Journal de Théorie des Nombres
de Bordeaux **12** (2000), 103–126

De l'euclidianité de $\mathbb{Q}\Big(\sqrt{2+\sqrt{2+\sqrt{2}}}\Big)$ et $\mathbb{Q}\Big(\sqrt{2+\sqrt{2}}\Big)$ pour la norme

par JEAN-PAUL CERRI

RÉSUMÉ. Cet article a pour objectif de présenter un algorithme permettant de montrer, à l'aide d'un ordinateur, l'euclidianité pour la norme du sous-corps réel maximal K du corps cyclotomique $\mathbb{Q}(\zeta_{32})$ où $\zeta_{32} = \mathrm{e}^{\mathrm{i}\pi/16}$, corps totalement réel de degré 8 et de discriminant 2 147 483 648, et plus précisément de prouver que $M(K) = \frac{1}{2}$. La méthode utilisée permet par ailleurs de prouver que pour $K = \mathbb{Q}\left(\zeta_{16} + \zeta_{16}^{-1}\right)$, on a également $M(K) = \frac{1}{2}$ (conjecture de H. Cohn et J. Deutsch). Les résultats relatifs à ce cas sont exposés en fin d'article.

ABSTRACT. This article presents an algorithm which has allowed us to show, with the help of a computer, that the maximal real subfield K of the cyclotomic field $\mathbb{Q}(\zeta_{32})$ where $\zeta_{32} = \mathrm{e}^{\mathrm{i}\pi/16}$, totally real number field of degree 8 and discriminant 2 147 483 648, is norm-Euclidean, and more precisely, to prove that $M(K) = \frac{1}{2}$. Furthermore, it can be proved using the same method that if $K = \mathbb{Q}\left(\zeta_{16} + \zeta_{16}^{-1}\right)$, we also have $M(K) = \frac{1}{2}$ (as conjectured by H. Cohn and J. Deutsch). The results relative to this case are presented at the end of this paper.

1. INTRODUCTION

Soit n un élément de $\mathbb{N}^*$. Soit $\zeta_{2^{n+2}}$ la racine primitive 2^{n+2}-ième de l'unité définie par : $\zeta_{2^{n+2}} = \mathrm{e}^{\mathrm{i}\pi/2^{n+1}}$. Le corps cyclotomique $\mathbb{Q}(\zeta_{2^{n+2}})$ est une extension galoisienne de $\mathbb{Q}$ de degré 2^{n+1}. $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^{n+2}})/\mathbb{Q})$ est constitué par les $\mathbb{Q}$-automorphismes τ_l définis par : $\tau_l(\zeta_{2^{n+2}}) = \zeta_{2^{n+2}}^l$, l impair et $|l| \leq 2^{n+1} - 1$. On a :

$$\mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{2^{n+2}}\right)/\mathbb{Q}\right) \simeq \left(\mathbb{Z}/2^{n+2}\mathbb{Z}\right)^* \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z}.$$

Dans cette décomposition, $\mathbb{Z}/2\mathbb{Z}$ correspond à $\{\tau_1, \tau_{-1}\}$ (l'identité et la conjugaison complexe), $\mathbb{Z}/2^n\mathbb{Z}$ correspond par exemple à $\{\tau_3^k,\ 1 \leq k \leq 2^n\}$

Manuscrit reçu le 30 juin 1999.

qui est cyclique (on a les congruences $3^{2^n} \equiv 1 \bmod 2^{n+2}$ pour tout $n \geq 1$ et $3^{2^{n-1}} \equiv 2^{n+1} + 1 \bmod 2^{n+2}$ dès que $n \geq 2$).

Par ailleurs, l'anneau des entiers de $\mathbb{Q}(\zeta_{2^{n+2}})$ est $\mathbb{Z}[\zeta_{2^{n+2}}]$ (cf [B-S] ou [W]).

Soit maintenant $\mathbb{Q}_n$, le sous-corps réel maximal de $\mathbb{Q}(\zeta_{2^{n+2}})$.
$\mathbb{Q}_n = \mathbb{Q}(\zeta_{2^{n+2}}) \cap \mathbb{R}$. On a : $\mathbb{Q}\left(\zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1}\right) \subset \mathbb{Q}_n \subsetneq \mathbb{Q}(\zeta_{2^{n+2}})$ et comme $[\mathbb{Q}(\zeta_{2^{n+2}}) : \mathbb{Q}\left(\zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1}\right)] = 2$, nécessairement $\mathbb{Q}_n = \mathbb{Q}\left(\zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1}\right)$.
Les τ_l induisent (deux à deux) sur $\mathbb{Q}_n$ 2^n $\mathbb{Q}$-automorphismes σ_l définis par : $\sigma_l(\zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1}) = \zeta_{2^{n+2}}^{l} + \zeta_{2^{n+2}}^{-l}$ où $1 \leq l \leq 2^{n+1} - 1$ et l est impair.
$\mathbb{Q}_n$ est une extension cyclique de $\mathbb{Q}$ de degré 2^n car $\mathrm{Gal}(\mathbb{Q}_n/\mathbb{Q})$ que nous noterons G_n est engendré par σ_3. Notons également que pour tout n de $\mathbb{N}^*$, $\mathbb{Q}_{n+1}$ est une extension de $\mathbb{Q}_n$ de degré 2.
L'anneau des entiers de $\mathbb{Q}_n$ est $\mathbb{Z}[\zeta_{2^{n+2}}+\zeta_{2^{n+2}}^{-1}]$ (cf [W]). Nous le noterons $\mathcal{R}_n$.

Montrons désormais quelques propriétés élémentaires qui serviront pour la suite.
Soit e_i défini par :

$$e_0 = 1 \text{ et } e_i = \zeta_{2^{n+2}}^{i} + \zeta_{2^{n+2}}^{-i} \text{ si } 1 \leq i \leq 2^n - 1.$$

Alors on peut énoncer le

Théorème 1. *La famille $(e_i)_{0 \leq i \leq 2^n - 1}$ constitue une $\mathbb{Q}$-base de $\mathbb{Q}_n$ et une $\mathbb{Z}$-base de $\mathcal{R}_n$. En outre (e_i) vérifie :*

(i) $\mathrm{Tr}_{\mathbb{Q}_n/\mathbb{Q}}(e_i) = 0$, *si* $i \neq 0$. *Sinon* $\mathrm{Tr}_{\mathbb{Q}_n/\mathbb{Q}}(e_0) = \mathrm{Tr}_{\mathbb{Q}_n/\mathbb{Q}}(e_0^2) = 2^n$.

(ii) $\mathrm{Tr}_{\mathbb{Q}_n/\mathbb{Q}}(e_i^2) = 2^{n+1}$ *si* $i \neq 0$, $\mathrm{Tr}_{\mathbb{Q}_n/\mathbb{Q}}(e_i e_j) = 0$ *si* $i \neq j$.

(iii) *soit σ de G_n alors $\sigma(e_0) = e_0$ et il existe s de $\mathcal{S}_{2^n-1}$ groupe des permutations de $\{1, 2, ..., 2^n - 1\}$ et $(\alpha_1, \alpha_2, ..., \alpha_{2^n-1})$ de $\{-1, 1\}^{2^n-1}$ tels que, pour tout i de $\{1, 2, ..., 2^n - 1\}$ on ait $\sigma(e_i) = \alpha_i e_{s(i)}$. Alors σ induit une bijection de $\{\pm e_l\}$ sur lui-même.*

Preuve. Comme $\mathcal{R}_n = \mathbb{Z}[\zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1}]$, la famille $\left((\zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1})^j\right)_{0 \leq j \leq 2^n-1}$ est à la fois $\mathbb{Q}$-base de $\mathbb{Q}_n$ et $\mathbb{Z}$-base de $\mathcal{R}_n$. Par ailleurs pour tout i on a évidemment : $e_i \in \mathbb{Q}(\zeta_{2^{n+2}}) \cap \mathbb{R} = \mathbb{Q}_n$ et pour tout j on a :

$$(1.1) \qquad \left(\zeta_{2^{n+2}} + \zeta_{2^{n+2}}^{-1}\right)^j = \sum_{k=0}^{k=j} \binom{j}{k} \zeta_{2^{n+2}}^{2k-j} = \sum_{k=0}^{k=\lfloor \frac{j}{2} \rfloor} \binom{j}{k} e_{j-2k}$$

ce qui s'écrit matriciellement :

$$\begin{bmatrix} 1 \\ \left(\zeta_{2^{n+2}}+\zeta_{2^{n+2}}^{-1}\right) \\ \left(\zeta_{2^{n+2}}+\zeta_{2^{n+2}}^{-1}\right)^2 \\ . \\ . \\ \left(\zeta_{2^{n+2}}+\zeta_{2^{n+2}}^{-1}\right)^{2^n-1} \end{bmatrix} = M \begin{bmatrix} e_0 \\ e_1 \\ e_2 \\ . \\ . \\ e_{2^n-1} \end{bmatrix}$$

où M est une matrice à coefficient entiers.

Ceci prouve que tout élément de $\mathbb{Q}_n$ qui s'exprime comme combinaison linéaire à coefficients dans $\mathbb{Q}$ des $\left(\zeta_{2^{n+2}}+\zeta_{2^{n+2}}^{-1}\right)^j$ est aussi combinaison linéaire à coefficients dans $\mathbb{Q}$ des e_i. $(e_i)_{0\le i\le 2^n-1}$ est donc une partie génératrice de $\mathbb{Q}_n$ et comme elle compte 2^n éléments c'en est une base.

Mais ceci prouve aussi que tout élément de $\mathcal{R}_n$ qui s'exprime comme combinaison linéaire à coefficients dans $\mathbb{Z}$ des $\left(\zeta_{2^{n+2}}+\zeta_{2^{n+2}}^{-1}\right)^j$ est aussi combinaison linéaire à coefficients dans $\mathbb{Z}$ des e_i.

Par ailleurs (1.1) montre que M est triangulaire inférieure et que tous ses termes diagonaux valent 1. Elle est inversible et son inverse est aussi à coefficients dans $\mathbb{Z}$ (transposée des cofacteurs et déterminant égal à 1). Ceci prouve que les e_i sont dans $\mathcal{R}_n$. Comme $\mathcal{R}_n$ est un $\mathbb{Z}$-module libre de rang 2^n, comme les e_i sont 2^n éléments de $\mathcal{R}_n$ et en constituent une partie génératrice, on a la conclusion.

(i) Trivialement $\mathrm{Tr}_{\mathbb{Q}_n/\mathbb{Q}}(e_0)=\mathrm{Tr}_{\mathbb{Q}_n/\mathbb{Q}}(e_0^2)=\sum_{\sigma\in G_n}\sigma(1)=2^n$.

Supposons $i\neq 0$. Alors :

$$\begin{aligned}
\mathrm{Tr}_{\mathbb{Q}_n/\mathbb{Q}}(e_i) &= \sum_{\sigma\in G_n}\sigma(e_i) \\
&= \sum_{k=0}^{2^n-1}\left(\zeta_{2^{n+2}}^{i(2k+1)}+\zeta_{2^{n+2}}^{-i(2k+1)}\right) \\
&= 2\ \mathrm{Re}\ \left(\zeta_{2^{n+2}}^{i}\frac{1-\zeta_{2^{n+2}}^{2^{n+1}i}}{1-\zeta_{2^{n+2}}^{2i}}\right) \\
&= 2\ \mathrm{Re}\ \left(\frac{1-\zeta_{2^{n+2}}^{2^{n+1}i}}{\zeta_{2^{n+2}}^{-i}-\zeta_{2^{n+2}}^{i}}\right).
\end{aligned}$$

Or si i est pair, $\frac{1-\zeta_{2^{n+2}}^{2^{n+1}i}}{\zeta_{2^{n+2}}^{-i}-\zeta_{2^{n+2}}^{i}}=0$ et, si i est impair $\frac{1-\zeta_{2^{n+2}}^{2^{n+1}i}}{\zeta_{2^{n+2}}^{-i}-\zeta_{2^{n+2}}^{i}}=\frac{2}{\zeta_{2^{n+2}}^{-i}-\zeta_{2^{n+2}}^{i}}$ qui est un imaginaire pur. Ainsi, si $i\neq 0$, $\mathrm{Tr}_{\mathbb{Q}_n/\mathbb{Q}}(e_i)=0$.

(ii) Observons maintenant $\mathrm{Tr}_{\mathbb{Q}_n/\mathbb{Q}}(e_ie_j)$.

