Lattices over Dedekind domains

Markus Kirschmer

TRR 195 - Summer School 2023

UNIVERSITÄT PADERBORN

Dedekind domains

Definition

Let $S \subseteq T$ be domains. The integral closure of S in T is the subring

$$\mathrm{Int}_S(T) = \{t \in T \mid f(t) = 0 \text{ for some monic } f \in S[X]\} \subseteq T\,.$$

Definition

An integral domain R with field of fractions K is called a Dedekind domain, if

- R is noetherian.
- every nonzero prime ideal of R is maximal.
- $R = \mathrm{Int}_R(K)$.

Example

- $R = \mathbb{Z}$ is a Dedekind domain.
- Let K be an algebraic number field (i.e. a finite field extension of $\mathbb{Q}$). Then $\mathbb{Z}_K := \mathrm{Int}_{\mathbb{Z}}(K)$ is a Dedekind domain.
- Localizations/Completions of Dedekind domains are Dedekind domains.

Fractional ideals

Let R be a Dedekind domain with field of fractions K. Let $\mathbb{P}(R)$ denote the set of maximal ideals of R.

Theorem

1. *The set of fractional ideals*

$$\mathcal{I}(R) = \{aI \mid a \in K^*, \{0\} \neq I \trianglelefteq R\}$$

forms a free abelian group under multiplication with basis $\mathbb{P}(R)$.

2. *The neutral element of* $\mathcal{I}(R)$ *is* R *and the inverse of* $\mathfrak{a} \in \mathcal{I}(R)$ *is*

$$\mathfrak{a}^{-1} = \{x \in K \mid x\mathfrak{a} \subseteq R\}\,.$$

3. *Two fractional ideals* $\mathfrak{a}$ *and* $\mathfrak{b}$ *are isomorphic (as* R*-modules) if and only if* $\mathfrak{b} = a\mathfrak{a}$ *for some* $a \in K^*$. *Hence the class group*

$$\mathrm{Cl}(R) := \mathcal{I}(R)/\{aR \mid a \in K^*\}$$

describes the isomorphism classes of fractional ideals of R.

Completions

Definition

A valuation of K is a map $|.|\colon K \to \mathbb{R}_{\geq 0}$ such that for all $x, y \in K$

1. $|x| = 0 \iff x = 0$.
2. $|xy| = |x| \cdot |y|$.
3. $|x + y| \leq |x| + |y|$.

If $|.|$ satisfies the stronger condition $|x + y| \leq \max\{|x|, |y|\}$ it is called non-archimedean.

Theorem

There is a (unique) minimal field extension $\hat{K}/K$ such $|.|$ extends to a valuation on $\hat{K}$ and $(\hat{K}, |.|)$ is complete (i.e. every Cauchy sequence in $\hat{K}$ converges). The field $\hat{K}$ is called the completion of K with respect to $|.|$.

Proof: See the construction of $\mathbb{R}$ from $\mathbb{Q}$.

Completion - Examples

1. Every embedding $\iota\colon K \to \mathbb{C}$ yields an archimedean valuation
$$|.|_\iota\colon K \to \mathbb{R}_{\geq 0},\ x \mapsto |\iota(x)|\,.$$
2. Since $\mathbb{P}(R)$ is a basis of $\mathcal{I}(R)$, every $\mathfrak{a} \in \mathcal{I}(R)$ admits a unique factorization
$$\mathfrak{a} = \prod_{\mathfrak{p} \in \mathbb{P}(R)} \mathfrak{p}^{v_\mathfrak{p}(\mathfrak{a})}\,.$$
This gives rise to an archimedean valuation
$$|.|_\mathfrak{p}\colon K \to \mathbb{R}_{\geq 0},\ x \mapsto 2^{-v_\mathfrak{p}(xR)}\,.$$
We denote the corresponding completion of K by $K_\mathfrak{p}$ and set
$$R_\mathfrak{p} = \mathrm{Int}_R(K_\mathfrak{p}) = \{x \in K_\mathfrak{p} \mid |x| \leq 1\}\,.$$
Then $R_\mathfrak{p}$ is a complete local Dedekind ring with field of fractions $K_\mathfrak{p}$.

Theorem (Ostrowski)

All completions of algebraic number fields arise in these ways (up to isomorphism).

Lattices

Definition

An R-lattice is a finitely generated, torsion free R-module.

Equivalently:

An R-lattice is a finitely generated R-submodule of a finite dimensional K-vector space V. It is said to be full, if it contains a K-basis of V.

