Lecture 2.
THE ARAKELOV CLASS GROUP

Ha Tran

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

We have studied:

- Number field, the ring of integers.
- Fractional ideals: J/α for some $0 \neq \alpha \in O_F$ 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: $\Phi = (\sigma_1, \cdots, \sigma_{r_1}, \sigma_{r_1+1}, \cdots, \sigma_{r_1+r_2})$. $\Phi(I)$ is a lattice in $F_{\mathbb{R}}$.
- The L map: $L(x) = (\log|\sigma(f)|)_\sigma$, $\forall x \in F^\times$. $\Lambda = L(O_F^\times)$ is a lattice in $H = \ldots$. $T^0 = H/\Lambda$ is a real torus of dim. $r_1 + r_2 - 1$.
- Ideal lattices: (I, q), where ... I: factional ideal; $u = \in (\mathbb{R}_{>0})^{r_1+r_2}$. Then (I, q_u) is an ideal lattice.
- Many famous lattices arise from ideal lattices.

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

Denote by

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

and

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

Denote by

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

and

$$\Lambda = L(O_F^\times).$$

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

Denote by

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

and

$$\Lambda = L(O_F^\times).$$

Λ is a lattice contained in the vector space H.

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

Denote by

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

and

$$\Lambda = L(O_F^\times).$$

Λ is a lattice contained in the vector space H.

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

Denote by

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

and

$$\Lambda = L(O_F^\times).$$

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

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

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

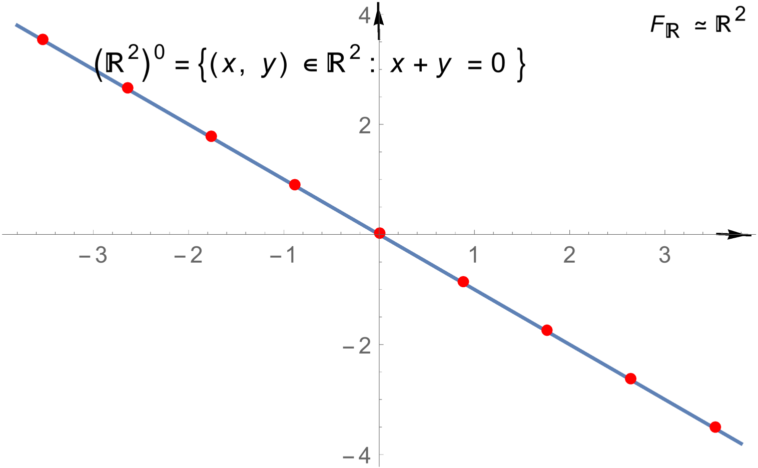
$$H = \{(x, y) \in \mathbb{R}^2 : x + y = 0\} \simeq \mathbb{R}.$$

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

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

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

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

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

What we study today?

The Arakelov class group Pic_F^0,

- Pic_F^0 tells you the class number h_F, the regulator R_F,...
- (Main Theorem) There is a bijection

$$Pic_F^0 \xrightarrow{\psi} \{\text{Isometry classes of ideal lattices of covol. } \sqrt{|\Delta_F|}$$

Content

What are Arakalov divisors?

Arakelov divisors of a number field are analogous to divisors on an algebraic curve.

What are Arakalov divisors?

Arakelov divisors of a number field are analogous to divisors on an algebraic curve.

Algebraic curve

Divisor

$$D = \sum_{P \text{ points}} n_P P$$

$n_P \in \mathbb{Z}$.

What are Arakalov divisors?

Arakelov divisors of a number field are analogous to divisors on an algebraic curve.

Algebraic curve

Divisor

$$D = \sum_{P \text{ points}} n_P P$$

$n_P \in \mathbb{Z}$.

Number field F

Arakelov divisor

$$D = \sum_{\mathfrak{p} \text{ primes}} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\sigma} x_{\sigma} \sigma$$

σ infinite primes of F.