Si i ou $j=0$ on est dans la cas de figure précédent et $\mathrm{Tr}_{\mathbb{Q}_n/\mathbb{Q}}(e_ie_j)=0$ si $i\neq j$.

Supposons i et j distincts de 0. On a :

$$e_ie_j = \left(\zeta_{2^{n+2}}^{i+j} + \zeta_{2^{n+2}}^{-i-j}\right) + \left(\zeta_{2^{n+2}}^{i-j} + \zeta_{2^{n+2}}^{-i+j}\right).$$

Si $i + j = 2^n$ alors $\left(\zeta_{2^{n+2}}^{i+j} + \zeta_{2^{n+2}}^{-i-j}\right) = 0$, sinon cette expression est au signe près un e_l avec $l \neq 0$. Dans tous les cas $\mathrm{Tr}_{\mathbb{Q}_n/\mathbb{Q}}\left(\zeta_{2^{n+2}}^{i+j} + \zeta_{2^{n+2}}^{-i-j}\right) = 0$.
Si $i = j$ alors $\zeta_{2^{n+2}}^{i-j} + \zeta_{2^{n+2}}^{-i+j} = 2$, qui a pour trace 2^{n+1}, sinon cette expression est un e_l où $l \neq 0$ et sa trace est 0.
Ainsi lorsque i et j sont distincts de 0, si $i \neq j$, $\mathrm{Tr}_{\mathbb{Q}_n/\mathbb{Q}}(e_ie_j) = 0$. Et lorsque $i \neq 0$, $\mathrm{Tr}_{\mathbb{Q}_n/\mathbb{Q}}(e_i^2) = 2^{n+1}$.

(iii) Soit σ de G_n. Alors $\sigma(e_0) = e_0$ et si $i \neq 0$ $\sigma(e_i)$ est de la forme $\zeta_{2^{n+2}}^{il} + \zeta_{2^{n+2}}^{-il}$ où l est impair. Comme $i \leq 2^n - 1$ et comme l est impair, il n'est pas un multiple de 2^n, et $\zeta_{2^{n+2}}^{il} + \zeta_{2^{n+2}}^{-il} \in \{\pm e_k; 1 \leq k \leq 2^n - 1\}$. Il existe donc $(\alpha_1, \alpha_2, ..., \alpha_{2^n-1})$ de $\{-1, 1\}^{2^n-1}$ et f application de $\{1, 2, ..., 2^n - 1\}$ dans lui-même tels que pour tout $i \neq 0$ on ait : $\sigma(e_i) = \alpha_i e_{f(i)}$.
Si $i \neq j$ on ne peut avoir $f(i) = f(j)$ sinon on aurait $\sigma(e_i \pm e_j) = 0$ et $e_i \pm e_j = 0$ ce qui est impossible. f est donc injective et c'est une permutation de $\{1, 2, ..., 2^n - 1\}$, d'où la conclusion. □

On peut d'ailleurs déduire de ces propriétés de la $\mathbb{Z}$-base (e_i) de $\mathcal{R}_n$ la valeur du discriminant de $\mathbb{Q}_n$. En effet $d(\mathbb{Q}_n) = \det(\mathrm{Tr}_{\mathbb{Q}_n/\mathbb{Q}}(e_ie_j))$.

Corollaire. *Le discriminant absolu de* $\mathbb{Q}_n$ *est* $D_n = 2^{(n+1)2^n - 1}$.

Désormais tous les calculs seront menés dans la base $(e_i)_{0 \leq i \leq 2^n-1}$.
Notons ψ l'isomorphisme canonique de $\mathbb{Q}^{2^n}$ dans $\mathbb{Q}_n$ défini par :

$$\psi(a_0, a_1, ..., a_{2^n-1}) = \sum_{i=0}^{2^n-1} a_ie_i.$$

Chaque σ de G_n induit un automorphisme de $\mathbb{Q}^{2^n}$ noté g_σ défini par :

$$g_\sigma(a_0, a_1, ..., a_{2^n-1}) = \psi^{-1} \circ \sigma \circ \psi(a_0, a_1, ..., a_{2^n-1}).$$

Les g_σ forment un groupe pour la loi $\circ$, isomorphe à G_n (par $\sigma \longmapsto g_\sigma$), cyclique engendré par g_{σ_3} (on a $g_\sigma \circ g_\tau = g_{\sigma\circ\tau}$ et $g_{\sigma^i} = g_\sigma^i$). Le (iii) du théorème 1 montre que σ de G_n étant donné, il existe $(\beta_1, \beta_2, ..., \beta_{2^n-1})$ de $\{-1, 1\}^{2^n-1}$ et t de $\mathcal{S}_{2^n-1}$ (permutation de $\{1, 2, ..., 2^n - 1\}$), tels que :

$$g_\sigma(a_0, a_1, ..., a_{2^n-1}) = (a_0, \beta_1 a_{t(1)}, ..., \beta_{2^n-1} a_{t(2^n-1)}) \tag{1.2}$$

(il suffit de poser avec les notations du théorème 1, $t = s^{-1}$ et $\beta_i = \alpha_{t(i)}$).
On peut étendre les g_σ à $\mathbb{R}^{2^n}$ par les mêmes formules, et l'on obtient 2^n automorphismes de $\mathbb{R}^{2^n}$ qui constituent un groupe cyclique noté H_n. On

les notera encore g_σ, et on a toujours : $g_\sigma \circ g_\tau = g_{\sigma\circ\tau}$ et $g_{\sigma^i} = g_\sigma^i$.
Soit H'_n le sous groupe de $Gl(\mathbb{R}^{2^n})$ engendré par g_{σ_3} et par $-Id_{\mathbb{R}^{2^n}}$.
$H'_n = \{\pm g_\sigma, \sigma \in G_n\}$. H'_n est d'ordre 2^{n+1}, isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^n\mathbb{Z}$.
On prolonge ψ à $\mathbb{R}^{2^n}$ par :

$$\forall (r_0, r_1, ..., r_{2^n-1}) \in \mathbb{R}^{2^n}, \quad \psi(r_0, r_1, ..., r_{2^n-1}) = \sum_{i=0}^{2^n-1} r_i e_i.$$

On prolonge aussi chaque $\sigma \circ \psi$ (où $\sigma \in G_n$) à $\mathbb{R}^{2^n}$ par $\psi \circ g_\sigma$. On a :

$$\psi \circ g_\sigma(r_0, r_1, ..., r_{2^n-1}) = \sum_{i=0}^{2^n-1} r_i \sigma(e_i).$$

Définition 1. Compte tenu de ce qui précède, on peut définir $\overline{N_n}$, prolongement de $N_{\mathbb{Q}_n/\mathbb{Q}} \circ \psi$ à $\mathbb{R}^{2^n}$ par :

$$\overline{N_n}(r_0, r_1, ..., r_{2^n-1}) = \prod_{\sigma \in G_n} \psi \circ g_\sigma(r_0, r_1, ..., r_{2^n-1}) = \prod_{\sigma \in G_n} \left(\sum_{i=0}^{2^n-1} r_i \sigma(e_i) \right).$$

On peut remarquer que tous les prolongements ainsi définis sont continus.

Proposition. $\forall h \in H'_n,\ \overline{N_n} \circ h = \overline{N_n}$.

Preuve. Soit h de H'_n. $h = \alpha g_\sigma$ où $\sigma \in G_n$ et $\alpha \in \{-1, 1\}$. Alors, pour tout $(r_0, r_1, ..., r_{2^n-1})$ de $\mathbb{R}^{2^n}$ on a :

$$\begin{aligned} \overline{N_n} \circ h(r_0, r_1, ..., r_{2^n-1}) &= \prod_{\tau \in G_n} \psi \circ g_\tau \circ (\alpha g_\sigma)(r_0, r_1, ..., r_{2^n-1}) \\ &= \prod_{\tau \in G_n} \alpha \psi \circ g_{\tau\circ\sigma}(r_0, r_1, ..., r_{2^n-1}) \\ &= \alpha^{2^n} \prod_{\rho \in G_n} \psi \circ g_\rho(r_0, r_1, ..., r_{2^n-1}). \end{aligned}$$

Comme $\alpha^{2^n} = 1$, on a bien le résultat annoncé. □

Soit ϕ le plongement canonique de $\mathbb{Q}_n$ dans $\mathbb{R}^{2^n}$ défini par :

$$\phi(x) = \left(x, \sigma_3(x), \sigma_3^2(x), ..., \sigma_3^{2^n-1}(x)\right).$$

Si $(x, y) \in {\mathbb{Q}_n}^2$, on a $\langle \phi(x) | \phi(y) \rangle = \mathrm{Tr}_{\mathbb{Q}_n/\mathbb{Q}}(xy)$ et $\|\phi(x)\| = \sqrt{\mathrm{Tr}_{\mathbb{Q}_n/\mathbb{Q}}(x^2)}$ où $\langle\ |\ \rangle$ et $\|\ \|$ désignent respectivement le produit scalaire et la norme euclidienne de $\mathbb{R}^{2^n}$. Ainsi le théorème 1 montre que $(\phi(e_i))_{0 \leq i \leq 2^n-1}$ est une base orthogonale de $\mathbb{R}^{2^n}$, vérifiant : $\|\phi(e_0)\| = 2^{\frac{n}{2}}$ et $\|\phi(e_i)\| = 2^{\frac{n+1}{2}}$ sinon.

Définition 2. On définit également $\overline{\phi}$ prolongement de $\phi \circ \psi$ à $\mathbb{R}^{2^n}$ par :

$$\overline{\phi}(r_0, ..r_{2^n-1}) = \left(\psi(r_0, ..r_{2^n-1}), \psi \circ g_{\sigma_3}(r_0, ..r_{2^n-1}), ..\psi \circ g_{\sigma_3}^{2^n-1}(r_0, ..r_{2^n-1})\right).$$

$\overline{\phi}$ est un endomorphisme de $\mathbb{R}^{2^n}$. Sa matrice par rapport à la base canonique sera notée M_n. La j-ième colonne de M_n correspond à $\phi(e_{j-1})$, et si par commodité on fait varier les indices de 0 à 2^n-1, on a :

$$M_n = \left[\sigma_3^i(e_j)\right]_{\substack{0\le i\le 2^n-1\\ 0\le j\le 2^n-1}}.$$

Théorème 2. *$M_n \in Gl_{2^n}(\mathbb{R})$. Plus précisément $|\det(M_n)| = \sqrt{D_n}$ et*

$$M_n^{-1} = \left[\frac{\lambda_i\sigma_3^j(e_i)}{2^{n+1}}\right]_{\substack{0\le i\le 2^n-1\\ 0\le j\le 2^n-1}}$$

où $\lambda_0 = 2$ et $\lambda_i = 1$ si $i \neq 0$.

Preuve. Soit P_n la matrice définie par : $P_n = [\lambda_i\sigma_3^j(e_i)]_{\substack{0\le i\le 2^n-1\\ 0\le j\le 2^n-1}}$.
Alors $P_nM_n = [c_{i,j}]$ où :

$$c_{i,j} = \sum_{k=0}^{2^n-1}\lambda_i\sigma_3^k(e_i)\sigma_3^k(e_j) = \lambda_i\mathrm{Tr}_{\mathbb{Q}_n/\mathbb{Q}}(e_ie_j).$$

Ainsi, si $i \neq j$, $c_{i,j} = 0$, $c_{0,0} = 2\times 2^n$ et si $i\neq 0$, $c_{i,i} = 1\times 2^{n+1}$. D'où :

$$P_nM_n = 2^{n+1}I_{2^n}. \tag{1.3}$$

M_n est donc inversible d'inverse $\frac{1}{2^{n+1}}P_n$.
Par ailleurs on a évidemment :

$$\det(P_n) = 2\det(M_n^t) = 2\det(M_n),$$

où M_n^t désigne la transposée de M_n.
En prenant les déterminants des deux membres de (1.3) on obtient :

$$2\det(M_n)^2 = \det(2^{n+1}I_{2^n}) = 2^{2^n(n+1)}.$$

Ceci, compte tenu de la valeur de D_n déterminée plus haut, donne la valeur de $|\det(M_n)|$ annoncée. □

2. Position du problème

Si K est un corps de nombres d'anneau d'entiers $\mathcal{O}_K$, et si $x\in K$, notons $M(K,x)$ le minimum euclidien de x défini par :

$$M(K,x) = \inf\{|N_{K/\mathbb{Q}}(x-X)|\ ;\ X\in\mathcal{O}_K\},$$

puis définissons le minimum euclidien de K par :

$$M(K) = \sup\{M(K,x)\ ;\ x\in K\}.$$

Nous allons déjà montrer que $M(\mathbb{Q}_n) \ge \frac{1}{2}$.

