\alpha + \tau^2(\alpha)\tau(\alpha) & \tau(\alpha^2) + \tau^2(\alpha^2) \end{vmatrix}$$

ce qui compte-tenu de $\tau^2(\alpha) = -\alpha$ donne :

$$\Delta_{\mathrm{T}_{E_1/\mathbb{Q}}}((1-\tau^2)O_E) = \mathrm{T}_{E_1/\mathbb{Q}}(\alpha^2)^2 \tag{4}$$

qui implique $\mathfrak{f}(\phi_c) = |\mathrm{T}_{E_1/\mathbb{Q}}(\alpha^2)|$.

Proposition 1. *On a l'égalité* $\mathrm{T}_{E_1/\mathbb{Q}}(\alpha^2) = \epsilon\prod_{p|\Delta_E} p$ *avec* $\epsilon = +1$ *(resp.* -1*) si* N *est réel (resp. complexe).*

Démonstration. Pour la valeur absolue, il suffit de comparer les deux expressions du discriminant de $E/\mathbb{Q}$, pour le signe E_1 est réelle et $E = E_1\left(\sqrt{\alpha^2}\right) = E_1\left(\sqrt{\tau(\alpha^2)}\right)$ montre que α^2 et son conjugué sont de même signe, négatif si et seulement si E est complexe. $\square$

3. Première réduction

Le diagramme suivant :

$$\begin{array}{ccccccccc}
0 & \longrightarrow & (1+\tau^2)O_N & \longrightarrow & O_N & \longrightarrow & O_N/O_{N_1} & \longrightarrow & 0 \\
 & & \Big\| & & \Big\| & & \downarrow\simeq & & \\
0 & \longrightarrow & O_{N_1} & \longrightarrow & O_N & \xrightarrow{1-\tau^2} & (1-\tau^2)O_N & \longrightarrow & 0
\end{array}$$

est commutatif, les applications sont des morphismes de $\mathbb{Z}[G]$-modules car τ^2 est dans le centre de G. Le noyau $(1-\tau^2)O_N$ de l'application trace (surjective, de O_N dans O_{N_1}) est un module sur l'algèbre $\Lambda = \mathbb{Z}[G]/(1+\tau^2)$, cette algèbre est isomorphe à l'image de $\mathbb{Z}[G]$ dans $\mathbb{Q}(i) \oplus \mathbb{Q}_{(-1,-3)}$. Il en résulte que O_N/O_{N_1} est isomorphe à $\mathbb{Z}[G]/(1+\tau^2) \otimes_{\mathbb{Z}[G]} O_N$, c'est un Λ-module projectif.

Si O_N admet une base normale, le Λ-module O_N/O_{N_1} est libre et $O_{N_1} = (1+\tau^2)O_N$ est libre sur $\mathbb{Z}[S_3] \simeq \mathbb{Z}[G]/(1-\tau^2)$, montrons que la réciproque est vérifiée.

Proposition 2. *O_N admet une base normale si et seulement si le Λ-module O_N/O_{N_1} et le $\mathbb{Z}[S_3]$-module O_{N_1} sont libres.*

Démonstration. Il ne reste que la réciproque à établir. Pour cela, on se base sur les produits fibrés :

$$\begin{array}{ccc}
\mathbb{Z}[G] & \longrightarrow & \mathbb{Z}[G]/(1+\tau^2) \simeq \Lambda \\
\downarrow & & \downarrow \\
\mathbb{Z}[G]/(1-\tau^2) \simeq \mathbb{Z}[S_3] & \longrightarrow & \mathbb{Z}/2\mathbb{Z}[S_3]
\end{array}
\qquad
\begin{array}{ccc}
O_N & \longrightarrow & O_N/O_{N_1} \\
\downarrow & & \downarrow \\
O_{N_1} & \longrightarrow & O_{N_1}/2O_{N_1}
\end{array}$$

Si le morphisme d'anneaux $\mathbb{Z}[S_3] \longrightarrow \mathbb{Z}/2\mathbb{Z}[S_3]$ vérifie les conditions de Milnor [M] (i.e. si le morphisme de groupes de $\mathbb{Z}[S_3]^*$ dans $\mathbb{Z}/2\mathbb{Z}[S_3]^*$ qui s'en déduit est surjectif) alors O_N est $\mathbb{Z}[S_3]$-libre, c'est ce qu'on établit dans le lemme suivant.

Lemme 2. *Le morphisme de groupes de $\mathbb{Z}[S_3]^*$ dans $\mathbb{Z}/2\mathbb{Z}[S_3]^*$ déduit de la réduction modulo 2 est surjectif.*

Démonstration du lemme : Dans l'algèbre $\mathbb{Q}[S_3] \simeq \mathbb{Q} \oplus \mathbb{Q} \oplus M_2(\mathbb{Q})$, le facteur $\mathbb{Q} \oplus \mathbb{Q}$ est isomorphe à $\mathbb{Q}[C_2]$ (C_2, groupe cyclique d'ordre 2) et est égal à $\frac{1+\sigma+\sigma^2}{3}\mathbb{Q}[S_3]$, comme l'idempotent central $\frac{1+\sigma+\sigma^2}{3}$ est inversible dans $\mathbb{Z}/2\mathbb{Z}[S_3]$, on en déduit que $\mathbb{Z}/2\mathbb{Z}[S_3] \simeq \mathbb{Z}/2\mathbb{Z}[C_2] \oplus M_2(\mathbb{F}_2)$ et donc :

$$\mathbb{Z}/2\mathbb{Z}[S_3]^* \simeq \mathbb{Z}/2\mathbb{Z}[C_2]^* \oplus \mathrm{Gl}_2(\mathbb{F}_2) \simeq \mathbb{Z}/2\mathbb{Z}[C_2]^* \oplus S_3$$

