Lecture 3.
REDUCED ARAKELOV DIVISORS

Ha Tran

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

Review

We have studied:

- Arakelov divisors (I, u).
- The degree.
- Ideal lattices: $(I, u) \leftrightarrow (I, q_D)$.
- The Arakelov class group $Pic_F^0 = Div_F^0/Princ_F$.
- $\Lambda = L(O_F^\times)$ and $T^0 = H/\Lambda$ ...
- $0 \longrightarrow T^0 \xrightarrow{\phi_1} Pic_F^0 \xrightarrow{\phi_2} Cl_F \longrightarrow 0$ is exact.
- $Pic_F^0 \xrightarrow{1:1}$ $\{\text{Isometry classes of ideal lattices of covol.} \sqrt{|\Delta_F|}\}$.

Review

We have studied:

- ...
- Pic^0_F tells us: the regulator R_F and the class number h_F.

Review

We have studied:

- ...
- Pic_F^0 tells us: the regulator R_F and the class number h_F.

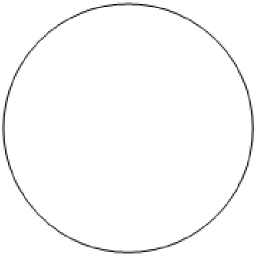


Figure: Pic_F^0 of a real quadratic field, $h_F =?$

Review

We have studied:

- ...
- Pic_F^0 tells us: the regulator R_F and the class number h_F.

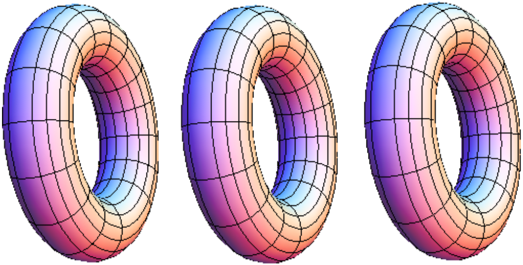


Figure: Pic_F^0 of a totally real cubic field, $h_F = ?$

Review

We have studied:

- ...
- Pic_F^0 tells us: the regulator R_F and the class number h_F.

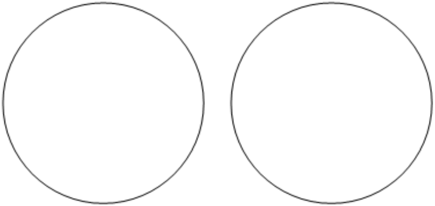


Figure: Pic_F^0 of a real quadratic field $F = \mathbb{Q}(\sqrt{10})$

$$vol(Pic_F^0) = 2\sqrt{2}\log(3+\sqrt{10}), \qquad R_F = ?$$

Review

We have studied:

- ...
- Pic_F^0 tells us: the regulator R_F and the class number h_F.

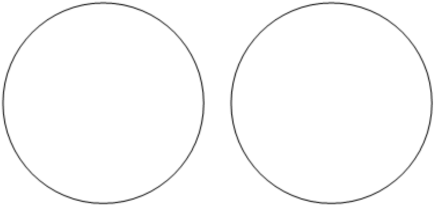


Figure: Pic_F^0 of a real quadratic field $F = \mathbb{Q}(\sqrt{10})$

$vol(Pic_F^0) = 2\sqrt{2}\log(3+\sqrt{10})$, $\qquad R_F = ?$
$vol(T^0) = \sqrt{n}2^{-r_2/2}R_F$ and $vol(Pic_F^0) = h_F vol(T^0)$.

Review

We have studied:

- ...
- Pic_F^0 tells us: the regulator R_F and the class number h_F.

Today: Metric on Pic_F^0 and Reduced Arakelov divisors.

Content

1. Metric on the Arakelov class group Pic_F^0
2. Reduced Arakelov divisors
3. Properties of reduced Arakelov divisors

Metric on Pic_F^0

Let F be a number field of degree n and $\Lambda = L(O_F^\times)$. Let $u = (u_\sigma) \in \prod_\sigma \mathbb{R}_{>0}$. Denote by

$$L(u) := (\log(u_\sigma))_\sigma \in \prod_\sigma \mathbb{R} \subset F_\mathbb{R}.$$

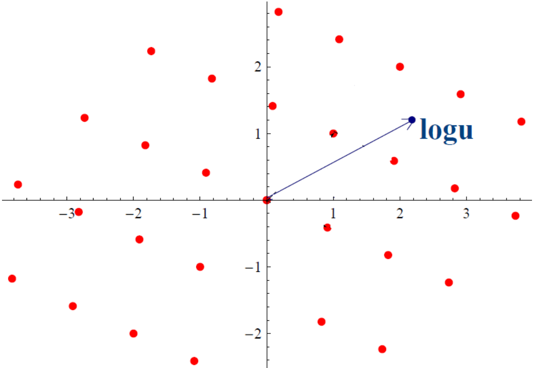
$$\|u\|_{Pic} = \min_\Lambda \|L(u)\|.$$

