JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Eva BAYER-FLUCKIGER et Piotr MACIAK

Upper bounds for the Euclidean minima of abelian fields

Upper bounds for the Euclidean minima of abelian fields

par Eva BAYER-FLUCKIGER et Piotr MACIAK

Résumé. Le but de cet article est de donner des bornes supérieures pour les minima euclidiens de corps abéliens, en particulier dans le cas des corps abéliens de conducteurs des puissances de nombres premiers.

Abstract. The aim of this paper is to survey and extend recent results concerning bounds for the Euclidean minima of algebraic number fields. In particular, we give upper bounds for the Euclidean minima of abelian fields of prime power conductor.

1. Introduction

Let K be an algebraic number field, and let $\mathcal{O}_K$ be its ring of integers. We denote by $\mathrm{N} : K \to \mathbb{Q}$ the absolute value of the norm map. The number field K is said to be *Euclidean* (with respect to the norm) if for every $a, b \in \mathcal{O}_K$ with $b \neq 0$ there exist $c, d \in \mathcal{O}_K$ such that $a = bc + d$ and $\mathrm{N}(d) < \mathrm{N}(b)$. It is easy to check that K is Euclidean if and only if for every $x \in K$ there exists $c \in \mathcal{O}_K$ such that $\mathrm{N}(x - c) < 1$. This suggests to look at

$$M(K) = \sup_{x \in K} \inf_{c \in \mathcal{O}_K} \mathrm{N}(x - c),$$

called the *Euclidean minimum* of K.

The study of Euclidean number fields and Euclidean minima is a classical one. However, little is known about the precise value of $M(K)$ (see for instance [11] for a survey, and the tables of Cerri [7] for some numerical results). Hence, it is natural to look for *upper bounds* for $M(K)$. This is also a classical topic, for which a survey can be found in [11].

Let n be the degree of K and D_K the absolute value of its discriminant. It is shown in [3] that for any number field K, we have $M(K) \leq 2^{-n} D_K$. The case of *totally real* fields is especially interesting, and has been the subject matter of several papers. In particular, a conjecture attributed to Minkowski states that if K is totally real, then $M(K) \leq 2^{-n}\sqrt{D_K}$. This conjecture is proved for $n \leq 8$, cf. [13], [9], [10].

Several recent results concern the case of *abelian fields*. In [4], upper bounds are given for abelian fields of conductor p^r, where p is an odd prime. The present paper complements these results by handling the case of abelian fields of conductor a power of 2. In particular, we have

Theorem. *If K is totally real of conductor p^r, where p is a prime and $r \geq 2$, then*

$$M(K) \leq 2^{-n}\sqrt{D_K}.$$

In other words, Minkowski's conjecture holds for such fields.

These results are based on the study of lattices associated to number fields (see [1], [2]). In §2, we recall some results on lattices and number fields, and in §3 we survey the results of [4] concerning abelian fields of conductor an odd prime power. The case of abelian fields of power of 2 conductor is the subject matter of §4. Finally, we survey some results concerning cyclotomic fields and their maximal totally real subfields in §5.

2. Lattices and number fields

We start by recalling some standard notions concerning Euclidean lattices (see for instance [8] and [12]). A *lattice* is a pair (L, q), where L is a free $\mathbb{Z}$–module of finite rank, and $q : L_{\mathbb{R}} \times L_{\mathbb{R}} \to \mathbb{R}$ is a positive definite symmetric bilinear form, where $L_{\mathbb{R}} = L \otimes_{\mathbb{Z}} \mathbb{R}$. If (L, q) is a lattice and $a \in \mathbb{R}$, then we denote by $a(L, q)$ the lattice (L, aq). Two lattices (L, q) and (L', q') are said to be *similar* if and only if there exists $a \in \mathbb{R}$ such that (L', q') and $a(L, q)$ are isomorphic, in other words if there exists an isomorphism of $\mathbb{Z}$-modules $f : L \to L'$ such that $q'(f(x), f(y)) = aq(x, y)$.

