EUCLIDEAN MINIMA AND CENTRAL DIVISION ALGEBRAS

EVA BAYER–FLUCKIGER*
Ecole Polytechnique Fédérale de Lausanne
EPFL–FSB–IMB–CSAG
Station 8, 1015 Lausanne, Switzerland
eva.bayer@epfl.ch

JEAN–PAUL CERRI
Université de Bordeaux 1
IMB, Laboratoire A2X
351, cours de la Libération, 33405 Talence, France
Jean-Paul.Cerri@math.u-bordeaux1.fr.

JÉRÔME CHAUBERT *
Ecole Polytechnique Fédérale de Lausanne
EPFL–FSB–IMB–CSAG
Station 8, 1015 Lausanne, Switzerland
jerome.chaubert@gmail.com.

Abstract. The notion of Euclidean minimum of a number field is a classical one. In this paper we generalize it to central division algebras and establish some general results in this new context.

Keywords: Euclidean minimum, central division algebras, quaternion fields.

Mathematics Subject Classification 2000: 11R52, 11H50, 13F07.

Introduction

Let k be an algebraic number field, let D be a central division algebra over k, and let Λ be an order of D. Let us denote by $\mathrm{N} : D \to \mathbf{Q}$ the absolute value of the reduced norm map $\mathrm{nrd} : D \to \mathbf{Q}$, where $\mathbf{Q}$ is the field of rational numbers. We say that Λ is *Euclidean* if for all $x \in D$ there exists $y \in \Lambda$ such that $\mathrm{N}(x - y) < 1$. It is easy to see that this is equivalent to each of the two natural Euclidean division proprieties : for all $a, b \in \Lambda$, $b \neq 0$, there exist $c, c', d, d' \in \Lambda$ such that $a = bc + d$, $a = c'b + d'$, and $\mathrm{N}(d) < \mathrm{N}(b)$, $\mathrm{N}(d') < \mathrm{N}(b)$.

Let us also define the *Euclidean minimum* $M(\Lambda)$ of Λ by

$$M(\Lambda) = \sup_{x \in D} \inf_{y \in \Lambda} \mathrm{N}(x - y).$$

* Partially supported by the Swiss National Science Fundation, grant 200020-111814/1

These notions are straightforward generalizations of the well–known Euclidean property and Euclidean minimum of algebraic number fields. Both are classical and have been studied very extensively in the case of algebraic number fields (see for instance [7] for a survey). In the non–commutative case, very little is known about them. The aim of this paper is to give some basic results concerning Euclidean and inhomogeneous minima of central division algebras (cf. §1), and to generalize some recent results concerning the commutative case (cf. [1], [4]). In particular, we apply Berend's results to show that $M(\Lambda)$ is a rational number if the unit rank of the number field is greater than 1 (§1). We also obtain a general upper bound for the Euclidean minimum of an order (see §2 – 4). Let $d(\Lambda/\mathbf{Z})$ denote the discriminant of the order Λ. Then we have

$$M(\Lambda) \leq (\frac{m}{2})^{nm} d(\Lambda/\mathbf{Z})^{1/m}.$$

Section 5 contains some examples, and sharper bounds in some special cases. For instance, we show that if k is a real quadratic field, D a totally definite quaternion algebra such that no finite place of k ramifies in D, and if the fundamental unit of k has norm -1, then

$$\frac{d_k}{7552 + 3072\sqrt{6}} \leq M(\Lambda) \leq \frac{d_k}{16},$$

where d_k is the absolute value of the discriminant of k.

§1. Euclidean minima

1.1. Definitions, notation and basic facts

We keep the notation of the introduction. For any unexplained terminology concerning division algebras and orders, we refer the reader to [8].

Let k be an algebraic number field of degree $n = r_1 + 2r_2$, where r_1 is the number of real embeddings and r_2 the number of pairs of complex embeddings of k. Set $k_{\mathbf{R}} = k \otimes_{\mathbf{Q}} \mathbf{R}$, where $\mathbf{R}$ is the field of real numbers. We denote by $\mathrm{N}_{k/\mathbf{Q}} : k \to \mathbf{Q}$ and $\mathrm{N}_{k_{\mathbf{R}}/\mathbf{R}} : k_{\mathbf{R}} \to \mathbf{R}$ the norm maps. Let O_k be the ring of integers of k.

Let D be a central division algebra of degree m over k, let Λ be an O_k–order of D, and let I be a right Λ–ideal. Set $D_{\mathbf{R}} = D \otimes_{\mathbf{Q}} \mathbf{R}$. Let $\mathrm{nrd}_{D/k} : D \to k$ and $\mathrm{nrd}_{D_{\mathbf{R}}/k_{\mathbf{R}}} : D_{\mathbf{R}} \to k_{\mathbf{R}}$ be the reduced norm maps. Let $\mathrm{nrd}_{D_{\mathbf{R}}/\mathbf{R}} : D_{\mathbf{R}} \to \mathbf{R}$ be the reduced norm of the separable $\mathbf{R}$–algebra $D_{\mathbf{R}}$; note that $\mathrm{nrd}_{D_{\mathbf{R}}/\mathbf{R}}(x) = \mathrm{N}_{k_{\mathbf{R}}/\mathbf{R}}(\mathrm{nrd}_{D_{\mathbf{R}}/k_{\mathbf{R}}}(x))$, for all $x \in D_{\mathbf{R}}$. Let $\mathrm{N} : D_{\mathbf{R}} \to \mathbf{R}$ be the absolute value of $\mathrm{nrd}_{D_{\mathbf{R}}/\mathbf{R}}$. We define the *Euclidean minimum* of I by

$$M(I) = \sup_{x \in D} \inf_{y \in I} \mathrm{N}(x - y),$$

and the *inhomogeneous minimum* of I by

$$M_{\mathbf{R}}(I) = \sup_{x \in D_{\mathbf{R}}} \inf_{y \in I} \mathrm{N}(x-y).$$