Lemme. *pour tout l impair de $\{1,...,2^n-1\}$, on a :*

$$|N_{\mathbb{Q}_n/\mathbb{Q}}(e_l)| = 2.$$

Preuve. Procédons par récurrence sur n.
La propriété est évidemment vraie pour $n = 1$, car $N_{\mathbb{Q}_1/\mathbb{Q}}(\sqrt{2}) = -2$.
Supposons qu'elle soit vraie à l'ordre $n \geq 1$ et montrons qu'elle est alors vérifiée à l'ordre $n+1$.
Pour éviter toute confusion nous noterons $(e_i)_{0\leq i\leq 2^n-1}$ la base de $\mathbb{Q}_n$ et $(e'_i)_{0\leq i\leq 2^{n+1}-1}$ celle de $\mathbb{Q}_{n+1}$.
Pour tout l impair, e'_l est un conjugué de e'_1 (cf introduction). Par conséquent, tous les e'_l (l impair) ont la même norme, $N_{\mathbb{Q}_{n+1}/\mathbb{Q}}(e'_1)$.
En particulier, on peut écrire :

$$\left(N_{\mathbb{Q}_{n+1}/\mathbb{Q}}(e'_1)\right)^2 = N_{\mathbb{Q}_{n+1}/\mathbb{Q}}(e'_1)N_{\mathbb{Q}_{n+1}/\mathbb{Q}}(e'_{2^{n+1}-1}) = N_{\mathbb{Q}_{n+1}/\mathbb{Q}}(e'_1 e'_{2^{n+1}-1}).$$

Or, comme $\zeta_{2^{n+3}}^{2^{n+1}} + \zeta_{2^{n+3}}^{-2^{n+1}} = 0$, et comme $\zeta_{2^{n+3}}^{2k} = \zeta_{2^{n+2}}^{k}$ pour tout entier k, on a :

$$\begin{aligned} e'_1 e'_{2^{n+1}-1} &= \left(\zeta_{2^{n+3}} + \zeta_{2^{n+3}}^{-1}\right)\left(\zeta_{2^{n+3}}^{2^{n+1}-1} + \zeta_{2^{n+3}}^{-2^{n+1}+1}\right) \\ &= \left(\zeta_{2^{n+3}}^{2^{n+1}} + \zeta_{2^{n+3}}^{-2^{n+1}}\right) + \left(\zeta_{2^{n+3}}^{2^{n+1}-2} + \zeta_{2^{n+3}}^{-2^{n+1}+2}\right) \\ &= 0 + \left(\zeta_{2^{n+2}}^{2^{n}-1} + \zeta_{2^{n+2}}^{-2^{n}+1}\right) \\ &= e_{2^n-1}. \end{aligned}$$

Par suite on a :

$$\left(N_{\mathbb{Q}_{n+1}/\mathbb{Q}}(e'_1)\right)^2 = N_{\mathbb{Q}_{n+1}/\mathbb{Q}}(e_{2^n-1}). \tag{2.1}$$

Comme $\mathbb{Q}_{n+1}$ est une extension de degré 2 de $\mathbb{Q}_n$, et comme $e_{2^n-1} \in \mathbb{Q}_n$, on a :

$$\begin{aligned} N_{\mathbb{Q}_{n+1}/\mathbb{Q}}(e_{2^n-1}) &= N_{\mathbb{Q}_n/\mathbb{Q}}\left(N_{\mathbb{Q}_{n+1}/\mathbb{Q}_n}(e_{2^n-1})\right) \\ &= N_{\mathbb{Q}_n/\mathbb{Q}}(e_{2^n-1}^2) \\ &= \left(N_{\mathbb{Q}_n/\mathbb{Q}}(e_{2^n-1})\right)^2. \end{aligned}$$

D'où par (2.1),

$$\left(N_{\mathbb{Q}_{n+1}/\mathbb{Q}}(e'_1)\right)^2 = \left(N_{\mathbb{Q}_n/\mathbb{Q}}(e_{2^n-1})\right)^2. \tag{2.2}$$

L'hypothèse de récurrence indiquant que $|N_{\mathbb{Q}_n/\mathbb{Q}}(e_{2^n-1})| = 2$, (2.2) donne :

$$|N_{\mathbb{Q}_{n+1}/\mathbb{Q}}(e'_1)| = 2.$$

Ainsi la propriété est vraie à l'ordre $n+1$. $\square$

Remarque 1. On peut montrer qu'en fait, on a : $N_{\mathbb{Q}_n/\mathbb{Q}}(e_l) = 2$ pour l impair, dès que $n \geq 2$.

Théorème 3. *Pour tout n de $\mathbb{N}^*$, $M(\mathbb{Q}_n) \geq \frac{1}{2}$.*

Preuve. Pour cela il suffit de trouver x de $\mathbb{Q}_n$ vérifiant $M(\mathbb{Q}_n, x) \geq \frac{1}{2}$. Posons

$$\gamma_n = \frac{1}{2} \sum_{\substack{i=1 \\ i \text{ impair}}}^{2^n-1} e_i.$$

Comme les coordonnées de γ_n dans $(e_i)_{0 \leq i \leq 2^n-1}$, $\mathbb{Z}$-base de $\mathcal{R}_n$ ne sont pas toutes entières,

$$\gamma_n \notin \mathcal{R}_n. \tag{2.3}$$

Par ailleurs, en se servant de $\zeta_{2^{n+2}}^{2^{n+1}} = -1$ et de $\zeta_{2^{n+2}}^{2^n} = -\zeta_{2^{n+2}}^{-2^n}$ on établit :

$$\begin{aligned}
\sum_{\substack{i=1 \\ i \text{ impair}}}^{2^n-1} e_i &= \sum_{k=0}^{2^{n-1}-1} \left(\zeta_{2^{n+2}}^{2k+1} + \zeta_{2^{n+2}}^{-2k-1} \right) \\
&= \zeta_{2^{n+2}}^{-2^n+1} \sum_{k'=0}^{2^n-1} \zeta_{2^{n+2}}^{2k'} \\
&= \zeta_{2^{n+2}}^{-2^n+1} \frac{1 - (\zeta_{2^{n+2}}^2)^{2^n}}{1 - \zeta_{2^{n+2}}^2} \\
&= \frac{2\zeta_{2^{n+2}}^{-2^n+1}}{1 - \zeta_{2^{n+2}}^2} \\
&= \frac{2}{\zeta_{2^{n+2}}^{2^n-1} - \zeta_{2^{n+2}}^{2^n+1}} \\
&= \frac{2}{\zeta_{2^{n+2}}^{2^n-1} + \zeta_{2^{n+2}}^{-2^n+1}}
\end{aligned}$$

On en déduit :

$$\gamma_n = \frac{1}{e_{2^n-1}} \tag{2.4}$$

Soit alors X quelconque de $\mathcal{R}_n$. De (2.4) on tire :

$$\begin{aligned}
|N_{\mathbb{Q}_n/\mathbb{Q}}(\gamma_n - X)| &= \left| N_{\mathbb{Q}_n/\mathbb{Q}} \left(\frac{1 - Xe_{2^n-1}}{e_{2^n-1}} \right) \right| \\
&= \frac{|N_{\mathbb{Q}_n/\mathbb{Q}}(1 - Xe_{2^n-1})|}{|N_{\mathbb{Q}_n/\mathbb{Q}}(e_{2^n-1})|}
\end{aligned}$$

Or $1 - Xe_{2^n-1} \in \mathcal{R}_n$ donc $N_{\mathbb{Q}_n/\mathbb{Q}}(1 - Xe_{2^n-1}) \in \mathbb{Z}$, et le lemme indique que $|N_{\mathbb{Q}_n/\mathbb{Q}}(e_{2^n-1})| = 2$. On en déduit :

$$|N_{\mathbb{Q}_n/\mathbb{Q}}(\gamma_n - X)| \in \frac{1}{2}\mathbb{Z}. \tag{2.5}$$

En utilisant (2.3) qui implique que l'on ne peut avoir $N_{\mathbb{Q}_n/\mathbb{Q}}(\gamma_n - X) = 0$ si $X \in \mathcal{R}_n$ et (2.5) on peut même préciser :

$$|N_{\mathbb{Q}_n/\mathbb{Q}}(\gamma_n - X)| \in \frac{1}{2}\mathbb{Z}^*.$$

Ceci implique que

$$M(\mathbb{Q}_n, \gamma_n) \geq \frac{1}{2}.$$

On voit (en faisant $X = 0$ dans ce qui précède) qu'en fait $M(\mathbb{Q}_n, \gamma_n) = \frac{1}{2}$. Finalement,

$$M(\mathbb{Q}_n) \geq \frac{1}{2}.$$

Ceci achève la démonstration. □

Venons en maintenant au problème en lui-même.
Nous désirons montrer (pour $n = 3$ et accessoirement pour $n = 2$) que $\mathbb{Q}_n$ est euclidien pour la norme, c'est-à-dire que :

$$\forall x \in \mathbb{Q}_n,\ \exists X \in \mathcal{R}_n \text{ tel que } |N_{\mathbb{Q}_n/\mathbb{Q}}(x - X)| < 1.$$

En fait, nous allons montrer que l'on a mieux encore, à savoir :

$$\forall x \in \mathbb{Q}_n,\ \exists X \in \mathcal{R}_n \text{ tel que } |N_{\mathbb{Q}_n/\mathbb{Q}}(x - X)| \leq \frac{1}{2},$$

ce qui revient, compte tenu du précédent théorème à :

$$M(\mathbb{Q}_n) = \frac{1}{2}.$$

Pour cela, nous allons chercher à montrer de façon plus précise que $\mathbb{Q}_n$ (pour $n = 3$ et 2) vérifie le critère du théorème suivant.

Théorème 4. *Si $\forall r \in [-\frac{1}{2}, \frac{1}{2}]^{2^n}$, $\exists R \in \{-\frac{1}{2}, \frac{1}{2}\}^{2^n}$ tel que $|\overline{N_n}(r - R)| \leq \frac{1}{2}$ alors $M(\mathbb{Q}_n) = \frac{1}{2}$.*

Preuve. Soit $x \in \mathbb{Q}_n$ et soit $(a_0, a_1, ..., a_{2^n-1}) = \psi^{-1}(x) \in \mathbb{Q}^{2^n}$.
Pour tout i posons : $r_i = a_i - \lfloor a_i \rfloor - \frac{1}{2}$.
Alors $r = (r_0, r_1, ..., r_{2^n-1}) \in \left([-\frac{1}{2}, \frac{1}{2}) \cap \mathbb{Q}\right)^{2^n} \subset [-\frac{1}{2}, \frac{1}{2}]^{2^n}$ et par hypothèse il existe $R = (R_0, R_1, ..., R_{2^n-1}) \in \{-\frac{1}{2}, \frac{1}{2}\}^{2^n}$ tel que $|\overline{N_n}(r - R)| \leq \frac{1}{2}$.
Posons $R'_i = R_i + \lfloor a_i \rfloor + \frac{1}{2}$.
Alors $R' = (R'_0, R'_1, ..., R'_{2^n-1}) \in \mathbb{Z}^{2^n}$, et $X = \psi(R') \in \mathcal{R}_n$.
Par ailleurs $x - X = \psi(r - R)$, et $x - X$ vérifie donc :
$|N_{\mathbb{Q}_n/\mathbb{Q}}(x - X)| = |\overline{N_n} \circ \psi^{-1}(x - X)| = |\overline{N_n}(r - R)| \leq \frac{1}{2}$.
On a bien : $\forall x \in \mathbb{Q}_n$, $\exists X \in \mathcal{R}_n$ tel que $|N_{\mathbb{Q}_n/\mathbb{Q}}(x - X)| \leq \frac{1}{2}$. □

Remarque 2. Si ce critère est vérifié cela prouve que pour un élément x de $\mathbb{Q}_n$ donné de coordonnées (x_i) dans (e_i), un entier convenable peut être trouvé à proximité de x à savoir un entier de coordonnées ($\lfloor x_i \rfloor$ ou $\lceil x_i \rceil$). Pour $n = 1$ l'entier le plus proche de x c'est-à-dire celui de coordonnées ($\lfloor x_i + \frac{1}{2} \rfloor$) convient mais ce n'est plus le cas dès que $n \geq 2$.

