Inhomogeneous and Euclidean spectra of number fields with unit rank strictly greater than 1

Jean-Paul Cerri

Inhomogeneous and Euclidean spectra of number fields with unit rank strictly greater than 1

Jean-Paul Cerri

Abstract

Let K be a number field with unit rank $r > 1$. In this article we show that the inhomogeneous minimum $M(\overline{K})$ of K is attained by at least one rational point. In particular, if $M(K)$ is the Euclidean minimum of K, we have $M(K) = M(\overline{K}) \in \mathbb{Q}$. This phenomenon has consequences on the decidability of the Euclidean nature of such a field. Moreover, in case K is not a CM-field, we prove that $M(\overline{K})$ is attained, isolated, and that the inhomogeneous minimum function takes discrete rational values.

Mathematics Subject Classification: Primary 11R04, Secondary 13F07, 37B05.

1 Introduction

The Euclidean minimum $M(K)$ of a number field K and the inhomogeneous minimum $M(\overline{K})$ of the lattice associated to its ring of integers have been, until today, the object of many conjectures. For instance, it has been showed that $M(K) = M(\overline{K})$ if the unit rank r of K verifies $r \leq 1$, but nothing was known for $r > 1$. In this paper we prove that the equality holds in all cases, and we establish a more powerful property relative to the rationality of $M(K)$, which corresponds, for the case $r > 1$, to a conjecture made by Barnes and Swinnerton-Dyer in the real quadratic case. Since the case $r = 0$ is obvious, it only leaves open the problem for $r = 1$.
In the same way, we prove other conjectures (e.g. $M(\overline{K})$ is attained and isolated) when $r > 1$ and K is not a CM-field. The different problems are introduced in section 3.
Our approach rests on important results of ergodic theory and topological dynamics, which have been established by Berend and which give information on the closed subsets of the torus, invariant under the action of a semigroup of endomorphisms, according to some properties of this semigroup. Here, the semigroup that we use is defined thanks to the unit group of K, which plays a fundamental part in the different proofs.

2 Berend's results

Let n be a positive integer. From now on, we denote the n-dimensional torus $\mathbb{R}^n/\mathbb{Z}^n$ by $\mathbb{T}_n$. It is an additive group which is compact for the topology induced by the metric topology of $\mathbb{R}^n$. Continuous endomorphisms of $\mathbb{T}_n$ can be represented by $n \times n$ matrices with integer entries. Points and endomorphisms of $\mathbb{T}_n$ can be lifted to points and to linear transformations of $\mathbb{R}^n$, respectively.

Let f be an endomorphism of $\mathbb{T}_n$. We shall indifferently denote by f its matrix, its lift to $\mathbb{R}^n$ whose matrix is the same, and when we shall speak of the eigenvalues and eigenvectors of f, it will be in the ordinary sense for f as an endomorphism of $\mathbb{C}^n$ (extended to $\mathbb{C}^n$ by linearity so that the matrix of f is the same).

Let $\mathcal{E}$ be a set of continuous endomorphisms of $\mathbb{T}_n$.
A subset F of $\mathbb{T}_n$ will be said *$\mathcal{E}$-invariant* if for all $f \in \mathcal{E}$ we have $f(F) \subset F$.
A nonempty closed $\mathcal{E}$-invariant set F will be said *$\mathcal{E}$-minimal* if it contains no nonempty closed $\mathcal{E}$-invariant proper subset.
Using Zorn's lemma, it is easy to see that every nonempty closed $\mathcal{E}$-invariant subset of $\mathbb{T}_n$ contains a $\mathcal{E}$-minimal set (see for instance [9] or [4]).

Assume that Σ is a commutative semigroup of endomorphisms of $\mathbb{T}_n$. The set of common eigenvectors of Σ lying in $\mathbb{C}^n$ is denoted by $\mathrm{evec}\Sigma$. If $v \in \mathrm{evec}\Sigma$ then $\mathrm{spec}_v\Sigma$ is the set of eigenvalues corresponding to v of all the elements of Σ.

Definition 1. Σ is called *hyperbolic* if for each $v \in \mathrm{evec}\Sigma$, $\mathrm{spec}_v\Sigma \not\subseteq \mathbb{C}_1$, where $\mathbb{C}_1$ is the unit circle in $\mathbb{C}$.

Definition 2. Σ is called *multi-parameter* if for each $v \in \mathrm{evec}\Sigma$, $\mathrm{spec}_v\Sigma$ contains two rationally independent elements.

We can now give the results which have been established by Berend (see [2] and [3]).

Theorem 1. *Let Σ be a commutative semigroup of epimorphisms of $\mathbb{T}_n$. The following conditions are equivalent:*
(1) *Any Σ-minimal set of $\mathbb{T}_n$ is composed of torsion elements.*
(2) *Σ is hyperbolic and multiparameter.*

Theorem 2. *Let Σ be a commutative semigroup of endomorphisms of $\mathbb{T}_n$. Then the only infinite closed Σ-invariant subset of $\mathbb{T}_n$ is $\mathbb{T}_n$ itself if and only if the following conditions are satisfied:*
(1) *there exists $\sigma \in \Sigma$ such that the characteristic polynomial of σ^p is irreductible over $\mathbb{Z}$ for every positive integer p.*
(2) *for every $v \in \mathrm{evec}\Sigma$, there exists $\lambda \in \mathrm{spec}_v\Sigma$ of modulus strictly greater than 1.*
(3) *Σ contains a pair of rationally independent endomorphisms.*

Theorem 1 is a part of [3], Thm 2.1, and Theorem 2 is [2], Thm 2.1. The proof of the implication (2)⇒(1) of Theorem 1 needs the following Lemma (Lemma 4.2. in [3]) that we shall also use later.

