Journal de Théorie des Nombres
de Bordeaux **17** (2005), 437–454

On the Euclidean minimum of some real number fields

par EVA BAYER-FLUCKIGER et GABRIELE NEBE

RÉSUMÉ. Le but de cet article est de donner des bornes pour le minimum euclidien des corps quadratiques réels et des corps cyclotomiques réels dont le conducteur est une puissance d'un nombre premier.

ABSTRACT. General methods from [3] are applied to give good upper bounds on the Euclidean minimum of real quadratic fields and totally real cyclotomic fields of prime power discriminant.

1. Introduction

Throughout the paper let K be a number field of degree $n = [K : \mathbf{Q}]$, O_K its ring of integers, and denote by D_K the absolute value of the discriminant of K. Then the Euclidean minimum of K is

$$M(K) := \inf\{\mu \in \mathbf{R}_{>0} \mid \forall x \in K\ \exists y \in O_K \text{ such that } |\operatorname{Norm}(x-y)| \leq \mu\}.$$

If $M(K) < 1$ then O_K is a Euclidean ring (with respect to the absolute value of the norm).

It is conjectured that

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

for totally real number fields K of degree n. This conjecture follows from a conjecture in the geometry of numbers that is usually attributed to Minkowski (see [7, Chapter 7 (xvi)]) and which is proven to be true for $n \leq 6$ (see [10]).

If K is not an imaginary quadratic field, then there is no efficient general method to calculate $M(K)$. In this paper we use the general upper bounds for $M(K)$ given in [3] in terms of the covering properties of ideal lattices (see Theorem 2.1) to calculate good upper bounds for $M(K)$ for real quadratic fields (Section 3) and for the maximal totally real subfields of cyclotomic fields of prime power discriminant (Section 4). The last section deals with *thin* totally real fields, which are those fields K for which the bounds in Theorem 2.1 allow to show that $M(K) < 1$.

Manuscrit reçu le 12 février 2004.

Part of the work was done, during a stay of the last author at Harvard university from September to December 2003. G.N. would like to thank the Radcliffe institute which enabled this stay. We also acknowledge Prof. Curtis T. McMullen's valuable remarks on the real quadratic case.

2. Generalities

2.1. Ideal lattices. This section gives a short introduction into the notion of ideal lattices. More detailed expositions can be found in [1], [2], and [3].

Let K be a number field of degree $n = r_1 + 2r_2$ over $\mathbf{Q}$ and denote by

$$K_{\mathbf{R}} := K \otimes_{\mathbf{Q}} \mathbf{R} \cong \mathbf{R}^{r_1} \oplus \mathbf{C}^{r_2}.$$

Note that field automorphisms of K extend uniquely to $\mathbf{R}$-linear ring automorphism of $K_{\mathbf{R}}$. Moreover $K_{\mathbf{R}}$ has a canonical involution $^-$ which is the identity on $\mathbf{R}^{r_1}$ and complex conjugation on $\mathbf{C}^{r_2}$. This involution does not necessarily preserve K. Let

$$\mathfrak{P} := \{\alpha \in K_{\mathbf{R}} \mid \alpha = \overline{\alpha} \text{ and all components of } \alpha \text{ are positive } \}.$$

Then the real valued positive definite symmetric bilinear forms q on $K_{\mathbf{R}}$ that satisfy $q(x, \lambda y) = q(\overline{\lambda} x, y)$ for all $x, y, \lambda \in K_{\mathbf{R}}$ are of the form

$$T(\alpha) : K_{\mathbf{R}} \times K_{\mathbf{R}} \to \mathbf{R}, (x, y) \mapsto \mathrm{Trace}(\alpha x \overline{y})$$

with $\alpha \in \mathfrak{P}$ where $\mathrm{Trace}(x_1, \ldots, x_n) = \sum_{i=1}^{r_1} x_i + \sum_{j=r_1+1}^{r_1+r_2} x_j + \overline{x_j}$ denotes the regular trace of the $\mathbf{R}$-algebra $K_{\mathbf{R}}$.

Definition. Let O_K denote the ring of integers in the number field K. A *generalized O_K-ideal* I is an O_K-submodule $I \subset K_{\mathbf{R}}$ of K-rank 1 in $K_{\mathbf{R}}$. An *ideal lattice* $(I, T(\alpha))$ is a generalized O_K-ideal in $K_{\mathbf{R}}$ together with a positive definite symmetric bilinear form $T(\alpha)$ for some $\alpha \in \mathfrak{P}$.

It is easy to see that generalized O_K-ideals I are of the form $I = \alpha J$ for some $\alpha \in K_{\mathbf{R}}$ and an ideal J in O_K. Then we define the norm $N(I) := \mathrm{Norm}(\alpha) N(J)$ where the norm of $\alpha \in K_{\mathbf{R}}$ is

$$\mathrm{Norm}(\alpha) := \prod_{i=1}^{r_1} |\alpha_i|_{\mathbf{R}} \prod_{j=r_1+1}^{r_1+r_2} |\alpha_j|_{\mathbf{C}}^2 .$$

The inverse of I is $I^{-1} := \alpha^{-1} J^{-1}$ and again a generalized O_K-ideal.

The most important ideal lattices are provided by fractional ideals in K. We are often interested in ideal lattices, where the underlying O_K-module $I = O_K$ is the ring of integers in K. We call such ideal lattices *principal ideal lattices.*

2.2. Covering thickness and packing density. With a lattice L in Euclidean space $(\mathbf{R}^n, (\ ,\ ))$ one associates two sets of spheres: the associated sphere packing and the sphere covering of $\mathbf{R}^n$. The centers of the spheres are in both cases the lattice points. For the sphere packing, one maximizes the common radius of the spheres under the condition that they do not overlap, for the covering, one minimizes the common radius of the spheres such that they still cover the whole space (see [6, Chapter 1 and 2]).

Definition. Let L be a lattice in Euclidean space $(\mathbf{R}^n, (\ ,\ ))$.

(1) The *minimum* of L is

$$\min(L) := \min\{(\ell, \ell) \mid 0 \neq \ell \in L\}$$

the square of the minimal distance of two distinct points in L.

(2) The *maximum* of L is

$$\max(L) := \sup\{\min\{(x - \ell, x - \ell) \mid \ell \in L\} \mid x \in \mathbf{R}^n\}$$

the square of the maximal distance of a point in $\mathbf{R}^n$ from L.