qui est d'ordre 12. L'image de S_3, engendrée par les images de σ, égale à $(\overline{\sigma}, \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right))$, et de τ, égale à $(\overline{\tau}, \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right))$ est isomorphe à S_3. Par ailleurs, l'élément $\sigma - \sigma^2 + \tau(1+\sigma-\sigma^2) \notin S_3$ de $\mathbb{Z}[S_3]$ a pour image $\big(1, -1, \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)\big)$

dans la décomposition de $\mathbb{Q}[S_3]$, c'est un élément d'ordre 2 donc il appartient à $\mathbb{Z}[S_3]^*$, son image dans $\mathbb{Z}/2\mathbb{Z}[C_2]^* \oplus \mathrm{Gl}_2(\mathbb{F}_2)$ est égale à $(\overline{\tau}, (\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}))$ qui n'appartient pas à l'image de S_3, on en déduit bien la surjectivité voulue. Ceci termine le démonstration du lemme et celle de la proposition. $\square$

Remarque. Si θ_1 est une base normale de O_{N_1} et θ' une Λ-base de $(1-\tau^2)O_N$, il existe une unité ϵ de $\mathbb{Z}[S_3]$ (qui appartient soit à S_3, soit à $(\sigma - \sigma^2 + \tau(1+\sigma-\sigma^2))S_3$) telle que $\epsilon\theta_1 - \theta' \equiv 0 \bmod (2O_N)$ et $(\epsilon\theta_1 - \theta')/2$ est une base normale de O_N.

Corollaire 1. *Le $\mathbb{Z}[G]$-module O_N possède une base normale si et seulement si $(1-\tau^2)O_N$ est un Λ-module libre.*

Démonstration. On sait que O_{N_1} est $\mathbb{Z}[S_3]$-libre lorsque $N/\mathbb{Q}$ est modérément ramifiée [M1]. $\square$

4. Réduction pour l'étude de $(1-\tau^2)O_N$

Les représentations fournies par $(1-\tau^2)O_N$ sont les deux représentations irréductibles qui ne se factorisent pas par S_3. On va introduire une décomposition de $(1-\tau^2)O_N$ pour exploiter cette propriété. La trace dans N/E associe à x, $T_{N/E}(x) = x + \sigma^2(x) + \sigma^4(x)$, comme $\tau^2 = \sigma^3$ est dans le centre de G, la trace applique $(1-\tau^2)O_N = (1-\sigma^3)O_N$ dans $(1-\tau^2)O_E$ noyau de la trace dans l'extension E/E_1 restreinte à O_E.

Lemme 3. *La trace dans N/E induit une surjection de $(1-\tau^2)O_N$ sur $(1-\tau^2)O_E$.*

Démonstration. C'est immédiat puisque la trace est surjective de O_N sur O_E et que σ^2 commute avec τ^2. $\square$

Lemme 4. *Le noyau de la trace dans N/E restreinte à $(1-\tau^2)O_N$ est égal à $(1-\sigma^2)(1-\tau^2)O_N$.*

Démonstration. Soit x dans le noyau de la trace dans N/E restreinte à $(1-\tau^2)O_N$, il existe $t \in O_N$ tel que $x = t - \sigma^2(t)$ et il faut montrer que t peut être choisi dans $(1-\tau^2)O_N$. On sait que l'on a aussi $\sigma^3(x) = -x$ soit $\sigma^3(t) - \sigma^5(t) = -t + \sigma^2(t)$, ce qui donne $t + \sigma^3(t) = \sigma^2(t + \sigma^3(t))$ et montre que $t + \sigma^3(t)$ qui appartient à N_1 est invariant par σ^2, c'est un élément de E_1, on peut donc l'écrire $u + \sigma^3(u)$, $u \in O_E$. Il en résulte qu'il existe $u \in O_E$ tel que $t - u = -\sigma^3(t-u) \in (1-\tau^2)O_N$ et $(t-u) - \sigma^2(t-u) = t - \sigma^2(t) = x$. $\square$

On peut résumer ces deux lemmes par la suite exacte :

$$(5)\quad 0 \longrightarrow (1-\sigma^2)(1-\tau^2)O_N \longrightarrow (1-\tau^2)O_N \xrightarrow{1+\sigma^2+\sigma^4} (1-\tau^2)O_E \longrightarrow 0$$

On en déduit que $(1-\tau^2)O_E \simeq (1-\tau^2)O_N/(1-\sigma^2)(1-\tau^2)O_N$ est un module projectif sur $\Lambda/(1-\sigma^2)$ mais on remarque que dans Λ, $\sigma^3 = -1$;

on en déduit $1-\sigma^2 = 1-\sigma^3\sigma^{-1} = 1+\sigma^{-1}$ qui engendre le même idéal bilatère que $1+\sigma$. Il n'est pas difficile de constater que $\Lambda/(1+\sigma) \simeq \mathbb{Z}[i]$:

Soit le morphisme d'anneaux de $\Lambda = \mathbb{Z}[G]/(1+\tau^2)$ sur $\mathbb{Z}[i]$ obtenu en envoyant τ sur i et σ sur -1. L'image de $a+b\tau+c\sigma+d\sigma\tau+e\sigma^2+f\sigma^2\tau$ est égale à $(a-c+e)+(b-d+f)i$, elle est nulle si et seulement si $e=-a+c$, $f=-b+d$, les éléments du noyau sont ceux de la forme $a(1-\sigma^2)+c(1+\sigma)+b(1-\sigma^2)\tau+d(1+\sigma)\tau$ ils sont dans l'idéal engendré par $1+\sigma$ qui est lui-même dans le noyau. On a bien :

$$\mathbb{Z}[i] \simeq \Lambda/(1+\sigma).$$

Finalement

$$(1-\tau^2)O_E \simeq \Lambda/(1+\sigma) \otimes_\Lambda (1-\tau^2)O_N$$

est un $\mathbb{Z}[i]$-module sans torsion, donc libre (ce que l'on avait rappelé en considérant uniquement l'extension $E/\mathbb{Q}$).