Lemma 1. *Let K be a number field and S a subsemigroup of the multiplicative group K^* of K. Suppose that for every $s \in S$ there exists a positive integer k such that $\mathbb{Q}(s^k)$ is a proper subfield of K. Then there exists a positive integer N and a proper subfield F of K such that $s^N \in F$ for every $s \in S$.*

3 Euclidean and inhomogeneous spectra of a number field

From now on K will be a number field of degree $n \geq 2$ and of signature (r_1, r_2). Denote by σ_i, $1 \leq i \leq r_1$, the r_1 real embeddings of K in $\mathbb{R}$, and σ_i, $\sigma_{r_2+i} = \overline{\sigma_i}$, where $r_1 + 1 \leq i \leq r_1 + r_2$, the $2r_2$ complex embeddings of K in $\mathbb{C}$. Let $N_{K/\mathbb{Q}}$

be the norm defined on K by

$$\forall \xi \in K,\ N_{K/\mathbb{Q}}(\xi) = \prod_{i=1}^{n} \sigma_i(\xi) = \prod_{i=1}^{r_1} \sigma_i(\xi) \prod_{i=r_1+1}^{r_1+r_2} \left|\sigma_i(\xi)\right|^2.$$

Let us denote $\mathbb{Z}_K$ the ring of integers of K, E_K the multiplicative group of units of K, r the unit rank of K, $r = r_1 + r_2 - 1$, and $\mathcal{L}$ the logarithmic embedding of $K\backslash\{0\}$ in $\mathbb{R}^{r_1+r_2}$ defined by

$$\forall \xi \in K\backslash\{0\}, \mathcal{L}(\xi) = \left(\ln|\sigma_1(\xi)|, ..., \ln|\sigma_{r_1+r_2}(\xi)|\right).$$

In this section we give definitions and elementary properties relative to the notions of Euclidean minimum and inhomogeneous minimum of K. The results are classical and given without proofs.

Definition 3. Let $\xi \in K$. The *Euclidean minimum of* ξ is the real number $m_K(\xi)$ defined by

$$m_K(\xi) = \inf\Big\{ |N_{K/\mathbb{Q}}(\xi - \Upsilon)|;\ \Upsilon \in \mathbb{Z}_K \Big\}.$$

It is elementary to see that m_K has the following properties.

Proposition 1. *We have*

i) $\forall (\xi, \Upsilon, \varepsilon) \in K \times \mathbb{Z}_K \times E_K,\ m_K(\varepsilon\xi - \Upsilon) = m_K(\xi)$.

ii) $\forall \xi \in K,\ \exists \Upsilon \in \mathbb{Z}_K$ *such that* $m_K(\xi) = |N_{K/\mathbb{Q}}(\xi - \Upsilon)|$.

iii) $\forall \xi \in K,\ m_K(\xi) \in \mathbb{Q}$ *and* $m_K(\xi) = 0 \iff \xi \in \mathbb{Z}_K$.

Now we can extend m_K to $\overline{K} = K \otimes_{\mathbb{Q}} \mathbb{R}$, the product of the archimedian completions of K, which is usually identified to $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$, but that we shall identify here to

$$H = \mathbb{R}^{r_1} \times \Big\{ z \in \mathbb{C}^{2r_2};\ \forall i \in \{1, ..., r_2\},\ z_{r_2+i} = \overline{z_i} \Big\},$$

which will be more convenient for later computations. Under this identification, an element ξ of K is viewed as the n-tuple $(\sigma_i(\xi))_{i=1...n}$ of H.
If $(x, y) \in H^2$, we shall denote $x.y$ the element z of H defined by $z_i = x_i y_i$ for every i (extension of the product of K).

Definition 4. Let $x \in H$. The *inhomogeneous minimum of* x is the real number $m_{\overline{K}}(x)$ defined by

$$m_{\overline{K}}(x) = \inf\Big\{ \prod_{i=1}^{n} |x_i - \sigma_i(\Upsilon)|;\ \Upsilon \in \mathbb{Z}_K \Big\}.$$

Of course for $\xi \in K$ we have $m_{\overline{K}}(\xi) = m_K(\xi)$.

Proposition 2. $m_{\overline{K}}$ *has the following properties:*

i) $\forall (x, \Upsilon, \varepsilon) \in H \times \mathbb{Z}_K \times E_K,\ m_{\overline{K}}(x) = m_{\overline{K}}(\varepsilon.x - \Upsilon)$.

ii) $m_{\overline{K}}$ *is upper semi-continuous on* H.

Remark 1. Properties 1.ii) and 1.iii) of m_K cannot be extended to H via $m_{\overline{K}}$.

Proposition 2.i), with $\varepsilon = 1$, shows that $m_{\overline{K}}$ induces an upper semi-continuous map on $H/\mathbb{Z}_K$ which is a compact set (isomorphic to $\mathbb{T}_n$), so that $m_{\overline{K}}$ is bounded and attains its maximum on H. Thus we can write the following definition.

Definition 5. We call *inhomogeneous minimum of* K and we denote $M(\overline{K})$ the positive real number defined by

$$M(\overline{K}) = \sup\{m_{\overline{K}}(x);\ x \in H\} < +\infty.$$

As a consequence, we obtain that m_K is bounded on K and we can give the following definition.

