Arch. Math. 86 (2006) 217–225
0003–889X/06/030217–09
DOI 10.1007/s00013-005-1469-9


**Archiv der Mathematik**

# Ideal lattices over totally real number fields and Euclidean minima

By

EVA BAYER-FLUCKIGER and IVAN SUAREZ

**Introduction.** Euclidean lattices defined over algebraic number fields have been studied in several papers, and from different points of view. On one hand, it is often possible to construct interesting lattices in this way (see [1], [2], [3], [4], [7], [12]); on the other hand, the geometric properties of the lattices yield arithmetic information about the number field (cf. [6]). As in [5], we call these lattices *ideal lattices* (see §1 for the precise definition). They correspond bijectively with Arakelov divisors over the number field (see [13]).

Most of the existing constructions of ideal lattices concern CM–fields, especially cyclotomic fields. One of the objectives of the present paper is to give constructions over totally real number fields as well.

Let $K$ be an algebraic number field, and let $\mathcal{O}_K$ be its ring of integers. Let $\sigma : K \to K$ be a $\mathbb{Q}$–linear involution, let $F$ be the fixed field of this involution, and let us denote by $\mathcal{O}_F$ the ring of integers of $F$. In §2, we define a number field $K'$, a quadratic extension of $F$, with the property that some ideal lattices over $\mathcal{O}_K$ are also ideal lattices over $\mathcal{O}_{K'}$. Using this method, we obtain well-known lattices, such as root lattices, the Coxeter-Todd lattice, the Leech lattice, as ideal lattices over totally real fields, in particular maximal totally real subfields of cyclotomic fields (see §3).

The second part of the paper is concerned with upper bounds of Euclidean minima. Recall that for any number field $L$, one defines the Euclidean minimum $M(L)$ of $L$ as

$$M(L) = \sup_{x \in L} \inf_{c \in \mathcal{O}_L} |\mathbb{N}_{L/\mathbb{Q}}(x - c)|.$$

---

*Mathematics Subject Classification* (2000): 11E12, 11H06, 11R80.

The authors gratefully acknowledge support from the Swiss National Science Foundation, grant No 200021-101918/1.

Let $d_L$ be the absolute value of the discriminant of $L$ and $n = [L : \mathbb{Q}]$. For totally real number fields $L$, a conjecture attributed to Minkowski states that

$$M(L) \leqq 2^{-n}\sqrt{d_L}$$

(see for instance [9, §3]). This conjecture has been proved for $n \leqq 6$ (cf [10]). The conjecture also holds for the maximal totally real subfields of cyclotomic fields of prime power conductor (see [6], [8]). The results of §2 combined with some results of [6] give the following proposition.

**Proposition.** *Let $m > 1$ be an odd integer. Then Minkowski's conjecture holds for the maximal totally real subfield of the $4m$-th cyclotomic field.*

## 1. Definitions and notation.

**1.1. Lattices.** A *lattice* is a pair $(L, b)$, where $L$ is a free $\mathbb{Z}$-module of finite rank and $b : L \times L \to \mathbb{R}$ a positive definite symmetric bilinear form.

Let $(L, b)$ be a lattice of rank $n$, set $q(x) = b(x, x)$ and set $L_{\mathbb{R}} = L \otimes_{\mathbb{Z}} \mathbb{R}$. Define the *minimum* (resp. the *maximum*) of $(L, b)$ as

$$\begin{aligned}\min(L, b) &= \inf\{q(x) : x \in L, x \neq 0\},\\ \max(L, b) &= \inf\{\lambda \in \mathbb{R} \ : \ \text{for all } x \in L_{\mathbb{R}}, \text{ there exists}\\ &\qquad y \in L \text{ with } q(x - y) \leqq \lambda\}.\end{aligned}$$

Let $\det(L, b)$ be the determinant of $(L, b)$. The *Hermite invariants* of $(L, b)$ are

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

and

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

The invariant $\gamma$ is related to the sphere packing density of a lattice $(L, b)$, and the invariant $\tau$ is related to its thickness. The invariants $\gamma$ and $\tau$ only depend on the isometry class of a lattice.

**1.2. Euclidean minima.** Let $K$ be a number field, and let $\mathcal{O}_K$ be its ring of integers.

Definition 1.1 (see [9, §3]). The *Euclidean minimum* of the field $K$ is

$$M(K) = \sup_{x \in K} \inf_{c \in \mathcal{O}_K} |\mathbb{N}_{K/\mathbb{Q}}(x - c)|.$$

If $K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$, we can define in a similar way

$$M(K_{\mathbb{R}}) = \sup_{x \in K_{\mathbb{R}}} \inf_{c \in \mathcal{O}_K} |\mathbb{N}_{K_{\mathbb{R}}/\mathbb{R}}(x - c)|.$$

Clearly, we have $M(K_{\mathbb{R}}) \geqq M(K)$.

**1.3. Ideal lattices.** Let $K$ be a CM-field or a totally real field of degree $n$ over $\mathbb{Q}$. Let $\sigma$ be the complex conjugation if $K$ is a CM-field, and the identity if $K$ is a totally real field. The ring of integers of $K$ is denoted $\mathcal{O}_K$ and $d_K$ denotes the absolute value of the discriminant of $K$.