On s'intéresse à la structure de $(1-\sigma^2)(1-\tau^2)O_N$, noyau de la trace dans N/E restreinte à $(1-\tau^2)O_N$, c'est d'abord un sous-Λ-module sans $\mathbb{Z}$-torsion de $(1-\tau^2)O_N$, il est annulé par $1+\sigma^2+\sigma^4$ qui, dans Λ, est égal à $1-\sigma+\sigma^2$. On peut aussi l'interpréter au moyen de la suite exacte :

$$0 \longrightarrow \big((1-\tau^2)O_N\big)^{<\sigma^2>} \longrightarrow (1-\tau^2)O_N \xrightarrow{1-\sigma^2} (1-\sigma^2)(1-\tau^2)O_N \longrightarrow 0$$

Mais dire que $y \in \big((1-\tau^2)O_N\big)^{<\sigma^2>}$ revient à dire que y est dans E et de trace nulle dans E/E_1 donc est de la forme $y = x-\tau^2(x)$, $x \in O_E$. On obtient ainsi une autre structure de Λ-module sur $(1-\sigma^2)(1-\tau^2)O_N$ car la multiplication par $1-\sigma^2$ n'est pas un morphisme de Λ module. Le lemme précédent nous dit donc que $\big((1-\tau^2)O_N\big)^{<\sigma^2>} = (1+\sigma^2+\sigma^4)(1-\tau^2)O_N = (1-\sigma+\sigma^2)(1-\tau^2)O_N$. On conclut, pour cette structure que :

$$(1-\sigma^2)(1-\tau^2)O_N \simeq \Lambda/(1-\sigma+\sigma^2) \otimes_\Lambda (1-\tau^2)O_N$$

On peut étudier le Λ-module projectif $(1-\tau^2)O_N$ au moyen du diagramme commutatif :

$$\begin{tikzcd}
(1-\tau^2)O_N \arrow[r, equal] \arrow[d, "1+\sigma^2+\sigma^4"] & (1-\tau^2)O_N \arrow[r, "\frac{\Lambda}{1-\sigma+\sigma^2}\otimes_\Lambda"] \arrow[d, "\frac{\Lambda}{1+\sigma}\otimes_\Lambda"] & \frac{(1-\tau^2)O_N}{(1-\tau^2)O_E} \arrow[d, "1+\sigma^2+\sigma^4"] \\
(1-\tau^2)O_E \arrow[r, "\simeq"] & \frac{(1-\tau^2)O_N}{(1+\sigma)(1-\tau^2)O_N} \arrow[r] & \frac{(1-\tau^2)O_E}{3(1-\tau^2)O_E}
\end{tikzcd} \tag{6}$$

associé à la décomposition de Λ donnée par :

$$\begin{tikzcd}
\Lambda \arrow[r] \arrow[d] & \Lambda/(1-\sigma+\sigma^2) \arrow[d] \\
\mathbb{Z}[i] \arrow[r] & \mathbb{Z}[i]/3\mathbb{Z}[i]
\end{tikzcd}$$

On montre que les idéaux $(1-\sigma)$ et $(1-\sigma+\sigma^2)$ ont une intersection réduite à $\{0\}$. Les diagrammes ci-dessus sont des produits fibrés.

5. L'anneau Λ et ses quotients

$\Lambda_{(-1,-3)}$ est un ordre maximal de $\mathbb{Q}_{(-1,-3)}$ de $\mathbb{Z}$-base $1, i, \omega, \omega i$. Construisons le morphisme d'anneaux de Λ dans $\Lambda_{(-1,-3)}$ obtenu en envoyant l'image de τ sur i et celle de σ sur ω. L'image de $a+b\tau+c\sigma+d\sigma\tau+e\sigma^2+f\sigma^2$ est égale à $a+bi+c\omega+d\omega i+e\omega+f\omega i$ qui peut se récrire $(a-e)+(b-f)i+(c+e)\omega+(d+f)\omega i$, cette image est nulle si et seulement si $a=e=-c$, $b=f=-d$, le noyau est donc formé des éléments $a(1-\sigma+\sigma^2)+b(1-\sigma+\sigma^2)\tau$ c'est donc l'idéal bilatère engendré par $1-\sigma+\sigma^2$. On a donc l'isomorphisme :

$$\Lambda_{(-1,-3)} \simeq \Lambda/(1-\sigma+\sigma^2)$$

Rappelons que tout module projectif sur $\mathbb{Z}[i]$ est libre ainsi que tout module projectif sur l'ordre maximal $\Lambda_{(-1,-3)}$ [V]. On a ainsi, pour tout Λ-module projectif de rang un :

$$\begin{array}{ccc} \Lambda & \longrightarrow & \Lambda_{(-1,-3)} \simeq \Lambda/(1-\sigma+\sigma^2) \\ \downarrow & & \downarrow \\ \Lambda/(1+\sigma) \simeq \mathbb{Z}[i] & \longrightarrow & \mathbb{Z}[i]/3 \simeq \mathbb{F}_9 \end{array}$$

$$\begin{array}{ccc} M & \longrightarrow & M/(1-\sigma+\sigma^2) \\ \downarrow & & \downarrow \\ M/(1+\sigma) & \longrightarrow & M/(3, 1+\sigma) \end{array}$$

