ACTA ARITHMETICA
LXX.1 (1995)

Réseaux unimodulaires quaternioniens en dimension ≤ 32

par

Renaud Coulangeon (Talence)

1. Introduction. L'objet de cette étude est la classification des réseaux unimodulaires pairs, munis d'une structure additionnelle sur un corps de quaternions. Dans le cas classique, à un réseau Λ d'un espace euclidien E de dimension n muni d'un produit scalaire $S(x,y)$, on associe son dual Λ^* défini par

$$\Lambda^* = \{x \in E \mid S(x,y) \in \mathbb{Z} \ \ \forall y \in \Lambda\}.$$

Un réseau Λ est dit *entier* s'il est contenu dans son dual Λ^*, i.e. si les produits scalaires de ses éléments deux à deux sont entiers, et *unimodulaire* si $\Lambda = \Lambda^*$. Enfin Λ est *pair* si la forme quadratique qui lui est associée prend des valeurs paires sur Λ. On définit par ailleurs pour un vecteur x de Λ sa *norme* $N(x) = S(x,x)$, et la *norme* (ou *norme minimale*) de Λ par

$$N(\Lambda) = \min_{x \in \Lambda \setminus \{0\}} N(x).$$

On désigne par *vecteurs minimaux* les vecteurs dont la norme est égale à $N(\Lambda)$.

Le problème de la classification, à isométrie près, des réseaux unimodulaires pairs est complètement résolu jusqu'à la dimension 24 (cf. par exemple [S], et [Nie] pour le cas de la dimension 24). Parmi les techniques fréquemment utilisées, citons la formule de masse de Minkowski–Siegel (cf. [Sie], [S]), qui montre entre autres qu'en dimension 32 le nombre de classes d'isométrie de réseaux unimodulaires pairs est supérieur à $8 \cdot 10^7$, ainsi que la notion de *voisin* introduite par Kneser (cf. [K]).

Les réseaux qui vont nous intéresser ici sont munis d'une structure de module sur un ordre maximal d'un corps de quaternions sur un corps quadratique réel. On définit au paragraphe 2 une notion de voisinage adaptée à ce contexte et analogue à la définition de Kneser, ce qui permet, au paragraphe 3, d'obtenir une classification complète jusqu'en dimension 32 dans le cas où le corps de base est $\mathbb{Q}(\sqrt{5})$. Cette classification fait apparaître notamment trois réseaux irréductibles de norme 4, dont le réseau de Leech en

dimension 24 et deux réseaux en dimension 32. Comme dans le cas usuel (i.e. des réseaux unimodulaires pairs sur $\mathbb{Z}$), le problème de la classification devient inaccessible dès lors que la dimension augmente. Signalons enfin, bien qu'il n'en soit pas fait usage ici, que le résultat de "connexité" du graphe de voisinage au sens de Kneser (cf. [K]) a été étendu au cas des voisinages quaternioniens définis au paragraphe 2 par C. Bachoc (cf. [B]).

Je remercie W. Plesken de m'avoir signalé une erreur dans la démonstration de la proposition 3.5, qui a été rectifiée sur ses conseils.

2. Voisins quaternioniens

2.1. *Définitions.* Soient K un corps de nombres totalement réel de degré d sur $\mathbb{Q}$, et H l'unique corps de quaternions sur K totalement défini (i.e. ramifié aux places infinies de K) et non ramifié aux places finies (l'unicité est un résultat classique sur la classification des algèbres de quaternions sur un corps global, cf. [V], Théorème 3.1, p. 74). On note $\mathcal{O}_K$ l'anneau des entiers de K, et l'on fixe un ordre maximal $\mathfrak{M}$ de H. Enfin, $y \mapsto \overline{y}$ désignant la conjugaison de H, on munit le H-espace vectoriel (à gauche) H^m de la forme hermitienne standard

$$h(x,y) = \sum_{i=1}^{m} x_i \overline{y}_i.$$

Un $\mathfrak{M}$-*réseau* de (H^m, h) est par définition un sous $\mathfrak{M}$-module projectif de H^m de rang m, muni de la forme hermitienne h. On pose

$$\Lambda^{\#} = \{y \in H^m \mid h(x,y) \in \mathfrak{M} \ \ \forall x \in \Lambda\}.$$

On peut considérer un tel $\mathfrak{M}$-réseau comme un réseau (au sens usuel) de rang $n = dm$ sur $\mathbb{Z}$ grâce au procédé suivant : on suppose que la différente $\mathcal{D}_{K/\mathbb{Q}}$ est principale au sens restreint, et l'on note α un générateur totalement positif de $\mathcal{D}_{K/\mathbb{Q}}$. On munit alors H^m du produit scalaire

$$S(x,y) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha^{-1} \,\mathrm{tr}(h(x,y)))$$

(que cela définisse bien une forme *définie positive* provient du fait que α est totalement positif). Si l'on note Λ^* le dual de Λ pour ce produit scalaire, on a alors les équivalences :

$$\begin{aligned} y \in \Lambda^* &\Leftrightarrow \mathrm{Tr}_{K/\mathbb{Q}}(\alpha^{-1} \,\mathrm{tr}(h(\Lambda, y))) \subset \mathbb{Z} \\ &\Leftrightarrow \alpha^{-1} \,\mathrm{tr}(h(\Lambda, y)) \subset \mathcal{D}_{K/\mathbb{Q}}^{-1} \\ &\Leftrightarrow h(\Lambda, y) \subset \mathfrak{M} \\ &\quad \text{puisque } (\alpha) = \mathcal{D}_{K/\mathbb{Q}} \text{ et puisque } H/K \text{ est non ramifiée} \\ &\quad \text{aux places finies,} \\ &\Leftrightarrow y \in \ \Lambda^{\#}. \end{aligned}$$

Ainsi, un $\mathfrak{M}$-réseau est entier (respectivement unimodulaire) si et seulement si $\Lambda \subset \Lambda^{\#}$ (respectivement $\Lambda = \Lambda^{\#}$). Noter par ailleurs qu'un $\mathfrak{M}$-réseau entier est automatiquement pair : en effet, pour tout élément x d'un tel $\mathfrak{M}$-réseau, on a $S(x,x) = 2\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^{-1}h(x,x)) \in 2\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^{-1}\mathfrak{M}) \subset 2\mathbb{Z}$.

Remarque. L'hypothèse sur la différente $\mathcal{D}_{K/\mathbb{Q}}$ n'intervient que pour pouvoir définir un produit scalaire pour lequel les deux notions de dualité (i.e. dualité pour la forme hermitienne et dualité pour le produit scalaire) coïncident. Elle ne joue donc aucun rôle tant que l'on ne s'intéresse qu'à la structure *hermitienne* d'un $\mathfrak{M}$-réseau, ce qui sera le cas dans le reste de ce paragraphe. En revanche, on fera largement appel, dans le paragraphe suivant, aux propriétés en tant que réseaux sur $\mathbb{Z}$ des $\mathfrak{M}$-réseaux rencontrés.

Si $\mathfrak{A}$ est un idéal à gauche de $\mathfrak{M}$, on a

$$\overline{\mathfrak{A}}\Lambda^{\#} = \{y \in H^m \mid h(x,y) \in \mathfrak{A} \ \ \forall x \in \Lambda\}.$$

La définition qui suit est un analogue *quaternionien* de la notion de réseau voisin au sens de Kneser ([K]). On trouve une définition du même type dans [Q], dans le cas d'une algèbre de quaternions sur $\mathbb{Q}$ et pour un idéal premier (bilatère) ramifié, ainsi que dans [B].

2.1.1. Définition. Soient $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ et $\mathfrak{P}$ un idéal maximal (à gauche) de $\mathfrak{M}$ au-dessus de $\mathfrak{p}$.

(1) Deux $\mathfrak{M}$-réseaux entiers Λ et Λ' sont dits $\mathfrak{p}\mathfrak{M}$-*voisins*, ou simplement *voisins* lorsqu'il n'y a pas d'ambiguïté, si $\Lambda/\Lambda \cap \Lambda' \simeq \Lambda'/\Lambda \cap \Lambda' \simeq \mathfrak{M}/\mathfrak{P}$.

