Algorithmic Number Theory
MSRI Publications
Volume **44**, 2008

Computing Arakelov class groups

RENÉ SCHOOF

ABSTRACT. Shanks's infrastructure algorithm and Buchmann's algorithm for computing class groups and unit groups of rings of integers of algebraic number fields are most naturally viewed as computations inside Arakelov class groups. In this paper we discuss the basic properties of Arakelov class groups and of the set of reduced Arakelov divisors. As an application we describe Buchmann's algorithm in this context.

CONTENTS

1. Introduction 447
2. The Arakelov class group 449
3. Étale $\mathbb{R}$-algebras 451
4. Hermitian line bundles and ideal lattices 452
5. The oriented Arakelov class group 456
6. Metrics on Arakelov class groups 459
7. Reduced Arakelov divisors 464
8. Quadratic fields 472
9. Reduced Arakelov divisors; examples and counterexamples 474
10. Computations with reduced Arakelov divisors 479
11. A deterministic algorithm 484
12. Buchmann's algorithm 489
Acknowledgements 493
References 493

1. Introduction

Daniel Shanks [1972] observed that the forms in the principal cycle of reduced binary quadratic forms of positive discriminant exhibit a group-like behavior. This was a surprising phenomenon, because the principal cycle itself constitutes the trivial class of the class group. Shanks called this group-like

structure 'inside' the neutral element of the class group the *infrastructure*. He exploited it by designing an efficient algorithm to compute the regulator of a real quadratic number field. Later, H. W. Lenstra [1982] (see also [Schoof 1982]) made Shanks' observations more precise, introducing a certain topological group and providing a satisfactory framework for Shanks's algorithm. Both Shanks [1976, Section 1; 1979, 4.4], and Lenstra [1982, section 15] indicated that the infrastructure ideas could be generalized to arbitrary number fields. This was done first by H. Williams and his students [Williams et al. 1983] for complex cubic fields, then by J. Buchmann [1987a; 1987b; 1987c] and by Buchmann and Williams [1989]. Finally Buchmann [1990; 1991] described an algorithm for computing the class group and regulator of an arbitrary number field that, under reasonable assumptions, has a subexponential running time. It has been implemented in the computer algebra packages LiDIA, MAGMA and PARI.

In these expository notes we present a natural setting for the infrastructure phenomenon and for Buchmann's algorithm. It is provided by Arakelov theory [Szpiro 1985, 1987; Van der Geer and Schoof 2000]. We show that Buchmann's algorithm for computing the class number and regulator of a number field F has a natural description in terms of the *Arakelov class group* Pic_F^0 of F and the set Red_F of *reduced Arakelov divisors*. We show that Lenstra's topological group is essentially equal to the Arakelov class group of a real quadratic field. We also introduce the *oriented Arakelov class group* $\widetilde{\mathrm{Pic}}_F^0$. This is a natural generalization of Pic_F^0, useful for analyzing Buchmann's algorithm and for computing the units of the ring of integers O_F themselves rather than just the regulator.

The main result of this paper is formulated in Theorems 7.4 and 7.7. It says that the finite set Red_F of reduced Arakelov divisors is, in a precise sense, regularly distributed in the compact Arakelov class groups Pic_F^0 and $\widetilde{\mathrm{Pic}}_F^0$.

In Section 2 we introduce the Arakelov class group of a number field F. In Section 3 we study the étale $\mathbb{R}$-algebra $F \otimes_{\mathbb{Q}} \mathbb{R}$. In Section 4 we discuss the relations between Arakelov divisors, Hermitian line bundles and ideal lattices. In Section 5 we define the oriented Arakelov class group and in Section 6 we give both Arakelov class groups a natural translation invariant Riemannian structure. The rest of the notes is devoted to computational issues. Section 7 contains the main results. Here we introduce *reduced* Arakelov divisors and describe their basic properties. In Section 8, we work out the details for quadratic number fields. In Section 9 we present explicit examples illustrating various properties of reduced divisors. In Section 10 we discuss the computational aspects of reduced Arakelov divisors. In Section 11 we present a *deterministic* algorithm to compute the Arakelov class group. Finally, in Section 12 we present Buchmann's algorithm from the point of view of Arakelov theory. See [Marcus 1977] for the basic properties of algebraic number fields.

2. The Arakelov class group

In this section we introduce the Arakelov class group of a number field F. This group is analogous to the degree zero subgroup of the Picard group of a complete algebraic curve. In order to have a good analogy with the geometric situation, we formally 'complete' the spectrum of the ring of integers O_F by adjoining primes at infinity. An *infinite* prime of F is a field homomorphism $\sigma : F \longrightarrow \mathbb{C}$, considered up to complex conjugation. An infinite prime σ is called *real* when $\sigma(F) \subset \mathbb{R}$ and *complex* otherwise. We let r_1 and r_2 denote the number of real and complex infinite primes, respectively. We have $r_1 + 2r_2 = n$ where $n = [F : \mathbb{Q}]$.

An *Arakelov divisor* is a formal finite sum $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}}\mathfrak{p} + \sum_{\sigma} x_{\sigma}\sigma$, where $\mathfrak{p}$ runs over the nonzero prime ideals of O_F and σ runs over the infinite primes of F. The coefficients $n_{\mathfrak{p}}$ are in $\mathbb{Z}$ but the x_{σ} can be any number in $\mathbb{R}$. The Arakelov divisors form an additive group, the Arakelov divisor group Div_F. It is isomorphic to $\bigoplus_{\mathfrak{p}} \mathbb{Z} \times \bigoplus_{\sigma} \mathbb{R}$. The *principal* Arakelov divisor associated to an element $f \in F^*$ is the divisor $(f) = \sum_{\mathfrak{p}} n_{\mathfrak{p}}\mathfrak{p} + \sum_{\sigma} x_{\sigma}\sigma$ with $n_{\mathfrak{p}} = \mathrm{ord}_{\mathfrak{p}}(f)$ and $x_{\sigma}(f) = -\log|\sigma(f)|$. The principal Arakelov divisors form a subgroup of Div_F.

Since it is analogous to the Picard group of an algebraic curve, the quotient of Div_F by its subgroup of principal Arakelov divisors is denoted by Pic_F. A principal Arakelov divisor (f) is trivial if and only if f is a unit of O_F all of whose conjugates have absolute value equal to 1. It follows that (f) is trivial if and only if f is contained in the group of roots of unity μ_F. Therefore there is an exact sequence

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

We call $I = \prod_{\mathfrak{p}} \mathfrak{p}^{-n_{\mathfrak{p}}}$ the *ideal associated* to an Arakelov divisor $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}}\mathfrak{p} + \sum_{\sigma} x_{\sigma}\sigma$. The ideal associated to the zero Arakelov divisor is the ring of integers O_F. The ideal associated to a principal Arakelov divisor (f) is the principal ideal $f^{-1}O_F$. Here and in the rest of the paper we often call fractional ideals simply 'ideals'. If we want to emphasize that an ideal is integral, we call it an O_F-ideal.

The map that sends a divisor D to its associated ideal I is a homomorphism from Div_F to the group of fractional ideals Id_F of F. Its kernel is the group $\bigoplus_{\sigma} \mathbb{R}$ of divisors supported in the infinite primes. We have the commutative diagram at the top of the next page, the rows and columns of which are exact. In the diagram, Pid_F denotes the group of principal ideals of F. The map $F^*/\mu_F \longrightarrow \mathrm{Div}_F$ induces a homomorphism from O_F^*/μ_F to $\bigoplus_{\sigma} \mathbb{R}$. This homomorphism is given by $\varepsilon \mapsto (-\log|\sigma(\varepsilon)|)_{\sigma}$ and its cokernel is denoted by T.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & O_F^*/\mu_F & \longrightarrow & F^*/\mu_F & \longrightarrow & \mathrm{Pid}_F & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \bigoplus_\sigma \mathbb{R} & \longrightarrow & \mathrm{Div}_F & \longrightarrow & \mathrm{Id}_F & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & T & \longrightarrow & \mathrm{Pic}_F & \longrightarrow & Cl_F & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

The *norm* $N(\mathfrak{p})$ of a nonzero prime ideal $\mathfrak{p}$ of O_F is the order of its residue field $O_F/\mathfrak{p}$. The *degree* $\deg(\mathfrak{p})$ of $\mathfrak{p}$ is defined as $\log N(\mathfrak{p})$. The degree of an infinite prime σ is equal to 1 or 2 depending on whether σ is real or complex. The degree extends by linearity to a surjective homomorphism $\deg : \mathrm{Div}_F \longrightarrow \mathbb{R}$. The *norm* $N(D)$ of a divisor D is defined as $N(D) = e^{\deg(D)}$. The divisors of degree 0 form a subgroup Div_F^0 of Div_F. By the product formula, Div_F^0 contains the principal Arakelov divisors.

DEFINITION 2.1. Let F be a number field. The *Arakelov class group* Pic_F^0 of F is the quotient of Div_F^0 by its subgroup of principal divisors.