Let (L, q) be a lattice, and set $q(x) = q(x, x)$. The *maximum* of (L, q) is defined by

$$\max(L, q) = \sup_{x \in L_{\mathbb{R}}} \inf_{c \in L} q(x - c).$$

Note that $\max(L, q)$ 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 $\mathbb{Z}$–basis of L. The *Hermite–like thickness* of (L, q) is

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

where m is the rank of L. Note that $\tau(L, q)$ only depends on the similarity class of the lattice (L, q).

Next we introduce a family of lattices that naturally occur in connection with abelian fields, and for which one has good upper bounds of the Hermite-like thickness. This family is defined as follows:

Let $m \in \mathbb{N}$, and $b \in \mathbb{R}$ with $b > m$. Let $L = L_{b,m}$ be a lattice in $\mathbb{R}^m$ with Gram matrix

$$bI_m - J_m = \begin{pmatrix} b-1 & -1 & \cdots & & -1 \\ -1 & \ddots & \ddots & & \vdots \\ \vdots & \ddots & \ddots & & -1 \\ -1 & \cdots & -1 & & b-1 \end{pmatrix},$$

where I_m is the $m \times m$-identity matrix and J_m is the all-ones matrix of size $m \times m$. These lattices were defined in [5], §4.1. Note that the lattice $L_{m+1,m}$ is similar to the dual lattice $A_m^{\#}$ of the root lattice A_m (see for instance [8], Chapter 4, §6, or [12] for the definition of the root lattice A_m).

Let K be an number field of degree n, and suppose that K is either totally real or totally complex. Let us denote by $^-: K \to K$ the identity in the first case and the complex conjugation in the second one, and let P be the set of totally positive elements of the fixed field of this involution. Let us denote by $\mathrm{Tr} : K \to \mathbb{Q}$ the trace map. For any $\alpha \in P$, set $q_\alpha(x,y) = \mathrm{Tr}(\alpha x \overline{y})$ for all $x, y \in K$. Then $(\mathcal{O}_K, q_\alpha)$ is a lattice. Set

$$\tau_{\min}(\mathcal{O}_K) = \inf\{\tau(\mathcal{O}_K, q_\alpha) \mid \alpha \in P\}.$$

If D_K is the absolute value of the discriminant of K, then, by [3], Corollary 5.2, we have

(2.1) $$M(K) \leq \left(\frac{\tau_{\min}(\mathcal{O}_K)}{n}\right)^{\frac{n}{2}} \sqrt{D_K},$$

This is used in [3], [5], [6] and [4] to give upper bounds of Euclidean minima (see also §3 and §5). The bounds of §4 are also based on this result.

3. Abelian fields of odd prime power conductor

The set of all abelian extensions of $\mathbb{Q}$ of odd prime power conductor will be denoted by $\mathcal{A}$. For $K \in \mathcal{A}$ we denote by n the degree of $K/\mathbb{Q}$, by D the absolute value of the discriminant of K, by p the unique prime dividing the conductor of K, and by r the p-adic additive valuation of the conductor of K. If the dependence on the field K needs to be emphasized, we shall add the index K to the above symbols. For example, we shall write n_K instead of n.

Definition. Let $\mathcal{D} \subset \mathcal{A}$, and let $\psi : \mathcal{D} \to \mathbb{R}$ be a function. We shall say that $\psi_o \in \mathbb{R}$ is the limit of ψ as n_K goes to infinity and write

$$\lim_{n_K \to \infty} \psi(K) = \psi_0$$

if for every $\epsilon > 0$ there exists $N > 0$ such that for every field $K \in \mathcal{D}$

$$n_K > N \implies |\psi(K) - \psi_0| < \epsilon.$$

We shall also write

$$\lim_{p_K \to \infty} \psi(K) = \psi_0$$

if for every $\epsilon > 0$ there exists $N > 0$ such that for every field $K \in \mathcal{D}$

$$p_K > N \implies |\psi(K) - \psi_0| < \epsilon.$$

The following is proved in [4], theorems 3.1 and 3.2:

Theorem 3.1. *Let $K \in \mathcal{A}$. Then there exist constants $\varepsilon = \varepsilon(K) \leq 2$ and $C = C(K) \leq \frac{1}{3}$ such that*

$$M(K) \leq C^n (\sqrt{D_K})^{\varepsilon}.$$

If $[K : \mathbb{Q}] > 2$, then one may choose $\varepsilon(K) < 2$. Moreover,

$$\lim_{n_K \to \infty} \varepsilon(K) = 1.$$

If $r_K \geq 2$, or $r_K = 1$ and $[\mathbb{Q}(\zeta) : K]$ is constant, then we also have

$$\lim_{p_K \to \infty} C(K) = \frac{1}{2\sqrt{3}}.$$

Theorem 3.2. *Let $K \in \mathcal{A}$. Then there is a constant $\omega = \omega(K)$ such that*

$$M(K) \leq \omega^n \sqrt{D_K}.$$

If $r_K \geq 2$, or $r_K = 1$ and $[\mathbb{Q}(\zeta) : K]$ is constant, then

$$\lim_{p_K \to \infty} \omega(K) = \frac{1}{2\sqrt{3}}.$$

Moreover, if $r_K \geq 2$, then $\omega(K) \leq 3^{-2/3}$.

Note that this implies that Minkowski's conjecture holds for all totally real fields $K \in \mathcal{A}$ with composite conductor:

Corollary 3.3. *Let $K \in \mathcal{A}$, and suppose that the conductor of K is of the form p^r with $r > 1$. Then*

$$M(K) \leq 2^{-n} \sqrt{D_K}.$$

This follows from Theorem 3.2, since $3^{-2/3} < 1/2$, and for K totally real this is precisely Minkowski's conjecture.

The proofs of these results are based on the method of [3], outlined in the previous section. For $K \in \mathcal{A}$, we denote by $\mathcal{O}_K$ the ring of integers of K, and we consider the lattice $(\mathcal{O}_K, q)$, where q is defined by $q(x, y) = \mathrm{Tr}_{K/\mathbb{Q}}(x\overline{y})$. As we have seen in §2, the Hermite–like thickness of this lattice can be used to give an upper bound on the Euclidean minimum of K.

Let ζ be a primitive root of unity of order p^r, let us denote by e the degree $[\mathbb{Q}(\zeta) : K]$. Let Γ_K be the orthogonal sum of $\frac{p^{r-1}-1}{e}$ copies of the lattice

$p^{r-1}A_{p-1}^{\#}$. Set $d = \frac{p-1}{e}$, and let $\Lambda_K = ep^{r-1}L_{\frac{p}{e},d}$ (note that the scaling is taken in the sense of the previous section, that is it refers to multiplying the quadratic form by the scaling factor). We have (see [4], Theorem 6.1):

Theorem 3.4. *The lattice $(\mathcal{O}_K, q)$ is isometric to the orthogonal sum of Γ_K and of Λ_K.*

This leads to the following upper bound on $\tau_{\min}(\mathcal{O}_K)$:

Corollary 3.5. *We have*

$$\tau_{\min}(\mathcal{O}_K) \le \tau(\mathcal{O}_K, q) \le n \cdot p^{r - \frac{v}{n}} \cdot \frac{p^{r+1} + p^r + 1 - e^2}{12p^{r+1}},$$

where

$$v = rn - \frac{(p^{r-1} - 1)}{e} - 1.$$

This is proved in [4], Corollary 6.7. The proof uses an upper bound for the Hermite–like thickness of the lattices $\Lambda_{b,m}$ proved in [5], §4.1.

Using this corollary and (2.1), one proves (3.2) and (3.3) as in [4], §7.