(2) Soient Λ un $\mathfrak{M}$-réseau entier et $v \in \Lambda^{\#} \setminus \overline{\mathfrak{P}}\Lambda^{\#}$, vérifiant $h(v,v) \in \mathfrak{p}$. On pose

$$\Lambda^v = \{x \in \Lambda \mid h(x,v) \in \mathfrak{P}\} \quad \text{et} \quad \Lambda_v = \Lambda^v + \overline{\mathfrak{P}}^{-1}v.$$

Remarques. 1. Dans la définition (2), l'hypothèse que v appartienne à $\Lambda^{\#} \setminus \overline{\mathfrak{P}}\Lambda^{\#}$ assure que Λ^v soit un sous-$\mathfrak{M}$-réseau de Λ, distinct de Λ. Par ailleurs, l'hypothèse que $h(v,v)$ appartienne à $\mathfrak{p}$ garantit que le $\mathfrak{M}$-réseau Λ_v soit entier.

2. Rappelons que dans le cas où l'idéal $\mathfrak{p}$ de $\mathcal{O}_K$ est non ramifié dans H, le quotient $\mathfrak{M}/\mathfrak{p}\mathfrak{M}$ est isomorphe à $\mathcal{M}_2(\mathbb{F}_q)$, où $q = p^f = N_{K/\mathbb{Q}}(\mathfrak{p})$, et les idéaux maximaux à gauche de $\mathfrak{M}$ au-dessus de $\mathfrak{p}$ correspondent résiduellement aux idéaux maximaux à gauche de $\mathcal{M}_2(\mathbb{F}_q)$. On obtient une bijection entre l'ensemble de ces idéaux et la droite projective $\mathbb{P}_1(\mathbb{F}_q)$ en associant à un point de coordonnées homogènes (α,β) l'idéal

$$I_{(\alpha,\beta)} = \left\{ \begin{pmatrix} \alpha a & \beta a \\ \alpha b & \beta b \end{pmatrix} \in \mathcal{M}_2(\mathbb{F}_q) \;\middle|\; (a,b) \in \mathbb{F}_q^2 \right\}.$$

A un idéal maximal *à gauche* $\mathfrak{P}$, on associe l'idéal maximal *à droite* $\overline{\mathfrak{P}} = \{\overline{\lambda} \mid \lambda \in \mathfrak{P}\}$, qui vérifie $\mathfrak{P}\overline{\mathfrak{P}} = \mathfrak{p}\mathfrak{M}$, de sorte que $\overline{\mathfrak{P}}^{-1}$ est l'idéal fractionnaire $\mathfrak{p}^{-1}\mathfrak{P}$.

3. En particulier, la définition (1) ci-dessus ne dépend pas du choix de l'idéal $\mathfrak{P}$ au-dessus de $\mathfrak{p}$ car si $\mathfrak{P}'$ est un autre idéal maximal à gauche au-dessus de $\mathfrak{p}$, les quotients $\mathfrak{M}/\mathfrak{P}$ et $\mathfrak{M}/\mathfrak{P}'$ sont isomorphes en tant que $\mathfrak{M}$-modules.

4. Concernant la définition (2), il conviendrait d'écrire "$\Lambda^v(\mathfrak{P})$" plutôt que "Λ^v"; cependant, si $\mathfrak{P}$ et $\mathfrak{P}'$ sont deux idéaux maximaux distincts au-dessus de $\mathfrak{p}$, correspondant résiduellement à deux idéaux maximaux $\mathfrak{P}/\mathfrak{p}\mathfrak{M}$ et $\mathfrak{P}'/\mathfrak{p}\mathfrak{M}$ de $\mathcal{M}_2(\mathbb{F}_q)$, il existe $u \in \mathfrak{M}$ tel que $\mathfrak{P}'/\mathfrak{p}\mathfrak{M} = \mathfrak{P}u/\mathfrak{p}\mathfrak{M}$. Ainsi $\Lambda^v(\mathfrak{P}) = \Lambda^{\overline{u}v}(\mathfrak{P}')$, et l'ensemble des sous-réseaux $\Lambda^v(\mathfrak{P})$ est en bijection avec l'ensemble des sous-réseaux $\Lambda^{v'}(\mathfrak{P}')$.

2.1.2. Proposition. *Soient Λ un $\mathfrak{M}$-réseau unimodulaire de H^m (i.e. $\Lambda = \Lambda^\#$), $\mathfrak{p}$ un idéal premier de $\mathcal{O}_K$ et $\mathfrak{P}$ un idéal maximal (à gauche) de $\mathfrak{M}$ au-dessus de $\mathfrak{p}$.*

(1) *Si v appartient à $\Lambda \setminus \overline{\mathfrak{P}}\Lambda$ et vérifie $h(v,v) \in \mathfrak{p}$, Λ et Λ_v sont $\mathfrak{p}\mathfrak{M}$-voisins.*

(2) *Si M est un sous-$\mathfrak{M}$-module de Λ tel que $\Lambda/M \simeq \mathfrak{M}/\mathfrak{P}$, il existe $v \in \Lambda \setminus \overline{\mathfrak{P}}\Lambda$ tel que $M = \Lambda^v$. En particulier, tous les $\mathfrak{p}\mathfrak{M}$-voisins de Λ s'obtiennent comme Λ_v pour un $v \in \Lambda \setminus \overline{\mathfrak{P}}\Lambda$ convenable.*

(3) *Si v appartient à $\Lambda \setminus \overline{\mathfrak{P}}\Lambda$, les voisins de Λ au-dessus de Λ^v (i.e. dont l'intersection avec Λ est égale à Λ^v) sont au nombre de q ($q = N_{K/\mathbb{Q}}(\mathfrak{p})$).*

Démonstration. (1) Il est clair que l'homomorphisme

$$\Lambda \to \mathfrak{M}/\mathfrak{P}, \qquad x \mapsto h(x,v) \bmod \mathfrak{P},$$

induit un isomorphisme de Λ/Λ^v sur $\mathfrak{M}/\mathfrak{P}$. Par ailleurs, si l'on note C_v l'idéal à gauche défini par $C_v = \{\alpha \in \overline{\mathfrak{P}}^{-1} \mid \alpha v \in \Lambda^v\}$, le quotient Λ_v/Λ^v est canoniquement plongé dans $\overline{\mathfrak{P}}^{-1}/C_v$. Comme v appartient à Λ^v (puisque $h(v,v) \in \mathfrak{p}$), on a les inclusions $\mathfrak{M} \subset C_v \subset \overline{\mathfrak{P}}^{-1}$. Or le quotient $\overline{\mathfrak{P}}^{-1}/\mathfrak{M} = \mathfrak{p}^{-1}\mathfrak{P}/\mathfrak{M} \simeq \mathfrak{M}/\mathfrak{P}$ est simple et comme v n'appartient pas à $\overline{\mathfrak{P}}\Lambda$, on conclut que $C_v = \mathfrak{M}$. Donc $\Lambda_v/\Lambda^v \simeq \overline{\mathfrak{P}}^{-1}/\mathfrak{M} \simeq \mathfrak{M}/\mathfrak{P}$ et Λ et Λ_v sont voisins.

