Arakelov Class Groups

Rene Schoof

Let F be an number field. We will construct the Arakelov class group of F (a topological group) and introduce reduced divisors (a finite set of regularly distributed divisors in this group).

1. Arakelov Class Group

First, a bit of history. In 1970, Shanks computed the units and class group of the real quadratic field $\mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}_{>0}$, and utilized the idea of 'infrastructure'. In 1980, Lenstra explained this phenomenon by introducing a circle group and the theory of reduced binary quadratic forms, e.g. the continued fraction expansion of $\sqrt{d}$.

To generalize this situation, we define the Arakelov class group. Associated to the ring of integers $\mathcal{O}_F \subset F$, we have the ideal group I_F, which is isomorphic to $\bigoplus_{\mathfrak{p} \text{ prime}} \mathbb{Z}$. We add in the infinite primes $\sigma : F \to \mathbb{C}$ up to conjugation, real and complex as $\sigma(F) \subset \mathbb{R}$. Added together, we obtain the *Arakelov divisor group*

$$\mathrm{Div}_F = \textstyle\bigoplus_{\mathfrak{p}} \mathbb{Z} \times \bigoplus_{\sigma} \mathbb{R}.$$

An arbitrary divisor is of the form

$$D = \textstyle\sum_{\mathfrak{p}} n_p \mathfrak{p} + \sum_{\sigma} x_\sigma \sigma$$

where $n_p \in \mathbb{Z}$, $x_\sigma \in \mathbb{R}$. For example, for $f \in F^*$, we have the principal Arakelov divisor where $n_p = \mathrm{ord}_{\mathfrak{p}} f$, $x_\sigma = -\log|\sigma(f)|$. The assocation $F^* \to \mathrm{Div}_F$ by $f \mapsto (f)$ is easily seen to be a homomorphism, and we see that we have the following exact sequence

$$0 \to \mu_F \to F^* \to \mathrm{Div}_F \to \mathrm{Pic}_F \to 0$$

as any element which has trivial valuation at all places must be a root of unity. The cokernel is called the *Picard group of* F, which is a quotient of the idèle class group of F.

We also have the degree map

$$\begin{aligned} \deg : \mathrm{Div}_F &\to \mathbb{R} \\ \deg(\mathfrak{p}) &= \log(N\mathfrak{p}) \\ \deg(\sigma) &= \begin{cases} 1, & \sigma \text{ real} \\ 2, & \sigma \text{ complex} \end{cases} \end{aligned}$$

where $N\mathfrak{p} = \#\mathcal{O}_F/\mathfrak{p}$. The degree map is clearly surjective and a homomorphism.

Fact 1.1 (Product formula)**.** *We have* $\deg((f)) = 0$ *for any principal divisor* f.

Proof. This follows immediately from the ordinary product formula on F. $\square$

Example 1.2. *Let* $\alpha = 2 + i \in \mathbb{Z}[i]$. *We see that* $\mathrm{ord}_{\mathfrak{p}}(2+i) = 0$ *for all* $\mathfrak{p} \neq (2+i)$, *and otherwise is* 1 *at the prime* $\mathfrak{p} = 2 + i$.

We see $\mathrm{ord}_\sigma(\alpha) = \log|2+i| = 1/2\log 5$ *for* $\sigma : \mathbb{Q}(i) \hookrightarrow \mathbb{C}$, *so the degree of the principal divisor is indeed*

$$\begin{aligned}\deg(\alpha) &= \deg((2+i) + 1/2\log 5(\sigma)) \\ &= -1\log 5 + (1/2\log 5)(2) = 0\end{aligned}$$

since $\#\mathbb{Z}[i]/(2+i) = \#\mathbb{F}_5 = 5$.

Within the Arakelov class group we consider elements of degree zero and have the following exact sequence:

$$0 \to \mu_F \to F^* \to \mathrm{Div}_F^0 \to \mathrm{Pic}_F^0 \to 0$$

where the middle map sends $f \mapsto (f)$. We say the group Pic_F^0 is the *Arakelov class group*.

