Alberta Number Theory Days 2017

THE SIZE FUNCTION FOR A NUMBER FIELD

Ha Tran

Department of Mathematics and Statistics
University of Calgary

March 17, 2017

Content

Notations

- Let F be a number field of degree n. For simplicity, assume that F is totally real.

Notations

- Let F be a number field of degree n. For simplicity, assume that F is totally real.
- Let Δ be the discriminant of F.

Notations

- Let F be a number field of degree n. For simplicity, assume that F is totally real.
- Let Δ be the discriminant of F.
- Let O_F be the ring of integers of F.

Notations

- Let F be a number field of degree n. For simplicity, assume that F is totally real.
- Let Δ be the discriminant of F.
- Let O_F be the ring of integers of F.
- Let $\sigma_1, ..., \sigma_n$ be n real embeddings of F.

Notations

- Let F be a number field of degree n. For simplicity, assume that F is totally real.
- Let Δ be the discriminant of F.
- Let O_F be the ring of integers of F.
- Let $\sigma_1, \ldots, \sigma_n$ be n real embeddings of F.
- Denote by $\Phi = (\sigma_1, \ldots, \sigma_n)$. Then

$$\Phi : F \hookrightarrow \mathbb{R}^n \text{ takes } x \in F \text{ to } (\sigma_i(x))_i \in \mathbb{R}^n.$$

Lattices and ideal lattices

- A lattice is a discrete subgroup of an Euclidean space.
  Ex: $\mathbb{Z}^n \subset \mathbb{R}^n$.

Lattices and ideal lattices

- A lattice is a discrete subgroup of an Euclidean space.
  Ex: $\mathbb{Z}^n \subset \mathbb{R}^n$.

Ex: Let $F = \mathbb{Q}(\sqrt{5})$.

Lattices and ideal lattices

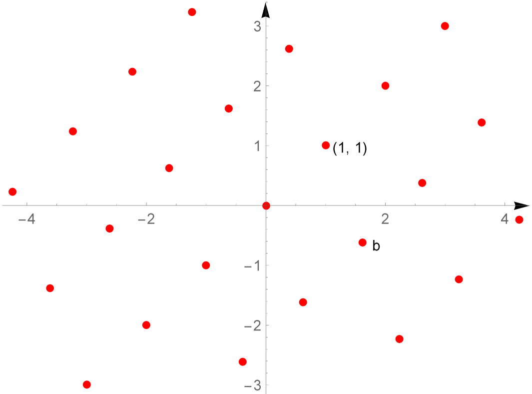
- A lattice is a discrete subgroup of an Euclidean space.
  Ex: $\mathbb{Z}^n \subset \mathbb{R}^n$.

Ex: Let $F = \mathbb{Q}(\sqrt{5})$. What $\Phi(O_F)$ looks like?

Lattices and ideal lattices

- A lattice is a discrete subgroup of an Euclidean space.
  Ex: $\mathbb{Z}^n \subset \mathbb{R}^n$.

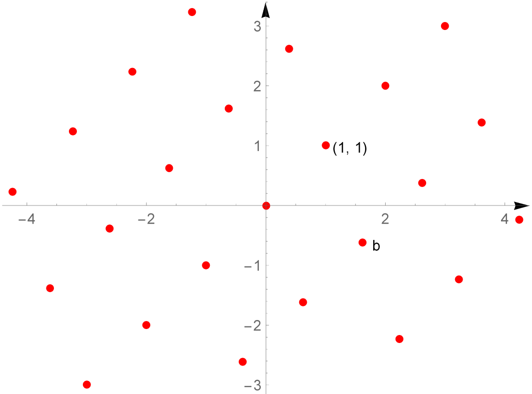
Ex: Let $F = \mathbb{Q}(\sqrt{5})$. What $\Phi(O_F)$ looks like?



Lattices and ideal lattices

- A lattice is a discrete subgroup of an Euclidean space.
  Ex: $\mathbb{Z}^n \subset \mathbb{R}^n$.

Ex: Let $F = \mathbb{Q}(\sqrt{5})$. Then $\Phi(O_F)$ is a lattice in $\mathbb{R}^2$.



Lattices and ideal lattices

- A lattice is a discrete subgroup of an Euclidean space.
  Ex: $\mathbb{Z}^n \subset \mathbb{R}^n$.

Proposition

Let I be a factional ideal of F. Then $\Phi(I)$ is a lattice in $\mathbb{R}^n$.