(2) Soit M vérifiant les conditions de (2) : l'annulateur du quotient $M^\#/\Lambda$ est un idéal *bilatèral* distinct de $\mathfrak{M}$ qui contient $\mathfrak{p}\mathfrak{M}$ puisque $M^\#/\Lambda \simeq \Lambda/M \simeq \mathfrak{M}/\mathfrak{P}$, donc

$$M^\# \cap \mathfrak{p}^{-1}\Lambda = M^\# \not\subset \Lambda.$$

Si $\mathfrak{P}'$ est un idéal maximal au-dessus de $\mathfrak{p}$ distinct de $\mathfrak{P}$, on a $\mathfrak{P} + \mathfrak{P}' = \mathfrak{M}$, d'où

$$\overline{\mathfrak{P}}^{-1} + \overline{\mathfrak{P}'}^{-1} = \mathfrak{p}^{-1}\mathfrak{P} + \mathfrak{p}^{-1}\mathfrak{P}' = \mathfrak{p}^{-1}\mathfrak{M},$$

donc

$$M^{\#} \cap \overline{\mathfrak{P}}^{-1}\Lambda \not\subset \Lambda \quad \text{ou} \quad M^{\#} \cap \overline{\mathfrak{P}'}^{-1}\Lambda \not\subset \Lambda.$$

Or il est facile de voir, par un argument résiduel analogue à celui de la remarque suivant la définition 2.1.1, que $M^{\#} \cap \overline{\mathfrak{P}}^{-1}\Lambda \not\subset \Lambda$ si et seulement si $M^{\#} \cap \overline{\mathfrak{P}'}^{-1}\Lambda \not\subset \Lambda$. Soit donc $v \in (\overline{\mathfrak{P}}M^{\#} \cap \Lambda) \setminus \overline{\mathfrak{P}}\Lambda$; en particulier, v appartient à $\Lambda \setminus \overline{\mathfrak{P}}\Lambda$ et l'homomorphisme

$$h_v : \Lambda/M \to \mathfrak{M}/\mathfrak{P}, \quad x \mapsto h(x,v) \bmod \mathfrak{P},$$

est non nul. Or $\mathfrak{M}/\mathfrak{P}$ est un $\mathfrak{M}$-module simple, donc h_v est un isomorphisme et $M = \Lambda^v$. En particulier, si Λ' est un $\mathfrak{p}\mathfrak{M}$-voisin de Λ, l'annulateur de $\Lambda/\Lambda \cap \Lambda'$ est égal à $\mathfrak{p}\mathfrak{M}$, donc par un raisonnement analogue au précédent on montre que $\overline{\mathfrak{P}}\Lambda' \cap \Lambda \not\subset \overline{\mathfrak{P}}\Lambda$ et $\Lambda' = \Lambda_z$ pour tout $z \in (\overline{\mathfrak{P}}\Lambda' \cap \Lambda) \setminus \overline{\mathfrak{P}}\Lambda$.

(3) Les voisins de Λ au-dessus de Λ^v correspondent à des sous-modules simples de $(\Lambda^v)^{\#}/\Lambda^v = (\Lambda + \overline{\mathfrak{P}}^{-1}v)/\Lambda^v$. Ils s'écrivent donc sous la forme $\Lambda^v + \mathfrak{M}y$, où y appartient à $(\Lambda^v)^{\#} \cap \overline{\mathfrak{P}}^{-1}v \setminus \Lambda^v$. Inversement, on vérifie facilement que tout élément de cette forme vérifie $h(y,y) \in \mathfrak{M}$ et définit donc un $\mathfrak{M}$-réseau entier. Il y a donc une bijection entre l'ensemble constitué de Λ et de ses voisins au-dessus de Λ^v et l'ensemble des sous-modules simples de $(\Lambda^v)^{\#}/\Lambda^v$. Par ailleurs, il est clair que le quotient $(\Lambda^v)^{\#}/\Lambda^v$ est d'ordre q^4, qu'il est annulé par $\mathfrak{p}\mathfrak{M}$ et donc qu'il est isomorphe à $\mathcal{M}_2(\mathbb{F}_q)$. La caractérisation des idéaux maximaux de $\mathcal{M}_2(\mathbb{F}_q)$ rappelée précédemment permet alors de conclure. ∎

3. Classification. On se place désormais dans le cas où $K = \mathbb{Q}(\sqrt{5})$ et où $H = K_{\{-1,-1\}}$ dans les notations classiques (cf. [V], p. 3). Explicitement, H est la K-algèbre engendrée sur K par les éléments i, j, k vérifiant les relations

$$i^2 = j^2 = -1 \quad \text{et} \quad ij = -ji = k.$$

L'anneau des entiers $\mathcal{O}_K$ est égal à $\mathbb{Z}[\tau]$, où $\tau = (1+\sqrt{5})/2$. On note U_K (respectivement U_K^+) l'ensemble des unités de $\mathcal{O}_K$ (respectivement l'ensemble des unités totalement positives). Un générateur totalement positif de la différente $\mathcal{D}_{K/\mathbb{Q}}$ est fourni dans ce cas par $\alpha = (5+\sqrt{5})/2$.

Les symboles $\perp$ et $\perp_h$ désignent respectivement les sommes directes orthogonales au sens du produit scalaire S et au sens de la forme hermitienne h. On désigne par h-isométries les H-endomorphismes f de H^m conservant la forme hermitienne h, i.e. tels que $\forall (x,y) \in (H^m)^2$, $h(f(x), f(y)) = h(x,y)$, et l'on note $\mathrm{Aut}(L,h)$ l'ensemble des h-isométries stabilisant un $\mathfrak{M}$-réseau L donné.

On rappelle ci-dessous un lemme classique (cf. par exemple [O'M, 82.15]) qui sera d'usage constant dans la suite.

3.1. Lemme. *Si L est un $\mathfrak{M}$-réseau de rang m et M un sous-$\mathfrak{M}$-réseau unimodulaire de L de rang inférieur ou égal à m, vérifiant $h(M,L) \subset \mathfrak{M}$, alors L est h-factorisable par M, i.e. il existe un sous-$\mathfrak{M}$-réseau M' de L tel que*

$$L = M \perp_h M'.$$

Démonstration. La forme hermitienne h étant non dégénérée, l'espace H^m se décompose sous la forme

$$H^m = HM \perp_h HM^\perp,$$

HM désignant le sous H-espace vectoriel engendré par M. Tout élément y de L s'écrit donc sous la forme

$$y = \lambda m + z \quad \text{où} \quad \lambda \in H,\ z \in HM^\perp.$$

On a alors $h(\lambda m, M) = h(y, M)$, qui est contenu dans $\mathfrak{M}$ par hypothèse. Or M est unimodulaire, donc λ appartient à $\mathfrak{M}$, d'où $L = M \perp_h (HM^\perp \cap L)$, et la conclusion. ∎

3.2. Lemme. (1) *Si L est un $\mathfrak{M}$-réseau entier de (H^m, S) de norme 2, un vecteur minimal u de L vérifie $h(u,u) \in U_K^+$.*

(2) *Si $m \geq 2$, tout $\mathfrak{M}$-réseau unimodulaire L de (H^m, S) de norme 2 est h-factorisable par un $\mathfrak{M}$-réseau isométrique à $\mathbb{E}_8$, i.e. il existe L_1 de rang 1 sur $\mathfrak{M}$ isométrique à $\mathbb{E}_8$, et L_2 de rang $(m-1)$, tels que $L = L_1 \perp_h L_2$.*

(3) *Tout $\mathfrak{M}$-réseau relatif L de (H^m, S) isométrique (sur $\mathbb{Z}$) à $\mathbb{E}_8$ est h-isométrique à $\mathfrak{M}$.*

(4) *Si L est un $\mathfrak{M}$-réseau unimodulaire de (H^m, S) de norme 4 et s'il existe un vecteur minimal u de L tel que $h(u,u) \in 2U_K$, alors L possède un $2\mathfrak{M}$-voisin h-réductible de la forme $L_v \simeq \mathbb{E}_8 \perp_h L'$.*

Démonstration. (1) Si u est un vecteur de L, $h(u,u)$ appartient à $\mathcal{O}_K$. On a donc $h(u,u) = a + b\tau$, $(a,b) \in \mathbb{Z}^2$, et, avec le choix de α précisé plus haut, $S(u,u) = 2\mathrm{Tr}_{K/\mathbb{Q}}(\alpha^{-1}h(u,u)) = 2a$. Si u est minimal on a alors $a = 1$ et la condition que $h(u,u)$ soit totalement positif implique que $h(u,u) = 1$ ou $1 + \tau = \tau^2$, d'où la conclusion.

(2) Soit $u \in L$ tel que $h(u,u)$ appartienne à U_K. Le sous-réseau de L (de rang 1) $L_1 = \mathfrak{M}u$ vérifie donc la relation $L_1 = (L_1)^\#$, et comme $h(L_1, L) \subset \mathfrak{M}$, ceci permet de conclure *via* le lemme 3.1 que $L = L_1 \perp_h L_2$. Par ailleurs, L_1 unimodulaire pair de rang 8 est nécessairement isométrique à $\mathbb{E}_8$ (cf. par exemple [S], pp. 94–95).

