A Short Introduction to Lattices from Noncommutative Fields

Roope Vehkalahti
Aalto University, Finland

8.5.2019
Lattice meeting
London

References

- The results that are presented here either classical or are done by me alone or in collaboration with Laura Luzzi and Francis Lu.

A lattice

- A lattice L is a discrete additive group in $\mathbb{R}^n$.
- This is equivalent with the condition that there exists a set of linearly independent elements $\{a_1, \ldots, a_k\}$ that generate L.
- If $L = a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_k\mathbb{Z}$, we say that L has degree k.

Matrix lattices

Lattices we consider in this presentation are based on additive groups in $M_{n\times n}(\mathbb{C})$.

Definition

A matrix lattice $L \subseteq M_{n\times n}(\mathbb{C})$ has the form

$$L = \mathbb{Z}B_1 \oplus \mathbb{Z}B_2 \oplus \cdots \oplus \mathbb{Z}B_k,$$

where the matrices $B_1, \ldots, B_k$ are linearly independent over $\mathbb{R}$, i.e., form a lattice basis, and k is called the dimension of the lattice.

Let us assume that $X, Y \in M_n(\mathbb{C})$. The natural inner-product is now

$$\langle X, Y \rangle = \Re(\, Tr(XY^\dagger).$$

- With respect to this inner-product $M_n(\mathbb{C})$ can be seen as a space $\mathbb{R}^{2n^2}$.
- Matrix form is just convenient way of presenting our vectors.

Matrix lattices

- We denote the measure (or hypervolume) of the fundamental parallelotope of a lattice $L \subset M_n(\mathbb{C})$ by $\mathrm{Vol}(L)$ and call it the *volume of the fundamental parallelotope of the lattice L*.

If $x_1, \ldots, x_k$ is a basis of L, we can form the *Gram matrix* of the lattice L

$$\left(\Re tr(x_i x_j^\dagger)\right)_{1 \leq i,j \leq k}.$$

The Gram matrix has a positive determinant equal to $\mathrm{Vol}(L)^2$.

Lattices from number fields

- Let us begin with a degree n algebraic integer a.
- Let $f_a(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + c_0$ be the minimal polynomial of a (here $c_i \in \mathbb{Z}$).
- We use notation $K = \mathbb{Q}(a) = \mathbb{Q} \oplus \mathbb{Q}a \oplus \cdots \oplus \mathbb{Q}a^{n-1}$.
- The set K is a *field*.
- This means that K is additively and multiplicatively closed and for every element $x \in K, x \neq 0$, there exists $y \in K$ such that $xy = 1$.

Lattices from number fields

We also have that

$$R_K = \mathbb{Z}[a] = \mathbb{Z} \oplus \mathbb{Z}a \oplus \cdots \oplus \mathbb{Z}a^{n-1}.$$

is a ring and a degree n free $\mathbb{Z}$-module.

- However, when seen as a subset in $\mathbb{C}$ it is a dense set.
- So it is an additive group, but it is not discrete in the natural ambient space.

Lattices from number fields

We will denote with $\sigma_i(a)$ the complex roots of polynomial $f_a(x)$.

$$f_a(x) = (x - \sigma_1(a))(x - \sigma_2(x)) \cdots (x - \sigma_n(a)),$$

here $\sigma_1(a) = a$.
These zeros allows us to define n mappings from K to $\mathbb{C}$. Remember that each $x \in K$ can be written as

$$x = d_0 + d_1 a + \cdots + d_{n-1} a^{n-1},$$

where $d_i \in \mathbb{Q}$.
Now we can define

$$\sigma_i(x) = d_0 + d_1 \sigma_i(a) + \cdots + d_{n-1} \sigma_i(a)^{n-1}.$$

Lattices from number fields

So defined mappings satisfy the following conditions.

- The mappings σ_i are $\mathbb{Q}$ algebra embeddings.
- We have $\sigma_i(x+y) = \sigma_i(x) + \sigma_i(y)$.
- And $\sigma_i(xy) = \sigma_i(x)\sigma_i(y)$.