Example

The non-zero lattices of R in $V := K$ are the fractional ideals of R and the class group $\mathrm{Cl}(R)$ describes the isomorphism classes of lattices in R.

Pseudo bases

Theorem (Steinitz)

Let L be a R-lattice in V. Then there exists a linearly independent system $(v_1, \ldots, v_r) \in V^r$ and fractional ideals $\mathfrak{a}_1, \ldots, \mathfrak{a}_r \in R$ such that

$$L = \mathfrak{a}_1 v_1 \oplus \ldots \oplus \mathfrak{a}_r v_r .$$

Moreover, L is free if and only if the Steinitz invariant $\prod_i \mathfrak{a}_i$ is principal.

The sequence $((\mathfrak{a}_1, v_1), \ldots, (\mathfrak{a}_r, v_r))$ is called a pseudo basis of L and $r = \dim_K(KL)$ is called the rank of L.

Using pseudo bases, CAS like Oscar/Hecke can store, compare, intersect and sum lattices, see Tommy's talk for details.

Completions

Let L a full R-lattice in a K-space V. Then

$$L_\mathfrak{p} := R_\mathfrak{p} \otimes_R L$$

is a full $R_\mathfrak{p}$ lattice in the $K_\mathfrak{p}$-space $V_\mathfrak{p} := K_\mathfrak{p} \otimes_K V$.

Remark

If $M = \mathfrak{a}_1 v_1 \oplus \ldots \oplus \mathfrak{a}_r v_r$ and $\pi \in K$ with $v_\mathfrak{p}(\pi) = 1$, then

$$(\pi^{v_\mathfrak{p}(\mathfrak{a}_1)} v_1, \ldots, \pi^{v_\mathfrak{p}(\mathfrak{a}_r)} v_r)$$

is an $R_\mathfrak{p}$-basis of $M_\mathfrak{p}$.

In particular:

Corollary

If M is a full lattice in V, then $L_\mathfrak{p} = M_\mathfrak{p}$ almost everywhere (i.e. at all but finitely many prime ideals).

Local-global principle for lattices

Theorem

We get bijections

$$\{\textit{full } R\textit{-lattices in } V\} \leftrightarrow \left\{ (M^{(\mathfrak{p})})_{\mathfrak{p}\in\mathbb{P}(R)} \;\middle|\; \begin{array}{l} M^{(\mathfrak{p})} \textit{ full } R_{\mathfrak{p}}\textit{-lattice in } V_{\mathfrak{p}} \textit{ with} \\ M^{(\mathfrak{p})} = L_{\mathfrak{p}} \textit{ almost everywhere} \end{array} \right\}$$

$$M \mapsto (M_{\mathfrak{p}})_{\mathfrak{p}\in\mathbb{P}(R)}$$

$$\bigcap_{\mathfrak{p}\in\mathbb{P}(R)} M^{(\mathfrak{p})} \leftarrow\!\shortmid (M^{(\mathfrak{p})})_{\mathfrak{p}\in\mathbb{P}(R)}$$

This allows for "local" manipulations of R-lattices: For example, to compute maximal sublattices $X_1, \ldots, X_s$ of $L := \bigoplus_{i=1}^r \mathfrak{a}_i x_i$ that contain $\mathfrak{p}L$ do:

1. Let M be the lattice with basis $(\pi^{v_{\mathfrak{p}}(\mathfrak{a}_1)} v_1, \ldots, \pi^{v_{\mathfrak{p}}(\mathfrak{a}_r)} v_r)$.
2. Since M is free and $M/\mathfrak{p}M \cong (\mathbb{Z}_K/\mathfrak{p})^r$, one can write down the maximal sublattices $Y_1, \ldots, Y_s$ of M that contain $\mathfrak{p}M$.
3. Set $X_i = (Y_i + \mathfrak{p}L) \cap L$.

Lattices in quadratic spaces

From now on: K is an algebraic number field. Then any bilinear form $\Phi\colon V \times V \to K$ induces a quadratic form $\Phi\colon V \to K, v \mapsto \Phi(v, v)$.

Definition

Let (V, Φ) and (V', Φ') be regular bilinear/quadratic spaces over K.