Definition 6. We call *Euclidean minimum of* K and we denote by $M(K)$ the positive real number defined by

$$M(K) = \sup\{m_K(\xi);\ \xi \in K\}.$$

By the definitions, it is clear that $M(K) \leq M(\overline{K})$. In the case $n = 2$ and K is totally real (the complex case is obvious), it has been proved by Barnes and Swinnerton-Dyer (see [1]), that, in fact, there is an equality, and they have conjectured that there is an element $\xi \in K$ such that $M(\overline{K}) = m_K(\xi)$. Of course, if it is true, we have $M(K) = M(\overline{K}) \in \mathbb{Q}$.
We shall prove here that this conjecture is verified by any K as soon as $r > 1$.

From Definition 6 and Proposition 1.ii) we can write

$$\forall \xi \in K,\ \exists \Upsilon \in \mathbb{Z}_K \text{ such that } |N_{K/\mathbb{Q}}(\xi - \Upsilon)| \leq M(K),$$

which leads to the following definition.

Definition 7. $M(\overline{K})$ will be said *attained* if

$$\forall x \in H,\ \exists \Upsilon \in \mathbb{Z}_K \text{ such that } |\prod_{i=1}^{n} x_i - \sigma_i(\Upsilon)| \leq M(\overline{K}).$$

It is known that, for $n = 2$, this property is not always true. For instance, it is not verified by $\mathbb{Q}(\sqrt{13})$ (see [1], [8] or [11]). We shall prove here that $M(\overline{K})$ is attained as soon as $r > 1$ and K is not a CM-field.

Definition 8. The set of values of m_K and $m_{\overline{K}}$ will be respectively called the *Euclidean spectrum* and the *inhomogeneous spectrum* of K.

Definition 9. The *second inhomogeneous minimum* and the *second Euclidean minimum* of K are defined by

$$M_2(\overline{K}) = \sup_{\substack{x \in H \\ m_{\overline{K}}(x) < M(\overline{K})}} \Big(m_{\overline{K}}(x)\Big) \quad \text{and} \quad M_2(K) = \sup_{\substack{\xi \in K \\ m_K(\xi) < M(K)}} \Big(m_K(\xi)\Big).$$

Going further we get by induction (with $p \geq 2$)

$$M_{p+1}(\overline{K}) = \sup_{\substack{x \in H \\ m_{\overline{K}}(x) < M_p(\overline{K})}} \Big(m_{\overline{K}}(x)\Big) \quad \text{and} \quad M_{p+1}(K) = \sup_{\substack{\xi \in K \\ m_K(\xi) < M_p(K)}} \Big(m_K(\xi)\Big).$$

Definition 10. $M(\overline{K})$ will be said *isolated* if $M_2(\overline{K}) < M(\overline{K})$.

These definitions lead to other questions. For instance, it has been conjectured

that, for $n = 2$ and K totally real, $M(\overline{K})$ is isolated, but this has only been proved when $M(\overline{K})$ is "attained" by a finite number of points of H modulo $\mathbb{Z}_K$ (see [1]). We shall prove here that $M(\overline{K})$ is isolated as soon as $r > 1$ and K is not a CM-field.

Another question could be: like for the inhomogeneous and Euclidean minima, is there an equality between the second minima? The answer is no when $n = 2$ (see [10], and for other related questions [11]): if $K = \mathbb{Q}(\sqrt{73})$, we have $M_2(K) < M_2(\overline{K})$. Nevertheless, we shall prove that there is an equality for $r > 1$ if K is not a CM-field, and we shall even generalize this phenomenon to the successive minima:

$$\forall p > 1,\ M_{p+1}(\overline{K}) = M_{p+1}(K) < M_p(\overline{K}) = M_p(K),$$

with $\lim_{p \to +\infty} M_p(\overline{K}) = 0$. In this case both spectra are identical, included in $\mathbb{Q}$, and only composed of the successive minima and 0.
Note that if we remove the assumption $r > 1$, the previous limit does not necessarily hold, as can show the elementary choice $K = \mathbb{Q}(\sqrt{5})$: in this case, the $M_p(\overline{K})$ form a strictly decreasing sequence and we have $\lim_{p \to +\infty} M_p(\overline{K}) = 1/(2 + 2\sqrt{5})$, even if it is possible to find $\xi \in K$ with $m_K(\xi)$ arbitrarily small.

4 Main results

4.1 The link

In view of the link with results of section 2, we fix from now on a $\mathbb{Z}$-basis $(e_i)_{1 \leq i \leq n}$ of $\mathbb{Z}_K$. Thus, K, $\mathbb{Z}_K$ and H can respectively be identified to $\mathbb{Q}^n$, $\mathbb{Z}^n$ and $\mathbb{R}^n$, via Φ, the isomorphism from $\mathbb{R}^n$ onto H defined by:

$$\forall x \in \mathbb{R}^n,\ \Phi(x) = \Big(\sum_{j=1}^{n} x_j \sigma_i(e_j) \Big)_{i=1 \ldots n}.$$