Remarque 3. En reprenant les notations utilisées dans [L], si ce critère est vérifié alors

$$M(\overline{\mathbb{Q}_n}) = \frac{1}{2}.$$

Mais avant de passer au cas particulier $n = 3$, montrons un résultat qui nous sera très utile dans la suite.

Théorème 5. *Soient deux éléments R_1 et R_2 de $\{-\frac{1}{2}, \frac{1}{2}\}^{2^n}$, tels que $|N_{\mathbb{Q}_n/\mathbb{Q}} \circ \psi(R_1 - R_2)| \leq 2^{2^n - 1}$. Si $r \in \mathbb{R}^{2^n}$ et si $z = \overline{\phi}(r)$ est tel que pour tout i, $(z_i - \sigma_3^i \circ \psi(R_1))(z_i - \sigma_3^i \circ \psi(R_2)) \leq 0$, alors :*

$$\exists j \in \{1, 2\} \text{ tel que } |\overline{N_n}(r - R_j)| \leq \frac{1}{2}.$$

Preuve. Soit i de $\{0, 1, ..., 2^n - 1\}$.
Supposons par exemple que $\sigma_3^i \circ \psi(R_1) \leq \sigma_3^i \circ \psi(R_2)$.
Alors l'hypothèse faite sur z_i signifie que $z_i \in [\sigma_3^i \circ \psi(R_1), \sigma_3^i \circ \psi(R_2)]$.
Ainsi $\lambda_i = z_i - \sigma_3^i \circ \psi(R_1) \geq 0$, $\mu_i = \sigma_3^i \circ \psi(R_2) - z_i \geq 0$ et $\lambda_i + \mu_i = C_i$, où $C_i = \sigma_3^i \circ \psi(R_2) - \sigma_3^i \circ \psi(R_1)$.
Or le produit de deux réels positifs ou nuls de somme donnée C_i est maximum lorsque ces deux nombres sont égaux à $\frac{C_i}{2}$ et vaut alors $\frac{C_i^2}{4}$. Par suite,

$$|(z_i - \sigma_3^i \circ \psi(R_1))(z_i - \sigma_3^i \circ \psi(R_2))| \leq \frac{(\sigma_3^i \circ \psi(R_2) - \sigma_3^i \circ \psi(R_1))^2}{4}.$$

Ceci étant valable pour tout i, on a :

$$\prod_{i=0}^{2^n-1} |z_i - \sigma_3^i \circ \psi(R_1)| \prod_{i=0}^{2^n-1} |z_i - \sigma_3^i \circ \psi(R_2)| \leq \frac{(N_{\mathbb{Q}_n/\mathbb{Q}} \circ \psi(R_2 - R_1))^2}{4^{2^n}},$$

ou encore, compte tenu du fait que $z = \overline{\phi}(r)$,

$$\prod_{i=0}^{2^n-1} |\psi \circ g_{\sigma_3}^i(r - R_1)| \prod_{i=0}^{2^n-1} |\psi \circ g_{\sigma_3}^i(r - R_2)| \leq \frac{(N_{\mathbb{Q}_n/\mathbb{Q}} \circ \psi(R_2 - R_1))^2}{4^{2^n}}.$$

Comme $|N_{\mathbb{Q}_n/\mathbb{Q}} \circ \psi(R_2 - R_1)| \leq 2^{2^n - 1}$, on obtient :

$$|\overline{N}_n(r - R_1)||\overline{N}_n(r - R_2)| \leq \frac{1}{4},$$

et ceci n'est possible que si l'un des deux termes $|\overline{N}_n(r - R_1)|$ ou $|\overline{N}_n(r - R_2)|$ est inférieur ou égal à $\frac{1}{2}$. $\square$

Remarque 4. On peut voir que, dans le cas $n = 1$, pour tout r de $[-\frac{1}{2}, \frac{1}{2}]^{2^n}$, il existe deux éléments R_1 et R_2 de $\{-\frac{1}{2},\frac{1}{2}\}^{2^n}$ tels que les hypothèses du théorème précédent soient vérifiées. Ce n'est plus le cas dès que $n \geq 2$.

3. La méthode (cas $n = 3$)

Désormais $n = 3$.
On a alors : $e_1 = \sqrt{2+\sqrt{2+\sqrt{2}}}$, $e_2 = \sqrt{2+\sqrt{2}}$, $e_3 = \sqrt{2+\sqrt{2-\sqrt{2}}}$, $e_4 = \sqrt{2}$, $e_5 = \sqrt{2-\sqrt{2-\sqrt{2}}}$, $e_6 = \sqrt{2-\sqrt{2}}$, $e_7 = \sqrt{2-\sqrt{2+\sqrt{2}}}$.
Pour tout $(a_i)_{0\leq i\leq 7}$ de $\mathbb{Q}^8$:

$$\sigma_3(\sum_{i=0}^{7} a_i e_i) = a_0e_0 + a_1e_3 + a_2e_6 - a_3e_7 - a_4e_4 - a_5e_1 - a_6e_2 - a_7e_5,$$

et donc pour tout $(r_i)_{0\leq i\leq 7}$ de $\mathbb{R}^8$:

$$g_{\sigma_3}(r_0,r_1,r_2,r_3,r_4,r_5,r_7) = (r_0,-r_5,-r_6,r_1,-r_4,-r_7,r_2,-r_3).$$

$$M_3 = \begin{bmatrix} e_0 & e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 \\ e_0 & e_3 & e_6 & -e_7 & -e_4 & -e_1 & -e_2 & -e_5 \\ e_0 & -e_7 & -e_2 & e_5 & e_4 & -e_3 & -e_6 & e_1 \\ e_0 & e_5 & -e_6 & -e_1 & -e_4 & e_7 & e_2 & e_3 \\ e_0 & -e_1 & e_2 & -e_3 & e_4 & -e_5 & e_6 & -e_7 \\ e_0 & -e_3 & e_6 & e_7 & -e_4 & e_1 & -e_2 & e_5 \\ e_0 & e_7 & -e_2 & -e_5 & e_4 & e_3 & -e_6 & -e_1 \\ e_0 & -e_5 & -e_6 & e_1 & -e_4 & -e_7 & e_2 & -e_3 \end{bmatrix}.$$

$$(3.1) \qquad M_3^{-1} = \frac{1}{16}\begin{bmatrix} 2e_0 & 2e_0 & 2e_0 & 2e_0 & 2e_0 & 2e_0 & 2e_0 & 2e_0 \\ e_1 & e_3 & -e_7 & e_5 & -e_1 & -e_3 & e_7 & -e_5 \\ e_2 & e_6 & -e_2 & -e_6 & e_2 & e_6 & -e_2 & -e_6 \\ e_3 & -e_7 & e_5 & -e_1 & -e_3 & e_7 & -e_5 & e_1 \\ e_4 & -e_4 & e_4 & -e_4 & e_4 & -e_4 & e_4 & -e_4 \\ e_5 & -e_1 & -e_3 & e_7 & -e_5 & e_1 & e_3 & -e_7 \\ e_6 & -e_2 & -e_6 & e_2 & e_6 & -e_2 & -e_6 & e_2 \\ e_7 & -e_5 & e_1 & e_3 & -e_7 & e_5 & -e_1 & -e_3 \end{bmatrix}.$$

On veut montrer que :

$$(\mathcal{P}) \qquad \forall r \in [-\frac{1}{2},\frac{1}{2}]^8,\ \exists R \in \{-\frac{1}{2},\frac{1}{2}\}^8 \text{ tel que } |\overline{N_3}(r-R)| \leq \frac{1}{2}.$$

L'idée générale est de travailler dans l'image par $\overline{\phi}$ de $[-\frac{1}{2},\frac{1}{2}]^8$. Alors, $(\mathcal{P})$ s'exprime sous la forme :

$$(\mathcal{P}') \ \forall z \in \overline{\phi}\left([-\frac{1}{2},\frac{1}{2}]^8\right), \exists R \in \{-\frac{1}{2},\frac{1}{2}\}^8 \text{ tel que } \prod_{i=0}^{7} |z_i - \sigma_3^i \circ \psi(R)| \leq \frac{1}{2}.$$

Il suffit alors de déterminer un recouvrement de $\overline{\phi}\left([-\frac{1}{2},\frac{1}{2}]^8\right)$ par des petits cubes $\mathcal{B}_l$ de la forme $\prod_{i=0}^{7}[\alpha_i,\alpha_i+\epsilon]$, et de montrer que pour chaque $\mathcal{B}_l$ de celui-ci, on a :

$$(\mathcal{P}_l^{(1)}) \qquad \exists R \in \{-\frac{1}{2},\frac{1}{2}\}^8 \text{ tel que } \forall z \in \mathcal{B}_l,\ \prod_{i=0}^{7}|z_i - \sigma_3^i \circ \psi(R)| \leq \frac{1}{2}$$

ou à défaut :

$$\exists (R_1,R_2) \in \left(\{-\frac{1}{2},\frac{1}{2}\}^8\right)^2 \text{ tel que}$$

$$(\mathcal{P}_l^{(2)}) \quad \forall z \in \mathcal{B}_l,\ \prod_{i=0}^{7}|z_i - \sigma_3^i \circ \psi(R_1)| \leq \frac{1}{2} \text{ ou } \prod_{i=0}^{7}|z_i - \sigma_3^i \circ \psi(R_2)| \leq \frac{1}{2}.$$

Le choix d'un tel découpage "dans le plongement canonique" plutôt qu'un découpage direct de $[-\frac{1}{2},\frac{1}{2}]^8$ s'explique ainsi :

- il permet de définir un critère très simple (critère 1) pour vérifier $(\mathcal{P}_l^{(1)})$ qui donne un majorant de $\sup\{\prod_{i=0}^{7}|z_i - \sigma_3^i \circ \psi(R)|; z \in \mathcal{B}_l\}$ ne nécessitant que peu de calculs.
- ce majorant ne peut être amélioré, il est nécessairement atteint en un sommet de $\mathcal{B}_l$.
- le découpage est facilement compatible avec un autre critère (critère 2) qui permet de vérifier $(\mathcal{P}_l^{(2)})$ et qui sera défini à partir du théorème 5.

Les critères 1 et 2 seront définis explicitement à la fin de la section 3.

Mais avant tout, on voit facilement qu'il n'est pas nécessaire de montrer $(\mathcal{P}')$ pour $\overline{\phi}\left([-\frac{1}{2},\frac{1}{2}]^8\right)$ entier et que l'on peut réduire l'ensemble d'étude. Une première méthode, que nous ne développerons pas ici, consiste à se ramener, en se servant de $-Id_{\mathbb{R}^8}$ puis de H_3, à l'étude de 16 sous-ensembles particuliers de $\overline{\phi}\left([-\frac{1}{2},\frac{1}{2}]^8\right)$, de la forme $\overline{\phi}\left([0,\frac{\varepsilon_0}{2}]\times[0,\frac{\varepsilon_1}{2}]\times\ldots\times[0,\frac{\varepsilon_7}{2}]\right)$ où $(\varepsilon_0,\varepsilon_1,\ldots,\varepsilon_7) \in \{1\}\times\{-1,1\}^7$. Toutefois, d'un point de vue pratique, cette procédure de réduction donne lieu à des calculs plus lourds que ceux auxquels conduit la méthode que nous allons exposer maintenant. La raison semble en être la plus forte présence de "faces obliques" qui nécessite de prélever beaucoup plus de petits cubes $\mathcal{B}_l$ pour être sûr de recouvrir entièrement chaque $\overline{\phi}\left([0,\frac{\varepsilon_0}{2}]\times[0,\frac{\varepsilon_1}{2}]\times\ldots\times[0,\frac{\varepsilon_7}{2}]\right)$.