Metric on Pic_F^0

Let F be a number field of degree n and $\Lambda = L(O_F^\times)$. Let $u = (u_\sigma) \in \prod_\sigma \mathbb{R}_{>0}$. Denote by

$$L(u) := (\log(u_\sigma))_\sigma \in \prod_\sigma \mathbb{R} \subset F_\mathbb{R}.$$

$$\|u\|_{Pic} = \min_\Lambda \|L(u)\|.$$

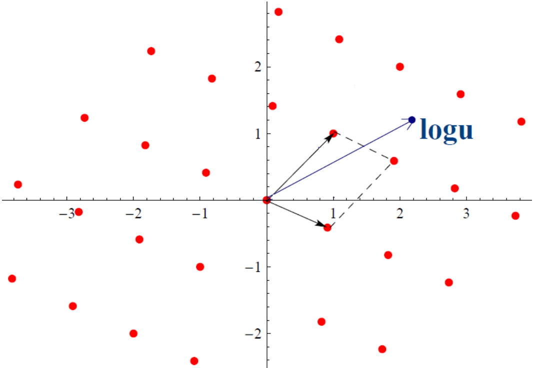


Metric on Pic_F^0

Let F be a number field of degree n and $\Lambda = L(O_F^\times)$. Let $u = (u_\sigma) \in \prod_\sigma \mathbb{R}_{>0}$. Denote by

$$L(u) := (\log(u_\sigma))_\sigma \in \prod_\sigma \mathbb{R} \subset F_\mathbb{R}.$$

$$\|u\|_{Pic} = \min_\Lambda \|L(u)\|.$$

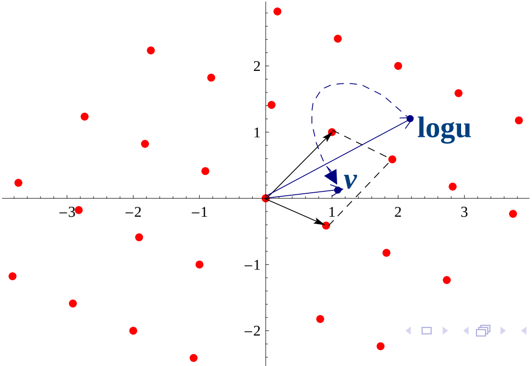


Metric on Pic_F^0

Let F be a number field of degree n and $\Lambda = L(O_F^\times)$. Let $u = (u_\sigma) \in \prod_\sigma \mathbb{R}_{>0}$. Denote by

$$L(u) := (\log(u_\sigma))_\sigma \in \prod_\sigma \mathbb{R} \subset F_\mathbb{R}.$$

$$\|u\|_{Pic} = \min_\Lambda \|L(u)\|.$$

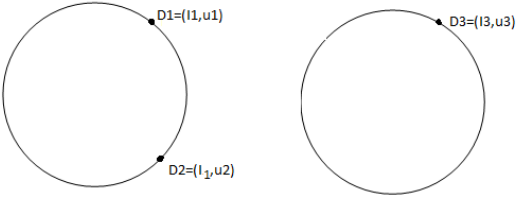


Metric on Pic_F^0

Let $[D]$ and $[D']$ be 2 divisor classes on the same connected component of Pic_F^0. Then there exists unique $u = (u_\sigma) \in \prod_\sigma \mathbb{R}_{>0}$ (up to multiplication by units) such that $D - D' = (O_F, u)$.

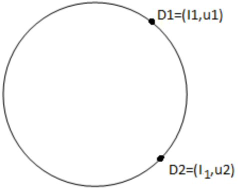
Metric on Pic_F^0

Let $[D]$ and $[D']$ be 2 divisor classes on the same connected component of Pic_F^0. Then there exists unique $u = (u_\sigma) \in \prod_\sigma \mathbb{R}_{>0}$ (up to multiplication by units) such that $D - D' = (O_F, u)$.



Metric on Pic_F^0

Let $[D]$ and $[D']$ be 2 divisor classes on the same connected component of Pic_F^0. Then there exists unique $u = (u_\sigma) \in \prod_\sigma \mathbb{R}_{>0}$ (up to multiplication by units) such that $D - D' = (O_F, u)$.

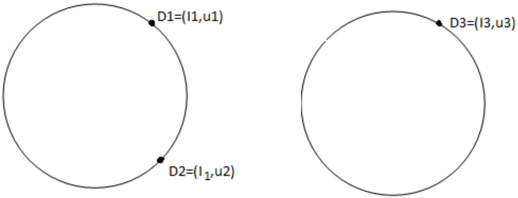


We define

$$\|D - D'\|_{Pic} := \|u\|_{Pic}.$$

Metric on Pic_F^0

Let $[D]$ and $[D']$ be 2 divisor classes on the same connected component of Pic_F^0. Then there exists unique $u = (u_\sigma) \in \prod_\sigma \mathbb{R}_{>0}$ (up to multiplication by units) such that $D - D' = (O_F, u)$.



We define

$$\|D - D'\|_{Pic} := \|u\|_{Pic}.$$

The function $\| \quad \|_{Pic}$ induces the natural topology of Pic_F^0.

Metric on Pic_F^0

Ex: $F = \mathbb{Q}(\sqrt{15})$ and $f = \frac{7+\sqrt{\Delta}}{2} \in F^*$
and $I = 1/4(6, \sqrt{15})$ a fractional ideal of F, $u = (10, 1/10)$.
Let $D_1 = (O_F, 1)$, $D_2 = (f)$, $D_3 = (O_F, u)$ and $D_4 = d(I)$.

- $\|D_2 - D_1\|_{Pic} =?$
- $\|D_3 - D_1\|_{Pic} =?$
- $\|D_4 - D_1\|_{Pic} =?$

What are reduced Arakelov divs.?

Reduced Arakelov divisors can be used for computing in the Arakelov class group.