Putting these maps together, we obtain:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{O}_F^*/\mu_F & \longrightarrow & F^*/\mu_F & \longrightarrow & P_F & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \sum_\sigma \mathbb{R} & \longrightarrow & \mathrm{Div}_F & \longrightarrow & I_F & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & T & \longrightarrow & \mathrm{Pic}_F & \longrightarrow & \mathrm{Cl}_F & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

We now take degree 0 parts:

$$
\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{O}_F^*/\mu_F & \longrightarrow & F^*/\mu_F & \longrightarrow & P_F & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle \log} & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & (\sum_\sigma \mathbb{R})^0 & \longrightarrow & \mathrm{Div}_F^0 & \longrightarrow & I_F & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & T^0 & \longrightarrow & \mathrm{Pic}_F^0 & \longrightarrow & \mathrm{Cl}_F & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}
$$

Notice that by the Dirichlet unit theorem, the unit group $\mathcal{O}_F^*/\mu_F$ is a full lattice in the real vector space $(\sum_\sigma \mathbb{R})^0$ of dimension $r_1 + r_2 - 1$; therefore the quotient T^0 is a compact topological group. Since the class group is finite, the Picard group Pic_F^0 is a compact topological group. In fact, it is equivalent: the compactness of Pic_F^0 implies the Dirichlet unit theorem and the finiteness of the class group.

2. Ideal Lattices

We would like to now interpret this group. Recall that the class group Cl_K, the group of fractional ideals modulo principal fractional ideals, is the same as the group of fractional ideals up to $\mathcal{O}_F$-isomorphism, which is the same as the group of projective rank 1 $\mathcal{O}_F$-modules up to $\mathcal{O}_F$-isomorphism. We would like to know if we have a similar moduli interpretation for Pic_F.

Now consider

$$\mathcal{O}_F \subset F \subset F_\mathbb{R} = F \otimes_\mathbb{Q} \mathbb{R} = \mathbb{R}[T]/(f(T))$$

where $F = \mathbb{Q}(\alpha)$ if α is a root of $f(T)$. Then $F_\mathbb{R}$ is a product of $\mathbb{R}$ or $\mathbb{C}$ as σ ranges over the infinite primes of F:

$$F_\mathbb{R} \cong \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}.$$

The algebra $F_\mathbb{R}$ is an étale $\mathbb{R}$-algebra.

The Divisors gives an additive notation, but we would also like a multiplicative notation. Let D be the Arakelov divisor $D = \sum n_\mathfrak{p} \mathfrak{p} + \sum x_\sigma \sigma$. To the finite component we associate the ideal $I = \prod \mathfrak{p}^{-n_\mathfrak{p}}$, and to the infinite component we consider

$$(x_\sigma)_\sigma \in \prod_\sigma \mathbb{R} \xrightarrow{\exp} \prod_\sigma \mathbb{R}_{>0}^* \subset F_\mathbb{R}^*;$$

we let u be the inverse of the totally positive unit that comes from $\sum x_\sigma \sigma$. Then we write $D = (I, u)$.

Example 2.1. *The neutral element of this group is* $D = 0$*, which is* $D = (\mathcal{O}_F, 1)$*. Therefore* $-D = (I^{-1}, u^{-1})$*. For a principal divisor we have* $D = (f^{-1}\mathcal{O}_F, |f|)$*, where* $|f|_\sigma = |\sigma_f|$*.*

As the algebra $F_\mathbb{R}$ is étale, there is a canonical involution. On the real coordinates it acts as the identity, and on all of the complex coordinates we apply complex conjugation: $\overline{(x_\sigma)_\sigma} = (\overline{x_\sigma})_\sigma$. Given this, we have a canonical Euclidean structure on the algebra where for $x \in F_\mathbb{R}$,

$$||x||_{\text{can}}^2 = ||x||^2 = \text{Tr}(x\overline{x}).$$

This involution does not preserve F, unfortunately. With this structure, $\mathcal{O}_F \subset F \subset F_\mathbb{R}$ becomes a lattice.

Example 2.2. *For* $F = \mathbb{Q}(i)$*, we have* $\mathbb{Z}[i] \subset \mathbb{Q}(i) \subset \mathbb{C}$*, the usual square lattice in the complex numbers.*

For $F = \mathbb{Q}(\sqrt{2})$*, we have* $\mathbb{Z}[\sqrt{2}] \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{R} \times \mathbb{R}$*. In this lattice, the image of the rational numbers is along the diagonal* $1 \mapsto (1, 1)$*, whereas* $\sqrt{2} \mapsto (\sqrt{2}, -\sqrt{2})$ *maps to the antidiagonal.*

The covolume of the lattice associated to the ring of integers is $\sqrt{|\Delta_F|}$, where $|\Delta_F| = \det(\text{Tr}(\omega_i\omega_j))$, if $\mathcal{O}_F = \mathbb{Z}\omega_1 \oplus \cdots \oplus \mathbb{Z}\omega_n$.

