Journal de Théorie des Nombres
de Bordeaux **12** (2000), 399–409

Construction de base normale pour les extensions de $\mathbb{Q}$ à groupe D_4

par Jean COUGNARD

À Jacques Martinet pour son soixantième anniversaire,
en témoignage de reconnaissance et d'amitié

Résumé. Dans son article de 1971, essentiellement consacré aux extensions quaternioniennes de degré 8, J. Martinet prouve, au passage, l'existence de bases normales pour les entiers des extensions modérément ramifiées de $\mathbb{Q}$ de groupe D_4. On en donne une construction en reprenant les méthodes de sa thèse.

Abstract. In a paper published in 1971, mainly devoted to quaternionian extensions, J. Martinet proved the existence of normal integral bases for tame D_4 extensions of $\mathbb{Q}$. We give a constructive proof of this result.

Introduction

Soit $N/\mathbb{Q}$ une extension galoisienne de groupe de Galois G et $\mathbb{Z}_N$ son anneau des entiers ; si les indices de ramification des idéaux sont premiers aux caractéristiques de leurs corps résiduels (on dit que l'extension est modérément ramifiée) $\mathbb{Z}_N$ est un $\mathbb{Z}[G]$-module projectif. La question se pose alors de savoir s'il est ou non libre. Si c'est le cas, il possède une $\mathbb{Z}$-base formée des conjugués d'un même élément : on dit qu'il possède une base normale.

Dans le cas des extensions abéliennes modérément ramifiées l'existence et la construction d'une base normale se déduit du Bericht Hilbert [H].

J. Martinet prouve dans [M1] l'existence d'une base normale pour les extensions à groupe de Galois diédral de degré $2p$, p premier. L'existence de base normale repose sur une étude qui conduit à un algorithme de construction.

Dans [M2], il donne un critère pour que l'anneau des entiers d'une extension quaternionienne de degré 8, modérément ramifiée possède une base

Manuscrit reçu le 6 janvier 2000.

normale ; l'article donne des exemples de chacun des cas ; on y trouve le premier exemple connu d'extension modérément ramifiée sans base normale. Lorsque la base normale existe, on peut la construire [C].

Dans le même article, J. Martinet montre que le groupe des classes projectives $C\ell[D_4]$ (D_4 groupe diédral d'ordre 8) est trivial d'où l'existence de bases normales pour les extensions modérément ramifiées de groupe D_4.

On donne une démonstration constructive de ce résultat en s'inspirant des méthodes de [M1]. La construction que l'on donne peut donc s'appliquer à tout $\mathbb{Z}[D_4]$-module dont on ne connaît qu'une $\mathbb{Z}$-base et dont on sait qu'il est $\mathbb{Z}[D_4]$-libre. On pourraît ainsi construire une base normale des entiers d'une extension $N/\mathbb{Q}$ modérément ramifiée à groupe $D_4 \times C_2$.

Soit le groupe D_4 : $\{\sigma,\ \tau \mid \sigma^4 = \tau^2 = 1,\ \tau\sigma\tau = \sigma^{-1}\}$ et $N/\mathbb{Q}$ une extension galoisienne de groupe D_4 modérément ramifiée. On note M_1 (resp. M_1') le sous-corps invariant par τ (resp. $\tau\sigma^2$), M_2 (resp. M_2') celui invariant par $\tau\sigma$ (resp. $\tau\sigma^3$), M le sous-corps invariant par σ^2, F le sous-corps invariant par σ et enfin F_1 (resp. F_2) le corps invariant par $<\tau,\ \sigma^2>$ (resp. $<\tau\sigma, \sigma^2>$). Pour chaque corps K, $\mathbb{Z}_K$ est l'anneau des entiers de K. On note d_1, d, d_2 les entiers non divisibles par un carré et congrus à 1 modulo 4 tels que $F_1 = \mathbb{Q}(\sqrt{d_1})$, $F = \mathbb{Q}(\sqrt{d})$, $F_2 = \mathbb{Q}(\sqrt{d_2})$. L'anneau des entiers $\mathbb{Z}_M$ possède une base normale, formée des conjugués de $\eta = \frac{\epsilon+\sqrt{d_1}+\sqrt{d}+\sqrt{d_2}}{4}$ où $\epsilon = 1$ (resp. -1) si le pgcd de d_1 et de d est congru à 1 modulo 4 (resp. à 3 modulo 4). L'anneau des entiers du corps F (resp. F_1, F_2) est la trace de $\mathbb{Z}_M$ sur F (resp. F_1, F_2) on note ω (resp. ω_1, ω_2) la trace de η sur F (resp. F_1, F_2). On a le diagramme de corps suivant :

$$\begin{tikzcd}
 & & N \arrow[dll, dash] \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] \arrow[drr, dash] & & \\
M_1 \arrow[dr, dash] & M_1' \arrow[d, dash] & M \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & M_2' \arrow[d, dash] & M_2 \arrow[dl, dash] \\
 & F_1 \arrow[dr, dash] & F \arrow[d, dash] & F_2 \arrow[dl, dash] & \\
 & & \mathbb{Q} & &
\end{tikzcd}$$

1. Images des traces

Proposition 1.1. *Supposons $M_1/\mathbb{Q}$ modérément ramifiée. Il existe des éléments φ, ψ de $\mathbb{Z}_{M_1}$ qui forment une $\mathbb{Z}$-base de $\mathbb{Z}_{M_1}/\mathbb{Z}_{F_1}$ et tels que $T_{M_1/F_1}(\varphi) = \omega_1$, $T_{M_1/F_1}(\psi) = \sigma(\omega_1)$.*