The degree map $\deg : \mathrm{Div}_F \longrightarrow \mathbb{R}$ factors through Pic_F and the Arakelov class group is the kernel of the induced homomorphism $\deg : \mathrm{Pic}_F \longrightarrow \mathbb{R}$. We let $(\bigoplus_\sigma \mathbb{R})^0$ denote the subgroup of divisors in $\bigoplus_\sigma \mathbb{R}$ that have degree zero and T^0 the cokernel of the homomorphism $O_F^* \longrightarrow (\bigoplus_\sigma \mathbb{R})^0$. In other words, T^0 is the quotient of the vector space $\left\{(v_\sigma)_\sigma \in \bigoplus_\sigma \mathbb{R} : \sum_\sigma \deg(\sigma) v_\sigma = 0\right\}$ by the group of vectors $\{(\log|\sigma(\varepsilon)|)_\sigma : \varepsilon \in O_F^*\}$. By Dirichlet's unit theorem, T^0 is a compact real torus.

PROPOSITION 2.2. *There is a natural exact sequence*

$$0 \longrightarrow T^0 \longrightarrow \mathrm{Pic}_F^0 \longrightarrow Cl_F \longrightarrow 0.$$

PROOF. Since F has at least one infinite prime, the composite map $\mathrm{Div}_F^0 \hookrightarrow \mathrm{Div}_F \longrightarrow \mathrm{Id}_F$ is still surjective. The result now follows by replacing the groups Div_F, Pic_F, T and $\bigoplus_\sigma \mathbb{R}$ in the diagram above by their degree 0 subgroups. □

The group T^0 is the connected component of the identity of the topological group Pic_F^0. It follows that Pic_F^0, being an extension of the finite class group by T^0, is a compact real Lie group of dimension $r_1 + r_2 - 1$.

DEFINITION 2.3. The natural homomorphism $\mathrm{Div}_F^0 \longrightarrow \mathrm{Id}_F$ admits a section

$$d : \mathrm{Id}_F \longrightarrow \mathrm{Div}_F^0.$$

It is given by $d(I) = D$ where $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}}\mathfrak{p} + \sum_\sigma x_\sigma \sigma$ is the Arakelov divisor for which $I = \prod_{\mathfrak{p}} \mathfrak{p}^{-n_{\mathfrak{p}}}$ and $x_\sigma = (1/n)\log N(I)$ for every infinite prime σ.

PROPOSITION 2.4. *Let $\bar{d} : \mathrm{Id}_F \longrightarrow \mathrm{Pic}_F^0$ denote the homomorphism that maps I to the class of the divisor $d(I)$. Then the sequence*

$$0 \longrightarrow \{f \in F^* : \textit{all } |\sigma(f)| \textit{ are equal}\}/\mu_F \longrightarrow \mathrm{Id}_F \xrightarrow{\bar{d}} \mathrm{Pic}_F^0$$

is exact. Moreover, the image of $\bar{d}$ is dense in Pic_F^0.

This proposition is not used in the rest of the paper. It can be proved along the lines of (and in fact follows immediately from) Proposition 6.4 below. The kernel of $\bar{d}$ is not a very convenient group to work with, and this is one of the reasons for introducing *oriented* Arakelov divisors below.

Finally we remark that there is a natural surjective continuous homomorphism $\mathbf{A}_F^* \longrightarrow \mathrm{Div}_F$ from the idèle group $\mathbf{A}_F^*$ to the Arakelov divisor group. It follows that Pic_F is a quotient of the idèle class group. We do not make any use of this fact in the rest of the paper.

3. Étale $\mathbb{R}$-algebras

Let F be a number field of degree n. In this section we study the $\mathbb{R}$-algebra $F_{\mathbb{R}} = F \otimes_{\mathbb{Q}} \mathbb{R}$.

For any infinite prime σ of F, we write F_σ for $\mathbb{R}$ or $\mathbb{C}$ depending on whether σ is real or complex. The natural map $F \longrightarrow \prod_\sigma F_\sigma$ sending $f \in F$ to the vector $(\sigma(f))_\sigma$ induces an isomorphism $F_{\mathbb{R}} = F \otimes_{\mathbb{Q}} \mathbb{R} \cong \prod_\sigma F_\sigma$ of $\mathbb{R}$-algebras. Let $u \mapsto \bar{u}$ denote the canonical conjugation of the étale algebra $F_{\mathbb{R}}$. In terms of the isomorphism $F_{\mathbb{R}} \cong \prod_\sigma F_\sigma$, it is simply the morphism that maps a vector $u = (u_\sigma)_\sigma$ to $\bar{u} = (\bar{u}_\sigma)_\sigma$. In these terms it is also easy to describe the set of invariants of the canonical conjugation. It is the subalgebra $\prod_\sigma \mathbb{R}$ of $\prod_\sigma F_\sigma$.

For any $u \in F_{\mathbb{R}}$, we define the norm $N(u)$ and trace $\mathrm{Tr}(u)$ of u as the determinant and trace of an $n \times n$-matrix (with respect to any $\mathbb{R}$-basis) of the $\mathbb{R}$-linear map $F_{\mathbb{R}} \longrightarrow F_{\mathbb{R}}$ given by multiplication by u. In terms of coordinates, we have for $u = (u_\sigma)_\sigma \in \prod_\sigma F_\sigma$ that $\mathrm{Tr}(u) = \sum_\sigma \deg(\sigma)\mathrm{Re}(u_\sigma)$ while $N(u) = \prod_{\sigma \text{ real}} u_\sigma \prod_{\sigma \text{ complex}} u_\sigma \bar{u}_\sigma$.

Being an étale $\mathbb{R}$-algebra, $F_{\mathbb{R}}$ admits a canonical Euclidean structure; see for instance [Groenewegen 2001]. It is given by the scalar product

$$\langle u, v\rangle = \mathrm{Tr}(u\bar{v}) \quad \text{for } u, v \in F_{\mathbb{R}}.$$

This scalar product has the 'Hermitian' property $\langle \lambda u, v\rangle = \langle u, \bar{\lambda} v\rangle$ for $u, v, \lambda \in F_{\mathbb{R}}$. In terms of coordinates, we have for $u = (u_\sigma)_\sigma$ and $v = (v_\sigma)_\sigma$ in $F_{\mathbb{R}} \cong \prod_\sigma F_\sigma$ that

$$\langle u, v\rangle = \sum_\sigma \deg(\sigma)\mathrm{Re}(u_\sigma \bar{v}_\sigma).$$

We write $\|u\| = \langle u, u\rangle^{1/2}$ for the *length* of $u \in F_{\mathbb{R}}$. For the element $1 \in F \subset F_{\mathbb{R}}$ we have $\|1\| = \sqrt{n}$. For every $u \in F_{\mathbb{R}}$, all coordinates of the product $u\bar{u} \in \prod_\sigma F_\sigma$ are nonnegative real numbers. We define $|u|$ to be the vector

$$|u| = (|u_\sigma|)_\sigma$$

in the group $\prod_\sigma \mathbb{R}_+^* \subset F_{\mathbb{R}}^*$. Here we let $\mathbb{R}_+^* = \{x \in \mathbb{R}^* : x > 0\}$. We have $|u|^2 = u\bar{u}$. The map $u \mapsto |u|$ is a homomorphism. It is a section of the inclusion map $\prod_\sigma \mathbb{R}_+^* \subset F_{\mathbb{R}}^*$.

PROPOSITION 3.1. *Let F be a number field of degree n. For every $u \in F_{\mathbb{R}}$,*

(i) $$N(u\bar{u})^{1/n} \le \tfrac{1}{n}\mathrm{Tr}(u\bar{u});$$

(ii) $$|N(u)| \le n^{-n/2}\|u\|^n.$$

In either case, equality holds if and only if u is contained in the subalgebra $\mathbb{R}$ of $F_{\mathbb{R}}$.

PROOF. Since all coordinates of $u\bar{u}$ are nonnegative, (i) is just the arithmetic-geometric mean inequality. The second inequality follows from (i) and the fact that $N(\bar{u}) = N(u)$. □

4. Hermitian line bundles and ideal lattices

In this section we introduce the Hermitian line bundles and ideal lattices associated to Arakelov divisors and study some of their properties.

Let F be a number field of degree n and let $D = \sum_{\mathfrak{p}} n_{\mathfrak{p}}\mathfrak{p} + \sum_\sigma x_\sigma \sigma$ be an Arakelov divisor. By $I = \prod_{\mathfrak{p}} \mathfrak{p}^{-n_{\mathfrak{p}}}$ we denote the ideal associated to D in Section 2 and by u the unit $(\exp(-x_\sigma))_\sigma \in \prod_\sigma \mathbb{R}_+^* \subset F_{\mathbb{R}}^*$. This leads to the following definition.

DEFINITION 4.1. Let F be a number field. A *Hermitian line bundle* is a pair (I, u) where I is a fractional F-ideal and u a unit of the algebra $F_{\mathbb{R}} \cong \prod_\sigma F_\sigma$ all of whose coordinates are positive real numbers.