For a more general Arakelov divisor $D = (I, u)$, then we map

$$I \hookrightarrow F_\mathbb{R}$$
$$f \mapsto uf$$

In this way, $I \subset I \otimes_\mathbb{Q} \mathbb{R}$ becomes a lattice. We then transport the metric and define $||f||_D = ||uf||_{\text{can}}$. Therefore I has both a structure of an $\mathcal{O}_F$-module and a Euclidean lattice, where $\langle \lambda x, y \rangle = \langle x, \overline{\lambda} y \rangle$ for $x, y \in I \otimes \mathbb{R}$, $\lambda \in F_\mathbb{R}$. In this case, the lattice has covolume $\sqrt{|\Delta_F|}e^{-\deg D}$.

We say that an *ideal lattice* is a fractional ideal with such a Euclidean structure; this is equivalent to giving a totally positive unit u.

We saw that the class group classifies projective rank 1 $\mathcal{O}_F$-modules up to isomorphism. Likewise, Pic_F classifies ideal lattices up to isometry (an $\mathcal{O}_F$-homomorphism which preserves length under the metric). Therefore Pic_F^0 classifies ideal lattices with fixed covolume $\sqrt{|\Delta_F|}$ up to isometry.

Recall from our complex we had the exact sequence

$$0 \to (\textstyle\prod_\sigma \mathbb{R})/\log|\mathcal{O}_F^*| \to \text{Pic}_F \to \text{Cl}_F \to 0.$$

The last map is the forgetful map $(I, u) \mapsto I$. Therefore different u give different metrics unless they arise from the image of $\log|\mathcal{O}_F^*|$.

Example 2.3. *For* $F = \mathbb{Q}$*,* $\text{Pic}_F = \mathbb{R} \cong \mathbb{R}_{>0}^*$ *by the exponential map. Every lattice looks like* $\mathbb{Z}$*, and the real number says how long the vector* 1 *is. If* F *is an imaginary quadratic field, then the factor* $(\prod_\sigma \mathbb{R})/\log|\mathcal{O}_F^*| = \mathbb{R}$*, again a scaling factor. The first interesting example is of a real quadratic field.*

3. Infrastructure and Reduced Divisors

First we see that ideal lattices do not contain very short vectors.

Proposition 3.1. *If $D = (I, u)$ is an ideal lattice of degree* 0*, then for $0 \neq f \in I$, then $||f||_D \geq \sqrt{n}$, where $n = [F : \mathbb{Q}]$.*

Proof. We write down

$$||f||_D^2 = ||uf||^2 = \mathrm{Tr}(uf\overline{uf}).$$

By the arithmetic-geometric mean, this is

$$\mathrm{Tr}(uf\overline{uf}) \geq nN(uf\overline{uf})^{1/n} = nN(uf)^{2/n}.$$

A short computation shows that $\deg D = -\log(NINu)$; since $\deg D = 0$, we see $N(Iu) = 1$, and since $f \in I$, $Nf \geq NI$, we conclude that

$$nN(uf)^{2/n} \geq nN(uI)^{2/n} = n.$$

□

For $F = \mathbb{Q}(\sqrt{d})$, $d > 0$, $\mathcal{O}_F^* = \pm\epsilon^{\mathbb{Z}}$. We have the exact sequence

$$0 \to (\prod_\sigma \mathbb{R})^0 / \log|\mathcal{O}_F^* \to \mathrm{Pic}_F^0 \to \mathrm{Cl}_F \to 0;$$

the first factor

$$(\prod_\sigma \mathbb{R})^0 / \log|\mathcal{O}_F^* \cong \mathbb{R}/(\log\epsilon)\mathbb{Z}$$

is a circle group. Dan Shanks first investigated this circle group in the 1970s to compute class groups of real quadratic fields and coined the term 'infrastructure'. This is already related to binary quadratic forms and the continued fraction expansion of $\sqrt{d}$. Lenstra in the 1980s and Buchmann in the 1990s generalized this our setting of Arakelov theory; now one computes the Picard group, and as a byproduct one obtains the class group.

We have seen that Pic_F^0 is a finite number $h_F = \#\,\mathrm{Cl}_F$ of circle groups (real vector space modulo a lattice). We will define a finite set of uniformly distributed divisors in Pic_F^0 to help us compute with this group. First we take the canonical metric on I coming from $\mathcal{O}_F$ and scale it uniformly so that it has degree 0.