Démonstration. Soit u et $v \in \mathbb{Z}_{M_1}$ dont les images forment une $\mathbb{Z}$-base de $\mathbb{Z}_{M_1}/\mathbb{Z}_{F_1}$. Les éléments de $\mathbb{Z}_{M_1}$ s'écrivent de manière unique sous la forme : $z_u u + z_v v + a\omega_1 + b\sigma(\omega_1)$ avec les coefficients a, b, z_u, $z_v \in \mathbb{Z}$. Comme l'extension M_1/F_1 est modérément ramifiée, les entiers de F_1 s'écrivent :

$$z_u T_{M_1/F_1}(u) + z_v T_{M_1/F_1}(v) + 2a\omega_1 + 2b\sigma(\omega_1)$$

Il en résulte immédiatement que $T_{M_1/F_1}(u)$, $T_{M_1/F_1}(v)$ forment une $\mathbb{F}_2$-base de $\mathbb{Z}_{F_1}/2\mathbb{Z}_{F_1}$ qui est un $\mathbb{F}_2[C_2]$-module libre dont une base est l'image de ω_1. On peut maintenant trouver φ_1, ψ_1 combinaisons linéaires, à coefficients entiers de u et v formant une $\mathbb{Z}$-base de $\mathbb{Z}_{M_1}/\mathbb{Z}_{F_1}$ tels que $T_{M_1/F_1}(\varphi_1)$, $T_{M_1/F_1}(\psi_1)$ aient même image respectivement que ω_1, $\sigma(\omega_1)$ dans $\mathbb{Z}_{F_1}/2\mathbb{Z}_{F_1}$. Comme la trace de $\mathbb{Z}_{M_1}$ dans $\mathbb{Z}_{F_1}$ est surjective, on peut retrancher à φ_1 un élément x de $\mathbb{Z}_{M_1}$ pour obtenir un élément φ dont la trace est ω_1. On a alors $T_{M_1/F_1}(\psi_1) - \sigma(T_{M_1/F_1}(\varphi_1)) \in 2\mathbb{Z}_{M_1} = T_{M_1/F_1}(\mathbb{Z}_{F_1})$, il suffit d'ajouter à ψ_1 un élément y de $\mathbb{Z}_{F_1}$ pour que l'on ait $\sigma(T_{M_1/F_1}(\varphi_1)) = T_{M_1/F_1}(\psi_1 + y)$; on pose : $\psi = \psi_1 + y$. □

Proposition 1.2. *Soit $\mathcal{R}$ un sous-$\mathbb{Z}[D_4]$-module projectif de $\mathbb{Z}_N$, contenant $\mathbb{Z}_{M_1}$ et $\mathbb{Z}_M$, φ et ψ deux éléments de $\mathbb{Z}_{M_1}$ tels que $\sigma(T_{M_1/F_1}(\varphi_1)) = T_{M_1/F_1}(\psi)$, alors il existe un élément $\theta \in \mathcal{R}$ tel que $\varphi = T_{N/M_1}(\theta)$, $\psi = T_{N/M_1}(\sigma(\theta))$. Deux choix de θ diffèrent par un élément de $\mathbb{Z}_M$ de trace nulle sur F_1.*

Démonstration. Si θ et θ' sont deux solutions du problème,

$$0 = T_{N/M_1}(\theta - \theta') = T_{N/M_1}(\sigma(\theta) - \sigma(\theta')) = T_{N/M_1}(\sigma(\theta - \theta')).$$

Posons $\lambda = \theta - \theta'$, la relation devient

$$\lambda + \tau(\lambda) = 0 \qquad \sigma(\lambda) + \tau(\sigma(\lambda)) = 0$$

soit en appliquant σ à la première égalité :

$$\sigma(\lambda) + \sigma(\tau(\lambda)) = 0 \qquad \sigma(\lambda) + \tau(\sigma(\lambda)) = 0$$

ce qui donne par soustraction : $\tau(\sigma(\lambda)) = \sigma(\tau(\lambda)) = \tau(\sigma^3(\lambda))$ (en tenant compte des relations dans le groupe). Ceci équivaut à $\lambda = \sigma^2(\lambda)$. Comme $\mathcal{R} \subset \mathbb{Z}_N$, $\lambda \in \mathcal{R}^{\sigma^2} \subset \mathbb{Z}_N^{\sigma^2} = \mathbb{Z}_M$ et $0 = \lambda + \tau(\lambda) = T_{M/F_1}(\lambda)$. Inversement, si θ est une solution et $\lambda \in \mathbb{Z}_M$ et $T_{M/F_1}(\lambda) = 0$, $\lambda \in \mathcal{R}^{\sigma^2}$ et il est évident que $\theta + \lambda$ est une autre solution.

Intéressons-nous maintenant à l'existence de θ. Prenons d'abord le cas particulier où $\varphi = 0$. On a donc $T_{M_1/F_1}(\psi) = 0$. On a les doubles inclusions :

$$\mathbb{Z}_{M_1} \subset \mathcal{R} \subset \mathbb{Z}_N \qquad \mathbb{Z}_M \subset \mathcal{R} \subset \mathbb{Z}_N$$

En prenant les invariants par τ dans la première, par σ^2 dans la seconde, on a :

$$\mathbb{Z}_{M_1} = \mathcal{R}^\tau \qquad \mathbb{Z}_M = \mathcal{R}^{\sigma^2}$$

Comme $\mathcal{R}$ est sans torsion et $\mathbb{Z}[D_4]$-projectif, il est cohomologiquement trivial, en particulier $(1+\tau)\mathcal{R} = \mathcal{R}^\tau = \mathbb{Z}_{M_1}$, il existe donc $u \in \mathcal{R}$ tel que $\psi = u + \tau(u)$. Le cas particulier envisagé implique $0 = (1+\sigma^2)(\psi) = (1+\sigma^2)T_{N/M_1}(u) = (1+\sigma^2)(1+\tau)(u) = 0$ ce qui est égal, puisque σ^2 est dans le centre du groupe D_4, à $(1+\tau)(1+\sigma^2)(u) = (1+\tau)(T_{N/M}(u))$. Comme $\mathcal{R}$ est cohomologiquement trivial il existe $v \in \mathbb{Z}_M$ tel que $T_{N/M}(u) = v - \tau(v)$, puis $w \in \mathcal{R}$ tel que $v = (1+\sigma^2)(w)$. Calculons :

$$\begin{aligned} T_{N/M}(u-(w-\tau(w))) &= v - \tau(v) - (1+\sigma^2)(w) + \tau((1+\sigma^2)(w)) \\ &= v - \tau(v) - v + \tau(v) = 0 \end{aligned}$$