- If $x \in K$, then $\prod_{i=1}^{n} \sigma_i(x) \in \mathbb{Q}$.
- We also have that $\sigma_i(x) = 0$ only if $x = 0$.
- If $x \in R_K$ then $\prod_{i=1}^{n} \sigma_i(x) \in \mathbb{Z}$.

Lattices from number fields

Let us suppose that $\sigma_1, \ldots, \sigma_n$ are the $\mathbb{Q}$-embeddings from K to $\mathbb{C}$. The Minkowski embedding $\psi : K \mapsto M_n(\mathbb{C})$ is then

$$\psi(x) = \mathrm{diag}(\sigma_1(x), \ldots, \sigma_n(x)) \in M_n(\mathbb{C}).$$

- This is really an algebraic representation.
- For example $\psi(xy) = \psi(x)\psi(y)$ and $\psi(x+y) = \psi(x) + \psi(y)$.
- Let us suppose that $x \in K$. As K is a field there exists an element $y \in K$, such that $xy = 1$. It follows that

$$\psi(x)\psi(y) = \psi(xy) = \psi(1_K) = I.$$

Special properties of number field lattices

- All the non-zero matrices in $\psi(K)$ are invertible!

Further

$$\det(\psi(x)) = \prod_{i=1}^{n} \sigma_i(x).$$

- If $x \in K$, then $\det(\psi(x)) \in \mathbb{Q}$.
- If $x \in R_K$, then $\det(\psi(x))) \in \mathbb{Z}$.
- Given $x \in R_K$, $x \neq 0$, then $|\det(\psi(x))| \geq 1$!

Number field lattices

- What can be said about the set $\psi(R_K) \subset M_n(\mathbb{C})$?
- As ψ is a group homomorphism, it must be an additive group.
- Is it a lattice?

- Note that for example $\mathbb{Z} \oplus \sqrt{2}\mathbb{Z}$ is a free group, but not a lattice.

Lattices from number fields

- Remember our inner product $\langle X, Y \rangle = \Re(Tr(XY^\dagger)$.
- Then we have the natural metric $||X - Y||_F = \sqrt{|\langle X - Y, X - Y \rangle|}$.

Lemma

Let A be an $n \times n$ complex matrix. We then have the inequality

$$|\det A| \leq \frac{\|A\|_F^n}{n^{n/2}}.$$

Lattices from number fields

- Let us suppose we have elements $x, y \in R_K$ and $x \neq y$.

We then have that

$$||\psi(x) - \psi(y)||_F = ||\psi(x - y)||_F \geq \sqrt{n}|\det(\psi(X - Y))|^{1/n}.$$

and because $x - y \in R_K$ we have that $|\det(\psi(x - y))| \geq 1$.

- It follows that $||\psi(x) - \psi(y)||_F \geq \sqrt{n}$.
- Hence $\psi(R_K)$ is a discrete additive group in $M_n(\mathbb{C})$.

Hermite invariant of a number field lattice

- We already saw that for any element $x \in \psi(R_K)$ we have that $||x||^2 \leq n$.
- We also know that $||\psi(1_K)||^2 = n$.
- A natural question is now what is the Hermite invariant of R_K and how large it can be.
- We only need no know what is the volume of the fundamental parallelotope of the lattice $\psi(R_K)$.
- It is actually something that can be directly calculated from the minimal polynomial $f_a(x)$.

Lattices from rings of algebraic integers

- The lattice $\psi(R_K)$ has many nice properties and we can measure it's Hermite invariant easily, but we can typically do better.
- Given any $a \in K$ and corresponding $\mathbb{Z}[a] = R_K$, there exists a maximal ring $\mathcal{O}_K$ such that $R_K \subseteq \mathcal{O}_K$.
- The ring of algebraic integers $\mathcal{O}_K$ consist of all the integral elements in K.
- It is obviously unique maximal ring with such properties.