$n_{\mathfrak{p}} \in \mathbb{Z}$ but $x_{\sigma} \in \mathbb{R}$.

What are Arakalov divisors?

Definition

An Arakelov divisor is of the form

$$D = \sum_{\mathfrak{p} \text{ primes}} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\sigma} x_{\sigma} \sigma$$

σ infinite primes of F; $n_{\mathfrak{p}} \in \mathbb{Z}$ but $x_{\sigma} \in \mathbb{R}$.

What are Arakalov divisors?

Definition

An Arakelov divisor is of the form

$$D = \sum_{\mathfrak{p} \text{ primes}} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\sigma} x_{\sigma} \sigma$$

σ infinite primes of F; $n_{\mathfrak{p}} \in \mathbb{Z}$ but $x_{\sigma} \in \mathbb{R}$.

Ex 4: $F = \mathbb{Q}$, $O_F = \mathbb{Z}$,

$\mathfrak{p}_1 = 2\mathbb{Z}, \mathfrak{p}_2 = 5\mathbb{Z}$: 2 prime ideals;

$\sigma : \mathbb{Q} \to \mathbb{C}$, $q \longmapsto q$ the infinite prime;

$D = \mathfrak{p}_1 - 3\mathfrak{p}_2 + \pi\sigma$ is an Arakelov divisor.

What are Arakalov divisors?

Definition

An Arakelov divisor is of the form

$$D = \sum_{\mathfrak{p} \text{ primes}} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\sigma} x_\sigma \sigma$$

σ infinite primes of F; $n_{\mathfrak{p}} \in \mathbb{Z}$ but $x_\sigma \in \mathbb{R}$.

- The set of all Arakelov divisors of F is an additive group denoted by $Div_F \simeq \oplus_{\mathfrak{p}}\mathbb{Z} \times \oplus_\sigma \mathbb{R}$.

What are Arakalov divisors?

Definition

An Arakelov divisor is of the form

$$D = \sum_{\mathfrak{p} \text{ primes}} n_{\mathfrak{p}}\mathfrak{p} + \sum_{\sigma} x_{\sigma}\sigma$$

σ infinite primes of F; $n_{\mathfrak{p}} \in \mathbb{Z}$ but $x_{\sigma} \in \mathbb{R}$.

- The set of all Arakelov divisors of F is an additive group denoted by $Div_F \simeq \oplus_{\mathfrak{p}}\mathbb{Z} \times \oplus_{\sigma}\mathbb{R}$.
- $D_1 + D_2 =?$, the neutral of Div_F, $-D =?$

What are Arakalov divisors?

Definition

An Arakelov divisor is of the form

$$D = \sum_{\mathfrak{p} \text{ primes}} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\sigma} x_\sigma \sigma$$

σ infinite primes of F; $n_{\mathfrak{p}} \in \mathbb{Z}$ but $x_\sigma \in \mathbb{R}$.

- The set of all Arakelov divisors of F is an additive group denoted by $Div_F \simeq \oplus_{\mathfrak{p}} \mathbb{Z} \times \oplus_\sigma \mathbb{R}$.
- $D_1 + D_2 = ?$, the neutral of Div_F, $-D = ?$

Ex 5: $Div_F = ?$

What are Arakalov divisors?

Definition

An Arakelov divisor is of the form

$$D = \sum_{\mathfrak{p} \text{ primes}} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\sigma} x_{\sigma} \sigma$$

σ infinite primes of F; $n_{\mathfrak{p}} \in \mathbb{Z}$ but $x_{\sigma} \in \mathbb{R}$.

- The set of all Arakelov divisors of F is an additive group denoted by $Div_F \simeq \oplus_{\mathfrak{p}} \mathbb{Z} \times \oplus_{\sigma} \mathbb{R}$.
- $D_1 + D_2 =?$, the neutral of Div_F, $-D =?$

Ex 5: $Div_F =?$

- $F = \mathbb{Q}$

What are Arakalov divisors?