Il existe $\theta' \in \mathcal{R}$ tel que $\theta' - \sigma^2(\theta') = u - (w - \tau(w)) = \sigma(\theta'') - \sigma^{-1}(\theta'')$ (avec $\theta'' = -\sigma(\theta')$). Posons alors $\theta = \theta'' - \tau(\theta'') \in \mathcal{R}$, on a bien évidemment $T_{N/M_1}(\theta) = 0$, tandis que :

$$\begin{aligned} T_{N/M_1}(\sigma(\theta)) &= (1+\tau)(\sigma(\theta'') - \sigma(\tau(\theta''))) \\ &= (1+\tau)(\sigma(\theta'') - \tau(\sigma^{-1}(\theta''))) \\ &= (1+\tau)(\sigma(\theta'') - \sigma^{-1}(\theta'')) \\ &= (1+\tau)(u - (w - \tau(w))) = \psi. \end{aligned}$$

Le passage au cas général se traite comme dans la proposition VI de [M1]. □

Remarque. Ce qui précède reste valable si on remplace $\mathbb{Z}$ par tout autre anneau de Dedekind A contenu dans $\mathbb{Q}$ et les $\mathbb{Z}_K$ par la clôture intégrale de A dans K. En particulier, on peut choisir $A = \mathbb{Q}$ ou un localisé de $\mathbb{Z}$.

Comme $N/\mathbb{Q}$ est modérément ramifiée, $\mathbb{Z}_N$ est $\mathbb{Z}[D_4]$-projectif, on en déduit :

Corollaire 1.3. *Soit $N/\mathbb{Q}$ modérément ramifiée, φ et ψ deux éléments de $\mathbb{Z}_{M_1}$ tels que $T_{M_1/F_1}(\psi) = \sigma(T_{N/M_1}(\varphi))$ alors il existe un élément $\theta \in \mathbb{Z}_N$ tel que $\varphi = T_{N/M_1}(\theta)$, $\psi = T_{N/M_1}(\sigma(\theta))$. Deux choix de θ diffèrent d'un élément de $\mathbb{Z}_M$ de trace nulle sur F_1.*

Remarque. Comme l'extension $N/\mathbb{Q}$ est modérément ramifiée, les $\lambda \in \mathbb{Z}_M$ de trace nulle sur F_1 sont tous de la forme $(1-\tau)(1+\sigma^2)(x)$ avec $x \in \mathbb{Z}_N$. L'élément $(1-\tau)(1+\sigma^2)$ est à nouveau mis en évidence plus loin.

Si on choisit $A = \mathbb{Q}$ comme anneau de Dedekind, on trouve un énoncé analogue où les anneaux d'entiers sont remplacés par les corps et N est $\mathbb{Q}[D_4]$-libre d'où :

Corollaire 1.4. *Soit φ et ψ deux éléments de M_1 tels que $T_{M_1/F_1}(\psi) = \sigma(T_{N/M_1}(\varphi))$ alors il existe un élément $\theta \in N$ tel que $\varphi = T_{N/M_1}(\theta)$, $\psi = T_{N/M_1}(\sigma(\theta))$. Deux choix de θ diffèrent d'un élément de M de trace nulle sur F_1.*

Corollaire 1.5. *Soit $\mathcal{R}$ un sous-$\mathbb{Z}[D_4]$-module projectif de $\mathbb{Z}_N$ contenant $\mathbb{Z}_{M_1}$ et $\mathbb{Z}_M$; alors $\mathcal{R} = \mathbb{Z}_N$.*

Démonstration. Soit θ dans $\mathbb{Z}_N$ et posons $\varphi = T_{N/M_1}(\theta)$, $\psi = T_{N/M_1}(\sigma(\theta))$ la proposition montre qu'il existe $\theta' \in \mathcal{R}$ tel que $\varphi = T_{N/M_1}(\theta')$, $\psi = T_{N/M_1}(\sigma(\theta'))$. Par le corollaire 1.4, $\theta - \theta' \in M$ et par construction $\theta - \theta' \in \mathbb{Z}_N$ par conséquent $\theta - \theta' \in \mathbb{Z}_M$ et $\theta = \theta' + (\theta - \theta') \in \mathcal{R}$ comme on a déjà l'inclusion $\mathcal{R} \subset \mathbb{Z}_N$ on a l'égalité de ces deux $\mathbb{Z}[D_4]$-modules. $\square$

2. Invariants associés à l'anneau $\mathbb{Z}_N$

Proposition 2.1. *Soit $\theta \in \mathbb{Z}_N$ vérifiant les conditions de la proposition 1.2 ; alors les éléments $(1+\tau)\sigma^i(\theta)$, $(0 \leq i \leq 3)$ forment une base de $\mathbb{Z}_{M_1}$, le θ peut être choisi de telle sorte qu'avec ses conjugués il forme une $\mathbb{Q}$-base de $N/\mathbb{Q}$.*

Démonstration. Avec les notations de la proposition 1.2, les éléments construits dans l'énoncé sont :

$$(1+\tau)(\theta) = \varphi, (1+\tau)\sigma(\theta) = \psi, (1+\tau)\sigma^2(\theta) = \sigma^2(\varphi), (1+\tau)\sigma^3(\theta) = \sigma^2(\psi)$$

On en déduit que le $\mathbb{Z}$-module engendré par les $(1+\tau)\sigma^i(\theta)$, $(0 \leq i \leq 3)$ contient $T_{M_1/F_1}(\varphi) = \omega_1$, $T_{M_1/F_1}(\psi) = \sigma(\omega_1)$ et par conséquent contient $\mathbb{Z}_{F_1}$, comme φ et ψ forment une $\mathbb{Z}$-base de $\mathbb{Z}_{M_1}/\mathbb{Z}_{F_1}$ la première partie est démontrée.