Hermite invariant of number field lattices

- The lattice $\psi(\mathcal{O}_K)$ has all the same properties that $\psi(R_K)$ has.
- For example the shortest vector in $\psi(\mathcal{O}_K)$ has length $\sqrt{n}$.
- However, typically $R_K \subset \mathcal{O}_K$ and $\mathrm{Vol}(\psi(\mathcal{O}_K)) < \mathrm{Vol}(\psi(R_K))$.
- In any case $h(\psi(\mathcal{O}_K)) \geq h(\psi(R_K))$.

Hermite invariant of number field lattices

- Let us simplify things little bit.
- Let us now assume that $K = \mathbb{Q}(a)$ is a *totally real field*.

It means that when

$$f_a(x) = (x - \sigma_1(a))(x - \sigma_2(a)) \cdots (x - \sigma_n(a)),$$

then all $\sigma_i(a) \in \mathbb{R}$.

- Obviously then $\psi(x) \in M_n(\mathbb{R})$ for all $x \in K$.
- The resulting lattice $\psi(\mathcal{O}_K)$ is totally real.

Lattices from number fields

Lemma

Let $K/\mathbb{Q}$ be a totally real extension of degree n and let ψ be the canonical embedding. Then

$$\mathrm{Vol}(\psi(\mathcal{O}_K)) = \sqrt{|d_K|}, \text{ and } \mathrm{h}(\psi(\mathcal{O}_K)) = \frac{n}{|d_K|^{\frac{1}{n}}}.$$

- Here d_K is the discriminant of the field K.
- It is an important algebraic invariant of the field K and has been under deep study for over 100 years.

Lattices from number fields

Now the study of Hermite invariants of number field lattices is reduced to study of discriminants.

- There exists plenty of good lower bounds. (Minkowski and variations of Odlyzko bounds etc)
- Best existence results are based on class field towers.

In the case of totally real fields Martinet proves the existence of a family of fields of degree n, where $n = 2^k$, such that

$$|d_{K_n}|^{\frac{1}{n}} = G_1, \tag{1}$$

where $G_1 \approx 1058$. If K is a degree n field from this family,

$$\mathrm{h}(\psi(\mathcal{O}_K)) = \frac{n}{G_1}. \tag{2}$$

Hermite invariants of number fields

- The actual asymptotic and non-asymptotic size of discriminants is not known.
- For entertainment one finds quite good collection of number fields from: http://www.lmfdb.org/NumberField/

Minimum determinant

- The Hermite invariant question is a general one that is relevant for all lattices.
- How about questions that are specific for number field lattices.

Remember that for any element $x \in \mathcal{O}_K$, $|\det(\psi(x))| \leq 1$.

- Think of your favourite lattice. Does it have this property?
- This is really rare condition.

Minimum determinant

Definition

The *minimum determinant* of the lattice $L \subseteq M_{n\times n}(\mathbb{C})$ is defined as

$$\mathrm{mindet}(L) := \inf_{X\in L\setminus\{\mathbf{0}\}} |\det(X)| .$$

If $\mathrm{mindet}(L) > 0$ we say that the lattice satisfies the *non-vanishing determinant* (NVD) property.

We can now define the *normalized minimum determinant* $\delta(L)$, which is obtained by first scaling the lattice L to have a unit size fundamental parallelotope and then taking the minimum determinant of the resulting scaled lattice.

$$\delta(L) = \frac{\mathrm{mindet}(L)}{(\mathrm{Vol}(L))^{n/k}}. \tag{3}$$

Minimum determinant

For number field lattices we have

$$\delta(\psi(\mathcal{O}_K)) = \frac{1}{\sqrt{|d_K|}}.$$

- The normalized minimum determinants of the number field lattices are greatest known.
- In fact it seem to be that only number fields provide lattices with non-vanishing determinants.

Density of determinant 1 elements

- For typical lattice we can naturally analyse the size of its Hermite invariant.
- Just as well we can ask how many shortest vectors the lattice have.

- How many elements $x \in \psi(\mathcal{O}_K)$ there are with the property $|\det(x)| = 1$?
- Usually there are infinitely many!
- Let us now denote them with $\psi(\mathcal{O}_K)^1$.
- As there are infinitely many of them, we can ask how dense set they are.