Definition

An Arakelov divisor is of the form

$$D = \sum_{\mathfrak{p} \text{ primes}} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\sigma} x_{\sigma} \sigma$$

σ infinite primes of F; $n_{\mathfrak{p}} \in \mathbb{Z}$ but $x_{\sigma} \in \mathbb{R}$.

- The set of all Arakelov divisors of F is an additive group denoted by $Div_F \simeq \oplus_{\mathfrak{p}} \mathbb{Z} \times \oplus_{\sigma} \mathbb{R}$.
- $D_1 + D_2 = ?$, the neutral of Div_F, $-D = ?$

Ex 5: $Div_F = ?$

- $F = \mathbb{Q}$
- $F = \mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{2})$.

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.

Analogies

Algebraic curve

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

Number field F

- Arakelov divisor.
- Principal Arakelov divisor.
- Arakelov class group.
- The inverse different.

Analogies

Algebraic curve

- Divisor.
- Principal divisor.
- Picard group.
- Canonical divisor κ.
- Riemann–Roch $h^0(D) - h^0(\kappa - D) = deg(D) - (g - 1)$.

Number field F

- Arakelov divisor.
- Principal Arakelov divisor.
- Arakelov class group.
- The inverse different.
- Riemann–Roch $h^0(D) - h^0(\kappa - D) = deg(D) - \frac{1}{2}\log|\Delta|$.

Analogies

Algebraic curve

- Divisor.
- Principal divisor.
- Picard group.
- Canonical divisor κ.
- Riemann–Roch $h^0(D) - h^0(\kappa - D) = deg(D) - (g-1)$.
- $h^0(D)$.

Number field F

- Arakelov divisor.
- Principal Arakelov divisor.
- Arakelov class group.
- The inverse different.
- Riemann–Roch $h^0(D) - h^0(\kappa - D) = deg(D) - \frac{1}{2}\log|\Delta|$.
- $h^0(D)$.

Analogies

Algebraic curve

- Divisor.
- Principal divisor.
- Picard group.
- Canonical divisor κ.
- Riemann–Roch $h^0(D) - h^0(\kappa - D) = deg(D) - (g - 1)$.
- $h^0(D)$.
- ...

Number field F

- Arakelov divisor.
- Principal Arakelov divisor.
- Arakelov class group.
- The inverse different.
- Riemann–Roch $h^0(D) - h^0(\kappa - D) = deg(D) - \frac{1}{2}\log|\Delta|$.
- $h^0(D)$.
- ...

Principal Arakelov divisors

- For $f \in F^\times$, the principal Arakelov divisor

$$(f) = \sum_{\mathfrak{p} \text{ primes}} n_\mathfrak{p} \mathfrak{p} + \sum_\sigma x_\sigma \sigma$$

where $n_\mathfrak{p} = ord_\mathfrak{p}(f)$ and $x_\sigma = -\log|\sigma(f)|, \forall \sigma$.

Principal Arakelov divisors

- For $f \in F^\times$, the principal Arakelov divisor

$$(f) = \sum_{\mathfrak{p} \text{ primes}} n_\mathfrak{p} \mathfrak{p} + \sum_\sigma x_\sigma \sigma$$

where $n_\mathfrak{p} = ord_\mathfrak{p}(f)$ and $x_\sigma = -\log|\sigma(f)|, \forall \sigma$.

Ex 6: $f = -1$. Then $(f) = ?$

Principal Arakelov divisors

- For $f \in F^\times$, the principal Arakelov divisor

$$(f) = \sum_{\mathfrak{p} \text{ primes}} n_\mathfrak{p} \mathfrak{p} + \sum_\sigma x_\sigma \sigma$$

where $n_\mathfrak{p} = ord_\mathfrak{p}(f)$ and $x_\sigma = -\log|\sigma(f)|, \forall \sigma$.

