LATTICES IN NUMBER THEORY

Ha Tran

ICTP–CIMPA summer school 2016
HCM University of Science– Saigon University

Lattices in Number Theory

We will study ideal lattices.

- They are lattices with structure of ideals.
- They are used in coding theory and cryptography.
- They have nice algebraic structure (so have nice and cheap representation, allows fast arithmetic,....)

Lattices in Number Theory

We will

1. Review about number fields, ideal lattices and ...
   Study Arakelov divisors.
2. Study the Arakelov class group.
3. Discuss about reduced Arakelov divisors and their properties.
   Discuss the reduction algorithm.

Lattices in Number Theory

We will

1. Review about number fields, ideal lattices and ...
   Study Arakelov divisors.
2. Study the Arakelov class group.
3. Discuss about reduced Arakelov divisors and their properties.
   Discuss the reduction algorithm.

PS: Questions are very welcome :)

ICTP–CIMPA summer school 2016

Lecture 1.
NUMBER FIELDS AND ...

HCM University of Science– Saigon University

Content

1. Review
   - Number fields and the ring of integers
   - Fractional ideals
   - The class group
   - $F_{\mathbb{R}}$
   - The Φ map
   - The L map
2. Ideal lattices

Review

Let F be a number field of degree n.

1. $F = \mathbb{Q}$,
2. $F = \mathbb{Q}(\sqrt{2})$,
3. $F = \mathbb{Q}(i)$ (the Gaussian field),
4. $F = \mathbb{Q}(\sqrt{5})$,
5. F is the splitting field of $x^3 + mx^2 - (m+3)x + 1$ ($m \geq -1, m \not\equiv 3 \mod 9$) (simplest cubic field),
6. $F = \mathbb{Q}(\sqrt[4]{2})$?
7. $F = \mathbb{Q}(\zeta_m)$ (cyclotomic field)?

Review

Let F be a number field of degree n.

$\sigma_1, \ldots, \sigma_{r_1}$ are r_1 real infinite primes

$\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}$ are r_2 complex infinite primes.

1. $F = \mathbb{Q}$,
2. $F = \mathbb{Q}(\sqrt{2})$,
3. $F = \mathbb{Q}(i)$ (the Gaussian field),
4. $F = \mathbb{Q}(\sqrt{5})$,
5. F is the splitting field of $x^3 + mx^2 - (m+3)x + 1$ ($m \geq -1, m \not\equiv 3 \mod 9$) (simplest cubic field),
6. $F = \mathbb{Q}(\sqrt[4]{2})$?
7. $F = \mathbb{Q}(\zeta_m)$ (cyclotomic field)?

Review

Let F be a number field of degree n.

$\sigma_1, \ldots, \sigma_{r_1}$ are r_1 real infinite primes

$\sigma_{r_1+1}, \ldots, \sigma_{r_1+r_2}$ are r_2 complex infinite primes.

O_F: The ring of integers of F $(n = r_1 + 2r_2)$.

1. $F = \mathbb{Q}$,
2. $F = \mathbb{Q}(\sqrt{2})$,
3. $F = \mathbb{Q}(i)$ (the Gaussian field),
4. $F = \mathbb{Q}(\sqrt{5})$,
5. F is the splitting field of $x^3 + mx^2 - (m+3)x + 1$ $(m \geq -1, m \not\equiv 3 \mod 9)$ (simplest cubic field),
6. $F = \mathbb{Q}(\sqrt[4]{2})$?
7. $F = \mathbb{Q}(\zeta_m)$ (cyclotomic field)?

Fractional ideals

I is called a fractional ideal of F if

- I is an additive subgroup of F, and
- there exists $\alpha \in F^\times$ st αI is an ideal of O_F.

Fractional ideals

I is called a fractional ideal of F if

- I is an additive subgroup of F, and
- there exists $\alpha \in F^{\times}$ st αI is an ideal of O_F.

Ex: $F = \mathbb{Q}(\sqrt{5})$. I_i is a factional ideal of F?

1. $I_1 = \{m_1 + \sqrt{2}m_2 : m_1, m_2 \in \mathbb{Z}\}$?

Fractional ideals

I is called a fractional ideal of F if

- I is an additive subgroup of F, and
- there exists $\alpha \in F^\times$ st αI is an ideal of O_F.