In the special case where $D = k$ and $I = \Lambda = O_k$, we set $M(O_k) = M(k)$, and $M_{\mathbf{R}}(O_k) = M(k_{\mathbf{R}})$; these are the Euclidean and inhomogeneous minima of the number field k.

Notation 1.1. Let $x \in D_{\mathbf{R}}$. Set $m_I(x) = \inf\{\ \mathrm{N}(x-y) \mid y \in I\ \}$.

Note that $M(I) = \sup\{m(x) \mid x \in D\}$, and $M_{\mathbf{R}}(I) = \sup\{m(x) \mid x \in D_{\mathbf{R}}\}$.

The following proposition is a straightforward generalization of a corresponding result in the commutative case, see [4], [5].

Proposition 1.2. *We have the following properties :*
(1) For all $u \in \Lambda^*$, $x \in D_{\mathbf{R}}$ and $y \in I$, we have $m_I(xu - y) = m_I(x)$.
(2) For all $x \in D$, there exists $y \in I$ such that $m_I(x) = N(x-y)$.
(3) For all $x \in D$, we have $m_I(x) \in \mathbf{Q}$.
(4) If $x \in D$, $m_I(x) = 0$ if and only if $x \in I$.

Proof. See [4], Proposition 1, and [5], Proposition 2.2.2.

Definition 1.3. We say that I is *Euclidean* if for all $x \in D$ there exists $y \in I$ such that $N(x-y) < 1$.

Proposition 1.4. *We have*
(1) If $M(I) < 1$, then I is Euclidean.
(2) If $M(I) > 1$, then I is not Euclidean.
(3) If $M(I) = 1$, then I is Euclidean if and only if there does not exist any $x \in D$ with $M(I) = m_I(x)$.

Proof. These are easy consequences of the definition, cf. [5], Proposition 2.2.5.

1.2. Comparison of the minima and rationality questions

In [4], it is proved that if the unit rank of k is at least 2, then $M(k) = M(k_{\mathbf{R}}) \in \mathbf{Q}$. The proof uses some results of Berend [2], [3]. The aim of the rest of this section is to show that one can apply the same methods to get analogous results in the non–commutative case. We start by briefly recalling Berend's results, see [2], [3] and [4] for more details.

Let T be a finite dimensional torus i.e. $T = \mathbf{R}^d/\mathbf{Z}^d$ for some $d \geq 1$, and let $\mathcal{E}$ be a set of continous endomorphisms of T. A subset A of T is said to be $\mathcal{E}$*–invariant* if we have $f(A) \subset A$ for every $f \in \mathcal{E}$. A non–empty closed $\mathcal{E}$–invariant set A is said to be $\mathcal{E}$*–minimal* if it contains no proper non–empty closed $\mathcal{E}$–invariant subset.

Let Σ be a commutative semigroup of endomorphisms of T. We say that Σ is *hyperbolic* if the eigenvalues of the common eigenvectors of Σ are not contained in the unit circle. We say that Σ is *multiparameter* if the set of eigenvalues of any common eigenvector of Σ contains two rationally independent elements.

We need the following result of Berend :

Theorem 1.5. (Berend, [3], Theorem 2.1) *Let Σ be a commutative semigroup of epimorphisms of T. Then the following conditions are equivalent :*

(1) Any Σ–minimal subset of T is composed of torsion elements;
(2) Σ is hyperbolic and multiparameter.

In order to apply this result, let us introduce some more notation.

Set $T_D = D_{\mathbf{R}}/I$. Then T_D is a finite dimensional torus. The map $m : D_{\mathbf{R}} \to \mathbf{R}$ induces

$$\tilde{m} : T_D \to \mathbf{R}.$$

Proposition 1.6. *The map $\tilde{m}$ is well-defined and upper semi–continuous. Moreover $\tilde{m}$ and m are bounded from above and attain their maximum.*

Proof. See [4], Proposition 3 and Corollary 2; [5], Proposition 2.2.11.

Let us consider the subset Σ_u of the automorphisms of T induced by right multiplication by the units O_k^* of k. Then we have

Proposition 1.7. *Suppose that $r_1+r_2-1 \geq 2$. Then Σ_u is hyperbolic and multiparameter.*

Proof. See [4], proof of Theorem 3, and [5], proof of Theorem 2.2.3.

From the previous properties, we can deduce the main result of this section :

Theorem 1.8. *Suppose that $r_1 + r_2 - 1 \geq 2$. Then there exists $x \in D$ such that $m_I(x) = M(I) = M_{\mathbf{R}}(I)$.*

Proof. This results from the previous results, as shown in [4], Theorem 3, and [5], Theorem 2.2.3.

