MINIMUM EUCLIDIEN DES ORDRES MAXIMAUX DANS LES ALGÈBRES CENTRALES À DIVISION

THÈSE N^{O} 3717 (2006)

PRÉSENTÉE LE 11 JANVIER 2006

À LA FACULTÉ DES SCIENCES DE BASE

Chaire des structures algébriques et géométriques

PROGRAMME DOCTORAL EN MATHÉMATIQUES

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

POUR L'OBTENTION DU GRADE DE DOCTEUR ÈS SCIENCES

PAR

Jérôme CHAUBERT

mathématicien diplômé de l'Université de Lausanne
de nationalité suisse et originaire de Corsier-Sur-Vevey (VD)

acceptée sur proposition du jury:

Prof. M. A. Shokrollahi, président du jury
Prof. E. Bayer Fluckiger, directrice de thèse
Prof. J.-C. Belfiore, rapporteur
Dr J.-P. Cerri, rapporteur
Prof. D. Testerman, rapporteur

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Suisse
2007

Résumé

Ce travail est consacré à l'étude des minima euclidiens des ordres maximaux dans les algèbres centrales simples.

Dans un premier temps, nous définissons la notion de réseau idéal dans un cadre non nécessairement commutatif. Soit A une algèbre semi-simple sur $\mathbb{Q}$. Un réseau idéal sur A est un triple (I, α, τ) où I est un idéal de A, τ est une involution positive sur $A_{\mathbb{R}}$, autrement dit, vérifiant $\mathrm{tr}_{A_{\mathbb{R}}/\mathbb{R}}(x\alpha x^{\tau}) > 0$ pour tout $x \in I_{\mathbb{R}}$ et α est un élément inversible de $A_{\mathbb{R}} = A \otimes_{\mathbb{Q}} \mathbb{R}$ fixe par τ. Nous étudions ensuite les propriétés des réseaux idéaux, notamment les invariants d'Hermite, afin de lier la notion de minimum euclidien d'un ordre maximal Λ à celle des réseaux idéaux de la forme (Λ, α, τ). Explicitement, nous démontrons qu'il est possible de borner le minimum euclidien de Λ à l'aide des invariants d'Hermite associés aux réseaux idéaux de Λ.

Cette borne nous permettra, entre autres, de calculer les minima euclidiens de plusieurs familles infinies d'ordres maximaux, dans le cas des corps de quaternions sur $\mathbb{Q}$.

Dans un deuxième temps, nous développons d'autres méthodes pour calculer ou borner, inférieurement et supérieurement, le minimum euclidien d'un ordre maximal d'un corps de quaternions. Ces méthodes nous permettent de donner une liste exhaustive des corps de quaternions euclidiens sur $\mathbb{Q}$, ainsi que leur minimum euclidien. Les mêmes méthodes nous permettent de résoudre partiellement le cas des corps de quaternions sur un corps quadratique.

Nous donnons, pour finir, des bornes des minima euclidiens de certains ordres maximaux de corps de quaternions sur un corps cyclotomique.

Mots clés : minimum euclidien, algèbre centrale simple, algèbre à division, quaternions, corps de quaternions, ordre maximal, réseau idéal, anneau euclidien.

Abstract

This work concerns the study of Euclidean minima of maximal orders in central simple algebras.

In the first part, we define the concept of ideal lattice in the non-commutative case. Let A be a semi-simple algebra over $\mathbb{Q}$. An ideal lattice over A is a triple (I, α, τ) where I is an ideal of A, α is a unit in $A_{\mathbb{R}} = A \otimes_{\mathbb{Q}} \mathbb{R}$ fixed by τ and τ is a positive involution on $A_{\mathbb{R}}$, in other words, $\mathrm{tr}_{A_{\mathbb{R}}/\mathbb{R}}(x\alpha x^{\tau}) > 0$ for all $x \in I_{\mathbb{R}}$. We study ideal lattices, especially their Hermite invariant, to link the concepts of Euclidean minimum of a maximal order and ideal lattices of the form (Λ, α, τ). Namely, we show that we can bound the Euclidean minimum of Λ by the Hermite invariant of the ideal lattices of Λ.

This upper bound allows us to calculate the Euclidean minima of some infinite families of maximal orders, when A is a quaternion skew field over $\mathbb{Q}$.

In the second part, we look for other ways to find upper and lower bounds of the euclidean minimum of a maximal order in a quaternion skew field. This research leads us to an exhaustive list of euclidean quaternion skew fields over $\mathbb{Q}$, and their euclidean minima. The quadratic case has also been studied but remains partially unsolved.

At the end, we give bounds for Euclidean minima of some maximal orders of quaternion skew fields over cyclotomic fields.

Keywords : Euclidean minimum, central simple algebra, division algebra, quaternions, quaternion skew fields, maximal order, ideal lattice.

Remerciements

En premier lieu, je tiens à remercier Eva Bayer Fluckiger de m'avoir offert un sujet d'étude passionnant et de m'avoir accueilli dans son groupe tout au long de mon travail de doctorat. Je remercie également Jean-Paul Cerri, Donna Testermann et Jean-Claude Belfiore d'avoir accepté d'expertiser mon travail ainsi qu'Amin Shokrollahi d'avoir présidé ce jury.

Un grand merci à toutes les personnes qui sont passées par la chaire de structures algébriques et géométriques pour les moments (mathématiques ou non) passés en leur compagnie. Je tiens en particulier à remercier Christian, Sylvia, Julien et Ivan d'avoir eu la patience de répondre à certaines interrogations mathématiques parfois un peu étranges ; Christine, Andrea, Marusia et Lara d'avoir partagé les petits soucis et les grandes satisfactions liées à l'enseignement. Merci encore à Klaas, Tania et Mathieu pour leur patience et leurs conseils durant les dernières semaines de mon travail. Je tiens à remercier tout particulièrement Lara dont les conseils allaient des mathématiques, à la posture à adopter devant un tableau noir, en passant par la façon de respirer !

Un immense merci à mes anciens collègues de l'IGAT et à mes anciens camarades d'études, en particulier à Nicolas, Jean-Marie, Raphaëlle, Caleb et David avec qui j'ai fait mes premiers pas dans la recherche lors de mon travail de diplôme et au début de ma thèse. Un merci particulier au même Nicolas qui m'a fait découvrir la clarinette, la photo, l'effet Larsen, et le quatuor à corde pour hélicoptère !

Je remercie du fond du coeur mes parents de m'avoir toujours soutenu dans mes choix durant mes études et dans la vie en général ; et de m'avoir donné l'envie d'apprendre. Un grand merci à mes amis avec qui j'ai vécu, et continue à vivre, les plus belles aventures : mon frère Sylvain, Carole, Marie, Vincent, Annick, Aline et Cindy.

Mille mercis à Marco et Martine d'avoir eu la patience de relire mon texte.

Un merci tout particulier à mes meilleurs amis Leslie et Marie-Jo pour toutes ces heures, passées, présentes et à venir de discussions, d'échanges, de cinéma, de gastronomie, de voyages et de jeux.

Finalement, un gigantesque merci à Muriel de partager ma vie et de la rendre si belle, de savoir me faire rire et d'être toujours là pour moi.

****

Table des matières

Introduction

L'objet de ce travail est l'étude du minimum euclidien des ordres maximaux dans les algèbres à division sur un corps de nombres.

Un anneau A est dit euclidien (à droite) pour l'algorithme $N : A \longrightarrow \mathbb{N}$ si pour tout $a, b \in A$ avec $b \neq 0$, il existe $q, r \in A$ tels que

$$a = bq + r \quad \text{et} \quad N(r) < N(b).$$

Les premiers exemples de tels anneaux sont $\mathbb{Z}$ avec la valeur absolue pour l'algorithme N et l'anneau des polynômes sur un corps avec le degré des polynômes pour l'algorithme. Dans le cadre de l'arithmétique il y a également certains anneaux d'entiers de corps de nombres, avec la norme pour l'algorithme, par exemple $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$ et $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$. Dans ce contexte arithmétique, on dira qu'un corps de nombres K, c'est-à-dire une extension algébrique de $\mathbb{Q}$, est euclidien si son anneau des entiers est euclidien pour la norme.

En arithmétique, l'intérêt historique pour l'euclidianité réside dans le fait qu'un anneau euclidien est principal, donc factoriel. Par conséquent la notion a préoccupé les mathématiciens du XIX$^{\text{ème}}$ dans l'infructueuse tentative, entre autres, de trouver une démonstration au théorème de Fermat-Wiles.

L'étude des corps de nombres euclidiens s'avère être un sujet difficile. Il faudra attendre plus d'un siècle pour avoir une liste exhaustive des corps quadratiques réels euclidiens. Le cas quadratique imaginaire, en revanche, peut-être rapidement résolu par des arguments géométriques. La liste exhaustive des corps cyclotomiques ou cubiques euclidiens n'est toujours pas connue.

Lorsque l'on s'intéresse à l'euclidianité pour la norme, une notion de minimum euclidien, qui "mesure" le fait d'être euclidien, s'impose naturellement.

On définit alors, pour un corps de nombres K, le minimum euclidien de K de la façon suivante :

$$\mathrm{M}(K) = \inf\left\{\lambda \in \mathbb{R} \mid \forall\ \xi \in K,\ \exists\ \gamma \in \mathcal{O}_K \text{ tel que } |\mathrm{N}_{K/\mathbb{Q}}(\xi - \gamma)| < \lambda\right\}$$

où $\mathcal{O}_K$ est l'anneau des entiers de K. Afin d'illustrer en quoi cette notion "mesure" l'euclidianité de K, remarquons que, pour tout $a, b \in \mathcal{O}_K$ avec $b \neq 0$, il existe $q, r \in \mathcal{O}_K$ tels que

$$a = bq + r \text{ et } \mathrm{N}_{K/\mathbb{Q}}(r) \leq \mathrm{M}(K) \cdot \mathrm{N}_{K/\mathbb{Q}}(b).$$

De plus, pour tout $k < \mathrm{M}(K)$, il existe $a, b \in A$ avec $b \neq 0$ tels que, pour tout $q, r \in A$ avec $a = bq + r$,

$$\mathrm{N}_{K/\mathbb{Q}}(r) \geq k \cdot \mathrm{N}_{K/\mathbb{Q}}(b).$$

En particulier, si $\mathrm{M}(K) < 1$ alors K est euclidien et si $\mathrm{M}(K) > 1$ alors K n'est pas euclidien pour la norme.

Les travaux anciens sur le minimum euclidien sont nombreux et une bonne partie d'entre eux sont résumés dans [Lem95]. La plupart de ces résultats s'appuient sur des considérations géométriques. C'est justement pour pouvoir approcher le problème géométriquement que les mathématiciens ont introduit la notion de minimum inhomogène, qui est une extension du minimum euclidien à $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$. Explicitement, on définit

$$\mathrm{M}(K_{\mathbb{R}}) = \inf\left\{\lambda \in \mathbb{R} \mid \forall\ \xi \in K_{\mathbb{R}},\ \exists\ \gamma \in \mathcal{O}_K \text{ tel que } |\mathrm{N}_{K_{\mathbb{R}}/\mathbb{Q}}(\xi - \gamma)| < \lambda\right\}.$$

Comme $\mathrm{M}(K) \leq \mathrm{M}(K_{\mathbb{R}})$, il est naturel de s'intéresser au minimum inhomogène de K. Parmi les questions encore ouvertes sur le minimum inhomogène, citons l'importante conjecture de Hermann Minkowski (1864-1909) :

Pour tout corps de nombres totalement réel K de degré n,

$$\mathrm{M}(K_{\mathbb{R}}) \leq 2^{-n}\sqrt{d_K}.$$

Plus récemment, il convient de citer les résultats obtenus par Eva Bayer-Fluckiger ainsi que ceux obtenus par Jean-Paul Cerri. Eva Bayer-Fluckiger démontre dans [BF99] et [BF06] qu'on peut borner le minimum inhomogène de K à l'aide des invariants d'Hermite associés aux réseaux idéaux construits sur les idéaux principaux de K. Explicitement, un réseau idéal est un couple (I, α) où I est un idéal de K, $\alpha \in K$ vérifie $\mathrm{T}_{K_{\mathbb{R}}/\mathbb{Q}}(x\alpha\bar{x}) > 0$ pour tout $x \in K_{\mathbb{R}}$ non nul et $\bar{}$ est l'involution canonique sur $K_{\mathbb{R}}$. Le résultat, simplifié, s'énonce alors de la façon suivante :

Soit $(\mathcal{O}_K, \alpha)$ un réseau idéal. Alors

$$\mathrm{M}(K_{\mathbb{R}}) \leq \left(\frac{\tau(\mathcal{O}_K, \alpha)}{\gamma_{\min}(\mathcal{O}_K)} \right)^n. \tag{1}$$

En s'appuyant sur ce résultat, Eva Bayer Fluckiger démontre dans [BF06], la conjecture de Minkowski pour les corps cyclotomiques, c'est-à-dire les corps de la forme $K = \mathbb{Q}(\xi_n)$ où ξ_n est une n$^{\text{ème}}$ racine de l'unité dans $\mathbb{C}$. Elle démontre également ce résultat pour les corps $\mathbb{Q}(\xi_{p^k} + \xi_{p^k}^{-1})$ où p est un premier impair.

Dans [Cer06], Jean-Paul Cerri démontre que si le rang rang des unités de K est strictement supérieur à 1, alors le minimum inhomogène et le minimum euclidien de K coïncident et sont rationnels. Dans [Cer] se trouve la description d'un algorithme qui permet de calculer le minimum inhomogène ainsi qu'une importante table de minima euclidiens illustrant cet algorithme (jusqu'en degré 8).

Après ce rapide survol des résultats relatifs à ce domaine, venons-en à ce qui nous préoccupera dans ce travail.

Nous nous placerons dans le cadre où K est un corps de nombres, A un corps gauche central sur K et Λ un ordre maximal de A. L'ordre Λ possède des propriétés s'approchant de celle de $\mathcal{O}_K$, autrement dit Λ peut être vu comme "un anneau des entiers" de $\mathcal{O}_K$ à la différence près qu'il n'est pas unique. La notion de norme sur K est remplacée par celle de norme réduite sur A. Nous pouvons donc définir, comme dans le cas commutatif, les minima euclidien et inhomogène de Λ :

$$\mathrm{M}(\Lambda) = \inf \left\{ \lambda \in \mathbb{R} \mid \forall\, \xi \in A,\ \exists\, \gamma \in \Lambda \text{ tel que } |\mathrm{nr}_{A/\mathbb{Q}}(\xi - \gamma)| < \lambda \right\}$$

et

$$\mathrm{M}(\Lambda_{\mathbb{R}}) = \inf \left\{ \lambda \in \mathbb{R} \mid \forall\, \xi \in A_{\mathbb{R}},\ \exists\, \gamma \in \Lambda \text{ tel que } |\mathrm{nr}_{A_{\mathbb{R}}/\mathbb{Q}}(\xi - \gamma)| < \lambda \right\}.$$

Comme les minima euclidiens de deux ordres maximaux de A ne coïncident pas nécessairement, on ne peut pas définir le minimum euclidien de A.

Le but de ce travail est d'abord de définir la notion de réseau idéal dans ce cadre non commutatif et d'étudier le comportement de ses invariants afin de démontrer une formule similaire à (1). Cette étude sur les réseaux idéaux fait l'objet du premier chapitre et le théorème sur la borne supérieure du

minimum inhomogène est énoncé dans la section 2.5 du chapitre II :

Soient A une algèbre à division de dimension m^2 sur un corps de nombres K de degré n et Λ un ordre maximal de A, alors

$$\mathrm{M}(\Lambda_{\mathbb{R}}) \leq \left(\frac{\tau_{\min}(\Lambda)}{\gamma_{\min}(\Lambda)}\right)^{nm/2}. \tag{2}$$

Nous démontrons également, dans le chapitre II, que sous certaines conditions sur K, les minima euclidien et inhomogène de Λ coïncident et sont rationnels.

Le dernier chapitre est entièrement consacré au cas particulier des corps de quaternions. Nous y obtenons des résultats généraux qui seront ensuite utilisés pour calculer ou borner des minima euclidiens. L'essentiel de ces résultats se résume de la façon suivante :

i) si $K = \mathbb{Q}$, alors $\mathrm{M}(\Lambda) = \frac{\max(\Lambda,1)}{2}$,

ii) si A est totalement définie, alors $\mathrm{M}(\Lambda) \geq \mathrm{M}(K)^2$,

iii) si K est principal et A totalement indéfinie, alors

$$\mathrm{M}(\Lambda) \leq \mathrm{M}(K)$$

avec égalité sous certaines conditions sur les points critiques de K,

iv) on peut donner une liste de conditions nécessaires et suffisantes sur A pour réaliser E_8 comme réseau idéal de A.

Les points i) à iv) ainsi que l'inégalité 2 nous permettent de donner explicitement, pour certaines familles infinies d'ordres maximaux, une liste de minima euclidiens, lorsque $K = \mathbb{Q}$. Ils nous permettent également de donner une liste exhaustive des corps de quaternions euclidiens sur $\mathbb{Q}$ (résultat connu dans le cas défini) et de donner leur minimum euclidien. Nous déterminons encore l'ensemble des corps de quaternions euclidiens sur un corps quadratique imaginaire, ainsi que leur minimum euclidien. Nous traitons également le cas des corps quadratiques réels qui reste partiellement ouvert. En dernier lieu, nous donnons une liste de résultats concernant le minimum eucliden des corps de quaternions sur un corps cyclotomique.

Pour obtenir les résultats résumés jusqu'ici, nous avons dû, à maintes reprises, trouver des familles infinies d'ordres maximaux. Ces recherches ont

été menées avec l'aide des logiciels Magma et Pari. Nous avons en particulier travaillé avec un ensemble de fonctions Magma développées par Markus Kirschmer lors de son travail de diplôme sous la direction de Gabrielle Nebe. Ces fonctions permettent de calculer l'ensemble des ordres maximaux d'un corps de quaternions totalement défini. Afin de trouver des familles infinies, nous avons développé une série de méthodes Magma qui permettent d'étudier le comportement de ces ordres maximaux lorsqu'on leur introduit des variables.

Dans le cadre du calcul du minimum euclidien des corps de quaternions sur $\mathbb{Q}$, nous avons également développé des méthodes, en Magma, qui permettent, sous certaines conditions, de calculer une cellule contenant la cellule de Voronoi d'une famille de réseaux. Explicitement, nous sommes en mesure de borner, sous certaines conditions, le rayon de recouvrement d'un réseau de petite dimension dont la matrice du produit scalaire dépend d'un paramètre. Dans tous les cas traités, la borne est en fait atteinte.

D'autres procédés informatiques, toujours en Magma, ont été implémentés, notamment pour exclure l'euclidianité de certains corps de quaternions sur un corps quadratique réel et pour calculer la forme standard d'une algèbre de quaternions.

Chapitre I

Réseaux idéaux

Ce chapitre met en place les notions dont nous aurons besoin dans la suite du travail. Les quatre premières sections contiennent de nombreux résultats connus qui forment les bases de la théorie des ordres dans les algèbres centrales simples, ainsi que des résultats techniques sur la forme bilinéaire "trace". Les sections suivantes introduisent la notion de réseaux idéaux dans ce cadre et traitent des propriétés de ces objets. En particulier, dans la section 1.7, nous démontrons un résultat analogue à l'inégalité entre norme et trace d'un corps de nombres dans le cadre des algèbres centrales simples. Les deux dernières sections sont consacrées au déterminant et aux invariants d'Hermite d'un réseau idéal.

Nous nous placerons parfois dans un cadre plus général que nécessaire. Pour le lecteur qui n'est pas familiarisé avec les notions d'algèbres centrales simples et d'ordres dans ces algèbres, nous conseillons de garder en tête les exemples qui suivent lors de la lecture de ce chapitre.

Le corps K est un corps de nombres (par exemple $K = \mathbb{Q}\left(\sqrt{2}\ \right)$), l'algèbre A est une algèbre de quaternions (par exemple, $A = (-1,-1)_K$). L'anneau R est l'anneau des entiers de K (dans cet exemple $R = \mathbb{Z}[\sqrt{2}]$). Un exemple d'ordre de A est

$$\Lambda = R \oplus iR \oplus jR \oplus kR.$$

Ici Λ n'est pas maximal. Pour avoir en tête un ordre maximal, on peut prendre, dans ce cadre,

$$\Lambda = \mathbb{Z}[\sqrt{2}] \oplus \sqrt{2}\frac{1+i}{2}\mathbb{Z}[\sqrt{2}] \oplus \sqrt{2}\frac{1+j}{2}\mathbb{Z}[\sqrt{2}] \oplus \frac{1+i+j+k}{2}\mathbb{Z}[\sqrt{2}].$$

Les notions de norme et trace réduite se résument comme suit :

i) la norme réduite de $x \in A$ est le produit de x par son conjugué : $\mathrm{nr}_{A/K}(x) = xx^{\gamma}$,

ii) la trace réduite de $x \in A$ est la somme de x et de son conjugué : $\mathrm{tr}_{A/K}(x) = x + x^{\gamma}$,

où γ est l'involution canonique sur l'algèbre de quaternions A (voir la proposition 3.1.3).

1.1 Ordres et idéaux

Dans cette section, R désigne un anneau intègre et nœthérien, K son corps des fractions et A une K-algèbre de dimension finie r.

Définition 1.1.1. *Un élément $\alpha \in A$ est dit entier sur R s'il existe un polynôme unitaire f, à coefficients dans R tel que $f(\alpha) = 0$. La clôture intégrale R^{cl} de R dans A est l'ensemble des éléments de A entiers sur R.*

Si A est commutative alors R^{cl} est un anneau. Sinon, par exemple pour les algèbres centrales simples, ce n'est pas nécessairement le cas (c.f. [Vig80] p.20).

Théorème 1.1.2. *Soit $\alpha \in A$. Les conditions suivantes sont équivalentes :*

i) L'élément α est entier sur R.

ii) Le module $R[\alpha]$ est de génération finie sur R.

iii) Il existe un sous-anneau B de A tel que B est un module de génération finie sur R et α est un élément de B.

Preuve : Voir [Rei03] p. 3 thm. 1.10 (par exemple).

Notation 1.1.3. *Soit M un R-sous-module de A, on pose*

$$KM = \left\{ \sum_{i \in I} k_i m_i \mid k_i \in K,\ m_i \in M, |I| < \infty \right\}.$$

Définition 1.1.4.

i) Un R-réseau complet de A (ou un idéal de A) est un R-sous-module de type fini M de A vérifiant $KM = A$.

ii) Un ordre (ou un R-ordre) Λ de A est un sous-anneau de A qui est également un R-réseau complet. Un ordre maximal est un ordre qui est maximal pour l'inclusion.

iii) L'ordre à gauche d'un idéal M est donné par

$$\mathcal{O}_l(M) = \{x \in A \mid xM \subset M\}$$

et son ordre à droite est défini, de la même manière, par

$$\mathcal{O}_r(M) = \{x \in A \mid Mx \subset M\}.$$

On vérifie facilement que ce sont bien des ordres.

iv) Un idéal à gauche d'un ordre Λ est un idéal I de A vérifiant $\Lambda = \mathcal{O}_l(I)$. Un idéal à droite de Λ est un idéal I de A vérifiant $\Lambda = \mathcal{O}_r(I)$ et I est dit bilatère si $\Lambda = \mathcal{O}_l(I) = \mathcal{O}_r(I)$.

REMARQUE : Dans le cas ou A est un corps de nombres, les idéaux de A, avec la définition précédente, sont exactement les idéaux fractionnaires de A au sens usuel.

Définition 1.1.5. *Soient A une K-algèbre de dimension r, a un élément de A et*

$$\begin{array}{rccc} \mu_a : & A & \longrightarrow & A \\ & x & \longmapsto & ax \end{array}$$

l'endomorphisme de K-espace vectoriel de multiplication à gauche par a. Le polynôme caractéristique de a, noté $C_{A/K,a}$, est le polynôme caractéristique de μ_a. Le polynôme minimal de a, noté m_a, est le polynôme minimal de μ_a. Ces deux polynômes sont à coefficients dans K. Le terme constant de $C_{A/K,a}$ est appelé la norme de a et on le note $\mathrm{N}_{A/K}(a)$. Le coefficient de degré $r-1$ de $C_{A/K,a}$ est appelé la trace de a et on le note $\mathrm{T}_{A/K}(a)$.

Proposition 1.1.6. *Tout élément d'un ordre Λ est entier sur R. De plus, si R est intégralement clos, le polynôme minimal et le polynôme caractéristique d'un élément de Λ sont à coefficients dans R.*

PREUVE : Voir [Rei03] p. 110 thm. 8.6.

Cette proposition met en évidence le rapport entre les notions de clôture intégrale et d'ordres maximaux. En particulier, R^{cl} est un ordre si est seulement si R^{cl} est l'unique ordre maximal dans A.

1.2 Norme et trace réduites sur une algèbre semi-simple

Soient K un corps et A une K-algèbre de dimension finie. On dit que A est centrale si son centre est K (i.e. si $K = \{x \in A \mid xy = yx \text{ pour tout } y \in A\}$). On dit que A est simple si les seuls idéaux bilatères de A sont A et $\{0\}$ (ici "idéal bilatère" est entendu au sens d'idéal de A en tant qu'anneau et non pas au sens de la définition 1.1.4).

Proposition 1.2.1. *Soit A une algèbre centrale simple sur un corps K. Les affirmations suivantes sont vérifiées :*

i) il existe un corps gauche D, de centre K, tel que $A \cong \mathrm{M}_n(D)$ et si D' est un corps gauche avec $A \cong \mathrm{M}_r(D')$, alors $r = n$ et $D \cong D'$.

ii) Il existe une extension E de K telle que $A \otimes_K E \cong \mathrm{M}_m(E)$. On dit que E est un corps déployant de A. Si F est une extension de E alors F est encore un corps déployant de A. Il existe toujours un corps déployant séparable sur K.

iii) La dimension de A comme K-espace vectoriel est un carré. Plus précisément, si E est un corps déployant de A avec $A \otimes_K E \cong \mathrm{M}_m(E)$ et si D est un corps gauche (de centre K) tel que $A \cong \mathrm{M}_n(D)$, alors $\dim_K(A) = n^2m^2$.

Preuve : La première affirmation est une conséquence du théorème de structure de Wedderburn (voir, par exemple, [Rei03] p.91 théorème 7.4). Les deux suivantes découlent directement des résultats de la section 7b du chapitre 1 de [Rei03] (voir, en particulier, le théorème 7.15 p.97).

Définition 1.2.2. *Soient A une algèbre centrale simple sur un corps K, E un corps déployant et a un élément de A. Soit encore h un isomorphisme entre $A \otimes_K E$ et $\mathrm{M}_m(E)$. Le polynôme caractéristique réduit de a est le polynôme caractéristique de $h(1 \otimes a)$. La trace réduite de a est la trace de $h(1 \otimes a)$ et la norme réduite, son déterminant. On les note respectivement $rC_a(t)$, $\mathrm{tr}_{A/K}(a)$ et $\mathrm{nr}_{A/K}(a)$. Le polynôme $rC_a(t)$ est à coefficients dans K et $\mathrm{tr}_{A/K}(a)$ et $\mathrm{nr}_{A/K}(a)$ sont des éléments de K.*

Remarque : Il faut vérifier (voir [Rei03] section 9 du chapitre 2) que ces notions ne dépendent ni du choix de E ni du choix de h et que $rC_a(t) \in K[t]$.

Afin d'étendre les notions de norme et trace réduite, nous avons besoin de définir les algèbres semi-simples et séparables.

Notation 1.2.3. *Soient A un anneau et M un module à gauche sur A. On note*

$$\text{ann } M = \{a \in A \mid aM = 0\}$$

l'annulateur de M. C'est un idéal bilatère de A. Soit

$$\mathcal{M} = \{[M] \mid [M] \text{ est une classe d'isomorphisme de } A\text{-modules simples }\},$$

on note

$$\text{rad } A = \bigcap_{[M]\in\mathcal{M}} \text{ann } M$$

le radical de Jacobson de A.

Définition 1.2.4. *Un anneau A est dit semi-simple si son radical de Jacobson est nul.*

Définition 1.2.5. *Une algèbre A sur un corps K est dite semi-simple si elle est semi-simple en tant qu'anneau.*

Remarque : Si A est un anneau artinien à gauche (c'est le cas d'une K-algèbre de dimension finie) alors A est semi-simple si et seulement si A est une somme directe finie de sous-anneaux simples : $A = A_1 \oplus \cdots \oplus A_t$ avec $A_iA_j = 0$ (en particulier, si $a, b \in A$ alors $ab = a_1b_1 + \cdots + a_tb_t$) et on appelle les A_i les composantes simples de A.

Définition 1.2.6. *Une algèbre A de dimension finie sur un corps K est dite séparable si elle est semi-simple et si le centre de chaque composante simple de A est une extension de corps séparable de K.*

Remarque : Si A_i désigne une composante simple de A, alors son centre est toujours une extension de corps finie de K. La seule exigence de la définition précédente est donc que cette extension soit séparable.

Proposition 1.2.7. *Soient $A = A_1 \oplus \cdots \oplus A_t$ une algèbre séparable sur K, K_i le centre de A_i et R_i la clôture intégrale de R dans K_i. Alors les R-ordres de A sont de la forme $\Lambda = \Lambda_1 \oplus \cdots \oplus \Lambda_t$ où les Λ_i sont des R_i-ordres de A_i. De plus Λ est maximal si et seulement si Λ_i est maximal pour tout i.*

Preuve : Voir [Rei03] thm 10.5 p.128.

Définition 1.2.8. *Soit K un corps et L une extension de K de degré n. A tout élément a de L, on associe $\tilde{a} \in \mathrm{M}_n(K)$, la matrice de la multiplication à gauche par a par rapport à une K-base fixée de L. De la même manière à un polynôme $f(X) = \sum a_i X^i \in L[X]$ on associe*

$$\tilde{f}(X) = \sum \tilde{a}_i X^i \in \mathrm{M}_n(K[X]).$$

Finalement, on définit

$$\begin{array}{rccc} \mathrm{N}_{L/K} : & L[X] & \longrightarrow & K[X] \\ & f & \longmapsto & \det(\tilde{f}). \end{array}$$

et

$$\begin{array}{rccc} \mathrm{T}_{L/K} : & L[X] & \longrightarrow & K[X] \\ & f & \longmapsto & \mathrm{Tr}(\tilde{f}). \end{array}$$

On appelle $\mathrm{N}_{L/K}$ la fonction norme et $\mathrm{T}_{L/K}$ la fonction trace.

Le lecteur pourra se référer au paragraphe 9b p.117 de [Rei03] pour plus de détails et propriétés.

Remarque : Les fonctions norme et trace restreintes au corps L sont simplement les fonctions usuelles de norme et trace sur une extension de corps.

Nous allons maintenant définir les notions de polynôme caractéristique réduit, trace réduite et norme réduite sur une algèbre semi-simple.

Définition 1.2.9. *Soit $A = A_1 \oplus \cdots \oplus A_t$ une algèbre semi-simple de dimension finie sur K. Pour tout i, notons K_i le centre de A_i. Soit $a = a_1 + \cdots + a_t$ un élément de A. On définit le polynôme caractéristique réduit de a :*

$$rC_{A/K,a} = \prod_{i=1}^{t} \mathrm{N}_{K_i/K}(rC_{A_i/K_i,a_i})$$

où $rC_{A_i/K_i,a_i}$ est le polynôme caractéristique réduit de a_i (au sens de la définition 1.2.2). Pour définir la norme et la trace réduite on pose

$$rC_{A/K,a}(t) = t^m + a_{m-1}t^{m-1} + \cdots + a_1 t + a_0 \in K[t]$$

et on définit $\mathrm{nr}_{A/K}(a) = a_0$, la norme réduite de a et $\mathrm{tr}_{A/K}(a) = a_{m-1}$, la trace réduite de a.

Notation : Les composantes simples d'une algèbre semi-simple A sont des algèbres centrales simples sur K_i. On notera $r_i = m_i^2 = [A_i : K_i]$ la dimension de A_i sur K_i.

Proposition 1.2.10. *Avec les mêmes notations que ci-dessus et celle de la définition 1.1.5, les relations suivantes sont vérifiées :*

i) $\mathrm{tr}_{A/K}(a) = \sum_{i=1}^{t} \mathrm{T}_{K_i/K}(\mathrm{tr}_{A_i/K_i}(a_i))$.

ii) $\mathrm{nr}_{A/K}(a) = \prod_{i=1}^{t} \mathrm{N}_{K_i/K}(\mathrm{nr}_{A_i/K_i}(a_i))$.

iii) $C_{A/K,a} = \prod_{i=1}^{t} \mathrm{N}_{K_i/K}(rC_{A_i/K_i,a_i})^{m_i}$.

iv) $\mathrm{T}_{A/K}(a) = \sum_{i=1}^{t} m_i \mathrm{T}_{K_i/K}(\mathrm{tr}_{A_i/K_i}(a_i))$ *et*
$\mathrm{N}_{A/K}(a) = \prod_{i=1}^{t} \mathrm{N}_{K_i/K}(\mathrm{nr}_{A_i/K_i}(a_i)^{m_i})$.

v) $\mathrm{tr}_{A/K}(ab) = \mathrm{tr}_{A/K}(ba)$, $\mathrm{tr}_{A/K}(a+b) = \mathrm{tr}_{A/K}(a) + \mathrm{tr}_{A/K}(b)$ *et* $\mathrm{tr}_{A/K}(ka) = k\mathrm{tr}_{A/K}(a)$.

vi) $\mathrm{nr}_{A/K}(ab) = \mathrm{nr}_{A/K}(a)\mathrm{nr}_{A/K}(b)$ *et* $\mathrm{nr}_{A/K}(ka) = k^m \mathrm{nr}_{A/K}(a)$

vii) $C_{A/K,a} = \prod_{i=1}^{t} C_{A_i/K,a_i} = \prod_{i=1}^{t} rC_{A_i/K,a_i}^{m_i}$

pour tout $a, b \in A$ *et tout* $k \in K$.
Si de plus A *est séparable, alors l'application*

$$\begin{array}{rccc} \tau : & A \times A & \longrightarrow & K \\ & (a,b) & \longmapsto & \mathrm{tr}_{A/K}(ab) \end{array}$$

définit une forme bilinéaire symétrique non dégénérée.

Preuve : voir [Rei03] paragraphe 9b (p. 121 et p. 116).

Proposition 1.2.11. *Soient* A *une algèbre centrale simple de dimension* $r = m^2$ *sur* K, L *un corps et* $\sigma : K \longrightarrow L$ *un homomorphisme de corps. Soit encore* B *une algèbre simple de même dimension sur* L. *L'application* σ *induit naturellement une structure de* K*-algèbre sur* B. *Supposons qu'il existe* $\Sigma : A \longrightarrow B$, *un homomorphisme injectif de* K*-algèbres tel que* $\Sigma\big|_K = \sigma$. *Alors*

$$rC_{B/L,\Sigma(a)} = \sigma(rC_{A/K,a})$$

où σ *agit sur les coefficients de* $rC_{A/K,a}$.
En particulier

$$\sigma(\mathrm{tr}_{A/K}(a)) = \mathrm{tr}_{B/L}(\Sigma(a))$$

et

$$\sigma(\mathrm{nr}_{A/K}(a)) = \mathrm{nr}_{B/L}(\Sigma(a)).$$

Preuve : Observons d'abord comment se comporte le polynôme caractéristique, plutôt que le polynôme caractéristique réduit. Soient $\mathcal{B} = \{e_1, \ldots, e_r\}$ une K-base de A et a un élément de A. Pour tout $1 \leq i \leq r$, il existe $a_{1i}, \ldots, a_{ri} \in K$ tels que

$$ae_i = a_{1i}e_1 + \cdots + a_{ri}e_r$$

d'où

$$\Sigma(ae_i) = \Sigma(a)\Sigma(e_i) = \sigma(a_{1i})\Sigma(e_1) + \cdots + \sigma(a_{ri})\Sigma(e_r)$$

de sorte que la matrice de la multiplication à gauche par a par rapport à la base $\mathcal{B}$ est donnée par

$$(a_{ij})_{1\leq i,j\leq r}$$

et celle de la multiplication à gauche par $\Sigma(a)$ par rapport à la base $\Sigma(\mathcal{B})$ est donnée par

$$(\sigma(a_{ij}))_{1\leq i,j\leq r}.$$

Comme le polynôme caractéristique est une fonction polynômiale des coefficients de la matrice,

$$C_{B/L,\Sigma(a)} = \sigma(C_{A/K,a}).$$

Or, par la proposition précédente, $C_{B/L,\Sigma(a)} = (rC_{B/L,\Sigma(a)})^m$ et $C_{A/K,\Sigma(a)} = (rC_{A/K,\Sigma(a)})^m$, ce qui nous permet de conclure.

□

De façon similaire au cas commutatif, on peut définir les notions de discriminant, de différente, de norme d'un idéal, etc. On retrouve également beaucoup de propriétés similaires au cas commutatif, notamment celle selon laquelle un idéal bilatère d'un ordre de A se décompose de façon unique en produit d'idéaux bilatères premiers. Le but de ce travail n'étant pas de discuter ces questions, nous ne donnerons ici que les définitions et les résultats utiles pour la suite. Pour les autres notions, nous renvoyons le lecteur à [Rei03].

Définition 1.2.12. *Soit Λ un ordre de A, I un idéal à droite de Λ et*

$$b : I \times I \longrightarrow K$$

une forme R-bilinéaire non dégénérée, qu'on étend linéairement à A.

i) Le dual de I par rapport à b est l'idéal

$$I_b^* = \{a \in A \mid b(a, I) \subset R\}.$$

ii) L'inverse de I est l'idéal $I^{-1} = \{a \in A \mid IaI \subset I\}$.

iii) La différente de Λ est l'idéal entier

$$\mathcal{D}(\Lambda) = \tilde{\Lambda}^{-1}$$

où

$$\tilde{\Lambda} = \{a \in A \mid \mathrm{tr}(a\Lambda) \subset R\}$$

est la différente inverse de Λ.

iv) Le déterminant de b est

$$\det(b) = \langle \det(b(x_i, x_j)_{1\leq i,j\leq r}) \mid x_1, \ldots, x_r \in I \rangle$$

c'est-à-dire l'idéal fractionnaire de R engendré par le detérminant des matrices $b(x_i, x_j)_{1\leq i,j\leq r}$ où les x_i, x_j parcourent I.

v) Le discriminant de Λ est l'idéal $\mathrm{d}(\Lambda) = \det(\tau)$ où τ est la forme bilinéaire trace définie dans la proposition 1.2.10. C'est un idéal entier de R.

REMARQUES : Si Λ est un R-module libre de base $\{e_1, \ldots, e_r\}$, alors $\mathrm{d}(\Lambda)$ est l'idéal principal engendré par $\det((\mathrm{tr}(e_i e_j))_{1\leq i,j\leq r})$ (c'est une conséquence de la proposition 1.2.13). Autre fait important : le discriminant est indépendant de l'ordre maximal choisi (voir [Rei03] p.218).

Si I est un R-module libre de base $\mathcal{B} = \{e_1, \ldots, e_r\}$, alors il existe une unique base $\mathcal{B}^* = \{e_1^*, \ldots, e_r^*\}$ de I_b^* vérifiant $b(e_i, e_j^*) = \delta_{ij}$. On l'appelle la base duale de B.

La notion habituelle de déterminant d'une forme bilinéaire b sur un module libre M de dimension n est le déterminant de la matrice $(b(e_i, e_j))_{1\leq i,j\leq n}$ où $\{e_1, \ldots, e_n\}$ est une base de M. La proposition suivante permet de faire le lien entre cette définition et celle donnée au point iv) de la définition 1.2.12.

Proposition 1.2.13. *Si I est un module libre sur R et $b : I \times I \longrightarrow K$ une forme bilinéaire non dégénérée, alors*

$$\det(b) = \det(b(e_i, e_j)_{1\leq i,j\leq r}) \cdot R$$

où $\mathcal{B} = \{e_1, \ldots, e_r\}$ est une R-base de I.

PREUVE : Il est clair que $\det(b(e_i, e_j)_{1\leq i,j\leq r}) \cdot R \subset \det(b)$. Réciproquement si $X = \det(b(x_i, x_j)_{1\leq i,j\leq r})$ et que l'on exprime $x_k = t_{1k}e_1 + \cdots + t_{rk}e_k$ dans la base $\mathcal{B}$. Posons $B = b(e_i, e_j)_{1\leq i,j\leq r}$ et $T = (t_{ij})_{1\leq i,j\leq r}$. Alors $X = T^t \cdot B \cdot T$ et donc $\det(X) \in \det(B) \cdot R$.

□

Il nous reste, dans cette section, une notion à définir. Il s'agit de la norme d'un idéal I d'une K-algèbre semi-simple A.

Définition 1.2.14. *Soient R un anneau commutatif nœthérien, M un R-module à gauche de type fini et m un élément de M. On définit les notions suivantes :*

i) Le spectre de R, noté $Spec(R)$ est l'ensemble des idéaux premiers de R.

ii) L'annulateur de m est l'idéal de R donné par

$$ann(m) = \{a \in R \mid am = 0\}.$$

iii) Le support de M est l'ensemble

$$Supp(M) = \{\mathcal{P} \in Spec(R) \mid M_{\mathcal{P}} \neq 0\}.$$

iv) L'ensemble des idéaux premiers associés à M est

$$Ass(M) = \{\mathcal{P} \in Spec(R) \mid \mathcal{P} = ann(m) \text{ pour un } m \in M\}.$$

Théorème 1.2.15. *Soient R un anneau commutatif nœthérien et M un R-module de génération finie. Alors il existe une chaîne de modules*

$$0 = M_n \subset \cdots \subset M_0 = M$$

avec $M_i/M_{i+1} \cong R/\mathcal{P}_i$ où les $\mathcal{P}_i$ sont des idéaux premiers de R. De plus,

$$Ass(M) \subset \{\mathcal{P}_0, \ldots, \mathcal{P}_n\} \subset Supp(M).$$

La suite $(M_i)_{0 \leq i \leq n}$ est appelée une suite de composition de M.

Preuve : Voir [Bou85] chapitre IV, §1,n°4, théorèmes 1 et 2.

□

Proposition 1.2.16. *Soit R un anneau commutatif nœthérien et M un R-module de type fini. Supposons que R est de dimension 1 (c'est-à-dire que les idéaux premiers non nuls de R sont maximaux) et que M est un module de torsion. Soit $\{\mathcal{P}_0, \ldots, \mathcal{P}_n\}$ comme dans le théorème précédent. Alors*

$$Ass(M) = \{\mathcal{P}_0, \ldots, \mathcal{P}_n\} = Supp(M).$$

Preuve : D'après [Bou85] chapitre IV, §1,n°4, théorèmes 2, les éléments minimaux de ces trois ensembles coïncident. Dans notre cas, ces ensembles ne contiennent que des idéaux maximaux ; l'idéal premier nul étant exclu de $\mathrm{Ass}(M)$ grâce au fait que M est un module de torsion. Ces trois ensembles n'ont donc que des éléments minimaux.

□

Définition 1.2.17. *Soit M un module de génération finie sur un anneau nœthérien R de dimension 1. On définit l'idéal ordre de M, noté $\mathrm{ord}_R M$, comme suit. Si $M = 0$ alors $\mathrm{ord}_R M = R$, si M est sans torsion alors $\mathrm{ord}_R M = 0$. Si M est un module de torsion et $(M_i)_{0\leq i\leq n}$ est une suite de composition de M avec $M_i/M_{i+1} \cong R/\mathcal{P}_i$, on pose*

$$\mathrm{ord}_R M = \prod_{i=0}^{n} \mathcal{P}_i.$$

Le théorème de Jordan-Hölder nous assure que les $R/\mathcal{P}_i$ et donc les $\mathcal{P}_i$ ne dépendent pas du choix de la suite de composition.

A partir d'ici, sauf mention du contraire, R est un anneau de Dedekind, A désigne une algèbre séparable sur un corps $K = \mathrm{Frac}(R)$, Λ un ordre de A et I un idéal à droite de Λ.

Définition 1.2.18. *Soient Λ un ordre de A et I un idéal de Λ. Alors il existe $\beta \in R$ avec $\beta I \subset \Lambda$. On définit la norme de I, que l'on note $\mathrm{N}_{A/K}(I)$, par*

$$\mathrm{N}_{A/K}(I) = \beta^{-r}\mathrm{ord}_R(\Lambda/\beta I).$$

On vérifie que $\mathrm{N}_{A/K}(I)$ ne dépend pas du choix de β et que c'est une fonction multiplicative pour les idéaux.

Remarque : Cette définition est une généralisation de la définition naturelle dans le cas commutatif. En effet, si K est un corps de nombres, $\mathcal{O}_K$ son anneau des entiers et I un idéal de $\mathcal{O}_K$, alors on vérifie que $\mathrm{ord}_{\mathbb{Z}}\mathcal{O}_K/I$ est l'idéal engendré par $|\mathcal{O}_K/I| = \mathrm{N}_{K/\mathbb{Q}}(I)$. Plus généralement si N et M sont des $\mathbb{Z}$-modules libres de même rang avec $N \subset M$, alors $\mathrm{ord}_{\mathbb{Z}}(M/N) = |M/N| \cdot \mathbb{Z}$.

Théorème 1.2.19. *Soient A une algèbre centrale simple et I un idéal de Λ. On a $\mathrm{N}_{A/K}(I) = \mathrm{nr}_{A/K}(I)^m$ où $\mathrm{nr}_{A/K}(I)$ est l'idéal de R engendré par $\{\mathrm{nr}_{A/K}(x) \mid x \in I\}$. De plus $\mathrm{nr}_{A/K}$ est une fonction multiplicative pour les idéaux.*

Preuve : Voir [Rei03] thm 24.11 p.214. et corollaire 24.12 p.215.

Proposition 1.2.20. *Soient Λ un ordre de A et I un idéal à droite de Λ.*

i) Si $0 \longrightarrow N \longrightarrow M \longrightarrow P \longrightarrow 0$ est une suite exacte courte de modules à gauche sur R, alors

$$\mathrm{ord}_R M = \mathrm{ord}_R N \cdot \mathrm{ord}_R P.$$

ii) Le discriminant de Λ est la norme de la différente de Λ :

$$\mathrm{d}(\Lambda) = \mathrm{N}_{A/K}(\mathcal{D}(\Lambda)).$$

PREUVE : Voir [Rei03] p.50 et p.218

Soit I un idéal à droite d'un ordre maximal Λ, et $b : I \times I \longrightarrow K$, une forme R-bilinéaire non dégénérée. Soit encore $\mathcal{P}$ un idéal premier de R. Nous notons $I_{\mathcal{P}}$ (respectivement $R_{\mathcal{P}}$) le localisé de I (respectivement de R) en $\mathcal{P}$ et nous étendons b par linéarité à $I_{\mathcal{P}}$ (en considérant $I \subset I_{\mathcal{P}}$) et même à A. Comme R est un anneau de Dedekind, $R_{\mathcal{P}}$ est un anneau de valuation discrète. En particulier, c'est un anneau principal et comme I est un R-module de type fini sans torsion (car $I \subset A$), alors $I_{\mathcal{P}}$ est un $R_{\mathcal{P}}$-module libre. De plus $\mathrm{rang}(I_{\mathcal{P}}) = \dim_K(A) = r$. On a même mieux :

Proposition 1.2.21. *Il existe une K-base $B = \{e_1, \ldots, e_r\}$ de A dont les éléments appartiennent à I et qui est également une $R_{\mathcal{P}}$-base de $I_{\mathcal{P}}$.*

PREUVE : Soit $\{f_1, \ldots, f_r\}$ une K-base de A. Alors il existe $\alpha \in R$ tel que $\{\alpha f_1, \ldots, \alpha f_r\} \subset I$ (car $f_i \in A = KI$). Il est clair que $\{\alpha f_1, \ldots, \alpha f_r\}$ est libre sur $R_{\mathcal{P}}$ (car libre sur K) et que la dimension de $I_{\mathcal{P}}$ est inférieure ou égale à celle de A. En d'autres termes, $\{\alpha f_1, \ldots, \alpha f_r\}$ est la base cherchée. □

REMARQUE : Si $B = \{e_1, \ldots, e_r\}$ est une K-base de A contenue dans I, alors il existe une unique K-base de A, notée $B^* = \{e_1^*, \ldots, e_r^*\}$ vérifiant $b(e_i, e_j^*) = \delta_{ij}$. C'est la base duale de B.

On montre facilement les résultats suivants, avec I, b et $\mathcal{P}$ comme ci-dessus.

Proposition 1.2.22. *On a les résultats suivants :*

i) Soit $\{e_1, \ldots, e_r\}$ une $R_{\mathcal{P}}$-base de $I_{\mathcal{P}}$ contenue dans I (comme dans la proposition précédente). Alors

$$\det(b)_{\mathcal{P}} = \det(b(e_i, e_j)_{1 \leq i,j \leq r}) \cdot R_{\mathcal{P}}.$$

ii) Soit $I^* = I_b^* = \{x \in A \mid b(x, I) \subset R\}$. Alors

$$(I_{\mathcal{P}})^* = (I^*)_{\mathcal{P}}.$$

iii) Pour tout R-module M de type fini, on a

$$(\mathrm{ord}_R M)_{\mathcal{P}} = \mathrm{ord}_{R_{\mathcal{P}}} M_{\mathcal{P}}.$$

PREUVE : Les deux premières affirmations se vérifient facilement et pour la troisième se référer à [Rei03] thm 4.20 p. 53.

Lemme 1.2.23. *Soit R un anneau principal. Soient M et N deux R-modules libres de même rang r. Soient $\{m_1, \ldots, m_r\}$ une base de M, $\{n_1, \ldots, n_r\}$ une base de N et $\beta \in R$ tel que $\beta N \subset M$. On considère la matrice*

$$A = (a_{ij})_{1 \leq i,j \leq r} \in \mathrm{GL}_r(R)$$

définie par $n_i = \sum_{j=1}^{r} a_{ij} m_j$. Alors

$$\beta^{-r} \mathrm{ord}_R M/\beta N = \det(A) \cdot R.$$

PREUVE : Comme $\{\beta n_1, \ldots, \beta n_r\}$ est une base de βN et que $\beta n_i = \sum_{j=1}^{r} \beta a_{ij} m_j$, l'exercice 2. p.65 de [Rei03] nous assure que $\mathrm{ord}_R M/\beta N = \det(\beta A) \cdot R$, ce qui est le résultat cherché.

□

Corollaire 1.2.24. *Soient I un R-module projectif de rang r, $b : I \times I \longrightarrow K$ une forme bilinéaire non dégénérée et $I^* = \{x \in A \mid b(x, I) \subset R\}$. On suppose encore qu'il existe $\beta \in R$ tel que $\beta I \subset I^*$. Alors*

$$\beta^{-r} \mathrm{ord}_R(I^*/\beta I) = \det(b).$$

PREUVE : Observons l'égalité localement. Soit $\mathcal{P}$ un idéal premier de R. On a

$$(\mathrm{ord}_R(I^*/\beta I))_{\mathcal{P}} = \mathrm{ord}_{R_{\mathcal{P}}}(I^*_{\mathcal{P}}/\beta I_{\mathcal{P}})$$

et

$$\det(b)_{\mathcal{P}} = \det(b(e_i, e_j)_{1 \leq i,j \leq r}) \cdot R_{\mathcal{P}}$$

où $\{e_1, \ldots, e_r\}$ est une $R_{\mathcal{P}}$-base de $I_{\mathcal{P}}$ (voir la proposition 1.2.22). Il suffit donc de montrer l'égalité

$$\beta^{-r} \mathrm{ord}_{R_{\mathcal{P}}}(I^*_{\mathcal{P}}/\beta I_{\mathcal{P}}) = \det(b(e_i, e_j)_{1 \leq i,j \leq r}) \cdot R_{\mathcal{P}}$$

pour tout idéal premier $\mathcal{P}$ de R. Il est donc possible de se restreindre au cas où I et I^* sont des modules libres de rang r sur un anneau principal. Dans ce cas, désignons par $B = \{e_1, \ldots, e_r\}$ une base de I et par $B^* = \{e_1^*, \ldots, e_r^*\}$ la base de I^* duale de B c'est-à-dire vérifiant $b(e_i, e_j^*) = \delta_{ij}$. Alors $e_i = \sum_{j=1}^{r} b(e_j, e_i) e_j^*$, et le lemme précédent nous permet de conclure.

□

REMARQUE : Ce corollaire s'applique en particulier aux idéaux d'une algèbre centrale simple.

Corollaire 1.2.25. *Soient I un idéal à droite d'un ordre maximal Λ d'une algèbre séparable A sur un corps $K = \mathrm{Frac}(R)$, $b : I \times I \longrightarrow K$ une forme bilinéaire symétrique non dégénérée et $I^* = \{x \in A \mid b(x, I) \subset R\}$. On suppose encore que $b(\Lambda, I) \subset R$. Alors*

$$\mathrm{N}_{A/K}(I) = \det(b) \cdot \mathrm{N}_{A/K}(I^*)$$

PREUVE : Soit $\Lambda = \mathcal{O}_r(I)$. Nous savons qu'il existe β et γ dans R tels que $\gamma\beta I \subset \beta I^* \subset \Lambda$. Nous pouvons donc écrire la suite exacte courte de R-modules

$$0 \longrightarrow \beta I^*/\gamma\beta I \longrightarrow \Lambda/\gamma\beta I \longrightarrow \Lambda/\beta I^* \longrightarrow 0.$$

Alors par la proposition 1.2.20

$$\mathrm{ord}_R(\Lambda/\gamma\beta I) = \mathrm{ord}_R(\Lambda/\beta I^*)\mathrm{ord}_R(\beta I^*/\gamma\beta I)$$

Le terme de gauche est par définition $(\gamma\beta)^r \mathrm{N}_{A/K}(I)$, le premier terme de l'expression de droite est par définition $\beta^r \mathrm{N}_{A/K}(I^*)$ (car $\Lambda = \mathcal{O}_r(I^*)$ vu que Λ est maximal) et, par le corollaire précédent, le deuxième est $\gamma^r \det(b)$, d'où le résultat.

□

1.3 Le cas des corps de nombres

Dans cette section nous abordons le cas qui nous préoccupera dans la suite de ce travail, c'est-à-dire le cas où K est un corps de nombres et $R = \mathcal{O}_K$ est son anneau des entiers. Nous noterons $n = [K : \mathbb{Q}]$ le degré de K sur $\mathbb{Q}$. Comme avant, A est une K-algèbre centrale simple de dimension finie $r = m^2$, Λ un ordre maximal de A, I un idéal à droite de Λ et $b : I \times I \longrightarrow K$ une forme bilinéaire non dégénérée.

Proposition 1.3.1. *L'algèbre centrale simple A est une algèbre séparable sur $\mathbb{Q}$ et on a $\mathrm{tr}_{A/\mathbb{Q}} = \mathrm{T}_{K/\mathbb{Q}} \circ \mathrm{tr}_{A/K}$. De plus les $\mathcal{O}_K$-ordres (maximaux) de A sont également des $\mathbb{Z}$-ordres de A (maximaux) et les idéaux de A sont aussi des $\mathbb{Z}$-idéaux de A, vue comme algèbre séparable sur $\mathbb{Q}$. Ces idéaux sont des $\mathbb{Z}$-modules libres de rang rn.*

PREUVE : C'est une conséquence des propositions 1.2.10 et 1.2.7.

□

REMARQUE : Si $\{e_1, \ldots, e_r\}$ est une K-base de A contenue dans un idéal I (qui existe pour tout idéal, voir la proposition 1.2.21) et $\{\omega_1, \ldots, \omega_n\}$ une

$\mathbb{Z}$-base de $\mathcal{O}_K$ alors $\{\omega_1 e_1, \ldots, \omega_n e_1, \omega_1 e_2 \ldots, \omega_n e_r\}$ est une $\mathbb{Z}$-base de I. Le fait de pouvoir considérer M à la fois comme module sur $\mathbb{Z}$ et sur $\mathcal{O}_K$ nous permet de calculer d'une part $\mathrm{ord}_{\mathbb{Z}}(M)$ et d'autre part $\mathrm{ord}_R(M)$. Le lien entre ces deux idéaux est donné par le résultat suivant.

Lemme 1.3.2. *Si $J \subset I$ sont des idéaux de Λ, alors*

$$|I/J| \cdot \mathbb{Z} = \mathrm{ord}_{\mathbb{Z}}(I/J) = \mathrm{N}_{K/\mathbb{Q}}(\mathrm{ord}_R(I/J)) \cdot \mathbb{Z}.$$

Preuve : La première égalité est facile. Pour la seconde, nous savons qu'il existe des idéaux $E_1, \ldots, E_s$ de R avec

$$I/J = \oplus_{i=1}^{s} R/E_i$$

et

$$\mathrm{ord}_R(I/J) = E_1 \cdots E_s$$

(voir [Rei03] p.49), de sorte que

$$\mathrm{N}_{K/\mathbb{Q}}(\mathrm{ord}_R(I/J)) = \mathrm{N}_{K/\mathbb{Q}}(E_1) \cdots \mathrm{N}_{K/\mathbb{Q}}(E_s) = |\oplus_{i=1}^{s} R/E_i| = |I/J|.$$

□

Corollaire 1.3.3. *Soit I un idéal à droite d'une algèbre centrale simple A sur un corps de nombres K. Alors*

$$\mathrm{N}_{A/\mathbb{Q}}(I) = \mathrm{N}_{K/\mathbb{Q}}(\mathrm{N}_{A/K}(I))$$

et si I est un idéal entier d'un ordre Λ, alors

$$\mathrm{N}_{A/\mathbb{Q}}(I) = |\Lambda/I|.$$

Preuve : Soit $\Lambda = \mathcal{O}_r(I)$ et $\beta \in \mathbb{Z}$ tel que $\beta I \subset \Lambda$. Alors

$$\mathrm{N}_{A/\mathbb{Q}}(I) = \beta^{-rn}\mathrm{ord}_{\mathbb{Z}}(\Lambda/\beta I) = \beta^{-rn}\mathrm{N}_{K/\mathbb{Q}}(\mathrm{ord}_{\mathcal{O}_K}(\Lambda/\beta I)) =$$

$$\mathrm{N}_{K/\mathbb{Q}}(\beta^{-r}\mathrm{ord}_{\mathcal{O}_K}(\Lambda/\beta I)) = \mathrm{N}_{K/\mathbb{Q}}(\mathrm{N}_{A/K}(I)).$$

La deuxième affirmation découle directement du lemme précédent.

□

Soit $b : I \times I \longrightarrow K$ une forme bilinéaire non dégénérée. Alors b permet de définir une forme $\mathbb{Z}$-bilinéaire de la façon suivante :

$$\begin{array}{rccc} T_b : & I \times I & \longrightarrow & \mathbb{Q} \\ & (x, y) & \longmapsto & \mathrm{T}_{K/\mathbb{Q}}(b(x, y)) \end{array}$$

On vérifie facilement que T_b est non dégénérée. Considérons

$$I_{T_b}^* = \{x \in A \mid T_b(x, I) \subset \mathbb{Z}\}$$

c'est encore un $\mathbb{Z}$-module libre de rang rn ; en revanche ce n'est pas nécessairement un $\mathcal{O}_K$-module. L'idéal I_b^* est également un $\mathbb{Z}$-module de rang rn et il est contenu dans $I_{T_b}^*$.

Proposition 1.3.4. *Le cardinal du quotient de $I_{T_b}^*$ par I_b^* ne dépend que du corps de base K. Plus précisément, on a*

$$|I_{T_b}^*/I_b^*| = |\mathrm{d}_K|^r$$

ou, de manière équivalente,

$$\mathrm{ord}_{\mathbb{Z}}(I_{T_b}^*/I_b^*) = \mathrm{d}_K^r\mathbb{Z}$$

où d_K est le discriminant de K.

Preuve : Soient $B = \{e_1, \dots e_r\}$ une K-base de A contenue dans I, $B^* = \{e_1^*, \dots, e_r^*\}$ la base de I_b^* duale de B, $\Omega = \{\omega_1, \dots, \omega_n\}$ une $\mathbb{Z}$-base de $\mathcal{O}_K$, $E = \{\omega_1 e_1, \dots, \omega_n e_1, \omega_2 e_1, \dots, \omega_n e_r\}$ la $\mathbb{Z}$-base de I construite avec B et Ω. Grâce à cela nous obtenons des $\mathbb{Z}$-bases de I_b^* et de $I_{T_b}^*$ bien particulières. Il s'agit de

$$F = \{\omega_1 e_1^*, \dots, \omega_n e_1^*, \omega_2 e_1^*, \dots, \omega_n e_r^*\}$$

(pour I_b^*) et de

$$E^* = \{(\omega_1 e_1)^*, \dots, (\omega_n e_1)^*, (\omega_2 e_1)^*, \dots, (\omega_n e_r)^*\}$$

la base duale de E (pour $I_{T_b}^*$).
Comme $I_b^* \subset I_{T_b}^*$ il existe une matrice $S \in \mathrm{M}_{nr}(\mathbb{Z}) \cap \mathrm{GL}_{nr}(\mathbb{Q})$ qui est la matrice de changement de base de F vers E^*. Cette matrice est constituée de r^2 blocs de même taille $n \times n$:

$$S = \begin{pmatrix} S^{11} & \dots & S^{1r} \\ \vdots & & \vdots \\ S^{r1} & \dots & S^{rr} \end{pmatrix}$$

où $S^{ij} = (s_{kl}^{ij})_{1 \le k,l \le n} \in \mathrm{M}_n(\mathbb{Z})$. Ainsi,

$$\omega_k e_i^* = \sum_{\substack{1 \le l \le n \\ 1 \le j \le r}} s_{lk}^{ji} (\omega_l e_j)^* \tag{I.1}$$

D'une part (en remplaçant $\omega_k e_i^*$ par sa valeur dans I.1) nous obtenons

$$T_b(\omega_k e_i^*, \omega_t e_u) = s_{tk}^{ui}$$

et d'autre part

$$T_b(\omega_k e_i^*, \omega_t e_u) = \mathrm{T}_{k/\mathbb{Q}}(\omega_k \omega_t b(e_i^*, e_u)) = \delta_{ui} \mathrm{T}_{K/\mathbb{Q}}(\omega_t \omega_k).$$

Par conséquent

$$S^{ij} = \begin{cases} (\mathrm{T}_{K/\mathbb{Q}}(\omega_t \omega_k))_{1 \leq t,k \leq n} & \text{si } i = j \\ 0 & \text{sinon.} \end{cases}$$

Ainsi $\det(S) = \prod_{i=1}^{r} \det(S^{ii}) = \mathrm{d}_K^r$. De plus le lemme 1.2.23 nous dit que $\mathrm{ord}_{\mathbb{Z}}(I_{T_b}^*/I_b^*) = \det(S)\mathbb{Z}$, ce qui termine la preuve.

□

Proposition 1.3.5. *Avec les mêmes notations que ci-dessus, on a :*

$$|\det(T_b)| = \mathrm{N}_{K/\mathbb{Q}}(\det(b)) \cdot |\mathrm{d}(K)|^r$$

Preuve : Soit $\gamma \in \mathbb{Z}$ tel que $\gamma I \subset I_b^*$. Alors $\gamma I \subset I_b^* \subset I_{T_b}^*$ et, d'après le corollaire 1.2.24,

$$|\gamma^{rn} \det(T_b)| = |I_{T_b}^*/\gamma I|$$

il faut donc calculer $|I_{T_b}^*/\gamma I|$. Nous savons que

$$\left(I_{T_b}^*/\gamma I\right) / \left(I_b^*/\gamma I\right) \cong I_{T_b}^*/I_b^*$$

de sorte que $|\gamma^{rn} \det(T_b)| = |I_{T_b}^*/I_b^*| \cdot |I_b^*/I|$. Ainsi, par la proposition précédente et le lemme 1.3.2,

$$|\gamma^{rn} \det(T_b)| = |\mathrm{d}(K)^r| \cdot \mathrm{N}_{K/\mathbb{Q}}(\mathrm{ord}_R(I_b^*/\gamma I))$$

Mais $\mathrm{ord}_R(I_b^*/\gamma I) = \gamma^r \det(b)$ (toujours par le corollaire 1.2.24), ce qui nous permet de conclure.

□

1.4 Nombre de classes d'idéaux et nombre de types des ordres maximaux

Dans cette section K désigne un corps de nombres, A une algèbre centrale simple sur K et Λ un ordre de A.

Définition 1.4.1. *Soient Λ et Γ deux ordres de A, on dit que Λ et Γ sont conjugués s'il existe $x \in A^\times$ tel que*

$$\Lambda = x^{-1}\Gamma x.$$

Définition 1.4.2. *Considérons la relation d'équivalence $\sim$ définie par*

$$\Lambda \sim \Gamma \text{ si } \Lambda \text{ et } \Gamma \text{ sont conjugués.}$$

Le nombre de types de A, noté t_A, est le cardinal de l'ensemble

$$\{\Lambda \mid \Lambda \text{ est un ordre maximal de } A\} / \sim .$$

Définition 1.4.3. *Deux idéaux I et J de A sont dit équivalents à droite s'il existe $a \in A^\times$ tel que*

$$I = Ja$$

et on note $I \sim J$ et on remarque que c'est une relation d'équivalence.
Le nombre de classes d'idéaux à gauche d'un ordre Λ, noté $h_l(\Lambda)$, est le cardinal de l'ensemble

$$\{I \mid I \text{ est un idéal à gauche de } \Lambda\}/ \sim$$

On définit symétriquement le nombre de classes d'idéaux à droite de Λ (et on le note $h_r(\Lambda)$.

Proposition 1.4.4. *Soit Λ un ordre maximal de A. Notons t_A le nombre de type de A, $h_l(\Lambda)$ le nombre de classes des idéaux à gauche de Λ et $h_r(\Lambda)$ le nombre de classe des idéaux à droite de Λ. Alors*

i) Les quantités t_A, $h_l(\Lambda)$ et $h_r(\Lambda)$ sont finies.

ii) Les nombres entiers $h_l(\Lambda)$ et $h_r(\Lambda)$ sont indépendants de l'ordre maximal Λ et sont égaux. On note alors h_A le nombre de classes d'idéaux (à droite ou à gauche) d'un ordre maximal quelconque de A.

iii) L'ordre maximal Λ est principal (à gauche et à droite) si et seulement si $h_A = 1$.

iv) Si A est une algèbre de quaternions (voir chapitre III) alors

$$t_A \leq h_A$$

PREUVE : Pour i) et ii) voir [Rei03] p.228 théorème 26.4 et exercice 8 p.232, et pour iii) voir [Vig80] p.26 corollaire 4.11 et théorème 5.4 p.87.

Nous terminons cette section en donnant le théorème qui lie les ordres maximaux entre eux.

Théorème 1.4.5. *Soit Λ et Γ des ordres maximaux de A. Soit $I(\Lambda)$ et $I(\Gamma)$ les groupes des idéaux bilatères de Λ et de Γ. Alors il existe un idéal M à gauche de Λ et à droite de Γ tel que*

$$\begin{array}{rccc} \varphi_M : & I(\Lambda) & \longrightarrow & I(\Gamma) \\ & J & \longmapsto & M^{-1}JM \end{array}$$

est un isomorphisme de groupe. Si N est un idéal vérifiant les mêmes propriétés que M alors $\varphi_M = \varphi_N$. L'isomorphisme φ_M est donc indépendant du choix de M, on le notera φ. En particulier

$$\Lambda = M^{-1}\Gamma M.$$

PREUVE : Voir [Rei03] théorème 22.21 p.198.

1.5 Réseaux et réseaux idéaux

Dans cette section nous définissons les réseaux idéaux ainsi que les constantes associées à ces réseaux qui nous permettront de borner le minimum euclidien d'un ordre maximal.

Définition 1.5.1. *Un réseau est une paire (L, q) où L est un $\mathbb{Z}$-module libre de rang fini et $q : L_{\mathbb{R}} \times L_{\mathbb{R}} \longrightarrow \mathbb{R}$, une forme bilinéaire symétrique définie positive, où $L_{\mathbb{R}} = L \otimes_{\mathbb{Z}} \mathbb{R}$.*

Définition 1.5.2.

i) Deux réseaux (L, q) et (L', q') sont dit isomorphes s'il existe un isomorphisme φ de L sur L' tel que $q'((\varphi \otimes \mathrm{id})(x), (\varphi \otimes \mathrm{id})(y)) = q(x, y)$ pour tout $x, y \in L_{\mathbb{R}}$.

ii) Le réseau dual de (L, q) est défini par

$$(L^*, q) = \{x \in L_{\mathbb{R}} \mid q(x, y) \in \mathbb{Z} \text{ pour tout } y \in L\}.$$

REMARQUE : Si $\text{rang}(L) = n$, alors q est un produit scalaire sur $\mathbb{R}^n$ de sorte que la notion de réseau est équivalente à celle de sous $\mathbb{Z}$-module de $\mathbb{R}^n$ de rang maximal (où q est le produit scalaire usuel).

Soit (L, q) un réseau. On pose $q(x) = q(x, x)$ pour tout $x \in L_{\mathbb{R}}$. On définit alors les invariants suivants.

