Publications mathématiques de Besançon
Algèbre et théorie des nombres

Gaëtan Chenevier et Frédéric Paulin

Sur les minima des formes hamiltoniennes binaires définies positives

2020, p. 5-25.
<http://pmb.centre-mersenne.org/item?id=PMB_2020_____5_0>

Publication éditée par le laboratoire de mathématiques de Besançon, UMR 6623 CNRS/UFC

cedram

Article mis en ligne dans le cadre du Centre de diffusion des revues académiques de mathématiques
http://www.centre-mersenne.org/

Publications mathématiques de Besançon – 2020, 5-25

SUR LES MINIMA DES FORMES HAMILTONIENNES BINAIRES DÉFINIES POSITIVES

par

Gaëtan Chenevier et Frédéric Paulin

Résumé. — Étant donné un ordre maximal $\mathscr{O}$ d'une algèbre de quaternions rationnelle définie A de discriminant D_A, nous montrons que le minimum des formes hamiltoniennes binaires sur $\mathscr{O}$, définies positives et de discriminant -1, est $\sqrt{D_A}$. Lorsque la différente de $\mathscr{O}$ est principale, nous explicitons une forme atteignant cette valeur, et lorsque $\mathscr{O}$ est principal, nous donnons la liste exacte des formes atteignant cette valeur. Nous donnons des critères et des algorithmes pour déterminer quand la différente de $\mathscr{O}$ est principale.

Abstract. — (*On the minima of positive definite binary Hamiltonian forms*) Let A be a definite quaternion algebra over $\mathbb{Q}$, with discriminant D_A, and $\mathscr{O}$ a maximal order of A. We show that the minimum of the positive definite Hamiltonian binary forms over $\mathscr{O}$ with discrimiminant -1 is $\sqrt{D_A}$. When the different of $\mathscr{O}$ is principal, we provide an explicit form representing this minimum, and when $\mathscr{O}$ is principal, we give the list of the equivalence classes of all such forms. We also give criteria and algorithms to determine when the different of $\mathscr{O}$ is principal.

1. Introduction

Soit A une algèbre de quaternions sur $\mathbb{Q}$ qui est définie, de sorte que $\mathbb{H} = A \otimes_{\mathbb{Q}} \mathbb{R}$ soit l'algèbre des quaternions de Hamilton sur $\mathbb{R}$ usuelle. Nous noterons $x \mapsto \overline{x}$ la conjugaison, $\mathtt{n}$ la norme réduite, $\mathtt{tr}$ la trace réduite de $\mathbb{H}$, D_A le discriminant réduit de A, h_A son nombre de classes et t_A son nombre de classes de conjugaison d'ordres maximaux. Soit $\mathscr{O}$ un ordre maximal dans A. Rappelons que la *différente* de $\mathscr{O}$ est l'unique idéal à droite de $\mathscr{O}$ de norme (réduite) D_A, et qu'il est bilatère. Nous renvoyons par exemple à [22] pour les prérequis.
En utilisant la terminologie de [24], notons $\mathscr{Q}^+$ l'ensemble des *formes hamiltoniennes binaires*

$$f : (u, v) \mapsto a\,\mathtt{n}(u) + \mathtt{tr}(\overline{u}\,b\,v) + c\,\mathtt{n}(v)$$

(où $b, u, v \in \mathbb{H}$ et $a, c \in \mathbb{R}$) qui sont définies positives, ou de manière équivalente avec $a, c > 0$ et de *discriminant* $\Delta(f) = \mathtt{n}(b) - ac$ strictement négatif, et $\mathscr{Q}_1^+$ le sous-ensemble des $f \in \mathscr{Q}^+$ telles que $\Delta(f) = -1$. Définissons la *constante d'Hermite* $\gamma_2(\mathscr{O})$ *de l'ordre maximal* $\mathscr{O}$ par

$$\gamma_2(\mathscr{O}) = \sup_{f \in \mathscr{Q}^+} \min_{(u,v) \in \mathscr{O} \times \mathscr{O} - \{0\}} \frac{1}{\sqrt{-\Delta(f)}}\, f(u, v) = \sup_{f \in \mathscr{Q}_1^+} \min_{(u,v) \in \mathscr{O} \times \mathscr{O} - \{0\}} f(u, v)\ .$$

Classification Mathématique (2020). — 11E39, 11R52, 11L05, 16H20, 11E20.
Mots clefs. — Quaternion algebra, binary Hamiltonian form, maximal order, Euclidean lattice.

Si nous remplaçons $\mathscr{O}$ par $\mathbb{Z}$ et si f varie parmi les formes quadratiques binaires réelles définies positives, cette constante $\gamma_2 = \gamma_2(\mathbb{Z})$, appelée la constante d'Hermite binaire, vaut $\frac{2}{\sqrt{3}}$, et la description des formes f qui réalisent la borne supérieure est bien connue (voir par exemple [2, p. 332]). Nous renvoyons à [14] pour le cas où $\mathscr{O}$ est remplacé par l'anneau des entiers d'une extension quadratique imaginaire de $\mathbb{Q}$, quand f varie sur les formes hermitiennes binaires complexes définies positives (par exemple $\gamma_2(\mathbb{Z}[i]) = 2$).
Le résultat principal de cette note, généralisant le cas $D_A = 2$ traité par [20, Satz 4], est le suivant.

Théorème 1.1. — *Nous avons* $\gamma_2(\mathscr{O}) = \sqrt{D_A}$.

L'inégalité $\gamma_2(\mathscr{O}) \leq \sqrt{D_A}$ découlera assez facilement du calcul (voir [1]) de la constante de Hermite γ_8 pour les formes quadratiques réelles définies positives en 8 variables. L'égalité résultera du fait que le réseau euclidien E_8 peut être muni, pour tout ordre maximal $\mathscr{O}$, d'une structure de $\mathscr{O}$-module libre (et pas seulement projectif) de rang 2, pour laquelle les éléments x de $\mathscr{O}$ agissent par des similitudes orthogonales de rapport $\mathtt{n}(x)$ (voir la proposition 2.1). Notre construction, reposant sur des techniques de résidus de réseaux euclidiens, généralise une construction classique de E_8 à l'aide des quaternions de Hurwitz (voir par exemple [11, Prop. 8.2.2]). Cette généralisation est très directe lorsque la différente de $\mathscr{O}$ est supposée principale, et conduit dans ce cas à des descriptions explicites : voir la proposition 3.1.
L'inégalité $\gamma_2(\mathscr{O}) \leq \sqrt{D_A}$ est utilisée dans [16], qui donne à l'aide d'outils de géométrie hyperbolique de dimension 5 une théorie graphique des formes hamiltoniennes binaires entières indéfinies, analogue à celle de Conway pour les formes quadratiques binaires.
Dans la partie 3, lorsque la différente de $\mathscr{O}$ est principale, nous donnons une liste (a priori incomplète, certainement redondante) de formes hamiltoniennes binaires définies positives atteignant $\gamma_2(\mathscr{O})$. Lorsque $\mathscr{O}$ lui-même est principal (c'est-à-dire lorsque $h_A = 1$), nous étudions l'unicité d'une telle forme. Deux formes hamiltoniennes binaires seront dites *$\mathscr{O}$-équivalentes* si elles se déduisent l'une de l'autre par précomposition par un élément de $\mathrm{GL}_2(\mathscr{O})$.

Proposition 1.2. — *Si $D_A = 2, 3, 5, 7$, il existe une unique classe de $\mathscr{O}$-équivalence de formes hamiltoniennes binaires définies positives de discriminant donné et réalisant la borne supérieure définissant la constante d'Hermite $\gamma_2(\mathscr{O})$. Si $D_A = 13$, il en existe exactement deux.*

Une étude générale des classes de $\mathscr{O}$-équivalence de telles formes serait intéressante (voir la remarque 3.8). Nous revenons dans la partie 4 sur la correspondance classique entre classes de conjugaison d'ordres maximaux de A et certaines formes quadratiques ternaires, par des techniques de résidus et sommes de Gauss. Cette correspondance associe à l'ordre maximal $\mathscr{O}$ deux réseaux euclidiens pairs de dimension 3 : d'une part $L(\mathscr{O}) = \{x \in \mathscr{O} \ : \ \mathtt{tr}\, x = 0\}$ muni de la restriction de la forme norme, et d'autre part le plus grand sous-réseau pair $M(\mathscr{O})$ de $N \cap N^\sharp$ avec $N = \frac{1}{\sqrt{D_A}} L(\mathscr{O})$. Dans la partie 5 (voir le théorème 5.3), nous montrons alors les équivalences entre :

- la différente de $\mathscr{O}$ est principale,
- $\mathscr{O}$ contient un élément de carré $-D_A$,
- $L(\mathscr{O})$ contient un élément x tel que $x \cdot x = 2D_A$ et $x \cdot y = 0 \bmod D_A$ pour tout $y \in L(\mathscr{O})$, et

– $M(\mathscr{O})$ contient un élément x tel que $x \cdot x = 2$.

Nous utilisons ces équivalences pour donner de nombreux exemples (voir la proposition 5.1 montrant que A admet toujours au moins un ordre maximal de différente principale) et contre-exemples (voir le tableau final de cette note).

Remerciements. — Le premier auteur a été financé par le C.N.R.S. et a reçu le soutien du projet ANR-14-CE25 (PerCoLaTor). Le second auteur remercie l'université de Warwick et l'EPSRC pour leur accueil et soutien financier lors de la rédaction d'une première version de cette note. Les auteurs remercient Lassina Dembélé d'avoir vérifié certains de leurs calculs avec le logiciel Magma.

2. Calcul de la constante d'Hermite binaire $\gamma_2(\mathscr{O})$

Dans toute cette note, nous munissons $\mathbb{H}$ du produit scalaire euclidien $(x, y) \mapsto \mathtt{tr}(\bar{x}\, y)$ (rendant la base usuelle $(1, i, j, k)$ de $\mathbb{H}$ orthogonale et constituée de vecteurs de norme $\sqrt{2}$), et $\mathbb{H}\times\mathbb{H}$ du produit scalaire euclidien produit, que nous notons $(w, w') \mapsto w\cdot w'$. En particulier, ceci définit une forme volume sur $\mathbb{H} \times \mathbb{H}$, et nous définissons le *covolume* d'un $\mathbb{Z}$-réseau Λ de $\mathbb{H} \times \mathbb{H}$ par

$$\operatorname{Covol} \Lambda = \operatorname{Vol}((\mathbb{H} \times \mathbb{H})/\Lambda) \ .$$

Puisque $\mathscr{O}$ est un $\mathbb{Z}$-réseau dans $\mathbb{H}$, le produit $\mathscr{O} \times \mathscr{O}$ est un $\mathbb{Z}$-réseau dans $\mathbb{H} \times \mathbb{H}$, de covolume (voir [9, Lem. 5.5])

$$\operatorname{Covol}(\mathscr{O} \times \mathscr{O}) = \operatorname{Vol}(\mathbb{H}/\mathscr{O})^2 = {D_A}^2 \ .$$

Nous munissons $\mathbb{H} \times \mathbb{H}$ de sa structure d'espace vectoriel à droite sur $\mathbb{H}$. Soit f_0 la forme hamiltonienne binaire définie positive

$$f_0(u, v) = \mathtt{n}(u) + \mathtt{n}(v) \ ,$$

de discriminant -1, de sorte que pour tout élément $w \in \mathbb{H} \times \mathbb{H}$, nous avons $f_0(w) = \frac{1}{2}\, w \cdot w$. Nous noterons h le produit scalaire hermitien sur $\mathbb{H} \times \mathbb{H}$ tel que $h(w, w) = f_0(w)$ pour tout $w \in \mathbb{H} \times \mathbb{H}$. Pour tout $w' = (x', y') \in \mathbb{H} \times \mathbb{H}$ et tout $w = (x, y) \in \mathbb{H} \times \mathbb{H}$, nous avons $h(w', w) = \bar{x}x' + \bar{y}y'$.

L'action à droite par précomposition du groupe $\mathrm{SL}_2(\mathbb{H})$ des matrices 2×2 à coefficients dans $\mathbb{H}$ de déterminant de Dieudonné 1 est transitive sur $\mathscr{Q}_1^+$ (voir par exemple [15, §7]). On appelle *$\mathscr{O}$-réseau* de $\mathbb{H} \times \mathbb{H}$ un $\mathbb{Z}$-réseau qui est en outre un sous-module libre de rang 2 du $\mathscr{O}$-module à droite $\mathbb{H} \times \mathbb{H}$. L'action linéaire à gauche de $\mathrm{SL}_2(\mathbb{H})$ sur l'ensemble des $\mathscr{O}$-réseaux de $\mathbb{H} \times \mathbb{H}$ qui sont de covolume donné en tant que $\mathbb{Z}$-réseaux est aussi transitive.