Le module M étant projectif le $\Lambda_{(-1,-3)}$-module (resp. $\mathbb{Z}[i]$-module) $M/(1-\sigma+\sigma^2)$ (resp. $M/(1+\sigma)$) est libre. On en déduit que l'ensemble des classes d'isomorphismes de Λ-modules de type fini sans torsion est en bijection avec $\mathrm{im}(\mathbb{Z}[i]^*)\backslash(\mathbb{Z}[i]/3)^*/\mathrm{im}(\Lambda^*_{-1,-3})$. Le groupe $(\mathbb{Z}[i]/3)^* \simeq \mathbb{F}_9^*$ est cyclique d'ordre 8 (engendré par l'image de $1+\tau$) et l'image de $\mathbb{Z}[i]^*$ en est un sous-groupe cyclique d'ordre 4. Il nous faut maintenant déterminer le groupe $\Lambda^*_{(-1,-3)}$. On sait que ce sont les éléments de $\Lambda_{(-1,-3)}$ de norme réduite 1. Pour cela, on a vu (1) que $a+bi+c\omega+d\omega i$ a pour norme réduite $(a+\frac{c}{2})^2+(b+\frac{d}{2})^2+\frac{3c^2}{4}+\frac{3d^2}{4}$. On étudie cas par cas l'égalité à 1 et on constate que les seules unités de $\Lambda_{(-1,-3)}$ sont les images de G. Comme dans G, il n'y a pas d'élément d'ordre 8, l'image de $\Lambda^*_{(-1,-3)}$ dans $\mathbb{F}_9^*$ est incluse dans le sous-groupe cyclique d'ordre 4. On peut donc conclure qu'il y a deux classes d'isomorphisme de Λ-modules projectifs de rang un. On redonne la démonstration du :

Théorème 2 ([Q]). *Si $N/\mathbb{Q}$ est modérément ramifiée, on peut trouver une base α de $(1-\tau^2)O_E$ et une base β de $(1-\sigma^2)(1-\tau^2)O_N$ telles que l'une* *des congruences suivantes qui s'excluent ait lieu :*

$$\alpha \equiv (1+2\sigma^2)\beta \mod 3(1-\tau^2)O_N$$
$$\alpha \equiv (1+2\sigma^2)(1+\tau)\beta \mod 3(1-\tau^2)O_N$$

et O_N admet une base normale si et seulement si la première de ces congruences est vérifiée.

Démonstration. On a démontré que le diagramme commutatif est un produit fibré. Les modules $(1-\tau^2)O_E \simeq \frac{(1-\tau^2)O_N}{(1-\sigma^2)(1-\tau^2)O_E}$ et $\frac{(1-\tau^2)O_N}{(1-\tau^2)O_E} \simeq (1-\sigma^2)(1-\tau^2)O_N$ sont des modules libres (le premier sur $\mathbb{Z}[i]$, le second, muni de la structure quotient, sur $\Lambda_{(-1,-3)}$), le module O_N est un module libre si et seulement si on peut choisir une base α (de $(1-\tau^2)O_E$) et une base β (de $(1-\sigma^2)(1-\tau^2)O_N$) telles qu'elles aient même image dans $\frac{(1-\tau^2)O_E}{3(1-\tau^2)O_E}$. Comme $\frac{(1-\tau^2)O_E}{3(1-\tau^2)O_E}$ est un espace vectoriel de dimension un sur $\mathbb{F}_9$, il existe un élément $\epsilon \in \mathbb{F}_9^*$ tel que $\overline{\alpha} = \epsilon\overline{\beta}$. On aura donc une $\mathbb{Z}[G]$-base de O_N si ϵ peut-être choisi dans le sous-groupe d'ordre 4 de $\mathbb{F}_9^*$. Quitte à changer l'une des bases α, β on peut supposer que l'on a soit $\overline{\alpha} = \overline{\beta}$ soit $\overline{\alpha} = (1+\tau)\overline{\beta}$.

Appelons β' celui des éléments qui satisfait une de ces deux relations qui s'excluent mutuellement. Il existe alors (on a un produit fibré) un unique $\theta \in (1-\tau^2)O_N$ tel que $\alpha = \mathrm{T}_{\mathrm{N/E}}(\theta)$, $\beta' = (1-\sigma^2)\theta$ (il suffit de prendre $\theta = \dfrac{\alpha - (1+2\sigma^2)\sigma^2(\beta')}{3}$). On a alors :

$$\begin{aligned}\alpha = \theta + \sigma^2(\theta) + \sigma^4(\theta) = \theta - \sigma^2(\theta) + 2\sigma^2(\theta) - 2\sigma^4(\theta) + 3\sigma^4(\theta) \\ = (1+2\sigma^2)\beta' + 3\sigma^4(\theta)\end{aligned}$$

ce qui montre que les congruences sont vérifiées.

Supposons, réciproquement, que l'on a $\alpha \equiv (1+2\sigma^2)\beta' \mod 3(1-\tau^2)O_N$. Il existe $z \in (1-\tau^2)O_N$ tel que $\beta' = (1-\sigma^2)(z)$ ce qui donne :

$$(1+2\sigma^2)(\beta') = z - \sigma^2(z) + 2\sigma^2(z) - 2\sigma^4(z) = \mathrm{T}_{N/E}(z) - 3\sigma^4(z).$$

On en déduit que $\alpha - \mathrm{T}_{N/E}(z) \in \mathrm{T}_{N/E}((1-\tau^2)O_N) \cap 3(1-\tau^2)O_N)$, comme 3 n'est pas ramifié dans N/E, $\alpha - \mathrm{T}_{N/E}(z) \in 3(1-\tau^2)O_E$, α et β' ont bien la même image dans $(1-\tau^2)O_E)/3(1-\tau^2)O_E$ (rappelons que l'on a choisi sur $(1-\sigma^2)(1-\tau^2)O_N$ la structure de Λ-module qui vient du quotient de $(1-\tau^2)O_N/(1-\tau^2)O_E$.

La première congruence est équivalente à $(1-\tau^2)O_N$ Λ-libre mais on a vu que cette propriété implique l'existence d'une base normale. $\square$

On se propose de traduire ce théorème en une propriété sur le corps des rationnels.