As we explained above, to every Arakelov divisor D there corresponds a Hermitian line bundle (I, u). This correspondence is bijective and we often identify the two notions. The zero Arakelov divisor corresponds to the trivial bundle $(O_F, 1)$. A principal Arakelov divisor (f) corresponds to the Hermitian line

bundle $(f^{-1}O_F, |f|)$ and the divisor $d(I)$ associated to a fractional ideal I at the end of Section 2, corresponds to the pair $(I, N(I)^{-1/n})$. Note that $N(I)^{-1/n}$ is contained in the 'diagonal' subgroup $\mathbb{R}_+^*$ of $\prod_\sigma \mathbb{R}_+^*$. It follows from the formulas for $N(u)$ given in the previous section that the degree of an Arakelov divisor $D = (I, u)$ is equal to $-\log(|N(u)|\,N(I))$.

DEFINITION 4.2. Let F be a number field. An *ideal lattice* of F is a projective O_F-module L of rank 1 equipped with a real-valued positive definite scalar product on $L \otimes_{\mathbb{Z}} \mathbb{R}$ satisfying $\langle \lambda x, y\rangle = \langle x, \bar{\lambda} y\rangle$ for $x, y \in L \otimes_{\mathbb{Z}} \mathbb{R}$ and $\lambda \in F_{\mathbb{R}}$. Two ideal lattices L, L' are called *isometric* if there is an O_F-isomorphism $L \cong L'$ that is compatible with the scalar products on $L \otimes_{\mathbb{Z}} \mathbb{R}$ and $L' \otimes_{\mathbb{Z}} \mathbb{R}$.

Here $\lambda \mapsto \bar{\lambda}$ is the canonical algebra involution of the étale $\mathbb{R}$-algebra $F_{\mathbb{R}}$ introduced in Section 3. Note that it need not preserve F. Note also that $L \otimes_{\mathbb{Z}} \mathbb{R}$ has the structure of an $F_{\mathbb{R}}$-module. See [Bayer-Fluckiger 1999; Groenewegen 2001] for more on ideal lattices. There is a natural way to associate an ideal lattice to an Arakelov divisor D. It is most naturally expressed in terms of the Hermitian line bundle (I, u) associated to D. The O_F-module I is projective and of rank 1. Multiplication by u gives an O_F-isomorphism with $uI = \{ux : x \in I\} \subset F_{\mathbb{R}}$. The canonical scalar product on $F_{\mathbb{R}}$ introduced in Section 3 gives uI the structure of an ideal lattice. Alternatively, putting

$$\|f\|_D = \|uf\|, \qquad \text{for } f \in I,$$

we obtain a scalar product on I itself that we extend by linearity to $I \otimes_{\mathbb{Z}} \mathbb{R}$. In additive notation, if $f \in I$ and $u \in F_{\mathbb{R}}^*$ is equal to $\exp((-x_\sigma)_\sigma)$, then uf is equal to the vector $(\sigma(f)e^{-x_\sigma})_\sigma \in F_{\mathbb{R}}$ and we have $\|f\|_D^2 = \|uf\|^2 = \sum_\sigma \deg(\sigma)|\sigma(f)e^{-x_\sigma}|^2$ for $f \in I$.

The ideal lattice corresponding to the zero Arakelov divisor, i.e. to the trivial bundle $(O_F, 1)$, is the ring of integers O_F viewed as a subset of $F \subset F_{\mathbb{R}}$ equipped with its canonical Euclidean structure. The covolume of this lattice is equal to $\sqrt{|\Delta_F|}$, where Δ_F denotes the discriminant of the number field F. The covolume of the lattice associated to an arbitrary divisor $D = (I, u)$ is equal to

$$\operatorname{covol}(D) = \sqrt{|\Delta_F|}\,N(I)|N(u)| = \sqrt{|\Delta_F|}/N(D) = \sqrt{|\Delta_F|}e^{-\deg(D)}.$$

For any ideal I, the lattice associated to the Arakelov divisor

$$d(I) = (I, N(I)^{-1/n})$$

can be thought of as the lattice $I \subset F \subset F_{\mathbb{R}}$ equipped with the canonical scalar product of $F_{\mathbb{R}}$, but *scaled* with a factor $N(I)^{-1/n}$ so that its covolume is equal to $\sqrt{|\Delta_F|}$.

PROPOSITION 4.3. *Let F be a number field of discriminant Δ_F.*

(i) *The map that associates the ideal lattice uI to an Arakelov divisor $D = (I, u)$, induces a bijection between the group* Pic_F *and the set of isometry classes of ideal lattices.*

(ii) *The same map induces a bijection between the group* Pic_F^0 *and the set of isometry classes of ideal lattices of covolume* $\sqrt{|\Delta_F|}$.

PROOF. Let $D = (I, u)$ be an Arakelov divisor and let $D' = D + (g)$ for some $g \in F^*$. Then $D' = (g^{-1}I, u|g|)$ and multiplication by g induces an isomorphism $g^{-1}I \cong I$ of O_F-modules. This map is also an isometry between the associated lattices since

$$\|g^{-1}f\|_{D'} = \|u\,|g|\,g^{-1}f\| = \|uf\| = \|f\|_D$$

for all $f \in I \otimes_{\mathbb{Z}} \mathbb{R}$. Here we have used the fact that $v = |g|\,g^{-1}$ satisfies $v\bar{v} = 1$ and that therefore $\|vh\| = \mathrm{Tr}(vh\bar{v}\bar{h}) = \mathrm{Tr}(h\bar{h}) = \|h\|$ for all $h \in I \otimes_{\mathbb{Z}} \mathbb{R}$. We conclude that the map that sends an Arakelov divisor to its associated ideal lattice induces a well defined map from Pic_F to the set of isometry classes of ideal lattices. This map is *injective*. Indeed, if $D = (I, u)$ and $D' = (I', u')$ give rise to isometric lattices, then there exists $g \in F^*$ so that $I' = gI$ and $\|gf\|_{D'} = \|f\|_D$ for all $f \in I \otimes_{\mathbb{Z}} \mathbb{R}$. This means that $\|u'gf\| = \|uf\|$ for all $f \in I \otimes_{\mathbb{Z}} \mathbb{R} = F_{\mathbb{R}}$. For any infinite prime σ, we let $e_\sigma \in F_{\mathbb{R}}$ be the idempotent for which $\sigma(e_\sigma) = 1$ while $\sigma'(e_\sigma) = 0$ for all $\sigma' \neq \sigma$. Substituting $f = e_\sigma$, we find that $|\sigma(g)u'_\sigma| = |u_\sigma|$ for every σ. It follows that $|g| = u/u'$, implying that $D' = D + (g)$ as required.

To see that the map is *surjective*, consider an ideal lattice L with Hermitian scalar product $\langle\langle -, - \rangle\rangle$ on $L \otimes_{\mathbb{Z}} \mathbb{R} = F_{\mathbb{R}}$. We may assume that L is actually an O_F-ideal. The idempotent elements e_σ in $F_{\mathbb{R}} \cong \prod_\sigma F_\sigma$ are invariant under the canonical involution. This implies that the e_σ are pairwise orthogonal because $\langle\langle e_\sigma, e_{\sigma'} \rangle\rangle = \langle\langle e_\sigma^2, e_{\sigma'} \rangle\rangle = \langle\langle e_\sigma, e_\sigma e_{\sigma'} \rangle\rangle = 0$. Therefore the real numbers $u_\sigma = \langle\langle e_\sigma, e_\sigma \rangle\rangle^{1/2}$ determine the metric on $I \otimes_{\mathbb{Z}} \mathbb{R}$. The Arakelov divisor (L, u) with $u = (u_\sigma)_\sigma \in \prod_\sigma \mathbb{R}_+^*$ is then mapped to the isometry class of L.

This proves (i). Part (ii) follows immediately from this. □

The following proposition deals with the lengths of the shortest nonzero vectors in the lattices associated to Arakelov divisors.

PROPOSITION 4.4. *Let F be a number field of degree n and let $D = (I, u)$ be an Arakelov divisor.*

(i) *For every nonzero f in I we have*

$$\|f\|_D \geq \sqrt{n}e^{-\frac{1}{n}\deg D}.$$

Moreover, equality holds if and only if $D = (fO_F, \lambda|f|^{-1})$ *for some* $\lambda > 0$. *In other words, if and only if* D *is equal to the principal Arakelov divisor* $-(f)$, *scaled by a positive factor* λ.

(ii) *There exists a nonzero* $f \in I$ *such that* $|u_\sigma \sigma(f)| < (2/\pi)^{r_2/n} \operatorname{covol}(D)^{1/n}$ *for every* σ *and hence*

$$\|f\|_D \leq \sqrt{n} \cdot (2/\pi)^{r_2/n} \operatorname{covol}(D)^{1/n}.$$

Here r_2 *is the number of complex primes of* F.