(3) The *Hermite function* of L is

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

(4) The *Hermite-like thickness* of L is

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

Note that $\min(L)$ is the square of twice the packing radius of L and $\max(L)$ is the square of the covering radius of L. Therefore the density of the associated sphere packing of L is

$$\delta(L) = 2^{-n}\gamma(L)^{n/2}V_n,$$

where V_n is the volume of the n-dimensional unit ball and the thickness the associated sphere packing of L is

$$\theta(L) = \tau(L)^{n/2}V_n.$$

The functions τ and γ only depend on the similarity class of the lattice.

Motivated by the applications in information technology one tries to find lattices that maximize γ and minimize τ. For our applications to number fields, the minimal γ and minimal τ are of interest.

Definition. Let K be a number field and I be a generalized O_K-ideal in $K_{\mathbf{R}}$.

$$\gamma_{\min}(I) := \min\{\gamma((I, T(\alpha))) \mid \alpha \in \mathfrak{P}\}$$
$$\tau_{\min}(I) := \min\{\tau((I, T(\alpha))) \mid \alpha \in \mathfrak{P}\}$$

For $I = O_K$ one gets

Proposition 2.1. (see [3, Prop. 4.1 and 4.2]) *Let K be a number field of degree n and denote the absolute value of the discriminant of K by D_K. Then for all generalized O_K-ideals I in $K_{\mathbf{R}}$*

$$\gamma_{\min}(I) \geq \frac{n}{\sqrt[n]{D_K}} \text{ with equality for } I = O_K$$

and

$$\tau_{\min}(I) \leq n\sqrt[n]{D_K}.$$

2.3. The Euclidean minimum. The Euclidean minimum of a number field K is a way to measure how far is K from having a Euclidean algorithm. A very nice survey on Euclidean number fields is given in [9].

Definition. Let K be an algebraic number field and O_K be its ring of integers. The *Euclidean minimum* of K is

$$M(K) := \inf\{\mu \in \mathbf{R}_{>0} \mid \forall x \in K\ \exists y \in O_K \text{ such that } |\mathrm{Norm}(x-y)| \leq \mu\}.$$

More general, let I be a generalized ideal in $K_{\mathbf{R}}$. Then we define

$$M(I) := \inf\{\mu \in \mathbf{R}_{>0} \mid \forall x \in K_{\mathbf{R}}\ \exists y \in I \text{ such that } |\mathrm{Norm}(x-y)| \leq \mu\}.$$

Note that $M(K) \leq M(O_K)$.
In [3] it is shown that

Theorem 2.1.

$$M(I) \leq \left(\frac{\tau_{\min}(I)}{\gamma_{\min}(O_K)}\right)^{n/2} N(I)$$

for all number fields K with $[K : \mathbf{Q}] = n$.

In particular

$$M(K) \leq \left(\frac{\tau_{\min}(O_K)}{n}\right)^{n/2} \sqrt{D_K}.$$

Together with Proposition 2.1 this implies that

$$M(K) \leq D_K$$

for all number fields K. Moreover $M(K) \leq 2^{-n}\sqrt{D_K}$ if K has a principal ideal lattice of thickness smaller than the thickness of the standard lattice.

The purpose of the paper is to use Theorem 2.1 to get good upper bounds on $\tau_{min}(O_K)$ for certain number fields K. The next section treats real quadratic fields and in Section 4 we deal with the maximal real subfields of cyclotomic fields of prime power discriminant.

3. Real quadratic fields

This section treats real quadratic fields $K = \mathbf{Q}[\sqrt{D}]$. Then for any generalized O_K-ideal I the similarity classes of ideal lattices $(I, T(\alpha))$ with $\alpha \in \mathfrak{P}$ form a one-parametric family in the space of all similarity classes of two-dimensional lattices. The latter can be identified with $\mathbf{H}/\operatorname{SL}_2(\mathbf{Z})$, the upper half-plane

$$\mathbf{H} := \{x + iy \in \mathbf{C} \mid y > 0\}$$

modulo the action of $\operatorname{SL}_2(\mathbf{Z})$.

We show that for any generalized O_K-ideal I there is an $\alpha \in \mathfrak{P}$ such that the lattice $(I, T(\alpha))$ has a basis of minimal vectors. In particular $\tau_{\min}(I) \leq \frac{1}{2}$ which implies the Theorem of Minkowski that $M(K) \leq \frac{1}{4}\sqrt{D_K}$ (see [4, Section XI.4.2]). In most of the cases we find better bounds.

3.1. Two-dimensional lattices. There is a well known identification of the set of similarity classes of two-dimensional lattices and the quotient of the upper half plane $\mathbf{H}$ modulo $SL_2(\mathbf{Z})$.

To explain this, we pass to the language of quadratic forms. Up to rescaling we may assume that any positive definite two-dimensional quadratic form is of the form

$$q(t_1, t_2) := wt_1^2 + 2xt_1t_2 + t_2^2 \text{ with } w, x \in \mathbf{R}, w > x^2.$$

Then q is mapped to $z = x + iy \in \mathbf{H} := \{z \in \mathbf{C} \mid \Im(z) > 0\}$ where y is the positive solution of $x^2 + y^2 = w$.

The group $\operatorname{SL}_2(\mathbf{R})$ acts on $\mathbf{H}$ by Möbius transformations $A \cdot z := \frac{az+b}{cz+d}$ for all $A := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \operatorname{SL}_2(\mathbf{R})$. It also acts on the positive definite quadratic forms in two variables by variable substitution,

$$(A \cdot q)(t_1, t_2) := q(at_1 + ct_2, bt_1 + dt_2) = (wc^2 + 2xdc + d^2)(w_1t_1^2 + 2x_1t_1t_2 + t_2^2)$$

for certain $w_1, x_1 \in \mathbf{R}$. Then the mapping above is a similarity of $\operatorname{SL}_2(\mathbf{R})$-sets.

Any proper similarity class of two-dimensional lattices corresponds to a unique $\operatorname{SL}_2(\mathbf{Z})$-orbit of similarity classes of quadratic forms in two variables and hence to an element in $\mathbf{H}/\operatorname{SL}_2(\mathbf{Z})$.