Density of determinant 1 elements

- This question is again classical problem in algebraic number theory.
- It is so central because $\psi(\mathcal{O}_K)^1 = \psi(\mathcal{O}_K^*)$, where $\mathcal{O}_K^*$ is the unit group of the ring $\mathcal{O}_K$.
- The unit group consists of all the elements in $\mathcal{O}_K$ who's inverse belongs to $\mathcal{O}_K$ as well.

Density of determinant 1 elements

We will use the notation

$$B(M) = \{X \in M_n(\mathbb{C}) \ : \ ||X||_F \leq M\}$$

for the sphere with radius M.
We are now interested on the asymptotic behaviour of

$$|B(M) \cap \psi(\mathcal{O}_K)^1|,$$

when M grows.

Density of determinant 1 elements

Remember that

$$f_a(x) = (x - \sigma_1(a))(x - \sigma_2(a)) \cdots (x - \sigma_n(a)).$$

Let us denote by r_1 the number of times $\sigma_i(a)$ is real and by $2r_2$ the number of times $\sigma_i(a)$ is complex.

- The pair (r_1, r_2) is called the *signature* of the field K. The signature is independent of the chosen generator a.

A geometric interpretation of the Dirichlet's theorem now gives us

$$|\psi(\mathcal{O}_K)^1 \cap B(M)| \sim c \log(M)^{r_2+r_1-1}, \tag{4}$$

where c is a constant independent of M.

Density of determinant 1 elements

Dirichlet's unit theorem also almost completely defines the group structure of the units $\mathcal{O}_K^*$ of the ring of algebraic integers $\mathcal{O}_K$. It states that

$$\mathcal{O}_K^* \cong U \times \mathbb{Z}^{r_2+r_1-1}, \tag{5}$$

where U is a finite group consisting of the *roots of unity* in the field K. In particular we can see that in some sense the signature of the field describes the "size" of the unit group.

General matrix lattices

- Let us now assume we have any matrix lattice $L \subset M_n(\mathbb{C})$ from a number field.
- It is then a set of invertible (except 0) and commuting matrices.
- We know that there exists a matrix A such that ALA^{-1} consist of diagonal matrices.
- We can see that irrespective of the used number field and representation we are considering a small subset of lattices.
- In particular we know that always $\deg(L) \leq 2n$.

A division algebra

- Let us consider field $\mathbb{Q}[i] = \mathbb{Q} + \mathbb{Q}i$. (minimal polynomial $x^2 + 1$)
- Here σ is the complex conjugation.
- Let u be an auxiliary element that satisfy $u^2 = -1$.

We can then define an algebra H

$$\mathbb{Q}(i) + u\mathbb{Q}(i),$$

where

$$au = u\sigma(a) = u\bar{a}.$$

- This simple condition is enough to calculate all the needed ring operations.
- The resulting $\mathbb{Q}$-algebra is non-commutative.

Quaternion algebra

- Quaternion algebra also has a well known matrix presentation

$$H = \left\{ \begin{pmatrix} a & -b^* \\ b & a^* \end{pmatrix} \mid a, b \in \mathbb{Q}(i) \right\}.$$

Now for example

$$R = \left\{ \begin{pmatrix} a & -b^* \\ b & a^* \end{pmatrix} \mid a, b \in \mathbb{Z}(i) \right\}$$

is a lattice in $M_2(\mathbb{C})$.

- The set R is a ring and also $|\det(X)| \geq 1$, when $X \neq 0$.

Galois group

- Before we can generalize the quaternions we have to give some definitions.

Let us again consider a field K with a generating element a and the minimal polynomial

$$f_a(x) = (x - \sigma_1(a))(x - \sigma_2(a)) \cdots (x - \sigma_n(a)).$$

If now for each i we have that $\mathbb{Q}(\sigma_i(a)) = \mathbb{Q}(a)$, then the corresponding mappings

$$\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma_1, \sigma_2, \ldots, \sigma_n\},$$

form a multiplicative group, with respect to composition.

- If $\mathrm{Gal}(K/\mathbb{Q}) = \{\sigma, \sigma^2, \ldots, \sigma^n\}$, we say that the Galois group is cyclic.