Definition 3.2. *The Arakelov divisor $D = (I, u)$ is* reduced *if $I \subset \mathcal{O}_F$,*

$$u = (NI)^{-1/n} \in \mathbb{R}_{>0}^* \subset F_{\mathbb{R}}^*$$

embedded diagonally, and $1 \in I^{-1}$ is a minimal element.

If J is a fractional ideal, then we say that $0 \neq f \in J$ is minimal *if $g \in J$ has $|\sigma(g)| < |\sigma(f)|$ for all σ, then $g = 0$.*

Note that $\deg D = -\log NI + n \log NI^{1/n} = 0$. Put another way, f is minimal if there is no other nonzero lattice point in the 'box' defined by f.

We have the following:

- The statement that f is minimal in J does not depend on the metric on J (the unit only serves as a scaling factor).
- If f is a shortest nonzero element, then f is minimal. (However, the shortest vector might depend on the metric.) For example, $1 \in \mathcal{O}_F$ is a shortest vector for $D = (\mathcal{O}_F, 1)$, so it is minimal, and this is independent of the metric.
- If f in J is minimal, and $h \in F^*$, then $hf \in hJ$ is minimal. In particular, if $h = \epsilon$ is a unit, then $\epsilon f \in J$ is minimal. Therefore there are infinitely many minimal elements, but there are only finitely many shortest elements.

Example 3.3. *The neutral element* $(\mathcal{O}_F, 1)$ *is reduced, because* 1 *is a shortest vector.*

For a nonexample, if $\alpha \in \mathcal{O}_F$ *has* $|\sigma(\alpha)| > 1$ *for all* σ*, then* $I = (\alpha)$ *has* $D = (I, NI^{-1/n})$ *is not reduced. For* $1/\alpha \in I^{-1}$*, and* $|\sigma(1/\alpha)| < |\sigma(1)|$ *for all* σ*, so the divisor is not reduced.*

Proposition 3.4. *If* $D = (I, NI^{-1/n})$ *is reduced, then*

$$N(I^{-1}) \leq \sqrt{|\Delta_F|}.$$

Corollary 3.1. *There are only finitely many reduced divisors.*

In fact, with a bit of work we see that there are approximately $\sqrt{|\Delta_F|}$ ideals I with $N(I) \leq \sqrt{|\Delta_F|}$.

Proof. Consider $-D = (I^{-1}, NI^{-1/n})$. This gives rise to the lattice

$$I^{-1} \hookrightarrow F_{\mathbb{R}}$$
$$f \mapsto NI^{-1/n} f = uf.$$

Then the 'box' B of the image of 1 does not contain any lattice point, so by Minkowski

$$2^n NI \leq 2^{r_1}(2\pi)^{r_2}(NI^{1/n})^n = \mathrm{vol}(B) \leq 2^n\sqrt{|\Delta|}.$$

□

We now want to say that these reduced divisors are regularly distributed. To do this, we put a metric on Pic_F. But this is disconnected (it is a product of circle groups); recall we have

$$0 \to (\textstyle\prod_\sigma \mathbb{R})/\log|\mathcal{O}_F^*| \to \mathrm{Pic}_F \to \mathrm{Cl}_F \to 0;$$

We define the translation invariant metric on the connected component $\prod_\sigma \mathbb{R} \subset F_{\mathbb{R}}$. But $\prod_\sigma \mathbb{R} \subset F_{\mathbb{R}}$, which has a canonical metric which we carry back to Pic_F. Writing this down explicitly, we see for the element $(\mathcal{O}_F, u) \in \prod_\sigma \mathbb{R}/\log|\mathcal{O}_F^*|$ we define

$$||u||^2_{\mathrm{can}} = \sum_\sigma \deg\sigma |\log(u_\sigma)|^2$$

and thereby

$$||u||^2_{\mathrm{Pic}} = \min_{\epsilon \in \mathcal{O}_F^*} ||\epsilon u||^2_{\mathrm{can}}.$$

(Note that these are *not* the metrics on I, which are the objects parametrized by Pic_F.) From this we see that

$$\mathrm{vol}(\mathrm{Pic}_F^0) = h_F R_f \sqrt{n/2^{r_2}}$$

which by Brauer-Siegel is $\approx \sqrt{|\Delta_F|}$.

Now we show that for every divisor D, there is a reduced divisor which is close to it in Pic_F^0.