3.2. Real quadratic ideal lattices. Let $K = \mathbf{Q}[\sqrt{D}]$ be a real quadratic field, with $D \in \mathbf{N}$, square-free. Let O_K be the ring of integers in K and ϵ a fundamental unit in O_K. Fix the two different embeddings of σ_1 and σ_2 of K into $\mathbf{R}$. Then $(\sigma_1, \sigma_2) : K_{\mathbf{R}} = K \otimes_{\mathbf{Q}} \mathbf{R} \to \mathbf{R} \oplus \mathbf{R}$ is an isomorphism. As above let $\mathfrak{P}$ be the set of totally positive elements in $K_{\mathbf{R}}$. Then $\mathbf{R}_{>0}$ acts on $\mathfrak{P}$ by $\alpha \cdot r := (\alpha_1 r, \alpha_2 r)$ for $\alpha = (\alpha_1, \alpha_2) \in \mathfrak{P}$ and $r \in \mathbf{R}_{>0}$. Every orbit under this action contains a unique element $\alpha = (\alpha_1, \alpha_2)$ with $\operatorname{Norm}(\alpha) =$

$\alpha_1\alpha_2 = 1$. Since $\alpha_1 > 0$, there is a unique $t \in \mathbf{R}$ with $\alpha_1 = \sigma_1(\epsilon^2)^t$. This establishes a bijection

$$\mathbf{R} \to \mathfrak{P}/\mathbf{R}_{>0}, t \mapsto (\epsilon^2)^t(\mathbf{R}_{>0}).$$

Theorem 3.1. *Let $I \subset K_{\mathbf{R}}$ be a generalized O_K-ideal. Then the set of similarity classes of ideal lattices*

$$\mathfrak{S}_I := \{[(I, T(\alpha))] \mid \alpha \in \mathfrak{P}\}$$

corresponds to a closed geodesics on $\mathbf{H}/\operatorname{SL}_2(\mathbf{Z})$.

Proof. Let $B := (b_1, b_2)$ be a $\mathbf{Z}$-basis of I. With respect to this basis B, the action of ϵ^2 on I corresponds to right multiplication with a unique matrix $A \in \operatorname{SL}_2(\mathbf{Z})$.

Let $W \in \operatorname{SL}_2(\mathbf{R})$ such that $WAW^{-1} = \operatorname{diag}(s_1, s_2)$ where s_1 and $s_2 = s_1^{-1}$ are the eigenvalues of A.

The forms $T(\alpha)$ with $\alpha \in \mathfrak{P}$ are precisely the forms for which ϵ^2 is self-adjoint. Therefore the two eigenvectors of A are orthogonal with respect to any of the forms $T(\alpha)$. Hence in this basis, the set $\mathfrak{S}_I$ is identified with the geodesics $\{is \mid s > 0\} \subset \mathbf{H}$. Since $\operatorname{SL}_2(\mathbf{R})$ acts as isometries on the hyperbolic plane $\mathbf{H}$, W^{-1} maps this geodesics to some other geodesics $\mathfrak{G}$ in $\mathbf{H}$ that corresponds under the identification above to the set $\mathfrak{S}_I$ with respect to the basis B. Since $A \in \operatorname{SL}_2(\mathbf{Z})$ induces an isometry between $(I, T(\alpha))$ and $(I, T(\alpha\epsilon^4))$, the image of $\mathfrak{G}$ in $\mathbf{H}/\operatorname{SL}_2(\mathbf{Z})$ is a closed geodesics that corresponds to the ideal lattices in $\mathfrak{S}_I$. □

The theorem (together with the two examples above) yields a method to calculate $\tau_{\min}(O_K)$ for real quadratic fields K, by calculating the image of the geodesics $\mathfrak{G}$ in the fundamental domain

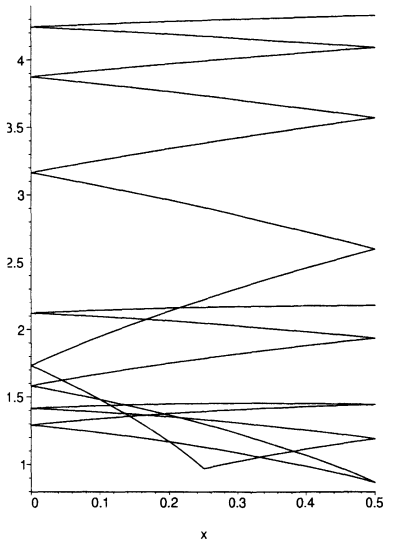
$$\mathfrak{X} := \{z \in \mathbf{H} \mid |\mathbf{R}e(z)| \leq \frac{1}{2}, |z| \geq 1\}$$

of the action of $\operatorname{SL}_2(\mathbf{Z})$ on $\mathbf{H}$. For $x + iy \in \mathfrak{X}$ one has

$$\tau(x + iy) = \frac{1}{4}\frac{(x^2 + y^2)((|x| - 1)^2 + y^2)}{y^3}$$

where, of course, $\tau(x+iy)$ is the Hermite-like thickness of the corresponding two-dimensional lattice.

For $D = 19$, the image of the geodesics $\mathfrak{G}$ in $\mathfrak{X}/\langle$ diag(-1,1) $\rangle$ drawn with MAPLE looks as follows:



The next lemma is certainly well known. Since we did not find a precise reference, however, we include a short elementary proof for the reader's convenience.

Lemma 3.1. *Every geodesics in* $\mathbf{H}/\mathrm{SL}_2(\mathbf{Z})$ *meets the geodesic segment* $\mathfrak{E} := (\frac{-1+i\sqrt{3}}{2}, \frac{1+i\sqrt{3}}{2})$.

