Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 70 (1995)

Artikel: Voisinage au sens de Kneser pour les réseaux quaternioniens.
Autor: Bachoc, Christine
DOI: https://doi.org/10.5169/seals-53002

Comment. Math. Helvetici 70 (1995) 350–374 0010–2571/95/030350–25$1.50 + 0.20/0

Voisinage au sens de Kneser pour les réseaux quaternioniens

CHRISTINE BACHOC

1. Introduction

La notion de réseaux voisins fut introduite par M. Kneser ([K1]) pour les réseaux usuels. Deux réseauz L et L' entiers sur $\mathbb{Z}$ sont voisins si $[L : L \cap L'] = [L' : L \cap L'] = 2$. Dans [K1], Kneser montre que deux classes d'isométrie de réseaux unimodulaires peuvent toujours êtres jointes par une chaîne finie de réseaux voisins. Ce résultat lui permet de classifier les réseaux unimodulaires jusqu'à la dimension 16. Cette méthode fut également utilisée par Niemeier pour la classification des réseaux unimodulaires en dimension 24.

Cette notion de voisinage se généralise aux réseaux ayant une structure hermitienne sur un ordre maximal d'un corps de quaternions (appelés réseaux quaternioniens). On démontre un résultat analogue au théorème de Kneser (théorème 3.1), que l'on peut exprimer de la façon suivante: le graphe des voisinages sur les classes d'isométrie de réseaux quaternioniens unimodulaires est connexe.

Le reste de l'article est consacré au corps de quaternions sur $\mathbb{Q}$ ramifié en 2 et à l'infini. À conjugaison près, celui-ci a un unique ordre maximal $\mathfrak{M}$ appelé l'ordre de Hurwitz. Au paragraphe 4, on classifie les réseaux unimodulaires sur $\mathfrak{M}$ jusqu'à la dimension 28, et l'on construit les graphes correspondants. Le paragraphe 5 concerne la dimension 32; on y construit un réseau sur l'ordre de Hurwitz ayant même densité que celui déjà construit par H.-G. Quebbemann ([Q1]), et réalisant donc la meilleure densité connue en dimension 32. Ils ne sont en fait pas isométriques, comme l'a montré l'algorithme de recherche du groupe des isométries d'un réseau conçu et implémenté par W. Plesken and B. Souvignier ([P.S]), que nous remercions ici. Ce résultat renforce la constatation expérimentale selon laquelle la plupart des réseaux intéressants connus dans des dimensions multiples de 4 ont une structure quaternionienne (par exemple les réseaux de Coxeter-Todd, de Barnes-Wall, de Leech,...) ([M2]).

La construction du réseau de dimension 32 utilise un code autodual de longueur 8 sur une algèbre de rang 4 sur $\mathbb{F}_2$ (paragraphe 5).

2. Définitions et terminologie

Soit K un corps de nombres d'anneau des entiers $\mathfrak{O}_K$ et soit H un corps de quaternions défini sur K. Soit V un espace vectoriel sur H de dimension m, muni d'une forme hermitienne non dégénérée, c'est-à-dire d'une forme $h : V \times V \to H$, vérifiant: pour tout λ appartenant à H et tout x, y appartenant à V, $h(y, x) = \overline{h(x, y)}$; $h(\lambda x, y) = \lambda h(x, y)$; si $h(x, y) = 0$ pour tout y appartenant à V, alors $x = 0$.

Soit $\mathfrak{M}$ un ordre maximal de H fixé. Un **réseau quaternionien** L est un $\mathfrak{M}$-module contenu dans V et engendrant V. On définit le **réseau dual** de L par: $L^* = \{x \in V / h(x, L) \subset \mathfrak{M}\}$. On dit alors que L est **entier** si $L \subset L^*$; que L est **unimodulaire** si $L = L^*$.

La **somme orthogonale** (pour la forme hermitienne) de deux réseaux L et L' est notée $L \perp L'$. On dit qu'un réseau est **irréductible** s'il n'est pas somme orthogonale de sous-réseaux.

Une **isométrie hermitienne** entre deux réseaux L et L' est un isomorphisme de $\mathfrak{M}$-modules de L sur L' qui conserve la forme h. Le groupe des isométries hermitiennes qui stabilisent un réseau L est appelé **groupe unitaire de** L et est noté $U(L)$. Si L est un réseau entier et si a est un élément de L tel que $h(a, a) = 2$, la **réflexion hermitienne** $s_a(x) = x - h(x, a)a$ appartient au groupe unitaire de L. On dit que a est une **racine** de L. Le sous-groupe de $U(L)$ engendré par les s_a est un groupe de rêflexions hermitiennes. Ces groupes ont été classifiés dans [C].

Soit v une place de K. On définit le **localisé de L en** v par: $L_v = \mathfrak{O}_{K_v} \otimes_{\mathfrak{O}_K} L$. C'est un réseau hermitien relativement à l'algèbre de quaternions $H_v = K_v \otimes_K H$, pour la forme induite par la forme h.

Soit $x.y = \mathrm{Trace}_{K/\mathbb{Q}}(\mathrm{trd}\,(h(x, y)))$, où trd est la trace réduite dans H. Cette forme bilinéaire symétrique sur le $\mathbb{Q}$-espace vectoriel V est définie positive si et seulement si les conditions suivantes sont réalisées: le corps K est totalement réel; toutes ses places à l'infini sont ramifiés dans H; les localisées de la forme h en les places à l'infini de K sont toutes définies positives. Sous ces conditions, que l'on suppose toujours réalisées, on associe à L un réseau au sens usuel par: $L_{\mathbb{Z}} = (L, x.y)$. Le dual au sens usuel de $L_{\mathbb{Z}}$ et le dual hermitien de L sont liés par la relation:

$$L_{\mathbb{Z}}^* = \mathscr{D}_{H/\mathbb{Q}}^{-1} L^* \tag{2.1}$$

où $\mathscr{D}_{H/\mathbb{Q}}$ est le produit des différentes de H ([V]) et de K.

En particulier, si L est unimodulaire, alors $L_{\mathbb{Z}}^* = \mathscr{D}_{H/\mathbb{Q}}^{-1} L$, et $\det(L_{\mathbb{Z}}) = N(\mathscr{D}_{H/\mathbb{Q}})^m = (d_K \prod_{\mathfrak{p} \in Ram(H)} N_{K/\mathbb{Q}}(\mathfrak{p}))^{2m}$.

Soit $\mathfrak{p}$ un idéal premier de K; nous allons définir la notion de **réseaux $\mathfrak{p}$-voisins.** Si $\mathfrak{p}$ est ramifié dans H, alors il existe un idéal $\mathfrak{P}$ bilatère de $\mathfrak{M}$, maximal parmi les

idéaux contenus dans $\mathfrak{M}$ contenant $\mathfrak{p}$ et d'ordre à gauche $\mathfrak{M}$, et tel que $\mathfrak{p}\mathfrak{M} = \mathfrak{P}^2$. Le quotient $\mathfrak{M}/\mathfrak{P}$ est un corps. On dit que deux réseaux L et L' sont $\mathfrak{p}$-voisins si ce sont des réseaux quaternioniens tels que $L/L \cap L' \simeq L'/L \cap L' \simeq \mathfrak{M}/\mathfrak{P}$. Si $\mathfrak{p}$ n'est pas ramifié dans H, alors il y a plusieurs idéaux maximaux à gauche $\mathfrak{P}_i$ contenus dans $\mathfrak{M}$ et contenant $\mathfrak{p}$, mais les quotients $\mathfrak{M}/\mathfrak{P}_i$ sont des $\mathfrak{M}$-modules simples isomorphes. On dit que deux réseaux L et L' sont $\mathfrak{p}$-voisins si ce sont des réseaux quaternioniens tels que $L/L \cap L' \simeq L'/L \cap L' \simeq \mathfrak{M}/\mathfrak{P}_i$.

3. Connexité du graphe des voisinages

On fixe un espace hermitien (V, h) non dégénéré de dimension m sur un corps de quaternions H sur un corps de nombres totalement réel K, tel que les places à l'infini de K soient ramifiées dans H. Les notations sont celles du paragraphe précédent.

Dans ce paragraphe, nous démontrons un théorème analogue au théorème de Kneser ([K1]). Il est valable pour une catégorie de réseaux un peu plus générale que celle des réseaux unimodulaires, que nous définissons maintenant: avec les notations du paragraphe précédent, soit $\mathfrak{A}$ un idéal bilatère de l'ordre maximal $\mathfrak{M}$. On dit que le réseau L est $\mathfrak{A}$ modulaire si $L^* = \mathfrak{A}L$. Par exemple, un réseau unimodulaire est $\mathfrak{M}$-modulaire; d'après (2.1), un réseau L tel que $L_{\mathbb{Z}}$ soit unimodulaire pour la forme $x.y$ est $\mathscr{D}_{H/\mathbb{Q}}$-modulaire.

THÉORÈME 3.1. *Soient L et L' deux réseaux quaternioniens $\mathfrak{A}$-modulaires de (V, h). On suppose $m \geq 2$. Soit $\mathfrak{p}$ un idéal maximal de K. Alors il existe f appartenant à $U(V, h)$ et il existe une suite de réseaux $\mathfrak{A}$-modulaires $L_1, L_2, \ldots, L_s$* tels que $L_1 = L$, $L_s = f(L')$, *et L_i et L_{i+1} sont* $\mathfrak{p}$-voisins pour tout $i = 1, 2, \ldots, s-1$.

On démontre d'abord deux propositions:

PROPOSITION 3.2. *Soit L et L' deux réseaux quaternioniens $\mathfrak{A}$-modulaires de (V, h). Les propositions suivantes sont équivalentes*:

(1) *Il existe une suite de réseaux $\mathfrak{A}$-modulaires $L_1, L_2, \ldots, L_s$ tels que $L_1 = L$, $L_s = L'$, et L_i et L_{i+1} sont $\mathfrak{p}$-voisins pour tout $i = 1, 2, \ldots, s-1$*

(2) *Pour tout idéal maximal $\mathfrak{p}$ de K différent de $\mathfrak{p}$, $L_{\mathfrak{q}} = L'_{\mathfrak{q}}$.*

Démonstration de la proposition 3.2. L'implication (1) $\Rightarrow$ (2) est évidente. Supposons que $L_{\mathfrak{q}} = L'_{\mathfrak{q}}$ pour tout $\mathfrak{q}$ différent de $\mathfrak{p}$. Alors $[L : L \cap L']_{\mathfrak{O}_K} = [L' : L \cap L']_{\mathfrak{O}_K}$ et est une puissance de $\mathfrak{p}$. Nous allons procéder par récurrence sur la valuation de cette puissance. Il suffit de construire un réseau $\mathfrak{A}$-modulaire R qui soit un $\mathfrak{p}$-voisin de L et tel que $v_{\mathfrak{p}}(|L' : R \cap L']_{\mathfrak{O}_K}) < v_{\mathfrak{p}}(|L : L \cap L']_{\mathfrak{O}_K})$. Définissons R par ses localisés: on pose $R_{\mathfrak{q}} = L_{\mathfrak{q}}$ pour tout $\mathfrak{q}$ différent de $\mathfrak{p}$.