Nous procéderons donc de la façon suivante.
Pour $\varepsilon = (\varepsilon_0,\varepsilon_1,\varepsilon_2,\varepsilon_3,\varepsilon_4,\varepsilon_5,\varepsilon_6,\varepsilon_7) \in \{-1,1\}^8$, notons :

$$\mathcal{C}_\varepsilon = \{z \in \overline{\phi}\left([-\frac{1}{2},\frac{1}{2}]^8\right) \text{ tels que } \forall i \in \{0,1,\ldots,7\}\ \varepsilon_i z_i \geq 0\}.$$

Théorème 6. *Pour que $(\mathcal{P}')$ soit vérifiée, il suffit que l'on ait :*

$$(\mathcal{P}_\varepsilon) \qquad \forall z \in \mathcal{C}_\varepsilon,\ \exists R \in \{-\frac{1}{2}, \frac{1}{2}\}^8 \text{ tel que } \prod_{i=0}^{7} |z_i - \sigma_3^i \circ \psi(R)| \leq \frac{1}{2}$$

pour les 20 *valeurs de* ε *suivantes :*

$$\begin{cases} \varepsilon^{(1)} = (1,1,1,1,1,1,1,1), & \varepsilon^{(2)} = (1,-1,1,-1,1,-1,1,-1), \\ \varepsilon^{(3)} = (1,1,-1,-1,1,1,-1,-1), & \varepsilon^{(4)} = (1,1,1,-1,1,1,1,-1), \\ \varepsilon^{(5)} = (1,1,1,1,-1,-1,-1,-1), & \varepsilon^{(6)} = (1,-1,1,1,-1,1,-1,-1), \\ \varepsilon^{(7)} = (1,1,1,1,1,1,1,-1), & \varepsilon^{(8)} = (1,1,1,1,1,1,-1,-1), \\ \varepsilon^{(9)} = (1,1,1,1,1,-1,1,-1), & \varepsilon^{(10)} = (1,1,1,1,-1,1,1,-1), \\ \varepsilon^{(11)} = (1,1,1,1,1,-1,-1,-1), & \varepsilon^{(12)} = (1,1,1,1,-1,1,-1,-1), \\ \varepsilon^{(13)} = (1,1,1,-1,1,1,-1,-1), & \varepsilon^{(14)} = (1,1,-1,1,1,1,-1,-1), \\ \varepsilon^{(15)} = (1,-1,1,1,1,1,-1,-1), & \varepsilon^{(16)} = (1,1,1,-1,1,-1,1,-1), \\ \varepsilon^{(17)} = (1,1,-1,1,1,-1,1,-1), & \varepsilon^{(18)} = (1,1,1,-1,1,-1,-1,-1), \\ \varepsilon^{(19)} = (1,1,-1,1,1,-1,-1,-1), & \varepsilon^{(20)} = (1,1,-1,1,-1,1,-1,-1). \end{cases}$$

Preuve. Soit ε quelconque de $\{-1,1\}^8$, et soit $h = \alpha g_{\sigma_3}^l$ où $\alpha \in \{-1,1\}$ et où $0 \leq l \leq 7$, un élément quelconque de H_3'.
Si $\mathcal{C}$ est l'ensemble des $\mathcal{C}_{\varepsilon'}$, où ε' décrit $\{-1,1\}^8$, nous allons d'abord montrer que $\overline{\phi} \circ h \circ \overline{\phi}^{-1}(\mathcal{C}_\varepsilon) \in \mathcal{C}$.
Notons c l'application de $\mathbb{R}^8$ dans $\mathbb{R}^8$ définie par :

$$c(r_0, r_1, ..., r_6, r_7) = (r_1, r_2, ..., r_7, r_0).$$

D'une part si $z \in \mathbb{R}^8$ et si $z = \overline{\phi}(r) = \big(\psi(r), \psi \circ g_{\sigma_3}(r), ..., \psi \circ g_{\sigma_3}^7(r)\big)$ où $r \in \mathbb{R}^8$ on a :

$$\begin{aligned} \overline{\phi} \circ h \circ \overline{\phi}^{-1}(z) &= \overline{\phi} \circ h(r) \\ &= \alpha \overline{\phi} \circ g_{\sigma_3}^l(r) \\ &= \alpha \left(\psi \circ g_{\sigma_3}^l(r), \psi \circ g_{\sigma_3}^{l+1}(r), ..., \psi \circ g_{\sigma_3}^{l+7}(r)\right) \\ &= \alpha \left(\psi \circ g_{\sigma_3}^{l \bmod 8}(r), ..., \psi \circ g_{\sigma_3}^{l+7 \bmod 8}(r)\right) \\ &= \alpha c^l(z). \end{aligned}$$

On en déduit que :

$$\overline{\phi} \circ h \circ \overline{\phi}^{-1}\big(\{z \in \mathbb{R}^8 \text{ tels que } \forall i, \varepsilon_i z_i \geq 0\}\big) = \{z \in \mathbb{R}^8 \text{ tels que } \forall i, \varepsilon_i' z_i \geq 0\}$$

où $\varepsilon' = \alpha c^l(\varepsilon)$.

D'autre part, comme $h(r_0, r_1, ..., r_7) = \alpha(r_0, \beta_1 r_{t(1)}, ..., \beta_7 r_{t(7)})$ où $t \in \mathcal{S}_7$ et $\beta_i \in \{-1, 1\}$ pour tout i (cf (1.2)), on a : $h\left([-\frac{1}{2}, \frac{1}{2}]^8\right) = [-\frac{1}{2}, \frac{1}{2}]^8$, d'où

$$\overline{\phi} \circ h \circ \overline{\phi}^{-1}\left(\overline{\phi}\left([-\frac{1}{2}, \frac{1}{2}]^8\right)\right) = \overline{\phi}\left([-\frac{1}{2}, \frac{1}{2}]^8\right).$$

Comme $\overline{\phi} \circ h \circ \overline{\phi}^{-1}$ est bijective on obtient par intersection :

$$\overline{\phi} \circ h \circ \overline{\phi}^{-1}(\mathcal{C}_\varepsilon) = \mathcal{C}_{\varepsilon'} \text{ où } \varepsilon' = \alpha c^l(\varepsilon).$$

On voit alors facilement que $\overline{\phi} \circ h \circ \overline{\phi}^{-1}$ induit une permutation de $\mathcal{C}$, et l'on peut définir une action du groupe H_3' sur $\mathcal{C}$ par :

$$\text{si } h \in H_3' \text{ et si } \varepsilon \in \{-1, 1\}^8, h.\mathcal{C}_\varepsilon = \overline{\phi} \circ h \circ \overline{\phi}^{-1}(\mathcal{C}_\varepsilon).$$

On a en effet trivialement : $h.(h'.\mathcal{C}_\varepsilon) = h \circ h'.\mathcal{C}_\varepsilon$.
Soient alors $\mathcal{C}_\varepsilon$ et $\mathcal{C}_{\varepsilon'}$ deux éléments de $\mathcal{C}$ situés dans une même orbite sous cette action. Supposons que $\mathcal{C}_\varepsilon$ vérifie $(\mathcal{P}_\varepsilon)$ et montrons que $\mathcal{C}_{\varepsilon'}$ vérifie $(\mathcal{P}_{\varepsilon'})$. $\mathcal{C}_\varepsilon$ et $\mathcal{C}_{\varepsilon'}$ étant dans la même orbite, il existe $h \in H_3'$ tel que $\mathcal{C}_{\varepsilon'} = h.\mathcal{C}_\varepsilon$.
Soit z' quelconque de $\mathcal{C}_{\varepsilon'}$. Alors : $z' = \overline{\phi} \circ h \circ \overline{\phi}^{-1}(z)$ où $z \in \mathcal{C}_\varepsilon$ et

$$\exists R \in \{-\frac{1}{2}, \frac{1}{2}\}^8 \text{ tel que } \prod_{i=0}^{7} |z_i - \sigma_3^i \circ \psi(R)| \leq \frac{1}{2}.$$

Soient $r = \overline{\phi}^{-1}(z)$ et $r' = \overline{\phi}^{-1}(z')$. On a : $r' = h(r)$. Soit $R' = h(R)$. $R' \in \{-\frac{1}{2}, \frac{1}{2}\}^8$, car $h(R_0, R_1, ..., R_7) = \alpha(R_0, \beta_1 R_{t(1)}, ..., \beta_7 R_{t(7)})$ où $t \in \mathcal{S}_7$, $\alpha \in \{-1, 1\}$ et $\beta_i \in \{-1, 1\}$ pour tout i. De plus :

$$\begin{aligned}
\prod_{i=0}^{7} |z_i' - \sigma_3^i \circ \psi(R')| &= \prod_{i=0}^{7} |\psi \circ g_{\sigma_3}^i (r' - R')| \\
&= |\overline{N_3} \circ h(r - R)| \\
&= |\overline{N_3}(r - R)| \qquad \text{(cf proposition - section 1)} \\
&= \prod_{i=0}^{7} |z_i - \sigma_3^i \circ \psi(R)| \ \leq \frac{1}{2}.
\end{aligned}$$

Ainsi, $\mathcal{C}_{\varepsilon'}$ vérifie $(\mathcal{P}_{\varepsilon'})$.
Par suite, pour montrer que tous les $\mathcal{C}_\varepsilon$ vérifient $(\mathcal{P}_\varepsilon)$ et donc que $(\mathcal{P}')$ est vraie (car $\overline{\phi}\left([-\frac{1}{2}, \frac{1}{2}]^8\right)$ est réunion des $\mathcal{C}_\varepsilon$), il suffit de montrer qu'un élément $\mathcal{C}_\varepsilon$ de chaque orbite vérifie $(\mathcal{P}_\varepsilon)$. Pour déterminer les orbites on peut par exemple raisonner sur les stabilisateurs.
Le stabilisateur de $\mathcal{C}_\varepsilon$ ne peut contenir $-Id_{\mathbb{R}^8}$ car on ne peut avoir $-\varepsilon = \varepsilon$. Les stabilisateurs sont donc d'ordre 8, 4, 2 ou 1. Les seuls sous-groupes

d'ordre 8 de H_3' ne contenant pas $-Id_{\mathbb{R}^8}$ sont $H_3 = \langle g_{\sigma_3}\rangle$ et $\langle -g_{\sigma_3}\rangle$, et conduisent respectivement aux orbites de $\mathcal{C}_{\varepsilon(1)}$ et $\mathcal{C}_{\varepsilon(2)}$ (qui ont donc pour cardinal 2). Les seuls sous-groupes d'ordre 4 de H_3' ne contenant pas $-Id_{\mathbb{R}^8}$ sont $\langle g_{\sigma_3}^2\rangle$ et $\langle -g_{\sigma_3}^2\rangle$. Mais si $\mathcal{C}_\varepsilon$ est invariant sous l'action de $g_{\sigma_3}^2$, on retrouve les valeurs de ε précédemment rencontrées. $\langle -g_{\sigma_3}^2\rangle$ conduit à l'orbite de $\mathcal{C}_{\varepsilon(3)}$, qui a pour cardinal 4. En continuant on détermine l'orbite de $\mathcal{C}_{\varepsilon(4)}$ de stabilisateur $\langle g_{\sigma_3}^4\rangle$, celle de $\mathcal{C}_{\varepsilon(5)}$ et celle de $\mathcal{C}_{\varepsilon(6)}$ de stabilisateur $\langle -g_{\sigma_3}^4\rangle$, toutes trois de cardinal 8. Enfin toutes les autres orbites ont pour cardinal 16, il y en a nécessairement 14 ($\frac{256-2\times 2-4-3\times 8}{16}$). Il ne reste plus qu'à déterminer 14 éléments de $\mathcal{C}$ appartenant chacun à une orbite différente et n'appartenant pas aux 6 orbites précédemment déterminées. Les 14 éléments $\mathcal{C}_{\varepsilon(j)}$, j variant de 7 à 20, cités dans le théorème, le vérifient. $\square$

Soit ε donné de la famille définie dans le théorème 6. Décrivons maintenant l'algorithme permettant de montrer que $(\mathcal{P}_\varepsilon)$ est vérifiée.