(3) D'après (1), il existe u appartenant à L tel que $h(u,u)$ appartienne à U_K. Comme de plus $h(u,u)$ est totalement positif, et puisque $U_K^+ = U_K^2$ lorsque $K = \mathbb{Q}(\sqrt{5})$, on peut se ramener à $h(u,u) = 1$. Par conséquent, le

réseau $\mathfrak{M}u$ qui est contenu *a priori* dans L, lui est égal puisque tous deux sont unimodulaires. En outre, il est clair que l'application :

$$L \to \mathfrak{M}, \qquad \lambda u \mapsto \lambda,$$

est une h-isométrie.

(4) Si u est un vecteur de norme 4 de L, on montre comme dans (1) que l'on a $h(u,u) = 2, 2\tau^2$ ou $2+\tau$ (ce dernier cas ne pouvant être exclu *a priori*). Soit $\mathfrak{P}$ un idéal maximal à gauche au-dessus de 2; dans le cas où u vérifie $h(u,u) \in 2U_K$, le réseau $L_1' = \overline{\mathfrak{P}}^{-1}u$ est unimodulaire (car $\overline{\mathfrak{P}}^{-1}\mathfrak{P}^{-1} = \frac{1}{2}\mathfrak{M}$), moyennant quoi le lemme 3.1 permet de conclure que le $2\mathfrak{M}$-voisin Λ_u est h-réductible. ∎

3.3. Proposition. *Le réseau* $(\mathbb{E}_8)^m$ (*somme h-orthogonale de m copies de* $\mathbb{E}_8$) *admet, à h-isométrie près, un unique* $2\mathfrak{M}$*-voisin irréductible* V_m (*ses autres* $2\mathfrak{M}$*-voisins étant h-factorisables par un* $\mathfrak{M}$*-réseau isométrique à* $\mathbb{E}_8$).

Démonstration. D'après le lemme 3.2(3), le problème se ramène à étudier les $2\mathfrak{M}$-voisins de $\Lambda = \mathfrak{M}^m$. On considère donc un élément $v = (v_1, \ldots, v_m)$ de $\Lambda \setminus \overline{\mathfrak{P}}\Lambda$. Si l'on note $\widetilde{v}$ la classe de v modulo $\overline{\mathfrak{P}}\Lambda$ et si v' est un élément de $\Lambda \setminus \overline{\mathfrak{P}}\Lambda$ tel que $\widetilde{v'}$ soit dans l'orbite de $\widetilde{v}$ sous l'action de $\mathrm{Aut}(\Lambda, h)$, $\Lambda^{v'}$ est h-isométrique à Λ^v. S'il existe i tel que v_i appartienne à $\overline{\mathfrak{P}}$, alors $\mathfrak{M}\overline{v_i} \subset \mathfrak{P}$, donc Λ^v contient un sous-réseau (de rang 1) h-isométrique à $\mathbb{E}_8$, qui est facteur direct h-orthogonal de Λ_v (même argument que dans 3.2). Sinon, on utilise le fait que dans le cas où $K = \mathbb{Q}(\sqrt{5})$, tout élément de $\mathfrak{M} \setminus \overline{\mathfrak{P}}$ est congru modulo $\overline{\mathfrak{P}}$ à un élément de $\mathfrak{M}^1$: en effet, la surjection canonique $\mathfrak{M} \to \mathfrak{M}/2\mathfrak{M} \simeq M_2(\mathbb{F}_4)$ envoie surjectivement $\mathfrak{M}^1$ sur $Sl_2(\mathbb{F}_4)$ (cf. [V], p. 149), moyennant quoi il suffit de vérifier la propriété résiduellement, ce qui est trivial. On peut donc supposer que v_i appartient à $\mathfrak{M}^1$ pour tout i, puis se ramener à $v = (1, \ldots, 1)$ en multipliant (à droite) chaque composante par l'élément v_i^{-1} correspondant, ce qui définit bien un élément de $\mathrm{Aut}(\Lambda, h)$. Par conséquent, Λ^v est h-isométrique à

$$L = \Big\{(\lambda_i) \in \mathfrak{M}^m \;\Big|\; \sum \lambda_i \equiv 0 \bmod \mathfrak{P}\Big\},$$

dont le dual $L^\#$ est donné par $L^\# = \{(\lambda_i) \in (\overline{\mathfrak{P}}^{-1})^m \mid \lambda_1 \equiv \ldots \equiv \lambda_m \bmod \mathfrak{M}\}$.

D'après (2.1.2(3)), l'ensemble constitué de $\mathfrak{M}^m$ et de ses voisins entiers au-dessus de L est en bijection avec l'ensemble des sous-modules simples de $L^\#/L \simeq \mathfrak{M}/2\mathfrak{M} \simeq \mathcal{M}_2(\mathbb{F}_4)$, donc avec l'ensemble des idéaux maximaux de $\mathcal{M}_2(\mathbb{F}_4)$, eux-mêmes en bijection avec les points de la droite projective $\mathbb{P}_1(\mathbb{F}_4)$. Il y a donc quatre $\mathfrak{M}$-réseaux unimodulaires, en dehors de $\mathfrak{M}^m$ lui-même, au-dessus de L, parmi lesquels le réseau $V_m = (\mathfrak{M}^m)_v$ où $v = (1, \ldots, 1)$ si m est pair et $(e, 1, \ldots, 1)$ si m est impair, e désignant un relèvement d'un idempotent primitif de $\mathfrak{P}/2\mathfrak{M}$. Pour tout $\varrho \in H_0 =$

$\{\pm 1, \pm i, \pm j, \pm k\}$, l'application

$$f_\varrho : \mathfrak{M}^m \to \mathfrak{M}^m, \quad (x_1, \dots, x_m) \mapsto (x_1\varrho, \dots, x_m),$$

est une h-isométrie de $\mathfrak{M}^m$ qui stabilise L (car $\forall \varrho \in H_0$, $\varrho \equiv 1 \bmod \mathfrak{P}$) et qui agit par permutation sur l'ensemble des $\mathfrak{M}$-réseaux unimodulaires au-dessus de L. On a vu que cet ensemble s'identifie à $\mathbb{P}_1(\mathbb{F}_4)$ et l'on vérifie facilement que, via cette identification, l'application f associant f_ϱ à ϱ induit un homomorphisme de H_0 dans $\mathrm{Aut}(\mathbb{P}_1(\mathbb{F}_4)) \simeq A_5$, de noyau $\{\pm 1\}$ (plus précisément, il est facile de voir que si ϱ induit une permutation triviale, alors $\varrho \equiv 1 \bmod 2\mathfrak{M}$, d'où $\varrho = \pm 1$). Qui plus est, $f(H_0)$ est un sous-groupe d'ordre 4 de l'ensemble des permutations paires sur 5 lettres fixant une lettre commune (car $f_\varrho(\mathfrak{M}^m) = \mathfrak{M}^m$). Il est alors clair que $f(H_0)$ agit transitivement sur les 4 lettres non fixées, et donc les 4 voisins de $\mathfrak{M}^m$ au-dessus de L sont h-isométriques à V_m. ∎

On peut donner une description plus explicite de V_m, à savoir :

(1) si m est pair,

$$V_m = \Big\{(\lambda_1, \dots, \lambda_m) \in (\overline{\mathfrak{P}}^{-1})^m \;\Big|\; \lambda_i - \lambda_1 \in \mathfrak{M}\ \forall i \ \text{ et } \ \sum \lambda_i \equiv 0 \bmod \mathfrak{P}\Big\},$$

(2) si m est impair,

$$V_m = \Big\{(\lambda_1, \dots, \lambda_m) \in (\overline{\mathfrak{P}}^{-1})^m \;\Big|\; \lambda_i - \lambda_1 \in \mathfrak{M}\ \forall i \ \text{ et } \ \sum \lambda_i \in \mathfrak{P}\frac{e}{2}\Big\}.$$

