Algorithms for lattices

Markus Kirschmer

RWTH Aachen University

June 2016

Bilinear spaces

Let K be an algebraic number field with ring of integers $\mathbb{Z}_K$. Let Ω be the set of places of K and $\mathbb{P}$ denotes the prime ideals of $\mathbb{Z}_K$.

Definition

1. A bilinear space (V, Φ) is a finite dimensional vector space V over K equipped with some regular bilinear form $\Phi\colon V \times V \to K$.
2. Two bilinear spaces (V, Φ) and (V', Φ') are said to be isometric, if there exists some isomorphism $\varphi \in \mathrm{Hom}_K(V, V')$ such that

$$\Phi'(\varphi(x), \varphi(y)) = \Phi(x, y) \text{ for all } x, y \in V \ .$$

   Then φ is called an isometry.
3. $\mathrm{O}(V, \Phi) = \{\varphi\colon V \to V \mid \varphi \text{ an isometry}\}$ the orthogonal group of (V, Φ).

Given a place $v \in \Omega$, let K_v and $V_v := V \otimes_K K_v$ be the completions of K and V at v.

Theorem (Local-Global Principle, Hasse-Kneser-Landherr-Springer)

The spaces (V, Φ) and (V', Φ') are isometric if and only if the completions (V_v, Φ) and (V'_v, Φ') are isometric for every place v of K.

This yields classifications of global bilinear spaces via the following invariants:

1. The rank m of V.
2. The determinant.
3. The signature of (V_v, Φ) at the real places v of K.
4. The finite set $\{\mathfrak{p} \in \mathbb{P} \mid \text{Hasse}(V_\mathfrak{p}, \Phi) = -1\}$.

Definition

A bilinear space (V, Φ) over K is said to be (totally positive) definite if

1. K is totally real
2. $\Phi(x, x)$ is totally positive for all nonzero $x \in V$.

We will concentrate on definite spaces for most of the talk.

Deciding if two bilinear spaces are isometric is trivial (compare invariants!).

Constructing one with given invariants is more difficult:

1. The case $m = 1$ is trival (determinant).
2. If $m \geq 3$ the local-global principle yields some $a \in K^*$ represented by Φ. So
$$(V, \Phi) = \langle a \rangle \perp (V', \Phi')$$
for some space (V', Φ') for which we know its invariants.
3. So this leaves the case $m = 2$:
   1. Let $S = \{v \in \Omega \mid \text{Hasse}(V_v, \Phi) = -1\}$.
   2. Let $a \in K^*$ such that $a \notin (K_v^*)^2$ for all $v \in S$.
   3. There exists some $b \in K^*$ supported at $(S \cap \mathbb{P}) \cup \{\mathfrak{q}\}$ with $\mathfrak{q}$ "small" such that
   $$\{v \in \Omega \mid (a, b)_v = -1\} = S$$
   and $\langle a, b \rangle$ has the correct signature at the real places of K.
   One can find such a b using linear algebra over $\mathbb{F}_2$ provided that one known tha class group $\text{Cl}(K)$ and generator for the unit group $\mathbb{Z}_K^*$.
   4. Then $(V, \Phi) \cong \langle a, b \rangle$.

This is the same as "Finding a quaternion algebra with given ramification".

Definition

Let L be a lattice in a bilinear space (V, Φ), i.e. a finitely generated $\mathbb{Z}_K$-submodule of V such that $KL = V$.

1. The dual $L^\# = \{x \in V \mid \Phi(x, L) \subseteq \mathbb{Z}_K\}$ is also a lattice.
2. L is called unimodular if $L = L^\#$.
3. More generally, if $L = \mathfrak{a}L^\#$ for some fractional ideal $\mathfrak{a}$ of $\mathbb{Z}_K$, then L is called $\mathfrak{a}$-modular.
4. Lattices L, L' in bilinear spaces (V, Φ) and (V', Φ') are isometric if there exists some isometry $\varphi\colon (V, \Phi) \to (V', \Phi)$ such that $\varphi(L) = L'$.
5. The automorphism group of L is

$$\mathrm{Aut}(L) = \{\varphi\colon L \to L \mid \ \varphi \text{ an isometry } \}.$$

Similarly, one can define isometries between $L_\mathfrak{p}$ and $L'_\mathfrak{p}$ where $L_\mathfrak{p} = L \otimes_{\mathbb{Z}_K} \mathbb{Z}_{K_\mathfrak{p}}$ is the completion of L at a prime ideal $\mathfrak{p}$ of $\mathbb{Z}_K$.