An *ideal lattice* over $K$ is a pair $(\mathcal{I}, b)$, where $\mathcal{I}$ is a (fractional) ideal of $K$ and

$$b : \mathcal{I} \times \mathcal{I} \to \mathbb{R}$$

is a positive definite symmetric bilinear form satisfying the invariance relation $b(\lambda x, y) = b(x, \lambda^\sigma y)$ for all $x, y \in \mathcal{I}$, and for all $\lambda \in \mathcal{O}_K$. For each ideal lattice $(\mathcal{I}, b)$, there exists a totally positive element $\alpha \in K_{\mathbb{R}} = K \otimes_{\mathbb{Q}} \mathbb{R}$ such that $b(x, y) = Tr_{K_{\mathbb{R}}/\mathbb{R}}(\alpha x y^\sigma)$ (cf [5, Proposition 1]).

Let $\mathcal{P}$ be the subset of totally positive elements of $K_{\mathbb{R}}$. For $\alpha \in \mathcal{P}$, the ideal lattice $(\mathcal{I}, b_\alpha)$, with $b_\alpha(x, y) = Tr(\alpha x y^\sigma)$ is denoted $(\mathcal{I}, \alpha)$.

For an ideal $\mathcal{I}$ of $K$, define

$$\gamma_{\min}(\mathcal{I}) = \inf\{\gamma(\mathcal{I}, \alpha) : \alpha \in \mathcal{P}\}, \text{ and}$$

$$\tau_{\min}(\mathcal{I}) = \inf\{\tau(\mathcal{I}, \alpha) : \alpha \in \mathcal{P}\}.$$

These definitions only depend on the class of $\mathcal{I}$ in the ideal class group of $K$. Indeed, if $\mathcal{J} = \beta\mathcal{I}$, then the ideal lattices $(\mathcal{I}, \alpha)$ and $(\mathcal{J}, \beta^{-1-\sigma}\alpha)$ are isomorphic.

These invariants are related to the Euclidean minimum of the field $K$ thanks to Theorem 5.1 of [6]:

**Theorem 1.2.** *We have*

$$M(K_{\mathbb{R}}) \leqq \left(\frac{\tau_{\min}(\mathcal{O}_K)}{\gamma_{\min}(\mathcal{O}_K)}\right)^{\frac{n}{2}}.$$

Notice that $\gamma_{\min}(\mathcal{O}_K) = n d_K^{-\frac{1}{n}}$ (cf. [6, Lemma 4.3]), so in order to get an upper bound to the Euclidean minimum of the number field $K$, it only remains to construct an ideal lattice over $\mathcal{O}_K$ having a good invariant $\tau$. The following corollary will be helpful in the sequel (cf. [6, Corollary 5.3]).

**Corollary 1.3.** *If $\tau_{\min}(\mathcal{O}_K) \leqq \frac{n}{4}$, then $M(K_{\mathbb{R}}) \leqq 2^{-n}\sqrt{d_K}$.*

**2. A construction.** Let $F$ be a field of characteristic not 2. Let $K$ be a quadratic extension of $F$, and let $\vartheta \in F$ be such that $K = F(\sqrt{\vartheta})$. Assume that $-1 \notin K^{\times 2}$, and let $K' = F(\sqrt{-\vartheta})$. The field $K'$ is then a quadratic extension of $F$ different from $K$. Set $L = KK'$, and let $\sigma$ (resp. $\sigma'$) be a generator of $\mathrm{Gal}(K/F)$ (resp. of $\mathrm{Gal}(K'/F)$).

Define $\varphi : K \to K'$ to be an $F$-linear map such that $\varphi(1) = 1$ and $\varphi(\sqrt{\vartheta}) = \sqrt{-\vartheta}$. Notice that for all $x, y \in K$ we have:

$$Tr_{K/F}(xy^{\sigma}) = Tr_{K'/F}(\varphi(x)\varphi(y)). \tag{1}$$

We have the following formulas, which can be obtained by straightforward computation.

- $\mathbb{N}_{K'/F}(\varphi(x)) = -\mathbb{N}_{K/F}(x) + \frac{Tr_{K/F}(x)^2}{2} = \frac{Tr_{K/F}(x^2)}{2}$,
- $\mathbb{N}_{K/F}(\varphi^{-1}(x)) = -\mathbb{N}_{K'/F}(x) + \frac{Tr_{K'/F}(x)^2}{2} = \frac{Tr_{K'/F}(x^2)}{2}$,
- $\varphi(x^{\sigma}) = \varphi(x)^{\sigma'} \Rightarrow Tr_{K'/F}(\varphi(x)) = Tr_{K/F}(x)$,
- $\varphi^{-1}(\varphi(x)\varphi(y)) = xy - \frac{(x-x^{\sigma})(y-y^{\sigma})}{2}$,
- $\varphi(\varphi^{-1}(x)\varphi^{-1}(y)) = xy - \frac{(x-x^{\sigma'})(y-y^{\sigma'})}{2}$.