Proof. As usual let $T := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$. The orbit $C := \langle T \rangle \mathfrak{E}$ is a continuous curve in $\mathbf{H}$ separating the fundamental domain $\mathfrak{X}$ and the real axis. The geodesics in $\mathbf{H}$ are half-circles perpendicular to the real axis. Let $\mathfrak{G}$ be such a geodesics. Up to the action of $\mathrm{SL}_2(\mathbf{Z})$ we may assume that $\mathfrak{G}$ meets $\mathfrak{X}$ in some point. Since $\mathfrak{G}$ also meets the real axis, it passes through C and hence an image of $\mathfrak{G}$ under $\langle T \rangle$ meets the geodesic segment $\mathfrak{E}$. □

Corollary 3.1. *Let* I *be a generalized* O_K*-ideal. Then there is an* $\alpha \in \mathfrak{P}$ *such that the lattice* $(I, T(\alpha))$ *has a* $\mathbf{Z}$*-basis of minimal vectors.*

Corollary 3.2. *Let* I *be a generalized* O_K*-ideal. Then* $M(I) \leq \frac{1}{4}\sqrt{D_K}N(I)$. *In particular*

$$M(K) \leq \frac{1}{4}\sqrt{D_K} \text{ (Minkowski, see [4])}.$$

For the special case $I = O_K$, it seems to be worthwhile to perform some explicit calculations:

Example. Let $O_K = \mathbf{Z}[\sqrt{D}]$. Then $B := (\sqrt{D}, 1)$ is a $\mathbf{Z}$-basis of O_K and the matrix of $\epsilon^2 =: a + b\sqrt{D}$ with respect to this basis is $A := \left(\begin{smallmatrix} a & bD \\ b & a \end{smallmatrix}\right)$. The matrix W can be chosen as

$$W := \frac{1}{\sqrt{2\sqrt{D}}} \begin{pmatrix} 1 & \sqrt{D} \\ -1 & \sqrt{D} \end{pmatrix}.$$

Then the geodesics $\{is \mid s > 0\}$ is mapped under W^{-1} to the geodesics $\mathfrak{G}$ which is the upper half circle with center 0 meeting the real axis in $\sqrt{D}$ and $-\sqrt{D}$. The trace bilinear form $T(1)$ corresponds to i in the basis of eigenvectors of A (since the two eigenvectors are Galois conjugate) which is mapped to $i\sqrt{D} \in \mathfrak{G}$ under W^{-1}.

To calculate an intersection of $\mathfrak{G}$ and the geodesic segment $\mathfrak{E}$ of Lemma 3.1 let $t' := \lfloor\sqrt{D}\rfloor$. If $t'^2 + t' + 1 \geq D$ then let $t := t'$ and if $t'^2 + t' + 1 < D$ then let $t := t' + 1$. Let $\alpha := 1 + \frac{D+t^2-1}{2tD}\sqrt{D} \in K$. With respect to the new basis $B' := (\sqrt{D} - t, 1)$ the Gram matrix of $T(\alpha)$ is

$$\begin{pmatrix} 2 & x \\ x & 2 \end{pmatrix} \text{ where } x = \frac{D - t^2 - 1}{t} \in [-1, 1]$$

by the choice of t. The thickness of the corresponding ideal lattice

$$\tau(O_K, T(\alpha)) = \frac{2t^2}{(2t + |D - t^2 - 1|)(4t^2 - (D - t^2 - 1)^2)^{1/2}} \leq \frac{1}{2}$$

with equality if and only if $D = t^2 + 1$.

Example. Let $O_K = \mathbf{Z}[\frac{1+\sqrt{D}}{2}]$. Then $B := (\frac{1+\sqrt{D}}{2}, 1)$ is a $\mathbf{Z}$-basis of O_K and the matrix of $\epsilon^2 =: a + b\sqrt{D}$ with respect to this basis is $A := \begin{pmatrix} a+b & b\frac{D-1}{2} \\ 2b & a-b \end{pmatrix}$. The matrix W can be chosen as

$$W := \frac{1}{\sqrt[4]{D}} \begin{pmatrix} 1 & \frac{\sqrt{D}-1}{2} \\ -1 & \frac{\sqrt{D}+1}{2} \end{pmatrix}.$$

Then the geodesics $\{is \mid s > 0\}$ is mapped under W^{-1} to the geodesics $\mathfrak{G}$ which is the upper half circle meeting the real axis in $(1 - \sqrt{D})/2$ and $(1 + \sqrt{D})/2$. The trace bilinear form $T(1)$ corresponds to i in the basis of eigenvectors of A (since the two eigenvectors are Galois conjugate) which is mapped to $\frac{1}{2} + i\frac{\sqrt{D}}{2} \in \mathfrak{G}$ under W^{-1}.

As in the previous example we calculate an intersection of $\mathfrak{G}$ and the geodesic segment $\mathfrak{E}$ of Lemma 3.1. Let $t' := \lfloor\frac{1+\sqrt{D}}{2}\rfloor$. Then

$$t'^2 - t' < \frac{D-1}{4} < t'^2 + t'.$$

For $D = 5$ let $t := 0$, otherwise let $t := \begin{cases} t' & \text{if } t'^2 \geq \frac{D-1}{4} \\ t' + 1 & \text{if } t'^2 < \frac{D-1}{4} \end{cases}$ and put

$$\alpha := 1 + \frac{\frac{D+1}{2} + 2t^2 - 2t - 2}{D(2t-1)}\sqrt{D} \in K.$$

With respect to the new basis $B' := (\frac{1+\sqrt{D}}{2} - t, 1)$ the Gram matrix of $T(\alpha)$ is

$$\begin{pmatrix} 2 & x \\ x & 2 \end{pmatrix} \text{ where } x = \frac{D - (2t-1)^2 - 4}{2(2t-1)} \in [-1, 1]$$

by the choice of t. With $s := 2t - 1$, the thickness of the corresponding ideal lattice

$$\tau(O_K, T(\alpha)) = \frac{8s^2}{(4s + |D - s^2 - 4|)(16s^2 - (D - s^2 - 4)^2)^{1/2}} \leq \frac{1}{2}$$

with equality if and only if $D = s^2 + 4$.

These explicit upper bounds on $\tau_{\min}(O_K)$ yield the following corollary:

Corollary 3.3. *Assume that $D_K \neq 4(t^2+1)$ and $D_K \neq (2t-1)^2 + 4$ (for all $t \in \mathbf{N}$). Then $M(K) < \frac{1}{4}\sqrt{D_K}$. In particular this is true if O_K does not contain a unit of norm -1.*

3.3. Special lattices in real quadratic fields. In view of the results in the last subsection, it is interesting to calculate all points, where the geodesics $\mathfrak{G}$ meets the geodesic segment $\mathfrak{E}$ in $\mathbf{H}/\mathrm{SL}_2(\mathbf{Z})$. This section characterizes the real quadratic fields K that have the square lattice $\mathbf{Z}^2 \leftrightarrow i \in \mathfrak{E}$ respectively the hexagonal lattice $A_2 \leftrightarrow \frac{1+\sqrt{3}i}{2} \in \mathfrak{E}$ as principal ideal lattice.