Pseudo bases

- A lattice L in V is represented efficiently on a computer using a pseudo-basis

$$L = \bigoplus_{i=1}^{m} \mathfrak{a}_i x_i \quad \text{where } x_i \in V \text{ and fractional ideals } \mathfrak{a}_i \text{ of } K.$$

  Using pseudo-bases one can perform basic operations like comparison, addition, intersection,...
- But is also good for taking completions at $\mathfrak{p} \in \mathbb{P}$, since $L_{\mathfrak{p}}$ has the basis

$$(\pi^{\mathsf{ord}_{\mathfrak{p}}(\mathfrak{a}_1)} x_1, \ldots, \pi^{\mathsf{ord}_{\mathfrak{p}}(\mathfrak{a}_m)} x_m)$$

  where $\pi \in K$ denotes a uniformizer of $\mathfrak{p}$.
- Pseudo bases are also useful for local "manipulations". For example, to compute maximal sublattices $X_1, \ldots, X_r$ of L that contain $\mathfrak{p}L$, do this:
  1. Let M be the lattice with the basis above basis.
  2. Since M is free and $M/\mathfrak{p}M \cong (\mathbb{Z}_K/\mathfrak{p})^m$, one can write down the maximal sublattices $Y_1, \ldots, Y_r$ of M that contain $\mathfrak{p}M$.

Jordan decomposition

A variation of the Gram-Schmidt orthogonalization shows that

$$L_{\mathfrak{p}} \cong L_0 \perp L_1 \perp \ldots \perp L_s$$

where L_i is $\mathfrak{p}^i$-modular.

If $\mathfrak{p} \nmid 2$, then the isometry class of $L_{\mathfrak{p}}$ is uniquely determined by

$$\mathsf{rank}(L_0), \ldots, \mathsf{rank}(L_s) \text{ and } \det(L_0), \ldots, \det(L_s)\,.$$

The description of the isometry classes in the case $\mathfrak{p} \mid 2$ is much more involved and is due to O'Meara.

Example

Suppose $K = \mathbb{Q}$. Let L and L' be lattices with Gram matrices

$$\begin{pmatrix} 1 & 1/2 \\ 1/2 & 8 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 2 & 1/2 \\ 1/2 & 4 \end{pmatrix}.$$

The envelopping quadratic spaces of L and L' are isometric and $L_p \cong L'_p$ for all primes p but $L \ncong L'$ since L represents 1 while L' does not.

So the local-global principle does not hold for lattices. This leads to the following definition.

Definition

The class and the genus of a lattice L in a bilinear space (V, Φ) are

$$\begin{aligned} \mathrm{cls}(L) &= \{L' \subset V \mid L' \text{ a lattice such that } L \cong L'\} \\ \mathrm{gen}(L) &= \{L' \subset V \mid L' \text{ a lattice such that } L_{\mathfrak{p}} \cong L'_{\mathfrak{p}} \text{ for all } \mathfrak{p} \in \mathbb{P}\}. \end{aligned}$$

Theorem (Borel)

The genus decomposes into finitely many isometry classes

$$\mathrm{gen}(L) = \biguplus_{i=1}^{h} \mathrm{cls}(L_i)$$

and $h(L) = h(\mathrm{gen}(L)) = h$ *is called the class number of* L *or of* $\mathrm{gen}(L)$.

The local-global principle holds for L if and only if $h = 1$. Otherwise h measures "by how much" it fails.