In the sequel, we assume that $F$ is a number field and that $K/\mathbb{Q}$ is not ramified at 2. We are now ready to investigate the nature of $\varphi(\mathcal{O}_K)$ and $\varphi^{-1}(\mathcal{O}_{K'})$.

**Proposition 2.1.** *If $K/\mathbb{Q}$ is not ramified at 2, then $\varphi(\mathcal{O}_K)$ is a fractional ideal of $\mathcal{O}_{K'}$. Moreover, the ideal $\mathfrak{b} = \varphi(\mathcal{O}_K)$ satisfies $\mathfrak{b}^2 = \frac{1}{2}\mathcal{O}_{K'}$.*

We will need the following lemma.

**Lemma 2.2.** *With the above assumptions, we have $\mathcal{D}_{L/K'} = \mathcal{O}_L$ and $\mathcal{D}_{K'/F} = 2\mathfrak{c}$, where $\mathfrak{c}$ is an integral ideal prime to 2.*

Proof. Let $K'' = F(\sqrt{-1})$. Then $\mathcal{D}_{K''/F} = 2\mathcal{O}_{K''}$.

Since all primes $\mathfrak{q}$ of $F$ dividing 2 are unramified in $K/F$, $K$ is the fixed field of their group of inertia. Any such $\mathfrak{q}$ is then ramified in $K'/F$ and all primes of $K'$ resp. $K''$ dividing 2 are unramified in $L/K'$ resp. $L/K''$.

Hence $2\mathcal{D}_{L/K''} = \mathcal{D}_{K''/F}\mathcal{D}_{L/K''} = \mathcal{D}_{L/F} = \mathcal{D}_{K'/F}\mathcal{D}_{L/K'}$ implies $\mathcal{D}_{K'/F} = 2\mathfrak{c}$ with $\mathfrak{c}$ as asserted. □

Proof of Proposition 2.1. Notice that since $K'/F$ is wildly ramified, we have $Tr_{K'/F}(\mathcal{O}_{K'}) \subseteqq 2\mathcal{O}_F$. Let's show first that $\varphi(\mathcal{O}_K) \supseteqq \mathcal{O}_{K'} \supseteqq 2\varphi(\mathcal{O}_K)$. Let $x \in \mathcal{O}_K$. Using the formulas, we see that $Tr_{K'/F}(2\varphi(x)) = Tr_{K/F}(2x) \in \mathcal{O}_F$ and $\mathbb{N}_{K'/F}(2\varphi(x)) = \frac{Tr_{K/F}(4x^2)}{2} \in \mathcal{O}_F$, so $\varphi(2x) \in \mathcal{O}_{K'}$. Conversely, if $y \in \mathcal{O}_{K'}$, then $\mathbb{N}_{K/F}\varphi^{-1}(y) = \frac{Tr_{K'/F}(y^2)}{2} \in \mathcal{O}_F$ (since $Tr(\mathcal{O}_{K'}) \subseteqq 2\mathcal{O}_F$), and $Tr_{K/F}(\varphi^{-1}y) = Tr_{K'/F}(y) \in \mathcal{O}_F$. Therefore $\varphi^{-1}y \in \mathcal{O}_K$.

Let's show now that $\varphi(\mathcal{O}_K)$ is an $\mathcal{O}_{K'}$-module. Take $x \in \mathcal{O}_K$ and $y \in \mathcal{O}_{K'}$. We want to show that $y\varphi(x) \in \varphi(\mathcal{O}_K)$. We have $\varphi^{-1}(y\varphi(x)) = x\varphi^{-1}y - (x - x^{\sigma})\varphi^{-1}(\frac{y-y^{\sigma'}}{2})$. Recall

that $\mathcal{O}_{K'} \subseteqq \varphi(\mathcal{O}_K)$, so $x\varphi^{-1}y \in \mathcal{O}_K$. Moreover, $y - y^{\sigma'} \in \mathcal{D}_{K'/F} \subseteqq 2\mathcal{O}_{K'}$. It follows that $\varphi^{-1}(y\varphi(x))$ belongs to $\mathcal{O}_K$.