Let $K = \mathbf{Q}[\sqrt{D_K}]$ be a real quadratic field of discriminant D_K and let O_K be its ring of integers.

Theorem 3.2. *The square lattice $\mathbf{Z}^2$ is a principal ideal lattice for K, if and only if the fundamental unit of K has norm -1.*

Proof. Let ϵ be a unit in K of norm -1. Then $\alpha = \pm\frac{\epsilon}{\sqrt{D_K}}$ is a totally positive element in K and $L_\alpha := (O_K, T(\alpha))$ is an integral lattice of determinant 1 and dimension 2. Therefore $L_\alpha \cong \mathbf{Z}^2$.
On the other hand let $L_\alpha := (O_K, T(\alpha))$ be a positive definite unimodular lattice. Since $L_\alpha^{\#} = L_\alpha$ one finds that $\epsilon := \alpha\sqrt{D_K}$ is a unit in O_K. Since α is totally positive, the norm of ϵ is -1. □

In view of Lemma 3.1 this gives a better bound for $M(K)$ for those real quadratic fields K where all units have norm 1:

It is well known that all real quadratic fields of prime discriminant $D_K = p \equiv 1 \pmod 4$ have a fundamental unit of norm -1 (see e.g. [12, Exercise 6.3.4]). In general one can characterize the real quadratic fields that have units of norm -1, though this characterization is algorithmically not very helpful:

Remark. A real quadratic field K has a unit of norm -1 if and only if $K = \mathbf{Q}[\sqrt{D}]$ for some (not necessarily square-free) D of the form $t^2 + 4$. If

fact, in this case the norm of $\frac{t+\sqrt{D}}{2}$ is -1. On the other hand any integral element

$$u := \frac{a+\sqrt{D}}{2} = \frac{a+b\sqrt{D/b^2}}{2} = \frac{a+b\sqrt{D_K}}{2}$$

of norm -1 yields a decomposition $D = a^2 - 4$.

There is a similar characterization of the fields that contain an element of norm -3 (and of course other norms):

Remark. A real quadratic field K contains an integral element of norm -3 if and only if there are $b, t \in \mathbf{Z}$ with

$$(\star) \quad b^2 D_K = t^2 + 12.$$

Then $\alpha = \frac{t+b\sqrt{D_K}}{2}$ is such an element of norm -3.

Similarly as above, one constructs a definite integral lattice

$$L_\alpha := (O_K, T(\frac{\alpha}{\sqrt{D_K}}))$$

of determinant 3. Up to isometry, there are two such positive definite lattices, the hexagonal lattice A_2 and $\mathbf{Z} \oplus \sqrt{3}\mathbf{Z}$. The lattice A_2 is the only even lattice of determinant 3 and dimension 2. To characterize the fields that have A_2 as ideal lattice, it therefore remains to characterize those α for which the lattice L_α above is even.

This is shown by an explicit calculation of the Gram matrix with respect to an integral basis of O_K. Note that

$$\frac{\alpha}{\sqrt{D_K}} = \frac{1}{2D_K}(t\sqrt{D_K} + bD_K).$$

If $D_K \equiv 1 \pmod 4$ then $(1, \frac{1+\sqrt{D_K}}{2})$ is a basis of O_K for which the Gram matrix of L_α is

$$\begin{pmatrix} b & (b+t)/2 \\ (b+t)/2 & \frac{1}{4}(b(1+D_K)+2t) \end{pmatrix}$$

Hence L_α is an even lattice, if and only if $b, t \in 2\mathbf{Z}$ and $b \equiv t \pmod 4$ (which is impossible in view of equation $(\star)$).

If $D_K \equiv 0 \pmod 4$ then $(1, \frac{\sqrt{D_K}}{2})$ is a basis of O_K for which the Gram matrix of L_α is

$$\begin{pmatrix} b & t/2 \\ t/2 & bD_K/4 \end{pmatrix}$$

Hence L_α is an even lattice, if and only if b is even. Equation $(\star)$ then shows that t is even and $D_K/4 \equiv 3 \pmod 4$.

Clearly the prime 3 has to be either decomposed or ramified in K. Summarizing we get:

Theorem 3.3. *The hexagonal lattice A_2 is a principal ideal lattice for the real quadratic field $K = \mathbf{Q}[\sqrt{D_K}]$ if and only if 4 divides D_K, $D_K/4 \equiv 3$ or 7 (mod 12), and there is $b \in 2\mathbf{Z}$ with $b^2 D_K = t^2 + 12$.*

Numerical examples:

$D_K/4$	3	7	19	31	43	67	91	103	111	127
$b/2$	1	1	7	1	1	553	1	1669	1	13
$t/2$	3	5	61	11	13	9077	19	33877	21	293

Corollary 3.4. *Assume that the real quadratic field $K = \mathbf{Q}[\sqrt{D_K}]$ satisfies the condition of Theorem 3.3. Then*

$$M(K) \leq \frac{\sqrt{D_K}}{3\sqrt{3}} < 0.2\sqrt{D_K}.$$

4. Real cyclotomic fields of prime power discriminant

In this section we give a good upper bound on $\tau_{\min}(O_K)$ where $K = \mathbf{Q}(\zeta + \zeta^{-1})$ and ζ is a p^a-th root of unity, for some prime p and $a \in \mathbf{N}$. [3] already shows that the standard lattice is a principal ideal lattice and hence these fields satisfy Minkowski's conjecture. For $p > 2$ the lattice $(O_K, T(1))$ – the ring of integers of K with the usual trace bilinear form – has a much smaller thickness than the standard lattice and the aim of this section is to calculate this thickness. Since the lattice is invariant under the natural permutation representation of the symmetric group S_n ($n = [K : \mathbf{Q}]$) we begin with a study of S_n-invariant lattices in the next subsection. Note that these lattices are of Voronoi's first kind and their Voronoi domain is for instance also investigated in [5]. We thank Frank Vallentin for pointing out this reference to us.