1. The $\mathbb{Z}_K$-lattices L, L' in (V, Φ) and (V', Φ') are called isometric, if there exists an isometry $\varphi\colon (V, \Phi) \to (V', \Phi')$ such that $\varphi(L) = L'$.
   We denote this by writing $L \cong L'$.
2. The automorphism group of L is
$$\mathrm{Aut}(L) = \{\varphi \in \mathrm{O}(V, \Phi) \mid \varphi(L) = L\} .$$
3. The dual of a full lattice L in V is
$$L^{\#} := \{v \in V \mid \Phi(v, L) \subseteq \mathbb{Z}_K\} .$$
   The lattice L is called integral if $L \subseteq L^{\#}$ and unimodular if $L = L^{\#}$.

Similar definitions hold for the completions $L_{\mathfrak{p}}$ for $\mathfrak{p} \in \mathbb{P}(\mathbb{Z}_K)$.

Local-global principle for quadratic spaces

Let $v \in \mathbb{P}(\mathbb{Z}_K)$ or $v \colon K \to \mathbb{C}$. The map Φ extends to the completion $V_v = V \otimes_K K_v$. This yields a bilinear/quadratic space (V_v, Φ) over K_v.

Theorem (Hasse-Minkowski)

Quadratic spaces over K are isometric if and only if their completions are isometric.

This yields a classification of regular quadratic spaces over K by the following invariants:

1. The dimension m of V.
2. The discriminant $\mathrm{disc}(V, \Phi)$.
3. The signatures of (V_ι, Φ) at the real embeddings $\iota \colon K \to \mathbb{R}$.
4. The finite set of prime ideals $\mathbb{P}(\mathbb{Z}_K)$ with Clifford invariant -1.

We say that (V, Φ) is definite, if all embeddings $\iota \colon K \to \mathbb{C}$ satisfy $\iota(K) \subseteq \mathbb{R}$ and (V_ι, Φ) is a definite space over $\mathbb{R}$.

Failure of the local-global principle

Example

The local-global principle does *not* hold over $\mathbb{Z}$. E.g.

$$Q(x,y) = x^2 + xy + 8y^2 \quad \text{and} \quad Q'(x,y) = 2x^2 + xy + 4y^2$$

are isometric over $\mathbb{R}$ and over $\mathbb{Z}_p$ for all primes p, but not over $\mathbb{Z}$ since $Q(1,0) = 1$ and $Q'(x,y) \neq 1$ for all $x, y \in \mathbb{Z}$.

The failure of the local-global principle for lattices leads to the following definition:

Definition

The genus and the isometry class of a $\mathbb{Z}$-lattice L in (V, Φ) are

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

Local isometry classes

Let $\pi \in \mathfrak{p} \in \mathbb{P}(\mathbb{Z}_K)$ with $v_\mathfrak{p}(\pi) = 1$. A variation of the Gram-Schmidt process shows that $L_\mathfrak{p}$ has a Jordan decomposition

$$L_\mathfrak{p} = L_1 \perp L_2 \perp \ldots \perp L_r$$

where $(L_i, \pi^{-s_i}\Phi)$ is unimodular and $s_1 < s_2 < \ldots < s_r$.

Theorem

If $2 \notin \mathfrak{p}$, then $(\mathrm{rank}(L_i), \mathrm{disc}(L_i, \pi^{-s_i}\Phi), s_i)_{1 \le i \le r}$ uniquely describe the isometry class of $L_\mathfrak{p}$.

If $2 \in \mathfrak{p}$, the classification of the isometry classes is due to O'Meara and much more involved.

Genera

Theorem (Kneser)

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

is a union of finitely many isometry classes and $h(L) = h(\mathrm{gen}(L)) = h$ *is called the class number of* L *or* $\mathrm{gen}(L)$*.*

So $h(L)$ measures by "how much" the local-global principle fails for L.

Goal

Work out representatives $L_1, \ldots, L_h$.

- If $m = 1$, then $\mathrm{gen}(L) = \mathrm{cls}(L)$.
- For $m = 2$, Gauß' famous composition of binary quadratic forms identifies the isometry classes in $\mathrm{gen}(L)$ with a (quotient) of a class group of a quadratic extension of $\mathbb{Z}_K$.
- For $m \geq 3$ we distinguish two cases: (V, Φ) is indefinite or definite.

Spinor norms

From now on, let $m \geq 3$.

Definition

Let $v \in V$ such that $\Phi(v,v) \neq 0$. Then the reflection

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

is an isometry on (V,Φ).