What are reduced Arakelov divs.?

Reduced Arakelov divisors can be used for computing in the Arakelov class group.

- D. Shanks [1972]: introduced "infrastructure". He discovered it when computing the regulator of a real quadratic field.

What are reduced Arakelov divs.?

Reduced Arakelov divisors can be used for computing in the Arakelov class group.

- D. Shanks [1972]: introduced "infrastructure". He discovered it when computing the regulator of a real quadratic field.
- H. Lenstra [1982]: described the infrastructure of a real quadratic number field in terms of "circle groups".

What are reduced Arakelov divs.?

Reduced Arakelov divisors can be used for computing in the Arakelov class group.

- D. Shanks [1972]: introduced "infrastructure". He discovered it when computing the regulator of a real quadratic field.
- H. Lenstra [1982]: described the infrastructure of a real quadratic number field in terms of "circle groups".
- H. Williams and his students [1983]: complex cubic fields.

What are reduced Arakelov divs.?

Reduced Arakelov divisors can be used for computing in the Arakelov class group.

- D. Shanks [1972]: introduced "infrastructure". He discovered it when computing the regulator of a real quadratic field.
- H. Lenstra [1982]: described the infrastructure of a real quadratic number field in terms of "circle groups".
- H. Williams and his students [1983]: complex cubic fields.
- J. Buchmann and H. Williams [1988] described the infrastructure for number fields with unit group of rank 1.

What are reduced Arakelov divs.?

Reduced Arakelov divisors can be used for computing in the Arakelov class group.

- D. Shanks [1972]: introduced "infrastructure". He discovered it when computing the regulator of a real quadratic field.
- H. Lenstra [1982]: described the infrastructure of a real quadratic number field in terms of "circle groups".
- H. Williams and his students [1983]: complex cubic fields.
- J. Buchmann and H. Williams [1988] described the infrastructure for number fields with unit group of rank 1.
- R. Schoof [2008]: The first description of infrastructure in terms of reduced Arakelov divisors and Arakelov class groups.

Reduced Arakelov divisors of real quadratic fields

- Let a real quadratic form $f(X, Y) = aX^2 + bXY + cY^2$ where
  $a, b, c \in \mathbb{Z}$ and $\gcd(a, b, c) = 1$.
  The discriminant of f is $\Delta = b^2 - 4ac > 0$.

Reduced Arakelov divisors of real quadratic fields

- Let a real quadratic form $f(X, Y) = aX^2 + bXY + cY^2$ where
  $a, b, c \in \mathbb{Z}$ and $\gcd(a, b, c) = 1$.
  The discriminant of f is $\Delta = b^2 - 4ac > 0$.
- f is call reduced if $|\sqrt{\Delta} - 2a| < b < \sqrt{\Delta}$.

Reduced Arakelov divisors of real quadratic fields

- Let a real quadratic form $f(X, Y) = aX^2 + bXY + cY^2$ where
  $a, b, c \in \mathbb{Z}$ and $\gcd(a, b, c) = 1$.
  The discriminant of f is $\Delta = b^2 - 4ac > 0$.
- f is call reduced if $|\sqrt{\Delta} - 2a| < b < \sqrt{\Delta}$.

Ex: $f(X, Y) = X^2 + 7XY - 6Y^2$ is reduced ($\Delta = 73$).

Reduced quadratic forms

$f(X, Y) = X^2 + 7XY - 6Y^2$ is reduced where
$a = 1, b = 7$ and $c = -6$, $\Delta = 73$ st:

$(\star)$ $\boxed{\Delta = b^2 - 4ac > 0 \text{ and } \gcd(a, b, c) = 1}$

$(\star\star)$ $\boxed{|\sqrt{\Delta} - 2a| < b < \sqrt{\Delta}.}$

Reduced quadratic forms

$f(X, Y) = X^2 + 7XY - 6Y^2$ is reduced where
$a = 1, b = 7$ and $c = -6$, $\Delta = 73$ st:

$(\star)$ $\boxed{\Delta = b^2 - 4ac > 0 \text{ and } \gcd(a, b, c) = 1}$

$(\star\star)$ $\boxed{|\sqrt{\Delta} - 2a| < b < \sqrt{\Delta}.}$

Reduced quadratic forms

$f(X, Y) = X^2 + 7XY - 6Y^2$ is reduced where
$a = 1, b = 7$ and $c = -6$, $\Delta = 73$ st:

$(\star)$ $\boxed{\Delta = b^2 - 4ac > 0 \text{ and } \gcd(a, b, c) = 1}$

$(\star\star)$ $\boxed{|\sqrt{\Delta} - 2a| < b < \sqrt{\Delta}.}$

???

- How many reduced quadratic forms of discriminant $\Delta = 73$?
- Can find all of them?