En l'idéal $\mathfrak{p}$, on a: $L_{\mathfrak{p}}^* = \mathfrak{A}_{\mathfrak{p}} L_{\mathfrak{p}}$. Comme $\mathfrak{A}_{\mathfrak{p}}$ est bilatère, quitte à remplacer la forme h par $\alpha_{\mathfrak{p}} h$ pour un certain $\alpha_{\mathfrak{p}}$, on peut supposer que $\mathfrak{A}_{\mathfrak{p}} = \mathfrak{M}_{\mathfrak{p}}$ si $\mathfrak{p}$ est non ramifié dans H, et que $\mathfrak{A}_{\mathfrak{p}} = \mathfrak{M}_{\mathfrak{p}}$ ou $\mathfrak{P}$ si $\mathfrak{p}$ est ramifié dans h (où $\mathfrak{P}$ est l'unique idéal bilatère maximal contenu dans $\mathfrak{M}_{\mathfrak{p}}$ et contenant $\mathfrak{p}\mathfrak{M}_{\mathfrak{p}}$). On a besoin du lemme suivant:

LEMME 3.3. *Si $L_{\mathfrak{p}} \neq L'_{\mathfrak{p}}$, il existe un idéal maximal $\mathfrak{P}$ d'ordre à gauche $\mathfrak{M}_{\mathfrak{p}}$, entier, contenant $\mathfrak{p}\mathfrak{M}_{\mathfrak{p}}$ et tel que $L_{\mathfrak{p}} \cap \bar{\mathfrak{P}} L'_{\mathfrak{p}} \not\subset \bar{\mathfrak{P}} L_{\mathfrak{p}}$.*

Démonstration: supposons $\mathfrak{p}$ non ramifié dans H, et $L_{\mathfrak{p}} \cap \bar{\mathfrak{P}} L'_{\mathfrak{p}} \subset \bar{\mathfrak{P}} L_{\mathfrak{p}}$ pour tout idéal $\mathfrak{P}$ à gauche de $\mathfrak{M}_{\mathfrak{p}}$ et contenant $\mathfrak{p}$. Soit x un élément de $L'_{\mathfrak{p}}$ n'appartenant pas à $L_{\mathfrak{p}}$. Soit $s \geq 1$ le plus petit entier tel que $\mathfrak{p}^s x \subset L_{\mathfrak{p}}$. Un tel s existe car $[L'_{\mathfrak{p}} : L_{\mathfrak{p}} \cap L'_{\mathfrak{p}}]$ est une puissance de $\mathfrak{p}$. Alors, pour tout $\mathfrak{P}$, $\mathfrak{p}^s x \subset L_{\mathfrak{p}} \cap \bar{\mathfrak{P}} L'_{\mathfrak{p}} \subset \bar{\mathfrak{P}} L_{\mathfrak{p}}$. Comme $\mathfrak{P}\bar{\mathfrak{P}} = \mathfrak{p}\mathfrak{M}_{\mathfrak{p}}$, $\mathfrak{P}\mathfrak{p}^s \subset \mathfrak{p} L_{\mathfrak{p}}$. Cette relation est vraie pour au moins deux idéaux maximaux d'ordre à gauche $\mathfrak{M}_{\mathfrak{p}}$ contenant $\mathfrak{p}$ (il y a $N(\mathfrak{p}) + 1$ tels idéaux); or, si $\mathfrak{P}$ et $\mathfrak{P}'$ sont deux tels idéaux alors $\mathfrak{P} + \mathfrak{P}' = \mathfrak{M}_{\mathfrak{p}}$. Donc $\mathfrak{p}^s x \subset \mathfrak{p} L_{\mathfrak{p}}$, soit $\mathfrak{p}^{s-1} x \subset L_{\mathfrak{p}}$, ce qui contredit la définition de s.

Si $\mathfrak{p}$ est ramifié dans H, il y a un seul idéal à gauche de $\mathfrak{M}_{\mathfrak{p}}$ contenant $\mathfrak{p}$ et maximal; il est bilatère et stable par conjugaison. La démonstration est analogue, en utilisant le plus petit entier s tel que $\mathfrak{P}^s x \subset L_{\mathfrak{p}}$. □

Supposons que $\mathfrak{A}_{\mathfrak{p}} = \mathfrak{M}_{\mathfrak{p}}$. Soit, d'après le lemme précédent, $\mathfrak{P}$ et x tels que $x \in L_{\mathfrak{p}} \cap \bar{\mathfrak{P}} L'_{\mathfrak{p}}$ et $x \notin \bar{\mathfrak{P}}_{\mathfrak{p}}$. On pose

$$L_{\mathfrak{p}}^x = \{y \in L_{\mathfrak{p}} / h(x, y) \in \mathfrak{P}\} \quad \text{et} \quad R_{\mathfrak{p}} = L_{\mathfrak{p}}^x + \bar{\mathfrak{P}}^{-1} x.$$

Ainsi défini, R est clairement un $\mathfrak{p}$-voisin de L. Montrons qu'il est $\mathfrak{A}_{\mathfrak{p}}$-modulaire, c'est-à-dire unimodulaire: on voit facilement que $R_{\mathfrak{p}}$ est entier si et seulement si $h(x, x) \in \mathfrak{p}$, ce qui est réalisé grâce à la condition $x \in \bar{\mathfrak{P}} L'_{\mathfrak{p}}$. Montrons que $v_{\mathfrak{p}}([L'_{\mathfrak{p}} : R_{\mathfrak{p}} \cap L'_{\mathfrak{p}}]_{\mathfrak{o}_{K_{\mathfrak{p}}}}) < v_{\mathfrak{p}}([L_{\mathfrak{p}} : L_{\mathfrak{p}} \cap L'_{\mathfrak{p}}]_{\mathfrak{o}_{K_{\mathfrak{p}}}})$: en effet, $R_{\mathfrak{p}} \cap L'_{\mathfrak{p}}$ contient strictement $L_{\mathfrak{p}}^x \cap L'_{\mathfrak{p}}$ car $\bar{\mathfrak{P}}^{-1} x \subset L'_{\mathfrak{p}}$ et $\bar{\mathfrak{P}}^{-1} x \not\subset L_{\mathfrak{p}}$, et $L_{\mathfrak{p}}^x \cap L'_{\mathfrak{p}} = L_{\mathfrak{p}} \cap L'_{\mathfrak{p}}$ car, si y appartient à $L_{\mathfrak{p}} \cap L'_{\mathfrak{p}}$, alors $h(y, x)$ appartient à $\mathfrak{P}$ ($x \in \bar{\mathfrak{P}} L'_{\mathfrak{p}}$ et $L'_{\mathfrak{p}}$ est entier).

Finalement, supposons que $\mathfrak{p}$ soit ramifié dans H et que $\mathfrak{A}_{\mathfrak{p}} = \mathfrak{P}$. Soit, d'aprés le lemme précédent, x tel que $x \in L_{\mathfrak{p}} \cap \mathfrak{P} L'_{\mathfrak{p}}$ et $x \notin \mathfrak{P} L_{\mathfrak{p}}$. Alors $h(x, L_{\mathfrak{p}}) = \mathfrak{P}^{-1}$ et $h(x, x) \in \mathfrak{p}$ car $x \in \mathfrak{P} L'_{\mathfrak{p}}$. On pose

$$L_{\mathfrak{p}}^x = \{y \in L_{\mathfrak{p}} / h(x, y) \in \mathfrak{M}\} \quad \text{et} \quad R_{\mathfrak{p}} = L_{\mathfrak{p}}^x + \mathfrak{P}^{-1} x.$$

De façon analogue au cas précédent, on montre que $R_{\mathfrak{p}}$ est un $\mathfrak{p}$-voisin de $L_{\mathfrak{p}}$, qui est $\mathfrak{P}$-modulaire car $h(x, x) \in \mathfrak{p}$, et qui vérifie: $v_{\mathfrak{p}}([L'_{\mathfrak{p}} : R_{\mathfrak{p}}]_{\mathfrak{o}_{K_{\mathfrak{p}}}}) < v_{\mathfrak{p}}([L_{\mathfrak{p}} : L_{\mathfrak{p}} \cap L'_{\mathfrak{p}}]_{\mathfrak{o}_{K_{\mathfrak{p}}}})$. □

PROPOSITION 3.4. *Soit L et L' deux réseaux quaternioniens de (V, h). On suppose que $m \geq 2$ et que, pour tout idéal maximal $\mathfrak{q} = \mathfrak{p}$ de K, il existe $f_\mathfrak{q}$ appartenant à $U(V_\mathfrak{q}, h)$ tels que $f_\mathfrak{q}(L_\mathfrak{q}) = L'_\mathfrak{q}$. Alors, il existe f appartenant à $U(V, h)$ tel que*

$$\forall \mathfrak{q} \neq \mathfrak{p} \quad f(L)_\mathfrak{q} = L'_\mathfrak{q}.$$

Démonstration. C'est une conséquence du théorème d'approximation forte pour le groupe $U(V, h)$. Rappelons de quoi il s'agit: soit G un groupe algébrique linéaire défini sur un corps de nombres K, et soit S un ensemble fini de places de K. On note G_K le groupe des points de G rationnels sur K, $G_S = \Pi_{v \in S} G_{K_v}$, et G_A le groupe des adèles de K. On dit que (G, S) vérifie le théorème d'approximation forte si le produit $G_K G_S$ est dense dans G_A. Le groupe $U(V, h)$ est une K-forme du groupe symplectique Sp_{2m} ([K2, §2.6]). A ce titre, il vérifie le théorème d'approximation forte pour tout ensemble de places S tel que G_S soit non compact ([K3]).

On prend ici $S = \{\mathfrak{p}\}$; alors $G_S = U(V_\mathfrak{p}, h)$. Montrons que ce groupe est non compact si m est supérieur ou égal à 2. Considérons la forme bilinéaire symétrique sur le $K_\mathfrak{p}$-espace vectoriel $V_\mathfrak{p}$ donnée par $b(x, y) = \mathrm{trd}\,(h(x, y))$, où trd est la trace réduite de la $K_\mathfrak{p}$-algèbre $H_\mathfrak{p}$. Comme $\dim_{K_\mathfrak{p}}(V_\mathfrak{p}) = 4m \geq 5$, la forme quadratique associée représente 0. Comme $b(x, x) = 2h(x, x)$, il existe $x \in V_\mathfrak{p}$ tel que $h(x, x) = 0$. Si $H_\mathfrak{p}$ est un corps, alors on montre facilement que $V_\mathfrak{p}$ contient un plan hyperbolique, c'est-à-dire un plan pour lequel la matrice de la forme hermitienne est $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Le groupe unitaire de $V_\mathfrak{p}$ contient donc le sous-groupe des matrices de la forme $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix}$, $\lambda \in K_\mathfrak{p}^*$ qui est non compact. Si $H_\mathfrak{p}$ est isomorphe à l'algèbre de matrices $\mathcal{M}_2(K_\mathfrak{p})$, c'est encore plus simple: le groupe unitaire de $V_\mathfrak{p}$ contient un sous-groupe isomorphe à $\{\lambda \in H_\mathfrak{p} / \lambda\bar{\lambda} = 1\}$ (en effet, on voit facilement que la forme hermitienne h est équivalente à $\Sigma_{i=1}^m a_i x_i \bar{y}_i$, où $a_i \in K_\mathfrak{p}$) qui est non compact dans le cas d'une algèbre de matrices (la condition $m \geq 2$ n'est donc pas nécessaire si $\mathfrak{p}$ est non ramifié dans H).