Non-commutative algebra

Definition

Let us assume that $K/\mathbb{Q}$ is a cyclic Galois extension of degree n with the Galois group $Gal(K/\mathbb{Q}) = \langle \sigma \rangle$. We can define an associative $\mathbb{Q}$-algebra

$$\mathcal{A} = (K/\mathbb{Q}, \sigma, \gamma) = K \oplus uK \oplus u^2K \oplus \cdots \oplus u^{n-1}K,$$

where $u \in \mathcal{A}$ is an auxiliary generating element subject to the relations $xu = u\sigma(x)$ for all $x \in K$ and $u^n = \gamma \in \mathbb{Q}^*$. We call this type of algebra *cyclic algebra*

- For example for H we had that $K = \mathbb{Q}(i)$, $u^2 = -1$, and $xu = u\bar{x}$.

Lattices from division algebras

- By selecting the element γ correctly we can assure that $\mathcal{A}$ is a field.
- For each non-zero element $x \in \mathcal{A}$ there exists y such that $xy = 1_{\mathcal{A}}$.

- We now have a more general algebraic structure than a commutative field.
- How can we embed it into suitable euclidean space?

- Remember that $\mathcal{A}$ is a degree n right K-vector space.
- Given any element $x \in \mathcal{A}$, multiplication from left is a linear mapping.
- $x(a+b) = x(a) + x(b)$ $x(a)k = x(ak)$.
- We can see each element of $\mathcal{A}$ as a matrix in $M_n(K)$!

Lattices from division algebras

Suppose that $K/\mathbb{Q}$ is a cyclic extension of algebraic number fields. Let $\mathcal{A} = (K/\mathbb{Q}, \sigma, \gamma)$ be a cyclic division algebra.
We can consider $\mathcal{A}$ as a right vector space over K and every element $x = x_0 + ux_1 + \cdots + u^{n-1}x_{n-1} \in \mathcal{A}$ has the following representation as a matrix $\psi(x) = A$

$$= \begin{pmatrix} x_0 & \gamma\sigma(x_{n-1}) & \gamma\sigma^2(x_{n-2}) & \cdots & \gamma\sigma^{n-1}(x_1) \\ x_1 & \sigma(x_0) & \gamma\sigma^2(x_{n-1}) & & \gamma\sigma^{n-1}(x_2) \\ x_2 & \sigma(x_1) & \sigma^2(x_0) & & \gamma\sigma^{n-1}(x_3) \\ \vdots & & & & \vdots \\ x_{n-1} & \sigma(x_{n-2}) & \sigma^2(x_{n-3}) & \cdots & \sigma^{n-1}(x_0) \end{pmatrix}.$$

Lattices from division algebras

- It is relatively easy to see that for example $\psi(ab) = \psi(a)\psi(b)$ and $\psi(a+b) = \psi(a) + \psi(b)$.
- The set of matrices $\psi(\mathcal{A})$ is an injective *representation* of $\mathcal{A}$.
- It follows that if $\mathcal{A}$ is a division algebra, then $\psi(\mathcal{A})$ consists of invertible matrices.
- Less obviously if $x \in \mathcal{A}$, then $\det(\psi(x)) \in \mathbb{Q}$.

Let us now assume that $u^n = \gamma \in \mathbb{Z}$. Then the ring

$$\mathcal{O}_K[u] = \mathcal{O}_K + u\mathcal{O}_K + \cdots + u^{n-1}\mathcal{O}_K$$

is a promising candidate for a pre-image of a lattice.

Lattices from division algebras

- We can directly see that $\psi(\mathcal{O}_K[u]) \subset M_n(\mathcal{O}_K)$.
- If $x \in \mathcal{O}_K[u]$, then $\det(\psi(x))) \in \mathbb{Z}$
- Given $x \in \mathcal{O}_K[u]$, $x \neq 0$, then $|\det(\psi(x))| \geq 1$!

- Just like previously we can use this information to prove that $\psi(\mathcal{O}_K[u])$ is a lattice.
- It also has shortest vector of length $\sqrt{n}$.
- $\psi(\mathcal{O}_K[u])$ is a subset in $M_n(\mathbb{C})$ and has degree n^2.