Ex: $F = \mathbb{Q}(\sqrt{5})$. I_i is a factional ideal of F?

2. $I_2 = \{m_1 + \frac{1+\sqrt{5}}{2} m_2 : m_1, m_2 \in \mathbb{Z}\}$?

Fractional ideals

I is called a fractional ideal of F if

- I is an additive subgroup of F, and
- there exists $\alpha \in F^\times$ st αI is an ideal of O_F.

Ex: $F = \mathbb{Q}(\sqrt{5})$. I_i is a factional ideal of F?

2. $I_2 = \{m_1 + \frac{1+\sqrt{5}}{2} m_2 : m_1, m_2 \in \mathbb{Z}\}$?
3. $I_3 = \{m_1 + \frac{2}{1+\sqrt{5}} m_2 : m_1, m_2 \in \mathbb{Z}\}$?

Fractional ideals

I is called a fractional ideal of F if

- I is an additive subgroup of F, and
- there exists $\alpha \in F^\times$ st αI is an ideal of O_F.

Ex: $F = \mathbb{Q}(\sqrt{5})$. I_i is a factional ideal of F?

4. $I_4 = \{2m_1 + (1-\sqrt{5})m_2 : m_1, m_2 \in \mathbb{Z}\}$?

Fractional ideals

I is called a fractional ideal of F if

- I is an additive subgroup of F, and
- there exists $\alpha \in F^\times$ st αI is an ideal of O_F.

Ex: $F = \mathbb{Q}(\sqrt{5})$. I_i is a factional ideal of F?

4. $I_4 = \{2m_1 + (1-\sqrt{5})m_2 : m_1, m_2 \in \mathbb{Z}\}$?
5. $I_5 = \{\frac{1}{2}m_1 + \frac{1-\sqrt{5}}{4}m_2 : m_1, m_2 \in \mathbb{Z}\}$?

Fractional ideals

I is called a fractional ideal of F if

- I is an additive subgroup of F, and
- there exists $\alpha \in F^\times$ st αI is an ideal of O_F.

Ex: $F = \mathbb{Q}(\sqrt{5})$. I_i is a factional ideal of F?

4. $I_4 = \{2m_1 + (1-\sqrt{5})m_2 : m_1, m_2 \in \mathbb{Z}\}$?
5. $I_5 = \{\frac{1}{2}m_1 + \frac{1-\sqrt{5}}{4}m_2 : m_1, m_2 \in \mathbb{Z}\}$?
6. $I_6 = \{\frac{\sqrt{5}}{5}m_1 + \frac{5-\sqrt{5}}{10}m_2 : m_1, m_2 \in \mathbb{Z}\}$? $= \frac{1}{2\sqrt{5}}I_4$.

The class group

Id_F: The group of all fractional ideals of F with multiplication.
Let $Princ_F :=$ the subgroup of principal ideals of F.
The class group of F is

$$Cl_F = Id_F / Princ_F.$$

The class group

Id_F: The group of all fractional ideals of F with multiplication.
Let $Princ_F :=$ the subgroup of principal ideals of F.
The class group of F is

$$Cl_F = Id_F / Princ_F.$$

- Cl_F is finite and $\# Cl_F = h_F$ (the class number).

The class group

Id_F: The group of all fractional ideals of F with multiplication.
Let $Princ_F :=$ the subgroup of principal ideals of F.
The class group of F is

$$Cl_F = Id_F / Princ_F.$$

- Cl_F is finite and $\# Cl_F = h_F$ (the class number).

Ex: $Cl_F = ?, h_F = ?$ if

1. $F = \mathbb{Q}$.
2. $F = \mathbb{Q}(\sqrt{2})$.
3. $F = \mathbb{Q}(i)$.
4. $F = \mathbb{Q}(\sqrt{10})$.

$F_{\mathbb{R}}$

- Let $F_{\mathbb{R}} := F \otimes_{\mathbb{Q}} \mathbb{R} \simeq \prod_{\sigma \text{ real}} \mathbb{R} \times \prod_{\sigma \text{ complex}} \mathbb{C} \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ an $\mathbb{R}$-algebra.