L'élément $(f_\mathfrak{p})_\mathfrak{p}$ appartient à G_A (complété par 1 en $\mathfrak{p}$ et aux places à l'infini de K) et peut donc être approché par un élément de $G_K G_S$. En prenant comme ouvert $\Pi_\mathfrak{q} U(L_q)$, il existe $f \in U(V, h)$ et $\sigma_\mathfrak{q} \in U(L_\mathfrak{q})$ tels que pour tout $\mathfrak{q} \neq \mathfrak{p}$, $f_\mathfrak{q}\sigma_\mathfrak{q} = f$. Alors $L'_\mathfrak{q} = f_\mathfrak{q}(L_\mathfrak{q}) = f(L)_\mathfrak{q}$. □

Fin de la démonstration du théorème 3.1. D'après les propositions 3.2 et 3.4, il suffit que les réseaux L et L' soient localement isométriques. Soit $\mathfrak{q}$ un idéal maximal fixé de K; si $\mathfrak{q}$ est ramifié dans H, alors $H_\mathfrak{q}$ est un corps et $L_\mathfrak{q}$ et $L'_\mathfrak{q}$ sont isométriques d'après le théorème 6.2 de [J]. Si $\mathfrak{q}$ n'est pas ramifié dans H, le résultat est également bien connu. Faute d'une référence précise, nous donnons une démonstration:

l'algèbre H_q est isomorphe à $\mathcal{M}_2(K_q)$. A conjugaison près, on peut supposer que $\mathfrak{M}_q = \mathcal{M}_2(\mathfrak{O}_{K_q})$ ([V]). Comme q n'est pas ramifié, quitte à changer h en $\alpha_q h$, on peut supposer que L_q et L'_q sont unimodulaires.

On note $\mathfrak{s}L_q$ l'idéal bilatère de H_q engendré par les $h(x, y)$ lorsque x, y appartiennent à L_q et $\mathfrak{n}L_q$ l'idéal bilatère de H_q engendré par les $h(x, x)$ losque x appartient à L_q. Grâce à la relation $h(x+y, x+y) = h(x, x) + h(y, y) + \mathrm{trd}\,(h(x, y))$, on a les inclusions: $\mathrm{trd}\,(\mathfrak{s}L_q) \subset \mathfrak{n}L_q \subset \mathfrak{s}l_q$. Comme L_q est unimodulaire, $\mathfrak{s}L_q = \mathfrak{M}_q$, et comme $\mathrm{trd}\,(\mathfrak{M}_q) = \mathfrak{O}_{K_q}$, $\mathfrak{n}L_q = \mathfrak{M}_q$. Par conséquent, il existe e_1 appartenant à L_q tel que $h(e_1, e_1) \in \mathfrak{O}_{K_q}^*$. Comme $\mathrm{nrd}\,(\mathfrak{M}_q) = \det(\mathcal{M}_2(\mathfrak{O}_{K_q})) = \mathfrak{O}_{K_q}$, on peut supposer que $h(e_1, e_1) = 1$. Alors, $L_q = \mathfrak{M}_q e_1 \perp L''_q$, et par récurrence on montre que $L_q = \mathfrak{M}_q e_1 \perp \cdots \perp \mathfrak{M}_q e_m$ avec $h(e_i, e_j) = \delta_{i,j}$. Il y a donc une seule classe d'isométrie hermitienne de réseau unimodulaire sur $\mathfrak{M}_q$. □

4. Classification des réseaux unimodulaires jusqu'à la dimension 28 sur l'ordre de Hurwitz

4.1. *L'ordre de Hurwitz*

On suppose désormais que $H = \mathbb{Q} + \mathbb{Q}i + \mathbb{Q}j + \mathbb{Q}k$, avec $i^2 = j^2 = -1$, $ij = -ji = k$. A conjugaison près, H a un unique ordre maximal qui est $\mathfrak{M} = \mathbb{Z}[1, i, j, (1+i+j+k)/2]$. L'unique nombre premier ramifié dans H est 2; on a $2\mathfrak{M} = \mathfrak{P}^2$, où $\mathfrak{P} = (1+i)\mathfrak{M} = \mathfrak{M}(1+i)$; le quotient $\mathfrak{M}/\mathfrak{P}$ est isomorphe au corps fini à quatre éléments $\mathbb{F}_4$.

Le groupe des unités de $\mathcal{M}$ est le groupe à 24 éléments $\mathfrak{M}^* = \{\pm 1, \pm i, \pm j, \pm k, (\pm 1 \pm i \pm j \pm k)/2\}$. On note $w = (-1+i+j+k)/2$; c'est un élément d'ordre 3 de $\mathfrak{M}^*$, dont la classe résiduelle engendre $(\mathfrak{M}/\mathfrak{P})^*$.

4.2. *Réseaux unimodulaires*

Tout espace hermitien (V, h) sur H tel que la forme associée $x \cdot y$ soit définie positive est isomorphe à $(H^m, \Sigma_{i=1}^m x_i \bar{y}_i)$. Sauf mention explicite du contraire, on se place dans cet espace. Toutefois, on considèrera parfois la forme $\frac{1}{2}\Sigma_{i=1}^m x_i \bar{y}_i$. Soit L un réseau unimodulaire sur l'ordre de Hurwitz de dimension m. Le réseau $L_{\mathbb{Z}}$ est un réseau entier, pair, de dimension $n = 4m$, de déterminant 2^{2m} d'après le paragraphe 2. On appelle **minimum hermitien** et on note $\min(L)$ le nombre $\min(L) = \min\{h(x, x)/x \in L - \{0\}\}$; on appelle **minimum** et on note $\min(L_{\mathbb{Z}})$ le nombre $\min(L_{\mathbb{Z}}) = \min\{x \cdot x/x \in L - \{0\}\}$; on a donc $\min(L_{\mathbb{Z}}) = 2\min(L)$. On note $S(L)$ l'ensemble des vecteurs minimaux de L, c'est-à-dire l'ensemble des éléments de L qui réalisent $\min(L)$.

Comme H est de nombre de classes 1, le seul réseau unimodulaire en dimension 1 est $L = (\mathfrak{M}, x\bar{y})$. Il est bien connu que $L_{\mathbb{Z}}$ est isométrique au réseau de racines $\mathbb{D}_4$ ([M2]). Remarquons qu'un réseau de minimum hermitien 1 est réductible car il contient des facteurs orthogonaux isométriques à $\mathfrak{M}$.

La construction suivante est due à J. Martinet; afin de travailler avec des coordonnées entières, on prend sur les réseaux suivants la forme $\frac{1}{2}\Sigma_{i=1}^{m} x_i\bar{y}_i$:

$$J_{4m} = \left\{(x_1, x_2, \ldots, x_m) \in \mathfrak{P}^m \Big/ \sum_{i=1}^{m} x_i \in 2\mathfrak{M}\right\}$$

$$J'_{4m} = \left\{(x_1, x_2, \ldots, x_m) \in \mathfrak{M}^m / x_i \equiv x_j \bmod \mathfrak{P} \text{ et } \sum_{i=1}^{m} x_i \in 2\mathfrak{M}\right\}$$

PROPOSITION 4.1. [M1]

On suppose que m est pair.

(1) *Si m est supérieur ou égal à quatre, le réseau J'_{4m} est unimodulaire, irréductible, de minimum hermitien 2.*

(2) *Si m est supérieur ou égal à 6, alors $S(J'_{4m}) = S(J_{4m})$ et a pour cardinal $24m(4m-3)$. Le groupe unitaire $U(J'_{4m})$ est de cardinal $3.2^{3m-2} \cdot m!$; il est engendré par les permutations des coordonnées et par les transformations $(x_1, x_2, \ldots, x_m) \to (x_1u_1, x_2u_2, \ldots, x_mu_m)$, où les u_i sont des unités de $\mathfrak{M}$ vérifiant: $u_i \equiv u_j \bmod \mathfrak{P}$, et $\Sigma u_i \in 2\mathfrak{M}$.*

(3) *Si $m = 4$, J'_{4m} est isométrique sur $\mathbb{Z}$ au réseau de Barnes-Wall BW_{16}. L'ensemble de ses vecteurs minimaux est $S(J'_{16}) = S(J_{16}) \cup \{(u_1, u_2, u_3, u_4)/ u_i \in \mathfrak{M}^*, u_i \equiv u_j \bmod \mathfrak{P}, \Sigma u_i \in 2\mathfrak{M}\}$. Son groupe unitaire est transitif sur l'ensemble de ses vecteurs minimaux.*

4.3. *Généralités sur les voisinages*

On regroupe dans ce paragraphe quelques résultats techniques faciles à établir sur la recherche des voisins d'un réseau qui seront utilisés au cours des démonstrations. Soit L un réseau unimodulaire sur l'ordre de Hurwitz; on cherche à décrire ses 2-voisins (ou plus simplement ses voisins).

Les sous-réseaux quaternioniens d'indice $\mathfrak{P}$ de L sont tous de la forme

$$L^x = \{y \in L / h(y, x) \in \mathfrak{P}\}$$

où x est un élément de L n'appartenant pas à $\mathfrak{P}L$. L'ensemble L^x ne dépend que de la classe de x dans le quotient $L/\mathfrak{P}L$; la classe d'isométrie de L^x ne dépend que de l'orbite de la classe de x sous l'action de $U(L)$ (car $\sigma(L^x) = L^{\sigma(x)}$).

Le dual du réseau L^x est

$$(L^x)^* = L + \mathfrak{P}^{-1}x.$$

Le réseau L^x est contenu dans un voisin de L si et seulement si $h(x, x)$ appartient à $2\mathfrak{M}$ (et donc à $2\mathbb{Z}$). Dans ce cas, il est contenu dans exactement cinq réseaux unimodulaires correspondant aux cinq droites de $(L^x)^*/L^x$ qui est un plan sur $\mathbb{F}_4$.

En particulier, si $h(x, x)$ est pair, on pose

$$L_x = L^x + \mathfrak{P}^{-1}x.$$

C'est l'un des quatre voisins de L contenant L^x.

Nous allons maintenant étudier les voisins irréductibles du réseau $L = (\mathfrak{M}^m, \Sigma_{i=1}^m x_i\bar{y}_i)$. Soit $x = (x_1, \ldots, x_m)$ un élément de $\mathfrak{M}^m$. Si l'un des x_i appartient à $\mathfrak{P}$, alors L^x contient un sous-réseau isométrique à $\mathfrak{M}$, et les voisins de L contenant L^x sont tous réductibles. Dans le cas contraire, les x_i sont tous congrus à une unité modulo $\mathfrak{P}$; or $U(L)$ contient tous les $(x_1, \ldots, x_m) \to (x_1u_1, \ldots, x_mu_m)$ où u_i appartient à $\mathfrak{M}^*$; on peut donc choisir $x = (1, 1, \ldots, 1)$. On a vu que L^x n'est contenu dans un réseau unimodulaire autre que L que si $h(x, x)$ est pair. Or $h(x, x) = m$. De plus, on voit facilement que $U(L)$ permute les quatre voisins de L contenant $L^{(1,1,\ldots,1)}$ (voir remarque 4.3). Ils sont donc tous isométriques à $L_{(1,1,\ldots,1)}$ dans lequel on reconnait J'_{4m}. Nous avons démontré la proposition:

PROPOSITION 4.2. *Si m est impair, le réseau $(\mathfrak{M}^m, \Sigma_{i=1}^m x_i\bar{y}_i)$ n'a aucun voisin irréductible. Si m est pair, les voisins irréductibles de $(\mathfrak{M}^m, \Sigma_{i=1}^m x_i\bar{y}_i)$* sont tous isométriques à J'_{4m}.