Définition 1.5.3. *Soit (L, q) un réseau de rang n. Alors*

i) Le minimum du réseau est $\min(L, q) = \inf_{x \in L \setminus \{0\}} q(x)$.

ii) Le maximum de $x \in L_{\mathbb{R}}$ par rapport au réseau est $\max_L(x) = \inf\{q(x - c) \mid c \in L\}$.

iii) Le maximum du réseau est $\max(L, q) = \sup\{\max_L(x) \mid x \in L_{\mathbb{R}}\}$.

iv) Le déterminant du réseau est le déterminant du produit scalaire q. C'est un nombre réel positif.

v) Le premier invariant d'Hermite est $\gamma(L, q) = \frac{\min(L,q)}{\det(L,q)^{1/n}}$.

vi) Le second invariant d'Hermite est $\tau(L, q) = \frac{\max(L,q)}{\det(L,q)^{1/n}}$.

REMARQUE : Si aucune confusion n'est possible, on notera parfois L au lieu de (L, q). Tous les invariants définis ici ne dépendent que de la classe d'isomorphisme du réseau. Intuitivement, et en tenant compte de la remarque précédente, $\det(L, q)$ est le volume d'une maille du réseau, $\min(L, q)$ est la longueur minimale des éléments de L et $\max(L, q)$ est le carré du rayon de recouvrement de L (c'est-à-dire le rayon r minimal pour lequel la réunion de toutes les boules, de rayon r, centrées sur les points de L, recouvrent $\mathbb{R}^n$).

On peut également définir le maximum de L comme suit :

$$\max(L, q) = \inf\{\lambda \in \mathbb{R} \mid \text{ pour tout } x \in L_{\mathbb{R}} \text{ il existe } y \in L \text{ avec } q(x-y) \leq \lambda\}.$$

Notation 1.5.4. *Soit A une algèbre munie d'une involution. On notera $\mathcal{F}_A$ l'ensemble des éléments de A stables par l'involution et $\mathcal{F}_A^\times = \mathcal{F}_A \cap A^\times$. S'il n'y a pas de confusion possible, on notera $\mathcal{F}$ au lieu de $\mathcal{F}_A$.*

Proposition 1.5.5. *Soient R un anneau de Dedekind, A une algèbre séparable sur* $\text{Frac}(R) = k$ *munie d'une involution k-linéaire γ, Λ un R-ordre de A stable par l'involution, I un idéal à droite de Λ et $b : I \times I \longrightarrow k$ une forme R-bilinéaire symétrique non dégénérée. On suppose encore que $b(\lambda x, y) = b(x, \lambda^\gamma y)$ pour tout $x, y \in I$ et tout $\lambda \in \Lambda$. Alors il existe $\alpha \in \mathcal{F}^\times$ tel que $b(x, y) = \text{tr}_{A/k}(x\alpha y^\gamma)$ pour tout $x, y \in I$.*

PREUVE : Tout d'abord nous étendons b à tout A par k-linéarité (car $kI = A$) et nous remarquons que $b(\lambda x, y) = b(x, \lambda^\gamma y)$ pour tout $\lambda \in A$ (car γ est k-linéaire et $A = k\Lambda$). Comme b et tr sont des formes bilinéaires non dégénérées, elles induisent des isomorphismes de A vers $A^\sharp = \mathrm{Hom}_k(A, k)$. Explicitement :

$$\begin{array}{rccccccc} b^* : & A & \longrightarrow & A^\sharp & & & & \\ & x & \longmapsto & b_x : & A & \longrightarrow & \mathrm{k} \\ & & & & y & \longmapsto & b(x,y) \end{array}$$

et

$$\begin{array}{rccccccc} \mathrm{tr}^* : & A & \longrightarrow & A^\sharp & & & & \\ & x & \longmapsto & t_x : & A & \longrightarrow & \mathrm{k} \\ & & & & y & \longmapsto & \mathrm{tr}_{A/k}(xy) \end{array}$$

sont des isomorphismes. En particulier, pour tout $x \in A$ il existe un unique $y_x \in A$ tel que $b_x = t_{y_x}$. Ainsi nous avons

$$\mathrm{tr}_{A/k}(y_x z) = b(x, z) = b(1, x^\gamma z) = \mathrm{tr}_{A/k}(y_1 x^\gamma z)$$

pour tout $z \in A$. De sorte que $y_x = y_1 x^\gamma$ et

$$b(x, z) = b(z, x) = \mathrm{tr}_{A/k}(y_1 z^\gamma x) = \mathrm{tr}_{A/k}(x y_1 z^\gamma)$$

pour tout $x, z \in A$. Il suffit donc de poser $\alpha = y_1$. Le fait que α est inversible découle du fait que b est non dégénérée. La stabilité de α par l'involution découle de la symétrie de b et du fait que
$\mathrm{tr}_{A/k}(x^\gamma) = \mathrm{tr}_{A/k}(x)$ pour tout $x \in A$.

□

On obtient immédiatement le corollaire suivant.

Corollaire 1.5.6. *Soit k un corps, A une algèbre séparable sur k avec une involution k-linéaire γ et $b : A \times A \longrightarrow k$ une forme bilinéaire non dégénérée vérifiant*

$$b(\lambda x, y) = b(x, \lambda^\gamma y)$$

pour tout $x, y, \lambda \in A$. Alors il existe $\alpha \in \mathcal{F}^\times$ tel que

$$b(x, y) = \mathrm{tr}_{A/k}(x \alpha y^\gamma)$$

pour tout $x, y \in A$.

Définition 1.5.7. *Soit A une $\mathbb{Q}$-algèbre semi-simple de dimension finie et Λ un $\mathbb{Z}$-ordre. On suppose encore que $A_{\mathbb{R}} = A \otimes_{\mathbb{Q}} \mathbb{R}$ est muni d'une involution $\mathbb{R}$-linéaire γ. Un réseau idéal de A est un triplet (I, b, γ) où I est un idéal (généralisé) à droite de Λ et $b : A_{\mathbb{R}} \times A_{\mathbb{R}} \longrightarrow \mathbb{R}$ une forme $\mathbb{R}$-bilinéaire symétrique définie positive vérifiant,*

$$b(\lambda x, y) = b(x, \lambda^{\gamma} y)$$

pour tout $x, y \in I_{\mathbb{R}}$ et tout $\lambda \in \Lambda_{\mathbb{R}}$.

Par idéal généralisé nous entendons un Ix où I est un idéal fractionnaire de A et $x \in A_{\mathbb{R}}$. En général nous nous bornerons à considérer des idéaux fractionnaires. Cependant, nous verrons par la suite qu'il y un cas où il est utile de remarquer que cette définition fonctionne dans le cas généralisé.

Remarque : Le lien entre l'idéal I et le réseau (I, b, γ) n'apparaît pas clairement dans la définition d'un réseau idéal. En fait, on a

$$I_{\mathbb{R}} = I \otimes_{\mathbb{Z}} \mathbb{R} \cong A_{\mathbb{R}}$$

ce qui prouve que (I, b, γ) est bien un réseau au sens de la définiton 1.5.1.

On peut d'ores et déjà distinguer deux classes d'algèbres sur $\mathbb{Q}$ possédant un réseau idéal : celles dont l'involution sur $A_{\mathbb{R}}$ provient d'une involution sur A et les autres. L'existence d'une involution sur A pour laquelle il existe un réseau idéal possible restreint le choix de A ; nous étudierons par la suite la mesure de cette restriction. Sauf mention du contraire lorsque A est munie d'une involution, on considérera toujours l'involution de $A_{\mathbb{R}}$ induite par celle de A.

Nous pouvons maintenant définir les invariants d'Hermite liés directement à l'idéal I.

Définition 1.5.8. *Soit Λ un ordre et I un idéal à droite de Λ. Le premier invariant d'Hermite de I est défini par*

$$\gamma_{\min}(I) = \min\{\gamma(I, b) \mid (I, b) \text{ est un réseau idéal } \}$$

et le second invariant d'Hermite est défini par

$$\tau_{\min}(I) = \min\{\tau(I, b) \mid (I, b) \text{ est un réseau idéal } \}.$$

Remarque : Nous donnerons par la suite une borne supérieure de $\gamma_{\min}(I)$ et une borne inférieure de $\tau_{\min}(I)$.

Proposition 1.5.9. *Soit (I, b, γ) un réseau idéal de A. Alors il existe $\alpha \in \mathcal{F}_{A_{\mathbb{R}}}^{\times}$ tel que*

$$b(x, y) = \mathrm{tr}_{A_{\mathbb{R}}/\mathbb{R}}(x\alpha y^{\gamma})$$

pour tout $x, y \in A_{\mathbb{R}}$ où $\mathrm{tr}_{A_{\mathbb{R}}/\mathbb{R}}$ désigne la trace réduite de la $\mathbb{R}$-algèbre séparable $A_{\mathbb{R}}$ (voir la définition 1.2.9).

Preuve : Comme A est séparable, c'est une conséquence du corollaire 1.5.6.

□

Nous allons maintenant étudier quelques propriétés des involutions sur les algèbres semi-simples. Comme la question est très vaste, nous ne mentionnerons que les résultats directement utiles à la suite de ce travail. Pour plus de détails voir [KMMT98].

Proposition 1.5.10. *Soient A et B des algèbres simples sur un corps k et γ une involution k-linéaire sur $A \oplus B$. Deux cas sont possibles :*

i. Soit $\gamma|_A$ est une involution sur A. Dans ce cas $\gamma|_B$ est également une involution et

$$\begin{array}{rccc} \gamma : & A \oplus B & \longrightarrow & A \oplus B \\ & (a, b) & \longmapsto & (a^{\gamma}, b^{\gamma}). \end{array}$$

ii. Soit $\gamma|_A$ n'est pas une involution sur A. Dans ce cas il existe un anti-isomorphisme d'algèbres $f : A \longrightarrow B$ avec

$$\begin{array}{rccc} \gamma : & A \oplus B & \longrightarrow & A \oplus B \\ & (a, b) & \longmapsto & (f^{-1}(b), f(a)). \end{array}$$

Preuve : Le cas où une des algèbres est réduite à 0 est clair. Supposons donc $A \neq 0$ et $B \neq 0$. Notons

$$\begin{array}{rccc} \gamma : & A \oplus B & \longrightarrow & A \oplus B \\ & (a, b) & \longmapsto & (g(a, b), h(a, b)). \end{array}$$

Alors $g : A \oplus B \longrightarrow A$ et $h : A \oplus B \longrightarrow B$ sont des anti-homomorphismes d'algèbres et comme γ est d'ordre 2,

$$g(g(a, b), h(a, b)) = a$$

et

$$h((g(a, b), h(a, b)) = b$$

pour tout $a \in A$ et $b \in B$. En particulier $(g(0, b), h(0, b)) \in \ker g$ pour tout $b \in B$ et $(g(a, 0), h(a, 0)) \in \ker h$ pour tout $a \in A$. Ainsi $\ker g + \ker h = A \oplus B$

(car $(g(a,b),h(a,b)) = (g(0,b),h(0,b)) + (g(a,0),h(a,0))$ et γ est surjective). Remarquons encore que $\ker g \cap \ker h = \{0\}$ (car γ est injective). Finalement $A \oplus B = \ker g \oplus \ker h$, mais les noyaux de g et h sont des idéaux bilatères propres (car g et h sont surjectives) et non nuls, de sorte qu'il n'existe plus que deux possibilités : soit $\ker g = B$ et $\ker h = A$, soit c'est l'inverse.
Dans le premier cas g induit

$$\begin{array}{rccc} \tilde{g}: & A & \longrightarrow & A \\ & a & \longmapsto & \tilde{g}(a) = g(a,b) \end{array}$$

et h induit

$$\begin{array}{rccc} \tilde{h}: & B & \longrightarrow & B \\ & b & \longmapsto & \tilde{h}(b) = h(a,b) \end{array}$$

avec $(a,b)^\gamma = (\tilde{g}(a),\tilde{h}(b))$ pour tout $a \in A$ et $b \in A$. Il suffit alors de remarquer que $\tilde{g} = \gamma|_A$ et que $\tilde{h} = \gamma|_B$.
Dans le second cas, g induit

$$\begin{array}{rccc} \tilde{g}: & B & \longrightarrow & A \\ & b & \longmapsto & \tilde{g}(b) = g(a,b) \end{array}$$

et h induit

$$\begin{array}{rccc} \tilde{h}: & A & \longrightarrow & B \\ & a & \longmapsto & \tilde{h}(a) = h(a,b) \end{array}$$

avec $(a,b)^\gamma = (\tilde{g}(b),\tilde{h}(a))$. Il suffit alors de poser $f = \tilde{h}$, et de vérifier que c'est un anti-isomorphisme d'algèbres et que $\tilde{h}^{-1} = \tilde{g}$.

□

Corollaire 1.5.11. *Soit $A = A_1 \oplus \cdots \oplus A_t$ une algèbre semi-simple de dimension finie sur un corps k munie d'une involution γ k-linéaire. Alors, à renumérotation près des composants simples, on peut trouver $1 \leq s \leq t$, avec s pair, et des anti-isomorphismes d'algèbres $f_{2i-1,2i} : A_{2i-1} \longrightarrow A_{2i}$ où $1 \leq i \leq \frac{s}{2}$ tels que :*

$$(a_1,\ldots,a_t)^\gamma = (f_{1,2}^{-1}(a_2), f_{1,2}(a_1), \ldots, f_{s-1,s}^{-1}(a_s), f_{s-1,s}(a_{s-1}), a_{s+1}^\gamma, \ldots, a_t^\gamma).$$

Preuve : Immédiat par la proposition précédente.

□

Ce résultat nous permet de restreindre les involutions qui peuvent donner lieu à des réseaux idéaux.

Corollaire 1.5.12. *Soit $A = A_1 \oplus \cdots \oplus A_t$ une algèbre séparable sur $k = \mathbb{Q}$ (ou $k = \mathbb{R}$) munie d'une involution γ k-linéaire. Supposons qu'il existe $\alpha \in \mathcal{F}^\times$ tel que la forme bilinéaire symétrique*

$$\begin{array}{rccc} b_\alpha : & A \times A & \longrightarrow & k \\ & (a,b) & \longmapsto & \mathrm{tr}_{A/k}(a\alpha b^\gamma) \end{array}$$

est définie positive. Alors, avec les notations du corollaire précédent, $s = 0$. En d'autres termes, γ induit une involution sur chaque composante simple et pour tout $a = (a_1, \ldots, a_t)$ on obtient $a^\gamma = (a_1^\gamma, \ldots, a_t^\gamma)$.

PREUVE : Supposons $s > 0$ et posons $f = f_{1,2}$ (voir le corollaire précédent). Soient $\mathcal{B}_1 = \{e_{11}, \ldots, e_{1u}\}$ une k-base de A_1 et

$$\mathcal{B}_2 = f^{-1}(\mathcal{B}_1) = \{f^{-1}(e_{11}) = e_{21}, \ldots, f^{-1}(e_{1u}) = e_{2u}\}$$

la base de A_2 image de $\mathcal{B}_1$. Alors

$$b_\alpha(e_{11}, e_{11}) = \mathrm{tr}(e_{11}\alpha e_{11}^\gamma) = \mathrm{tr}(e_{11}\alpha f^{-1}(e_{11})) = \mathrm{tr}(e_{11}\alpha e_{21}) = 0$$

car $A_1 A_2 = 0$, ce qui est impossible car b_α est définie positive.

□

Dans le cas où α est dans le centre de A, on peut énoncer un résultat plus précis.

Corollaire 1.5.13. *Soit $A = A_1 \oplus \cdots \oplus A_t$, une algèbre séparable sur $k = \mathbb{Q}$ (ou $k = \mathbb{R}$) munie d'une involution γ k-linéaire. Soit $\alpha \in \mathcal{F}^\times \cap \mathrm{Z}(A)$ et*

$$\begin{array}{rccc} b_\alpha : & A \times A & \longrightarrow & k \\ & (a,b) & \longmapsto & \mathrm{tr}_{A/k}(a\alpha b^\gamma). \end{array}$$

Alors, avec les notations du corollaire 1.5.11,

$$\mathrm{sign}\ b_\alpha = (\frac{s}{2}, \frac{s}{2}) + \sum_{i=s+1}^{t} \mathrm{sign} b_\alpha|_{A_i}$$

PREUVE : Choisissons $\mathcal{B}_{2i-1}$ et $\mathcal{B}_{2i} = f_{2i-1,2i}(\mathcal{B}_{2i-1})$ des bases de A_{2i-1} respectivement A_{2i} comme dans la preuve du corollaire précédent ($1 \leq i \leq \frac{s}{2}$) et $\mathcal{B}_j$, des bases de A_j pour $s+1 \leq j \leq t$. Alors la matrice de b_α par rapport à la base $\mathcal{B} = \bigcup_{i=1}^t \mathcal{B}_i$ est une matrice diagonale par blocs dont les $\frac{s}{2}$ premiers blocs sont de la forme

$$S = \begin{pmatrix} 0 & B_{2i-1,2i} \\ B_{2i-1,2i} & 0 \end{pmatrix}$$

où les $B_{2i-1,2i}$ sont des matrices symétriques de taille $\dim_{\mathbb{Q}}(A_{2i})$.
Les $t-s$ blocs restants (de taille $\dim_{\mathbb{Q}}(A_j)$ avec $s+1 \leq j \leq t$) sont les matrices de $b_\alpha|_{A_j}$.

□

Corollaire 1.5.14. *Soit $A = A_1 \oplus \cdots \oplus A_t$ une algèbre séparable sur $\mathbb{Q}$ munie d'une involution γ, Λ un ordre de A et (I, b, γ) un réseau idéal de A. Alors il existe $\alpha = \alpha_1 + \cdots + \alpha_t \in A$ tel que*

$$b(x,y) = \sum_{i=1}^{t} \mathrm{T}_{K_i/\mathbb{Q}}(\mathrm{tr}_{A_i/K_i}(x_i \alpha_i y_i^\gamma))$$

pour tout $x, y \in I$. De plus $(I, b, \gamma) = (I_1, b_1, \gamma_1) \oplus \cdots \oplus (I_t, b_t, \gamma_t)$ où $(I_i, b_i, \gamma_i) = (I \cap A_i, b|_{A_i}, \gamma|_{A_i})$ est un réseau idéal sur A_i vue comme algèbre centrale simple sur son centre K_i.

Preuve : La première affirmation est une conséquence directe des propositions 1.5.9 et 1.2.10. Soit $e_i \in A_i$ tels que $1 = e_1 + \cdots + e_t$. Alors $I = Ie_1 + \cdots + Ie_t$ et $Ie_i = A_i \cap I$. Posons $I_i = Ie_i$. Il est clair que I_i est un idéal de $\Lambda_i = \Lambda e_i$ et, par la proposition 1.2.7, Λ_i est un $\mathcal{O}_{K_i}$-ordre de l'algèbre centrale simple A_i. De plus, comme b est définie positive, le corollaire 1.5.12 nous assure que $\gamma\,|_{A_i}$ est une involution sur A_i.

Soit $\mathcal{B}_i$ une $\mathbb{Z}$-base de I_i. Alors la matrice de b par rapport à la base $\mathcal{B} = \bigcup_{i=1}^{t} \mathcal{B}_i$ est diagonale par blocs et les blocs diagonaux sont les matrices de $b|_{A_i}$ par rapport aux bases $\mathcal{B}_i$. En d'autres termes, $(I, b, \gamma) = (I_1, b_1, \gamma_1) \oplus \cdots \oplus (I_t, b_t, \gamma_t)$.

□

Dans ce corollaire, A est munie d'une involution et l'involution sur $A_{\mathbb{R}}$ est induite par celle de A. Il est aussi possible de formuler ce corollaire dans le cas général.

Corollaire 1.5.15. *Soit $A = A_1 \oplus \cdots \oplus A_t$ une algèbre séparable sur $\mathbb{Q}$, Λ un ordre de A et (I, b, γ) un réseau idéal de A. Il existe $\alpha = \alpha_1 + \cdots + \alpha_t \in A$ tel que*

$$b(x,y) = \sum_{i=1}^{t} \mathrm{tr}_{(A_i)_{\mathbb{R}}/\mathbb{R}}(x_i \alpha_i y_i^\gamma))$$

pour tout $x, y \in I_{\mathbb{R}}$. De plus $(I, b, \gamma) = (I_1, b_1, \gamma_1) \oplus \cdots \oplus (I_t, b_t, \gamma_t)$ où $(I_i, b_i, \gamma_i) = (I \cap A_i, b|_{(A_i)_{\mathbb{R}}}, \gamma|_{(A_i)_{\mathbb{R}}})$ est un réseau idéal sur A_i vue comme algèbre centrale simple sur son centre K_i.

Notation 1.5.16. *Les deux corollaires qui précèdent nous permettent d'introduire une nouvelle notation pour un réseau idéal (I, b_{alpha}, γ). En effet, la forme bilinéaire b_α ne dépend que de $\alpha \in \mathcal{F}^\times$. On notera donc parfois (I, α, γ) à la place de (I, b, γ).*

REMARQUE : Ces corollaires nous assurent que pour étudier les réseaux idéaux sur une $\mathbb{Q}$-algèbre séparable, il suffit d'étudier les réseaux d'une algèbre centrale simple sur un corps de nombres.

Avant d'étudier plus en détails les réseaux idéaux, nous devons donc nous pencher sur les algèbres centrales simples sur un corps de nombres.

1.6 Algèbre centrale simple sur un corps de nombres

Soit A une algèbre centrale simple sur un corps de nombres K. On note $r = m^2 = \dim_K A$ la dimension de l'algèbre A, $n = [K : \mathbb{Q}]$ le degré de K, $\mathcal{O}_K$ l'anneau des entiers de K et $\sigma_1, \ldots, \sigma_n$ les n plongements complexes de K. Nous conviendrons que les r_1 premiers plongements sont réels, les r_2 suivants sont complexes et les derniers r_2 sont leurs conjugués, de sorte que $n = r_1 + 2r_2$. Soit $\mathcal{P}$ un idéal premier de $\mathcal{O}_K$. On notera $K_\mathcal{P}$ le complété de K pour la valuation $\mathcal{P}$-adique. De même si σ est un plongement (un premier infini de K), on notera K_σ le complété de K pour la valuation induite par le plongement σ. Le terme de "place de K" désigne un premier de $\mathcal{O}_K$ ou un plongement de K dans $\mathbb{C}$. On parlera de *place infinie* lorsqu'il s'agit d'un plongement et de *place finie* dans le cas contraire.

Soit $\mathcal{P}$ une place de K, considérons la $K_\mathcal{P}$-algèbre centrale simple $A_\mathcal{P} = A \otimes_K K_\mathcal{P}$ et soit S un corps gauche de centre $K_\mathcal{P}$ tel que

$$A_\mathcal{P} \cong \mathrm{M}_{\kappa_\mathcal{P}}(S)$$

(voir la proposition 1.2.1). Soit $m_\mathcal{P}^2$ la dimension de S sur $K_\mathcal{P}$. On dit que $m_\mathcal{P}$ est *l'indice local* de A en $\mathcal{P}$ et $\kappa_\mathcal{P}$ est *la capacité locale* de A en $\mathcal{P}$.

L'algèbre $A_\mathcal{P}$ est matricielle si est seulement si $m_\mathcal{P} = 1$. Si $m_\mathcal{P} > 1$ on dit que A *ramifie en* $\mathcal{P}$ ou que $\mathcal{P}$ *est ramifiée* dans A.

Définition 1.6.1. *On note*

$$\mathrm{Ram}(A) = \{\mathcal{P} \mid \mathcal{P} \text{ est ramifiée dans } A\}$$

l'ensemble des places ramifiées,

$$\mathrm{Ram}_\infty(A) = \{\sigma \mid \sigma \text{ est ramifiée dans } A\}$$

l'ensemble des places infinies ramifiées et

$$\mathrm{Ram}_f(A) = \{\mathcal{P} \in \mathrm{Spec}(\mathcal{O}_K) \mid \mathcal{P} \text{ est ramifié dans } A\}$$

l'ensemble des places ramifiées finies de A. On pose encore $w = |\mathrm{Ram}_\infty(A)|$.

Comme il n'y a aucun corps gauche au dessus de $\mathbb{C}$, aucune place complexe n'est ramifiée. Cela nous permet d'adopter une nouvelle convention pour l'ordre des places infinies. Les w premières places infinies réelles sont celles qui sont ramifiées et les $r_1 - w$ suivantes celles qui ne le sont pas.

Définition 1.6.2. *Soit Λ un ordre de A. Un idéal $\mathcal{B}$ bilatère de Λ est dit premier si pour toute paire d'idéaux bilatères S, T de Λ tels que $ST \subset \mathcal{B}$, on a soit $S \subset \mathcal{B}$ soit $T \subset \mathcal{B}$.*

Théorème 1.6.3. *Soit A une algèbre centrale simple comme ci-dessus, Λ un ordre maximal de A. Alors*

i) Les idéaux premiers non nuls de $\mathcal{O}_K$ sont en bijection avec les idéaux premiers de Λ. Cette bijection est donnée par :

$$\begin{array}{rccc} \varphi : & \mathrm{Spec}(\mathcal{O}_K) & \longmapsto & \mathrm{Spec}(\Lambda) \\ & \mathcal{P} & \longmapsto & \Lambda \cap \mathrm{rad}\ \Lambda_{\mathcal{P}} \\ & \mathcal{B} \cap \mathcal{O}_K & \longmapsfrom & \mathcal{B} \end{array}$$

ii) Pour presque tout idéal premier $\mathcal{P}$ de $\mathcal{O}_K$, $m_{\mathcal{P}} = 1$.

iii) Pour tout idéal premier $\mathcal{P}$ de $\mathcal{O}_K$, $\mathcal{P}\Lambda = \mathcal{B}_{\mathcal{P}}^{m_{\mathcal{P}}}$ (où $\mathcal{B}_{\mathcal{P}} = \varphi(\mathcal{P})$).

iv) On peut exprimer le discriminant et la différente de Λ en fonction des premiers ramifiés :

$$\mathcal{D}(\Lambda) = \prod_{\mathcal{P}} \mathcal{B}_{\mathcal{P}}^{m_{\mathcal{P}}-1} \quad \text{et} \quad \mathrm{d}(\Lambda) = \left(\prod_{\mathcal{P}} \mathcal{P}^{(m_{\mathcal{P}}-1)\kappa_{\mathcal{P}}} \right)^m .$$

v) On a les équivalences suivantes :

$$m_{\mathcal{P}} > 1 \iff \mathcal{P} \mid \mathrm{d}(\Lambda) \iff \mathcal{B}_{\mathcal{P}} \mid \mathcal{D}(\Lambda) \iff \mathcal{B}_{\mathcal{P}}^2 \mid \mathcal{P}\Lambda.$$

Preuve : Voir [Rei03] théorème 32.1, p.272-273.

Proposition 1.6.4. *Si σ est une place infinie de K, on peut donner explicitement A_σ. Plus précisément :*

$$A_\sigma \cong \begin{cases} \mathrm{M}_m(\mathbb{R}) & \text{si } \sigma \text{ est réel et n'est pas ramifié dans } A, \\ \mathrm{M}_{\frac{m}{2}}(\mathbb{H}) & \text{si } \sigma \text{ est réel et est ramifié dans } A, \\ \mathrm{M}_m(\mathbb{C}) & \text{si } \sigma \text{ est complexe } A, \end{cases}$$

où $\mathbb{H} = (-1,-1)_{\mathbb{R}}$ désigne le corps des quaternions de Hamilton (voir les définitions 3.1.1 et 3.1.2).

PREUVE : Il n'y a que deux possibilités pour K_σ ; soit σ est réel et alors $K_\sigma = \mathbb{R}$, soit σ n'est pas réel et $K_\sigma = \mathbb{C}$. Nous savons qu'il existe un corps gauche S_σ de dimension m_σ^2 sur K_σ tel que

$$A_\sigma \cong \mathrm{M}_{\kappa_\sigma}(S_\sigma).$$

Si $K_\sigma = \mathbb{R}$ et $m_\sigma = 1$ (i.e. σ n'est pas ramifiée dans A), alors $S_\sigma = \mathbb{R}$ et donc $A_\sigma \cong \mathrm{M}_m(\mathbb{R})$.
Si $K_\sigma = \mathbb{R}$ et $m_\sigma > 1$ (i.e. σ est ramifiée dans A), alors S_σ est un corps gauche au-dessus de $\mathbb{R}$ donc $S_\sigma \cong \mathbb{H}$. Ainsi $A_\sigma \cong \mathrm{M}_{\frac{m}{2}}(\mathbb{H})$.
Si $K_\sigma = \mathbb{C}$, alors nous avons nécessairement $m_\sigma = 1$ et donc $A_\sigma \cong \mathrm{M}_m(\mathbb{C})$.
□

Soit φ_σ un isomorphisme entre A_σ et $\mathrm{M}_{\kappa_\sigma}(S_\sigma)$. On considère la composition suivante :

$$\Sigma : A \xhookrightarrow{i_\sigma} A \otimes_K K_\sigma \xrightarrow{\varphi_\sigma} \mathrm{M}_{\kappa_\sigma}(S_\sigma)$$

$$a \longmapsto a \otimes 1 \longmapsto \varphi_\sigma(a \otimes 1)$$

C'est un homomorphisme injectif de K-algèbres. A chaque plongement σ de K dans $\mathbb{C}$ on peut donc associer un plongement Σ (défini ci-dessus). On dit que Σ est réel (respectivement ramifié) si le σ correspondant est réel (respectivement ramifié).

Remarquons que la structure naturelle de K-algèbre sur K_σ est donnée par $k \cdot \hat{k} = \sigma(k)\hat{k}$ où $k \in K$ et $\hat{k} \in K_\sigma$ de sorte que, si σ_1 et σ_2 sont deux plongements de même nature, on n'a pas nécessairement $K_{\sigma_1} \cong K_{\sigma_2}$ comme K-algèbres. En conséquence les $\mathbb{R}$-algèbres A_{σ_1} et A_{σ_2} ne sont pas non plus nécessairement isomorphes comme K-algèbres.

Nous avons déjà constaté que A peut être vue comme une algèbre séparable sur $\mathbb{Q}$. Nous pouvons donc considérer l'algèbre $A_\mathbb{R} = A \otimes_\mathbb{Q} \mathbb{R}$ qui est une $\mathbb{R}$-algèbre de dimension nm^2. Nous noterons d l'injection naturelle

$$\begin{array}{rccc} d : & A & \longrightarrow & A_\mathbb{R} \\ & a & \longmapsto & a \otimes 1 \end{array}$$

Nous pouvons donner une description précise de $A_\mathbb{R}$ comme produit d'algèbres de matrices. En effet, les applications

$$\begin{array}{rccc} i: & A_{\mathbb{R}} & \longrightarrow & A \otimes_K K \otimes_{\mathbb{Q}} \mathbb{R} \\ & a \otimes r & \longmapsto & a \otimes 1 \otimes r \end{array}$$

$$\begin{array}{rccc} \alpha: & A \otimes_K K \otimes_{\mathbb{Q}} \mathbb{R} & \longrightarrow & A \otimes_K \prod_{i=1}^{r_1+r_2} K_{\sigma_i} \\ & a \otimes k \otimes r & \longmapsto & a \otimes (r\sigma_1(k), \dots, r\sigma_{r_1+r_2}(k)) \end{array}$$

$$\begin{array}{rccc} j: & A \otimes_K \prod_{i=1}^{r_1+r_2} K_{\sigma_i} & \longrightarrow & \prod_{i=1}^{r_1+r_2} A \otimes_K K_{\sigma_i} \\ & a \otimes (k_1, \dots, k_{r_1+1}) & \longmapsto & (a \otimes k_1, \dots, a \otimes k_{r_1+r_2}) \end{array}$$

$$\begin{array}{rccc} \beta: & \prod_{i=1}^{r_1+r_2} A \otimes_K K_{\sigma_i} & \longrightarrow & \mathrm{M}_{\frac{m}{2}}(\mathbb{H})^w \times \mathrm{M}_m(\mathbb{R})^{r_1-w} \times \mathrm{M}_m(\mathbb{C})^{r_2} \\ & (a \otimes k_1, \dots, a \otimes k_{r_1+r_2}) & \longmapsto & (\varphi_{\sigma_1}(a \otimes k_1), \dots, \varphi_{\sigma_{r_1+r_2}}(a \otimes k_{r_1+r_2})) \end{array}$$

sont toutes des isomorphismes de $\mathbb{R}$-algèbres. De plus si $\delta = \beta \circ j \circ \alpha \circ i$ est la composition de ces isomorphismes, alors $\delta \circ d = \prod_{i=1}^{r_1+r_2} \Sigma_i$. Posons $c = \delta \circ d$. Nous obtenons alors le résultat suivant.

Proposition 1.6.5. *Avec les notations ci-dessus, l'application*

$$\begin{array}{rccc} \delta: & A_{\mathbb{R}} & \longrightarrow & \mathrm{M}_{\frac{m}{2}}(\mathbb{H})^w \times \mathrm{M}_m(\mathbb{R})^{r_1-w} \times \mathrm{M}_m(\mathbb{C})^{r_2} \end{array}$$

est un isomorphisme de $\mathbb{R}$-algèbres et l'application

$$\begin{array}{rccc} c: & A & \longrightarrow & \mathrm{M}_{\frac{m}{2}}(\mathbb{H})^w \times \mathrm{M}_m(\mathbb{R})^{r_1-w} \times \mathrm{M}_m(\mathbb{C})^{r_2} \\ & a & \longmapsto & (\Sigma_1(a), \dots, \Sigma_{r_1+r_2}(a)) \end{array}$$

est un homomorphisme injectif de $\mathbb{Q}$-algèbres.

Par commodité de calcul, nous allons identifier $\mathrm{M}_{\frac{m}{2}}(\mathbb{H})$ avec une sous-algèbre de $\mathrm{M}_m(\mathbb{C})$.

Notation 1.6.6. *Soit $m = 2k$ un entier pair. On pose*

$$\mathrm{M}_m^{\mathbb{H}}(\mathbb{C}) = \left\{ \begin{pmatrix} A & -\bar{B} \\ B & \bar{A} \end{pmatrix} \in \mathrm{M}_m(\mathbb{C}) \mid \ A, B \in \mathrm{M}_k(\mathbb{C}) \right\}.$$

Proposition 1.6.7. *Il existe un isomorphisme Φ de $\mathbb{R}$-algèbres entre $\mathrm{M}_{\frac{m}{2}}(\mathbb{H})$ et $\mathrm{M}_m^{\mathbb{H}}(\mathbb{C})$.*

PREUVE : Soit $q = q_0 + q_1 i + q_2 j + q_3 k \in \mathbb{H}$ un quaternion quelconque. Alors $q = (q_0 + iq_1) + j(q_2 - iq_3) = x_1 + jx_2$ avec $x_1, x_2 \in \mathbb{C}$. Avec ces notations l'application

$$\begin{array}{rccc} f: & \mathbb{H} & \longrightarrow & \mathrm{M}_2^{\mathbb{H}}(\mathbb{C}) \\ & q & \longmapsto & \begin{pmatrix} x_1 & -\bar{x}_2 \\ x_2 & \bar{x}_1 \end{pmatrix} \end{array}$$

est un isomorphisme de $\mathbb{R}$-algèbres. Cet isomorphisme induit un isomorphisme f_* entre $\mathrm{M}_{\frac{m}{2}}(\mathbb{H})$ et $\mathrm{M}_{\frac{m}{2}}(\mathrm{M}_2^{\mathbb{H}}(\mathbb{C}))$. Une permutation appropriée des vecteurs de bases permet de construire le dernier isomorphisme φ entre $\mathrm{M}_{\frac{m}{2}}(\mathrm{M}_2^{\mathbb{H}}(\mathbb{C}))$ et $\mathrm{M}_m^{\mathbb{H}}(\mathbb{C})$. L'application $\Phi = \varphi \circ f_*$ est l'isomorphisme cherché. □

REMARQUE : L'isomorphisme donné est en fait également un homéomorphisme (pour la topologie naturelle des deux espaces). C'est donc un isomorphisme d'algèbres topologiques.

On montre facilement que les inversibles de $\mathrm{M}_m^{\mathbb{H}}(\mathbb{C})$, qu'on note $\mathrm{GL}_m^{\mathbb{H}}(\mathbb{C})$, sont exactement les inversibles de $\mathrm{M}_m(\mathbb{C})$ contenus dans $\mathrm{M}_m^{\mathbb{H}}(\mathbb{C})$. En d'autres termes $\mathrm{GL}_m^{\mathbb{H}}(\mathbb{C}) = \mathrm{M}_m^{\mathbb{H}}(\mathbb{C}) \cap \mathrm{GL}_m(\mathbb{C})$.

Si Σ est réelle et ramifiée dans A, on note encore Σ la composition $\Phi \circ \Sigma$. De même $(\prod_{i=1}^{w} \Phi \times \mathrm{id} \times \mathrm{id}) \circ \delta$ est encore noté δ. Avec cet abus de notation nous pouvons réécrire la proposition 1.6.5 de la manière suivante.

Proposition 1.6.8. *L'application*

$$\delta: \quad A_{\mathbb{R}} \quad \longrightarrow \quad \mathrm{M}_m^{\mathbb{H}}(\mathbb{C})^w \times \mathrm{M}_m(\mathbb{R})^{r_1 - w} \times \mathrm{M}_m(\mathbb{C})^{r_2}$$

est un isomorphisme de $\mathbb{R}$-algèbres et l'application

$$\begin{array}{rccc} c: & A & \longrightarrow & \mathrm{M}_m^{\mathbb{H}}(\mathbb{C})^w \times \mathrm{M}_m(\mathbb{R})^{r_1 - w} \times \mathrm{M}_m(\mathbb{C})^{r_2} \\ & a & \longmapsto & (\Sigma_1(a), \ldots, \Sigma_{r_1 + r_2}(a)) \end{array}$$

est un homomorphisme injectif de $\mathbb{Q}$-algèbres.

Notation 1.6.9. *Comme chacun des $r_1 + r_2$ composants simples de l'algèbre $\mathrm{M}_m^{\mathbb{H}}(\mathbb{C})^w \times \mathrm{M}_m(\mathbb{R})^{r_1 - w} \times \mathrm{M}_m(\mathbb{C})^{r_2}$ correspond à un unique plongement σ, on notera aussi bien δ_i que δ_σ pour les composantes de δ et si $a \in A_{\mathbb{R}}$ alors a_i désignera toujours $\delta_i(a)$. De la même façon, nous noterons parfois M_i ou M_σ l'algèbre de matrices $\delta_i(A_{\mathbb{R}})$.*

Proposition 1.6.10. *Avec les notations ci-dessus, on a*

$$\mathrm{tr}_{A_{\mathbb{R}}/\mathbb{R}}(a) = \sum_{i=1}^{r_1} \mathrm{Tr}(a_i) + \sum_{i=r_1+1}^{r_1+r_2} \left(\mathrm{Tr}(a_i) + \overline{\mathrm{Tr}(a_i)}\right)$$

et

$$\mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(a) = \prod_{i=1}^{r_1} \det(a_i) \cdot \prod_{i=r_1+1}^{r_1+r_2} \left(\det(a_i) \cdot \overline{\det(a_i)}\right)$$

où $\mathrm{Tr}(a_i)$ *est la trace de la matrice* a_i*.*

Preuve : L'algèbre $A_{\mathbb{R}}$ (via δ) est un produit d'algèbres de matrices. Le point *i)* de la proposition 1.2.10 nous dit que

$$\mathrm{tr}_{A_{\mathbb{R}}/\mathbb{R}}(a) = \sum_{i=1}^{r_1} \mathrm{tr}_{\mathrm{M}_i/\mathbb{R}}(a_i) + \sum_{i=r_1+1}^{r_1+r_2} \mathrm{T}_{\mathbb{C}/\mathbb{R}}(\mathrm{tr}_{\mathrm{M}_i/\mathbb{C}}(a_i)).$$

De plus, la trace réduite sur $\mathrm{M}_n(\mathbb{R})$ est la trace matricielle ; idem sur $\mathrm{M}_m^{\mathbb{H}}(\mathbb{C})$ et sur $\mathrm{M}_m(\mathbb{C})$. Quant à la trace de $\mathbb{C}$ sur $\mathbb{R}$, nous avons $\mathrm{T}_{\mathbb{C}/\mathbb{R}}(x) = x + \bar{x}$. il faut procéder de même pour la norme réduite.

□

Corollaire 1.6.11. *Soient* τ *une involution sur* $A_{\mathbb{R}}$ *et* $\alpha \in \mathcal{F}^*_{A_{\mathbb{R}}}$*. La forme bilinéaire trace*

$$\begin{array}{rccc} \mathrm{tr}_\alpha : & A_{\mathbb{R}} \times A_{\mathbb{R}} & \longrightarrow & \mathbb{R} \\ & (a,b) & \longmapsto & \mathrm{tr}_{A_{\mathbb{R}}/\mathbb{R}}(a\alpha b^\tau) \end{array}$$

est définie positive si et seulement si les formes trace des différentes composantes matricielles de $A_{\mathbb{R}}$ *sont définies positives. Autrement dit, si et seulement si* $tr_\alpha|_{\mathrm{M}}$ *est définie positive pour toute composante matricielle* M *de* $A_{\mathbb{R}}$*.*

Preuve : La proposition précédente nous dit que

$$\mathrm{tr}_\alpha = \sum_{i=1}^{r_1+r_2} \mathrm{tr}_\alpha|_{\mathrm{M}_i}$$

où $A_{\mathbb{R}} \cong \bigoplus_{i=1}^{r_1+r_2} \mathrm{M}_i$. Si $\mathrm{tr}_\alpha|_{\mathrm{M}_i}$ est définie positive pour tout $1 \leq i \leq r_1 + r_2$ alors tr_α l'est également. Si $\mathrm{tr}_\alpha|_{\mathrm{M}_i}$ n'est pas définie positive pour un certain i, alors il existe $x \in \mathrm{M}_i$, non nul, tel que $\mathrm{tr}_\alpha|_{\mathrm{M}_i}(x,x) \leq 0$. Posons $a = \delta^{-1}(0,\ldots,0,x,0,\ldots,0)$ où δ est l'isomorphisme entre $A_{\mathbb{R}}$ et $\bigoplus_{i=1}^{r_1+r_2} \mathrm{M}_i$

donné dans la proposition 1.6.8. Il vient alors $\mathrm{tr}_\alpha(a,a) = \mathrm{tr}_\alpha|_{\mathrm{M}_i}(x,x) \leq 0$.
□

Proposition 1.6.12. *Soient $a \in A$ et $\mathrm{tr} : A \longrightarrow K$ la trace réduite de l'algèbre centrale simple A. Soient encore σ un plongement et Σ le plongement associé, alors*

$$\sigma(rC_{A/K,a}) = C_{\Sigma(a)}$$

où $C_{\Sigma(a)}$ désigne le polynôme caractéristique de la matrice $\Sigma(a)$. En particulier

$$\sigma(\mathrm{tr}_{A/K}(a)) = \mathrm{Tr}(\Sigma(a))$$

et

$$\sigma(\mathrm{nr}_{A/K}(a)) = \det(\Sigma(a))$$

pour tout $a \in A_{\mathbb{R}}$.

Preuve : Comme $\Sigma|_K = \sigma$ pour les r_1+r_2 plongements Σ, nous appliquons la proposition 1.2.11 et nous obtenons

$$\sigma(rC_{A/K,a}) = \begin{cases} rC_{\mathrm{M}_m(\mathbb{R})/\mathbb{R},\Sigma(a)} & \text{si } \sigma \text{ est réel et n'est pas ramifié dans } A, \\ rC_{\mathrm{M}_m^{\mathbb{H}}(\mathbb{C})/\mathbb{R},\Sigma(a)} & \text{si } \sigma \text{ est réel et est ramifié dans } A, \\ rC_{\mathrm{M}_m(\mathbb{C})/\mathbb{C},\Sigma(a)} & \text{si } \sigma \text{ est complexe } A. \end{cases}$$

Il suffit donc de voir que $rC_{\mathrm{M}_m(\mathbb{R})/\mathbb{R},\Sigma(a)} = C_\Sigma(a)$, que $rC_{\mathrm{M}_m(\mathbb{C})/\mathbb{C},\Sigma(a)} = C_\Sigma(a)$ et que $rC_{\mathrm{M}_m^{\mathbb{H}}(\mathbb{C})/\mathbb{R}} = C_\Sigma(a)$. Les deux premières affirmations sont claires. Pour la dernière il faut calculer le polynôme caractéristique réduit de la $\mathbb{R}$-algèbre centrale simple $\mathrm{M}_m^{\mathbb{H}}(\mathbb{C})$. Comme $\mathbb{C}$ est algébriquement clos, nous avons nécessairement $\mathrm{M}_m^{\mathbb{H}}(\mathbb{C}) \otimes_{\mathbb{R}} \mathbb{C} \cong \mathrm{M}_m(\mathbb{C})$. Mais $\mathbb{C} \cong \mathbb{R} \oplus i\mathbb{R}$, donc

$$\mathrm{M}_m^{\mathbb{H}}(\mathbb{C}) \otimes_{\mathbb{R}} \mathbb{C} \cong \mathrm{M}_m^{\mathbb{H}}(\mathbb{C}) \oplus i\mathrm{M}_m^{\mathbb{H}}(\mathbb{C})$$

et l'image par cet isomorphisme d'un élément de la forme $x \otimes 1$ est la matrice x vue dans $M_m(\mathbb{C})$, d'où le résultat.

□

Corollaire 1.6.13. *Soit $a \in A$. Alors*

$$\begin{aligned} \mathrm{T}_{K/\mathbb{Q}}(\mathrm{tr}_{A/K}(a)) &= \mathrm{tr}_{A_{\mathbb{R}}/\mathbb{R}}(d(a)) \\ &= \sum_{i=1}^{r_1} \mathrm{Tr}(\Sigma_i(a)) + \sum_{i=r_1+1}^{r_1+r_2} \left(\mathrm{Tr}(\Sigma_i(a)) + \overline{\mathrm{Tr}(\Sigma_i(a))} \right) \end{aligned}$$

et

$$\begin{aligned}\mathrm{N}_{K/\mathbb{Q}}(\mathrm{nr}_{A/K}(a)) &= \mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(d(a)) \\ &= \prod_{i=1}^{r_1} \det(\Sigma_i(a)) \cdot \prod_{i=r_1+1}^{r_1+r_2} \left(\det(\Sigma_i(a)) \cdot \overline{\det(\Sigma_i(a))}\right).\end{aligned}$$

PREUVE : Nous faisons la preuve pour la trace, l'autre est similaire. La deuxième égalité est une conséquence du fait que $\delta_i \circ d = \Sigma_i$ et de la proposition 1.6.10. La proposition précédente nous donne

$$\sum_{i=1}^{r_1} \mathrm{Tr}(\Sigma_i(a)) + \sum_{i=r_1+1}^{r_1+r_2} \left(\mathrm{Tr}(\Sigma_i(a)) + \overline{\mathrm{Tr}(\Sigma_i(a))}\right) =$$

$$\sum_{i=1}^{r_1} \sigma_i(\mathrm{tr}_{A/K}(a)) + \sum_{i=r_1+1}^{r_1+r_2} \left(\sigma_i(\mathrm{tr}_{A/K}(a)) + \overline{\sigma_i(\mathrm{tr}_{A/K}(a))}\right)$$

et cette dernière expression est exactement $\mathrm{T}_{K/\mathbb{Q}}(\mathrm{tr}_{A/K}(a))$, d'où le résultat.

□

Proposition 1.6.14. *Soit A une algèbre centrale simple sur un corps de nombres K, Λ un ordre de A et (I, α, τ) un réseau idéal sur A. Identifions encore $A_{\mathbb{R}}$ à $\mathrm{M}_m^{\mathbb{H}}(\mathbb{C})^w \times \mathrm{M}_m(\mathbb{R})^{r_1-w} \times \mathrm{M}_m(\mathbb{C})^{r_2}$. Alors*

i) L'involution sur $A_{\mathbb{R}}$ restreinte à chacune des composantes est une involution $\mathbb{R}$-linéaire que l'on notera encore τ.

ii) $c(\Lambda) = \bigoplus_{i=1}^{r_1+r_2} \Sigma_i(\Lambda)$ et chaque $\Sigma_i(\Lambda)$ est un $\mathbb{Z}$-module libre de rang $\dim_{\mathbb{R}}(\mathrm{M}_i)$ contenu dans M_i. De plus $c(\Lambda)$ est un $\mathbb{Z}$-réseau, dans le sens où c'est un $\mathbb{Z}$-module libre de rang maximal de $\mathbb{R}^{rn}$.

iii) $c(I) = \bigoplus_{i=1}^{r_1+r_2} \Sigma_i(I)$ et chaque $\Sigma_i(I)$ est un idéal à droite de $\Sigma_i(\Lambda)$. De plus $c(I)$ est un $\mathbb{Z}$-réseau, dans le sens où c'est un $\mathbb{Z}$-module libre de rang maximal, de $\mathbb{R}^{rn}$.

iv) Les formes bilinéaires traces

$$\begin{array}{rccc} \mathrm{Tr}: & \mathrm{M}_i \times \mathrm{M}_i & \longrightarrow & \mathbb{R} \\ & (a_i, b_i) & \longmapsto & \mathrm{Tr}(a_i \alpha_i b_i^{\tau}) \end{array}$$

sont définies positives pour tout $1 \leq i \leq r_1$.
Les formes bilinéaires traces

$$\begin{array}{rccc} \mathrm{Tr}: & \mathrm{M}_i \times \mathrm{M}_i & \longrightarrow & \mathbb{R} \\ & (a_i, b_i) & \longmapsto & \mathrm{Tr}(a_i \alpha_i b_i^{\tau}) + \overline{\mathrm{Tr}(a_i \alpha_i b_i^{\tau})} \end{array}$$

sont définies positives pour tout $r_1 + 1 \leq i \leq r_1 + r_2$.

PREUVE : Comme $b_\alpha(x,y) = \mathrm{tr}_{A_\mathbb{R}/\mathbb{R}}(x\alpha y^\tau)$ est définie positive *i)* est une conséquence directe du corollaire 1.5.12.
ii) et *iii)* sont de simples vérifications et *iv)* est une conséquence de la proposition 1.6.10.

□

Cette proposition nous dit que le choix de l'involution sur

$$A_\mathbb{R} = \mathrm{M}_m^{\mathbb{H}}(\mathbb{C})^w \times \mathrm{M}_m(\mathbb{R})^{r_1-w} \times \mathrm{M}_m(\mathbb{C})^{r_2}$$

pour qu'un réseau (I, b_α) existe, se restreint aux choix d'involutions sur M_i telles que la forme trace soit définie positive. Cela nous amène donc à étudier les involutions sur les M_i. C'est le but de la prochaine section.

1.7 Involutions sur $\mathrm{M}_m^{\mathbb{H}}(\mathbb{C})$, $\mathrm{M}_m(\mathbb{R})$ et $\mathrm{M}_m(\mathbb{C})$

Soit τ une involution $\mathbb{R}$-linéaire sur $\mathrm{M}_m(\mathbb{R})$. On sait (voir [KMMT98] proposition 2.19 p.24) qu'il existe une matrice $u \in \mathrm{M}_n(\mathbb{R})$, symétrique ou antisymétrique telle que $\tau = \mathrm{Int}(u) \circ t$ où $\mathrm{Int}(u)$ est l'automorphisme intérieur de $\mathrm{M}_m(\mathbb{R})$ donné par la conjugaison par u :

$$\begin{array}{rccc} \mathrm{Int}(u): & \mathrm{M}_m(\mathbb{R}) & \longrightarrow & \mathrm{M}_m(\mathbb{R}) \\ & a & \longmapsto & u^{-1}au \end{array}$$

et t est la transposition matricielle. De plus ${}^t u = u$ si et seulement si l'involution est orthogonale.

Proposition 1.7.1. *Soient τ une involution $\mathbb{R}$-linéaire sur $\mathrm{M}_m(\mathbb{R})$ et $\alpha \in \mathcal{F}^\times = \{x \in \mathrm{GL}_m(\mathbb{R}) \mid x^\tau = x\}$. Alors*
la forme bilinéaire trace

$$\begin{array}{rccc} \mathrm{Tr}_\alpha: & \mathrm{M}_m(\mathbb{R}) \times \mathrm{M}_m(\mathbb{R}) & \longrightarrow & \mathbb{R} \\ & (a,b) & \longmapsto & \mathrm{Tr}(a\alpha b^\tau) \end{array}$$

est définie positive si et seulement si

i) Il existe un automorphisme intérieur $\varphi = \mathrm{Int}(S)$ tel que $\varphi(y^\tau) = {}^t\varphi(y)$.

ii) La forme bilinéaire $\varphi(\alpha)$ est symétrique et définie positive.

De plus, dans ce cas,

iii) L'involution τ est orthogonale.

iv) On a $\tau = \mathrm{Int}(u) \circ t$ où $u \in \mathrm{M}_m(\mathbb{R})$ est symétrique et définie positive ou définie négative.

PREUVE : Supposons *i)* et *ii)* et notons $\varphi(x) = x_\varphi$ pour tout $x \in \mathrm{M}_m(\mathbb{R})$. Alors $\mathrm{Tr}(x\alpha x^\tau) = \mathrm{Tr}(x_\varphi \alpha_\varphi {}^t x_\varphi)$. De plus, α_φ est orthogonalement diagonalisable et ses valeurs propres sont strictement positives. Soit $s \in \mathrm{GL}_n(\mathbb{R})$ telle que $\beta = s^{-1}\alpha_\varphi s$ est diagonale et $s^{-1} = {}^t s$. Alors

$$\mathrm{Tr}(x_\varphi \alpha_\varphi {}^t x_\varphi) = \mathrm{Tr}(x_\varphi s \beta s^{-1} {}^t x_\varphi) = \mathrm{Tr}(s^{-1} x_\varphi s \beta s^{-1} {}^t x_\varphi s) =$$

$$= \mathrm{Tr}(y_\varphi \beta {}^t y_\varphi) = \sum_{i,k}^{m} y_{ki}^2 \beta_{ii}$$

est un nombre réel strictement positif. Cela prouve que *i)* et *ii)* impliquent que Tr_α est définie positive.

Supposons maintenant que Tr_α est définie positive. Nous savons que $\tau = \mathrm{Int}(u) \circ t$ où $u \in \mathrm{GL}_n(\mathbb{R})$ est une matrice symétrique ou antisymétrique. Supposons d'abord que ${}^t u = -u$. Soit $\{E_{ij} \mid 1 \leq i, j \leq m\}$ la base canonique de $\mathrm{M}_m(\mathbb{R})$. Définissons encore $B = \alpha u^{-1}$ et calculons $\mathrm{Tr}(E_{ij}\alpha E_{ij}^\tau)$:

$$\mathrm{Tr}(E_{ij}\alpha E_{ij}^\tau) = \mathrm{Tr}(E_{ij} B {}^t E_{ij} u) = B_{jj} u_{ii}. \tag{I.2}$$

Comme u est antisymétrique, $u_{ii} = 0$ donc Tr_α est dégénérée, ce qui est absurde. Ainsi u est symétrique (ce qui prouve que τ est orthogonale, et règle en même temps le point *iii)*). Soit $S \in \mathrm{GL}_m(\mathbb{R})$ tel que

$${}^t S u S = D \text{ où } D = \begin{pmatrix} \mathrm{I}_r & 0 \\ 0 & -\mathrm{I}_s \end{pmatrix}.$$

Considérons l'automorphisme intérieur $\varphi = \mathrm{Int}(S)$, et l'involution $\sigma = \mathrm{Int}(D) \circ t$. Un rapide calcul permet de voir que φ est un isomorphisme d'algèbres à involution entre $(\mathrm{M}_m(\mathbb{R}), \tau)$ et $(\mathrm{M}_m(\mathbb{R}), \sigma)$, c'est-à-dire :

$$\varphi(x^\tau) = \varphi(x)^\sigma \text{ pour tout } x \in \mathrm{M}_m(\mathbb{R}).$$

En particulier,

$$\mathrm{Tr}(x\alpha y^\tau) = \mathrm{Tr}(\varphi(x)\varphi(\alpha)\varphi(y)^\sigma) \text{ pour tout } x, y \in \mathrm{M}_m(\mathbb{R}).$$

Pour terminer la preuve de *i)* il suffit de voir que σ est en fait la transposition matricielle, en d'autres termes que $D = \pm \mathrm{I}_m$. Dans ce but, nous vérifions que

$$E_{ij}\alpha D^{-1} E_{ji} D = \begin{cases} \alpha_{jj} E_{ii} & \text{si } i, j \leq r \text{ ou } i, j \geq r+1 \\ -\alpha_{jj} E_{ii} & \text{sinon.} \end{cases} \tag{I.3}$$

Mais

$$\mathrm{Tr}(E_{ij}\alpha E_{ij}^\tau) = \mathrm{Tr}(\varphi(E_{ij})\varphi(\alpha)\varphi(E_{ij})^\sigma) = \mathrm{Tr}(E_{ij}\alpha D^{-1} E_{ji} D) > 0$$

pour tout $1 \leq i, j \leq m$. Nous avons donc forcément $r = 0$ ou $r = m$, autrement dit $D = \pm \mathrm{I}_m$. Donc σ est la transposition matricielle. En particulier u est définie positive ou définie négative, ce qui montre le point *iv)*.

Il ne reste plus qu'à prouver *ii)*. Comme ${}^t\varphi(\alpha) = \varphi(\alpha^\tau) = \varphi(\alpha)$, $\varphi(\alpha)$ est symétrique. Posons $\varphi(\alpha) = \alpha_\varphi$. Soit $T \in \mathrm{GL}_m(\mathbb{R})$ telle que $T^{-1} = {}^tT$ et $T^{-1}\alpha_\varphi T = D$ où D est une matrice diagonale. Posons $X_{ij} = E_{ij}\,{}^tT$; alors

$$\mathrm{Tr}(X_{ij}\alpha_\varphi\,{}^tX_{ij}) = D_{jj}$$

donc $D_{jj} > 0$ pour tout $1 \leq j \leq m$ et donc α_φ est définie positive.

□

Définition 1.7.2. *Une involution sur* $\mathrm{M}_m(\mathbb{R})$ *vérifiant les conditions de la proposition 1.7.1 (pour un certain* α*) est dite positive. Plus simplement dit, une involution positive sur* $\mathrm{M}_m(\mathbb{R})$ *est une involution sur* $\mathrm{M}_m(\mathbb{R})$ *isomorphe à la transposition matricielle.*

Corollaire 1.7.3. *Sous les hypothèses de la proposition précédente,*

$$\left(\frac{\mathrm{Tr}(x\alpha x^\tau)}{m}\right)^m \geq \det(x\alpha x^\tau)$$

pour tout $x \in \mathrm{M}_m(\mathbb{R})$.

Preuve : Si x n'est pas inversible alors le terme de droite est nul et l'inégalité découle du fait que Tr_α est définie positive. Si x est inversible, alors, d'après la proposition précédente,

$$\mathrm{Tr}(x\alpha x^\tau) = \mathrm{Tr}(\varphi(x)\varphi(\alpha)\,{}^t\varphi(x))$$

où φ est un automorphisme et $\varphi(\alpha)$ est symétrique et définie positive. Comme x est inversible, $\varphi(x)\varphi(\alpha)\,{}^t\varphi(x)$ est encore une forme bilinéaire symétrique définie positive. Elle est donc orthogonalement diagonalisable et l'inégalité entre moyennes arithmétique et géométrique nous assure que

$$\left(\frac{\mathrm{Tr}(\varphi(x)\varphi(\alpha)\,{}^t\varphi(x))}{m}\right)^m \geq \det(\varphi(x)\varphi(\alpha)\,{}^t\varphi(x)).$$

Comme $\det(\varphi(x)\varphi(\alpha)\,{}^t\varphi(x)) = \det(x\alpha x^\tau)$ nous obtenons le résutat escompté.

□

Soit maintenant τ une involution $\mathbb{R}$-linéaire sur $\mathrm{M}_m(\mathbb{C})$. Deux cas sont possibles :

1. L'involution τ est $\mathbb{C}$-linéaire. Dans ce cas, il existe $u \in \mathrm{GL}_m(\mathbb{C})$ symétrique ou anti-symétrique telle que $\tau = \mathrm{Int}(u) \circ t$.
2. L'involution τ n'est pas $\mathbb{C}$-linéaire. Dans ce cas, il existe $u \in \mathrm{GL}_m(\mathbb{C})$ hermitienne telle que $\tau = \mathrm{Int}(u) \circ t \circ {}^-$.

(voir [KMMT98] proposition 2.19 et 2.20, p.24)

Proposition 1.7.4. *Soient τ une involution $\mathbb{R}$-linéaire sur $\mathrm{M}_m(\mathbb{C})$ et $\alpha \in \mathcal{F}^\times = \{x \in \mathrm{GL}_m(\mathbb{C}) \mid x^\tau = x\}$. La forme bilinéaire trace*

$$\begin{array}{rccl} \mathrm{Tr}_\alpha : & \mathrm{M}_m(\mathbb{C}) \times \mathrm{M}_m(\mathbb{C}) & \longrightarrow & \mathbb{R} \\ & (a, b) & \longmapsto & \mathrm{Tr}(a\alpha\tau(b)) + \overline{\mathrm{Tr}(a\alpha\tau(b))} \end{array}$$

est définie positive si et seulement si

i) Il existe un automorphisme intérieur $\varphi = \mathrm{Int}(S)$ tel que $\varphi(y^\tau) = {}^t\overline{\varphi(y)}$.

ii) La forme bilinéaire $\varphi(\alpha)$ est définie positive et hermitienne.

De plus, dans ce cas, les affirmations suivantes sont vérifiées :

iii) L'involution τ n'est pas $\mathbb{C}$-linéaire.

iv) Les quantités $\mathrm{Tr}(a\alpha\tau(a))$ et $\det(a\alpha\tau(a))$ sont des nombres réels pour tout $a \in \mathrm{M}_m(\mathbb{C})$.

v) On a $\tau = \mathrm{Int}(u) \circ t \circ {}^-$ où $u \in M_m(\mathbb{C})$ est hermitienne et définie positive ou définie négative.

Preuve : De la même manière que dans la proposition 1.7.1nous montrons que *i)* et *ii)* impliquent que Tr_α est définie positive.

La réciproque est également très similaire à la proposition 1.7.1. Nous nous convainquons, en utilisant les équations I.2 et I.3 (dans la preuve de 1.7.1) et l'équation :

$$\mathrm{Tr}(iE_{kl}B^t(iE_{kl})u) = -B_{ll}u_{kk} \text{ où } i = \sqrt{-1} \in \mathbb{C} \tag{I.4}$$

que u est hermitienne. Cela signifie que τ n'est pas $\mathbb{C}$-linéaire et que $\tau = \mathrm{Int}(u) \circ t \circ {}^-$ avec ${}^t\bar{u} = u$. Pour le reste de la preuve nous procèdons de la même manière en utilisant le fait que u est une forme sesquilinéaire hermitienne.

□

Définition 1.7.5. *Une involution sur $\mathrm{M}_m(\mathbb{C})$ vérifiant les conditions de la proposition 1.7.4 (pour un certain α) est dite positive. Plus simplement, une involution positive est une involution sur $\mathrm{M}_m(\mathbb{C})$ isomorphe à la transconjugaison matricielle.*

Corollaire 1.7.6. *Sous les hypothèses de la proposition précédente,*

$$\left(\frac{\mathrm{Tr}(x\alpha x^\tau)}{m}\right)^m \geq \det(x\alpha x^\tau)$$

pour tout $x \in \mathrm{M}_m(\mathbb{C})$.

PREUVE : Nous procédons comme dans le corollaire 1.7.3 en utilisant le fait qu'une forme hermitienne définie positive est unitairement diagonalisable et que toutes ses valeurs propres sont réelles et positives.

□

Il reste à étudier le cas de $\mathrm{M}_{\frac{m}{2}}(\mathbb{H}) \cong \mathrm{M}_m^{\mathbb{H}}(\mathbb{C})$. Nous avons déjà vu dans la section précédente que

$$\mathrm{nr}_{\mathrm{M}_{\frac{m}{2}}(\mathbb{H})/\mathbb{R}}(x) = \det(\Phi(x))$$

et

$$\mathrm{tr}_{\mathrm{M}_{\frac{m}{2}}(\mathbb{H})/\mathbb{R}}(x) = \mathrm{Tr}(\Phi(x))$$

pour tout $x \in \mathrm{M}_{\frac{m}{2}}(\mathbb{H})$ (où Φ est l'isomorphisme entre $\mathrm{M}_{\frac{m}{2}}(\mathbb{H})$ et $\mathrm{M}_m^{\mathbb{H}}(\mathbb{C})$ défini dans la proposition 1.6.7). Il est facile de montrer que si γ est l'involution canonique sur les coefficients des matrices de $\mathrm{M}_{\frac{m}{2}}(\mathbb{H})$ et $^-$ la conjugaison complexe sur les coefficients des matrices de $\mathrm{M}_m^{\mathbb{H}}(\mathbb{C})$, alors

$$\Phi \circ t \circ \gamma = t \circ {}^-.$$

Soit τ une involution $\mathbb{R}$-linéaire sur $\mathrm{M}_{\frac{m}{2}}(\mathbb{H})$; alors il existe (voir [KMMT98] proposition 2.20, p.24) un automorphisme intérieur $\mathrm{Int}(u)$ de $\mathrm{M}_{\frac{m}{2}}(\mathbb{H})$ tel que

$$\tau = \mathrm{Int}(u) \circ t \circ \gamma$$

avec ${}^t u^\gamma = \pm u$. De plus τ est symplectique si et seulement si ${}^t u^\gamma = u$.

Vu ce qui précède, les involutions sur $\mathrm{M}_m^{\mathbb{H}}(\mathbb{C})$ sont de la forme $\mathrm{Int}(u) \circ t \circ {}^-$ où ${}^t\bar{u} = \pm u$ et $u \in \mathrm{GL}_m^{\mathbb{H}}(\mathbb{C})$.

Proposition 1.7.7. *Soient* τ *une involution* $\mathbb{R}$*-linéaire sur* $\mathrm{M}_m^{\mathbb{H}}(\mathbb{C})$ *et* $\alpha \in \mathcal{F}^\times = \{x \in \mathrm{GL}_m^{\mathbb{H}}(\mathbb{C}) \mid \tau(x) = x\}$. *La forme bilinéaire trace*

$$\begin{array}{rccc} \mathrm{Tr}_\alpha : & \mathrm{M}_m^{\mathbb{H}}(\mathbb{C}) \times \mathrm{M}_m^{\mathbb{H}}(\mathbb{C}) & \longrightarrow & \mathbb{R} \\ & (a,b) & \longmapsto & \mathrm{Tr}(a\alpha\tau(b)) \end{array}$$

est définie positive si et seulement si les deux conditions suivantes sont vérifiées :

i) Il existe un automorphisme intérieur $\varphi = \mathrm{Int}(S)$ *de* $\mathrm{M}_m^{\mathbb{H}}(\mathbb{C})$ *tel que* $\varphi(y^\tau) = {}^t\overline{\varphi(y)}$.

ii) La forme sesquilinéaire $\varphi(\alpha)$ *est définie positive et hermitienne.*

De plus, dans ce cas, les conditions suivantes sont vérifiées

iii) L'involution τ *est symplectique.*

iv) On a $\tau = \mathrm{Int}(u) \circ t \circ {}^- $ *où* $u \in \mathrm{M}_m^{\mathbb{H}}(\mathbb{C})$ *est hermitienne et définie positive ou définie négative.*

PREUVE : Une fois de plus la démonstration est analogue à celle de la proposition 1.7.1. La partie "si" se démontre comme dans 1.7.1 sans présenter de difficultés.

Pour la partie "seulement si", posons $m = 2k$ et considérons $\tau = \mathrm{Int}(u) \circ {}^- \circ t$ avec ${}^t\bar{u} = \pm u$. Supposons que ${}^t\bar{u} = -u$. Alors, par un théorème spectral classique, il existe $T \in \mathrm{GL}_m(\mathbb{C})$ avec ${}^t\overline{T} = T^{-1}$, telle que $T^{-1}uT = D$ où $D = \mathrm{Diag}(i\theta_1, \ldots, i\theta_m)$ avec les θ_i réels. Remarquons de plus que si $v = (v_1, \ldots, v_k, v_{k+1}, \ldots, v_m)$ est un vecteur propre de u alors $v' = (-\bar{v}_{k+1}, \ldots, -\bar{v}_m, \bar{v}_1, \ldots, \bar{v}_k)$ est encore un vecteur propre de u. Il est donc possible de choisir, quitte à réarranger les colonnes, $T \in \mathrm{GL}_m^{\mathbb{H}}(\mathbb{C})$ de sorte que $D = \mathrm{Diag}(i\theta_1, \ldots, i\theta_k, -i\theta_1, \ldots, -i\theta_k)$. Nous procédons comme dans 1.7.1 pour voir que l'involution τ est isomorphe à l'involution $\mathrm{Int}(D) \circ t \circ {}^-$. Nous allons maintenant voir que cette involution est incompatible avec le fait que Tr_α est définie positive.