Problems

1. Find some lattice in a given genus.
2. Decide if $L' \in \mathrm{cls}(L)$.
3. Find representatives $L_1, \ldots, L_h$ of the isometry classes in $\mathrm{gen}(L)$.

A lattice M in (V, Φ) is called maximal, if $\Phi(x, x) \in \mathbb{Z}_K$ for all $x \in M$ and M is maximal with this property. The maximal lattices always form a single genus.

Finding a lattice L in a genus G given by invariants

1. Let M be a maximal lattice in (V, Φ).
2. Let $P = \{\mathfrak{p} \in \mathbb{P} \mid L_\mathfrak{p} \ncong M_\mathfrak{p} \text{ for } L \in G\}$.
3. For $\mathfrak{p} \in P$, find a sublattice $X^{(\mathfrak{p})}$ of M such that

$$X^{(\mathfrak{p})}_\mathfrak{p} \cong L_\mathfrak{p} \text{ for } L \in G \quad \text{and } X^{(\mathfrak{p})}_\mathfrak{q} = M_\mathfrak{q} \text{ for } \mathfrak{q} \neq \mathfrak{p}\,.$$

4. $L := \bigcap_{\mathfrak{p} \in P} X^{(\mathfrak{p})} \in G$ does the trick.

Step (3) is easy if $\mathfrak{p} \nmid 2$ (manipulate a Jordan decomposition of M).
For $\mathfrak{p} \mid 2$, one can do it like that: Let Y be a lattice with $Y_\mathfrak{p} \cong L_\mathfrak{p}$.
Construct a minimal chain of overlattices

$$Y = Y^{(0)} \subsetneq Y^{(1)} \subsetneq \ldots \subsetneq Y^{(r)}$$

such that $Y^{(r)}_\mathfrak{p}$ is maximal and $Y^{(i)} \subseteq \mathfrak{p}^{-1} Y^{(i-1)}$.
Find a lattice $X^{(r-1)}$ between $\mathfrak{p}M$ and M such that $X^{(r-1)} \sim Y^{(r-1)}$ etc.

Computing isometries of definite lattices I

Suppose first $K = \mathbb{Q}$ and let L be a lattice in a definite space (V, Φ). Let $(b_1, \ldots, b_m)$ be a basis of L and $B > 0$.

First: Enumerate $L_{\leq B} := \{x \in L \mid \Phi(x, x) \leq B\}$

The Finke-Pohst method is based on the Cholesky decomposition: There are $q_{i,j} \in \mathbb{Q}$ such that

$$\Phi(x, x) = \sum_{i=1}^{m} q_{i,i} \left(x_i + \sum_{j=i+1}^{m} q_{ij} x_j \right)^2 \text{ for all } x = \textstyle\sum_i x_i b_i \in L.$$

Then $\Phi(x, x) \leq B$ implies $x_m^2 q_{m,m} \leq B$. Hence there are only finitely many possibilities for x_m.

Similarly, $q_{m-1,m-1}(x_{m-1} + q_{m-1,m} x_m)^2 \leq B - q_{m,m} x_m^2$. Thus for fixed x_m there are only finitely many possibilities for x_{m-1}, etc.

So $L_{\leq B}$ is finite and can be enumerated by backtracking.

Computing isometries of definite lattices II

The following algorithm computes an isometry $\varphi\colon L \to L'$ between lattices L, L' in definite spaces (V, Φ) and (V', Φ').

Plesken & Souvignier

1. Let $B > 0$ such that $L_{\leq B} := \{x \in L \mid \Phi(x,x) \leq B\}$ generates L.
2. Suppose $\{b_1, \ldots, b_m\} \subseteq L_{\leq B}$ generates V, so φ is uniquely determined by $\varphi(b_i) \in L'_{\leq B}$.
3. If $\varphi(b_1), \ldots, \varphi(b_{i-1})$ are already chosen, pick $\varphi(b_i) \in L'_{\leq B}$ such that

$$\Phi(b_i, b_j) = \Phi'(\varphi(b_i), \varphi(b_j)) \text{ for all } 1 \leq j \leq i\,.$$

   If no such image $\varphi(b_i)$ exists, backtrack and choose a different image for b_{i-1}.