Pour tout $n \in \mathbb{N}-\{0\}$, rappelons (voir par exemple [2]) que, avec $Q^+(n)$ l'ensemble des formes quadratiques réelles f définies positives en n variables, $M(f)$ la matrice[1] de f et $(x, y) \mapsto x \cdot y$ le produit scalaire usuel sur $\mathbb{R}^n$, la *constante d'Hermite* γ_n en dimension n est définie par

$$\gamma_n = \sup_{f \in Q^+(n)} \ \min_{x \in \mathbb{Z}^n - \{0\}} \ \frac{f(x)}{\sqrt[n]{\det M(f)}} \ = \sup_{\substack{L \ \mathbb{Z}\text{-réseau de } \mathbb{R}^n \\ \operatorname{Covol} L = 1}} \ \min_{x \in L - \{0\}} \ x \cdot x \ .$$

Les valeurs de γ_n sont connues si $n \leq 8$, par exemple Blichfeld [1] a montré que

$$\gamma_8 = 2 \ .$$

[1] de sorte que $f(x) = {}^t X M(f) X$ si X est la matrice colonne des coordonnées de x

Il est bien connu que cette valeur est atteinte pour le réseau E_8, engendré par un système de racines de longueur 2 et de type E_8, qui contient 240 vecteurs x tels que $x \cdot x = 2$. On rappelle que d'après Mordell [12], E_8 est l'unique (à isométrie près) $\mathbb{Z}$-réseau euclidien entier pair, unimodulaire (*i.e.* de covolume 1) et de rang 8 : voir les rappels ci-dessous pour ces terminologies classiques. Mieux, on sait d'après Vetchinkin [21, Theo. 2] qu'à isométrie près, E_8 est le seul $\mathbb{Z}$-réseau unimodulaire atteignant la borne supérieure définissant γ_8.
Tout $\mathscr{O}$-réseau de $\mathbb{H} \times \mathbb{H}$ est en particulier un $\mathbb{Z}$-réseau de l'espace euclidien réel $\mathbb{H} \times \mathbb{H}$ de dimension 8. Donc

$$\begin{aligned}
\gamma_2(\mathscr{O}) &= \sup_{f \in \mathscr{Q}_1^+} \min_{w \in \mathscr{O} \times \mathscr{O} - \{0\}} f(w) = \sup_{g \in \mathrm{SL}_2(\mathbb{H})} \min_{w \in \mathscr{O} \times \mathscr{O} - \{0\}} f_0 \circ g(w) \\
&= \sup_{g \in \mathrm{SL}_2(\mathbb{H})} \min_{w \in g(\mathscr{O} \times \mathscr{O}) - \{0\}} f_0(w) = \sup_{\substack{\Lambda \ \mathscr{O}\text{-réseau de } \mathbb{H} \times \mathbb{H} \\ \mathrm{Covol}\,\Lambda = D_A^2}} \min_{w \in \Lambda - \{0\}} w \cdot w/2 \\
&= \sqrt{D_A} \sup_{\substack{\Lambda \ \mathscr{O}\text{-réseau de } \mathbb{H} \times \mathbb{H} \\ \mathrm{Covol}\,\Lambda = 1}} \min_{w \in \Lambda - \{0\}} w \cdot w/2 \\
&\leq \frac{\sqrt{D_A}}{2} \sup_{\substack{L \ \mathbb{Z}\text{-réseau de } \mathbb{R}^8 \\ \mathrm{Covol}\, L = 1}} \min_{x \in L - \{0\}} x \cdot x \ = \frac{\sqrt{D_A}}{2} \gamma_8 = \sqrt{D_A}\,.
\end{aligned}$$

De plus, ce calcul montre que nous avons égalité dans l'inégalité $\gamma_2(\mathscr{O}) \leq \sqrt{D_A}$ si et seulement s'il existe un $\mathscr{O}$-réseau Λ de covolume 1 dans $\mathbb{H} \times \mathbb{H}$ tel que $\min_{w \in \Lambda - \{0\}} \ w \cdot w = 2$. Le théorème 1.1 découle donc du résultat suivant.

Proposition 2.1. — *L'espace euclidien* $\mathbb{H} \times \mathbb{H}$ *contient des* $\mathscr{O}$*-réseaux isométriques à* E_8.

Nous allons utiliser la technique bien connue des résidus de $\mathbb{Z}$-réseaux euclidiens (aussi appelés "formes quadratiques discriminantes", voire "glue groups" dans [4]), voir par exemple [6, §3.3], [3, §II.1]. Rappelons brièvement les éléments utiles à notre propos.
Un *module quadratique d'enlacement*, ou pour faire court un qe-*module* au sens de [3, §II.1], est la donnée d'un groupe abélien fini V muni d'une application $q : V \to \mathbb{Q}/\mathbb{Z}$ vérifiant $q(mx) = m^2 q(x)$ pour tous les $m \in \mathbb{Z}$ et x dans V, et telle que l'application $V \times V \to \mathbb{Q}/\mathbb{Z}$, définie par $(x, y) \mapsto q(x + y) - q(x) - q(y)$, est $\mathbb{Z}$-bilinéaire non dégénérée. Un qe-module (V, q) est *anisotrope* si le seul élément x de V tel que $q(x) = 0$ est $x = 0$.
Soient E un espace vectoriel réel euclidien de produit scalaire noté $(x, y) \mapsto x \cdot y$, et L un $\mathbb{Z}$-réseau de E. Notons $L^\sharp = \{x \in E \ : \forall\, y \in L, \ \ x \cdot y \in \mathbb{Z}\}$ le $\mathbb{Z}$-réseau *dual* de L. Le réseau L est dit *entier* si l'on a $L \subset L^\sharp$, *pair* si de plus $x \cdot x \in 2\mathbb{Z}$ pour tout $x \in L$. Supposons désormais L entier et pair. Alors l'application

$$q : L^\sharp/L \longrightarrow \mathbb{Q}/\mathbb{Z}, \qquad x + L \longmapsto \frac{x \cdot x}{2} \mod \mathbb{Z}, \tag{1}$$

munit $L^\sharp/L$ d'une structure de qe-module notée $\mathrm{res}\, L$ et appelée le *résidu* de L.
Le groupe abélien fini $L^\sharp/L$ est d'ordre le *déterminant* de L (le déterminant de la matrice de Gram de n'importe quelle $\mathbb{Z}$-base de L), noté $\det L$; nous avons

$$\det L' = [L : L']^2 \det L$$

si L' est un sous-$\mathbb{Z}$-réseau de L. La projection canonique $\mathrm{pr} : L^\sharp \to L^\sharp/L$ induit une bijection de l'ensemble des réseaux entiers et pairs Λ contenant L avec indice m sur l'ensemble des

sous-groupes I de $\operatorname{res} L$, d'ordres m et *isotropes* (tels que $q(x) = 0$ pour tout $x \in I$), de sorte que $\Lambda = \mathrm{pr}^{-1}(I)$.
Pour tout nombre premier p, on pose $L_p = L \otimes_{\mathbb{Z}} \mathbb{Z}_p$. C'est un $\mathbb{Z}_p$-module muni de la forme $\mathbb{Z}_p$-bilinéaire $L_p \times L_p \to \mathbb{Z}_p$, $(x, y) \mapsto x \cdot y$, déduite par extension des scalaires du produit scalaire sur L. On a $x \cdot x \in 2\mathbb{Z}_p$ pour tout x dans L_p. Le $\mathbb{Z}_p$-réseau L_p possède un *dual* défini par $L_p^\sharp = \{x \in L_p[\frac{1}{p}] \ : \ \forall\ y \in L_p, \quad x \cdot y \in \mathbb{Z}_p\}$, contenant L_p, ainsi qu'un *résidu* $\operatorname{res} L_p$ qui est le p-groupe abélien fini $L_p^\sharp / L_p$ muni de la forme quadratique à valeurs dans $\mathbb{Q}_p/\mathbb{Z}_p$ définie comme dans (1). L'application naturelle $\mathbb{Q}/\mathbb{Z} \to \mathbb{Q}_p/\mathbb{Z}_p$ induit un isomorphisme de la composante p-primaire du groupe abélien de torsion $\mathbb{Q}/\mathbb{Z}$ vers $\mathbb{Q}_p/\mathbb{Z}_p$. Cet isomorphisme permet de voir $\operatorname{res} L_p$ comme un qe-module. Le qe-module $\operatorname{res} L$ est la somme orthogonale de ses composantes p-primaires, et pour tout premier p, le morphisme évident $L^\sharp \to L_p^\sharp$ induit une identification de la composante p-primaire de $\operatorname{res} L$ à $\operatorname{res} L_p$.
Notons que $\operatorname{res} L$ est anisotrope si et seulement si $\operatorname{res} L_p$ est anisotrope pour tout premier p. En effet, un élément de $\mathbb{Q}/\mathbb{Z}$ est nul si et seulement si toutes ses composantes p-primaires sont nulles.
Supposons de plus E muni d'une structure de $\mathbb{H}$-espace vectoriel à droite telle que tout élément a de $\mathbb{H}$ agisse sur E par une similitude orthogonale de rapport $\mathtt{n}(a)$. On a alors $(xa) \cdot y = x \cdot (y\bar{a})$ pour tous les x, y dans E et a dans $\mathbb{H}$. Si L est stable par $\mathscr{O}$, il en va de même de $L^\sharp$ car $\mathscr{O}$ est stable par la conjugaison $x \mapsto \bar{x}$, et $\operatorname{res} L$ est donc muni d'une structure de $\mathscr{O}$-module à droite. De même, $L_p^\sharp$ et $\operatorname{res} L_p$ sont des $\mathscr{O}$-modules à droite, et l'application naturelle $\operatorname{res} L \to \operatorname{res} L_p$ est $\mathscr{O}$-linéaire, pour tout premier p.
Nous renvoyons à [22] pour les faits très classiques suivants sur les algèbres de quaternions. Soit p un nombre premier divisant D_A. Alors $\mathscr{O}_p$ est l'unique ordre maximal de la $\mathbb{Q}_p$-algèbre de quaternions $A \otimes_{\mathbb{Q}} \mathbb{Q}_p$ (une algèbre à division). De plus, la norme réduite $\mathtt{n} : \mathscr{O}_p \to \mathbb{Z}_p$ est surjective, et l'on peut donc choisir un élément π_p de $\mathscr{O}_p$ vérifiant $\mathtt{n}(\pi_p) = p$. Tout idéal (à droite ou à gauche) de $\mathscr{O}_p$ est bilatère, de la forme $\pi_p^n \mathscr{O}_p$ pour un unique entier $n \geq 0$ (d'indice p^{2n}). En particulier, on a $p\mathscr{O}_p = \pi_p^2 \mathscr{O}_p$, $\pi_p \mathscr{O}_p$ est l'idéal maximal de $\mathscr{O}_p$, et $\mathbb{F}_{p^2} = \mathscr{O}_p / \pi_p \mathscr{O}_p$ est un corps d'ordre p^2. Nous noterons respectivement $\mathrm{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}$ et $\mathrm{N}_{\mathbb{F}_{p^2}/\mathbb{F}_p}$ la trace et la norme de l'extension $\mathbb{F}_{p^2}$ de $\mathbb{F}_p = \mathbb{Z}_p / p\mathbb{Z}_p$.
D'après ces rappels, il existe un unique idéal à droite $\mathscr{M}$ de $\mathscr{O}$ d'indice D_A^2 : c'est l'idéal vérifiant $\mathscr{M}_p = \pi_p \mathscr{O}_p$ pour p divisant D_A, et $\mathscr{M}_p = \mathscr{O}_p$ sinon. C'est un idéal bilatère de $\mathscr{O}$ car $\mathscr{M}_p$ est bilatère dans $\mathscr{O}_p$ pour tout p. Puisque sa norme est égale à D_A, l'idéal $\mathscr{M}$ est la différente de $\mathscr{O}$, donc égal à $(\mathscr{O}^\sharp)^{-1}$ où $I^{-1} = \{x \in A \ : \ IxI \subset I\}$ pour tout $\mathbb{Z}$-réseau I de A. Puisque $\mathtt{tr}(\bar{x}\, x) = 2\,\mathtt{n}(x)$ pour tout x dans $\mathbb{H}$, l'ordre maximal $\mathscr{O}$ est un $\mathbb{Z}$-réseau entier et pair de l'espace euclidien $\mathbb{H}$, de déterminant ${D_A}^2$. Posons $\mathscr{N} = \frac{1}{\sqrt{D_A}} \mathscr{M} \subset \mathbb{H}$. C'est un sous-$\mathscr{O}$-module bilatère de $\mathbb{H}$ vérifiant trivialement $\mathtt{n}(xa) = \mathtt{n}(ax) = \mathtt{n}(a)\,\mathtt{n}(x)$ pour tout $x \in \mathscr{N}$ et tout $a \in \mathscr{O}$.

Lemme 2.2. —

1. *Pour tout premier p divisant D_A, le résidu de $\mathscr{O}_p$ est isomorphe au groupe additif $\mathbb{F}_{p^2}$ muni de la forme quadratique $x \mapsto \frac{1}{p} \mathrm{N}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(x) \bmod \mathbb{Z}$.*

2. *Le $\mathbb{Z}$-réseau euclidien $\mathscr{N}$ est entier et pair, de dual $\mathscr{N}^\sharp = \frac{1}{\sqrt{D_A}} \mathscr{O}$, et pour tout premier p, il existe une isométrie $\mathscr{O}_p$-linéaire (à droite) entre $\mathscr{N}_p$ et $\mathscr{O}_p$.*

Démonstration. — Soit p un nombre premier divisant D_A. La conjugaison $a \mapsto \bar{a}$ de $\mathscr{O}$ induit une anti-involution de $\mathscr{O}_p$, préservant nécessairement son idéal maximal $\mathscr{M}_p$, ainsi donc qu'un automorphisme $\mathbb{F}_p$-linéaire de $\mathbb{F}_{p^2}$, nécessairement non trivial à cause de l'identité $\mathtt{n}(a) = a\bar{a}$, et donc égal à l'automorphisme de Frobenius $y \mapsto y^p$. Pour tout x dans $\mathscr{O}_p$ d'image y dans $\mathbb{F}_{p^2}$, et puisque $\pi_p \mathscr{O}_p \cap \mathbb{Z}_p = p\mathbb{Z}_p$, on a donc

$$\mathtt{tr}(x) \equiv \mathrm{Tr}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(y) \bmod p\mathbb{Z}_p \quad \text{et} \quad \mathtt{n}(x) \equiv \mathrm{N}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(y) \bmod p\mathbb{Z}_p \ . \tag{2}$$

De la congruence (2) portant sur $\mathtt{tr}$, on déduit aisément les relations bien connues

$$\mathtt{tr}\, \mathscr{M}_p \subset p\mathbb{Z}_p, \quad \mathscr{O}_p^\sharp = p^{-1}\mathscr{M}_p = \pi_p^{-1}\mathscr{O}_p \quad \text{et} \quad \mathscr{M}_p^\sharp = p^{-1}\,\mathscr{O}_p \ . \tag{3}$$

La congruence (2) portant sur $\mathtt{n}$, la relation $\mathscr{O}_p^\sharp = \pi_p^{-1}\mathscr{O}_p$ ci-dessus, l'égalité $\mathtt{n}(\pi_p) = p$, et la multiplicativité de la norme, entraînent l'assertion 1 du lemme 2.2.
Montrons l'assertion 2. Pour tout x dans $\mathscr{M}$, l'élément $\frac{1}{D_A}\,\mathtt{n}(x)$ est dans $\mathbb{Z}_p$ pour tout premier p, et donc dans $\mathbb{Z}$: les réseaux $\mathscr{M}$ et $\mathscr{N}$ sont entiers et pairs. On a $\mathscr{M}^\sharp = D_A^{-1}\mathscr{O}$ d'après (3), et donc $\mathscr{N}^\sharp = \sqrt{D_A}\,\mathscr{M}^\sharp = \frac{1}{\sqrt{D_A}}\mathscr{O}$. Soit p un nombre premier, il ne reste qu'à montrer qu'il existe une bijection $\mathscr{O}_p$-linéaire à droite $f_p : \mathscr{O}_p \to \mathscr{M}_p$ vérifiant $\frac{1}{D_A}\,\mathtt{n}(f_p(x)) = \mathtt{n}(x)$ pour tout x dans $\mathscr{O}_p$. Il suffit de prendre pour f_p la multiplication à gauche par un élément $x_p \in \mathscr{O}_p$ avec $\mathtt{n}(x_p) = D_A$. Un tel élément existe par la surjectivité de $\mathtt{n} : \mathscr{O}_p \to \mathbb{Z}_p$. □