Remarque 4.3. Jusqu'à la dimension 28, un réseau L unimodulaire est toujours son propre voisin. En effet, quitte à se placer en dimension inférieure, on peut supposer qu'il est irréductible. Alors on verra au paragraphe suivant qu'il est de minimum hermitien 2. Si x appartenant à L est tel que $h(x, x) = 2$, alors L est voisin de $\Lambda = L_x$ qui est de minimum hermitien 1, donc de la forme $\mathfrak{M} \perp \Lambda'$. Le groupe unitaire de Λ contient un sous-groupe isomorphe à $\mathfrak{M}^*$ (agissant par multiplication à droite sur la composante $\mathfrak{M}$). On peut écrire $\Lambda \cap L = \Lambda^y$ avec $y = (u, y') \in \Lambda$. Alors le sous-groupe de $\mathfrak{M}^*$ $U = \{\varepsilon \in \mathfrak{M}^*/\varepsilon \equiv 1 \bmod \mathfrak{P}\} = \{\pm 1, \pm i, \pm j, \pm k\}$ stabilise Λ^y et donc opère sur le $\mathbb{F}_4$-espace vectoriel de dimension 2 $(\Lambda^y)^*/\Lambda^y$. L'élément -1 agit trivialement; les autres induisent l'identité sur la droite Λ/Λ^y mais pas sur tout le plan (regarder d'image de $(1 + i)^{-1}y$); comme ils sont d'ordre 2, ils n'ont pas d'autre droite stable que Λ/Λ^y. Ainsi, le groupe bicyclique $U/\{\pm 1\}$ opère sans point fixe sur les quatre réseaux unimodulaires contenant Λ^y et distincts

de Λ. Il opère donc transitivement, et ces quatre réseaux sont isométriques et voisins les uns des autres.

Le graphe des voisinages présente donc une boucle en chacun de ses sommets jusqu'à la dimension 28, que nous avons omis de représenter dans les figures 1, 2, 3, 4.

4.4. *Formes modulaires*

D'après (2.1), le réseau $L_{\mathbb{Z}}$ vérifie $L_{\mathbb{Z}}^* = (1+i)^{-1}L_{\mathbb{Z}}$; l'application $x \to (1+i)x$ est une similitude de rapport $\sqrt{2}$ de $L_{\mathbb{Z}}^*$ sur $L_{\mathbb{Z}}$. Ce réseau est donc, dans le vocabulaire de [Q2], un réseau modulaire de niveau 2. H.-G. Quebbemann démontre ([Q2, §1.2]) que la série theta d'un tel réseau est modulaire de poids $\dim(L_{\mathbb{Z}})/2 = 2m$ pour le groupe de Fricke $\Gamma_*(2)$, et pour un certain caractère χ. L'étude de l'espace des formes modulaires correspondant montre que

$$\min(L_{\mathbb{Z}}) \leq 2 + 2[m/4] \tag{1}$$

et que, de plus, lorsque l'égalité est réalisée, la série theta est déterminée et facilement calculable. Avec les notations de [Q2], soit θ_4 la série theta du réseau de racines $\mathbb{D}_4$, et soit $\Delta_{16} = (\eta(z)\eta(2z))^8$; un réseau L unimodulaire sur l'ordre de Hurwitz de dimension 24 ($m = 6$) et de minimum 4 a pour série theta $\theta_L = \theta_4^6 - 144\theta_4^2\Delta_{16} = 1 + 3024q^2 + \cdots$; si la dimension est 28, $\theta_L = \theta_4^7 - 168\theta_4^2\Delta_{16} = 1 + 1512q^2 + \cdots$.

On déduit immédiatement de (1) que, pour les dimensions $m = 2, 3$, il y a une seule classe de réseau unimodulaire, à savoir $(\mathfrak{M}^m, \Sigma_{i=1}^m x_i\bar{y}_i)$; en effet, un tel réseau a pour minimum hermitien 1. Un argument de H.-G. Quebbemann, que nous restituons ici, montre qu'il y a en dimension 4 une seule classe de réseau unimodulaire irréductible. Soit L un tel réseau; d'après ce qui précède, $\min(L) = 2$. Soit x l'un de ses vecteurs minimaux. Le réseau $L_x = L^x + \mathfrak{P}^{-1}x$ est unimodulaire sur l'ordre de Hurwitz et de minimum hermitien 1; il est donc isométrique à $(\mathfrak{M}^4, \Sigma_{i=1}^4 x_i\bar{y}_i)$. Mais on a vu que celui-ci a (à isométrie près) un seul voisin irréductible qui est J'_{16}.

4.5. *Une formule de masse*

Hashimoto a démontré une formule de masse pour les réseaux unimodulaires quaternioniens analogue à la formule de Siegel. Dans le cas particulier que nous considérons, soit E_m l'ensemble des classes d'isométrie hermitienne de réseaux unimodulaires de rang m sur l'ordre de Hurwitz; on a:

$$\sum_{[L] \in E_m} \frac{1}{\# U(L)} = \prod_{k=1}^{m} (2^k + (-1)^k) \frac{B_{2k}}{4k} \tag{2}$$

où les B_{2k} sont les nombres de Bernoulli ([H, §3 (25)]).

4.6. *La dimension* 16

THÉORÈME 4.

(1) *Le réseau J'_{16} est, à isométrie hermitienne près, le seul réseau irréductible et unimodulaire sur l'ordre de Hurwitz en dimension* 16.

(2) *Son groupe unitaire est de cardinal $2^{13} \cdot 3^4 \cdot 5$, et est engendré par les réflexions relatives à ses vecteurs minimaux.*

(3) *Les classes du quotient $J'_{16}/\mathfrak{P}J'_{16}$ sont représentées par des éléments de norme hermitienne* 0, 2, 3.

(4) *Le groupe $U(J'_{16})$ est transitif sur l'ensemble des classes d'éléments de norme* 2 *de $J'_{16}/\mathfrak{P}J'_{16}$ (respectivement sur l'ensemble des classes d'éléments de norme* 3).

Démonstration: le (1) est démontré au paragraphe précédent. La formule de masses donne le cardinal de $U(J'_{16})$; en effet, le groupe unitaire de $\mathfrak{M}^m$ est engendré par les permutations des m coordonnées et par les applications de la forme $(x_1, \ldots, x_m) \to (x_1 u_1, \ldots, x_2 u_2)$ avec $u_i \in \mathfrak{M}^*$, et est donc de cardinal $24^m m!$. Par ailleurs, on trouve dans [C] un système de racines isométrique à l'ensemble des vecteurs minimaux du réseau J'_{16}; c'est le système noté S_3. Le groupe engendré par ses réflexions est de cardinal $2^{13} \cdot 3^4 \cdot 5$ ([C, Table 3]); c'est un sous-groupe du groupe unitaire de J'_{16}; il lui est donc égal.

On sait que les classes modulo 2 des vecteurs du réseau de Barnes-Wall ont pour représentants les vecteurs de norme au plus 12 ([C.S1, chap. 6, §5]). Montrons que l'on peut en déduire que les classes modulo $\mathfrak{P}$ de J'_{16} ont pour représentants les vecteurs de norme hermitienne 0, 2, 3: en effet, soit x un élément de J'_{16}. Alors il existe z appartenant à $2J'_{16}$ tel que $((1+i)x - z) \cdot ((1+i)x - z) \leq 12$, ou encore $h(x - (1+i)^{-1}z, x - (1+i)^{-1}z) \leq 3$. D'où le résultat, puisque $(1+i)^{-1}z \in \mathfrak{P}J'_{16}$.

On a déjà vu que le groupe unitaire de J'_{16} est transitif sur l'ensemble de ses vecteurs minimaux. Montrons qu'il est transitif sur les classes de vecteurs de norme hermitienne 3. Les vecteurs de norme 3 sont de deux types à permutation des coordonnées près: soit du type (x, u_1, u_2, u_3) avec $x\bar{x} = 3$ et $u_i \in \mathfrak{M}^*$, soit du type $(x_1, x_2, x_3, 0)$ avec $x_i \in \mathfrak{P}$. On voit facilement que les transformations décrites au (2) de la proposition 4.1 permutent transitivement chacun des types modulo $\mathfrak{P}J'_{16}$. Pour passer d'un type à l'autre, on utilise la transformation suivante qui stabilise le réseau J'_{16}:

$$\frac{1}{2}\begin{bmatrix} 1-i & 1-i & 0 & 0 \\ 1-i & -1+i & 0 & 0 \\ 0 & 0 & 1-i & 1-i \\ 0 & 0 & 1-i & -1+i \end{bmatrix}$$

□

$$\mathfrak{M}^4 \text{ ——————— } J'_{16}$$

Figure 1. Graphe des voisins en dimension 16.

4.7. *La dimension* 20

Le cas de la dimension 20 est analogue à celui de la dimension 16; on trouve également une seule classe de réseau irréductible unimodulaire, dont on verra la construction explicite au cours de la démonstration du théorème suivant:

THÉORÈME 4.5.

(1) *Il y a, à isométrie hermitienne près, un seul réseau irréductible et unimodulaire sur l'ordre de Hurwitz en dimension* 20, *que l'on note* R_{20}.

(2) *Son groupe unitaire est isomorphe au groupe* $SU_5(2) \times \{\pm 1\}$, *et est de cardinal* $2^{11} \cdot 3^5 \cdot 5 \cdot 11$. *Il est engendré par les réflexions relatives à ses vecteurs minimaux.*

(3) *Les classes du quotient* $R_{20}/\mathfrak{P}R_{20}$ *sont représentées par des éléments de norme hermitienne* 0, 2, 3.

(4) *Le groupe* $U(R_{20})$ *est transitif sur l'ensemble des classes d'éléments de norme* 2 (*respectivement de norme* 3) *de* $R_{20}/\mathfrak{P}R_{20}$.

Démonstration: la formule de masse (2) montre l'existence d'au moins un réseau unimodulaire et irréductible; en effet, les réseaux réductibles de la dimension 20 sont, d'après le théorème 4.4, $\mathfrak{M}^5$ et $\mathfrak{M} \perp J'_{16}$. Leur groupe unitaire a pour ordre respectivement $24^5 \cdot 5!$ et $24 \cdot 2^{13} \cdot 3^4 \cdot 5$; il reste dans la formule de masse le terme $1/(2^{11} \cdot 3^5 \cdot 5 \cdot 11)$. Soit R un tel réseau; d'après (1), son minimum hermitien est 2, il est donc voisin d'un réseau réductible. Comme 5 est impair, le réseau $\mathfrak{M}^5$ n'a pas de voisin irréductible. Le réseau $L = \mathfrak{M} \perp J'_{16}$ a, à isométrie près, un seul sous-réseau d'indice $\mathfrak{P}$ et de minimum hermitien 2 grâce au (4) du théorème 4.4, qui est L^x avec $x = 1 + x_0$, x_0 étant un élément de J'_{16} de norme hermitienne 3.

Les quatre réseaux unimodulaires qui contiennent L^x sont permutés transitivement par le sous-groupe de $U(L)$ isomorphe à $\mathfrak{M}^*$ (agissant sur le facteur $\mathfrak{M}$ de L), et sont donc isométriques. Cela démontre l'unicité à isométrie près du réseau R_{20} que l'on peut prendre égal à $L_x = L^x + \mathfrak{P}^{-1}x$, pour un choix quelconque de x_0.

On trouve dans [C] un système de racines irréductible en dimension 20 défini sur l'ordre de Hurwitz et noté U (Table 2). On peut vérifier qu'il engendre en réseau unimodulaire de minimum hermitien 2, qui est donc isométrique à R_{20}. D'après la Table 3, le groupe engendré par les réflexions relatives à ses racines, est d'ordre $2^{11} \cdot 3^5 \cdot 5 \cdot 11$ et est isomorphe à $PSU_5(2) \times \{\pm 1\}$; de plus, il est transitif sur celles-ci. D'après la formule de masse, il est égal au groupe $U(R_{20})$.