Theorem 3.5. *For all $D \in \mathrm{Div}_F^0$, there exists a reduced divisor D' and an $f \in F^*$, and $v \in F_{\mathbb{R}}$ such that*

$$D - D' = (f) + (\mathcal{O}_F, v)$$

with

$$||v||_{can} = ||(\mathcal{O}_F, v)||_{\mathrm{Pic}} < \sqrt{n} \log |\Delta_F|.$$

Proof. Let $D = (I, u)$, where $u = (u_\sigma)_\sigma$. By Minkowski, there is a $0 \neq f \in I^{-1}$ such that

$$|\sigma(f) u_\sigma^{-1}| < \mathrm{covol}(D)^{1/n} = \sqrt{|\Delta_F|}^{1/n}.$$

Take a shortest such vector f, which is therefore minimal. Since $f \in I^{-1}$, then $1 \in f^{-1} I^{-1}$ is minimal, so $D' = (fI, Nf(I)^{-1/n})$ is reduced.

Then

$$D - D' = (f) + (\mathcal{O}_F, v)$$

with

$$v_\sigma = u_\sigma |\sigma(f)|^{-1} N(fI)^{1/n}.$$

We want to show this is small, so we want to show $\log |u_\sigma|$ small. First we estimate the length of its inverse:

$$\log(v_\sigma^{-1}) = \log(u_\sigma^{-1} |\sigma(f)| N(fI)^{-1/n}) \leq \log |u_\sigma^{-1} \sigma(f)| \leq (1/n) \log |\Delta_F|$$

since $N(fI) \geq 1$. Also, since $D, D', (f)$ have degree 0, so does $(\mathcal{O}_F, v)$, and

$$\log(v_\sigma^{-1}) \geq -\frac{n-1}{n} \log \sqrt{\Delta_F}.$$

Therefore

$$|\log(v_\sigma)| \leq \log \sqrt{\Delta_F} = ||v||_{\mathrm{can}} \leq \sqrt{n} \log \sqrt{|\Delta_F|}.$$

□

This is an algorithmic proof, since there are good algorithms for computing shortest vectors in lattices. Also, this is more or less best possible, as one can see in the case of the real quadratic fields.

Now we would like to show that two reduced divisors cannot be too close to each other, but first we must modify the setup a bit.

The *modified Arakelov divisors* is the group

$$\widetilde{\mathrm{Div}}_F = I_F \times F_{\mathbb{R}}^*$$

where $D = (I, u)$, u any unit (not necessarily totally positive). A *principal modified divisor* $f \in F^*$ is $(f) = (f^{-1}\mathcal{O}_F, f)$. The quotient group is $\widetilde{\mathrm{Pic}}_F$, and defining the degree $\deg(I,u) = \deg(I,|u|)$, we see that inside we have the degree 0 part $\widetilde{\mathrm{Pic}}_F^0$. This is the *modified Arakelov divisor group.*

We have the exact sequence

$$0 \to (\mathbb{T}^{r_2} \times \{\pm 1\}^{r_1})/\mu_F \to \widetilde{\mathrm{Pic}}_F^0 \to \mathrm{Pic}_F^0 \to 0.$$

Here $\mathbb{T} = \{z \in \mathbb{C} : |z| = 1\}$. The kernel is often very small, e.g. for F real quadratic, it is $\{\pm 1\}$. We see that the reduced divisors in Pic_F^0 are 'rather dense' while they are 'rather sparse' in $\widetilde{\mathrm{Pic}}_F^0$.

But now we must also define a metric on $\widetilde{\mathrm{Pic}}_F^0$. Again we do it only on the connected component. Now we have an exact sequence

$$0 (\prod_\sigma U_\sigma)/\mathcal{O}_F^* \to \widetilde{\mathrm{Pic}}_F \to \mathrm{Cl}_{F,+} \to 0$$

where U_σ is $\mathbb{R}_{>0}^*$ or $\mathbb{C}^*$ as σ is real or complex, and $\mathrm{Cl}_{F,+}$ is the narrow class group. We have a map

$$F_\mathbb{R}/\exp^{-1}(\mathcal{O}_F^*) \xrightarrow{\exp} (\prod_\sigma U_\sigma)/\mathcal{O}_F^*$$

by the exponential map; but now we have a translation-invariant canonical metric on $F_\mathbb{R}$, which we transport back.