Putting

$$\forall x \in \mathbb{R}^n,\ m(x) = m_{\overline{K}}(\Phi(x)),$$

we obtain a function defined and upper semi-continuous on $\mathbb{R}^n$, taking the same values as $m_{\overline{K}}$, which study is equivalent to the study of $m_{\overline{K}}$. Clearly m is defined modulo $\mathbb{Z}^n$ so that it induces an upper semi-continuous function $\tilde{m}$ on $\mathbb{T}_n$ given by:

$$\forall x \in \mathbb{R}^n,\ \tilde{m}(\overline{x}) = m(x),$$

where $\overline{x}$ is the class of x modulo $\mathbb{Z}^n$.
Proposition 2.i) with $\Upsilon = 0$ shows that, if $\varepsilon \in E_K$, m is invariant under the action of the function $f_\varepsilon : \mathbb{R}^n \longrightarrow \mathbb{R}^n$ defined by

$$f_\varepsilon(x) = \Phi^{-1}(\varepsilon . \Phi(x)),$$

which is the continuous extension to $\mathbb{R}^n$ of the function which sends $y \in \mathbb{Q}^n$ on the coordinates in the basis (e_i) of $\varepsilon \Sigma y_j e_j$.
The set $\{f_\varepsilon;\ \varepsilon \in E_K\}$ is a group of automorphisms of $\mathbb{R}^n$, isomorphic to the multiplicative group E_K. Moreover, for every ε, the matrix of f_ε relatively to the canonical basis, has integer entries, so that f_ε induces an endomorphism of $\mathbb{T}_n$, denoted by g_ε and defined by

$$g_\varepsilon(\overline{x}) = \overline{f_\varepsilon(x)}.$$

Obviously, since for all $x \in \mathbb{R}^n$ we have $m(f_\varepsilon(x)) = m(x)$, we get

$$\forall \alpha \in \mathbb{T}_n,\ \tilde{m}(g_\varepsilon(\alpha)) = \tilde{m}(\alpha).$$

Now we put

$$\Sigma = \Big\{ g_\varepsilon;\ \varepsilon \in E_K \Big\}.$$

It is easy to see that $g_\varepsilon \circ g_{\varepsilon'} = g_{\varepsilon\varepsilon'}$ and that, in fact, Σ is a commutative group of automorphisms of $\mathbb{T}_n$, isomorphic to the multiplicative group E_K.
In view of the determination of the eigenvalues of the f_ε (or of the g_ε), it is necessary to extend Φ to $\mathbb{C}^n$. This is done as follows: if $(u, v) \in \mathbb{R}^n \times \mathbb{R}^n$, then we put $\Phi'(u + Iv) = \Phi(u) + I\Phi(v)$ and Φ' is an automorphism of $\mathbb{C}^n$.
From now on, we denote v_i $(1 \leq i \leq n)$ the vectors of the canonical basis of $\mathbb{R}^n$ (or $\mathbb{C}^n$) defined by

$$(v_i)_j = \delta_{i,j},$$

where $\delta_{i,j}$ is the Kronecker symbol, equal to 1 if $i = j$ and to 0 otherwise, and we put

$$w_i = \Phi'^{-1}(v_i) \in \mathbb{C}^n.$$

Since Φ' is an automorphism of $\mathbb{C}^n$, the w_i form a basis of $\mathbb{C}^n$. Moreover, with the notations of section 2, we have the following property.

Proposition 3. *If $u \in \mathrm{evec}\Sigma$, there exists $i \in \{1, ..., n\}$ such that*

$$\mathrm{spec}_u \Sigma = \{\sigma_i(\varepsilon);\ \varepsilon \in E_K\}.$$

Proof. If we still denote f_ε the linear function on $\mathbb{C}^n$ whose restriction to $\mathbb{R}^n$ is f_ε, we have

$$\forall z \in \mathbb{C}^n,\ f_\varepsilon(z) = \Phi'^{-1}(\varepsilon.\Phi'(z)),$$

so that for every i

$$f_\varepsilon(w_i) = \Phi'^{-1}(\varepsilon.v_i) = \Phi'^{-1}(\sigma_i(\varepsilon)v_i) = \sigma_i(\varepsilon)w_i.$$

Thus w_i is an eigenvector for f_ε, corresponding to the eigenvalue $\sigma_i(\varepsilon)$, and we see that $w_i \in \mathrm{evec}\Sigma$.
Now let u be an element of $\mathrm{evec}\Sigma$. Since the w_i form a basis of $\mathbb{C}^n$ we can write $u = \sum u_i w_i$ where for every i, $u_i \in \mathbb{C}$. Then for every $\varepsilon \in E_K$, u is an eigenvector for f_ε and there exists $\lambda_\varepsilon \in \mathbb{C}$ which verifies $f_\varepsilon(u) = \lambda_\varepsilon u$, or, since for every i $f_\varepsilon(w_i) = \sigma_i(\varepsilon)w_i$, $\sum u_i\sigma_i(\varepsilon)w_i = \sum \lambda_\varepsilon u_i w_i$. But $u \neq 0$ and there exists i_0 in $\{1, ..., n\}$ such that $u_{i_0} \neq 0$. Since the w_i are independent, we must have $u_{i_0}\sigma_{i_0}(\varepsilon) = u_{i_0}\lambda_\varepsilon$, so that $\lambda_\varepsilon = \sigma_{i_0}(\varepsilon)$.
This yields $\mathrm{spec}_u \Sigma = \{\lambda_\varepsilon;\ \varepsilon \in E_K\} = \{\sigma_{i_0}(\varepsilon);\ \varepsilon \in E_K\}$. □

4.2 Inhomogeneous and Euclidean minima

Now, we can give the first important result.

Theorem 3. *Let K be a number field of degree $n \geq 3$. If the unit rank r of K is strictly greater than 1, in particular if K is totally real, there exists $\xi \in K$ such that*

$$M(\overline{K}) = m_{\overline{K}}(\xi) = m_K(\xi).$$

Proof. First of all, since it is a group of automorphisms, Σ is a semigroup of epimorphisms of $\mathbb{T}_n$ and we can easily check that it is hyperbolic and multi-parameter.