On vient de voir que le groupe unitaire du réseau R_{20} est transitif sur l'ensemble de ses vecteurs minimaux. Considérons le quotient $R_{20}/\mathfrak{P}R_{20}$; muni de la forme induite de celle du réseau R_{20}, c'est un espace hermitien non dégénéré sur $\mathbb{F}_4$ pour le Frobenius de $\mathbb{F}_4$. D'après le théorème de Witt, son groupe unitaire $U_5(2)$ est transitif sur l'ensemble de ses vecteurs isotropes non nuls, ainsi que sur l'ensemble de ses vecteurs non isotropes. En utilisant des produits pairs de réflexions, on peut vérifier que $SU_5(2)$ est transitif sur les vecteurs non isotropes. Comme l'image de $U(R_{20})$ dans le groupe unitaire de cet espace est $SU_5(2)$, les vecteurs non isotropes du quotient sont représentés par des vecteurs de norme hermitienne 3. Le groupe $SU_5(2)$ est au moins transitif sur les droites isotropes. Comme les classes non nulles de $\mathfrak{M}/\mathfrak{P}$ sont représentées par des unités de $\mathfrak{M}$, on en déduit que les vecteurs isotropes non nuls de $R_{20}/\mathfrak{P}R_{20}$ sont représentés par les vecteurs minimaux du réseau R_{20}. □

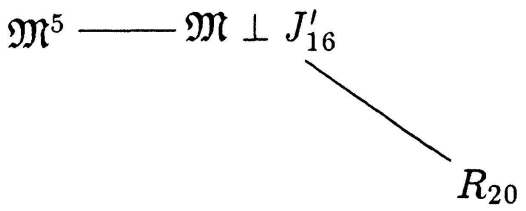

Figure 2. Graphe des voisins en dimension 20.

(D'après la proposition 4.2, les réseaux $\mathfrak{M}^5$ et R_{20} ne sont pas voisins.)

4.8. *La dimension* 24

En dimension 24, on trouve deux classes de réseaux unimodulaires irréductibles. Il y a le réseau J'_{24} (voir proposition 4.1), et un réseau construit à partir du réseau de Coxeter-Todd de la façon suivante: le réseau K_{12} de Coxeter-Todd a une structure de réseau hermitien sur l'anneau des entiers d'Eisenstein (qui est l'anneau des entiers du corps quadratique de discriminant 9) ([F]). De plus, il est unimodulaire sur cet anneau. Si $w = (-1+i+j+k)/2$, on peut identifier $\mathbb{Z}[w]$ aux entiers d'Eisenstein, ce qui nous permet de définir le réseau

$$R_{24} = \mathfrak{M} \otimes_{\mathbb{Z}[w]} K_{12}.$$

Comme K_{12} est unimodulaire sur $\mathbb{Z}[w]$, R_{24} est unimodulaire sur $\mathfrak{M}$. Montrons que son minimum est encore 4: soit $\mathfrak{O}$ l'ordre $\mathbb{Z}[w] + (i-j)\mathbb{Z}[w]$. Les inclusions $\mathfrak{M}(1-w) \subset \mathfrak{O} \subset \mathfrak{M}$ permettent d'écrire la décomposition orthogonale sur $\mathbb{Z}$: $R_{24} \subset ((1-\bar{w})/3)K_{12} \perp_{\mathbb{Z}} (i-j)((1-\bar{w})/3)K_{12}$. La norme d'un élément non nul x de R_{24} est donc de la forme $x \cdot x = \frac{1}{3}(x_1 \cdot x_1 + 2x_2 \cdot x_2)$, où x_1 et x_2 sont dans K_{12} et donc sont soit nuls soit de norme au moins égale à 4; Les facteurs de la décomposition ayant pour intersection avec R_{24} respectivement K_{12} et $(i-j)K_{12}$, la norme de x est au moins égale à 4.

L'ensemble des vecteurs minimaux de R_{24} contient les éléments de la forme ux où u est une unité de $\mathfrak{M}$ et x un vecteur minimal de K_{12}, ce qui fait $4.756 = 3024$ éléments distincts ($\{\pm 1, \pm w, \pm w^2\} \subset \mathbb{Z}[w]$). Or la théorie des formes modulaires (§4.4) prévoit qu'un réseau unimodulaire sur l'ordre de Hurwitz en dimension 24 a exactement 3024 vecteurs minimaux; ils sont donc tous de cette forme.

De plus, on peut remarquer que ces deux réseaux ne peuvent pas être isométriques; en effet, le réseau R_{24} est engendré par ses vecteurs minimaux, alors que ceux de J'_{24} engendrent J_{24} (proposition 4.1).

THÉORÈME 4.6.

(1) *Les réseaux J'_{24} et R_{24} sont, à isométrie hermitienne près, les seuls réseaux irréductibles et unimodulaires sur l'ordre de Hurwitz en dimension* 24.

(2) *Le groupe unitaire du réseau R_{24} est égal au groupe unitaire du réseau de Coxeter-Todd (comme réseau hermitien sur les entiers d'Eisenstein) qui est engendré par les réflexions relatives à ses vecteurs minimaux; il est de cardinal* $2^9 \cdot 3^7 \cdot 5 \cdot 7$.

(3) *Les classes du quotient $R_{24}/\mathfrak{P}R_{24}$ sont représentées par des éléments de norme hermitienne* 0, 2, 3, 4.

(4) *Le groupe $U(R_{24})$ est transitif sur l'ensemble des classes d'éléments de norme* 2 (*respectivement de norme* 3; *respectivement de norme* 4) *de $R_{24}/\mathfrak{P}R_{24}$.*

Démonstration: pour terminer la démonstration du point (1), il suffit de montrer qu'il y a au plus deux classes de réseaux irréductibles. Par un raisonnement analogue à celui du théorème précédent, il suffit de compter les voisins irréductibles des réseaux réductibles de la dimension 24, qui sont: $\mathfrak{M}^6$, $\mathfrak{M}^2 \perp J'_{16}$ et $\mathfrak{M} \perp R_{20}$. Le réseau $\mathfrak{M}^6$ a pour seul voisin irréductible J'_{24} (proposition 4.1(1)). Grâce aux assertions (3) et (4) du théorème 4.4, on voit que le réseau $\mathfrak{M}^2 \perp J'_{16}$ a, à isométrie près, un seul voisin irréductible, qui correspond à un élément de la forme $(1, 1) + x$, où x est un vecteur minimal de J'_{16}. De même, grâce au théorème 4.5, le réseau $\mathfrak{M} \perp R_{20}$ a, à isométrie près, un seul voisin irréductible, correspondant à un élément de la forme $1 + x$, où x est un vecteur de norme hermitienne 3 de R_{20}.

Montrons que le voisin V de $\mathfrak{M}^2 \perp J'_{16}$ précédemment décrit est isométrique à J'_{24}: notons $y = (1, 1) \in \mathfrak{M}^2$; alors $V = (\mathfrak{M}^2 \perp J'_{16})_{y+x}$, et on voit facilement que V est aussi voisin de $(\mathfrak{M}^2)_y \perp (J'_{16})_x = \mathfrak{M}^6$. La seule possibilité est que V soit isométrique à J'_{24}.

Le groupe $U(R_{24})$ contient le groupe unitaire de K_{12}; celui-ci est de cardinal $2^9 \cdot 3^7 \cdot 5 \cdot 7$ et est engendré par les réflexions relatives aux vecteurs minimaux ([F], [S.T]). Ces groupes sont en fait égaux, car si on met dans la formule de masse (2) les cardinaux (connus) des groupes unitaires de $\mathfrak{M}^2 \perp J'_{16}$, $\mathfrak{M} \perp R_{20}$ et J'_{24}, il reste exactement $1/(2^9 \cdot 3^7 \cdot 5 \cdot 7)$.

La décomposition $\mathfrak{M} = \mathbb{Z}[w] + (1 + i)\mathbb{Z}[w]$ montre que $R_{24} = K_{12} + (1 + i)K_{12}$ (la somme est une somme directe mais non orthogonale de $\mathbb{Z}$-modules). Ainsi, tout élément de R_{24} est congru modulo $\mathfrak{P}R_{24}$ à un élément de K_{12}. Or, d'après [C.S2, §3], tout élément de K_{12} est congru modulo $2K_{12}$ à un élément de norme hermitienne 0, 2, 3 ou 4, et le groupe unitaire de K_{12} est transitif sur chacune de ces catégories (remarquons que les quotients $K_{12}/2K_{12}$ et $R_{24}/\mathfrak{P}R_{24}$ ont même cardinal). □

Déterminons le graphe des voisins: au cours de la démonstration du théorème 4.6, on a vu que J'_{24} est le seul voisin irréductible de $\mathfrak{M}^2 \perp J'_{16}$, et que R_{24} est le seul voisin irréductible de $\mathfrak{M} \perp R_{20}$ (à isométrie près). Pour avoir le graphe complet, il reste à montrer que J'_{24} et R_{24} sont voisins. Soit x un élément de R_{24} de norme hermitienne 4 et appartenant à K_{12}. Nous allons montrer que $(R_{24})_x$ est isométrique

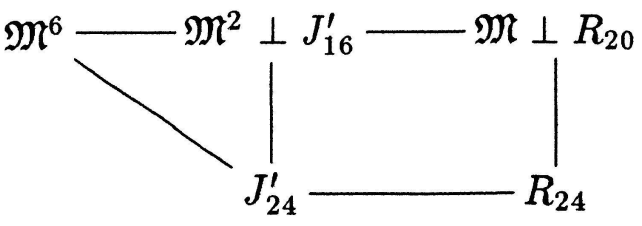

Figure 3. Graphe des voisins en dimension 24.

à J'_{24}. En effet, ce réseau est irréductible (sinon il contiendrait un élément y de norme hermitienne 1, tel que $x \equiv (1+i)y \bmod \mathfrak{P}R_{24}$; or la classe d'un élément de norme hermitienne 4 modulo $\mathfrak{P}R_{24}$ ne contient pas d'élément de norme hermitienne 2). De plus, $(R_{24})_x$ est clairement voisin de $\mathfrak{M} \otimes_{\mathbb{Z}[w]} (K_{12}^x + \mathbb{Z}[w]_2^x)$. Or $K_{12}^x + \mathbb{Z}[w]_2^x$ est isométrique sur $\mathbb{Z}[w]$ à $\mathbb{Z}[w]^6$ ([F]), donc $\mathfrak{M} \otimes_{\mathbb{Z}[w]} (K_{12}^x + \mathbb{Z}[w]_2^x)$ est isométrique à $\mathfrak{M}^6$ dont le seul voisin irréductible est J'_{24}.

4.9. *La dimension* 28

Nous allons construire trois réseaux non isométriques, irréductibles et unimodulaires en dimension 28. Rappelons qu'un tel réseau a 1512 vecteurs minimaux (§4.4).

Le premier se construit à partir du réseau de racines $\mathbb{E}_7$ de la façon suivante: le réseau $\mathbb{E}_7$ est de déterminant 2, et son dual $\mathbb{E}_7^*$ est tel que: $\mathbb{E}_7^* = \mathbb{E}_7 + \mathbb{Z}e$, où e est un vecteur de norme 3/2 ($e = \frac{1}{4}(1, 1, 1, 1, 1, 1, -3, -3)$ dans le système de coordonnées pair de E_8 ([C.S1 chap 4])). On pose alors:

$$R_{28} = \mathfrak{M} \otimes_{\mathbb{Z}} \mathbb{E}_7 + \mathfrak{P}e.$$

On voit facilement que ce réseau est unimodulaire sur l'ordre de Hurwitz; c'est le seul réseau unimodulaire contenant $\mathfrak{M} \otimes_{\mathbb{Z}} \mathbb{E}_7$.