A modification can be used to compute generators of $\mathrm{Aut}(L)$.

There are several tricks that speed up this search

1. Every isometry φ must respect the fingerprint

$$\#\{y \in L_{=D} \mid \Phi(x,y) = c\}$$

for $D \in \{\varphi(x,x) \mid x \in L_{\leq B}\}$ and $c \in \{\varphi(x,y) \mid x,y \in L_{\leq B}\}$.

2. R. Bacher associates to any $v \in L$ with $\ell := \Phi(v,v)$ a polynomial $B_v(T) \in \mathbb{Z}[T]$ as follows.
For $w \in W_v := \{x \in L \mid \Phi(x,x) = \ell, \Phi(x,v) = \ell/2\}$. Let

$$n_w = \#\{(x,y) \in W_v^2 \mid \Phi(x,w) = \Phi(y,v) = \Phi(x,y) = \ell/2\}.$$

Then $B_v(T) := \sum_{w \in W_v} T^{n_w}$. Since B_v is defined by scalar products, we have $B_v = B_{\varphi(v)}$ for each isometry φ.

3. W. Unger uses J. Leon's ideas on partition refinement to speed up the backtrack search in recent versions of Magma.

4. φ induces isometries between certain canonical sub/overlattices of L and L'. E.g. between $\rho_p(L)$ and $\rho_p(L')$ where ρ_p is Watson p-maps (more later).

Computing isometries of definite lattices III

Obvious changes to the above method only computes isometries $L \to L$ which preserve some additional bilinear forms.

Suppose now $K \neq \mathbb{Q}$ and let L be a $\mathbb{Z}_K$-lattice in a definite bilinear space (V, Φ). For $a \in K$,

$$\Phi_a \colon V \times V \to \mathbb{Q},\ (x, y) \mapsto \mathsf{Tr}_{K/\mathbb{Q}}(a\Phi(x, y))$$

defines a bilinear form on the $\mathbb{Q}$-vector space $V_{\mathbb{Q}}$.

Note that Φ_1 is positive definite. Further, for any $\mathbb{Z}$-linear map $\varphi \colon L \to L$, the following statements are equivalent:

- φ is an isometry in (V, Φ).
- φ is an isometry in $(V_{\mathbb{Q}}, \Phi_1)$ which preserves Φ_a where $K = \mathbb{Q}(a)$.

The maps φ satisfying the latter property can be enumerated as seen before.

How to compute $h(L)$?

Problem:

The orthogonal group $\mathrm{O}(V, \Phi)$ does not have the strong approximation property.

1. For an anisotropic vector $v \in V$, the reflection

$$\tau_v \colon V \to V,\ w \mapsto w - \frac{2\Phi(w,v)}{\Phi(v,v)} v$$

is isometry on (V, Φ) and $\mathrm{O}(V, \Phi)$ is generated by reflections.

2. The spinor norm is the homomorphism defined by

$$\theta \colon \mathrm{O}(V, \Phi) \to K^*/(K^*)^2,\ \tau_v \mapsto \Phi(v,v)\,.$$

The subgroup

$$\mathrm{S}(V, \Phi) = \{\varphi \in \mathrm{O}(V, \Phi) \mid \det(\varphi) = 1 \text{ and } \theta(\varphi) = 1\}$$

does have the strong approximation property.

1. Two lattices L and M in (V, Φ) are said to be in the same spinor genus if there exists some $\varphi \in \mathsf{O}(V, \Phi)$ such that

$$\varphi(L)_{\mathfrak{p}} = \sigma_{\mathfrak{p}}(M_{\mathfrak{p}}) \quad \text{with } \sigma_{\mathfrak{p}} \in \mathsf{S}(V_{\mathfrak{p}}, \Phi) \text{ for all } \mathfrak{p} \in \mathbb{P}.$$

   The spinor genus of L is denoted by $\mathsf{sgen}(L)$.
2. Every genus is a finite union of spinor genera.
3. Every spinor genus is a finite union of isometry classes.