Considérons les ensembles

$$\begin{aligned}
\mathcal{B}_1 &= \{E_{r,j} + E_{r+k,j+k} \mid 1 \leq r, j \leq k\} \\
\mathcal{B}_2 &= \{E_{r,j} - E_{r-k,r+k} \mid k+1 \leq r \leq m,\ 1 \leq j \leq k\} \\
\mathcal{B}_3 &= \{iE_{r,j} - iE_{r+k,j+k} \mid 1 \leq r, j \leq k\} \\
\mathcal{B}_4 &= \{iE_{r,j} + iE_{r-k,j+k} \mid k+1 \leq r, j \leq m\}
\end{aligned}$$

et

$$\mathcal{B} = \bigcup_{s=1}^{4} \mathcal{B}_s$$

alors $\mathcal{B}$ est une $\mathbb{R}$-base de $\mathrm{M}_m^{\mathbb{H}}(\mathbb{C})$. Pour tout $D \in \mathrm{M}_m^{\mathbb{H}}(\mathbb{C})$

$$\mathrm{Tr}(b_1 \alpha D {}^t\bar{b}_1 D) = D_{jj} D_{ii} (\alpha_{jj} + \bar{\alpha}_{jj})$$

pour tout $1 \leq i, j \leq k$ et tout $b_1 \in \mathcal{B}_1$ et

$$\mathrm{Tr}(b_2 \alpha D {}^t\bar{b}_2 D) = D_{j+k,j+k} D_{i-k,i-k} (\alpha_{jj} + \bar{\alpha}_{jj})$$

pour tout $i \geq k+1$, $j \leq k$, et tout $b_2 \in \mathcal{B}_2$.

En particulier, si Tr_α est définie positive, alors $\mathrm{sign}(D_{jj}) = \mathrm{sign}(D_{j+k,j+k})$ pour tout $j \leq k$, ce qui est faux dans notre situation. Donc $\tau = \mathrm{Int}(u) \circ {}^- \circ t$ avec ${}^t\bar{u} = u$ et donc τ est symplectique.

En suivant la même démarche que ci-dessus (et en s'inspirant de 1.7.1) nous démontrons que τ est isomorphe à ${}^- \circ t$ ce qui prouve *i)*. Le point *ii)* se traite comme dans 1.7.1).

□

Définition 1.7.8. *Une involution sur* $\mathrm{M}_m^{\mathbb{H}}(\mathbb{C})$ *vérifiant les conditions de la proposition 1.7.7 (pour un certain* α*) est dite positive. Plus simplement, une involution positive est une involution sur* $\mathrm{M}_m^{\mathbb{H}}(\mathbb{C})$ *isomorphe à la transconjugaison matricielle.*

Corollaire 1.7.9. *Sous les hypothèses de la proposition précédente,*

$$\left(\frac{\mathrm{Tr}(x\alpha x^\tau)}{m}\right)^m \geq \det(x\alpha x^\tau)$$

pour tout $x \in \mathrm{M}_m^{\mathbb{H}}(\mathbb{C})$*. Autrement dit*

$$\left(\frac{\mathrm{tr}_{\mathrm{M}_{\frac{m}{2}}(\mathbb{H})/\mathbb{R}}(x\alpha x^\tau)}{m}\right)^m \geq \mathrm{nr}_{\mathrm{M}_{\frac{m}{2}}(\mathbb{H})/\mathbb{R}}(x\alpha x^\tau)$$

pour tout $x \in \mathrm{M}_{\frac{m}{2}}(\mathbb{H})$.

Preuve : Nous procédons comme dans la preuve du corollaire 1.7.3.

□

Comme conséquence de ces résultats, nous pouvons énoncer un théorème qui est une généralisation de l'inégalité entre norme et trace sur un corps de nombres.

Théorème 1.7.10. *Soit* A *une algèbre centrale simple de dimension* $r = m^2$ *sur un corps de nombres de degré* n*. Soit* τ *une involution* $\mathbb{R}$*-linéaire sur* $A_{\mathbb{R}}$*. On suppose qu'il existe* $\alpha \in \mathcal{F}_{A_{\mathbb{R}}}^{\times}$ *tel que la forme bilinéaire*

$$\begin{array}{rccc} \mathrm{T}_\alpha : & A_{\mathbb{R}} \times A_{\mathbb{R}} & \longrightarrow & \mathbb{R} \\ & (a,b) & \longmapsto & \mathrm{tr}_{A_{\mathbb{R}}/\mathbb{R}}(a\alpha b^\tau) \end{array}$$

est définie positive. Alors

$$\left(\frac{\mathrm{tr}_{A_{\mathbb{R}}/\mathbb{R}}(x\alpha x^{\tau})}{n\cdot m}\right)^{n\cdot m} \geq \mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(x\alpha x^{\tau})$$

pour tout $x \in A_{\mathbb{R}}$.

Preuve : Rappelons que τ induit sur chaque composante matricielle de $A_{\mathbb{R}}$ une involution $\mathbb{R}$-linéaire que nous noterons τ_i. Par la proposition 1.6.10,

$$\left(\frac{\mathrm{tr}_{A_{\mathbb{R}}/\mathbb{R}}(x\alpha x^{\tau})}{n\cdot m}\right)^{n\cdot m} = \left(\left(\frac{1}{n}(v_1+v_2+v_3)\right)^n\right)^m$$

où

$$\begin{aligned}
v_1 &= \frac{1}{m}\sum_{i=1}^{w}\mathrm{Tr}(x_i\alpha_i x_i^{\tau_i})\\
v_2 &= \frac{1}{m}\sum_{i=w+1}^{r_1}\mathrm{Tr}(x_i\alpha_i x_i^{\tau_i})\\
v_3 &= \frac{1}{m}\sum_{i=r_1+1}^{r_1+r_2}\mathrm{Tr}(x_i\alpha_i x_i^{\tau_i}) + \overline{\mathrm{Tr}(x_i\alpha_i x_i^{\tau_i})}
\end{aligned}$$

où $\tau_i = \tau|_{\mathrm{M}_i}$. L'inégalité entre moyennes arithmétique et géométrique nous dit que cette dernière expression est supérieure ou égale à

$$\left(\prod_{i=1}^{w}\frac{\mathrm{Tr}(x_i\alpha_i x_i^{\tau_i})}{m}\cdot\prod_{i=w+1}^{r_1}\frac{\mathrm{Tr}(x_i\alpha_i x_i^{\tau_i})}{m}\cdot\prod_{i=r_1+1}^{r_1+r_2}\frac{\mathrm{Tr}(x_i\alpha_i x_i^{\tau_i})}{m}\cdot\frac{\overline{\mathrm{Tr}(x_i\alpha_i x_i^{\tau_i})}}{m}\right)^m$$

qui, par les corollaires 1.7.3, 1.7.6, 1.7.9, est elle-même supérieure ou égale à

$$\prod_{i=1}^{w}\det(x_i\alpha_i x_i^{\tau_i})\cdot\prod_{i=w+1}^{r_1}\det(x_i\alpha_i x_i^{\tau_i})\cdot\prod_{i=r_1+1}^{r_1+r_2}\det(x_i\alpha_i x_i^{\tau_i})\cdot\overline{\det(x_i\alpha_i x_i^{\tau_i})}$$

qui est exactement $\mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(x\alpha x^{\tau})$.

□

Le théorème est énoncé ici sous la version qui interviendra par la suite. Il est possible d'en donner une version qui rappelle l'inégalité entre norme et trace dans le cas des corps de nombres :

Théorème 1.7.11. *Soient A une algèbre centrale simple de dimension $r = m^2$ sur un corps de nombres de degré n, $\alpha \in A_{\mathbb{R}}$ tel que α_i est (à automorphisme près) symétrique et définie positive pour tout $w+1 \leq i \leq r_1$ et (à automorphisme près) hermitienne, définie positive pour tout $1 \leq i \leq w$ et tout $r_1 + 1 \leq i \leq r_1 + r_2$, alors*

$$\left(\frac{\mathrm{tr}_{A_{\mathbb{R}}/\mathbb{R}}(\alpha)}{n \cdot m}\right)^{n \cdot m} \geq \mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(\alpha)$$

Preuve : La démonstration se fait comme dans le théorème précédent. □

1.8 Déterminant d'un réseau idéal

Si nous résumons une partie des résultats des deux sections précédentes en termes de réseaux idéaux, nous obtenons le théorème suivant.

Théorème 1.8.1. *Soit A une algèbre centrale simple de dimension finie sur un corps de nombres et (I, b_α) un réseau idéal de A. Alors*

$$b_\alpha(x,y) =$$

$$\sum_{i=1}^{w} \mathrm{Tr}(x_i \alpha_i {}^t\overline{y_i}) + \sum_{i=w+1}^{r_1} \mathrm{Tr}(x_i \alpha_i {}^t y_i) + \sum_{i=r_1+1}^{r_2} \left(\mathrm{Tr}(x_i \alpha_i {}^t\overline{y_i}) + \overline{\mathrm{Tr}(x_i \alpha_i {}^t\overline{y_i})}\right)$$

où les x_i, α_i, y_i désignent (à automorphisme intérieur près) les images de x, α, y par δ_i (voir la notation 1.6.9) dans l'algèbre matricielle correspondante.

Remarque : Pour simplifier les notations et en même temps parce qu'il s'agit du cas qui nous préoccupera par la suite, nous nous sommes limités dans ce théorème aux algèbres centrales simples sur un corps de nombres, c'est-à-dire aux algèbres séparables sur $\mathbb{Q}$ avec une seule composante simple. Pourtant le théorème se généralise facilement à toute algèbre séparable sur $\mathbb{Q}$.

Corollaire 1.8.2. *Soit I un idéal de A. Alors (I, b_1) est un réseau idéal.*

Preuve : Il suffit de vérifier que $b_1(x,x) > 0$ si $x \neq 0$, ce qui découle du théorème précédent.

□

Nous allons maintenant donner une caractérisation du déterminant d'un réseau idéal. Pour cela nous avons besoin de quelques résultats supplémentaires dont certains généralisent les résultats obtenus à la section 1.2.

Définition 1.8.3. *Soient R un anneau de Dedekind, $k = \mathrm{Frac}(R)$, L un corps contenant k, A une k-algèbre séparable de dimension r, I un idéal de A et $b : I_L \times I_L \longrightarrow L$ une forme bilinéaire non dégénérée.*

i) On définit le dual de I par rapport à b de la façon suivante :

$$I_b^* = \{x \in A_L \mid b(x, I) \subset R\}.$$

ii) Le déterminant de b est l'idéal fractionnaire de R engendré par le déterminant des matrices $b(x_i, x_j)_{1\leq i,j\leq r}$ où les x_i parcourent I. Autrement dit

$$\det(b) = \langle \det(b(x_i, x_j)_{1\leq i,j\leq r}) \mid x_1, \ldots, x_r \in I\rangle.$$

iii) Si b est la forme bilinéaire trace, on note

$$\tilde{I}_L = \{x \in A_L \mid \mathrm{tr}_{A_L/L}(xI) \subset R\}$$

le dual de b. C'est la différente inverse de I.

Remarque : Si

$$\begin{array}{rccc} d: & I & \longrightarrow & I_L \\ & x & \longmapsto & x \otimes 1 \end{array}$$

est l'inclusion canonique, alors I_b^* est simplement l'idéal dual $d(I)_b^*$ défini dans 1.2.12.

Proposition 1.8.4. *Soient R un anneau de Dedekind, $k = \mathrm{Frac}(R)$, L un corps contenant k, A une k-algèbre séparable, I un idéal de A et*

$$b : I_L \times I_L \longrightarrow L$$

une forme bilinéaire non dégénérée. Alors I_b^* est un R-réseau complet de A_L et pour tout $\beta \in R$ avec $\beta I \subset I_b^*$,

$$\beta^{-r}\mathrm{ord}_R(I_b^*/\beta I) = \det(b).$$

Preuve : Soit $\mathcal{B} = \{e_1, \ldots, e_r\}$ une k-base de A contenue dans I. Alors $\mathcal{B}^*$, la base duale de $\mathcal{B}$, est une L-base de A_L. Comme I est un idéal de A, il existe une base $\mathcal{B}' = \{f_1, \ldots, f_r\}$ de A avec

$$Re_1 \oplus \cdots \oplus Re_r \subset I \subset Rf_1 \oplus \cdots \oplus Rf_r$$

En passant au dual, nous obtenons

$$Rf_1^* \oplus \cdots \oplus Rf_r^* \subset I^* \subset Re_1^* \oplus \cdots \oplus Re_r^*,$$

donc I^* est contenu dans un R-réseau complet. De plus

$$Lf_1^* \oplus \cdots \oplus Lf_r^* \subset LI^* \subset Le_1^* \oplus \cdots \oplus Le_r^*$$

donc I_b^* est bien un module de génération finie tel que $LI_b^* = A_L$. La même démarche montre que $I^*_{b|_{I\times I}} = I^* \cap A$ est un idéal de A, donc il existe $\beta \in R$ tel que $\beta I \subset I^* \cap A \subset I^*$.
Pour la deuxième affirmation, nous procèdons comme dans le corollaire 1.2.24.

□

Le dual, I_b^*, de I est donc un R-réseau complet de la L-algèbre séparable A_L, pourtant nous ne pouvons parler d'idéal de A_L pour I_b^*. En effet, dans ce cas, $L \neq \mathrm{Frac}(R)$, en particulier nous n'avons pas de notion de norme de I_b^*.

Afin de simplifier les notations nous introduisons ici la notion de norme dans un cadre plus général.

Définition 1.8.5. *Soient R un anneau de Dedekind, $k = \mathrm{Frac}(R)$, L un corps contenant k, A une k-algèbre séparable de dimension r, I un R-réseau complet de A_L et $\Lambda = \mathcal{O}_l(I) = \{x \in A_L \mid xI \subset I\}$ l'ordre à gauche de I. On suppose que $\mathcal{O}_l(I) \subset LI$ et qu'il existe $\alpha \in A_L$ tel que $\alpha I \subset \Lambda$. La norme de I est l'idéal fractionnaire généralisé de R donné par :*

$$\mathrm{N}_{A_L/L}(I) = \mathrm{N}_{A_L/L}(\alpha)^{-1}\mathrm{ord}_R(\Lambda/\alpha I).$$

On vérifie que cette norme est indépendante du choix de α et qu'elle vérifie les mêmes propriétés que la norme des idéaux.

Il est clair que si I est un idéal de A on a

$$\mathrm{N}_{A/k}(I) = \mathrm{N}_{A_L/L}(I).$$

On suppose maintenant que A_L est muni d'une involution L-linéaire τ et que la forme bilinéaire b est donnée par

$$b(x, y) = b_\alpha(x, y) = \mathrm{tr}_{A_L/L}(x\alpha y^\tau)$$

où $\alpha \in \mathcal{F}_{A_L}^\times$.

Proposition 1.8.6. *Soient R un anneau de Dedekind, $k = \mathrm{Frac}(R)$, L un corps contenant k, A une k-algèbre séparable et Λ un ordre de A. Soient encore τ une involution sur A_L et I un idéal à droite de Λ. Alors*

i) $\mathcal{O}_r(I^\tau) = \mathcal{O}_l(I)^\tau$ *et* $\mathcal{O}_l(I^\tau) = \Lambda^\tau$.

ii) $I^*_{b_\alpha} = I^{-\tau}\tilde{\Lambda}^\tau\alpha^{-1}$.

Preuve : simples vérifications.

□

Corollaire 1.8.7. *Sous les hypothèses de la proposition précédente Λ^τ est un ordre de la k-algèbre A^τ et $I^*_{b_\alpha}\alpha$ (respectivement I^τ) est un idéal à droite (respectivement à gauche) de Λ^τ. De plus*

$$\mathrm{N}_{A_L/L}(I^\tau) = \mathrm{N}_{A^\tau/k}(I^\tau) = \mathrm{N}_{A/k}(I) \tag{I.5}$$

et

$$\mathrm{N}_{A_L/L}(I^*_{b_\alpha}) = \mathrm{N}_{A_L/L}(\alpha^{-1})\mathrm{d}(\Lambda)^{-1}\mathrm{N}_{A/k}(I)^{-1} \tag{I.6}$$

Preuve : Les premières affirmations sont claires. Pour les affirmations sur les normes, remarquons d'abord le résultat général suivant. Si J est un idéal de Λ^τ, alors il existe $\beta \in R$ avec $\beta J \subset \Lambda^\tau$ de sorte que, par définition,

$$\mathrm{N}_{A_L/L}(J) = \mathrm{N}_{A_L/L}(\beta^{-1})\mathrm{ord}_R(\Lambda^\tau/\beta J) = \beta^{-r}\mathrm{ord}_R(\Lambda^\tau/\beta J) = \mathrm{N}_{A^\tau/k}(J).$$

En d'autres termes, la norme sur A_L d'un idéal de A^τ coïncide avec sa norme sur A^τ. Pour montrer I.5 il suffit donc de vérifier la seconde égalité. Celle-ci découle du fait que

$$\Lambda^\tau/\beta I^\tau \cong \Lambda/\beta I.$$

Pour I.6, nous avons

$$\mathrm{N}_{A_L/L}(I^*_{b_\alpha}) = \mathrm{N}_{A_L/L}(\alpha^{-1})\mathrm{N}_{A_L/L}(I^*_{b_\alpha}\alpha).$$

Le calcul de $\mathrm{N}_{A_L/L}(I^*_{b_\alpha}\alpha)$ est facilité par le fait que $I^*_{b_\alpha}\alpha$ est un idéal de Λ^τ :

$$\mathrm{N}_{A_L/L}(I^*_{b_\alpha}\alpha) = \mathrm{N}_{A^\tau/k}(\tilde{\Lambda}^\tau)\mathrm{N}_{A^\tau/k}(I)^{-\tau} = \mathrm{d}(\Lambda)^{-1}\mathrm{N}_{A/k}(I)^{-1}$$

où la première égalité découle de la proposition 1.8.6 et la seconde de la suite d'égalités

$$\mathrm{N}_{A^\tau/k}(\tilde{\Lambda}^\tau) = \mathrm{N}_{A/k}(\tilde{\Lambda}) = \mathrm{N}(\mathcal{D}(\Lambda))^{-1} = \mathrm{d}(\Lambda)^{-1}.$$

□

Afin de calculer le déterminant de b_α, nous avons besoin d'un dernier résultat.

Proposition 1.8.8. *Soient A comme ci-dessus et I un idéal à droite de Λ, un ordre de A. On sait que $I^*_{b_\alpha}\alpha$ et I^τ sont des idéaux de Λ^τ, donc il existe $\beta \in R$ avec $\beta I^\tau \subset I^*_{b_\alpha}\alpha$. On a*

$$\mathrm{N}_{A_L/L}(\alpha^{-1})\det(b_\alpha) = \beta^{-r}\mathrm{ord}_R(I^*_{b_\alpha}\alpha/\beta I^\tau).$$

Preuve : Nous procèdons comme dans le corollaire 1.2.24 pour nous ramener au cas où les idéaux sont libres. Dans ce cas posons $\mathcal{B} = \{e_1, \ldots, e_r\}$ une R-base de I et $\mathcal{B}^*$ sa base duale. Alors

$$e_i = \sum_{j=1}^{r} b(e_j, e_i)e_j^*.$$

Observons le changement de bases entre les bases $\mathcal{B}^\tau$ de I^τ et $\mathcal{B}^*\alpha$ de $I^*_{b_\alpha}\alpha$. Le changement de base se fait en deux temps. Tout d'abord, la matrice de passage M' de $\mathcal{B}^\tau$ à $\alpha(\mathcal{B}^*)^\tau$ est donnée par la matrice de la multiplication par α^{-1} multipliée par la matrice $b(e_i, e_j)$ (car $e_i^\tau = \sum_{j=1}^r \alpha^{-1}b(e_j, e_i)\alpha(e_j^*)^\tau$).

Ensuite, la matrice de passage M de $\alpha(\mathcal{B}^*)^\tau$ à $\mathcal{B}^*\alpha$ est son propre inverse (car τ est d'ordre 2).

Finalement, la matrice de passage entre $\mathcal{B}^\tau$ et $\mathcal{B}^*\alpha$ est donnée par $P = M'M$. Le lemme 1.2.23 nous assure que

$$\det(P)\cdot R = \beta^{-r}\mathrm{ord}_R(I^*_{b_\alpha}\alpha/\beta I^\tau).$$

Or

$$\det(P) = \det(M'M) = \pm\det(M') = \pm\mathrm{N}_{A_L/L}(\alpha^{-1})\det(b_\alpha).$$

□

Corollaire 1.8.9. *Soient A une algèbre séparable de dimension r sur k, L un corps contenant k, Λ un ordre de A, I un idéal à droite de Λ et $b_\alpha : I_L \times I_L \longrightarrow L$, la forme bilinéaire symétrique non dégénérée donnée par*

$$b(x, y) = \mathrm{tr}_{A_L/L}(x\alpha y^\tau)$$

où τ est une involution L-linéaire sur A_L et $\alpha \in \mathcal{F}^\times_{A_L}$. Alors

$$\det(b_\alpha) = \mathrm{N}_{A_L/L}(\alpha)\mathrm{N}_{A/k}(I)^2\mathrm{d}(\Lambda/R).$$

PREUVE : Soient $\beta, \gamma \in R$ tels que $\gamma\beta I^\tau \subset \gamma I^*_{b_\alpha}\alpha \subset \Lambda^\tau$. Considérons la suite exacte courte de R-modules

$$0 \longrightarrow I^*_{b_\alpha}\alpha/\beta I^\tau \longrightarrow \Lambda^\tau/\gamma\beta I^\tau \longrightarrow \Lambda^\tau/\gamma I^*_{b_\alpha}\alpha \longrightarrow 0$$

alors (voir proposition 1.2.20)

$$\mathrm{ord}_R(\Lambda^\tau/\gamma\beta I^\tau) = \mathrm{ord}_R(\Lambda^\tau/\gamma I^*_{b_\alpha}\alpha)\mathrm{ord}_R(I^*_{b_\alpha}\alpha/\beta I^\tau)$$

autrement dit,

$$\gamma^r\beta^r \mathrm{N}_{A/k}(I) = \mathrm{N}_{A_L/L}(\alpha)\gamma^r \mathrm{N}_{A_L/L}(I^*_{b_\alpha})\mathrm{N}_{A_L/L}(\alpha^{-1})\beta^r \det(b_\alpha)$$

ou encore

$$\mathrm{N}_{A/k}(I) = \mathrm{N}_{A_L/L}(I^*_{b_\alpha}) \det(b_\alpha).$$

En remplaçant la valeur de $\mathrm{N}_{A_L/L}(I^*_{b_\alpha})$ par celle donnée dans le corollaire 1.8.7, nous obtenons

$$\mathrm{N}_{A/k}(I) = \mathrm{N}_{A_L/L}(\alpha^{-1})\mathrm{d}(\Lambda/R)^{-1}\mathrm{N}_{A/k}(I)^{-1} \det(b_\alpha)$$

d'où le résultat.

□

Nous allons maintenant appliquer ces résultats au cas qui nous intéresse, c'est-à-dire $R = \mathbb{Z}$, $k = \mathbb{Q}$, A est une K-algèbre centrale simple de dimension $r = m^2$ où K est un corps de nombres de degré n, $L = \mathbb{R}$ et (I, b_α) est un réseau idéal sur A.
Commençons par un résultat qui lie le discriminant d'un ordre Λ en tant que $\mathbb{Z}$-ordre et son discriminant en tant que $\mathcal{O}_K$-ordre.

Proposition 1.8.10. *Soient K un corps de nombres, A une algèbre centrale simple de dimension $r = m^2$ sur K et Λ un ordre de A. Alors*

$$\mathrm{d}(\Lambda/\mathbb{Z}) = \mathrm{N}_{K/\mathbb{Q}}(\mathrm{d}(\Lambda/\mathcal{O}_K))\mathrm{d}_K^r$$

où $\mathrm{d}(\Lambda/\mathbb{Z})$ désigne le discriminant de Λ vu comme $\mathbb{Z}$-ordre de la $\mathbb{Q}$-algèbre séparable A, $\mathrm{d}(\Lambda/\mathcal{O}_K) = \mathrm{d}(\Lambda)$ est le discriminant de Λ (vu comme $\mathcal{O}_K$-ordre de A) et d_K est le discriminant de K.

PREUVE : Voir [Rei03] exercices 1 et 2, p.223

Ce dernier résultat nous permet d'énoncer le résultat final qui donne une expression du déterminant d'un réseau idéal.

Proposition 1.8.11. *Soient K un corps de nombres de degré n, A une algèbre centrale simple de dimension $r = m^2$ sur K, Λ un ordre de A, I un idéal à droite de Λ et (I, α) un réseau idéal de A. Alors*

$$\det(I, \alpha) = \mathrm{N}_{A_{\mathbb{R}}/\mathbb{R}}(\alpha)\mathrm{N}_{K/\mathbb{Q}}(\mathrm{N}_{A/K}(I)^2\mathrm{d}(\Lambda/\mathcal{O}_K))\mathrm{d}_K^r$$

ou encore

$$\det(I, \alpha) = \mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(\alpha)^m\mathrm{N}_{K/\mathbb{Q}}(\mathrm{nr}_{A/K}(I)^{2m}\mathrm{d}(\Lambda/\mathcal{O}_K))\mathrm{d}_K^r.$$

Preuve : La première affirmation est une conséquence directe du corollaire 1.8.9 et de la proposition précédente. Pour la seconde affirmation, il suffit d'observer que

$$\mathrm{N}_{A_{\mathbb{R}}/\mathbb{R}}(\alpha) = \mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(\alpha)^m.$$

Cette égalité est toujours vraie dans le cas d'une algèbre centrale simple de dimension m^2, cependant $A_{\mathbb{R}}$ n'est pas une algèbre centrale simple sur $\mathbb{R}$ mais seulement séparable. Pourtant, par la proposition 1.2.10, nous avons

$$\mathrm{N}_{A_{\mathbb{R}}/\mathbb{R}}(\alpha) = \prod_{i=1}^{r_1+r_2} \mathrm{nr}_{A_i/\mathbb{R}}(\alpha)^{m_i}$$

où les A_i sont les composantes simples de $A_{\mathbb{R}}$ avec $m_i^2 = [A_i : K_i]$ où K_i est le centre de A_i. Mais toutes les composantes simples de $A_{\mathbb{R}}$ sont de dimension m^2 sur leur centre respectif (voir section 1.6) de sorte que

$$\mathrm{N}_{A_{\mathbb{R}}/\mathbb{R}}(\alpha) = \prod_{i=1}^{r_1+r_2} \mathrm{nr}_{A_i/\mathbb{R}}(\alpha)^m = \mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(\alpha)^m$$

où la seconde égalité découle encore de la proposition 1.2.10.

□

On préférera parfois, pour la simplicité de certains calculs, utiliser le résultat sous sa forme quasi originale :

Proposition 1.8.12. *Soient K un corps de nombres de degré n, A une algèbre centrale simple de dimension $r = m^2$ sur K, Λ un ordre de A, I un idéal bilatère de Λ et (I, b_α) un réseau idéal de A. Alors*

$$\det(I, b_\alpha) = \mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(\alpha)^m\mathrm{N}_{A/\mathbb{Q}}(I)^2\mathrm{d}(\Lambda/\mathbb{Z}).$$

Dans le cas particulier où $\alpha \in A$ et où l'involution sur $A_{\mathbb{R}}$ est induite par une involution sur A, on peut réécrire ce résultat et en donner une preuve différente.

Proposition 1.8.13. *Soient K un corps de nombres de degré n, A une algèbre centrale simple de dimension $r = m^2$ sur K munie d'une involution τ, Λ un ordre de A, I un idéal à droite de Λ et (I, α, τ) un réseau idéal de A avec $\alpha \in A$. Alors*

$$\det(I, \alpha, \tau) = \mathrm{N}_{K/\mathbb{Q}}(\mathrm{N}_{A/K}(\alpha)\mathrm{N}_{A/K}(I)^2\mathrm{d}(\Lambda/\mathcal{O}_K))\mathrm{d}_K^r$$

ou encore

$$\det(I, \alpha, \tau) = \mathrm{N}_{K/\mathbb{Q}}(\mathrm{nr}_{A/K}(\alpha)^m\mathrm{nr}_{A/K}(I)^{2m}\mathrm{d}(\Lambda/\mathcal{O}_K))\mathrm{d}_K^r.$$

Preuve : C'est bien sûr une conséquence directe de la proposition précédente. Cependant, dans ce cas

$$b_\alpha(x, y) = \mathrm{T}_{K/\mathbb{Q}}(\mathrm{tr}(x\alpha y^\tau))$$

pour tout $x, y \in A$ et cette forme bilinéaire a abondamment été étudiée dans la section 1.3. Sachant que $I^* = \tilde{\Lambda} I^{-\tau}\alpha^{-1}$ (comme Λ est maximal et comme τ est une involution sur A, $\Lambda^\tau = \Lambda$) en combinant les résutats 1.3.5 et 1.2.25 nous obtenons le résultat cherché.

□

1.9 Invariants d'Hermite

Toujours dans l'optique de déterminer les invariants des réseaux idéaux nous allons calculer l'invariant d'Hermite $\gamma_{\min}(\Lambda)$, où Λ est un ordre maximal, et borner inférieurement $\gamma_{\min}(I)$, où I est un idéal à droite de Λ. Nous donnerons également une borne supérieure de $\tau_{\min}(I)$. Dans cette section A est une algèbres centrales simples de dimension $r = m^2$ sur le corps de nombres K

Rappelons que si (I, α, η) est un réseau idéal de A, alors

1. $\gamma(I, \alpha, \eta) = \frac{\min(I,\alpha,\eta)}{\det(I,\alpha,\eta)^{\frac{1}{rn}}}$ et

$$\gamma_{\min}(I) = \min\{\gamma(I, \alpha, \eta) \mid (I, \alpha, \eta) \text{ est un réseau idéal de } A\}$$

2. $\tau(I, \alpha, \eta) = \frac{\max(I,\alpha,\eta)}{\det(I,\alpha,\eta)^{\frac{1}{rn}}}$ et

$$\tau_{\min}(I) = \min\{\tau_{\min}(I, \alpha, \eta) \mid (I, \alpha, \eta) \text{ est un réseau idéal de } A\}$$

Définition 1.9.1. *Soient I, J des idéaux dans une algèbre séparable A. On dit que I est équivalent à J s'il existe $x \in A^\times$ tel que $xI = J$. Le minimum d'un idéal I, noté* $\min(I)$*, est défini par*

$$\min(I) = \min\{\mathrm{N}_{A/\mathbb{Q}}(J) \mid J \text{ est équivalent à } I^{-1}\}.$$

Proposition 1.9.2. *Soient K un corps de nombres de degré n, A une K-algèbre centrale à division de dimension $r = m^2$, Λ un ordre de A et I un idéal à droite (ou à gauche) de Λ. Alors*

i) $\gamma_{\min}(I) \geq \frac{mn}{\mathrm{d}(\Lambda/\mathbb{Z})^{1/rn}} \min(I)^{2/rn} = \frac{mn}{\mathrm{N}_{K/\mathbb{Q}}(\mathrm{d}(\Lambda/\mathcal{O}_K))^{1/rn}\mathrm{d}_K^{1/n}} \min(I)^{2/rn}$,

ii) $\gamma_{\min}(\Lambda) = \frac{mn}{\mathrm{d}(\Lambda/\mathbb{Z})^{1/rn}} = \frac{mn}{\mathrm{N}_{K/\mathbb{Q}}(\mathrm{d}(\Lambda/\mathcal{O}_K))^{1/rn}\mathrm{d}_K^{1/n}}$.

Preuve : Soient $\alpha \in A_{\mathbb{R}}$ et τ une involution sur $A_{\mathbb{R}}$ tels que (I, α, τ) est un réseau idéal. Nous notons $q_\alpha(x) = \mathrm{tr}_{A_{\mathbb{R}}/\mathbb{R}}(x\alpha x^\tau)$ pour tout $x \in A_{\mathbb{R}}$. Pour tout $x \in A_{\mathbb{R}}$,

$$q_\alpha(x) = \mathrm{tr}_{A_{\mathbb{R}}/\mathbb{R}}(x\alpha x^\tau) \geq nm(\mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(x\alpha x^\tau))^{1/nm}$$

où l'inégalité découle du théorème 1.7.10. Le terme de droite de l'inégalité est $nm \cdot \mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(x)^{2/nm}\mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(\alpha)^{1/nm}$, mais l'expression de $\mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(\alpha)$ en fonction du déterminant de (I, α, τ) nous est donnée par la proposition 1.8.12. Par conséquent,

$$\frac{q_\alpha(x)}{\det(I, \alpha, \tau)^{1/rn}} \geq \frac{nm}{\mathrm{d}(\Lambda/\mathbb{Z})^{1/rn}} \frac{\mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(x)^{2/nm}}{\mathrm{N}_{A/\mathbb{Q}}(I)^{2/rn}}.$$

Observons l'inégalité lorsque $x \in A$. Dans ce cas, $\mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(x) = \mathrm{nr}_{A/\mathbb{Q}}(x) = \mathrm{N}_{A/\mathbb{Q}}(x)^{1/m}$ et il vient

$$\frac{q_\alpha(x)}{\det(I, \alpha, \tau)^{1/rn}} \geq \frac{nm}{\mathrm{d}(\Lambda/\mathbb{Z})^{1/rn}} \mathrm{N}_{A/\mathbb{Q}}(xI^{-1})^{2/rn}.$$

Comme $\mathrm{N}(xI^{-1}) \geq \min(I)$ pour tout $x \in A^\times$ et que

$$\gamma(I, \alpha, \tau) = \min\left\{ \frac{q_\alpha(x)}{\det(I, \alpha, \tau)^{1/rn}} \;\middle|\; x \in I \setminus \{0\} \right\}$$

nous obtenons *i)*.
Pour *ii)*, il suffit de voir que $\gamma_{\min}(\Lambda) \leq \frac{mn}{\mathrm{d}(\Lambda/\mathbb{Z})^{1/rn}}$ (l'autre inégalité découle de *i)*). Considérons le réseau $(\Lambda, 1)$, nous avons $\det(\Lambda, 1) = \mathrm{d}(\Lambda/\mathbb{Z})$ et $q_1(1) = nm$ de sorte que

$$\gamma_{\min}(\Lambda) \leq \gamma(\Lambda, 1) \leq \frac{nm}{\mathrm{d}(\Lambda/\mathbb{Z})^{1/rn}}$$

d'où le résultat.

□

Soit (I, α, τ) un réseau idéal de A. Remarquons que (I^*, α, τ) est un réseau idéal de A^τ (au sens de la définition 1.5.7). Afin de borner $\tau_{\min}(I)$, nous avons besoin d'énoncer la proposition précédente pour le réseau (I^*, α, τ). Cette proposition ne peut s'appliquer telle qu'elle est, car I^* est un idéal généralisé de A^τ. Bien que tous les résultats utilisés dans la proposition précédente s'étendent facilement aux idéaux généralisés, nous préférons donner ici une preuve du résultat qui nous intéresse en utilisant uniquement ce qui précède.

Corollaire 1.9.3. *Soient K un corps de nombres de degré n, A une K-algèbre centrale à division de dimension $r = m^2$, Λ un ordre de A et I un idéal à droite de Λ. Alors*

i) $\gamma_{\min}(I^*) \geq \frac{mn}{\mathrm{d}(\Lambda/\mathbb{Z})^{1/rn}} \min(I^*)^{2/rn} = \frac{mn}{\mathrm{N}_{K/\mathbb{Q}}(\mathrm{d}(\Lambda/\mathcal{O}_K))^{1/rn}\mathrm{d}_K^{1/n}} \min(I^*)^{2/rn}$,

ii) $\gamma_{\min}(\Lambda^*) = \frac{mn}{\mathrm{d}(\Lambda/\mathbb{Z})^{1/rn}} = \frac{mn}{\mathrm{N}_{K/\mathbb{Q}}(\mathrm{d}(\Lambda/\mathcal{O}_K))^{1/rn}\mathrm{d}_K^{1/n}}$.

Preuve : Nous savons que $I^*\alpha$ est un idéal à gauche de Λ^τ. De plus $(I^*\alpha, \alpha^{-1}, \tau) \cong (I^*, \alpha, \tau)$. Il suffit donc de montrer la proposition pour le réseau idéal $(I^*\alpha, \alpha^{-1}, \tau)$. Ainsi

$$\gamma(I^*\alpha, \alpha^{-1}, \tau) \geq \min_{\beta \in \mathcal{F}^\times_{A_\mathbb{R}}} \{\gamma(I^*\alpha, \beta, \tau)\} = \gamma_{\min}(I^*\alpha) \geq$$

$$\frac{mn}{\mathrm{d}(\Lambda^\tau/\mathbb{Z})^{1/rn}} \min(I^*\alpha)^{2/rn} = \frac{mn}{\mathrm{d}(\Lambda^\tau/\mathbb{Z})^{1/rn}} \min(I^*)^{2/rn}$$

Comme $\mathrm{d}(\Lambda^\tau/\mathbb{Z}) = \mathrm{d}(\Lambda/\mathbb{Z})$ on obtient *i)*. Le second point s'obtient comme dans la proposition précédente.

□

Lemme 1.9.4. *Pour tout réseau (L, q) de rang n,*

$$\tau(L, q)\gamma(L^*, q) \leq \frac{n^2}{4}.$$

Preuve : voir [BF06] lemme 4.4, p.8

Corollaire 1.9.5. *Soient K un corps de nombres de degré n, A une K-algèbre centrale à division de dimension $r = m^2$, Λ un ordre de A et I un idéal à droite de Λ. Alors*

$$\tau_{\min}(I) \leq \frac{nm^3}{4} \cdot \mathrm{d}(\Lambda/\mathbb{Z})^{1/rn}.$$

PREUVE : Nous avons

$$\frac{r^2 n^2}{4} \geq \tau(I, b_\alpha)\gamma(I^*, b_\alpha) \geq \tau(I, b_\alpha)\frac{mn}{\mathrm{d}(\Lambda/\mathbb{Z})^{1/rn}}$$

où les inégalités proviennent du lemme précédent (pour la première) et du corollaire 1.9.3 (pour la seconde).

□

Chapitre II

Minimum euclidien des ordres maximaux

Dans ce chapitre, nous définissons le minimum euclidien et le minimum inhomogène d'un ordre dans une algèbre centrale simple. Nous montrons, dans la section 2.3, que ces minima coïncident et sont rationnels sous certaines conditions. Dans la section 2.4, nous énonçons les résultats qui permettent de comparer le minimum euclidien de deux ordres d'une même algèbre. C'est dans la section 2.5 que se trouve le théorème principal du chapitre qui lie le minimum euclidien d'un idéal aux invariants d'Hermite des réseaux idéaux que l'on peut construire sur cet idéal. La section 2.6 classifie les algèbres à involution sur lesquelles la construction d'un réseau idéal est possible.

2.1 Anneaux euclidiens

Dans cette section nous allons définir un anneau euclidien et donner quelques résultats généraux. Les anneaux seront quelconques, sauf mention du contraire. Les propositions sont énoncées pour un anneau euclidien à droite mais reste vraies pour un anneau euclidien à gauche.

Définition 2.1.1. *Soient A un anneau et $\varphi : A \longrightarrow \mathbb{N}$ une application. On dit que A est euclidien à droite pour φ si, pour tout $a, b \in A$ avec $b \neq 0$, il existe $q, r \in A$ tels que $a = bq + r$ et $\varphi(r) < \varphi(b)$.*
L'application φ est alors appelée un algorithme d'Euclide. On définit, de manière analogue, un anneau euclidien à gauche en remplaçant bq par qb.

Les preuves des résultats suivants se trouvent dans [Sam71]. L'hypothèse de commutativité de A n'est jamais utilisée.

Proposition 2.1.2. *Soient A est un anneau euclidien à droite pour φ et $b \in A$. On a*

$$\varphi(b) = 0 \text{ si et seulement si } b = 0.$$

Proposition 2.1.3. *Soient A un anneau euclidien à droite pour φ et $b \in A$ tel que $\varphi(b) = \min\{\varphi(A) \setminus \{0\}\}$. Alors b est inversible dans A.*

Proposition 2.1.4. *Soit A un anneau euclidien à droite pour φ. Alors tout idéal à droite dans A est principal.*

Proposition 2.1.5. *Soit A un anneau euclidien à droite pour φ. Posons $\varphi_1(a) = \inf_{b \in aA \setminus \{0\}} \varphi(b)$. Alors A est euclidien pour φ_1 et*

a) $\varphi_1(ca) \geq \varphi_1(a)$ *pour* $ca \neq 0$,

b) $\varphi_1(ca) = \varphi_1(a)$ *si et seulement si* $caA = aA$,

c) $\varphi_1(a) \leq \varphi(a)$ *pour tout* $a \in A$.

Corollaire 2.1.6 (réciproque de la proposition 2.1.3). *Si φ_1 est comme dans la proposition ci-dessus, alors u est inversible dans A si et seulement si $\varphi_1(u)$ est le plus petit élément de $\varphi_1(A) \setminus \{0\}$.*

Proposition 2.1.7. *Soient I un ensemble d'indices et $(\varphi_\alpha)_{\alpha \in I}$ une famille d'algorithmes d'Euclide pour l'anneau euclidien à droite A. Alors $\varphi = \inf_{\alpha \in I} \varphi_\alpha$ est encore un algorithme d'Euclide pour A.*

Cette proposition montre l'existence d'un algorithme minimal pour un anneau euclidien.

Proposition 2.1.8. *Soit θ l'algorithme minimal pour un anneau euclidien à droite A. Pour tout $n \in \mathbb{N}$, on pose*

$$A_n = \{x \in A \mid \theta(x) \leq n\} \quad et \quad A'_n = \{x \in A \mid \theta(x) < n\}.$$

Alors A_n est la réunion de $\{0\}$ et des éléments $b \in A$ tels que l'application canonique $A'_n \longrightarrow A/bA$ est surjective.

PREUVE : Soient $b \in A_n$ non nul, $a \in A$ et $\bar{a} \in A/bA$. Comme A est euclidien pour θ, il existe $q, r \in A$ tels que $a = bq + r$ (c'est-à-dire $\bar{a} = \bar{r}$) et $\theta(r) < \theta(b) \leq n$; autrement dit $r \in A'_n$ et r est un représentant de la classe de a dans A/bA, ce qui signifie que $A'_n \longrightarrow A/bA$ est surjective pour tout $b \in A_n$ non nul.
Réciproquement, considérons $b \in A$ non nul tel que $A'_n \longrightarrow A/bA$ est surjective et supposons que $b \notin A_n$ (i.e. $\theta(b) > n$). Définissons l'application $\theta_b : A \longrightarrow \mathbb{N}$ de la façon suivante :

i) $\theta_b(b) = n$,

ii) $\theta_b(x) = \theta(x)$ pour tout $x \in A$ différent de b.

Nous allons voir que θ_b est un algorithme d'Euclide pour A plus petit que θ (ce qui est absurde). Soient $x, y \in A$ avec $y \neq 0$. Il existe $q, r \in A$ tels que $x = yq + r$ et $\theta(r) < \theta(y)$. Si, dans cette relation, $q \neq b$ et $r \neq b$ alors $\theta_b(r) = \theta(r) < \theta(q) = \theta_b(q)$. Si $q = b$, alors nous savons que la classe $\bar{x} \in A/bA$ admet un représentant $r \in A_n$, autrement dit $x = by + r$ avec $\theta_b(r) = \theta(r) < n = \theta_b(b)$. Finalement, si $r = b$, $\theta_b(r) = n < \theta(b) < \theta(y) = \theta_b(y)$. Nous avons donc prouvé que θ_b est un algorithme d'Euclide pour A. De plus il est clair que $\theta_b < \theta$, ce qui est absurde, donc $b \in A_n$.

□

Cette proposition nous amène à la définition suivante.

Définition 2.1.9. *Soit A un anneau. On définit une suite de sous-ensembles $(A_i)_{i\in\mathbb{N}}$ de A récursivement de la façon suivante :*

a) $A_0 = \{0\}$,

b) $A'_n = \bigcup_{i=0}^{n-1} A_i$,

c) $A_n = \{b \in A \mid A'_n \longrightarrow A/bA$ *est surjective* $\} \cup \{0\}$.

Proposition 2.1.10. *Un anneau A est euclidien à droite si et seulement si $\varinjlim A_n = A$ et, dans ce cas, l'algorithme θ défini par*

$$\theta(x) = n \iff x \in A_n \setminus A'_n$$

est l'algorithme minimal pour A.

PREUVE : Supposons que A est euclidien à droite d'algorithme minimal θ. Par la proposition précédente, nous savons que

$$\theta(x) = n \iff x \in A_n \setminus A'_n.$$

Ainsi, pour tout $x \in A$, il existe $n \in \mathbb{N}$ tel que $x \in A_n$, et donc $\varinjlim A_n = A$.

Réciproquement, supposons que $\varinjlim A_n = A$. Soient $a, b \in A$ avec $b \neq 0$.

Alors il existe (un unique) $n \in \mathbb{N}$ tel que $b \in A_n \setminus \bigcup_{i=0}^{n-1} A_i$. Par hypothèse, il existe $r \in A'_n = \bigcup_{i=0}^{n-1} A_i$ tel que $r + bA = a + bA$. Autrement dit, il existe $r \in A'_n$ et $q \in A$ tel que $a = bq + r$. Comme $r \in \bigcup_{i=0}^{n-1} A_i$ il est clair que $\theta(r) \leq n - 1 < n = \theta(b)$. Cela prouve que A est euclidien pour l'algorithme θ. La minimalité de θ découle de la proposition précédente.

□

Remarque : Si $A_i \subset A'_i$ (i.e. si $A_i \setminus A'_i = \emptyset$), alors $A_k = A_i$ pour tout $k \geq i$. Dans ce cas A est euclidien si et seulement si $A = A_i$.

On utilisera parfois le résultat plus simple suivant.

Corollaire 2.1.11. *Soit A un anneau euclidien à droite. Alors il existe $b \in A \setminus A^\times$ tel que l'application canonique $A^\times \cup \{0\} \longrightarrow A/bA$ est surjective.*

Preuve : Nous excluons le cas où A est un corps (gauche), car dans ce cas $b = 0$ fait l'affaire. Remarquons d'abord que $A_1 = A^\times \cup \{0\}$. En effet, $\{0\} \longrightarrow A/bA$ est surjective si et seulement si $b \in A^\times$. Nous avons donc $A'_2 = A^\times \cup \{0\}$, de sorte que, si un tel $b \in A$ n'existe pas, alors $A_2 = A_1 = A^\times \cup \{0\}$. Plus généralement $A_n = A_1$ pour tout $n \geq 1$. Comme A est euclidien, on doit avoir $A = \varinjlim A_n = A_1 = A^\times \cup \{0\}$ ce qui est impossible car A n'est pas un corps.

□

2.2 Minimum euclidien et minimum inhomogène

Dans cette section K est un corps de nombres de degré n, A une algèbre centrale à division m^2 sur K, Λ un ordre de A et I un idéal à droite de Λ. Nous noterons r_1 le nombre de plongements réels de K dans $\mathbb{C}$ et $2r_2$ le nombre de plongements complexes. La dimension de A sur $\mathbb{Q}$ sera notée r ($r = nm^2$). Les définitions et résultats de cette section s'inspirent de ceux obtenus dans le cas commutatif par Jean-Paul Cerri dans [Cer06].

Nous allons nous intéresser à l'euclidianité de Λ pour la norme réduite. En d'autres termes nous nous demandons si Λ est euclidien pour l'algorithme

$|\mathrm{nr}_{A/\mathbb{Q}}| : \Lambda \longrightarrow \mathbb{N}$. Pour cela il faut que $\mathrm{nr}_{A/\mathbb{Q}}(a) = 0$ si et seulement si $a = 0$, ce qui n'est possible que si A est une algèbre à division.

Nous allons définir les notions de minima euclidien et inhomogène de Λ, qui nous renseigne sur l'euclidianité de Λ. Lorsqu'il s'agit de ces minima l'algèbre est toujours supposée à division.

Définition 2.2.1. *Soient A une algèbre centrale à division sur un corps de nombres K, I un idéal à droite d'un ordre de A et $\xi \in A$. Le minimum euclidien de ξ par rapport à I (relativement à la norme réduite) est le nombre réel $m_I(\xi)$ donné par :*

$$m_I(\xi) = \inf\left\{|\mathrm{nr}_{A/\mathbb{Q}}(\xi - \gamma)| \mid \gamma \in I\right\}.$$

Notons les propriétés élémentaires suivantes de m_I :

Proposition 2.2.2. *Les propriétés suivantes sont vérifiées :*

i) Pour tout $u \in \Lambda^\times$, $\xi \in A$ et $\gamma \in I$, on a $m_I(\xi u - \gamma) = m_I(\xi)$.

ii) Pour tout $\xi \in A$, il existe $\gamma \in I$ tel que $m_I(\xi) = |\mathrm{nr}_{A/\mathbb{Q}}(\xi - \gamma)|$.

iii) Pour tout $\xi \in A$, $m_I(\xi) \in \mathbb{Q}$ et $m_I(\xi) = 0 \iff \xi \in I$.

Preuve : Montrons *i)*. Nous avons

$$m_I(\xi u - \gamma) = \inf\left\{|\mathrm{nr}_{A/\mathbb{Q}}(\xi u - \gamma - c) \mid c \in I\right\}.$$

comme $\gamma + I = I = Iu$, il vient

$$m_I(\xi u - \gamma) = \inf\left\{|\mathrm{nr}_{A/\mathbb{Q}}(\xi u - cu) \mid c \in I\right\} =$$

$$= \inf\left\{|\mathrm{nr}_{A/\mathbb{Q}}(\xi - c) \mid c \in I\right\} = m_I(\xi)$$

car $|\mathrm{nr}_{A/\mathbb{Q}}(u)| = 1$.

Montrons *ii)* et *iii)*. Soit $\xi \in A$. Il existe $\beta \in I$ et $d \in \mathbb{N}^*$ tels que $\xi = \frac{\beta}{d}$. Par conséquent,

$$m_I(\xi) = \frac{1}{d^{nm^2}} \inf\left\{|\mathrm{nr}_{A/\mathbb{Q}}(\beta - d\gamma)| \mid \gamma \in I\right\}$$

où $n = [K : \mathbb{Q}]$ est le degré du corps de nombres K et $m^2 = \dim_K(A)$, la dimension de A sur K. Comme $|\mathrm{nr}_{A/\mathbb{Q}}(\beta - d\gamma)| \in \mathbb{N}$, cette borne inférieure est atteinte par un $\gamma_0 \in I$ et

$$m_I(\xi) = \frac{1}{d^{nm^2}} |\mathrm{nr}_{A/\mathbb{Q}}(\beta - d\gamma_0)| \in \mathbb{Q}.$$

De plus $\mathrm{nr}_{A/\mathbb{Q}}(\beta - d\gamma_0) = 0$ si et seulement si $\beta = d\gamma_0$, c'est-à-dire $\xi = \gamma_0 \in I$.

□

Définition 2.2.3. *Soient A et I comme dans la définition 2.2.1. Le minimum euclidien (par rapport à la norme réduite) de I est le nombre réel* $\mathrm{M}(I)$ *donné par :*

$$\mathrm{M}(I) = \sup\{m_I(\xi) \mid \xi \in A\}.$$

En vue d'établir le lien entre le fait d'être euclidien et le minimum euclidien d'un ordre, énonçons le résultat suivant.

Lemme 2.2.4. *Les conditions suivantes sont équivalentes :*

i) L'ordre Λ est euclidien à droite.

ii) L'ordre Λ est euclidien à gauche.

iii) Pour tout $\xi \in A$, il existe $\gamma \in \Lambda$ tel que $|\mathrm{nr}_{A/\mathbb{Q}}(\xi - \gamma)| < 1$.

Preuve : Supposons que Λ est euclidien à droite. Alors pour tout $a, b \in \Lambda$ avec $b \neq 0$ il existe $c, r \in \Lambda$ tel que

$$a = bc + r \text{ et } 0 \leq |\mathrm{nr}_{A/\mathbb{Q}}(r)| < |\mathrm{nr}_{A/\mathbb{Q}}(b)|.$$

Soit $\xi = b^{-1}a$. Nous avons $|\mathrm{nr}_{A/\mathbb{Q}}(\xi - c)| = |\mathrm{nr}_{A/\mathbb{Q}}(b^{-1}r)| < 1$. La démarche est analogue si Λ est euclidien à gauche.

Réciproquement, si pour tout élément ξ de A il existe $c_\xi \in \Lambda$ tel que $|\mathrm{nr}_{A/\mathbb{Q}}(\xi - c_\xi)| < 1$, nous voulons démontrer que Λ est euclidien à droite et à gauche. Soient $a, b \in \Lambda$ avec $b \neq 0$; posons $\xi = ab^{-1}$, $\eta = b^{-1}a$, $r = (\xi - c_\xi)b$ et $s = b(\eta - c_\eta)$. Alors $a = c_\xi b + r = bc_\eta + s$ et $|\mathrm{nr}_{A/\mathbb{Q}}(r)| = |\mathrm{nr}_{A/\mathbb{Q}}(b)| \cdot |\mathrm{nr}_{A\mathbb{Q}}(\xi - c_\xi)| < |\mathrm{nr}_{A/\mathbb{Q}}(b)|$. Nous montrons de la même manière que $|\mathrm{nr}_{A/\mathbb{Q}}(s)| < |\mathrm{nr}_{A/\mathbb{Q}}(b)|$, ce qui prouve que Λ est euclidien à gauche et à droite.

□

On peut maintenant donner le lien classique entre le minimum euclidien et le fait d'être euclidien pour la norme réduite.

Proposition 2.2.5. *Soient Λ un ordre de A et I un idéal à droite de Λ. Les propriétés suivantes sont vérifiées :*

- *Si* $\mathrm{M}(\Lambda) < 1$ *alors* Λ *est euclidien (pour la norme réduite).*
- *Si* $\mathrm{M}(\Lambda) > 1$ *alors* Λ *n'est pas euclidien (pour la norme réduite).*
- *Si* $\mathrm{M}(\Lambda) = 1$ *alors il existe* $\xi \in A$ *avec* $\mathrm{M}(\Lambda) = m_\Lambda(\xi)$*, si et seulement si* Λ *n'est pas euclidien (pour la norme réduite).*
- $M(I) = \inf\left\{\lambda \in \mathbb{R} \mid \forall\ \xi \in A,\ \exists\ \gamma \in I \text{ tel que } |\mathrm{nr}_{A/\mathbb{Q}}(\xi - \gamma)| < \lambda\right\}$.

Preuve : Pour tout $\xi \in A$, il existe $\gamma \in \Lambda$ tel que

$$|\mathrm{nr}_{A/\mathbb{Q}}(\xi - \gamma)| = m_\Lambda(\xi) \leq \mathrm{M}(\Lambda)$$

ce qui prouve le premier point (voir le lemme précédent).

Pour tout $\epsilon > 0$, il existe $\xi \in A$ tel que

$$|\mathrm{nr}_{A/\mathbb{Q}}(\xi - \gamma)| + \epsilon \geq m_\Lambda(\xi) + \epsilon \geq \mathrm{M}(\Lambda)$$

pour tout $\gamma \in \Lambda$, ce qui prouve le second point (voir le lemme précédent).

Si $\mathrm{M}(\Lambda) = 1 = m_\Lambda(\xi)$, alors il existe $\gamma \in \Lambda$ tel que pour tout $\delta \in \Lambda$,

$$1 = m_\Lambda(\xi) = |\mathrm{nr}_{A/\mathbb{Q}}(\xi - \gamma)| \leq |\mathrm{nr}_{A/\mathbb{Q}}(\xi - \delta)|$$

où la seconde égalité provient de la proposition 2.2.2. Le lemme précédent nous assure alors que Λ n'est pas euclidien. Réciproquement, si Λ n'est pas euclidien, alors il existe $\xi \in A$ tel que, pour tout $\delta \in \Lambda$, nous avons $|\mathrm{nr}_{A/\mathbb{Q}}(\xi - \delta)| \geq 1$ et donc $m_\Lambda(\xi) = 1$.

Pour la dernière affirmation, notons

$$M_1 = \inf\left\{\lambda \in \mathbb{R} \mid \forall\ \xi \in A,\ \exists\ \gamma \in I \text{ tel que } |\mathrm{nr}_{A/\mathbb{Q}}(\xi - \gamma)| < \lambda\right\}.$$

Soit $k > M_1$. Alors, pour tout $\xi \in A$, il existe $\gamma \in I$ tel que $|\mathrm{nr}_{A/\mathbb{Q}}(\xi - \gamma)| < k$. Nous avons donc $m_I(\xi) < k$ pour tout $\xi \in A$, de sorte que $M(I) < k$. Ainsi, $M(I) \leq M_1$. Supposons maintenant que cette inégalité est stricte et posons $\epsilon = \frac{M(I) - M_1}{2} > 0$. Pour tout $\xi \in A$, il existe $\gamma \in I$ tel que

$$|\mathrm{nr}_{A/\mathbb{Q}}(\xi - \gamma)| \leq m_I(\xi) + \epsilon \leq M(I) + \epsilon = \frac{M_1 + M(I)}{2}.$$

Par définition de M_1, cela ne peut arriver que si $M_1 \leq \frac{M_1 + M(I)}{2}$, autrement dit si $\epsilon = \frac{M_1 - M(I)}{2} \leq 0$, ce qui est en contradiction avec l'hypothèse. Ainsi, l'inégalité stricte est impossible et donc $M(I) = M_1$.

□

Nous pouvons maintenant passer à la définition du minimum inhomogène.

Nous avons vu dans le chapitre précédent (voir proposition 1.6.8) que A se plonge (comme $\mathbb{Q}$-algèbre) dans un produit d'algèbre de matrices via l'application :

$$\begin{array}{rccc} c: & A & \longrightarrow & \mathrm{M}_m^{\mathbb{H}}(\mathbb{C})^w \times \mathrm{M}_m(\mathbb{R})^{r_1-w} \times \mathrm{M}_m(\mathbb{C})^{r_2} \\ & a & \longmapsto & (\Sigma_1(a), \ldots, \Sigma_{r_1+r_2}(a)) \end{array}$$

où m^2 est la dimension de A, w est le nombre de places réelles ramifiées dans A, r_1 le nombre de place réelles et $2r_2$ le nombre de places complexes de K. Les Σ sont définis dans la section 1.6.

Pour simplifier la suite, nous allons modifier légèrement ce plongement. On choisit dorénavant d'ordonner les places infinies de K de sorte que les w premières sont réelles et ramifiées dans A, les $r_1 - w$ suivantes sont réelles et non ramifiées dans A, les r_2 suivantes sont complexes et les r_2 dernières sont les conjuguées des précédentes (c'est-à-dire $\sigma_i = \overline{\sigma_{r_2+i}}$ pour tout $1 \leq i \leq r_2$). On note $\overline{\Sigma}$ le plongement de A dans $\mathrm{M}_m(\mathbb{C})$ correspondant à $\overline{\sigma}$.

Lemme 2.2.6. *Soient σ un plongement complexe de K et $\overline{\sigma}$ le plongement conjugué. Il existe $S_\sigma \in \mathrm{GL}_m(\mathbb{C})$ tel que*

$$\overline{\Sigma}(a) = S_\sigma^{-1}\overline{\Sigma(a)}S_\sigma$$

pour tout $a \in A$.

Preuve : Soient $A_\sigma = A \otimes_K K_\sigma$, φ_σ un isomorphisme entre A_σ et $\mathrm{M}_m(\mathbb{C})$ et

$$\begin{array}{rccc} \theta: & A_\sigma & \longrightarrow & A_{\overline{\sigma}} \\ & a \otimes v & \longmapsto & a \otimes \overline{v} \end{array}.$$

Alors $\varphi_{\overline{\sigma}} \circ \theta \circ \varphi_\sigma^{-1}$ est un $\mathbb{R}$-automorphisme de $\mathrm{M}_m(\mathbb{C})$ qui n'est pas $\mathbb{C}$-linéaire. C'est donc un automorphisme intérieur à conjugaison près. C'est ce que nous voulions.

□

Définition 2.2.7. *Soit*

$$\mathcal{M} = \mathrm{M}_m^{\mathbb{H}}(\mathbb{C})^w \times \mathrm{M}_m(\mathbb{R})^{r_1-w} \times \left\{ z \in \mathrm{M}_m(\mathbb{C})^{2r_2} \mid z_{r_2+i} = S_{\sigma_i}^{-1}\overline{z_i}S_{\sigma_i} \right\}$$

où S_σ est comme dans le lemme précédent. On note Φ le plongement de A dans $\mathcal{M}$ défini par

$$\Phi(a) = (\Sigma_1(a), \ldots, \Sigma_n(a))$$

pour tout $a \in A$, où $n = [K : \mathbb{Q}] = r_1 + 2r_2$ est le degré du corps de nombres K.

Avec cette définition, on a

$$\mathrm{nr}_{A/\mathbb{Q}}(a) = \prod_{i=1}^{n} \det(\Phi(a)_i)$$

pour tout $a \in A$. En effet, le corollaire 1.6.13 nous assure que

$$\mathrm{nr}_{A/\mathbb{Q}}(a) = \prod_{i=1}^{r_1} \det(\Sigma_i(a)) \cdot \prod_{i=r_1+1}^{r_2} \left(\det(\Sigma_i(a)) \cdot \overline{\det(\Sigma_i(a))}\right).$$

REMARQUE : L'algèbre $\mathcal{M}$ est en fait isomorphe à $A_{\mathbb{R}}$. En effet,

$$\left\{z \in \mathrm{M}_m(\mathbb{C})^{2r_2} \mid z_{r_2+i} = S_{\sigma_i}^{-1}\overline{z_i}S_{\sigma_i}\right\} \cong \mathrm{M}_m(\mathbb{C})^{r_2}.$$

Considérons maintenant Λ un ordre de A, I un idéal à droite de Λ et $\{e_1, \ldots, e_{nm^2}\}$ une $\mathbb{Z}$-base de I. On peut identifier A à $\mathbb{Q}^{nm^2}$ via l'isomorphisme d'espaces vectoriels suivant :

$$\begin{array}{rccc} \Psi : & \mathbb{Q}^{nm^2} & \longrightarrow & A \\ & x = (x_1, \ldots, x_{nm^2}) & \longmapsto & \sum_{i=1}^{nm^2} x_i e_i \end{array}$$

En tensorisant par $\mathbb{R}$ on peut prolonger l'homomorphisme $\Phi \circ \Psi$ en un isomorphisme continu (pour les topologies usuelles) de $\mathbb{R}$-espace vectoriel de $\mathbb{R}^{nm^2}$ dans $\mathcal{M}$:

$$\begin{array}{rccc} \overline{\Phi} : & \mathbb{R}^{nm^2} & \longrightarrow & \mathcal{M} \\ & x = (x_1, \ldots, x_{nm^2}) & \longmapsto & \left(\sum_{i=1}^{nm^2} x_i \Sigma_1(e_i), \ldots, \sum_{i=1}^{nm^2} x_i \Sigma_n(e_i)\right) \end{array}$$

L'application $\overline{\Phi}$ est bien un isomorphisme, car $\Psi \otimes \mathrm{id}$ et $\Phi \otimes \mathrm{id}$ sont des isomorphismes par exactitude de la tensorisation.

On peut encore étendre $\overline{\Phi}$ à $\mathbb{C}^{nm^2}$; on obtient alors un isomorphisme continu, $\overline{\Phi}'$, de $\mathbb{C}^{nm^2}$ dans $\mathrm{M}_m(\mathbb{C})^n$:

$$\begin{array}{rccc} \overline{\Phi}' : & \mathbb{C}^{nm^2} & \longrightarrow & \mathrm{M}_m(\mathbb{C})^n \\ & x + iy & \longmapsto & \overline{\Phi}(x) + i\overline{\Phi}(y) \end{array}$$

où $x, y \in \mathbb{R}^{nm^2}$ et $i = \sqrt{-1} \in \mathbb{C}$.

On a alors le diagramme commutatif suivant :

$$\begin{array}{ccccc} \mathbb{Q}^{nm^2} & \xhookrightarrow{i_1} & \mathbb{R}^{nm^2} & \xhookrightarrow{i_2} & \mathbb{C}^{nm^2} \\ \cong \downarrow \Psi & & \cong \downarrow \overline{\Phi} & & \cong \downarrow \overline{\Phi}' \\ A & \xhookrightarrow[\Phi]{} & \mathcal{M} & \xhookrightarrow[i_3]{} & \mathrm{M}_m(\mathbb{C})^n \end{array}$$

où i_1, i_2 et i_3 sont les inclusions canoniques.

On peut munir $\mathcal{M}$ d'une structure de $\mathbb{R}$-algèbre. Soit $a = (a_i)_{1\leq i\leq n}$, $b = (b_i)_{1\leq i\leq n} \in \mathcal{M}$. On pose $ab = (a_i b_i)_{1\leq i\leq n}$. Avec cette multiplication, Φ est un homomorphisme de $\mathbb{R}$-algèbres ; autrement dit on a :

$$\Phi(\xi_1\xi_2) = \Phi(\xi_1)\Phi(\xi_2)$$

pour tout $\xi_1, \xi_2 \in A$.

On peut prolonger la norme réduite $\mathrm{nr}_{A/\mathbb{Q}}$ en une application de $\mathbb{R}^{nm^2}$ dans $\mathbb{R}$ donnée par

$$\begin{array}{rccc} \mathcal{N}: & \mathbb{R}^{nm^2} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \prod_{i=1}^{n} \det(\sum_{j=1}^{nm^2} x_j \Sigma_i(e_j)) \end{array}.$$

L'identification de A avec $\mathbb{Q}^{nm^2}$ (via l'isomorphisme Ψ) nous suggère une définition d'un mimimum euclidien prolongé à $\mathbb{R}^{nm^2}$:

Définition 2.2.8. *Soient I un idéal à droite d'un ordre de A, $z \in \mathcal{M}$ et $t \in \mathbb{R}^{nm^2}$. Les minima inhomogènes de z et t par rapport à I sont définis respectivement par*

$$m_{I_{\mathbb{R}}}(z) = \inf\left\{ \left| \prod_{i=1}^{n} \det(z_i - Z_i) \right| \ \mid \ Z \in \Phi(I) \right\}$$

et

$$m(t) = \inf\left\{ |\mathcal{N}(t-s)| \ \mid \ s \in \mathbb{Z}^{nm^2} \right\}$$

Proposition 2.2.9. *On a les propriétés suivantes :*

i) $m_{I_{\mathbb{R}}} \circ \overline{\Phi} = m$.

ii) $m_{I_{\mathbb{R}}} \circ \Phi = m_I$.

Preuve : Soient $x = (x_1, \ldots, x_{nm^2}) \in \mathbb{R}^{nm^2}$ et $a \in A$. Calculons $m_{I_{\mathbb{R}}} \circ \overline{\Phi}(x)$.

$$\begin{aligned} m_{I_{\mathbb{R}}}(\overline{\Phi}(x)) &= m_{I_{\mathbb{R}}}\left(\sum_{i=1}^{nm^2} x_i \Sigma_1(e_i), \ldots, \sum_{i=1}^{nm^2} x_i \Sigma_n(e_i) \right) \\ &= \inf\left\{ \left| \prod_{i=1}^{n} \det\left(\sum_{j=1}^{nm^2} x_j \Sigma_i(e_j) - Z_i \right) \right| \ \mid \ Z \in \Phi(I) \right\} \end{aligned} \tag{II.1}$$

mais $\overline{\Phi} : \mathbb{Z}^{nm^2} \longrightarrow \Phi(I)$ est un isomorphisme. Nous pouvons donc reprendre l'équation II.1 en écrivant :

$$\begin{aligned} m_{I_{\mathbb{R}}}(\overline{\Phi}(x)) &= \inf\left\{ \left| \prod_{i=1}^{n} \det\left(\sum_{j=1}^{nm^2} x_j \Sigma_i(e_j) - Z_i \right) \right| \ \middle|\ Z \in \Phi(I) \right\} \\ &= \inf\left\{ \left| \prod_{i=1}^{n} \det\left(\sum_{j=1}^{nm^2} x_j \Sigma_i(e_j) - \sum_{j=1}^{nm^2} z_j \Sigma_i(e_j) \right) \right| \ \middle|\ z \in \mathbb{Z}^{nm^2} \right\} \\ &= \inf\left\{ |\mathcal{N}(x-z)| \ \middle|\ z \in \mathbb{Z}^{nm^2} \right\} \\ &= m(x). \end{aligned}$$

ce qui démontre *i)*. Nous procédons de la même manière pour démontrer *ii)* :

$$\begin{aligned} m_{I_{\mathbb{R}}}(\Phi(a)) &= m_{I_{\mathbb{R}}}\left(\Sigma_1(a), \ldots, \Sigma_n(a)\right) \\ &= \inf\left\{ \left| \prod_{i=1}^{n} \det\left(\Sigma_i(a) - Z_i\right) \right| \ \middle|\ Z \in \Phi(I) \right\} \\ &= \inf\left\{ \left| \prod_{i=1}^{n} \det\left(\Sigma_i(a) - \Sigma_i(z)\right) \right| \ \middle|\ z \in I \right\} \\ &= \inf\left\{ \left| \prod_{i=1}^{n} \det\left(\Phi(a-z)_i\right) \right| \ \middle|\ z \in I \right\} \\ &= \inf\left\{ \left| \mathrm{nr}_{A/\mathbb{Q}}(a-z) \right| \ \middle|\ z \in I \right\} \\ &= m_I(a) \end{aligned}$$

□

Nous allons voir, dans la proposition suivante, que le minimum inhomogène vérifie les mêmes propriétés que le minimum euclidien.

Proposition 2.2.10. *L'application m a les propriétés suivantes :*

i) Pour tout $x \in \mathbb{R}^{nm^2}$ et tout $X \in \mathbb{Z}^{nm^2}$, on a $m(x - X) = m(x)$.

ii) Pour tout $u \in \Lambda^{\times}$ et tout $x \in \mathbb{R}^{nm^2}$, on a

$$m(\overline{\Phi}^{-1}(\overline{\Phi}(x)\Phi(u))) = m(x).$$

iii) m est semi-continue supérieurement sur $\mathbb{R}^{nm^2}$.