Let $\mathfrak{b} = \varphi(\mathcal{O}_K)$ and let's show that $\mathfrak{b}^2 = \frac{1}{2}\mathcal{O}_{K'}$. Recall that for all $x, y \in \mathcal{O}_K$, we have $Tr_{K'/F}(\varphi x \varphi y) \in \mathcal{O}_F$. So $\mathfrak{b} \subseteqq \mathfrak{b}^{-1}\mathcal{D}_{K'/F}^{-1} = \frac{1}{2}\mathfrak{c}^{-1}\mathfrak{b}^{-1}$, where $\mathfrak{c}$ is an integral ideal prime to 2 (see Lemma 2.2). Hence $\mathfrak{b}^2 \subseteqq \frac{1}{2}\mathfrak{c}^{-1}$, which is possible only if $\mathfrak{b}^2 \subseteqq \frac{1}{2}\mathcal{O}_{K'}$ since $\mathcal{O}_{K'} \subseteqq \mathfrak{b} \subseteqq \frac{1}{2}\mathcal{O}_{K'}$ from the first part of the proof. Moreover, the extension $K/F$ is tamely ramified therefore there exists $\gamma \in \mathcal{O}_K$ such that $Tr_{K/F}\,\gamma = 1$. For such a $\gamma$, we have $Tr_{K'/F}(\varphi(\gamma)) = 1$. As the extension $K'/F$ is wildly ramified, this is only possible if for each prime ideal $\mathfrak{P}$ of $K'$ above 2, we have $\mathrm{val}_{\mathfrak{P}}(\varphi\gamma) \leqq -1$. Therefore, $\mathrm{val}_{\mathfrak{P}}(\mathfrak{b}) \leqq -1$ for all $\mathfrak{P}|2$. Given that $\mathfrak{b}^2 \subseteqq \frac{1}{2}\mathcal{O}_{K'}$, we obtain that $\mathfrak{b}^2 = \frac{1}{2}\mathcal{O}_{K'}$, and this achieves the proof.

**Proposition 2.3.** *If $\mathfrak{a}$ is a (fractional) ideal of $\mathcal{O}_K$ satisfying $\mathfrak{a}^\sigma = \mathfrak{a}$, then $\varphi(\mathfrak{a})$ is an $\mathcal{O}_{K'}$-ideal.*

*If $\mathfrak{a}$ is an ideal of $\mathcal{O}_K$ such that $\mathfrak{a}^\sigma \neq \mathfrak{a}$, then $\varphi(\mathfrak{a})$ is not an ideal of $\mathcal{O}_{K'}$.*

Proof. The proof of the first point is similar to the one which shows that $\varphi(\mathcal{O}_K)$ is an $\mathcal{O}_{K'}$-module. In fact, for $x \in \mathfrak{a}$ and $y \in \mathcal{O}_{K'}$, we have $\varphi^{-1}(y\varphi(x)) = x\varphi^{-1}y - (x - x^\sigma)\varphi^{-1}(\frac{y-y^{\sigma'}}{2})$. Moreover, both $x\varphi^{-1}y$ and $x - x^\sigma$ are in $\mathfrak{a}$, so the conclusion comes from the fact that $\varphi^{-1}(\frac{y-y^{\sigma'}}{2}) \in \mathcal{O}_K$.

Let $\mathfrak{a}$ be an ideal such that $\mathfrak{a}^\sigma \neq \mathfrak{a}$ and assume that $\varphi(\mathfrak{a})$ is an $\mathcal{O}_{K'}$-module. Notice that for all $x \in \mathfrak{a}$ and for all $y \in \mathcal{O}_{K'}$, we have $\varphi^{-1}(\varphi(x)y) = x\varphi^{-1}(y) - x\varphi^{-1}(\frac{y-y^{\sigma'}}{2}) - x^\sigma\varphi^{-1}(\frac{y-y^{\sigma'}}{2})$. Since $x\varphi^{-1}(y)$ and $x\varphi^{-1}(\frac{y-y^{\sigma'}}{2})$ are in $\mathfrak{a}$, $\varphi(\mathfrak{a})$ is an ideal if and only if for all $x \in \mathfrak{a}$ and for all $y \in \mathcal{O}_{K'}$, we have $x^\sigma\varphi^{-1}(\frac{y-y^{\sigma'}}{2}) \in \mathfrak{a}$. This is the case if and only if the ideal $\mathcal{I}$ of $K$ generated by $\varphi^{-1}(\frac{y-y^{\sigma'}}{2})$ for $y \in \mathcal{O}'_K$ satisfies $\mathcal{I} \subseteqq \mathfrak{a}^{1-\sigma}$. Given that $\mathcal{I}^\sigma = \mathcal{I}$, this is equivalent to asking that $\mathcal{I} \subseteqq \mathfrak{a}^{1-\sigma} \cap \mathfrak{a}^{\sigma-1}$. Let $\mathfrak{b} = \mathfrak{a}^{1-\sigma} \cap \mathfrak{a}^{\sigma-1}$. Notice first that $\mathfrak{b}$ is an integral ideal different from $\mathcal{O}_K$ since $\mathfrak{a} \neq \mathfrak{a}^\sigma$. Let $\mathfrak{P}$ be a prime ideal dividing $\mathfrak{b}$, and let $\mathfrak{p} = \mathfrak{P} \cap F$. The ideal $\mathcal{I}$ is generated by the elements $b\sqrt{\vartheta}$ such that $b^2\vartheta \in F$. By the strong approximation theorem, there exists $b \in F$ such that $\mathrm{val}_{\mathfrak{p}}(b) = -\lfloor \frac{\mathrm{val}_{\mathfrak{p}}(\vartheta)}{2} \rfloor$ and $\mathrm{val}_{\mathfrak{q}}(b) \geqq -\mathrm{val}_{\mathfrak{p}}(\vartheta)$ for all $\mathfrak{p} \neq \mathfrak{p}$. Take such $b$ and notice that $\mathrm{val}_{\mathfrak{p}}(b^2\vartheta) = 0$ or 1. But $b^2\vartheta \in \mathcal{I} \cap F \subseteqq \mathfrak{p}$, so $\mathrm{val}_{\mathfrak{p}}(b^2\vartheta) = 1$. This implies that $\mathfrak{p}$ ramifies in $K$ and contradicts the fact that $\mathfrak{P} \neq \mathfrak{P}^\sigma$. Hence $\varphi(\mathfrak{a})$ is not an ideal of $\mathcal{O}_{K'}$, and the proposition is proved. □

In order to be complete, the case of $\varphi^{-1}(\mathcal{O}_{K'})$ is handled in the next proposition.