- Step (2) from above is completely understood and can be made explicit in terms of a ray class groups of K and the spinor norm groups of $L_{\mathfrak{p}}$. The latter can be computed by work of Kneser and Beli.
- If (V, Φ) is indefinite, then $\mathsf{cls}(L) = \mathsf{sgen}(L)$.
- So we have to discuss step (3) for definite spaces.

Representatives of the isometry classes in sgen(L).

Let (V, Φ) be definite and let L be a lattice in (V, Φ) and let $\mathfrak{p} \in \mathbb{P}$.
W.l.o.g. $L \subseteq L^{\#}$, $\mathfrak{p} \nmid 2$, $L_{\mathfrak{p}}$ is unimodular and $(V_{\mathfrak{p}}, \Phi)$ is isotropic.

Definition

A lattice L' in V is called a $\mathfrak{p}$-neighbour of L, if $L'_{\mathfrak{p}}$ is unimodular and

$$L/(L \cap L') \cong L'/(L \cap L') \cong \mathbb{Z}_K/\mathfrak{p} \quad \text{as } \mathbb{Z}_K\text{-modules.}$$

1. There exists an explicit finite subset $X \subset L$ such that

   $$\{\{y \in L \mid \Phi(x, y) \in \mathfrak{p}\} + \mathfrak{p}^{-1}x \mid x \in X\}$$

   is the set of all $\mathfrak{p}$-neighbours of L.

   This allows us to compute the set of all $\mathfrak{p}$-neighbours quickly.
2. Every $\mathfrak{p}$-neighbour of L lies in gen(L).
3. Every isometry class in sgen(L) is represented by an iterated $\mathfrak{p}$-neighbour of L.

Hermitian spaces

Let E be one of the following K-algebras with involution $\overline{}: E \to E$:

1. $E = K$ and $\overline{} = \mathrm{id}_K$.
2. E/K a quadratic field extension with $\mathrm{Gal}(E/K) = \{\mathrm{id}_E, \overline{}\}$.
3. E a quaternion algebra over K (i.e. a four-dimensional central simple K-algebra) and $\overline{}$ the canonical involution on E.

Definition

A hermitian space is a finite dimensional (left) vector space V over E equipped with a regular sesquilinear form $\Phi\colon V \times V \to E$ such that

- $\Phi(\alpha x + x', y) = \alpha\Phi(x, y) + \Phi(x', y)$ for all $\alpha \in E$ and $x, x', y \in V$,
- $\Phi(x, y) = \overline{\Phi(y, x)}$ for all $x, y \in V$.

Definite lattices with class number $\leq B$

Let $\mathcal{O}$ be a maximal order in E and let L be a lattice in a hermitian space $(V\Phi)$ over E.

1. The definitions of isometries, genera, class numbers, etc. carry over to hermitian lattices.
2. The algorithms from before can be extended to lattices in hermitian spaces.
3. If (V, Φ) is indefinite, then the class number of L is again known a priori and depends only on some invariants of L and E (strong approximation).
4. If (V, Φ) is definite, the class number of L is not known a priori, but it can be computed using Kneser's method just as before.

Goal

Classify all one-class genera of lattices in definite hermitian spaces.

Known: There are only finitely many such genera (up to similarity).

Watson's transformations

Suppose $E = K$. For $\mathfrak{p} \in \mathbb{P}$ define

$$\rho_{\mathfrak{p}}(L) := L + (\mathfrak{p}^{-1}L \cap \mathfrak{p}L^{\#})$$

If $L_{\mathfrak{p}} = L_0 \perp \ldots \perp L_s$ is a Jordan decomposition, then

- $h(L) \geq h(\rho_{\mathfrak{p}}(L))$.
- $\rho_{\mathfrak{p}}(L_{\mathfrak{p}}) = (L_0 \perp \mathfrak{p}^{-1}L_2) \perp (L_1 \perp \mathfrak{p}^{-1}L_3) \perp \mathfrak{p}^{-1}(L_4 \perp \ldots \perp L_s)$
- $\rho_{\mathfrak{p}}(L) = L \iff L_{\mathfrak{p}} = L_0 \perp L_1$ if this is the case, then $L_{\mathfrak{p}}$ is called square-free.