Posons pour $n \geq 1$

$$\alpha_n = \sum_{i=0}^{2^n-1} e_i = \frac{1+\cos\left(\frac{\pi}{2^{n+1}}\right)}{\sin\left(\frac{\pi}{2^{n+1}}\right)}.$$

On a facilement :

$$\overline{\phi}\left([-\frac{1}{2},\frac{1}{2}]^8\right) \subset [-\frac{\alpha_3}{2},\frac{\alpha_3}{2}]^8. \tag{3.2}$$

Découpons ce dernier cube de la façon suivante.
Choisissons un entier p pair, non nul et posons :

$$y_k = -\frac{\alpha_3}{2} + kh \text{ où } h = \frac{\alpha_3}{p} \text{ et } 0 \leq k \leq p. \tag{3.3}$$

Si $l = (l_0, l_1, \ldots, l_7) \in \{0,1,\ldots,p-1\}^8$, définissons $\mathcal{B}_l$ par :

$$\mathcal{B}_l = \{(z_0, z_1, \ldots, z_7) \in \mathbb{R}^8 \text{ tel que } \forall k \in \{0,1,\ldots,7\}, y_{l_k} \leq z_k \leq y_{l_k+1}\}.$$

$[-\frac{\alpha_3}{2},\frac{\alpha_3}{2}]^8$ est réunion des $\mathcal{B}_l$, donc par (3.2) ceux-ci recouvrent $\overline{\phi}\left([-\frac{1}{2},\frac{1}{2}]^8\right)$.
Soit $\varepsilon = (\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_7)$ de $\{-1,1\}^8$. Posons

$$k_i = (1+\varepsilon_i)\frac{p}{4} \quad \text{et} \quad K_i = (1+\varepsilon_i)\frac{p}{4} + \frac{p}{2}.$$

Ainsi si $\varepsilon_i = 1$, $k_i = \frac{p}{2}$ et $K_i = p$, et si $\varepsilon_i = -1$, $k_i = 0$ et $K_i = \frac{p}{2}$. Comme

$$[-\frac{\alpha_3}{2}, 0] = \bigcup_{k=0}^{\frac{p}{2}-1} [y_k, y_{k+1}] \text{ et } [0, \frac{\alpha_3}{2}] = \bigcup_{k=\frac{p}{2}}^{p-1} [y_k, y_{k+1}],$$

on voit que $\{z \in [-\frac{\alpha_3}{2}, \frac{\alpha_3}{2}]^8$ tels que $\forall i \in \{0,1,...,7\}$ $\varepsilon_i z_i \geq 0\}$ est réunion des $\mathcal{B}_l$ vérifiant $k_i \leq l_i \leq K_i - 1$ pour tout i de $\{0,1,...,7\}$. A fortiori, $\mathcal{C}_\varepsilon$ qui en est un sous-ensemble, est recouvert par ces mêmes $\mathcal{B}_l$:

$$\mathcal{C}_\varepsilon \subset \bigcup_{\substack{l \in \{0,1,\dots,p-1\}^8 \\ \text{tels que } \forall i \ k_i \leq l_i \leq K_i - 1}} \mathcal{B}_l. \tag{3.4}$$

Cependant dans les recouvrements ainsi obtenus de $\overline{\phi}\left([-\frac{1}{2},\frac{1}{2}]^8\right)$ et des $\mathcal{C}_\varepsilon$ par les $\mathcal{B}_l$, beaucoup d'entre ceux-ci sont inutiles dès que p est assez grand. En effet lorsque p tend vers $+\infty$, la probabilité pour qu'un $\mathcal{B}_l$ rencontre $\overline{\phi}\left([-\frac{1}{2},\frac{1}{2}]^8\right)$ tend vers :

$$\frac{\mathrm{vol}\left(\overline{\phi}\left([-\frac{1}{2},\frac{1}{2}]^8\right)\right)}{\mathrm{vol}\left([-\frac{\alpha_3}{2},\frac{\alpha_3}{2}]^8\right)} = \frac{\sqrt{D_3}}{\alpha_3^8} \approx 0,0004.$$

Il convient donc de définir un recouvrement plus raisonnable de chaque $\mathcal{C}_\varepsilon$. A cet effet, introduisons les 8 formes linéaires s_i(où $0 \leq i \leq 7$) définies sur $\mathbb{R}^8$ par :

$$s_i(z) = \frac{\lambda_i}{16}\sum_{j=0}^{7}\sigma_3^j(e_i)z_j,$$

où $\lambda_0 = 2$ et $\lambda_i = 1$ sinon.
Alors le théorème 2 montre que :

$$\overline{\phi}^{-1}(z) = (s_i(z))_{0 \leq i \leq 7}.$$

La matrice M_3^{-1} (cf (3.1)) fournit les formules explicitant les s_i. On peut alors énoncer le

Théorème 7. *On obtient un recouvrement de $\mathcal{C}_\varepsilon$ en ne considérant que les $\mathcal{B}_l$ pour lesquels l_7 vérifie, si c'est possible :*

$$k_7 \leq l_7 \leq K_7 - 1$$

et

$$\max\left(m_i - 1, i \in \{0,1,...,7\}\right) \leq l_7 \leq \min\left(m'_i, i \in \{0,1,...,7\}\right) \textit{ où :}$$

$$\begin{cases} m_0 &= \frac{1}{h}\left(-4-8s_0(y_{l_0+1},y_{l_1+1},y_{l_2+1},y_{l_3+1},y_{l_4+1},y_{l_5+1},y_{l_6+1},0)-y_0\right)\\ m'_0 &= \frac{1}{h}\left(4-8s_0(y_{l_0},y_{l_1},y_{l_2},y_{l_3},y_{l_4},y_{l_5},y_{l_6},0)-y_0\right)\\ m_1 &= \frac{1}{he_5}\left(-8+16s_1(y_{l_0},y_{l_1},y_{l_2+1},y_{l_3},y_{l_4+1},y_{l_5+1},y_{l_6},0)-y_0e_5\right)\\ m'_1 &= \frac{1}{he_5}\left(8+16s_1(y_{l_0+1},y_{l_1+1},y_{l_2},y_{l_3+1},y_{l_4},y_{l_5},y_{l_6+1},0)-y_0e_5\right)\\ m_2 &= \frac{1}{he_6}\left(-8+16s_2(y_{l_0},y_{l_1},y_{l_2+1},y_{l_3+1},y_{l_4},y_{l_5},y_{l_6+1},0)-y_0e_6\right)\\ m'_2 &= \frac{1}{he_6}\left(8+16s_2(y_{l_0+1},y_{l_1+1},y_{l_2},y_{l_3},y_{l_4+1},y_{l_5+1},y_{l_6},0)-y_0e_6\right)\\ m_3 &= \frac{1}{he_1}\left(-8-16s_3(y_{l_0+1},y_{l_1},y_{l_2+1},y_{l_3},y_{l_4},y_{l_5+1},y_{l_6},0)-y_0e_1\right)\\ m'_3 &= \frac{1}{he_1}\left(8-16s_3(y_{l_0},y_{l_1+1},y_{l_2},y_{l_3+1},y_{l_4+1},y_{l_5},y_{l_6+1},0)-y_0e_1\right)\\ m_4 &= \frac{1}{he_4}\left(-8+16s_4(y_{l_0},y_{l_1+1},y_{l_2},y_{l_3+1},y_{l_4},y_{l_5+1},y_{l_6},0)-y_0e_4\right)\\ m'_4 &= \frac{1}{he_4}\left(8+16s_4(y_{l_0+1},y_{l_1},y_{l_2+1},y_{l_3},y_{l_4+1},y_{l_5},y_{l_6+1},0)-y_0e_4\right)\\ m_5 &= \frac{1}{he_7}\left(-8+16s_5(y_{l_0},y_{l_1+1},y_{l_2+1},y_{l_3},y_{l_4+1},y_{l_5},y_{l_6},0)-y_0e_7\right)\\ m'_5 &= \frac{1}{he_7}\left(8+16s_5(y_{l_0+1},y_{l_1},y_{l_2},y_{l_3+1},y_{l_4},y_{l_5+1},y_{l_6+1},0)-y_0e_7\right)\\ m_6 &= \frac{1}{he_2}\left(-8-16s_6(y_{l_0+1},y_{l_1},y_{l_2},y_{l_3+1},y_{l_4+1},y_{l_5},y_{l_6},0)-y_0e_2\right)\\ m'_6 &= \frac{1}{he_2}\left(8-16s_6(y_{l_0},y_{l_1+1},y_{l_2+1},y_{l_3},y_{l_4},y_{l_5+1},y_{l_6+1},0)-y_0e_2\right)\\ m_7 &= \frac{1}{he_3}\left(-8+16s_7(y_{l_0},y_{l_1+1},y_{l_2},y_{l_3},y_{l_4+1},y_{l_5},y_{l_6+1},0)-y_0e_3\right)\\ m'_7 &= \frac{1}{he_3}\left(8+16s_7(y_{l_0+1},y_{l_1},y_{l_2+1},y_{l_3+1},y_{l_4},y_{l_5+1},y_{l_6},0)-y_0e_3\right). \end{cases}$$

Preuve. Le premier encadrement vient de (3.4). Pour le reste, raisonnons en termes d'exclusion et tenons compte du fait que l'on peut éliminer les $\mathcal{B}_l$ tels qu'il existe i de $\{0,1,...7\}$ pour lequel :

$$(R_i) : \left(\forall z \in \mathcal{B}_l,\ r=\overline{\phi}^{-1}(z) \text{ vérifie } r_i < -\frac{1}{2}\right)$$

ou

$$(R'_i) : \left(\forall z \in \mathcal{B}_l,\ r=\overline{\phi}^{-1}(z) \text{ vérifie } r_i > \frac{1}{2}\right).$$

On a alors en effet : $\overline{\phi}^{-1}(\mathcal{B}_l)\cap[-\frac{1}{2},\frac{1}{2}]^8=\emptyset$, et par bijectivité de $\overline{\phi}$: $\mathcal{B}_l\cap\overline{\phi}\left([-\frac{1}{2},\frac{1}{2}]^8\right)=\emptyset$ et $\mathcal{B}_l\cap\mathcal{C}_\varepsilon=\emptyset$.

Si $r=(r_0,r_1,...,r_7)=\overline{\phi}^{-1}(z)$ alors $r_0=s_0(z)$.

L'expression de s_0 que l'on peut déduire de (3.1), à savoir

$$s_0(z)=\frac{1}{8}\sum_{i=0}^{7}z_i, \tag{3.5}$$

montre que, si $z\in\mathcal{B}_l$, la plus petite valeur possible de $s_0(z)$ est $s_0(y_{l_0},y_{l_1},y_{l_2},y_{l_3},y_{l_4},y_{l_5},y_{l_6},y_{l_7})$ et que la plus grande valeur possible de $s_0(z)$ est $s_0(y_{l_0+1},y_{l_1+1},y_{l_2+1},y_{l_3+1},y_{l_4+1},y_{l_5+1},y_{l_6+1},y_{l_7+1})$.

Pour que $\mathcal{B}_l$ ne vérifie pas (R'_0), il est nécessaire d'avoir :

$$s_0(y_{l_0},y_{l_1},y_{l_2},y_{l_3},y_{l_4},y_{l_5},y_{l_6},y_{l_7})\le\frac{1}{2}. \tag{3.6}$$

Pour que $\mathcal{B}_l$ ne vérifie pas (R_0), il est nécessaire d'avoir :

$$s_0(y_{l_0+1}, y_{l_1+1}, y_{l_2+1}, y_{l_3+1}, y_{l_4+1}, y_{l_5+1}, y_{l_6+1}, y_{l_7+1}) \geq -\frac{1}{2}. \tag{3.7}$$

L'inégalité (3.6) donne, compte tenu de (3.5) :

$$s_0(y_{l_0}, y_{l_1}, y_{l_2}, y_{l_3}, y_{l_4}, y_{l_5}, y_{l_6}, 0) + \frac{1}{8} y_{l_7} \leq \frac{1}{2},$$

ou encore, par (3.3) :

$$l_7 \leq \frac{1}{h}\left(4 - 8 s_0(y_{l_0}, y_{l_1}, y_{l_2}, y_{l_3}, y_{l_4}, y_{l_5}, y_{l_6}, 0) - y_0\right).$$

De même (3.7) conduit à :

$$l_7 + 1 \geq \frac{1}{h}\left(-4 - 8 s_0(y_{l_0+1}, y_{l_1+1}, y_{l_2+1}, y_{l_3+1}, y_{l_4+1}, y_{l_5+1}, y_{l_6+1}, 0) - y_0\right).$$

Et l_7 peut être choisi de telle sorte que : $m_0 - 1 \leq l_7 \leq m'_0$.
En observant M_3^{-1} et en raisonnant de la même manière sur les valeurs extrêmes des $s_i(z)$ $(1 \leq i \leq 7)$ sur $\mathcal{B}_l$, et sur les conditions d'exclusion (R_i) et (R'_i), on trouverait les encadrements : $m_i - 1 \leq l_7 \leq m'_i$, avec les valeurs de m_i et m'_i indiquées dans l'énoncé du théorème. □