Corollary 1.9. *Suppose that $r_1 + r_2 - 1 \geq 2$. Then $M_{\mathbf{R}}(I) \in \mathbf{Q}$.*

Proof. This is an immediate consequence of 1.8 and 1.2 (3).

In some special cases, we can weaken the hypothesis $r_1 + r_2 - 1 \geq 2$. This is based on the following observation :

Proposition 1.10. *Let G be a subgroup of $\mathcal{U} = \{u \in \Lambda^* \mid \sigma(u)$ is a diagonal matrix for any embedding σ of D in a real, complex or quaternionian matrix algebra$\}$. If G is abelian and if the set of automorphisms Σ_G induced by G is hyperbolic and multiparameter, then there exists $x \in D$ such that $m_I(x) = M(I) = M_{\mathbf{R}}(I)$.*

Proof. This is deduced from Berend's results in the same way as 1.8.

Quaternion fields are special cases of central division algebras. Let us recall that such an algebra D is a 4-dimensional algebra over k with basis $(1, i, j, l)$ such that $i^2 = a$, $j^2 = b$ and $l = ij = -ji$, where a, b are non zero elements of k. This algebra is denoted by $(a, b)_k$. It is a division algebra if and only if the quadratic form $\mathrm{nrd}_{D/k}(x + yi + zj + tl) = x^2 - ay^2 - bz^2 + abt^2$ represents zero on k only trivially.

Corollary 1.11. *Let k be a real quadratic field, and let D be a totally indefinite quaternion field over k, i.e. such that no infinite place of k ramifies in D. Then there exists $x \in D$ such that $m_I(x) = M(I) = M_{\mathbf{R}}(I)$.*

Proof. It suffices to find an abelian subgroup G of $\mathcal{U}$ satisfying the hypothesis of 1.10. Let us write $D = (a, b)_k$, with $a, b \in k^*$ and a totally positive. Let $L = k(\sqrt{a})$. Then L is totally real and $[L : \mathbf{Q}] \geq 4$. Hence by Dirichlet's theorem there exists a unit $w = u + v\sqrt{a} \in O_L^* - O_k^*$ that has infinite order in O_L^*. Set G be the subgroup of Λ^* generated by O_k^* and $u + vi$, where $i \in D$ is such that $i^2 = a$. The group G is clearly abelian, and Σ_G is hyperbolic, as the group Σ_u induced by O_k^* is hyperbolic by 1.7, and O_k^* is a subgroup of G. It remains to check that G is a subgroup of $\mathcal{U}$, and that Σ_G is multiparameter. The quadratic field k has two real embeddings, each of which extends to an embedding of D in $M_2(\mathbf{R})$. A straigthforward computation shows that the images of the elements of G are diagonal matrices in both cases (cf. [5], 2.3.6) hence G is indeed a subgroup of $\mathcal{U}$. To show that Σ_G is multiparameter, let ϵ_1 be a unit of O_k^*, $\epsilon_1 \neq \pm 1$, and let $\epsilon_2 = u + vi$. Then ϵ_1 and ϵ_2 are rationally independent. This implies that Σ_G is multiparameter (cf. [5], 2.3.6).

§2. Ideal lattices

The aim of this section is to define the notion of *ideal lattice*, and to prove a few basic facts. As we will see later, packing and covering invariants of ideal lattices can be used to obtain upper bounds for Euclidean and inhomogeneous minima. We start by recalling some definitions and basic facts concerning lattices.

2.1. Lattices

A *lattice* is a pair (L, q), where L is a free $\mathbf{Z}$–module of finite rank, and $q : L_{\mathbf{R}} \times L_{\mathbf{R}} \to \mathbf{R}$ is a positive definite symmetric bilinear form, where $L_{\mathbf{R}} = L \otimes_{\mathbf{Z}} \mathbf{R}$. Two lattices (L, q) and (L', q') are *isomorphic* if and only if there exists an isomorphism $f : L \to L'$ such that

$q'(f(x), f(y)) = q(x, y)$. We then use the notation $(L, q) \simeq (L', q')$. If (L, q) is a lattice, then the *dual lattice* is by definition the lattice $(L^\sharp, q)$, where

$$L^\sharp = \{x \in L_{\mathbf{R}} \mid q(x, y) \in \mathbf{Z} \text{ for all } y \in L\}.$$

A lattice (L, q) is said to be *integral* if $L \subset L^\sharp$, i.e. if $q(x, y) \in \mathbf{Z}$ for all $x, y \in L$. An integral lattice (L, q) is *even* if $q(x, x) \equiv 0 \pmod 2$ for all $x \in L$.

Let (L, q) be a lattice of rank n. Set $q(x) = q(x, x)$. The *minimum* of (L, q) is defined by

$$\min(L, q) = \inf\{q(x) \mid x \in L, x \neq 0\}.$$

The *maximum* of (L, q) is by definition

$$\max(L, q) = \inf\{\lambda \in \mathbf{R} \mid \text{for all } x \in L_{\mathbf{R}}, \text{ there exists } y \in L \text{ with } q(x - y) \leq \lambda\}.$$

Note that $\max(L, q)$ is often called the inhomogeneous minimum of the lattice, and that it is the square of the covering radius of the associated sphere covering.