PREUVE : Le premier point découle directement de la définition de m. Pour montrer le deuxième point, il suffit de calculer :

$$m(\overline{\Phi}^{-1}(\overline{\Phi}(x)\Phi(u))) = m_{I_{\mathbb{R}}}(\overline{\Phi}(x)\Phi(u)) =$$

$$= \inf\left\{ \left| \prod_{i=1}^{n} \det(\overline{\Phi}(x)_i \Phi(u)_i - Z_i \Phi(u)_i) \right| \mid Z \in \Phi(I) \right\}$$

car $\Phi(I)\Phi(u) = \Phi(I)$. Comme $1 = |\mathrm{nr}_{A/\mathbb{Q}}(u)| = \prod_{i=1}^{n} \det(\Phi(u)_i)$, il vient

$$m(\overline{\Phi}^{-1}(\overline{\Phi}(x)\Phi(u))) = \inf\left\{ \left| \prod_{i=1}^{n} \det(\overline{\Phi}(x)_i - Z_i) \right| \mid Z \in \Phi(I) \right\} =$$

$$= m_{I_{\mathbb{R}}}(\overline{\Phi}(x)) = m(x).$$

Pour prouver *iii)* nous nous appuyons sur la continuité de $\mathcal{N}$. Il faut montrer que pour tout $\epsilon > 0$ et tout $x \in \mathbb{R}^{nm^2}$, il existe un voisinage V_x de x, tel que pour tout $y \in V_x$

$$m(y) \leq m(x) + \epsilon$$

Par définition de m, il existe $X \in \mathbb{Z}^{nm^2}$ tel que

$$|\mathcal{N}(x - X)| \leq m(x) + \frac{\epsilon}{2}$$

et, par continuité de $\mathcal{N}$, il existe un voisinage V_x de x tel que pour tout $y \in V_x$

$$|\mathcal{N}(y - X)| \leq |\mathcal{N}(x - X)| + \frac{\epsilon}{2}.$$

Ainsi

$$m(y) \leq |\mathcal{N}(x - X)| + \frac{\epsilon}{2} \leq m(x) + \epsilon$$

□

La propriété *i)* de la proposition précédente nous permet de définir une application induite par m sur le tore $\mathbb{T}^{nm^2} = \mathbb{R}^{nm^2}/\mathbb{Z}^{nm^2}$.

Proposition 2.2.11. *L'application*

$$\begin{array}{rccc} \widetilde{m} : & \mathbb{T}^{nm^2} = \mathbb{R}^{nm^2}/\mathbb{Z}^{nm^2} & \longrightarrow & \mathbb{R} \\ & \overline{x} & \longmapsto & m(x) \end{array}$$

est bien définie et semi-continue supérieurement. De plus, $\widetilde{m}$ et m sont bornées supérieurement et atteignent leur maximum.

PREUVE : Le fait que $\widetilde{m}$ est bien définie et semi-continue supérieurement découle de la proposition précédente. L'application $\widetilde{m}$ est alors bornée et atteint son maximum, car le tore $\mathbb{T}^{nm^2}$ est compact. Nous en déduisons que m vérifie les mêmes propriétés.

□

On peut maintenant donner la définition du minimum inhomogène d'un idéal à droite (d'un ordre Λ) de A.

Définition 2.2.12. *On appelle minimum inhomogène de I, et on note $\mathrm{M}(I_{\mathbb{R}})$, le nombre réel*

$$\mathrm{M}(I_{\mathbb{R}}) = \sup\left\{m(x) \mid x \in \mathbb{R}^{nm^2}\right\} = \sup\left\{\widetilde{m}(\alpha) \mid \alpha \in \mathbb{T}^{nm^2}\right\}.$$

Donnons encore le résultat suivant qui lie le minimum euclidien et le minimum inhomogène d'un idéal I.

Proposition 2.2.13. *Soit I un idéal à droite d'un ordre Λ dans A. On a*

i) $\mathrm{M}(I) \leq \mathrm{M}(I_{\mathbb{R}})$.

ii) $M(I_{\mathbb{R}}) = \inf\{\lambda \in \mathbb{R} \mid \forall\ x \in A_{\mathbb{R}},\ \exists\ \gamma \in I$ *tel que* $|\mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(x-\gamma)| < \lambda\}$ *(l'idéal I est contenu dans $A_{\mathbb{R}}$ via $\delta^{-1} \circ c$, voir proposition 1.6.8).*

PREUVE : La première affirmation découle directement des définitions. Pour la seconde, remarquons que, si on identifie $\mathcal{M}$ et $A_{\mathbb{R}}$, nous pouvons écrire

$$\mathcal{N}(t) = \mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(\overline{\Phi}(t)).$$

Posons

$$M_1 = \inf\{\lambda \in \mathbb{R} \mid \forall\ x \in A_{\mathbb{R}},\ \exists\ \gamma \in I \text{ tel que } |\mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(x-\gamma)| < \lambda\}.$$

Soit $k > M_1$. Alors pour tout $\xi \in A$, il existe $\gamma \in I$ tel que

$$|\mathcal{N}(\overline{\Phi}^{-1}(\xi-\gamma))| = |\mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(\xi-\gamma)| < k$$

de sorte que $m(\overline{\Phi}^{-1}(\xi)) < k$ et, comme $\overline{\Phi}$ est un isomorphisme,

$$M(I_{\mathbb{R}}) = \sup\left\{m(x) \mid x \in \mathbb{R}^{nm^2}\right\} = \sup\left\{m(\overline{\Phi}^{-1}(x)) \mid x \in \mathcal{M} \cong A_{\mathbb{R}}\right\} < k.$$

Ainsi $M(I_{\mathbb{R}}) \leq M_1$. En procèdant comme dans la preuve du dernier point de la proposition 2.2.5 nous voyons que $M(I_{\mathbb{R}}) < M_1$ est impossible.

□

2.3 Rationalité du minimum euclidien et du minimum inhomogène

Dans cette section nous nous inspirons des résultats de Jean-Paul Cerri dans [Cer06] pour montrer que le minimum euclidien et le minimum inhomogène d'un idéal I sont rationnels, sous certaines conditions. Comme dans la section précédente, A est une algèbre à division centrale (de dimension m^2) sur un corps de nombres K de degré n, Λ est un ordre de A et I un idéal à droite de Λ.

Considérons

$$\mathcal{B} = \left\{v_{11}^1, v_{12}^1, \dots, v_{1m}^1, v_{21}^1, \dots, v_{mm}^1, \dots, v_{11}^n, \dots, v_{mm}^n\right\}$$

la base canonique de $\mathrm{M}_m(\mathbb{C})^n$. C'est-à-dire, pour tout $1 \leq i \leq n$, v_{kl}^i est la matrice composée de zéros avec un unique 1 en position (k,l) (et $1 \leq k,l \leq m$).

On note

$$w_{kl}^i = \overline{\Phi}'^{-1}(v_{kl}^i) \in \mathbb{C}^{nm^2}$$

l'image réciproque des éléments de la base $\mathcal{B}$, et $\mathcal{B}' = \{w_{kl}^i \mid 1 \leq i \leq n, 1 \leq k,l \leq m\}$ la base de $\mathbb{C}^{nm^2}$ formée des images réciproques des v_{kl}^i.

Soit $u \in \Lambda^\times$. On définit

$$\begin{array}{rccc} f_u : & \mathbb{R}^{nm^2} & \longrightarrow & \mathbb{R}^{nm^2} \\ & x & \longmapsto & \overline{\Phi}^{-1}(\overline{\Phi}(x)\Phi(u)). \end{array}$$

C'est un automorphisme continu de $\mathbb{R}^{nm^2}$.

Remarquons que la proposition 2.2.10 nous assure que le minimum inhomogène m est invariant par l'action de f_u, c'est-à-dire que

$$m \circ f_u = m \qquad \text{pour tout } u \in \Lambda^\times.$$

La matrice de f_u par rapport à la base canonique est à coefficients entiers, de sorte que, pour tout $x \in \mathbb{R}^{nm^2}$ et tout $X \in \mathbb{Z}^{nm^2}$, on a

$$f_u(x+X) \equiv f_u(x) \mod \mathbb{Z}^{nm^2}.$$

On peut alors définir un automorphisme continu de $\mathbb{T}^{nm^2}$ induit par f_u :

$$\begin{array}{rccc} g_u : & \mathbb{T}^{nm^2} & \longrightarrow & \mathbb{T}^{nm^2} \\ & \overline{x} & \longmapsto & \overline{f_u(x)} \end{array}.$$

Le comportement de g_u vis-à-vis de $\widetilde{m}$ est le même que celui de f_u vis-à-vis de m, c'est-à-dire :

$$\widetilde{m} \circ g_u = \widetilde{m}.$$

On pose

$$\mathcal{T} = \left\{ g_u \mid u \in \Lambda^\times \right\}.$$

Comme $g_u \circ g_v = g_{uv}$, $\mathcal{T}$ est un sous groupe de $\mathrm{Aut}(\mathbb{T}^{nm^2})$ (isomorphe à $\Lambda^\times$).

Nous allons maintenant nous intéresser au sous-groupe suivant de $\mathcal{T}$:

$$\mathcal{S}_\mathcal{U} = \{ g_u \in \mathcal{T} \mid u \in \mathcal{U} \}$$

où $\mathcal{U} = \{ u \in \Lambda^\times \mid \Sigma(u) \text{ est une matrice diagonale pour tout plongement } \Sigma \}$, et particulièrement aux vecteurs propres communs à tous les automorphismes de $\mathcal{S}_\mathcal{U}$. Plus généralement, si G est un sous-groupe de $\mathcal{U}$, on pose

$$\mathcal{S}_G = \{ g_u \in \mathcal{T} \mid u \in G \}$$

et on définit

$$evec\mathcal{S}_G = \left\{ x \in \mathbb{T}^{nm^2} \mid x \text{ est un vecteur propre de } g_u \text{ pour tout } u \in G \right\}$$

et, si $x \in evec\mathcal{S}_G$,

$$spec_x\mathcal{S}_G = \left\{ \lambda_x \in \mathbb{C}^{nm^2} \mid \lambda_x \text{ est valeur propre de } g_x \right\}.$$

Notons encore que $\mathcal{S}_\mathcal{U}$ est non vide, car $\mathcal{O}_K^\times \subset \mathcal{U}$.

Proposition 2.3.1. *Soit $\mathcal{B}' = \{ w_{kl}^i \mid 1 \leq i \leq n, 1 \leq k, l \leq m \}$ la base de $\mathbb{C}^{nm^2}$ définie plus haut. Alors*

$$\overline{\mathcal{B}'} = \{ \overline{w_{kl}^i} \mid 1 \leq i \leq n, 1 \leq k, l \leq m \} \subset evec\mathcal{S}_G$$

pour tout sous-groupe G de $\mathcal{U}$.

Preuve : Notons encore f_u l'automorphisme $\mathbb{C}$-linéaire de $\mathbb{C}^{nm^2}$ dont la restriction à $\mathbb{R}^{nm^2}$ est f_u (défini ci-dessus). Nous avons

$$f_u(z) = \overline{\Phi}'^{-1}(\overline{\Phi}'(z)\Phi(u)) \qquad \text{pour tout } z \in \mathbb{C}^{nm^2}.$$

Soit $u \in G$. Calculons $f_u(w_{kl}^i)$:

$$f_u(w_{kl}^i) = \overline{\Phi}'^{-1}(\overline{\Phi}'(w_{kl}^i)\Phi(u)) = \overline{\Phi}'^{-1}(v_{kl}^i\Phi(u)) = (\Sigma_i(u))_{ll} w_{kl}^i$$

de sorte que w_{kl}^i est un vecteur propre de f_u correspondant à la valeur propre $(\Sigma_i(u))_{ll}$. Par définition de g_u, $\overline{w_{kl}^i}$ est également un vecteur propre de g_u. □

Proposition 2.3.2. *Soit $x \in evec\mathcal{S}$. Il existe $1 \leq i \leq n$ et $1 \leq l \leq m$ tels que*

$$spec_x\mathcal{S}_G = \{(\Sigma_i(u))_{ll} \mid u \in G\}$$

pour tout sous-groupe G de

$$\mathcal{U} = \left\{u \in \Lambda^\times \mid \Sigma(u) \text{ est une matrice diagonale pour tout plongement } \Sigma\right\}.$$

PREUVE : Soit $x \in evec\mathcal{S}_G$, un vecteur propre commun à tous les éléments de $\mathcal{S}_G$. Comme $\mathcal{B}'$ est une base de $\mathbb{C}^{nm^2}$, nous pouvons écrire

$$x = \sum_{1\leq i\leq n, 1\leq k,l\leq m} x^i_{kl} w^i_{kl}.$$

Par définition, pour tout $u \in G$, il existe $\lambda_u \in \mathbb{C}^{nm^2}$ avec

$$f_u(x) = \sum_{1\leq i\leq n, 1\leq k,l\leq m} x^i_{kl} f_u(w^i_{kl}) = \sum_{1\leq i\leq n, 1\leq k,l\leq m} x^i_{kl}(\Sigma(u)_i)_{ll} w^i_{kl}$$

$$= \lambda_u \sum_{1\leq i\leq n, 1\leq k,l\leq m} x^i_{kl} w^i_{kl}.$$

Comme $x \neq 0$, il existe des indices i_0, k_0, l_0 tels que $x^{i_0}_{k_0 l_0} \neq 0$, et comme $\mathcal{B}'$ est une base de $\mathbb{C}^{nm^2}$, nous obtenons

$$x^{i_0}_{k_0 l_0}(\Sigma(u)_{i_0})_{l_0 l_0} = \lambda_u x^{i_0}_{k_0 l_0}$$

et donc

$$\lambda_u = (\Sigma_{i_0}(u))_{l_0 l_0}$$

d'où le résultat cherché.

□

Théorème 2.3.3. *Soit A une algèbre centrale à division (de dimension m^2) sur un corps de nombres K de degré $n = r_1 + 2r_2$. Soient Λ un ordre de A et I un idéal à droite de Λ. Supposons que $r_1 + r_2 \geq 3$, alors il existe $\xi \in A$ tel que*

$$\mathrm{M}(I_{\mathbb{R}}) = \mathrm{M}(I) = m_{I_{\mathbb{R}}}(\Phi(\xi)) = m_I(\xi).$$

En particulier

$$\mathrm{M}(I_{\mathbb{R}}) \text{ est un nombre rationnel.}$$

PREUVE : Posons $G = \mathcal{O}_K^\times$.
Remarquons que $\mathcal{S}_G$ est un groupe abélien d'automorphismes de $\mathbb{T}^{nm^2}$. Nous allons montrer que $\mathcal{S}_G$ possède les deux propriétés suivantes :

1. Pour tout vecteur propre $x \in evec\mathcal{S}_G$, il existe $\lambda \in spec_x\mathcal{S}_G$ tel que $|\lambda| \neq 1$. Alors $\mathcal{S}_G$ est dit *hyperbolique*.
2. Pour tout vecteur propre $x \in evec\mathcal{S}_G$, il existe $\lambda_1, \lambda_2 \in spec_x\mathcal{S}_G$ tels que $\lambda_1^s\lambda_2^t = 1 \Rightarrow s = t = 0$, autrement dit, λ_1 et λ_2 sont rationnellement indépendantes. Alors $\mathcal{S}_G$ est dit *multi-paramétré*.

Montrons d'abord 1.
Si $\mathcal{S}_G$ n'est pas hyperbolique, alors il existe $1 \leq i \leq n$ et $1 \leq l \leq m$ tels que $|(\Sigma_i(v))_{ll}| = 1$ pour tout $v \in G$. Pour $\epsilon \in \mathcal{O}_K^\times$, nous avons

$$|(\Sigma_i(\epsilon))_{ll}| = |\sigma_i(\epsilon)|$$

pour tout $1 \leq l \leq m$. Si $i > r_1 + r_2$, alors $|\sigma_{i-r_2}(y)| = |\sigma_i(y)|$ pour tout $y \in K$. Nous pouvons donc supposer que $i \leq r_1 + r_2$ et que

$$|\sigma_i(\epsilon)| = 1 \qquad \text{pour tout } \epsilon \in \mathcal{O}_K^\times. \tag{II.2}$$

Considérons le plongement suivant de K^* dans $\mathbb{R}^{r_1+r_2}$:

$$\begin{array}{rccl} \mathcal{L}: & K^* & \longrightarrow & \mathbb{R}^{r_1+r_2} \\ & y & \longmapsto & (\ln|\sigma_1(y)|, \ldots, \ln|\sigma_{r_1+r_2}(y)|) \end{array}$$

Rappelons que, par le théorème du rang des unités de Dirichlet, $\mathcal{L}(\mathcal{O}_K^\times)$ est un réseau de l'hyperplan d'équation $\sum_{j=1}^{r_1} y_j + 2\sum_{j=r_1+1}^{r_1+r_2} y_j = 0$. Par II.2, nous avons également que $\mathcal{L}(\mathcal{O}_K^\times)$ est contenu dans l'hyperplan d'équation $y_i = 0$. Comme $r_1 + r_2 \geq 2$, ces deux hyperplans sont distincts, de sorte que $\mathcal{L}(\mathcal{O}_K^\times)$ est contenu dans l'intersection des deux hyperplans, qui est de dimension r_1+r_2-2. Ceci est en contradiction avec le théorème de Dirichlet, donc $\mathcal{S}_G$ est hyperbolique.

Montrons maintenant la propriété 2.
Il existe deux éléments de G rationnellement indépendants (car le rang des unités de K est $r_1 + r_2 - 1 \geq 2$). Soient donc $\epsilon_1, \epsilon_2 \in G$ rationnellement indépendants. Pour tout $x \in evec\mathcal{S}_G$, il existe $1 \leq i \leq n$ tel que

$$\sigma_i(\epsilon_1), \sigma_i(\epsilon_2) \in spec_x\mathcal{S}_G.$$

Soient $k, l \in \mathbb{Z}$ tels que

$$\sigma_i(\epsilon_1)^k = \sigma_i(\epsilon_2)^l.$$

Par injectivité de σ_i, $\epsilon_1^k\epsilon_2^{-l} = 1$ et donc $k = l = 0$, ce qui prouve que $\mathcal{S}_G$ est multi-paramétré.

Posons maintenant

$$S = \left\{\alpha \in \mathbb{T}^{nm^2} \mid \widetilde{m}(\alpha) = \mathrm{M}(I_{\mathbb{R}})\right\}.$$

Comme $\widetilde{m}$ atteint son maximum (voir proposition 2.2.11), S est non vide. Par semi-continuité supérieure de $\widetilde{m}$, si $(\alpha_k)_{k\in\mathbb{N}}$ est une suite de S convergeant vers β, alors

$$\mathrm{M}(I_{\mathbb{R}}) = \lim_{k\to\infty} \sup \widetilde{m}(\alpha_k) \leq \widetilde{m}(\beta)$$

et donc $\beta \in S$. Cela prouve que S est une partie fermée de $\mathbb{T}^{nm^2}$. Remarquons encore que, pour tout $g_\epsilon \in \mathcal{S}_G$ et tout $\overline{x} \in S$,

$$\widetilde{m}(g_\epsilon(\overline{x})) = \widetilde{m}(\overline{f_\epsilon(x)}) = m(f_\epsilon(x)) = m(x) = \widetilde{m}(\overline{x}).$$

Alors S est dit $\mathcal{S}_G$-invariant. Soit $S' \subset S$ un ensemble $\mathcal{S}_G$-minimal (c'est-à-dire qui ne contient pas de sous-ensemble fermé, propre, non vide et $\mathcal{S}_G$-invariant). Grâce au caractère hyperbolique et multi-paramétré de $\mathcal{S}_G$, nous savons que les éléments de S' sont de torsion (voir [Ber84] et [Ber83]). Soit $\overline{x} \in S'$. Il existe $k \in \mathbb{Z}$ tel que $k\overline{x} = 0 \in \mathbb{T}^{nm^2} = \mathbb{R}^{nm^2}/\mathbb{Z}^{nm^2}$, autrement dit il existe un représentant x de $\overline{x}$ avec $x \in \mathbb{Q}^{nm^2}$. Posons $\xi = \Psi(x) \in A$. Alors il vient

$$\mathrm{M}(I_{\mathbb{R}}) = \widetilde{m}(\overline{x}) = m(x) = m_{I_{\mathbb{R}}}(\overline{\Phi}(x)) = m_{I_{\mathbb{R}}}(\Phi(\Psi(x)) = m_I(\xi)$$

et, comme $\mathrm{M}(I) \geq m_I(\xi) = \mathrm{M}(I_{\mathbb{R}}) \geq \mathrm{M}(I)$, nous obtenons

$$\mathrm{M}(I_{\mathbb{R}}) = \mathrm{M}(I) = m_{I_{\mathbb{R}}}(\Phi(\xi)) = m_I(\xi)$$

comme annoncé.

□

Corollaire 2.3.4. *Avec les hypothèses du théorème précédent, si Λ est un ordre de A et que $\mathrm{M}(\Lambda) = 1$, alors Λ n'est pas euclidien pour la norme réduite.*

Preuve : C'est une conséquence directe du théorème précédent et de la proposition 2.2.5.

□

Il faut remarquer que le théorème 2.3.3 s'appuie uniquement sur le fait que G est un sous-groupe abélien de

$$\mathcal{U} = \left\{ u \in \Lambda^\times \mid \Sigma(u) \text{ est une matrice diagonale pour tout plongement } \Sigma \right\}$$

et que $\mathcal{S}_G$ est hyperbolique et multi-paramétré. Nous pouvons donc énoncer le théorème suivant.

Théorème 2.3.5. *Soient A une algèbre centrale à division sur un corps de nombres K, I un idéal à droite d'un ordre Λ de A et G un sous-groupe de*

$$\mathcal{U} = \left\{ u \in \Lambda^\times \mid \Sigma(u) \text{ est une matrice diagonale pour tout plongement } \Sigma \right\}.$$

Si le groupe G est abélien et si l'ensemble de fonctions $\mathcal{S}_G$ (voir ci-dessus) est hyperbolique et multi-paramétré, alors il existe $\xi \in A$ tel que

$$\mathrm{M}(I_{\mathbb{R}}) = \mathrm{M}(I) = m_{I_{\mathbb{R}}}(\Phi(\xi)) = m_I(\xi).$$

En particulier $\mathrm{M}(I_{\mathbb{R}})$ est un nombre rationnel.

Ce théorème nous permet, dans certains cas, de nous passer de certaines hypothèses du théorème 2.3.3. Nous allons donner un exemple où l'hypothèse $r_1 + r_2 \geq 3$ du théorème 2.3.3 n'est pas vérifiée pour lequel le minimum euclidien est quand même rationnel. Nous renvoyons le lecteur aux chapitre III pour la définition du corps de quaternions $A = (a, b)_K$ apparaissant dans le corollaire suivant.

Corollaire 2.3.6. *Soient K un corps quadratique réel, $a, b \in K^\times$ tels que a est totalement positif et $A = (a, b)_K$ un corps de quaternions sur K. Soient encore Λ un ordre de A et I un idéal à droite de Λ. Alors, il existe $\xi \in A$ tel que*

$$\mathrm{M}(I_{\mathbb{R}}) = \mathrm{M}(I) = m_{I_{\mathbb{R}}}(\Phi(\xi)) = m_I(\xi).$$

En particulier $\mathrm{M}(I_{\mathbb{R}})$ est un nombre rationnel.

Preuve : Par le théorème précédent, il suffit de trouver un sous-groupe abélien G de $\mathcal{U}$ tel que $\mathcal{S}_G$ est hyperbolique et multi-paramétré.

Soit $L = \mathbb{Q}(\sqrt{a})$. Le corps L est totalement réel et de degré supérieur ou égal à 2 (car si a est un carré dans K alors A n'est pas un corps). Par le théorème des unités de Dirichlet, il existe une unité

$$\omega = u + v\sqrt{a} \in \mathcal{O}_L^\times - \mathcal{O}_K^\times$$

qui est d'ordre infini dans $\mathcal{O}_L^\times$. Posons

$$G = \langle \mathcal{O}_K^\times, u + vi \rangle$$

où $i \in A$ vérifie $i^2 = a$, le groupe engendré par $u + iv$ et les unités de K. Le groupe G est évidement abélien et $\mathcal{S}_G$ est hyperbolique, car $\mathcal{O}_K^\times$ l'est et $\mathcal{O}_K^\times \subset G$ (voir la preuve du théorème 2.3.3). Il reste à voir que G est bien un sous-groupe de $\mathcal{U}$ et que $\mathcal{S}_G$ est multi-paramétré.

Soient σ_1 et σ_2 les deux plongements de K dans $\mathbb{R}$. Il existe deux plongements Σ_1 et Σ_2 de A dans $\mathrm{M}_2(\mathbb{R})$ donnés par :

$$\Sigma_i : A \longrightarrow \mathrm{M}_2(\mathbb{R})$$

où

$$\Sigma_i(x_0 + ix_1 + jx_2 + kx_3) =$$
$$\begin{pmatrix} \sigma_i(x_0) + \sigma_i(x_1)\sqrt{\sigma_i(a)} & X \\ Y & \sigma_i(x_0) - \sigma_i(x_1)\sqrt{\sigma_i(a)} \end{pmatrix}$$

avec

$$X = \sigma_i(x_2)\sqrt{|\sigma_i(b)|} + \sigma_i(x_3)\sqrt{\sigma_i(a)|\sigma_i(b)|}$$

et

$$Y = \mathrm{sign}(\sigma_i(b)) \left(\sigma_i(x_2)\sqrt{|\sigma_i(b)|} - \sigma_i(x_3)\sqrt{\sigma_i(a)|\sigma_i(b)|}\right).$$

Ainsi $\Sigma_i(u + iv)$ est bien une matrice diagonale et $u + iv$ est bien une unité de A car $(u + iv)(u - iv) = \pm 1$, donc G est un sous-groupe de $\mathcal{U}$.

Montrons que $\mathcal{S}_G$ est multi-paramétré.

Soient $\epsilon_1 \in \mathcal{O}_K^\times \setminus \{1, -1\}$ et $\epsilon_2 = u + iv$. Pour tout $x \in evec\mathcal{S}_G$. Il existe $1 \leq i \leq 2$ et $1 \leq l \leq 2$ tels que $\Sigma_i(\epsilon_1)_{ll}, \Sigma_i(\epsilon_2)_{ll} \in spec_x\mathcal{S}_G$. L'application

$$\begin{array}{rccc} \Sigma_{il} : & \mathcal{U} & \longrightarrow & \mathbb{R} \\ & x & \longmapsto & \Sigma_i(x)_{ll} \end{array}$$

est injective (car $\sqrt{a} \notin L$). Il suffit donc de montrer que ϵ_1 et ϵ_2 sont rationnellement indépendants pour montrer que $\mathcal{S}_G$ est multi-paramétré, ce qui est clair puisque $\epsilon_1^r \in K$ est $\epsilon_2^s \in A \setminus K$ quels que soient les entiers r, s.

□

Remarque : Soit A un corps de quaternions totalement indéfini sur un corps quadratique réel K. Alors il existe a et b, satisfaisant aux hypothèses du corollaire, tels que $A = (a, b)_K$. Le résultat du corollaire précédent est donc vrai pour tout corps de quaternions totalement indéfini sur un corps quadratique réel.

2.4 Propriétés du minimum euclidien

Dans cette section, A est une algèbre à division de dimension $r = m^2$ sur un corps de nombres K, Λ est un ordre de A et I un idéal à droite de Λ. On note $n = [K : \mathbb{Q}]$, le degré de K sur $\mathbb{Q}$; $\mathrm{M}(I)$ et $\mathrm{M}(I_{\mathbb{R}})$ désignent respectivement le minimum euclidien et le minimum inhomogène de I.

Proposition 2.4.1. *Soit Λ' un ordre non maximal de A. Alors*

$$\mathrm{M}(\Lambda') \geq 1$$

et Λ' n'est pas euclidien pour la norme réduite.

PREUVE : Soit Λ un ordre maximal de A contenant Λ'. Il existe $x \in \Lambda \setminus \Lambda'$, et pour tout $\gamma \in \Lambda'$,

$$|\mathrm{nr}_{A/\mathbb{Q}}(x-\gamma)| \in \mathbb{N}.$$

En particulier $|\mathrm{nr}_{A/\mathbb{Q}}(x-\gamma)| \geq 1$. Ainsi,

$$\mathrm{M}(\Lambda') = \sup\{m_{\Lambda'}(\xi) \mid \xi \in A\} \geq m_{\Lambda'}(x) \geq 1.$$

De plus si $\mathrm{M}(\Lambda') = 1$, alors les inégalités ci-dessus sont des égalités, donc

$$M(\Lambda') = m_{\Lambda'}(x).$$

La proposition 2.2.5 nous assure alors que Λ' n'est pas euclidien.

□

Proposition 2.4.2. *Soient $I \subset J$ deux idéaux de A. Alors*

$$\mathrm{M}(J) \leq \mathrm{M}(I).$$

PREUVE : Comme

$$m_J(\xi) = \inf\{|\mathrm{nr}_{A/\mathbb{Q}}(\xi-\gamma)| \mid \gamma \in J\} \leq \inf\{|\mathrm{nr}_{A/\mathbb{Q}}(\xi-\gamma)| \mid \gamma \in I\} = m_I(\xi)$$

nous obtenons

$$\mathrm{M}(J) = \sup\{m_J(\xi) \mid \xi \in A\} \leq \sup\{m_I(\xi) \mid \xi \in A\} = \mathrm{M}(I).$$

□

Proposition 2.4.3. *Soient Λ et Γ deux ordres conjugués de A. Alors*

$$\mathrm{M}(\Lambda) = \mathrm{M}(\Gamma).$$

PREUVE : Soit $x \in A^\times$ tel que $\Lambda = x^{-1}\Gamma x$. Pour tout $\xi \in A$,

$$m_\Lambda(\xi) = m_{x^{-1}\Gamma x}(\xi) = \inf\{|\mathrm{nr}_{A/\mathbb{Q}}(\xi - x^{-1}\gamma x)| \mid \gamma \in \Gamma\} =$$

$$= \inf\{|\mathrm{nr}_{A/\mathbb{Q}}(x\xi x^{-1} - \gamma)| \mid \gamma \in \Gamma\} = m_\Gamma(x\xi x^{-1})$$

et comme la conjuguaison par x est un automorphisme de A, il vient

$$\mathrm{M}(\Lambda) = \sup\{m_\Lambda(\xi) \mid \xi \in A\} = \sup\{m_\Gamma(x\xi x^{-1}) \mid \xi \in A\} =$$

$$= \sup\{m_\Gamma(\xi) \mid \xi \in A\} = \mathrm{M}(\Gamma).$$

□

Cette proposition nous permet, si le nombre de type est 1, de parler du minimum euclidien de l'algèbre A plutôt que de celui d'un ordre maximal de A :

Définition 2.4.4. *Soit A une algèbre centrale à division sur un corps de nombres K. Supposons que $t_A = 1$. Alors tous les ordres maximaux de A ont le même minimum euclidien. On définit donc le minimum euclidien de A comme le minimum euclidien de n'importe lequel de ces ordres maximaux. On le note $\mathrm{M}(A)$. De la même manière on note $m_A(\xi)$ à la place de $m_\Lambda(\xi)$, si Λ est un ordre maximal de A.*

Nous verrons dans le chapitre III que deux ordres maximaux non conjugués d'une même algèbre à division A n'ont pas nécessairement le même minimum euclidien (voir le corollaire 3.7.8). Nous pouvons donner un intervalle contenant le rapport des minima euclidiens de deux ordres maximaux en fonction des idéaux qui les lient.

Proposition 2.4.5. *Soient Λ et Γ deux ordres maximaux de A et $\mathcal{I}$ l'ensemble des idéaux à gauche de Λ et à droite de Γ. Posons*

$$s = \inf_{I\in\mathcal{I}} \left(\inf_{x\in I\setminus\{0\}, y\in I^{-1}\setminus\{0\}} \left\{ |\mathrm{nr}_{A/\mathbb{Q}}(xy)| \right\} \right).$$

Alors

$$\frac{1}{s} \leq \frac{\mathrm{M}(\Lambda)}{\mathrm{M}(\Gamma)} \leq s.$$

Preuve : Nous savons que $I^{-1}\Lambda I = \Gamma$ pour tout $I \in \mathcal{I}$ (voir le théorème 1.4.5). Pour tout $I \in \mathcal{I}$, tout $x \in I$, $y \in I^{-1}$ et tout $\xi \in A$,

$$\begin{aligned} m_\Gamma(\xi) = m_{I^{-1}\Lambda I}(\xi) &= \inf\left\{ |\mathrm{nr}_{A/\mathbb{Q}}(\xi - \gamma)| \mid \gamma \in I^{-1}\Lambda I \right\} \\ &\leq \inf\left\{ |\mathrm{nr}_{A/\mathbb{Q}}(\xi - y\lambda x)| \mid \lambda \in \Lambda \right\} \\ &= |\mathrm{nr}_{A/\mathbb{Q}}(xy)| \cdot m_\Lambda(y^{-1}\xi x^{-1}). \end{aligned}$$

Comme les multiplications à gauche par y et à droite par x sont bijectives sur A, il vient

$$\begin{aligned}\mathrm{M}(\Gamma) &= \sup\{m_\Gamma(\xi) \mid \xi \in A\} \\ &\leq |\mathrm{nr}_{A/\mathbb{Q}}(xy)| \sup\{m_\Lambda(\xi) \mid \xi \in A\} \\ &= |\mathrm{nr}_{A/\mathbb{Q}}(xy)| \cdot \mathrm{M}(\Lambda).\end{aligned}$$

En remplaçant I par I^{-1} dans ce qui précède, nous obtenons :

$$\mathrm{M}(\Lambda) \leq |\mathrm{nr}_{A/\mathbb{Q}}(xy)| \cdot \mathrm{M}(\Gamma).$$

Comme ces inégalités sont valables pour tout $I \in \mathcal{I}$ et tout $x \in I$, $y \in I^{-1}$, nous avons le résultat voulu.

□

Remarque : Le nombre s est toujours un nombre entier positif. En effet, si $x \in I$ et $y \in I^{-1}$ sont tels que $s = |\mathrm{nr}_{A/\mathbb{Q}}(xy)|$, alors $xy \in II^{-1} = \Lambda$ et $yx \in I^{-1}I = \Gamma$, donc $\mathrm{nr}_{A/\mathbb{Q}}(xy) = \mathrm{nr}_{A/\mathbb{Q}}(yx) \in \mathrm{nr}_{A/\mathbb{Q}}(\Lambda \cap \Gamma) \subset \mathbb{Z}$.

En pratique, la détermination de s n'est pas forcément aisée. Toutefois, on peut facilement calculer un $r \geq s$ de la manière suivante : si Λ et Γ sont donnés, on cherche un idéal entier I à gauche de Λ et à droite de Γ et on calcule $I \cap \mathbb{Z} = r\mathbb{Z}$. Comme $1 \in \Lambda \subset I^{-1}$, on obtient

$$\left|\frac{1}{r}\right|^{nm^2} = \frac{1}{|\mathrm{nr}_{A/\mathbb{Q}}(r)|} \leq \frac{\mathrm{M}(\Lambda)}{\mathrm{M}(\Gamma)} \leq |\mathrm{nr}_{A/\mathbb{Q}}(r)| = |r|^{nm^2}$$

où $n = [K : \mathbb{Q}]$ est le degré de K sur $\mathbb{Q}$ et m^2, la dimension de A sur le corps de nombres K.

2.5 Borne supérieure du minimum euclidien

Théorème 2.5.1. *Soient A une algèbre centrale à division de dimension $r = m^2$ sur un corps de nombres K de degré n et I un idéal à droite d'un ordre Λ de A. Alors*

$$\mathrm{M}(I_{\mathbb{R}}) \leq \left(\frac{\tau_{\min}(I)}{\gamma_{\min}(\Lambda)}\right)^{nm/2} \mathrm{nr}_{A/\mathbb{Q}}(I).$$

Preuve : Soit (I, α, τ) un réseau idéal de A, où τ est une involution positive sur $A_{\mathbb{R}}$ (voir la définition 2.6.8). Un tel réseau sur I existe toujours, voir le

corollaire 1.8.2. Pour tout $x \in A_{\mathbb{R}}$, posons $q_\alpha(x) = \mathrm{tr}_{A_{\mathbb{R}}/\mathbb{R}}(x\alpha x^\tau)$. Alors pour tout $x \in A_{\mathbb{R}}$,

$$\mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(x)^2 = \mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(\alpha)^{-1}\mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(x\alpha x^\tau).$$

Ainsi, par le théorème 1.7.10,

$$\mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(x)^2 \leq \mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(\alpha)^{-1}\left(\frac{\mathrm{tr}_{A_{\mathbb{R}}/\mathbb{R}}(x\alpha x^\tau)}{nm}\right)^{nm}.$$

Or la valeur de $\mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(\alpha)^{-1}$ nous est donnée par la proposition 1.8.12 et il vient

$$\mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(x)^2 \leq \frac{\mathrm{N}_{A/\mathbb{Q}}(I)^{2/m}\mathrm{d}(\Lambda/\mathbb{Z})^{1/m}}{\det(I,\alpha,\tau)^{1/m}}\left(\frac{q_\alpha(x)}{nm}\right)^{nm}.$$

En utilisant la valeur de $\gamma_{\min}(\Lambda)$ donnée dans la proposition 1.9.2, nous obtenons

$$\mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(x) \leq \frac{\mathrm{N}_{A/\mathbb{Q}}(I)^{1/m}}{\gamma_{\min}(\Lambda)^{nm/2}}\left(\frac{q_\alpha(x)}{\det(I,\alpha,\tau)^{1/rn}}\right)^{nm/2}.$$

Pour tout $x \in A_{\mathbb{R}}$, il existe $c = c_x \in I$ tel que $q_\alpha(x-c) \leq \max(I,\alpha,\tau)$. Ainsi, en reprenant la dernière inégalité, nous obtenons

$$\mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(x-c) \leq \frac{\mathrm{N}_{A/\mathbb{Q}}(I)^{1/m}}{\gamma_{\min}(\Lambda)^{nm/2}}\left(\frac{\max(I,\alpha,\tau)}{\det(I,\alpha,\tau)^{1/rn}}\right)^{nm/2}$$

c'est-à-dire

$$\mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(x-c) \leq \left(\frac{\tau(I,\alpha,\tau)}{\gamma_{\min}(\Lambda)}\right)^{nm/2}\mathrm{N}_{A/\mathbb{Q}}(I)^{1/m}$$

et cela pour tout réseau idéal (I,α,τ). Donc

$$\mathrm{nr}_{A_{\mathbb{R}}/\mathbb{R}}(x-c) \leq \left(\frac{\tau_{\min}(I)}{\gamma_{\min}(\Lambda)}\right)^{nm/2}\mathrm{N}_{A/\mathbb{Q}}(I)^{1/m} = \left(\frac{\tau_{\min}(I)}{\gamma_{\min}(\Lambda)}\right)^{nm/2}\mathrm{nr}_{A/\mathbb{Q}}(I)$$

où la dernière égalité découle du fait que A est une $\mathbb{Q}$-algèbre simple. Par définition du minimum euclidien, nous avons donc

$$\mathrm{M}(I_{\mathbb{R}}) \leq \left(\frac{\tau_{\min}(I)}{\gamma_{\min}(\Lambda)}\right)^{nm/2}\mathrm{nr}_{A/\mathbb{Q}}(I).$$

□

Malheureusement, le calcul de $\tau_{\min}(I)$ s'avère très difficile, c'est pourquoi nous utiliserons souvent un résultat plus faible pour borner le minimum euclidien dans les cas concrets. Ce résultat découle directement de la preuve du théorème précédent.

Corollaire 2.5.2. *Soient A une algèbre centrale à division de dimension $r = m^2$ sur un corps de nombres K de degré n, I un idéal à droite d'un ordre Λ de A et (I, α, τ) un réseau idéal. Alors*

$$\mathrm{M}(I_{\mathbb{R}}) \leq \left(\frac{\tau(I,\alpha,\tau)}{\gamma_{\min}(\Lambda)}\right)^{nm/2} \mathrm{nr}_{A/\mathbb{Q}}(I).$$

Corollaire 2.5.3. *Soient A une algèbre centrale à division de dimension finie sur un corps de nombres et Λ un ordre maximal de A alors, si $\gamma_{\min}(\Lambda) > \tau_{\min}(\Lambda)$, Λ est euclidien.*

Preuve : Il suffit d'appliquer le théorème 2.5.1 :

$$\mathrm{M}(\Lambda) \leq \mathrm{M}(\Lambda_{\mathbb{R}}) \leq \left(\frac{\tau_{\min}(\Lambda)}{\gamma_{\min}(\Lambda)}\right)^{nm} \cdot \mathrm{nr}_{A/\mathbb{Q}}(\Lambda) < 1.$$

Donc le minimum euclidien de Λ est strictement inférieur à 1, ce qui prouve que Λ est euclidien.

□

Dans le cas où $A = K$ est un corps de nombres et $\Lambda = \mathcal{O}_K$, on retrouve le théorème 5.1 énoncé dans "Upper bounds for Euclidean minima" par Eva Bayer-Fluckiger (voir [BF06]).

Les bornes que nous avons vues de $\tau_{\min}$ et $\gamma_{\min}$ (voir la proposition 1.9.2 et le corollaire 1.9.5) permettent de donner une borne générale de $\mathrm{M}(I_{\mathbb{R}})$.

Proposition 2.5.4. *Soit A une algèbre centrale à division de dimension $r = m^2$ sur un corps de nombres K de degré n, et I un idéal à droite d'un ordre Λ de A. Alors*

$$\mathrm{M}(I_{\mathbb{R}}) \leq \left(\frac{m}{2}\right)^{nm} \mathrm{d}(\Lambda/\mathbb{Z})^{1/m} \mathrm{nr}_{A/\mathbb{Q}}(I).$$

Preuve : D'une part, $\gamma_{\min}(\Lambda) = \frac{mn}{\mathrm{d}(\Lambda/\mathbb{Z})^{1/rn}}$ (c'est la proposition 1.9.2), d'autre part $\tau_{\min}(I) \leq \frac{nm^3}{4} \cdot \mathrm{d}(\Lambda/\mathbb{Z})^{1/rn}$ (c'est le corollaire 1.9.5). Nous avons également la borne principale de $M(I_{\mathbb{R}})$:

$$\mathrm{M}(I_{\mathbb{R}}) \leq \left(\frac{\tau_{\min}(I)}{\gamma_{\min}(\Lambda)}\right)^{nm/2} \mathrm{nr}_{A/\mathbb{Q}}(I)$$

(c'est le théorème 2.5.1). Le tout mis ensemble donne le résultat annoncé.

□

2.6 Les algèbres à involution

En complément à la section 1.6 du chapitre I, nous allons étudier les algèbres centrales simples sur un corps de nombres munies d'une involution. En particulier, si (A, τ) est une telle algèbre à involution, nous déterminerons sous quelles conditions A possède un réseau idéal avec $A_{\mathbb{R}}$ munie de l'involution induite par celle de A. Comme précédemment, A désigne une algèbre centrale simple de dimension m^2 sur un corps de nombres K.

Rappelons qu'une involution sur une algèbre est un anti-automorphisme d'anneaux d'ordre 2. Il y a deux types d'involution distincts sur une K-algèbre centrale simple :

I. Les involutions K-linéaires (c'est-à-dire celles qui fixent K point par point). Ce sont les involutions de type I.

II. Les involutions qui ne fixent pas le corps de base K point par point. Ce sont les involutions de type II.

Nous adopterons les notations suivantes.

Notation 2.6.1. *Le couple (A, τ) désigne une algèbre centrale simple munie d'une involution. Soit $x \in A$; on note x^τ l'image de x par l'involution τ.*

L'étude des involutions est un vaste sujet (voir en particulier [KMMT98]) que nous n'allons pas traiter ici dans les détails. Nous nous contenterons de rappeler les quelques résultats standards suivants :

Proposition 2.6.2. *Soit (A, τ) une algèbre centrale simple sur un corps de nombres K, alors*

i) Le corps de base K est invariant par l'involution (c'est-à-dire $K^\tau = K$)

ii) Si l'involution est de type II, alors $F = \{x \in K \mid x^\tau = x\}$ est un corps et $[K : F] = 2$. De plus, si $K = F(\sqrt{\theta})$, alors $\sqrt{\theta}^\tau = -\sqrt{\theta}$.

Preuve : Pour *i)*, il suffit de voir que $k^\tau x = (x^\tau k)^\tau = (kx^\tau)^\tau = xk^\tau$ pour tout $k \in K$ et tout $x \in A$, de sorte que K^τ est contenu dans le centre de A. Donc $K^\tau \subset K$ et $\tau|_K$ est un automorphisme de corps. Ainsi $K^\tau = K$.
Pour *ii)* il est facile de voir que F est un corps (différent de K, puisque τ est de type II) ; de plus pour tout $k \in K$ le polynôme $X^2 - (k + k^\tau)X + k^\tau k$ est à coefficients dans F et il annule k, ce qui prouve que $[K : F] = 2$. Posons maintenant $K = F(\sqrt{\theta})$. Nous avons $\theta = \theta^\tau = (\sqrt{\theta}^\tau)^2$ de sorte que $\sqrt{\theta}^\tau = \pm\sqrt{\theta}$. Le résultat découle du fait que K et F sont distincts.

□

Cette proposition nous permet d'introduire quelques notations utiles.

Comme d'habitude (voir section 1.6 du chapitre I), on notera $\sigma_1, \ldots, \sigma_w$ les w places réelles de K qui sont ramifiées dans A, $\sigma_{w+1}, \ldots, \sigma_{r_1}$ les $r_1 - w$ places réelles qui ne sont pas ramifiées dans A et $\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}$ les r_2 places complexes (à conjugaison près). On notera encore $W = \mathrm{Ram}_\infty(A)$ l'ensemble des places réelles qui sont ramifiées dans A, R l'ensemble des places réelles de K et C l'ensemble des places complexes (un représentant par paire de places conjuguées) de K.

Si A est munie d'une involution τ de type II, on note $F = \{x \in K \mid x^\tau = x\}$ et $K = F(\sqrt{\theta})$. Alors une place infinie $\sigma : F \longrightarrow \mathbb{C}$ s'étend en deux places infinies de $K \longrightarrow \mathbb{C}$. La proposition suivante donne le comportement de ces extensions et les notations que nous adopterons.

Proposition 2.6.3. *Soit (A, τ) une algèbre centrale simple sur un corps de nombres K. On suppose l'involution τ de type II et on note $K = F(\sqrt{\theta})$ (où $F = \{x \in K \mid x^\tau = x\}$). Soit $\sigma : F \longrightarrow \mathbb{C}$ une place infinie de F.*

i) Si σ est réelle et $\sigma(\theta) > 0$, alors

$$\begin{array}{rccc} \sigma_1 : & K & \longrightarrow & \mathbb{R} \\ & a + b\sqrt{\theta} & \longmapsto & \sigma(a) + \sigma(b)\sqrt{\sigma(\theta)} \end{array}$$

et

$$\begin{array}{rccc} \sigma_2 : & K & \longrightarrow & \mathbb{R} \\ & a + b\sqrt{\theta} & \longmapsto & \sigma(a) - \sigma(b)\sqrt{\sigma(\theta)} \end{array}$$

sont des places réelles de K qui étendent σ. De plus, $\sigma_1(x^\tau) = \sigma_2(x)$ et $\sigma_2(x^\tau) = \sigma_1(x)$ pour tout $x \in K$, et $\sigma_1 \in \mathrm{Ram}_\infty(A)$ si et seulement si $\sigma_2 \in \mathrm{Ram}_\infty(A)$.

ii) Si σ n'est pas réelle, alors

$$\begin{array}{rccc} \sigma_1 : & K & \longrightarrow & \mathbb{C} \\ & a + b\sqrt{\theta} & \longmapsto & \sigma(a) + \sigma(b)\sqrt{\sigma(\theta)} \end{array}$$

et

$$\begin{array}{rccc} \sigma_2 : & K & \longrightarrow & \mathbb{C} \\ & a + b\sqrt{\theta} & \longmapsto & \sigma(a) - \sigma(b)\sqrt{\sigma(\theta)} \end{array}$$

sont des places complexes de K qui étendent σ. De plus $\sigma_1(x^\tau) = \sigma_2(x)$ et $\sigma_2(x^\tau) = \sigma_1(x)$ pour tout $x \in K$.

iii) Si σ est réelle et $\sigma(\theta) < 0$, alors

$$\begin{array}{rccc} \sigma_1 : & K & \longrightarrow & \mathbb{C} \\ & a + b\sqrt{\theta} & \longmapsto & \sigma(a) + i\sigma(b)\sqrt{|\sigma(\theta)|} \end{array}$$

est, à conjuguaison près, l'unique place infinie de K qui étend σ. De plus $\sigma_1(x^\tau) = \overline{\sigma_1(x)}$ pour tout $x \in K$ (où $^-$ désigne l'involution canonique sur $\mathbb{C}$).

iv) Toutes les places infinies de K sont décrites dans i), ii) et iii).

PREUVE : Nous vérifions facilement que tous les prolongements proposés ont bien les propriétés requises pour être des places de K. Le fait que $\sigma_1(x^\tau) = \sigma_2(x)$ (et vice versa) dans i) et ii) découle directement des définitions, de même que l'affirmation $\sigma_1(x^\tau) = \overline{\sigma_1(x)}$. Pour se convaincre du point iv), il suffit de compter les places de K obtenues dans la proposition. La seule assertion qui n'est pas claire est "$\sigma_1 \in \mathrm{Ram}_\infty(A)$ si et seulement si $\sigma_2 \in \mathrm{Ram}_\infty(A)$" dans le point i). Pour montrer cette affirmation, fixons une K-base $\mathcal{B} = \{e_1, \ldots, e_r\}$ de A. Il suffit alors de vérifier que l'application définie par

$$\begin{array}{rccc} \varphi : & A \otimes_K K_{\sigma_1} & \longrightarrow & A \otimes_K K_{\sigma_2} \\ & k e_i \otimes r & \longmapsto & k^\tau e_i \otimes r \end{array}$$

prolongée par linéarité définit un isomorphisme de $\mathbb{R}$-algèbres.

□

Notation 2.6.4. *Dans la situation de la proposition précédente, on numérotera les places de K de façon qu'elles se trouvent par paire de places qui prolongent une même place de F. En d'autre termes les w premières places $\sigma_1, \ldots, \sigma_w$ de K sont ordonnées de sorte que $\sigma_{2i-1}|_F = \sigma_{2i}|_F$ pour tout $1 \leq i \leq \frac{w}{2}$, les $r_1 - w$ suivantes sont ordonnées selon les mêmes critères. Soit $C_F = \{\sigma : F \to \mathbb{C} \mid \sigma \text{ n'est pas réelle }\}$ et $c = \sharp C_F$. Alors les c premières places complexes de K sont ordonnées de sorte que $\sigma_{2i-1}|_F = \sigma_{2i}|_F$ pour tout $r_1 + 1 \leq i \leq \frac{c}{2}$. Aucun ordre particulier ne peut être introduit pour les $r_2 - c$ places restantes.*

Il existe encore une distinction que l'on peut faire facilement pour classer les involutions de type I. Considérons une forme bilinéaire non dégénérée b sur un K-espace vectoriel V,

$$b : V \times V \longrightarrow K.$$

Soit

$$\widehat{b} : V \longrightarrow V^*$$

définie par $\widehat{b}(x)(y) = b(x, y)$ l'isomorphisme induit par b entre V et son dual.

On peut alors définir l'anti-automorphisme de l'anneau $\mathrm{End}_K(V)$ suivant :

$$\begin{array}{rccc} \sigma_b : & \mathrm{End}_K(V) & \longrightarrow & \mathrm{End}_K(V) \\ & f & \longmapsto & \widehat{b}^{-1} \circ {}^t f \circ \widehat{b} \end{array}$$

où ${}^t f$ est la transposée de f (c'est-à-dire ${}^t f(\varphi) = \varphi \circ f$ pour tout $\varphi \in V^*$).

Proposition 2.6.5. *Posons*

$$B = \{b : V \times V \to K \mid b \text{ est une forme bilinéaire non dégénérée symétrique ou alternée } \} / K^\times$$

et

$$I = \{\sigma \mid \sigma \text{ est une involution sur } \mathrm{End}_K(V)\}.$$

Alors, l'application

$$\begin{array}{rccc} s: & B & \longrightarrow & I \\ & b & \longmapsto & \sigma_b \end{array}$$

est une bijection.

Preuve : Voir [KMMT98] p.1.

Soient maintenant (A, σ) une algèbre centrale simple (de dimension m^2) sur un corps K, munie d'une involution de type I et L un corps déployant de A. Posons $\sigma_L = \sigma_K \otimes \mathrm{id}_L$, c'est une involution sur A_L, et $V = L^m$. Alors

$$(A_L, \sigma_L) \cong (\mathrm{End}_L(V), \sigma_b)$$

pour une certaine forme bilinéaire non dégénérée b (symétrique ou alternée). On vérifie que la symétrie (ou l'alternance) de b est indépendante du choix de l'isomorphisme et du corps déployant (voir [KMMT98] p.16 définition 2.5).

Définition 2.6.6. *Si b est alternée, on dit que l'involution σ sur A est symplectique.*
Si b est symétrique, on dit que l'involution σ sur A est orthogonale.

Remarque 2.6.7. *Si L est une extension de corps de K, l'involution σ_L sur A_L est symplectique si et seulement si σ est symplectique sur A.*

Nous pouvons maintenant passer aux cas qui nous préoccupent.

Remarquons d'abord que si (A, τ) est une algèbre à involution, alors τ induit une involution sur $A_{\mathbb{R}}$. En effet,

$$\begin{array}{rccc} \tau' = \tau \otimes \mathrm{id}_{\mathbb{R}}: & A_{\mathbb{R}} & \longrightarrow & A_{\mathbb{R}} \\ & a \otimes r & \longmapsto & a^\tau \otimes r \end{array}$$

est une involution $\mathbb{R}$-linéaire.

Définition 2.6.8. *On dit qu'une involution τ' sur*

$$A_{\mathbb{R}} \cong \mathrm{M}_m^{\mathbb{H}}(\mathbb{C})^w \times \mathrm{M}_m(\mathbb{R})^{r_1-w} \times \mathrm{M}_m(\mathbb{C})^{r_2}$$

est positive, si la restriction de τ' à n'importe quelle composante matricielle de $A_{\mathbb{R}}$ est encore une involution qui, de plus, est elle-même positive (voir section 1.6 du chapitre I).
Une involution τ sur A est dite positive, si l'involution induite τ' sur $A_{\mathbb{R}}$ l'est.

Proposition 2.6.9. *Soit τ une involution sur l'algèbre centrale simple A. Munissons $A_{\mathbb{R}}$ de l'involution τ' induite par celle de A. Il existe un réseau idéal (I, b, τ') sur A, si et seulement si l'involution τ est positive.*

Preuve : Supposons qu'il existe un réseau idéal (I, b, τ') sur A. Les propositions 1.5.9 et 1.5.12 nous assurent que $\tau'_i = \tau'|_{\mathrm{M}_i}$ est une involution pour toute composante matricielle M_i de $A_{\mathbb{R}}$. Il existe $\alpha \in \mathcal{F}_{A_{\mathbb{R}}}^{\times}$ tel que $b(x, y) = \mathrm{tr}_{A_{\mathbb{R}}/\mathbb{R}}(x\alpha y^{\tau'})$ pour tout $x, y \in A_{\mathbb{R}}$. Par le corollaire 1.6.11, pour que b soit définie positive, il faut et il suffit que les formes bilinéaire traces :

$$\begin{array}{rccll} \mathrm{Tr}_i : & \mathrm{M}_i \times \mathrm{M}_i & \longrightarrow & \mathbb{R} & \\ & (a_i, b_i) & \longmapsto & \mathrm{Tr}(a_i \alpha_i b_i^{\tau'_i}) & (1 \leq i \leq r_1) \end{array}$$

et

$$\begin{array}{rccll} \mathrm{Tr}_j : & \mathrm{M}_j \times \mathrm{M}_j & \longrightarrow & \mathbb{R} & \\ & (a_j, b_j) & \longmapsto & \mathrm{Tr}(a_j \alpha_j b_j^{\tau'_j}) + \overline{\mathrm{Tr}(a_j \alpha_j b_j^{\tau'_j})} & (r_1 + 1 \leq j \leq r_1 + r_2) \end{array}$$

soient définies positives. Les M_i désignent les composantes matricielles associées à σ_i. Ces formes bilinéaires sont définies positives si et seulement si τ'_i est une involution positive sur M_i (voir propositions 1.7.1, 1.7.4 et 1.7.7) pour tout $1 \leq i \leq r_1 + r_2$, en d'autres termes si et seulement si l'involution τ' est positive.

□

Il suffit donc d'observer les involutions positives sur une algèbre centrale simple munie d'une involution τ pour comprendre les réseaux idéaux (avec involution induite) sur A. La proposition suivante permet de mieux comprendre le comportement d'une telle involution de type I.

Proposition 2.6.10. *Soient τ une involution de type I sur A et τ' l'involution induite sur $A_{\mathbb{R}} \cong \mathrm{M}_m^{\mathbb{H}}(\mathbb{C})^w \times \mathrm{M}_m(\mathbb{R})^{r_1-w} \times \mathrm{M}_m(\mathbb{C})^{r_2}$ par τ. La restriction de τ' à une composante matricielle de $A_{\mathbb{R}}$ est une involution $\mathbb{R}$-linéaire sur cette algèbre de matrices. Si la composante choisie est $\mathrm{M}_m(\mathbb{C})$ alors l'involution est même $\mathbb{C}$-linéaire.*

Preuve : Soient $k \in K$ et $a \in A$. Posons $x = ka \otimes r \in A_{\mathbb{R}}$. L'image de x par l'isomorphisme $\delta : A_{\mathbb{R}} \longrightarrow \mathrm{M}_m^{\mathbb{H}}(\mathbb{C})^w \times \mathrm{M}_m(\mathbb{R})^{r_1-w} \times \mathrm{M}_m(\mathbb{C})^{r_2}$ (voir proposition 1.6.8 et précédentes) est donnée par

$$\delta(x) = (\varphi_{\sigma_1}(a \otimes r\sigma_1(k)), \ldots, \varphi_{\sigma_{r_1+r_2}}(a \otimes r\sigma_{r_1+r_2}(k))).$$

Pour $x^\tau = ka^\tau \otimes r$, nous obtenons

$$\delta(x^\tau) = (\varphi_{\sigma_1}(a^\tau \otimes r\sigma_1(k)), \ldots, \varphi_{\sigma_{r_1+r_2}}(a^\tau \otimes r\sigma_{r_1+r_2}(k))).$$

Ainsi l'involution, restreinte à la composante matricielle M_i correspondant au plongement σ_i, est donnée par

$$\begin{array}{rccc} \tau'|_{\mathrm{M}_i} : & \mathrm{M}_i & \longrightarrow & \mathrm{M}_i \\ & \varphi_{\sigma_i}(a \otimes s) & \longmapsto & \varphi_{\sigma_i}(a^\tau \otimes s) \end{array}.$$

Comme φ_{σ_i} est un isomorphisme de $\mathbb{R}$-algèbres, il est clair que $\tau'|_{\mathrm{M}_i}$ est une involution. Cette involution est bien $\mathbb{C}$-linéaire si $\mathrm{M}_i = \mathrm{M}_m(\mathbb{C})$.

□

Cette proposition nous permet d'introduire la notation suivante.

Notation 2.6.11. *Si τ est une involution de type I sur A et que τ' désigne l'involution induite sur $A_{\mathbb{R}}$, on note $\tau'_i = \tau'|_{\mathrm{M}_i}$ où M_i est la composante matricielle de $A_{\mathbb{R}}$ correspondant au plongement σ_i. On appelle τ'_i l'involution restreinte.*

Corollaire 2.6.12. *Soit τ une involution positive de type I sur A. Alors deux cas sont possibles :*

i) L'involution τ est symplectique et dans ce cas
le corps de nombres K est totalement réel, autrement dit $r_2 = 0$, et l'algèbre A est totalement définie sur K (c'est-à-dire que toutes les places infinies de K sont ramifiées dans A), autrement dit $r_1 = w$.

ii) L'involution τ est orthogonale et dans ce cas

Le corps de nombres K est totalement réel, autrement dit $r_2 = 0$, et l'algèbre A est totalement indéfinie sur K (c'est-à-dire qu'aucune place infinie de K n'est ramifiée dans A), autrement dit $w = 0$.

PREUVE : La proposition précédente nous dit que l'involution induite sur les composantes matricielles $\mathrm{M}_m(\mathbb{C})$ de $A_{\mathbb{R}}$ est $\mathbb{C}$-linéaire ce qui est impossible puisque τ est positive (voir proposition 1.7.4), donc $r_2 = 0$ dans tous les cas. Supposons que l'involution τ est symplectique ; alors τ_i' est encore une involution symplectique (remarque 2.6.7). La proposition 1.7.1 nous assure alors qu'il ne peut y avoir de composante matricielle de la forme $\mathrm{M}_m(\mathbb{R})$ dans $A_{\mathbb{R}}$ (i.e. $r_1 = w$). De la même façon, si τ est orthoghonale alors ce sont les composantes de la forme $\mathrm{M}_m^{\mathbb{H}}(\mathbb{C})$ qui ne peuvent apparaître (i.e. $w = 0$). □

Ce corollaire nous donne une liste de conditions nécessaires sur K pour qu'une K-algèbre à involution de type I admette un réseau idéal. Il reste à voir ce qui se passe avec une involution de type II.

Proposition 2.6.13. *Soient τ une involution de type II sur A et τ' l'involution induite sur $A_{\mathbb{R}} \cong \mathrm{M}_m^{\mathbb{H}}(\mathbb{C})^w \times \mathrm{M}_m(\mathbb{R})^{r_1-w} \times \mathrm{M}_m(\mathbb{C})^{r_2}$. On ordonne $\sigma_1, \ldots, \sigma_{r_1+r_2}$ les places infinies de K de la même façon que dans la notation 2.6.4.*

Si $1 \leq i \leq c$,
la restriction de l'involution τ' à une composante matricielle M_i n'est pas une involution sur M_i. Plus précisément, $\tau'|_{\mathrm{M}_i}$ échange les composantes issues de la même place de F :

$$\tau'|_{\mathrm{M}_{2i-1}} \; : \; \mathrm{M}_{2i-1} \longrightarrow \mathrm{M}_{2i}$$

$$\tau'|_{\mathrm{M}_{2i}} \; : \; \mathrm{M}_{2i} \longrightarrow \mathrm{M}_{2i-1}$$

Si $c+1 \leq i \leq r_1 + r_2$,
la restriction de l'involution τ' à une composante matricielle $\mathrm{M}_i = \mathrm{M}_m(\mathbb{C})$ est une involution $\mathbb{R}$-linéaire sur $\mathrm{M}_m(\mathbb{C})$. Cette involution n'est pas $\mathbb{C}$-linéaire. On la note τ_i'.

PREUVE : Réglons d'abord le cas où $i \leq c$. Sans perte de généralité, nous pouvons faire la démonstration d'abord pour σ_1, σ_2 (deux places réelles de K qui étendent la même place σ de F), puis pour $\sigma_{r_1+1}, \sigma_{r_1+2}$ (deux places complexes de K qui étendent la même place réelle σ' de F).

Considérons $x = ka \otimes \sigma_2(l) - la \otimes \sigma_2(k) \in A_{\mathbb{R}}$ où $a \in A$ et $k, l \in K$. Un calcul montre que

$$\delta(x) = (x_1, 0, x_3, \ldots, x_{r_1+r_2}) \quad \text{avec } x_i \neq 0 \text{ pour tout } 1 \leq i \leq r_1 + r_2.$$

De plus, en utilisant la relation $\sigma_1(k^\tau) = \sigma_2(k)$ pour tout $k \in K$, nous observons que

$$\delta(x^{\tau'}) = (0, x'_2, x'_3, \ldots, x'_{r_1+r_2}) \quad \text{avec } x'_i \neq 0 \text{ pour tout } 1 \leq i \leq r_1 + r_2.$$

Cela prouve que $\mathrm{Im}(\tau'|_{\mathrm{M}_2}) \subset \mathrm{M}_1$. La proposition 1.5.10 nous assure dès lors que $\mathrm{Im}(\tau'|_{\mathrm{M}_1}) \subset \mathrm{M}_2$. Ce qui résout le cas des places réelles de K.

La démarche est la même pour les places complexes de K :

$$K_{\sigma_{r_1+1}} \cong K_{\sigma_{r_1+2}} \cong \mathbb{C}.$$

Considérons les éléments

$$1 \otimes i \in A \otimes_K \mathbb{C}$$

et

$$y = (0, \ldots, 0, \varphi_{\sigma_{r_1+1}}(1 \otimes i), \varphi_{\sigma_{r_1+2}}(1 \otimes i), 0, \ldots, 0) \in A_{\mathbb{R}}.$$

Posons $z = \delta^{-1}(y)$. Nous vérifions que $z^{\tau'} = z$. En utilisant

$$\begin{aligned} x = {} & ka \otimes \mathrm{Re}(\sigma_{r_1+2}(l)) - la \otimes \mathrm{Re}(\sigma_{r_1+2}(k)) \\ & + z\,(ka \otimes \Im(\sigma_{r_1+2}(l)) - la \otimes \Im(\sigma_{r_1+2}(k))) \end{aligned}$$

et en répétant le raisonnement fait dans le cas réel nous obtenons que $\tau^{|}_{M_i}$ n'est pas une involution.

Il reste à voir que la restriction de τ' aux composantes matricielles M_i avec $i > c$ est bien une involution sur M_i. Soit $\sigma = \sigma_i$ (avec $i > c$). Un raisonnement similaire à celui qui précède permet de voir que $\mathrm{Im}(M_i) \subset M_i$. La proposition 2.6.3 dit que $\sigma(k^\tau) = \overline{\sigma(k)}$ pour tout $k \in K$, de sorte que l'involution restreinte à M_i est donnée par

$$\begin{array}{rccc} \tau'_i : & \mathrm{M}_i & \longrightarrow & \mathrm{M}_i \\ & \varphi_{\sigma_i}(a \otimes z) & \longmapsto & \varphi_{\sigma_i}(a^\tau \otimes \bar{z}) \end{array}$$

qui n'est pas $\mathbb{C}$-linéaire.

□

Corollaire 2.6.14. *Soit τ une involution positive de type II sur A et F le sous-corps de $K = F(\sqrt{\theta})$ fixé par l'involution. Alors F est totalement réel et $\sigma(\theta) < 0$ pour toute place σ de F. Autrement dit K est un corps CM.*

PREUVE : Comme τ est une involution positive, $\tau'|_{\mathrm{M}_i}$ est une involution (positive) sur chaque composante matricielle de $A_{\mathbb{R}}$. La proposition précédente nous dit alors que les places de $F = \{x \in K \mid x^\tau = x\}$ sont toutes réelles et qu'en plus $\sigma(\theta) < 0$ pour toute place σ de F (c'est la traduction de $c = 0$ dans la notation 2.6.4).

□

Ce corollaire nous donne une liste de conditions nécessaires sur K pour qu'une K-algèbre à involution de type II admette un réseau idéal.

Nous verrons plus tard que ces conditions peuvent être encore précisées dans le cas d'une algèbre de quaternions.

2.7 Réseaux idéaux particuliers

Afin de construire des exemples de bornes supérieures du minimum euclidien, nous aurons besoin de résultats plus précis sur les réseaux entiers. Cette section donne l'essentiel de ces résultats.

Proposition 2.7.1. *Soient A une algèbre centrale à division sur un corps de nombres K, Λ un ordre maximal et (I, α, τ) un réseau idéal de A. Le réseau (I, α) est entier si et seulement si*

$$I\alpha I^\tau \subset \mathcal{D}(\Lambda/\mathbb{Z})^{-\tau}.$$

PREUVE : Par définition, (I, α) est entier si et seulement si $I \subset I^*$, mais $I^* = \mathcal{D}(\Lambda/\mathbb{Z})^{-\tau} I^{-\tau} \alpha^{-1}$ (voir proposition 1.8.6). Donc l'inclusion $I \subset I^*$ devient $I \subset \mathcal{D}(\Lambda/\mathbb{Z})^{-\tau} I^{-\tau} \alpha^{-1}$.

□

Corollaire 2.7.2. *Soient A et Λ comme dans la proposition précédente et (I, α, τ) un réseau idéal entier de A. Alors*

$$\det(I, \alpha, \tau) = 1 \iff I\alpha I^\tau = \mathcal{D}(\Lambda/\mathbb{Z})^{-\tau}.$$

PREUVE : D'après la proposition 1.8.12,

$$\det(I, \alpha, \tau) = 1 \iff \mathrm{N}_{A_{\mathbb{R}}/\mathbb{R}}(I\alpha I^\tau \mathcal{D}(\Lambda/\mathbb{Z})^\tau) = 1.$$

Par la proposition précédente $I\alpha I^\tau \subset \mathcal{D}(\Lambda/\mathbb{Z})^{-\tau}$, donc la seule possibilité est $I\alpha I^\tau = \mathcal{D}(\Lambda/\mathbb{Z})^{-\tau}$.