Reduced quadratic forms

$(\star)$ $\boxed{\Delta = b^2 - 4ac > 0 \text{ and } \gcd(a, b, c) = 1}$

$(\star\star)$ $\boxed{|\sqrt{\Delta} - 2a| < b < \sqrt{\Delta}.}$

The reduction algorithm can find all reduced quadratic forms of given discriminant.

	a	b	c	distance
a = - c	1	7	-6	
	6	5	-2	1.632850979
	2	7	-3	2.580939751
	3	5	-4	4.21379073
	4	3	-4	5.161879503
	4	5	-3	5.680471616
	3	7	-2	6.628560388
	2	5	-6	8.261411367
	6	7	-1	9.215298415
	1	7	-6	10.84235112
				7.6667

$a > 0$

Reduced Arakelov divisors of real quadratic fields

- $f(X,Y) = X^2 + 7XY - 6Y^2$ is reduced where $a = 1, b = 7$ and $c = -6$ st:

  $(\star)$ $\boxed{a, b, c \in \mathbb{Z} \text{ and } \gcd(a,b,c) = 1}$

  $(\star\star)$ $\boxed{|\sqrt{\Delta} - 2a| < b < \sqrt{\Delta}.}$

Reduced Arakelov divisors of real quadratic fields

- $f(X,Y) = X^2 + 7XY - 6Y^2$ is reduced where $a = 1, b = 7$ and $c = -6$ st:

  $(\star)$ $\boxed{a, b, c \in \mathbb{Z} \text{ and } \gcd(a, b, c) = 1}$

  $(\star\star)$ $\boxed{|\sqrt{\Delta} - 2a| < b < \sqrt{\Delta}.}$

Reduced Arakelov divisors of real quadratic fields

- $f(X, Y) = X^2 + 7XY - 6Y^2$ is reduced where $a = 1, b = 7$ and $c = -6$ st:

  $(\star)$ $\boxed{a, b, c \in \mathbb{Z} \text{ and } \gcd(a, b, c) = 1}$

  $(\star\star)$ $\boxed{|\sqrt{\Delta} - 2a| < b < \sqrt{\Delta}.}$

- Let $F = \mathbb{Q}(\sqrt{\Delta})$ with $\Delta = 73 > 0$. Then

$$O_F = \mathbb{Z}\left[\frac{1+\sqrt{73}}{2}\right] = 1 \cdot \mathbb{Z} \oplus \frac{b+\sqrt{\Delta}}{2a} \cdot \mathbb{Z}.$$

Here $a = 1 = N(O_F)$ and $b, c \in \mathbb{Z}$ satisfy $(\star)$ and $(\star\star)$.

Reduced Arakelov divisors of real quadratic fields

- $f(X, Y) = X^2 + 7XY - 6Y^2$ is reduced where $a = 1, b = 7$ and $c = -6$ st:

  $(\star)$ $\boxed{a, b, c \in \mathbb{Z} \text{ and } \gcd(a, b, c) = 1}$

  $(\star\star)$ $\boxed{|\sqrt{\Delta} - 2a| < b < \sqrt{\Delta}.}$

- Let $F = \mathbb{Q}(\sqrt{\Delta})$ with $\Delta = 73 > 0$. Then

$$O_F = \mathbb{Z}\left[\frac{1+\sqrt{73}}{2}\right] = 1 \cdot \mathbb{Z} \oplus \frac{b+\sqrt{\Delta}}{2a} \cdot \mathbb{Z}.$$

Here $a = 1 = N(O_F)$ and $b, c \in \mathbb{Z}$ satisfy $(\star)$ and $(\star\star)$.

Reduced Arakelov divisors of real quadratic fields

- $f(X,Y) = X^2 + 7XY - 6Y^2$ is reduced where $a = 1, b = 7$ and $c = -6$ st:
  $(\star)$ $\boxed{a, b, c \in \mathbb{Z} \text{ and } \gcd(a,b,c) = 1}$
  $(\star\star)$ $\boxed{|\sqrt{\Delta} - 2a| < b < \sqrt{\Delta}.}$
- Let $F = \mathbb{Q}(\sqrt{\Delta})$ with $\Delta = 73 > 0$. Then

$$O_F = \mathbb{Z}\left[\frac{1+\sqrt{73}}{2}\right] = 1 \cdot \mathbb{Z} \oplus \frac{b+\sqrt{\Delta}}{2a} \cdot \mathbb{Z}.$$

  Here $a = 1 = N(O_F)$ and $b, c \in \mathbb{Z}$ satisfy $(\star)$ and $(\star\star)$.
- So, O_F corresponds to a reduced quadratic form $f(X,Y) \equiv (1, 7, -6)$ with discriminant $\Delta = 73$ and $a > 0$.

Reduced Arakelov divisors of real quadratic fields

- $f(X, Y) = X^2 + 7XY - 6Y^2$ is reduced where $a = 1, b = 7$ and $c = -6$ st:

  $(\star)$ $\boxed{a, b, c \in \mathbb{Z} \text{ and } \gcd(a, b, c) = 1}$

  $(\star\star)$ $\boxed{|\sqrt{\Delta} - 2a| < b < \sqrt{\Delta}.}$
- Let $F = \mathbb{Q}(\sqrt{\Delta})$ with $\Delta = 73 > 0$. Then

$$O_F = \mathbb{Z}\left[\frac{1+\sqrt{73}}{2}\right] = 1 \cdot \mathbb{Z} \oplus \frac{b+\sqrt{\Delta}}{2a} \cdot \mathbb{Z}.$$

  Here $a = 1 = N(O_F)$ and $b, c \in \mathbb{Z}$ satisfy $(\star)$ and $(\star\star)$.
- So, O_F corresponds to a reduced quadratic form $f(X, Y) \equiv (1, 7, -6)$ with discriminant $\Delta = 73$ and $a > 0$. The Arakelov divisor $d(O_F) = (O_F, N(O_F)^{-1/n})$ is called reduced.

Reduced Arakelov divisors of real quadratic fields

$F = \mathbb{Q}(\sqrt{\Delta})$ with dis. $\Delta = 73 > 0$.