Corollaire 1. *Si 3 n'est pas ramifié dans E/E_1, les éléments α et β vérifient l'une des deux congruences qui s'excluent mutuellement :*

$$\begin{aligned} \mathrm{T}_{E_1/\mathbb{Q}}(\alpha^2) &\equiv -\mathrm{T}_{N_1/\mathbb{Q}}(\beta^2) \mod 3 \\ \mathrm{T}_{E_1/\mathbb{Q}}(\alpha^2) &\equiv \mathrm{T}_{N_1/\mathbb{Q}}(\beta^2) \mod 3 \end{aligned}$$

avec cette condition, O_N possède une base normale si et seulement si la première de ces congruences est vérifiée.

Démonstration. On pose $\lambda = 1$ ou $1+\tau$ suivant le cas. On a la congruence $\alpha - (1+2\sigma^2)\lambda\beta \equiv 0 \mod 3(1-\tau^2)O_N$; si on élève au carré, le membre de gauche appartient à O_{N_1} et est divisible par 9. On développe le carré : $\alpha^2 + [(1+2\sigma^2)\lambda\beta]^2 - 2\alpha(1+2\sigma^2)\lambda\beta$.

On prend d'abord la trace sur E_1, comme $\alpha^2 \in E_1$, $\mathrm{T}_{N_1/E_1}(\alpha^2) = 3\alpha^2$, ensuite

$$\mathrm{T}_{N_1/E_1}(\alpha(1+2\sigma^2)\lambda\beta) = \mathrm{T}_{N/E}(\alpha(1+2\sigma^2)\lambda\beta) = \alpha\mathrm{T}_{N/E}((1+2\sigma^2)\lambda\beta) = 0$$

car $\lambda\beta \in (1-\sigma^2)(1-\tau^2)O_N$. On obtient donc $3\alpha^2 \equiv -\mathrm{T}_{N_1/E_1}([\lambda\beta + 2\sigma^2(\lambda\beta)]^2) \mod 9O_{E_1}$. Étudions séparément ce qui se passe pour chacune des valeurs de λ.

Si $\lambda = 1$. On a $\mathrm{T}_{N_1/E_1}([\beta+2\sigma^2(\beta)]^2) = \mathrm{T}_{N_1/E_1}(\beta^2) + 4\mathrm{T}_{N_1/E_1}(\sigma^2(\beta^2) + 4\mathrm{T}_{N_1/E_1}(\beta\sigma^2(\beta))$, on évalue le dernier terme en remarquant que

$$0 = \mathrm{T}_{N/E}(\beta)^2 = (\beta + \sigma^2(\beta) + \sigma^4(\beta))^2 = \mathrm{T}_{N_1/E_1}(\beta^2) + 2\mathrm{T}_{N_1/E_1}(\beta\sigma^2(\beta))$$

d'où l'on déduit $4\mathrm{T}_{N_1/E_1}(\beta\sigma^2(\beta)) = -2\mathrm{T}_{N_1/E_1}(\beta^2))$ ce qui donne $3\alpha^2 \equiv -3\mathrm{T}_{N_1/E_1}(\beta^2)) \mod 9O_{E_1}$, soit

$$\alpha^2 \equiv -\mathrm{T}_{N_1/E_1}(\beta^2)) \qquad \mod 3O_{E_1}$$

d'où l'on déduit la première congruence.

Si $\lambda = 1+\tau$. On peut reprendre le même calcul en remplaçant β par $\beta' = \beta+\tau\beta$. On obtient alors : $\alpha^2 \equiv -\mathrm{T}_{N_1/E_1}((\beta+\tau\beta)^2)) \mod 3O_{E_1}$. En prenant la trace sur $\mathbb{Q}$ on a $\mathrm{T}_{E_1/\mathbb{Q}}(\alpha^2) \equiv -\mathrm{T}_{N_1/\mathbb{Q}}((\beta+\tau\beta)^2))$, mais $\mathrm{T}_{N_1/\mathbb{Q}}((\beta+\tau\beta)^2)) = \mathrm{T}_{N_1/\mathbb{Q}}(\beta^2 + \tau(\beta)^2 + 2\beta\tau\beta))$ or $\mathrm{T}_{N_1/\mathbb{Q}}(2\beta\tau\beta) = \mathrm{T}_{N/\mathbb{Q}}(\beta\tau\beta)$ ce dernier terme est invariant par τ et en même temps $\tau(\mathrm{T}_{N/\mathbb{Q}}(\beta\tau\beta)) = \mathrm{T}_{N/\mathbb{Q}}(\tau\beta\tau^2\beta) = -\mathrm{T}_{N/\mathbb{Q}}(\beta\tau\beta)$ et est donc nul. Il ne reste alors que

$$\mathrm{T}_{E_1/\mathbb{Q}}(\alpha^2) \equiv -\mathrm{T}_{N_1/\mathbb{Q}}(\beta^2 + \tau(\beta)^2) \equiv \mathrm{T}_{N_1/\mathbb{Q}}(\beta^2) \mod 3.$$

L'hypothèse de ramification implique que $\mathrm{T}_{E_1/\mathbb{Q}}(\alpha^2)$ est premier avec 3, les deux congruences sont incompatibles. □

Supposons maintenant que 3 est ramifié dans E/E_1, on sait (proposition 1) que $\mathrm{T}_{E_1/\mathbb{Q}}(\alpha^2) \equiv 0 \mod 3$ et $\not\equiv 0 \mod 9$.