The hyperbolic character of Σ comes from Proposition 3. If Σ is not hyperbolic, then there exists an i such that $|\sigma_i(\varepsilon)| = 1$ for every ε of E_K. If $i > r_1 + r_2$ the property is still true with $i - r_2$ instead of i, and we can suppose $i \leq r_1 + r_2$, so that $\mathcal{L}(E_K)$ is included in an hyperplane of equation $x_i = 0$ with $i \leq r_1 + r_2$. But it is also included in the hyperplane of equation $\sum_{1 \leq j \leq r_1} x_j + 2\sum_{r_1+1 \leq j \leq r_1+r_2} x_j = 0$, which is distinct of the latter, since $r \geq 1$. Thus, we obtain a contradiction to Dirichlet's theorem, by which $\mathcal{L}(E_K)$ is a lattice of rank $r = r_1 + r_2 - 1$.

The multi-parameter character of Σ comes from Proposition 3 and $r \geq 2$. Since $r \geq 2$ there are at least two independent units, say ε_1 and ε_2. Then, i being given, if $\sigma_i(\varepsilon_1)^l = \sigma_i(\varepsilon_2)^m$ with l and m integers, by injectivity of σ_i, we have $\varepsilon_1^l \varepsilon_2^{-m} = 1$ which yields $l = m = 0$.

Thus Theorem 1 can be applied.
Consider the set S defined by

$$S = \{\alpha \in \mathbb{T}_n \text{ such that } \tilde{m}(\alpha) = M(\overline{K})\}.$$

Recall that $\tilde{m}$ is upper semi-continuous so that it attains its upper bound on $\mathbb{T}_n$. In particular S is nonempty. Moreover, by upper semi-continuity of $\tilde{m}$, S is a closed subset of $\mathbb{T}_n$: it is easy to see that if (α_p) is a sequence of S, which converges to α, we have

$$M(\overline{K}) = \limsup_{p \to +\infty} \tilde{m}(\alpha_p) \leq \tilde{m}(\alpha)$$

by upper semi-continuity, so that $\alpha \in S$, by the definitions of $M(\overline{K})$ and S.
Now, if $\alpha \in S$, we know that for every $\varepsilon \in E_K$, $\tilde{m}(g_\varepsilon(\alpha)) = \tilde{m}(\alpha)$ which gives $g_\varepsilon(\alpha) \in S$. This shows that S is Σ-invariant.

Let S' be a Σ-minimal subset of S. By Theorem 1, S' is composed of torsion elements i.e. of elements α of $\mathbb{T}_n$ for which there exists $k_\alpha \in \mathbb{Z}\backslash\{0\}$ such that $k_\alpha \alpha = 0$ (in $\mathbb{T}_n$). Such an element has necessarily its lifts in $\mathbb{Q}^n$, and if X/k_α with $X \in \mathbb{Z}^n$ is one of them, $\xi = 1/k_\alpha \sum X_i e_i$ is suitable. □

Since it is known that if $r \leq 1$, $M(K) = M(\overline{K})$ (see [11]) we get the following result.

Corollary 1. *For every number field K we have $M(K) = M(\overline{K})$. Moreover if the unit rank of K is strictly greater than 1, then $M(K) = M(\overline{K}) \in \mathbb{Q}$.*

Proof. The equality $M(K) = M(\overline{K})$ is a direct consequence of definitions and Theorem 3. The rationality of this number follows from Proposition 1.iii). □

4.3 The decidability of the Euclideanity of a number field

From the definition of $M(K)$ and the standard definition of *norm-Euclideanity* of number fields, it is well known that the value of $M(K)$ gives the following information:

- If $M(K) < 1$, K is norm-Euclidean,
- If $M(K) > 1$, K is not norm-Euclidean,
- If $M(K) = 1$, we cannot conclude except if there is an element ξ of K such that $M(K) = m_K(\xi)$; in this case K is not norm-Euclidean,

so that Theorem 3 and Corollary 1 give the following result.

Corollary 2. *Let K be a number field with unit rank strictly greater than 1. If $M(K) = 1$, then K is not norm-Euclidean.*

Let us put now

$$\mathcal{A} = \{z \in H \text{ such that } \prod_{i=1}^{n} |z_i| < 1\}.$$

It is obvious that if $\mathbb{Z}_K + \mathcal{A} = H$ then K is norm-Euclidean. H.W. Lenstra Jr. has conjectured that it is in fact an equivalence (see [12]). Thanks to Theorem 3, we can prove that this is true as soon as $r > 1$.

Theorem 4. *Let K be a number field with unit rank strictly greater than 1. We have*

$$K \textit{norm-Euclidean} \Longleftrightarrow \mathbb{Z}_K + \mathcal{A} = H.$$

Proof. If K is norm-Euclidean, we have $M(K) = M(\overline{K}) \leq 1$. Assume that $M(\overline{K}) = 1$. Then by Theorem 3, there exists $\xi \in K$ such that $m_K(\xi) = 1$. But, since K is norm-Euclidean, this is impossible, so that

$$M(K) = M(\overline{K}) = M < 1.$$

Let $z \in H$. We have $m_{\overline{K}}(z) \leq M < 1$ and, by definition of $m_{\overline{K}}(z)$, there exists $Z \in \mathbb{Z}_K$ such that

$$\prod_{i=1}^{n} |z_i - \sigma_i(Z)| \leq \frac{M+1}{2} < 1.$$

This implies $\mathbb{Z}_K + \mathcal{A} = H$. □

Remark 2. In fact we have the following more precise result.
If $\mathcal{A}_k = \{z \in H \text{ such that } \prod_{i=1}^{n} |z_i| \leq k\}$, then we can write

$$K \text{ norm-Euclidean} \iff \exists\, k \in]0,1[\text{ such that } \mathbb{Z}_K + \mathcal{A}_k = H.$$

Let us give now an important corollary of Theorem 4 which has already been pointed out by H.W. Lenstra Jr.