Supposons maintenant que l'on ait une relation de dépendance linéaire entre les conjugués de θ, on l'écrit : $0 = \sum_{j=0}^{3}(a_j + a'_j\tau)\sigma^j(\theta)$. Appliquons $(1+\tau)\sigma^i$ à cette relation, on obtient quel que soit i :
$\sum_{j=0}^{3}(a_{j-i} + a'_{j+i})(1+\tau)\sigma^j(\theta) = 0$. Comme les $(1+\tau)\sigma^j(\theta)$ forment une base de $\mathbb{Z}_{M_1}$, on en déduit :

$$(*) \qquad a_0 = a_2 = -a'_0 = -a'_2 \ ; \quad a_1 = a_3 = -a'_1 = -a'_3$$

La relation de dépendance linéaire devient :

$$(**) \qquad a_0(1-\tau)(1+\sigma^2)\sigma(\theta) + a_1(1-\tau)(1+\sigma^2)(\theta) = 0;$$

où l'on peut remplacer θ par $\theta + \mu$ avec $\mu \in \mathbb{Z}_M$, $T_{M/F_1}(\mu) = 0$. On peut donc écrire $\mu = \lambda - \tau(\lambda)$, $\lambda \in \mathbb{Z}_M$ et la relation de dépendance se ramène à : $4(1-\tau)(a_0\lambda + a_1\sigma(\lambda))$ et λ peut être choisi de telle sorte que cette relation implique $a_0 = a_1 = 0$. $\square$

On a, en résumé, montré l'existence d'un élément θ de $\mathbb{Z}_N$ tel que :

1 - avec ses conjugués il forme une $\mathbb{Q}$-base de N,

2 - $T_{N/M_1}(\theta)$, $T_{N/M_1}(\sigma(\theta))$, $T_{N/M_1}(\sigma^2(\theta))$, $T_{N/M_1}(\sigma^3(\theta))$ forment une base de $\mathbb{Z}_{M_1}$

3 - $T_{N/F_1}(\theta) = \omega_1$, $T_{N/F_1}(\sigma(\theta)) = \sigma(\omega_1)$.

Intéressons nous aux éléments $\theta \in \mathbb{Z}_N$ vérifiant la condition 2. On a alors :

Lemme 2.2. *Soit θ tel que $T_{N/M_1}(\theta)$, $T_{N/M_1}(\sigma(\theta))$, $T_{N/M_1}(\sigma^2(\theta))$ et $T_{N/M_1}(\sigma^3(\theta))$ forment une base de $\mathbb{Z}_{M_1}$; alors la trace dans M_1/F_1 de $(1+\tau)(\theta)$ est l'un des éléments $\pm(\eta+\tau(\eta))$, $\pm\sigma(\eta+\tau(\eta))$.*

Démonstration. La trace de $\mathbb{Z}_{M_1}$ dans M_1/F_1 est égale à $\mathbb{Z}_{F_1}$ (ramification modérée), or elle est engendrée par $(1+\tau)(1+\sigma^2)(\theta)$ et $(1+\tau)(1+\sigma^2)\sigma(\theta)$ qui sont conjugués : c'est donc une base normale de $\mathbb{Z}_{F_1}$. On sait que $\eta+\tau(\eta)$ en est une et que les autres s'en déduisent par conjugaison et multiplication par ± 1. □

Pour $u \in \mathbb{Z}[D_4]$ et $\theta \in \mathbb{Z}_N$ on fabrique le quadruplet :

$$((u\theta)_i) = \{(1+\tau)(u\theta), (1+\tau)\sigma(u\theta), (1+\tau)\sigma^2(u\theta), (1+\tau)\sigma^3(u\theta)\}$$

Soit θ et $\theta' \in \mathbb{Z}_N$ tels que les $(1+\tau)\sigma^i(\theta)$ $(0 \le i \le 3)$ forment une base de $\mathbb{Z}_{M_1}$ et tels que $(1+\tau)\sigma^i(\theta) = (1+\tau)\sigma^i(\theta')$ $(0 \le i \le 3)$ alors :

$$(u\theta)_i - (u\theta')_i = (1+\tau)\sigma^i(u(\theta-\theta'))$$

mais $\theta - \theta' \in M$ extension abélienne, les restrictions des automorphismes commutent. On a donc $(1+\tau)\sigma^i(u(\theta-\theta')) = \sigma^i(u(1+\tau)(\theta-\theta'))$ mais on sait (proposition 1.2) que $(1+\tau)(\theta-\theta') = 0$. Le quadruplet $((u\theta)_i)$ est indépendant du choix de θ vérifiant la condition 2. On a par ailleurs les relations :

$$\tau(1-\tau)(1+\sigma^2) = (1-\tau)(1+\sigma^2)\tau \quad \text{et} \quad \sigma(1-\tau)(1+\sigma^2) = (1-\tau)(1+\sigma^2)\sigma.$$

L'élément $(1-\tau)(1+\sigma^2)$ appartient au centre de $\mathbb{Z}[D_4]$ (divisé par 4 c'est un idempotent central de l'algèbre $\mathbb{Z}[D_4]$) donc $(1-\tau)(1+\sigma^2)\mathbb{Z}[D_4]$ est un idéal bilatère de $\mathbb{Z}[D_4]$ noté $\mathfrak{A}$.