On reprend la congruence $\alpha - (1+2\sigma^2)\lambda\beta \equiv 0 \mod 3(1-\tau^2)O_N$ si on suppose 3 ramifié, il l'est dans N/N_1 et $(1-\tau^2)O_N$ est congru à 0 modulo le produit des idéaux premiers au-dessus de 3 dans N, si on élève au carré, on obtient cette fois-ci : $\alpha^2 + [(1+2\sigma^2)\lambda\beta]^2 - 2\alpha(1+\sigma^2)\lambda\beta \equiv 0 \bmod 27$. Les calculs se poursuivent comme précédemment et on aboutit à :

Corollaire 2. *Si 3 est ramifié dans E/E_1, les éléments α et β vérifient l'une des deux congruences qui s'excluent mutuellement :*

$$\begin{aligned} \mathrm{T}_{E_1/\mathbb{Q}}(\alpha^2) &\equiv -\mathrm{T}_{N_1/\mathbb{Q}}(\beta^2) \mod 9 \\ \mathrm{T}_{E_1/\mathbb{Q}}(\alpha^2) &\equiv \mathrm{T}_{N_1/\mathbb{Q}}(\beta^2) \mod 9 \end{aligned}$$

dans ce cas condition, O_N possède une base normale si et seulement si la première de ces congruences est vérifiée.

Il reste à donner une expression plus simple de $T_{N_1/\mathbb{Q}}(\beta^2)$.

6. Calcul d'indice

La proposition 1 et les identités (2), (2') du paragraphe 2 montrent que l'on peut écrire $\Delta_N = \Delta_{N_1}\mathrm{T}_{E_1/\mathbb{Q}}(\alpha^2)^2\mathfrak{f}(\psi)^2$ ce qui comparé à la formule (3′) donnant également ce discriminant implique :

$$\Delta_{\mathrm{T}_{N_1/\mathbb{Q}}}((1-\tau^2)O_N) = \left(\mathrm{T}_{E_1/\mathbb{Q}}(\alpha^2)\right)^2 \mathfrak{f}(\psi)^2 = \left(\mathrm{T}_{E_1/\mathbb{Q}}(\alpha^2)\right)^2 \mathfrak{A}^4$$

où $\mathfrak{A} = \prod_{p \text{ ramifié dans } N/\mathbb{Q}} p$.

Si on se place dans l'extension N/E cyclique de degré 3 dont le groupe de Galois est engendré par σ^2, avec le module $(1-\tau^2)O_N$, comme $(1-\tau^2)O_E$ est de dimension 2, on obtient grâce à (3) :

$$\Delta_{\mathrm{T}_{N_1/\mathbb{Q}}}((1-\tau^2)O_N) = \frac{1}{9}\Delta_{\mathrm{T}_{E_1/\mathbb{Q}}}((1-\tau^2)O_E)\Delta_{\mathrm{T}_{N_1/\mathbb{Q}}}((1-\sigma^2)(1-\tau^2)O_N)$$

On peut maintenant calculer $\Delta_{\mathrm{T}_{N_1/\mathbb{Q}}}((1-\sigma^2)(1-\tau^2)O_N)$ en utilisant la formule ci-dessus, (2), (2') et la proposition (1), ce qui donne :

$$\begin{aligned} \Delta_{\mathrm{T}_{N_1/\mathbb{Q}}}((1-\tau^2)O_N) &= \frac{1}{9}\Delta_{\mathrm{T}_{E_1/\mathbb{Q}}}((1-\tau^2)O_E)\Delta_{\mathrm{T}_{N_1/\mathbb{Q}}}((1-\sigma^2)(1-\tau^2)O_N) \\ &= \frac{1}{9}\left(\mathrm{T}_{E_1/\mathbb{Q}}(\alpha^2)\right)^2 \Delta_{\mathrm{T}_{N_1/\mathbb{Q}}}((1-\sigma^2)(1-\tau^2)O_N) \\ &= \left(\mathrm{T}_{E_1/\mathbb{Q}}(\alpha^2)\right)^2 \mathfrak{A}^4. \end{aligned}$$

D'où l'on déduit :

$$\Delta_{\mathrm{T}_{N_1/\mathbb{Q}}}((1-\sigma^2)(1-\tau^2)O_N) = 9\mathfrak{A}^4.$$

On peut également calculer ce discriminant au moyen de sa base β comme $\Lambda_{(-1,-3)}$-module. Il possède en effet une $\mathbb{Z}$-base $\{\beta, \sigma(\beta), \tau(\beta), \tau\sigma(\beta)\}$ ce qui conduit au calcul :

$$\Delta_{\mathrm{T}_{N_1/\mathbb{Q}}}((1-\sigma^2)(1-\tau^2)O_N)$$
$$= \begin{vmatrix} \mathrm{T}_{N_1/\mathbb{Q}}(\beta^2) & \mathrm{T}_{N_1/\mathbb{Q}}(\beta\sigma(\beta)) & \mathrm{T}_{N_1/\mathbb{Q}}(\beta\tau(\beta)) & \mathrm{T}_{N_1/\mathbb{Q}}(\beta\tau\sigma(\beta)) \\ \mathrm{T}_{N_1/\mathbb{Q}}(\sigma(\beta)\beta) & \mathrm{T}_{N_1/\mathbb{Q}}(\sigma(\beta)^2) & \mathrm{T}_{N_1/\mathbb{Q}}(\sigma(\beta)\tau(\beta)) & \mathrm{T}_{N_1/\mathbb{Q}}(\sigma(\beta)\tau\sigma(\beta)) \\ \mathrm{T}_{N_1/\mathbb{Q}}(\tau(\beta)\beta) & \mathrm{T}_{N_1/\mathbb{Q}}(\tau(\beta)\sigma(\beta)) & \mathrm{T}_{N_1/\mathbb{Q}}(\tau(\beta)^2) & \mathrm{T}_{N_1/\mathbb{Q}}(\tau(\beta)\tau\sigma(\beta)) \\ \mathrm{T}_{N_1/\mathbb{Q}}(\tau\sigma(\beta)\beta) & \mathrm{T}_{N_1/\mathbb{Q}}(\tau\sigma(\beta)\sigma(\beta)) & \mathrm{T}_{N_1/\mathbb{Q}}(\tau\sigma(\beta)\tau(\beta)) & \mathrm{T}_{N_1/\mathbb{Q}}(\tau\sigma(\beta)^2) \end{vmatrix}$$