Lattices from division algebras

- Just like in the case of number fields, the ring $\mathcal{O}_K[u]$ is always contained into a maximal ring Λ.
- However this ring is not unique. In fact typically a division algebra contains number of maximal orders.

- Again the set $\psi(\Lambda)$ has all the properties that $\psi(\mathcal{O}_K[u])$ has.
- For example the shortest vector in $\psi(\mathcal{O}_K[u])$ has length $\sqrt{n}$.

Lattices from division algebras

Proposition

Let us suppose that we have a $\mathbb{Z}$-order Λ in a $\mathbb{Q}$-central division algebra $\mathcal{A}$ of index n then

$$h(\psi(\Lambda)) = \frac{n}{\mathrm{Vol}(\psi(\Lambda))^{2/n^2}}.$$

Lemma

Suppose that $\mathcal{A}$ is a real division algebra and ψ some cyclic representation. Let Λ be a $\mathbb{Z}$-order inside $\mathcal{A}$. Then

$$\mathrm{Vol}(\psi(\Lambda)) = |\sqrt{d(\Lambda/\mathbb{Z})}|,$$

where $d(\Lambda/\mathbb{Z})$ is *discriminant* of the algebra $\mathcal{A}$.

Maximal Hermite invariant of a division algebra lattice

By real algebra we referred to an algebra where the field K is a subset in $\mathbb{R}$.

- In this case $\psi(\Lambda) \subset M_n(\mathbb{R})$.
- This restriction was done just in order to get as clear result as possible.
- We can now ask how large Hermite invariants maximal orders can have.
- Or equivalently how small discriminants division algebras can have.

Largest possible Hermite invariant

Theorem (V. 2010)

The absolute values of the discriminants of all the $\mathbb{Q}$-central real division algebras of index n are lower bounded by

$$|2 \cdot 3|^{n(n-1)},$$

and this bound can always be achieved.

- This result can be achieved, because we have complete control over discriminants of division algebras.
- This is completely different from the number field case, where discriminant is rather mysterious.

Largest possible Hermite invariant

- We now have that $h(\psi(\Lambda)) \sim \frac{n}{6}$ at best.
- Sounds good. However, this lattice lives in space $M_n(\mathbb{R}) \simeq \mathbb{R}^{n^2}$.
- Hence these are not very dense packings.
- However, these lattices are likely close to optimal in the determinant sense.

Minimum determinant of division algebra lattice

Remember the *minimum determinant* of the lattice $L \subseteq M_{n\times n}(\mathbb{C})$

$$\delta(L) := \frac{\inf_{X\in L\setminus\{\mathbf{0}\}} |\det(X)|}{\mathrm{Vol}(L)^{n/k}}.$$

For every n there exists n^2-dimensional lattice $L_n \subset M_n(\mathbb{R})$, with the property that

$$\delta(L_n) = 6^{\frac{(1-n)}{2}}.$$

- These lattices fill the whole space $M_n(\mathbb{R})$ completely.
- Yet their minimum determinant is 1.
- As far as I know the values of $\delta(L_n)$ are the largest known.

Minimum determinant of division algebra lattices

- The following lattice basis is the optimal 4-dimensional lattice in $M_2(\mathbb{R})$.

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} \sqrt{3} & 0 \\ 0 & -\sqrt{3} \end{pmatrix}, \begin{pmatrix} 0 & -\sqrt{3} \\ -\sqrt{3} & 0 \end{pmatrix},$$

$$\begin{pmatrix} 1/2(1+\sqrt{3}) & 1/2(-1-\sqrt{3} \\ 1/2(1-\sqrt{3}) & 1/2(1-\sqrt{3}) \end{pmatrix}$$

Density of units in orders of division algebras

- How many elements $x \in \psi(\Lambda)$ there are with the property $|\det(x)| = 1$?
- Usually there are infinitely many!
- Let us now denote them with $\psi(\Lambda)^1$.
- As there are infinitely many of them, we can ask how dense set they are.