The *determinant* of (L, q) is denoted by $\det(L, q)$. It is by definition the determinant of the matrix of q in a $\mathbf{Z}$–basis of L. The *Hermite invariants* of (L, q) are

$$\gamma(L, q) = \frac{\min(L, q)}{\det(L, q)^{1/n}},$$

and

$$\tau(L, q) = \frac{\max(L, q)}{\det(L, q)^{1/n}}.$$

These invariants only depend on the isomorphism class of the lattice (L, q).

Set $\gamma_n = \sup\{\gamma(L, q) \mid \text{rank}(L) = n\}$, $\tau_n = \inf\{\tau(L, q) \mid \text{rank}(L) = n\}$.

2.2. Ideal lattices

We keep the notation of the previous section. In particular, k is an algebraic number field of degree n, having r_1 real and $2r_2$ complex places. We denote by O_k the ring of integers of k.

Let D be a central division algebra over k of degree m. Let us denote by $\mathbf{H}$ the usual Hamilton quaternion field over $\mathbf{R}$. Set $D_{\mathbf{R}} = D \otimes_{\mathbf{Q}} \mathbf{R}$. Then we have

$$D_{\mathbf{R}} \simeq M_{\frac{m}{2}}(\mathbf{H})^w \times M_m(\mathbf{R})^{r_1 - w} \times M_m(\mathbf{C})^{r_2}$$

where w is the number of real places at which D ramifies.

The *canonical involution* of $D_{\mathbf{R}}$ is by definition the $\mathbf{R}$–linear involution which is induced by the canonical involution of the quaternion field on the first factor, by the identity

on the second, and complex conjugation on the third. We denote this involution by $x \mapsto \overline{x}$. An element $\alpha = (\alpha_1, \ldots, \alpha_{r_1+r_2})$ of $D_{\mathbf{R}}$ is said to be *positive*, denoted by $\alpha > 0$, if $\overline{\alpha} = \alpha$ and if each α_i is a positive definite matrix. Set $\mathcal{P} = \{\alpha \in D_{\mathbf{R}} \mid \alpha > 0\}$.

Let us denote by $\mathrm{tr}_{D_{\mathbf{R}}/\mathbf{R}} : D_{\mathbf{R}} \to \mathbf{R}$ the reduced trace of the separable $\mathbf{R}$–algebra $D_{\mathbf{R}}$. The following lemma is easy to prove :

Lemma 2.1. *Let $q : D_{\mathbf{R}} \times D_{\mathbf{R}} \to \mathbf{R}$ be a symmetric bilinear form. The following are equivalent :*

(i) There exists $\alpha \in D_{\mathbf{R}}$ with $\overline{\alpha} = \alpha$ such that $q(x, y) = \mathrm{tr}_{D_{\mathbf{R}}/\mathbf{R}}(x\alpha\overline{y})$ for all $x, y \in D_{\mathbf{R}}$.

(ii) We have $q(\lambda x, y) = q(x, \overline{\lambda} y)$ for all $x, y, \lambda \in D_{\mathbf{R}}$.

Moreover, a symmetric bilinear form q satisfying these conditions is positive definite if and only if $\alpha \in \mathcal{P}$.

Notation 2.2. We denote by q_α the symmetric bilinear form of condition (i) of the above lemma.

Definition 2.3. A *generalized ideal* of Λ is a set of the form $I = xJ$ where $x \in D_{\mathbf{R}}^*$ and J is a right Λ–ideal J. If I is a generalized ideal of Λ, we define the *norm* of I by $\mathrm{N}_{D_{\mathbf{R}}/\mathbf{R}}(I) = \mathrm{nrd}_{D_{\mathbf{R}}/\mathbf{R}}(x)^m \mathrm{N}_{D/\mathbf{Q}}(J)$. An *ideal lattice* is a pair (I, q_α), where I is a generalized ideal and $\alpha \in \mathcal{P}$.

Let $\mathcal{D}(\Lambda/O_k)$ be the different of Λ over O_k. We have

Proposition 2.4. *Let (I, q_α) be an ideal lattice. The dual of the lattice (I, q_α) is $(I^\sharp, q_\alpha)$, where*

$$I^\sharp = \overline{I}^{-1} \mathcal{D}(\Lambda/O_k)\alpha^{-1}.$$

Moreover, $(I^\sharp, q_\alpha)$ is an ideal lattice for $\overline{D}$, $\overline{\Lambda}$.

Proof. Straightforward computation.

Let $d(\Lambda/\mathbf{Z})$ be the discriminant of Λ over $\mathbf{Z}$.

Proposition 2.5. *Let (I, q_α) be an ideal lattice. Then we have*

$$\det(I, q_\alpha) = \mathrm{nrd}_{D_{\mathbf{R}}/\mathbf{R}}(\alpha)^m \mathrm{N}_{D_{\mathbf{R}}/\mathbf{R}}(I)^2 d(\Lambda/\mathbf{Z}).$$

Proof. This follows from 2.4, as $\det(I, q_\alpha)$ is the cardinal of $I^\sharp/I$.