Ex 6: $f = -1$. Then $(f) = ?$
Ex 7: $F = \mathbb{Q}(\sqrt{2})$, $f = 1 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})^\times : (f) = ?$
$g = 3 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})^\times : (g) = ?$

Principal Arakelov divisors

- For $f \in F^\times$, the principal Arakelov divisor

$$(f) = \sum_{\mathfrak{p} \text{ primes}} n_\mathfrak{p} \mathfrak{p} + \sum_\sigma x_\sigma \sigma$$

where $n_\mathfrak{p} = ord_\mathfrak{p}(f)$ and $x_\sigma = -\log|\sigma(f)|, \forall \sigma$.

Ex 6: $f = -1$. Then $(f) =?$
Ex 7: $F = \mathbb{Q}(\sqrt{2})$, $f = 1 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})^\times : (f) =?$
$g = 3 - \sqrt{2} \in \mathbb{Q}(\sqrt{2})^\times : (g) =?$
Ex 8: Let $F = \mathbb{Q}(i)$ and $f = 2 + i \in F^\times$. Then $(f) =?$

Degree

$$deg(\mathfrak{p}) = log(N(\mathfrak{p})) \text{ where } N(\mathfrak{p}) = \#O_F/\mathfrak{p},$$

$$deg(\sigma) = \begin{cases} 1 \text{ if } \sigma \text{ real} \\ 2 \text{ if } \sigma \text{ complex} \end{cases}$$

Degree

$$deg(\mathfrak{p}) = log(N(\mathfrak{p})) \text{ where } N(\mathfrak{p}) = \#O_F/\mathfrak{p},$$

$$deg(\sigma) = \begin{cases} 1 \text{ if } \sigma \text{ real} \\ 2 \text{ if } \sigma \text{ complex} \end{cases}$$

- The degree of D is defined by $\deg(D) := \sum_{\mathfrak{p}} n_{\mathfrak{p}} \log N(\mathfrak{p}) + \sum_{\sigma} deg(\sigma) x_{\sigma}$.

Degree

$$deg(\mathfrak{p}) = log(N(\mathfrak{p})) \text{ where } N(\mathfrak{p}) = \#O_F/\mathfrak{p},$$

$$deg(\sigma) = \begin{cases} 1 \text{ if } \sigma \text{ real} \\ 2 \text{ if } \sigma \text{ complex} \end{cases}$$

- The degree of D is defined by $\deg(D) := \sum_{\mathfrak{p}} n_{\mathfrak{p}} \log N(\mathfrak{p}) + \sum_{\sigma} deg(\sigma) x_{\sigma}$.

Let $f \in F^{\times}$. Compute $deg(f)$ if

Ex 6: $f = -1$?

Degree

$$deg(\mathfrak{p}) = log(N(\mathfrak{p})) \text{ where } N(\mathfrak{p}) = \#O_F/\mathfrak{p},$$

$$deg(\sigma) = \begin{cases} 1 \text{ if } \sigma \text{ real} \\ 2 \text{ if } \sigma \text{ complex} \end{cases}$$

- The degree of D is defined by $\deg(D) := \sum_{\mathfrak{p}} n_{\mathfrak{p}} \log N(\mathfrak{p}) + \sum_{\sigma} deg(\sigma) x_{\sigma}$.

Let $f \in F^{\times}$. Compute $deg(f)$ if

Ex 6: $f = -1$?

Ex 7: $F = \mathbb{Q}(\sqrt{2})$, $f = 1 - \sqrt{2}$? , $f = 3 - \sqrt{2}$?

Degree

$$deg(\mathfrak{p}) = log(N(\mathfrak{p})) \text{ where } N(\mathfrak{p}) = \#O_F/\mathfrak{p},$$

$$deg(\sigma) = \begin{cases} 1 \text{ if } \sigma \text{ real} \\ 2 \text{ if } \sigma \text{ complex} \end{cases}$$

- The degree of D is defined by $\deg(D) := \sum_{\mathfrak{p}} n_{\mathfrak{p}} \log N(\mathfrak{p}) + \sum_{\sigma} deg(\sigma) x_{\sigma}$.