Theorem 3.6. *If $D, D' \in \widetilde{\mathrm{Div}}_F^0$ are reduced divisors and*

$$D - D' = (f) + (\mathcal{O}_F, v)$$

with

$$||v||_{\widetilde{\mathrm{Pic}}} < \log(4/3)$$

then $D = D'$.

Proof. Let $D = (I, NI^{-1/n})$, $D' = (J, NJ^{-1/n})$; then $1 \in I, J$ minimal. Since $IJ^{-1} = (f)^{-1}$ if and only if $fJ^{-1} = I^{-1}$, we see $f \in I^{-1}$ and $1 \in I^{-1}$ is minimal. Now $\lambda = (NJ/NI)^{1/n} = \sigma(f)v_\sigma$ for all sigma, where $\lambda \in \mathbb{R}_{>0}^* \subset F_\mathbb{R}^*$.

We will see now that f is very close to λ in $F_\mathbb{R}$. To see this, we will show

$$|\sigma(f) - \lambda| < \lambda/3.$$

This follows from

$$|(\sigma(f)/\lambda) - 1| = |v_\sigma^{-1} - 1| = |\exp^{-\log(v_\sigma)} - 1|$$
$$\leq \exp^{|\log(v_\sigma)| - 1} \leq \exp^{\log(4/3)} - 1 = 1/3.$$

If $0 < \lambda \leq 1/2$, then clearly f is in the box defined by 1. Indeed

$$|\sigma(f)| \leq |\sigma(f) - \lambda| + \lambda < \lambda/3 + \lambda \leq (4/3)(1/2) = 2/3 < 1 = \sigma(1)$$

for all σ, a contradiction.

If $\lambda \geq 3/2$ is large, then

$$|\sigma(f)| \geq \lambda - |\sigma(f) - \lambda| \geq \lambda - \lambda/3 \geq (3/2)(2/3) = 1 = |\sigma(1)|$$

contradicting the minimality of 1.

So $1/2 < \lambda < 3/2$. But now the vector $1 - f$ lives in the box of 1:

$$|\sigma(f-1)| \leq |\sigma(f) - \lambda| + |\lambda - 1| < (\lambda)/3 + 1/2 \leq (1/3)(3/2) + 1/2 = |\sigma(1)|.$$

So $1 - f = 0$, so $I = J$, and the two divisors are equal. □

For example, if $F = \mathbb{Q}(\sqrt{21})$, and $I = \mathbb{Z} + \mathbb{Z}(3 + \sqrt{21})/6$. Then $1 \in \mathbb{Z}$ is minimal, and show that for no metric u, 1 is the shortest vector.

Exercises

Exercise 5.1. Let $\alpha = \sqrt[3]{2}$ and $F = \mathbb{Q}(\alpha)$. Compute all valuations of the elements α, $\alpha - 1$ and $\alpha + 1$ and check that the degrees of the corresponding principal Arakelov divisors are zero.

Exercise 5.2. Show that the natural homomorphism from the group Div_F^0 of Arakelov divisors of degree 0 to the ideal group I_F is surjective.

Exercise 5.3. The ring of integers $\mathcal{O}_F$ of a number field F is in a natural way a lattice in the $\mathbb{R}$-algebra $F \otimes \mathbb{R}$ equipped with its canonical metric. Make a drawing of this lattice for $F = \mathbb{Q}(\sqrt{-23})$ and $F = \mathbb{Q}(\sqrt{21})$. Find the shortest vectors and exhibit all minimal vectors x for which $\|x\|_{\mathrm{can}} \leq 5$.

Exercise 5.4. Let $F = \mathbb{Q}(\sqrt{-5})$. For the fractional ideals $I = \mathcal{O}_F$ and $I = (2, 1 + \sqrt{-5})^{-1}$, the Arakelov divisors $(I, N(I)^{1/2})$ are reduced. Show this and draw the corresponding lattices.

Exercise 5.5. Let F be a number field. Show that the group of roots of unity μ_F of F is finite. Show that for $x \in \mathcal{O}_F$ one has that $\|x\|_{\mathrm{can}} = \sqrt{n}$ if and only if x is a root of unity.

Exercise 5.6. Let $F = \mathbb{Q}(\sqrt{61})$. Draw the Arakelov class group Pic_F^0 and the images of all reduced divisors in Pic_F^0.

Università di Roma "Tor Vergata",
Dipartimento di Matematica,
Via della Ricerca Scientifica,
I-00133 Roma, Italy,
schoof@mat.uniroma2.it
E-mail address: `schoof@mat.uniroma2.it`