□

Remarquons encore le fait suivant qui permet de modifier l'idéal sans changer le réseau.

Proposition 2.7.3. *Soient A et Λ comme dans la proposition précédente, (I, α, τ) un réseau idéal de A et $s \in A^\times$. On a*

$$(I, \alpha, \tau) \cong (sI, s^{-1}\alpha s^{-\tau}, \tau)$$

PREUVE : Considérons l'automorphisme φ de A donné par la conjuguaison par s. Pour tout $sx, sy \in sI$,

$$\mathrm{tr}_{A/\mathbb{Q}}(sxs^{-1}\alpha s^{-\tau}(sy)^\tau) = \mathrm{tr}_{A/\mathbb{Q}}(\varphi(x)\alpha\varphi(y)^\tau),$$

ce qui prouve que les réseaux sont isométriques.

□

Pour terminer nous allons décrire un cas particulier dans lequel le réseau (I, α, τ) est un produit tensoriel de réseaux plus simples. Cela nous sera utile, en particulier lorsque l'algèbre considérée est une algèbre de quaternions.

Soient Λ un ordre de A, I un idéal de Λ libre comme $\mathcal{O}_K$-module, $\alpha \in A$ et τ une involution positive sur A telle que la forme bilinéaire

$$\begin{array}{rccc} \mathrm{tr}_\alpha : & I \times I & \longrightarrow & K \\ & (x, y) & \longmapsto & \mathrm{tr}_{A/K}(x\alpha y^\tau) \end{array}$$

est à coefficients rationnels et définie positive (en d'autres termes (I, tr_α) est un réseau). Dans cette situation, $(I, \alpha\beta)$, où $\beta \in K$, est caractérisé de la manière suivante.

Proposition 2.7.4. *Soient (I, tr_α) comme ci-dessus et $\beta \in K$ tel que $(\mathcal{O}_K, \beta)$ est un réseau. Alors*

$$(I, \alpha\beta, \tau) \cong (I, \mathrm{tr}_\alpha) \otimes_{\mathbb{Z}} (\mathcal{O}_K, \beta).$$

PREUVE : Soient $E = \{e_1, \ldots, e_r\}$ une $\mathcal{O}_K$-base de I et $F = \{f_1, \ldots, f_n\}$ une $\mathbb{Z}$-base de $\mathcal{O}_K$. La base $E \otimes F = \{f_1e_1, \ldots, f_ne_1, \ldots, f_1e_r, \ldots, f_ne_r\}$ est une $\mathbb{Z}$-base de I. Or

$$\mathrm{T}_{K/\mathbb{Q}}(\mathrm{tr}_{A/K}(f_ie_j\alpha\beta(f_ke_l)^\tau) = \mathrm{T}_{K/\mathbb{Q}}(\beta f_i f_k^\tau)\mathrm{tr}_{A/K}(e_j\alpha e_l^\tau)$$

car tr_α est à coefficients rationnels. De plus nous savons que τ est soit de type I, et dans ce cas K est totalement réel et $\tau|_K = \mathrm{id}_K$, soit de type II, et dans ce cas K est un corps CM et $\tau|_K$ est la conjugaison complexe (voir section précédente). Dans les deux cas $(\mathrm{T}_{K/\mathbb{Q}}(\beta f_i f_k^\tau))_{1\leq i,k\leq n}$ est une matrice de Gram du réseau $(\mathcal{O}_K, \beta)$.
Cela nous assure qu'une matrice de Gram de $(I, \alpha\beta)$ est donnée par le produit tensoriel des matrices de Gram des réseaux (I, tr_α) et $(\mathcal{O}_K, \beta)$.

□

Chapitre III

Minimum euclidien des corps de quaternions

Nous allons voir dans ce chapitre quelques exemples, dans le cas des quaternions, de la borne du minimum euclidien donnée dans la section 2.5 du chapitre II. Nous donnerons en particulier une liste de conditions nécessaires et suffisantes pour réaliser le réseau E_8 et les conséquences que cela engendre sur le minimum euclidien des corps de quaternions quadratiques. Nous donnerons également une liste exhaustive des corps de quaternions euclidiens sur $\mathbb{Q}$ et sur un corps quadratique imaginaire. La détermination des corps de quaternions euclidiens sur un corps quadratique fait l'objet des sections 3.11 et 3.13 mais reste partiellement ouverte.

La détermination des corps de quaternions euclidiens, que ce soit sur $\mathbb{Q}$ ou sur un corps quadratique, s'appuie sur trois résultats importants, dont deux se trouvent dans ce chapitre.

i) Le premier est le théorème 2.5.1 du chapitre II qui permet de borner supérieurement le minimum euclidien d'un ordre maximal Λ dans une algèbre à division, en fonction des invariants d'Hermite des réseaux idéaux associés à Λ.

ii) Le deuxième est le théorème 3.4.10. Il permet de borner supérieurement le minimum euclidien d'un corps de quaternions principal totalement indéfini sur K par le minimum euclidien de K.

iii) Le dernier est le corollaire 3.10.3. Il permet de borner inférieurement le minimum euclidien d'un corps de quaternions totalement défini sur K par le carré du minimum euclidien de K.

Les sections 3.5 à 3.7 donnent des formules explicites du minimum euclidien de certaines familles infinies d'ordres maximaux dans les corps de quaternions définis sur $\mathbb{Q}$.

Tout au long du chapitre nous verrons apparaître des familles infinies d'ordres maximaux. Ces ordres ont, pour la plupart, été découverts en s'appuyant sur des moyens informatiques.

Nous commençons par rappeler une liste de définitions équivalentes d'une algèbre de quaternions et quelques propriétés fondamentales.

3.1 Définitions et propriétés fondamentales

Pour simplifier et rester dans le cadre qui nous préoccupe, nous supposons que K est un corps de caractéristique différente de 2 (bien que toutes les définitions et tous les résultats donnés dans cette section puissent être généralisés au cas d'un corps de caractéristique 2).

Définition 3.1.1. *Soient K un corps et $\overline{K}$ une clôture algébrique de K. Une algèbre de quaternions sur K est une K-algèbre vérifiant une des conditions équivalentes suivantes :*

i) L'algèbre A est une algèbre centrale de dimension 4 sur K engendrée comme K-espace vectoriel par la famille $\{1, i, j, k = ij\}$ vérifiant

$$i^2 = a, \quad j^2 = b, \quad ij = -ji$$

où a, b sont des éléments fixés de K.

ii) L'algèbre A est une algèbre centrale de dimension 4 sur K, telle qu'il existe une algèbre $L = K(\alpha) \subset A$, séparable et de dimension 2 sur K, un élément inversible θ de K et un élément u de A avec

$$A = L + Lu, \quad u^2 = \theta, \quad um = \overline{m}u$$

pour tout $m \in L$, où $^- : L \to L$ est le K-automorphisme non trivial de L.

iii) L'algèbre A est la sous-K-algèbre de $\mathrm{M}_2(\overline{K})$ engendrée par les matrices suivantes :

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad i = \begin{pmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{pmatrix},$$

$$j = \begin{pmatrix} 0 & \sqrt{-b} \\ -\sqrt{-b} & 0 \end{pmatrix}, \quad k = \begin{pmatrix} 0 & \sqrt{-ab} \\ \sqrt{-ab} & 0 \end{pmatrix}$$

où a, b sont des éléments fixés de K.

iv) L'algèbre A est une algèbre centrale simple de dimension 4 sur K.

On montre facilement l'équivalence des quatre définitions. Sans entrer dans les détails, si $L = K(\sqrt{\alpha})$ est comme dans la définition *ii)* alors le couple (α, θ) correspond au couple (a, b) de la définition *i)*. De même, les couples (a, b) des définitions *i)* et *iii)* se correspondent.

On note l'algèbre de quaternions $A = (a, b)_K$, et, si $x = x_0 + ix_1 + jx_2 + kx_3 \in A$, on appelle x_0 le terme constant de x.

Définition 3.1.2. *Le corps gauche $(-1, -1)_{\mathbb{R}}$, noté $\mathbb{H}$, est appelé le corps des quaternions de Hamilton.*

La liste des propriétés connues des algèbres de quaternions est énorme et impossible à énoncer ici. Nous ne donnons que les propriétés indispensables pour la suite de ce travail.

Proposition 3.1.3. *Soient $A = (a, b)_K$ une algèbre de quaternions et*

$$\begin{array}{rccc} \gamma : & A & \longrightarrow & A \\ & x_0 + ix_1 + jx_2 + kx_3 & \longmapsto & x_0 - ix_1 - jx_2 - kx_3. \end{array}$$

Alors :

i) L'application γ est l'unique involution symplectique sur A (appelée involution canonique et notée aussi $^-$). Si τ est une involution orthogonale sur A alors il existe un unique $u \in \{x \in A \mid x^\gamma = -x\}$, à multiplication par un élément de $K^\times$ près, avec $\tau = \mathrm{Int}(u) \circ \gamma$.

ii) Soient τ une involution de type II sur $A = (a, b)_K$ et $\iota = \tau|_K$ le F-automorphisme non trivial de K (où F est le sous corps de K fixé par l'involution). L'algèbre $A_0 = \{x \in A \mid x^\tau = x^\gamma\}$ est l'unique algèbre de quaternions sur F, contenue dans A, vérifiant

$$A = A_0 \otimes_F K, \quad et \quad \tau = \gamma_0 \otimes \iota$$

où γ_0 est l'involution canonique sur A_0. De plus $a, b \in F$ et $A_0 \cong (a, b)_F$.

iii) La norme et la trace réduite de A sont données par :

$$\mathrm{nr}_{A/K}(x) = xx^\gamma \quad et \quad \mathrm{tr}_{A/K}(x) = x + x^\gamma$$

pour tout $x \in A$.

iv) L'algèbre A est soit une algèbre de matrices sur K, soit une algèbre à division sur K.

Preuve : Pour *i)* et *ii)* voir [KMMT98] proposition 2.21 et 2.22, p.26.
Pour *iii)* il suffit de voir que le polynôme caractéristique réduit de $x \in A$ est

$X^2 - (x + x^\gamma)X + xx^\gamma$. Le point *iv)* découle du fait que $A \cong \mathrm{M}_n(D)$ où D est un corps gauche. Pour des raisons de dimension, soit $D = K$ et $n = 2$, soit $A = D$.

Proposition 3.1.4. *Soit $A = (a, b)_K$ un corps de quaternions sur un corps de nombres K. Supposons que A est muni d'une involution τ, alors l'involution τ est positive si et seulement si on est dans une des situations suivantes :*

L'involution τ est symplectique.
Alors $\tau = \gamma$ est l'involution canonique, K est totalement réel et A est totalement défini. Dans ce cas, (I, α, τ) est un réseau idéal de A si et seulement si $\alpha \in K$ et α est totalement positif.

L'involution τ est orthogonale.
Alors K est totalement réel et A est totalement indéfini.

L'involution τ est de type II.
Alors K est un corps CM et, si F est le sous-corps de K fixé par l'involution et $A_0 = \{x \in A \mid x^\tau = x^\gamma\}$, alors $A_0 = (a, b)_F$ est une algèbre de quaternions totalement définie sur F (a et b sont totalement négatifs). Dans ce cas, (I, α, τ) est un réseau idéal sur A, si et seulement si $\alpha = a_0 + i\sqrt{\theta}a_1 + j\sqrt{\theta}a_2 + k\sqrt{\theta}a_3$ où $K = F(\sqrt{\theta})$ et $a_i \in F$ pour tout $0 \leq i \leq 3$ et

$$0 < \sigma(\mathrm{nr}_{A/K}(\alpha)) < \sigma\left(\frac{\mathrm{tr}(\alpha)^2}{2}\right)$$

pour tout plongement σ de F dans $\mathbb{R}$.

Preuve : Si l'involution est symplectique nous avons vu (voir corollaire 2.6.12) que K est totalement réel et A totalement définie. L'unique involution symplectique sur A est l'involution canonique γ, donc $\tau = \gamma$. Soit (I, α, γ) un réseau idéal. Alors $\alpha^\gamma = \alpha$, donc $\alpha \in K$. nous vérifions que l'involution induite par γ sur $A_\mathbb{R} = \mathrm{M}_2^\mathbb{H}(\mathbb{C})^w$ est l'involution $^- \circ\, t$ sur chaque composante matricielle (où w est le nombre de places réelles de K, c'est-à-dire $w = [K : \mathbb{Q}]$). La proposition 1.7.7 nous assure que chaque composante de l'image de α dans $A_\mathbb{R}$ est définie positive. Comme $\alpha \in K$, cela revient à dire que α est positif à toutes les places infinies.

Si l'involution est orthogonale, alors le résultat découle directement du corollaire 2.6.12.

Si l'involution est de type II nous savons déjà que K est un corps CM (voir corollaire 2.6.14). Remarquons que l'involution induite par τ sur

$$A \otimes_K K_\sigma \cong \mathrm{M}_2(\mathbb{C})$$

est positive si et seulement si $\sigma(a)$ et $\sigma(b)$ sont négatifs (dans ce cas l'involution sur $\mathrm{M}_2(\mathbb{C})$ est $^- \circ t$). Autrement dit, A_0 est totalement définie. Par la proposition précédente, $\tau = \gamma_0 \otimes \iota$ où γ_0 est l'involution canonique sur A_0 et ι est le F-automorphisme non trivial de K. Ainsi $\alpha = \alpha^\tau$ si et seulement si α est de la forme annoncée. De plus si (I, α, τ) est un réseau idéal, alors (voir la proposition 1.7.4) l'image de α dans chaque composante de $\mathrm{M}_2(\mathbb{C})$ est définie positive. Nous vérifions que cela arrive si et seulement si $\sigma(\mathrm{nr}_{A/K}(\alpha)) < \sigma(\frac{\mathrm{tr}(\alpha)^2}{2})$ pour tout plongement σ de F dans $\mathbb{R}$.

□

Notation 3.1.5. *Soit $x = x_0 + ix_1 + jx_2 + kx_3 \in A = (a,b)_K$ et ι le F-automorphisme non trivial de K, alors ι agit sur les coefficients de x. On note $x^\iota = x_0^\iota + ix_1^\iota + jx_2^\iota + kx_3^\iota$, et avec cette notation on a $\tau = \gamma \circ \iota = \gamma\iota$.*

3.2 Réseaux pairs et réseaux primitifs

Définition 3.2.1. *Soit (L, q) un réseau entier. On dit que (L, q) est pair si $q(x) \in 2\mathbb{Z}$ pour tout $x \in L$, qu'il est primitif si $q(L) = \mathbb{Z}$ et qu'il est unimodulaire si* $\det(L, q) = 1$.

Proposition 3.2.2. *Soient $A = (a,b)_K$ un corps de quaternions, Λ un ordre maximal de A, τ une involution symplectique ou de type II sur A et (I, α, τ) un réseau idéal entier de A. Si τ est de type II, on suppose encore qu'aucun premier de F au-dessus de 2 n'est ramifié dans K. Alors (I, α, τ) est pair.*

Preuve : Comme A est modérément ramifié il existe $z \in \Lambda$ tel que $\mathrm{tr}_{A/K}(z) = z + z^\gamma = 1$. Supposons d'abord que τ est une involution de type II. Alors

$$\mathrm{tr}_{A/K}(x\alpha x^\tau) = \mathrm{tr}_{A/K}(zx\alpha x^\tau) + \mathrm{tr}_{A/K}(z^\gamma x\alpha x^\tau).$$

Soient F le sous-corps totalement réel de K fixé par τ et soit ι le F-automorphisme non trivial de K. Comme $\tau = \gamma\iota = \iota\gamma$, nous obtenons

$$\mathrm{tr}_{A/K}(x^\tau) = x^\tau + x^{\tau\gamma} = x^\tau + x^\iota = (x^\gamma + x)^\iota = \mathrm{tr}_{A/K}(x)^\iota.$$

Ainsi

$$\mathrm{tr}_{A/K}(zx\alpha x^\tau)^\iota = \mathrm{tr}_{A/K}((zx\alpha x^\tau)^\tau) = \mathrm{tr}_{A/K}(z^\tau x\alpha x^\tau)$$

et

$$\mathrm{tr}_{A/K}(z^\gamma x\alpha x^\tau)^\iota = \mathrm{tr}_{A/K}(z^\iota x\alpha x^\tau).$$

De plus $(z+z^\gamma)^\tau = z^\tau + z^\iota = 1$, donc

$$\mathrm{tr}_{A/K}(x\alpha x^\tau) = \mathrm{tr}_{A/K}(z^\tau x\alpha x^\tau) + \mathrm{tr}_{A/K}(z^\iota x\alpha x^\tau) =$$

$$\mathrm{tr}_{A/K}(zx\alpha x^\tau)^\iota + \mathrm{tr}_{A/K}(z^\gamma x\alpha x^\tau)^\iota = \mathrm{tr}_{A/K}(x\alpha x^\tau)^\iota,$$

autrement dit $\mathrm{tr}_{A/K}(x\alpha x^\tau) \in F$, de sorte que

$$\mathrm{tr}_{A/\mathbb{Q}}(x\alpha x^\tau) = \mathrm{T}_{F/\mathbb{Q}}\mathrm{T}_{K/F}(\mathrm{tr}_{A/K}(x\alpha x^\tau)) = 2\mathrm{T}_{F/\mathbb{Q}}(\mathrm{tr}_{A/K}(x\alpha x^\tau)).$$

D'autre part,

$$\mathrm{T}_{K/\mathbb{Q}}(\mathrm{tr}_{A/K}(I\alpha I^\tau)) = \mathrm{T}_{K/\mathbb{Q}}(\mathrm{tr}_{A/K}(I\alpha I^\tau)\mathcal{O}_K) \subset \mathbb{Z},$$

autrement dit

$$\mathrm{tr}_{A/K}(I\alpha I^\tau) \subset \mathcal{D}_K \cap F = \mathcal{D}_F$$

où l'égalité vient du fait que K/F est modérément ramifié (car sans ramification dyadique). Donc

$$\mathrm{T}_{F/\mathbb{Q}}(\mathrm{tr}_{A/K}(x\alpha x^\tau)) \in \mathbb{Z}$$

ce qui nous permet de conclure.

Si l'involution τ est symplectique, alors $\tau = \gamma$ et

$$\mathrm{tr}_{A/\mathbb{Q}}(x\alpha x^\gamma) = \mathrm{tr}_{A/\mathbb{Q}}(zx\alpha x^\gamma) + \mathrm{tr}_{A/\mathbb{Q}}(z^\gamma x\alpha x^\gamma) = 2\mathrm{tr}_{A/\mathbb{Q}}(zx\alpha x^\gamma)$$

Nous concluons, comme avant grâce au fait que $x\alpha x^\gamma \in \mathcal{D}(\Lambda/\mathbb{Z})^{-1}$.

□

Remarque 3.2.3. *La condition qui exige que les premiers de F au-dessus de 2 ne sont pas ramifiés dans K est plus forte que nécessaire. En effet, il suffit d'avoir*

$$\mathrm{tr}_{A/K}(x\alpha x^\tau) \in \{a \in F \mid \mathrm{T}_{F/\mathbb{Q}}(a) \in \mathbb{Z}\} \quad \textit{pour tout } x \in I.$$

Nous utiliserons parfois cette condition moins forte dans la suite.

Proposition 3.2.4. *Soient A, Λ, τ et (I,α,τ) comme dans la proposition précédente. Alors (I,α,τ) est primitif si et seulement si $I\alpha I^\tau \not\subset p\mathcal{D}(\Lambda/\mathbb{Z})^{-1}$ pour tout nombre premier $p \in \mathbb{Z}$.*

PREUVE : Remarquons d'abord que

$$\mathrm{tr}_{A/\mathbb{Q}}(J) \subset n\mathbb{Z} \iff J \subset n\mathcal{D}(\Lambda/\mathbb{Z})^{-1}$$

pour tout idéal J de Λ et tout entier n. En effet, considérons la différente inverse de J, donné par $\widetilde{J} = \{x \in A \mid \mathrm{tr}_{A/\mathbb{Q}}(xJ) \subset \mathbb{Z}\}$. Alors

$$\mathrm{tr}_{A/\mathbb{Q}}(J) \subset n\mathbb{Z} \iff \Lambda \subset n\widetilde{J}.$$

Mais $\widetilde{J} = J^{-1}\widetilde{\Lambda} = J^{-1}\mathcal{D}(\Lambda/\mathbb{Z})^{-1}$ (voir [Rei03] théorème 25.1, p. 217), d'où le résultat. Cela implique la proposition car (I, α, τ) est primitif si et seulement si $\mathrm{tr}_{A/\mathbb{Q}}(I\alpha I^{\tau})$ n'est contenue dans aucun idéal premier de $\mathbb{Z}$.

□

3.3 Ordres maximaux dans les algèbres de quaternions

Toujours dans le but de borner leur minimum euclidien, nous allons donner, dans cette section, des exemples d'ordre maximaux d'un corps de quaternions sur un corps de nombres.

Rappelons d'abord la notion de symbole de Legendre généralisée.

Définition 3.3.1. *Soient K un corps de nombres, $\mathcal{P}$ un idéal premier de $\mathcal{O}_K$ et $a \in \mathcal{O}_K$. On définit le symbole de Legendre (généralisé)*

$$\left(\frac{a}{\mathcal{P}}\right) = \begin{cases} -1 & \text{si } a\mathcal{O}_K \text{ n'est pas un carré modulo } \mathcal{P} \text{ et } (a\mathcal{O}_K, \mathcal{P}) = 1, \\ 1 & \text{si } a\mathcal{O}_K \text{ est un carré modulo } \mathcal{P} \text{ et } (a\mathcal{O}_K, \mathcal{P}) = 1, \\ 0 & \text{si } (a\mathcal{O}_K, \mathcal{P}) \neq 1. \end{cases}$$

Lorsque $\left(\frac{a}{\mathcal{P}}\right) = 1$, on dit que a est un résidu quadratique modulo $\mathcal{P}$.

La proposition suivante donne une description de la forme $(a, b)_K$ d'une algèbre de quaternions.

Proposition 3.3.2. *Soit A une algèbre de quaternions sur un corps de nombres K ramifiée aux places finies $\mathrm{Ram}_f(A) = \{\mathcal{P}_1, \ldots, \mathcal{P}_r\}$ et aux places infinies réelles $\mathrm{Ram}_\infty(A) = \{\sigma_1, \ldots, \sigma_s\}$ (ces ensembles de places peuvent être vides). Supposons qu'il existe des entiers impairs $n_1, \ldots, n_r \in \mathbb{N}$ tels que $\mathcal{P}_1^{n_1} \cdots \mathcal{P}_r^{n_r}$ est un idéal principal (disons engendré par d'). On choisit un $b \in \mathcal{O}_K$ tel que :*

– $\mathrm{pgcd}(d', b) = 1$,
– $d = d'b$ *est positif en chaque place de* $\mathrm{Ram}_\infty(A)$,
– b *n'est divisible par aucun premier dyadique.*
Il existe alors $a \in \mathcal{O}_K$ *tel que*

i) $L'idéal\ a\mathcal{O}_K$ *est premier dans* $\mathcal{O}_K$ *distinct de* $\mathcal{P}_i$ *pour tout* $1 \leq i \leq r$.

ii) $\sigma(a) < 0$ *si et seulement si* $\sigma \in \mathrm{Ram}_\infty(A)$.

iii) Le symbole de Legendre $\left(\frac{a}{\mathcal{P}}\right)$ *vaut* -1 *pour tout* $\mathcal{P} \in \mathrm{Ram}_f(A)$ *tel que* $\mathcal{P}$ *ne divise pas* $2\mathcal{O}_K$.

iv) L'élément a *n'est pas un carré dans* $(\mathcal{O}_K)_\mathcal{P}$ *mais c'est un carré dans* $(\mathcal{O}_K)_\mathcal{P}/4(\mathcal{O}_K)_\mathcal{P}$, *pour tout idéal dyadique* $\mathcal{P}$.

v) Le symbole de Legendre $\left(\frac{a}{\mathcal{P}}\right)$ *vaut* 1 *pour tout* $\mathcal{P}$ *divisant* b.

Un tel a *satisfait alors*

$$A \cong (a, -d)_K.$$

PREUVE : voir [LJ] proposition 2.10, p.18.

Proposition 3.3.3. *Soit* A *comme dans la proposition précédente. On suppose encore que* $\mathcal{P}_1 \cdots \mathcal{P}_r$ *est un idéal pincipal, on choisit* a *et* d *comme dans la proposition précédente de façon à ce que* $A \cong (a, -d)_K$. *Il existe alors* $x, c \in \mathcal{O}_K$ *tels que* $a \equiv x^2 \mod 4\mathcal{O}_K$ *et* $-d \equiv c^2 \mod a\mathcal{O}_K$. *De plus,*

$$\Lambda = \mathcal{O}_K \oplus \frac{x+i}{2}\mathcal{O}_K \oplus \frac{ci+k}{a}\mathcal{O}_K \oplus \frac{(x+i)(ci+k)}{2a}\mathcal{O}_K$$

est un ordre maximal de $(a, -d)_K$. *Si, de plus,* $d \equiv 3 \mod 4\mathcal{O}_K$ *et si* $c \equiv 1 \mod 2\mathcal{O}_K$, *alors*

$$\Gamma = \mathcal{O}_K \oplus i\mathcal{O}_K \oplus \frac{1+j}{2}\mathcal{O}_K \oplus \frac{-ci-k}{2a}\mathcal{O}_K$$

est également un ordre maximal de $(a, -d)_K$.

PREUVE : Le fait que Λ est un ordre maximal se trouve dans [LJ] proposition 6.9 p.31. Pour Γ il suffit de constater que c'est un anneau pour voir que c'est un ordre et que $\mathrm{d}(\Gamma) = d^2$ pour en déduire qu'il est maximal.

□

Dans la suite de ce travail, nous utiliserons souvent l'algèbre de quaternions usuelle $A = (-1, -1)_K$ sur un corps de nombres K. Les propositions précédentes ne donnent pas d'information sur ce cas. Nous allons donc donner quelques résultats concernant spécifiquement $(-1, -1)_K$ et ses ordres maximaux.

Proposition 3.3.4. *Soit K un corps de nombres et $A = (-1,-1)_K$ l'algèbre de quaternions usuelle sur K. Alors A est ramifiée en $\mathcal{P}$ si et seulement si $\mathcal{P}$ est un premier dyadique et $e(\mathcal{P})f(\mathcal{P})$ est impair (où $e(\mathcal{P})$ et $f(\mathcal{P})$ sont respectivement le degré de ramification et le degré résiduel de $\mathcal{P}$).*

PREUVE : Seuls les premiers dyadiques peuvent ramifier dans A. En effet, nous savons que si $\mathcal{P}$ n'est pas un premier dyadique et si $a, b \in (O_K)^\times_{\mathcal{P}}$ alors $(a,b)_{\mathcal{P}} = 1$ (voir [LJ] proposition 2.8). Soit $\mathcal{P}$ un premier dyadique. Alors $\mathcal{P}$ est ramifié dans A si et seulement si $(-1,-1)_{K_{\mathcal{P}}}$ est un corps. Nous savons que $(-1,-1)_{\mathbb{Q}_2}$ est un corps (voir [Ser77] théorème 1 chapitre I) et que $(-1,-1)_{K_{\mathcal{P}}}$ est un corps si et seulement si $[K_{\mathcal{P}} : \mathbb{Q}_2]$ est impair (voir [Vig80] théorème 1.3, chapitre 2). On conclut en rappelant que $[K_{\mathcal{P}} : \mathbb{Q}_2] = e(\mathcal{P})f(\mathcal{P})$.

□

Nous aurons besoin du lemme suivant qui est, sans doute, bien connu mais que nous rappelons ici, faute de le trouver explicitement dans la littérature.

Lemme 3.3.5. *Soient K un corps de nombres, p un nombre premier et $p\mathcal{O}_K = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r}$. Alors*

$$\mathcal{O}_K/P_i^{e_i} \cong (\mathcal{O}_K/\mathcal{P}_i)[X]/X^{e_i}$$

pour tout $1 \leq i \leq r$. En particulier $\mathcal{O}_K/\mathcal{P}_i^{e_i}$ est un $\mathcal{O}_K/\mathcal{P}_i$ espace vectoriel de degré e_i et

$$\mathcal{O}_K/p\mathcal{O}_K \cong (\mathcal{O}_K/\mathcal{P}_1)[X]/X^{e_1} \times \cdots \times (\mathcal{O}_K/\mathcal{P}_r)[X]/X^{e_r}$$

PREUVE : Sans perte de généralité, nous pouvons raisonner sur $\mathcal{P} = \mathcal{P}_1$. Posons $e = e_1$. Soient $\mathbb{Q}_p$ le corps complété de $\mathbb{Q}$ pour la valuation p-adique et $K_{\mathcal{P}}$ le complété de K pour la valuation $\mathcal{P}$-adique. Notons $\mathcal{O}_{K_{\mathcal{P}}}$ l'anneau de valuation de $K_{\mathcal{P}}$. Nous savons (voir [Nar04] corollaire 3, p. 223) qu'il existe une extension intermédiaire L ($\mathbb{Q}_p \subset L \subset K_{\mathcal{P}}$) telle que $L/\mathbb{Q}_p$ est non ramifiée et $K_{\mathcal{P}}/L$ est totalement ramifiée. Soit $\mathcal{O}_L$ l'anneau de valuation de L. Remarquons que $p\mathcal{O}_L$ est l'idéal maximal de $\mathcal{O}_L$ et que $p\mathcal{O}_{K_{\mathcal{P}}} = \mathcal{P}^e$. De plus $\mathcal{O}_L/p\mathcal{O}_L \cong \mathbb{F}_{p^f} \cong \mathcal{O}_{K_{\mathcal{P}}}/\mathcal{P}$, où $f = [L : \mathbb{Q}_p] = f(\mathcal{P}, p)$ est le degré résiduel de $\mathcal{P}$ sur p. Soit $\alpha \in \mathcal{O}_{K_{\mathcal{P}}}$ tel que $\mathcal{O}_{K_{\mathcal{P}}} = \mathcal{O}_L[\alpha]$. Il vient

$$\mathcal{O}_{K_{\mathcal{P}}}/\mathcal{P}^e \cong \mathcal{O}_L[\alpha]/p\mathcal{O}_L[\alpha] \cong (\mathcal{O}_L/p)[X]/\overline{m_\alpha(X)}$$

où $\overline{m_\alpha(X)}$ désigne la classe dans $\mathcal{O}_L/p$ du polynôme minimal m_α de α sur $\mathcal{O}_L$.

Supposons maintenant que $\overline{m_\alpha(X)}$ n'est pas scindé. Alors il existe un entier $n > 1$ et une surjection de $\mathcal{O}_K/\mathcal{P}^e$ sur $\mathbb{F}_{p^{nf}}$. Ainsi $\mathbb{F}_{p^{nf}}$ est un quotient de $\mathcal{O}_{K_\mathcal{P}}$ ce qui est absurde car $\mathcal{P}$ est l'unique idéal maximal de $\mathcal{O}_{K_\mathcal{P}}$ et $\mathcal{O}_{K_\mathcal{P}}/\mathcal{P} \cong \mathbb{F}_{p^f}$. Donc

$$(\mathcal{O}_L/p)[X]/\overline{m_\alpha(X)} \cong (O_L/p)[X]/X^e$$

puisque m_α est de degré $e = [K_\mathcal{P} : L]$. Finalement, il vient

$$\mathcal{O}_K/\mathcal{P}^e \cong \mathcal{O}_{K_\mathcal{P}}/\mathcal{P}^e \cong (\mathcal{O}_L/p)[X]/X^e \cong$$
$$\cong (\mathcal{O}_{K_\mathcal{P}}/\mathcal{P})[X]/X^e \cong (\mathcal{O}_K/\mathcal{P})[X]/X^e$$

ce qui termine la preuve.

□

Proposition 3.3.6. *Soient K un corps de nombres et $A = (-1,-1)_K$ un corps de quaternions. Le degré résiduel de $\mathcal{P}$ est pair pour tout premier $\mathcal{P}$ au-dessus de 2 si et seulement s'il existe $s \in \mathcal{O}_K$ tel que $s^2 + s + 1 \in 2\mathcal{O}_K$. Dans ce cas,*

$$\Lambda = \mathcal{O}_K \oplus i\mathcal{O}_K \oplus \frac{s + (s+1)i + j}{2}\mathcal{O}_K \oplus \frac{1 + i + j + k}{2}\mathcal{O}_K$$

est un ordre maximal de A, et A est non ramifiée aux places finies.

Preuve :

Ecrivons $2\mathcal{O}_K = \mathcal{P}_1^{e_1} \dots \mathcal{P}_r^{e_r}$ et supposons que $f_i = [\mathcal{O}_K/\mathcal{P}_i : \mathbb{F}_2]$ est pair pour tout $1 \leq i \leq r$. Le lemme précédent nous dit que $R = \mathcal{O}_K/2\mathcal{O}_K$ est un produit cartésien de $\mathbb{F}_4$-espaces vectoriels, donc il existe $s \in R$ avec $s^2 + s + 1 \in 2\mathcal{O}_K$, car $X^2 + X + 1$ est réductible dans $\mathbb{F}_4[X]$.

Inversément, supposons $f(\mathcal{P})$ impair. L'anneau $R = \mathcal{O}_K/2\mathcal{O}_K$ contient

$$S = \mathcal{O}_K/\mathcal{P}^e\mathcal{O}_K \cong (\mathcal{O}_K/\mathcal{P})[X]/X^e \cong \mathbb{F}_{p^f}[X]/X^e$$

vu le lemme précédent. Or $Y^2 + Y + 1$ est irréductible dans $S[Y]$. En effet, si x désigne la classe de X dans S et que $a_0 + a_1x + \dots + a_{e-1}x^{e-1}$ est une racine de $Y^2 + Y + 1$, alors $a_0^2 + a_0 + 1 = 0$. Ce qui est impossible car $Y^2 + Y + 1$ est irréductible sur $\mathbb{F}_{2^f}$ (puisque f est impair).

Il est facile de vérifier que Λ est un anneau (avec la condition $s^2 + s + 1 \in 2\mathcal{O}_K$) et que son discriminant est $\mathcal{O}_K$. Cela prouve que Λ est un ordre maximal de A et que A n'est pas ramifiée aux places finies.

□

Proposition 3.3.7. *Soient K un corps de nombres et $A = (-1,-1)_K$ une algèbre de quaternions. On suppose que $2\mathcal{O}_K = \mathcal{P}_1^{2e_1} \cdots \mathcal{P}_r^{2e_r}$ et on pose $I = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}$. Alors A est non ramifiée aux places finies. De plus, si I est principal, alors*

$$\Lambda = \mathcal{O}_K + \frac{1+i}{2}I + \frac{1+j}{2}I + \frac{1+i+j+k}{2}\mathcal{O}_K$$

est un ordre maximal de A.

PREUVE : Comme $e(\mathcal{P})$ est pair pour tout premier dyadique $\mathcal{P}$, A est non ramifiée aux places finies (voir la proposition 3.3.4). Pour montrer que Λ est un ordre, il suffit de vérifier la stabilité pour la multiplication, ce qui est facile. Soit $\mathrm{D}(\Lambda/\mathcal{O}_K)$ le discriminant de Λ. Par définition,

$$\mathrm{D}(\Lambda/\mathcal{O}_K) = \langle \det(\mathrm{tr}(x_i x_j)_{1\leq i,j\leq 4}) \mid \ x_1, \ldots, x_4 \in \Lambda \rangle.$$

Il existe $\alpha, \beta \in I$ tels que $\alpha\beta = 2$ (car I est principal). Posons $x_1 = 1$, $x_2 = \alpha\frac{1+i}{2}$, $x_3 = \beta\frac{1+j}{2}$, $x_3 = \frac{1+i+j+k}{2}$. Nous pouvons alors vérifier que $\det(\mathrm{tr}((x_i x_j)_{1\leq i,j\leq 4}) = 1$. Ainsi, $1 \in \mathrm{D}(\Lambda/\mathcal{O}_K)$ et donc $\mathrm{D}(\Lambda/\mathcal{O}_K) = \mathcal{O}_K$, ce qui démontre que Λ est un ordre maximal.

□

Proposition 3.3.8. *Soient K un corps de nombres et $A = (-1,-1)_K$ une algèbre de quaternions. On suppose que $e(\mathcal{P})$ et $f(\mathcal{P})$ sont impairs pour tout premier dyadique $\mathcal{P}$, alors*

$$\Lambda = \mathcal{O}_K \oplus i\mathcal{O}_K \oplus j\mathcal{O}_K \oplus \frac{1+i+j+k}{2}\mathcal{O}_K$$

est un ordre maximal de A, et A est ramifié en $\mathcal{P}$ pour tout premier dyadique $\mathcal{P}$.

PREUVE : La proposition 3.3.4 nous assure que tout premier dyadique ramifie dans A. Il suffit alors de vérifier que Λ est un ordre et que son discriminant est $4\mathcal{O}_K$.

□

3.4 Borne supérieure du minimum euclidien dans le cas totalement indéfini

Nous avons déterminé, dans le chapitre II, une borne supérieure du minimum euclidien d'un ordre maximal dans une algèbre à division sur un corps

de nombres. Dans le cas particulier des corps de quaternions totalement indéfinis (c'est-à-dire non ramifiés aux places infinies réelles), on peut comparer le minimum euclidien d'un ordre maximal à celui de K (à condition que K soit principal). C'est le but de cette section.

Dans cette section, A est un corps de quaternions totalement indéfini sur un corps de nombres K et Λ est un ordre maximal de A.

Proposition 3.4.1. *Soient A un corps de quaternions totalement indéfini sur un corps de nombres K. Notons h_K le nombre de classes d'idéaux de K et h_A le nombre de classes d'idéaux à gauche (ou à droite) de n'importe quel ordre maximal de A. On a*

$$h_A = h_K.$$

PREUVE : Le théorème d'Hasse-Schilling-Mass (voir [Rei03] théorème 33.15, p.289) nous dit que $\alpha \in K^\times$ est la norme réduite d'un élément de A, si et seulement si $\sigma(\alpha) > 0$ pour toute place réelle σ ramifiée dans A. Dans notre cas, cette condition est toujours vérifiée (car $\mathrm{Ram}_\infty(A)$ est vide), donc la norme réduite est surjective.

Le premier point du corollaire 5.7, p.89 de [Vig80] nous dit que $h_A = h$ où h est le nombre de classes d'idéaux de K au sens restreint (c'est-à-dire $h = |I(K)/\sim|$ où $I(K)$ est le groupe des idéaux de K et $I \sim J$ si IJ^{-1} est un idéal principal de K admettant un générateur dans $\mathrm{nr}_{A/K}(A)$). Dans notre cas, comme $\mathrm{nr}_{A/K}$ est surjective, on a $h = h_K$.

□

Lemme 3.4.2. *Soient R un anneau et I un idéal à droite de R. Soient a, $b \in R$ tels que bR et I sont premiers entre eux (c'est-à-dire $bR + I = R$). Alors les ensembles*

$$\mathcal{I}_1 = \{x \in R \mid a - bx \in I\} \quad \text{et} \quad \mathcal{I}_2 = \{x \in R \mid a - bx \notin I\}$$

sont non vides.

PREUVE : Il existe $x \in R$ tel que $a - bx \in I$ (car b et I sont premiers entre eux), ce qui prouve que $\mathcal{I}_1$ est non vide. Considérons maintenant $x \in \mathcal{I}_1$ et $z = x + 1$. Supposons que $a - bz \in I$, alors $b = (a - bx) - (a - bz) \in I$, ce qui est absurde puisque bR et I sont premiers entre eux. Cela montre que $\mathcal{I}_2$ est non vide.

□

Lemme 3.4.3. *Soient R un anneau, a, $b \in R$ et $I_1, \ldots, I_n$ des idéaux à droite de R tels que bR et I_i sont premiers entre eux pour tout $1 \leq i \leq n$. Alors l'ensemble*

$$\mathcal{I} = \{x \in R \mid a - bx \notin \cup_{i=1}^{n} I_i\}$$

est non vide.

Preuve : Considérons l'idéal $J = \cap_{i=1}^{n} I_i$. Remarquons d'abord que l'idéal J est premier à bR. En effet, $bR + I_i = R$ pour tout $1 \leq i \leq n$, donc

$$R = \bigcap_{i=1}^{n} (bR + I_i) \subset bR + \bigcap_{i=1}^{n} I_i = bR + J.$$

Par le lemme précédent, il existe donc $x \in R$ tel que $a - bx \in I_i$, pour tout $1 \leq i \leq n$ de sorte que $a - b(x+1) \notin I_i$ pour tout $1 \leq i \leq n$ (car sinon $b = (a - bx) - (a - b(x+1)) \in I_i$).

□

Corollaire 3.4.4. *Soient R un anneau principal à droite, a, $b \in R$ sans diviseur commun à gauche et $I_1 = c_1R, \ldots, I_n = c_nR$ des idéaux de R tels que pour tout $1 \leq i \leq n$, soit $b \in I_i$, soit bR et I_i sont premiers entre eux. Alors*

$$\mathcal{I} = \{x \in R \mid a - bx \notin \cup_{i=1}^{n} I_i\}$$

est non vide.

Preuve : Supposons que $b \in I_i$. Alors $a - bx \notin I_i$ pour tout $x \in R$. En effet, si $a - bx \in I_i$, alors $a \in I_i = c_iR$, donc il existe r et $s \in R$ tels que $a = c_ir$ et $b = c_is$, ce qui contredit le fait que a et b n'ont pas de diviseur commun à gauche. Les idéaux I_i tels que $b \in I_i$ n'interviennent donc pas ; il suffit alors d'appliquer le lemme précédent.

□

Nous pouvons également énoncer ce résultat dans le cas d'un anneau non principal. Dans ce cas il faut ajouter une hypothèse sur A.

Corollaire 3.4.5. *Soient R un anneau, a, $b \in R$ et $I_1, \ldots, I_n$ des idéaux de R tels que pour tout $1 \leq i \leq n$, soit $b \in I_i$ et $a \notin I_i$, soit bR et I_i sont premiers entre eux. Alors*

$$\mathcal{I} = \{x \in R \mid a - bx \notin \cup_{i=1}^{n} I_i\}$$

est non vide.

PREUVE : Supposons que $b \in I_i$. Alors $a - bx \notin I_i$ pour tout $x \in R$. En effet, si $a - bx \in I_i$, alors $a \in I_i$, ce qui est absurde. Les idéaux I_i tels que $b \in I_i$ n'interviennent donc pas ; il suffit alors d'appliquer le lemme 3.4.3.
□

Proposition 3.4.6. *Soient Λ un ordre maximal principal d'un corps de quaternions A et x un élément de A. Alors il existe $a, b, c \in \Lambda$ tels que $x = b^{-1}a + c$, et $\mathrm{nr}_{A/K}(a)$ et $\mathrm{nr}_{A/K}(b)$ sont premiers entre eux.*

PREUVE : Nous savons qu'il existe $u, b \in \Lambda$ tels que $x = b^{-1}u$. Remarquons d'abord qu'on peut supposer que u et b n'ont pas de diviseur commun à gauche. En effet, si $u = ru'$ et $b = rb'$, alors $x = b^{-1}u = b'^{-1}r^{-1}ru' = b'^{-1}u'$. Posons $max = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_n\}$ l'ensemble des idéaux maximaux à droite de Λ, qui contiennent $\mathrm{nr}_{A/K}(b)\Lambda$. Comme les $\mathfrak{m}_i$ sont maximaux, nous avons soit $b\Lambda + \mathfrak{m}_i = \Lambda$, soit $b \in \mathfrak{m}_i$. Par le corollaire précédent, il existe donc $c \in \Lambda$ tel que

$$u - bc \notin \mathfrak{m} \text{ pour tout } \mathfrak{m} \in max. \tag{III.1}$$

Supposons que $\mathrm{nr}_{A/K}(b)$ et $\mathrm{nr}_{A/K}(u - bc)$ ne sont pas premiers entre eux. Alors il existe un idéal premier bilatère β de Λ tel que

$$\mathrm{nr}_{A/K}(b)\Lambda, \mathrm{nr}_{A/K}(u - bc)\Lambda \subset \beta.$$

Notons que l'ensemble des idéaux maximaux à droite au-dessus de β est contenu dans max. Nous pouvons décomposer $\mathrm{nr}_{A/K}(u - bc)\Lambda$ en produit d'idéaux premiers :

$$\mathrm{nr}_{A/K}(u - bc)\Lambda = \beta^e \beta_1^{e_1} \cdots \beta_r^{e_r}$$

pour des idéaux premiers bilatères $\beta_1, \ldots, \beta_r$. Soient

$$I = (u - bc)\Lambda \quad \text{et} \quad maxI = \{\mathfrak{M}_1, \ldots, \mathfrak{M}_s\}$$

l'ensemble des idéaux maximaux à droite de Λ contenant I. Posons

$$\Gamma_i = \mathrm{ann}_\Lambda \mathfrak{M}_i = \{x \in \Lambda \mid \Lambda x \subset \mathfrak{M}_i\}$$

l'unique idéal premier bilatère contenu dans $\mathfrak{M}_i$ (voir [Rei03] théorème 22.15, p.195). Comme $\mathrm{nr}_{A/K}(u - bc)\Lambda$ est bilatère et contenu dans $\mathfrak{M}_i$ pour tout i,

$$\mathrm{nr}_{A/K}(u - bc)\Lambda \subset \bigcap_{i=1}^{s} \Gamma_i.$$

Sans perte de généralité, il est donc possible de supposer que $\Gamma_1 = \beta$, et comme $\beta = \Gamma_1 \subset \mathfrak{M}_1$, il existe $1 \leq i \leq n$ tel que $\mathfrak{M}_1 = \mathfrak{m}_i$, ce qui est en contradiction avec III.1 puisque

$$u - bc \in \mathfrak{M}_1 = \mathfrak{m}_i \quad \text{et} \quad \mathfrak{m}_\mathrm{i} \supset \mathrm{nr}_{A/K}(b)\Lambda.$$

Nous avons donc démontré que $\mathrm{nr}_{A/K}(u - bc)$ et $\mathrm{nr}_{A/K}(b)$ sont premiers entre eux. Pour terminer, posons $a = u - bc$. Alors

$$b^{-1}a + c = b^{-1}u - c + c = x$$

ce qui est le résultat annoncé.

□

Nous pouvons aussi énoncer ce résultat pour certains éléments de A, lorsque Λ n'est pas principal.

Proposition 3.4.7. *Soient Λ un ordre maximal d'un corps de quaternions A et $a, b \in \Lambda$. Soit max l'ensemble des idéaux maximaux à droite de Λ qui contiennent $\mathrm{nr}_{A/K}(b)\Lambda$. Supposons que si $\mathfrak{m} \in max$ et si $b \in max$, alors $a \notin max$. Posons $x = b^{-1}a$. Alors il existe $u, v, c \in \Lambda$ tels que $x = u^{-1}v + c$, et $\mathrm{nr}_{A/K}(u)$ et $\mathrm{nr}_{A/K}(v)$ sont premiers entre eux.*

Preuve : Il suffit de reprendre la preuve de la proposition précédente en utilisant le corollaire 3.4.5 à la place du corollaire 3.4.4.

Il nous reste deux lemmes à énoncer avant de passer au résultat principal de cette section. Le premier concerne le lien entre la norme réduite d'un idéal I et l'intersection de I avec $\mathcal{O}_K$. Le second donne certaines propriétés en relation avec l'additivité de la norme.

Lemme 3.4.8. *Soient A une algèbre de quaternions sur un corps de nombres K, Λ un ordre maximal de A et I un idéal entier à droite de Λ. Posons*

$$I \cap \mathcal{O}_K = \mathcal{P}_1^{f_1} \cdots \mathcal{P}_r^{f_r}$$

où les $\mathcal{P}_i$ sont des idéaux premiers de $\mathcal{O}_K$ et les f_i des entiers strictement positifs, alors il existe r entiers e_i avec $f_i \leq e_i$, tels que

$$\mathrm{nr}_{A/K}(I) = \mathcal{P}_1^{e_1} \cdots \mathcal{P}_r^{e_r}.$$

Preuve : Il existe des idéaux entiers maximaux $\mathfrak{m}_{i,i+1}$ tels que

$$I = \mathfrak{m}_{12}\mathfrak{m}_{23} \cdots \mathfrak{m}_{n-2,n-1}\mathfrak{m}_{n-1,n}$$

et

$$\Lambda_1 = \mathcal{O}_l(\mathfrak{m}_{12}) = \mathcal{O}_l(I), \quad \mathcal{O}_r(\mathfrak{m}_{n-1,n}) = \mathcal{O}_r(I) = \Lambda,$$
$$\mathcal{O}_r(\mathfrak{m}_{i,i+1}) = \mathcal{O}_l(\mathfrak{m}_{i+1,i+2}) = \Lambda_{i+1}$$

(voir [Rei03] théorème 22.18 et suivants, p.196). Posons $\mathcal{P}_i = \mathfrak{m}_{i,i+1} \cap \mathcal{O}_K$ (les $\mathcal{P}_i$ ne sont pas nécessairement distincts). Alors

$$\mathcal{P}_1 \cdots \mathcal{P}_{n-1} \subset I \cap \mathcal{O}_K \subset \mathcal{P}_i$$

pour tout $1 \leq i \leq n-1$. Autrement dit, chaque $\mathcal{P}_i$ apparaît dans la décomposition de $I \cap \mathcal{O}_K$. D'autre part,

$$\mathrm{nr}_{A/K}(I) = \mathrm{nr}_{A/K}(\mathfrak{m}_{12}) \cdots \mathrm{nr}_{A/K}(\mathfrak{m}_{n-1,n}) = \mathcal{P}_1 \cdots \mathcal{P}_{n-1}$$

ce qui prouve que les premiers apparaissant dans les décompositions de $I \cap \mathcal{O}_K$ et de $\mathrm{nr}_{A/K}(I)$ coïncident. Soit $x \in I$. Comme $x \in \Lambda$, $x^\gamma \in \Lambda$, donc $\mathrm{nr}_{A/K}(x) = xx^\gamma \in I$, de sorte que $\mathrm{nr}_{A/K}(I) \subset I \cap \mathcal{O}_K$, ce qui prouve que $f_i \leq e_i$.

□

Remarque : Des calculs explicites permettent de voir que $e_i \leq 2f_i$ et de déterminer complétement les f_i, en fonction des e_i, si I est bilatère. Si $\mathfrak{m}$ est un idéal maximal de Λ, alors $\mathrm{nr}_{A/K}(\mathfrak{m}) = \mathfrak{m} \cap \mathcal{O}_K$ (autrement dit $e_i = f_i$ pour tout $1 \leq i \leq r$).

Lemme 3.4.9. *Soient A un corps de quaternions totalement indéfini sur un corps de nombres K, Λ un ordre maximal de A, $x \in \Lambda$ et I un idéal bilatère de Λ. On suppose que $\mathrm{nr}_{A/K}(x)$ et $\mathrm{nr}_{A/K}(I)$ sont premiers entre eux. Alors*

$$\mathrm{nr}_{A/K}(x + I) = \mathrm{nr}_{A/K}(x) + I \cap \mathcal{O}_K.$$

Preuve : Voir proposition 5.8, p.90 de [Vig80].

Nous pouvons maintenant énoncer le résultat important de la section.

Théorème 3.4.10. *Soient A un corps de quaternions totalement indéfini sur un corps de nombres principal K et Λ un ordre maximal de A. Soit $\xi' = b^{-1}a - c \in A$ (où $a, b, c \in \Lambda$ sont comme dans la proposition 3.4.6). Posons $\xi = b^{-1}a$. Alors*

$$m_\Lambda(\xi') = m_\Lambda(\xi) \leq m_K(\mathrm{nr}_{A/K}(b^{-1}a)).$$

En particulier,

$$\mathrm{M}(A) \leq \mathrm{M}(K).$$

Si, de plus, $b\Lambda$ est bilatère alors

$$C_b \cdot m_K\left(\frac{\mathrm{nr}_{A/K}(a)}{t_b}\right) \leq m_\Lambda(\xi') = m_\Lambda(\xi)$$

où t_b est un générateur de $b\Lambda \cap \mathcal{O}_K$ et $C_b = \left|\mathrm{N}_{K/\mathbb{Q}}\left(\frac{\mathrm{nr}_{A/K}(b)}{t_b}\right)\right|^{-1}$.

PREUVE : Nous savons que $m_\Lambda(x) = m_\Lambda(x-c)$ pour tout $x \in A$ et tout $c \in \Lambda$ (voir la proposition 2.2.2). Nous avons donc bien $m_\Lambda(\xi') = m_\Lambda(\xi)$. Nous allons d'abord démontrer la seconde inégalité. Nous pouvons donc supposer que $b\Lambda$ est bilatère. Soit $\gamma \in \Lambda$ tel que

$$m_\Lambda(\xi) = |\mathrm{nr}_{A/\mathbb{Q}}(\xi - \gamma)|.$$

Par le lemme précédent,

$$\mathrm{nr}_{A/K}(a - b\gamma) \in \mathrm{nr}_{A/K}(a) - b\Lambda \cap \mathcal{O}_K = \mathrm{nr}_{A/K}(a) - t_b\mathcal{O}_K$$

de sorte qu'il existe $v \in \mathcal{O}_K$ avec

$$\mathrm{nr}_{A/K}(a - b\gamma) = \mathrm{nr}_{A/K}(a) - t_b v.$$

Calculons $m_\Lambda(\xi)$:

$$\begin{aligned} m_\Lambda(\xi) &= |\mathrm{nr}_{A/\mathbb{Q}}(b^{-1})| \cdot |\mathrm{nr}_{A/\mathbb{Q}}(a - b\gamma)| \\ &= |\mathrm{N}_{K/\mathbb{Q}}(\mathrm{nr}_{A/K}(b^{-1})t_b t_b^{-1})| \cdot |\mathrm{N}_{K/\mathbb{Q}}(\mathrm{nr}_{A/K}(a) - t_b v)| \\ &= |\mathrm{N}_{K/\mathbb{Q}}(\mathrm{nr}_{A/K}(b^{-1})t_b)| \cdot |\mathrm{N}_{K/\mathbb{Q}}(t_b^{-1}\mathrm{nr}_{A/K}(a) - v)| \\ &\geq C_b \cdot m_K(t_b^{-1}\mathrm{nr}_{A/K}(a)). \end{aligned}$$

Cela prouve la seconde inégalité. Montrons maintenant que

$$m_\Lambda(\xi) \leq m_K(\mathrm{nr}_{A/K}(\xi)).$$

Soit $u \in \mathcal{O}_K$ tel que

$$m_K(\mathrm{nr}_{A/K}(\xi)) = |\mathrm{N}_{K/\mathbb{Q}}(\mathrm{nr}_{A/K}(\xi) - u)|.$$

Nous avons,

$$\mathrm{nr}_{A/K}(a) - \mathrm{nr}_{A/K}(b)u \in \mathrm{nr}_{A/K}(a) - \mathrm{nr}_{A/K}(b)\mathcal{O}_K \subset$$

$$\subset \mathrm{nr}_{A/K}(a) - \mathrm{nr}_{A/K}(b)\Lambda \cap \mathcal{O}_K.$$

Comme $\mathrm{nr}_{A/K}(a)$ et $\mathrm{nr}_{A/K}(b)^2$ sont premiers entre eux et que $\mathrm{nr}_{A/K}(b)\Lambda$ est bilatère, le lemme précédent nous dit que

$$\mathrm{nr}_{A/K}(a) - \mathrm{nr}_{A/K}(b)\Lambda \cap \mathcal{O}_K = \mathrm{nr}_{A/K}(a - \mathrm{nr}_{A/K}(b)\Lambda).$$

Donc il existe $\gamma \in \Lambda$ tel que

$$\mathrm{nr}_{A/K}(a) - \mathrm{nr}_{A/K}(b)u = \mathrm{nr}_{A/K}(a - \mathrm{nr}_{A/K}(b)\gamma).$$

Nous pouvons maintenant borner $m_K(\mathrm{nr}_{A/K}(\xi))$:

$$\begin{aligned} m_K(\mathrm{nr}_{A/K}(\xi)) &= |\mathrm{N}_{K/\mathbb{Q}}(\mathrm{nr}_{A/K}(\xi) - u)| \\ &= |\mathrm{nr}_{A/\mathbb{Q}}(b^{-1})| \cdot |\mathrm{N}_{K/\mathbb{Q}}(\mathrm{nr}_{A/K}(a) - \mathrm{nr}_{A/K}(b)u)| \\ &= |\mathrm{nr}_{A/\mathbb{Q}}(b^{-1})| \cdot |\mathrm{N}_{K/\mathbb{Q}}(\mathrm{nr}_{A/K}(a - \mathrm{nr}_{A/K}(b)\gamma))| \\ &= |\mathrm{nr}_{A/\mathbb{Q}}(b^{-1})| \cdot |\mathrm{nr}_{A/\mathbb{Q}}(a - b\bar{b}\gamma)| \\ &= |\mathrm{nr}_{A/\mathbb{Q}}(\xi - \bar{b}\gamma)| \\ &\geq m_\Lambda(\xi). \end{aligned}$$

Nous avons donc démontré que

$$m_\Lambda(\xi) \leq m_K(\mathrm{nr}_{A/K}(\xi)).$$

Comme la norme réduite est surjective,

$$\mathrm{M}(A) = \sup\{m_\Lambda(\xi) \mid \xi \in A\} \leq \sup\{m_K(\mathrm{nr}_{A/K}(\xi)) \mid \xi \in A\} = \mathrm{M}(K)$$

ce qui prouve la dernière affirmation du théorème.

□

Ce théorème a des conséquences importantes pour la classification des corps de quaternions euclidiens (voir les sections 3.5, 3.11 et 3.13).

Remarquons que l'hypothèse de principalité sur Λ n'est nécessaire que dans l'utilisation de la proposition 3.4.6 qui nous dit que pour tout $\xi \in A$, il existe $a, b, c \in \Lambda$ avec $(\mathrm{nr}_{A/K}(b), \mathrm{nr}_{A/K}(a)) = 1$ et $\xi = b^{-1}a + c$. Nous pouvons donc énoncer le théorème suivant.

Théorème 3.4.11. *Soient A un corps de quaternions totalement indéfini sur un corps de nombres K et Λ un ordre maximal de A. Soient $a, b \in \Lambda$ tels que $(\mathrm{nr}_{A/K}(a), \mathrm{nr}_{A/K}(b)) = 1$. Alors*

$$m_\Lambda(\xi) \leq m_K(\mathrm{nr}_{A/K}(\xi)).$$

Si, de plus, $b\Lambda \cap \mathcal{O}_K$ est principal et $b\Lambda$ est bilatère, alors

$$C_b \cdot m_K\left(\frac{\mathrm{nr}_{A/K}(a)}{t_b}\right) \leq m_\Lambda(\xi)$$

où t_b est un générateur de $b\Lambda \cap \mathcal{O}_K$ et $C_b = \left|\mathrm{N}_{K/\mathbb{Q}}\left(\frac{\mathrm{nr}_{A/K}(b)}{t_b}\right)\right|^{-1}$.
En particulier :
Supposons que $\mathrm{M}(K)$ est atteint et posons

$$S(K) = \{x \in K \mid \mathrm{M}(K) = m_K(x)\}.$$

S'il existe $\xi = b^{-1}a \in A$ *avec* $a, b \in \Lambda$ *comme ci dessus tels que*

$$C_b = 1 \quad et \quad \mathrm{nr}_{A/K}(\xi) \in S(K)$$

alors

$$\mathrm{M}(\Lambda) \geq \mathrm{M}(K).$$

Preuve : Pour la première partie le procédé est le même que dans le théorème précédent. Si les hypothèses de la seconde partie sont vérifiées, alors

$$m_\Lambda(\xi) = m_K(\mathrm{nr}_{A/K}(\xi)) = \mathrm{M}(K).$$

Nous avons donc

$$\begin{aligned}
\mathrm{M}(\Lambda) &= \sup\{m_\Lambda(x) \mid x \in A\} \\
&\geq \sup\{m_\Lambda(b^{-1}a) \mid a, b \in \Lambda \text{ et } (\mathrm{nr}_{A/K}(a), \mathrm{nr}_{A/K}(b)) = 1\} \\
&= \sup\{m_K(\mathrm{nr}_{A/K}(b^{-1}a)) \mid a, b \in \Lambda \text{ et } (\mathrm{nr}_{A/K}(a), \mathrm{nr}_{A/K}(b)) = 1\} \\
&= \sup\{m_K(x) \mid x \in K\} \\
&= \mathrm{M}(K).
\end{aligned}$$

□

3.5 Algèbres de quaternions sur $\mathbb{Q}$

Nous allons nous intéresser, dans cette section, au minimum euclidien des ordres maximaux sur des corps de quaternions sur $\mathbb{Q}$. Nous verrons qu'on peut alors calculer explicitement le minimum euclidien d'un ordre maximal.

Commençons par régler le cas des corps de quaternions indéfinis (c'est-à-dire non ramifiés à l'infini) sur $\mathbb{Q}$.

Proposition 3.5.1. *Soient* A *un corps de quaternions indéfini sur* $\mathbb{Q}$ *et* Λ *un ordre maximal de* A*, alors* Λ *est euclidien pour la norme réduite et*

$$\frac{1}{4} \leq \mathrm{M}(\Lambda) \leq \frac{1}{2}.$$

Si, de plus, 2 *est ramifié dans* A *alors* $\mathrm{M}(\Lambda) = \frac{1}{2}$

PREUVE : Posons $b = 2$ et $a = 1$. Avec les mêmes notations qu'au théorème 3.4.10, $t_b = \mathrm{nr}_{A/\mathbb{Q}}(b) = 4$ et $C_b = \frac{1}{2}$. De sorte que,

$$\frac{1}{2} m_K\left(\frac{1}{2}\right) \geq m_\Lambda(b^{-1}),$$

ce qui prouve que $\frac{1}{4} \leq \mathrm{M}(\Lambda)$. L'autre inégalité découle également directement du théorème 3.4.10, en effet, $\mathrm{M}(\Lambda) \leq \mathrm{M}(\mathbb{Q}) = \frac{1}{2}$.

Supposons maintenant que 2 est ramifié alors il existe un unique idéal premier bilatère $\mathfrak{P}$ tel que $\mathfrak{P}^2 = 2\Lambda$, de plus cet idéal est maximal (voir le lemme 3.12.6). Soit b un générateur de $\mathfrak{P}$. Comme $\mathfrak{P}$ est maximal, $\mathfrak{P} \cap \mathbb{Z} = 2\mathbb{Z}$ et $\mathrm{nr}_{A/\mathbb{Q}}(\mathfrak{P}) = 2\mathbb{Z}$. Nous pouvons donc supposer $\mathrm{nr}_{A/\mathbb{Q}}(b) = t_b = 2$ et donc $C_b = 1$. Posons $a = 1$. Le théorème 3.4.10 nous dit alors que

$$m_K\left(\frac{1}{2}\right) \leq m_\Lambda(b^{-1}) \leq m_K\left(\frac{1}{2}\right).$$

Autrement dit $m_\Lambda(b^{-1}) = \frac{1}{2}$. De sorte que $\mathrm{M}(\Lambda) \geq \frac{1}{2}$. L'inégalité inverse étant toujours vraie, le théorème est démontré.

□

Nous pouvons maintenant nous intéresser au cas des corps de quaternions définis sur $\mathbb{Q}$.

Proposition 3.5.2. *Soient $A = (a, b)_\mathbb{Q}$ un corps de quaternions défini (c'est-à-dire ramifié à l'infini) sur $\mathbb{Q}$, Λ un ordre maximal de A et $(\Lambda, 1)$ le réseau idéal trace sur Λ. Alors*

$$\mathrm{M}(\Lambda) = \frac{\max(\Lambda, 1)}{2}.$$

PREUVE : Remarquons tout d'abord que pour tout $x \in A$,

$$\mathrm{nr}_{A/\mathbb{Q}}(xx^\gamma) = \mathrm{nr}_{A/\mathbb{Q}}(x^2) = \left(\frac{\mathrm{tr}_{A/\mathbb{Q}}(xx^\gamma)}{2}\right)^2.$$

Nous pouvons ainsi calculer $\mathrm{M}(\Lambda)$:

$$\begin{aligned}
\mathrm{M}(\Lambda) &= \sup_{x \in A}\left(\inf_{c \in \Lambda} |\mathrm{nr}_{A/\mathbb{Q}}(x - c)|\right) \\
&= \sup_{x \in A}\left(\inf_{c \in \Lambda}\left|\frac{\mathrm{tr}_{A/\mathbb{Q}}((x-c)(x-c)^\gamma)}{2}\right|\right) \\
&= \frac{\max(\Lambda, 1)}{2}.
\end{aligned}$$

□

REMARQUE : L'hypothèse de ramification à l'infini est nécessaire. En effet, si A n'est pas ramifié à l'infini, alors $(\Lambda, 1, \gamma)$ ne forme pas un réseau idéal de A. Il faut donc choisir une involution orthogonale τ sur A pour former un réseau idéal. Avec un tel réseau idéal, il est facile de trouver des exemples où $\mathrm{nr}_{A/\mathbb{Q}}(x^2) \neq \left(\frac{\mathrm{tr}_{A/\mathbb{Q}}(xx^\tau)}{2}\right)^2$.

Cette proposition nous permet de calculer le minimum euclidien de n'importe quel ordre maximal d'un corps de quaternions A sur $\mathbb{Q}$ donné. Malheureusement, le nombre de classes d'ordres maximaux de A augmente, en moyenne, avec le nombre de places ramifiées de A. Il nous est donc impossible d'espérer donner explicitement le minimum euclidien des ordres maximaux de tous les corps de quaternions sur $\mathbb{Q}$.

En revanche, nous allons nous intéresser à certaines familles infinies de corps de quaternions pour lesquels nous pouvons exhiber au moins un ordre maximal.

Afin de calculer des minima euclidiens précis, nous allons étudier en détail certaines algèbres de quaternions sur $\mathbb{Q}$. C'est le but des sections suivantes.

3.6 Ordres maximaux des algèbres de quaternions sur $\mathbb{Q}$

Considérons le cas d'une algèbre de quaternions sur $\mathbb{Q}$ ramifiée à l'infini et aux places finies $\{p_1, \ldots, p_s\}$ (avec s impair). Une telle algèbre est unique à isomorphisme près (à condition de fixer l'ensemble des places ramifiées). Le résultat suivant donne une manière de représenter une telle algèbre ainsi qu'un ordre maximal.

Proposition 3.6.1. *Soit A une algèbre de quaternions sur $\mathbb{Q}$ ramifiée aux places $\mathrm{Ram}_f(A) = \{p_1, \ldots, p_s\}$ et à l'infini. Posons $d = p_1 \cdots p_s$ et soit $q \equiv 3 \mod 4$ un premier tel que $\left(\frac{-q}{p_i}\right) = -1$ pour tout $p_i > 2$. Alors*

$$A \cong (-q, -d)_{\mathbb{Q}}$$

et, si $c^2 \equiv -d \mod q$,

$$\Lambda = \mathbb{Z} \oplus \frac{1+i}{2}\mathbb{Z} \oplus \frac{-ci-k}{q}\mathbb{Z} \oplus \frac{-(1+i)(ci+k)}{2q}\mathbb{Z}$$

est un ordre maximal de $(-q,-d)_{\mathbb{Q}}$.

PREUVE : C'est une conséquence de la proposition 3.3.3.

□

Définition 3.6.2. *On appelle forme standard d'une algèbre de quaternions A, l'algèbre* $(-q,-d)_{\mathbb{Q}}$ *isomorphe à A où q et d sont définis dans la proposition précédente.*

En distinguant certains cas particuliers on peut obtenir un résultat encore plus précis.

Proposition 3.6.3. *Soit* $A = (-q,-d)_{\mathbb{Q}}$ *la forme standard d'une algèbre de quaternions. Supposons* $d \equiv 3 \mod 4$ *et choisissons un entier impair c tel que* $-d \equiv c^2 \mod q$. *Alors*

$$\Lambda = \mathbb{Z} \oplus \frac{1+i}{2}\mathbb{Z} \oplus \frac{-ci-k}{q}\mathbb{Z} \oplus \frac{-(1+i)(ci+k)}{2q}\mathbb{Z}$$

et

$$\Gamma = \mathbb{Z} \oplus i\mathbb{Z} \oplus \frac{1+j}{2}\mathbb{Z} \oplus \frac{ci+k}{2q}\mathbb{Z}$$

sont des ordres maximaux de A. De plus

$$I = 2\mathbb{Z} \oplus (1+i)\mathbb{Z} \oplus (1+j)\mathbb{Z} \oplus (\frac{1}{2} + \frac{c}{2q}i + \frac{1}{2}j + \frac{1}{2q}k)\mathbb{Z}$$

est un idéal entier maximal à gauche de Λ *et à droite de* Γ.
L'idéal I est principal si et seulement si les deux idéaux premiers (conjugués) au-dessus de q dans $K = \mathbb{Q}(\sqrt{-d})$ *sont principaux. Dans ce cas I est engendré par*

$$1 + \frac{y}{q}i - \frac{x}{q}k$$

où $x, y \in \mathbb{Z}$ *vérifient* $q = y^2 + dx^2$ *et* $cx + y \equiv 0 \mod q$.