Remarque. Le réseau V_m apparaissant dans l'énoncé précédent n'est autre, à normalisation près, que le réseau U_{8m} de Martinet, dont on rappelle la définition ci-dessous :

3.4. Définition et Théorème ([M]). *Soient $\mathfrak{P}$ et $\mathfrak{P}'$ deux idéaux maximaux (à gauche) de $\mathfrak{M}$ au-dessus de 2. On pose $n = 8m$; pour $m \geq 3$, le $\mathfrak{M}$-module*

$$\begin{aligned} U_n &= U_n[\mathfrak{P}', \mathfrak{P}] \\ &= \Big\{(\lambda_1, \dots, \lambda_m) \in \mathfrak{M}^m \;\Big|\; \lambda_i \equiv \lambda_1 \bmod \mathfrak{P} \ \ \textit{et} \ \ \sum \lambda_i \equiv 0 \bmod \mathfrak{P}'\Big\}, \end{aligned}$$

muni de la forme quadratique définie positive

$$S(x, y) = \mathrm{Tr}_{K/\mathbb{Q}}(\alpha^{-1} h'(x, y)),$$

où $h'(x, y)$ désigne la forme hermitienne $h'(x, y) = \frac{1}{2}\sum x_i \overline{y}_i$, est un réseau unimodulaire pair de rang n, de norme 4.

Si l'on choisit pour e un générateur de norme réduite 2 de $\mathfrak{P}$ (qui existe toujours dans le cas où $K = \mathbb{Q}(\sqrt{5})$, puisque le nombre de classes de H est 1, cf. [V]), et si $\mathfrak{P}'$ est l'idéal $\mathfrak{M}\overline{e}$, on vérifie aisément que l'application

$$V_m \to U_n[\mathfrak{P}', \mathfrak{P}], \quad (x_1, \dots, x_m) \mapsto (x_1\overline{e}, \dots, x_m\overline{e}),$$

est une isométrie hermitienne de (V_m, h) sur (U_n, h') (qui fournit *a fortiori* une isométrie de $(V_m, \mathrm{Tr}_{K/\mathbb{Q}}(\alpha^{-1}h(\,,\,)))$ sur $(U_n, \mathrm{Tr}_{K/\mathbb{Q}}(\alpha^{-1}h'(\,,\,)))$, en tant que réseaux usuels sur $\mathbb{Z}$).

Il est à noter également qu'à h-isométrie près, $U_n[\mathfrak{P}, \mathfrak{P}']$ ne dépend pas du choix de $\mathfrak{P}$ et de $\mathfrak{P}'$ (cela provient du fait que, dans le cas où $K = \mathbb{Q}(\sqrt{5})$, les idéaux maximaux de $\mathcal{M}_2(\mathbb{F}_4)$ sont permutés transitivement par multiplication *à droite* par les unités de norme réduite 1).

On retrouve avec U_{24} (ou V_3) la construction du réseau de Leech donnée par Tits dans [T], et l'on a montré dans [C] que U_{32} (ou V_4) pouvait être identifié avec le réseau obtenu par "construction B" à partir du code de Reed–Muller $RM(2,5)$. ∎

On suppose désormais (ce qui ne restreint pas la généralité) que l'ordre maximal $\mathfrak{M}$ considéré est l'ordre

$$\mathbb{Z}[\tau]\left(1, i, \omega, \frac{i + \tau j + (1-\tau)k}{2}\right) \quad \text{où } \omega = \frac{-1 + i + j + k}{2},$$

et l'on choisit pour $\mathfrak{P}$ l'idéal principal engendré par $e = \omega + \tau$, c'est-à-dire $\mathfrak{P} = \mathfrak{M}e$ que l'on peut encore écrire $\mathfrak{P} = \mathfrak{M}(1+i)$. On pose

$$e_1 = (e, 0, 0), \quad e_2 = (0, e, 0), \quad e_3 = (0, 0, e).$$

Rappelons (3.2(4)) que les vecteurs minimaux du réseau V_3 sont de deux types :

• d'une part, les x vérifiant $h(x,x) = 2$ (type 1) ou $h(x,x) = 2\tau^2$ (qui s'obtiennent en multipliant les précédents par τ),

• d'autre part, les x vérifiant $h(x,x) = 2 + \tau$ (type 2).

(*N.B.* Dans [T], la description des vecteurs minimaux est donnée pour le réseau U_{24}, et les valeurs de $h(x,x)$ correspondantes sont donc $4, 4\tau^2, 4+2\tau$ et non $2, 2\tau^2, 2+\tau$. Dans toute la suite, les références à [T] seront donc à comprendre *modulo* cette renormalisation.)

La proposition et les deux lemmes suivants permettent de déterminer, à h-isométrie près, les $2\mathfrak{M}$-voisins du réseau V_3. La proposition 3.5 est l'analogue, pour les vecteurs minimaux de type 2, d'un résultat établi par Tits pour les vecteurs minimaux de type 1 (cf. [T], 6.3, Corollary 8, où le terme "short vectors" désigne ce que nous appelons ici "vecteurs minimaux de type 1").

3.5. Proposition. *Le groupe $G = \mathrm{Aut}(V_3, h)$ agit transitivement sur les vecteurs minimaux de type* 2.

Démonstration. On sait depuis Tits ([T]) que G est isomorphe au revêtement double $\widetilde{J}_2$ du groupe sporadique de Hall–Janko. Son action sur V_3 définit une représentation irréductible ϱ de degré 6 sur $\mathbb{C}$ (ou, ce qui revient au même, sur n'importe quelle extension quadratique totalement imaginaire

de $\mathbb{Q}(\sqrt{5})$), dont le caractère χ est donné par l'ATLAS ([A], ligne 22). Dans la suite on notera V le $\mathbb{Q}$-espace vectoriel $\mathbb{Q}V_3$. Comme $\#G = 2^8 \cdot 3^3 \cdot 5^2 \cdot 7$ et comme il y a $120960 = 2^7 \cdot 3^3 \cdot 5 \cdot 7$ vecteurs minimaux de type 2, tout revient à montrer que le stabilisateur G_x de l'un quelconque de ces vecteurs est d'ordre 10. On choisit par exemple le vecteur

$$x = (0, \tau, \omega).$$

On remarque tout d'abord que 7 ne divise pas $\#G_x$; en effet, si σ est un élément d'ordre 7 appartenant à G_x, son polynôme minimal sur $\mathbb{Q}(\sqrt{5})$ est $(X-1)\Phi_7(X)$. Le sous-espace $\ker(\sigma - 1)$ est de dimension multiple de 4 sur $\mathbb{Q}(\sqrt{5})$ (car stable par H) et $\ker \Phi_7(\sigma)$ est de dimension multiple de 6. Comme $V = \ker(\sigma - 1) \perp \ker \Phi_7(\sigma)$, ce qui précède est incompatible avec le fait que V soit de dimension 12 sur $\mathbb{Q}(\sqrt{5})$.

De même, 3 ne divise pas $\#G_x$. En effet, l'ATLAS montre qu'il y a 2 classes de conjugaison σ_1 et σ_2 d'éléments d'ordre 3 dans G, caractérisées respectivement par $\chi(\sigma_1) = -3$ et $\chi(\sigma_2) = 0$. On voit facilement que les éléments d'ordre 3 de G admettant 1 pour valeur propre sont conjugués à σ_2, donc en particulier, tout élément σ d'ordre 3 de G_x est conjugué à l'élément γ de G qui à $x = (x_1, x_2, x_3)$ associe $\gamma(x) = (x_3, x_1, x_2)$. Il est clair que si un élément σ de $\mathrm{Aut}(V_3, h)$ stabilise au moins un vecteur minimal de type 2, il en va de même de chacun de ses conjugués ($\sigma x = x$ implique $\eta\sigma\eta^{-1}(\eta x) = \eta x$). Or, si $y = (y_1, y_2, y_3)$ est stabilisé par l'automorphisme γ défini ci-dessus, on a $y_1 = y_2 = y_3$, moyennant quoi $h(y, y)$ appartient à $3\mathcal{O}_K$, ce qui exclut $h(y, y) = 2 + \tau$.