4.1. The thickness of certain S_n-lattices.

Theorem 4.1. *Let $n \in \mathbf{N}$, and $b \in \mathbf{R}$ with $b > n$. Let $L = L_{b,n}$ be a lattice in $\mathbf{R}^n$ with Gram matrix*

$$A := bI_n - J_n = \begin{pmatrix} b-1 & -1 & \dots & -1 \\ -1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & -1 \\ -1 & \dots & -1 & b-1 \end{pmatrix}$$

where I_n is the $n \times n$-identity matrix and $J_n \in \{1\}^{n \times n}$ is the all-ones matrix. Then L is a positive definite lattice of determinant

$$(b-n)b^{n-1}.$$

Moreover the automorphism group of L contains

$$\langle -I_n \rangle \times S_n,$$

where the symmetric group S_n acts by permuting the coordinates. For a subset $J \subseteq \{1,\dots,n\}$ let v_J be the "characteristic vector", i.e.

$$(v_J)_i = \begin{cases} 1 & i \in J \\ 0 & i \notin J \end{cases}.$$

Then the Dirichlet domain $\mathfrak{D}$ centered in 0 with respect to the $2(2^n-1)+1$ vectors v_J, $-v_J$ (where $J \subseteq \{1,\dots,n\}$) has circumradius R with

$$R^2 = \frac{n}{12b}(3b^2 + n^2 - 3nb - 1).$$

In particular

$$\max(L) \leq \frac{n}{12b}(3b^2 + n^2 - 3nb - 1).$$

Proof. Since I_n and J_n commute, they can be diagonalized simultaneously. Therefore the eigenvalues of $bI_n - J_n$ are $(b-n)$ (multiplicity 1) and b (multiplicity $(n-1)$), from which one gets the positive definiteness of L and the determinant. It is clear that $\langle -I_n \rangle \times S_n$ acts on L as automorphisms. It remains to calculate the Dirichlet domain $\mathfrak{D}$. By definition a vector $x = (x_1,\dots,x_n)$ belongs to $\mathfrak{D}$, if and only if

$$|b\sum_{k\in J} x_k - |J| \sum_{k=1}^{n} x_k| \leq \frac{b|J| - |J|^2}{2}$$

for all $\emptyset \neq J \subset \{1,\dots,n\}$. Modulo the action of S_n we may assume that

$$x_1 \geq x_2 \geq \dots \geq x_\ell \geq 0 > x_{\ell+1} \geq x_{\ell+2} \geq \dots \geq x_n$$

for some $\ell \in \{0,\dots,n\}$. Then $x \in \mathfrak{D} \Leftrightarrow$

$$b\sum_{k=1}^{j} x_k - j\sum_{k=1}^{n} x_k \leq \frac{bj - j^2}{2}, \quad \text{for } j = 1,\dots,\ell$$

and

$$-b\sum_{k=1}^{j} x_{n-k+1} + j\sum_{k=1}^{n} x_k \leq \frac{bj - j^2}{2}, \quad \text{for } j = 1,\dots,n-\ell.$$

We first show that $\mathfrak{D}$ is bounded, i.e. that (x,x) is bounded for $x \in \mathfrak{D}$. Then it is clear that the points of maximal norm in $\mathfrak{D}$ are the vertices of $\mathfrak{D}$, these are the elements of $\mathfrak{D}$, where at least n of the inequalities describing $\mathfrak{D}$ become equalities. Hence we may assume that all the inequalities above are equalities, which determines the vertex x uniquely.

To show that $\mathfrak{D}$ is bounded, we note that the ℓ-th inequality above reads as

$$(b-\ell)\sum_{k=1}^{\ell} x_k - \ell \sum_{k=\ell+1}^{n} x_k \leq \frac{b\ell - \ell^2}{2}.$$

Since $x_k \leq 0$ for $k \geq \ell + 1$, this implies that

$$\sum_{k=1}^{\ell} x_k \leq \frac{\ell}{2}.$$

Since all $x_k \geq 0$ for $k \leq \ell$, one has $0 \leq x_k \leq \frac{\ell}{2}$ for $k = 1, \ldots, \ell$. Similarly one gets $0 \leq -x_k \leq \frac{n-\ell}{2}$ for $k = \ell + 1, \ldots, n$. Therefore the norm of x and hence $\mathfrak{D}$ is bounded.

Now assume that x is a vertex of $\mathfrak{D}$. Then

$$b\sum_{k=1}^{j} x_k - j\sum_{k=1}^{n} x_k = \frac{bj - j^2}{2}, \quad \text{for } j = 1, \ldots, \ell$$

and

$$-b\sum_{k=1}^{j} x_{n-k+1} + j\sum_{k=1}^{n} x_k = \frac{bj - j^2}{2}, \quad \text{for } j = 1, \ldots, n - \ell.$$

The difference of the ℓ-th and the last equality yields

$$\sum_{k=1}^{n} x_k = \frac{2\ell - n}{2}$$

from which one now easily gets that

$$x_k = \frac{b + 2\ell - n + 1 - 2k}{2b}, \quad \text{for } k = 1, \ldots, \ell$$

and

$$-x_{n-k+1} = \frac{b - 2\ell + n + 1 - 2k}{2b}, \quad \text{for } k = 1, \ldots, n - \ell.$$

Therefore one calculates

$$(x, x) = b\sum_{k=1}^{n} x_k^2 - (\sum_{k=1}^{n} x_k)^2 = \frac{1}{12b}(n^3 - n + 3nb^2 - 3n^2 b)$$

as claimed. □

Corollary 4.1. *The Hermite-like thickness of the lattice $L_{b,n}$ is*

$$\tau(L_{b,n}) \leq \tau(n, b) := \frac{R^2}{\sqrt[n]{\det(L)}} = \frac{n(3b^2 + n^2 - 3nb - 1)}{12b(b - n)^{1/n} b^{\frac{n-1}{n}}}.$$

For $n \geq 2$ and $b > n$ the function $\tau(n, b)$ attains its unique global minimum for $b = n + 1$. Then the lattice $L_{n+1,n} \sim A_n^{\#}$ is similar to the dual lattice of the root lattice A_n.