Prenons maintenant u et $v \in \mathbb{Z}[D_4]$ tels que $u - v \in \mathfrak{A}$. Le calcul suivant :

$$\begin{aligned}(u\theta)_i - (v\theta)_i &= (1+\tau)\sigma^i((u-v)\theta)\\ &= (1+\tau)\sigma^i(1-\tau)(1+\sigma^2)g(\theta)\\ &= (1+\tau)(1-\tau)(1+\sigma^2)\sigma^i g = 0\end{aligned}$$

avec $g \in \mathbb{Z}[D_4]$ conduit à :

Proposition 2.3. *Le quadruplet $((u\theta)_i)$ ne dépend que de l'image de u dans l'algèbre $\mathbb{Z}[D_4]/\mathfrak{A}$ et est indépendant du choix de θ vérifiant la condition 2.*

Proposition 2.4. *Soit $u \in \mathbb{Q}[D_4]$ tel que pour tout i, $0 \le i \le 3$ $(1+\tau)\sigma^i u \in \mathbb{Z}[D_4]$, alors il existe $v \in \mathbb{Z}[D_4]$ tel que pour tout i : $(1+\tau)\sigma^i u = (1+\tau)\sigma^i v$.*

Démonstration. On écrit $u = (a_0 + a'_0\tau) + (a_1 + a'_1\tau)\sigma + (a_2 + a'_2\tau)\sigma^2 + (a_3 + a'_3\tau)\sigma^3$. L'écriture de $(1+\tau)\sigma^i u \in \mathbb{Z}[D_4]$ montre (en utilisant le calcul $(*)$ de la proposition 2.1) que les sommes :

$$a_0 + a'_0,\ a_0 + a'_2,\ a_2 + a'_0,\ a_2 + a'_2, a_1 + a'_1,\ a_1 + a'_3,\ a_3 + a'_1,\ a_3 + a'_3,$$

appartiennent à $\mathbb{Z}$. Posons : $h_0 = h_1 = 0$, $h_2 = a_2 - a_0$, $h_3 = a_3 - a_1$, $h'_0 = a_0 + a'_0$, $h'_1 = a_1 + a'_1$, $h'_2 = a_0 + a'_2$, $h'_3 = a_1 + a'_3$ et $v = \sum_{j=0}^{3}(h_j + h'_j\tau)\sigma^j$ les propriétés sur les sommes de a_i et a'_k montrent que $v \in \mathbb{Z}[D_4]$ et le calcul de la proposition 2.1 déjà invoqué montre que l'on a bien $(1+\tau)\sigma^i u = (1+\tau)\sigma^i v$. □

Lemme 2.5. *Les images de $1 + \sigma - \sigma\tau$ et $\tau + \sigma - \sigma\tau$ sont inversibles dans l'algèbre $\mathbb{Z}[D_4]/\mathfrak{A}$.*

Démonstration. Cela résulte immédiatement des identités :

$$(1 + \sigma - \sigma\tau)(1 - \sigma + \sigma\tau) = 1 - (1 - \tau)(1 + \sigma^2) = (1 - \sigma + \sigma\tau)(1 + \sigma - \sigma\tau)$$

$$(\tau + \sigma - \sigma\tau)(\tau + \sigma - \sigma\tau) = 1 + (1 - \sigma)(1 - \tau)(1 + \sigma^2).$$

□

3. Existence et construction de la base normale

Definition 3.1. Soit $\theta \in \mathbb{Z}_N$ tel que le quadruplet : $\{(1+\tau)(\theta), (1+\tau)\sigma((\theta)), (1+\tau)\sigma^2(\theta), (1+\tau)\sigma^3(\theta)\}$ forme une base $\mathcal{B}$ de $\mathbb{Z}_{M_1}$. Une telle base est appelée base «normale» de $\mathbb{Z}_{M_1}$. On a vu que l'on peut supposer que θ engendre avec ses conjugués une $\mathbb{Q}$-base de N.

À tout élément $u \in \mathbb{Z}[D_4]$ et toute base «normale» $\mathcal{B}$ de $\mathbb{Z}_{M_1}$, on associe le quadruplet

$$\{(1+\tau)(u\theta), (1+\tau)\sigma((u\theta)), (1+\tau)\sigma^2(u\theta), (1+\tau)\sigma^3(u\theta)\}\ ;$$

on a vu qu'il ne dépend pas du choix de θ définissant la base $\mathcal{B}$ et ne dépend que de la classe $\overline{u}$ de u dans $\mathbb{Z}[D_4]/\mathfrak{A}$, on note donc $(\overline{u}(\mathcal{B}))$ le quadruplet $((u\theta)_i)$ $(0 \leq i \leq 3)$; nous en étudions maintenant les propriétés.

Théorème 3.2. *Soit $\mathcal{B}$ une base «normale» de $\mathbb{Z}_{M_1}$, l'application qui à un élément $\overline{u}$ de $(\mathbb{Z}[D_4]/\mathfrak{A})^*$ associe le quadruplet $\overline{u}(\mathcal{B})$ d'éléments de $\mathbb{Z}_{M_1}$ établit une bijection avec l'ensemble des bases «normales» de $\mathbb{Z}_{M_1}$.*

Démonstration. On remarque d'abord que si $u \in \mathbb{Z}[D_4]$ les éléments $(u\theta)_i = (1+\tau)\sigma^i(u\theta)$ sont des combinaisons linéaires des θ_j. Si $\overline{u}$ est inversible dans $\mathbb{Z}[D_4]/\mathfrak{A}$, il existe ν et $\mu \in \mathbb{Z}[D_4]$ tels que $\nu u = 1 + \mu(1-\tau)(1+\sigma^2)$ et donc :

$$\begin{aligned}\nu u(\theta_i) &= \theta_i + \mu(1-\tau)(1+\sigma^2)(\theta_i)\\ &= \theta_i + \mu(1-\tau)(1+\sigma^2)(1+\tau)\sigma^i(\theta) = \theta_i.\end{aligned}$$

Comme $\nu u(\theta_i)$ s'exprime comme combinaison linéaire à coefficients entiers des $u\theta_i$, ces derniers forment une nouvelle base. Si $\mathcal{B}$ est une base «normale» de $\mathbb{Z}_{M_1}$, alors $\overline{u}(\mathcal{B})$ en est une autre.