Reduced Arakelov divisors of real quadratic fields

$F = \mathbb{Q}(\sqrt{\Delta})$ with dis. $\Delta = 73 > 0$.

- $f_1(X, Y) \equiv (1, 7, -6) \leftrightarrow O_F = 1 \cdot \mathbb{Z} \oplus \frac{7+\sqrt{\Delta}}{2 \cdot 1} \cdot \mathbb{Z}$: reduced.

Reduced Arakelov divisors of real quadratic fields

$F = \mathbb{Q}(\sqrt{\Delta})$ with dis. $\Delta = 73 > 0$.

- $f_1(X, Y) \equiv (1, 7, -6) \leftrightarrow O_F = 1 \cdot \mathbb{Z} \oplus \frac{7+\sqrt{\Delta}}{2 \cdot 1} \cdot \mathbb{Z}$: reduced.
- $f_2(X, Y) \equiv (6, 5 - 2) \leftrightarrow I_2 = 1 \cdot \mathbb{Z} \oplus \frac{5+\sqrt{\Delta}}{2 \cdot 6} \cdot \mathbb{Z}$: reduced.

Reduced Arakelov divisors of real quadratic fields

$F = \mathbb{Q}(\sqrt{\Delta})$ with dis. $\Delta = 73 > 0$.

- $f_1(X, Y) \equiv (1, 7, -6) \leftrightarrow O_F = 1 \cdot \mathbb{Z} \oplus \frac{7+\sqrt{\Delta}}{2 \cdot 1} \cdot \mathbb{Z}$: reduced.
- $f_2(X, Y) \equiv (6, 5 - 2) \leftrightarrow I_2 = 1 \cdot \mathbb{Z} \oplus \frac{5+\sqrt{\Delta}}{2 \cdot 6} \cdot \mathbb{Z}$: reduced.
- $\cdots$

Reduced Arakelov divisors of real quadratic fields

$F = \mathbb{Q}(\sqrt{\Delta})$ with dis. $\Delta = 73 > 0$.

- $f_1(X, Y) \equiv (1, 7, -6) \leftrightarrow O_F = 1 \cdot \mathbb{Z} \oplus \frac{7+\sqrt{\Delta}}{2 \cdot 1} \cdot \mathbb{Z}$: reduced.
- $f_2(X, Y) \equiv (6, 5 - 2) \leftrightarrow I_2 = 1 \cdot \mathbb{Z} \oplus \frac{5+\sqrt{\Delta}}{2 \cdot 6} \cdot \mathbb{Z}$: reduced.
- $\cdots$

Reduced Arakelov divisors of real quadratic fields

$F = \mathbb{Q}(\sqrt{\Delta})$ with dis. $\Delta = 73 > 0$.

$$\boxed{f(X,Y) \equiv (a,b,c) \leftrightarrow I = 1 \cdot \mathbb{Z} \oplus \frac{b+\sqrt{\Delta}}{2 \cdot a} \cdot \mathbb{Z}\text{: reduced.}}$$

Reduced Arakelov divisors of real quadratic fields

$F = \mathbb{Q}(\sqrt{\Delta})$ with dis. $\Delta = 73 > 0$.

$$\boxed{f(X,Y) \equiv (a,b,c) \leftrightarrow I = 1 \cdot \mathbb{Z} \oplus \frac{b+\sqrt{\Delta}}{2 \cdot a} \cdot \mathbb{Z}\text{: } \textcolor{red}{\text{reduced}}.}$$

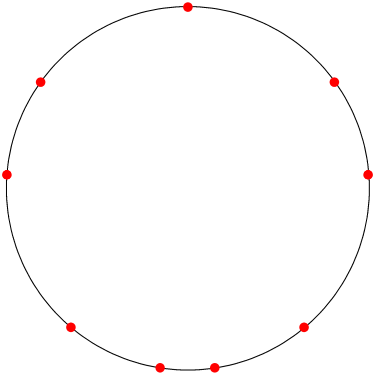
	a	b	c	distance
a = - c	1	7	-6	
	6	5	-2	1.632850979
	2	7	-3	2.580939751
	3	5	-4	4.21379073
	4	3	-4	5.161879503
	4	5	-3	5.680471616
	3	7	-2	6.628560388
	2	5	-6	8.261411367
	6	7	-1	9.215298415
	1	7	-6	10.84235112
				7.6667

Reduced Arakelov divisors of real quadratic fields

$F = \mathbb{Q}(\sqrt{\Delta})$ with dis. $\Delta = 73 > 0$.

$$\boxed{f(X,Y) \equiv (a,b,c) \leftrightarrow I = 1 \cdot \mathbb{Z} \oplus \tfrac{b+\sqrt{\Delta}}{2 \cdot a} \cdot \mathbb{Z}\text{: reduced.}}$$

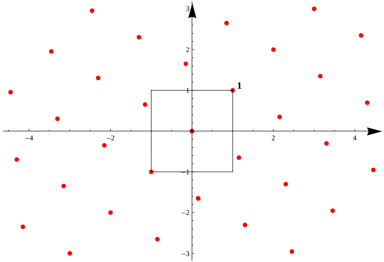
	a	b	c	distance
a = - c	1	7	-6	
	6	5	-2	1.632850979
	2	7	-3	2.580939751
	3	5	-4	4.21379073
	4	3	-4	5.161879503
	4	5	-3	5.680471616
	3	7	-2	6.628560388
	2	5	-6	8.261411367
	6	7	-1	9.215298415
	1	7	-6	10.84235112
				7.6667



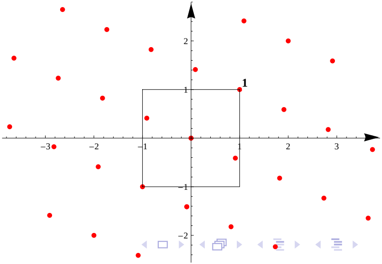
Reduced Arakelov divisors

How to generalize the reducedness?