PROOF. (i) Take $f \in I$. By Proposition 3.1 we have

$$\|f\|_D^2 = \|uf\|^2 \geq n|N(uf)|^{2/n}.$$

Since $|N(f)| \geq N(I)$ we find that

$$\|f\|_D^2 \geq n|N(u)N(I)|^{2/n} = ne^{-(2/n)\deg(D)}.$$

The last inequality follows from the fact that $\deg(D) = -\log|N(u)N(I)|$. This proves the first statement. By Proposition 3.1, equality holds if and only if all $|u_\sigma \sigma(f)|$ are equal to some $\lambda > 0$ and if I is the principal ideal generated by f. This implies that D is of the form $(f^{-1}O_F, |f|^{-1}\lambda)$ as required.

(ii) Consider the set $V = \{(y_\sigma)_\sigma \in F_\mathbb{R} : |y_\sigma| \leq (2/\pi)^{r_2/n} \operatorname{covol}(D)^{1/n} \text{ for all } \sigma\}$. This is a bounded symmetric convex set of volume

$$2^{r_1}(2\pi)^{r_2}(2/\pi)^{r_2} \operatorname{covol}(D) = 2^n \operatorname{covol}(D).$$

By Minkowski's Convex Body Theorem there exists a nonzero element $f \in I$ for which $(u_\sigma \sigma(f))_\sigma \in uI \subset F_\mathbb{R}$ is in V. This implies (ii). □

We mention the following special case of the proposition.

COROLLARY 4.5. *Let* $D = (I, u)$ *be an Arakelov divisor of degree 0. Then any nonzero* $f \in I$ *has the property that* $\|f\|_D \geq \sqrt{n}$, *with equality if and only if* $D = -(f)$. *On the other hand, there exists a nonzero* $f \in I$ *with*

$$\|f\|_D \leq \sqrt{n}\,(2/\pi)^{r_2/n}\,\sqrt{|\Delta_F|}^{1/n}.$$

Proposition 4.4(i) says that the lattices uI associated to Arakelov divisors $D = (I.u)$ are rather 'nice'. They are not very skew in the sense that they do not contain any nonzero vectors that are extremely short with respect to $\operatorname{covol}(D)^{1/n}$. This property can be expressed by means of the *Hermite constant* $\gamma(D) = \gamma(uI)$. The latter is defined as the square of the length of the shortest nonzero vector in the lattice uI associated to D divided by $\operatorname{covol}(D)^{2/n}$. The more skew the lattice, the smaller is its Hermite constant. The constant $\gamma(D)$ only depends on the class of D in Pic_F.

COROLLARY 4.6. *Let F be a number field of degree n and let $D = (I, u)$ be an Arakelov divisor. Then*

$$\frac{n}{|\Delta_F|^{1/n}} \;\le\; \gamma(D) \;\le\; n\Big(\frac{2}{\pi}\Big)^{2r_2/n}.$$

The lower bound is attained if and only if D is a principal divisor scaled by some $\lambda > 0$ as in Proposition 4.4(i).

The function $h^0(D) = \log\big(\sum_{f\in I} \exp(-\pi \| f \|_D^2)\big)$ introduced in [Van der Geer and Schoof 2000] and briefly discussed in Section 10 is related to the Hermite constant $\gamma(D)$. Indeed, for most Arakelov divisors $D = (I, u)$ the shortest nonzero vectors in the associated lattice are equal to products of a root of unity by one fixed shortest vector. Moreover, for most D the contributions of the zero vector and these vectors contribute the bulk to the infinite sum $\sum_{f\in I} \exp(-\pi \| f \|_D^2)$. Therefore, for most Arakelov divisors D the quantity $(h^0(D) - 1)/w_F$ is close to $\exp(-\pi\gamma(D)\operatorname{covol}(D)^{2/n})$. Here w_F denotes the number of roots of unity in the field F.

5. The oriented Arakelov class group

In this section we introduce the oriented Arakelov divisor group $\widetilde{\operatorname{Pic}}_F$ associated to a number field F.

In Section 4 we have associated to an Arakelov divisor D a Hermitian line bundle (I, u). Here I is an ideal and u is a unit in the *subgroup* $F^*_{\mathbb{R},+} = \prod_\sigma \mathbb{R}^*_+$ of $F^*_{\mathbb{R}}$. An *oriented* Hermitian line bundle is a pair (I, u) where I is an ideal and u is an *arbitrary* unit in $F^*_{\mathbb{R}} \cong \prod_\sigma F^*_\sigma$. The corresponding *oriented Arakelov divisors* are formal sums $\sum_{\mathfrak{p}} n_{\mathfrak{p}}\mathfrak{p} + \sum_\sigma x_\sigma \sigma$ with $n_{\mathfrak{p}} \in \mathbb{Z}$ and $x_\sigma \in F^*_\sigma$. They form a group $\widetilde{\operatorname{Div}}_F$ and we have

$$\widetilde{\operatorname{Div}}_F \cong \operatorname{Id}_F \times F^*_{\mathbb{R}} \cong \bigoplus_{\mathfrak{p}} \mathbb{Z} \times \prod_\sigma F^*_\sigma.$$

The *principal* oriented Arakelov divisor associated to $f \in F^*$ is simply the oriented divisor corresponding to the oriented Hermitian bundle $(f^{-1}O_F, f)$, where the second coordinate f is viewed as an element of $F^*_{\mathbb{R}}$. The cokernel of the injective homomorphism $F^* \longrightarrow \widetilde{\operatorname{Div}}_F$ is denoted by $\widetilde{\operatorname{Pic}}_F$. The inclusion $\operatorname{Div}_F \subset \widetilde{\operatorname{Div}}_F$ admits the natural section $\widetilde{\operatorname{Div}}_F \longrightarrow \operatorname{Div}_F$ given by $(I, u) \mapsto (I, |u|)$. The degree $\deg(D)$ of an oriented Arakelov divisor $D = (I, u)$ is by definition the degree of the 'ordinary' Arakelov divisor $(I, |u|)$. In this way principal oriented Arakelov divisors have degree 0.

DEFINITION 5.1. The quotient of the group $\widetilde{\mathrm{Div}}_F^0$ of oriented Arakelov divisors of degree 0 by the subgroup of principal divisors is called the *oriented Arakelov class group*. It is denoted by $\widetilde{\mathrm{Pic}}_F^0$.

The commutative diagram below has exact rows and columns. The bottom row relates the groups $\widetilde{\mathrm{Pic}}_F^0$ and Pic_F^0 to one another.

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mu_F & \longrightarrow & F^* & \longrightarrow & F^*/\mu_F & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \prod_\sigma K_\sigma & \longrightarrow & \widetilde{\mathrm{Div}}_F^0 & \longrightarrow & \mathrm{Div}_F^0 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & (\prod_\sigma K_\sigma)/\mu_F & \longrightarrow & \widetilde{\mathrm{Pic}}_F^0 & \longrightarrow & \mathrm{Pic}_F^0 & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

Here K_σ denotes the maximal compact subgroup of F_σ^*. In other words $K_\sigma = \{1, -1\}$ if σ is real, while $K_\sigma = \{z \in \mathbb{C}^* : |z| = 1\}$ if σ is complex. Since Pic_F^0 and the groups K_σ are compact, it follows from the exactness of the bottom row of the diagram that $\widetilde{\mathrm{Pic}}_F^0$ is compact as well.

In order to see the topological structure of $\widetilde{\mathrm{Pic}}_F^0$ better, we construct a second exact sequence. Let $F^*_{\mathbb{R},\,\mathrm{conn}}$ denote the connected component of $1 \in F_{\mathbb{R}}^*$. It is isomorphic to a product of copies of $\mathbb{R}_+^*$ for the real primes and $F_\sigma^* = \mathbb{C}^*$ for the complex ones. It is precisely the kernel of the homomorphism

$$\widetilde{\mathrm{Div}}_F \longrightarrow \mathrm{Id}_F \times \prod_{\sigma \text{ real}} \{\pm 1\},$$

given by mapping $D = (I, u)$ to $(I, \mathrm{sign}(u))$. Here $\mathrm{sign}(u)$ denotes the vector $(\mathrm{sign}(u_\sigma))_{\sigma \text{ real}}$.

DEFINITION 5.2. By $\widetilde{T}$ we denote the quotient of the group $F^*_{\mathbb{R},\,\mathrm{conn}}$ by its subgroup $O^*_{F,+} = \{\varepsilon \in O_F^* : \sigma(\varepsilon) > 0 \text{ for all real } \sigma\}$. Taking degree zero subgroups, we put

$$(F^*_{\mathbb{R},\,\mathrm{conn}})^0 = \{u \in F^*_{\mathbb{R},\,\mathrm{conn}} : N(u) = 1\} \quad \text{and} \quad \widetilde{T}^0 = (F^*_{\mathbb{R},\,\mathrm{conn}})^0 / O^*_{F,+}.$$

The map $\widetilde{T} \longrightarrow \widetilde{\mathrm{Pic}}_F$ given by $v \mapsto (O_F, v)$ is a well defined homomorphism. So is the map $\widetilde{\mathrm{Pic}}_F \longrightarrow Cl_{F,+}$ that sends the class of the divisor (I, u) to the narrow ideal class of gI where $g \in F^*$ is any element for which $\mathrm{sign}(g) =$

sign(u). Here the *narrow* ideal class group $Cl_{F,+}$ is defined as the group of ideals modulo the principal ideals that are generated by $f \in F_+^* = \{f \in F^* : \sigma(f) > 0 \text{ for all real } \sigma\}$. It is a finite group.