Montrons que le minimum hermitien de R_{28} est encore 2: l'inclusion $\mathfrak{M} \subset \frac{1}{2}\mathbb{Z}[1, i, j, k]$ montre que $\mathfrak{M} \otimes \mathbb{E}_7^* \subset \frac{1}{2}\mathbb{E}_7^* \perp_{\mathbb{Z}} \frac{i}{2}\mathbb{E}_7^* \perp_{\mathbb{Z}} \frac{j}{2}\mathbb{E}_7^* \perp_{\mathbb{Z}} \frac{k}{2}\mathbb{E}_7^*$; le minimum hermitien de $\mathfrak{M} \otimes_{\mathbb{Z}} \mathbb{E}_7^*$ est donc égal à 3/2. Comme R_{28} est un sous-réseau entier de ce dernier réseau, son minimum hermitien est au moins égal à 2.

L'ensemble de ses vecteurs minimaux est égal à $\{ux, u \in \mathfrak{M}^*, x \in S(\mathbb{E}_7)\}$ qui est de cardinal 1512.

Le deuxième réseau est construit comme un voisin du réseau $\mathfrak{M}^3 \perp J'_{16}$. Soit $e = (i+j+k, 1, 1, 1)$ un élément de J'_{16} de norme hermitienne 3. Soit $x = (1, 1, 1) + e \in \mathfrak{M}^3 \perp J'_{16}$ de norme hermitienne 6. On pose:

$$R'_{28} = (\mathfrak{M}^3 \perp J'_{16})_x.$$

Posons $L_{16} = (J'_{16})^e$; il est engendré par l'ensemble de ses vecteurs minimaux qui apparaît comme système de racines dans [C] sous le nom de S_1. Son cardinal est $864 = 24.18$. Le réseau $\mathfrak{M}^{(1,1,1)}$ est isométrique à J_{12} qui a $648 = 24.27$ vecteurs minimaux. Le réseau R'_{28} contient (avec un indice 16) la somme orthogonale $L_{16} \perp J_{12}$; comme $864 + 648 = 1512$, l'ensemble des vecteurs minimaux de R'_{28} est la réunion $S(J_{12}) \cup S(L_{16})$.

Le troisième réseau est un cas particulier d'une construction générale due à J. Martinet et dont les réseaux J'_{4m} font également partie ([M2]). Nous donnons ici le cas particulier qui nous intéresse. Soit $\mathfrak{q}$ et $\mathfrak{q}'$ deux idéaux à gauche de $\mathfrak{M}$ contenant $3\mathfrak{M}$. On prendra $\mathfrak{q} = \mathfrak{M}(1-w)$ et $\mathfrak{q}' = \mathfrak{M}(1-w)i$, mais le choix est indifférent. On pose:

$$R''_{28} = \left\{(x_1, x_2, \ldots, x_7) \in \mathfrak{M}^7 / x_i \equiv x_j \bmod \mathfrak{q} \text{ et } \sum_{i=1}^{7} x_i \equiv 0 \bmod \mathfrak{q}'\right\},$$

muni de la forme $\frac{1}{3}\Sigma_{i=1}^{7} x_i \bar{y}_i$.

On montre que ce réseau est unimodulaire sur l'ordre de Hurwitz, de minimum hermitien 2. L'ensemble de ses vecteurs minimaux est, à permutation près des coordonnées, l'ensemble des vecteurs de la forme $u((1-w), v(1-w), 0, 0, \ldots, 0)$, où u appartient à $\mathfrak{M}^*$ et v appartient à $\{1, w, w^2\}$; on peut vérifier que cela fait bien 1512 vecteurs minimaux. Ils engendrent le sous-réseau d'indice 9 suivant: $\{(x_1, x_2, \ldots, x_7) \in \mathfrak{q}^7 / \Sigma_{i=1}^{7} x_i \in 3\mathfrak{M}\}$. On peut remarquer que R''_{28} est un 3-voisin au sens du paragraphe 2 de $\mathfrak{M}^7$.

Ces trois réseaux ne peuvent pas être isométriques car les sous-réseaux engendrés par leurs vecteurs minimaux respectifs ne le sont pas: en effet, dans le premier cas il est d'indice 4, dans le deuxième cas il est d'indice 16, et dans le troisième cas, il est d'indice 9.

THÉORÈME 4.7.

(1) *Les réseaux R_{28}, R'_{28} et R''_{28} sont, à isométrie hermitienne près, les seuls réseaux irréductibles et unimodulaires sur l'ordre de Hurwitz en dimension* 28.

(2) *Le groupe unitaire du réseau R_{28} est isomorphe au produit direct $\mathfrak{M}^*/\{\pm 1\} \times W(\mathbb{E}_7)$, où $W(\mathbb{E}_7)$ est le groupe de Weil du système de racines $\mathbb{E}_7$. Il est de cardinal $2^{12} \cdot 3^5 \cdot 5 \cdot 7$.*

(3) *Le groupe unitaire du réseau R'_{28} est de cardinal $2^{18} \cdot 3^5$.*

(4) *Le groupe unitaire du réseau R''_{28} est le produit direct de $\{\pm Id\}$ par le groupe engendré par les réflexions relatives à ses vecteurs minimaux; il est de cardinal $2 \cdot 3^6 \cdot 7!$.*

Démonstration: comme pour le théorème précédent, il suffit de démontrer que les réseaux réductibles ont au plus trois voisins irréductibles non isométriques. D'après les résultats précédents, les réseaux réductibles de la dimension 28 sont: $\mathfrak{M}^7$, $\mathfrak{M}^3 \perp J'_{16}$, $\mathfrak{M}^2 \perp R_{20}$, $\mathfrak{M} \perp R_{24}$, $\mathfrak{M} \perp J'_{24}$.

Le réseau $\mathfrak{M}^7$ n'a pas de voisin de minimum hermitien égal à 2.

Le réseau $\mathfrak{M} \perp J'_{16}$, a, à isométrie près, un seul voisin irréductible correspondant à un élément de la forme $(1, 1, 1) + x$, où x est de norme hermitienne 3 dans J'_{16}:

en effet, on a vu que le groupe unitaire de J'_{16} est transitif sur les éléments non isotropes du quotient $J'_{16}/\mathfrak{P}J'_{16}$ (théorème 4.4(4)). Ce réseau est aussi un voisin de $\mathfrak{M}^2_{(1,1)} \perp (\mathfrak{M} \perp J'_{16})_{1+x}$ qui est isométrique à $\mathfrak{M}^2 \perp R_{20}$.

Le réseau $\mathfrak{M}^2 \perp R_{20}$ a, à isométrie près, un seul voisin irréductible correspondant à un élément de la forme $(1, 1) + x$, où x est de norme hermitienne 2 dans R_{20}: en effet, on a vu que le groupe unitaire de R_{20} est transitif sur les éléments isotropes du quotient $R_{20}/\mathfrak{P}R_{20}$ (théorème 4.5 (4)).

Le réseau $\mathfrak{M} \perp R_{24}$ a, à isométrie près, un seul voisin irréductible correspondant à un élément de la forme $1 + x$, où x est de norme hermitienne 3 dans R_{24}: en effet, on a vu que le groupe unitaire de R_{24} est transitif sur les éléments non isotropes du quotient $R_{24}/\mathfrak{P}R_{24}$ (théorème 4.6 (4)).

On a trouvé jusque-là au plus deux classes de réseaux irréductibles; il reste à examiner les voisins de $\mathfrak{M} \perp J'_{24}$. Soit V un voisin irréductible de $L = \mathfrak{M} \perp J'_{24}$ contenant L^x. On pose $x = 1 + x_0$, avec $x_0 \in J'_{24}$. Montrons que $S(V)$ ne peut pas être inclus dans $S(L^x)$; dans ce cas, $S(L^x)$ serait de cardinal 1512, et donc $S((J'_{24})^{x_0})$ serait de cardinal 1488. L'examen de $S((J'_{24})^{x_0})$ montre que cela ne peut pas arriver avec un x_0 de norme hermitienne impaire. Comme $S(V)$ n'est pas inclus dans L^x, on peut écrire $V = L^x + \mathfrak{M}y$, avec $h(y, y) = 2$. Alors $(L^x)^* = L + \mathfrak{P}^{-1}x = L + \mathfrak{M}y$; x et $(1 + i)y$ déterminent la même droite du $\mathfrak{M}/\mathfrak{P}$-espace vectoriel $L/\mathfrak{P}L$, la classe de x dans $L/\mathfrak{P}L$ contient donc un élément de norme hermitienne 4. On est donc ramenés au cas où $h(x_0, x_0) = 3$. On voit facilement que, sous l'action du groupe unitaire de J'_{24}, les éléments de norme hermitienne 3 se répartissent en deux orbites: celle de $(1, 1, 1, 1, 1, 1)$, et celle de $(1 + i, (1 + i)w, (1 + i)w^2, 0, 0, 0)$. On montre alors que, dans le dernier cas, V contient un sous-réseau isométrique à $J_{12} \perp L_{16}$ (considérer $\{x \in V / x_0 = x_1 = x_2 = x_3 = 0\} \perp \{x \in V / x_4 = x_5 = x_6 = 0\}$), et que, à isométrie près, il y a un seul réseau irréducible et unimodulaire contenant $J_{12} \perp L_{16}$, qui est également un voisin de $\mathfrak{M}^3 \perp J'_{16}$. Le point (1) est donc démontré.

Le groupe $\mathfrak{M}^*/\{\pm 1\} \times W(\mathbb{E}_7)$ est un sous-groupe du groupe unitaire de $\mathfrak{M} \otimes_{\mathbb{Z}} \mathbb{E}_7$ (agissant par $a \otimes x \to au \otimes f(x)$); comme R_{28} est le seul réseau unimodulaire contenant $\mathfrak{M} \otimes_{\mathbb{Z}} \mathbb{E}_7$, il est stable par ce groupe.

Comme les vecteurs minimaux de R'_{28} engendrent $J_{12} \perp L_{16}$, son groupe unitaire est un sous-groupe du produit $U(J_{12}) \times U(L_{16})$. Il y a exactement 12 réseaux contenant $J_{12} \perp L_{16}$ et isométriques à R'_{28} (correspondants au choix d'un parmi les trois réseaux d'indice $\mathfrak{P}$ de $\mathfrak{M}^3 \perp J'_{16}$, mais distincts de $\mathfrak{M}^3 \perp L_{16}$ et de $J_{12} \perp J'_{16}$, puis d'un parmi les quatre réseaux unimodulaires contenant celui-ci et distinct de $\mathfrak{M}^3 \perp J'_{16}$). Ils sont permutés transitivement par le groupe $U(J_{12}) \times U(L_{16})$. Donc $\# U(L) = \frac{1}{12} \# U(J_{12}) \# U(L_{16})$. Il reste à calculer le cardinal du groupe unitaire de L_{16}. On voit facilement que $L^*_{16} \cap \{x / h(x, x) = 2\} = S(J'_{16})$. Le groupe unitaire de L_{16} est donc un sous-groupe du groupe unitaire de J'_{16}; comme $L_{16} = (J'_{16})^e$, $U(L_{16})$ est formé des éléments de $U(J'_{16})$ qui stabilisent la droite issue de e du $\mathfrak{M}/\mathfrak{P}$-espace

vectoriel $J'_{16}/\mathfrak{P}J'_{16}$. Or on a vu (théorème 4.4) que $U(J'_{16})$ est transitif sur les vecteurs non isotropes de ce quotient. Dans un espace hermitien de dimension 4 sur $\mathbb{F}^4$, il y a 40 droites non isotropes, sonc $\#U(L_{16}) = \#U(J'_{16})/40$. On trouve finalement que $U(R'_{28})$ a $2^{18} \cdot 3^5$ éléments.