I is reduced.



I is not reduced.



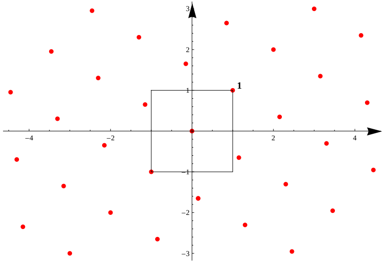
Reduced Arakelov divisors

How to generalize the reducedness?

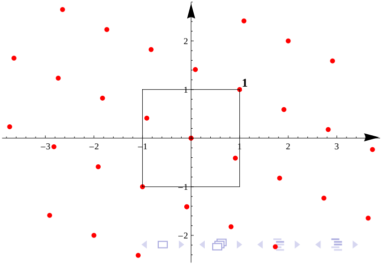
Definition

A fractional idea I is called reduced if 1 is minimal in I.
(i.e., $1 \in I$ and for any $g \in I$, if $|\sigma(g)| < 1, \forall \sigma$ then $g = 0$.)

I is reduced.



I is not reduced.



Reduced Arakelov divisors

How to generalize the reducedness?

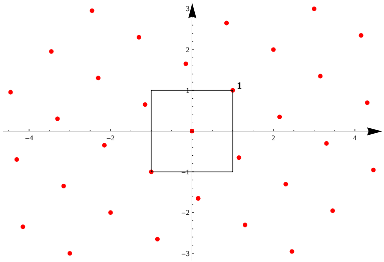
Definition

A fractional idea I is called reduced if 1 is minimal in I.
(i.e., $1 \in I$ and for any $g \in I$, if $|\sigma(g)| < 1, \forall \sigma$ then $g = 0$.)

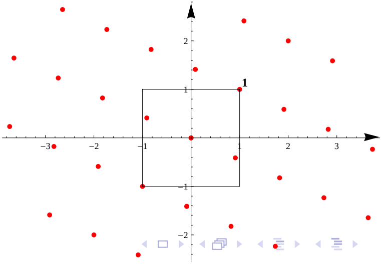
Definition

An Arakelov divisor D is called reduced if
$D = d(I) := (I, N(I)^{-\frac{1}{n}})$ for some reduced ideal I.

I is reduced.



I is not reduced.



Examples of reduced Arakelov divisors

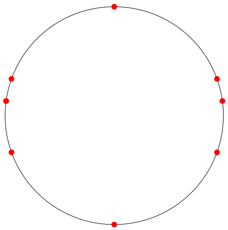
1. $D = (O_F, 1)$ is reduced.

Examples of reduced Arakelov divisors

1. $D = (O_F, 1)$ is reduced.
2. Let $F = \mathbb{Q}(\sqrt{\Delta})$ with $\Delta > 0$ and $I = \mathbb{Z} + \frac{b+\sqrt{\Delta}}{2a}\mathbb{Z}$ with $a, b, c \in \mathbb{Z}$, $b^2 - 4ac = \Delta$ and $|\sqrt{\Delta} - 2a| < b < \sqrt{\Delta}$. Then $d(I)$ is reduced.

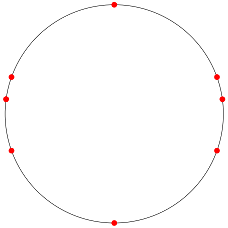
Examples of reduced Arakelov divisors

1. $D = (O_F, 1)$ is reduced.
2. Let $F = \mathbb{Q}(\sqrt{\Delta})$ with $\Delta > 0$ and $I = \mathbb{Z} + \frac{b+\sqrt{\Delta}}{2a}\mathbb{Z}$ with $a, b, c \in \mathbb{Z}$, $b^2 - 4ac = \Delta$ and $|\sqrt{\Delta} - 2a| < b < \sqrt{\Delta}$. Then $d(I)$ is reduced.
3. Reduced Arakelov divisors on T^0 with $F = \mathbb{Q}(\sqrt{983})$.



Examples of reduced Arakelov divisors

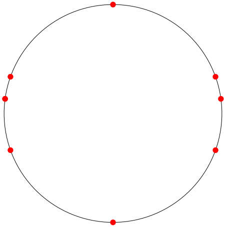
1. $D = (O_F, 1)$ is reduced.
2. Let $F = \mathbb{Q}(\sqrt{\Delta})$ with $\Delta > 0$ and $I = \mathbb{Z} + \frac{b+\sqrt{\Delta}}{2a}\mathbb{Z}$ with $a, b, c \in \mathbb{Z}$, $b^2 - 4ac = \Delta$ and $|\sqrt{\Delta} - 2a| < b < \sqrt{\Delta}$. Then $d(I)$ is reduced.
3. Reduced Arakelov divisors on T^0 with $F = \mathbb{Q}(\sqrt{983})$.