The following proposition says that the groups $\widetilde{T}$ and $\widetilde{T}^0$ are the connected components of identity of $\widetilde{\mathrm{Pic}}_F$ and $\widetilde{\mathrm{Pic}}_F^0$ respectively. It provides an analogue to Proposition 2.2.

PROPOSITION 5.3. *Let F be a number field of degree n.*

(i) *The natural sequences*

$$0 \longrightarrow \widetilde{T} \longrightarrow \widetilde{\mathrm{Pic}}_F \longrightarrow Cl_{F,+} \longrightarrow 0$$

and

$$0 \longrightarrow \widetilde{T}^0 \longrightarrow \widetilde{\mathrm{Pic}}_F^0 \longrightarrow Cl_{F,+} \longrightarrow 0$$

are exact.

(ii) *The groups $\widetilde{T}$ and $\widetilde{T}^0$ are the connected components of identity of $\widetilde{\mathrm{Pic}}_F$ and $\widetilde{\mathrm{Pic}}_F^0$ respectively. The group $\widetilde{T}$ has dimension n while $\widetilde{T}^0$ is a compact torus of dimension $n-1$.*

PROOF. (i) Let $\widetilde{\mathrm{Pid}}_F$ denote the image of the map

$$F^* \longrightarrow \widetilde{\mathrm{Div}}_F \longrightarrow \mathrm{Id}_F \times \prod_{\sigma \text{ real}} \{\pm 1\}.$$

This leads to a commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & O_{F,+}^* & \longrightarrow & F^* & \longrightarrow & \widetilde{\mathrm{Pid}}_F & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & F_{\mathbb{R},\,\mathrm{conn}}^* & \longrightarrow & \widetilde{\mathrm{Div}}_F & \longrightarrow & \mathrm{Id}_F \times \prod_{\sigma \text{ real}} \{\pm 1\} & \longrightarrow & 0, \end{array}$$

where the vertical maps are all injective. An application of the snake lemma shows the sequence of cokernels to be exact: this is the first exact sequence of (i). Indeed, the kernel of the surjective homomorphism $\mathrm{Id}_F \times \prod_{\sigma \text{ real}} \{\pm 1\} \to Cl_{F,+}$ given by mapping a pair (I, s) to the narrow ideal class of gI, where $g \in F^*$ is any element for which $\mathrm{sign}(g) = \mathrm{sign}(s)$, is precisely equal to $\widetilde{\mathrm{Pid}}_F$. The second exact sequence is obtained by taking degree-zero parts.

(ii) Since $Cl_{F,+}$ is finite and both groups $\widetilde{T}$ and $\widetilde{T}^0$ are connected, the first statement is clear. Since the Lie group $F_{\mathbb{R},\,\mathrm{conn}}^*$ has dimension n, so do the groups $\widetilde{T}$ and $\widetilde{\mathrm{Pic}}_F$. It follows that the groups $\widetilde{T}^0$ and $\widetilde{\mathrm{Pic}}_F^0$ have dimension $n-1$. □

The classes of two oriented Arakelov divisors (I, u) and (J, v) are on the same connected component of $\widetilde{\mathrm{Pic}}_F^0$ if and only if $J = gI$ for some $g \in F^*$ for which $u_\sigma v_\sigma \sigma(g) > 0$ for each real σ.

DEFINITION 5.4. An *embedded ideal lattice* is an ideal lattice L together with an O_F-linear isometric embedding $L \hookrightarrow F_{\mathbb{R}}$. To every oriented Arakelov divisor $D = (I, u)$ we associate the ideal lattice uI together with the embedding $uI \subset F_{\mathbb{R}}$. Two embedded ideal lattices are called isometric if there is an isometry of ideal lattices that commutes with the embeddings. We have the following analogue of Proposition 4.3.

PROPOSITION 5.5. *Let F be a number field of discriminant Δ_F.*

(i) *The map that associates to an oriented Arakelov divisor $D = (I, u)$ its associated embedded ideal lattice, induces a bijection between the oriented Arakelov class group $\widetilde{\mathrm{Pic}}_F$ and the set of isometry classes of embedded ideal lattices.*
(ii) *The same map induces a bijection between $\widetilde{\mathrm{Pic}}^0_F$ and the set of isometry classes of embedded ideal lattices of covolume $\sqrt{|\Delta_F|}$.*

PROOF. If two oriented Arakelov divisors $D = (I, u)$ and $D' = (I', u')$ differ by a principal divisor $(f^{-1}O_F, f)$, then multiplication by f induces an isometry between the embedded lattices uI and $u'I'$. Therefore the map in (i) is well defined. If the embedded lattices uI and $u'I'$ are isometric, then this isometry is given by multiplication by some $x \in F_{\mathbb{R}}^*$. Then $f = u^{-1}xu'$ is contained in F^* and we have $D - D' = (f^{-1}O_F, f)$. This shows that the map is injective. To see that the map is surjective, let I be a fractional ideal and let $\iota : I \hookrightarrow F_{\mathbb{R}}$ be an O_F-linear embedding. Tensoring I with $\mathbb{R}$, we obtain an $F_{\mathbb{R}}$-linear isomorphism $F_{\mathbb{R}} \cong I \otimes_{\mathbb{Z}} \mathbb{R} \longrightarrow F_{\mathbb{R}}$, which is necessarily multiplication by some $u \in F_{\mathbb{R}}^*$. Therefore $\iota(I) = uI$ and the oriented divisor (I, u) maps to the embedded ideal lattice $\iota : I \hookrightarrow F_{\mathbb{R}}$. □

We will not use this in the rest of the paper, but note that there is a natural surjective continuous homomorphism from the idèle group $\mathbf{A}_F^*$ to the oriented Arakelov divisor group $\widetilde{\mathrm{Div}}_F$. It follows that the group $\widetilde{\mathrm{Pic}}_F$ is a quotient of the idèle class group.

6. Metrics on Arakelov class groups

Let F be a number field. In this section we provide the Arakelov class groups Pic_F and $\widetilde{\mathrm{Pic}}_F$ with translation invariant Riemannian structures.

By the diagram in Section 2, the connected component T of the group Pic_F is isomorphic to $\bigoplus_\sigma \mathbb{R}$ modulo the closed discrete subgroup $\Lambda = \{(\log|\sigma(\varepsilon)|)_\sigma : \varepsilon \in O_F^*\}$. Therefore the tangent space at 0 is isomorphic to $\bigoplus_\sigma \mathbb{R}$. Identifying this vector space with the subalgebra $\prod_\sigma \mathbb{R}$ of $F_{\mathbb{R}} = \prod_\sigma F_\sigma$, it inherits the canonical scalar product from $F_{\mathbb{R}}$. Since this $\mathbb{R}$-valued scalar product is positive

definite, both groups T and Pic_F are in this way equipped with a translation invariant Riemannian structure.

For $u \in \prod_\sigma \mathbb{R}_+^* \subset F_{\mathbb{R}}^*$ we let $\log u$ denote the element $(\log \sigma(u))_\sigma \in \prod_\sigma \mathbb{R} \subset F_{\mathbb{R}}$. We have

$$\|\log u\|^2 = \sum_\sigma \deg(\sigma) \left|\log \sigma(u)\right|^2.$$

DEFINITION 6.1. For $u \in T$ we put

$$\|u\|_{\mathrm{Pic}} = \min_{\substack{u' \in F_{\mathbb{R},+}^* \\ u' \equiv u \pmod{\Lambda}}} \|\log u'\| = \min_{\varepsilon \in O_F^*} \|\log(|\varepsilon| u)\|.$$

Every divisor class in T is represented by a divisor of the form $D = (O_F, u)$ for some $u \in \bigoplus_\sigma \mathbb{R}_+^*$. Here u is unique up to multiplication by units $\varepsilon \in O_F^*$. For such a divisor class in T we define

$$\|D\|_{\mathrm{Pic}} = \|u\|_{\mathrm{Pic}}.$$

The function $\|u\|_{\mathrm{Pic}}$ on T satisfies the triangle inequality. It gives rise to a distance function that induces the natural topology of Pic_F. The distance is only defined for divisor classes D and D' that lie on the same connected component. By Proposition 2.2, the class of the difference $D - D'$ is then equal to (O_F, u) for some unique $u \in T$ and we define the *distance* $\|D - D'\|_{\mathrm{Pic}}$ between D and D' as $\|u\|_{\mathrm{Pic}}$. The closed subgroups T^0 and Pic_F^0 inherit Riemannian structures from Pic_F.