4.2. Some real cyclotomic fields. One motivation to consider the lattices $L_{b,n}$ is that the trace form of the maximal real subfield of a cyclotomic number field with prime power discriminant is the orthogonal sum of lattices similar to $L_{b,n}$. Let $T_p := pI_{(p-1)/2} - 2J_{(p-1)/2}$ such that $\frac{1}{2}T_p$ is the Gram matrix of $L_{p/2,(p-1)/2}$ and let $U_p := pI_{p-1} - J_{p-1}$ be the Gram matrix of $L_{p,p-1} \sim A_{p-1}^{\#}$. Then we get

Proposition 4.1. *Let p be a prime, $a \in \mathbf{N}$ and let $\zeta := \zeta_{p^a}$ be a primitive p^a-th root of unity in $\mathbf{C}$. Let $K := \mathbf{Q}[\zeta + \zeta^{-1}]$ be the maximal real subfield of the p^a-th cyclotomic number field and $O_K := \mathbf{Z}[\zeta + \zeta^{-1}]$ be its ring of integers.*

a) *If $p > 2$ is odd then the lattice $(O_K, T(1))$ is isometric to a lattice with Gram matrix*

$$\perp^{\frac{p^{a-1}-1}{2}} p^{a-1}U_p \perp p^{a-1}T_p.$$

b) *If $p = 2$ then let $\alpha := 2 + \zeta + \zeta^{-1} \in O_K$. Then $(O_K, 2^{1-a}T(\alpha))$ is isometric to the standard lattice $\mathbf{Z}^{2^{a-2}}$.*

Proof. Let $\widetilde{K} := \mathbf{Q}[\zeta]$. Then the trace of $\zeta^i \in \widetilde{K}$ over $\mathbf{Q}$ is

$$\mathrm{Trace}_{\widetilde{K}/\mathbf{Q}}(\zeta^i) = \begin{cases} 0 & i \not\equiv 0 \pmod{p^{a-1}} \\ -p^{a-1} & 0 \neq i \equiv 0 \pmod{p^{a-1}} \\ p^{a-1}(p-1) & i = 0 \end{cases}$$

Let $\Theta_i := \zeta^i + \zeta^{-i} \in O_K$ $(i = 1, \ldots, p^{a-1}(p-1)/2)$.
a) Assume first that p is odd. Then Θ_1 is a unit in O_K, and hence the Θ_i $(i = 1, \ldots, p^{a-1}(p-1)/2)$ form a $\mathbf{Z}$-basis of O_K. One calculates

$$\mathrm{Trace}(\Theta_i\Theta_j) = \begin{cases} 0 & \text{if } i \not\equiv \pm j \pmod{p^{a-1}} \\ -p^{a-1} & \text{if } i \equiv \pm j \not\equiv 0 \pmod{p^{a-1}}, i \neq j \\ (p-1)p^{a-1} & \text{if } i = j \not\equiv 0 \pmod{p^{a-1}}, \\ -2p^{a-1} & \text{if } i \equiv \pm j \equiv 0 \pmod{p^{a-1}}, i \neq j \\ (p-2)p^{a-1} & \text{if } i = j \equiv 0 \pmod{p^{a-1}}, \end{cases}$$

where now Trace is the trace of K over $\mathbf{Q}$. Hence with respect to $T(1)$, O_K is the orthogonal sum of lattices L_i

$$O_K = \perp_{i=1}^{(p^{a-1}-1)/2} L_i \perp L_0$$

where L_i is spanned by the Θ_j with $j \equiv \pm i \pmod{p^{a-1}}$ and has Gram matrix $p^{a-1}U_p$ for $i > 0$ and $p^{a-1}T_p$ for $i = 0$.
b) If $p = 2$ then $(1, \Theta_1, \ldots, \Theta_{2^{a-2}-1})$ is a $\mathbf{Z}$-basis of O_K for which the Gram

matrix of $T(\alpha)$ has the form

$$2^{a-1}\begin{pmatrix} 1 & 1 & & & & \\ 1 & 2 & 1 & & & \\ & 1 & 2 & 1 & & \\ & & 1 & 2 & 1 & \\ & & & \ddots & \ddots & \end{pmatrix}$$

(only the non zero entries are given). This lattice is easily seen to be similar to the standard lattice. □

Corollary 4.2. *Let K be as in Proposition 4.1 and assume that p is odd. Then*

$$\max(O_K, T(1)) \leq \frac{p^{a-2}}{24}(p^{a+2} - p^a - 3p + 3).$$

Proof. The maxima $\max(T_p)$ and $\max(U_p)$ of the lattices with Gram matrix T_p respectively U_p satisfy

$$\max(T_p) \leq \frac{p^3 - 4p + 3}{24p}$$

and

$$\max(U_p) = \frac{p^2 - 1}{12}.$$

If $a = 1$ then the claim follows immediately. If $a \geq 2$, then

$$\max(O_K, T) \leq p^{a-1}\Big(\frac{p^{a-1} - 1}{2}\frac{p^2 - 1}{12} + \frac{p^3 - 4p + 3}{24p}\Big) =$$

$$\frac{p^{a-2}}{24}(p^{a+2} - p^a - 3p + 3).$$

□

Since

$$n := [K : \mathbf{Q}] = \frac{p^{a-1}(p-1)}{2}$$

we find with Proposition 2.1:

Corollary 4.3. *Let K be as in Proposition 4.1. If p is odd then the Euclidean minimum of K satisfies*

$$M(K) \leq \Big(\frac{\max(O_K, T)}{n}\Big)^{n/2} \leq \Big(\frac{p^a(p+1) - 3}{12p}\Big)^{n/2} = z^n\sqrt{D_K}$$

where

$$z = \frac{1}{2\sqrt{3}}\Big(\frac{p^{a+1} + p^a - 3}{p}\Big)^{1/2} p^{-a/2} p^{\frac{1+p^{1-a}}{2(p-1)}} < \frac{1}{2\sqrt{3}}1.6 < \frac{1}{2}$$

(where we assume $a \geq 2$ if $p = 3$). The value of z tends to $\frac{1}{2\sqrt{3}}$ (from above) when p tends to infinity.
If $p = 2$ then

$$M(K) \leq \left(\frac{\tau(O_K, T(\alpha))}{\gamma_{\min}(O_K)}\right)^{n/2} = 2^{-n}\sqrt{D_K}.$$

5. Thin totally real fields.

In [3] a number field K is called *thin*, if $\tau_{\min}(O_K) < \gamma_{\min}(O_K)$. We call K *weakly thin*, if $\tau_{\min}(O_K) \leq \gamma_{\min}(O_K)$. By Theorem 2.1, thin fields are Euclidean and it is usually also possible to show that weakly thin fields are Euclidean.