Remarque 5. Pour un 7-uplet donné $(l_0, l_1, l_2, l_3, l_4, l_5, l_6)$, l'ensemble des l_7 déterminé par le théorème 7 est souvent réduit à $\emptyset$. Comme d'un point de vue pratique, étudier $(\frac{p}{2})^7$ cas dont beaucoup sont inutiles n'est pas envisageable, on peut définir des conditions sur l_6 de la façon suivante :
$(l_0, l_1, l_2, l_3, l_4, l_5, l_6)$ étant donné on peut encadrer $s_0(z)$ où $z \in \mathcal{C}_\varepsilon$ par :
$s_0(z) \leq s_0(y_{l_0+1}, y_{l_1+1}, y_{l_2+1}, y_{l_3+1}, y_{l_4+1}, y_{l_5+1}, y_{l_6+1}, y_{K_7})$
et $s_0(z) \geq s_0(y_{l_0}, y_{l_1}, y_{l_2}, y_{l_3}, y_{l_4}, y_{l_5}, y_{l_6}, y_{k_7})$.
Compte tenu du fait que l'on peut écarter les $\mathcal{B}_l$ vérifiant (R_0) ou (R'_0), on peut imposer à $(l_0, l_1, l_2, l_3, l_4, l_5, l_6)$ les deux conditions :

$$s_0(y_{l_0+1}, y_{l_1+1}, y_{l_2+1}, y_{l_3+1}, y_{l_4+1}, y_{l_5+1}, y_{l_6+1}, y_{K_7}) \geq -\frac{1}{2}$$
$$s_0(y_{l_0}, y_{l_1}, y_{l_2}, y_{l_3}, y_{l_4}, y_{l_5}, y_{l_6}, y_{k_7}) \leq \frac{1}{2}.$$

Ces inégalités conduisent à :

$$\begin{cases} l_6 + 1 & \geq \frac{1}{h}\left(-4 - 8 s_0(y_{l_0+1}, y_{l_1+1}, y_{l_2+1}, y_{l_3+1}, y_{l_4+1}, y_{l_5+1}, 0, y_{K_7}) - y_0\right) \\ l_6 & \leq \frac{1}{h}\left(4 - 8 s_0(y_{l_0}, y_{l_1}, y_{l_2}, y_{l_3}, y_{l_4}, y_{l_5}, 0, y_{k_7}) - y_0\right). \end{cases}$$

De la même manière, en travaillant avec les s_i $(1 \leq i \leq 7)$, on trouverait 14 autres inégalités devant être vérifiées par l_6. Les premières sont :

$$\begin{cases} l_6+1 & \geq \frac{1}{he_7}\left(-8-16s_1(y_{l_0+1},y_{l_1+1},y_{l_2},y_{l_3+1},y_{l_4},y_{l_5},0,y_{k_7})-y_0e_7\right) \\ l_6 & \leq \frac{1}{he_7}\left(8-16s_1(y_{l_0},y_{l_1},y_{l_2+1},y_{l_3},y_{l_4+1},y_{l_5+1},0,y_{K_7})-y_0e_7\right) \\ l_6+1 & \geq \frac{1}{he_2}\left(-8+16s_2(y_{l_0},y_{l_1},y_{l_2+1},y_{l_3+1},y_{l_4},y_{l_5},0,y_{K_7})-y_0e_2\right) \\ l_6 & \leq \frac{1}{he_2}\left(8+16s_2(y_{l_0+1},y_{l_1+1},y_{l_2},y_{l_3},y_{l_4+1},y_{l_5+1},0,y_{k_7})-y_0e_2\right) \\ l_6+1 & \geq \frac{1}{he_5}\left(-8+16s_5(y_{l_0},y_{l_1+1},y_{l_2},y_{l_3+1},y_{l_4+1},y_{l_5},0,y_{k_7})-y_0e_5\right) \\ l_6 & \leq \frac{1}{he_5}\left(8+16s_5(y_{l_0+1},y_{l_1},y_{l_2+1},y_{l_3},y_{l_4},y_{l_5+1},0,y_{K_7})-y_0e_5\right) \\ \textit{etc.} & \end{cases}$$

A ces 16 inégalités on ajoute la condition : $k_6 \leq l_6 \leq K_6 - 1$.
On peut alors recommencer avec l_5 et définir un encadrement des valeurs possibles de l_5 en fonction de $(l_0, l_1, l_2, l_3, l_4)$, puis faire la même chose avec l_4 en fonction de (l_0, l_1, l_2, l_3). Ces procédures permettent un gain de temps considérable.

Il ne nous reste plus qu'à énoncer les critères fondamentaux permettant de montrer qu'un cube $\mathcal{B}_l$ vérifie la propriété $(\mathcal{P}_l^{(1)})$ ou à défaut la propriété $(\mathcal{P}_l^{(2)})$.

Critère 1. *Soient ε une des 20 valeurs déterminées dans le théorème 6 et $\mathcal{B}_l$ un cube élément du recouvrement de $\mathcal{C}_\varepsilon$ déterminé précédemment. S'il existe R de $\{-\frac{1}{2}, \frac{1}{2}\}^8$ tel que :*

$$\prod_{j=0}^{7} \max\left(|y_{l_j} - \sigma_3^j \circ \psi(R)|, |y_{l_j+1} - \sigma_3^j \circ \psi(R)|\right) \leq \frac{1}{2},$$

alors $\mathcal{B}_l$ vérifie $(\mathcal{P}_l^{(1)})$.

Preuve. Soit $z = (z_0, z_1, ..., z_7)$ quelconque de $\mathcal{B}_l$. Alors on a :

$$\forall j \in \{0,1,...,7\},\ y_{l_j} \leq z_j \leq y_{l_j+1}.$$

Par convexité de l'application : $t \longmapsto |t|$, on a alors pour tout R de $\mathbb{Q}^8$ et pour tout j de $\{0,1,...,7\}$:

$$|z_j - \sigma_3^j \circ \psi(R)| \leq \max\left(|y_{l_j} - \sigma_3^j \circ \psi(R)|, |y_{l_j+1} - \sigma_3^j \circ \psi(R)|\right),$$

et par conséquent :

$$\prod_{j=0}^{7} |z_j - \sigma_3^j \circ \psi(R)| \leq \prod_{j=0}^{7} \max\left(|y_{l_j} - \sigma_3^j \circ \psi(R)|, |y_{l_j+1} - \sigma_3^j \circ \psi(R)|\right).$$

D'où le théorème. $\square$

Remarque 6. Le majorant précédemment déterminé ne peut être amélioré car il est atteint par un des sommets du cube. Par ailleurs on peut remarquer que

$$\max\left(|y_{l_j}-\sigma_3^j\circ\psi(R)|,|y_{l_j+1}-\sigma_3^j\circ\psi(R)|\right)=\left|\frac{y_{l_j}+y_{l_j+1}}{2}-\sigma_3^j\circ\psi(R)\right|+\frac{h}{2}.$$

Critère 2. *Sous les mêmes hypothèses, s'il existe R_1 et R_2 de $\{-\frac{1}{2},\frac{1}{2}\}^8$ tels que :*
$\forall j\in\{0,1,...,7\},\ (y_{l_j}-\sigma_3^j\circ\psi(R_1))(y_{l_j}-\sigma_3^j\circ\psi(R_2))\leq 0,$
$\forall j\in\{0,1,...,7\},\ (y_{l_j+1}-\sigma_3^j\circ\psi(R_1))(y_{l_j+1}-\sigma_3^j\circ\psi(R_2))\leq 0,$
et $|N_{\mathbb{Q}_3/\mathbb{Q}}\circ\psi(R_1-R_2)|\leq 128,$
alors $\mathcal{B}_l$ vérifie $(\mathcal{P}_l^{(2)})$.

Preuve. Ce résultat n'est qu'une variante du théorème 5.
Soit z quelconque de $\mathcal{B}_l$. Par hypothèse, pour tout j, y_{l_j} et y_{l_j+1} donc z_j sont compris (au sens large) entre $\sigma_3^j\circ\psi(R_1)$ et $\sigma_3^j\circ\psi(R_2)$. Ainsi z vérifie les hypothèses du théorème 5 et nécessairement

$$\prod_{j=0}^{7}|z_j-\sigma_3^j\circ\psi(R_1)|\leq\frac{1}{2}\text{ ou }\prod_{j=0}^{7}|z_j-\sigma_3^j\circ\psi(R_2)|\leq\frac{1}{2}.$$

Ainsi $\mathcal{B}_l$ vérifie $(\mathcal{P}_l^{(2)})$. □

4. Le programme et les résultats

L'algorithme est alors simple. On se donne un ε de la famille définie au théorème 6. On choisit p suffisamment grand (le seul critère est la réussite du test). Pour montrer $(\mathcal{P}_\varepsilon)$ on fait prendre à (l_0,l_1,l_2,l_3) toutes les valeurs de $\{k_0,...,K_0-1\}\times\{k_1,...,K_1-1\}\times\{k_2,...,K_2-1\}\times\{k_3,...,K_3-1\}$, à chaque nouvelle valeur de ce quaduplet on calcule l'intervalle des possibilités pour l_4 (cf la remarque 5), on fait varier l_4 dans cet intervalle, à chaque nouvelle valeur de l_4 on calcule l'intervalle des possibilités pour l_5,...etc, jusqu'à faire varier l_7 dans l'intervalle défini par le théorème 7. On cherche alors un élément R de $\{-\frac{1}{2},\frac{1}{2}\}^8$ tel que le cube $\mathcal{B}_l$ vérifie le critère 1. Si un tel élément n'existe pas, on cherche s'il existe un couple (R_1,R_2) de $\left(\{-\frac{1}{2},\frac{1}{2}\}^8\right)^2$ vérifiant le critère 2. Si le test est positif pour chaque $\mathcal{B}_l$ défini à l'aide des inégalités du théorème 7 et de la remarque 5, alors la propriété $(\mathcal{P}_\varepsilon)$ est vraie. On fait la même chose pour les 19 autres valeurs de ε données au théorème 6.

En pratique, pour que le programme montre le résultat, il faut prendre p assez grand (de l'ordre de 40), mais les calculs sont alors abondants. Aussi a-t-on défini une procédure de dichotomie, qui, lorsqu'on rencontre un cube $\mathcal{B}_l$ ne vérifiant pas le critère 1, le divise en 256 petits cubes de même taille, élimine parmi ceux-ci ceux dont on est sûr que leur intersection avec $\mathcal{C}_\varepsilon$ est vide (par un test semblable à celui du théorème 7), et fait subir à ceux qui restent le test relatif au critère 1. Si un de ces petits cubes ne vérifie pas le critère, ce qui est très rare en pratique, on revient à $\mathcal{B}_l$ et on lui fait subir le test relatif au critère 2. Ainsi p de l'ordre de 20 suffit.

Par ailleurs, quand on cherche pour un $\mathcal{B}_l$ donné un R adéquat (vérifiant le critère 1), on parcourt d'abord, par ordre d'indice décroissant, un tableau dans lequel sont stockés au fur et à mesure les R utilisés. Ce tableau est initialisé à $\emptyset$. Si un R du tableau convient, on réindexe celui-ci, en mettant le R adéquat en dernière position. Si aucun élément du tableau ne convient on lance une recherche systématique et le premier R convenable détecté est placé en dernière position dans le tableau. Le gain de temps ainsi réalisé est appréciable.