Proposition 2.3. — *Il existe un $\mathscr{O}$-réseau de $\mathbb{H}\times\mathbb{H}$ contenant $\mathscr{O}\times\mathscr{N}$ et qui est isométrique à E_8 en tant que $\mathbb{Z}$-réseau euclidien.*

Démonstration. — Notons L le $\mathbb{Z}$-réseau $\mathscr{O} \times \mathscr{N}$ de l'espace euclidien $\mathbb{H} \times \mathbb{H}$. Il est stable par multiplication à droite par $\mathscr{O}$, mais n'est pas nécessairement un $\mathscr{O}$-réseau car $\mathscr{N}$ n'est pas libre de rang 1 sur $\mathscr{O}$ en général.[2] Notons que le $\mathbb{Z}$-réseau $L^\sharp$, et donc le groupe abélien $L^\sharp/L$ de $\operatorname{res} L$, ont des structures de $\mathscr{O}$-modules (à droite) telles que la projection canonique $\mathrm{pr} : L^\sharp \to L^\sharp/L$ soit un morphisme de $\mathscr{O}$-modules. Montrons qu'il existe un sous-$\mathscr{O}$-module isotrope I de $\operatorname{res} L$, d'ordre ${D_A}^2$ et tel que le sous-$\mathscr{O}$-module $\Lambda = \mathrm{pr}^{-1}(I)$ de $\mathbb{H} \times \mathbb{H}$ soit un $\mathscr{O}$-réseau de $\mathbb{H} \times \mathbb{H}$. Alors Λ est un $\mathbb{Z}$-réseau euclidien entier et pair en dimension 8, de covolume $\operatorname{Covol}\Lambda = \frac{\operatorname{Covol} L}{[\Lambda:L]} = \frac{{D_A}^2}{{D_A}^2} = 1$ donc unimodulaire. Par unicité, il est isométrique à E_8, ce qui conclut.
Nous avons $\operatorname{res} L = \operatorname{res}\mathscr{O} \times \operatorname{res}\mathscr{N}$ et $\operatorname{res} L_p = \operatorname{res}\mathscr{O}_p \times \operatorname{res}\mathscr{N}_p$ pour tout premier p. Il suffit donc de définir la composante p-primaire I_p de I pour p divisant D_A. Fixons un tel p et identifions $\operatorname{res}\mathscr{O}_p$ et $\operatorname{res}\mathscr{N}_p$ au $\mathscr{O}$-module $\mathbb{F}_{p^2}$ muni de la forme quadratique $x \mapsto \frac{1}{p}\mathrm{N}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(x) \bmod \mathbb{Z}$, ce qui est loisible d'après les points 1 et 2 du lemme 2.2. Soit $a_p \in \mathbb{F}_{p^2}$ tel que $\mathrm{N}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(a_p) = -1$, qui existe par la surjectivité de la norme pour les corps finis. Posons

$$I_p = \{(x_p, y_p) \in \mathbb{F}_{p^2} \times \mathbb{F}_{p^2} \ : \ y_p = a_p x_p\} \ . \tag{4}$$

C'est un sous-$\mathscr{O}$-module de $\operatorname{res} L_p$ d'ordre p^2. Il est isotrope car pour $(x_p, y_p) \in I_p$ on a

$$\mathrm{N}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(x_p) + \mathrm{N}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(y_p) = \mathrm{N}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(x_p)(1 + \mathrm{N}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(a_p)) = 0 \ .$$

Enfin, $\Lambda = \mathrm{pr}^{-1}(I)$ est dans une suite exacte de $\mathscr{O}$-modules

$$0 \longrightarrow \mathscr{O} \longrightarrow \Lambda \longrightarrow \mathscr{N}^\sharp \longrightarrow 0 \ ,$$

[2] Voir la partie 5 pour des listes et des caractérisations de quand $\mathscr{M}$ (et donc $\mathscr{N}$) est libre de rang 1 sur $\mathscr{O}$.

où l'application $\Lambda \to \mathscr{N}^\sharp$ est la restriction à Λ de la seconde projection $\mathscr{O}^\sharp \times \mathscr{N}^\sharp \to \mathscr{N}^\sharp$. En effet, cette application est surjective de noyau $\mathscr{O} \times \{0\}$ car la seconde projection de I_p dans $\operatorname{res} \mathscr{N}_p$ est bijective. Mais on a $\mathscr{N}^\sharp = \frac{1}{\sqrt{D_A}}\mathscr{O}$ d'après le lemme 2.2 2. Donc $\mathscr{N}^\sharp$ est libre de rang 1 sur $\mathscr{O}$, et Λ est un $\mathscr{O}$-réseau, ce qui conclut la démonstration de la proposition. □

La proposition 2.1, et donc le théorème 1.1, en découlent.
Notons $\mathrm{U}_2(\mathbb{H})$ le groupe unitaire du $\mathbb{H}$-espace vectoriel à droite $\mathbb{H} \times \mathbb{H}$ muni de la forme hamiltonienne $f_0(u, v) = \mathtt{n}(u) + \mathtt{n}(v)$. Ce groupe agit naturellement sur l'ensemble des $\mathscr{O}$-réseaux de $\mathbb{H} \times \mathbb{H}$. À tout tel réseau Λ, disons de base (e_1, e_2), on associe la forme hamiltonienne binaire $(u, v) \mapsto f_0(e_1u + e_2v)$. La classe de $\mathscr{O}$-équivalence de cette forme ne dépend que de Λ, et nous la notons f_Λ. Il découle immédiatement des définitions que pour deux réseaux Λ et Λ', on a l'égalité $f_\Lambda = f_{\Lambda'}$ si, et seulement si, il existe $g \in \mathrm{U}_2(\mathbb{H})$ vérifiant $g(\Lambda) = \Lambda'$. Comme toute forme hamiltonienne binaire définie positive est de la forme $f_0(e_1u + e_2v)$ pour une base (e_1, e_2) bien choisie du $\mathbb{H}$-espace vectoriel $\mathbb{H} \times \mathbb{H}$, on en déduit le résultat suivant, analogue naturel d'un énoncé classique sur les réseaux euclidiens. (L'assertion portant sur le covolume a déjà été vue plus haut.)

Proposition 2.4. — *L'application $\Lambda \mapsto f_\Lambda$ induit une bijection entre l'ensemble des $\mathrm{U}_2(\mathbb{H})$-orbites de $\mathscr{O}$-réseaux dans $\mathbb{H} \times \mathbb{H}$ et l'ensemble des classes de $\mathscr{O}$-équivalence de formes hamiltoniennes binaires définies positives. Dans cette bijection, le discriminant de f_Λ et le covolume de Λ sont liés par la formule $\sqrt{\operatorname{Covol}\Lambda} = -D_A\,\Delta(f_\Lambda)$.*

Notons $\mathscr{X}(\mathscr{O})$ l'ensemble des $\mathscr{O}$-réseaux de $\mathbb{H} \times \mathbb{H}$ isométriques à E_8 en tant que réseau euclidien. Il est stable sous l'action de $\mathrm{U}_2(\mathbb{H})$.

Corollaire 2.5. —

1. *L'ensemble $\mathscr{X}(\mathscr{O})$ est non vide.*

2. *L'application $f \mapsto f_\Lambda$ induit une bijection entre $\mathrm{U}_2(\mathbb{H})\backslash\mathscr{X}(\mathscr{O})$ et l'ensemble des classes de $\mathscr{O}$-équivalence de formes hamiltoniennes binaires définies positives de discriminant $-1/D_A$ qui réalisent la (borne supérieure définissant la) constante d'Hermite $\gamma_2(\mathscr{O})$.*

Démonstration. — La première assertion est la proposition 2.1. La seconde résulte de l'analyse précédant cette proposition et du théorème déjà cité de Vetchinkin [21, Theo. 2], □

Bien que nous ne l'utiliserons pas, mentionnons que pour des raisons générales il n'y a qu'un nombre fini de $\mathrm{U}_2(\mathbb{H})$-orbites dans $\mathscr{X}(\mathscr{O})$.

3. Étude du cas d'égalité

Dans cette partie, nous explicitons d'abord certains éléments de $\mathscr{X}(\mathscr{O})$ quand la différente de $\mathscr{O}$ est principale, ainsi donc que des formes hamiltoniennes binaires définies positives réalisant $\gamma_2(\mathscr{O})$. Ensuite, nous déterminerons $\mathrm{U}_2(\mathbb{H})\backslash\mathscr{X}(\mathscr{O})$ quand $\mathscr{O}$ est principal.
Supposons donc que $\mathscr{O}$ est un ordre maximal de différente $\mathscr{M}$ principale. Choisissons $\pi \in \mathscr{O}$ vérifiant $\mathscr{M} = \pi\mathscr{O} = \mathscr{O}\pi$. En particulier, nous avons $\mathtt{n}(\pi) = D_A$ et $\mathscr{O}^\sharp = \pi^{-1}\mathscr{O}$ (observer par exemple $\pi_p \in \pi\mathscr{O}_p^\times$ pour tout premier p divisant D_A et utiliser la formule (3)). Notons

$\mathscr{E}_{\mathscr{O}}$ l'ensemble des $\lambda \in \mathscr{O}$ tels que $\mathtt{n}(\lambda) \equiv -1 \mod D_A$. Cet ensemble est non vide par la surjectivité de la norme pour les corps finis et la formule (2). Pour $\lambda \in \mathscr{E}_{\mathscr{O}}$, posons

$$\Lambda_\lambda = \{(\pi^{-1}u, \pi^{-1}v) \in \pi^{-1}\mathscr{O} \times \pi^{-1}\mathscr{O} \ : \ \lambda u \equiv v \mod \pi\mathscr{O}\} \ . \tag{5}$$

C'est un $\mathbb{Z}$-réseau de $\mathbb{H} \times \mathbb{H}$ stable par $\mathscr{O}$ et contenant $\mathscr{O} \times \mathscr{O}$. L'anneau $\mathscr{O}/\pi\mathscr{O}$ étant commutatif (il est isomorphe à $\prod_{p \mid D_A} \mathbb{F}_{p^2}$), le réseau Λ_λ ne change pas si l'on remplace π par $a\pi$, avec $a \in \mathscr{O}^\times$, dans sa définition. Autrement dit, Λ_λ ne dépend pas du choix du générateur π de $\mathscr{M}$, ce qui justifie sa notation. Enfin, il ne dépend que de la classe de λ dans $\mathscr{O}/\pi\mathscr{O}$, de sorte qu'il y a également un sens à définir Λ_λ pour tout $\lambda \in \mathscr{O}/\pi\mathscr{O}$ avec $\mathtt{n}(\lambda) \equiv -1 \bmod D_A$. En considérant l'élément $(\pi^{-1}, \pi^{-1}\lambda)$ de Λ_λ, on constate l'équivalence $\Lambda_\lambda = \Lambda_{\lambda'} \Leftrightarrow \lambda \equiv \lambda' \bmod \pi\mathscr{O}$.

Proposition 3.1. — *Supposons la différente de $\mathscr{O}$ principale et engendrée par π. Soit $\lambda \in \mathscr{E}_{\mathscr{O}}$.*

1. *Le $\mathbb{Z}$-réseau Λ_λ appartient à $\mathscr{X}(\mathscr{O})$.*

2. *L'application de $\mathbb{H} \times \mathbb{H}$ dans $\mathbb{R}$ définie par*

$$f_{\pi;\lambda} : (u, v) \mapsto \frac{\mathtt{n}(\lambda) + 1}{D_A}\, \mathtt{n}(u) + \mathtt{tr}(\,\bar{u}\,\pi^{-1}\lambda\, v) + \mathtt{n}(v)$$

est une forme hamiltonienne binaire définie positive, qui réalise la borne supérieure définissant $\gamma_2(\mathscr{O})$.

Enfin, tout élément de $\mathscr{X}(\mathscr{O})$ contenant $\mathscr{O} \times \mathscr{O}$ est de la forme Λ_λ pour $\lambda \in \mathscr{E}_{\mathscr{O}}$.