Soit $\mathcal{B}'$ une autre base «normale» de $\mathbb{Z}_{M_1}$ il existe, par définition, $\theta' \in \mathbb{Z}_N$ tel que $\mathcal{B}' = (\theta_i)$; comme on peut aussi supposer que θ' engendre avec ses conjugués une $\mathbb{Q}$-base de N, il existe u et $u' \in \mathbb{Q}[D_4]$ tels que $\theta' = u\theta$, $\theta = u'\theta'$ et $uu' = 1$. On en déduit immédiatement que $\theta_i' = (1+\tau)\sigma^i u(\theta)$ et que $\theta_i = (1+\tau)\sigma^i u'(\theta')$; comme on a deux bases de $\mathbb{Z}_{M_1}$ il en résulte que quel que soit i, $(1+\tau)\sigma^i u$ et $(1+\tau)\sigma^i u'$ appartiennent à $\mathbb{Z}[D_4]$. En appliquant la proposition 2.3, il existe v et $v' \in \mathbb{Z}[D_4]$ tels que pour tout i : $\theta_i' = (1+\tau)\sigma^i v(\theta)$ et $\theta_i = (1+\tau)\sigma^i v'(\theta')$. Le calcul de la proposition 2.1 montre que $u-v$, $u'-v'$ appartiennent à $(1-\tau)(1+\sigma^2)\mathbb{Q}[D_4]$, il s'ensuit que $uu' - vv' = 1 - vv' \in \mathbb{Z}[D_4] \cap (1-\tau)(1+\sigma^2)\mathbb{Q}[D_4]$. Déterminons cette intersection. Soit

$$\sum_i (a_i + a_i'\tau)\sigma^i(1-\tau)(1+\sigma^2) \in \mathbb{Z}[D_4] \cap (1-\tau)(1+\sigma^2)\mathbb{Q}[D_4]\ .$$

En développant on obtient :

$$(a_0 + a_0' + a_2 + a_2')(1-\tau)(1+\sigma^2) + (a_1 + a_1' + a_3 + a_3')\sigma(1-\tau)(1+\sigma^2),$$

autrement dit $\overline{vv'} = 1$ dans $\mathbb{Z}[D_4]/\mathfrak{A}$. L'application de $(\mathbb{Z}[D_4]/\mathfrak{A})^*$ dans l'ensemble des bases «normales» est surjective.

Enfin, l'application $\overline{u} \mapsto \overline{u}(\mathcal{B})$ est injective. Soit $\overline{u}$, $\overline{v}$ tels que $\overline{u}(\mathcal{B}) = \overline{v}(\mathcal{B})$, u, v des représentants de $\overline{u}$ et $\overline{v}$ puisque les deux bases construites sont les mêmes, quel que soit i $(0 \le i \le 3)$ $(1+\tau)\sigma^i(u-v)(\theta) = 0$. Si on pose $u - v = \sum_j (a_j + a_j'\tau)\sigma^j$, comme θ est une $\mathbb{Q}[D_4]$-base de N on a $(1+\tau)\sigma^i(u-v) = 0$ ce qui implique que l'on a les relations $a_{j-i} + a_{j+i}' = 0$, on en déduit comme précédemment que $u - v \in \mathfrak{A}$ et donc $\overline{u} = \overline{v}$. □

Ces propriétés étant établies, on peut passer à la construction de la base normale.

Soit $\theta \in \mathbb{Z}_N$ tel que $\{(1+\tau)\sigma^i(\theta) \mid 0 \le i \le 3\}$ est une base «normale» de $\mathbb{Z}_{M_1}$, ce θ est défini à l'addition près par un élément $\lambda \in \mathbb{Z}_M$ tel que $T_{M/F_1}(\lambda) = 0$. On en déduit que si $\theta' \in \mathbb{Z}_N$ donne la même base «normale» de $\mathbb{Z}_{M_1}$, $T_{N/M}(\theta') = T_{N/M}(\theta) + 2\lambda$. La base «normale» de $\mathbb{Z}_{M_1}$ définit ainsi un élément de $\mathbb{Z}_M/2\mathbb{Z}_M$.

Écrivons :

$$T_{N/M}(\theta) = a\eta + b\sigma(\eta) + c\tau(\eta) + d\sigma\tau(\eta)$$

On s'est imposé $T_{M_1/F_1}(T_{N/M_1}(\theta)) = \frac{\epsilon+\sqrt{d_1}}{2} = \eta + \tau(\eta)$.
On obtient, puisque $T_{M_1/F_1}(T_{N/M_1}(\theta)) = T_{M/F_1}(T_{N/M}(\theta))$, l'égalité :