Proposition 2.6. *Suppose that D is a quaternion field with center k, and suppose that the restriction of the canonical involution to k is the identity. Then every integral ideal lattice over D is even.*

Proof. As D is tamely ramified, there exists $\tau \in \Lambda$ such that $\tau + \overline{\tau} = 1$. Let (I, q_α) be an integral ideal lattice. For every $x \in I$ we have

$$q_\alpha(x,x) = \mathrm{tr}_{D_{\mathbf{R}}/\mathbf{R}}(x\alpha\overline{x}) = \mathrm{tr}_{D_{\mathbf{R}}/\mathbf{R}}(\tau x\alpha\overline{x}) + \mathrm{tr}_{D_{\mathbf{R}}/\mathbf{R}}(\overline{\tau}x\alpha\overline{x}) = 2\mathrm{tr}_{D_{\mathbf{R}}/\mathbf{R}}(\tau x\alpha\overline{x}).$$

As $\tau x\alpha\overline{x} \in \mathcal{D}(\Lambda/\mathbf{Z})^{-1}$, this implies that the lattice (I, q_α) is even.

§3. Bounds for ideal lattices over division algebras

The results of this section will be applied to obtain upper bounds for Euclidean and inhomogeneous minima of orders of division algebras (cf. §4). The following proposition is a consequence of the inequality between arithmetic and geometric means.

Proposition 3.1. *Let $\alpha \in \mathcal{P}$. Then we have*

$$\mathrm{nrd}_{D_{\mathbf{R}}/\mathbf{R}}(x\alpha\overline{x}) \leq (\frac{q_\alpha(x,x)}{nm})^{nm}.$$

Proof. Recall that q_α is definite positive and that $D_{\mathbf{R}} \simeq M_{\frac{m}{2}}(\mathbf{H})^w \times M_m(\mathbf{R})^{r_1-w} \times M_m(\mathbf{C})^{r_2}$, so

$$(\frac{q_\alpha(x,x)}{nm})^{nm} = ((\frac{v_1+v_2+v_3}{n})^n)^m,$$

where

$$v_1 = \frac{1}{m}\sum_{i=1}^{w} \mathrm{Tr}(x_i\alpha_i\overline{x}_i^t)$$

$$v_2 = \frac{1}{m}\sum_{i=w+1}^{r_1} \mathrm{Tr}(x_i\alpha_i x_i^t)$$

$$v_3 = \frac{1}{m}\sum_{i=r_1+1}^{r_1+r_2} \mathrm{Tr}(x_i\alpha_i\overline{x}_i^t) + \overline{\mathrm{Tr}(x_i\alpha_i\overline{x}_i^t)}.$$

By the inequality between the arithmetic and geometric means, this is greater or equal to

$$(\prod_{i=1}^{w} \frac{\mathrm{Tr}(x_i\alpha_i\overline{x}_i^t)}{m} \prod_{i=w+1}^{r_1} \frac{\mathrm{Tr}(x_i\alpha_i x_i^t)}{m} \prod_{i=r_1+1}^{r_1+r_2} \frac{\mathrm{Tr}(x_i\alpha_i\overline{x}_i^t)}{m}\,\overline{\frac{\mathrm{Tr}(x_i\alpha_i\overline{x}_i^t)}{m}})^m.$$

Applying again the inequality between arithmetic and geometric means, we see that the last expression is greater or equal to

$$\prod_{i=1}^{w} \det(x_i\alpha_i\overline{x}_i^t) \prod_{i=w+1}^{r_1} \det(x_i\alpha_i x_i^t) \prod_{i=r_1+1}^{r_1+r_2} \det(x_i\alpha_i\overline{x}_i^t)\overline{\det(x_i\alpha_i\overline{x}_i^t)},$$

which is equal to $\mathrm{nrd}_{D_{\mathbf{R}}/\mathbf{R}}(x\alpha\overline{x})$.

Notation 3.2. For any ideal lattice (I, q_α) and for all $x \in D_{\mathbf{R}}$, set

$$\beta_{(I,q_\alpha)}(x) = \frac{q_\alpha(x,x)}{\det(I,q_\alpha)^{\frac{1}{nm^2}}}$$

For every order Λ of D, set

$$\gamma(\Lambda) = \frac{nm}{d(\Lambda/\mathbf{Z})^{\frac{1}{nm^2}}}.$$

Proposition 3.3. *Let (I, q_α) be an ideal lattice. We have*

$$\mathrm{nrd}_{D_{\mathbf{R}}/\mathbf{R}}(x) \leq (\frac{\beta_{(I,q_\alpha)}(x)}{\gamma(\Lambda)})^{nm/2}\mathrm{nrd}_{D_{\mathbf{R}}/\mathbf{R}}(I).$$

Proof. Using proposition 2.5, we see that

$$(\frac{\beta_{(I,q_\alpha)}(x)}{\gamma(\Lambda)})^{nm/2}\mathrm{nrd}_{D_{\mathbf{R}}/\mathbf{R}}(I) = \mathrm{nrd}_{D_{\mathbf{R}}/\mathbf{R}}(\alpha)^{-1/2}(\frac{q_\alpha(x,x)}{nm})^{nm/2}.$$

On the other hand, by proposition 3.1 we have

$$\mathrm{nrd}_{D_{\mathbf{R}}/\mathbf{R}}(x)^2 = \mathrm{nrd}_{D_{\mathbf{R}}/\mathbf{R}}(\alpha)^{-1}\mathrm{nrd}_{D_{\mathbf{R}}/\mathbf{R}}(x\alpha\overline{x}) \leq \mathrm{nrd}_{D_{\mathbf{R}}/\mathbf{R}}(\alpha)^{-1}(\frac{q_\alpha(x,x)}{nm})^{nm}.$$

This concludes the proof of the proposition.