Table 1: Candidates for totally real thin fields.

n	$b(n)$	D_K	K	thin	α
2	27	5	$\mathbf{Q}[\sqrt{5}]$	+	1
		8	$\mathbf{Q}[\sqrt{2}]$	+	$10+3\sqrt{2}$
		12	$\mathbf{Q}[\sqrt{3}]$	+	$2+\sqrt{3}$
		13	$\mathbf{Q}[\sqrt{13}]$	+	$13+3\sqrt{13}$
		17	$\mathbf{Q}[\sqrt{17}]$	+	$187+45\sqrt{17}$
		21	$\mathbf{Q}[\sqrt{21}]$	+	$5+\sqrt{21}$
		24	$\mathbf{Q}[\sqrt{6}]$	+	$13+5\sqrt{6}$
3	221.2	49	$\mathbf{Q}[\zeta_7+\zeta_7^{-1}]$	+	1
		81	$\mathbf{Q}[\zeta_9+\zeta_9^{-1}]$	+	1
		148	$\mathbf{Q}[x]/(x^3+x^2-3x-1)$	+	$1-18\bar{x}+10\bar{x}^2$
		169	$\mathbf{Q}[x]/(x^3+x^2-4x+1)$	?	
4	2000	725	$\mathbf{Q}[x]/(x^4-x^3-3x^2+x+1)$	+	1
		1125	$\mathbf{Q}[\zeta_{15}+\zeta_{15}^{-1}]$	+	$9-4(\zeta_{15}+\zeta_{15}^{-1})$
		1600	$\mathbf{Q}[\sqrt{2},\sqrt{5}]$	?	
		1957	$\mathbf{Q}[x]/(x^4-4x^2-x+1)$	?	
		2000	$\mathbf{Q}[\zeta_{20}+\zeta_{20}^{-1}]$	(+)	$2-\zeta_{20}-\zeta_{20}^{-1}$
5	19187.6	14641	$\mathbf{Q}[\zeta_{11}+\zeta_{11}^{-1}]$	+	1

The first column lists the degree, followed by the bound $b(n)$ (rounded to the first decimal place for $n = 3$ and $n = 5$). Then we list all totally real fields K of degree n and D_K smaller this bound. A + in the second last column indicates that K is thin, a (+) says that K is weakly thin and a ? means that we don't know whether K is thin or not. The last column gives an $\alpha \in K$ such that $\tau(O_K, T(\alpha))$ is smaller (respectively equal) to $\frac{n}{D_K^{1/n}}$ if K is thin (respectively weakly thin). Note that all fields in the Table 1 are Euclidean (see e.g. [11]). For degrees > 2 we do not have a general algorithm to calculate $\tau_{\min}(O_K)$ for a given number field K.

Theorem 5.1. *All totally real weakly thin fields are listed in Table 1.*

Proof. By [3, Proposition 10.4] there are only finitely many (weakly) thin fields, since the general lower bounds on the Hermite-like thickness of an n-dimensional lattice (see [6]) give an upper bound on $D_K^{1/n}$ for a thin field K. In particular all thin totally real fields have degree $n \leq 5$ (see [3, Proposition 10.4]). The thinnest lattice coverings are known up to dimension $n \leq 5$ ([6, Section 2.1.3]) and provided by the dual lattice $A_n^{\#}$ of the root lattice A_n with

$$\tau(A_n^{\#}) = \frac{n(n+2)}{12(n+1)^{(n-1)/n}}.$$

This gives the bound

$$D_K \leq \left(\frac{n}{\tau(A_n^{\#})}\right)^n = 12^n \frac{(n+1)^{n-1}}{(n+2)^n} =: b(n).$$

Together with the list of fields of small discriminant in [8] this implies that the totally real thin fields are among the ones listed in Table 1. □

It is an interesting question to find good lower bounds for $\tau_{\min}(O_K)$ other than the general bounds for lattices.

Note added in proof: In the meantime Mathieu Dutour, Achill Schürmann and Frank Vallentin [13] have shown that the three remaining candidates for thin fields marked with a question mark in Table 1 are not thin.

References

[1] E. Bayer-Fluckiger, *Lattices and number fields.* Contemp. Math. **241** (1999), 69–84.

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

[3] E. Bayer-Fluckiger, *Upper bounds for Euclidean minima.* J. Number Theory (to appear).

[4] J.W.S. Cassels, *An introduction to the geometry of numbers.* Springer Grundlehren **99** (1971).

[5] J.H. Conway, N.J.A. Sloane, *Low Dimensional Lattices VI: Voronoi Reduction of Three-Dimensional Lattices.* Proc. Royal Soc. London, Series A **436** (1992), 55–68.

[6] J.H. Conway, N.J.A. Sloane, *Sphere packings, lattices and groups.* Springer Grundlehren **290** (1988).

[7] P.M. Gruber, C.G. Lekkerkerker, *Geometry of Numbers.* North Holland (second edition, 1987)

[8] The KANT Database of fields. http://www.math.tu-berlin.de/cgi-bin/kant/database.cgi.

[9] F. Lemmermeyer, *The Euclidean algorithm in algebraic number fields.* Expo. Math. **13** (1995), 385–416. (updated version available via http://public.csusm.edu/public/FranzL/publ.html).

[10] C.T. McMullen, *Minkowski's conjecture, well-rounded lattices and topological dimension.*, Journal of the American Mathematical Society **18** (3) (2005), 711–734.

[11] R. Quême, *A computer algorithm for finding new euclidean number fields.* J. Théorie de Nombres de Bordeaux **10** (1998), 33–48.

[12] E. Weiss, *Algebraic number theory.* McGraw-Hill Book Company (1963).

[13] M. Dutour. A. Schürmann. F. Vallentin, *A Generalization of Voronoi's Reduction Theory and Applications*, (preprint 2005).

Eva BAYER-FLUCKIGER
Département de Mathématiques
EPF Lausanne
1015 Lausanne
Switzerland
E-mail : eva.bayer@epfl.ch
URL: http://alg-geo.epfl.ch/

Gabriele NEBE
Lehrstuhl D für Mathematik
RWTH Aachen
52056 Aachen
Germany
E-mail : nebe@math.rwth-aachen.de
URL: http://www.math.rwth-aachen.de/homes/Gabriele.Nebe/