$$(a+c)(\eta+\tau(\eta)) + (b+d)(\sigma(\eta+\tau(\eta)) = \eta + \tau(\eta),$$

soit $a+c=1$, $b+d=0$. L'image de $T_{N/M}(\theta)$ est congrue, modulo 2, à l'un des éléments η, $\tau(\eta)$, $\eta+\sigma(\eta)-\sigma\tau(\eta)$, $\tau(\eta)+\sigma(\eta)-\sigma\tau(\eta)$. On a vu (lemme 2.4) que l'image de u dans $\mathbb{Z}[D_4]/\mathfrak{A}$ où u est l'un des éléments τ, $1+\sigma-\sigma\tau$ et $\tau+\sigma-\sigma\tau$ est inversible, on en a calculé l'inverse. Soit v un représentant dans $\mathbb{Z}[D_4]$ de cet inverse, on remplace θ par $\theta_1 = v(\theta)$. Le théorème 2.2 montre que les $(1+\tau)\sigma^i(\theta_1)$ forment encore une base «normale» de $\mathbb{Z}_{M_1}$. De plus $T_{N/M}(\theta_1) = T_{N/M}(v\theta) = vu(\eta)$. Les identités $(1+\sigma-\sigma\tau)(1-\sigma+\sigma\tau) = 1-(1-\tau)(1+\sigma^2)$; $(\tau+\sigma-\sigma\tau)^2 = 1+(1-\tau)(1-\sigma)(1+\sigma^2)$ montrent que $T_{N/M}(\theta_1)-\eta = 2x$ avec $x \in \mathbb{Z}_M$ dans le noyau de la trace de M dans F_1. On peut donc remplacer θ_1 par $\theta_1' = \theta_1 - x$ sans changer la base «normale» et supposer que $T_{N/M}(\mathbb{Z}[D_4]\theta_1') = \mathbb{Z}_M$, $T_{N/M_1}(\mathbb{Z}[D_4]\theta_1') = \mathbb{Z}_{M_1}$.

Proposition 3.3. *Le module $\mathbb{Z}[D_4]\theta$ est libre et contient $\mathbb{Z}_{M_1}$ et $\mathbb{Z}_M$.*

Démonstration. Si $\mathbb{Z}[D_4]\theta$ n'est pas libre, on a une relation de dépendance linéaire $(**)$ comme dans la proposition 2.1, mais en prenant la trace sur M, en utilisant que $T_{N/M}(\theta) = \eta$, on obtient

$$2a_0\eta - 2a_0\tau(\eta) + 2a_1\sigma(\eta) - 2a_1\sigma\tau(\eta) = 0,$$

ce qui implique $a_0 = a_1 = 0$. On utilise alors $(*)$ qui montre que les conjugués de θ sont linéairement indépendant.
Les inclusions de l'énoncé sont prouvées dans les calculs précédents. □

On conclut grâce au corollaire 1.5 que le θ ainsi construit définit une $\mathbb{Z}[D_4]$-base de $\mathbb{Z}_N$.

4. Un exemple

Le nombre de classes (au sens large et au sens restreint) du corps $F = \mathbb{Q}(\sqrt{37 \times 761})$ vaut 4. Le corps de classes de Hilbert N de F est une extension diédrale modérément ramifiée de $\mathbb{Q}$ à groupe D_4 ; construisons une base normale de son anneau des entiers.

N contient le corps des genres $M = \mathbb{Q}(\sqrt{37}, \sqrt{761})$ de F. On pose $F_1 = \mathbb{Q}(\sqrt{37})$, son anneau des entiers admet comme base 1, $\omega_1 = \frac{1+\sqrt{37}}{2}$, il est principal ce qui facilite les calculs. On note $\omega_1' = \frac{1-\sqrt{37}}{2}$, racine avec ω_1 de $X^2 - X - 9$.

L'idéal (761) est décomposé dans F_1 : $761 = (29+5\omega_1)(29+5\omega_1')$. La relation $29+5\omega_1 = (9+\omega_1)+4(5+\omega_1) \equiv \omega_1^2 \bmod 4$ prouve d'une part que N est la clôture galoisienne de $M_1 = \mathbb{Q}(\sqrt{29+5\omega_1})$ et d'autre part que les entiers de M_1 admettent 1, $\frac{\omega_1+\sqrt{29+5\omega_1}}{2}$ comme base relative sur ceux de F_1.

Le corps N est le composé des corps M_1 et $M'_1 = \mathbb{Q}(\sqrt{29+5\omega'_1})$ dont les discriminants sur F_1 sont premiers entre eux. On a donc une base des entiers de N relativement à M_1 : 1, $\frac{\omega'_1+\sqrt{29+5\omega'_1}}{2}$.

On veut maintenant construire des entiers ϕ et ψ de M_1 dont les traces sur F_1 sont ω_1 et $\omega'_1 = 1-\omega_1$. Puisque $T_{M_1/F_1}(\frac{\omega_1+\sqrt{29+5\omega_1}}{2}) = \omega_1$, on pose : $\phi = \frac{\omega_1+\sqrt{29+5\omega_1}}{2}$; comme $T_{M_1/F_1}(\omega_1\phi) = \omega_1^2 = \omega_1+9$, on choisit $\psi = 5-\omega_1\phi$. On vérifie immédiatement que $\{\omega_1,\ \omega'_1,\ \phi,\ \psi\}$ constitue une base de l'anneau des entiers de M_1.

L'étape suivante consiste à construire un élément θ entier de N tel que $T_{N/M_1}(\theta) = \phi$, $T_{N/M_1}(\sigma(\theta)) = \psi$. Pour cela on précise l'action du groupe de Galois de $N/\mathbb{Q}$, σ et τ sont caractérisés par :
$\sigma(\sqrt{761}) = -\sqrt{761}$, $\sigma(\sqrt{29+5\omega_1}) = \sqrt{29+5\omega'_1} = \frac{\sqrt{761}}{\sqrt{29+5\omega_1}}$,
$\tau(\phi) = \phi$, $\tau(\sqrt{761}) = -\sqrt{761}$.