Ideal lattices

Definition (Ideal lattices)

An ideal lattice is a lattice (I, q), where

- I is a (fractional) O_F-ideal and
- $q : I \times I \longrightarrow \mathbb{R}$ is a non-degenerate symmetric bilinear form st
  $q(\lambda x, y) = q(x, \bar{\lambda} y)$ (Hermitian property)
  for all $x, y \in I$ and for all $\lambda \in O_F$.

Ideal lattices

Definition (Ideal lattices)

An ideal lattice is a lattice (I, q), where

- I is a (fractional) O_F-ideal and
- $q : I \times I \longrightarrow \mathbb{R}$ is a non-degenerate symmetric bilinear form st
  $q(\lambda x, y) = q(x, \bar{\lambda} y)$ (Hermitian property)
  for all $x, y \in I$ and for all $\lambda \in O_F$.

Let I be a factional ideal of F and let $u = (u_i)_i \in (\mathbb{R}_{>0})^n$.

Ideal lattices

Definition (Ideal lattices)

An ideal lattice is a lattice (I, q), where

- I is a (fractional) O_F-ideal and
- $q : I \times I \longrightarrow \mathbb{R}$ is a non-degenerate symmetric bilinear form st
  $q(\lambda x, y) = q(x, \bar{\lambda} y)$ (Hermitian property)
  for all $x, y \in I$ and for all $\lambda \in O_F$.

Let I be a factional ideal of F and let $u = (u_i)_i \in (\mathbb{R}_{>0})^n$.
Define $q_u(x, y) = \langle u\Phi(x), u\Phi(y)\rangle$ for any $x, y \in I$.

$$\|x\|_u^2 = q_u(x, x) = \|u\Phi(x)\|^2 = \sum_{i=1}^{n} u_i^2[\sigma_i(x)]^2.$$

Ideal lattices

Definition (Ideal lattices)

An ideal lattice is a lattice (I, q), where

- I is a (fractional) O_F-ideal and
- $q : I \times I \longrightarrow \mathbb{R}$ is a non-degenerate symmetric bilinear form st
  $q(\lambda x, y) = q(x, \bar{\lambda} y)$ (Hermitian property)
  for all $x, y \in I$ and for all $\lambda \in O_F$.

Let I be a factional ideal of F and let $u = (u_i)_i \in (\mathbb{R}_{>0})^n$.
Define $q_u(x, y) = \langle u\Phi(x), u\Phi(y)\rangle$ for any $x, y \in I$.

$$\|x\|_u^2 = q_u(x, x) = \|u\Phi(x)\|^2 = \sum_{i=1}^{n} u_i^2 [\sigma_i(x)]^2.$$

Then (I, q_u) is an ideal lattice.

The size function for lattices

Let L be a lattice of $\mathbb{R}^n$.

$$h^0(L) := \log \sum_{x \in L} e^{-\pi \|x\|^2}.$$

The size function for a number field

Similarly, h^0 is defined for the ideal lattice (I, q_u).

$$h^0(I, q_u) = \log \sum_{x \in I} e^{-\pi \|x\|_u^2}.$$

The size function for a number field

Similarly, h^0 is defined for the ideal lattice (I, q_u).

$$h^0(I, q_u) = \log \sum_{x \in I} e^{-\pi \|x\|_u^2}.$$

Definition

- The pair $D = (I, u)$ is also called an Arakelov divisor of F.

The size function for a number field

Similarly, h^0 is defined for the ideal lattice (I, q_u).

$$h^0(I, q_u) = \log \sum_{x \in I} e^{-\pi \|x\|_u^2}.$$

Definition

- The pair $D = (I, u)$ is also called an Arakelov divisor of F.
- (I, q_u) is also called the ideal lattice associated to D.

The size function for a number field

Similarly, h^0 is defined for the ideal lattice (I, q_u).

$$h^0(I, q_u) = \log \sum_{x \in I} e^{-\pi \|x\|_u^2}.$$

Definition

- The pair $D = (I, u)$ is also called an Arakelov divisor of F.
- (I, q_u) is also called the ideal lattice associated to D.
- $h^0(D) := h^0(I, q_u)$.

Analogies

Algebraic curve

- Divisor.

Number field F

- Arakelov divisor.

Analogies

Algebraic curve

- Divisor.
- Principal divisor.

Number field F

- Arakelov divisor.
- Principal Arakelov divisor.

Analogies

Algebraic curve

- Divisor.
- Principal divisor.
- Picard group.

Number field F

- Arakelov divisor.
- Principal Arakelov divisor.
- Arakelov class group Pic_F^0.

Analogies

Algebraic curve

- Divisor.
- Principal divisor.
- Picard group.
- Canonical divisor κ.

Number field F

- Arakelov divisor.
- Principal Arakelov divisor.
- Arakelov class group Pic_F^0.
- The inverse different.