Ex: $F_{\mathbb{R}} = ?$ if

1. $F = \mathbb{Q}$,
2. $F = \mathbb{Q}(\sqrt{2})$,
3. $F = \mathbb{Q}(i)$,
4. $F = \mathbb{Q}(\sqrt{5})$,
5. F is a simplest cubic field,
6. $F = \mathbb{Q}(\sqrt[4]{2})$,
7. $F = \mathbb{Q}(\zeta_m)$ (cyclotomic field)?

$F_{\mathbb{R}}$

- Let $F_{\mathbb{R}} := F \otimes_{\mathbb{Q}} \mathbb{R} \simeq \prod_{\sigma \text{ real}} \mathbb{R} \times \prod_{\sigma \text{ complex}} \mathbb{C} \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ an $\mathbb{R}$-algebra.

$F_{\mathbb{R}}$

- Let $F_{\mathbb{R}} := F \otimes_{\mathbb{Q}} \mathbb{R} \simeq \prod_{\sigma \text{ real}} \mathbb{R} \times \prod_{\sigma \text{ complex}} \mathbb{C} \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ an $\mathbb{R}$-algebra.
- A scalar product on $F_{\mathbb{R}}$, for any $u = (u_\sigma), v = (v_\sigma) \in F_{\mathbb{R}}$,
  $\langle u, v \rangle := Tr(u\overline{v})$

$$= \sum_{\sigma \text{ real}} Re(u_\sigma \overline{v_\sigma}) + 2 \sum_{\sigma \text{ complex}} Re(u_\sigma \overline{v_\sigma}).$$

$\Rightarrow \|u\|^2 = \sum_{\sigma \text{ real}} u_\sigma^2 + 2 \sum_{\sigma \text{ complex}} |u_\sigma|^2.$

$F_{\mathbb{R}}$

- Let $F_{\mathbb{R}} := F \otimes_{\mathbb{Q}} \mathbb{R} \simeq \prod_{\sigma \text{ real}} \mathbb{R} \times \prod_{\sigma \text{ complex}} \mathbb{C} \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ an $\mathbb{R}$-algebra.
- A scalar product on $F_{\mathbb{R}}$, for any $u = (u_\sigma), v = (v_\sigma) \in F_{\mathbb{R}}$,
  $\langle u, v \rangle := Tr(u\overline{v})$
$$= \sum_{\sigma \text{ real}} Re(u_\sigma \overline{v_\sigma}) + 2 \sum_{\sigma \text{ complex}} Re(u_\sigma \overline{v_\sigma}).$$
$$\Rightarrow \|u\|^2 = \sum_{\sigma \text{ real}} u_\sigma^2 + 2 \sum_{\sigma \text{ complex}} |u_\sigma|^2.$$

Ex: $F = \mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(i), \mathbb{Q}(\sqrt{5})$,
simplest cubic fields,
$F = \mathbb{Q}(\sqrt[4]{2})$?

$F_{\mathbb{R}}$

- Let $F_{\mathbb{R}} := F \otimes_{\mathbb{Q}} \mathbb{R} \simeq \prod_{\sigma \text{ real}} \mathbb{R} \times \prod_{\sigma \text{ complex}} \mathbb{C} \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ an $\mathbb{R}$-algebra.

$$\Rightarrow \|u\|^2 = \sum_{\sigma \text{ real}} u_\sigma^2 + 2 \sum_{\sigma \text{ complex}} |u_\sigma|^2.$$

$F_{\mathbb{R}}$

- Let $F_{\mathbb{R}} := F \otimes_{\mathbb{Q}} \mathbb{R} \simeq \prod_{\sigma \text{ real}} \mathbb{R} \times \prod_{\sigma \text{ complex}} \mathbb{C} \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ an $\mathbb{R}$-algebra.

$$\Rightarrow \|u\|^2 = \sum_{\sigma \text{ real}} u_\sigma^2 + 2 \sum_{\sigma \text{ complex}} |u_\sigma|^2.$$

- $N(u) := \prod_{\sigma \text{ real}} u_\sigma \times \prod_{\sigma \text{ complex}} |u_\sigma|^2$.