Corollary 3. *K being given with unit rank strictly greater than 1, the question whether K is norm-Euclidean is decidable.*

The reader can refer to [12] for more details.

4.4 Inhomogeneous and Euclidean spectra

We can be more precise and look at all the values of $m_{\overline{K}}$ or m. It is a remarkable fact that, contrary to what can happen in degree 2, all these values are rational as soon as $r > 1$ and K is not a CM-field (totally complex quadratic extension of a totally real number field). More precisely, inhomogeneous and Euclidean spectra are equal, included in $\mathbb{Q}$ and we have the following result.

Theorem 5. *Let K a number field of degree $n \geq 3$. If the unit rank r of K is strictly greater than 1 and if K is not a CM-field, in particular if K is totally real, there exists a strictly decreasing sequence $(r_p)_{p\geq 1}$ of positive rational numbers, which verifies:*

(i) $\lim_{p \to +\infty} r_p = 0.$

(ii) $m_{\overline{K}}(H) = m(\mathbb{R}^n) = \tilde{m}(\mathbb{T}_n) = \{r_p;\ p \geq 1\} \cup \{0\}$.

(iii) *for each* $p \geq 1$ *the set of* $\alpha \in \mathbb{T}_n$ *such that* $\tilde{m}(\alpha) = r_p$ *is finite and lifts to points in* $\mathbb{Q}^n$, *which implies that if* $x \notin K$, $m_{\overline{K}}(x) = 0$.

The proof of Theorem 5 uses the following lemma.

Lemma 2. *Let* K *be as in Theorem 5. There exists a unit* $\varepsilon \in E_K$ *such that for every positive integer* p *we have* $\mathbb{Q}(\varepsilon^p) = K$.

Proof of Lemma 2. Assume that this result is false and that for every $\varepsilon \in E_K$, there exists a $p_\varepsilon > 0$ such that $\mathbb{Q}(\varepsilon^{p_\varepsilon})$ is a proper subfield of K. Then, as E_K is a subsemigroup of the multiplicative group K^* of K, we know by Lemma 1 that there exists a positive integer N and a proper subfield F of K such that $\varepsilon^N \in F$ for every $\varepsilon \in E_K$.
Let us put $n' = [F : \mathbb{Q}]$. Since F is a proper subfield of K, n' is a proper divisor of n and we have $2n' \leq n$. Let us denote (r_1', r_2') the signature of F.
Let $(\varepsilon_1, ..., \varepsilon_r)$ be a set of fundamental units of K. Since $\varepsilon_1, ..., \varepsilon_r$ are independent and $N > 0$, $\varepsilon_1^N, ..., \varepsilon_r^N$ are r independent units of F, so that $r \leq r'$ where $r' = r_1' + r_2' - 1$ is the unit rank of F, i.e. the maximal number of independent units of F. Thus $r_1 + r_2 \leq r_1' + r_2'$, which implies $n - r_2 \leq n' - r_2'$. From this inequality and from $2n' \leq n$, we deduce

$$r_2 \geq r_2 - r_2' \geq n - n' \geq n/2,$$

But $n = r_1 + 2r_2$ so that the only possibility is $(r_1, r_2) = (0, n/2)$, which leads to $r_2' = 0$, $n' = n/2$ and $r_1' = n/2$. This proves that K is a totally complex quadratic extension of the totally real field F, which was excluded by hypothesis. □

Proof of Theorem 5. Let k be a positive real number verifying

$$0 < k \leq M(\overline{K}).$$

Let us denote S_k the set of $\alpha \in \mathbb{T}_n$ such that $\tilde{m}(\alpha) \geq k$. By upper semi-continuity of $\tilde{m}$ and choice of k, S_k is a nonempty closed proper subset of $\mathbb{T}_n$ (proper because otherwise we should have $m(x) \geq k > 0$ for all $x \in \mathbb{R}^n$ which is obviously impossible). Moreover as in proof of Theorem 3, S_k, like S, is Σ-invariant, so that, if hypotheses of Theorem 2 are verified, we know that S_k is finite.
But condition (1) comes from Lemma 2. $\varepsilon \in E_K$ being given, since f_ε^p has the $\sigma_i(\varepsilon)^p = \sigma_i(\varepsilon^p)$ as eigenvalues associated to the eigenvectors w_i, the characteristic polynomial of g_ε^p is $\prod_{i=1}^n (X - \sigma_i(\varepsilon^p))$, which is the characteristic polynomial of ε^p so that it is irreductible over $\mathbb{Z}$ if $[\mathbb{Q}(\varepsilon^p) : \mathbb{Q}] = n$.
We can deduce condition (2) from the existence, i being given, of a unit ε such that $|\sigma_i(\varepsilon)| > 1$ (take ε such that $\sigma_i(\varepsilon) \notin \mathbb{C}_1$ as in proof of Theorem 3, and if $|\sigma_i(\varepsilon)| < 1$ take $1/\varepsilon$).
Finally, since $r > 1$, condition (3) is given by two independent units, say ε_1 and ε_2: if $g_{\varepsilon_1}^l = g_{\varepsilon_2}^m$, with l and m integers, then, in particular, for every $x \in K$, $\varepsilon_1^l x \equiv \varepsilon_2^m x \bmod \mathbb{Z}_K$ which leads to $(\varepsilon_1^l \varepsilon_2^{-m} - 1)x \in \mathbb{Z}_K$. But this is possible only if $\varepsilon_1^l \varepsilon_2^{-m} - 1 = 0$ and this implies $l = m = 0$. Thus Theorem 2 can be applied and S_k is finite.