Analogies

Algebraic curve

- Divisor.
- Principal divisor.
- Picard group.
- Canonical divisor κ.
- Riemann–Roch theorem

Number field F

- Arakelov divisor.
- Principal Arakelov divisor.
- Arakelov class group Pic_F^0.
- The inverse different.
- Riemann–Roch theorem.

Analogies

Algebraic curve

- Divisor.
- Principal divisor.
- Picard group.
- Canonical divisor κ.
- Riemann–Roch theorem
- $h^0(D)$.

Number field F

- Arakelov divisor.
- Principal Arakelov divisor.
- Arakelov class group Pic_F^0.
- The inverse different.
- Riemann–Roch theorem.
- $h^0(D)$

Analogies

Algebraic curve

- Divisor.
- Principal divisor.
- Picard group.
- Canonical divisor κ.
- Riemann–Roch theorem
- $h^0(D)$.
- ...

Number field F

- Arakelov divisor.
- Principal Arakelov divisor.
- Arakelov class group Pic^0_F.
- The inverse different.
- Riemann–Roch theorem.
- $h^0(D)$
- ...

Analogies

Algebraic curve

- Divisor.
- Principal divisor.
- Picard group.
- Canonical divisor κ.
- Riemann–Roch theorem
- $h^0(D)$.
- ...

Number field F

- Arakelov divisor.
- Principal Arakelov divisor.
- Arakelov class group Pic_F^0.
- The inverse different.
- Riemann–Roch theorem.
- $h^0(D)$ the size function of F.
- ...

The Riemann-Roch Theorem

For an algebraic curve

$$h^0(D) - h^0(\kappa - D) = deg(D) - (g - 1).$$

The Riemann-Roch Theorem

For an algebraic curve

$$h^0(D) - h^0(\kappa - D) = deg(D) - (g - 1).$$

We define the canonical Arakelov divisor κ to be the Arakelov divisor $(\partial, 1)$ whose ideal part is the inverse of the different ∂ of F.

The Riemann-Roch Theorem

For an algebraic curve

$$h^0(D) - h^0(\kappa - D) = deg(D) - (g - 1).$$

We define the canonical Arakelov divisor κ to be the Arakelov divisor $(\partial, 1)$ whose ideal part is the inverse of the different ∂ of F.

van der Geer and Schoof (1999)

Let F be a number field with discriminant Δ and let D be an Arakelov divisor. Then

$$h^0(D) - h^0(\kappa - D) = \deg(D) - \frac{1}{2}\log|\Delta|.$$

The Arakelov class group Pic_F^0

- Let $D = (I, u)$. Then $deg(D) := -\log(\mathrm{covol}(I, q_u))$.

The Arakelov class group Pic_F^0

- Let $D = (I, u)$. Then $deg(D) := -\log(\mathrm{covol}(I, q_u))$.
- The set of all Arakelov divisors of degree 0 form a group, denoted by Div_F^0.

The Arakelov class group Pic_F^0

- Let $D = (I, u)$. Then $deg(D) := -\log(\mathrm{covol}(I, q_u))$.
- The set of all Arakelov divisors of degree 0 form a group, denoted by Div_F^0.
- A principal Arakelov divisor has the form (I, u) where $I = x^{-1}O_F$ and $u = |\Phi(x)| = (|\sigma_i(x)|)_i$ and $x \in F^\times$.

The Arakelov class group Pic_F^0

- Let $D = (I, u)$. Then $deg(D) := -\log(\mathrm{covol}(I, q_u))$.
- The set of all Arakelov divisors of degree 0 form a group, denoted by Div_F^0.
- A principal Arakelov divisor has the form (I, u) where $I = x^{-1}O_F$ and $u = |\Phi(x)| = (|\sigma_i(x)|)_i$ and $x \in F^\times$.
- The Arakelov class group Pic_F^0 is the quotient of Div_F^0 by its subgroup of principal divisors.

The Arakelov class group Pic_F^0

- Let $D = (I, u)$. Then $deg(D) := -\log(\mathrm{covol}(I, q_u))$.
- The set of all Arakelov divisors of degree 0 form a group, denoted by Div_F^0.
- A principal Arakelov divisor has the form (I, u) where $I = x^{-1}O_F$ and $u = |\Phi(x)| = (|\sigma_i(x)|)_i$ and $x \in F^\times$.
- The Arakelov class group Pic_F^0 is the quotient of Div_F^0 by its subgroup of principal divisors.