Montrons ensuite que les 2-sous-groupes de Sylow de G_x sont cycliques d'ordre 2. Il est clair que l'élément σ_0 défini par $\sigma_0(y_1, y_2, y_3) = (-y_1, y_2, y_3)$ appartient à G_x. De plus, tous les éléments d'ordre 2 de G_x sont conjugués, et ont pour trace 2 : on vérifie en effet en consultant l'ATLAS qu'il y a dans G deux classes de conjugaison γ_1 et γ_2 d'éléments d'ordre 2, caractérisées respectivement par $\chi(\gamma_1) = 2$ et $\chi(\gamma_2) = -2$; l'élément μ défini par $\mu(y_1, y_2, y_3) = (-y_1, y_3, y_2)$ appartient à la deuxième classe, et il ne peut stabiliser aucun vecteur minimal de type 2 (si $\mu(y) = y$, alors $y_1 = 0$ et $y_2 = y_3$, donc $h(y, y)$ appartient à $2\mathcal{O}_K$, ce qui exclut que $h(y, y) = 2 + \tau$). Les carrés des éléments d'ordre 4 de G n'ayant pas pour trace 2 (cf. ATLAS), on en conclut que G_x ne contient pas d'élément d'ordre 4, ni d'élément d'ordre 8. Comme G ne contient pas d'élément d'ordre 2^k pour $k > 3$, on en conclut que les 2-Sylow de G_x sont d'exposant 2, donc en particulier abéliens. Les éléments d'ordre 2 de G_x étant conjugués, ils ont le même polynôme caractéristique sur $\mathbb{C}$, à savoir $(X-1)^4(X+1)^2$. Plus précisément, si s est un élément d'ordre 2 de G_x, on a une décomposition $V = \ker(s-1) \perp_h \ker(s+1)$ en deux sous-espaces h-orthogonaux de dimensions respectives 2 et 1 sur H, et le sous-espace $\ker(s + 1)$ détermine entièrement s. Si s et t sont deux

éléments d'ordre 2 d'un même 2-Sylow, on a $st = ts$. Posons $\ker(s+1) = Hy$; on a alors, puisque s et t commutent, $t(y) = y$ ou $t(y) = -y$. Le premier cas entraîne que $st(y) = -y$ donc $st = s$, ce qui est absurde, et le deuxième que $s = t$. Les 2-Sylow de G_x sont donc d'ordre 2.

Enfin, il est clair que 5 divise l'ordre de G_x (sinon, l'orbite de x sous G serait de cardinal > 120960). Il reste donc à montrer que 5^2 ne divise pas $\#G_x$. Sinon, G_x contiendrait un 5-Sylow G' de G, de type $\mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ (car G ne contient pas d'élément d'ordre 25). Soit χ' le caractère de la restriction ϱ' de ϱ à G'. Si l'on pose $\nu = \tau - 1 = 2\cos\frac{2\pi}{5}$ et $\nu' = -1 - \nu$ son conjugué (sur $\mathbb{Q}$), on constate (cf. ATLAS, ligne 22) que les valeurs prises par χ sur les éléments d'ordre 5 sont -2ν, $\nu - 1$, $-2\nu'$, $\nu' - 1$. En particulier, χ' prend ses valeurs dans $\mathbb{Q}(\sqrt{5})$, ce qui implique, puisque G' est commutatif, que ϱ' est réalisable sur $\mathbb{Q}(\sqrt{5})$. Ainsi χ' se décompose sous la forme

$$\chi' = n_1 \cdot 1 + \sum_{(h,k) \not\equiv (0,0) \bmod 5} n_{h,k} \cdot \chi_{h,k},$$

où $\chi_{h,k}$ est le caractère de degré 2 sur $\mathbb{C}$ défini par

$$\chi_{h,k}(l,m) = 2\cos\frac{2(hl+km)\pi}{5}, \qquad \text{pour } (l,m) \in (\mathbb{Z}/5\mathbb{Z})^2.$$

De plus, $n_1 + 2\sum_{(h,k)} n_{h,k} = 6$, et n_1 est pair, le sous $\mathbb{Q}(\sqrt{5}, i)$-espace vectoriel stable (point par point) par G' étant un H-espace vectoriel. Si l'on fait l'hypothèse que $G' \subset G_x$, alors n_1 est non nul, i.e. $n_1 = 2$ ou 4. Si $n_1 = 4$ alors $\chi' = 4 \cdot 1 + \chi_{h,k}$ avec mettons $h \not\equiv 0 \bmod 5$, moyennant quoi, si l'on choisit l tel que $lh \equiv 1 \bmod 5$ on a $\chi'(l,0) = 4 + \nu$. Or $4 + \nu$ n'appartient pas à l'ensemble précédemment cité des valeurs prises par χ sur les éléments d'ordre 5. Donc $n_1 = 2$, ce qui conduit à deux possibilités :

• Soit $\chi' = 2 \cdot 1 + 2\chi_{h,k}$, avec par exemple $h \not\equiv 0 \bmod 5$, et en choisissant $(l,m) \not\equiv (0,0) \bmod 5$ tels que $hl + km \equiv 0 \bmod 5$, on obtient $\chi'(l,m) = 4 + 2 = 6$, ce qui est absurde, par le même type d'arguments que dans le cas précédent.

• Soit $\chi' = 2 \cdot 1 + \chi_{h_0,k_0} + \chi_{h_1,k_1}$, avec $(h_0,k_0) \not\equiv (h_1,k_1) \not\equiv (0,0) \bmod 5$. Pour un choix convenable de (l,m) on a $h_0 l + k_0 m \not\equiv h_1 l + k_1 m$, d'où $\chi'(l,m) = 2 + \nu + \nu'$, $2 + 2 + \nu$ ou $2 + 2 + \nu'$ ce qui conduit à nouveau à une contradiction, aucun de ces trois nombres n'appartenant à l'ensemble des valeurs permises.

Donc $G' \not\subset G_x$, ce qui achève la démonstration de la proposition. ∎

Le lemme suivant donne une description du quotient $V_3/\overline{\mathfrak{P}}V_3$ qui sera utile pour déterminer les $2\mathfrak{M}$-voisins de V_3.

3.6. Lemme. (1) *Chaque classe non nulle de $V_3/\overline{\mathfrak{P}}V_3$ contient exactement* 24 *couples $\{\pm x\}$ de vecteurs minimaux deux à deux orthogonaux.*

(2) *Il y a exactement* 1575 *classes représentées par des vecteurs de type* 1, *les* 2520 *classes restantes étant représentées par des vecteurs de type* 2.

Démonstration. (1) Le sous-réseau $\overline{\mathfrak{P}}V_3$ étant de norme au moins 8 (car $\mathfrak{P}\overline{\mathfrak{P}} = 2\mathfrak{M}$) et $V_3/\overline{\mathfrak{P}}V_3$ étant d'exposant 2, si deux vecteurs minimaux de V_3 sont dans la même classe modulo $\overline{\mathfrak{P}}V_3$, ils vérifient

$$8 \leq N(x \pm y) = 4 + 4 \pm 2S(x, y),$$

donc $S(x, y) = 0$. Chaque classe non nulle contient donc *au plus* 24 couples $\{\pm x\}$ de vecteurs minimaux deux à deux orthogonaux. Or, le nombre total de couples $\{\pm x\}$ de vecteurs minimaux du réseau de Leech est $s = 98280$, et $\frac{s}{24} + 1 = 2^{12} = (V_3 : \overline{\mathfrak{P}}V_3)$. Cela prouve que chacune des classes non nulles contient *exactement* 24 couples de vecteurs minimaux deux à deux orthogonaux.