Idea:

It suffices to enumerate the definite, square-free hermitian lattices with class number 1.

One-class genera

Definition

If $\mathrm{gen}(L) = \biguplus_{i=1}^{h} \mathrm{cls}(L_i)$, then $\mathrm{Mass}(L) := \sum_{i=1}^{h} \frac{1}{\#\mathrm{Aut}(L_i)}$ is the mass of L.

To avoid case distinctions, suppose that E/K is a CM-extension with $n = [K : \mathbb{Q}]$. The other cases work along the same lines.

Let χ be the non-trivial character of $\mathrm{Gal}(E/K)$. Set

$$\begin{aligned} \mathfrak{L}_K(1, s) &= \zeta_K(s) && \text{the Dedekind zeta funkcion of } K \\ \mathfrak{L}_K(\chi, s) &= \zeta_E(s)/\zeta_K(s) && \text{the L-function attached to } \chi \end{aligned}$$

Siegels Maßformel

Theorem (Siegel, 1935)

Let L be a lattice in a definite hermitian space over E of rank m. Then

$$\mathrm{Mass}(L) = 2^{1-nm} \cdot \prod_{i=1}^{m} |\mathfrak{L}_K(\chi^i, 1-i)| \cdot \prod_{\mathfrak{p}} \lambda(L_{\mathfrak{p}})$$

with some local factors $\lambda(L_{\mathfrak{p}}) \in \mathbb{Q}_{>0}$.

The local factors are known in almost all cases, e.g.

- if $2 \notin \mathfrak{p}$ or $\mathfrak{p}$ is unramified in E (Gan&Yu).
- if $L_{\mathfrak{p}}$ is maximal (Shimura).
- if $2 \in \mathfrak{p}$ is ramified in E and $K_{\mathfrak{p}}/\mathbb{Q}_2$ is unramified (Cho).
- if $L_{\mathfrak{p}}$ is square-free (K.)

Fact: $\lambda(L_{\mathfrak{p}}) \in \frac{1}{2}\mathbb{Z}$ and if $\lambda(L_{\mathfrak{p}}) = \frac{1}{2}$ then m is odd and $\mathfrak{p}$ ramifies in E.

The possible spaces

Suppose L is square-free, has rank $m \geq 3$ and $h(L) \leq B$. Siegel's Maß formula and the analytic class number formula show that

$$\begin{aligned} B &\geq \#\mu(E) \cdot \mathsf{Mass}(L) \\ &\geq \left(\frac{2\pi}{\gamma_m}\right)^n \cdot d_K^{(m^2-1)/2} \cdot \underbrace{\mathsf{Nr}_{K/\mathbb{Q}}(d_{E/K})^{m'-1/2} \cdot \prod_{\mathfrak{p}} \lambda(L_{\mathfrak{p}})}_{\geq 1} . \end{aligned} \qquad (\star)$$

where

- $\mu(E) =$ roots of unity in E^*.
- $m' = \frac{m(m-(-1)^m)}{4} \geq 3$.
- $\gamma_m = \prod_{i=1}^{m} \frac{(2\pi)^i}{(i-1)!}$.
- $d_K =$ absolute value of the discriminant of K.
- $d_{E/K} =$ relative discriminant of E/K.