**Proposition 2.4.** *$\varphi^{-1}(\mathcal{O}_{K'})$ is an order of $K$. Moreover, if $\mathfrak{b}$ is an ideal of $\mathcal{O}_{K'}$ satisfying $\mathfrak{b} = \mathfrak{b}^{\sigma'}$, then $\varphi^{-1}(\mathfrak{b})$ is a $\varphi^{-1}(\mathcal{O}_{K'})$ fractional ideal.*

Proof. If $x, y \in \mathcal{O}_{K'}$, then the formula $\varphi(\varphi^{-1}(x)\varphi^{-1}(y)) = xy - \frac{(x-x^{\sigma'})(y-y^{\sigma'})}{2}$ associated to the fact that $y \equiv y^{\sigma'} \mod 2\mathcal{O}_{K'}$ gives that $\varphi^{-1}(\mathcal{O}_{K'})$ is an order of $K$. Moreover, the same formula (with $x \in \mathfrak{b}$ and $y \in \mathcal{O}_{K'}$) shows that $\varphi^{-1}(\mathfrak{b})$ is a $\varphi^{-1}(\mathcal{O}_{K'})$-ideal. □

**3. Ideal lattices over totally real fields.** Let $K$ be a CM-field, let $F$ be the maximal totally real subfield of $K$, and let $K'$ be as in Section 2. We assume in this section that 2 does not ramify in $K$. Thanks to the map $\varphi$, and in particular thanks to the equality (1), we can sometimes shift ideal lattices from $K$ to $K'$. More precisely, we have the next proposition.

**Proposition 3.1.** *If $(\mathcal{I}, \alpha)$ is an ideal lattice over $K$ such that $\mathcal{I}$ is an ambiguous ideal, then $(\varphi(\mathcal{I}), \alpha)$ is an ideal lattice over $K'$ isomorphic to $(\mathcal{I}, \alpha)$.*

Actually, we have the following stronger result.

**Proposition 3.2.** *Let $(\mathcal{I}, \alpha)$ be an ideal lattice of $K$. If the ideal $\mathcal{I}$ is in the same ideal class as an ambiguous ideal, then there is an ideal lattice over $K'$ isomorphic (as a lattice) to $(\mathcal{I}, \alpha)$.*

Proof. If $\beta \in K$, then the lattices $(\mathcal{I}, \alpha)$ and $(\beta\mathcal{I}, \beta^{-1-\sigma}\alpha)$ are isomorphic, where $\sigma$ denotes the complex conjugation. □

We will now use this proposition to shift ideal lattices constructed over CM-fields on some totally real fields. In the sequel, $\zeta_m$ denotes a primitive $m$-th root of unity, and set $\eta_m = \zeta_m + \zeta_m^{-1}$.

The root lattice $\mathbb{A}_{p-1}$. For an odd prime $p$, this lattice is an ideal lattice over the field $\mathbb{Q}(\zeta_p)$ (see [3, §3]). If $\mathfrak{P}$ is the ideal generated by $1 - \zeta_p$, then the ideal lattice $(\mathfrak{P}, \frac{1}{p})$ is isomorphic to $\mathbb{A}_{p-1}$. Therefore, Proposition 3.2 asserts that the lattice $\mathbb{A}_{p-1}$ is an ideal lattice over the field $\mathbb{Q}(\eta_{4p})$. A direct construction can be obtained as follow. The ideal lattice $(\mathfrak{P}, \frac{1}{p})$ is isomorphic to the ideal lattice $(\mathbb{Z}[\zeta_p], (2 - \eta_p)p^{-1})$. Let $\mathfrak{a}$ be the ideal of $\mathbb{Q}(\eta_{4p})$ satisfying $\mathfrak{a}^{-2} = 2\mathbb{Z}[\eta_{4p}]$. This ideal is the principal ideal generated by $a = \frac{1}{2}\sum_{i=0}^{p}(-1)^i \binom{p}{i}(\zeta_{4p}^i + \zeta_{4p}^{-i})$. Proposition 2.1 implies that the ideal lattice $(\mathfrak{a}, (2 - \eta_p)p^{-1})$ is isomorphic to $\mathbb{A}_{p-1}$. Since $\mathfrak{a}$ is principal, the lattice $(\mathbb{Z}[\eta_{4p}], \alpha)$ is also isomorphic to $\mathbb{A}_{p-1}$, where $\alpha = a\overline{a}(2 - \eta_p)p^{-1}$.