(2) Le groupe $G = \mathrm{Aut}(V_3, h)$ étant transitif sur les $315 \cdot 120 = 24 \cdot 1575$ vecteurs minimaux de type 1 (cf. [T], 6.3, Corollary 8), il suffit de vérifier que la classe de l'un quelconque d'entre eux, par exemple $e_1 = (e, 0, 0)$, contient exactement 24 vecteurs de type 1. Si $y = (y_1, y_2, y_3)$ est un vecteur de type 1, la condition que y appartienne à la classe de e_1 modulo $\overline{\mathfrak{P}}V_3$ implique

$$\begin{cases} y_i \in \mathfrak{M} & \text{pour } i = 1, 2, 3, \\ y_i - y_j \in \overline{\mathfrak{P}} & \text{pour } i, j = 1, 2, 3. \end{cases}$$

La condition que y soit un vecteur de norme 4, ajoutée à la condition que y_i appartienne à $\mathfrak{M}$, implique que l'un des y_i est nul (puisque $\mathfrak{M} \simeq \mathbb{E}_8$ en tant que réseau sur $\mathbb{Z}$), d'où finalement y_i appartient à $\overline{\mathfrak{P}}$ $\forall i$, *via* la deuxième condition. Il est alors clair que les vecteurs minimaux de type 1 équivalents à e_1 modulo $\overline{\mathfrak{P}}V_3$ sont les 24 éléments αe_i, $\alpha \in \{\pm 1, \pm i, \pm j, \pm k\} = H_0$, d'où la première partie de l'assertion (2). Noter par ailleurs que pour tout vecteur minimal x de type 1, τx est équivalent à $\omega^2 x$ modulo $\overline{\mathfrak{P}}V_3$. Les $2520 = (V_3 : \overline{\mathfrak{P}}V_3) - 1 - 1575$ classes non nulles restantes contiennent donc chacune exactement 48 vecteurs minimaux, nécessairement de type 2. ∎

De façon tout à fait analogue, on montre le lemme suivant :

3.7. Lemme. *Soit* $\mathfrak{Q}$ *un idéal maximal (à gauche) de* $\mathfrak{M}$ *au-dessus de* $\mathfrak{q} = \sqrt{5}\mathcal{O}_K$. *Alors les* $25^3 - 1$ *classes non nulles de* $V_3/\overline{\mathfrak{Q}}V_3$ *se répartissent en* 7560 *classes représentées par des vecteurs minimaux de type* 1 *et* 8064 *par des vecteurs minimaux de type* 2.

On est maintenant en mesure d'énoncer le résultat principal :

3.8. Théorème. *On pose* $n = 8m$. *La classification complète, à h-isométrie près, des* $\mathfrak{M}$*-réseaux unimodulaires de* (H^m, S) *de dimension* $n \leq 32$ *s'établit de la façon suivante* :

(1) $n = 8 : \mathbb{E}_8$.

(2) $n = 16 : \mathbb{E}_8 \perp_h \mathbb{E}_8$.

(3) $n = 24 : \mathbb{E}_8 \perp_h \mathbb{E}_8 \perp_h \mathbb{E}_8$ *et le réseau* V_3 *qui est isométrique, en tant que réseau sur* $\mathbb{Z}$*, au réseau de Leech* Λ_{24}.

(4) $n = 32 : \mathbb{E}_8 \perp_h \mathbb{E}_8 \perp_h \mathbb{E}_8 \perp_h \mathbb{E}_8$, $\mathbb{E}_8 \perp_h V_3$, V_4 *et un réseau h-irréductible (non h-isométrique à* V_4*) noté* C_{32} .

Démonstration. (1) Pour $n = 8$: puisqu'un $\mathfrak{M}$-réseau entier est automatiquement pair, le seul $\mathfrak{M}$-réseau unimodulaire de (H, S) est $\mathbb{E}_8$, dont $(\mathfrak{M}, S)$ est la seule réalisation à h-isométrie près d'après 3.2(3).

(2) Pour $n = 16$: les deux seules possibilités sont *a priori* $\mathbb{E}_8 \perp \mathbb{E}_8$ et $\mathbb{D}_{16}^+$. Ces deux réseaux étant de norme 2, on conclut par le lemme 3.2(2) que $\mathbb{D}_{16}^+$ est exclu, et que la seule réalisation à h-isométrie près de $\mathbb{E}_8 \perp \mathbb{E}_8$ est $(\mathfrak{M}^2, S) \simeq \mathbb{E}_8 \perp_h \mathbb{E}_8$.

(3) Pour $n = 24$: d'après le lemme 3.2(2), les $\mathfrak{M}$-réseaux unimodulaires de (H^m, S) de norme 2 sont h-réductibles, moyennant quoi l'on est ramené à la dimension 16. Dans le cas de la norme 4, il reste donc à vérifier que tout $\mathfrak{M}$-réseau unimodulaire isométrique (sur $\mathbb{Z}$) au réseau de Leech est h-isométrique à V_3. Si Λ est un tel réseau, on suppose dans un premier temps qu'il contient au moins un vecteur minimal de type 1 (i.e. $h(x, x) = 2$). Alors, par 3.2(4), Λ possède un $2\mathfrak{M}$-voisin h-factorisable par $\mathbb{E}_8$ qui ne peut être (vu la classification en dimension 16) que $\mathbb{E}_8 \perp_h \mathbb{E}_8 \perp_h \mathbb{E}_8$. Or le seul $2\mathfrak{M}$-voisin irréductible de ce dernier est précisément (à h-isométrie près) le réseau V_3 (cf. 3.3). Il reste à prouver que l'hypothèse d'existence d'un vecteur minimal de type 1 est toujours vérifiée; on suppose par l'absurde qu'il existe Λ de norme 4 ne possédant que des vecteurs minimaux de type 2 (i.e. $h(x, x) = 2 + \tau$). Si x est un vecteur minimal de Λ et $\mathfrak{Q}$ un idéal maximal à gauche de $\mathfrak{M}$ au-dessus de $\sqrt{5}\mathcal{O}_K$, on démontre (de la même façon que pour 3.2(4)) que le $\sqrt{5}\mathfrak{M}$-voisin $\Lambda_x = L^x + \overline{\mathfrak{Q}}^{-1}x$ de Λ est h-factorisable par $\mathbb{E}_8$: il est donc isométrique à $(\mathbb{E}_8)^3$ d'après la classification en dimension 16. Inversement, on démontre comme dans 3.2(2) (l'argument principal étant que la surjection canonique de $\mathfrak{M}$ sur $\mathfrak{M}/\sqrt{5}\mathfrak{M} \simeq \mathcal{M}_2(\mathbb{F}_5)$ induit une surjection de $\mathfrak{M}^1$ sur $Sl_2(\mathbb{F}_5)$), que $(\mathbb{E}_8)^3$ possède (à h-isométrie près) un unique $\sqrt{5}\mathfrak{M}$-voisin h-irréductible (obtenu *via* le vecteur $v = (1, 1, 1)$) et que ce dernier contient des vecteurs minimaux de type 1. Donc Λ contient des vecteurs minimaux de type 1.

(4) Pour $n = 32$: le cas des $\mathfrak{M}$-réseaux unimodulaires de norme 2 se ramène à la dimension 24 *via* le lemme 3.2(2). Soit donc Λ un $\mathfrak{M}$-réseau unimodulaire de norme 4, que l'on peut de plus supposer h-irréductible. Comme précédemment, on suppose dans un premier temps que Λ contient un vecteur minimal de type 1. En appliquant le lemme 3.2(4), on en déduit que Λ possède un $2\mathfrak{M}$-voisin M h-factorisable par $\mathbb{E}_8$. Si $M \simeq (\mathbb{E}_8)^4$ on conclut

par la proposition 3.3 que Λ est h-isométrique à V_4. Sinon, $M \simeq \mathbb{E}_8 \perp_h \Lambda_{24}$ c'est-à-dire $M \simeq \mathfrak{M} \perp_h V_3$. On a donc $\Lambda = M_{v_1+v_2}$ avec $v_1 \in \mathfrak{M} \setminus \overline{\mathfrak{P}}$, $v_2 \in V_3 \setminus \overline{\mathfrak{P}}V_3$. Or, d'après le lemme 3.6, il existe $v_2' \in V_3$ congru à v_2 modulo $\overline{\mathfrak{P}}V_3$, et tel que $h(v_2', v_2') = 2$ ou $2+\tau$:

• Dans le premier cas (i.e. $h(v_2', v_2') = 2$), $M^{v_1+v_2} + \overline{\mathfrak{P}}^{-1}v_2'$ est un $2\mathfrak{M}$-voisin unimodulaire de M et de Λ, qui est de plus h-factorisable par $\mathbb{E}_8$ (puisque $\overline{\mathfrak{P}}^{-1}v_2'$ est unimodulaire, donc isométrique à $\mathbb{E}_8$). Enfin, $M^{v_1+v_2} + \overline{\mathfrak{P}}^{-1}v_2' \supset (\mathbb{E}_8)^3$, donc $M^{v_1+v_2}+\overline{\mathfrak{P}}^{-1}v_2' \simeq (\mathbb{E}_8)^4$. Par suite, Λ est un $2\mathfrak{M}$-voisin de $\mathfrak{M}^4 \simeq (\mathbb{E}_8)^4$: puisqu'il est h-irréductible, ce ne peut être que V_4.