En utilisant les relations $\beta + \sigma^2(\beta) + \sigma^4(\beta) = 0$ et $\tau^2(\beta) = -\beta$ on a facilement :

$$\Delta_{\mathrm{T}_{N_1/\mathbb{Q}}}((1-\sigma^2)(1-\tau^2)O_N) = \begin{vmatrix} \mathrm{T}_{N_1/\mathbb{Q}}(\beta^2) & -\frac{1}{2}\mathrm{T}_{N_1/\mathbb{Q}}(\beta^2) \\ -\frac{1}{2}\mathrm{T}_{N_1/\mathbb{Q}}(\beta^2) & \mathrm{T}_{N_1/\mathbb{Q}}(\beta^2) \end{vmatrix}^2$$
$$= \frac{9}{16}\left(\mathrm{T}_{N_1/\mathbb{Q}}(\beta^2)\right)^4$$

Proposition 3. *On a l'égalité* $\mathrm{T}_{N_1/\mathbb{Q}}(\beta^2) = 2\epsilon\prod_{q|\Delta_N} q$ *où* $\epsilon = +1$ *(resp.* -1*) si* $N/\mathbb{Q}$ *est réelle (resp. imaginaire).*

Démonstration. Pour la valeur absolue cela se déduit des deux égalités précédentes et pour le signe avec les mêmes arguments que dans la proposition 1. □

En comparant les valeurs de $T_{N_1/\mathbb{Q}}(\beta^2)$, $T_{E_1/\mathbb{Q}}(\alpha^2)$ et les corollaires 1 et 2 de la section précédent, on a maintenant un critère de base normale. Il suffit de remarquer que si 3 est ramifié N, il l'est dans E. Les deux corollaires se transforment en :

O_N admet une base normale si et seulement si :

$$\prod_{p|\Delta_E, p\neq 3} p \equiv -2 \prod_{q|\Delta_N, q\neq 3} q \mod 3$$

ce qui après simplification donne l'énoncé du théorème 1.

Pour la construction, le seul point qui reste est la détermination de la $\Lambda_{(-1,-3)}$-base β de $(1-\sigma^2)(1-\tau^2)O_N$. Considérons le sous-module $(1-\sigma^2)O_{N_1}$ de O_{N_1}, il est libre sur $\mathbb{Z}[S_3]/(1+\sigma^2+\sigma^4)$ puisque O_{N_1} possède une base normale, il possède donc une $\mathbb{Z}$-base $\{\gamma, \tau(\gamma), \sigma^4(\gamma), \tau\sigma^4(\gamma)\}$ constructible (puisque la base normale de O_{N_1} l'est (cf. [M1] chapitre 6)). Si on construit maintenant le $\mathbb{Z}$-module de base $\{\gamma\alpha, \tau(\gamma)\alpha, \sigma^4(\gamma)\alpha, \tau\sigma^4(\gamma)\alpha\}$ il est inclus dans O_N, annulé par $1+\tau^2$ et par $1+\sigma^2+\sigma^4$, c'est un sous-$\Lambda_{(-1,-3)}$ module libre de base $\gamma\alpha$. Si on connaît son indice dans $(1-\sigma^2)(1-\tau^2)O_N = \Lambda_{(-1,-3)}\beta$ on va pouvoir déterminer β. En effet on peut alors écrire $\mathcal{I}^{-1}\Lambda_{(-1,-3)}\gamma\alpha = \Lambda_{(-1,-3)}\beta \subset O_N$ avec un idéal $\mathcal{I}$ de $\Lambda_{(-1,-3)}$ (donc principal) engendré par un élément ρ de norme réduite connue. Comme la norme réduite est une forme quadratique définie positive on a un nombre fini de possibilités pour ρ (défini à multiplication à droite près par une unité de $\Lambda_{(-1,-3)}$), le critère d'intégralité permet alors de conclure et d'obtenir β à conjugaison près. Il faut donc calculer l'indice des deux $\Lambda_{(-1,-3)}$ modules libres engendrés l'un par $\gamma\alpha$ l'autre par β. Pour cela il suffit de calculer leurs discriminants relativement à la forme trace qui se déduit de celle de $N_1/\mathbb{Q}$. Pour le premier, il est donné par la proposition 3 ; pour le second, comme $\gamma\alpha$ vérifie les mêmes relations galoisiennes que β, on a $\Delta_{\mathcal{T}_1}(\Lambda_{(-1,-3)})\gamma\alpha) = \frac{9}{16}T_{N_1/\mathbb{Q}}(\gamma^2\alpha^2)^4$ ce qui donne l'indice :

$$\chi\left((1-\sigma^2)(1-\tau^2)O_N, \Lambda_{(-1,-3)}\gamma\alpha\right) = \left(\frac{T_{N_1/\mathbb{Q}}(\gamma^2\alpha^2)}{2\prod_{q|\Delta_N} q}\right)^2.$$

Puisque $\alpha^2 \in E_1$ le numérateur peut se transformer :

$$T_{N_1}(\gamma^2\alpha^2) = T_{E_1/\mathbb{Q}}(\alpha^2 T_{N_1/E_1}(\gamma^2)).$$

L'indice devient :

$$\chi\left((1-\sigma^2)(1-\tau^2)O_N, \Lambda_{(-1,-3)}\gamma\alpha\right) = \left(\frac{T_{E_1/\mathbb{Q}}(\alpha^2 T_{N_1/E_1}(\gamma^2))}{2\prod_{q|\Delta_N} q}\right)^2.$$

Il faut maintenant trouver dans $\Lambda(-1,-3)$ les éléments ρ de norme réduite $\frac{T_{E_1/\mathbb{Q}}(\alpha^2 T_{N_1/E_1}(\gamma^2))}{2\prod_{q|\Delta_N} q}$. Comme β est défini à multiplication près par les unités de $\Lambda(-1,-3)$, il suffit de prendre pour ρ les représentants des orbites des éléments de la norme réduite voulue sous l'action à droite des éléments inversibles de $\Lambda_{(-1,-3)}$.