Then, if $\alpha = \overline{x} \in S_k$, since for all non-torsion unit ε (here $r \geq 1$), $g_\varepsilon(S_k) \subset S_k$, there exists distinct positive integers $l > p > 0$ such that $g_\varepsilon^l(\alpha) = g_\varepsilon^p(\alpha)$ which leads to $\varepsilon^{l-p}.\Phi(x) \equiv \Phi(x) \bmod \mathbb{Z}_K$ and $\Phi(x) \in K = \Phi(\mathbb{Q}^n)$ so that $x \in \mathbb{Q}^n$.

Thus, S_k is a finite subset of elements whose lifts are in $\mathbb{Q}^n$ and necessarily $\tilde{m}(S_k) = \tilde{m}(\mathbb{T}_n) \cap [k, M(\overline{K})]$ is a finite subset of $\mathbb{Q}$ by Proposition 1.iii).

Let us put $r_1 = M(\overline{K}) > 0$, and for $p \geq 1$, if $r_p > 0$, $r_{p+1} = \sup \tilde{m}(\mathbb{T}_n \backslash S_{r_p})$, which is well defined since $S_{r_p} \subsetneq \mathbb{T}_n$.

We see that, p being given, if r_p is defined and if $r_p > 0$, since S_{r_p} is finite and the set of $\overline{1/q}$ $(q \geq 2)$ infinite, there exists $q \in \mathbb{N}$, $q \geq 2$, such that $\overline{1/q} \in \mathbb{T}_n \backslash S_{r_p}$, so that $r_{p+1} \geq \tilde{m}(\overline{1/q}) = 1/q^n > 0$.
Thus, by induction, for all p, r_p is defined and $r_p > 0$.

By construction (r_p) is decreasing. Assume that for some p we have $r_{p+1} = r_p$. Then, $\sup \tilde{m}(\mathbb{T}_n \backslash S_{r_p}) = r_p$, which means that there are elements α in $\mathbb{T}_n$ with $\tilde{m}(\alpha) < r_p$ as close to r_p as desired. But this is in contradiction for instance with the fact that $S_{r_p/2}$ is finite. Thus the sequence (r_p) is strictly decreasing.

The same argument ($S_{r_p/2}$ is finite) shows that for every p, r_p is in $\tilde{m}(\mathbb{T}_n)$.

The decreasing sequence (r_p) converges to a real number $L \geq 0$. Assume that $L > 0$. Since $S_{L/2}$ is finite, the set of r_p, which is a subset of $\tilde{m}(\mathbb{T}_n)$ whose all elements are greater than $L/2$, would be finite. We obtain a contradiction to the fact that (r_p) is strictly decreasing, and necessarily $L = 0$. This is (i).

The inclusion $\{r_p;\ p \geq 1\} \cup \{0\} \subset \tilde{m}(\mathbb{T}_n)$ is obvious. Assume that it is a strict one. Then there is an α in $\mathbb{T}_n$ such that $r_{p+1} < \tilde{m}(\alpha) < r_p$ for some p, but this contradicts the definition of r_{p+1}. We have (ii).

(iii) comes from the fact that $\{\alpha \in \mathbb{T}_n \text{ such that } \tilde{m}(\alpha) = r_p\} = S_{r_p} \backslash S_{r_{p+1}}$, so that it is finite and has its lifts in $\mathbb{Q}^n$, by the general property of the S_k previously seen. Moreover, for all p, r_p is obviously rational. □

Corollary 4. *Under the same hypotheses, $M(\overline{K}) = M(K)$ is attained.*
If we put $M_1(K) = M(K)$ and $M_1(\overline{K}) = M(\overline{K})$, we have:

$$\forall p \geq 1,\ M_p(K) = M_p(\overline{K}) \in \mathbb{Q} \text{ and } M_{p+1}(\overline{K}) < M_p(\overline{K}).$$

In particular, $M(\overline{K})$ is isolated. Moreover $\lim_{p \to +\infty} M_p(\overline{K}) = 0.$

Proof. We know that the set of $\alpha \in \mathbb{T}_n$ such that $\tilde{m}(\alpha) = M(\overline{K})$ is finite and lifts in $\mathbb{Q}^n$, so that Proposition 1.ii) gives the first result. The rest is a direct consequence of Theorem 5, since by the definitions it is clear that in fact $M_p(K) = M_p(\overline{K}) = r_p$. □

Remark 3. It can be interesting to see that things cannot happen in the same way when K is a CM-field, even if $r > 1$. Suppose that K is a totally complex quadratic extension of a totally real field K^+, of degree n. Denote the n embeddings of K in $\mathbb{C}$ by σ_i (with $\sigma_{i+n/2} = \overline{\sigma_i}$) and the $n/2$ embeddings of K^+ by τ_i. We know that the complex conjugation τ induces an automorphism of K and commutes with each σ_i, that $[K : K^+]$ is Galois and that $\mathrm{Gal}(K/K^+) = \{\mathrm{id}, \tau\}$. Let $z \in K$ and $Z \in \mathbb{Z}_K$. Then $\mathrm{Tr}_{K/K^+}(z) = z + \overline{z} \in K^+$ and $Z + \overline{Z} \in \mathbb{Z}_{K^+}$, and we have

$$N_{K/\mathbb{Q}}(z - Z) = \prod_{i=1}^{n/2} \sigma_i(z - Z)\overline{\sigma_i(z - Z)}.$$