Definition 3.4. Let I be a generalized ideal. We define its Hermite invariants by

$$\gamma_{\min}(I) = \inf_{\alpha\in P}\{\gamma(I,q_\alpha)\},$$

and

$$\tau_{\min}(I) = \inf_{\alpha\in P}\{\tau(I,q_\alpha)\}.$$

Definition 3.5. Let I and J be two generalized ideals. We say that I and J are *equivalent* if there exists $x \in D_{\mathbf{R}}^*$ such that $xI = J$.

Definition 3.6. Let I be a generalized ideal. The *minimum* of I, denoted by $\min(I)$, is by definition

$$\min(I) = \min(\mathrm{N}_{D/\mathbf{Q}}(J) \mid J \text{ is an integral ideal and } J \text{ is equivalent to } I^{-1}\}.$$

Proposition 3.7. *Let Λ be an order of D, and let I be a generalized Λ–ideal. We have*

(i) $\gamma_{\min}(I) \geq \frac{nm}{d(\Lambda/\mathbf{Z})^{1/nm^2}} \min(I)^{2/nm^2}$

(ii) $\gamma_{\min}(\Lambda) = \frac{nm}{d(\Lambda/\mathbf{Z})^{1/nm^2}}$.

Proof. By 3.3, we have

$$\frac{q_\alpha(x,x)}{\det(I,q_\alpha)^{\frac{1}{nm^2}}} \geq \frac{nm}{d(\Lambda/\mathbf{Z})^{1/nm^2}} \left(\frac{\mathrm{nrd}_{D_\mathbf{R}/\mathbf{R}}(x)}{\mathrm{nrd}_{D_\mathbf{R}/\mathbf{R}}(I)}\right)^{2/nm}$$

for all $x \in D_\mathbf{R}$. Using the equalities

$$\mathrm{nrd}_{D_\mathbf{R}/\mathbf{R}}(x) = \mathrm{N}_{D_\mathbf{R}/\mathbf{R}}(x)^{1/m}, \mathrm{nrd}_{D_\mathbf{R}/\mathbf{R}}(I) = \mathrm{N}_{D_\mathbf{R}/\mathbf{R}}(I)^{1/m},$$

we obtain

$$\frac{q_\alpha(x,x)}{\det(I,q_\alpha)^{\frac{1}{nm^2}}} \geq \frac{nm}{d(\Lambda/\mathbf{Z})^{1/nm^2}} \mathrm{N}_{D_\mathbf{R}/\mathbf{R}}(xI^{-1})^{2/nm^2},$$

hence

$$\gamma(I,q_\alpha) \geq \frac{nm}{d(\Lambda/\mathbf{Z})^{1/nm^2}} \min(I)^{2/nm^2}.$$

As this holds for all $\alpha \in \mathcal{P}$, this proves (i). For (ii), it suffices to show that

$$\gamma_{\min}(\Lambda) \leq \frac{nm}{d(\Lambda/\mathbf{Z})^{1/nm^2}}.$$

This is done by considering the ideal lattice (Λ, q_1). Indeed, we have $\det(\Lambda, q_1) = d(\Lambda/\mathbf{Z})$, and $q_1(1,1) = nm$, hence we have

$$\gamma_{\min}(\Lambda) \leq \gamma(\Lambda, q_1) \leq \frac{nm}{d(\Lambda/\mathbf{Z})^{1/nm^2}}.$$

Lemma 3.8. *For any lattice (L,q) of rank r, we have*

$$\tau(L,q)\gamma(L^\sharp,q) \leq r^2/4.$$

Proof. See [1], Lemma 4.4.

Corollary 3.9. *Let I be a generalized ideal. Then we have*

$$\tau_{\min}(I) \leq \frac{nm^3}{4} d(\Lambda/\mathbf{Z})^{1/nm^2}.$$

Proof. By 3.7 and 3.8, we have

$$\frac{n^2m^4}{4} \geq \tau(I,q_\alpha)\gamma(I^\sharp,q_\alpha) \geq \tau(I,q_\alpha)\frac{nm}{d(\Lambda/\mathbf{Z})^{1/nm^2}}$$

for all $\alpha \in \mathcal{P}$. This implies the desired statement.

§4. Upper bounds for Euclidean minima

The aim of this section is to apply the results of §3 to obtain bounds for Euclidean and inhomogeneous minima in terms of Hermite invariants of ideal lattices.