The Euclidean structures of the ideal lattices corresponding to Arakelov divisors and the metric on Pic_F are not unrelated. The following proposition says that the difference between the Euclidean structures of two Arakelov divisors D, D' is bounded in terms of $\|D - D'\|_{\mathrm{Pic}}$.

PROPOSITION 6.2. *Let F be a number field and let $D = (I, u)$ and $D' = (I, u')$ be two Arakelov divisors. Then there exists a unit $\varepsilon \in O_F^*$ for which the divisor $D'' = (I, u'|\varepsilon|)$ satisfies*

$$e^{-\|D - D''\|_{\mathrm{Pic}}} \leq \frac{\|x\|_D}{\|x\|_{D''}} \leq e^{\|D - D''\|_{\mathrm{Pic}}}, \qquad \text{for every } x \in I.$$

The classes of D' and D'' in Pic_F are the same, so $\|D - D'\|_{\mathrm{Pic}} = \|D - D''\|_{\mathrm{Pic}}$.

PROOF. Let $\varepsilon \in O_F^*$ be such that the expression $\sum_\sigma \deg(\sigma) \left|\log(|\sigma(\varepsilon)| u'_\sigma / u_\sigma)\right|^2$ is minimal. Let $D'' = (I, |\varepsilon| u')$. Putting $v = u'|\varepsilon|/u$ we have as a consequence

$$\|D - D''\|_{\mathrm{Pic}}^2 = \sum_\sigma \deg(\sigma) \, |\log v_\sigma|^2.$$

For any $x \in I$ we have

$$\|x\|_{D''}^2 = \|u'\varepsilon x\|^2 = \|vux\|^2 = \sum_\sigma \deg(\sigma)|u_\sigma v_\sigma \sigma(x)|^2$$
$$\leq \max_\sigma |v_\sigma|^2 \sum_\sigma \deg(\sigma)|u_\sigma \sigma(x)|^2 = \Big(\max_\sigma |v_\sigma|\Big)^2 \|x\|_D^2.$$

Since

$$\log \max_\sigma |v_\sigma| = \max_\sigma \log |v_\sigma| \leq \max_\sigma |\log |v_\sigma|| \leq \|D - D''\|_{\mathrm{Pic}},$$

the first inequality follows. The second follows by symmetry. The last line of the proposition is clear. □

We now define a similar metric on the *oriented* Arakelov class group. By Proposition 5.3, the connected component of $\widetilde{\mathrm{Pic}}_F$ is $\widetilde{T} = F_{\mathbb{R},\,\mathrm{conn}}^*/O_{F,+}^*$. We recall that $F_{\mathbb{R},\,\mathrm{conn}}^*$ is the connected component of identity of the group $F_{\mathbb{R}}^*$. It is isomorphic to a product of copies of $\mathbb{R}_+^*$, one for each real prime, and of $\mathbb{C}^*$, one for each complex prime. The group $O_{F,+}^*$ is the subgroup of $\varepsilon \in O_F^*$ for which $\sigma(\varepsilon) > 0$ for every real infinite prime σ.

The exponential homomorphism $\exp : F_{\mathbb{R}} \longrightarrow F_{\mathbb{R}}^*$ is defined in terms of the usual exponential function by $\exp(u) = (\exp(u_\sigma))_\sigma$ for $u = (u_\sigma) \in F_{\mathbb{R}} \cong \prod_\sigma F_\sigma$. The image of the exponential function is precisely the group $F_{\mathbb{R},\,\mathrm{conn}}^*$. The preimage of $O_{F,+}^*$ is a discrete closed subgroup Λ of $F_{\mathbb{R}}$. We have a natural isomorphism of Lie groups

$$\exp : F_{\mathbb{R}}/\Lambda \xrightarrow{\cong} F_{\mathbb{R},\,\mathrm{conn}}^*/O_{F,+}^* = \widetilde{T}.$$

Therefore the tangent space of $\widetilde{T}$ at 0 is isomorphic to $F_{\mathbb{R}}$. The canonical scalar product on $F_{\mathbb{R}}$ provides both groups $\widetilde{T}$ and $\widetilde{\mathrm{Pic}}$ with a translation invariant Riemannian structure.

DEFINITION 6.3. For $u \in \widetilde{T}$ we put

$$\|u\|_{\widetilde{\mathrm{Pic}}} = \min_{\substack{y \in F_{\mathbb{R}} \\ \exp(y) \equiv u \pmod{O_{F,+}^*}}} \|y\|$$

Explicitly, for $u \in F_{\mathbb{R}}^* = \prod_\sigma F_\sigma^*$ we let $\log u$ denote the element $(\log(\sigma(u))_\sigma \in \prod_\sigma F_\sigma \subset F_{\mathbb{R}}$. Here we use the principal branch of the complex logarithm. We have

$$\|u\|_{\widetilde{\mathrm{Pic}}}^2 = \min_{\varepsilon \in O_{F,+}^*} \|\log(\varepsilon u)\|^2 = \min_{\varepsilon \in O_{F,+}^*} \sum_\sigma \deg(\sigma) \left|\log \sigma(\varepsilon u)\right|^2.$$

Every divisor class in $\widetilde{T}$ can be represented by a divisor of the form $D = (O_F, u)$ for some $u \in F^*_{\mathbb{R},\,\mathrm{conn}}$. Here u is unique up to multiplication by units $\varepsilon \in O^*_{F,+}$. For any divisor D of the form (O_F, u) with $u \in \widetilde{T}$ we define

$$\|D\|_{\widetilde{\mathrm{Pic}}} = \|u\|_{\widetilde{\mathrm{Pic}}}.$$

The function $\|u\|_{\widetilde{\mathrm{Pic}}}$ on $\widetilde{T}$ satisfies the triangle inequality and this gives rise to a distance function that induces the natural topology on $\widetilde{\mathrm{Pic}}_F$. The distance is only defined for divisor classes D and D' that lie on the same connected component. By Proposition 5.3, the class of the difference $D - D'$ is then equal to (O_F, u) for some unique $u \in \widetilde{T}$ and we define the *distance* $\|D - D'\|_{\widetilde{\mathrm{Pic}}}$ between D and D' as $\|u\|_{\widetilde{\mathrm{Pic}}}$.

The closed subgroups $\widetilde{T}^0$ and $\widetilde{\mathrm{Pic}}^0_F$ inherit Riemannian structures from Pic_F. We leave to the reader the task of proving an "oriented" version of Proposition 6.2.

The morphism $d : \mathrm{Id}_F \longrightarrow \widetilde{\mathrm{Div}}^0_F$ given by $d(I) = (I, N(I)^{-1/n})$ is a section of the natural map $\widetilde{\mathrm{Div}}^0_F \longrightarrow \mathrm{Id}_F$. The embedded ideal lattice associated to $d(I)$ is the ideal lattice $I \subset F_{\mathbb{R}}$ scaled by a factor $N(I)^{-1/n}$. This lattice has covolume $\sqrt{|\Delta_F|}$.

Next we prove an oriented version of Proposition 2.4. It says that the classes of the divisors of the form $d(I)$ are dense in $\widetilde{\mathrm{Pic}}^0_F$ and it implies Proposition 2.4. The exactness of the first sequence of [Lenstra 1982, Section 9] is a special case.

PROPOSITION 6.4. *Let F be a number field of degree n. Let $\bar{d} : \mathrm{Id}_F \longrightarrow \widetilde{\mathrm{Pic}}^0_F$ be the map that sends I to the class of the oriented Arakelov divisor $d(I)$ in $\widetilde{\mathrm{Pic}}^0_F$. Then the sequence*

$$0 \longrightarrow \mathrm{Id}_{\mathbb{Q}} \longrightarrow \mathrm{Id}_F \xrightarrow{\bar{d}} \widetilde{\mathrm{Pic}}^0_F$$

is exact. The image of the map $\bar{d}$ is dense in $\widetilde{\mathrm{Pic}}^0_F$.

PROOF. Every ideal in $\mathrm{Id}_{\mathbb{Q}}$ is generated by some $f \in \mathbb{Q}^*_{>0}$. Let $f \in \mathbb{Q}^*_{>0}$. Then $\bar{d}$ maps the F-ideal fO_F to the class of the oriented Arakelov divisor $(fO_F, |N(f)|^{-1/n})$. Since $|N(f)| = |f|^n$, this divisor is equal to (fO_F, f^{-1}). Therefore its image in $\widetilde{\mathrm{Pic}}^0_F$ is trivial.

Conversely, suppose that a fractional ideal I has the property that the class of $(I, N(I)^{-1/n})$ is trivial in $\widetilde{\mathrm{Pic}}^0_F$. This means that $I = fO_F$ for some $f \in F^*$ and that $f = N(I)^{1/n}$. In other words, $\sigma(f) = N(I)^{1/n}$ for all infinite primes σ. Thus all conjugates of f are equal, so that $f \in \mathbb{Q}^*$. This shows that the sequence is exact.