Theorem

1. *The orthogonal group* $\mathrm{O}(V,\Phi)$ *is generated by reflections.*
2. *There exists a unique homomorphism* $\mathrm{spn}\colon \mathrm{O}(V,\Phi) \to K^*/K^{*,2}$ *such that* $\mathrm{spn}(\sigma_v) = \Phi(v,v)K^{*,2}$ *called the Spinor norm.*

We set

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

Spinor genera

Definition

The spinor genus of a full lattice L in V is

$$\mathrm{sgen}(L) := \left\{ \sigma(M) \,\middle|\, \begin{array}{c} \sigma \in \mathrm{O}(V,\Phi) \text{ and } M \subseteq V \text{ a full lattice such that for all} \\ \mathfrak{p} \in \mathbb{P}(\mathbb{Z}_K) \text{ exists some } \sigma_\mathfrak{p} \in \mathrm{S}(V_\mathfrak{p},\Phi) \text{ with } M_\mathfrak{p} = \sigma_\mathfrak{p}(L_\mathfrak{p}) \end{array} \right\}$$

We clearly have

$$\mathrm{cls}(L) \subseteq \mathrm{sgen}(L) \subseteq \mathrm{gen}(L) \, .$$

So we are left with two problems:

1. Decompose the genus of L into spinor genera.
2. Decompose each spinor genus into isometry classes.

Neighbors

Definition

Let $\mathfrak{p} \in \mathbb{P}(\mathbb{Z}_K)$ such that $(V_\mathfrak{p}, \Phi)$ is isotropic (automatically holds for $m \geq 5$) and $L_\mathfrak{p}$ is unimodular. A $\mathfrak{p}$-neighbor of L is a full lattice M in V such that

$$L/L \cap M \cong \mathbb{Z}_K/\mathfrak{p} \cong M/L \cap M \ .$$

Facts

1. The $\mathfrak{p}$-neighbors of L can be written down explicitly.
2. The $\mathfrak{p}$-neighbors of L lie in the genus of L.
3. The number of spinor genera in $\mathrm{gen}(L)$ is 2^r for some $r \geq 0$.
4. There exists a computable quotient $Q \cong (\mathbb{Z}/2\mathbb{Z})^r$ of a ray class group of $\mathbb{Z}_K$ such that the image of $[\mathfrak{p}] \in Q$ decides in which spinor genus the $\mathfrak{p}$-neighbors of L fall. In particular, any spinor genus in $\mathrm{gen}(L)$ can be reached by some suitable neighbor (Kneser, O'Meara, Beli, Chan, Lorch, K).

Strong approximation

Theorem (Strong approximation, Kneser)

Assume $m = \dim(V) \geq 3$. *Let* $T \subseteq S \subseteq \mathbb{P}(\mathbb{Z}_K)$ *with* T *finite. Let* K_v *be a completion with* $v \notin S$ *and* (V_v, Φ) *isotropic. Let* L *be a full lattice in* V *and for* $\mathfrak{p} \in T$ *fix some* $\sigma_\mathfrak{p} \in \mathrm{S}(V_\mathfrak{p}, \Phi)$. *Then for any* $k \in \mathbb{N}$ *there exists some* $\sigma \in \mathrm{S}(V\Phi)$ *such that*

$$(\sigma - \sigma_\mathfrak{p})(L_\mathfrak{p}) \subseteq \mathfrak{p}^k L_\mathfrak{p} \quad \text{for } \mathfrak{p} \in T$$

$$\sigma(L)_\mathfrak{p} = L_\mathfrak{p} \quad \text{for } \mathfrak{p} \in S \setminus T$$

Corollary

If $m \geq 3$ *and* (V, Φ) *is indefinite, then* $\mathrm{sgen}(L) = \mathrm{cls}(L)$.

Note: In the indefinite case, this settles the problem of finding representatives of the isometry classes in $\mathrm{sgen}(L)$ *without* testing for isometries!

The definite case

Pick $\mathfrak{p} \in \mathbb{P}(\mathbb{Z}_K)$ s.t. $(V_\mathfrak{p}, \Phi)$ is isotropic and the $\mathfrak{p}$-neighbors of L lie in $\mathrm{sgen}(L)$.

Theorem (Kneser)

By strong approximation, any isometry class in $\mathrm{sgen}(L)$ has a representative M such that $M_\mathfrak{q} = L_\mathfrak{q}$ for all $\mathfrak{q} \neq \mathfrak{p}$ and there exists a sequence

$$L = L_0, L_1, \ldots, L_r = M$$

of lattices such that L_i is a $\mathfrak{p}$-neighbor of L_{i-1}.