Let $f \in F^{\times}$. Compute $deg(f)$ if

Ex 6: $f = -1$?

Ex 7: $F = \mathbb{Q}(\sqrt{2})$, $f = 1 - \sqrt{2}$? , $f = 3 - \sqrt{2}$?

Ex 8: $F = \mathbb{Q}(i)$ and $f = 2 + i$?

Degree

$$deg(\mathfrak{p}) = log(N(\mathfrak{p})) \text{ where } N(\mathfrak{p}) = \#O_F/\mathfrak{p},$$

$$deg(\sigma) = \begin{cases} 1 \text{ if } \sigma \text{ real} \\ 2 \text{ if } \sigma \text{ complex} \end{cases}$$

- The degree of D is defined by $\deg(D) := \sum_{\mathfrak{p}} n_{\mathfrak{p}} \log N(\mathfrak{p}) + \sum_{\sigma} deg(\sigma) x_{\sigma}$.

Let $f \in F^{\times}$. Compute $deg(f)$ if

Ex 6: $f = -1$?

Ex 7: $F = \mathbb{Q}(\sqrt{2})$, $f = 1 - \sqrt{2}$? , $f = 3 - \sqrt{2}$?

Ex 8: $F = \mathbb{Q}(i)$ and $f = 2 + i$?

- The set of all Arakelov divisors of degree 0 form a group, denoted by Div_F^0 $(\supset Princ_F)$.

The Hermitian line bundle

- Let $D = \sum_{\mathfrak{p} \text{ primes}} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\sigma} x_{\sigma} \sigma$. Denote

$$I := \prod_{\mathfrak{p}} \mathfrak{p}^{-n_{\mathfrak{p}}} \text{ and } u := (e^{-x_{\sigma}})_{\sigma} \in F_{\mathbb{R}}.$$

  Then (I, u) is called the Hermitian line bundle associated to D. We can identity $D = (I, u)$.

The Hermitian line bundle

- Let $D = \sum_{\mathfrak{p} \text{ primes}} n_{\mathfrak{p}} \mathfrak{p} + \sum_{\sigma} x_\sigma \sigma$. Denote

$$I := \prod_{\mathfrak{p}} \mathfrak{p}^{-n_{\mathfrak{p}}} \text{ and } u := (e^{-x_\sigma})_\sigma \in F_{\mathbb{R}}.$$

  Then (I, u) is called the Hermitian line bundle associated to D. We can identity $D = (I, u)$.
  Ex: The Hermitian line bundle ass. to
  - the zero divisor $D = 0$?
  - the principal divisor $D = (f)$?
  - $D_1 + D_2 =$? if $D_1 = (I_1, u_1)$, $D_2 = (I_2, u_2)$?
  - $-D =$? if $D = (I, u)$.

What is the Arakelov class group Pic_F^0?

It is an analogue of the Picard group of an algebraic curve.

Definition

The Arakelov class group Pic_F^0 is the quotient of Div_F^0 by its subgroup of principal divisors.

What is the Arakelov class group Pic_F^0?

It is an analogue of the Picard group of an algebraic curve.

Definition

The Arakelov class group Pic_F^0 is the quotient of Div_F^0 by its subgroup of principal divisors.

Ex 1: $F = \mathbb{Q}$, $Pic_F^0 = ?$
Ex 2: $F = \mathbb{Q}(\sqrt{-1})$, $Pic_F^0 = ?$
Ex 3: $F = \mathbb{Q}(\sqrt{2})$, $Pic_F^0 = ?$

The structure of Pic_F^0

Consider the maps

$$\phi_1 : T^0 \longrightarrow Pic_F^0$$

$$(x_\sigma)_\sigma + \Lambda \longmapsto \text{ class of } (O_F, u) \text{ where } u = (e^{x_\sigma})_\sigma,$$