4. Abelian fields of power of two conductor

We keep the notation of §§1 and 2. In particular, K is a number field of degree $n = n_K$, and the absolute value of its disciriminant is denoted by $D = D_K$. Let $r \in \mathbb{N}$, and let ζ be a primitive 2^r-th root of unity. A field K is said to have *conductor 2^r* if K is contained in the cyclotomic field $\mathbb{Q}(\zeta)$, but not in $\mathbb{Q}(\zeta^2)$. Note that there is no field of conductor 2 and the only field of conductor 4 is $\mathbb{Q}(i)$. For $r \ge 3$, we have:

Proposition 4.1. *Suppose that K is an abelian field of conductor 2^r, where $r \ge 3$. Then we have*

$$K = \mathbb{Q}(\zeta), \mathbb{Q}(\zeta + \zeta^{-1}), \text{ or } \mathbb{Q}(\zeta - \zeta^{-1}).$$

Moreover,

(a) *If $K = \mathbb{Q}(\zeta)$ or $\mathbb{Q}(\zeta + \zeta^{-1})$, then*

$$M(K) \le 2^{-n}\sqrt{D_K}.$$

(b) *If $K = \mathbb{Q}(\zeta - \zeta^{-1})$, then*

$$M(K) \le 2^{-n}(2n - 1)^{\frac{n}{2}}.$$

Proof. Let us first prove that $K = \mathbb{Q}(\zeta)$, $\mathbb{Q}(\zeta + \zeta^{-1})$ or $\mathbb{Q}(\zeta - \zeta^{-1})$. Let $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. Then $G = \langle \sigma, \tau \rangle$ where τ is the complex conjugation, and $\sigma(\zeta) = \zeta^3$. The subgroups of order 2 of G are

$$H_1 = \langle \tau \rangle, H_2 = \left\langle \sigma^{2^{r-3}} \right\rangle, \text{ and } H_3 = \left\langle \sigma^{2^{r-3}}\tau \right\rangle.$$

It is easy to check that we have $\mathbb{Q}(\zeta)^{H_1} = \mathbb{Q}(\zeta + \zeta^{-1})$, $\mathbb{Q}(\zeta)^{H_2} = \mathbb{Q}(\zeta^2)$ and $\mathbb{Q}(\zeta)^{H_3} = \mathbb{Q}(\zeta - \zeta^{-1})$. Note that any proper subfield of $\mathbb{Q}(\zeta)$ is a subfield of $\mathbb{Q}(\zeta)^{H_i}$ for $i = 1, 2$ or 3, and the statement easily follows from this observation.

Part (a) follows from Proposition 10.1 in [3] for $K = \mathbb{Q}(\zeta)$, and from Corollary 4.3 in [5] for $K = \mathbb{Q}(\zeta + \zeta^{-1})$.

Let us prove (b). Suppose that $K = \mathbb{Q}(\zeta - \zeta^{-1})$. Recall that $\mathbb{Q}(\zeta)^{H_3} = \mathbb{Q}(\zeta - \zeta^{-1})$, and that the ring of integers of $\mathbb{Q}(\zeta)$ is $\mathbb{Z}[\zeta]$. Therefore the ring of integers of $\mathbb{Q}(\zeta - \zeta^{-1})$ is $\mathbb{Z}[\zeta - \zeta^{-1}]$. Set $e_i = \zeta + (-1)^i \zeta^{-1}$ for all $i \in \mathbb{Z}$ and $n = 2^{r-2}$. Then an easy computation shows that the elements $1, e_1, \ldots, e_{n-1}$ form an integral basis of $\mathcal{O}_K = \mathbb{Z}[\zeta - \zeta^{-1}]$, and that for $-2n \leq i \leq 2n$ we have

$$\mathrm{Tr}_{K/\mathbb{Q}}(e_i) = \begin{cases} 2n & \text{if } i = 0, \\ -2n & \text{if } i = \pm 2n, \\ 0 & \text{otherwise.} \end{cases}$$

Recall that $\tau : K \to K$ is the complex conjugation, and let

$$q : \mathcal{O}_K \times \mathcal{O}_K \to \mathbb{Z}$$

given by

$$q(x, y) = \mathrm{Tr}_{K/\mathbb{Q}}(x\tau(y))$$

be the trace form. Then the Gram matrix of $(\mathcal{O}_K, q)$ with respect to the basis $1, e_1, \ldots, e_n$ is

$$\mathrm{diag}(n, 2n, \ldots, 2n).$$

Note that this implies that we have

$$D_K = n^n 2^{n-1}.$$

Since $1, e_1, \ldots, e_{n-1}$ is an orthogonal basis for $(\mathcal{O}_K, q)$, it follows from the Pythagorean theorem that the point $x = \frac{1}{2}(1 + e_1 + \cdots + e_{n-1})$ is a deep hole of the lattice $(\mathcal{O}_K, q)$. Thus we have

$$\max(\mathcal{O}_K, q) = \inf_{c \in \mathcal{O}_K} q(x - c) = q(x) = \frac{n(2n-1)}{4}.$$