Le groupe engendré par les réflexion relatives aux vecteurs minimaux de R''_{28} est un sous-groupe de son groupe unitaire; c'est le groupe de réflexions noté $G_7(\{1, w, w^2\}, \{1\})$ dans [C], il est de cardinal $3^6 \cdot 7!$

Pour chaque classe d'isométrie hermitienne de réseau, on connait un sous-groupe du groupe unitaire; or la formule de masse donne un reste nul quand on remplace les cardinaux des groupes unitaires par les cardinaux de ces sous-groupes. Ceux-ci sont donc les groupes unitaires tout entiers. □

Déterminons le graphe des voisins: au cours de la démonstration du théorème 4.7, on a montré que $\mathfrak{M} \perp J'_{24}$ a deux voisins irréductibles, sont un qu'il partage avec $\mathfrak{M}^3 \perp J'_{16}$ et $\mathfrak{M}^2 \perp R_{20}$. Ce dernier est donc R'_{28}. Par ailleurs, si $x = (1, 1, 1, 1, 1, 1, 1, 1)$, on montre facilement que $(\mathfrak{M} \perp J'_{24})_x$ est isométrique à R_{28}. R''_{28} est donc l'unique (à isométrie près) voisin irréductible de $\mathfrak{M} \perp R_{24}$.

Dans le système de coordonnées pair de $\mathbb{E}_8$, soit $x = (0, -1, 1, -w, w, 0, 0, 0)$ qui appartient à R_{28}. Alors $(R_{28})_x$ est isométrique à R'_{28} (ceci a été vérifié dans le système PARI, en calculant l'indice du sous-réseau engendré par les vecteurs minimaux).

Les voisins irréductibles de R''_{28} n'ont pas été explorés systématiquement; nous n'avons pas déterminé si R'_{28} et R''_{28} sont voisins.

5. Réseaux unimodulaires sur l'ordre de Hurwitz en dimension 32

En dimension 32, l'inégalité (1) laisse la possibilité pour un réseau modulaire de niveau 2 d'avoir un minimum égal à 6. Dans [Q1], H.-G. Quebbemann a construit un tel réseau; c'est la meilleure densité connue en dimension 32.

Dans ce paragraphe, nous allons construire un réseau Q de minimum 6, modulaire de niveau 2, ayant une structure quaternionienne sur l'ordre de Hurwitz, mais non unimodulaire. (Remarquons que, pour que le réseau $L_{\mathbb{Z}}$ associé à un réseau L hermitien sur l'ordre de Hurwitz soit entier, il n'est pas nécessaire que la forme $h(x, y)$ prenne des valeurs entières sur L; il suffit que $h(x, y)$ appartienne à $\mathfrak{P}^{-1}$ qui est la codifférente de H.) La question de l'existence d'un tel réseau, qui soit en outre unimodulaire sur l'ordre de Hurwitz, reste ouverte; son existence est toutefois peu probable. Il semble qu'il y ait un trop grand nombre de réseaux de minimum 4 (nous en avons trouvé 9 et cette liste n'est surement pas complète) pour pouvoir utiliser la formule de masses (2).

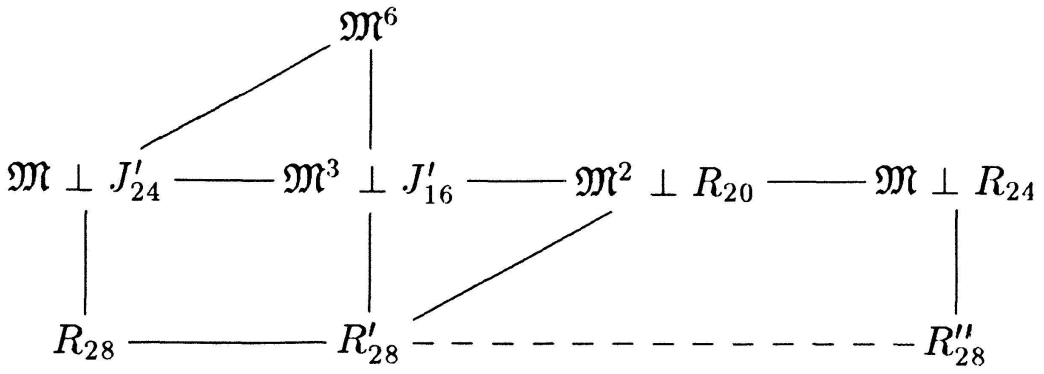

Figure 4. Graphe des voisins en dimension 28.

La méthode s'inspire de la construction bien connue du réseau de Leech comme voisin (au sens de Kneser) du réseau unimodulaire de système de racines $\mathbb{A}_1^{24}$. Ce dernier est construit à l'aide du code de Golay ([C.S1 chap. 4–18]). Nous allons d'abord construire un réseau unimodulaire sur l'ordre de Hurwitz, de minimum 4, et ayant pour vecteurs minimaux huit vecteurs deux à deux orthogonaux ainsi que leurs multiples par une unité de $\mathfrak{M}$. Autrement dit, l'ensemble de ses vecteurs minimaux engendre un réseau isométrique à J_4^8. Notons un tel réseau $\tilde{J}_4^8$. Pour cela, on utilise un code de longueur 8 sur l'algèbre $\mathfrak{M}/2\mathfrak{M}$ (qui remplace $\mathbb{Z}/2\mathbb{Z}$ dans le cas de $\mathbb{A}_1^{24}$). Ensuite, on cherche Q comme voisin (non entier) de $\tilde{J}_4^8$.

5.1. *Codes sur* $\mathfrak{M}/2\mathfrak{M}$

L'algèbre $\mathfrak{M}/2\mathfrak{M}$ a la structure suivante: en identifiant les classes modulo $2\mathfrak{M}$ de $0, 1, w, w^2$ avec le corps $\mathbb{F}_4$, et en notant u la classe de $1+i$,

$$\mathfrak{M}/2\mathfrak{M} = \mathbb{F}_4 + \mathbb{F}_4 u,$$

avec les relations $u^2 = 0$ et $u\lambda = \bar{\lambda}u$, où $\lambda \to \bar{\lambda}$ est le Frobenius de $\mathbb{F}_4$; la somme est une somme directe de $\mathbb{F}_4$-espace vectoriel. On note (x, y) l'élément $x + yu$ de $\mathfrak{M}/2\mathfrak{M}$. Remarquons qu'un tel élèment contient une unité de $\mathfrak{M}$ si et seulement si x est non nul.

Un code (linéaire) sur $\mathfrak{M}/2\mathfrak{M}$ de longueur m est un sous-module C de $(\mathfrak{M}/2\mathfrak{M})^m$. Il n'est pas nécessairement libre, mais admet une matrice génératrice de la forme:

$$G = \begin{pmatrix} I_{k_1} & M_1 & M_2 \\ 0 & I_{k_2} u & M_3 u \end{pmatrix}.$$

où M_1, M_2 sont des matrices à coefficients dans $\mathfrak{M}/2\mathfrak{M}$ et M_3 est à coefficients dans

$\mathbb{F}_4$. Le code C est libre si et seulement si $k_2 = 0$; son cardinal est $16^{k_1} \cdot 4^{k_2}$. L'orthogonalité dans $(\mathfrak{M}/2\mathfrak{M})^m$ est définie relativement à la forme $\Sigma_{i=1}^m x_i \bar{y}_i$; le poids d'un mot est défini en comptant 1 par coordonnée n'appartenant pas à $\mathbb{F}_4 u$, et 2 par coordonnée appartenant à $\mathbb{F}_4 u - \{0\}$.

A partir d'un code C on définit un réseau L_C hermitien sur l'ordre de Hurwitz par:

$$L_C = \{(x_1, x_2, \ldots, x_m) \in \mathfrak{M}^m / (x_1, x_2, \ldots, x_m) \bmod 2\mathfrak{M} \in C\}$$

pour la forme $\frac{1}{2} \Sigma_{i=1}^m x_i \bar{y}_i$. Alors L_C est un réseau entier si et seulement si $C \subset C^\perp$, unimodulaire si et seulement si $C = C^\perp$. Supposons que $C \subset C^\perp$. Le minimum du réseau L_C est 4 si le poids minimal de C est au moins égal à 4, et le réseau engendré par son système de racines contient $(2\mathfrak{M})^m$, qui est isométrique à J_4^m. Si le poids minimal de C est au moins égal à 6, alors L_C ne contient pas d'autre racine.

À un code C sur $\mathfrak{M}/2\mathfrak{M}$, on associe de façon naturelle deux codes sur $\mathbb{F}_4$ de la façon suivante: soit $C_t = \{x \in C / ux = 0\}$ la torsion de C. C'est un $\mathbb{F}_4$-espace vectoriel de dimension $k_1 + k_2$. On pose

$$T = \{(y_1, \ldots, y_m) \in \mathbb{F}_4^m / (y_1 u, \ldots, y_m u) \in C_t\}$$

On définit également un code C_1 par projection sur la première coordonnée:

$$C_1 = \{(y_1, \ldots, y_m) \in \mathbb{F}_3^m / \exists (z_1, \ldots, z_m) \in \mathbb{F}_4^m / (y_1 + z_1 u, \ldots, y_m + z_m u) \in C\}.$$

Remarquons que, si $C \subset C^\perp$, alors $T \subset C_1^\perp$ (pour la forme $\Sigma x_i y_i$): en effet, soit $(x_1, \ldots, x_m) \in C_1$ et $(y_1, \ldots, y_m) \in T$. Alors il existe $(z_1, \ldots, z_m)$ tel que $(x_1 + z_1 u, \ldots, x_m + z_m u)$ et $(y_1 u, \ldots, y_m u)$ soient dans C. Ils sont donc orthogonaux, ce qui équivaut à la condition $\Sigma x_i y_i = 0$.

5.2. *Construction de* $\tilde{J}_4^8$

On définit un code C de longueur 8 par la matrice génératrice:

$$G = \begin{bmatrix} 1 & 0 & 0 & (1,1) & (1,\bar{w}) & (0,1) & (0,w) & (1,1) \\ 0 & 1 & 0 & (1,1) & (w,1) & (\bar{w},w) & (w,1) & (\bar{w},w) \\ 0 & 0 & 1 & 1 & (w,w) & (w,\bar{w}) & (\bar{w},\bar{w}) & (\bar{w},w) \\ 0 & 0 & 0 & (0,1) & 0 & (0,w) & (0,w) & (0,1) \\ 0 & 0 & 0 & 0 & (0,1) & (0,1) & (0,1) & (0,1) \end{bmatrix}.$$

PROPOSITION 5.1. *Le code C sur $\mathfrak{M}/2\mathfrak{M}$ de matrice génératrice G a les propriétés suivantes*:

(1) $C = C^{\perp}$

(2) *C est de poids minimal* 6.

(3) *Le réseau L_c associé à C est un réseau unimodulaire sur l'ordre de Hurwitz, de minimum hermitien* 2; *ses vecteurs minimaux sont au nombre de* 192 *et engendrent un réseau isométrique à J_4^8.*

Notation: on notera $\tilde{J}_4^8$ le réseau L_C ainsi défini.

Démonstration: on vérifie facilement sur la matrice G que $C \subset C^{\perp}$. Le cardinal de C montre que $C = C^{\perp}$. Remarquons que cela entraine que le poids d'un mot de C est pair.