The structure of Pic_F^0

Consider the maps

$$\phi_1 : T^0 \longrightarrow Pic_F^0$$

$$(x_\sigma)_\sigma + \Lambda \longmapsto \text{ class of } (O_F, u) \text{ where } u = (e^{x_\sigma})_\sigma,$$

and

$$\phi_2 : Pic_F^0 \longrightarrow Cl_F$$

$$\text{class of } (I, u) \longmapsto \text{ class of } I$$

The structure of Pic_F^0

Proposition

The following sequence is exact.

$$0 \longrightarrow T^0 \xrightarrow{\phi_1} Pic_F^0 \xrightarrow{\phi_2} Cl_F \longrightarrow 0.$$

The structure of Pic_F^0

Proposition

The following sequence is exact.

$$0 \longrightarrow T^0 \xrightarrow{\phi_1} Pic_F^0 \xrightarrow{\phi_2} Cl_F \longrightarrow 0.$$

Remark

- T^0 is a compact topological group and $\# Cl_F < \infty \Rightarrow Pic_F^0$ is a compact topo. gp.
- The compactness of $Pic_F^0 \Rightarrow$ the Dirichlet unit theorem and the finiteness of the class group.
- $D, D' \in Pic_F^0$ on the same connected component, then there exists unique $u \in T^0$ st $D - D' = (O_F, u)$.

The structure of Pic_F^0

$vol(T^0) = \sqrt{n} 2^{-r_2/2} R_F$ with R_F the regulator of F. The number of connected components of Pic_F^0 is the class number h_F.

The structure of Pic_F^0

$vol(T^0) = \sqrt{n} 2^{-r_2/2} R_F$ with R_F the regulator of F.
The number of connected components of Pic_F^0 is the class number h_F.
$F = \mathbb{Q}$ then $Pic_F^0 = 0$.

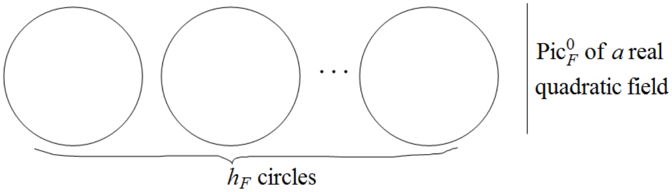
The structure of Pic_F^0

$vol(T^0) = \sqrt{n}2^{-r_2/2}R_F$ with R_F the regulator of F.
The number of connected components of Pic_F^0 is the class number h_F.

$r_1 = 0, r_2 = 1$ so T^0 is a point.

The structure of Pic_F^0

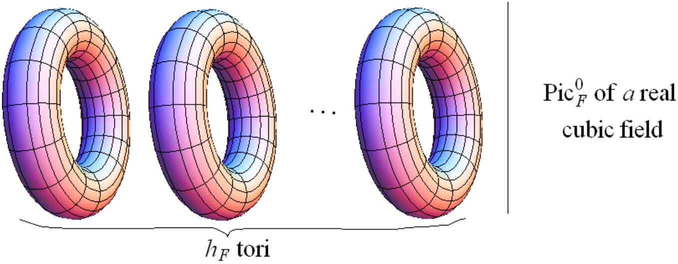
$vol(T^0) = \sqrt{n}2^{-r_2/2}R_F$ with R_F the regulator of F.
The number of connected components of Pic_F^0 is the class number h_F.



$r_1 = 2, r_2 = 0$ so T^0 is a circle.

The structure of Pic_F^0

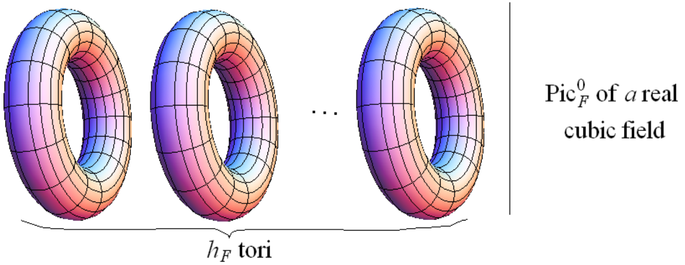
$vol(T^0) = \sqrt{n}2^{-r_2/2}R_F$ with R_F the regulator of F.
The number of connected components of Pic_F^0 is the class number h_F.