7. Exemple

Les calculs exposés ci-dessous ne sont pas détaillés, mais le lecteur peut les reconstituer facilement en utilisant PARI [P].

Le polynôme $P = X^3 - X^2 - 11X + 5$ a pour discriminant $5 \times (2 \times 17)^2$, si x est une racine de ce polynôme elle engendre une extension cubique $K = \mathbb{Q}(x)$ non galoisienne dont la clôture galoisienne N_1 est obtenue en composant K et $E_1 = \mathbb{Q}(\sqrt{5})$. On obtient une extension N à groupe Q_{12} en composant K et $E = \mathbb{Q}(\zeta_5)$.

Comme 2 et 17 sont les seuls premiers à avoir un indice de ramification égal à 3, le critère de base normale est vérifié.

On choisit pour v une racine de $X^4 - X^3 + X^2 - X + 1$ telle que $u = v + \tau^2(v) = v + \overline{v} = \frac{1+\sqrt{5}}{2}$, on fixe σ par son action sur les racines de P, τ est l'automorphisme qui laisse fixe K , tel que $\tau(v) = -v^2$. Pour construire une base normale de O_{N_1}, on peut suivre l'algorithme exposé dans [M1], ici il n'est pas difficile de constater que $\theta_1 = xu$ convient. On construit $\gamma = \theta_1 - \sigma^2(\theta_1)$. On calcule $T_{E_1/\mathbb{Q}}(\alpha^2 T_{N_1/E_1}(\gamma^2))$ qui vaut -340, c'est donc que l'on peut choisir $\beta = \gamma\alpha$.

Il faut maintenant trouver une base θ' de $(1-\tau^2)O_N$ comme Λ-module. Pour cela on doit déterminer lequel des éléments $\pm(v-\tau^2(v))$, $\pm(\tau(v)-\tau^3(v))$ est congru à $(1+2\sigma^2)(\beta)$ modulo 3. Il suffit de calculer les polynômes minimaux correspondants pour voir que l'on peut choisir

$$\theta' = \frac{(1+2\sigma^2)(\beta)+(\tau(v)-\tau^3(v))}{3}$$

qui a pour polynôme minimal

$$X^{12}+115X^{10}+4610X^8+76575X^6+472150X^4+409375X^2+78125.$$

On termine de la même manière : on cherche une unité $\epsilon \in \mathbb{Z}[S_3]^*$ (voir la remarque à la suite du lemme 2) de sorte que θ' soit congru à $\epsilon\theta_1$ modulo2 (on calcule les polynômes minimaux pour vérifier la congruence) ; on trouve que c'est le cas avec $\epsilon = \sigma\tau$ ce qui donne la base normale formée des conjugués de :

$$\theta = \frac{1}{2}\Bigg(\frac{(x-2\sigma(x)+\sigma^2(x))(v+\tau^2(v)(v-\tau^2(v))+\tau(v)-\tau^3(v))}{3} \\ -\sigma(x)\big(\tau(v)+\tau^3(v)\big)\Bigg)$$

qui a pour polynôme minimal :

$$X^{12}+X^{11}+12X^{10}+18X^9+145X^8-78X^7+1427X^6-156X^5 \\ +15931X^4+7080X^3+3150X^2+1375X+625.$$

Bibliographie

[C] J. Cougnard, *Construction de bases normales pour les extensions modérément ramifiées des rationnels à groupe D_4*. J. Théor. Nombres Bordeaux **12** (2000), 399–409.

[F1] A. Fröhlich, *Arithmetic and Galois module structure for tame extension*. J. Reine Angew. Math. **286/87** (1976), 380–440

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

[F3] A. Fröhlich, *Galois module structure and root numbers for quaternion extensions of degree 2^n*. J. Number Theory **12** (1980), 499–518.

[M1] J. Martinet, *Sur l'arithmétique d'une extension galoisienne à groupe de Galois diédral d'ordre $2p$*. Ann. Inst. Fourier **19** (1969), 1–80.

[M2] J. Martinet, *Modules sur l'algèbre du groupe quaternionien*. Annales Sci. de l'Ec. normale sup. 4e série fasc. 3 (1971), 399–408.

[MP] J. Martinet, J.-J. Payan, *Sur les extensions cubiques non Galoisiennes des rationnels et leur clôture galoisienne*. J. Reine Angew. Math. **228** (1967), 29–33.

[M] J. Milnor, *Introduction to algebraic K-theory*. Annals of Mathematics Studies, No. 72. Princeton University Press, Princeton, N.J.; University of Tokyo Press, Tokyo, 1971.

[P] C. Batut, K. Belabas, D. Bernardi, H. Cohen, M. Olivier, *User's Guide to Pari-GP*, version 2.02.12, 1999.

[Q] J. Queyrut, *Extensions quaternioniennes généralisées et constante de l'équation fonctionnelle des séries L d'Artin*. Publications Mathématiques de l'Université de Bordeaux I fascicule 4 (1972-73).

[S] R. G. SWAN, *Projective modules over binary polyhedral groups.* J. Reine Angew. Math. **342** (1982), 66–172.

[V] M.-F. VIGNÉRAS, *Simplification pour les ordres des corps de quaternions totalement définis.* J. Reine Angew. Math. **286/287** (1976), 257–277.

Jean COUGNARD
UMR 6139 S.D.A.D.
Université de Caen, Campus II
Bd. M^{al} Juin, BP 5186
14032 Caen Cedex, France
E-mail : cougnard@math.unicaen.fr

Jacques QUEYRUT
Laboratoire A2X
Université de Bordeaux I
351, cours de la libération
33405 Talence Cedex, France
E-mail : queyrut@math.u-bordeaux.fr