Démonstration. — Le $\mathbb{Z}$-réseau Λ_λ contient $\mathscr{O} \times \mathscr{O}$ avec indice $|\mathscr{O}/\pi\mathscr{O}| = D_A^2 = \mathrm{Covol}(\mathscr{O} \times \mathscr{O})$, il est donc bien de covolume 1. Pour $(\pi^{-1}u, \pi^{-1}v) \in \Lambda_\lambda$, le rationnel

$$\mathtt{n}(\pi^{-1}u) + \mathtt{n}(\pi^{-1}v) = \mathtt{n}(\pi)^{-1}(\mathtt{n}(u) + \mathtt{n}(v)) = \frac{1}{D_A}(\mathtt{n}(u) + \mathtt{n}(v))$$

est un entier, à cause de la congruence $\mathtt{n}(u) + \mathtt{n}(v) \equiv \mathtt{n}(u) + \mathtt{n}(\lambda)\,\mathtt{n}(u) \equiv 0 \bmod D_A$ pour $\lambda \in \mathscr{E}_{\mathscr{O}}$. Cela montre que Λ_λ est entier pair. C'est trivialement un sous-$\mathscr{O}$-module (à droite) de $\mathbb{H} \times \mathbb{H}$, dont les éléments $e_1 = (\pi^{-1}, \pi^{-1}\lambda)$ et $e_2 = (0, 1)$ constituent une $\mathscr{O}$-base : c'est un $\mathscr{O}$-réseau, et nous avons montré l'assertion 1. On constate les égalités $f_0(e_1) = \frac{1+\mathtt{n}(\lambda)}{D_A}$, $f_0(e_2) = 1$ et $h(e_1, e_2) = \pi^{-1}\lambda$. Pour $u, v \in \mathbb{H}$, nous avons donc $f_0(e_1 u + e_2 v) = f_{\pi;\lambda}(u, v)$. L'assertion 2 découle alors de l'assertion 1 et du point 2 du corollaire 2.5.
Montrons la dernière assertion. On raisonne comme dans la démonstration de la proposition 2.3, en remplaçant $\mathscr{O} \times \mathscr{N}$ par $\mathscr{O} \times \mathscr{O}$. Nous avons $\mathrm{res}\,\mathscr{O} = \pi^{-1}\mathscr{O}/\mathscr{O}$ et l'anneau $\mathscr{O}/\pi\mathscr{O}$ est produit direct sur les premiers p divisant D_A des corps finis $\mathscr{O}_p/\pi\mathscr{O}_p = \mathbb{F}_{p^2}$. Un sous-$\mathscr{O}/\pi\mathscr{O}$-module I isotrope de $\mathrm{res}\,\mathscr{O} \times \mathrm{res}\,\mathscr{O}$ intersecte trivialement le sous-espace anisotrope $\{0\} \times \mathrm{res}\,\mathscr{O}_p$ pour p divisant D_A. Si I est en outre libre de rang 1 sur $\mathscr{O}/\pi\mathscr{O}$ (ou ce qui revient au même, de cardinal $|\mathscr{O}/\pi\mathscr{O}|$), il est engendré sur $\mathscr{O}/\pi\mathscr{O}$ par la classe d'un élément e de $\pi^{-1}\mathscr{O} \times \pi^{-1}\mathscr{O}$, disons $e = (\pi^{-1}\mu', \pi^{-1}\mu)$, avec $\mu', \mu \in \mathscr{O}$ vérifiant $\mathtt{n}(\mu') + \mathtt{n}(\mu) \equiv 0 \bmod D_A$ et $\mu' \in \mathscr{O}_p^\times$ pour tout p divisant D_A. On en déduit $\mu' \in \mathscr{O}^\times$: on peut donc supposer $\mu' = 1$. Par définition, l'image inverse de I par la projection canonique $\pi^{-1}\mathscr{O} \times \pi^{-1}\mathscr{O} \to \mathrm{res}\,\mathscr{O} \times \mathrm{res}\,\mathscr{O}$ est $e\mathscr{O} + \mathscr{O} \times \mathscr{O} = \Lambda_\mu$. □

Remarque 3.2. — Supposons $D_A = 2$ et $\mathscr{O} = \mathbb{Z}\frac{1+i+j+k}{2} + i\mathbb{Z} + j\mathbb{Z} + k\mathbb{Z}$ (*ordre de Hurwitz*). Nous pouvons prendre $\pi = i + 1$ (car $\mathtt{n}(1 + i) = 2$) et $\lambda = 1$ (car $1 = -1 \bmod 2$). Nous retrouvons alors la réalisation quaternionique usuelle $\{(u', v') \in \mathscr{O} \times \mathscr{O} \ : \ u' \equiv v' \bmod (1+i)\mathscr{O}\}$

du réseau euclidien E_8 : voir [11, Prop. 8.2.2] (cette construction diffère de la nôtre d'une homothétie car elle utilise le produit scalaire $\frac{1}{2}\,\mathtt{tr}(\bar{x}y)$ sur $\mathbb{H}$).

Déterminons maintenant $\mathrm{U}_2(\mathbb{H})\backslash\mathscr{X}(\mathscr{O})$ lorsque $\mathscr{O}$ est principal, ce qui se produit si et seulement si $h_A = 1$, ou de manière équivalente si $D_A = 2, 3, 5, 7$ ou 13 (voir [23, Theo. 25.4.1] ou [22, haut de page 155], ainsi que [22, Prop. 3.2, p. 146] pour le calcul de h_A en fonction de D_A). En particulier, D_A est un nombre premier, que nous noterons simplement p. La proposition 1.2 de l'introduction découle du résultat suivant.

Proposition 3.3. — *Pour $D_A \leq 7$, il existe une unique $\mathrm{U}_2(\mathbb{H})$-orbite de $\mathscr{O}$-réseaux de $\mathbb{H}\times\mathbb{H}$ isométriques à E_8. Pour $D_A = 13$, il existe exactement deux telles orbites.*

Comme $\mathscr{O}$ est principal, sa différente l'est aussi, et on en fixe comme précédemment un générateur π. Rappelons que si $h_A = 1$, la formule de masse d'Eichler [7, p. 103] donne

$$\frac{1}{|\mathscr{O}^\times|} = \frac{p-1}{24}\ .$$

Écrivons l'entier 24 sous la forme $(p-1)p^n m$ avec m un entier premier à p. Le morphisme d'anneaux $\mathscr{O}_p \to \mathscr{O}_p/\pi\mathscr{O}_p = \mathbb{F}_{p^2}$ induit un morphisme de groupes $\mathscr{O}_p^\times \to \mathbb{F}_{p^2}^\times$ de noyau $1+\pi\mathscr{O}_p$. Ce dernier est un pro-p-groupe et $\mathbb{F}_{p^2}^\times$ est d'ordre premier à p. En composant $\mathscr{O}_p^\times \to \mathbb{F}_{p^2}^\times$ et l'inclusion canonique $\mathscr{O}^\times \to \mathscr{O}_p^\times$, nous obtenons un morphisme de groupes

$$\varepsilon : \mathscr{O}^\times \to \mathbb{F}_{p^2}^\times\ ,$$

dont l'image est incluse dans le sous-groupe d'ordre $p+1$ des éléments de norme 1 de $\mathbb{F}_{p^2}^\times$. Le lemme suivant en découle.

Lemme 3.4. — *Nous avons $|\ker\varepsilon| = p^n$, $|\mathrm{Im}\,\varepsilon| = m$, et m divise $p+1$.*

D'après le dernier point de la proposition 3.1, et puisqu'ici $D_A = p$ est premier, les réseaux $\Lambda \in \mathscr{X}(\mathscr{O})$ contenant $\mathscr{O}\times\mathscr{O}$ sont ceux de la forme Λ_x pour un unique x dans $\mathscr{O}/\pi\mathscr{O} = \mathbb{F}_{p^2}$ vérifiant

$$\mathrm{N}_{\mathbb{F}_{p^2}/\mathbb{F}_p}(x) = x^{1+p} = -1.$$

Notons $X_p \subset \mathbb{F}_{p^2}^\times$ le sous-ensemble des x ci-dessus. Nous avons $|X_p| = p+1$. On munit X_p d'une structure de $\mathscr{O}^\times$-ensemble par la formule $(a, x) \mapsto \varepsilon(\pi a \pi^{-1})x$. Cette formule a un sens car la relation $\pi\mathscr{O} = \mathscr{O}\pi$ montre que $x \mapsto \pi x \pi^{-1}$ est un automorphisme de l'anneau $\mathscr{O}$, et en particulier du groupe $\mathscr{O}^\times$. Observons que le $\mathscr{O}^\times$-ensemble X_p ainsi défini ne dépend pas du choix du générateur π de la différente de $\mathscr{O}$, car l'anneau $\mathscr{O}/\pi\mathscr{O} = \mathbb{F}_{p^2}$ est commutatif.
Pour $x \in X_p$, le $\mathbb{Z}$-réseau Λ_x contient l'élément $\alpha_0 = (1, 0)$ qui vérifie $\alpha_0 \cdot \alpha_0 = 2$. Pour tout a dans $\mathscr{O}^\times$, notons m_a l'élément de $\mathrm{U}_2(\mathbb{H})$ défini par $\mathrm{m}_a(x, y) = (x, ay)$. Le morphisme $a \mapsto \mathrm{m}_a$ identifie $\mathscr{O}^\times$ au sous-groupe de $\mathrm{U}_2(\mathbb{H})$ fixant α_0 et préservant $\mathscr{O}\times\mathscr{O}$. Pour $a \in \mathscr{O}^\times$, nous avons l'identité $\mathrm{m}_a(\pi^{-1}, \pi^{-1}\lambda) = (\pi^{-1}, \pi^{-1}\pi a \pi^{-1}\lambda)$. La définition (5) montre donc

$$\mathrm{m}_a(\Lambda_x) = \Lambda_{\varepsilon(\pi a \pi^{-1})x}$$

pour $x \in X_p$ et $a \in \mathscr{O}^\times$. Notons enfin $\mathscr{Y}(\mathscr{O})$ l'ensemble des couples (α, Λ) avec Λ dans $\mathscr{X}(\mathscr{O})$, $\alpha \in \Lambda$ et $\alpha \cdot \alpha = 2$, muni de l'action diagonale de $\mathrm{U}_2(\mathbb{H})$. Les observations ci-dessus montrent que l'application $X_p \to \mathscr{Y}(\mathscr{O})$, définie par $x \mapsto (\alpha_0, \Lambda_x)$, et le morphisme $\mathscr{O}^\times \to \mathrm{U}_2(\mathbb{H})$,

défini par $a \mapsto \mathrm{m}_a$, définissent un morphisme de groupoïdes entre le $\mathscr{O}^\times$-ensemble X_p et le $\mathrm{U}_2(\mathbb{H})$-ensemble $\mathscr{Y}(\mathscr{O})$.

Lemme 3.5. — *Le morphisme de groupoïdes $X_p \to \mathscr{Y}(\mathscr{O})$ ci-dessus est une équivalence (de catégorie).*

Démonstration. — Il y a deux points à démontrer : (i) pour tout y dans $\mathscr{Y}(\mathscr{O})$, il existe u dans $\mathrm{U}_2(\mathbb{H})$ et x dans X_p tels que $uy = (\alpha_0, \Lambda_x)$; (ii) pour tout x dans X_p, le stabilisateur de (α_0, Λ_x) dans $\mathrm{U}_2(\mathbb{H})$ est le sous-groupe des m_a avec $a \in \mathscr{O}^\times$ et $\varepsilon(\pi a \pi^{-1}) = 1$.
Soient $\Lambda \in \mathscr{X}(\mathscr{O})$, $\alpha \in \Lambda - \{0\}$ et $N = \alpha\mathscr{O}$. Pour x dans $\mathscr{O}$, la relation $\alpha x \cdot \alpha x = \mathtt{n}(x)\,\alpha\cdot\alpha = \mu\,(x \cdot x)$, avec $\mu = \frac{\alpha\cdot\alpha}{2} = f_0(\alpha)$, montre que le $\mathbb{Z}$-réseau euclidien de rang 4 sous-jacent à N est isométrique à $\sqrt{\mu}\mathscr{O}$, et donc de covolume $\mu^2 \operatorname{Covol}\mathscr{O}$. Supposons maintenant $\alpha \cdot \alpha = 2$. Dans ce cas, N est isométrique à $\mathscr{O}$. Le résidu de $\mathscr{O}$ étant anisotrope, le seul réseau entier pair de $N \otimes_{\mathbb{Z}} \mathbb{Q}$ contenant N est N lui-même. En particulier, le réseau N est saturé dans Λ : on a $\Lambda \cap (N \otimes_{\mathbb{Z}} \mathbb{Q}) = N$ et le groupe abélien Λ/N est sans $\mathbb{Z}$-torsion. Comme E_8 est unimodulaire, on en déduit que l'orthogonal $N^\perp$ de N dans Λ est de même covolume que N [3, Prop. B 2.2 (d)]. Mais $N^\perp$ est stable par $\mathscr{O}$ car N l'est. Il est donc libre de rang 1 sur $\mathscr{O}$ car $\mathscr{O}$ est principal. Nous pouvons donc écrire $N^\perp = \beta\mathscr{O}$ avec $\beta \in \Lambda$. L'égalité des covolumes de N et $N^\perp$ implique $\beta \cdot \beta = 2$. Ainsi, le couple (α, β) est une $\mathbb{H}$-base orthonormée de $\mathbb{H} \times \mathbb{H}$, et donc quitte à remplacer Λ par $u(\Lambda)$ où u est l'unique élément de $\mathrm{U}_2(\mathbb{H})$ envoyant α sur $\alpha_0 = (1, 0)$ et β sur $(0, 1)$, nous pouvons supposer que Λ, qui est un $\mathscr{O}$-réseau, contient $\mathscr{O} \times \mathscr{O}$, et que l'orthogonal de $(1, 0)\mathscr{O}$ dans Λ est $\{0\} \times \mathscr{O}$. En particulier, d'après la dernière assertion de la proposition 3.1, le réseau Λ est de la forme Λ_x pour x dans X_p : le premier point (i) en découle.
De plus, le sous-groupe de $\mathrm{U}_2(\mathbb{H})$ fixant α_0 et Λ préserve l'orthogonal de $\alpha_0\mathscr{O}$ dans Λ, c'est-à-dire $\{0\} \times \mathscr{O}$: c'est donc l'ensemble des m_a avec a dans $\mathscr{O}^\times$. La relation $\mathrm{m}_a(\Lambda_x) = \Lambda_{\epsilon(\pi a \pi^{-1})x}$, et la propriété $\Lambda_x = \Lambda_y \Leftrightarrow x = y$, montrent que $\mathrm{m}_a(\Lambda_x) = \Lambda_x$ équivaut à $\epsilon(\pi a \pi^{-1}) = 1$. Le second point (ii) en découle. □

Pour $\Lambda \subset \mathbb{H} \times \mathbb{H}$, notons $\mathrm{U}(\Lambda)$ le stabilisateur de Λ dans $\mathrm{U}_2(\mathbb{H})$ (le *groupe unitaire de* Λ) et $\mathrm{R}(\Lambda)$ l'ensemble des $\alpha \in \Lambda$ vérifiant $\alpha\cdot\alpha = 2$ (les *racines* de Λ). Nous avons $|\mathrm{R}(\Lambda)| = 240$ pour Λ dans $\mathscr{X}(\mathscr{O})$, car E_8 admet 240 racines. Le groupe $\mathrm{U}(\Lambda)$ agit naturellement sur $\mathrm{R}(\Lambda)$, et on note r_Λ le nombre d'orbites pour cette action. Ce nombre ne dépend que de la $\mathrm{U}_2(\mathbb{H})$-orbite de Λ.