Proposition

$$\mathrm{Pic}_F^0 \longrightarrow \{\text{isometry classes of ideal lattices of covolume } \sqrt{\Delta}\}$$
$$\text{the class of } D = (I, u) \longmapsto \text{ the isometry class of } (I, q_u)$$
is a bijection.

The Arakelov class group Pic_F^0

- Let $D = (I, u)$. Then $deg(D) := -\log(\mathrm{covol}(I, q_u))$.
- The set of all Arakelov divisors of degree 0 form a group, denoted by Div_F^0.
- A principal Arakelov divisor has the form (I, u) where $I = x^{-1}O_F$ and $u = |\Phi(x)| = (|\sigma_i(x)|)_i$ and $x \in F^\times$.
- The Arakelov class group Pic_F^0 is the quotient of Div_F^0 by its subgroup of principal divisors.

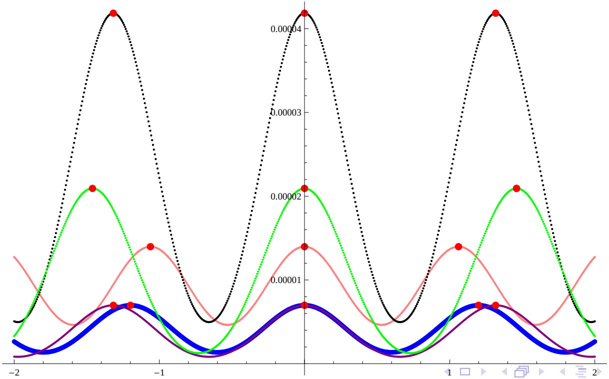
Proposition

$\mathrm{Pic}_F^0 \longrightarrow \{\text{isometry classes of ideal lattices of covolume } \sqrt{\Delta}\}$
the class of $D = (I, u) \longmapsto$ the isometry class of (I, q_u)
is a bijection.

Note: h^0 is well defined on Pic_F^0.

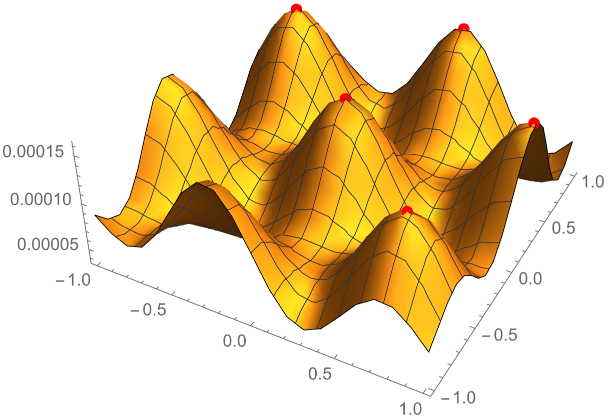
The conjecture of van der Geer and Schoof

Let F be a real quadratic field (Galois over $\mathbb{Q}$) or quadratic extension of a complex quadratic field K (Galois over K). The origin is the divisor $(O_F, 1)$.



The conjecture of van der Geer and Schoof

A cyclic cubic field (Galois over $\mathbb{Q}$).
The origin is the divisor $(O_F, 1)$.



The conjecture of van der Geer and Schoof

Conjecture. Let F be a number field that is Galois over $\mathbb{Q}$ or over an imaginary quadratic field. Then the function h^0 on Pic_F^0 assumes its maximum on the trivial class $(O_F, 1)$.

The conjecture of van der Geer and Schoof

Conjecture. Let F be a number field that is Galois over $\mathbb{Q}$ or over an imaginary quadratic field. Then the function h^0 on Pic_F^0 assumes its maximum on the trivial class $(O_F, 1)$.

Results. The conjecture is proved for number fields of degree:

- $n = 2$: Francini (2001).
- $n = 3$: Francini (2004) - For some certain pure cubic fields.
- $n = 4$: (2014) For quadratic extensions of imaginary quadratic fields.
- $n = 3$: (2016) For cyclic cubic fields.

References

Paolo Francini.
The size function h^0 for quadratic number fields.
J. Théor. Nombres Bordeaux, 13(1):125–135, 2001.
21st Journées Arithmétiques (Rome, 2001).

Paolo Francini.
The size function h° for a pure cubic field.
Acta Arith., 111(3):225–237, 2004.

Richard P. Groenewegen.
The size function for number fields.
Doctoraalscriptie, Universiteit van Amsterdam, 1999.

René Schoof.
Computing Arakelov class groups.
In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 447–495. Cambridge Univ. Press, Cambridge, 2008.

Gerard van der Geer and René Schoof.
Effectivity of Arakelov divisors and the theta divisor of a number field.
Selecta Math. (N.S.), 6(4):377–398, 2000.