The root lattice $\mathbb{E}_6$. An ideal lattice isomorphic to $\mathbb{E}_6$ can be found in $\mathbb{Q}(\zeta_9)$ (see [3, §3]). Since $\mathbb{Q}(\zeta_9)$ has class number 1, Proposition 3.2 implies that there exists an ideal lattice isomorphic to $\mathbb{E}_6$ in $\mathbb{Q}(\eta_{36})$. Actually, let $\mathfrak{P}_3$ be a prime ideal of $\mathbb{Q}(\zeta_9)$ above 3, let $\mathfrak{P}_2'$ be a prime ideal of $\mathbb{Q}(\eta_{36})$ above 2, and let $\mathfrak{P}_3'$ be a prime ideal of $\mathbb{Q}(\eta_{36})$ above 3. The ideal lattice $(\mathfrak{P}_3^{-4}, 1)$ is isomorphic to $\mathbb{E}_6$ (cf. [3, §3]). Moreover, the ideal $\mathfrak{P}_3^{-4}$ is the principal ideal generated by $(2 - \eta_9)^{-2}$. Therefore, $\varphi(\mathfrak{P}_3^{-4}) = \varphi((2 - \eta_9)^{-2}\mathbb{Z}[\zeta_9]) = (2 - \eta_9)^{-2}\varphi(\mathbb{Z}[\zeta_9]) = \mathfrak{P}_3'^{-4}\mathfrak{P}_2'^{-1}$. So, the ideal lattice $(\mathfrak{P}_2'^{-1}\mathfrak{P}_3'^{-4}, 1)$ over $\mathbb{Q}(\eta_{36})$ is isomorphic to $\mathbb{E}_6$.

The root lattice $\mathbb{E}_8$. The lattice $\mathbb{E}_8$ can be realised as an ideal lattice over $\mathbb{Q}(\zeta_{15})$ (see [3, §3]). Since $\mathbb{Q}(\zeta_{15})$ has class number 1, this lattice can also be realised over $\mathbb{Q}(\eta_{60})$.

Actually, let $\psi$ be the minimal polynomial of $\eta_{15}$ and set $\alpha = \frac{1}{\psi'(\eta_{15})}\eta_{15}(\zeta_{15}^7 + \zeta_{15}^{-7})$. Let $\mathfrak{P}_2'$ be a prime ideal of $\mathbb{Q}(\eta_{60})$ above 2. The element $\alpha$ is totally positive and the ideal lattice $(\mathbb{Z}[\zeta_{15}], \alpha)$ is isomorphic to $\mathbb{E}_8$ (cf. [3, §3]). Therefore, the ideal lattice $(\mathfrak{P}_2'^{-1}, \alpha)$ over $\mathbb{Q}(\eta_{60})$ is isomorphic to $\mathbb{E}_8$.

The Coxeter-Todd lattice $\mathbb{K}_{12}$. The Coxeter-Todd lattice can be realised as an ideal lattice over $\mathbb{Q}(\zeta_{21})$ (cf. [7, §4]). Actually, if $\mathfrak{P}_7$ is a prime ideal above 7, then the ideal lattice $(\mathfrak{P}_7^{-5}, 1)$ is isomorphic to the lattice $\mathbb{K}_{12}$. Let $\zeta = \zeta_{21}$ be a primitive 21-st root of unity. We can choose for $\mathfrak{P}_7$ the principal ideal generated by $\alpha = 1 + \zeta^7 - \zeta^8 + \zeta^9$. Therefore, the ideal lattice $(\mathcal{O}_K, (\alpha\overline{\alpha})^{-5})$ is isomorphic to $\mathbb{K}_{12}$. Let $K' = \mathbb{Q}(\eta_{84})$ and let $\mathfrak{P}_2'$ be a prime ideal of $\mathcal{O}_{K'}$ above 2. We can now use the results from Section 2 to see that the ideal lattice $(\mathfrak{P}_2', (\alpha\overline{\alpha})^{-5})$ over $\mathbb{Q}(\eta_{84})$ is isomorphic to the Coxeter-Todd lattice $\mathbb{K}_{12}$.

The Leech lattice $\Lambda_{24}$. The Leech lattice can be realised as an ideal lattice over the field $\mathbb{Q}(\zeta_{35})$. Let $\psi$ be the minimal polynomial of $\zeta_{35}+\zeta_{35}^{-1}$. Set $u = (\zeta_{35}^{-3}+\zeta_{35}^{3})(\zeta_{35}^{-6}+\zeta_{35}^{6})$ $(\zeta_{35}^{-9} + \zeta_{35}^{9})(\zeta_{35}^{-12} + \zeta_{35}^{12})$ and $\alpha = \frac{u}{\psi'(\zeta_{35}+\zeta_{35}^{-1})}$. Then $\alpha$ is a totally positive element and the ideal lattice $(\mathbb{Z}[\zeta_{35}], \alpha)$ is isomorphic to the Leech lattice (see [2, §5]). Therefore, if $\mathfrak{a}$ is the ideal of $\mathbb{Z}[\eta_{140}]$ such that $\mathfrak{a}^2 = \frac{1}{2}\mathbb{Z}[\eta_{140}]$, then Proposition 2.1 implies that the ideal lattice $(\mathfrak{a}, \alpha)$ over $\mathbb{Q}(\eta_{140})$ is isomorphic to the Leech lattice.