$F_{\mathbb{R}}$

- Let $F_{\mathbb{R}} := F \otimes_{\mathbb{Q}} \mathbb{R} \simeq \prod_{\sigma \text{ real}} \mathbb{R} \times \prod_{\sigma \text{ complex}} \mathbb{C} \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ an $\mathbb{R}$-algebra.

$$\Rightarrow \|u\|^2 = \sum_{\sigma \text{ real}} u_\sigma^2 + 2 \sum_{\sigma \text{ complex}} |u_\sigma|^2.$$

- $N(u) := \prod_{\sigma \text{ real}} u_\sigma \times \prod_{\sigma \text{ complex}} |u_\sigma|^2$.

Ex: $F = \mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(i), \mathbb{Q}(\sqrt{5})$,
simplest cubic fields,
$F = \mathbb{Q}(\sqrt[4]{2})$?

The Φ map

Let $\Phi : F \longrightarrow F_{\mathbb{R}}$ with $\Phi(f) = (\sigma_1(f), \ldots, \sigma_{r_1+r_2}(f))$ for $f \in F$.

Ex: $\Phi =?$ if

1. $F = \mathbb{Q}$,
2. $F = \mathbb{Q}(\sqrt{2})$,
3. $F = \mathbb{Q}(i)$,
4. $F = \mathbb{Q}(\sqrt{5})$,
5. F is a simplest cubic field,
6. $F = \mathbb{Q}(\sqrt[4]{2})$?

Lattices

Definition (Lattices)

A lattice is a pair (L, q) where

- L is a free $\mathbb{Z}$-module of finite rank, and
- $q : L \times L \longrightarrow \mathbb{R}$ is a non-degenerate symmetric bilinear form.

Lattices

Definition (Lattices)

A lattice is a pair (L, q) where

- L is a free $\mathbb{Z}$-module of finite rank, and
- $q : L \times L \longrightarrow \mathbb{R}$ is a non-degenerate symmetric bilinear form.

Ex: $L = \mathbb{Z}^n$ with the standard metric inherited from $\mathbb{R}^n$ is a lattice.

Lattices

Definition (Lattices)

A lattice is a pair (L, q) where

- L is a free $\mathbb{Z}$-module of finite rank, and
- $q : L \times L \longrightarrow \mathbb{R}$ is a non-degenerate symmetric bilinear form.

Ex: $L = \mathbb{Z}^n$ with the standard metric inherited from $\mathbb{R}^n$ is a lattice.
Ex: Let $F = \mathbb{Q}(\sqrt{5})$. Then $\Phi(O_F)$ is a lattice in $F_{\mathbb{R}} \simeq \mathbb{R}^2$.

The Φ map

Let $\Phi : F \longrightarrow F_{\mathbb{R}}$ with $\Phi(f) = (\sigma_1(f), ..., \sigma_{r_1+r_2}(f))$ for $f \in F$.

The Φ map

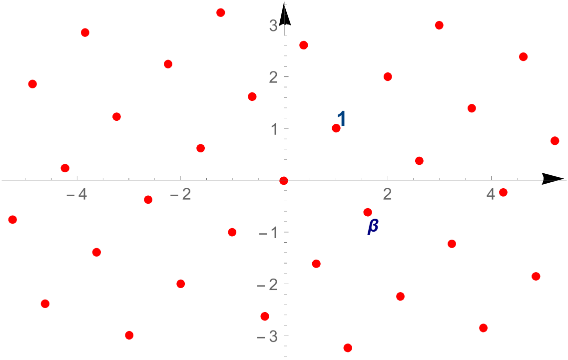
Let $\Phi : F \longrightarrow F_{\mathbb{R}}$ with $\Phi(f) = (\sigma_1(f), ..., \sigma_{r_1+r_2}(f))$ for $f \in F$.

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

The Φ map

Let $\Phi : F \longrightarrow F_{\mathbb{R}}$ with $\Phi(f) = (\sigma_1(f), ..., \sigma_{r_1+r_2}(f))$ for $f \in F$.

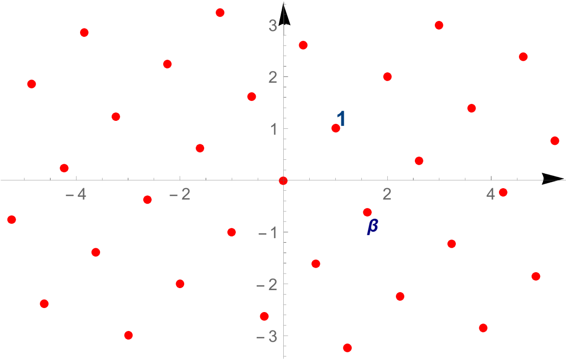
Ex: Let $F = \mathbb{Q}(\sqrt{5})$. What $\Phi(O_F)$ looks like?