But for $u \in \mathbb{C}$ we have

$$u\overline{u} \geq \frac{1}{4}(u + \overline{u})^2,$$

so that we obtain

$$\begin{aligned}
\Big|N_{K/\mathbb{Q}}(z-Z)\Big| &\geq \frac{1}{4^{n/2}}\prod_{i=1}^{n/2}\Big(\sigma_i(z-Z)+\overline{\sigma_i(z-Z)}\Big)^2\\
&\geq \frac{1}{2^n}\prod_{i=1}^{n/2}\Big(\sigma_i(z+\overline{z})-\sigma_i(Z+\overline{Z})\Big)^2\\
&\geq \frac{1}{2^n}\inf_{Z'\in\mathbb{Z}_{K+}}\prod_{i=1}^{n/2}\Big(\sigma_i(z+\overline{z})-\sigma_i(Z')\Big)^2\\
&\geq \frac{1}{2^n}\left(\inf_{Z'\in\mathbb{Z}_{K+}}\prod_{i=1}^{n/2}\Big|\tau_i(z+\overline{z})-\tau_i(Z')\Big|\right)^2\\
&\geq \frac{1}{2^n}\left(\inf_{Z'\in\mathbb{Z}_{K+}}\Big|N_{K+/\mathbb{Q}}\Big((z+\overline{z})-Z'\Big)\Big|\right)^2\\
&\geq \frac{1}{2^n}\Big(m_{K+}(z+\overline{z})\Big)^2
\end{aligned}$$

This implies

$$m_K(z)\geq\frac{1}{2^n}\Big(m_{K+}(z+\overline{z})\Big)^2,$$

so that if $y\in K^+\backslash\mathbb{Z}_{K+}$, and if we put $\lambda=m_{K+}(y)>0$, then for every $z\in K$ such that $z+\overline{z}=y$, we have

$$m_K(z)\geq\frac{1}{2^n}\lambda^2>0.$$

But there are infinitely many such z in K modulo $\mathbb{Z}_K$, and, by upper semi-continuity, we find a non countable infinity of $x\in\mathbb{R}^n$ modulo $\mathbb{Z}^n$ such that

$$m(x)\geq\frac{1}{2^n}\lambda^2.$$

Thus, the situation is quite different than in Theorem 5. Moreover, under the hypothesis $r>1$, we have the equivalence

$$\forall k>0,\ S_k=\{\alpha\in\mathbb{T}_n;\ \tilde{m}(\alpha)\geq k\}\text{ is finite }\iff K\text{ is not a CM-field.}$$

5 Acknowledgements

I thank Guillaume Hanrot for his constant support and his many advices. I am also grateful to Hendrik Lenstra for having pointed out to me the impact of my results on the decidability problem of section 4.3 and for his encouragements. Likewise, I thank Christine Bachoc, Eva Bayer, Harvey Cohn and Franz Lemmermeyer for their interest. I also thank the anonymous referee for his remarks and suggestions which have enabled me to improve the presentation of this article.

References

[1] *E.S. Barnes and H.P.F Swinnerton-Dyer,* The inhomogeneous minima of binary quadratic forms I, Acta Mathematica 87 (1952), 259-323, The inhomogeneous minima of binary quadratic forms II, Acta Mathematica 88 (1952), 279-316.

[2] *D. Berend,* Multi-invariant sets on tori. Transactions of the American Mathematical Society 280, Number 2 (1983), 509-532.

[3] *D. Berend,* Minimal sets on tori. Ergodic Theory and Dynamical Systems 4 (1984), 499-507.

[4] *J.R. Brown,* Ergodic Theory and Topological Dynamics, Academic Press, Pure and Applied Mathematics (1976).

[5] *J.W.S. Cassels,* Introduction to the Geometry of Numbers, Springer-Verlag, Classics in Mathematics (1971).

[6] *S. Cavallar and F. Lemmermeyer,* Euclidean algorithm in cubic number fields, Győry, Pethő, Sos eds., Proceedings Number Theory Eger 1996, de Gruyter (1998), 123-146.

[7] *S. Cavallar and F. Lemmermeyer,* Euclidean Windows, LMS Journal of Computation and Mathematics 3 (2000), 335-355.

[8] *J-P. Cerri,* Euclidean minima of totally real number fields. Algorithmic determination (Submitted).

[9] *H. Furstenberg,* Recurrence in Ergodic Theory and Combinatorial Number Theory, Princeton University Press, Princeton, New Jersey (1981).

[10] *H.J. Godwin,* On the inhomogeneous minima of certain norm-forms, J. London Math. Soc. 30 (1955), 114-119.

[11] *F. Lemmermeyer,* The Euclidean algorithm in algebraic number fields, Expositiones Mathematicae (1995), 385-416.

[12] *H.W. Lenstra Jr.,* Euclidean Number Fields, The Mathematical Intelligencer, Springer-Verlag (1980).

Jean-Paul Cerri
2, route de Saint-Dié 88600 Aydoilles France
e-mail: Jean-Paul.CERRI@wanadoo.fr