Lemme 3.6. — *Le groupe $\mathrm{U}_2(\mathbb{H})$ admet $\frac{p+1}{m}$ orbites dans $\mathscr{Y}(\mathscr{O})$, avec stabilisateurs d'ordre p^n. Par conséquent, nous avons $\sum_{[\Lambda]\in \mathrm{U}_2(\mathbb{H})\backslash\mathscr{X}(\mathscr{O})} \mathrm{r}_\Lambda = \frac{p+1}{m}$, et $240 = \mathrm{r}_\Lambda \frac{|\mathrm{U}(\Lambda)|}{p^n}$ pour tout Λ dans $\mathscr{X}(\mathscr{O})$.*

Démonstration. — Le $\mathscr{O}^\times$-ensemble X_p a clairement $(p+1)/m$ orbites, et des stabilisateurs isomorphes à $\ker\varepsilon$. L'énoncé est donc une conséquence des lemmes 3.5 et 3.4. □

Démonstration de la proposition 3.3. — Pour $p = 2, 3, 5$, nous avons $m = p + 1$. D'après le lemme 3.6, le groupe $\mathrm{U}_2(\mathbb{H})$ agit transitivement sur $\mathscr{X}(\mathscr{O})$, et pour tout Λ dans $\mathscr{X}(\mathscr{O})$, nous avons $\mathrm{r}_\Lambda = 1$.

Remarque 3.7. — Pour $p = 2, 3, 5$ et Λ dans $\mathscr{X}(\mathscr{O})$, nous avons montré $|\mathrm{U}(\Lambda)| = 240\,p^n$, soit encore

$$|\mathrm{U}(\Lambda)| = 1920,\ 720,\ 240 \quad \text{pour} \quad p = 2,\ 3,\ 5 \quad \text{respectivement.}$$

C'est un point de départ pour une étude plus fine du groupe $\mathrm{U}(\Lambda)$ que nous laissons au lecteur. Par exemple pour $p = 3$ (resp. $p = 5$), on peut montrer que $\mathrm{U}(\Lambda)$ est une extension centrale du groupe alterné $\mathfrak{A}_6$ (resp. du groupe symétrique $\mathfrak{S}_5$) par $\mathbb{Z}/2\mathbb{Z}$. [3]

Supposons maintenant $p = 7$. Alors $m = 4 = \frac{p+1}{2}$ et $n = 0$. Considérons l'élément τ de $\mathrm{U}_2(\mathbb{H})$ défini par $\tau(x, y) = (y, x)$. Il préserve $\mathscr{O} \times \mathscr{O}$ et permute donc également les Λ_x pour x dans X_p. Nous avons en fait évidemment $\tau(\Lambda_x) = \Lambda_{x^{-1}}$.
Il suffit donc pour conclure de remarquer (voir figure 1) que si G est le sous-groupe des permutations de l'ensemble $X_7 \subset \mathbb{F}_{49}^\times$ engendré par $x \mapsto x^{-1}$ et les multiplications par un élément d'ordre 4, alors G agit transitivement sur X_7.

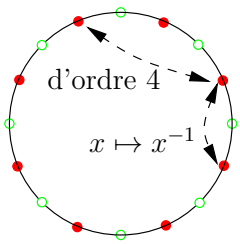

Figure 1.

Considérons enfin le cas plus délicat $p = 13$. Alors $m = 2$, $n = 0$ et $\mathscr{O}^\times = \{\pm 1\}$. Fixons Λ dans $\mathscr{X}(\mathscr{O})$. D'après le lemme 3.6, nous avons

$$240 = \mathrm{r}_\Lambda \, |\mathrm{U}(\Lambda)| \quad \text{et} \quad \sum_{[\Lambda] \in \mathrm{U}_2(\mathbb{H}) \backslash \mathscr{X}(\mathscr{O})} \mathrm{r}_\Lambda = 7 \, . \tag{6}$$

Si $\mathrm{U}_2(\mathbb{H})$ agit transitivement sur $\mathscr{X}(\mathscr{O})$, nous avons $\mathrm{r}_\Lambda = 7$ pour tout $\Lambda \in \mathscr{X}(\mathscr{O})$ et donc $240 = 7 \, |\mathrm{U}(\Lambda)|$, une contradiction car 240 n'est pas divisible pas 7. Donc $\mathrm{U}_2(\mathbb{H})$ admet au moins deux orbites distinctes, puis $\mathrm{r}_\Lambda \leq 6$ et $40 \leq |\mathrm{U}(\Lambda)| \leq 240$ pour tout $\Lambda \in \mathscr{X}(\mathscr{O})$.
Soit $\lambda \in \mathscr{O}$ tel que $\mathtt{n}(\lambda) = 12$; l'arithmétique des quaternions montre qu'il existe exactement $|\mathscr{O}^\times| \cdot 7 \cdot 4 = 56$ tels éléments λ. Nous avons $\mathtt{n}(\lambda) \equiv -1 \bmod p$, de sorte que $\lambda \in \mathscr{E}_{\mathscr{O}}$. La démonstration de la proposition 3.1 assure que dans la $\mathscr{O}$-base de Λ_λ définie par les élements $e_1 = (\pi^{-1}, \pi^{-1}\lambda)$ et $e_2 = (0, 1)$, on a pour tous $u, v \in \mathscr{O}$

$$f_0(e_1 u + e_2 v) = f_{\pi;\lambda}(u, v) = \mathtt{n}(u) \, + \, \mathtt{tr}(\, \bar{u} \, b \, v \,) \, + \, \mathtt{n}(v), \quad \text{avec} \quad b = \pi^{-1}\lambda \, .$$

En particulier, le cardinal de $\mathrm{U}(\Lambda_\lambda)$ est le nombre de couples de racines (α, β) de Λ_λ de produit scalaire $\mathbb{H}$-hermitien $h(\alpha, \beta) = \pi^{-1}\lambda$. Il est facile d'énumérer ces couples à l'aide d'un ordinateur : il suffit d'énumérer $\mathrm{R}(\Lambda_\lambda)$, ou ce qui revient au même, les (u, v) dans $\mathscr{O} \times \mathscr{O}$ tels que $\mathtt{n}(u) + \mathtt{n}(v) = 13$ et $\lambda u \equiv v \bmod \pi\mathscr{O}$. Décrivons le résultat. Nous pouvons prendre (voir par exemple [22, p. 98]) pour A l'algèbre de quaternions $\mathbb{Q} + \mathbb{Q}\, i + \mathbb{Q}\, j + \mathbb{Q}\, k$ avec $i^2 = -2$,

[3] On pourra d'abord observer que le groupe unitaire de $\Lambda \otimes \mathbb{Z}/2\mathbb{Z}$ est isomorphe à $\mathrm{Sp}_4(\mathbb{Z}/2\mathbb{Z}) \simeq \mathfrak{S}_6$. De plus, les fibres non vides de la projection canonique $\mathrm{R}(\Lambda) \to \Lambda \otimes \mathbb{Z}/2\mathbb{Z}$ sont de la forme $\{\alpha, -\alpha\}$ (une propriété classique de E_8). Ainsi, pour $\alpha \in \mathrm{R}(L)$, le sous-groupe de $\mathrm{U}(\Lambda)$ fixant $\alpha \bmod 2\Lambda$ est d'orde $2p^n$ d'après le lemme 3.6. Le noyau du morphisme naturel de $\mathrm{U}(\Lambda)$ vers le groupe unitaire de $\Lambda \otimes \mathbb{Z}/2\mathbb{Z}$ est un 2-groupe, il est donc égal à $\{\pm 1\}$. On conclut car un sous-groupe d'indice 2 (resp. 6) de $\mathfrak{S}_6$ est isomorphe à $\mathfrak{A}_6$ (resp. $\mathfrak{S}_5$).

$j^2 = -13$ et $ij = k = -ji$, et pour $\mathscr{O}$ l'ordre maximal $\mathbb{Z} + \mathbb{Z}\,i + \mathbb{Z}\,\frac{1+i-j}{2} + \mathbb{Z}\,\frac{2+i+k}{4}$. Nous pouvons alors prendre $\pi = j$. Considérons les deux éléments de $\mathscr{O}$ de norme 12

$$\lambda_1 = \frac{3+j-k}{2} \quad \text{et} \quad \lambda_2 = \frac{1+2i-j+k}{2}\,. \tag{7}$$

L'ordinateur nous dit que Λ_{λ_1} (resp. Λ_{λ_2}) contient exactement 48 (resp. 120) couples de racines (α, β) de produit scalaire $\mathbb{H}$-hermitien $j^{-1}\lambda_1$ (resp. $j^{-1}\lambda_2$). Cela montre

$$|\mathrm{U}(\Lambda_{\lambda_1})| = 48 \quad \text{et} \quad |\mathrm{U}(\Lambda_{\lambda_2})| = 120\,.$$

Il découle de la formule (6) les égalités $\mathrm{r}_{\Lambda_{\lambda_1}} = 5$, $\mathrm{r}_{\Lambda_{\lambda_2}} = 2$, puis $\mathrm{r}_{\Lambda_{\lambda_1}} + \mathrm{r}_{\Lambda_{\lambda_2}} = 7$, et donc $\mathrm{U}_2(\mathbb{H})\backslash\mathscr{X}(\mathscr{O}) = \{\Lambda_{\lambda_1}, \Lambda_{\lambda_2}\}$. Ceci démontre la proposition 3.3. □

D'après le corollaire 2.5 et la proposition 3.3, nous avons déterminé, à $\mathscr{O}$-équivalence près, les formes hamiltoniennes binaires définies positives de discriminant $-\frac{1}{D_A}$ (ou ce qui revient au même, de "covolume 1") réalisant $\gamma_2(\mathscr{O})$ lorsque $\mathscr{O}$ est principal. Décrivons les formes trouvées. La principalité de $\mathscr{O}$ entaîne que la norme réduite $\mathtt{n} : \mathscr{O} \to \mathbb{Z}_{\geq 0}$ est surjective. Le sous-ensemble $\mathscr{E}'_{\mathscr{O}} = \{\lambda \in \mathscr{O} \ : \ \mathtt{n}(\lambda) = D_A - 1\}$ de $\mathscr{E}_{\mathscr{O}}$ est donc non vide. Pour $\lambda \in \mathscr{E}'_{\mathscr{O}}$, nous avons simplement

$$f_{\pi;\lambda}(u, v) = \mathtt{n}(u) + \mathtt{tr}(\bar{u}\,\pi^{-1}\lambda\,v) + \mathtt{n}(v).$$

Pour $D_A = 2, 3, 5$ et 7, cette forme est donc l'unique forme de covolume 1, à $\mathscr{O}$-équivalence près, réalisant $\gamma_2(\mathscr{O})$. Pour $D_A = 13$, il y a deux classes d'équivalences, chacune étant représentée par une telle forme. Explicitons des choix possibles de π et λ dans chacun des cas.

- Pour $D_A = 2$ et $\mathscr{O}$ l'ordre de Hurwitz usuel, les choix $\pi = 1 + i$ et $\lambda = 1$ conduisent à $\pi^{-1}\lambda = \frac{1-i}{2}$, conformément à [20].

- Pour $D_A = 3, 7$, la $\mathbb{Q}$-algèbre A est engendrée par deux éléments i et j vérifiant $i^2 = -1$, $j^2 = -D_A$ et $ij = -ji$. L'élément i normalise $\mathbb{Z}[\frac{1+j}{2}]$, de sorte que l'on peut choisir l'ordre maximal $\mathscr{O}$ contenant i et $\frac{1+j}{2}$, et prendre $\pi = j$. On constate que $\lambda = 1 + i$ (cas $D_A = 3$) et $\lambda = 2 + i\frac{1+j}{2}$ (cas $D_A = 7$) conviennent, et conduisent respectivement à $\pi^{-1}\lambda = \frac{k-j}{3}$ et $\pi^{-1}\lambda = \frac{k-i-4j}{14}$, où l'on a posé $k = ij$.

- Pour $D_A = 5, 13$, la $\mathbb{Q}$-algèbre A est engendrée par deux éléments i et j vérifiant $i^2 = -2$, $j^2 = -D_A$ et $ij = -ji$. Dans le cas $D_A = 5$, on peut prendre pour $\mathscr{O}$ tout ordre maximal contenant j, puis $\pi = j$ et $\lambda = 2$, auquel cas nous avons $\pi^{-1}\lambda = -\frac{2}{5}j$. Dans le cas $D_A = 13$, l'analyse faite dans la démonstration de la proposition précédente montre que, pour le choix de $\mathscr{O}$ de cette démonstration et pour $\pi = j$, les deux classes sont obtenues en prenant pour λ les éléments λ_1 et λ_2 de la formule (7).

Remarque 3.8. — Il serait intéressant de poursuive cette analyse en déterminant des représentants de $\mathrm{U}_2(\mathbb{H})\backslash\mathscr{X}(\mathscr{O})$ pour d'autres discriminants D_A, et aussi d'expliciter une formule donnant la masse du groupoïde $\mathrm{U}_2(\mathbb{H})\backslash\mathscr{X}(\mathscr{O})$ pour un ordre maximal $\mathscr{O}$ général.

4. Ordres maximaux et réseaux euclidiens

Dans cette partie, nous rappelons certains aspects de la correspondance classique (voir par exemple [10, 17] et [23, Chap. 22]) entre classes de conjugaison d'ordres maximaux de A et certaines formes quadratiques ternaires. Nous utiliserons cette correspondance dans la partie 5 pour donner des caractérisations des ordres maximaux des algèbres de quaternions rationnelles définies dont la différente est principale.

Fixons un entier d strictement positif sans facteur carré, ayant un nombre impair de facteurs premiers. Fixons aussi une algèbre de quaternions A sur $\mathbb{Q}$, qui est définie, de discriminant d. Notons $\mathscr{R}(d)$ l'ensemble des classes d'isométrie de réseaux euclidiens entiers pairs L de rang 3, de déterminant $2d^2$, et tels que, pour tout premier p impair divisant d, le résidu de L_p est anisotrope.

Remarquons que si L est dans $\mathscr{R}(d)$, et si p est un premier impair divisant d, nous avons $\operatorname{res} L_p \simeq \operatorname{res} \mathscr{O}_p$, où $\mathscr{O}$ désigne un ordre maximal quelconque de A. En effet, le groupe abélien $\operatorname{res} L_p$ est d'ordre p^2 et ne peut être isomorphe à $\mathbb{Z}/p^2\mathbb{Z}$, car sa p-torsion serait constituée d'éléments isotropes. C'est donc un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel de dimension 2 muni d'une forme quadratique anisotrope, nécessairement à valeurs dans $(\frac{1}{p}\mathbb{Z})/\mathbb{Z} \simeq \mathbb{Z}/p\mathbb{Z}$ car p est impair. Il n'y a qu'une telle forme à isométrie près, donnée au lemme 2.2 1.