Partons d'un élément de M'_1 dont la trace sur F_1 vaut 1. On peut choisir $-(4+\omega_1\sigma(\phi))$; on construit alors $\theta_1 = -\phi(4+\omega_1\sigma(\phi))$ qui est tel que : $T_{N/M_1}(-\phi(4+\omega_1\sigma(\phi)) = \phi$. Calculons $T_{N/M_1}(\sigma(\theta_1))$. On a :

$$\begin{aligned}\sigma(\theta_1) &= -4\sigma(\phi) - \omega'_1\sigma(\phi)\sigma^2(\phi)\\ &= -4\sigma(\phi) - \omega'_1\left(\frac{\omega'_1+\sqrt{29+5\omega'_1}}{2}\right)\left(\frac{\omega_1-\sqrt{29+5\omega_1}}{2}\right)\\ &= -4\sigma(\phi) - \omega'_1\frac{-9-\sqrt{761}-\omega'_1\sqrt{29+5\omega_1}+\omega_1\sqrt{29+5\omega'_1}}{4}\end{aligned}$$

de trace sur M_1 égale à $-4\omega'_1 + \omega'_1\frac{9+\omega'_1\sqrt{29+5\omega_1}}{2}$, qui se récrit :

$$T_{N/M_1}(\sigma(\theta_1)) = 5-5\omega_1+(10-\omega_1)\phi = \psi - 5\omega_1 + 10\phi.$$

Il faut remplacer θ_1 par $\theta_1 + (1-\tau)(z)$ où z est un entier de N tel que $T_{N/M_1}(\sigma(1-\tau)(z)) = 5\omega_1 - 10\phi$.

On sait que z s'écrit de manière unique $a + b\sigma(\phi) = a + b\frac{\omega'_1+\sqrt{29+5\omega'_1}}{2}$ avec a et b entiers de M_1, on a alors : $(1-\tau)(z) = b\sqrt{29+5\omega'_1}$, ensuite $\sigma(1-\tau)(z) = -\sigma(b)\sqrt{29+5\omega_1}$ et enfin :

$$\begin{aligned}(1+\tau)\sigma(1-\tau)(z) &= -(\sigma(b)+\sigma^3(b))\sqrt{29+5\omega_1}\\ &= -(\sigma(b)+\sigma^3(b))(2\phi-\omega_1)\\ &= (\sigma(b)+\sigma^3(b))\omega_1 - 2(\sigma(b)+\sigma^3(b))\phi.\end{aligned}$$

Il suffit de trouver b entier de M_1 dont la trace sur F_1 vaut 5. Les calculs de traces déjà effectués dans M_1/F_1 mènent à $b = -(20+3\omega_1)+(5\omega_1+1)\phi$.

On pose maintenant :

$$\begin{aligned}\theta' &= -\phi(4+\omega_1\sigma(\phi)) + (-(20+3\omega_1)+(1+5\omega_1)\phi))\,(2\sigma(\phi)-\omega_1')\\ &= (-7-20\omega_1)+(40+\omega_1)\phi-(40+6\omega_1)\sigma(\phi)+(2+9\omega_1)\phi\sigma(\phi).\end{aligned}$$

On calcule la trace sur M de θ' : $T_{N/M}(\theta') = -(1+4\omega_1)+(2+9\omega_1)\frac{1+\sqrt{761}}{2}$ que l'on exprime ensuite au moyen de $\alpha = \omega_1\frac{1+\sqrt{761}}{2}$ et de ses conjugués : $T_{N/M}(\theta') = \tau(\alpha)+\sigma(\alpha)-\sigma\tau(\alpha)+2\,(3\alpha-\sigma(\alpha)-3\tau(\alpha)+\sigma\tau(\alpha))$. Il faut donc remplacer θ' par $\theta'' = \tau(\theta')+\sigma(\theta')-\sigma\tau(\theta')$. On obtient : $\theta'' = (61-20\omega_1)+(40+13\omega_1')\phi+(-41+8\omega_1)\sigma(\phi)-(15+9\omega_1')\phi\sigma(\phi)$ dont la trace sur M est :

$$\begin{aligned}T_{N/M}(\theta'') &= (8+4\omega_1')-(15+9\omega_1')\frac{1+\sqrt{761}}{2}\\ &= \alpha-8\alpha+8\tau(\alpha)+12\sigma(\alpha)-12\sigma\tau(\alpha)\end{aligned}$$

qui diffère de α par le double d'un élément du noyau de la trace de M/F_1. On en déduit une base normale $\theta = \theta''+4\alpha-4\tau(\alpha)-6\sigma(\alpha)+6\sigma\tau(\alpha)$. On écrit $4\alpha-4\tau(\alpha)-6\sigma(\alpha)+6\sigma\tau(\alpha) = 4\omega_1\sqrt{761}+6\omega_1'\sqrt{741} = (4+2\omega_1')\sqrt{741}$ où $\sqrt{741} = (2\phi-\omega_1)(2\sigma(\phi)-\omega_1')$ ce qui donne : $(4+2\omega_1')\sqrt{741} = (-36-18\omega_1')-(12\omega_1'+36)\phi-(8\omega_1-36)\sigma(\phi)+(16+8\omega_1')\phi\sigma(\phi)$ qui conduit finalement à

$$\theta = (7-2\omega_1)+(5-\omega_1)\phi-5\sigma(\phi)+\omega_1\phi\sigma(\phi).$$

Un calcul de déterminant valide le résultat.

Bibliographie

[C] J. Cougnard, *Anneau d'entiers stablement libre sur* $\mathbb{Z}[H_8\times C_2]$. J. Théor. Nombres Bordeaux **10** (1998), 163–201.

[H] D. Hilbert, *Die Theorie der algebraischen Zahlkörper* (Zahlbericht). Jahr. Ber. der deutschen Math. Ver. **4** (1897), 175–146, ou Gesammelte Abhandlungen, 63–363.

[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. (4) **3** (1971), 399–408.

Jean Cougnard
CNRS FRE 2271
Structures Discrètes et Analyse Diophantienne
Campus II
Bd du maréchal Juin
14032 CAEN cedex
France
E-mail : cougnard@math.unicaen.fr