PREUVE : Le fait que Λ et Γ sont des ordres maximaux de $(-q,-d)_{\mathbb{Q}}$ découle directement de la proposition 3.3.3. Il est facile de vérifier que $\Lambda I \subset I$ et $I\Gamma \subset I$. Comme Λ et Γ sont maximaux, nous avons même $\mathcal{O}_l(I) = \Lambda$ et $\mathcal{O}_r(I) = \Gamma$ ce qui prouve que I est un idéal à gauche de Λ et à droite de Γ. L'idéal I est propre, car il ne contient pas 1. Déterminons la norme réduite de I :

$$\mathrm{nr}(I) = \langle \mathrm{nr}(2), \mathrm{nr}(1+i), \mathrm{nr}(1+j), \mathrm{nr}(\frac{1}{2} + \frac{c}{2q}i + \frac{1}{2}j + \frac{1}{2q}k) \rangle =$$

$$\langle 4, 1-q, 1-d, \frac{c^2+d+qd+q}{4q} \rangle = 2\mathbb{Z}$$

En effet, les quatre générateurs sont pairs et $1-q$ n'est pas divisible par 4. Comme I est propre et que $\mathrm{nr}(I) = 2\mathbb{Z}$ est maximal, cela force I à être maximal dans Λ (et dans Γ). Pour que I soit principal il faut qu'il existe $z \in I$ tel que $\mathrm{nr}(z) = 2$ (-2 étant exclu à cause de la ramification à l'infini). Posons $z = 2x_0+(1+i)x_1+(1+j)x_2+(\frac{1}{2}+\frac{c}{2q}i+\frac{1}{2}j+\frac{1}{2q}k)x_3$ et nous calculons sa norme réduite. Pour simplifier, excluons manuellement les deux seuls cas pour lesquels $d \leq 7$ (c'est-à-dire $d = 3$ ou $d = 7$). Pour ces cas, le générateur proposé engendre bien I. Un calcul montre que $\mathrm{nr}(z) = 2$ si et seulement si $q - dx_2^2$ est un carré dans $\mathbb{Z}$, disons $y^2 = q - dx_2^2$. Nous déterminons ensuite, parmi les deux choix possibles de y, celui qui vérifie $cx + y \equiv 0 \mod q$, cela est toujours possible car $(cx+y)(cx-y) = c^2x^2-y^2 \equiv -dx^2-y^2 \equiv 0 \mod q$. Il suffit alors de vérifier que $1+\frac{y}{q}i-\frac{x}{q}k$ est bien un élément de I de norme 2 qui engendre I comme idéal à gauche de Λ. Pour compléter la démonstration de la proposition telle qu'elle est énoncée, il faut encore rappeler, d'une part que $q\mathcal{O}_K = Q\bar{Q}$ où $K = \mathbb{Q}(\sqrt{-d})$ car $-d$ est un résidu quadratique modulo q (voir [Sam67] paragraphe 5.4, proposition 1) et d'autre part que Q est principal si et seulement si l'équation de Pell ($q = x^2 + dy^2$) admet une solution entière.

□

Corollaire 3.6.4. *Soient Γ et Λ les ordres maximaux de la proposition précédente. Les minima euclidiens de Γ et Λ sont liés par la relation*

$$\frac{1}{4} \leq \frac{\mathrm{M}(\Lambda)}{\mathrm{M}(\Gamma)} \leq 4.$$

Preuve : Soit I l'idéal de la proposition précédente. Remarquons que $2 \in I$ et que $1 \in I^{-1}$. La proposition 2.4.5 nous dit alors que

$$\frac{1}{\mathrm{nr}_{A/\mathbb{Q}}(2)} \leq \frac{\mathrm{M}(\Lambda)}{\mathrm{M}(\Gamma)} \leq \mathrm{nr}_{A/\mathbb{Q}}(2).$$

□

Si Γ et Λ sont donnés, on peut calculer explicitement leur minimum euclidien (voir la proposition 3.5.2). Dans le cas de Γ on peut obtenir facilement une borne explicite du minimum euclidien. C'est l'objet de la proposition suivante.

Proposition 3.6.5. *Avec les hypothèses et notations de la proposition 3.6.3,*

$$\mathrm{M}(\Gamma) = \frac{(d+1)^2}{16d} + \frac{\max(\mathbb{Z}^2, b)}{2}$$

où b est la forme bilinéaire donnée par la matrice

$$\begin{pmatrix} 2q & c \\ c & \frac{c^2+d}{2q} \end{pmatrix}.$$

Preuve : Remarquons que le réseau idéal $(\Gamma, 1)$ est isomorphe à

$$(\mathbb{Z}^2 \oplus \mathbb{Z}^2, b_1 \oplus b_2)$$

où

$$b_1 = \begin{pmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{pmatrix} \quad \text{et} \quad b_2 = \begin{pmatrix} 2q & c \\ c & \frac{c^2+d}{2q} \end{pmatrix}$$

de sorte que $\max(\Gamma, 1) = \max(\mathbb{Z}^2, b_1) + \max(\mathbb{Z}^2, b_2)$. Il est facile de vérifier que $\max(\mathbb{Z}^2, b_1) = \frac{(d+1)^2}{8d}$ (car la forme b_1 est réduite) et de conclure grâce à la proposition 3.5.2, qui nous dit que $\mathrm{M}(\Gamma) = \frac{\max(\Gamma,1)}{2}$.

□

Etudions maintenant le cas où $d \equiv 1 \mod 4$.

Proposition 3.6.6. *Soit $A = (-q, -d)_{\mathbb{Q}}$ la forme standard d'une algèbre de quaternions A'. Supposons $d \equiv 1 \mod 4$ et choisissons c impair tel que $-d \equiv c^2 \mod q$. Posons $l = 1$ si $c \equiv 3 \mod 4$ et $l = 3$ sinon. Alors*

$$\Lambda = \mathbb{Z} \oplus \frac{1+i}{2}\mathbb{Z} \oplus \frac{-ci-k}{q}\mathbb{Z} \oplus \frac{-(1+i)(ci+k)}{2q}\mathbb{Z}$$

et

$$\Gamma = \mathbb{Z} \oplus i\mathbb{Z} \oplus \frac{i+j}{2}\mathbb{Z} \oplus \frac{q+(a-c)i+k}{2q}\mathbb{Z}$$

sont des ordres maximaux. De plus

$$I = 2\mathbb{Z} \oplus (1+i)\mathbb{Z} \oplus (1+j)\mathbb{Z} \oplus (\frac{la+ci+qj+k}{2q})\mathbb{Z}$$

est un idéal entier maximal à droite de Λ et à gauche de Γ.

PREUVE : Nous procédons comme dans la preuve de 3.6.3. Autrement dit, nous vérifions d'abord que Λ et Γ sont bien des anneaux, que leur discriminant est $d^2\mathbb{Z}$, et que $\Gamma I = I$ et $I\Lambda = I$. Finalement nous nous assurons que $\mathrm{nr}_{A/\mathbb{Q}}(I) = 2\mathbb{Z}$.

□

Il semble plus difficile de déterminer, dans ce cas, à quelles conditions les ordres Γ et Λ sont dans la même classe de conjuguaison, c'est-à-dire quand I est principal. C'est au moins le cas si $d = 5$, comme nous le verrons à la fin de cette section.

Le problème de la représentation standard d'un corps de quaternions est, d'une part, qu'elle dépend de deux paramètres et, d'autre part, que les ordres maximaux proposés dépendent de deux ou trois paramètres. Le réseau idéal $(\Lambda, 1)$ associé à un de ces ordres dépend également de ces trois paramètres. Il est donc très difficile de calculer explicitement le maximum de $(\Lambda, 1)$ et par conséquent, nous ne pouvons pas donner explicitement le minimum euclidien de ces ordres.

En précisant les hypothèses sur la ramification de A, il est parfois possible de trouver des représentations plus simples de A, et surtout des ordres maximaux de A dont le réseau idéal associé ne dépend que d'un paramètre. Il devient alors raisonnable d'espérer calculer le maximum du réseau et donc de donner le minimum euclidien de l'ordre. C'est le but de la section suivante.

3.7 Minimum euclidien des corps de quaternions sur $\mathbb{Q}$: cas particuliers

Nous nous limitons aux corps de quaternions A définis, ramifiés en $\{p_1, \ldots, p_s\}$ (avec s impair), tel que $p_1 \equiv \cdots \equiv p_s \mod 4$.

Proposition 3.7.1. *Soit A une algèbre de quaternions sur $\mathbb{Q}$ ramifiée à l'infini et aux places finies $\mathrm{Ram}_f(A) = \{p_1, \ldots, p_s\}$ avec s impair, et soit $d = p_1 \cdots p_s$ le discriminant réduit de A. On a*

Si $d = 2$

$A \cong (-1,-1)_{\mathbb{Q}}$ et l'unique ordre maximal (à conjugaison près) est donné par

$$\Lambda_2 = \mathbb{Z} \oplus i\mathbb{Z} \oplus j\mathbb{Z} \oplus \frac{1+i+j+k}{2}\mathbb{Z}.$$

Si $p_i \equiv 3 \mod 4$ *pour tout* $1 \leq i \leq s$
$A \cong (-1,-d)_{\mathbb{Q}}$ *et un ordre maximal est donné par*

$$\Lambda_3 = \mathbb{Z} \oplus i\mathbb{Z} \oplus \frac{i+j}{2}\mathbb{Z} \oplus \frac{1+k}{2}\mathbb{Z}.$$

De plus, si $d \equiv 11 \mod 16$ *alors un autre ordre maximal (non conjugué à* Λ*) est donné par*

$$\Lambda_{16} = \mathbb{Z} \oplus \frac{1+2i+j}{2}\mathbb{Z} \oplus 2i\mathbb{Z} \oplus \frac{2-i-k}{4}\mathbb{Z}.$$

En particulier $h_A \geq 2$.

Si $p_i \equiv 5 \mod 8$ *pour tout* $1 \leq i \leq s$
$A \cong (-2,-d)_{\mathbb{Q}}$ *et un ordre maximal est donné par*

$$\Lambda_5 = \mathbb{Z} \oplus \frac{1+i+j}{2}\mathbb{Z} \oplus j\mathbb{Z} \oplus \frac{2+i+k}{4}\mathbb{Z}.$$

Si $p_i \equiv 1 \mod 8$ *et que* $p_i \equiv 2 \mod 3$ *pour tout* $1 \leq i \leq s$
$A \cong (-3,-d)_{\mathbb{Q}}$ *et un ordre maximal est donné par*

$$\Lambda_1 = \mathbb{Z} \oplus \frac{1+i}{2}\mathbb{Z} \oplus \frac{i+k}{3}\mathbb{Z} \oplus \frac{(1+i)(i+k)}{6}\mathbb{Z}.$$

PREUVE : Nous commençons par vérifier les isomorphismes annoncés. Si $d = 2$, alors 2 est l'unique place ramifiée de A et donc $A \cong (-1,-1)_{\mathbb{Q}}$ et l'ordre donné est bien un ordre maximal. Pour les autres cas rappelons d'abord le résultat suivant (voir, par exemple, [LJ] proposition 2.8, p.17) : Si p est un premier différent de 2, a, b des entiers tels que que p ne divise pas a, alors p est ramifié dans $(a,pb)_{\mathbb{Q}}$ si et seulement si a n'est pas un carré modulo p. De plus p n'est pas ramifié dans $(a,b)_{\mathbb{Q}}$ si p ne divise ni a ni b.

Soit $B = (-1,-d)_{\mathbb{Q}}$ où $d = p_1 \dots p_s$ est un produit de nombres premiers congrus à 3 modulo 4 et s est impair. Comme -1 n'est pas un carré modulo p_i pour tout $1 \leq i \leq s$, les seuls premiers impairs ramifiés sont $p_1, \dots, p_s$. Il est clair que A est ramifié à l'infini, de sorte que B ne peut être ramifié en 2 puisqu'il doit être ramifié en un nombre pair de places. Nous avons donc démontré que B est ramifié en l'infini et aux premiers $p_1, \dots, p_s$. Donc B est isomorphe à A.

Soit $B = (-2,-d)_{\mathbb{Q}}$ où $d = p_1 \dots p_s$ avec $p_i \equiv 5 \mod 8$, alors

$$\left(\frac{-2}{p_i}\right) = \left(\frac{-1}{p_i}\right)\left(\frac{2}{p_i}\right) = (-1)^{\frac{p_i^2-1}{8}} = -1,$$

donc les p_i sont ramifiés et ce sont les seuls premiers impairs ramifiés. Comme avant, B est ramifié à l'infini et ne peut donc pas être ramifié en 2 par parité

du nombre de places ramifiées.

Soit $B = (-3, -d)_{\mathbb{Q}}$ avec $d = p_1 \dots p_s$, où $p_i \equiv 1 \mod 8$ et $p_i \equiv 2 \mod 3$. Alors

$$\left(\frac{-3}{p_i}\right) = \left(\frac{3}{p_i}\right) = \left(\frac{p_i}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

donc les p_i sont ramifiés. Le seul premier impair qui peut ramifier (en dehors des p_i) est 3. Nous avons

$$\left(\frac{-d}{3}\right) = \left(\frac{-1}{3}\right) \prod_{i=1}^{s} \left(\frac{p_i}{3}\right) = -(-1)^s = 1$$

donc 3 n'est pas ramifié.

Comme deux algèbres de quaternions ramifiées aux mêmes places sont isomorphes, cela prouve les isomorphismes annoncés. Nous vérifions que les ordres proposés sont bien des anneaux et que leur discriminant est d^2, ce qui prouve que ce sont des ordres maximaux. La dernière chose à voir, c'est que les ordres Λ_3 et Λ_{16} du deuxième cas ne sont pas conjugués. Nous allons voir que les minima euclidiens de Λ_3 et Λ_{16} diffèrent (voir le corollaire 3.7.8). Or deux ordres conjugués ont le même minimum euclidien (voir la proposition 2.4.3), donc Λ_3 et Λ_{16} ne sont pas conjugués.

□

Cette proposition couvre les cas où A est ramifiée en une seule place finie p, à l'exception du cas $p \equiv 1 \mod 8$ qui n'est traité que partiellement.

Nous allons maintenant calculer le minimum euclidien de chacun de ces ordres maximaux. Pour cela nous devrons, à chaque fois, calculer le maximum du réseau $(\Lambda, 1)$.

Corollaire 3.7.2. *Soient $A = (-1, -1)_{\mathbb{Q}}$ et*

$$\Lambda_2 = \mathbb{Z} \oplus i\mathbb{Z} \oplus j\mathbb{Z} \oplus \frac{1+i+j+k}{2}\mathbb{Z}$$

comme ci-dessus. Alors

$$\mathrm{M}(\Lambda) = \frac{1}{2}.$$

En particulier Λ est euclidien pour la norme réduite.

PREUVE : Il suffit d'observer que le réseau $(\Lambda, 1)$ est isomorphe au réseau D_4 dont le maximum est 1. Le résultat vient alors du fait que $\mathrm{M}(\Lambda) = \frac{\max(\Lambda,1)}{2}$ (voir la proposition 3.5.2).

□

Corollaire 3.7.3. *Soient $d = p_1 \cdots p_s$ avec s impair et $p_i \equiv 3 \mod 4$ premiers pour tout $1 \leq i \leq s$, $A = (-1, -d)_{\mathbb{Q}}$ le corps de quaternions ramifié aux places p_i et à l'infini et*

$$\Lambda_3 = \mathbb{Z} \oplus i\mathbb{Z} \oplus \frac{i+j}{2}\mathbb{Z} \oplus \frac{1+k}{2}\mathbb{Z}$$

un ordre maximal de A. alors

$$\mathrm{M}(\Lambda_3) = \frac{(d+1)^2}{8d}.$$

PREUVE : Nous observons que le réseau $(\Lambda_3, 1)$ est isomorphe au réseau $L \oplus L$ où L est le réseau donné par la matrice de Gram suivante :

$$\begin{pmatrix} 2 & 1 \\ 1 & \frac{d+1}{2} \end{pmatrix}.$$

Il est facile de calculer $\max(L) = \frac{(d+1)^2}{8d}$ et donc $\max(\Lambda, 1) = \frac{(d+1)^2}{4d}$. La proposition 3.5.2 nous permet de conclure. En effet, $\mathrm{M}(\Lambda_3) = \frac{\max(\Lambda_3,1)}{2}$.

□

Jusqu'ici le calcul du maximum de $(\Lambda, 1)$ était très facile ; dans le premier cas parce que $(\Lambda_2, 1) \cong D_4$ est un réseau bien connu, et dans le second cas parce que $(\Lambda_3, 1)$ est décomposable. Les trois derniers cas, Λ_{16}, Λ_5 et Λ_1 sont beaucoup plus difficiles à traiter car les réseaux $(\Lambda_i, 1)$, pour $i \in \{1, 5, 16\}$, sont indécomposables.

Commençons par étudier le cas de Λ_5.

Dans ce cas, $d = p_1 \cdots p_s$ avec s impair et $p_i \equiv 5 \mod 8$ premier, $A = (-2, -d)_{\mathbb{Q}}$ est l'algèbre de quaternions sur $\mathbb{Q}$ ramifiée à l'infini et en p_i $(1 \leq i \leq s)$ et

$$\Lambda_5 = \mathbb{Z} \oplus \frac{1+i+j}{2}\mathbb{Z} \oplus j\mathbb{Z} \oplus \frac{2+i+k}{4}\mathbb{Z}$$

est un ordre maximal de A. Le calcul de la matrice de Gram du réseau $(\Lambda_5, 1)$ nous donne le résultat suivant :

$(\Lambda_5, 1) \cong (\mathbb{Z}^4, q)$ où q est le produit scalaire donné par la matrice

$$\begin{pmatrix} 2 & 1 & 0 & 1 \\ 1 & \frac{d+3}{2} & d & 1 \\ 0 & d & 2d & 0 \\ 1 & 1 & 0 & \frac{d+3}{4} \end{pmatrix}.$$

Pour calculer le minimum euclidien de Λ_5, il faut donc calculer le maximum du réseau (L, q). C'est l'objet de la proposition suivante.

Proposition 3.7.4. *Soit (L, q) où $L = \mathbb{Z}^4$, et où la forme bilinéaire q est donnée par la matrice*

$$\begin{pmatrix} 2 & 1 & 0 & 1 \\ 1 & \frac{d+3}{2} & d & 1 \\ 0 & d & 2d & 0 \\ 1 & 1 & 0 & \frac{d+3}{4} \end{pmatrix}.$$

d étant, soit un entier plus petit ou égal à 5, soit un nombre rationnel plus grand que 5. Alors le maximum du réseau (L, q) est donné par

$$\max(L, q) = \frac{3d^2 + 10d + 3}{16d}.$$

Preuve : Pour des raisons calculatoires, commençons par exclure les cas où $d \in \{1, 2, 3, 4\}$. Dans ces quatre cas, il est possible de calculer à la main (ou à l'ordinateur) la cellule de Voronoi du réseau et de constater que les sommets de cette cellule les plus éloignés de l'origine sont bien de norme $\frac{3d^2+10d+3}{16d}$. Nous pouvons donc supposer que $d > 5$.

Considérons maintenant l'ensemble suivant de 24 vecteurs du réseau :

$$P = \{p_1 = (1, -2, 1, 0), p_2 = (1, 0, 0, 0), p_3 = (0, 0, 0, 1),$$
$$p_4 = (0, 1, 0, 0), p_5 = (0, 1, -1, 0), p_6 = (1, -1, 0, 0),$$
$$p_7 = (0, 1, 0, -1), p_8 = (-1, 2, -1, 0), p_9 = (-1, 1, -1, 0),$$
$$p_{10} = (0, -2, 1, 1), p_{11} = (1, -2, 1, 1), p_{12} = (1, -1, 1, 0),$$
$$p_{13} = (1, 0, 0, -1), p_{14} = (0, 2, -1, -1), p_{15} = (0, -1, 0, 1),$$
$$p_{16} = (-1, 0, 0, 1), p_{17} = (-1, 0, 0, 0), p_{18} = (0, -1, 1, 1),$$
$$p_{19} = (0, 1, -1, -1), p_{20} = (0, 0, 0, -1), p_{21} = (0, -1, 0, 0),$$

$$p_{22} = (-1, 2, -1, -1)\,, p_{23} = (0, -1, 1, 0)\,, p_{24} = (-1, 1, 0, 0)\}\,.$$

Notons

$$\mathcal{V} = \left\{x \in \mathbb{R}^4 \mid q(x,x) \leq q(x-l, x-l) \text{ pour tout } l \in L\right\}$$

la cellule de Voronoi du réseau L, et

$$\mathcal{P} = \left\{x \in \mathbb{R}^4 \mid q(x,x) \leq q(x-p, x-p) \text{ pour tout } p \in P\right\}.$$

L'ensemble $\mathcal{P}$ est une partie de $\mathbb{R}^4$ contenant la cellule de Voronoi $\mathcal{V}$. Nous allons voir que $\mathcal{P}$ est convexe et bornée.

Notons $\delta\mathcal{P}$ le bord de $\mathcal{P}$; alors

$$\delta\mathcal{P} = \left\{x \in \mathbb{R}^4 \mid \text{il existe } p \in P \text{ avec } q(x,x) = q(x-p, x-p)\right\} =$$

$$\left\{x \in \mathbb{R}^4 \mid \text{il existe } p \in P \text{ avec } q(x,p) = \frac{q(p,p)}{2}\right\}$$

ce qui prouve la convexité de $\mathcal{P}$ car, pour p fixé, $q(x,p) = \frac{q(p,p)}{2}$ est un hyperplan de $\mathbb{R}^4$.

Considérons maintenant

$$\mathcal{Q} = \left\{x \in \mathbb{R}^4 \mid q(x,x) \leq q(x-p, x-p) \text{ pour tout } p \in \{p_1, p_2, p_7, p_9, p_{16}\}\right\}$$

alors $\mathcal{P} \subset \mathcal{Q}$ et nous allons voir que $\mathcal{Q}$ est borné. Remarquons d'abord que $\{p_1, p_2, p_7, p_9\}$ est une base de $\mathbb{R}^4$ et que $p_{16} = -(p_1 + p_2 + p_7 + p_9)$, de sorte que pour tout $x \in \mathcal{Q}$, $x = x_1p_1 + x_2p_2 + x_3p_7 + x_4p_9$. Considérons les quatre premières inéquations qui définissent $\mathcal{Q}$:

$$q(x, p_i) \leq \frac{q(p_i, p_i)}{2} \quad \text{où } i \in \{1, 2, 7, 9\}.$$

Ces inéquations nous donnent un système d'inéquations linéaires qui admet une unique solution, de sorte qu'il existe $c_i \in \mathbb{R}$ $(1 \leq i \leq 4)$ tels que

$$x_i \leq c_i \text{ pour tout } 1 \leq i \leq 4.$$

En combinant ce résultat avec la dernière inéquation définissant $\mathcal{Q}$:

$$q(x, \sum_{i \in \{1,2,7,9\}} p_i) \geq -\frac{q(\sum_{i \in \{1,2,7,9\}} p_i, \sum_{i \in \{1,2,7,9\}} p_i)}{2},$$

nous obtenons l'existence de $b_i \in \mathbb{R}$ $(1 \leq i \leq 4)$ tels que

$$b_i \leq x_i \leq c_i \text{ pour tout } 1 \leq i \leq 4,$$

ce qui prouve que $\mathcal{Q}$ et $\mathcal{P}$ sont bornés.

Ainsi $\mathcal{P}$ est un domaine convexe borné et fermé dont le bord est l'intersection de 24 hyperplans, c'est donc un polytope à 24 faces de dimension 3. Un calcul (effectué avec Magma) permet d'obtenir les 52 sommets de ce polytope et d'observer que 28 d'entre eux sont de norme

$$n_1 = \frac{3d^2 + 10d + 3}{16d}$$

et les 24 autres de norme

$$n_2 = \frac{3d^2 + 2d + 43}{16d}.$$

Si $d \geq 5$, alors $n_1 \geq n_2$. Comme la cellule de Voronoi $\mathcal{V}$ est contenue dans $\mathcal{P}$, cela prouve que le maximum de L est borné supérieurement par n_1. Il reste donc à voir que $\max(L, q) \geq n_1$.

Soit

$$v = \frac{1}{d}\left(\frac{1+3d}{8}, \frac{1-d}{4}, \frac{-3-d}{8}, \frac{-1+d}{2}\right)$$

un des sommets de $\mathcal{P}$ de norme n_1. Pour vérifier que $\max(L, q) \geq n_1$, il suffit de voir que la distance entre v et L est n_1. Considérons la fonction

$$f(X) = q(X - v, X - v) - n_1.$$

Alors $\max(L, q) \geq n_1$ si et seulement si $\min_{X \in \mathbb{Z}^4} f(X) = 0$. Afin de pouvoir étudier agréablement ce minimum, nous allons faire un changement de variables (qui est simplement une orthogonalisation de la forme bilinéaire q). Posons

$$x = x' + y' - \frac{z'}{4}, \quad y = -2y' - \frac{z'}{2}, \quad z = y' + \frac{z'}{4} + \frac{t'}{2}, \quad t = z' \qquad \text{(III.2)}$$

et $Y = (x, y, z, t)$, alors

$$f(Y) =$$

$$2\left(x' - \frac{1}{2}\right)^2 + 4y'^2 + \frac{d}{4}\left(z' + \frac{1-d}{2d}\right)^2 + \frac{d}{2}\left(t' - \frac{d+1}{2d}\right)^2 - \frac{3d^2 + 10d + 3}{16d}.$$

Les formules de changement de variables donnée dans III.2, combinées avec le fait que $x, y, z, t \in \mathbb{Z}$ impliquent que $x', y' \in \frac{1}{4}\mathbb{Z}$, $z' \in \mathbb{Z}$, $t' \in \frac{1}{2}\mathbb{Z}$ (ces conditions sont nécessaires mais pas suffisantes).

On sait que $\min_{X\in\mathbb{Z}^4} f(X) \leq 0$ car $f(0) = 0$. Supposons donc $f(Y) \leq 0$. Un rapide calcul combinant l'inéquation $f(Y) \leq 0$ et le fait que $x, y, z, t \in \mathbb{Z}$ permet de voir que

$$z' \in \{0, 1\}, \quad t' \in \left\{-1, -\frac{1}{2}, 0\right\}$$

et que la valeur $t' = -\frac{1}{2}$ est exclue. En effet, supposons que $z' = 0$ et $t' = -\frac{1}{2}$. Alors $z = y' - \frac{1}{4}$ et $y = -2y'$ sont des entiers, ce qui est absurde. Supposons maintenant $z' = 1$ et $t' = -\frac{1}{2}$. Alors $z = y'$ et $y = -2y' - \frac{1}{2}$ sont des entiers, ce qui est impossible. Finalement les valeurs possibles de z' et t' sont :

$$z' \in \{0, 1\} \quad \text{et} \quad t' \in \{-1, 0\}.$$

Ces quatre cas fournissent un nombre fini de possibilités pour x' et y'. Nous obtenons alors, pour $X \in \mathbb{Z}^4$, que

$$f(X) \leq 0 \text{ si et seulement si } X \in \{(1,0,0,0), (0,0,0,1), (0,1,-1,0),$$

$$(1,-1,0,0), (0,-1,0,1), (1,-1,0,1), (0,0,0,0)\}$$

et dans tous ces cas, $f(X) = 0$. Par conséquent

$$\min_{X\in\mathbb{Z}^4} f(X) = 0,$$

donc $\max(L, q) \geq n_1$.

□

Corollaire 3.7.5. *Soient $d = p_1 \cdots p_s$ où s est impair et où les p_i sont des nombres premiers congrus à 5 modulo 8, $A = (-2, -d)_{\mathbb{Q}}$ l'algèbre de quaternions sur $\mathbb{Q}$ ramifiée à l'infini et en p_i $(1 \leq i \leq s)$ et*

$$\Lambda_5 = \mathbb{Z} \oplus \frac{1+i+j}{2}\mathbb{Z} \oplus j\mathbb{Z} \oplus \frac{2+i+k}{4}\mathbb{Z}$$

un ordre maximal de A. Alors le minimum euclidien de Λ est égal à

$$\mathrm{M}(\Lambda_5) = \frac{3d^2 + 10d + 3}{32d}.$$

Preuve : La proposition précédente nous dit que $\max(\Lambda, 1) = \frac{3d^2+10d+3}{16d}$. Donc

$$\mathrm{M}(\Lambda_5) = \frac{\max(\Lambda_5, 1)}{2} = \frac{3d^2 + 10d + 3}{32d}.$$

□

Etudions maintenant le cas où $d = p_1 \cdots p_s \equiv 11 \mod 16$ avec $p_i \equiv 3 \mod 4$. L'algèbre de quaternions $A = (-1, -d)_{\mathbb{Q}}$ est ramifiée à l'infini et en p_i pour $1 \leq i \leq s$. De plus,

$$\Lambda_{16} = \mathbb{Z} \oplus \frac{1+2i+j}{2}\mathbb{Z} \oplus 2i\mathbb{Z} \oplus \frac{2-i-k}{4}\mathbb{Z}$$

est un ordre maximal de A. On calcule facilement la matrice de Gram du réseau $(\Lambda_{16}, 1)$ ce qui nous donne le résultat suivant :

$(\Lambda_{16}, 1) \cong (\mathbb{Z}^4, q)$ où q est le produit scalaire donné par la matrice

$$\begin{pmatrix} 2 & 1 & 0 & 1 \\ 1 & \frac{d+5}{2} & 4 & 0 \\ 0 & 4 & 8 & -1 \\ 1 & 0 & -1 & \frac{d+5}{8} \end{pmatrix}.$$

Pour calculer le minimum euclidien de Λ_{16}, il faut donc calculer le maximum du réseau (L, q).

Proposition 3.7.6. *Soit (L, q) où $L = \mathbb{Z}^4$ et la forme bilinéaire q est donnée par la matrice*

$$\begin{pmatrix} 2 & 1 & 0 & 1 \\ 1 & \frac{d+5}{2} & 4 & 0 \\ 0 & 4 & 8 & -1 \\ 1 & 0 & -1 & \frac{d+5}{8} \end{pmatrix}$$

d étant, soit un entier compris entre 3 et 21, soit un nombre rationnel plus grand que 21. Alors le maximum du réseau (L, q) est donné par

$$\max(L, q) = \frac{5d^2 + 34d + 45}{32d}.$$

PREUVE : Nous procédons exactement comme dans la preuve de la proposition 3.7.4 en utilisant :

$$P = \{p_1 = (1,0,0,0)\,, p_2 = (0,0,0,1)\,, p_3 = (-1,1,0,0)\,,$$

$$p_4 = (0,0,1,0)\,, p_5 = (1,0,0,-1)\,, p_6 = (-1,0,0,1)\,,$$

$$p_7 = (-1,0,0,0)\,, p_8 = (0,0,0,-1)\,, p_9 = (1,-1,0,-1)\,,$$

$$p_{10} = (-1,1,0,1)\,, p_{11} = (1,-1,0,0)\,, p_{12} = (1,-1,1,0)\,,$$

$$p_{13} = (-1,1,-1,0)\,, p_{14} = (1,0,-1,-1)\,, p_{15} = (-1,0,1,1)\,,$$

$$p_{16} = (0,1,-1,-1)\,, p_{17} = (0,-1,1,1)\,, p_{18} = (0,1,-1,0)\,,$$

$$p_{19} = (0,-1,1,0)\,, p_{20} = (0,1,0,0)\,, p_{21} = (0,-1,0,0)\,,$$

$$p_{22} = (0,0,-1,0)\,, p_{23} = (0,0,1,1)\,, p_{24} = (0,0,-1,-1)\}\,,$$

$$\mathcal{Q} = \left\{x \in \mathbb{R}^4 \mid q(x,x) \leq q(x-p,x-p) \text{ pour tout } p \in \{p_1,p_2,p_3,p_{19},p_{24}\}\right\}$$

et

$$v = \frac{1}{d}\left(\frac{-3+d}{2}, \frac{3-d}{2}, \frac{-9+11d}{16}, \frac{3+d}{2}\right).$$

Nous avons d'une part que $\max(L,q) \leq q(v,v) = \frac{5d^2+34d+45}{32d}$ et d'autre part que

$$\min_{X\in\mathbb{Z}^4} q(X-v,X-v) - \frac{5d^2+34d+45}{32d} = 0.$$

De plus ce minimum est atteint aux points suivants, pour $d \geq 21$:

$$\{(0,0,0,0)\,, (0,0,0,1)\,, (0,0,1,1)\,,$$

$$(0,-1,1,1)\,, (1,0,0,0)\,, (1,-1,1,1)\,, (1,-1,1,0)\}$$

□

Corollaire 3.7.7. *Soient $d = p_1 \cdots p_s \equiv 11 \mod 16$ où s est impair et où les p_i sont des nombres premiers tels que $p_i \equiv 3 \mod 4$, $A = (-1,-d)_{\mathbb{Q}}$ l'algèbre de quaternions sur $\mathbb{Q}$ ramifiée à l'infini et en p_i, pour $1 \leq i \leq s$, et*

$$\Lambda_{16} = \mathbb{Z} \oplus \frac{1+2i+j}{2}\mathbb{Z} \oplus 2i\mathbb{Z} \oplus \frac{2-i-k}{4}\mathbb{Z}$$

un ordre maximal de A. Alors le minimum euclidien de Λ_{16} est donné par

$$\mathrm{M}(\Lambda_{16}) = \frac{5d^2+34d+45}{64d}.$$

Preuve : La proposition précédente nous dit que $\max(\Lambda_{16},1) = \frac{5d^2+34d+45}{32d}$, donc

$$\mathrm{M}(\Lambda_{16}) = \frac{\max(\Lambda,1)}{2} = \frac{5d^2+34d+45}{64d}.$$

□

Grâce à la détermination des minima euclidiens de Λ_3 et Λ_{16}, nous allons pouvoir vérifier que ces ordres ne sont pas conjugués.

Corollaire 3.7.8. *Soient Λ_3 et Λ_{16} les ordres maximaux de A donnés dans la proposition 3.7.1. Les minima euclidiens de Λ_3 et de Λ_{16} ne coïncident jamais. En particulier Λ_3 et Λ_{16} ne sont pas conjugués.*

PREUVE : Nous savons maintenant que $\mathrm{M}(\Lambda_3) = \frac{(d+1)^2}{8d}$ et que $\mathrm{M}(\Lambda_{16}) = \frac{5d^2+34d+45}{64d}$ (voir corollaire 3.7.3 et 3.7.7). Ces minima ne coïncident jamais. La proposition 2.4.3 nous dit que deux ordres conjugués ont le même minimum euclidien, ce qui prouve que Λ_3 et Λ_{16} ne sont pas conjugués.

□

Etudions, pour finir, le cas $d = p_1 \cdots p_s \equiv 1 \mod 8$ et $p_i \equiv 2 \mod 3$. L'algèbre $A = (-3, -d)_{\mathbb{Q}}$ est le corps de quaternions sur $\mathbb{Q}$ ramifiée à l'infini et en p_i, pour $1 \leq i \leq s$ et

$$\Lambda_1 = \mathbb{Z} \oplus \frac{1+i}{2}\mathbb{Z} \oplus \frac{i+k}{3}\mathbb{Z} \oplus \frac{(1+i)(i+k)}{6}\mathbb{Z}$$

est un ordre maximal de A. On calcule facilement la matrice de Gram du réseau $(\Lambda_1, 1)$, ce qui nous donne le résultat suivant :

$(\Lambda_1, 1) \cong (\mathbb{Z}^4, q)$ où q est le produit scalaire donné par la matrice

$$\begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 0 & 1 & 2\left(\frac{d+1}{3}\right) & -d \\ 0 & 0 & -d & 2d \end{pmatrix}.$$

Pour calculer le minimum euclidien de Λ_1 il faut donc calculer le maximum du réseau (L, q).

Proposition 3.7.9. *Soit (L, q) où $L = \mathbb{Z}^4$ et la forme bilinéaire q est donnée par la matrice*

$$\begin{pmatrix} 2 & 1 & 0 & 0 \\ 1 & 2 & 1 & 0 \\ 0 & 1 & 2\left(\frac{d+1}{3}\right) & -d \\ 0 & 0 & -d & 2d \end{pmatrix}$$

d étant égal à 1 ou 2 ou à un nombre rationnel plus grand que 2. Alors le maximum du réseau (L, q) est donné par

$$\max(L, q) = \frac{2(d+1)^2}{9d}.$$

PREUVE : Le procédé est le même que dans la preuve de la proposition 3.7.4 en utilisant :

$$P = \{p_1 = (1,0,0,0), p_2 = (0,1,0,0), p_3 = (0,0,1,0),$$

$$p_4 = (1,-2,2,1), p_5 = (1,-1,0,0), p_6 = (-1,1,0,0),$$

$$p_7 = (-1,0,0,0)\,, p_8 = (0,-1,0,0)\,, p_9 = (-1,2,-2,-1)\,,$$

$$p_{10} = (1,-1,1,0)\,, p_{11} = (-1,1,-1,0)\,, p_{12} = (1,-1,1,1)\,,$$

$$p_{13} = (-1,1,-1,-1)\,, p_{14} = (1,-1,2,1)\,, p_{15} = (-1,1,-2,-1)\,,$$

$$p_{16} = (0,1,-2,-1)\,, p_{17} = (0,-1,2,1)\,, p_{18} = (0,1,-1,-1)\,,$$

$$p_{19} = (0,-1,1,1)\,, p_{20} = (0,1,-1,0)\,, p_{21} = (0,-1,1,0)\,,$$

$$p_{22} = (0,0,-1,0)\,, p_{23} = (0,0,1,1)\,, p_{24} = (0,0,-1,-1)\}\,,$$

$\mathcal{Q} = \left\{x \in \mathbb{R}^4 \mid q(x,x) \leq q(x-p,x-p) \text{ pour tout } p \in \{p_1,p_2,p_{15},p_{19},p_{21}\}\right\}$

et

$$v = \frac{1}{d}\left(\frac{-1+d}{3}, \frac{2-d}{3}, -1+d, \frac{-2+d}{3}\right).$$

Nous obtenons, d'une part que $\max(L,q) \leq q(v,v) = \frac{2(d+1)^2}{9d}$, car les sommets du polytope $\mathcal{P} = \left\{x \in \mathbb{R}^4 \mid q(x,x) \leq q(x-p,x-p) \text{ pour tout } p \in P\right\}$ sont tous de norme $\frac{2(d+1)^2}{9d}$ et $\mathcal{P}$ contient la cellule de Voronoi de $(\mathbb{Z}^4,q)$, et d'autre part que

$$\min_{X \in \mathbb{Z}^4} q(X-v,X-v) - \frac{2(d+1)^2}{9d} = 0.$$

De plus ce minimum est atteint aux points suivants, pour $d > 2$:

$$\{(0,0,0,0)\,, (1,0,0,0)\,, (0,1,0,0)\,, (1,-1,2,1)\,,$$

$$(1,-1,1,0)\,, (0,0,1,0)\,, (1,0,1,0)\}$$

□

Corollaire 3.7.10. *Soient $d = p_1 \cdots p_s$ où s est impair et où les p_i sont des nombres premiers tels que $p_i \equiv 1 \mod 8$ et $p_i \equiv 2 \mod 3$, $A = (-3,-d)_{\mathbb{Q}}$ l'algèbre de quaternions sur $\mathbb{Q}$ ramifiée à l'infini et en p_i $(1 \leq i \leq s)$ et*

$$\Lambda_1 = \mathbb{Z} \oplus \frac{1+i}{2}\mathbb{Z} \oplus \frac{i+k}{3}\mathbb{Z} \oplus \frac{(1+i)(i+k)}{6}\mathbb{Z}$$

un ordre maximal de A. Alors le minimum euclidien de Λ est donné par

$$\mathrm{M}(\Lambda_1) = \frac{(d+1)^2}{9d}.$$

PREUVE : La proposition précédente nous dit que $\max(\Lambda_1, 1) = \frac{2(d+1)^2}{9d}$. Donc

$$\mathrm{M}(\Lambda_1) = \frac{\max(\Lambda_1, 1)}{2} = \frac{(d+1)^2}{9d}.$$

□

Les corollaires 3.7.3, 3.7.5, 3.7.7 et 3.7.10 nous donnent explicitement le minimum euclidien d'un ordre maximal dans les familles de corps de quaternions de la proposition 3.7.1. Nous pouvons toutefois faire deux objections à la généralité de ces résultats :

- La première concerne le choix des ordres maximaux. En effet, il existe dans A de nombreuses classes d'ordres maximaux, alors que les résultats énoncés ne s'appliquent qu'à l'une d'entre elles.
- La seconde concerne le choix des corps de quaternions A. En effet, nous nous sommes limités aux algèbres qui sont ramifiées en des premiers qui ont la même congruence modulo 4.

Pour répondre partiellement à la première objection, rappelons que les minima euclidiens de deux ordres non conjugués sont relativement proches. En effet, si Λ et Γ sont des ordres maximaux de A, il existe un entier s, relativement petit, tel que

$$\frac{1}{s} \leq \frac{\mathrm{M}(\Lambda)}{\mathrm{M}(\Gamma)} \leq s.$$

(Voir la proposition 2.4.5).

Pour répondre partiellement à la seconde objection, nous pouvons observer que les résultats obtenus nous donnent quand même de l'information sur un ordre maximal contenu dans d'autres corps de quaternions qui ne sont plus soumis aux mêmes hypothèses de ramification. C'est l'objet de la proposition suivante.

Proposition 3.7.11. *Soient $d_3 \equiv 3 \mod 4$, $d_{16} \equiv 11 \mod 16$, $d_5 \equiv 5 \mod 8$ et $d_1 \equiv 2 \mod 3$ des entiers et $A_3 = (-1, -d_3)_{\mathbb{Q}}, A_{16} = (-1, -d_{16})$, $A_5 = (-2, -d_5)$ et $A_1 = (-3, -d_1)$ des corps de quaternions sur $\mathbb{Q}$. Alors il*

existe dans A_i un ordre maximal Γ_i tel que :

$$\begin{aligned}
\mathrm{M}(\Gamma_3) &\leq \frac{(d+1)^2}{8d},\\
\mathrm{M}(\Gamma_{16}) &\leq \frac{5d^2+34d+45}{64d},\\
\mathrm{M}(\Gamma_5) &\leq \frac{3d^2+10d+3}{32d},\\
\mathrm{M}(\Gamma_1) &\leq \frac{(d+1)^2}{9d}.
\end{aligned}$$

PREUVE : Nous faisons la preuve pour A_1, les autres preuves sont similaires. Le $\mathbb{Z}$-module

$$\Lambda' = \mathbb{Z} \oplus \frac{1+i}{2}\mathbb{Z} \oplus \frac{i+k}{3}\mathbb{Z} \oplus \frac{(1+i)(i+k)}{6}\mathbb{Z}$$

est un ordre de A_1 (pas nécessairement maximal), le réseau $(\Lambda', 1)$ est identique au réseau (L, q) de la proposition 3.7.9, de sorte que $\max(\Lambda', 1) = \frac{2(d+1)^2}{9d}$. Soit $\Lambda \supset \Lambda'$ un ordre maximal de A. Alors $(\Lambda', 1)$ est un sous-réseau de $(\Lambda, 1)$, donc

$$\mathrm{M}(\Lambda) = \frac{\max(\Lambda, 1)}{2} \leq \frac{\max(\Lambda', 1)}{2} = \frac{(d+1)^2}{9d}.$$

□

Pour conclure cette section nous donnons les résultats obtenus sur les corps de quaternions euclidiens totalement définis sur $\mathbb{Q}$.

Proposition 3.7.12. *Soit $A = (a, b)_{\mathbb{Q}}$ un corps de quaternions défini de discriminant d^2. Alors A est euclidien pour la norme réduite si et seulement si $d = 2, 3$ ou 5. La valeur du minimum euclidien de A est donnée par*

$$\mathrm{M}(A) = \begin{cases} \frac{1}{2} \text{ si } d = 2 \\ \frac{2}{3} \text{ si } d = 3 \\ \frac{4}{5} \text{ si } d = 5. \end{cases}$$

PREUVE : Soit Λ un ordre maximal de A et $I_1, \ldots, I_h$ des représentants des classes d'idéaux à droite de Λ. Une formule de masse classique (voir [Vig80] corollaire 2.3 p.142) nous dit que

$$\sum_{k=1}^{h} \frac{1}{w_k} = \frac{1}{12} \prod_{p|d} (p-1)$$

où $w_k = \frac{|\mathcal{O}_d(I_k)^\times|}{2}$. Pour que h soit égal à 1, il faut donc que $d = 2, 3, 5, 7, 13$; sinon le terme de droite n'est pas l'inverse d'un entier (compte tenu du fait que $|\Lambda^\times|$ est pair pour tout ordre maximal Λ). Ce sont donc les seuls cas où A peut être principal et, *a fortiori* euclidien. Il ne reste plus qu'à calculer le minimum euclidien d'un ordre maximal dans chacun de ces cas. Nous utilisons les corollaires 3.7.2, 3.7.3 et 3.7.5 pour calculer ces minima euclidiens. Pour $d = 2$, $\mathrm{M}(A) = \frac{1}{2}$, pour $d = 3$, $\mathrm{M}(A) = \frac{2}{3}$, pour $d = 5$, $\mathrm{M}(A) = \frac{4}{5}$, pour $d = 7$, $\mathrm{M}(A) = \frac{8}{7}$, et pour $d = 13$, $\mathrm{M}(A) = \frac{20}{13}$.

□

3.8 Le cas des corps quadratiques : réalisation du réseau E_8

Le but de cette section est de donner une condition nécessaire et suffisante à la réalisation du réseau E_8 comme réseau idéal sur une algèbre de quaternions.

Définition 3.8.1. *Le réseau* E_8 *est le réseau* $(\mathbb{Z}^8, q)$ *où* q *est le produit scalaire donné par la matrice*

$$\begin{pmatrix} 2 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1 & 2 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 2 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 2 & -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}$$

Par la suite nous utiliserons uniquement les propriétés suivantes :

Le réseau E_8 est l'unique (à isométrie près) réseau unimodulaire pair de dimension 8. Le maximum de E_8 est 1.

Avant d'aller plus loin, nous allons énoncer quelques résultats utiles, propres, pour la plupart, aux algèbres de quaternions. Rappelons que l'ensemble des idéaux bilatères d'un ordre maximal dans une algèbre centrale simple est le groupe abélien libre engendré par les idéaux premiers (voir [Rei03] théorème 22.10, p.193). Si $I = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$ est un tel idéal, alors on notera $\nu_{\beta_i}(I) = e_i$ (la valuation $\mathfrak{P}_i$-adique de I).

Lemme 3.8.2. *Soient $A = (a,b)_K$ une algèbre de quaternions sur un corps de nombres K, Λ un ordre maximal de A et I, J des idéaux bilatères de Λ. Notons γ l'involution canonique de A. On a*

i) $I^\gamma = I$.

ii) $I = J \iff \mathrm{N}_{A/K}(I) = \mathrm{N}_{A/K}(J) \iff \mathrm{nr}_{A/K}(I) = \mathrm{nr}_{A/K}(J)$.

iii) Soit $\mathfrak{P}$ un idéal premier de Λ et $\mathcal{P} = \mathfrak{P} \cap \mathcal{O}_K$. Alors $\mathrm{nr}_{A/K}(\beta) = \mathcal{P}^{f_\mathcal{P}}$, avec $f_\mathcal{P} = 1$ si $\mathcal{P}$ est ramifié dans A, et $f_\mathcal{P} = 2$ sinon.

iv) La valuation $\mathfrak{P}$-adique de I est donnée par

$$\nu_\mathfrak{P}(I) = f_\mathcal{P} \nu_\mathcal{P}(\mathrm{nr}(I))$$

où $\mathcal{P}$ et $f_\mathcal{P}$ sont comme dans iii).

Preuve : Commençons par vérifier l'affirmation *iii)*. Nous savons que $\mathrm{N}_{A/K}(\mathfrak{P}) = \mathcal{P}^f$ avec $f = \kappa_\mathcal{P}^2 m_\mathcal{P}$, où $\kappa_\mathcal{P}$ est la capacité locale de A en $\mathcal{P}$ et $m_\mathcal{P}$ l'indice local de A en $\mathcal{P}$ (voir [Rei03] thm 24.6, p.213 et la preuve du thm 24.13, p.215). Comme $\kappa_\mathcal{P}^2 m_\mathcal{P}^2 = [A : K] = 4$,

$$\mathrm{N}_{A/K}(\mathfrak{P}) = \begin{cases} \mathcal{P}^2 & \text{si } m_\mathcal{P} = 2, \\ \mathcal{P}^4 & \text{si } m_\mathcal{P} = 1. \end{cases}$$

De plus, $\mathrm{nr}_{A/K}(\mathfrak{P})^2 = \mathrm{N}_{A/K}(\mathfrak{P})$, et $\mathcal{P}$ est ramifié dans A si et seulement si $m_\mathcal{P} > 1$. Ce qui prouve *iii)*.

Nous allons maintenant démontrer *i)* et *ii)* dans le cas particulier où I et J sont des idéaux premiers. Soient $\mathfrak{P}$ et $\mathfrak{Q}$ deux idéaux premiers de Λ, $\mathcal{P} = \mathfrak{P} \cap \mathcal{O}_K$ et $\mathcal{Q} = \mathfrak{Q} \cap \mathcal{O}_K$. L'idéal $\mathfrak{P}^\gamma$ est premier. En effet, si M et N sont deux idéaux bilatères de Λ tels que $MN \subset \mathfrak{P}^\gamma$, alors $N^\gamma M^\gamma \subset \mathfrak{P}$ donc, soit $N^\gamma \subset \mathfrak{P}$, soit $M^\gamma \subset \mathfrak{P}$. En appliquant à nouveau l'involution γ, nous obtenons

$$\text{soit } N \subset \mathfrak{P}^\gamma, \text{ soit } M \subset \mathfrak{P}^\gamma,$$

donc $\mathfrak{P}^\gamma$ est un idéal premier de Λ. De plus,

$$\mathfrak{P}^\gamma \cap \mathcal{O}_K = (\mathfrak{P} \cap \mathcal{O}_K)^\gamma = \mathfrak{P} \cap \mathcal{O}_K = \mathcal{P}.$$

L'ensemble des idéaux premier de Λ est en bijection avec l'ensemble des idéaux premiers de $\mathcal{O}_K$ (voir le théorème 1.6.3), donc $\mathfrak{P} = \mathfrak{P}^\gamma$. Vérifions maintenant *ii)* pour nos idéaux premiers $\mathfrak{P}$ et $\mathfrak{Q}$. Il est clair que si $\mathfrak{P} = \mathfrak{Q}$ alors $\mathrm{N}_{A/K}(\mathfrak{P}) = \mathrm{N}_{A/K}(\mathfrak{Q})$. Supposons que $\mathrm{N}_{A/K}(\mathfrak{P}) = \mathrm{N}_{A/K}(\mathfrak{Q})$. Alors $\mathcal{P}^{f_1} = \mathcal{Q}^{f_2}$ pour des entiers, donc $f_1 = f_2$ et $\mathcal{P} = \mathcal{Q}$, de sorte que $\mathfrak{P} = \mathfrak{Q}$. Pour montrer *ii)*, dans le cadre des idéaux premiers, il faut encore vérifier la deuxième équivalence. Nous savons que $\mathrm{nr}_{A/K}(\mathfrak{P})^2 = \mathrm{N}_{A/K}(\mathfrak{P}) = \mathcal{P}^{2f_1}$; l'équivalence est alors évidente. Passons maintenant au cas général. Soient

I et J des idéaux bilatères. Il existe des idéaux premiers $\mathfrak{P}_i$ et $\mathfrak{Q}_i$ et des entiers e_i et g_i tels que $I = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_s^{e_s}$ et $J = \mathfrak{Q}_1^{g_1} \cdots \mathfrak{Q}_r^{g_r}$. Alors

$$I^\gamma = \mathfrak{P}_s^{e_s\gamma} \cdots \mathfrak{P}_1^{e_1\gamma} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_s^{e_s} = I,$$

ce qui démontre *i)*. Supposons maintenant que $\mathrm{nr}_{A/K}(I) = \mathrm{nr}_{A/K}(J)$. Posons $\mathcal{P}_i = \mathfrak{P}_i \cap \mathcal{O}_K$ et $\mathcal{Q}_i = \mathfrak{Q}_i \cap \mathcal{O}_K$. Alors

$$\mathcal{P}_1^{f_{\mathcal{P}_1} e_1} \cdots \mathcal{P}_s^{f_{\mathcal{P}_s} e_s} = \mathrm{nr}_{A/K}(I) = \mathrm{nr}_{A/K}(J) = \mathcal{Q}_1^{f_{\mathcal{Q}_1} g_1} \cdots \mathcal{Q}_r^{f_{\mathcal{Q}_r} g_r}.$$

Donc $r = s$ et on peut supposer que $\mathcal{P}_i = \mathcal{Q}_i$ et $e_i = g_i$ pour tout $1 \leq i \leq s$. Cela prouve que $I = J$ et que $\mathrm{N}_{A/K}(I) = \mathrm{N}_{A/K}(J)$. L'implication

$$\mathrm{N}_{A/K}(I) = \mathrm{N}_{A/K}(J) \Longrightarrow I = J$$

ce montre de la même façon. Le point *iv)* est une conséquence directe de *iii)*.

□

Lemme 3.8.3. *Soient $A = (a, b)_K$ une algèbre de quaternions sur un corps K, Λ un ordre maximal et I un idéal à droite de Λ. Alors*

$$I^\gamma I = I I^\gamma = \mathrm{nr}_{A/K}(I)\Lambda.$$

Preuve : Remarquons d'abord que $I^\gamma I$ est un idéal bilatère de Λ. En effet,

$$\mathcal{O}_r(I^\gamma I) \supset \mathcal{O}_r(I) = \Lambda.$$

Donc $\mathcal{O}_r(I^\gamma I)$ égal Λ par maximalité de Λ. De plus par la proposition 1.8.6,

$$\mathcal{O}_l(I^\gamma I) \supset \mathcal{O}_l(I^\gamma) = \mathcal{O}_r(I)^\gamma = \Lambda^\gamma = \Lambda,$$

ce qui prouve que $I^\gamma I$ est un idéal bilatère de Λ. Par le lemme précédent, il suffit donc de vérifier que

$$\mathrm{N}_{A/K}(I^\gamma I) = \mathrm{N}_{A/K}(\mathrm{nr}_{A/K}(I)\Lambda).$$

Un calcul rapide montre que ces deux termes sont égaux à $\mathrm{nr}_{A/K}(I)^4$.

□

Lemme 3.8.4. *Soit K un corps de nombres quadratique réel. La différente de K est un idéal principal et cet idéal possède un générateur totalement positif si et seulement si l'unité fondamentale de K est de norme -1.*

PREUVE : Soit $K = \mathbb{Q}(\sqrt{d})$. Si $d \equiv 2, 3 \mod 4$, alors $\mathcal{D}_K = 2\sqrt{d}\mathcal{O}_K$ et si $d \equiv 1 \mod 4$, alors $\mathcal{D}_K = \sqrt{d}\mathcal{O}_K$ (voir [Sam67] § 2.5 et 4.6 et [Lan94] chap. 3 § 2 proposition 3). Nous faisons la preuve dans le cas où $d \equiv 1 \mod 4$, les autres cas sont similaires. Supposons qu'il existe une unité u dans K avec $\mathrm{N}_{K/\mathbb{Q}}(u) = -1$. Alors, soit $2\sqrt{d}u$, soit $-2\sqrt{d}u$ est un générateur totalement positif de $\mathcal{D}_K$. Réciproquement, s'il n'existe aucune unité de K de norme -1, alors pour tout unité u, $\mathrm{N}_{K/\mathbb{Q}}(2\sqrt{d}u) < 0$, donc $\mathcal{D}_K$ n'admet pas de générateur totalement positif. Pour conclure, rappelons qu'il existe une unité de norme -1 dans K si et seulement si l'unité fondamentale ω est elle-même de norme -1. En effet, pour tout unité u de K, $u = \pm\omega^n$ pour un certain entier n.

□

Lemme 3.8.5. *Soit $A = (a, b)_K$ un corps de quaternions sur un corps quadratique réel. Si aucune place finie de K n'est ramifiée dans A, alors A est totalement définie.*

PREUVE : Comme A est un corps gauche, il existe au moins une place infinie ramifiée dans A. De plus, le nombre de places ramifiées dans A est pair donc la seconde place infinie est également ramifiée.

□

A l'aide de ces quelques lemmes nous pouvons maintenant énoncer le résultat qui nous intéresse.

Proposition 3.8.6. *Soient $A = (a, b)_K$ un corps de quaternions muni de l'involution canonique γ, Λ un ordre maximal de A et (I, α, γ) un réseau idéal de A. Alors $(I, \alpha, \gamma) \cong \mathrm{E}_8$ si et seulement si les conditions suivantes sont vérifiées :*

i) Le corps K est quadratique réel.

ii) Aucune place finie de K ne ramifie dans A.

iii) La norme réduite $J = \mathrm{nr}_{A/K}(I)$ de l'idéal I est un idéal principal de K.

iv) L'élément α^{-1} est un générateur totalement positif de $\mathcal{D}_K J$.

PREUVE : Supposons les quatre conditions vérifiées. Alors d'une part

$$\mathcal{D}(\Lambda/\mathbb{Z}) = \mathcal{D}(\Lambda/\mathcal{O}_K)\mathcal{D}_K = \mathcal{D}_K\Lambda.$$

En effet, $\mathcal{D}(\Lambda/\mathcal{O}_K) = \Lambda$ car aucune place finie de K n'est ramifiée dans A. D'autre part,

$$I\alpha I^\gamma = I\mathcal{D}_K^{-1}J^{-1}I^\gamma = \mathcal{D}_K^{-1}J^{-1}II^\gamma = \mathcal{D}_K^{-1}J^{-1}\mathrm{nr}_{A/K}(I)\Lambda = \mathcal{D}_K^{-1}\Lambda$$

où la troisième égalité provient du lemme 3.8.3. Donc $I\alpha I^\gamma = \mathcal{D}(\Lambda/\mathbb{Z})^{-1}$, ce qui signifie que (I, α, γ) est unimodulaire (voir proposition 2.7.1 et corollaire 2.7.2) et pair (voir proposition 3.2.2). Comme K est quadratique, (I, α, γ) est un réseau de dimension 8 ; il est donc isomorphe à E_8.
Réciproquement, supposons que $(I, \alpha, \gamma) \cong \mathrm{E}_8$. Pour des raisons évidentes de dimension, K doit être un corps quadratique et K doit être réel par la proposition 3.1.4. De plus

$$I\alpha I^\gamma = \mathcal{D}(\Lambda/\mathbb{Z})^{-1}$$

car (I, α, γ) est unimodulaire et pair. En appliquant $\mathrm{N}_{A/K}$ à la dernière égalité, nous obtenons

$$\alpha^4 \mathrm{N}_{A/K}(I)^2 = \mathrm{d}(\Lambda/\mathcal{O}_K)^{-1}\mathcal{D}_K^{-4}$$

car $\alpha \in K$ (voir la proposition 3.1.4). Rappelons que

$$\mathrm{d}(\Lambda/\mathcal{O}_K) = \prod_{\mathcal{P}\in \mathrm{Ram}_f(A)} \mathcal{P}^2.$$

En comparant les exposants, nous remarquons que la seule possibilité est qu'il existe un idéal J de $\mathcal{O}_K$ tel que

$$\mathrm{N}_{A/K}(I) = \prod_{\mathcal{P}\in \mathrm{Ram}_f(A)} \mathcal{P}^{-1}J^2 \quad \text{et} \quad \alpha\mathcal{O}_K = \mathcal{D}_K^{-1}J^{-1}.$$

Mais l'idéal $\mathrm{N}_{A/K}(I)$ est le carré de l'idéal $\mathrm{nr}_{A/K}(I)$, donc $\mathrm{Ram}_f(A) = \emptyset$ et $\mathrm{nr}_{A/K}(I) = J$. Comme $\alpha\mathcal{O}_K$ et $\mathcal{D}_K^{-1}$ sont des idéaux principaux J, l'est également. Le point *iv)* découle directement du fait que α est totalement positif (voir proposition 3.1.4).

□

Dans le cadre de la construction d'une borne du minimum euclidien de l'ordre maximal Λ, il est intéressant de savoir quand on peut obtenir le réseau E_8 sur un idéal principal ou, de manière équivalente, sur Λ lui même. Ce résultat est donné par le corollaire suivant.

Corollaire 3.8.7. *Soient K un corps quadratique réel, $A = (a, b)_K$ un corps de quaternions sur K et Λ un ordre maximal de A. Alors il existe $\alpha \in A$ tel que $(\Lambda, \alpha, \gamma)$ est le réseau E_8 si et seulement si les conditions suivantes sont vérifiées :*

i) L'unité fondamentale de K est de norme -1.

ii) Le corps de quaternions A est non ramifié aux places finies de K.

PREUVE : Supposons *i)* et *ii)* vérifiées. Par le lemme 3.8.4, il existe $\alpha \in K$ totalement positif tel que $\alpha\mathcal{O}_K = \mathcal{D}_K^{-1}$. Il suffit de choisir $I = \Lambda$ puis d'appliquer la proposition précédente pour voir que $(\Lambda, \alpha, \gamma)$ est le réseau E_8. Réciproquement si $(\Lambda, \alpha, \gamma)$ est le réseau E_8, alors il existe un élément totalement positif $\alpha \in K$ qui engendre $\mathcal{D}_K^{-1}$. Le lemme 3.8.4 nous dit alors que l'unité fondamentale de K est de norme -1.

□

Une autre possibilité d'obtenir le réseau E_8 comme réseau idéal sur une algèbre centrale à division apparaît lorsque l'algèbre est une algèbre de quaternions sur un corps quadratique imaginaire. Il semble alors que les choix possibles d'idéaux sont plus nombreux que dans le cas réel, c'est pourquoi nous n'arrivons pas à donner un critère aussi précis que dans le cas réel. Les deux propositions suivantes résument ce que nous avons obtenu.

Proposition 3.8.8. *Soient $d \equiv 3 \mod 4$ un entier positif, $A = (a,b)_K$ où $K = \mathbb{Q}(\sqrt{-d})$, Λ un ordre maximal de A et $\tau = \iota\gamma$ la composition de l'involution canonique de A avec la conjuguaison complexe. Soit I un idéal bilatère de Λ et (I, α, τ) un réseau idéal de A. Alors*

$$(I, \alpha, \tau) \cong \mathrm{E}_8 \text{ si et seulement si } I\alpha I^\tau = \mathcal{D}(\Lambda/\mathbb{Z})^{-1}.$$

PREUVE : Comme $-d \equiv 1 \mod 4$, l'extension $K/\mathbb{Q}$ n'a pas de ramification dyadique. Par la proposition 2.7.1, le corollaire 2.7.2 et la proposition 3.2.2, (I, α, τ) est un réseau unimodulaire pair si et seulement si $I\alpha I^\tau = \mathcal{D}(\Lambda/\mathbb{Z})^{-1}$.

□

Les cas $-d \equiv 2 \mod 4$ et $-d \equiv 3 \mod 4$ exigent une hypothèse supplémentaire.

Proposition 3.8.9. *Soient $d \equiv 2 \mod 4$ ou $d \equiv 1 \mod 4$ un entier positif, $A = (a,b)_K$ où $K = \mathbb{Q}(\sqrt{-d})$, Λ un ordre maximal de A et $\tau = \iota\gamma$ la composition de l'involution canonique de A avec la conjuguaison complexe. Soit I un idéal bilatère de Λ et (I, α, τ) un réseau idéal de A. Alors $(I, \alpha, \tau) \cong \mathrm{E}_8$ si et seulement si $I\alpha I^\tau = \mathcal{D}(\Lambda/\mathbb{Z})^{-1}$ et $\mathrm{tr}_{A/K}(x\alpha x^\tau) \in \mathbb{Z}$ pour tout $x \in I$.*

PREUVE : Il s'agit du même résultat que la proposition précédente assorti de la remarque 3.2.3.

□

Ces deux derniers résultats sont moins satisfaisants que dans le cas réel. Nous allons maintenant expliciter les choix possibles pour a, b, I et α dans les deux propositions précédentes.

Lemme 3.8.10. *Soient $A = (a,b)_K$ une algèbre de quaternions sur un corps de nombres K munie d'une involution τ de type II, F le sous-corps de K fixé par l'involution et ι le F-automorphisme non trivial de K. Soit $\mathfrak{P}$ un idéal premier de l'ordre maximal Λ. Alors $\mathfrak{P} = \mathfrak{P}^\tau$ si et seulement si $\mathcal{P} = \mathfrak{P} \cap \mathcal{O}_K$ est un idéal premier ramifié ou inerte dans F.*

Preuve : Remarquons que $\mathfrak{P}^\iota$ est un idéal au dessus de $\mathcal{P}^\iota$, de sorte que $\mathfrak{P}^\iota = \mathfrak{P}$ si et seulement si $\mathcal{P}^\iota = \mathcal{P}$. Or cette dernière égalité n'est vraie que si $\mathcal{P}$ est ramifié ou inerte dans F. Finalement, comme $\mathfrak{P}^\tau = \mathfrak{P}^{\iota\gamma} = \mathfrak{P}^\iota$, nous obtenons le résultat annoncé.

□

Lemme 3.8.11. *Soient A, K, F et τ comme dans le lemme précédent et $\mathcal{P}$ un premier de $\mathcal{O}_K$. Alors $\mathcal{P}$ est ramifié dans A si est seulement si $p\mathcal{O}_K = \mathcal{P}\mathcal{P}^\iota$ où p est un premier totalement décomposé de $\mathcal{O}_F$ qui ramifie dans $A_0 = \{x \in A \mid x^\gamma = x^\tau\}$.*

Preuve : Supposons d'abord que p n'est pas ramifié dans A_0. Soit $\mathcal{P}$ un idéal premier de $\mathcal{O}_K$ au dessus de p. Nous avons

$$A_\mathcal{P} = A \otimes_K K_\mathcal{P} \cong A_0 \otimes_F K \otimes_K K_\mathcal{P} \cong A_0 \otimes_F F_p \otimes_{F_p} K_\mathcal{P} \cong (A_0)_p \otimes_{F_p} K_\mathcal{P}$$

de sorte que, si p n'est pas ramifié dans A_0, alors

$$A_\mathcal{P} \cong \mathrm{M}_2(F_p) \otimes_{F_p} K_\mathcal{P} \cong \mathrm{M}_2(K_\mathcal{P}).$$

Supposons maintenant que p est ramifié dans A_0. Dans cette situation trois cas se présentent :

i) L'idéal p est ramifié dans K. Dans ce cas, si $\mathcal{P}$ est l'idéal premier au-dessus de p, $[K_\mathcal{P} : F_p] = e(\mathcal{P},p)f(\mathcal{P},p) = 2 \cdot 1 = 2$, où $e(\mathcal{P},p)$ est l'indice de ramification et $f(\mathcal{P},p)$ le degré d'inertie.

ii) L'idéal p est inerte dans K. Dans ce cas, si $\mathcal{P} = p\mathcal{O}_K$ est l'idéal premier au dessus de p, $[K_\mathcal{P} : F_p] = e(\mathcal{P},p)f(\mathcal{P},p) = 1 \cdot 2 = 2$.

iii) L'idéal p est décomposé dans K. Dans ce cas, si $\mathcal{P}\mathcal{P}^\iota = p\mathcal{O}_K$, $[K_\mathcal{P} : F_p] = e(\mathcal{P},p)f(\mathcal{P},p) = 1 \cdot 1 = 1$, donc $K_\mathcal{P} = F_p$.

Dans les cas i) et ii),

$$A_{\mathcal{P}} \cong (A_0)_p \otimes_{F_p} K_{\mathcal{P}} \cong \mathrm{M}_2(K_{\mathcal{P}}).$$

En effet, l'extension $K_{\mathcal{P}}$ de F_p neutralise $(A_0)_p$ si et seulement si le degré de $K_{\mathcal{P}}$ sur F_p est pair (voir le théorème 1.3 du chapitre 2 de [Vig80]). Dans le cas iii), $A_{\mathcal{P}} \cong (A_0)_p \otimes_{F_p} F_p \cong (A_0)_p$ qui est un corps de quaternions puisque p est ramifié dans A_0.

□

Corollaire 3.8.12. *Soient K une extension quadratique de $\mathbb{Q}$, $A = (a,b)_K$ avec $a, b \in \mathbb{Q}$ et $\mathcal{P}$ un idéal premier de $\mathcal{O}_K$. L'idéal $\mathcal{P}$ est ramifié dans A si et seulement si le premier p tel que $p\mathbb{Z} = \mathcal{P} \cap \mathbb{Z}$ est ramifié dans $A_0 = (a,b)_{\mathbb{Q}}$ et décomposé dans K.*

Preuve : La composition de l'automorphisme non trivial de K avec l'involution canonique de A définit une involution τ de type II sur A. De plus $A_0 = \{x \in A \mid x^\gamma = x^\tau\} = (a,b)_{\mathbb{Q}}$. Il suffit alors d'appliquer le lemme précédent.

□

Lemme 3.8.13. *Soient A, K, F, τ et Λ comme dans le lemme précédent. Si $\mathcal{P}$ est un premier de $\mathcal{O}_K$ ramifié dans A, alors $\mathcal{P}^\iota$ est également un premier ramifié dans A. De plus si $\mathcal{P}_i, \mathcal{P}_i^\iota$ $(1 \leq i \leq s)$ désignent tous les idéaux premiers de $\mathcal{O}_K$ ramifiés dans A et si $\mathfrak{P}_i$ est l'unique idéal premier de Λ au-dessus de $\mathcal{P}_i$, alors*

$$\mathcal{D}(\Lambda/\mathcal{O}_K) = \prod_{i=1}^{s} \mathfrak{P}_i \mathfrak{P}_i^\tau.$$

Preuve : Le lemme 3.8.11 nous dit que si $\mathcal{P}$ ramifie alors $\mathcal{P}^\iota$ également. La différente de Λ est le produit des idéaux premiers ramifiés et $\mathfrak{P}^\iota = \mathfrak{P}^\tau$, d'où le résultat.