Theorem 4.1. *For any generalized ideal I, we have*

$$M_{\mathbf{R}}(I) \leq (\frac{\tau_{\min}(I)}{\gamma_{\min}(\Lambda)})^{nm/2}\mathrm{nrd}_{D_{\mathbf{R}}/\mathbf{R}}(I).$$

Proof. Let (I,q) be an ideal lattice. For all $x \in D_{\mathbf{R}}$, there exists $c \in I$ such that $q(x-c) \leq \max(I,q)$. Hence $\beta_{I,q}(x-c) \leq \tau(I,q)$. By 3.3 an 3.7.(ii), we have

$$\mathrm{nrd}_{\mathrm{D}_{\mathbf{R}}/\mathbf{R}}(x-c) \leq (\frac{\tau(I,q)}{\gamma_{\min}(\Lambda)})^{nm/2}\mathrm{nrd}_{D_{\mathbf{R}}/\mathbf{R}}(I).$$

By definition, this implies that

$$M_{\mathbf{R}}(I) \leq (\frac{\tau(I,q)}{\gamma_{\min}(\Lambda)})^{nm/2}\mathrm{nrd}_{D_{\mathbf{R}}/\mathbf{R}}(I),$$

which leads to

$$M_{\mathbf{R}}(I) \leq (\frac{\tau_{\min}(I)}{\gamma_{\min}(\Lambda)})^{nm/2}\mathrm{nrd}_{D_{\mathbf{R}}/\mathbf{R}}(I).$$

This concludes the proof of the theorem.

Corollary 4.2. *We have*

$$M_{\mathbf{R}}(I) \leq (\tau_{\min}(I))^{nm/2}(4/nm^2)^{nm/2}(\frac{\sqrt{m}}{2})^{nm}d(\Lambda/\mathbf{Z})^{1/2m}\mathrm{nrd}_{D_{\mathbf{R}}/\mathbf{R}}(I).$$

Proof. This follows from the equality $\gamma_{\min}(\Lambda) = \frac{nm}{d(\Lambda/\mathbf{Z})^{1/nm^2}}$ (cf. Proposition 3.7.(ii)).

Corollary 4.3. *We have*

$$M_{\mathbf{R}}(I) \leq (\frac{m}{2})^{nm} d(\Lambda/\mathbf{Z})^{1/m} \mathrm{nrd}_{D_{\mathbf{R}}/\mathbf{R}}(I).$$

Proof. This follows immediately from 4.2 and 3.9.

Note that in the commutative case – that is, $m = 1$ – this gives us the bound of [1], 6.1, namely $M(I) \leq 2^{-n} d_K \mathrm{N}(I)$. If moreover k is totally real, then conjecturally we have a much better upper bound, namely $M(I) \leq 2^{-n} \sqrt{d_K} \mathrm{N}(I)$. The following corollary gives a necessary condition for an analog of this conjecture to hold in the non–commutative case.

Corollary 4.4. *Suppose that* $\tau_{\min}(I) \leq \frac{nm^2}{4}$. *Then*

$$M_{\mathbf{R}}(I) \leq (\frac{\sqrt{m}}{2})^{nm} d(\Lambda/\mathbf{Z})^{1/2m} \mathrm{nrd}_{D_{\mathbf{R}}/\mathbf{R}}(I).$$

Proof. This is an immediate consequence of 4.2.

§5. Examples

The main purpose of this section is to illustrate the results of §4 with some examples. Throughout this section, k will be a totally real number field of degree n, and D will be a totally definite quaternion field over k, i.e. such that every infinite place of k ramifies in D. Let Λ be a maximal order of D. As usual, we denote by d_k the discriminant of the field k.

Proposition 5.1. *We have*

$$\frac{1}{2^{2n}} M(k)^2 \leq M(\Lambda).$$

Proof. Let $x \in k$. There exists $\alpha \in \Lambda$ such that $m_\Lambda(x) = \mathrm{N}(x - \alpha)$. Let $\alpha = \alpha_0 + \alpha_1$, where $\alpha_0 \in k$ and α_1 is a pure quaternion. Then

$$\mathrm{nrd}_{D/k}(x - \alpha) = (x - \alpha_0)^2 - \alpha_1^2.$$

Note that $-\alpha_1^2$ is totally positive, as D is totally definite. Therefore we have

$$m_\Lambda(x) = \mathrm{N}_{k/\mathbf{Q}}((x - \alpha_0)^2 - \alpha_1^2)) \geq \mathrm{N}_{k/\mathbf{Q}}(x - \alpha_0)^2.$$

As $\alpha \in \Lambda$, we have $\mathrm{Tr}_{D/k}(\alpha) \in O_k$. Note that $\mathrm{Tr}_{D/k}(\alpha) = 2\alpha_0$. Hence we have $2\alpha_0 \in O_k$ and

$$\mathrm{N}_{k/\mathbf{Q}}(x-\alpha_0)^2 = \frac{1}{2^{2n}}\mathrm{N}_{k/\mathbf{Q}}(2x-2\alpha_0)^2 \geq \frac{1}{2^{2n}}m_k(2x)^2$$

so that

$$M(\Lambda) \geq m_\Lambda(x) \geq \frac{1}{2^{2n}}m_k(2x)^2,$$

and the claim is proved.