The Φ map

Let $\Phi : F \longrightarrow F_{\mathbb{R}}$ with $\Phi(f) = (\sigma_1(f), \ldots, \sigma_{r_1+r_2}(f))$ for $f \in F$.

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



$\Phi(O_F)$ is a lattice in $F_{\mathbb{R}}$.

The Φ map and the images of fractional ideals

Let $\Phi : F \longrightarrow F_{\mathbb{R}}$ with $\Phi(f) = (\sigma_1(f), ..., \sigma_{r_1+r_2}(f))$ for $f \in F$.

Ex: Let $F = \mathbb{Q}(\sqrt{5})$ and $I_5 = \{\frac{1}{2}m_1 + \frac{1-\sqrt{5}}{4}m_2 : m_1, m_2 \in \mathbb{Z}\}$: a fractional ideal of F.

What $\Phi(I)$ looks like?

The Φ map and the images of fractional ideals

Let $\Phi : F \longrightarrow F_{\mathbb{R}}$ with $\Phi(f) = (\sigma_1(f), ..., \sigma_{r_1+r_2}(f))$ for $f \in F$.

Ex: Let $F = \mathbb{Q}(\sqrt{5})$ and $I_5 = \{\frac{1}{2}m_1 + \frac{1-\sqrt{5}}{4}m_2 : m_1, m_2 \in \mathbb{Z}\}$: a fractional ideal of F.

What $\Phi(I)$ looks like?

Proposition

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

The Φ map and the images of fractional ideals

Let $\Phi : F \longrightarrow F_{\mathbb{R}}$ with $\Phi(f) = (\sigma_1(f), ..., \sigma_{r_1+r_2}(f))$ for $f \in F$.

Ex: Let $F = \mathbb{Q}(\sqrt{5})$ and $I_5 = \{\frac{1}{2}m_1 + \frac{1-\sqrt{5}}{4}m_2 : m_1, m_2 \in \mathbb{Z}\}$: a fractional ideal of F.

What $\Phi(I)$ looks like?

Proposition

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

Ex: Draw the lattice $\Phi(I_5)$.

The L map

Consider to the map

$$L : F^\times \longrightarrow F_{\mathbb{R}} \text{ where } L(f) = (\log(|\sigma(f)|))_\sigma.$$

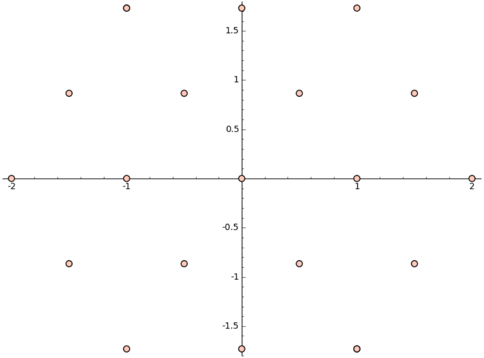
Ex: F is the splitting field of $x^3 - x^2 - 2x + 1$ (simplest cubic field). The roots: $\alpha_1 = \alpha, \alpha_2 = \frac{1}{1-\alpha}, \alpha_3 = 1 - \frac{1}{\alpha}$. Then

$$O_F^\times =< \pm 1, \alpha_1, \alpha_2 > .$$

What $L(O_F^\times)$ looks like?

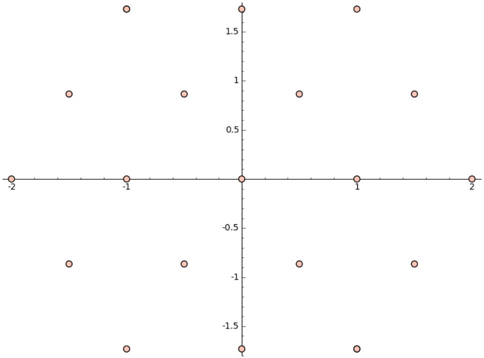
The L map

Ex: F is the splitting field of $x^3 - x^2 - 2x + 1$. The roots: $\alpha_1 = \alpha, \alpha_2 = \frac{1}{1-\alpha}, \alpha_3 = 1 - \frac{1}{\alpha}$. Then $O_F^\times = < \pm 1, \alpha_1, \alpha_2 >$.