Proposition 4.1. — *L'application qui à un ordre maximal $\mathscr{O}$ de A associe le $\mathbb{Z}$-réseau $L(\mathscr{O})$ de ses éléments de trace nulle, muni du produit scalaire $(x, y) \mapsto \mathtt{tr}(\bar{x}\, y)$, induit une bijection de l'ensemble des classes de conjugaison d'ordres maximaux de A dans $\mathscr{R}(d)$. En particulier, $|\mathscr{R}(d)| = t_A$.*

Démonstration. — Montrons tout d'abord que cette application est bien définie. Soit $L = L(\mathscr{O})$. Rappelons que $\mathtt{tr} : \mathscr{O} \to \mathbb{Z}$ est surjective puisque $\mathscr{O}$ est maximal : c'est évident si $\mathscr{O}_2 \simeq \mathscr{M}_2(\mathbb{Z}_2)$ et cela découle de la surjectivité de $\mathrm{Tr}_{\mathbb{F}_4/\mathbb{F}_2} : \mathbb{F}_4 \to \mathbb{F}_2$ et de la formule (2) concernant la trace si 2 divise d. Ainsi, $\mathbb{Z}1 + L$ est un $\mathbb{Z}$-réseau d'indice 2 dans $\mathscr{O}$. Son déterminant est donc $4 \det \mathscr{O} = 4d^2$ puisque $\mathscr{O}$ est maximal, et L est bien de déterminant $2d^2$. Enfin, si p est un premier impair divisant d, nous avons $\operatorname{res} L_p \simeq \operatorname{res}(\mathbb{Z}\,1 \oplus L)_p = \operatorname{res} \mathscr{O}_p$, donc $\operatorname{res} L_p$ est anisotrope.

Montrons l'injectivité. Soient $\mathscr{O}$ et $\mathscr{O}'$ deux ordres maximaux de A tels que les $\mathbb{Z}$-réseaux euclidiens $L = L(\mathscr{O})$ et $L' = L(\mathscr{O}')$ soient isométriques. Notons A_0 l'espace quadratique des quaternions purs de A. Soit $u : A_0 \to A_0$ une isométrie telle que $u(L) = L'$. Par un résultat classique (voir par exemple [22, p. 11 et 6]), u est la conjugaison par un élément de $A - \{0\}$. Quitte à remplacer $\mathscr{O}'$ par un conjugué, nous pouvons donc supposer $L = L'$. Les $\mathbb{Z}$-réseaux $\mathscr{O}$ et $\mathscr{O}'$ contiennent alors tous deux le $\mathbb{Z}$-réseau $\mathbb{Z}1 + L$, avec l'indice 2. Cela montre $\mathscr{O}_p = \mathscr{O}'_p$ pour $p \neq 2$. On a trivialement $\mathscr{O}_2 = \mathscr{O}'_2$ si 2 divise d, par unicité de l'ordre maximal dans $A \otimes_{\mathbb{Q}} \mathbb{Q}_2$. Nous pouvons donc supposer $\mathscr{O}_2 = \mathscr{M}_2(\mathbb{Z}_2)$ et que $\mathbb{Z}_2 1 + L_2$ est le sous-espace des matrices de trace paire. Mais ce sous-espace engendre $\mathscr{M}_2(\mathbb{Z}_2)$ comme anneau, on en déduit $\mathscr{O}_2 \subset \mathscr{O}'_2$, puis $\mathscr{O}_2 = \mathscr{O}'_2$ par maximalité de $\mathscr{O}$. D'où $\mathscr{O} = \mathscr{O}'$.

Montrons la surjectivité. Soit L un élément de $\mathscr{R}(d)$. Montrons d'abord que l'espace quadratique $L \otimes_{\mathbb{Z}} \mathbb{Q}$ est isométrique à A_0. Par le théorème de Hasse–Minkowski, il suffit de montrer qu'il est de déterminant 2 (dans $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$), et anisotrope sur $\mathbb{Q}_p$ si et seulement si p divise d. Le premier point est clair car L est de déterminant $2d^2$. De plus, il suffit de vérifier le second point pour les premiers impairs. En effet, par la formule du produit pour le symbole

de Hilbert (voir par exemple [19, §4]) une forme quadratique sur $\mathbb{Q}^3$ supposée non dégénérée et définie positive est anisotrope sur $\mathbb{Q}_p$ pour un nombre impair de p.
Supposons donc p impair. Si p ne divise pas d, alors L_p est de déterminant dans $\mathbb{Z}_p^\times$ et de rang ≥ 3, donc isotrope sur $\mathbb{Q}_p$. Supposons que p divise d. Alors par hypothèse, $\operatorname{res} L_p$ est anisotrope et de rang 2 sur $\mathbb{Z}/p\mathbb{Z}$. En particulier, le produit scalaire n'est pas identiquement nul sur $L \otimes_{\mathbb{Z}} (\mathbb{Z}/p\mathbb{Z})$. Il existe donc e dans L_p avec $\frac{1}{2}\, e \cdot e \in \mathbb{Z}_p^\times$ et on a $L_p = \mathbb{Z}_p\, e \oplus P$ avec P de rang 2 et de même résidu que L_p. Nous avons donc $P^\sharp = \frac{1}{p} P$. Ainsi, il existe une $\mathbb{Z}_p$-base de L_p dans laquelle la forme quadratique $v \mapsto \frac{v.v}{2}$ est de la forme $(x, y, z) \mapsto ax^2 + pf(y, z)$ avec $a \in \mathbb{Z}_p^\times$ et $f : \mathbb{Z}_p^2 \to \mathbb{Z}_p$ quadratique anisotrope modulo p. Une telle forme à 3 variables est manifestement anisotrope sur $\mathbb{Q}_p$.
Nous avons montré que L se plonge isométriquement dans A_0. Nous pouvons donc supposer $L \subset A_0$, le produit scalaire de L étant $\mathtt{tr}(\bar{x}y)$. En particulier, puisque L est pair, $\mathtt{n}(x) \in \mathbb{Z}$ pour tout x dans L. Mais pour tous les a, b dans A_0, nous avons $a^2 = -\mathtt{n}(a)$ puis $ab + ba = -\mathtt{n}(a + b) + \mathtt{n}(a) + \mathtt{n}(b)$. Par conséquent, si $\epsilon_1, \epsilon_2, \epsilon_3$ est une $\mathbb{Z}$-base de L, alors

$$\mathscr{O}_1 = \mathbb{Z} + \mathbb{Z}\,\epsilon_1 + \mathbb{Z}\,\epsilon_2 + \mathbb{Z}\,\epsilon_3 + \mathbb{Z}\,\epsilon_1\epsilon_2 + \mathbb{Z}\,\epsilon_1\epsilon_3 + \mathbb{Z}\,\epsilon_2\epsilon_3 + \mathbb{Z}\,\epsilon_1\epsilon_2\epsilon_3$$

est un sous-anneau de A, et donc un ordre de A. Soit $\mathscr{O}$ un ordre maximal contenant $\mathscr{O}_1$. Alors $L(\mathscr{O}) = \mathscr{O} \cap A_0$ contient L, et a même déterminant d'après le premier paragraphe de la démonstration. D'où $L(\mathscr{O}) = L$, ce qui montre la surjectivité. □

Corollaire 4.2. — *Soit $L \in \mathscr{R}(d)$. Le résidu de L_2 est isomorphe à $(\mathbb{Z}/2\mathbb{Z})^3$ muni de la forme quadratique $(x, y, z) \mapsto \frac{1}{4}(x^2 + y^2 + z^2) \bmod \mathbb{Z}$ si d est pair, et à $\mathbb{Z}/2\mathbb{Z}$ muni de la forme quadratique $x \mapsto -\frac{1}{4}x^2 \bmod \mathbb{Z}$ sinon. En particulier,* $\operatorname{res} L$ *est anisotrope.*

Démonstration. — D'après la proposition précédente, nous pouvons supposer $L = L(\mathscr{O})$, avec $\mathscr{O}$ un ordre maximal de A. Notons $\mathscr{O}'$ l'ordre de Hurwitz. Le $\mathbb{Z}_2$-réseau $\mathscr{O}_2$ muni de $x \mapsto \mathtt{n}(x)$ est isométrique à $\mathscr{O}_2'$ muni de cette même forme si d est pair, et à $\mathscr{M}_2(\mathbb{Z}_2)$ muni de $x \mapsto \det(x)$ sinon. Le sous-réseau de trace nulle de $\mathscr{O}_2'$ est $\mathbb{Z}_2\, i \oplus \mathbb{Z}_2\, j \oplus \mathbb{Z}_2\, k$ avec $\mathtt{n}(i) = \mathtt{n}(j) = \mathtt{n}(k) = 1$. Celui de $\mathscr{M}_2(\mathbb{Z}_2)$ est $\mathbb{Z}_2\, d \oplus P$ où d est la matrice diagonale $(-1, 1)$, vérifiant $\det(d) = -1$, et P est le plan hyperbolique des matrices antidiagonales. Le résultat en découle. □

Introduisons maintenant un second ensemble de réseaux euclidiens associés aux ordres maximaux de A. Pour tout premier p impair et $a \in \mathbb{Z}$, notons $(\frac{a}{p})$ le symbole de Legendre de a modulo p. Soit $\mathscr{S}(d)$ l'ensemble des classes d'isométrie des réseaux euclidiens entiers pairs M de dimension 3 et de déterminant $2d$, tels que pour tout premier p impair divisant d, le résidu de M_p soit isomorphe au groupe $\mathbb{Z}/p\mathbb{Z}$ muni de la forme quadratique $x \mapsto \frac{a}{p}x^2 \bmod \mathbb{Z}$, avec $a \in \mathbb{Z}$ non nul modulo p tel que $(\frac{a}{p}) = -(\frac{-d/p}{p})$. Le résultat suivant dit que la condition portant sur les $\operatorname{res} M_p$ est superflue si d est premier.

Lemme 4.3. — *Si d est premier, alors tout réseau euclidien entier pair M de dimension 3 et de déterminant $2d$ appartient à $\mathscr{S}(d)$.*

Rappelons (voir par exemple [18, Chap. 5, §2 & §8]) que pour tout qe-module (V, q), la *somme de Gauss* de (V, q) est

$$\gamma(V, q) = |V|^{-\frac{1}{2}} \sum_{x \in V} e^{2i\pi\, q(x)}\ .$$

La somme du Gauss d'une somme orthogonale finie de qe-modules V_i est le produit des sommes de Gauss des V_i (cela s'applique en particulier à la décomposition en composantes primaires). La formule de la signature de Milgram implique l'égalité $\gamma(\operatorname{res} M) = e^{2i\pi s/8}$ pour tout réseau euclidien entier pair M de rang s. En particulier, cette somme de Gauss vaut $e^{3i\pi/4}$ pour M de rang 3.

Démonstration. — Nous pouvons supposer d impair. Par la formule de Milgram et la décomposition orthogonale $\operatorname{res} M = \operatorname{res} M_2 \oplus \operatorname{res} M_d$, nous avons

$$e^{3i\pi/4} = \gamma(\operatorname{res} M) = \gamma(\operatorname{res} M_2)\,\gamma(\operatorname{res} M_d). \tag{8}$$

Le résidu de M_2 est isométrique à $\mathbb{Z}/2\mathbb{Z}$ muni de la forme quadratique $x \mapsto \epsilon\frac{x^2}{4} \bmod \mathbb{Z}$ pour un certain signe $\epsilon = \pm 1$. Un calcul immédiat donne $\gamma(\operatorname{res} M_2) = e^{i\pi\epsilon/4}$. Le résidu de M_d est isométrique à $\mathbb{Z}/d\mathbb{Z}$ muni de la forme $x \mapsto ax^2/d \bmod \mathbb{Z}$ avec $a \in \mathbb{Z} - d\mathbb{Z}$. D'après un théorème de Gauss (voir par exemple [5, Chap. 2]), nous avons donc $\gamma(\operatorname{res} M_d) = (\frac{a}{d})$ pour $d \equiv 1 \bmod 4$, et $\gamma(\operatorname{res} M_d) = (\frac{a}{d})i$ sinon. Si $d \equiv 1 \mod 4$, la formule (8) entraîne donc $(\frac{a}{d}) = \epsilon = -1$. De même, si $d \equiv 3 \mod 4$ alors $(\frac{a}{d}) = \epsilon = 1$. Dans les deux cas, nous avons bien $(\frac{a}{d}) = (-1)^{\frac{d+1}{2}} = -(\frac{-1}{d})$. □

Lemme 4.4. — *Si M est dans $\mathscr{S}(d)$ alors* $\operatorname{res} M$ *est anisotrope et* $\operatorname{res} M_2 \simeq \mathbb{Z}/4\mathbb{Z}$.

Démonstration. — Comme $\operatorname{res} M_p$ est anisotrope pour p impair par définition, $\operatorname{res} M$ est anisotrope si, et seulement si, $\operatorname{res} M_2$ (qui est d'ordre 4) l'est. Montrons que ce dernier est isomorphe à $\mathbb{Z}/4\mathbb{Z}$, ou de manière équivalente, que sa forme quadratique q n'est pas à valeurs dans $(\frac{1}{4}\mathbb{Z})/\mathbb{Z}$. Pour tout premier p impair divisant d, la somme de Gauss $\gamma(\operatorname{res} M_p)$ est (toujours par le théorème de Gauss) une racine 4-ème de l'unité. Par la formule de Milgram et la multiplicativité de la somme de Gauss, $\gamma(\operatorname{res} M_2)$ est, comme $e^{3i\pi/4}$, une racine 8-ème primitive de l'unité. En particulier, $\gamma(\operatorname{res} M_2)$ n'est pas réelle, donc q n'est pas à valeurs dans $(\frac{1}{2}\mathbb{Z})/\mathbb{Z}$. Si q était à valeurs dans $(\frac{1}{4}\mathbb{Z})/\mathbb{Z}$, alors $\operatorname{res} M_2$ serait isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$ muni de la forme $(x, y) \mapsto \frac{1}{4}(ux^2 + vy^2) \bmod \mathbb{Z}$, pour certains signes u et v. Comme la somme de Gauss de $\mathbb{Z}/2\mathbb{Z}$ muni de $x \mapsto \frac{\epsilon}{4}x^2 \bmod \mathbb{Z}$ avec $\epsilon = \pm 1$ vaut $e^{2i\pi\epsilon/8}$, la somme de Gauss de $\operatorname{res} M_2$ serait une racine 4-ème de l'unité : une contradiction. □

Soient L un réseau euclidien entier pair et d un entier ≥ 1, supposés pour l'instant quelconques. Considérons les réseaux euclidiens $\Lambda = \Lambda(L; d)$ et $M = \mathrm{M}(L; d)$ définis par

$$\Lambda = \{x \in (d^{-1}L) \cap L^\sharp \ : \ d\,x \cdot x \equiv 0 \bmod 2\} \quad \text{et} \quad M = \sqrt{d}\,\Lambda\,. \tag{9}$$

Autrement dit, M est le plus grand sous-réseau pair[4] du réseau entier $N \cap N^\sharp$ avec $N = \frac{1}{\sqrt{d}}L$. En particulier, M est entier. Par définition, nous avons $L \subset \Lambda \subset L^\sharp$ et

$$\Lambda/L = \{x \in \operatorname{res} L \ : \ d\,x = 0 \ \text{ et } \ d\,q(x) = 0\}\,. \tag{10}$$

Lemme 4.5. — *Soient L un réseau euclidien entier pair et $d \geq 1$ un entier. Soit W le sous-groupe des éléments x de* $\operatorname{res} L$ *vérifiant $dx = 0$ et $dq(x) = 0$. Si q ne s'annule pas sur $W \cap W^\perp - \{0\}$, on a l'égalité* $\mathrm{M}(\mathrm{M}(L; d); d) = L$.