The possible spaces

1. $(\star)$ yields an upper bound on the root discriminant $d_K^{1/n}$. For example $B = 2$ implies that $m \leq 16$ and

m	3	4	5	6	7	8	9	...
$d_K^{1/n} <$	9.13	6.83	5.49	4.59	3.95	3.47	3.09	

   J. Voight lists all totally real number fields K with $d_K^{1/n} \leq 14$, $\rightsquigarrow K$.
2. For fixed K, $(\star)$ yields all possibilities for $d_{E/K}$. Class field theory $\rightsquigarrow E$.
3. If $\det(V_{\mathfrak{p}}, \Phi) \notin \mathsf{Nr}(E_{\mathfrak{p}}^*)$, then

$$\mathfrak{p} \mid d_{E/K} \quad \text{or} \quad \lambda(L_{\mathfrak{p}}) \geq \frac{1}{2}\mathsf{Nr}(\mathfrak{p})^{m-1} .$$

   Hence $(\star)$ yields all possibilities for

$$\{\mathfrak{p} \mid \det(V_{\mathfrak{p}}, \Phi) \notin \mathsf{Nr}(E_{\mathfrak{p}}^*)\} .$$

All in all: Only finitely many combinations for $K, E, (V, \Phi)$.

The squarefree lattices in (V, Φ) with class number $\leq B$

Let L be a squarefree lattice in a definite hermitian space (V, Φ) with class number $\leq B$.

- Let M be a maximal lattice in (V, Φ). W.l.o.g. $L \subseteq M$.
- If $M_{\mathfrak{p}} \neq L_{\mathfrak{p}}$ then

$$\mathfrak{p} \mid d_{E/K} \quad \text{or} \quad \lambda(L_{\mathfrak{p}}) \geq \frac{1}{2}\mathsf{Nr}(\mathfrak{p})^{m-1} .$$

- Hence $(\star)$ yields all possibilities for

$$\{\mathfrak{p} \in \mathbb{P} \mid M_{\mathfrak{p}} \neq L_{\mathfrak{p}}\} .$$

This gives a bound $a \in \mathbb{N}$ which does not depend on L such that $aM \subseteq L \subseteq M$.

Binary hermitian lattices

If $m = \dim_E(V) = 2$, one gets all possible fields K just as before. But

$$B \geq \#\mu(E) \cdot \mathsf{Mass}(L) \geq (2\pi)^{-2n} \cdot \frac{\#\mathsf{Cl}(\mathcal{O})}{Q \cdot \#\mathsf{Cl}(\mathbb{Z}_K)} \cdot d_K^{3/2} \cdot \zeta_K(2)$$

where $Q = [\mathcal{O}^* : \mu(E)\mathbb{Z}_K^*] \in \{1, 2\}$ is Hasse's unit undex.

For example $K = \mathbb{Q}(\sqrt{5})$ and $B = 2$ yields $\#\mathsf{Cl}(\mathcal{O}) \leq 120$. If $E/\mathbb{Q}$ is cyclic, Louboutin shows that

$$\mathsf{Nr}_{K/\mathbb{Q}}(d_{E/K}) < 1.68 \cdot 10^{11} .$$

Without the assumptions on $E/\mathbb{Q}$ the bound becomes even worse. So $m = 2$ is out of reach with current methods.

If $K = \mathbb{Q}$ and $B = 2$ then $\#\mathsf{Cl}(\mathcal{O}) \leq 48$. All imaginary quadratic number fields with class number ≤ 100 were enumerated by Watkins in his theis. So $K = \mathbb{Q}$ is feasible.

Some results

Similarly, if $\dim_K(V) = 2$ this lead to relative class number problems (Gauß) which are currently out of reach.

In all other cases, a complete classification is possible. Below are the number of genera with class number one

case $h(L) = 1$	max rank(L)	max $[K : \mathbb{Q}]$	$\#E$	$\#K$	#genera
$E = \mathbb{Q}$	10				1884 (Watson)
$E = K \neq \mathbb{Q}$	6	5		29	4019 (Lorch)
$\dim_K(E) = 2$	8	3	10	5	164
$\dim_K(E) = 4$	4	5	69	29	–

and with class number two

case $h(L) = 2$	max rank(L)	max $[K : \mathbb{Q}]$	$\#E$	$\#K$	#genera
$E = \mathbb{Q}$	16				7283
$E = K \neq \mathbb{Q}$	8	5		75	17.064
$\dim_K(E) = 2$	9	4	19	9	406
$\dim_K(E) = 4$	5	8	148	60	–