We are now interested on the asymptotic behaviour of

$$|B(M) \cap \psi(\Lambda)^1|,$$

when M grows.

An example

Let us consider the following division algebras

$$\mathcal{D}_1 = (\mathbb{Q}(i)/\mathbb{Q}, \sigma, -3) \text{ and } \mathcal{D}_2 = (\mathbb{Q}(i)/\mathbb{Q}, \sigma, 3).$$

And their lattices

$$\psi(\Lambda_1) = \left\{ \begin{pmatrix} a & -3b^* \\ b & a^* \end{pmatrix} \mid a, b \in \mathbb{Z}(i) \right\}.$$

and

$$\psi(\Lambda_2) = \left\{ \begin{pmatrix} a & 3b^* \\ b & a^* \end{pmatrix} \mid a, b \in \mathbb{Z}(i) \right\}.$$

An example

$$\det\left(\begin{pmatrix} a & -3b^* \\ b & a^* \end{pmatrix}\right) = |a|^2 + 3|b|^2.$$

$$\det\left(\begin{pmatrix} a & 3b^* \\ b & a^* \end{pmatrix}\right) = |a|^2 - 3|b|^2.$$

We now have

$$|B(M) \cap \psi(\Lambda_1)^1| = \text{constant}.$$

and

$$|B(M) \cap \psi(\Lambda_2)^1| \sim cM^2,$$

for some constant c.

General density of norm 1 elements

The unit group Λ^* of Λ consists of elements $x \in \Lambda$ such that there exists $y \in \Lambda$, for which $xy = 1_{\mathcal{D}}$.
We also have

$$\Lambda^* = \{x \,|x \in \Lambda, |det(\psi(x))| = 1\}.$$

We are now interested on the sets

$$\{\psi(\Lambda^*) \cap B(M)\} = \{x | x \in \Lambda^*, ||\psi(x)|| \leq M\}.$$

- In particular we would like to find such a function f that $|\psi(\Lambda^*) \cap B(M)| \approx f(M)$.

Density of units in division algebras

Definition

Let us suppose that $\mathcal{D}$ is an index n $\mathbb{Q}$-central division algebra. If

$$\mathcal{D} \otimes_{\mathbb{Q}} \mathbb{R} \cong M_n(\mathbb{R}),$$

we say that $\mathcal{D}$ is not ramified at the infinite place. If $2|n$ and

$$\mathcal{D} \otimes_{\mathbb{Q}} \mathbb{R} \cong M_{n/2}(\mathbf{H}),$$

we say that $\mathcal{D}$ is ramified at the infinite place.

- The density of units heavily depend on the used algebra.
- This density is roughly defined by the ramification in the infinite place.

Density of the unit group

Let us suppose that we have an index n $\mathbb{Q}$-central division algebra $\mathcal{D} = (L/\mathbb{Q}, \sigma, \gamma)$ and an order $\Lambda \subset \mathcal{D}$.

Proposition (V., Lu, Luzzi, 2013)

If $\mathcal{D}$ is ramified at the infinite place we have that

$$|\psi(\Lambda^*) \cap B(M)| \approx cM^{n^2-2n},$$

where c is a constant.

Proposition (V., Lu, Luzzi, 2013)

If $\mathcal{D}$ is unramified at the infinite place we have that

$$|\psi(\Lambda^*) \cap B(M)| \approx KM^{n^2-n},$$

where K is a constant.

Structure of the unit group

In algebraic number fields we had that if

$$K \otimes_{\mathbb{Q}} \mathbb{R} \simeq \mathbb{C}^{r_2} \oplus \mathbb{R}^{r_1}.$$

Then the unit group did grow like

$$\log(M)^{r_2+r_1-1}.$$

The same way the structure of

$$\mathcal{A} \otimes_{\mathbb{Q}} \mathbb{R}$$

did define the density of the unit group of the division algebra.

Structure of the unit group

- In general we can find the density of the unit group of a division algebra.
- However, it's algebraic structure is a more or less complete mystery.
- To begin with it's an infinite non-commutative group inside some Lie group.
- This in unlike in the case of number fields, where the unit group had really simple structure.