[4]Si L est un réseau entier, observer que l'application $L \to \mathbb{Z}/2\mathbb{Z}$, définie par $x \mapsto x \cdot x \bmod 2$, est un morphisme de groupes. Son noyau est donc un réseau : c'est le plus grand sous-réseau pair de L.

Démonstration. — Posons $\Lambda = \Lambda(L;d)$ et $M = \mathrm{M}(L;d)$. Nous avons déjà vu $L \subset \Lambda \subset L^\sharp$ et $\Lambda/L = W$. Pour des raisons générales, nous avons alors $L \subset \Lambda^\sharp \subset L^\sharp$, et $\Lambda^\sharp/L$ est l'orthogonal de W dans $\operatorname{res} L$. Par l'hypothèse sur W, le seul sous-espace isotrope de $\operatorname{res} L$ contenu dans $W \cap W^\perp$ est $\{0\}$. Ainsi, L est le plus grand sous-réseau pair de $\Lambda \cap \Lambda^\sharp$. Mais par définition $\mathrm{M}(M;d)$ est le plus grand sous-réseau pair de $N \cap N^\sharp$ où $N = \frac{1}{\sqrt{d}} M = \Lambda$: nous avons montré $\mathrm{M}(M;d) = L$. □

Notons que l'hypothèse du lemme portant sur W est automatiquement satisfaite si $\operatorname{res} L$ est anisotrope.

Proposition 4.6. — *L'application $L \mapsto M(L;d)$ induit des bijections $\mathscr{R}(d) \to \mathscr{S}(d)$ et $\mathscr{S}(d) \to \mathscr{R}(d)$ qui sont inverses l'une de l'autre.*

Démonstration. — Tout élément L de $\mathscr{R}(d)$ ou $\mathscr{S}(d)$ a son résidu anisotrope d'après le corollaire 4.2 et le lemme 4.4. On en déduit $\mathrm{M}(\mathrm{M}(L;d);d) = L$ d'après le lemme 4.5. De plus, si L et L' sont des réseaux entiers pairs d'un espace euclidien E, et si $g \in \mathrm{O}(E)$ envoie L sur L', alors $g(\mathrm{M}(L;d)) = \mathrm{M}(L';d)$ pour tout $d \geq 1$. Autrement dit, l'application $L \mapsto M(L;d)$ passe aux classes d'isométrie, et il ne reste qu'à voir qu'elle échange $\mathscr{R}(d)$ et $\mathscr{S}(d)$.
Supposons L dans $\mathscr{R}(d)$ ou $\mathscr{S}(d)$. Posons $\Lambda = \Lambda(L;d)$ et $M = \mathrm{M}(L;d)$. Montrons que Λ est d'indice 2 dans $L^\sharp$. Considérons pour cela le sous-espace $W = \Lambda/L$ de $\operatorname{res} L$, également donné par la formule (10). Pour tout premier p, notons $W_p = W \cap \operatorname{res} L_p$ la composante p-primaire de W. Soit p un premier impair divisant d. Alors par les définitions de $\mathscr{R}(d)$ et $\mathscr{S}(d)$, l'entier p annule $\operatorname{res} L_p$ et la forme quadratique de $\operatorname{res} L_p$ est à valeurs dans $(\frac{1}{p}\mathbb{Z})/\mathbb{Z}$, et donc $W_p = \operatorname{res} L_p$. Il ne reste qu'à voir que W_2 est d'indice 2 dans $\operatorname{res} L_2$. Si d est impair, $\operatorname{res} L_2$ est isomorphe à $\mathbb{Z}/2\mathbb{Z}$ et sa forme quadratique prend la valeur $\pm\frac{1}{4}$, donc $W_2 = 0$. Supposons d pair. Si L est dans $\mathscr{R}(d)$, en identifiant $\operatorname{res} L_2$ à $(\mathbb{Z}/2\mathbb{Z})^3$ comme dans le corollaire 4.2, nous constatons que W_2 est le sous-espace des $(x,y,z) \in (\mathbb{Z}/2\mathbb{Z})^3$ vérifiant $x+y+z = 0$. Enfin, si L est dans $\mathscr{S}(d)$, et en identifiant $\operatorname{res} L_2$ à $\mathbb{Z}/4\mathbb{Z}$ muni de la forme quadratique $x \mapsto \frac{u}{8}x^2 \bmod \mathbb{Z}$ pour un $u \in \mathbb{Z}$ impair comme dans le lemme 4.4, nous constatons que W_2 est le sous-espace $2\mathbb{Z}/4\mathbb{Z}$. Dans tous ces cas, W_2 est bien d'indice 2 dans $\operatorname{res} L_2$.
Nous venons de montrer que Λ est d'indice 2 dans $L^\sharp$. Donc $\det \Lambda = [L^\sharp : \Lambda]^2 \det L^\sharp = \frac{4}{\det L}$. Écrivons $\det L = 2d^r$, avec $r = 2$ ou $r = 1$ selon que L est dans $\mathscr{R}(d)$ ou $\mathscr{S}(d)$. Alors le déterminant de M est $d^3 \det \Lambda = d^3 \frac{4}{\det L} = 2d^{3-r}$, comme affirmé dans l'énoncé. Fixons p premier impair divisant d et examinons de plus près les liens entre $\operatorname{res} L_p$ et $\operatorname{res} M_p$. Comme Λ est d'indice 2 dans $L^\sharp$, nous avons $\Lambda_p = L_p^\sharp$. Le groupe $\operatorname{res} L_p$ est isomorphe à $(\mathbb{Z}/p\mathbb{Z})^r$. Nous pouvons donc toujours trouver une décomposition orthogonale en somme de deux $\mathbb{Z}_p$-sous-réseaux

$$L_p = A_p \oplus B_p \tag{11}$$

avec $\det A_p \in \mathbb{Z}_p^\times$ et B_p de $\mathbb{Z}_p$-rang r vérifiant $B_p^\sharp = p^{-1}B_p$. En particulier, nous avons $\Lambda_p = L_p^\sharp = A_p \oplus p^{-1}B_p$. Mais nous avons une isométrie[5] $M_p \simeq \langle d \rangle \otimes \Lambda_p$. Comme $\langle d \rangle \otimes B_p^\sharp$ est de déterminant dans $(d/p)^r\,\mathbb{Z}_p^\times \subset \mathbb{Z}_p^\times$, car $\det B_p^\sharp = \frac{1}{\det B_p}$ est dans $\frac{1}{p^r}\mathbb{Z}_p^\times$, nous en déduisons une isométrie

$$\operatorname{res} M_p \simeq \operatorname{res}(\langle d \rangle \otimes A_p) \simeq \langle d/p \rangle \otimes (A_p/pA_p), \tag{12}$$

[5]Si (V,q) est un espace quadratique et si m est dans $\mathbb{Z}$, notons $\langle m \rangle \otimes V$ l'espace quadratique (V, mq).

où A_p/pA_p ($\simeq (\mathbb{Z}/p\mathbb{Z})^{3-r}$) est muni de la forme quadratique $x \mapsto \frac{1}{p}\frac{x\cdot x}{2} \bmod \mathbb{Z}_p$. La forme bilinéaire d'un qe-module W qui est un $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel avec p premier peut être vue à valeurs dans $\mathbb{Z}/p\mathbb{Z}$ via l'isomorphisme naturel $(\frac{1}{p}\mathbb{Z})/\mathbb{Z} = \mathbb{Z}/p\mathbb{Z}$ induit par la multiplication par p, et possède donc un déterminant (ou "discriminant") qui est un élément de $(\mathbb{Z}/p\mathbb{Z})^\times$ modulo les carrés : nous le noterons $\delta(W)$. La relation (12) entraîne

$$\delta(\operatorname{res} M_p) = \delta(\langle d/p\rangle \otimes (A_p/pA_p)) = (d/p)^{3-r}\delta(A_p/pA_p).$$

La relation (11) entraîne $2p^r \equiv \det A_p \det B_p$ modulo les carrés de $\mathbb{Z}_p^\times$. En utilisant les congruences $\det A_p \equiv \delta(A_p/pA_p)$ et $p^{-r}\det B_p \equiv \delta(\operatorname{res} B_p)$ dans $(\mathbb{Z}/p\mathbb{Z})^\times$ modulo les carrés, on en déduit $2(d/p)^r \equiv \delta(A_p/pA_p)\,\delta(\operatorname{res} B_p)$. L'isomorphisme $\operatorname{res} L_p \simeq \operatorname{res} B_p$ entraîne donc au final

$$2d/p \;\equiv\; \delta(\operatorname{res} M_p)\,\delta(\operatorname{res} L_p)\ .$$

(toujours modulo les carrés de $(\mathbb{Z}/p\mathbb{Z})^\times$.) Supposons maintenant L dans $\mathscr{R}(d)$, et donc $r = 2$. Le discriminant d'un plan quadratique anisotrope sur $\mathbb{Z}/p\mathbb{Z}$ étant différent de -1, nous avons $\delta(\operatorname{res} L_p) \not\equiv -1$, donc $\operatorname{res} M_p$ est de rang 1 sur $\mathbb{Z}/p\mathbb{Z}$ avec $\frac{1}{2}\delta(\operatorname{res} M_p) \not\equiv -d/p$. Si $\operatorname{res} M_p$ est le $\mathbb{Z}/p\mathbb{Z}$-espace vectoriel $\mathbb{Z}/p\mathbb{Z}$ muni de la forme quadratique $x \mapsto \frac{1}{p}ax^2 \bmod \mathbb{Z}$, le symbole de Legendre de $\frac{1}{2}\delta(\operatorname{res} M_p)$ est par définition celui de a. Nous avons donc montré $(\frac{a}{p}) = -(\frac{-d/p}{p})$: M est dans $\mathscr{S}(d)$. De même, si L est dans $\mathscr{S}(d)$, on a $r = 1$ et $\frac{1}{2}\delta(\operatorname{res} L_p) \not\equiv -d/p$, puis $\operatorname{res} M_p$ est de rang 2 sur $\mathbb{Z}/p\mathbb{Z}$ avec $\delta(\operatorname{res} M_p) \not\equiv -1$, et M est dans $\mathscr{R}(d)$. □

***Remarque 4.7* (Genre de $\mathscr{S}(d)$).** — Soit M un réseau euclidien entier pair de dimension 3 et déterminant $2d$, avec d sans facteur carré. Soit p premier impair divisant d. Dans la terminologie de Conway [4, Chap. 15 §7], la classe d'isomorphisme du $\mathbb{Z}_p$-réseau M_p est caractérisée par son *symbole p-adique*, de la forme $1^{2e_p}\,p^{e'_p}$ pour certains signes $e_p, e'_p \in \{\pm 1\}$. Par définition, on a une décomposition orthogonale $M_p = A_p \oplus B_p$ avec A_p de $\mathbb{Z}_p$-rang 2 et de déterminant dans $\mathbb{Z}_p^\times$, B_p de $\mathbb{Z}_p$-rang 1 et de déterminant dans $p\mathbb{Z}_p^\times$, et e_p (resp. e'_p) est le symbole de Legendre de $\det A_p$ (resp. $p^{-1}\det B_p$) modulo p. On en déduit la relation

$$\left(\frac{2d/p}{p}\right) = e_p e'_p.$$

Par définition, le réseau M est dans $\mathscr{S}(d)$ si, et seulement si, on a l'égalité $e'_p = -(\frac{-2d/p}{p})$ pour tout premier p impair divisant d (la présence du 2 dans cette formule s'explique par le passage de la forme quadratique à la forme bilinéaire). De manière équivalente, M est dans $\mathscr{S}(d)$ si, et seulement si, on a l'égalité $e_p = -(\frac{-1}{p})$ pour tout premier p impair divisant d.

5. Sur les ordres maximaux de différente principale

Dans cette dernière partie, motivée par la proposition 3.1, nous donnons des caractérisations des ordres maximaux dont la différente est principale, puis de nombreux exemples de tels ordres.

Proposition 5.1. — *Toute algèbre de quaternions A sur $\mathbb{Q}$, qui est définie, admet au moins une classe de conjugaison d'ordres maximaux dont la différente est principale.*

Démonstration. — Montrons tout d'abord le lemme suivant.

Lemme 5.2. — *Toute algèbre de quaternions A sur $\mathbb{Q}$, qui est définie, admet un élément de carré $-D_A$, unique à conjugaison près.*

Démonstration. — L'existence équivaut à demander qu'il existe un plongement de $\mathbb{Q}$-algèbres de $\mathbb{Q}(\sqrt{-D_A})$ dans A. Un tel plongement existe car les diviseurs premiers de D_A, et la place réelle, sont ramifiés dans $\mathbb{Q}(\sqrt{-D_A})$. L'unicité découle du théorème de Skolem–Noether (voir [22, p. 6]). □

Soit $x \in A$ tel que $x^2 = -D_A$. Alors $\mathtt{n}(x) = D_A$. De plus, x étant entier sur $\mathbb{Z}$, il existe des ordres maximaux de A contenant x. Si $\mathscr{O}$ est un tel ordre, alors $\mathscr{O}x$ est un idéal à gauche entier de $\mathscr{O}$ de norme D_A. Par unicité, il est égal à la différente de $\mathscr{O}$, qui est donc principale. □

Illustrons la proposition 5.1 dans le cas de l'algèbre de quaternions de discriminant $D_A = 11$. Il est bien connu que c'est la $\mathbb{Q}$-algèbre engendrée par des éléments i et j vérifiant $i^2 = -1$, $j^2 = -11$ et $ij = -ji$ (voir [22, p. 98]). Elle contient exactement deux classes de conjugaison d'ordres maximaux : voir la table de [22, p. 154] ou le tableau final de cette note. Vérifions que ces deux classes possèdent des représentants $\mathscr{O}$ et $\mathscr{O}'$ contenant tous les deux l'élément j, de carré -11, et donc sont tous les deux de différente principale.