To show that the image of $\bar{d}$ is dense, we let $0 < \varepsilon < 1$ and pick $D = (I, u) \in \widetilde{\mathrm{Div}}_F^0$. Note that $N(I)|N(u)| = 1$. Consider the set

$$B = \{(v_\sigma)_\sigma \in F_{\mathbb{R}} : |v_\sigma - u_\sigma| < \varepsilon |u_\sigma| \text{ for all } \sigma\}.$$

Then B is a an open subset of $F_{\mathbb{R}}^*$ and all $v \in B$ have the same signature as u. Since F is dense in $F_{\mathbb{R}}$, there is an element $f \in B \cap F$.

The difference between $d(fI)$ and the divisor D is equal to

$$(fO_F, N(fI)^{-1/n} u^{-1}).$$

Since $N(u)N(I) = 1$, this is equivalent to the Arakelov divisor (O_F, v), where

$$v = N(f/u)^{-1/n} u^{-1} f \in F_{\mathbb{R}}^*.$$

Therefore the distance between D and $\bar{d}(f)$ is $\|v\|_{\widetilde{\mathrm{Pic}}}$. Since

$$\left| \frac{\sigma(f)}{u_\sigma} - 1 \right| < \varepsilon,$$

it follows from the Taylor series expansion of the principal branch of the logarithm that

$$\left| \log \frac{\sigma(f)}{u_\sigma} \right| < \frac{\varepsilon}{1-\varepsilon}$$

for all σ and hence

$$\frac{1}{n} \left| \log \frac{N(f)}{N(u)} \right| < \frac{\varepsilon}{1-\varepsilon}.$$

It follows that

$$\begin{aligned} \|v\|_{\widetilde{\mathrm{Pic}}} &\leq \sqrt{n} \max_\sigma |\log(N(f/u)^{-1/n} u_\sigma^{-1} \sigma(f))| \\ &\leq \sqrt{n} \left(\frac{1}{n} \left| \log \frac{N(f)}{N(u)} \right| + \max_\sigma \left| \log \frac{\sigma(f)}{u_\sigma} \right| \right) < \frac{2\varepsilon\sqrt{n}}{1-\varepsilon}. \end{aligned}$$

This implies that the image of $\bar{d}$ is dense, as required. □

Finally we compute the volumes of the compact Riemannian manifolds Pic_F^0 and $\widetilde{\mathrm{Pic}}_F^0$.

PROPOSITION 6.5. *Let F be a number field of degree n and discriminant Δ_F. Then:*

(i) $$\mathrm{vol}(\mathrm{Pic}_F^0) = \frac{w_F \sqrt{n}}{2^{r_1} (2\pi\sqrt{2})^{r_2}} \cdot |\Delta_F|^{1/2} \cdot \operatorname*{Res}_{s=1} \zeta_F(s).$$

(ii) $$\mathrm{vol}(\widetilde{\mathrm{Pic}}_F^0) = \sqrt{n} \cdot |\Delta_F|^{1/2} \cdot \operatorname*{Res}_{s=1} \zeta_F(s).$$

Here r_1 is the number of real primes and r_2 is the number of complex primes of F. By w_F we denote the number of roots of unity and by $\zeta_F(s)$ the Dedekind zeta function of F.

PROOF. (i) The subspace $(\bigoplus_\sigma \mathbb{R})^0$ of divisors of degree 0 is the orthogonal complement of 1 in the subalgebra $\prod_\sigma \mathbb{R}$ of $F_\mathbb{R}$. Using the fact that $\|1\| = \sqrt{n}$, one checks that the volume of Pic_F^0 is equal to $\sqrt{n}\,2^{-r_2/2}R_F$ where R_F is the regulator of F. It follows from the exact sequence of Proposition 2.2 that the compact group Pic_F^0 has volume $\sqrt{n}\,2^{-r_2/2}h_F R_F$ where $h_F = \#Cl_F$ is the class number of F. The formula [Marcus 1977] for the residue of the zeta function at $s = 1$ now easily implies (i).

(ii) Since the natural volume of the group K_σ is 2 or $2\pi\sqrt{2}$ depending on whether σ is real or complex, it follows from the commutative diagram following Definition 5.1 that $\mathrm{vol}(\widetilde{\mathrm{Pic}}_F^0)$ is equal to $2^{r_1}(2\pi\sqrt{2})^{r_2}/w_F$ times the volume of Pic_F^0. This implies (ii). □

7. Reduced Arakelov divisors

Let F be a number field of degree n. In this section we introduce *reduced* Arakelov divisors associated to F. These form a finite subset of Div_F^0. The main result of this section is that the image of this set in the groups Pic_F^0 and $\widetilde{\mathrm{Pic}}_F^0$ is in a certain precise sense regularly distributed.

The results of this section extend work by Lenstra [1982] and Buchmann and Williams [1988] and make certain statements by Buchmann [1987b; 1990; 1991] more precise. In particular, Theorems 7.4 and 7.6 and Corollary 7.9 extend [Buchmann 1987b, Section 2; 1988, Proposition 2.7; 1990, Section 3.3]. Note that in deducing the Corollaries below we did not make any particular effort to obtain the best possible estimates. They can most certainly be improved upon.

Let I be a fractional ideal. A nonzero element $f \in I$ is called *minimal* if it is nonzero and if the only element $g \in I$ for which $|\sigma(g)| < |\sigma(f)|$ for all infinite primes σ, is $g = 0$. If $f \in I$ is minimal, then for every $h \in F^*$, the element hf is minimal in the ideal hI. In particular, if $h \in O_F^*$, the element hf is minimal in the same ideal I. Therefore there are, in general, infinitely many minimal elements in I.

If $D = (I, u)$ is an Arakelov divisor, the minimal elements $f \in I$ are precisely the ones for which the open boxes $\{(y_\sigma)_\sigma \in F_\mathbb{R} : |y_\sigma| < |u_\sigma \sigma(f)| \text{ for all } \sigma\}$ contain only the point 0 of the lattice uI. Note, however, that the notion of minimality depends only on I and is *independent* of the metric induced by the element u. *Shortest* elements $f \in I$ are the elements for which $\|f\|_D = \min\{\|g\|_D : g \in I - \{0\}\}$. This notion depends on the divisor $D = (I, u)$ and hence on the lattice uI. It does not merely depend on I. Since $\|g\|_D = \|ug\|$ for

each $g \in I$, the vector uf for any shortest $f \in I$ is a shortest nonzero vector of the lattice uI associated to D. The number of shortest elements in I is always finite. Shortest vectors are clearly minimal, but the converse is not true. It may even happen that a minimal element $f \in I$ is not a shortest element of the lattice $D = (I, u)$ for *any* choice of u. See Section 9 for an explicit example.

DEFINITION. An Arakelov divisor or oriented Arakelov divisor D in Div_F is called *reduced* if it is of the form $D = d(I) = (I, N(I)^{-1/n})$ for some fractional ideal I, and if 1 is a minimal element of I. The set of reduced Arakelov divisors is denoted by Red_F.

Since reduced Arakelov divisors have degree zero, the covolume of the lattices associated to reduced Arakelov divisors is $\sqrt{|\Delta_F|}$. With respect to the natural metric, $1 \in O_F$ is a shortest and hence minimal element. Therefore the trivial Arakelov divisor $(O_F, 1)$ is reduced. In general, if $D = d(I)$ is reduced, the element $1 \in I$ is merely minimal and need not be a shortest element. However, the next proposition shows that it is not too far away from being so.

PROPOSITION 7.1. *Let F be a number field of degree n and let $D = d(I) = (I, N(I)^{-1/n})$ be a reduced Arakelov divisor. Then*

$$\|1\|_D \leq \sqrt{n}\|x\|_D \quad \textit{for all nonzero } x \in I.$$

In particular, the element $1 \in I$ is at most $\sqrt{n}$ times as long as the shortest element in I.

PROOF. We have $\|1\|_D = \sqrt{n}N(I)^{-1/n}$. Since $1 \in I$ is minimal, every nonzero $x \in I$ satisfies $|\sigma(x)| \geq 1$ for some embedding $\sigma : F \longrightarrow \mathbb{C}$. Therefore $\|x\|_D \geq N(I)^{-1/n}|\sigma(x)| \geq N(I)^{-1/n}$. □

If $D = (I, u)$ is an Arakelov divisor and $f \in I$ is minimal, then $1 \in f^{-1}I$ is again minimal and the divisor $d(f^{-1}I) = (f^{-1}I, N(fI^{-1})^{1/n})$ is reduced. In particular, if $f \in I$ is a shortest element, the divisor $d(f^{-1}I)$ is reduced. However, even though the element $1 \in f^{-1}I$ is minimal, it *need not be* a shortest element. Indeed, even if 1 *is* a shortest vector of the lattice associated to $(f^{-1}I, |f|^{-1}u)$, it may not be a shortest vector of the lattice $d(f^{-1}I) = (f^{-1}I, N(fu^{-1})^{1/n})$, which has a different metric. In Section 9 we present an example of this phenomenon.