The L map

Ex: F is the splitting field of $x^3 - x^2 - 2x + 1$. The roots: $\alpha_1 = \alpha, \alpha_2 = \frac{1}{1-\alpha}, \alpha_3 = 1 - \frac{1}{\alpha}$. Then $O_F^\times =< \pm 1, \alpha_1, \alpha_2 >$.



$L(O_F^\times)$ is the hexagonal lattice.

The L map

$$\Lambda := L(O_F^\times) = \{L(x) : x \in O_F^\times\} \subset H.$$

The L map

$$\Lambda := L(O_F^\times) = \{L(x) : x \in O_F^\times\} \subset H.$$

The L map

$$\Lambda := L(O_F^\times) = \{L(x) : x \in O_F^\times\} \subset H.$$

$$H = \left\{ (x_\sigma) \in \oplus_\sigma \mathbb{R} : \sum_{\sigma \text{ real}} x_\sigma + 2 \sum_{\sigma \text{ complex}} x_\sigma = 0 \right\}.$$

The L map

$$\Lambda := L(O_F^\times) = \{L(x) : x \in O_F^\times\} \subset H.$$

$$H = \left\{ (x_\sigma) \in \oplus_\sigma \mathbb{R} : \sum_{\sigma \text{ real}} x_\sigma + 2 \sum_{\sigma \text{ complex}} x_\sigma = 0 \right\}.$$

Λ is a lattice contained in the vector space H.

The L map

$$\Lambda := L(O_F^\times) = \{L(x) : x \in O_F^\times\} \subset H.$$

$$H = \left\{ (x_\sigma) \in \oplus_\sigma \mathbb{R} : \sum_{\sigma \text{ real}} x_\sigma + 2 \sum_{\sigma \text{ complex}} x_\sigma = 0 \right\}.$$

Λ is a lattice contained in the vector space H.

Let $T^0 = H/\Lambda$. Then T^0 is a compact real torus of dimension $r_1 + r_2 - 1$ (Dirichlet).

T^0 and $\Lambda = L(O_F^\times)$

Ex: Let $F = \mathbb{Q}(\sqrt{-2})$. Then $r_1 = 0, r_2 = 1$ and
$T^0 =?$ $\quad dim(T^0) =?$

T^0 and $\Lambda = L(O_F^\times)$

Ex: Let $F = \mathbb{Q}(\sqrt{2})$. Then $r_1 = 2, r_2 = 0$ and

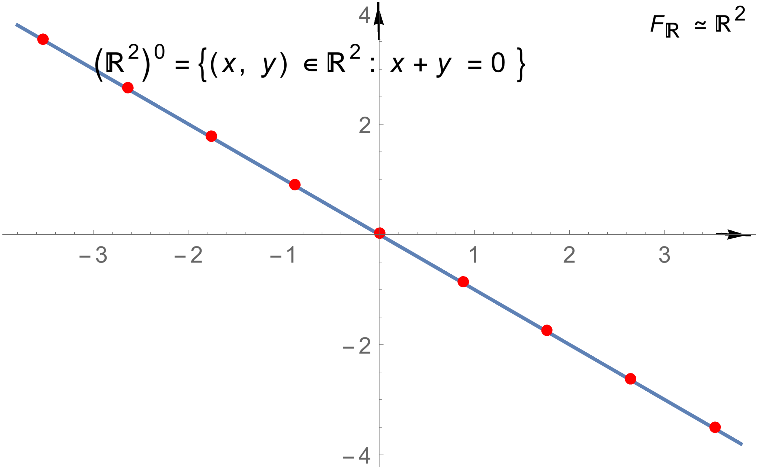
$$H = \{(x, y) \in \mathbb{R}^2 : x + y = 0\} \simeq \mathbb{R}.$$