- D'une part, si $t = \frac{1+j}{2}$, l'ordre $\mathscr{O} = \mathbb{Z}[t] + i\,\mathbb{Z}[t]$ est de discriminant 11, donc maximal, et contient $j = 2t - 1$.

- D'autre part, si $t' = -\frac{1}{2} + \frac{i+k}{4}$ alors $\mathscr{O}'' = \mathbb{Z}[t'] + j\,\mathbb{Z}[t']$ est un ordre de A (noter que $(t')^2 = -t' - 1$ et j normalise $\mathbb{Z}[t']$) contenant j. Si $\mathscr{O}'$ désigne un ordre maximal contenant $\mathscr{O}''$, alors $\mathscr{O}'$ est non conjugué à $\mathscr{O}$. En effet, puisque l'anneau $\mathbb{Z}[t']$ contient les 6 unités $\pm 1, \pm t', \pm (t')^2$, il n'est pas contenu dans un conjugué de $\mathscr{O}$, qui ne contient que les 4 unités $\pm 1, \pm i$.

Voici le résultat de caractérisation des ordres maximaux de différente principale. Deux de ces caractérisations feront intervenir les bijections des propositions 4.1 et 4.6. On rappelle que si $\mathscr{O}$ est un ordre maximal de A, alors $L(\mathscr{O})$ désigne le $\mathbb{Z}$-réseau euclidien des quaternions purs de $\mathscr{O}$ muni de $\mathtt{tr}(\bar{x}y)$; nous posons aussi $M(\mathscr{O}) = \mathrm{M}(L(\mathscr{O}); D_A)$ (voir la formule (9)).

Théorème 5.3. — *Soient A une algèbre de quaternions sur $\mathbb{Q}$, qui est définie, et $\mathscr{O}$ un ordre maximal de A. Les propriétés suivantes sont équivalentes :*

1. *la différente $\mathscr{M}$ de $\mathscr{O}$ est principale ;*

2. *l'ordre maximal $\mathscr{O}$ contient un élément de norme (réduite) D_A ;*

3. *l'ordre maximal $\mathscr{O}$ contient un élément de carré $-D_A$;*

4. *le $\mathbb{Z}$-réseau euclidien $L(\mathscr{O})$ contient un élément x tel que $x \cdot x = 2D_A$ et $x \cdot y = 0 \mod D_A$ pour tout $y \in L(\mathscr{O})$;*

5. *le $\mathbb{Z}$-réseau euclidien $M(\mathscr{O})$ contient un élément x tel que $x \cdot x = 2$.*

Démonstration. — Puisque $\mathscr{M}$ est l'unique idéal de norme D_A, il est principal si, et seulement si, $\mathscr{O}$ contient un élément de norme D_A : les assertions 1 et 2 sont équivalentes.

Il est évident que l'assertion 3 implique l'assertion 2. Montrons la réciproque. Supposons d'abord $D_A = 2, 3$. Alors $\mathscr{O}$ est principal car $h_A = 1$, l'unicité à conjugaison près de $\mathscr{O}$ (puisque $t_A = 1$) et le lemme 5.2 montrent que $\mathscr{O}$ contient un élément de carré $-D_A$ (il serait bien sûr facile d'exhiber un tel élément dans ces cas). Si $D_A \neq 2, 3$, on conclut par le lemme 5.4 ci-dessous.
Montrons que l'assertion 3 implique l'assertion 4. Soit $x \in \mathscr{O}$ vérifiant $x^2 = -D_A$. Un tel x n'est pas dans $\mathbb{Q}$, il est donc de trace nulle et de norme D_A. Cela montre $x \in L(\mathscr{O})$ et $x \cdot x = 2D_A$. De plus, x est dans $\mathscr{M}$ par l'équivalence de 1 et 3. Nous en déduisons $\mathtt{tr}(x\mathscr{O}) \subset D_A\mathbb{Z}$ par la formule 3, puis $x \cdot y \equiv 0 \bmod D_A$ pour tout y dans $L(\mathscr{O})$.
Montrons que l'assertion 4 implique l'assertion 5. Soit x dans $L(\mathscr{O})$ vérifiant $x \cdot x = 2D_A$ et $x \cdot y \equiv 0 \bmod D_A$ pour tout y dans $L(\mathscr{O})$. D'après la formule 9, cela entraîne $\frac{1}{D_A}\, x \in \Lambda(L(\mathscr{O}), D_A)$, puis $x' = \frac{1}{\sqrt{D_A}} x \in \mathscr{M}(\mathscr{O})$. On conclut car $x' \cdot x' = 2$.
Montrons que l'assertion 5 implique l'assertion 2. Soit x dans $\mathscr{M}(\mathscr{O})$ vérifiant $x' \cdot x' = 2$. L'inclusion évidente $\sqrt{D_A}\mathscr{M}(\mathscr{O}) \subset L(\mathscr{O})$ entraîne que l'élément $x = \sqrt{D_A}x'$, de norme D_A, est dans $L(\mathscr{O})$, et donc dans $\mathscr{O}$. □

Lemme 5.4. — *Si $D_A \neq 2, 3$ et si $x \in \mathscr{O}$ est de norme D_A, alors $x^2 = -D_A$.*

Démonstration. — L'élément x n'appartient pas à $\mathbb{Q}$, car D_A est sans facteur carré, donc son polynôme minimal est $X^2 - tX + d$ avec $t = \mathtt{tr}(x) \in \mathbb{Z}$ et $d = \mathtt{n}(x) = D_A$. Comme A ramifie sur $\mathbb{R}$, nous avons $t^2 < 4d$. De même, pour tout premier p divisant d, comme A ramifie sur $\mathbb{Q}_p$, le polynôme $X^2 - tX + d$ est irréductible sur $\mathbb{Q}_p$, donc $t^2 - 4d$ n'est pas un carré dans $\mathbb{Z}_p$. Comme $1 + 4p\mathbb{Z}_p$ est constitué de carrés de $\mathbb{Z}_p^\times$, la factorisation $t^2 - 4d = t^2(1 - 4d/t^2)$ entraîne que tout diviseur premier de d divise également t. Puisque d est sans facteur carré, on montré que d divise t. En utilisant l'inégalité $t^2 < 4d$, on en déduit $t = 0$, ou $t = \pm d$ et $d < 4$. □

Exemples. — Le plus petit discriminant d'une algèbre de quaternions sur $\mathbb{Q}$, définie et ayant au moins 1 (respectivement 2) classe(s) de conjugaison d'ordres maximaux dont la différente est non principale, est 37 (respectivement 67). En effet, le tableau suivant donne, pour tous les entiers positifs $d \leq 100$ sans facteur carré ayant un nombre impair de facteurs premiers,

- le nombre $t(d)$ de classes de conjugaison d'ordres maximaux dans une algèbre de quaternions sur $\mathbb{Q}$ définie et de discriminant d (voir [22, p. 152] pour une formule exacte), ainsi que

- le nombre $t_{dnp}(d)$ (strictement inférieur à $t(d)$ par la proposition 5.1) de classes de conjugaison d'ordres maximaux dont la différente est non principale.

D'après les propositions 4.1 et 4.6, $t(d)$ est aussi le nombre de classes d'équivalence de formes quadratiques ternaires entières définies positives de déterminant $2d$ appartenant au genre décrit dans la remarque 4.7. Nous utilisons les tables de formes ternaires de Brandt et Intrau, recalculées et rendues disponibles sur le site de Nebe et Sloane [13] par Schiemann. Dans la terminologie de ces tables, le *discriminant* d'une telle forme désigne l'entier $-d$. Nous en déduisons par inspection la ligne $t(d)$ de la table ci-dessous.
De plus, l'équivalence entre les assertions 1 et 5 du théorème 5.3 montre que $t_{dnp}(d)$ est le nombre de classes d'équivalence de formes ternaires ci-dessus qui ne représentent pas l'entier 1.

Étant donné que dans les tables sus-citées les formes ternaires sont données sous forme réduite, une telle forme représente 1 si, et seulement si, son premier coefficient est 1 (alternativement, on peut aussi vérifier en utilisant par exemple le logiciel SAGE (algorithme LLL) que le réseau euclidien associé à cette forme a ses plus courts vecteurs de carré scalaire égal à 2). On en déduit la ligne $t_{dnp}(d)$ de la table ci-dessous.

d	2	3	5	7	11	13	17	19	23	29	30	31	37	41	42
t	1	1	1	1	2	1	2	2	3	3	1	3	2	4	1
t_{dnp}	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
d	43	47	53	59	61	66	67	70	71	73	78	79	83	89	97
t	3	5	4	6	4	2	4	1	7	4	1	6	7	7	5
t_{dnp}	1	0	1	0	1	0	2	0	0	2	0	1	1	1	3

Dans l'article [8], Ibukiyama donne une formule pour le nombre de classes de conjugaison d'ordre maximaux de A contenant un élément de carré $-d$ avec $d = D_A$, ou ce qui revient au même, pour la quantité $t(d) - t_{dnp}(d)$ d'après le théorème 5.3. Dans le cas où d est un nombre premier impair p, cette formule est particulièrement simple et due à Deuring. Elle s'écrit

$$t(p) - t_{dnp}(p) = \frac{h(-p) + h(-4p)}{2},$$

où $h(-m)$ désigne le nombre de classes d'équivalence propre de formes quadratiques binaires entières positives et primitives de discriminant $-m$ (voir [8, Rema. 2.13]). Cette formule confirme la table ci-dessus. Nous pourrions en fait la redémontrer sans grande difficulté à partir de l'équivalence entre les assertions 1 et 5 du théorème 5.3, et des propositions 4.1 et 4.6 (observer, en guise de point de départ, que pour M dans $\mathscr{S}(p)$ et x dans M avec $x \cdot x = 2$, l'orthogonal de $\mathbb{Z}x$ dans M est de dimension 2 et de déterminant égal à p ou $4p$).

Références

[1] H.-F. Blichfeldt, « The minimum values of positive quadratic forms in six, seven and eight variables », *Math. Z.* **39** (1935), p. 1-15.

[2] J. W. S. Cassels, *An introduction to the geometry of numbers*, Grundlehren der Mathematischen Wissenschaften, vol. 99, Springer, 1971.

[3] G. Chenevier & J. Lannes, *Automorphic forms and even unimodular lattices*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge., vol. 69, Springer, 2019.

[4] J. Conway & N. Sloane, *Sphere Packings, Lattices and Groups*, Grundlehren der Mathematischen Wissenschaften, vol. 290, Springer, 1988.

[5] H. Davenport, *Multiplicative number theory*, Graduate Texts in Mathematics, vol. 74, Springer, 2000.

[6] W. Ebeling, *Lattices and codes*, Advanced Lectures in Mathematics, Springer, 2013.

[7] M. Eichler, « Über die Idealklassenzahl total definiter Quaternionenalgebren », *Math. Z.* **43** (1938), p. 102-109.

[8] T. Ibukiyama, « On maximal orders of division quaternion algebras over the rational number field with certain optimal embeddings », *Nagoya Math. J.* **88** (1982), p. 181-195.

[9] V. Krafft & D. Osenberg, « Eisensteinreihen für einige arithmetisch definierte Untergruppen von $\mathrm{SL}_2(\mathbb{H})$ », *Math. Z.* **204** (1990), n° 3, p. 425-449.

[10] C. Latimer, « The classes of integral sets in a quaternion algebra », *Duke Math. J.* **3** (1937), p. 237-247.

[11] J. Martinet, *Perfect lattices in Euclidean spaces*, Grundlehren der Mathematischen Wissenschaften, vol. 327, Springer, 2003.

[12] L. J. Mordell, « The definite quadratic forms in eight variables with determinant unity », *J. Math. Pures Appl.* **17** (1938), p. 41-46.

[13] G. Nebe & N. Sloane, « The Brandt-Intrau-Schiemann Table of Even Ternary Quadratic Forms », `http://www.math.rwth-aachen.de/~Gabriele.Nebe/LATTICES/Brandt_2.html`.

[14] A. Oppenheim, « The minima of positive definite Hermitian binary quadratic forms », *Math. Z.* **38** (1934), p. 538-545.

[15] J. Parkkonen & F. Paulin, « On the arithmetic and geometry of binary Hamiltonian forms », *Algebra Number Theory* **7** (2013), n° 1, p. 75-115.

[16] ———, « Integral binary Hamiltonian forms and their waterworlds », `https://arxiv.org/abs/1810.06222`, 2018.

[17] M. Peters, « Ternäre und quaternäre quadratische Formen und Quaternionenalgebren », *Acta Arith.* **15** (1969), p. 329-365.

[18] W. Scharlau, *Quadratic and Hermitian forms*, Grundlehren der Mathematischen Wissenschaften, vol. 270, Springer, 1985.

[19] J.-P. Serre, *Cours d'arithmétique*, Le Mathématicien, vol. 2, Presses Universitaires de France, 1970.

[20] A. Speiser, « Über die Minima Hermitescher Formen », *J. Reine Angew. Math.* **167** (1932), p. 88-97.

[21] N. M. Vetchinkin, « Uniqueness of the classes of positive quadratic forms on which the values of Hermite constants are attained for $6 \leq n \leq 8$ », *Proc. Steklov Inst. Math.* **152** (1980), p. 34-86.

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

[23] J. Voight, « Quaternion algebras », `https://math.dartmouth.edu/~jvoight/quat.html`.

[24] H. Weyl, « Theory of reduction for arithmetical equivalence I, II », *Trans. Am. Math. Soc.* **48** (1940), p. 126-164.

Gaëtan Chenevier, Laboratoire de Mathématiques d'Orsay, UMR 8628 CNRS, Université Paris-Saclay, F-91405 Orsay, France • *E-mail :* `gaetan.chenevier@math.cnrs.fr`

Frédéric Paulin, Laboratoire de Mathématiques d'Orsay, UMR 8628 CNRS, Université Paris-Saclay, F-91405 Orsay, France • *E-mail :* `frederic.paulin@universite-paris-saclay.fr`