□

Les lemmes ci-dessus suggèrent le résultat suivant.

Corollaire 3.8.14. *Soient $K = \mathbb{Q}(\sqrt{-d})$ un corps quadratique imaginaire, $A = (a,b)_K$ (avec $a, b \in \mathbb{Q}$) un corps de quaternions muni d'une involution*

$\tau = \iota\gamma$ de type II et Λ un ordre maximal de A. Soient $\mathcal{P}_1, \mathcal{P}_1^\iota, \ldots, \mathcal{P}_r, \mathcal{P}_r^\iota$ les places finies de K ramifiées dans A. Notons encore d le générateur usuel de la différente de K et supposons que les conditions suivantes sont vérifiées :

i) Il existe $x \in \Lambda^\times$ de norme négative tel que $\alpha = d^{-1}x$ vérifie

$$0 < \mathrm{nr}(\alpha) < \left(\frac{\mathrm{tr}(\alpha)^2}{2}\right) \quad et \quad \alpha = \alpha^\tau$$

ii) Pour tout $x \in I$,

$$\mathrm{tr}_{A/K}(x\alpha x^\tau) \in \mathbb{Z}$$

où $I = \prod_{i=1}^s \mathfrak{P}_i^{-1}$ et les $\mathfrak{P}_i$ sont comme dans le lemme ci-dessus.

Alors (I, α, τ) est le réseau E_8.

Preuve : Les conditions de *i)* exigées sur α impliquent que (I, α, τ) est un réseau idéal. Comme $I = \prod_{i=1}^s \beta_i^{-1}$ est un idéal bilatère,

$$I\alpha I^\tau = \prod_{i=1}^s \beta_i^{-1}\alpha\Lambda \prod_{i=1}^s \beta_i^{-\tau} = \prod_{i=1}^s \beta_i^{-1}\mathcal{D}_K^{-1}\Lambda \prod_{i=1}^s \beta_i^{-\tau} = \mathcal{D}(\Lambda/\mathbb{Z})^{-1}$$

En combinant ce résultat avec l'hypothèse de *ii)* et en appliquant les propositions 3.8.8 et 3.8.9, nous trouvons le résultat.

□

Remarque : Dans le cas $-d \equiv 1 \mod 4$ la condition *ii)* du corollaire précédent est automatiquement vérifiée puisqu'il n'y a pas ramification dyadique.

Nous allons maintenant donner les conséquences des réalisations du réseau E_8 sur les corps quadratiques en terme de bornes du minimum euclidien. Là encore le résultat est plus précis dans le cas réel que dans le cas imaginaire.

Corollaire 3.8.15. *Soient $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique réel dont l'unité fondamentale est de norme négative, $A = (a, b)_K$ un corps de quaternions totalement défini et non ramifié aux places finies de K et Λ un ordre maximal de A. Alors*

$$\mathrm{M}(\Lambda) \leq \frac{\mathrm{d}_K}{16}.$$

Preuve : La proposition 3.8.6 nous assure qu'en choisissant α un générateur totalement positif de $\mathcal{D}_K$, le réseau $(\Lambda, \alpha, \gamma)$ est le réseau E_8. D'autre part

nous savons que $\max(E_8) = 1$ et $\det(E_8) = 1$, de sorte que le corollaire 2.5.2 nous dit que

$$\mathrm{M}(\Lambda) \leq \left(\frac{1}{\gamma_{\min}(\Lambda)}\right)^2 = \left(\frac{\mathrm{d}(\Lambda/\mathbb{Z})^{1/8}}{4}\right)^2$$

où l'égalité découle de la proposition 1.9.2. Comme les places finies de K sont non ramifiées dans A, $\mathrm{d}(\Lambda/\mathbb{Z}) = \mathrm{d}(\Lambda/\mathcal{O}_K)\mathrm{d}_K^4 = \mathrm{d}_K^4$, d'où le résultat. □

Enonçons maintenant le résultat correspondant dans le cas quadratique imaginaire.

Corollaire 3.8.16. *Soit A, Λ, I, $\tau = \gamma\iota$ et α vérifiant les mêmes hypothèses que dans le corollaire 3.8.14. Soient $\mathcal{P}_1, \mathcal{P}_1^\iota \ldots \mathcal{P}_s, \mathcal{P}_s^\iota$ les idéaux premiers de K ramifiés dans A. Supposons que $\mathcal{P}_i$ est principal pour tout $1 \leq i \leq s$ et posons $q_i = \mathcal{P}_i \cap \mathbb{Z}$. Alors*

$$\mathrm{M}(\Lambda) \leq \frac{q_1 \ldots q_s \cdot \mathrm{d}_K}{16}.$$

Preuve : Nous savons que $\mathcal{P}_i\Lambda = \mathfrak{P}_i^2$ où les $\mathfrak{P}_i$ sont des idéaux premiers de Λ (car $\mathcal{P}_i$ ramifie dans A) et que $\mathrm{nr}_{A/K}(\mathfrak{P}_i) = \mathcal{P}_i$ pour la même raison. Comme les $\mathcal{P}_i$ sont principaux, d'après le théorème 34.9 p.298 de [Rei03], les $\mathfrak{P}_i$ sont des idéaux principaux. L'idéal I est donc un idéal bilatère principal. D'après le corollaire 3.8.14, on a donc que (I, α, τ) est le réseau E_8. Notons $I = t\Lambda$. Alors

$$(I, \alpha, \tau) \cong (\Lambda, t\alpha t^\tau, \tau)$$

(voir proposition 2.7.3), de sorte que E_8 est un réseau idéal sur Λ. Le raisonnement s'achève comme dans le résultat précédent, grâce au corollaire 2.5.2, en constatant que $\mathcal{D}(\Lambda/\mathbb{Z}) = \mathrm{N}_{K/\mathbb{Q}}(\mathrm{d}(\Lambda/O_K))\mathrm{d}_K^4 = (q_1 \ldots q_s \mathrm{d}_K)^4$. □

3.9 Ordres maximaux des algèbres de quaternions quadratiques

Dans cette section, nous donnons des familles d'ordres maximaux d'une algèbre de quaternions sur un corps quadratique ainsi qu'une borne de leur minimum euclidien dans les cas où cela est possible. Cette borne utilisera

souvent les résultats de la section précédente.

Nous allons observer les corps de quaternions A sur $K = \mathbb{Q}(\sqrt{d})$ ramifiés uniquement aux deux places infinies de K (dans ce cas K est donc totalement réel).

Proposition 3.9.1. *Soit $A' = (a,b)_K$ un corps de quaternions sur un corps quadratique réel $K = \mathbb{Q}(\sqrt{d})$. Supposons A' ramifié uniquement aux places infinies de K.*

Si $d \equiv 2 \mod 4$, $d \equiv 3 \mod 4$ ou $d \equiv 5 \mod 8$ alors
l'algèbre A' est isomorphe à $A = (-1,-1)_K$.

Si $d \equiv 1 \mod 8$ alors
l'algèbre A' est isomorphe à $A = (-1,-p)_K$ où p est un nombre premier, congru à 3 modulo 4, choisi de telle sorte que d n'est pas un carré dans $\mathbb{F}_p$, ou que p divise d.

Preuve : Deux algèbres de quaternions sur un corps K sont isomorphes si est seulement si leurs places ramifiées coïncident (voir [MR03] théorème 2.7.5, p.100). Il suffit donc, dans chaque cas, de montrer que $\mathrm{Ram}(A) = \{\sigma_1, \sigma_2\}$ où σ_1 et σ_2 sont les deux places infinies de K.

Dans tous les cas, il est clair que $\sigma_1, \sigma_2 \in \mathrm{Ram}(A)$ puisque $A = (a,b)_K$ avec a, b des nombres rationnels négatifs. Il faut donc se convaincre que ce sont les seules places qui sont ramifiées. Nous savons que la seule place finie ramifiée de $A_0 = (-1,-1)_{\mathbb{Q}}$ est 2 (voir proposition 3.7.1), et, par le corollaire 3.8.12, les seuls premiers ramifiés possibles de $A = (-1,-1)_K$ sont au-dessus de 2. Dans les cas $d \equiv 2 \mod 4$ ou $d \equiv 3 \mod 4$, 2 n'est pas totalement décomposé dans A, donc aucun premier de K n'est ramifié dans A.

Il reste à voir le cas $d \equiv 1 \mod 8$. Comme d n'est pas un carré dans $\mathbb{F}_p$ (ou que p divise d), p est inerte (ou ramifié) dans K (voir [Sam67], proposition 1, § 5.4). De plus, par la proposition 3.7.1, le seul premier ramifié de $(-1,-p)_{\mathbb{Q}}$ est p. Le résultat est alors une conséquence directe du corollaire 3.8.12.

□

Proposition 3.9.2. *Soient $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique réel avec $d \equiv 2 \mod 4$ (sans facteur carré) et $A = (-1,-1)_K$ le corps de quaternions non ramifié aux places finies. Notons $\mathcal{P}_2$ l'unique idéal premier de $\mathcal{O}_K$ au-dessus de 2. Précisément, $\mathcal{P}_2 = \langle 2, \sqrt{d} \rangle$ et $\mathcal{P}_2^2 = 2\mathcal{O}_K$. Alors*

$$\Lambda_1(d) = \mathcal{O}_K + \frac{1+i}{2}\mathcal{P}_2 + \frac{1+j}{2}\mathcal{P}_2 + \frac{1+i+j+k}{2}\mathcal{O}_K$$

est un ordre maximal de A.
Si, de plus, $d \equiv 0 \mod 6$ on pose $w = \frac{1+i+j+k}{2}$ et $\mathcal{P}_3 = \langle 3, \sqrt{d} \rangle$, l'unique idéal premier de $\mathcal{O}_K$ au dessus de 3. Alors

$$\Lambda_2(d) = \mathcal{O}_K + \frac{1+w}{3}\mathcal{P}_3 + \frac{j-i}{2}\mathcal{P}_2 + \frac{(1+w)(j-i)}{6}\mathcal{P}_2\mathcal{P}_3$$

est un ordre maximal de A non conjugué au précédent.
Si d vérifie encore $d = 6d'$ avec $d' \not\equiv 3 \mod 4$, alors

$$\Lambda_3(d) = \mathcal{O}_K + \frac{1+i}{2}\mathcal{P}_2 + \frac{j+k+\sqrt{d}}{2}\mathcal{O}_K + \frac{(1+i)(j+k+\sqrt{d})}{4}\mathcal{P}_2$$

est un troisième ordre maximal de A, non conjugué aux précédents.

PREUVE : Si $\Lambda \subset \Gamma$ sont des ordres d'une algèbre de quaternions, alors $\mathrm{d}(\Lambda) \subset \mathrm{d}(\Gamma)$ (voir par exemple [Vig80]). De plus, les ordres maximaux ont tous le même discriminant (voir théorème 1.6.3). Dans notre cas, nous obtenons donc que

$$\Lambda \text{ est un ordre maximal de A si et seulement si } \mathrm{d}(\Lambda/\mathcal{O}_K) = \mathcal{O}_K.$$

Calculons d'abord $\mathrm{d}(\Lambda_1(d)/\mathbb{Z})$. L'ensemble

$$B = \left\{1, \sqrt{d}, 1+i, \sqrt{d}\frac{1+i}{2}, 1+j, \sqrt{d}\frac{1+j}{2}, \frac{1+i+j+k}{2}, \sqrt{d}\frac{1+i+j+k}{2}\right\}$$

est une $\mathbb{Z}$-base de $\Lambda_1(d)$, car $\mathcal{P}_2 = 2\mathbb{Z} + \sqrt{d}\mathbb{Z}$. On peut donc calculer

$$\mathrm{d}(\Lambda_1(d)/\mathbb{Z}) = \det\left(\mathrm{tr}_{A/\mathbb{Q}}(B(s)B(t))_{1\leq s,t\leq 8}\right) = (4d)^4.$$

D'autre part, la proposition 1.8.10 nous assure que

$$\mathrm{d}(\Lambda_1(d)/\mathbb{Z}) = \mathrm{N}_{K/\mathbb{Q}}(\mathrm{d}(\Lambda_1(d)/\mathcal{O}_K))\mathrm{d}_K^4$$

Mais $\mathrm{d}_K = 4d$, donc $\mathrm{N}_{K/\mathbb{Q}}(\mathrm{d}(\Lambda_1(d)/\mathcal{O}_K)) = 1$, c'est-à-dire $\mathrm{d}(\Lambda_1(d)/\mathcal{O}_K) = \mathcal{O}_K$, ce qui montre que si $\Lambda_1(d)$ est un ordre, alors il est maximal. Nous obtenons la preuve que c'est un ordre en vérifiant la stabilité de la multiplication.

Pour $\Lambda_2(d)$ et $\Lambda_3(d)$ la démarche est la même.

Il reste à vérifier que $\Lambda_1(d)$, $\Lambda_2(d)$ et $\Lambda_3(d)$ ne sont pas conjugués dans A. Pour cela nous allons constater que leurs groupes d'unités de norme réduite 1 ne coïncident pas. C'est ce qui est fait dans la sous-section 3.9.1 (voir, en particulier, le corollaire 3.9.14).

□

Proposition 3.9.3. *Soient $d \equiv 3 \mod 4$, sans facteur carré, $K = \mathbb{Q}(\sqrt{d})$ et $A = (-1,-1)_K$, le corps de quaternions non ramifié aux places finies. Notons $\mathcal{P}_2$ l'unique idéal premier de $\mathcal{O}_K$ au-dessus de 2. Précisément, $\mathcal{P}_2 = \langle 2, \sqrt{d}+1\rangle$ et $\mathcal{P}_2^2 = 2\mathcal{O}_K$. Alors*

$$\Lambda_1(d) = \mathcal{O}_K + \frac{1+i}{2}\mathcal{P}_2 + \frac{1+j}{2}\mathcal{P}_2 + \frac{1+i+j+k}{2}\mathcal{O}_K$$

et

$$\Lambda_4(d) = \mathcal{O}_K \oplus i\mathcal{O}_K \oplus \frac{\sqrt{d}+j}{2}\mathcal{O}_K \oplus \frac{\sqrt{d}i-k}{2}\mathcal{O}_K$$

sont deux ordres maximaux non conjugués de A.

Preuve : La démarche est la même que dans la proposition précédente où il est démontré que $\Lambda_1(d)$ est un ordre maximal de A. Nous montrons que $\Lambda_4(d)$ est un ordre en vérifiant la stabilité de la multiplication. Pour voir qu'il est maximal, il faut et il suffit de montrer que son discriminant est $\mathcal{O}_K$.

Le calcul du discriminant de $\Lambda_4(d)$ est facile car c'est un $\mathcal{O}_K$-module libre. En effet, une O_K-base de $\Lambda_4(d)$ est donnée par

$$B_4 = \left\{1, i, \frac{\sqrt{d}+j}{2}, \frac{\sqrt{d}i-k}{2}\right\}.$$

Calculons le discriminant de $\Lambda_4(d)$

$$\mathrm{d}(\Lambda_4(d)/\mathcal{O}_K) = \det\left((\mathrm{tr}_{A/K}(B_4(s)B_4(t))_{1\leq s,t\leq 4}\right)\mathcal{O}_K = \mathcal{O}_K,$$

ce qui prouve que $\Lambda_4(d)$ est un ordre maximal.

Il faut encore vérifier que $\Lambda_1(d)$ et $\Lambda_4(d)$ ne sont pas conjugués dans A. Pour cela nous allons constater que leurs groupes d'unités de norme réduite 1 ne coïncident pas. C'est ce qui est fait dans la sous-section 3.9.1 (voir, en particulier, le corollaire 3.9.11).

□

Proposition 3.9.4. *Soient $d \equiv 5 \mod 8$, sans facteur carré, $K = \mathbb{Q}(\sqrt{d})$ et $A = (-1,-1)_K$, l'algèbre de quaternions non ramifiée aux places finies. Soit encore $s = \frac{1+\sqrt{d}}{2}$. Alors*

$$\Lambda_5(d) = \mathcal{O}_K \oplus i\mathcal{O}_K \oplus \frac{s+(1+s)i+j}{2}\mathcal{O}_K \oplus \frac{1+i+j+k}{2}\mathcal{O}_K$$

est un ordre maximal de A.

PREUVE : La proposition 3.3.6 nous dit qu'il suffit de vérifier que $s^2+s+1 \in 2\mathcal{O}_K$. Comme $s\overline{s} = \frac{1-d}{4}$ et que $1-d \equiv 4 \mod 8$, $\frac{1-d}{4}$ est un entier impair. Considérons $\varphi : \mathcal{O}_K \longrightarrow \mathcal{O}_K/2\mathcal{O}_K$ la surjection canonique ; alors $\varphi(s\overline{s}) = 1$, car $\mathcal{O}_K/2\mathcal{O}_K$ contient $\mathbb{F}_2$. Par conséquent,

$$\varphi(\overline{s}(s^2+s+1)) = \varphi(s+1+\overline{s}) = \varphi(2) = 0,$$

ce qui prouve que $s^2+s+1 \in 2\mathcal{O}_K$, car $\varphi(\overline{s})$ est inversible dans $\mathcal{O}_K/2\mathcal{O}_K$.

□

REMARQUE : Si l'unité fondamentale de K est de la forme $\omega = \frac{a+b\sqrt{d}}{2}$ avec a, b impairs, alors on peut également choisir $s = \omega$. Si, au contraire, l'unité fondamentale est de la forme $a+b\sqrt{d}$, on peut choisir $s = \frac{\omega+1}{2}$.

Proposition 3.9.5. *Soient $d \equiv 1 \mod 8$, sans facteur carré, tel que d n'est pas un carré dans $\mathbb{F}_3$, $K = \mathbb{Q}(\sqrt{d})$ et $A = (-1,-3)_K$, l'algèbre de quaternions non ramifiée aux places finies. Alors*

$$\Lambda_6(d) = \mathcal{O}_K \oplus i\mathcal{O}_K \oplus \frac{(\sqrt{d}+3)+(\sqrt{d}+1)i+2j}{4}\mathcal{O}_K \oplus$$

$$\frac{6+3(\sqrt{d}+3)i-(\sqrt{d}+3)j-2k}{12}\mathcal{O}_K$$

est un ordre maximal de A.

PREUVE : La démarche est la même que dans les propositions précédentes : il faut vérifier que c'est bien un ordre en observant la stabilité de la multiplication et qu'il est maximal en calculant son discriminant.

□

Dans le cas où la norme de l'unité fondamentale de K est négative, le corollaire 3.8.15 nous dit que les ordres maximaux de $A = (-1,-1)_K$ ont un minimum euclidien inférieur à $\frac{\mathrm{d}_K}{16}$. C'est en particulier le cas des ordres $\Lambda_i(d)$ des quatre propositions précédentes.

Proposition 3.9.6. *Soient $K = \mathbb{Q}(\sqrt{d})$ avec $d = 2, 5$ ou 13, et $A = (-1,-1)_K$, alors les ordres maximaux de A sont euclidiens pour la norme réduite.*
C'est en particulier le cas des ordres $\Lambda_1(2), \Lambda_5(5)$ et $\Lambda_5(13)$ définis dans les propositions ci-dessus.

PREUVE : Dans les trois cas de l'énoncé, la norme de l'unité fondamentale est -1. En effet, l'unité fondamentale de $\mathbb{Q}(\sqrt{2})$ est $1+\sqrt{2}$ et $\mathrm{N}_{K/\mathbb{Q}}(1+\sqrt{2}) = -1$, celle de $\mathbb{Q}(\sqrt{5})$ est $\frac{1+\sqrt{5}}{2}$ et $\mathrm{N}_{K/\mathbb{Q}}(\frac{1+\sqrt{5}}{2}) = -1$ et celle de $\mathbb{Q}(\sqrt{13})$ est $\frac{3+\sqrt{13}}{2}$ et $\mathrm{N}_{K/\mathbb{Q}}(\frac{3+\sqrt{13}}{2}) = -1$. Le corollaire 3.8.15 nous dit alors que le minimum euclidien d'un ordre maximal de A est inférieur ou égal à $\frac{\mathrm{d}_K}{16}$. Dans les trois cas cette quantité et strictement inférieure à 1 (pour $d = 2$, $\mathrm{d}_K = 8$, et pour $d = 5$ et $d = 13$, $\mathrm{d}_K = d$).

□

REMARQUE : Ce sont les trois seuls cas pour lesquels la réalisation du réseau E_8 comme réseau idéal de $A = (-1,-1)_K$ nous permet de montrer que les ordres maximaux sont euclidiens.

3.9.1 Unité de norme réduite 1 dans les corps de quaternions quadratiques

Pour que la démonstration des propositions 3.9.2 et 3.9.3 soit complète, il reste à voir que les groupes des unités de norme 1 de $\Lambda_1(d), \Lambda_2(d), \Lambda_3(d)$ sont tous distincts et qu'il en va de même pour $\Lambda_1(d)$ et $\Lambda_4(d)$. Ces résultats sont donnés dans cette section.

Lemme 3.9.7. *Soient K un corps de nombres totalement réel, A un corps de quaternions sur K avec au moins une place infinie σ ramifiée dans A et Λ un ordre maximal de A. Notons*

$$\Sigma : A \longrightarrow \mathbb{H}$$

l'inclusion de A dans les quaternions de Hamilton. Soit Λ^1 le groupe des unité de Λ de norme réduite 1. Alors $\Sigma(\Lambda^1)$ est conjugué à un des groupes finis suivants :

(1) Un groupe cyclique d'ordre n engendré par $s_n = \cos(2\pi/n)+i\sin(2\pi/n)$.

(2) Un groupe dicyclique d'ordre $4n$ engendrés par

$$s_{2n} = \cos(\pi/n) + i\sin(\pi/n) \quad et \quad j.$$

(3) Le groupe binaire tétraédral (d'ordre 24)

$$\mathrm{E}_{24} = \left\{ \pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2} \right\}$$

qui est isomorphe à $\mathrm{SL}_2(\mathbb{F}_3)$.

(4) Le groupe binaire octaédral (d'ordre 48*)*

$$\mathrm{E}_{48} = \mathrm{E}_{24} \cup \left\{ \frac{\sqrt{2}}{2} x \right\}$$

où x parcourt toutes les sommes et différences possibles de deux éléments distincts parmi $\{1, i, j, k\}$.

(5) Le groupe binaire icosaédral (d'ordre 120*)*

$$\mathrm{E}_{120} = \mathrm{E}_{24} \cup \left\{ \frac{x}{2} \right\}$$

où x parcourt tous les produits possibles d'un élément de E_{24} par $i + \tau j + \tau^{-1} k$ où $\tau = \frac{1+\sqrt{5}}{2}$. C'est un groupe isomorphe à $\mathrm{SL}_2(\mathbb{F}_5)$.

Preuve : Remarquons d'abord que Λ^1 est fini. Il est possible d'identifier $\mathbb{H}^1$, les quaternions usuels de norme réduite 1, à la sphère S^3, plongée dans $\mathbb{R}^4$. Comme Λ est un $\mathbb{Z}$-module libre, l'image par Σ de Λ^1, et donc Λ^1 lui-même, est un sous-groupe discret de S^3. La sphère S^3 est un groupe compact, donc Λ^1 est un sous-groupe discret d'un groupe compact ; il est donc fini.
Par le théorème 3.7 du chapitre I (p.17) de [Vig80], les sous-groupes finis de $\mathbb{H}^\times$ sont donnés par la liste de l'énoncé du lemme. Il faut encore vérifier les deux affirmations restantes : $\mathrm{E}_{120} \cong \mathrm{SL}_2(\mathbb{F}_5)$ et $\mathrm{E}_{24} \cong \mathrm{SL}_2(\mathbb{F}_3)$. C'est ce qu'affirme la proposition 3.4 du chapitre V (p.148) de [Vig80].

□

Corollaire 3.9.8. *Soient $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique réel, A un corps de quaternions sur K admettant au moins une place infinie ramifiée, Λ un ordre maximal de A et Λ^1 le groupe des unités de norme réduite* 1*. Les assertions suivantes sont vérifiées.*

i) Si $d \neq 5$ et $d \neq 2$, alors Λ^1 n'est conjugué ni à E_{48} ni à E_{120}.

ii) Si Λ^1 est cyclique, alors il est conjugué au groupe d'ordre n engendré par $\cos(2\pi/n) + i\sin(2\pi/n)$. Les valeurs possibles de n sont les suivantes :

(a) $n = 1, 2, 3, 4, 6$.

(b) $n = 5, 10$ et dans ce cas $d = 5$,

(c) $n = 8$ et dans ce cas $d = 2$,

(d) $n = 12$ et dans ce cas $d = 3$.

iii) Si Λ^1 est conjugué au groupe dicyclique d'ordre $4n$ engendré par $\cos(\pi/n) + i\sin(\pi/n)$ et j, alors les valeurs possibles de n sont :

(a) $n = 1, 2, 3$.

(b) $n = 4$ *et dans ce cas* $d = 2$,

(c) $n = 5$ *et dans ce cas* $d = 5$,

(d) $n = 6$ *et dans ce cas* $d = 3$.

PREUVE : Supposons que Λ^1 est conjugué à E_{48}. Alors il existe $x \in \mathbb{H}^\times$ tel que $\Sigma(\Lambda^1) = x^{-1}\mathrm{E}_{48}x$ où $\Sigma|_K = \sigma$ est la place infinie ramifiée. Or Σ est un homomorphisme de $\mathbb{Q}$-algèbres de A dans $\mathbb{H}$, en particulier, il existe $c = c_0 + ic_1 + jc_2 + kc_3 \in \Lambda^1$ tel que

$$\Sigma(c) = \frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}x^{-1}ix.$$

Notons $A = K \oplus A'$ où A' est l'espace vectoriel, engendré par $\{i, j, k\}$, des quaternions purs. Nous avons $\Sigma(K) = \sigma(K) \subset \mathbb{R}$ et $\Sigma(A') \cap \mathbb{R} = \{0\}$. Notons encore que $x^{-1}ix$ a un terme constant nul pour tout $x \in \mathbb{H}^\times$, ce qui prouve que $\sigma(c_0) = \frac{\sqrt{2}}{2}$. De plus $\sigma(c_0) \in K$, car K est galoisien. Finalement, l'élément $\sqrt{2}$ appartient à K, ce qui n'est possible que lorsque $d = 2$. Le raisonnement dans le cas de E_{120} est identique. Ainsi le premier point de la proposition est démontré.

Supposons maintenant que $\Sigma(\Lambda^1)$ est conjugué au groupe cyclique d'ordre n engendré par $\cos(2\pi/n) + i\sin(2\pi/n)$. Le même raisonnement que dans la première partie de la preuve nous permet de dire que cela force l'élément $\cos(2\pi/n)$ à appartenir à K. En d'autres termes, $\mathbb{Q}(\cos(2\pi/n)) \subset K$. Posons $\zeta = e^{i2\pi/n}$ (ici $i \in \mathbb{C}$). Alors

$$\mathbb{Q}(\cos(2\pi/n)) = \mathbb{Q}(\zeta + \zeta^{-1}).$$

Pour que $\cos(\pi/n) \in K$, il faut que $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}]$ soit égal à 1 ou à 2, mais nous savons que $[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = \frac{\varphi(n)}{2}$, où φ est la fonction d'Euler. Par conséquent

$$[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = 1 \text{ si et seulement si } n = 1, 2, 3, 4, 6$$

et

$$[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = 2 \text{ si et seulement si } n = 5, 8, 10, 12.$$

Dans les cas où $n = 5, 8, 10, 12$, pour que $\mathbb{Q}(\zeta + \zeta^{-1}) \subset K = \mathbb{Q}(\sqrt{d})$, il faut encore que $d = 5$ (si $n = 5$ ou 10), $d = 2$ (si $n = 8$) et $d = 3$ (si $n = 12$). Ceci démontre le deuxième point.

Pour le dernier point, il suffit de suivre la démonstration de la deuxième partie, en remplaçant n par $2n$.

□

Lemme 3.9.9. *Lorsque $d \neq 2$ est un entier positif, sans facteur carré, congru à 2 ou à 3 modulo 4, le groupe des unités de norme réduite 1 de $\Lambda_1(d)$ est E_{24}. Si $d = 2$, alors le groupe des unités de norme 1 de $\Lambda_1(d)$ est E_{48}. (Voir section précédente pour la définition des $\Lambda_i(d)$).*

PREUVE : Rappelons d'abord que $\Lambda_1(d)$ n'est un ordre maximal de $A = (-1,-1)_{\mathbb{Q}(\sqrt{d})}$ que lorsque $d \equiv 2, 3 \mod 4$. Il faut donc se placer dans ce contexte. Il est facile de vérifier que le groupe des unités de norme réduite 1, noté Λ^1, de $\Lambda = \Lambda_1(d)$ contient E_{24}. Le corollaire 3.9.8 nous assure, si $d \neq 2$, que Λ^1 n'est pas conjugué à E_{48} ou à E_{120}. Il est donc égal à E_{24}. Le cas où $d = 2$ se règle en remarquant que $\mathrm{E}_{48} \subset \Lambda_1(2)^1$.

□

Lemme 3.9.10. *Soit $d \equiv 3 \mod 4$ un entier positif sans facteur carré. Si $d \neq 3$ alors le groupe des unités de norme réduite 1 de $\Lambda_4(d)$ est égal à*

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}.$$

Le groupe des unités de norme réduite 1 de $\Lambda_4(3)$ est le groupe dicyclique à 24 éléments engendré par $s'_{12} = \frac{\sqrt{3}+j}{2}$ et k.

PREUVE : Remarquons d'abord qu'aucun conjugué de $w = \frac{1+i+j+k}{2}$ n'appartient à $\Lambda_4(d)^1$. En effet, si $x \in \mathbb{H}^\times$, alors $x^{-1}wx = \frac{1}{2} + ai + bj + ck$ où $a, b, c \in \mathbb{Q}(\sqrt{d})$. Autrement dit, $x^{-1}wx$ est de terme constant $\frac{1}{2}$ pour tout $x \in \mathbb{H}^\times$. Or aucun élément de $\Lambda_4(d)$ n'a pour terme constant $\frac{1}{2}$. Cela nous permet d'affirmer que $\Lambda_4(d)^1$ n'est pas conjugué à E_{24} (ni à E_{48} ni à E_{120}). De plus $\Lambda_4(d)^1$ contient $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$, donc il n'est pas cyclique. La seule possibilité est donc que $\Lambda_4(d)^1$ est conjugué à un groupe dicyclique engendré par $s_{2n} = \cos(\pi/n) + i\sin(\pi/n)$ et j.

Le corollaire 3.9.8 nous dit que, si $d \neq 3$ alors $n = 1, 2$ ou 3. Supposons que $n = 3$. Alors il existe $x \in \mathbb{H}^\times$ tel que $s = x^{-1}(\cos(\pi/3) + i\sin(\pi/3))x = \frac{1}{2} + x^{-1}ix\frac{\sqrt{3}}{2} \in \Lambda_4(d)$. Cela est impossible, car aucun élément de $\Lambda_4(d)$ n'a $\frac{1}{2}$ comme terme constant. Il ne reste donc que $n = 1$ ou 2 comme possibilités, mais Q_8 est le groupe engendré par s_4 et j, donc $\Lambda_4(d)^1 = Q_8$.

Si, au contraire, $d = 3$, il faut vérifier que le groupe G engendré par $s'_{12} = \cos(\pi/6) + j\sin(\pi/6) = \frac{\sqrt{3}+j}{2}$ et k est conjugué au groupe engendré par $s_{12} = \cos(\pi/6) + i\sin(\pi/6)$ et j. Nous vérifions encore que G est bien contenu dans $\Lambda_4(3)$. Comme G est le plus grand groupe possible, étant donné les critères du corollaire 3.9.8, $G = \Lambda_4(3)^1$.

□

Corollaire 3.9.11. *Les ordres maximaux $\Lambda_1(d)$ et $\Lambda_4(d)$ de la proposition 3.9.3 ne sont pas conjugués.*

PREUVE : Les deux lemmes précédents nous assurent que les groupes des unités de norme réduite 1 de ces deux ordres ne sont pas isomorphes.

□

Lemme 3.9.12. *Soit $d \equiv 0 \mod 6$ un entier positif sans facteur carré.*
Si $d \neq 6$, alors le groupe des unités de norme réduite 1 de $\Lambda_2(d)$ est cyclique d'ordre 6, engendré par $w = \frac{1+i+j+k}{2}$.

Le groupe des unités de norme réduite 1 de $\Lambda_2(6)$ est le groupe dicyclique à 12 éléments engendré par $s'_{12} = \frac{1+i+j+k}{2}$ et $\frac{\sqrt{6}}{6}(2-j-k)$.

PREUVE : Des calculs explicites sur un élément générique de $\Lambda_2(d)$ permettent de remarquer que s'il existe $z \in \Lambda_2(d)$ avec $z^2 = -1$, alors $d < 24$. Comme d est un multiple de 6 sans facteur carré, cela ne se produit que si $d = 6$. Voilà qui prouve, si $d \neq 6$, que $\Lambda_2(d)$ ne contient aucun élément d'ordre 4. En particulier, il ne contient aucun conjugué de E_{24} et aucun conjugué du groupe dicyclique d'ordre 12 ou d'ordre 8. Les autres groupes dicycliques possibles sont également exclus par le corollaire 3.9.8. Le groupe cherché est donc un groupe cyclique d'ordre $1, 2, 3, 4$ ou 6 car les autres ordres sont exclus par le corollaire 3.9.8. Le résultat provient alors du fait que $w = \frac{1+i+j+k}{2} \in \Lambda_2(d)$ est de norme réduite 1 et d'ordre 6.

Pour $d = 6$, observons que $\frac{\sqrt{6}}{6}(2-j-k) \in \Lambda_2(6)^1$, ce qui signifie que $\Lambda_2(6)$ ne contient aucun conjugué de E_{24}, E_{48} ou E_{120}, car les conjugués des éléments de ces groupes ne peuvent pas avoir de terme constant dans $\mathbb{Q}(\sqrt{6})$. Donc $\Lambda_2(6)^1$ est dicyclique d'ordre au maximum 12, par le corollaire 3.9.8. Nous pouvons conclure en constatant que w et $\frac{\sqrt{6}}{6}(2-j-k)$ engendrent un groupe d'ordre 12.

□

Lemme 3.9.13. *Soit d avec $d = 6d'$ et $d' \not\equiv 3 \mod 4$ un entier positif sans facteur carré.*
Le groupe des unités de norme réduite 1 de $\Lambda_3(d)$ est égal à

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}.$$

PREUVE : Vérifier que Q_8 est contenu dans $\Lambda_3(d)^1$ est facile. Le corollaire 3.9.8 nous assure que les seules possibilités pour $\Lambda_3(d)$ sont, à conjuguaison près, les trois suivantes :

– Le groupe des quaternions Q_8,
– Le groupe dicyclique engendré par $\frac{1+i\sqrt{3}}{2}$ et j,
– Le groupe binaire tétraédral E_{24}.

Supposons que $\Lambda_3(d)^1$ n'est pas Q_8. Il possède alors un élément d'ordre 6 de la forme $w = \frac{1}{2} + ai + bj + ck$ et son inverse w^γ. Des calculs explicites, en utilisant un élément générique de cette forme dans $\Lambda_3(d)$, permettent de voir qu'il n'existe aucun couple (w, w^γ) avec $w \in \Lambda_3(d)$ satisfaisant les propriétés demandées. Cela prouve que $\Lambda_3(d)^1 = Q_8$.

□

Corollaire 3.9.14. *Soit d un entier positif multiple de 6 et sans facteur carré. Les ordres maximaux $\Lambda_1(d)$, $\Lambda_2(d)$, $\Lambda_3(d)$ donnés dans la proposition 3.9.2 ne sont pas conjugués deux à deux.*

Preuve : Les lemmes 3.9.9, 3.9.12 et 3.9.13 nous assurent que les groupes des unités de norme réduite 1 de ces trois ordres sont toujours non isomorphes deux à deux.

□

3.10 Borne inférieure du minimum euclidien dans le cas totalement défini

Dans le chapitre II, nous avons donné une borne supérieure pour le minimum euclidien d'un ordre maximal d'une algèbre à division sur un corps de nombres. Dans le cas particulier des corps de quaternions totalement défini sur un corps de nombres, il est possible de donner une borne inférieure de ce minimum. C'est le but de cette section.

Lemme 3.10.1. *Soient K un corps de nombres totalement réel, a et b des éléments totalement positifs de K. Alors*

$$\mathrm{N}_{K/\mathbb{Q}}(a+b) \geq \mathrm{N}_{K/\mathbb{Q}}(a)$$

avec égalité si et seulement si $b = 0$.

Preuve : Si n désigne le degré de K sur $\mathbb{Q}$ et $\{\sigma_1, \ldots, \sigma_n\}$ les n plongements

de K dans $\mathbb{R}$, alors

$$\begin{aligned} \mathrm{N}_{K/\mathbb{Q}}(a+b) &= \prod_{i=1}^{n} (\sigma_i(a) + \sigma_i(b)) \\ &= \prod_{i=1}^{n} \sigma_i(a) + \sum \text{ termes positifs} \\ &= \mathrm{N}_{K/\mathbb{Q}}(a) + f(a,b) \end{aligned}$$

où $f(a,b)$ est positif, et nul seulement si $b = 0$.

□

Proposition 3.10.2. *Soient $A = (a,b)_K$ un corps de quaternions totalement défini sur un corps de nombres totalement réel K et Λ un ordre maximal de A. Pour tout $x \in K$,*

$$m_\Lambda(x) = m_K(x)^2.$$

Preuve : Il existe $\alpha \in \Lambda$ tel que $|\mathrm{nr}_{A/\mathbb{Q}}(x-\alpha)| = m_\Lambda(x)$ (voir la proposition 2.2.2). Posons $\alpha = \alpha_0 + i\alpha_1 + j\alpha_2 + k\alpha_3$. Nous obtenons

$$\mathrm{nr}_{A/K}(x-\alpha) = (x-\alpha_0)^2 - a\alpha_1^2 - b\alpha_2^2 + ab\alpha_3^2$$

avec $-a, -b, ab$ totalement positifs dans K. Par le lemme précédent,

$$\begin{aligned} |\mathrm{nr}_{A/\mathbb{Q}}(x-\alpha_0)| &= \mathrm{N}_{K/\mathbb{Q}}(x-\alpha_0)^2 \\ &\leq |\mathrm{N}_{K/\mathbb{Q}}(\mathrm{nr}_{A/K}(x-\alpha))| \\ &= m_\Lambda(x); \end{aligned}$$

or $m_K(x)^2 \leq \mathrm{N}_{A/\mathbb{Q}}(x-\alpha_0)^2$, donc $m_K(x)^2 \leq m_\Lambda(x)$.

Réciproquement, il existe $a \in \mathcal{O}_K$ tel que

$$|\mathrm{N}_{K/\mathbb{Q}}(x-a)|^2 = m_K(x)^2.$$

De plus

$$\begin{aligned} m_\Lambda(x) &\leq |\mathrm{nr}_{A/\mathbb{Q}}(x-a)| \\ &= |\mathrm{N}_{K/\mathbb{Q}}(x-a)^2| \\ &= m_K(x)^2. \end{aligned}$$

□

Corollaire 3.10.3. *Soient A et Λ comme dans la proposition précédente. Alors*

$$\mathrm{M}(\Lambda) \geq \mathrm{M}(K)^2.$$

PREUVE : Nous avons

$$\mathrm{M}(\Lambda) = \sup_{x \in A} m_\Lambda(x) \geq \sup_{x \in K} m_\Lambda(x) = \sup_{x \in K} m_K(x)^2 = \mathrm{M}(K)^2$$

□

Nous pouvons maintenant exploiter cette borne pour discuter l'euclidianité de certains ordres maximaux d'algèbres de quaternions totalement définies. C'est ce que nous allons faire dans la section suivante.

3.11 Corps de quaternions quadratiques réels euclidiens

Dans cette section, A est un corps de quaternions totalement défini sur un corps quadratique réel K, et Λ est un ordre maximal de A. Le but est, dans ce cadre, de déterminer les corps de quaternions qui sont euclidiens pour la norme réduite.

Dans le cas où A est euclidien (ou même seulement principal), il n'existe qu'un seul ordre maximal, à conjuguaison près, dans A. On parlera alors du minimum euclidien de A plutôt que de celui de Λ.

Proposition 3.11.1. *Si A est un corps de quaternions euclidien totalement défini sur un corps quadratique réel, alors $K = \mathbb{Q}(\sqrt{n})$ avec*

$$n \in \{2, 3, 5, 6, 13, 17, 21, 29, 33\}\,.$$

en particulier, K est euclidien.

PREUVE : Comme $\mathrm{M}(A) \geq \mathrm{M}(K)^2$, vu le corollaire 3.10.3, il faut que $\mathrm{M}(K) \leq 1$ pour que A puisse être euclidien. Soit $d = \mathrm{d}_K$, le discriminant de K. Nous savons que si $\mathrm{M}(K) \leq 1$ alors $d \leq 192\sqrt{6} + 472 < 943$ (voir [Lem95], théorème 4.2). Supposons donc que A est principal et que $d \leq 942$. Une formule de masse classique (voir [Vig80], corollaire 2.3, p.142) nous dit que

$$[\Lambda^\times : \mathcal{O}_K^\times]^{-1} = \frac{1}{2} h_K \zeta_K(-1) \prod_{\mathcal{P} \mid \mathrm{D}(\Lambda/\mathcal{O}_K)} (1 - \mathrm{N}_{K/\mathbb{Q}}(\mathcal{P}))$$

où Λ est un ordre maximal de A, h_K est le nombre de classes d'idéaux de K et où le produit est effectué sur les idéaux premiers de K qui divisent le discriminant de Λ.

Pour que cette égalité soit vérifiée, il faut que

$$\frac{2}{h_K \zeta_K(-1)} \in \mathbb{Z}.$$

Dans le cas contraire la formule ci-dessus n'est pas vérifiée et A n'est pas principal. Nous avons vérifier par ordinateur (avec Pari) que pour $2 \leq n \leq 942$ et n sans facteur carré,

$$\frac{2}{h_{\mathbb{Q}(\sqrt{n})} \zeta_{\mathbb{Q}(\sqrt{n})}(-1)} \in \mathbb{Z} \quad \text{si et seulement si} \quad n \in \{2, 3, 5, 6, 13, 17, 21, 29, 33\} .$$

dans tous les autres cas A ne peut être principal et, *a fortiori*, pas euclidien. □

Remarque : Les valeurs de n données sont les valeurs (inférieures à 943) pour lesquelles A peut être principal.

La formule de masse utilisée dans la preuve de la proposition précédente nous permet de calculer précisément les corps de quaternions totalement définis sur un corps quadratique réel qui sont principaux.

Corollaire 3.11.2. *Soient $K = \mathbb{Q}(\sqrt{d})$ un corps quadratique réel euclidien et A un corps de quaternions totalement défini et principal sur K. Alors A est isomorphe à une des* 13 *algèbres apparaissant dans le tableau III.1.*

Remarque : Si A est un corps de quaternions totalement défini, euclidien sur un corps quadratique réel, alors A est isomorphe à une des 13 algèbres apparaissant dans le tableau III.1.

Nom	K	D	A	Λ	M(A)	Euclidien
$2l$	$\mathbb{Q}(\sqrt{2})$	$\mathcal{O}_K$	$(-1,-1)_K$	$\left\{1, \frac{\sqrt{2}}{2}(1+i), \frac{\sqrt{2}}{2}(1+j), \frac{1+i+j+k}{2}\right\}$	$\frac{1}{4} \leq \mathrm{M}(A) \leq \frac{1}{2}$	oui
$2l23$		$\mathcal{P}_2\mathcal{P}_3 = (\sqrt{2}) \cdot (3)$	$(-4\sqrt{2}-11, -3\sqrt{2}-6)_K$	$\left\{1, \frac{1+i}{2}, \frac{4\sqrt{2}-11}{89}(46i+k), \frac{4\sqrt{2}-11}{178}(1+i)(46i+k)\right\}$	$1 \leq \mathrm{M}(A) \leq \frac{49}{9}$	non
$2l25$		$\mathcal{P}_2\mathcal{P}_5 = (\sqrt{2}) \cdot (5)$	$(-12\sqrt{2}-19, -5\sqrt{2}-10)_K$	$\left\{1, \frac{1+i}{2}, \frac{(12\sqrt{2}-19)}{73}(2i+k), \frac{1}{2}j + \frac{12\sqrt{2}-19}{146}(2i+k)\right\}$	$1 \leq \mathrm{M}(A) \leq \frac{196}{25}$	non
$2l27$		$\mathcal{P}_2\mathcal{P}_7 = (\sqrt{2}) \cdot (2\sqrt{2}+1)$	$(-4\sqrt{2}-11, -\sqrt{2}-4)_K$	$\left\{1, \frac{1+i}{2}, \frac{4\sqrt{2}-11}{89}(33i+k), \frac{1}{2} + \frac{1}{2}j + \frac{4\sqrt{2}-11}{178}(33i+k)\right\}$	$1 \leq \mathrm{M}(A) \leq 4$	non
$2l27b$		$\mathcal{P}_2\overline{\mathcal{P}_7} = (\sqrt{2}) \cdot (-2\sqrt{2}+1)$	$(-12\sqrt{2}-19, \sqrt{2}-4)_K$	$\left\{1, \frac{1+i}{2}, \frac{12\sqrt{2}-19}{73}(16i+k), \frac{1}{2}j + \frac{12\sqrt{2}-19}{73}(16i+k)\right\}$	$1 \leq \mathrm{M}(A) \leq 4$	non
$5l$	$\mathbb{Q}(\sqrt{5})$	$\mathcal{O}_K$	$(-1,-1)_K$	$\left\{1, i, \frac{\omega+(1+\omega)i+j}{2}, \frac{1+i+j+k}{2}\right\}$	$\frac{1}{16} \leq \mathrm{M}(A) \leq \frac{5}{16}$	oui
$5l25$		$\mathcal{P}_2\mathcal{P}_5 = (2) \cdot (\sqrt{5})$	$(-12b-11, -2b-4)_K$	$\left\{1, \frac{1+i}{2}, \frac{6\sqrt{5}-17}{109}(105i+k), \frac{1}{2} + \frac{1}{2}j + \frac{6\sqrt{5}-17}{218}(105i+k)\right\}$	$1 \leq \mathrm{M}(A) \leq \frac{5}{2}$	non
$5l211$		$\mathcal{P}_2\mathcal{P}_{11} = (2) \cdot (-3b+1)$	$(3b-10, -4b-6)_K$	$\left\{1, \frac{\sqrt{5}+3}{4} + \frac{1}{2}i, \frac{-3\sqrt{5}-17}{122}(i+k), \frac{1}{2} + \frac{-13\sqrt{5}-33}{244}(i+k) + \frac{1}{2}j\right\}$	$1 \leq \mathrm{M}(A) \leq \frac{81}{16}$	non
$5l211b$		$\mathcal{P}_2\overline{\mathcal{P}_{11}} = (2) \cdot (-3b+2)$	$(-3b-7, -2b-6)_K$	$\left\{1, \frac{\sqrt{5}+1}{4} + \frac{1}{2}i, \frac{3\sqrt{5}-17}{122}(43i+k), \frac{1}{2} + \frac{-7\sqrt{5}-1}{244}(43i+k) + \frac{1}{2}j\right\}$	$1 \leq \mathrm{M}(A) \leq \frac{81}{16}$	non
$13l$	$\mathbb{Q}(\sqrt{13})$	$\mathcal{O}_K$	$(-1,-1)_K$	$\left\{1, i, \frac{\omega+(1+\omega)i+j}{2}, \frac{1+i+j+k}{2}\right\}$	$\frac{1}{9} \leq \mathrm{M}(A) \leq \frac{13}{16}$	oui
$13l23$		$\mathcal{P}_2\mathcal{P}_3 = (2) \cdot (b)$	$(-4b-7, -4b-6)_K$	$\left\{1, \frac{1+i}{2}, \frac{2\sqrt{13}-9}{29}(i+k), \frac{1}{2} + \frac{2\sqrt{13}-9}{58}(i+k) + \frac{1}{2}j\right\}$	$1 \leq \mathrm{M}(A) \leq \frac{25}{4}$	non
$13l23b$		$\mathcal{P}_2\overline{\mathcal{P}_3} = (2) \cdot (-b+1)$	$(-5b-8, -2b-4)_K$	$\left\{1, \frac{3+\sqrt{13}}{4} + \frac{1}{2}i, \frac{5\sqrt{13}-21}{58}(18i+k), \frac{-3\sqrt{13}+1}{116}(18i+k) + \frac{1}{2}j\right\}$	$1 \leq \mathrm{M}(A) \leq \frac{25}{4}$	non
$17l$	$\mathbb{Q}(\sqrt{17})$	$\mathcal{O}_K$	$(-1,-3)_K$	$\left\{1, i, \frac{i+j}{2}, \frac{3+3\sqrt{17}i+\sqrt{17}j+k}{6}\right\}$	$\frac{1}{4} \leq \mathrm{M}(A) \leq \frac{17}{16}$	?

TAB. III.1 – Les 13 corps de quaternions totalement définis principaux sur un corps quadratique réel K avec $\mathrm{M}(K) \leq 1$.

Dans le tableau de la page précédente, la première colonne donne le nom de l'unique ordre maximal Λ de A, la deuxième colonne désigne le corps de base K du corps de quaternions A, la troisième colonne est le discriminant réduit de A, c'est-à-dire $\mathrm{D}^2 = \mathrm{D}(A)$ et, dans cette colonne, b désigne un générateur de $\mathcal{O}_K$ comme $\mathbb{Z}$-module. La quatrième colonne donne un couple (a, b) tel que $A \cong (a, b)_K$, la cinquième colonne donne une $\mathcal{O}_K$-base d'un ordre maximal (unique à conjuguaison près) de $(a, b)_K$ et, dans cette colonne, ω désigne l'unité fondamentale de $\mathcal{O}_K$. L'avant-dernière colonne donne les bornes du minimum euclidien.

Remarque : La borne supérieure du minimum euclidien de A donnée dans le tableau est obtenue en appliquant le corollaire 2.5.2 au réseau $(\Lambda, 1)$, à l'exception des cas où A n'est pas ramifiée aux places finies (i.e. $\mathrm{D} = \mathcal{O}_K$). Dans ces cas, on obtient la borne supérieure en réalisant le réseau E_8 comme on l'a vu dans la section 3.8 de ce chapitre. La borne inférieure, lorsque elle est strictement inférieure à 1, découle du corollaire 3.10.3. Dans le cas contraire elle provient des résultats généraux sur les ordres euclidiens donnés dans la section suivante (voir le corollaire 3.12.5 et les propositions 3.12.9 à 3.12.12). Ces propositions justifient également les "non" de la dernière colonne.

Notons encore que, parmi les 13 corps de quaternions possibles la sixième et la septième colonne nous donnent le résultat suivant.

Corollaire 3.11.3. *Soit A un corps de quaternions euclidien totalement défini sur un corps quadratique réel K.*
Si A n'est pas isomorphe à $(-1,-3)_{\mathbb{Q}(\sqrt{17})}$, alors

$$A \cong (-1,-1)_K$$

où $K = \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{5})$ ou $\mathbb{Q}(\sqrt{13})$.

Afin d'être complet, nous devrions traiter deux cas supplémentaires d'algèbres de quaternions sur un corps quadratique réel. Il s'agit des cas où A est ramifié en au plus une place infinie. Nous ne traiterons pas ces deux situations en détail. Dans le cas où aucune place infinie n'est ramifiée, on peut tout de même énoncer le résultat partiel suivant :

Proposition 3.11.4. *Soient K un corps quadratique réel et A un corps de quaternions totalement indéfini sur K. Si A est euclidien alors K est principal et si K est euclidien alors A est euclidien.*

Preuve : On sait que le nombre de classes d'idéaux à droite de A et de K sont les mêmes (voir la proposition 3.4.1), ce qui montre la première

affirmation. La seconde affirmation est une conséquence du fait que, si K est principal, alors $\mathrm{M}(A) \leq \mathrm{M}(K)$ (voir le théorème 3.4.10).

□

Nous terminerons par un cas particulier qui nous fournit à la fois un exemple où le minimum euclidien atteint la borne supérieure donnée dans la section 2.5 du chapitre II, et un exemple de corps de quaternions quadratique (non-euclidien) de minimum 1.

Proposition 3.11.5. *Soient $K = \mathbb{Q}(\sqrt{3})$, $A = (-1,-1)_K$ et*

$$\Lambda = \mathcal{O}_K \oplus \frac{1+i}{2}(\sqrt{3}+1)\mathcal{O}_K \oplus \frac{1+j}{2}(\sqrt{3}+1)\mathcal{O}_K \oplus \frac{1+i+j+k}{2}\mathcal{O}_K$$

l'un des deux ordres maximaux non conjugués de A. Alors

$$\mathrm{M}(\Lambda) = 1.$$

De plus A n'est pas euclidien pour la norme réduite

Preuve : Considérons γ l'involution canonique sur A et le réseau $L = (\Lambda, \frac{1}{2}, \gamma)$. Alors L est un réseau irréductible, pair, de minimum 2, de déterminant 81 et de maximum 2. Par le corollaire 2.5.2,

$$\mathrm{M}(\Lambda) \leq \left(\frac{\max(L)}{\det(L)^{\frac{1}{8}}\gamma_{\min}(\Lambda)}\right)^2 = \frac{4\mathrm{d}_K}{16\det(L)^{\frac{1}{4}}} = 1.$$

D'autre part, Λ n'est pas principal donc $\mathrm{M}(\Lambda) \geq 1$.

□

3.12 Ordres maximaux non euclidiens

Dans cette section K désigne un corps de nombres totalement réel et $A = (a,b)_K$ est une algèbre de quaternions sur K admettant au moins une place infinie ramifiée.

Proposition 3.12.1. *Soient $\mathcal{O}_K$ l'anneau des entiers de K, Λ un ordre maximal de A et Λ^1 le groupe multiplicatif des unités de norme 1 de Λ. Soit $\mathfrak{m}$ un idéal maximal à droite de Λ. Notons $I_{\mathfrak{m}}$ l'image de l'application canonique $\mathcal{O}_K^\times \longrightarrow \mathcal{O}_K/(\mathfrak{m} \cap \mathcal{O}_K)$. Si les conditions suivantes sont vérifiées*

1. *pour tout idéal maximal* $\mathfrak{m}$ *à droite de* Λ *tel que* $\mathfrak{m} \cap \mathbb{Z} = p\mathbb{Z}$ *et* p *est un premier impair, on a*

$$|I_{\mathfrak{m}}| \cdot |\Lambda^1| \cdot [\Lambda^\times : \Lambda^1 \mathcal{O}_K^\times] + 1 < \mathrm{N}_{A/\mathbb{Q}}(\mathfrak{m}),$$

2. *pour tout idéal maximal* $\mathfrak{m}$ *à droite de* Λ *tel que* $\mathfrak{m} \cap \mathbb{Z} = 2\mathbb{Z}$*, on a*

$$|I_{\mathfrak{m}}| \cdot |\Lambda^1| \cdot [\Lambda^\times : \Lambda^1 \mathcal{O}_K^\times] + 2 < 2\mathrm{N}_{A/\mathbb{Q}}(\mathfrak{m}),$$

alors Λ *n'est pas euclidien à droite.*

Preuve : Supposons que Λ est euclidien à droite. Par le corollaire 2.1.11, il existe $b \in \Lambda \backslash \Lambda^\times$ tel que l'application canonique $\Lambda^\times \cup \{0\} \longrightarrow \Lambda/b\Lambda$ est surjective. Soit $\mathfrak{m}$ un idéal maximal à droite de Λ tel que $bA \subset \mathfrak{m}$. Alors l'application canonique

$$\varphi_{\mathfrak{m}} : \Lambda^\times \cup \{0\} \longrightarrow \Lambda/\mathfrak{m}$$

est encore surjective. Remarquons d'abord que

$$|\varphi_{\mathfrak{m}}(\Lambda^1 \mathcal{O}_K^\times)| = |\varphi_{\mathfrak{m}}(\Lambda^1)| \cdot |\varphi_{\mathfrak{m}}(\mathcal{O}_K^\times)|.$$

En effet, $\varphi_{\mathfrak{m}} : \Lambda^\times \to \Lambda \to \Lambda/\mathfrak{m}$ et la deuxième application est un homomorphisme de $\mathcal{O}_K$-modules. Soient $s_1, \ldots, s_r$ des représentants des classes de $\Lambda^\times/\Lambda^1\mathcal{O}_K^\times$. Alors

$$\Lambda^\times = \bigcup_{i=1}^{r} s_i \Lambda^1 \mathcal{O}_K^\times,$$

de sorte que

$$|\varphi_{\mathfrak{m}}(\Lambda^\times)| \leq \sum_{i=1}^{r} |\varphi_{\mathfrak{m}}(s_i \Lambda^1 \mathcal{O}_K^\times)| = |\varphi_{\mathfrak{m}}(\mathcal{O}_K^\times)| \cdot \sum_{i=1}^{r} |\varphi_{\mathfrak{m}}(s_i \Lambda^1)|. \qquad \text{(III.3)}$$

Finalement, comme Λ^1 est fini, $|\varphi_{\mathfrak{m}}(s_i\Lambda^1)| \leq |\Lambda^1|$. Nous avons donc que

$$|\varphi_{\mathfrak{m}}(\Lambda^\times)| \leq |I_{\mathfrak{m}}| \cdot |\Lambda^1| \cdot [\Lambda^\times : \Lambda^1 \mathcal{O}_K^\times].$$

Comme $\varphi_{\mathfrak{m}}$ est surjective,

$$|I_{\mathfrak{m}}| \cdot |\Lambda^1| \cdot [\Lambda^\times : \Lambda^1 \mathcal{O}_K^\times] + 1 \geq |\varphi(\Lambda^\times)| + 1 = |\Lambda/\mathfrak{m}| = \mathrm{N}_{A/\mathbb{Q}}(\mathfrak{m}).$$

Cette inégalité est en contradiction avec la première condition de l'énoncé. Autrement dit, si 1. est vérifiée, alors pour tout idéal maximal $\mathfrak{m}$ tel que $\mathfrak{m} \cap \mathbb{Z}$ est un premier impair, $\varphi_{\mathfrak{m}}$ n'est pas surjective. Comme A est euclidien, il existe un idéal maximal $\mathfrak{m}$ tel que $\varphi_{\mathfrak{m}}$ est surjective. Nous pouvons donc

supposer qu'un tel idéal maximal est au-dessus de 2. Dans ce cas, $\varphi_{\mathfrak{m}}(1) = \varphi_{\mathfrak{m}}(-1)$, donc

$$|\varphi(s\Lambda^1)| \leq \frac{|\Lambda^1|}{2}$$

pour tout $s \in \Lambda^\times$. L'inégalité III.3 devient alors

$$|\varphi(\Lambda^\times)| \leq |I_{\mathfrak{m}}| \cdot \frac{|\Lambda^1|}{2} \cdot [\Lambda^\times : \Lambda^1\mathcal{O}_K^\times].$$

Pour avoir la surjectivité il faut donc que

$$\frac{|I_{\mathfrak{m}}| \cdot |\Lambda^1| \cdot [\Lambda^\times : \Lambda^1\mathcal{O}_K^\times]}{2} + 1 \geq |\varphi(\Lambda^\times)| + 1 = |\Lambda/\mathfrak{m}| = \mathrm{N}_{A/\mathbb{Q}}(\mathfrak{m})$$

ce qui est impossible si la deuxième condition de l'énoncé est vérifiée. Nous avons donc démontré que si 1. et 2. sont vérifiées, alors $\varphi_{\mathfrak{m}}$ n'est jamais surjective, et donc A n'est pas euclidien à droite.

□

Corollaire 3.12.2. *Soit Λ un ordre maximal de A. Notons $f(\mathcal{P}|p)$ le degré résiduel de l'idéal premier $\mathcal{P}$ de $\mathcal{O}_K$ au-dessus de $p \in \mathbb{Z}$. Supposons que les deux conditions suivantes sont vérifiées :*

1. pour tout idéal premier $\mathcal{P}$ au-dessus d'un premier impair p,

$$|\Lambda^1| \cdot [\Lambda^\times : \Lambda^1\mathcal{O}_K^\times] < p^{f(\mathcal{P}|p)} + 1,$$

2. pour tout idéal dyadique $\mathcal{P}$,

$$|\Lambda^1| \cdot [\Lambda^\times : \Lambda^1\mathcal{O}_K^\times] < 2 \cdot (2^{f(\mathcal{P}|2)} + 1).$$

Alors Λ n'est pas euclidien à droite.

Preuve : Soient p un nombre premier impair, $\mathfrak{m}$ un idéal maximal à gauche de Λ au-dessus de p et $\mathcal{P} = \mathfrak{m} \cap \mathcal{O}_K$. Nous savons que $\mathrm{N}_{A/K}(\mathfrak{m}) = \mathcal{P}^2$ (voir [Rei03], théorème 24.13, p.215), de sorte que $\mathrm{N}_{A/\mathbb{Q}}(\mathfrak{m}) = p^{2f(\mathcal{P}|p)}$. De plus $I_{\mathfrak{m}}$, l'image de l'application canonique $\mathcal{O}_K^\times \to \mathcal{O}_K/(\mathfrak{m} \cap \mathcal{O} : K)$, est de cardinal inférieur ou égal à $|\mathcal{O}_K/\mathcal{P}| - 1$, où le"$-1$" vient du fait que $\mathcal{P}$ ne contient pas d'unité, et $|\mathcal{O}_K/\mathcal{P}| = \mathrm{N}_{K/\mathbb{Q}}(\mathcal{P}) = p^{f(\mathcal{P}|p)}$. Supposons que

$$|\Lambda^1| \cdot [\Lambda^\times : \Lambda^1\mathcal{O}_K^\times] < p^{f(\mathcal{P}|p)} + 1.$$

Alors

$$|\Lambda^1] \cdot [\Lambda^\times : \Lambda^1\mathcal{O}_K^\times] \cdot |I_{\mathfrak{m}}| \leq |\Lambda^1| \cdot [\Lambda^\times : \Lambda^1\mathcal{O}_K^\times] \cdot (p^{f(\mathcal{P}|p)} - 1) < p^{2f(\mathcal{P}|p)} - 1$$

et il en va de même avec la seconde condition. Le résultat est alors une conséquence directe de la proposition précédente.

□

Il est important de noté que nous avons donner, au passage, une caractérisation de la surjectivité de l'application canonique $\Lambda^\times \cup \{0\} \to \Lambda/\mathfrak{m}$, où $\mathfrak{m}$ est un idéal maximal à droite de Λ. Cette caractérisation s'énonce de la façon suivante.

Corollaire 3.12.3. *Soit Λ un ordre maximal de A. Notons $f(\mathcal{P}|p)$ le degré résiduel de l'idéal premier $\mathcal{P}$ de $\mathcal{O}_K$ au-dessus de $p \in \mathbb{Z}$. Soit $\mathfrak{m}_\mathcal{P}$ un idéal maximal à droite de Λ contenant $\mathcal{P}\Lambda$. Si p est impair et que*

$$|\Lambda^1| \cdot [\Lambda^\times : \Lambda^1 \mathcal{O}_K^\times] < p^{f(\mathcal{P}|p)} + 1$$

ou si $p = 2$ et que

$$|\Lambda^1| \cdot [\Lambda^\times : \Lambda^1 \mathcal{O}_K^\times] < 2 \cdot (2^{f(\mathcal{P}|2)} + 1),$$

alors l'application canonique

$$\varphi_{\mathfrak{m}_\mathcal{P}} : \Lambda^\times \cup \{0\} \longrightarrow \Lambda/\mathfrak{m}_\mathcal{P}$$

n'est pas surjective.

Preuve : En suivant la preuve des deux résultats précédents, nous constatons que nous avons démontré ce résultat intermédiaire.

□

Ces deux corollaires vont nous permettre de prouver que certains des ordres maximaux apparaissant dans le tableau III.1 ne sont pas euclidiens. Commençons par le résultat suivant qui simplifiera les calculs.

Lemme 3.12.4. *Soit Λ l'un des ordres de la table III.1. Alors*

$$\Lambda^\times = \Lambda^1 \mathcal{O}_K^\times.$$

Preuve : Soit $w = [\Lambda^\times : \mathcal{O}_K^\times]$. Comme Λ est principal, nous savons, par une formule de masse classique, que

$$w = \left(\zeta_K(-1) \prod_{\mathcal{P}|D} (\mathrm{N}(\mathcal{P}) - 1) \right)^{-1}$$

où D est le discriminant réduit de Λ, autrement dit $\mathrm{d}(\Lambda) = D^2$. Remarquons que

$$[\Lambda^\times : \Lambda^1\mathcal{O}_K^\times] = \frac{2w}{|\Lambda^1|}.$$

En effet, le noyau de l'homomorpisme surjectif $\Lambda^\times/\mathcal{O}_K^\times \longrightarrow \Lambda^\times/\Lambda^1\mathcal{O}_K^\times$ est $\Lambda^1\mathcal{O}_K^\times/\mathcal{O}_K^\times \cong \Lambda^1/(\Lambda^1 \cap \mathcal{O}_K^\times) = \Lambda^1/\{\pm 1\}$, donc

$$[\Lambda^\times : \mathcal{O}_K^\times] = [\Lambda^\times : \Lambda^1\mathcal{O}_K^\times] \cdot \left|\Lambda^1/\{\pm 1\}\right|.$$

Nous vérifions que pour tous les ordres du tableau, $\frac{2w}{|\Lambda^1|} = 1$.

□

Ce lemme nous permet d'appliquer le corollaire 3.12.2 en ne tenant compte que de la cardinalité de Λ^1.

Corollaire 3.12.5. *Les ordres maximaux 2l25, 5l211, 5l211b de la table III.1 ne sont pas euclidiens à droite. En particulier leur minimum euclidien pour la norme réduite est supérieur ou égal à* 1.

Preuve : Un calcul permet d'obtenir les unités de norme 1 de ces différents ordres. Nous avons $2l25^1 = \{\pm 1\}$, $5l211^1$ est le groupe cyclique d'ordre 4 engendré par $1 + \frac{-7\sqrt{5}+1}{122}(i+k)$, et $5l211b^1$ est le groupe cyclique d'ordre 4 engendré par $1 + \frac{7\sqrt{5}+1}{122}i + \frac{3\sqrt{5}-17}{122}k$. Il suffit alors d'appliquer le corollaire 3.12.2.

1. Pour $\Lambda = 2l25$, $|\Lambda^1| = 2$ et $2 < p^f + 1$ pour tout premier p et tout entier positif f, ce qui prouve que $2l25$ n'est pas euclidien à droite.
2. Pour $\Lambda = 5l211$, $|\Lambda^1| = 4$ et $4 \geq p^f + 1$ si et seulement si $1 \leq p^f \leq 3$, mais 3 est inerte dans $K = \mathbb{Q}(\sqrt{5})$, donc $f(3\mathcal{O}_K|3) = 2$ et donc $4 < p^{f(\mathcal{P}|p)} + 1$ pour tout premier impair p. De plus $4 < 2(2^f + 1)$ pour tout entier positif f, ce qui prouve que $5l211$ n'est pas euclidien.
3. Le cas $\Lambda = 5l211b$ est identique au précédent.

□

Dans certains cas, la borne sur les unités de norme 1 est insuffisante pour conclure que l'ordre n'est pas euclidien. En affinant le résultat, on peut parfois arriver facilement à la même conclusion. Dans ce but, énonçons d'abord le résultat suivant sur le nombre d'idéaux maximaux à droite de Λ contenant un premier $\mathcal{P}$ donné de $\mathcal{O}_K$.

Lemme 3.12.6. *Soient A une algèbre de quaternions sur un corps de nombres galoisien K et Λ un ordre maximal de A. Soient p un nombre premier et $f = f(p)$ le degré résiduel de p. Notons encore $\mathcal{P}_1, \ldots, \mathcal{P}_r$ les idéaux premiers de $\mathcal{O}_K$ au-dessus de p. Posons*

$$B(n) = \left\{ I \subset \Lambda \mid I \text{ est un idéal à droite de } \Lambda \text{ et } \mathrm{nr}_{A/\mathbb{Q}}(I) = n \right\}$$

et $b(n) = |B(n)|$. Définissons encore l'ensemble d'idéaux premiers suivants :

$$\mathrm{Ram}_p(A) = \{\mathcal{P} \subset \mathcal{O}_K \mid \mathcal{P} \text{ divise } p \text{ et } \mathcal{P} \in \mathrm{Ram}_f(A)\}$$

et notons s le cardinal de $\mathrm{Ram}_p(A)$. Alors

1. *$B(p^f)$ est l'ensemble des idéaux maximaux à droite de Λ qui contiennent $\mathcal{P}_i\Lambda$ pour un certain $1 \leq i \leq r$.*
2. *Le cardinal de $B(p^f)$ est donné par*
$$b(p^f) = s + (1 + p^f)(r - s).$$
3. *Soit $\mathcal{P}_i$ un idéal au-dessus de p, ramifié dans A. Alors il existe un unique idéal maximal $\mathfrak{m}$ à droite de Λ contenant $\mathcal{P}_i\Lambda$. De plus $\mathfrak{m}$ est un idéal premier bilatère et $\mathcal{P}_i\Lambda = \mathfrak{m}^2$.*
4. *Soit $a(\mathcal{P})$ le nombre d'idéaux maximaux à droite de Λ contenant $\mathcal{P}\Lambda$. Alors*
$$\sum_{\mathcal{P}|p, \mathcal{P} \notin \mathrm{Ram}_p(A)} a(\mathcal{P}) = (1 + p^f)(r - s).$$

Preuve : Montrons d'abord la première assertion.