Using classical results concerning the Euclidean minimum of real quadratic fields, the previous result yields immediately the following lower bound for the Euclidean minimum of orders of totally definite quaternion algebras :

Theorem 5.2. *We have*

$$M(\Lambda) \geq \frac{d_k}{7552+3072\sqrt{6}}.$$

Proof. Indeed, we have $M(k) \geq \frac{\sqrt{d_k}}{16+6\sqrt{6}}$ (see for instance [7], th. 4.2.). This, combined with the previous proposition, gives the desired result.

Applying 4.3, we get the following bounds :

Corollary 5.3. *We have*

$$\frac{d_k}{7552+3072\sqrt{6}} \leq M(\Lambda) \leq \sqrt{d(\Lambda)}.$$

Proof. This follows immediately from 4.3 and 5.2.

In order to apply the results of §4, we need to investigate the ideal lattices that can be realized over a given maximal order. In the following proposition we do this for the root lattice E_8 :

Proposition 5.4. *Let (I, q_α) be an ideal lattice over Λ. Suppose that no finite place of k ramifies in D, and $\mathrm{nrd}_{D/k}(I)\mathcal{D}_k = \alpha^{-1}O_k$. Then $(I, q_\alpha) \simeq E_8$.*

Proof. As D is unramified at the finite places of k, we have $\mathcal{D}(\Lambda/O_k) = \Lambda$, hence $\mathcal{D}(\Lambda/\mathbf{Z}) = \mathcal{D}_k\Lambda$. Set $J = \mathrm{nrd}_{D/k}(I)$. We have

$$I\alpha\overline{I} = I\mathcal{D}_k^{-1}J^{-1}\overline{I} = \mathcal{D}_k^{-1}J^{-1}\mathrm{nrd}_{D/k}(I)\Lambda = \mathcal{D}_k^{-1}\Lambda.$$

This implies that $I\alpha\overline{I} = \mathcal{D}(\Lambda/\mathbf{Z})^{-1}$, and hence by prop. 2.4. (I, q_α) is unimodular. Moreover, by prop. 2.6. the lattice (I, q_α) is even. As the rank of this lattice is equal to 8, this implies that $(I, q_\alpha) \simeq E_8$ (see for instance [6], 4.8.1).

Note that the conditions of prop. 5.4 are actually necessary and sufficient for an ideal lattice to be isomorphic to E_8, cf. [5], 3.8.6.

Proposition 5.5. *Suppose that no finite place of k ramifies in D, and that the fundamental unit of O_k has norm -1. Then there exists an ideal lattice (Λ, q_α) that is isomorphic to E_8.*

Proof. The existence of a unit of O_k with norm -1 implies that $\mathcal{D}_k^{-1}$ has a totally positive generator α. By the previous proposition, we have $(\Lambda, q_\alpha) \simeq E_8$.

We can now apply 5.5 and the results of §4 to obtain an upper bound for the Euclidean minimum of some quaternionian orders :

Proposition 5.6. *Suppose that no finite place of k ramifies in D, and that the fundamental unit of O_k has norm -1. Then*

$$M(\Lambda) \leq \frac{d_k}{16}.$$

Proof. By 5.5, the lattice E_8 is an ideal lattice over Λ. As E_8 is unimodular and $\max(E_8)$ (see for instance [6], 4.8.1), we have by 4.1 and 3.7 that

$$M(\Lambda) \leq (\frac{1}{\gamma_{\min}(\Lambda)})^2 = (\frac{d(\Lambda/\mathbf{Z})^{1/8}}{4})^2.$$

As the finite places of k are unramified in D, we have $d(\Lambda/\mathbf{Z}) = d(\Lambda/O_k)d_k^4 = d_k^4$. This implies $M(\Lambda) \leq \frac{d_k}{16}$.

We obtain the following bounds :

Corollary 5.7. *Suppose that no finite place of k ramifies in D, and that the fundamental unit of O_k has norm -1. Then*

$$\frac{d_k}{7552 + 3072\sqrt{6}} \leq M(\Lambda) \leq \frac{d_k}{16}.$$

Note that a direct application of 5.3 would only have given the upper bound d_k^2.

Bibliography

[1] E. Bayer–Fluckiger, Upper bounds for Euclidean minima of algebraic number fields, *J. Number Th.* **121** (2006), 305–323.

[2] D. Berend, Multi–invariant sets of tori, *Trans. Amer. Math. Soc.* **280** (1983), 509–532.

[3] D. Berend, Minimal sets of tori, *Ergodic Theory Dyn. Syst.* **4** (1984), 499–507.

[4]. J.-P. Cerri, Euclidean and inhomogeneous spectra of number fields with unit rank strictly greater than 1, *J. Reine Angew. Math.* **592** (2006), 49–62.

[5] J. Chaubert, Minimum euclidien des ordres maximaux dans les algèbres centrales à division, thèse EPFL, 2006.

[6] J.H. Conway, N.J.A. Sloane, *Sphere packings, lattices and groups*, Springer–Verlag (1988).

[7] F. Lemmermeyer, The Euclidean algorithm in algebraic number fields, *Expo. Math.* **13** (1995), 385–416.

[8] I. Reiner, *Maximal orders*, London Mathematical Society Monographs **28**, Oxford University Press (2003).

[9] P. Samuel, About Euclidean rings, *J. Algebra* **19** (1971), 282–301.

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