Ex: Find all reduced Arakelov divisors of $\mathbb{Q}(\sqrt{10})$.

Examples of reduced Arakelov divisors

1. $D = (O_F, 1)$ is reduced.
2. Let $F = \mathbb{Q}(\sqrt{\Delta})$ with $\Delta > 0$ and $I = \mathbb{Z} + \frac{b+\sqrt{\Delta}}{2a}\mathbb{Z}$ with $a, b, c \in \mathbb{Z}$, $b^2 - 4ac = \Delta$ and $|\sqrt{\Delta} - 2a| < b < \sqrt{\Delta}$. Then $d(I)$ is reduced.
3. Reduced Arakelov divisors on T^0 with $F = \mathbb{Q}(\sqrt{983})$.



Denote the set of all reduced Arakelov divisors of F is Red_F.
??? $\#Red_F$? How does Red_F distribute?

Red_F (Schoof 2008)

Denote the set of all reduced Arakelov divisors of F is Red_F.

??? $\#Red_F$? How does Red_F distribute?

Red_F (Schoof 2008)

Proposition 1. (cardinality of Red_F)

Let $D = d(I)$ be a reduced Arakelov divisor. Then
(i) $I^{-1} \subset O_F$ and $N(I^{-1}) \leq \partial_F$ where $\partial_F = (\frac{2}{\pi})^{r_2}\sqrt{|\Delta|}$.
(ii) Red_F is finite.

Red_F (Schoof 2008)

Proposition 1. (cardinality of Red_F)

Let $D = d(I)$ be a reduced Arakelov divisor. Then
(i) $I^{-1} \subset O_F$ and $N(I^{-1}) \leq \partial_F$ where $\partial_F = (\frac{2}{\pi})^{r_2}\sqrt{|\Delta|}$.
(ii) Red_F is finite.

Theorem 1.

Let $D = (I, u)$ be an Arakelov divisor of degree 0. Then there is a reduced Arakelov divisor D' lying on the same connected component of Pic_F^0 as D such that: $\|D - D'\|_{Pic_F} \leq log(\partial_F)$.

Red_F (Schoof 2008)

Proposition 1. (cardinality of Red_F)

Let $D = d(I)$ be a reduced Arakelov divisor. Then
(i) $I^{-1} \subset O_F$ and $N(I^{-1}) \leq \partial_F$ where $\partial_F = (\frac{2}{\pi})^{r_2}\sqrt{|\Delta|}$.
(ii) Red_F is finite.

Theorem 1.

Let $D = (I, u)$ be an Arakelov divisor of degree 0. Then there is a reduced Arakelov divisor D' lying on the same connected component of Pic_F^0 as D such that: $\|D - D'\|_{Pic_F} \leq log(\partial_F)$.

Theorem 2.

The number of reduced Arakelov divisors contained in a ball of radius 1 in Pic_F^0 is at most $\left(\frac{2}{\log 2}\right)^n \approx 2.8854^n$.

Red_F (Schoof 2008)

$\partial_F = (\frac{2}{\pi})^{r_2}\sqrt{|\Delta|}$.

Lemma

Let $D = (I, u)$ be of deg 0. Then there exists $0 \neq f \in I$ st

$$|u_\sigma \sigma(f)| < \partial_F^{1/n} \text{ for every } \sigma$$

$$(\Rightarrow \|f\|_D \leq \sqrt{n}\partial_F^{1/n}).$$

Proof. Use the Minkowskis Convex Body Theorem with the bounded symmetric convex set

$$V = \{(y_\sigma)_\sigma \in F_\mathbb{R} : |y_\sigma| \leq \partial_F^{1/n} \text{ for all } \sigma\}.$$

Red_F (Schoof 2008)

Denote the set of all reduced Arakelov divisors of F is Red_F.

??? $\#Red_F$? How does Red_F distribute?

Red_F (Schoof 2008)

Proposition 1. (cardinality of Red_F)

Let $D = d(I)$ be a reduced Arakelov divisor. Then
(i) I^{-1} is integral and $N(I^{-1}) \leq \partial_F$ where $\partial_F = (\frac{2}{\pi})^{r_2}\sqrt{|\Delta|}$.
(ii) Red_F is finite.

Red_F (Schoof 2008)

Proposition 1. (cardinality of Red_F)

Let $D = d(I)$ be a reduced Arakelov divisor. Then
(i) I^{-1} is integral and $N(I^{-1}) \le \partial_F$ where $\partial_F = (\frac{2}{\pi})^{r_2}\sqrt{|\Delta|}$.
(ii) Red_F is finite.

Proof.

i) $I \subset O_F$ since $1 \in I$, we have $I^{-1} \subset O_F$.
By the lemma, there is a nonzero element $f \in I$ such that

$$N(I)^{-1/n}|\sigma(f)| \le \partial_F^{1/n} \text{ for all } \sigma.$$

If $N(I)^{-1} > \partial_F$ then we have $|\sigma(f)| < 1$ for all σ, contradicting the minimality of 1. This proves part (i).

ii) It follows (i) because the number integral ideals of bounded norm is finite.

Red_F (Schoof 2008)

Theorem 1.
Let $D = (I, u)$ be a divisor of deg 0. Then there is a reduced Arakelov divisor D' lying on the same connected component of Pic_F^0 as D st $\|D - D'\|_{Pic_F} \leq log(\partial_F)$.

Red_F (Schoof 2008)

Theorem 1.