Soit I un idéal à droite de Λ tel que $\mathrm{nr}_{A/\mathbb{Q}}(I) = p^f$. Alors $\mathrm{nr}_{A/K}(I) = \mathcal{P}_i$, puisque $\mathrm{nr}_{A/\mathbb{Q}} = \mathrm{N}_{K/\mathbb{Q}} \circ \mathrm{nr}_{A/K}$ et que $\mathrm{N}_{K/\mathbb{Q}}(J) = p^f$ si et seulement si $J = \mathcal{P}_i$ pour un $1 \leq i \leq r$. Donc I est maximal. En effet, dans le cas contraire, il existerait un idéal $M \supsetneq I$ propre, et alors $\mathrm{nr}_{A/K}(I) = \mathcal{P}_i \subsetneq \mathrm{nr}_{A/K}(M) \subsetneq \mathcal{O}_K$ ce qui est absurde. Réciproquement, si $\mathfrak{m}$ est un idéal maximal contenant $\mathcal{P}_i\Lambda$, alors $\mathrm{nr}_{A/K}(\mathfrak{m}) = \mathcal{P}_i$ (voir [Rei03] théorème 24.13, p. 215), et donc $\mathrm{nr}_{A/\mathbb{Q}}(\mathfrak{m}) = p^f$.

Montrons la troisième assertion.

Soit $\mathfrak{m}$ un idéal maximal à droite de Λ contenant $\mathcal{P}_i\Lambda$. On sait que

$$\mathfrak{P} = \mathrm{ann}_\Lambda\ \Lambda/\mathfrak{m}$$

est l'unique idéal premier bilatère contenu dans $\mathfrak{m}$ (voir [Rei03], théorème 22.15, p.195). De plus, comme $\mathcal{P}_i$ est ramifié dans A, on a $\mathcal{P}_i\Lambda = \mathfrak{P}^2$ (voir

[Rei03], théorème 32.1, p.273), de sorte que $\mathrm{nr}_{A/K}(\mathfrak{P}) = \mathcal{P}_i$ et donc $\mathfrak{P}$ est maximal comme idéal à droite de Λ (voir preuve de 1.). Nous avons donc montré que $\mathfrak{m} = \mathfrak{P}$.

Montrons la deuxième assertion.

Considérons

$$\zeta_A(s) = \sum_{I \subset \Lambda} \mathrm{N}_{A/\mathbb{Q}}(I)^{-s}$$

où s est un nombre complexe avec $\mathrm{Re}(s) > 1$, et I parcourt les idéaux à droite de Λ, et

$$\zeta_{A_\mathcal{P}}(s) = \sum_{I \subset \Lambda_\mathcal{P}} \mathrm{N}_{A_\mathcal{P}/\mathbb{Q}_p}(I)^{-s}$$

où s est un nombre complexe avec $\mathrm{Re}(s) > 1$, I parcourt les idéaux à droite de $\Lambda_\mathcal{P}$ et $\mathcal{P}$ est un idéal premier de $\mathcal{O}_K$.
Soit $b_\mathcal{P}(p^e) = \sharp\{I \subset \Lambda_\mathcal{P} \mid I \text{ idéal à droite de } \Lambda_\mathcal{P} \text{ tel que } \mathrm{nr}_{A_\mathcal{P}/\mathbb{Q}_p}(I) = p^e\}$. Notons que $b_\mathcal{P}(p^e) = 0$ si f ne divise pas e. Nous savons que $\mathrm{nr}_{A/\mathbb{Q}}(I)^2 = \mathrm{N}_{A/\mathbb{Q}}(I)$ pour tout idéal I (et de même localement). De plus

$$\zeta_A(s) = \prod_\mathcal{P} \zeta_{A_\mathcal{P}}(s)$$

(voir [Vig80], chapitre III, §2, p.64). Avec les notations ci-dessus, il vient alors

$$\zeta_A(s) = \sum_{n=1}^{\infty} \frac{b(n)}{n^{2s}} = \prod_\mathcal{P} \sum_{e=0}^{\infty} \frac{b_\mathcal{P}(p^e)}{p^{2es}}.$$

En comparant les coefficients et en utilisant le fait que $b_\mathcal{P}(p^e)$ est nul si f ne divise pas e, nous voyons que

$$b(p^f) = \sum_{\mathcal{P}|p} b_\mathcal{P}(p^f).$$

Le lemme 4.1 du § 4 du chapitre III de [Vig80] (p.48) nous donne la valeur de $b_\mathcal{P}(p^f)$:

$$b_\mathcal{P}(p^f) = \begin{cases} 1 & \text{si } \mathcal{P} \in \mathrm{Ram}_f(A) \\ 1 + p^f & \text{sinon} \end{cases}$$

ce qui nous permet de conclure.

Montrons la quatrième assertion.

En utilisant 1., 2. et 3., on trouve

$$s + (1 + p^f)(r - s) = b(p^f) = \sum_{\mathcal{P}|p} a(\mathcal{P}) =$$

$$= \sum_{\mathcal{P}\in \mathrm{Ram}_p(A)} a(\mathcal{P}) + \sum_{\mathcal{P}|p, \mathcal{P}\notin \mathrm{Ram}_p(A)} a(\mathcal{P}) = s + \sum_{\mathcal{P}|p, \mathcal{P}\notin \mathrm{Ram}_p(A)} a(\mathcal{P})$$

d'où le résultat.

□

Nous utiliserons également le résultat suivant :

Lemme 3.12.7. *Soient A une algèbre séparable sur un corps K, Λ un ordre maximal de A, $\mathfrak{m}$ un idéal maximal à droite de Λ. Si I et J sont des idéaux bilatères de Λ tels que $IJ \subset \mathfrak{m}$, alors $I \subset \mathfrak{m}$ ou $J \subset \mathfrak{m}$.*

PREUVE : Soit $\mathfrak{P} = \mathrm{ann}_\Lambda\, \Lambda/\mathfrak{m}$ l'unique idéal bilatère premier contenu dans $\mathfrak{m}$ (voir [Rei03], thm 22.15, p.195). Si $IJ \subset \mathfrak{m}$, alors $IJ \subset \mathfrak{P}$ et comme $\mathfrak{P}$ est premier soit $I \subset \mathfrak{P} \subset \mathfrak{m}$ soit $J \subset \mathfrak{P} \subset \mathfrak{m}$.

□

Enonçons encore un résultat technique que nous utiliserons abondamment dans les preuves des résultats 3.12.9 à 3.12.12.

Lemme 3.12.8. *Soient A une algèbre de quaternions sur un corps de nombres K, Λ un ordre maximal de A, $\mathfrak{m}$ un idéal maximal à droite de Λ et $s\Lambda$ un idéal bilatère de Λ. On considère encore la surjection canonique*

$$\varphi : \Lambda \longrightarrow \Lambda/\mathfrak{m}$$

et un sous-ensemble T de Λ. Supposons qu'il existe $a \in \mathcal{O}_K$ tel que

$$\varphi(s^2) = \overline{a}^2 \in \mathcal{O}_K/\mathcal{P}$$

où $\mathcal{P} = \mathcal{O}_K \cap \mathfrak{m}$ et supposons que $aT \subset T$. Alors

$$\varphi(T \cup sT) = \varphi(T).$$

PREUVE : Par hypothèse, $(s-a)(s+a) \in \mathfrak{m}$. Comme $(s-a)\Lambda$ et $(s+a)\Lambda$ sont des idéaux bilatères, $s-a \in \mathfrak{m}$ ou $s+a \in \mathfrak{m}$ (voir le lemme précédent). Sans perte de généralité, supposons que $s-a \in \mathfrak{m}$. Remarquons que $\varphi(su) = \varphi(au)$ pour tout $u \in \Lambda$. En effet, $\varphi(au) - \varphi(su) = \varphi(au - su) = \varphi((a-s)u) = 0$ car $(a-s)u \in \mathfrak{m}$. Ainsi

$$\varphi(sT) = \overline{a}\varphi(T) = \varphi(aT) \subset \varphi(T).$$

Finalement $\varphi(T \cup sT) = \varphi(T) \cup \varphi(sT) = \varphi(T)$.

□

Proposition 3.12.9. *L'ordre 2l23 de la table III.1 n'est pas euclidien à droite. En particulier son minimum euclidien pour la norme réduite est supérieur ou égal à* 1.

PREUVE : Dans toute la preuve, $\mathfrak{m}_{\mathcal{P}}$ désigne un idéal maximal à droite de Λ contenant $\mathcal{P}\Lambda$ et $\mathcal{P}$ est un idéal premier de $\mathcal{O}_K$. Posons $\Lambda = 2l23$. Le groupe Λ^1 des unités de norme 1 est le groupe cyclique d'ordre 6 engendré par $\frac{1}{2} + \frac{12\sqrt{2}-33}{178}i + \frac{4\sqrt{2}-11}{89}k$. Dans la section 2.1 du chapitre II, nous avons défini des suites de sous-ensembles de Λ notées $(\Lambda_i)_{i\in\mathbb{N}}$ et $(\Lambda'_i)_{i\in\mathbb{N}}$. Ici, $\Lambda_0 = \{0\}$, $\Lambda_1 = \Lambda^\times \cup \{0\}$ et $\Lambda'_2 = \Lambda_1$ (voir la définition 2.1.9 et la preuve du corollaire 2.1.11). L'ensemble Λ_2 est l'ensemble des $s \in \Lambda$ tels que l'application canonique

$$\varphi_s : \Lambda'_2 \longrightarrow \Lambda/s\Lambda$$

est surjective. Les premiers 3 et 5 sont inertes dans $K = \mathbb{Q}(\sqrt{2})$, donc de degré résiduel 2, et $|\Lambda^1| = 6 < 3^2 + 1 < 5^2 + 1$. Le corollaire 3.12.3 nous assure que, si $s\Lambda \subset \mathfrak{m}_3$ ou $s\Lambda \subset \mathfrak{m}_5$, alors φ_s n'est pas surjective. De plus $|\Lambda^1| = 6 < p^f + 1$ pour tout $p \geq 7$ et tout $f \geq 1$. Donc que φ_s ne peut être surjective que si $s \in \mathfrak{m}_{(\sqrt{2})}$. Mais $|\Lambda^1| = 6 = 2(2+1)$ donc, si $s\Lambda$ est proprement inclus dans $\mathfrak{m}_{(\sqrt{2})}$, alors φ_s n'est pas surjective. Nous pouvons ainsi nous restreindre à l'étude de $\mathfrak{m}_{(\sqrt{2})}$.

Comme $(\sqrt{2})$ est ramifié dans A (voir le tableau III.1), $\sqrt{2}\Lambda = \mathfrak{P}^2$ où $\mathfrak{P}$ est l'unique idéal maximal à droite de Λ au-dessus de $(\sqrt{2})$ et $\mathfrak{P}$ est bilatère (voir le lemme 3.12.6). Soit t un générateur de $\mathfrak{P}$ (il est possible de choisir $t = \frac{-6\sqrt{2}-28}{89}i + \frac{-4\sqrt{2}+11}{89}k$), Nous vérifions que φ_t est effectivement surjective. Nous avons donc démontré que $\Lambda_2 = t\Lambda^\times \cup \Lambda_1 = t\Lambda^\times \cup \Lambda^\times \cup \{0\}$.

La démarche est la même pour calculer Λ_3.

Nous avons $\Lambda'_3 = \Lambda_2$ et nous cherchons les $s \in \Lambda$, qui ne sont pas déjà dans Λ_2, tels que l'application canonique :

$$\varphi_s : \Lambda'_3 \longrightarrow \Lambda/s\Lambda$$

est surjective. Si $s\Lambda$ contient 2 et aucun premier impair, qu'il est proprement inclus dans $\mathfrak{P}$, alors $s\Lambda \subset \sqrt{2}\Lambda$, car $\beta^2 = \sqrt{2}\Lambda$. Ainsi, si φ_s est surjective, alors $\varphi_{\sqrt{2}}$ l'est. Nous allons voir que $|\mathrm{Im}\varphi_{\sqrt{2}}| \leq 10$. En effet,

$$|\varphi_s(\Lambda^\times)| \leq \left(|\mathcal{O}_K/\sqrt{2}\mathcal{O}_K| - 1\right)\frac{|\Lambda^1|}{2} = 3$$

et donc $|\varphi_{\sqrt{2}}(\{0\} \cup \Lambda^\times \cup s\Lambda^\times)| \leq 1 + 3 + 3 = 10$. Comme

$$\left|\Lambda/\sqrt{2}\Lambda\right| = \mathrm{N}_{A/\mathbb{Q}}(\sqrt{2}) = 16$$

cela veut dire que φ_s n'est pas surjective si $s\Lambda$ contient 2, aucun premier impair et qu'il est proprement inclus dans $\mathfrak{P}$.

Nous pouvons donc nous intéresser aux idéaux qui sont contenu dans un $\mathfrak{m}_\mathcal{P}$ où $\mathcal{P}$ est au-dessus d'un premier impair. Soient $\mathcal{P}$ un idéal premier de $\mathcal{O}_K = \mathbb{Z}[\sqrt{2}]$ et $\mathfrak{m}_\mathcal{P} = x\Lambda$ un idéal maximal à droite de Λ tel que $x\Lambda \cap \mathcal{O}_K = \mathcal{P}$. Notons encore $p\mathbb{Z} = \mathcal{P} \cap \mathcal{O}_K$ et supposons p impair. Pour les mêmes raisons que dans le cas dyadique,

$$|\mathrm{Im}\varphi_x| \leq 1 + |\Lambda^1| \cdot (p^{f(\mathcal{P}|p)} - 1) + |\Lambda^1| \cdot (p^{f(\mathcal{P}|p)} - 1) = 12p^{f(\mathcal{P}|p)} - 11.$$

D'un autre côté,

$$|\Lambda / x\Lambda| = \mathrm{N}_{A/\mathbb{Q}}(\mathfrak{m}_\mathcal{P}) = p^{2f(\mathcal{P}|p)},$$

donc pour que φ_x soit surjective, il faut que $1 \leq p^f \leq 11$ ce qui n'est possible que si $p = 3$ ou 7 (les cas 5 et 11 sont exclus car $f(5\mathcal{O}_K|5) = f(11\mathcal{O}_K|11) = 2$).

Nous allons voir que φ_x n'est pas surjective. Commençons par le cas $p = 3$. Comme $\langle 3 \rangle$ est ramifié dans A, $3\Lambda = \mathfrak{P}^2$ où $\mathfrak{P}$ est l'unique idéal maximal à droite de Λ contenant 3Λ, et $\mathfrak{P}$ est bilatère (voir le lemme 3.12.6). Soit s un générateur de $\mathfrak{P}$ (il est possible de choisir $s = \frac{12\sqrt{2}-33}{89}i + \frac{8\sqrt{2}-22}{89}k$). Nous vérifions que $|\varphi_s(\{0\} \cup \Lambda^\times \cup t\Lambda^\times)| = 16$, donc φ_s n'est pas surjective, car $|\Lambda / s\Lambda| = \mathrm{N}_{A/\mathbb{Q}}(\mathfrak{P}) = 3^4 = 81$. Par conséquent si $x \in \mathfrak{m}_3$, alors $x \notin \Lambda_3$.

Considérons maintenant le cas $p = 7$. Nous avons

$$7\mathcal{O}_K = \left(1 + 2\sqrt{2}\right)\mathcal{O}_K \left(1 - 2\sqrt{2}\right)\mathcal{O}_K = \mathcal{P}_7\overline{\mathcal{P}_7}.$$

Soit u un générateur de $\mathfrak{m}_{\mathcal{P}_7}$. Nous pouvons identifier $\mathcal{O}_K/\mathcal{P}_7$ à $\mathbb{F}_7$. Rappelons que $\Lambda_3' = t\Lambda^\times \cup \Lambda_1$ et que $(t\Lambda)^2 = \sqrt{2}\Lambda$. Explicitement, $t^2(1-\sqrt{2}) = \sqrt{2}$ et $1 - \sqrt{2} \in \mathcal{O}_K^\times$. On a

$$3 = \varphi_u(\sqrt{2}) = \varphi_u(t^2(1 - \sqrt{2})) = 5\varphi_u(t^2)$$

ce qui prouve que $\varphi_u(t^2) = 2 = 4^2$. De plus il existe $v \in \mathcal{O}_K^\times$ tel que $\varphi_u(v) = 4 : v = 1 + \sqrt{2}$ fait l'affaire. Le lemme 3.12.8 nous dit alors que $\varphi_u(\Lambda^\times) = \varphi_u(\Lambda^\times \cup t\Lambda^\times)$ et, comme $u \notin \Lambda_2$, alors $u \notin \Lambda_3$.

La démarche est la même avec $\mathfrak{m}_{\overline{\mathcal{P}_7}}$. Si u est un générateur de $\mathfrak{m}_{\overline{\mathcal{P}_7}}$,

$$4 = \varphi_u(\sqrt{2}) = \varphi_u(t^2(1 - \sqrt{2})) = 4\varphi_u(t^2)$$

et donc $\varphi_u(t^2) = 1 = 1^2$, comme $\varphi_u(1) = 1$. En procédant comme auparavant, nous obtenons que $u \notin \Lambda_3$.

Finalement, nous avons montré que $\Lambda_3 = \Lambda_3' = \Lambda_2 \neq \Lambda$. Par la proposition 2.1.10, Λ n'est pas euclidien à droite.

□

Proposition 3.12.10. *L'ordre 5l25 de la table III.1 n'est pas euclidien à droite. En particulier son minimum euclidien pour la norme réduite est supérieur ou égal à* 1.

PREUVE : Comme la preuve est essentiellement la même que celle de la proposition précédente, nous ne donnons pas les détails des calculs. Posons $\Lambda = 5l25$ et vérifions, à l'aide du corollaire 3.12.2, que si $\varphi_{\mathfrak{m}} : \{0\} \cup \Lambda^\times \longrightarrow \Lambda/\mathfrak{m}$ est surjective, alors $\mathfrak{m}$ est un idéal maximal au-dessus de 2, de 3 ou de $\sqrt{5}$. Nous démontrons que $\varphi_{\mathfrak{m}}$ n'est pas surjective si $\mathfrak{m}$ est un des dix idéaux maximaux à droite de Λ contenant 3Λ (il y a exactement dix idéaux de ce type par le lemme 3.12.6) ou si $\mathfrak{m}$ est l'unique idéal maximal contenant $\sqrt{5}\Lambda$. En revanche, si $s = \frac{-12\sqrt{5}+34}{109}i - \frac{1}{2}j + \frac{6\sqrt{5}-17}{218}k$ est un générateur de l'unique idéal maximal à droite de Λ contenant 2Λ, alors $\varphi_s(\Lambda^\times \cup \{0\}) = \Lambda/s\Lambda$, de sorte que $\Lambda_2 = \{0\} \cup \Lambda^\times \cup s\Lambda^\times$.

Nous vérifions ensuite que les seuls candidats pour Λ_3 sont au-dessus de $3, 5, 11$ ou 19. Dans ces quatre cas l'application $\varphi_{\mathfrak{m}}$ n'est pas surjective. En effet, soit u un générateur de $\mathfrak{m}_3$, un idéal maximal à droite de Λ au-dessus de $\langle 3 \rangle$. Nous avons

$$1 = \varphi_u(-2) = \varphi_u(s^2)$$

ce qui exclut le cas 3 (voir la preuve précédente pour les détails).

Soit u un générateur de l'unique idéal maximal au-dessus de $(\sqrt{5})$. Vérifier que $|\varphi_u(\Lambda_2)| = 9 < 25$ exclut le cas 5.

Soit u un générateur de $\mathfrak{m}_{\mathcal{P}}$, un idéal maximal à droite de Λ au-dessus de $\mathcal{P}$ (où $\mathcal{P}\overline{\mathcal{P}} = 11\mathcal{O}_K$). Alors

$$3^2 = \varphi_u(-2) = \varphi_u(t^2)$$

et $3 \in \varphi_u(\mathcal{O}_K^\times)$ ce qui exclut le cas 11.

Soit u un générateur de $\mathfrak{m}_{\mathcal{P}}$, un idéal maximal à droite de Λ au-dessus de $\mathcal{P}$ (où $\mathcal{P}\overline{\mathcal{P}} = 19\mathcal{O}_K$). Alors

$$6^2 = \varphi_u(-2) = \varphi_u(t^2)$$

et $6 \in \varphi_u(\mathcal{O}_K^\times)$ ce qui exclut le cas 19.

Finalement, $\Lambda_3 = \Lambda_2 \neq \Lambda$ et donc Λ n'est pas euclidien à droite.

□

Proposition 3.12.11. *Les ordres 13l23 et 13l23b de la table III.1 ne sont pas euclidiens à droite. En particulier leur minimum euclidien pour la norme réduite est supérieur ou égal à* 1.

PREUVE : Dans les deux cas, le corollaire 3.12.3 nous dit que s'il existe $s \in \Lambda$, où Λ désigne un des ordres 13l23 ou 13l23b, tel que l'application canonique

$$\varphi_s : \Lambda^\times \cup \{0\} \longrightarrow \Lambda/s\Lambda$$

est surjective, alors $s\Lambda \subset \mathfrak{m}_3$, où $\mathfrak{m}_3$ est un idéal maximal à droite de Λ au dessus de $(\frac{1+\sqrt{13}}{2})\Lambda$ ou au-dessus de $(\frac{1-\sqrt{13}}{2})\Lambda$.

Il faut donc étudier le cas de $\mathfrak{m}_3$. Distinguons les deux ordres.

Posons d'abord $\Lambda = 13l23$. Soit $s = \frac{-\sqrt{13}-10}{29}i + \frac{1}{2}j + \frac{-2\sqrt{13}+9}{58}k$. Alors $\mathfrak{P} = s\Lambda$ est l'unique idéal maximal à droite de Λ contenant $\frac{1+\sqrt{13}}{2}\Lambda$ (l'unicité est assurée par le lemme 3.12.6). Nous vérifions que φ_s n'est pas surjective. Nous savons qu'il y a exactement quatre idéaux maximaux à gauche distinct contenant $\frac{1-\sqrt{13}}{2}\Lambda$ (voir lemme 3.12.6). Ils sont engendré par les quatre éléments suivants :

1. $t_1 = \frac{1+i}{2}$,
2. $t_2 = \frac{1-i}{2}$,
3. $t_3 = \frac{1}{2} + \frac{2\sqrt{13}-9}{58}i - \frac{1}{2}j + \frac{2\sqrt{13}-9}{58}k$
4. $t_4 = \frac{1}{2} + \frac{-4\sqrt{13}-11}{58}i - \frac{1}{2}j + \frac{-2\sqrt{13}+9}{29}k$.

Il suffit de vérifier encore que les applications φ_{t_i} ne sont pas surjectives, car le corollaire 2.1.11 nous dit alors que $13l23$ n'est pas euclidien à droite.

Posons maintenant $\Lambda = 13l23b$. Nous procédons de même avec l'unique idéal maximal à droite contenant $\frac{1-\sqrt{13}}{2}\Lambda$ (engendré par $s = \frac{-\sqrt{13}-10}{29}i - \frac{1}{2}j + \frac{-3\sqrt{13}-1}{116}k$) et les quatre idéaux maximaux à droite contenant $\frac{1+\sqrt{13}}{2}\Lambda$, engendrés par :

1. $t_1 = -\frac{1}{2} + \frac{-\sqrt{13}+3}{4}i$,
2. $t_2 = -\frac{1}{2} - \frac{-\sqrt{13}+3}{4}i$,

3. $t_3 = \frac{1}{2} + \frac{-3\sqrt{13}+1}{116}i + \frac{\sqrt{13}-3}{4}j + \frac{-5\sqrt{13}+21}{116}k$,
4. $t_4 = -\frac{1}{2} + \frac{-23\sqrt{13}+83}{116}i + \frac{-5\sqrt{13}-21}{58}k$.

□

Proposition 3.12.12. *Les ordres 2l27 et 2l27b de la table III.1 ne sont pas euclidiens à droite. En particulier leur minimum euclidien pour la norme réduite est supérieur ou égal à* 1.

PREUVE : La preuve est la même que dans la proposition précédente. Il faut voir que φ_s ne peut être surjective que lorsque $s\Lambda$ est un idéal maximal au dessus de $(\sqrt{2})$, $(2\sqrt{2}+1)$ ou $(-2\sqrt{2}+1)$. Dans ces trois cas il faut vérifier que φ_s n'est pas surjective.

□

3.13 Corps de quaternions quadratiques imaginaires euclidiens

Dans la section 3.11, nous avons donné une liste presque exhaustive des corps de quaternions totalement définis sur un corps quadratique réel qui sont euclidiens. Dans cette section nous donnons un résultat semblable pour le cas quadratique imaginaire.

Proposition 3.13.1. *Soient d un nombre entier positif sans facteur carré et $K = \mathbb{Q}(\sqrt{-d})$ un corps quadratique imaginaire. Alors le minimum euclidien de K est donné par*

$$\mathrm{M}(K_{\mathbb{R}}) = \mathrm{M}(K) = \begin{cases} \frac{d+1}{4} & \text{si } d \equiv 1 \text{ ou } 2 \mod 4 \\ \frac{(d+1)^2}{16d} & \text{sinon.} \end{cases}$$

Si $d \equiv 1$ ou $2 \mod 4$, alors $\mathrm{M}(K) = m_K(x)$ pour tout $x \equiv \frac{1+\sqrt{-d}}{2} \mod \mathcal{O}_K$.
Si $d \equiv 3 \mod 4$, alors $\mathrm{M}(K) = m_K(x)$ pour tout $x \equiv \pm\frac{\frac{1}{4}(1+d)}{\sqrt{-d}} \mod \mathcal{O}_K$.

PREUVE : voir [Lem95], propostions 3.1 et 3.2, p.7

Corollaire 3.13.2. *Soit A un corps de quaternions sur un corps quadratique imaginaire $K = \mathbb{Q}(\sqrt{-d})$ (où d est un entier positif sans facteur carré). Supposons que A n'est pas isomorphe à $(-2,-5)_{\mathbb{Q}(\sqrt{-19})}$. Alors*

A est euclidien si et seulement si $d \in \{1, 2, 3, 7, 11\}$

On peut encore donner les bornes suivantes du minimum euclidien

i) Si $d = 1$ ou $d = 2$, alors $\frac{d+1}{8} \leq \mathrm{M}(A) \leq \frac{d+1}{4}$.

ii) Si $d \in \{3, 7, 11, 19, 43, 67, 163\}$, alors $\frac{d+1}{64} \leq \mathrm{M}(A) \leq \frac{(d+1)^2}{16d}$.

PREUVE : Comme le nombre de classes d'idéaux à droite d'un ordre maximal de A est égal au nombre de classes d'idéaux de K (voir proposition 3.4.1), si A est euclidien, alors K est principal. Les corps quadratiques imaginaires principaux sont bien connus ; il s'agit de $\mathbb{Q}(\sqrt{-d})$ pour $d = 1, 2, 3, 7, 11, 19, 43, 67, 163$. Ces neuf corps sont les seuls candidats possibles pour que A soit euclidien.

Observons d'abord $K = \mathbb{Q}(i)$. Nous avons $\mathrm{M}(K) = \frac{1}{2} = m_K\left(\frac{1}{1-i}\right)$. Fixons un ordre maximal Λ de A et posons $b = 1 - i$ et $a = 1$. Le théorème 3.4.10 nous dit alors que

$$\frac{1}{2} m_K\left(\frac{1}{1+i}\right) \leq m_\Lambda(b^{-1})$$

ce qui prouve que $\frac{d+1}{8} \leq \mathrm{M}(A)$. L'autre inégalité provient de $\mathrm{M}(A) \leq \mathrm{M}(K)$. Le procédé est le même pour $d = 2$, en utilisant $b = 2$ et $a \in \Lambda$ tel que $\mathrm{nr}_{A/K}(a) = 1 + \sqrt{-2}$.

Les sept cas restants se règlent de la même manière : nous choisissons $a \in \Lambda$ tel que $\mathrm{nr}_{A/K}(a) = \frac{1+\sqrt{d}}{2}$ et $b = 2$. Nous avons donc, avec les notations du théorème 3.4.10,

$$\mathrm{nr}_{A/K}(b) = 4, \quad t_b = 2, \quad C_b = \mathrm{N}_{K/\mathbb{Q}}\left(\frac{1}{2}\right) = \frac{1}{4}.$$

Nous avons alors

$$\frac{1}{4} m_K\left(\frac{\mathrm{nr}_{A/K}(a)}{2}\right) = \frac{1}{4} m_K\left(\frac{1+\sqrt{-d}}{4}\right) \leq m_\Lambda(b^{-1}a).$$

De plus on voit facilement que

$$m_K\left(\frac{1+\sqrt{-d}}{4}\right) = \mathrm{N}_{K/\mathbb{Q}}\left(\frac{1+\sqrt{-d}}{4}\right) = \frac{1+d}{16}.$$

Donc $\frac{d+1}{64} \leq \mathrm{M}(A)$. L'autre inégalité provient de

$$\mathrm{M}(A) \leq \mathrm{M}(K).$$

Nous avons démontré toutes les inégalités voulues et, en particulier, que si $d \in \{1,2,3,7,11\}$ alors $A = (a,b)_{\mathbb{Q}(\sqrt{-d})}$ est euclidien. Les inégalités démontrent également que si $d \in \{67,163\}$ alors A n'est pas euclidien.

Il nous reste à démontrer que si $d \in \{19,43\}$ et $A \ncong (-2,-5)_{\mathbb{Q}(\sqrt{-19})}$ alors A n'est pas euclidien. Notons pour la suite que $(-2,-5)_{\mathbb{Q}(\sqrt{-19})}$ est le corps de quaternions ramifié exactement aux premiers $s = \frac{1+\sqrt{-19}}{2}$ et $\overline{s} = \frac{1-\sqrt{-19}}{2}$. Par commodité nous considérons $\mathbb{Q}(\sqrt{-d})$ plongé dans $\mathbb{C}$ et nous notons $I = \sqrt{-1} \in \mathbb{C}$.

Soit $\mathcal{P}_1, \ldots, \mathcal{P}_{2t}$ les premiers ramifiés de A. Soit $b_i\Lambda = \mathfrak{P}_i$ l'unique idéal maximal de Λ au-dessus de $\mathcal{P}_i$. Rappelons que $\mathfrak{P}_i$ est bilatère, que $\mathfrak{P}_i^2 = \mathcal{P}_i\Lambda$ (voir le lemme 3.12.6) et que $\mathrm{nr}_{A/K}(b_i)$ est un générateur de $\mathcal{P}_i = \mathfrak{P}_i \cap \mathcal{O}_K$. Supposons qu'il existe un indice i_0 ($1 \leq i_0 \leq 2t$) et $a \in \Lambda$ tel que $\mathrm{nr}_{A/K}(a)$ et $\mathrm{nr}_{A/K}(b_{i_0})$ sont premier entre eux et

$$m_K(\mathrm{nr}_{A/K}(b_{i_0}^{-1}a)) \geq 1,$$

alors A n'est pas euclidien. En effet, dans ce cas, en reprenant les notations du théorème 3.4.10, nous avons

$$t_{b_i} = \mathrm{nr}_{A/K}(b_i) \quad \text{et} \quad C_{b_i} = 1$$

donc

$$1 \leq m_K(\mathrm{nr}_{A/K}(b_{i_0}^{-1}a)) = m_K\left(\frac{\mathrm{nr}_{A/K}(a)}{t_{b_{i_0}}}\right) \leq m_\Lambda(b_{i_0}^{-1}a).$$

Il n'est pas difficile de voir que si $x \in K$ est à l'intérieur (ou au bord) du parallélogramme Q défini par les sommets

$$\left\{\frac{1}{\sqrt{d}} + I, \frac{\sqrt{d}-2}{2\sqrt{d}} + I\left(\frac{\sqrt{d}-2}{2}\right), \frac{1}{\sqrt{d}} + 1 + I, \frac{3\sqrt{d}-2}{2\sqrt{d}} + I\left(\frac{\sqrt{d}-2}{2}\right)\right\}$$

alors $m_K(x) \geq 1$.

Soient $\mathcal{P}$ un des $\mathcal{P}_i$ et t_b un générateur de $\mathcal{P}$. Soit $a \in \Lambda$ tel que $\mathrm{nr}_{A/K}(a) = t_b + 1$, si $\mathrm{Re}(P) \geq \sqrt{d}$, alors $\frac{\mathrm{nr}_{A/K}(a)}{t_b} \in Q$ et donc A n'est pas euclidien. De même si $a' \in \Lambda$ est tel que $\mathrm{nr}_{A/K}(a') = t_b + \sqrt{-d}$ et si $\mathrm{Im}(P) \geq \frac{4\sqrt{d}}{\sqrt{d}-2}$, alors $\frac{\mathrm{nr}_{A/K}(a')}{t_b} \in Q$ et donc A n'est pas euclidien.

Comme t_b est un générateur de $\mathcal{P}$, il est toujours possible de supposer que, soit la partie réelle de t_b est positive, soit la partie imaginaire de t_b est

positive. Nous avons donc démontré que si A est euclidien alors les premiers ramifiés de A vérifient

$$-\sqrt{d} \leq \mathrm{Re}(t_b) \leq \sqrt{d} \quad \text{et} \quad -\frac{4\sqrt{d}}{\sqrt{d}-2} \leq \mathrm{Im}(t_b) \leq \frac{4\sqrt{d}}{\sqrt{d}-2}.$$

Pour $d \in \{19, 43\}$ il n'y a qu'un ensemble fini E de tels idéaux premiers. Notons E' l'ensemble des générateurs de ces idéaux. Il est facile de vérifier par ordinateur que pour tout $P \in E'$, à l'exception de $P = s$ et $P = \overline{s}$ lorsque $d = 19$, il existe $a \in \Lambda$, dont la norme réduite est première à P, tel que $m_K\left(\frac{\mathrm{nr}_{A/K}(a)}{P}\right) \geq 1$. Cela prouve que le seul candidat restant qui peut être euclidien est le corps de quaternions ramifié exactement aux premiers s et $\overline{s}$ lorsque $d = 19$

□

Nous savons que, lorsque K est principal, $\mathrm{M}(A) \leq \mathrm{M}(K)$. Nous avons déjà vu qu'il est possible que $\mathrm{M}(A) = \mathrm{M}(K)$, c'est le cas lorsque $K = \mathbb{Q}$, A est indéfini et que 2 ramifie dans A. Il est alors naturel de se demander si $\mathrm{M}(A) < \mathrm{M}(K)$ est possible. La proposition suivante, sans répondre à la question, donne un candidat pour cette inégalité.

Proposition 3.13.3. *Soient $K = \mathbb{Q}(\sqrt{-2})$, A un corps de quaternions sur K ramifié en $\sqrt{-2}\mathcal{O}_K$ et Λ un ordre maximal de A, alors*

$$\frac{3}{8} \leq \mathrm{M}(A) \leq \frac{3}{4}$$

et,

$$m_\Lambda(\xi) < \frac{3}{4}$$

pour tout $\xi \in A$

Preuve : Par le corollaire 3.13.2, la seule chose qu'il faut montrer c'est que $m_\Lambda(\xi) \neq \frac{3}{4}$ pour tout $\xi \in A$. Soit $\xi \in A$. Nous savons qu'il existe $a, b, c \in \Lambda$ tels que

$$\xi = b^{-1}a + c, \quad (\mathrm{nr}_{A/K}(a), \mathrm{nr}_{A/K}(b)) = 1 \quad \text{et} \quad m_\Lambda(\xi) \leq m_K(\mathrm{nr}_{A/K}(b^{-1}a)).$$

Supposons, dans un premier temps, que $\mathrm{nr}_{A/K}(b^{-1}a) \not\equiv \frac{1+\sqrt{-2}}{2} \mod \mathcal{O}_K$. Autrement dit, $m_K(\mathrm{nr}_{A/K}(b^{-1}a)) < \mathrm{M}(K)$. Alors, par le théorème 3.4.10,

$$m_\Lambda(\xi) \leq m_K(\mathrm{nr}_{A/K}(b^{-1}a)) < \mathrm{M}(K) = \frac{3}{4}.$$

Supposons maintenant que $\mathrm{nr}_{A/K}(b^{-1}a) \equiv \frac{1+\sqrt{-2}}{2} \mod \mathcal{O}_K$. Il existe alors $k = k_0 + k_1\sqrt{-2} \in \mathcal{O}_K$ tel que $\mathrm{nr}_{A/K}(b^{-1}a) = \frac{1+\sqrt{-2}+2k}{2}$. Comme

$$(\mathrm{nr}_{A/K}(a), \mathrm{nr}_{A/K}(b)) = (2, 1 + \sqrt{-2} + 2k) = 1,$$

nous devons avoir $\mathrm{nr}_{A/K}(b) = \pm 2$ et $\mathrm{nr}_{A/K}(a) = \pm(1 + \sqrt{-2} + 2k)$. Soit $b\Lambda$ l'idéal à droite de Λ engendré par b. Il existe des idéaux maximaux $\{\mathfrak{m}_1, \dots \mathfrak{m}_s\}$ tels que $b\Lambda = \mathfrak{m}_1 \cdots \mathfrak{m}_s$, et donc

$$2\mathcal{O}_K = \mathrm{nr}_{A/K}(\mathfrak{m}_1) \cdots \mathrm{nr}_{A/K}(\mathfrak{m}_s).$$

Cela n'est possible que si $s = 2$ et $\mathrm{nr}_{A/K}(\mathfrak{m}_1) = \mathrm{nr}_{A/K}(\mathfrak{m}_2) = \sqrt{-2}\mathcal{O}_K$. Comme $\mathcal{P} = \sqrt{-2}\mathcal{O}_K$ est ramifié dans A, il n'y a qu'un idéal maximal au-dessus de $\mathcal{P}$, de plus cet idéal est bilatère et son carré est $\sqrt{-2}\Lambda$ (voir le lemme 3.12.6). Nous avons donc démontré que $b\Lambda = \sqrt{-2}\Lambda$. Sans perte de généralité, nous pouvons supposer que $b = \sqrt{-2}$.

Posons $t = b^{-1}a = \frac{a}{\sqrt{-2}}$. Comme $\sqrt{-2}\Lambda$ est un idéal bilatère, le lemme 3.4.9, nous dit que

$$\mathrm{nr}_{A/K}(a) - \sqrt{-2}\mathcal{O}_K = \mathrm{nr}_{A/K}(a - \sqrt{-2}\Lambda).$$

Posons $v = 1 + 2k_1 - \sqrt{-2}k_0$. Il existe $\gamma \in \Lambda$ tel que

$$\mathrm{nr}_{A/K}(a) - \sqrt{-2}v = \mathrm{nr}_{A/K}(a - \sqrt{-2}\gamma).$$

Calculons $\mathrm{nr}_{A/K}(t - \gamma)$:

$$\begin{aligned}
\mathrm{nr}_{A/K}(t - \gamma) &= \mathrm{nr}_{A/K}(\sqrt{-2})^{-1}\mathrm{nr}_{A/K}(a - \sqrt{-2}\gamma) \\
&= -\frac{1}{2}(\mathrm{nr}_{A/K}(a) - \sqrt{-2}v) \\
&= \frac{-1 - \sqrt{-2} - 2k_0 - 2k_1\sqrt{-2} + (1 + 2k_1)\sqrt{-2} + 2k_0}{2} \\
&= -\frac{1}{2}.
\end{aligned}$$

Ainsi

$$m_\Lambda(\xi) = m_\Lambda(t) \leq \mathrm{nr}_{A/\mathbb{Q}}(t - \gamma) = \mathrm{N}_{K/\mathbb{Q}}\left(-\frac{1}{2}\right) = \frac{1}{4} < \frac{3}{4} = \mathrm{M}(K).$$

Nous avons donc démontré que pour tout $\xi \in A$, $m_\Lambda(\xi) < \mathrm{M}(K) = \frac{3}{4}$.

□

Si $d \equiv 3 \mod 4$ et que K n'est pas principal nous pouvons nous servir du théorème 3.4.11 pour borner le minimum euclidien d'un ordre maximal Λ.

Proposition 3.13.4. *Soient $d \equiv 3 \mod 4$, $K = \mathbb{Q}(\sqrt{-d})$, A un corps de quaternions sur K et Λ un ordre maximal de A. Supposons que A est ramifié en $\sqrt{-d}$ et que l'unique idéal maximal $\mathfrak{P}$ de Λ au-dessus de $\sqrt{-d}$ est principal. Alors*

$$\mathrm{M}(\Lambda) \geq \mathrm{M}(K).$$

PREUVE : Il existe $a \in \Lambda$ tel que $\mathrm{nr}_{A/K}(a) = \frac{1+d}{4}$. Notons $\mathfrak{P} = b\Lambda$. Nous savons que $\mathrm{nr}_{A/K}(b\Lambda) = b\Lambda \cap \mathcal{O}_K = \sqrt{-d}\mathcal{O}_K$. Avec les notations du théorème 3.4.11,

$$t_b = \sqrt{-d} \quad \text{et} \quad C_b = 1$$

de plus $(\mathrm{nr}_{A/K}(a), \mathrm{nr}_{A/K}(b)) = 1$. Il suffit alors d'appliquer le théorème 3.4.11, qui nous dit que $\mathrm{M}(\Lambda) \geq \mathrm{M}(K)$.

□

3.14 Corps de quaternions sur les corps cyclotomiques

Nous allons, dans cette section, donner une borne du minimum euclidien de certains ordres maximaux d'algèbres de quaternions sur des corps cyclotomiques et cyclotomiques réels. Dans ce but nous allons énoncer quelques résultats généraux.

Proposition 3.14.1. *Soient $a, b \in \mathbb{Z}$ négatifs, K un corps de nombres totalement réel ou CM de degré n, $A = (a,b)_K$ un corps de quaternions. Il existe, dans A, un ordre maximal Λ tel que*

$$\mathrm{M}(\Lambda) \leq (1 - a - b + ab)^n \left(\frac{\tau_{\min}(\mathcal{O}_K)}{\gamma_{\min}(\mathcal{O}_K)} \right)^n.$$

PREUVE : Soit $\Lambda_0 = \mathcal{O}_K \oplus i\mathcal{O}_K \oplus j\mathcal{O}_K \oplus k\mathcal{O}_K$ un ordre de A et Λ un ordre maximal de A contenant Λ_0. Soit τ une involution positive sur A. L'involution τ est l'involution canonique γ si K est totalement réel et $\tau = \iota\gamma$ si K est CM, où ι est la conjuguaison complexe. Par la proposition 2.7.4,

$$(\Lambda_0, \beta) \cong (\Lambda_0, \mathrm{tr}_1) \otimes_{\mathbb{Z}} (\mathcal{O}_K, \beta)$$

pour tout $\beta \in F = \{x \in K \mid x^\tau = x\}$. Or

$$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & -2a & 0 & 0 \\ 0 & 0 & -2b & 0 \\ 0 & 0 & 0 & 2ab \end{pmatrix}$$

est une matrice de Gram du réseau $(\Lambda_0, \mathrm{tr}_1)$ (avec la base $\{1, i, j, k\}$ de Λ_0) ; ainsi

$$(\Lambda_0, \beta) \cong (\mathcal{O}_K, 2\beta) \oplus (\mathcal{O}_K, -2a\beta) \oplus (\mathcal{O}_K, -2b\beta) \oplus (\mathcal{O}_K, 2ab\beta).$$

Comme

$$\max(\Lambda, \beta) \leq \max(\Lambda_0, \beta) = 2(1 - a - b + ab) \max(\mathcal{O}_K, \beta)$$

nous obtenons, par le corollaire 2.5.2 :

$$\mathrm{M}(\Lambda) \leq \left(\frac{\tau(\Lambda, \beta)}{\gamma_{\min}(\Lambda)} \right)^n \leq \left(\frac{2(1 - a - b + ab) \max(\mathcal{O}_K, \beta) / \det(\Lambda, \beta)^{\frac{1}{4n}}}{2n / \mathrm{d}(\Lambda/\mathbb{Z})^{\frac{1}{4n}}} \right)^n.$$

La valeur de $\det(\Lambda, \beta)$ nous est donnée par la proposition 1.8.13 :

$$\det(\Lambda, \beta) = \mathrm{N}_{K/\mathbb{Q}}(\beta^4 \mathrm{d}(\Lambda/\mathcal{O}_K))\mathrm{d}_K^4 = \mathrm{N}_{K/\mathbb{Q}}(\mathrm{d}(\Lambda/\mathcal{O}_K)) \det(\mathcal{O}_K, \beta)^4$$

et la valeur de $\mathrm{d}(\Lambda/\mathbb{Z})$ nous est donnée par la proposition 1.8.10 :

$$\mathrm{d}(\Lambda/\mathbb{Z}) = \mathrm{N}_{K/\mathbb{Q}}(\mathrm{d}(\Lambda/\mathcal{O}_K))\mathrm{d}_K^4.$$

Par conséquent,

$$\begin{aligned} \mathrm{M}(\Lambda) &\leq \left(\frac{2(1 - a - b + ab) \max(\mathcal{O}_K, \beta) / \det(\mathcal{O}_K, \beta)^{\frac{1}{n}}}{2n / \mathrm{d}_K^{\frac{1}{n}}} \right)^n \\ &= (1 - a - b + ab)^n \left(\frac{\tau(\mathcal{O}_K, \beta)}{\gamma_{\min}(\mathcal{O}_K)} \right)^n \end{aligned}$$

et comme cette borne est valable pour tout réseau idéal $(\mathcal{O}_K, \beta)$, nous obtenons le résultat annoncé.

□

Ce résultat est directement applicable à beaucoup de cas apparaissant dans les sections précédentes, mais il donne une moins bonne borne que celles proposées jusqu'ici.

Si K est un corps cyclotomique, ou cyclotomique réel, nous pouvons d'ores et déjà énoncer les résultats suivants.

Proposition 3.14.2. *Soit $K = \mathbb{Q}(\zeta_{p^r})^+ = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$ où p est un nombre premier et ζ_{p^r} une racine primitive p^r-ème de l'unité. Soit encore, $A = (a, b)_K$ où a et b sont des nombres entiers négatifs. Il existe un ordre maximal Λ de A tel que*

$$\mathrm{M}(\Lambda) \leq (1 - a - b + ab)^n \frac{\mathrm{d}_K}{4^n}$$

où $n = [K : \mathbb{Q}] = \frac{p^{r-1}(p-1)}{2}$ est le degré de K sur $\mathbb{Q}$.

PREUVE : Le lemme 8.5 de [BF06] nous dit que $\tau_{\min}(\mathcal{O}_K) \leq \frac{n}{4}$. Il suffit alors d'appliquer la proposition 3.14.1.

□

Dans les résultats 3.14.3 à 3.14.7 nous supposerons toujours que l'algèbre A est un corps de quaternions, sinon le minimum euclidien n'est pas défini.

Proposition 3.14.3. *Soit $K = \mathbb{Q}(\zeta_m)$ où m est un nombre entier et ζ_m une racine primitive m-ème de l'unité. Soit encore $A = (a, b)_K$ où a et b sont des nombres entiers négatifs. Il existe un ordre maximal Λ de A tel que*

$$\mathrm{M}(\Lambda) \leq (1 - a - b + ab)^n \frac{\mathrm{d}_K}{4^n}$$

où $n = [K : \mathbb{Q}] = \varphi(m)$ est le degré de K sur $\mathbb{Q}$.

PREUVE : La preuve de la proposition 9.1 de [BF06] nous dit que $\tau_{\min}(\mathcal{O}_K) \leq \frac{n}{4}$. Il suffit alors d'appliquer la proposition 3.14.1.

□

Dans le cas $a = b = -1$, nous pouvons parfois donner une meilleure borne.

Proposition 3.14.4. *Soient $p \geq 5$ un nombre premier et $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ le corps cyclotomique réel correspondant. Considérons le corps de quaternions $A = (-1, -1)_K$. Il existe un ordre maximal Λ de A avec*

$$\mathrm{M}(\Lambda) \leq \frac{\mathrm{d}_K}{2^n}.$$

PREUVE : Soit $\Lambda_0 = \mathcal{O}_K \oplus i\mathcal{O}_K \oplus j\mathcal{O}_K \oplus \frac{1+i+j+k}{2}\mathcal{O}_K$ un ordre de A. Le lemme 8.2 de [BF06] nous dit que $(\mathcal{O}_K, \alpha)$, avec $\alpha = \frac{1}{p}(1 - \zeta_p)(1 - \zeta_p^{-1})$, est isomorphe au réseau unité $\mathbb{Z}^n$. D'un autre côté le réseau $(\Lambda_0, 1)$ est isomorphe à D_4. La proposition 2.7.4 nous dit alors que

$$(\Lambda_0, \alpha) \cong (\Lambda_0, \mathrm{tr}_1) \otimes_{\mathbb{Z}} (\mathcal{O}_K, \alpha) = \bigoplus_{i=1}^{n} D_4$$

où $n = [K : \mathbb{Q}] = \frac{p-1}{2}$ est le degré de K sur $\mathbb{Q}$. Soit Λ un ordre maximal contenant Λ_0, alors

$$\max(\Lambda, \alpha) \leq \max(\Lambda_0, \alpha) = n \max(D_4) = n.$$

En procédant comme dans la proposition 3.14.1 nous obtenons

$$\mathrm{M}(\Lambda) \leq \left(\frac{n/\det(\mathcal{O}_K, \alpha)^{\frac{1}{n}}}{2n/\mathrm{d}_K^{\frac{1}{n}}} \right)^n = \frac{\mathrm{d}_K}{2^n}.$$

□

Dans la section 3.6, nous avons vu quelques exemples d'ordre maximaux sur $(a,b)_{\mathbb{Q}}$ et calculé leur maximum. Nous allons donc pouvoir utiliser ces résultats.

Proposition 3.14.5. *Soient $q \equiv 3 \mod 4$ un nombre premier, $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ où $p \geq 5$ est un nombre premier. Considérons $A = (-1,-q)_K$, alors il existe un ordre maximal Λ de A avec*

$$\mathrm{M}(\Lambda) \leq \left(\frac{(q+1)^2}{4q} \right)^n \frac{\mathrm{d}_K}{2^n}$$

où $n = [K : \mathbb{Q}]$ est le degré de K sur $\mathbb{Q}$.

Preuve : Même démarche que dans la proposition 3.14.4, avec l'ordre $\Lambda_0 = \mathcal{O}_K \oplus i\mathcal{O}_K \oplus \frac{i+j}{2}\mathcal{O}_K \oplus \frac{1+k}{2}\mathcal{O}_K$ ainsi que la valeur de $\max(\Lambda_0, 1) = \frac{(q+1)^2}{4q}$ donnée dans la preuve du corollaire 3.7.3.

□

Proposition 3.14.6. *Soient $q \equiv 5 \mod 8$ un nombre premier, $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ où $p \geq 5$ est un nombre premier. Considérons $A = (-2,-q)_K$, alors il existe un ordre maximal Λ de A avec*

$$\mathrm{M}(\Lambda) \leq \left(\frac{3q^2 + 10q + 3}{16q} \right)^n \frac{\mathrm{d}_K}{2^n}$$

où $n = [K : \mathbb{Q}]$ est le degré de K sur $\mathbb{Q}$.

Preuve : Même démarche que dans la proposition 3.14.4, avec l'ordre $\Lambda_0 = \mathcal{O}_K \oplus \frac{1+i+j}{2}\mathcal{O}_K \oplus j\mathcal{O}_K \oplus \frac{2+i+k}{4}\mathcal{O}_K$ ainsi que la valeur de $\max(\Lambda_0, 1) = \frac{3q^2+10q+3}{16q}$ donnée dans la proposition 3.7.4.

□

Proposition 3.14.7. *Soient $p \geq 7$ un nombre premier, r un entier positif et $K = \mathbb{Q}(\zeta_{p^r})$. Considérons $A = (-1,-1)_K$. Alors il existe un ordre maximal Λ de A avec*

$$\mathrm{M}(\Lambda) \leq \left(\frac{p+1}{3p^{r-1}}\right)^n \mathrm{d}_K$$

où $n = p^{r-1}(p-1) = [K:\mathbb{Q}]$ est le degré de K sur $\mathbb{Q}$.

PREUVE : D'après la proposition 9.1 de [BF06], le réseau $\bigoplus_{i=1}^{p^{r-1}} A_{p-1}^*$ est un réseau idéal sur $\mathcal{O}_K$; notons-le $(\mathcal{O}_K, \alpha)$. Nous savons, par la proposition 3.14.1, qu'il existe un ordre maximal Λ de A tel que

$$\mathrm{M}(\Lambda) \leq 4^n \left(\frac{\tau(\mathcal{O}_K,\alpha)}{\gamma_{\min}\mathcal{O}_K}\right). \tag{III.4}$$

Le maximum de A_{p-1}^* est donné par $\max(A_{p-1}^*) = \frac{p^2-1}{12p}$ et $\gamma_{\min}(\mathcal{O}_K) = \frac{n}{\mathrm{d}_K^{1/n}}$. Il suffit alors de calculer III.4 pour obtenir le résultat.

□

Afin de compléter les résultats précédents, nous allons donner des exemples des ordres maximaux qui interviennent dans ces propositions.

Proposition 3.14.8. *Soient n un entier, $K = \mathbb{Q}(\zeta_n)$ et $A = (-1,-1)_K$ l'algèbre de quaternions usuelle sur K. Supposons qu'il existe un diviseur m de n avec $m \equiv \pm 3 \mod 8$. Si $m \equiv -3 \mod 8$, posons $s = \frac{1+\sqrt{m}}{2} \in \mathcal{O}_K$; sinon posons $s = \frac{1+\sqrt{-m}}{2} \in \mathcal{O}_K$. Alors*

$$\Lambda = \mathcal{O}_K \oplus i\mathcal{O}_K \oplus \frac{s+(s+1)i+j}{2}\mathcal{O}_K \oplus \frac{1+i+j+k}{2}\mathcal{O}_K$$

est un ordre maximal de A et A est non ramifié aux places finies.
Si $m \equiv -3 \mod 8$ est un diviseur de n, alors le résultat est encore vrai pour $K = \mathbb{Q}(\zeta_n)^+$, et Λ satisfait aux hypothèses des propositions 3.14.2 et 3.14.4.

PREUVE : Il suffit de montrer que $s^2+s+1 \in 2\mathcal{O}_K$ (voir proposition 3.3.6). Comme $s + \overline{s} = 1$ et que $s\overline{s}$ est un entier impair,

$$\overline{s}(s^2+s+1) \equiv s+1+\overline{s} \equiv 0 \mod 2\mathcal{O}_K.$$

Et comme $\overline{s}$ est inversible modulo $2\mathcal{O}_K$, cela implique le résultat pour $K = \mathbb{Q}(\zeta_n)$.

Dans le cas où $m \equiv -3 \mod 8$, $s \in \mathcal{O}_{\mathbb{Q}(\zeta_n)^+}$ et donc le résultat est encore vrai pour $\mathbb{Q}(\zeta_n)^+$.

□

Corollaire 3.14.9. *Soit $K = \mathbb{Q}(\zeta_n)$ où n satisfait les hypothèses de la proposition précédente. Alors*

$$(-1,-1)_K \cong \mathrm{M}_2(K).$$

PREUVE : Le corps K est totalement imaginaire et, d'après la proposition précédente, $A = (-1,-1)_K$ n'est pas ramifiée aux places finies, de sorte que A est non ramifiée. C'est donc une algèbre de matrices.

□

Pour résoudre le cas où n n'a pas de diviseurs congrus à ± 3 modulo 8 nous avons besoin du résultat suivant.

Lemme 3.14.10. *Soit n un entier impair. L'ordre de 2 dans $(\mathbb{Z}/n\mathbb{Z})^\times$ est impair si et seulement si l'ordre de 2 dans $\mathbb{F}_p^\times$ est impair pour tout diviseur premier de n.*

PREUVE : Supposons que l'ordre de 2 dans $(\mathbb{Z}/n\mathbb{Z})^\times$ est un entier impair, disons f. Alors $2^f \equiv 1 \mod p$ pour tout diviseur premier p de n, donc l'ordre de 2 dans $\mathbb{F}_p^\times$ est impair. Réciproquement, supposons que $2^{f_p} \equiv 1 \mod p$ pour tout diviseur premier p de n où f_p est l'ordre de 2 dans $\mathbb{F}_p^\times$. Il suffit de constater que $2^{f_p f_q} \equiv 1 \mod pq$ et que $2^{p^i f_p} \equiv 1 \mod p^{i+1}$ pour conclure.

□

Corollaire 3.14.11. *Soit n un entier dont les diviseurs premier sont congrus à ± 1 modulo 8. Si $p \equiv 1 \mod 8$ est un diviseur premier de n, on suppose encore que 2 est d'ordre impair dans $\mathbb{F}_p^\times$. Soient $K = \mathbb{Q}(\zeta_n)$ (ou $K = \mathbb{Q}(\zeta_n)^+$) et $A = (-1,-1)_K$ le corps de quaternions usuel sur K, alors tous les premiers dyadiques sont ramifiés dans A et*

$$\Lambda = \mathcal{O}_K \oplus i\mathcal{O}_K \oplus j\mathcal{O}_K \oplus \frac{1+i+j+k}{2}\mathcal{O}_K$$

est un ordre maximal de A. De plus, l'ordre Λ satisfait aux hypothèses des propositions 3.14.2, 3.14.4 et 3.14.7.

PREUVE : Rappelons que le degré résiduel de 2 dans $\mathbb{Q}(\zeta_n)$ est l'ordre de 2 dans $(\mathbb{Z}/n\mathbb{Z})^\times$ (voir [Was82], théorème 2.13, p.14) et que 2 est non ramifié dans $\mathbb{Q}(\zeta_n)$ (voir [Was82] théorème 2.3, p.10). La proposition 3.3.4 nous dit que si $\mathcal{P}$ est un premier dyadique et que $f(\mathcal{P})$ est impair, alors $\mathcal{P}$ ramifie

dans A. Par le lemme précédent si le degré résiduel de 2 dans $\mathbb{Q}(\zeta_p)$ est impair pour tout premier p divisant n, alors les premiers dyadiques sont ramifiés dans $A = (-1,-1)_{\mathbb{Q}(\zeta_n)}$. Par hypothèse, c'est le cas des premiers congrus à 1 modulo 8. Pour les autres, nous constatons que $\varphi(p) = p-1 \equiv 6 \mod 8$, donc que $\varphi(p)/2$ est impair, et que $\mathbb{Q}(\zeta_p)$ contient $\mathbb{Q}(\sqrt{-p})$. Nous avons donc $2\mathcal{O}_{\mathbb{Q}(\sqrt{-p})} = \mathcal{P}\overline{\mathcal{P}}$ et $2\mathcal{O}_{\mathbb{Q}(\zeta_p)} = \mathcal{P}_1 \cdots \mathcal{P}_{2s}$.

Il vient

$$2sf = \varphi(p) = [\mathbb{Q}(\zeta_p) : \mathbb{Q}]$$

ce qui force f à être impair. Cela règle le cas $K = \mathbb{Q}(\zeta_n)$. Pour $K = \mathbb{Q}(\zeta_n)^+$, le degré résiduel de 2 dans $\mathbb{Q}(\zeta_n)^+$ divise celui de 2 dans $\mathbb{Q}(\zeta_n)$, ce qui prouve qu'il est également impair.

Nous avons donc prouvé que A est ramifié aux places dyadiques. Pour montrer que Λ est un ordre maximal de A, il suffit de voir que c'est un anneau et qu'il est de discriminant $4\mathcal{O}_K$.

□

Le cas des premiers $p \equiv 1 \mod 8$ semble plus compliqué à résoudre.

Observons maintenant ce qui arrive dans le cas cyclotomique réel.

Proposition 3.14.12. *Soient p un nombre premier congru à 3 modulo 4 ou à 9 modulo 16, r un entier, $K = \mathbb{Q}(\zeta_{p^r})^+$ et $A = (-1,-1)_K$. Alors tous les premiers dyadiques de K sont ramifiés dans A et*

$$\Lambda = \mathcal{O}_K \oplus i\mathcal{O}_K \oplus j\mathcal{O}_K \oplus \frac{1+i+j+k}{2}\mathcal{O}_K$$

est un ordre maximal de A. De plus l'ordre Λ satisfait aux hypothèses des propositions 3.14.2 et 3.14.4.

Preuve : Dans tous les cas cités, le degré de K sur $\mathbb{Q}$ est impair ; en particulier le degré résiduel de 2 est impair et l'indice de ramification également puisqu'il n'y a pas de ramification dyadique. Le résultat est alors une conséquence immédiate de la proposition 3.3.8.

□

Conclusion

Tout en rappelant les différents résultats obtenus dans notre étude sur le minimum des ordres maximaux dans les algèbres centrales à division, la conclusion va établir dans chaque cas les directions susceptibles de prolonger cette recherche.

Les résultats obtenus dans ce travail nous ont permis, entre autres choses, d'obtenir des informations sur les corps de quaternions euclidiens sur $\mathbb{Q}$ et dans le cas quadratique. Le cas des corps de quaternions sur $\mathbb{Q}$ est complètement résolu. Dans le cadre des corps de quaternions sur un corps quadratique imaginaire, seul $(-2,-5)_{\mathbb{Q}(\sqrt{-19})}$ reste en suspens. Dans le cas quadratique réel totalement défini, seul $(-1,-3)_{\mathbb{Q}(\sqrt{17})}$ reste en suspens. Nous avons tenté, en collaboration avec Jean-Paul Cerri, de résoudre ce cas de façon algorithmique, mais sans succès jusqu'à présent. Le cas indéfini sur un corps quadratique réel n'a été que peu étudié. Une approche possible utiliserait une généralisation du théorème 3.4.10 qui lie le minimum euclidien du corps de quaternions A à celui du centre K.

Afin de mieux comprendre les minima euclidiens d'une algèbre à division, il faudrait chercher une amélioration de la proposition 2.4.5 qui lie les minima d'ordres maximaux qui ne sont pas conjugués. Dans un premier temps il conviendrait de mieux comprendre les idéaux qui lient deux ordres maximaux et en particulier sous quelles conditions ces ordres sont liés par un idéal de petite norme.

Nous avons vu que la réalisation du réseau E_8 comme réseau idéal nous permettait de donner de bonnes bornes du minimum euclidien dans le cas quadratique. Il est donc naturel de se demander sous quelles conditions on peut réaliser des réseaux simples dont le maximum est petit. Nous avons également tenté d'explorer cette voie, mais sans entrer dans les détails, il semble impossible de réaliser d'autres réseaux de racines que E_8 et D_4. Il conviendrait de s'assurer de la véracité de ce résultat.

Dans ce travail, nous nous sommes limités à l'étude des ordres maximaux.

Il est naturel de se demander quels résultats reste vrais si l'ordre n'est pas maximal. Cette question ne concerne pas le théorème 2.5.1 sur la borne supérieure du minimum euclidien d'un ordre, qui est déjà énoncé dans le cadre général.

Bibliographie

[Ber83] Daniel Berend. Multi-invariant sets on tori. *Trans. Am. Math. Soc.*, 280 : 509–532, 1983.

[Ber84] Daniel Berend. Minimal sets on tori. *Ergodic Theory Dyn. Syst.*, 4 : 499–507, 1984.

[BF99] Eva Bayer-Fluckiger. Lattices and number fields. In *American Mathematical Society. Contemp. Math. 241, 69-84* . 1999.

[BF06] Eva Bayer-Fluckiger. Upper Bounds for Eucledean minima of algebraic number fields. *J. Number Theory*, 121 :305–323, 2006.

[Bou85] N. Bourbaki. *Eléments de mathématique. Algèbre commutative. Chapitre 4 : Idéaux premiers associés et décomposition primaire. Nouveau tirage.* Paris etc. : Masson, 1985.

[Cer] Jean-Paul Cerri. Euclidean minima of totally real number fields. Algorithmic determination. *À paraître dans Mathematics of Computation.*

[Cer06] Jean-Paul Cerri. Inhomogeneous and Euclidean spectra of number fields with unit rank strictly greater than 1. *J. Reine Angew. Math.*, 592 : 49–62, 2006.

[KMMT98] Max-Albert Knus, Alexander Merkurjev, Rost Markus, and Jean-Pierre Tignol. *The book of involutions.* Colloquium Publications. American Mathematical Society (AMS). 44. Providence, RI : American Mathematical Society (AMS). xxi, 1998.

[Lan94] Serge Lang. *Algebraic number theory.* Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1994.

[Lem95] Franz Lemmermeyer. The Euclidean algorithm in algebraic number fields. *Expo. Math., voir aussi http ://www.rzuser.uni-heidelberg.de/˜ hb3/prep.html pour une version mise à jour*, 13(5) :385–416, 1995.

[LJ] Stefan Lemurell (Johansson). A Description of quaternion algebra. *voir http ://www.math.chalmers.se/˜ sj/forskning.html.*

[MR03] Colin Maclachlan and Alan W. Reid. *The arithmetic of hyperbolic 3-manifolds.* Graduate Texts in Mathematics. Springer-Verlag. New York, 2003.

[Nar04] Wladyslaw Narkiewicz. *Elementary and analytic theory of algebraic numbers.* Springer Monographs in Mathematics. Berlin : Springer. xi, 708 p., third edition, 2004.

[Rei03] I. Reiner. *Maximal orders.* London Mathematical Society Monographs. New Series. 28. Oxford : Oxford University Press. xiv, 2003.

[Sam67] Pierre Samuel. *Théorie algébrique des nombres.* Hermann, Paris, 1967.

[Sam71] Pierre Samuel. About Euclidean rings. *J. Algebra*, 19 : 282–301, 1971.

[Ser77] Jean-Pierre Serre. *Cours d'arithmétique.* Le Mathématicien. Paris : Presses Universitaires de France, second edition, 1977.

[Vig80] Marie-France Vigneras. *Arithmétique des algèbres de quaternions.* Lecture Notes in Mathematics. 800. Berlin-Heidelberg-New York : Springer-Verlag. VII, 1980.

[Was82] Lawrence C. Washington. *Introduction to cyclotomic fields.* Graduate Texts in Mathematics, 83. New York - Heidelberg - Berlin : Springer-Verlag. XI, 1982.

Index

Jérôme Chaubert
Grey 64
1018 Lausanne
Jerome.Chaubert@epfl.ch
Tél. prof : 021 693 55 66
Né le 11.10.1976 à Lausanne

Formation

depuis 2002 Préparation d'une thèse de doctorat à l'EPFL.
- Recherche en théorie non commutative des nombres

1996-2002 **Diplôme de mathématicien**, Université de Lausanne.
- Travail de diplôme en topologie algèbrique.

1996-2001 **Licence es sciences, mathématiques et informatique**, Université de Lausanne.
- Réalisation de divers projets en programmation et programmation génétique.

1993-1996 **Certificat de maturité, type C** (mathématiques-sciences), Gymnase de la cité à Lausanne.

1985-1993 Ecoles primaires et secondaires, Lausanne.

Expériences professionelles

2002-2006 **Assistant diplômé** en mathématiques à l'Université de Lausanne et à l'EPFL.
- Encadrement des étudiants lors de séances d'exercices (français et anglais) dans divers domaines des mathématiques.
- Directions de divers travaux de semestre d'étudiants en mathématiques.
- Prime de rendement décernée par l'EPFL en octobre 2005.
- Expertises d'examens à l'EPFL et au secondaire I (maths-physique).

2002 **Assistant diplômé** en informatique à l'Université de Lausanne.
- Création d'une page internet et travail en collaboration avec l'entreprise "Etat de la planète".

2000-2001 **Assistant-étudiant** en informatique à l'Université de Lausanne.
- Encadrement des étudiants lors de séances d'exercices en informatique (programmation Java).

Autres expériences

2004-2005 **Projet à caractère humanitaire** à Quito, en collaboration avec la fondation suisso-équatorienne Sol de Primavera.

- Brève découverte du travail d'éducateur à la fondation Sol de Primavera à Quito.
- Recherche de fonds et de matériel, organisation d'un projet en collaboration avec une fondation s'occupant de jeunes (7 à 16 ans) défavorisés du quartier du Placer à Quito.
- Réalisation d'un camp de découverte de 4 jours dans les Andes avec les enfants de la fondation (11 à 16 ans).

1997-1998 **Projet inter culturel au Mali.**

- Recherche de fonds et de matériel, organisation et réalisation d'un projet en collaboration avec un groupe scout de Bamako : création de panneaux indicateurs dans un quartier de Bamako.
- Gestion du budget et des comptes du projet.

1996 **Formation** de moniteur Jeunesse et Sport 1, excursion en plein air.

1994-2005 **Responsable** au groupe scout de Notre-Dame, Lausanne.

- Encadrement d'enfants et d'adolescents lors de diverses activités souvent en pleine nature.
- Organisation et réalisation de plusieurs camps d'hiver ou d'été avec des enfants et des adolescents.
- Gestion administrative des budgets et comptes de diverses unités scouts.