Reste le problème de la précision. Le programme a été rédigé en *Pascal* (Turbo Pascal 6.0 de Borland). Compte tenu de l'imprécision relative en mode *real* (les calculs ont cependant été menés en mode *extended*), on a pris comme test effectif pour le critère 1 :

$$\prod_{j=0}^{7} \max\Big(|y_{l_j} - \sigma_3^j \circ \psi(R)|, |y_{l_j+1} - \sigma_3^j \circ \psi(R)|\Big) < 0.49,$$

ou encore (cf remarque 6), ce qui est légèrement plus rapide,

$$\prod_{j=0}^{7} \left(\left|\frac{y_{l_j} + y_{l_j+1}}{2} - \sigma_3^j \circ \psi(R)\right| + \frac{h}{2}\right) < 0.49,$$

et comme test effectif pour le critère 2 :

$$\forall j \in \{0, 1, ..., 7\},\ (y_{l_j} - \sigma_3^j \circ \psi(R_1))(y_{l_j} - \sigma_3^j \circ \psi(R_2)) < -0.0001,$$
$$\forall j \in \{0, 1, ..., 7\},\ (y_{l_j+1} - \sigma_3^j \circ \psi(R_1))(y_{l_j+1} - \sigma_3^j \circ \psi(R_2)) < -0.0001,$$
$$\text{et } |N_{\mathbb{Q}_3/\mathbb{Q}} \circ \psi(R_1 - R_2)| \leq 128.5.$$

De fait, $N_{\mathbb{Q}_3/\mathbb{Q}} \circ \psi(R_1 - R_2)$ est un entier car $\psi(R_1 - R_2) \in \mathcal{R}_3$.
De plus, il se peut que les valeurs déterminées pour $\max(m_i - 1) = m_{i_0} - 1$ et $\min(m'_i) = m'_{j_0}$ soient presqu'entières. On a alors pris les précautions suivantes : si $0 < (m_{i_0} - 1) - m < 0.01$ où m est entier, on ajoute le cas $l_7 = m$ à l'intervalle défini par le théorème 7, si $k_7 \leq m$; de même, si $0 < m' - m'_{j_0} < 0.01$ où m' est entier, on ajoute le cas $l_7 = m'$ à l'intervalle défini par le théorème 7, si $m' \leq K_7 - 1$. On procède de même avec les encadrements fournis par la remarque 5. Une étude simple tenant compte des ordres de grandeur des nombres utilisés montre que ces précautions sont amplement suffisantes (en agissant ainsi, on est amené à étudier de nombreux $\mathcal{B}_l$ périphériques inutiles).

Le programme a été exécuté pour la première fois en 1997 sur un micro-ordinateur de type 486 DX 33, mais sous une forme incomplète (sans le critère 2 et avec 0.99 à la place de 0.49), ce qui à l'époque nous a permis de conclure à l'euclidianité de $\mathbb{Q}_3$ pour la norme. Pour la forme complète décrite ici, nous avons utilisé un micro-ordinateur "familial" plus récent, équipé d'un processeur Pentium II cadencé à 300 Mhz et doté de 64 Mo de mémoire vive. Le temps de calcul varie de 2 secondes pour $\mathcal{C}_{\varepsilon^{(1)}}$ (avec $p = 24$) à environ 5 minutes pour $\mathcal{C}_{\varepsilon^{(14)}}$ (mais avec $p = 38$ pour ne se servir que du critère 1, et 22 653 868 $\mathcal{B}_l$ retenus, ce qui est exceptionnel par rapport aux autres $\mathcal{C}_\varepsilon$ pour lesquels le temps de calcul est beaucoup moins long).

Tous les résultats obtenus figurent dans le tableau ci-dessous. Pour chaque $\mathcal{C}_\varepsilon$, N désigne le nombre de $\mathcal{B}_l$ retenus, P le nombre de tels cubes à avoir subi la procédure de dichotomie avec succès, T le nombre de petits cubes issus de cette procédure et ayant été retenus, U le nombre de R de $\{-\frac{1}{2}, \frac{1}{2}\}^8$ utilisés, et S le nombre de $\mathcal{B}_l$ pour lesquels la critère 1 n'a pas suffi et qui ont subi le test du critère 2.

ε	p	N	P	T	U	S
$\varepsilon^{(1)}$	24	24310	93	1425	64	0
$\varepsilon^{(2)}$	30	733309	562	80238	128	0
$\varepsilon^{(3)}$	24	399441	7067	655685	140	70
$\varepsilon^{(4)}$	36	14353759	488	43450	126	13
$\varepsilon^{(5)}$	30	4103990	302	15578	106	0
$\varepsilon^{(6)}$	24	562422	1333	48599	100	0
$\varepsilon^{(7)}$	24	637996	8895	558965	142	0
$\varepsilon^{(8)}$	24	1109300	8633	548482	148	0
$\varepsilon^{(9)}$	30	5384843	974	61515	132	0
$\varepsilon^{(10)}$	24	1437219	14092	765423	146	0
$\varepsilon^{(11)}$	24	2081635	11419	744146	147	0
$\varepsilon^{(12)}$	24	1438477	12700	862541	144	0
$\varepsilon^{(13)}$	24	1855806	12701	1026360	146	0
$\varepsilon^{(14)}$	38	22653868	44	4455	95	0
$\varepsilon^{(15)}$	24	893842	6159	311249	126	0
$\varepsilon^{(16)}$	24	1413671	15318	1100781	162	0
$\varepsilon^{(17)}$	30	6805470	288	9693	100	0
$\varepsilon^{(18)}$	24	1829921	10229	827058	150	0
$\varepsilon^{(19)}$	24	1785354	6175	477394	140	0
$\varepsilon^{(20)}$	24	2242889	12716	966337	146	0

Nous avons essayé au maximum de nous passer du critère 2 pour bien faire apparaître les points critiques, quitte à avoir parfois recours à des

découpages très fins (par exemple pour l'étude de $\mathcal{C}_{\varepsilon^{(14)}}$), alors qu'un découpage plus grossier eût suffi en utilisant les deux critères.
Ainsi, nous n'avons eu besoin d'utiliser le critère 2 que pour $\mathcal{C}_{\varepsilon^{(3)}}$ et $\mathcal{C}_{\varepsilon^{(4)}}$ qui sont les seuls parmi les $\mathcal{C}_\varepsilon$ étudiés à contenir des points critiques (les γ_3 mod $\mathcal{R}_3$, c'est à dire compte tenu de la translation effectuée dans le théorème 4, les $\overline{\phi}(\pm\frac{1}{2},0,\pm\frac{1}{2},0,\pm\frac{1}{2},0,\pm\frac{1}{2},0))$.
- Pour ce qui est de $\mathcal{C}_{\varepsilon^{(3)}}$, avec $p = 24$, les $\mathcal{B}_l$ nécessitant le critère 2 sont ceux qui se trouvent aux voisinages de $\overline{\phi}(\frac{1}{2},0,\frac{1}{2},0,-\frac{1}{2},0,-\frac{1}{2},0)$ et de $\overline{\phi}(-\frac{1}{2},0,\frac{1}{2},0,\frac{1}{2},0,-\frac{1}{2},0)$, qui sont tous deux dans $\mathcal{C}_{\varepsilon^{(3)}}$.
- Pour ce qui est de $\mathcal{C}_{\varepsilon^{(4)}}$, tant que $p < 36$ certains $\mathcal{B}_l$ ne devant pas a priori poser problème nécessitent le recours au critère 2, car ils sont voisins de $\overline{\phi}(\frac{1}{2},0,-\frac{1}{2},0,\frac{1}{2},0,-\frac{1}{2},0)$ qui n'appartient pourtant pas à $\mathcal{C}_{\varepsilon^{(4)}}$. Mais avec $p = 36$, les $\mathcal{B}_l$ nécessitant le critère 2 sont ceux qui se trouvent au voisinage de $\overline{\phi}(\frac{1}{2},0,\frac{1}{2},0,\frac{1}{2},0,-\frac{1}{2},0)$ qui est bien dans $\mathcal{C}_{\varepsilon^{(4)}}$.

5. Retour au cas $n = 2$. Conclusion

Si la méthode utilisée somme toute rudimentaire (choix d'une base pratique, réduction du domaine d'étude, découpage dans le plongement canonique) est généralisable à d'autres extensions totalement réelles de $\mathbb{Q}$, elle peut évidemment servir à démontrer une des conjectures émises par H. Cohn et J. Deutsch (cf [C-D]) à propos de $\mathbb{Q}_2$, à savoir

$$M(\mathbb{Q}_2) = \frac{1}{2}.$$

La démarche est la même, en plus simple du point de vue des calculs, cela va sans dire. On est amené par le même raisonnement que dans le cas $n = 3$ à montrer qu'il suffit d'étudier $\mathcal{C}_\varepsilon$ pour les 4 valeurs suivantes de ε :

$$\begin{cases} \varepsilon^{(1)} = (1,1,1,1) & , \quad \varepsilon^{(2)} = (1,1,1,-1) \\ \varepsilon^{(3)} = (1,1,-1,-1) & et \quad \varepsilon^{(4)} = (1,-1,1,-1) \end{cases}$$

On définit un recouvrement optimisé de chaque $\mathcal{C}_\varepsilon$ par des formules analogues à celles du théorème 7 et (sans mémoriser au fur et à mesure les "entiers" utilisés, et sans avoir recours à la procédure de dichotomie, le temps de calcul étant négligeable) on obtient les résultats suivants :

ε	p	N	S
$\varepsilon^{(1)}$	20	330	0
$\varepsilon^{(2)}$	20	1612	0
$\varepsilon^{(3)}$	18	1058	0
$\varepsilon^{(4)}$	18	967	20

Pour les trois premiers $\mathcal{C}_\varepsilon$, le test du critère 1 suffit. Pour le quatrième qui contient des points critiques, le recours au critère 2 (avec 8 à la place de 128) est nécessaire. Les $\mathcal{B}_l$ nécessitant le critère 2 sont ceux qui se trouvent

aux voisinages de $\overline{\phi}(\frac{1}{2},0,\frac{1}{2},0)$ et de $\overline{\phi}(-\frac{1}{2},0,\frac{1}{2},0)$, qui appartiennent bien à $\mathcal{C}_{\varepsilon(4)}$ et correspondent à $\gamma_2+e_0+e_2$ et γ_2+e_2.
En résumé, on a le résultat suivant (en tenant compte de la translation effectuée dans le théorème 4) :

Théorème principal. *Pour $n=2$ et 3,*

$$M(\mathbb{Q}_n)=M(\overline{\mathbb{Q}_n})=\frac{1}{2}.$$

De façon plus précise, pour tout x de $\mathbb{Q}_n$ de coordonnées (x_i) dans la base (e_i), il existe X dans $\mathcal{R}_n$, de coordonnées (X_i) vérifiant $X_i=\lfloor x_i\rfloor$ ou $\lceil x_i\rceil$, tel que $|N_{\mathbb{Q}_n/\mathbb{Q}}(x-X)|\leq\frac{1}{2}$.

Par ailleurs $\gamma_n=\dfrac{1}{2}\displaystyle\sum_{\substack{i=1\\ i \text{ impair}}}^{2^n-1} e_i$ vérifie $M(\mathbb{Q}_n,\gamma_n)=\frac{1}{2}$.

Qu'en est-il de $\mathbb{Q}_4$? Un test ponctuel et aléatoire (10^9 essais) laisse supposer que la propriété vérifiée par $\mathbb{Q}_n$ pour $n=1,2$ et 3 est encore valable, à savoir qu'avec les notations utilisées jusqu'ici,

$$\forall r\in[-\frac{1}{2},\frac{1}{2}]^{16},\ \exists R\in\{-\frac{1}{2},\frac{1}{2}\}^{16} \text{ tel que } |\overline{N_4}(r-R)|\leq\frac{1}{2},$$

ce qui impliquerait en particulier : $M(\mathbb{Q}_4)=M(\overline{\mathbb{Q}_4})=\frac{1}{2}$.

Remerciements. L'auteur tient à remercier Pr. Georges Gras pour ses conseils, Pr. Harvey Cohn pour son intérêt, et le rapporteur anonyme pour ses remarques et suggestions.

Bibliographie

[S] P. Samuel, *Théorie algébrique des nombres.* Hermann, Paris, 1971.

[B-S] Z.I. Borevitch, I.R. Safarevitch, *Théorie des nombres.* Gauthier-Villars, Paris, 1967.

[W] L.C. Washington, *Introduction to cyclotomic fields.* Graduate Texts in Mathematics, Springer-Verlag, New-York, 1982.

[L] F. Lemmermeyer, *The euclidean algorithm in algebraic number fields.* Expositiones Mathematicae (1995), 385–416.

[C] H. Cohn, *A numerical study of Weber's real class number calculation.* Numerische Mathematik **2** (1960), 347–362.

[C-D] H. Cohn, J. Deutsch, *Use of a computer scan to prove $\mathbb{Q}\left(\sqrt{2+\sqrt{2}}\right)$ and $\mathbb{Q}\left(\sqrt{3+\sqrt{2}}\right)$ are euclidean.* Mathematics of Computation **46** (1986), 295–299.

Jean-Paul Cerri
2, route de Saint-Dié
88600 Aydoilles, FRANCE
E-mail : Jean-Paul.CERRI@wanadoo.fr