Hence the directed graph $\Gamma_\mathfrak{p}$ of isometry classes in $\mathrm{sgen}(L)$ defined by

$$\mathrm{cls}(M) \bullet\!\!-\!\!>\!\!-\!\!\bullet \mathrm{cls}(M') \iff M' \text{ is a } \mathfrak{p}\text{-neighbour of } M$$

is connected.

Essence

To split $\mathrm{sgen}(L)$ into isometry classes, we need to find a spanning tree of $\Gamma_\mathfrak{p}$.

Note: This requires that we can test for isometries!

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

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

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

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

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

So $L_{\le B}$ 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 $\{b_1, \dots, b_m\} \subseteq L_{\leq B}$ generates V, so φ is uniquely determined by $\varphi(b_i) \in L'_{\leq B}$.
3. If $\varphi(b_1), \dots, \varphi(b_{i-1})$ 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-map (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 $a \in K$,

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

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.

Siegel's Mass formula

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.

Theorem (Siegel)

If $m \geq 3$ is odd, then

$$\mathrm{Mass}(L) = c(m)^{[K:\mathbb{Q}]} \cdot d_K^{m(m-1)/4} \cdot \prod_{i=1}^{(m-1)/2} \zeta_K(2i) \cdot \prod_{\mathfrak{p} \in \mathbb{P}(\mathbb{Z}_K)} \lambda(L_\mathfrak{p})$$

where

1. $c(m)$ *is a constant depending on* m.
2. d_K *is the absolute value of the discriminant of* $K/\mathbb{Q}$.
3. ζ_K *is the Dedekind zeta function of* K.
4. $\lambda(L_\mathfrak{p})$ *are the local densities (fudge factors).*

A similar formula holds for $m \geq 4$ even.

Siegel's Mass formula

Note

The mass formula yields an oracle to decide if all vertices in the graph $\Gamma_{\mathfrak{p}}$ have already been found.

We now turn to the enumeration of all definite lattices with class number one.

- The main tool is again the mass formula.
- By Gauß' composition of binary quadratic forms, the enumeration of all one-class genera in the case $m = 2$ yields relative class number problems in quadratic extensions of K. There is currently no unconditional solution.
- So for the remainder of the talk let (V, Φ) be a definite quadratic space over K of dimension $m \geq 3$.

Watson's transformations

For $\mathfrak{p} \in \mathbb{P}(\mathbb{Z}_K)$ define

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

Let $\pi \in K$ with $v_{\mathfrak{p}}(\pi) = 1$ and let

$$L_{\mathfrak{p}} = L_0 \perp \ldots \perp L_s$$

be a Jordan decomposition such that $(L_i, \pi^{-i}\Phi)$ is unimodular. 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 lattices with class number 1.

Enumeration of one-class genera

Suppose L is a definite square-free lattice of rank $m \geq 3$ with class number 1. Then there exists an explicit constant $b(m)$ such that

$$1 \geq \mathrm{Mass}(L) = c(m)^n \cdot d_K^{m(m-1)/4} \cdot \prod_{\mathfrak{p}} \lambda_{\mathfrak{p}}(L) \geq c(m)^n \cdot d_K^{m(m-1)/4} \cdot b(m)^n \tag{1}$$

where $n := [K : \mathbb{Q}]$. Thus

$$d_K^{1/n} \leq (b(m)c(m))^{\frac{-4}{m(m-1)}} . \tag{2}$$

1. The rhs of (2) is $\leq 10 \rightsquigarrow$ finitely many K (enumerated by J. Voight).
2. For K fixed, the rhs of (2) tends to ∞ if $m \to \infty \rightsquigarrow$ finitely many m.
3. For K and m fixed, there are only finitely many square-free L satisfying (1). $\rightsquigarrow$ Construct them and check if class number is 1.
4. Investigate $\rho_{\mathfrak{p}}^{-1}$ to get the non-square-free lattices with class number 1.

One-class genera

Theorem (Watson, Lorch, K.)

1. *There are 30 (totally real) number fields K that admit definite lattices of rank ≥ 3 and class number one.*
2. *Over $K = \mathbb{Q}$ there are up to similarity (isometry + rescaling the quadratic form) 1884 definite lattices of rank ≥ 3 with class number one:*

rank	*3*	*4*	*5*	*7*	*6*	*8*	*9*	*10*	> 10	*total*
lattices	*794*	*481*	*295*	*186*	*86*	*36*	*4*	*2*	*0*	*1884*

3. *Over the 29 fields $K \neq \mathbb{Q}$ there are (up to similarity) 5903 definite lattices of rank ≥ 3 with class number one and they all have rank ≤ 6.*