## 4. Upper bounds for Euclidean minima.

**4.1. General bounds.** Let $F$ be a totally real number field, and let $K$, $K'$ and $L$ be as in Section 2. Set $n = [K : \mathbb{Q}] = [K' : \mathbb{Q}]$. Assume that $K$ is a CM-field and assume also that $K/\mathbb{Q}$ does not ramify above 2. Then we have the following bounds for the Euclidean minima.

**Proposition 4.1.** *We have $M(K') \leqq 2^n M(K)$. Moreover, if $\varphi(\mathcal{O}_K)$ is a principal ideal of $K'$, then $M(K') \leqq 2^{\frac{n}{2}} M(K)$.*

**Lemma 4.2.** *Let $x \in K$. For all embeddings $F \hookrightarrow \mathbb{R}$, we have $|\mathbb{N}_{K/F}x| \geqq |\mathbb{N}_{K'/F}\varphi(x)|$.*

Proof. Recall that $\mathfrak{a} := \varphi(\mathcal{O}_K)$ is an ideal of $\mathcal{O}_{K'}$ satisfying $\mathfrak{a}^2 = \frac{1}{2}\mathcal{O}_{K'}$. Let $\alpha$ be a generator of $\mathfrak{a}$ if this one is principal, and let $\alpha = \frac{1}{2}$ otherwise. Let $x \in K'$ and set $y = \varphi^{-1}(\alpha x)$. Let a real $\varepsilon > 0$ be given. Choose $d \in \mathcal{O}_K$ such that $|\mathbb{N}_{K/\mathbb{Q}}(y-d)| < M(K)+\varepsilon$. Set $c = \varphi^{-1}d$. Thanks to the lemma, we have $|\mathbb{N}_{K'/\mathbb{Q}}(\alpha x - c)| \leqq |\mathbb{N}_{K/\mathbb{Q}}(y - d)| < M(K) + \varepsilon$. This can be rewritten as $|\mathbb{N}_{K'/\mathbb{Q}}(x - \alpha^{-1}c)| < |\mathbb{N}_{K'/\mathbb{Q}}\alpha^{-1}|(M(K) + \varepsilon)$. Since $\alpha^{-1}c \in \mathcal{O}_{K'}$, and since $|\mathbb{N}_{K'/\mathbb{Q}}\alpha^{-1}| = 2^n$ (resp. $2^{\frac{n}{2}}$) when $\mathfrak{a}$ is not principal (resp. when $\mathfrak{a}$ is principal), this concludes the proof. □

The $F$-linear map $\varphi$ can be extended to an $F_{\mathbb{R}}$-linear map $\tilde{\varphi} : K_{\mathbb{R}} \to K'_{\mathbb{R}}$. It is easily checked that the analogue of Lemma 4.2 for $x \in K_{\mathbb{R}}$ and for $\tilde{\varphi}$ remains true. Hence we get the following proposition.

**Proposition 4.3.** *We have* $M(K'_{\mathbb{R}}) \leqq 2^n M(K_{\mathbb{R}})$. *Moreover, if* $\varphi(\mathcal{O}_K)$ *is a principal ideal, then* $M(K'_{\mathbb{R}}) \leqq 2^{\frac{n}{2}} M(K_{\mathbb{R}})$.

**Proposition 4.4.** *We have* $M(L) \geqq M(K)^2$.

Proof. The ring of integers of $L$ is $\mathcal{O}_L = \mathcal{O}_K + \sqrt{-1}\mathcal{O}_K$, since $\mathcal{D}_{L/K} = 2\mathcal{O}_L$. Let $a + b\sqrt{-1} \in L$, with $a, b \in K$. A straightforward computation shows that $\mathbb{N}_{L/F}(a + b\sqrt{-1}) = \mathbb{N}_{K/F}(a - b)^2 + (Tr_{K/F}(ab^\sigma))^2$ for all $a, b \in K$. In particular, for each embedding $F \hookrightarrow \mathbb{R}$ we have $\mathbb{N}_{L/F}(a + b\sqrt{-1}) \geqq \mathbb{N}_{K/F}(a - b)^2$. By adding to $a$ and to $b$ elements of $\mathcal{O}_K$, we may assume that $\mathbb{N}_{L/\mathbb{Q}}(a + b\sqrt{-1}) \leqq M(L) + \varepsilon$. Therefore $\mathbb{N}_{K/F}(a - b)^2 \leqq M(L) + \varepsilon$ for each $\varepsilon > 0$, and this implies that $M(L) \geqq M(K)^2$. □

**4.2. Maximal totally real subfields of some cyclotomic fields.** Let $m > 1$ be an odd integer and let $n = \varphi(m)$. We keep the notation of the preceding section. In particular, $\zeta_m$ denotes a primitive $m$-th root of unity and $\eta_m = \zeta_m + \zeta_m^{-1}$. We will apply the results of Section 2 to get the upper bound $M(K') \leqq 2^{-n}\sqrt{d_{K'}}$ for the totally real field $K' = \mathbb{Q}(\eta_{4m})$.