Let $D = (I, u)$ be a divisor of deg 0. Then there is a reduced Arakelov divisor D' lying on the same connected component of Pic_F^0 as D st $\|D - D'\|_{Pic_F} \leq log(\partial_F)$.

Proof.

- $deg(D) = 0$, $\exists$ minimal element $f \in I$ (lemma) st

$$u_\sigma |\sigma(f)| < \partial_F^{1/n} \text{ for all } \sigma.$$

- Let $J = f^{-1}I$. Then $D' = d(J)$ is reduced.
- D' is on the same connected component of Pic_F^0 as D bc $D - D' = (f) + (O_F, v)$ with $v = u|f|N(J)^{1/n}$.
- $\|D - D'\|_{Pic_F} = \|v\|_{Pic} \leq log(\partial_F)$ since $v_\sigma = u_\sigma |\sigma(f)| N(J)^{1/n}$ for all σ and $\sum_\sigma \log v_\sigma = 0$.

Red_F (Schoof 2008)

Theorem 2.

The number of reduced Arakelov divisors contained in a ball of radius 1 in Pic_F^0 is at most $\left(\frac{2}{\log 2}\right)^n \approx 2.8854^n$.

Red_F (Schoof 2008)

Theorem 2.

The number of reduced Arakelov divisors contained in a ball of radius 1 in Pic_F^0 is at most $\left(\frac{2}{\log 2}\right)^n \approx 2.8854^n$.

$B_{red}^1 =$ the reduced Arakelov divisors contained in a ball of radius 1 in Pic_F^0.

- $n = 1$, $\#B_{red}^1 \leq 2$.
- $n = 2$, $\#B_{red}^1 \leq 8$.
- $n = 3$, $\#B_{red}^1 \leq 24$.
- $n = 4$, $\#B_{red}^1 \leq 69$.
- ...

Red_F (Schoof 2008)

Theorem 2. (For totally real fields).

Red_F (Schoof 2008)

Theorem 2. (For totally real fields).

- There exists $D = d(I)$ and $D' = d(I')$ reduced divisors in the ball with
  $D - D' + (f) = (O_F, v)$
  for some $f \in F^*$ such that $\sigma(f) > 0$ for all real σ.

Red_F (Schoof 2008)

Theorem 2. (For totally real fields).

- There exists $D = d(I)$ and $D' = d(I')$ reduced divisors in the ball with
  $D - D' + (f) = (O_F, v)$
  for some $f \in F^*$ such that $\sigma(f) > 0$ for all real σ.
  There are at most 2^n reduced divisors in the ball of radius $\log 2$ in Pic_F^0.
  Bc if not, then fix one of them: D_0 and consider $D - D_0$ where D runs through the other D. They are all equal to $(f) + (O_F, u)$ for some $u \in \prod_\sigma \mathbb{R}_{>0}$.
  By the box principle, for two distinct divisors, let's say D, D', the signatures of g and g' are equal.
  Then $D - D' = (f) + (O_F, u)$ for some $u \in \prod_\sigma \mathbb{R}_{>0}$, and $f = g/g'$ totally positive.

Red_F (Schoof 2008)

Theorem 2. (For totally real fields).

- There exists $D = d(I)$ and $D' = d(I')$ reduced divisors in the ball with
  $D - D' + (f) = (O_F, v)$
  for some $f \in F^*$ such that $\sigma(f) > 0$ for all real σ.
- $I = fI'$.

Red_F (Schoof 2008)

Theorem 2. (For totally real fields).

- There exists $D = d(I)$ and $D' = d(I')$ reduced divisors in the ball with
  $D - D' + (f) = (O_F, v)$
  for some $f \in F^*$ such that $\sigma(f) > 0$ for all real σ.
- $I = fI'$.
- Let $\lambda = N(I/I')^{\frac{1}{n}} = |N(f)|^{\frac{1}{n}}$. Then $\lambda \geq \frac{1}{2}$.

Red_F (Schoof 2008)

Theorem 2. (For totally real fields).

- There exists $D = d(I)$ and $D' = d(I')$ reduced divisors in the ball with
  $D - D' + (f) = (O_F, v)$
  for some $f \in F^*$ such that $\sigma(f) > 0$ for all real σ.
- $I = fI'$.
- Let $\lambda = N(I/I')^{\frac{1}{n}} = |N(f)|^{\frac{1}{n}}$. Then $\lambda \geq \frac{1}{2}$.
- Assume that $\lambda \leq 1$. $\Rightarrow f - 1 \in I$ satisfies that

  $$|\sigma(f) - 1| \leq |\sigma(f) - \lambda| + |\lambda - 1| < \lambda + 1 - \lambda = 1 \text{ for all } \sigma.$$

  By the minimality of 1, we must have $f - 1 = 0$, so $I = I'$ and then $D = D'$.

How to find a reduced divisor?

The reduction algorithm.

Recap

- Metric on Pic_F^0. Let $D, D' \in Pic_F^0$ st $D - D' = (O_F, u)$. Then
$$\|D' - D\|_{Pic} = \|u\|_{Pic} = \min_{\Lambda} \|L(u)\|.$$
- A fractional ideal I is reduced if $1 \in I$ is minimal.
- Red_F is finite.
- There is at least one reduced Arakelov divisor in the ball of radius $log(\partial_F)$ in Pic_F^0.
- The number of reduced Arakelov divisors contained in a ball of radius 1 in Pic_F^0 is at most 2.8854^n.

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.