$T^0 =?$ $\qquad dim(T^0) =?$

T^0 and $\Lambda = L(O_F^\times)$

Ex: Let $F = \mathbb{Q}(\sqrt{2})$. Then $r_1 = 2, r_2 = 0$ and

$$H = \{(x, y) \in \mathbb{R}^2 : x + y = 0\} \simeq \mathbb{R}.$$



T^0 and $\Lambda = L(O_F^\times)$

Ex: Let F be a totally real cubic field. Then $r_1 = 3, r_2 = 0$ and

$$H = \{(x, y, z) \in \mathbb{R}^3 : x + y + z = 0\} \simeq \mathbb{R}^2.$$

$T^0 =?$ $\qquad$ $dim(T^0) =?$

T^0 and $\Lambda = L(O_F^\times)$

Ex: Let F be a totally real cubic field. Then $r_1 = 3, r_2 = 0$ and

$$H = \{(x, y, z) \in \mathbb{R}^3 : x + y + z = 0\} \simeq \mathbb{R}^2.$$

$T^0 =?$ $\quad\quad dim(T^0) =?$

Ex: $F = \mathbb{Q}(\sqrt[4]{2})$?

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 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 st
  $q(\lambda x, y) = q(x, \bar{\lambda} y)$ (Hermitian property)
  for all $x, y \in I$ and for all $\lambda \in O_F$.

Ex 1: Let I be a factional ideal of F.

$$q(x, y) := \langle x, y \rangle \text{ for any } x, y \in I.$$

(the scalar product defined on $F_{\mathbb{R}}$)

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 st
  $q(\lambda x, y) = q(x, \bar{\lambda} y)$ (Hermitian property)
  for all $x, y \in I$ and for all $\lambda \in O_F$.

Ex 1: Let I be a factional ideal of F.

$$q(x, y) := \langle x, y \rangle \text{ for any } x, y \in I.$$

(the scalar product defined on $F_{\mathbb{R}}$)
Then (I, q) is an ideal lattice.

Ideal lattices

Ex 2: Let I be a factional ideal of F and
$u = (u_\sigma) \in (\mathbb{R}_{>0})^{r_1+r_2}$.
$z \in I$, $uz := (u_\sigma \cdot \sigma(z))_\sigma \in F_\mathbb{R}$.
We define

$$q_u(x, y) := \langle ux, uy \rangle \text{ for any } x, y \in I.$$

(the scalar product defined on $F_\mathbb{R}$)

Ideal lattices

Ex 2: Let I be a factional ideal of F and
$u = (u_\sigma) \in (\mathbb{R}_{>0})^{r_1+r_2}$.
$z \in I$, $uz := (u_\sigma \cdot \sigma(z))_\sigma \in F_\mathbb{R}$.
We define

$$q_u(x, y) := \langle ux, uy \rangle \text{ for any } x, y \in I.$$

(the scalar product defined on $F_\mathbb{R}$)

Proposition

(I, q_u) is an ideal lattice.

Isometric ideal lattices

Definition

Two ideal lattices (I, q) and (I', q') are called **isometric** if

- there exists $f \in F^\times$ such that $I' = fI$ and
- $q'(fx, fy) = q(x, y)$ for all $x, y \in I$.

Lattices from fractional ideals

A full rank lattice in $F_{\mathbb{R}}$ is also a full rank lattice in $\mathbb{R}^n$ via

$$F_{\mathbb{R}} \simeq \mathbb{R}^{r_1} \times \mathbb{C}^{r_2} \longrightarrow \mathbb{R}^n$$

$$\begin{bmatrix} x_1 \\ x_2 \\ \cdots \\ x_{r_1} \\ x_{r_1+1} \\ \cdots \\ x_{r_1+r_2} \end{bmatrix} \longmapsto \begin{bmatrix} x_1 \\ x_2 \\ \cdots \\ x_{r_1} \\ Re(x_{r_1+1}) \\ Im(x_{r_1+1}) \\ \cdots \\ Re(x_{r_1+r_2}) \\ Im(x_{r_1+r_2}) \end{bmatrix}.$$

EX: $F = \mathbb{Q}(\sqrt[4]{2})$?

Lattices from fractional ideals

- $\mathbb{Z}^2$?

Lattices from fractional ideals

- $\mathbb{Z}^2$?
- The hexagonal lattice?

Lattices from fractional ideals

- $\mathbb{Z}^2$?
- The hexagonal lattice?
- Let p is an odd prime, $\mathfrak{p} = (1 - \zeta_p)O_F$: principal ideal of $F = \mathbb{Q}(\zeta_p)$. Then $(\mathfrak{p}, q_{1/p})$ is an ideal lattice $\simeq$?