$r_1 = 3, r_2 = 1$ so T^0 is a real torus in $\mathbb{R}^3$.

The structure of Pic_F^0

$vol(T^0) = \sqrt{n}2^{-r_2/2}R_F$ with R_F the regulator of F.
The number of connected components of Pic_F^0 is the class number h_F.



Note: Buchmann's algorithm to find the regulator and class number of the number field.

The structure of Pic_F^0

Let $D = (I, u)$. $z \in I, \Phi(z) = (\sigma(z))_\sigma \in F_\mathbb{R}$,
$uz := (u_\sigma \cdot \sigma(z))_\sigma \in F_\mathbb{R}$.
We define

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

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

The structure of Pic_F^0

Let $D = (I, u)$. $z \in I, \Phi(z) = (\sigma(z))_\sigma \in F_{\mathbb{R}}$,
$uz := (u_\sigma \cdot \sigma(z))_\sigma \in F_{\mathbb{R}}$.
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.

Proof. Ex.

The structure of Pic_F^0

Let $D = (I, u)$. $z \in I, \Phi(z) = (\sigma(z))_\sigma \in F_\mathbb{R}$,
$uz := (u_\sigma \cdot \sigma(z))_\sigma \in F_\mathbb{R}$.
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.

Proof. Ex.

We called (I, q_u) the ideal lattice associated to D.

The structure of Pic^0_F

Let $D = (I, u)$. $z \in I, \Phi(z) = (\sigma(z))_\sigma \in F_\mathbb{R}$,
$uz := (u_\sigma \cdot \sigma(z))_\sigma \in F_\mathbb{R}$.
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.

Proof. Ex.

We called (I, q_u) the ideal lattice associated to D.
In particular, $\|x\|_u^2 = q_u(x, x) =?$

Main theorem

Theorem

Let F be a number field of discriminant Δ_F. There is a bijection

$$Pic_F^0 \xrightarrow{\psi} \{\text{Isometry classes of ideal lattices of covol. } \sqrt{|\Delta_F|}\}$$

$$\text{class of } D = (I, u) \longmapsto \text{ class of } (I, q_u).$$

Main theorem

Proof.

ψ is injective

ψ is surjective

Main theorem

Proof. ψ is injective:

Main theorem

Proof. ψ is injective: Assume $\psi(D) = \psi(D')$ for some $D = (I, u), D' = (I', u') \in Pic_F^0$
we have to show that

$$D' \equiv D \text{ in } Pic_F^0$$

$$\Leftrightarrow D' - D = (f) \text{ for some } f \in F^*.$$

Main theorem

Proof. ψ is injective: Assume $\psi(D) = \psi(D')$ for some $D = (I, u), D' = (I', u') \in Pic_F^0$

$\Rightarrow D' - D = (f)$.

Main theorem

Proof. ψ is injective: Assume $\psi(D) = \psi(D')$ for some $D = (I, u), D' = (I', u') \in Pic_F^0$

- $(I, q_u) \simeq (I', q_{u'})$.
- $\exists f \in F^*$ st $I' = fI$ and $q_{u'}(fx, fx) = q_u(x, x), \forall x \in I$. Hence $\|u'fx\| = \|ux\|$ for all $x \in I$.
- Extend q_u and $q_{u'}$ to $I \otimes \mathbb{R} = F_{\mathbb{R}}$. $\Rightarrow \|u'fx\| = \|ux\|, \forall x \in F_{\mathbb{R}}$.
- For each σ, let $e_\sigma \in F_{\mathbb{R}} : \sigma(e_\sigma) = 1$ while $\sigma'(e_\sigma) = 0$ for all $\sigma' \neq \sigma$.
- Substituting e_σ with $x \Rightarrow |\sigma(f)u'_\sigma| = |u_\sigma|, \forall \sigma$ $\Rightarrow |f| = u'/u$.