Set

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

Then we have

$$\tau(\mathcal{O}_K, q) = \frac{n(2n-1)}{4(n^n 2^{n-1})^{1/n}} = \sqrt[n]{2} \cdot \left(\frac{2n-1}{8}\right).$$

By (2.1), we have

$$M(K) \leq \left(\frac{\tau(\mathcal{O}_K, q)}{n}\right)^{\frac{n}{2}} \sqrt{D_K}.$$

Thus we obtain

$$M(K) \leq 2^{-n}(2n-1)^{\frac{n}{2}}.$$

This completes the proof of the proposition. $\qquad\square$

Let $r \geq 3$ and let K be an abelian field of conductor 2^r of the form $\mathbb{Q}(\zeta - \zeta^{-1})$. The following two corollaries show an asymptotic behavior of the bound obtained in Proposition 4.1(b).

Corollary 4.2. *We have*

$$M(K) \leq 2^{-n}(\sqrt{D_K})^{1+\varepsilon(n)},$$

where

$$\varepsilon(n) \sim \frac{\ln 2 - \frac{1}{2}}{n \ln n}.$$

Proof. We set

$$\varepsilon(n) = \frac{\ln a_n + \ln 2}{n \ln(2n) - \ln 2},$$

where

$$a_n = \left(1 - \frac{1}{2n}\right)^n.$$

Using the fact that $D_K = n^n 2^{n-1}$, the inequality of Proposition 4.1(b) can rewritten as

$$M(K) \leq 2^{-n}(\sqrt{D_K})^{1+\varepsilon(n)}.$$

A simple calculation shows that

$$\lim_{n \to \infty}(n \ln n) \cdot \varepsilon(n) = \ln 2 - \frac{1}{2}.$$

The result follows. $\qquad\square$

Corollary 4.3. *We have*

$$M(K) \leq (\sqrt{2}\, e^{-1/4}) \cdot 2^{-n}\sqrt{D_K}.$$

Proof. Using the same notation as in the proof of Corollary 4.2, we can rewrite the inequality of Proposition 4.1(b) as

$$M(K) \leq (\sqrt{2a_n}) \cdot 2^{-n}\sqrt{D_K}.$$

The result follows from the fact that the sequence (a_n) is increasing and its limit equals to $e^{-1/2}$. $\qquad\square$

5. Cyclotomic fields and their maximal totally real subfields

Let $m \in \mathbb{N}$, and let ζ be a primitive m-th root of unity. Let $K = \mathbb{Q}(\zeta)$, and let $F = \mathbb{Q}(\zeta + \zeta^{-1})$ be its maximal totally real subfield. Let us denote by n_K, respectively n_F, their degrees, and by D_K, respectively D_F, the absolute values of their discriminants. The aim of this section is to survey some results concerning $M(K)$ and $M(F)$.

Theorem 5.1. *We have*

$$M(K) \leq 2^{-n_K} \sqrt{D_K}$$

Proof. This is proved in [3], Proposition 10.1. □

For certain values of m, one obtains better bounds:

Theorem 5.2. *We have*

(i) *Suppose that m is of the form $m = 2^r 3^s 5^t$, with $r \geq 0$, $s \geq 1$ and $t \geq 1$; $m = 2^r 5^s$ with $r \geq 2$, $s \geq 1$; $m = 2^r 3^s$ with $r \geq 3$, $s \geq 1$. Then*

$$M(K) \leq 8^{-n_K/2} \sqrt{D_K}.$$

(ii) *Suppose that m is of the form $m = 2^r 5^s 7^t$, with $r \geq 0$, $s \geq 1, t \geq 1$; $m = 2^r 3^s 5^t$ with $r \geq 0, s \geq 2, t \geq 1$; $m = 2^r 3^s 7^t$ with $r \geq 2, s \geq 1, t \geq 1$. Then*

$$M(K) \leq 12^{-n_K/2} \sqrt{D_K}.$$

Proof. This is proved in [3], Proposition 10.2. The result follows from (2.1), and the fact that an orthogonal sum of lattices of type E_8 is defined over K in the sense of §2 in case (i), and an orthogonal sum of lattices isomorphic to the Leech lattice in case (ii). □