Lattices from fractional ideals

- $\mathbb{Z}^2$?
- The hexagonal lattice?
- Let p is an odd prime, $\mathfrak{p} = (1 - \zeta_p)O_F$: principal ideal of $F = \mathbb{Q}(\zeta_p)$. Then $(\mathfrak{p}, q_{1/p})$ is an ideal lattice $\simeq$?
- Let $I = \frac{1}{(1-\zeta_9)^4} O_F$: principal ideal of $F = \mathbb{Q}(\zeta_9)$. Then (I, q_1) is an ideal lattice $\simeq$?

Lattices from fractional ideals

- Let $I = \frac{1}{(1-\zeta_9)^4} O_F$: principal ideal of $F = \mathbb{Q}(\zeta_9)$. Then (I, q_1) is an ideal lattice $\simeq$?

```
[ 2.00 -1.00        1.00       -1.00       -1.00       -1.00]
[-1.00  2.00       -1.00        1.00        1.00        1.00]
[ 1.00 -1.00        2.00 -4.06 E-38       -1.00 1.47 E-39]
[-1.00  1.00 -4.06 E-38        2.00 4.35 E-38        1.00]
[-1.00  1.00       -1.00  4.35 E-38        2.00 7.35 E-39]
[-1.00  1.00  1.47 E-39        1.00 7.35 E-39        2.00]
```

Figure: The Gram matrix of (I, q_1).

Lattices from fractional ideals

- Let $F = \mathbb{Q}(\zeta_{15})$ and $I = \beta O_F$ for some $\beta \in F$. Then (O_F, q_β) is an ideal lattice $\simeq$?

Lattices from fractional ideals

- Let $F = \mathbb{Q}(\zeta_{15})$ and $I = \beta O_F$ for some $\beta \in F$.
  Then (O_F, q_β) is an ideal lattice $\simeq$?
- Let $F = \mathbb{Q}(\zeta_{35})$ and
  $\alpha = (\zeta_{35}^{-3} + \zeta_{35}^{3})(\zeta_{35}^{-6} + \zeta_{35}^{6})(\zeta_{35}^{-9} + \zeta_{35}^{9})(\zeta_{35}^{-12} + \zeta_{35}^{12})/\psi'(\zeta_{35} + \zeta_{35}^{-1})$.
  Then (O_F, q_α) is an ideal lattice $\simeq$?

Recap

- Number field, the ring of integers.
- Fractional ideals: $1/\alpha J$ for some $\alpha \in O_F$ and $J \subset O_F$ is an ideal.
- The class group $Cl_F = Id_F/Princ_F$ and class number $h_F = \#Cl_F$.
- The Φ map:
  $\Phi = (\sigma_1, \cdots, \sigma_{r_1}, \sigma_{r_1+1}, \cdots, \sigma_{r_1+r_2})$.
- The L map: $L(x) = (\log|\sigma(f)|)_\sigma$, $\forall x \in F^\times$.
- Ideal lattices: (I, q), where
  - I is a (fractional) O_F-ideal and
  - $q : L \times L \longrightarrow \mathbb{R}$ is a non-degenerate symmetric bilinear form with Hermitian property.

  I: factional ideal; $u = \in (\mathbb{R}_{>0})^{r_1+r_2}$.
  Then (I, q_u) is an ideal lattice.

Oh, no : (: (: (

Exercise: Let $F = \mathbb{Q}(\sqrt[4]{2})$. Prove that $O_F = \mathbb{Z}[\sqrt[4]{2}]$.

Oh, no : (: (: (

Exercise: Let $F = \mathbb{Q}(\sqrt[4]{2})$. Prove that $O_F = \mathbb{Z}[\sqrt[4]{2}]$.

There will be a gift for this :).

References

Eva Bayer-Fluckiger. Lattices and number fields.
In *Algebraic geometry: Hirzebruch 70 (Warsaw, 1998)*, volume 241 of *Contemp. Math.*, pages 69–84. Amer. Math. Soc., Providence, RI, 1999.

Hendrik W. Lenstra, Jr. Lattices.
In *Algorithmic number theory: lattices, number fields, curves and cryptography*, volume 44 of *Math. Sci. Res. Inst. Publ.*, pages 127–181. Cambridge Univ. Press, Cambridge, 2008.

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.