$\Rightarrow D' - D = (f)$.

Main theorem

Proof.

ψ is injective: done

ψ is surjective

Main theorem

Proof. ψ is surjective:

Main theorem

Proof. ψ is surjective: Let (I, q) be an ideal lattice. We have to show that

$$(I, q) \simeq \psi(D) \text{ for some } D = (J, u) \in Pic_F^0$$

Main theorem

Proof. ψ is surjective: Let (I, q) be an ideal lattice. We have to show that

$$(I, q) \simeq \psi(D) \text{ for some } D = (J, u) \in Pic_F^0$$

$$\Leftrightarrow (I, q) \simeq (J, q_u) \text{ for some } D = (J, u) \in Pic_F^0.$$

Main theorem

Proof. ψ is surjective: Let (I, q) be an ideal lattice. We have to show that

$$(I, q) \simeq \psi(D) \text{ for some } D = (J, u) \in Pic_F^0$$

$$\Leftrightarrow (I, q) \simeq (J, q_u) \text{ for some } D = (J, u) \in Pic_F^0.$$

Here we let $J = I$ and

construct u

and then construct q_u using q st $(I, q) \simeq (I, q_u)$.

Main theorem

Proof. ψ is surjective: Let (I, q) be an ideal lattice.

$\Rightarrow (I, q) \simeq (I, q_u)$ for some $D = (I, u) \in Pic_F^0$.

Main theorem

Proof. ψ is surjective: Let (I, q) be an ideal lattice.

- Extend q to $F_{\mathbb{R}}$.
- $u = \sum_\sigma q(e_\sigma, e_\sigma)^{1/2} e_\sigma \in F_{\mathbb{R}}^*$, $D = (I, u)$.

$\Rightarrow (I, q) \simeq (I, q_u)$ for some $D = (I, u) \in Pic_F^0$.

Main theorem

Proof. ψ is surjective: Let (I, q) be an ideal lattice.

- Extend q to $F_{\mathbb{R}}$.
- $u = \sum_\sigma q(e_\sigma, e_\sigma)^{1/2} e_\sigma \in F_{\mathbb{R}}^*$, $D = (I, u)$.
- $e_\sigma^2 = e_\sigma$, q is Hermitian and $e_\sigma e_\tau = 0$,

$$\Rightarrow q(e_\sigma, e_\tau) = q(e_\sigma^2, e_\tau) = q(e_\sigma, e_\sigma e_\tau) = 0, \forall \sigma \neq \tau.$$

- For all $x, y \in F_{\mathbb{R}}$,

$$q_u(x, y) = \langle ux, uy \rangle = \sum_\sigma u_\sigma^2 x_\sigma \overline{y_\sigma}$$

$$= \sum_\sigma q(e_\sigma, e_\sigma) x_\sigma \overline{y_\sigma} = q(x, y).$$

$\Rightarrow (I, q) \simeq (I, q_u)$.

Oh, no : (: (: (

Show at least 2 points that have been lacked in the proof!
Prove these points!

Oh, no : (: (: (

Show at least 2 points that have been lacked in the proof!

Prove these points!

Your exercise : (.

Oh, no : (: (: (

Show at least 2 points that have been lacked in the proof!
Prove these points!
Your exercise : (.
There will be a gift for this :).

Recap

- Arakelov divisors (I, u).
- The degree, norm.
- Principal Arakelov divisors.
- The Hermitian line bundle.
- The Arakelov class group $Pic_F^0 = Div_F^0 / Princ_F$.
- The structure of the Arakelov class group.

  $0 \longrightarrow T^0 \xrightarrow{\phi_1} Pic_F^0 \xrightarrow{\phi_2} Cl_F \longrightarrow 0$ is exact.
- There is a bijection

  $Pic_F^0 \xrightarrow{\psi} \{\text{Isometry classes of ideal lattices of covol. } \sqrt{|\Delta_F|}\}$

  class of $D = (I, u) \longmapsto$ class of (I, q_u).

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.