Let $K = \mathbb{Q}(\zeta_m)$. The field $K'$ associated to $K$ by Section 2 is the field $K' = \mathbb{Q}(\eta_{4m})$.

**Proposition 4.5.** *We have* $M(K'_{\mathbb{R}}) \leqq 2^{-n}\sqrt{d_{K'}}$.

Proof. Let $n = [K : \mathbb{Q}] = [K' : \mathbb{Q}]$. Following [6, §9], we have $\tau(\mathbb{Z}[\zeta_m], 1) \leqq \frac{n}{4}$. Therefore, we can apply Proposition 3.1 to get that $\tau(\mathfrak{b}, 1) \leqq \frac{n}{4}$, where $\mathfrak{b} = \varphi(\mathbb{Z}[\zeta_m])$ is an $\mathcal{O}_{K'}$-ideal satisfying $\mathfrak{b}^2 = \frac{1}{2}\mathbb{Z}[\eta_{4m}]$. Recall that the map from the class group of $\mathbb{Q}(\eta_{4m})$ to the class group of $\mathbb{Q}(\zeta_{4m})$ which maps a class $[\mathfrak{a}]$ to the class $[\mathfrak{a}\mathbb{Z}[\zeta_{4m}]]$ is injective (cf. [14, Theorem 4.14]). Therefore, $\mathfrak{b}$ is a principal ideal since $\mathfrak{b}\mathbb{Z}[\zeta_{4m}]$ is the principal ideal generated by $\frac{1+\sqrt{-1}}{2}$. As $\mathfrak{b}$ is principal, we have $\tau_{\min}(\mathfrak{b}) = \tau_{\min}(\mathcal{O}_{K'})$, and so $\tau_{\min}(\mathcal{O}_{K'}) \leqq \frac{n}{4}$. Hence Corollary 1.3 implies that $M(K'_{\mathbb{R}}) \leqq 2^{-n}\sqrt{d_{K'}}$. □

Alternative proof. Since $\varphi(\mathbb{Z}[\zeta_m])$ is principal in $\mathbb{Z}[\eta_{4m}]$, we can apply Proposition 4.3 to get $M(K'_{\mathbb{R}}) \leqq 2^{\frac{n}{2}} M(K_{\mathbb{R}})$. Following [6, §10], the euclidean minimum of $K$ satisfies $M(K_{\mathbb{R}}) \leqq 2^{-n}\sqrt{d_K}$. The conclusion follows then from the equality $\sqrt{d_{K'}} = 2^{\frac{n}{2}}\sqrt{d_K}$.

## References


[1] C. BATUT, H.-G. QUEBBEMANN and R. SCHARLAU, Computations of cyclotomic lattices. Exp. Math. **4**, 175–179 (1995).

[2] E. BAYER-FLUCKIGER, Definite unimodular lattices having an automorphism of given characteristic polynomial. Comment. Math. Helv. **59**, 509–538 (1984).

[3] E. BAYER-FLUCKIGER, Lattices and Number Fields. Contemp. Math. **241**, 69–84 (1999).

[4] E. BAYER-FLUCKIGER, Cyclotomic Modular Lattices. J. Théorie Nombres Bordeaux **12**, 273–280 (2000).

[5] E. BAYER-FLUCKIGER, Ideal Lattices. In: A Panorama of Number Theory or The View from Baker's Garden. G. Wustholz, ed., 168–184, Cambridge (2002).

[6] E. BAYER-FLUCKIGER, Upper bounds for Euclidean minima. Preprint.

[7] E. BAYER-FLUCKIGER and J. MARTINET, Formes quadratiques liées aux algèbres semi-simples. J. Reine Angew. Math. **451**, 51–69 (1994).
[8] E. BAYER-FLUCKIGER and G. NEBE, On the Euclidean minimum of some real number fields. Preprint.
[9] F. LEMMERMEYER, The Euclidean algorithm in algebraic number fields. Exp. Math. **13**(5), 385–416 (1995).
[10] C. T. MC MULLEN, Minkowski's conjecture, well-rounded lattices and topological dimension. Preprint.
[11] O. T. O'MEARA, Introduction to Quadratic Forms, 1963.
[12] R. SCHARLAU and R. SCHULZE-PILLOT, Extremal lattices. In: Algorithmic algebra and number theory. Selected papers from a conference, Heidelberg, Germany, October 1997. B. H. Matzat et al. eds., 139–170, Berlin (1999).
[13] R. SCHOOF, Computing Arakelov class groups. Preprint.
[14] L. C. WASHINGTON, Introduction to Cyclotomic Fields. Graduate Texts in Math. **83**, Berlin-Heidelberg-New York 1982.

Received: 14 February 2005

E. Bayer-Fluckiger and Ivan Suarez
Institut de Mathématiques Bernoulli
Ecole Polytechnique Fédérale de Lausamme
CH-1015 Lausanne
Switzerland
eva.bayer@epfl.ch