Pour calculer son poids minimal, on étudie les codes T et C_1. Notons e_1, e_2, e_3, e_4, e_5 les lignes de la matrice G. Une base de C_t est $\{ue_1, ue_2, ue_3, e_4, e_5\}$. On obtient pour matrice génératrice du code T:

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & \bar{w} & w & \bar{w} & w \\ 0 & 0 & 1 & 1 & \bar{w} & \bar{w} & w & w \\ 0 & 0 & 0 & 1 & 0 & w & w & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

qui est équivalent à:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \bar{w} & \bar{w} & 1 \\ 0 & 1 & 0 & 0 & 0 & \bar{w} & w & 0 \\ 0 & 0 & 1 & 0 & 0 & w & \bar{w} & 0 \\ 0 & 0 & 0 & 1 & 0 & w & w & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Le code T est clairement un code sur $\mathbb{F}_4$ de poids minimal 3 (pour le poids usuel, c'est-à-dire le nombre de coordonnées non nulles). Le code C_1 a pour matrice génératrice

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & w & \bar{w} & w & \bar{w} \\ 0 & 0 & 1 & 1 & w & w & \bar{w} & \bar{w} \end{pmatrix},$$

qui est équivalente à

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & w & w & \bar{w} & \bar{w} \end{pmatrix}.$$

Le code C_1 est de poids pair, son poids minimal est 4, et il n'est atteint que sur les mots 10011001 et 01100110.

Soit maintenant c un mot du code C. Notons c_1 le mot de C_1 associé à c. Le nombre de coordonnées de c n'appartenant pas à $\mathbb{F}_4 u$ est égal au poids de c_1. il y a trois cas à considérer: si le poids de c_1 est 0, alors c appartient à C_t; or on a vu que T est de poids minimal 3, donc C_t est de poids minimal 6. Si le poids de c_1 est au moins égal à 6, alors c a au moins six coordonnées non nulles, et c est de poids au moins égal à 6. Si le poids de c_1 est 4, il faut montrer qu'au moins une coordonnée de c appartient à $\mathbb{F}_4 u - \{0\}$. Comme C_1 n'a que deux mots de poids 4, c est de l'un des deux types suivants:

$$c = (1, 0)(0, 0)(0, 0)(1, 1)(1, \bar{w})(0, 1)(0, w)(1, 1) + t$$

ou

$$c = (0, 0)(1, 0)(1, 0)(0, 1)(0, \bar{w})(1, 1)(1, w)(0, 1) + t$$

avec t appartenant à C_t. Pour faire baisser le poids à 4, il faudrait que t annule les coordonnées qui sont dans $\mathbb{F}_4 u$ (t ne peut pas annuler les autres). Pour cela, t doit être de la forme $t = t'u$ avec $t' \in T$ du type $*00 * *(0, 1)(0, w)*$ dans le premier cas, et $0* *(0, 1)(0, \bar{w})* *(0, 1)$ dans le deuxième (les $*$ pouvant être n'importe quoi). L'examen du code T montre que c'est impossible.

D'après le paragraphe precédent, le point (3) se déduit du point (2). □

Remarques. 1. On peut aussi construire le réseau $\tilde{J}_4^8$ par voisinages successifs à partir du réseau J'_{32}. On passe alors successivement par des réseaux dont les vecteurs minimaux engendrent des réseaux isométriques à J_{32}, $J_{16}^2, J_8^4, \mathfrak{M} \otimes_{\mathbb{Z}} \mathbb{D}_4^2, J_4^8$. Cette méthode a été mise en œuvre en utilisant le système PARI.

2. Le code C permet d'écrire une base du réseau $\tilde{J}_4^8$. Elle est donnée par les colonnes de la matrice suivante:

$$\begin{pmatrix}
1 & & & & & & & \\
1 & 1 & & & & & & \\
1 & 0 & 1 & & & & & \\
1 & 1 & 1 & 1+i & & & & \\
1 & \frac{1-i+j+k}{2} & \frac{-1+i+j+k}{2} & 0 & 1+i & & & \\
1 & \frac{1+i+j+k}{2} & \frac{1-i+j+k}{2} & 1+j & 1+i & 2 & & \\
1 & \frac{1+i+j-k}{2} & \frac{1+i-j-k}{2} & 1+j & 1+i & 0 & 2 & \\
1 & \frac{1-i+j-k}{2} & \frac{1+i+j+k}{2} & 1+i & 1+i & 0 & 0 & 2
\end{pmatrix}$$

pour la forme $\frac{1}{2}\Sigma_{i=1}^{8} x_i\bar{y}_i$.

5.3. *Construction de Q*

Le code C contient le mot 11111111 (c'est la somme des trois premières lignes de G). Soit $e = (1, 1, 1, 1, 1, 1, 1, 1)$ l'élément de $\tilde{J}_4^8$ correspondant. Le réseau $(\tilde{J}_4^8)^e$ ne contient plus les vecteurs minimaux de $\tilde{J}_4^8$; nous avons cherché Q parmi les réseaux contenant $(\tilde{J}_4^8)^e$ avec un indice $\mathfrak{P}$.

Le calcul montre que les cinq réseaux unimodulaires sur l'ordre de Hurwitz et contenant $(\tilde{J}_4^8)^e$ ont pour minimum hermitien 2. En faisant décrire à y les classes de $(\tilde{J}_4^8)^e/\mathfrak{P}(\tilde{J}_4^8)^e$, on trouve que le réseau

$$Q = (\tilde{J}_4^8)^e + \mathfrak{P}^{-1}y, \qquad \text{avec } y = (1, 1, 1, 1, 1, 1, -1, 1-2k)$$

a pour minimum hermitien 3. Les calculs numériques ont été effectués dans le système PARI.

THÉORÈME 5.2.

(1) *Il existe une isométrie hermitienne* σ *telle que* $Q^* = \sigma(Q)$.

(2) *Le réseau* $Q_{\mathbb{Z}}$ *est entier, pair, modulaire de niveau* 2, *a pour minimum* 6 *et pour déterminant* 2^{16}.

Démonstration: soit σ l'isométrie hermitienne définie par: $\sigma(x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) = (x_1, x_2, x_3, x_4, x_5, x_6, -x_7, -x_8)$. C'est clairement une isométrie du réseau $\tilde{J}_4^8$, puisque c'est l'identité sur le code C. montrons que $Q^* = \sigma(Q)$, c'est-à-dire

que $h(x, \sigma(y)) \in \mathfrak{M}$ pour tout x, y appartenant à Q. Comme $Q = (\tilde{J}_4^8)^e + \mathfrak{P}^{-1}y$, $\sigma(Q) = \sigma((\tilde{J}_4^8)^e) + \mathfrak{P}^{-1}\sigma(y)$. Or $h((\tilde{J}_4^8)^e, \sigma((\tilde{J}_4^8)^e)) \subset \mathfrak{M}$ puisque σ conserve $\tilde{J}_4^8$, et $h((\tilde{J}_4^8)^e, \mathfrak{P}^{-1}\sigma(y)) \subset \mathfrak{M}$ si et seulement si $\mathfrak{P}^{-1}\sigma(y) \subset ((\tilde{J}_4^8)^e)^* = \tilde{J}_4^8 + \mathfrak{P}^{-1}e$. Or $\sigma(y) = (1, 1, 1, 1, 1, 1, 1, -1 + 2k) = e + (k-1)(0, 0, 0, 0, 0, 0, 0, 2)$ appartient bien à $\mathfrak{P}\tilde{J}_4^8 + \mathfrak{M}e$. Puisque $\sigma^{-1} = \sigma$, on a aussi l'inclusion $h(\sigma((\tilde{J}_4^9)^e), \mathfrak{P}^{-1}(y)) \subset \mathfrak{M}$. Enfin, $h(y, \sigma(y)) = 0$ appartient à $2\mathfrak{M}$.

Comme y appartient à $(\tilde{J}_4^8)^e$, pour que le réseau $Q_{\mathbb{Z}}$ soit pair, il suffit que $h(y, y)$ appartienne à $2\mathbb{Z}$. Or $h(y, y) = 6$. Le dual du réseau $Q_{\mathbb{Z}}$ est $(1+i)^{-1}\sigma(Q)$. La transformation $x \to (1+i)\sigma^{-1}(x)$ est une similitude de rapport $\sqrt{2}$ de $Q_{\mathbb{Z}}^*$ sur Q.

La valeur du minimum de $Q_{\mathbb{Z}}$ a été vérifiée dans le système PARI. Il a 261120 vecteurs minimaux, comme prévu par la théorie des formes modulaires. □

Remarque. La méthode de construction de Q permet d'en donner une $\mathfrak{M}$-base:

$$\begin{pmatrix}
\frac{1-i}{2} & & & & & & & \\
\frac{1-i}{2} & 1 & & & & & & \\
\frac{1-i}{2} & 0 & 1 & & & & & \\
\frac{1-i}{2} & 1 & 1 & 1+i & & & & \\
\frac{1-i}{2} & \frac{1-i+j+k}{2} & \frac{-1+i+j+k}{2} & 0 & 1+i & & & \\
\frac{1-i}{2} & \frac{1+i+j+k}{2} & \frac{1-i+j+k}{2} & 1+j & 1+i & 2 & & \\
\frac{-1+i}{2} & \frac{1+i+j-k}{2} & \frac{1+i-j-k}{2} & 1+j & 1+i & 0 & 2 & \\
\frac{1-i-2j-2k}{2} & \frac{1-i+5j-k}{2} & \frac{3-i-j-k}{2} & 1+i & 1+i & -2 & -2 & 2(1+i)
\end{pmatrix}$$

pour la forme $\frac{1}{2}\Sigma_{i=1}^{8} x_i\bar{y}_i$.

BIBLIOGRAPHIE

[C] COHEN, A. M., *Finite quaternionic reflection groups*, J. Algebra *64* (1980), 293–324.

[C.S1] CONWAY, J. H. and SLOANE, N. J. A., *Sphere Packings, Lattices and Groups*, Springer-Verlag, Heidelberg, 1988.

[C.S2] CONWAY, J. H. and SLOANE, N. J. A., *The Coxeter-Todd lattice, the Mitchell group, and related sphere packings*, Math. Proc of the Cambridge Phil. Soc. *93* (1983), 421–440.

[F] FEIT, W., *Some lattices over* $\mathbb{Q}(\sqrt{-3})$, J. Algebra *52* (1978), 248–263.

[H] HASHIMOTO, K., *On Brandt matrices associated with the positive definite quaternion hermitian forms*, J. Fac. Sci. Univ. Tokyo *27(1)* (1980), 227–245.

[J] JACOBOWITZ, R., *Hermitian forms over local fields*, Amer. J. Math. *84* (1962), 441–465.
[K1] KNESER, M., *Klassenzahlen definiter quadratischer Formen*, Archiv der Math. *8* (1957), 241–250.
[K2] KNESER, M., *Lectures on Galois cohomology of classical groups*, Tata Institute of Fundamental Research, Bombay, 1969.
[K3] KNESER, M., *Strong approximation*, Proc. Sympos. Pure Math., Amer. Math. Soc. *9* (1966).
[M1] MARTINET, J., *Les réseaux parfaits des espaces euclidiens* (livre en préparation).
[M2] MARTINET, J., *Structures algébriques sur les réseaux, Séminaire de Théorie des Nombres de Paris 1992–1993*, Cambridge University Press, à paraître.
[P.S] PLESKEN, W. and SOUVIGNIER, B., *Computing isometries of lattices*, to appear.
[Q1] QUEBBEMANN, H.-G., *Lattices with theta-function for $G(\sqrt{2})$ and linear codes*, J. Algebra *105* (1987), 443–450.
[Q2] QUEBBEMANN, H.-G., *Modular lattices in euclidean spaces*, to appear.
[S.T] SHEPPARD, G. C. and TODD, J. A., *Finite unitary reflexion groups*, Canad. J. Math. *6* (1954), 274–304.
[V] VIGNERAS, M.-F., *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics *800* (1980), Springer-Verlag.

Recherche effectuée au sein de l'Unitée Mixte C.N.R.S.-Enseignement supérieur U.R.M. 9936.

Laboratoire d'Algorithmique Arithmètique
351, cours de la Libération
F-33405 Talence

Received November 26, 1993.