The results are less complete for the maximal totally real subfields. We have

Theorem 5.3. *Suppose that $m = p^r$ where p is a prime and $r \in \mathbb{N}$, or that $m = 4k$ with $k \in \mathbb{N}$ odd. Then we have*

$$M(F) \leq 2^{-n_F} \sqrt{D_F}$$

Proof. This is proved in [3], Proposition 8.4 for $m = p^r$ and p an odd prime; in [5], Corollary 4.3 for $m = 2^r$; and in [6], Proposition 4.5 for $m = 4k$. □

References

[1] E. Bayer-Fluckiger, "Lattices and number fields", in *Algebraic geometry: Hirzebruch 70 (Warsaw, 1998)*, Contemp. Math., vol. 241, Amer. Math. Soc., Providence, RI, 1999, p. 69-84.

[2] ———, "Ideal lattices", in *A panorama of number theory or the view from Baker's garden (Zürich, 1999)*, Cambridge Univ. Press, Cambridge, 2002, p. 168-184.

[3] ———, "Upper bounds for Euclidean minima of algebraic number fields", *J. Number Theory* **121** (2006), no. 2, p. 305-323.

[4] E. BAYER-FLUCKIGER & P. MACIAK, "Upper bounds for the Euclidean minima of abelian fields of odd prime power conductor", *Math. Ann.* **357** (2013), no. 3, p. 1071-1089.

[5] E. BAYER-FLUCKIGER & G. NEBE, "On the Euclidean minimum of some real number fields", *J. Théor. Nombres Bordeaux* **17** (2005), no. 2, p. 437-454.

[6] E. BAYER-FLUCKIGER & I. SUAREZ, "Ideal lattices over totally real number fields and Euclidean minima", *Arch. Math. (Basel)* **86** (2006), no. 3, p. 217-225.

[7] J.-P. CERRI, "Euclidean minima of totally real number fields: algorithmic determination", *Math. Comp.* **76** (2007), no. 259, p. 1547-1575 (electronic).

[8] J. H. CONWAY & N. J. A. SLOANE, *Sphere packings, lattices and groups*, third ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 290, Springer-Verlag, New York, 1999, With additional contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov, lxxiv+703 pages.

[9] R. J. HANS-GILL, M. RAKA & R. SEHMI, "On conjectures of Minkowski and Woods for $n = 7$", *J. Number Theory* **129** (2009), no. 5, p. 1011-1033.

[10] ———, "On conjectures of Minkowski and Woods for $n = 8$", *Acta Arith.* **147** (2011), no. 4, p. 337-385.

[11] F. LEMMERMEYER, "The Euclidean algorithm in algebraic number fields", *Exposition. Math.* **13** (1995), no. 5, p. 385-416.

[12] J. MARTINET, *Les réseaux parfaits des espaces euclidiens*, Mathématiques. [Mathematics], Masson, Paris, 1996, iv+439 pages.

[13] C. T. MCMULLEN, "Minkowski's conjecture, well-rounded lattices and topological dimension", *J. Amer. Math. Soc.* **18** (2005), no. 3, p. 711-734 (electronic).

Eva BAYER-FLUCKIGER
École polytechnique fédérale de Lausanne
EPFL–FSB–MATHGEOM–CSAG
1015 Lausanne
Switzerland SWITZERLAND
E-mail: `eva.bayer@epfl.ch`

Piotr MACIAK
University of Copenhagen
Dpt of Mathematical Sciences
Universitetsparken 5
2100 Copenhagen
DENMARK
E-mail: `maciak@math.ku.dk`