• Dans le second cas, le choix du vecteur v_2' tel que $h(v_2', v_2') = 2+\tau$ est indifférent à h-isométrie près, d'après la proposition 3.5, et l'on peut supposer par ailleurs que $v_1 = \tau^{-1}\omega^2$ (car $\tau^{-1}\omega^2 \equiv 1 \bmod \overline{\mathfrak{P}}$). Comme précédemment (3.3), l'ensemble constitué de M et de ses voisins entiers au-dessus de $M^{v_1+v_2'}$ est en bijection avec $\mathbb{P}_1(\mathbb{F}_4)$. Il y a donc quatre $\mathfrak{M}$-réseaux unimodulaires, en dehors de M lui-même, au-dessus de $M^{v_1+v_2'}$, parmi lesquels le réseau $C_{32} = M_{v_1+v_2'}$. Pour tout $\varrho \in H_0 = \{\pm 1, \pm i, \pm j, \pm k\}$, l'application

$$f_\varrho : M = \mathbb{E}_8 \perp V_3 \to \mathbb{E}_8 \perp V_3, \qquad x_1 + x_2 \mapsto x_1\varrho + x_2,$$

est une h-isométrie de M qui stabilise $M^{v_1+v_2'}$ (car $\forall \varrho \in H_0$, $\varrho \equiv 1 \bmod \mathfrak{P}$) et qui agit par permutation sur l'ensemble des $\mathfrak{M}$-réseaux unimodulaires au-dessus de $M^{v_1+v_2'}$. Comme dans 3.3, l'application f associant f_ϱ à ϱ induit un homomorphisme de H_0 dans $\mathrm{Aut}(\mathbb{P}_1(\mathbb{F}_4)) \simeq A_5$, de noyau $\{\pm 1\}$. Qui plus est, $f(H_0)$ est un sous-groupe d'ordre 4 de l'ensemble des permutations paires sur 5 lettres fixant une lettre commune (car $f_\varrho(M) = M$), d'où l'on déduit que $f(H_0)$ agit transitivement sur les 4 lettres non fixées, et donc les 4 voisins de M au-dessus de $M^{v_1+v_2'}$ sont h-isométriques à C_{32}.

Il reste à montrer que l'hypothèse d'existence d'un vecteur minimal de type 1 dans Λ est toujours vérifiée. On procède comme dans le cas de la dimension 24 et l'on montre que, *via* un vecteur minimal de type 2, et à h-isométrie près, Λ est $\sqrt{5}\mathfrak{M}$-voisin de $(\mathbb{E}_8)^4$ ou de $\mathbb{E}_8 \perp V_3$. Dans le premier cas, on constate (comme pour $(\mathbb{E}_8)^3$) qu'à h-isométrie près, $(\mathbb{E}_8)^4$ possède un seul $\sqrt{5}\mathfrak{M}$-voisin irréductible et que celui-ci contient des vecteurs minimaux de type 1. Dans le second cas, les $\sqrt{5}\mathfrak{M}$-voisins de $\mathbb{E}_8 \perp V_3$ s'obtiennent *via* un vecteur $v = v_1 + v_2$, où $v_1 \in \mathbb{E}_8$ et $v_2 \in V_3$; la proposition 3.5 et le lemme 3.7 permettent de choisir pour v_2 soit l'un (quelconque) des vecteurs minimaux de type 1, soit l'un des vecteurs de minimaux de type 2. On constate alors que $V_3^{v_2}$ (qui est contenu dans $(\mathbb{E}_8 \perp V_3)^{v_1+v_2}$) contient des vecteurs minimaux de type 1 (explicitement, on peut prendre dans le premier cas $v_2 = e_1 = (e, 0, 0)$ et dans le second $v_2 = (0, \omega, \tau)$ et dans les deux cas $V_3^{v_2}$ contient e_1). Donc tout $\sqrt{5}\mathfrak{M}$-voisin de $\mathbb{E}_8 \perp V_3$ contient des vecteurs minimaux de type 1.

Le raisonnement précédent prouve qu'il y a au plus deux $\mathfrak{M}$-réseaux unimodulaires irréductibles en dimension 32. Il reste à prouver que V_4 et C_{32} ne sont pas h-isométriques, ce qui se fait *via* la formule de masse suivante, due à Hashimoto :

THÉORÈME (Hashimoto, [H]). *Soit $\mathfrak{M}$ un ordre maximal de l'unique corps de quaternions sur $K = \mathbb{Q}(\sqrt{5})$ non ramifié aux places finies. Soient E_m l'ensemble des classes de h-isométrie de $\mathfrak{M}$-réseaux unimodulaires de rang m, et $M_m = \sum_{[L]\in E_m} 1/(\#\operatorname{Aut}(L,h))$. Alors,*

$$M_m = \frac{5^{m(2m+1)/2}}{(2\pi)^{2m(m+1)}} \prod_{k=1}^{m} (2k-1)!^2 \zeta_K(2k).$$

Pour $m = 4$, la "masse" restante une fois pris en compte les deux $\mathfrak{M}$-réseaux unimodulaires h-réductibles $(\mathbb{E}_8)^4$ et $\mathbb{E}_8 \perp_h \Lambda_{24}$ est

$$M_4 - \frac{1}{4!120^4} - \frac{1}{120\#\widetilde{J}_2} = \frac{67\cdot 19^2 - 7 - 2^4\cdot 3\cdot 5}{2^{15}\cdot 3^5\cdot 5^4\cdot 7} = \frac{19}{2^{13}\cdot 3^3\cdot 5^3},$$

ce qui prouve qu'il reste au moins deux classes de h-isométrie, d'où la conclusion. ∎

Bibliographie

[B] C. Bachoc, *Voisinages au sens de Kneser pour les réseaux hermitiens*, en préparation.

[A] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of Finite Groups*, Oxford Univ. Press, Oxford, 1985.

[C] R. Coulangeon, *Réseaux quaternioniens et invariant de Venkov*, à paraître.

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

[K] M. Kneser, *Klassenzahlen definiter quadratischer Formen*, Arch. Math. (Basel) 8 (1957), 241–250.

[M] J. Martinet, *Structures algébriques sur les réseaux*, Séminaire de Théorie des Nombres de Paris (1993), en préparation.

[Nie] H.-V. Niemeier, *Definite quadratischen Formen der Discriminante* 1 *und der Dimension* 24, J. Number Theory 5 (1973), 141–178.

[O'M] O. T. O'Meara, *Introduction to Quadratic Forms*, Grundlehren Math. Wiss. 117, Springer, Heidelberg, 1963.

[Q] H. G. Quebbemann, *An application of Siegel's formula over quaternions orders*, Mathematika 31 (1984), 12–16..

[S] J.-P. Serre, *Cours d'arithmétique*, PUF, Paris, 1970.

[Sie] C. L. Siegel, *Gesammelte Abhandlungen*, I n° 20 et III n° 79, Springer, 1966.

[T] J. Tits, *Quaternions over $\mathbb{Q}(\sqrt{5})$, Leech's lattice and the sporadic group of Hall–Janko*, J. Algebra 63 (1980), 56–75.

[V] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Math. 800, Springer, 1980.

MATHÉMATIQUES
UNIVERSITÉ BORDEAUX I
351, COURS DE LA LIBÉRATION
33405 TALENCE CEDEX, FRANCE

Reçu le 4.10.1993
et révisé le 28.10.1994 (2500)