It is not so easy to say in terms of the associated ideal lattice uI precisely what it means for a divisor $D = (I, u)$ to be reduced. We make the following imprecise observation. When $1 \in I$ is not merely minimal, but happens to be a shortest element in I, then all roots of unity in F are also shortest elements in I. Usually, these are the *only* shortest elements in I. In that case the arithmetic-geometric mean inequality implies that $\gamma(D) = \gamma(uI)$, viewed as a function on Pic^0_F,

attains a local minimum at $D = (I, N(I)^{-1/n})$. So, the lattice corresponding to a reduced divisor is the "skewest" O_F-lattice in a small neighborhood in Pic^0_F. But this is just a rule of thumb; it is not always true.

DEFINITION. Let F be a number field. Let Δ_F denote its discriminant and r_2 its number of complex infinite primes. Then we put

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

PROPOSITION 7.2. *Let F be a number field of degree n.*

(i) *Let I be a fractional ideal. If $d(I) = (I, N(I)^{-1/n})$ is a reduced Arakelov divisor, the inverse I^{-1} of I is an O_F-ideal of norm at most ∂_F.*
(ii) *The set Red_F of reduced Arakelov divisors is finite.*
(iii) *The natural map $\mathrm{Red}_F \longrightarrow \widetilde{\mathrm{Pic}}^0_F$ is injective.*

PROOF. Since $1 \in I$, the ideal I^{-1} is contained in O_F. By Proposition 4.4(ii) there exists a nonzero $f \in I$ for which $|N(I)^{-1/n}\sigma(f)| < \partial_F^{1/n}$ for each σ. Therefore, if $N(I^{-1}) > \partial_F$, we have $|\sigma(f)| < 1$ for each σ, contradicting the minimality of $1 \in I$. This proves (i). Part (ii) follows at once from (i) and the fact that there are only finitely many O_F-ideals of bounded norm.

To prove (iii), suppose that the reduced Arakelov divisors $D = d(I)$ and $D' = d(I')$ have the same image in $\widetilde{\mathrm{Pic}}^0_F$. Then there exists $f \in F^*$ so that $I' = fI$ and $N(I')^{1/n} = N(I)^{1/n} f$. As in the proof of Proposition 6.4, it follows that all conjugates of f are equal and hence that $f \in \mathbb{Q}^*$. Since both I and I' contain 1 as a minimal vector, this implies that $f = \pm 1$. Since $f = N(I'I^{-1})^{1/n} > 0$, we have $f = 1$ and hence $D = D'$ as required. □

Part (iii) of Proposition 7.2 does not hold when we replace $\widetilde{\mathrm{Pic}}^0_F$ by Pic^0_F. See Example 9.3 for an example. Incidentally, Theorem 7.7 below strengthens the statement considerably.

Before we begin our discussion of the distribution of the reduced divisors in the Arakelov class groups, we characterize them 'geometrically'. This characterization plays no role in the sequel. For every fractional ideal I with $1 \in I$ consider the following set of divisors of degree zero:

$$\Sigma_I = \{(I, v) \in \mathrm{Div}^0_F : \log v_\sigma \leq (1/n) \log \partial_F \text{ for all } \sigma\}.$$

The set Σ_I is not empty if and only if $N(I^{-1}) \leq \partial_F$. Indeed, under this condition Σ_I contains the divisor $(I, N(I)^{-1/n})$ and its elements have the form $(I, N(I)^{-1/n}) + (O_F, w)$ with w running over the exponentials of the vectors $y \in \left(\bigoplus_\sigma \mathbb{R}\right)^0$ satisfying

$$y_\sigma \leq \frac{1}{n}(\log \partial_F + \log N(I)) \qquad \text{for every } \sigma.$$

Since $\sum_\sigma \deg(\sigma) y_\sigma = 0$, the set Σ_I is a bounded simplex.

The following proposition says what it means for a divisor

$$d(I) = (I, N(I)^{-1/n})$$

to be reduced in terms of its simplex Σ_I.

PROPOSITION 7.3. *Let I be a fractional ideal with $1 \in I$. The Arakelov divisor $D = d(I) = (I, N(I)^{-1/n})$ is reduced if and only if it has the property that for every fractional ideal I' with $1 \in I'$ for which $\Sigma_I \subset \Sigma_{I'} + (f)$ for some $f \in F^*$, we necessarily have $fI = I'$ and $|\sigma(f)| = 1$ for all σ.*

PROOF. Suppose that $D = (I, N(I)^{-1/n})$ is reduced. Let I' be a fractional ideal with $1 \in I'$ and $f \in F^*$. Suppose that for some $f \in F^*$ the simplex Σ_I is contained in the translated simplex $\Sigma_{I'} + (f) = \{(I', v) + (f) : (I', v) \in \Sigma_{I'}\}$. This implies $I' = fI$. In addition, we have $\log(v_\sigma/|\sigma(f)|) \le (1/n)\log \partial_F$ whenever $\log v_\sigma \le (1/n)\log \partial_F$. It follows that $|\sigma(f)| \ge 1$ for all σ. Since $1 \in I$ is minimal, so is $f \in I'$. Since $1 \in I'$, this implies $|\sigma(f)| = 1$ for every σ.

Conversely, suppose that $D = (I, N(I)^{-1/n})$ has the property described in the proposition. We want to show that $1 \in I$ is minimal. Let therefore $g \in I$ such that $|\sigma(g)| \le 1$ for all σ. Consider the O_F-ideal $I' = g^{-1}I$. Then we have $1 \in I'$ and $\Sigma_I \subset \Sigma_{I'} + (g^{-1})$. Indeed, if $(I, v) \in \Sigma_I$, then $\log v_\sigma \le (1/n)\log \partial_F$ and hence $\log(v_\sigma |\sigma(g)|) \le (1/n)\log \partial_F$. This means precisely that (I, v) is contained in $\Sigma_{I'} + (g^{-1})$. We conclude that $|\sigma(g)| = 1$ for every σ. It follows that $1 \in I$ is minimal, as required. □

When F is totally real, we necessarily have $f = \pm 1$ and hence $I = I'$ in Proposition 7.3. The proposition says therefore that, in a certain sense, the image in Pic_F^0 of Σ_I is not contained in the image of any other simplex. When F is not totally real, this is still true for most I.

In the rest of this section we study the distribution of the image of the set Red_F in the compact groups Pic_F^0 and $\widetilde{\mathrm{Pic}}_F^0$ and estimate its size. First we look at the image of the set Red_F in Pic_F^0. Theorem 7.4 says that Red_F is rather *dense* in Pic_F^0.

THEOREM 7.4. *Let F be a number field of degree n admitting r_2 complex infinite primes.*

(i) *For any Arakelov divisor $D = (I, u)$ of degree 0 there is a reduced divisor D' and an element $f \in F^*$ so that*

$$D - D' = (f) + (O_F, v)$$

with

$$\log |v_\sigma| \le \frac{1}{n} \log \partial_F \quad \text{for each } \sigma.$$

In particular,

$$\|D - D'\|_{\mathrm{Pic}} \leq \log \partial_F.$$

(ii) *The natural map*

$$\bigcup_D \Sigma_I \quad \longrightarrow \quad \mathrm{Pic}_F^0$$

is surjective. Here the union runs over the reduced Arakelov divisors $D = (I, N(I)^{-1/n})$.

PROOF. By Minkowski's Theorem (Proposition 4.4(ii)), there is a nonzero element $f \in I$ satisfying

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

Then there is also a shortest and hence a minimal such element f. The divisor $D' = d(f^{-1}I)$ is then *reduced*. It lies on the same component of Pic_F^0 as D. We have

$$D - D' + (f) = (O_F, v),$$

where v is the vector $(v_\sigma)_\sigma \in \prod_\sigma \mathbb{R}_+^*$ with $v_\sigma = u_\sigma |\sigma(f)| N(f^{-1}I)^{1/n}$ and hence $\log |v_\sigma| = \log |u_\sigma \sigma(f)| + (1/n) \log(N(f^{-1}I))$ for every σ. Because $N(f^{-1}I) \leq 1$, this implies that $\log |v_\sigma| \leq \log |u_\sigma \sigma(f)|$ which by assumption is at most $\frac{1}{n} \log \partial_F$, as required.

Since $\sum_\sigma \deg(\sigma) \log v_\sigma = 0$, Lemma 7.5 below implies that

$$\|D - D'\|_{\mathrm{Pic}}^2 = \|v\|_{\mathrm{Pic}}^2 \leq n(n-1)\Big(\frac{1}{n} \log \partial F\Big)^2.$$

This proves (i). Part (ii) is merely a reformulation of part (i). □

LEMMA 7.5. *Let* $x_i \in \mathbb{R}$ *for* $i = 1, \ldots, n$. *Suppose that* $\sum_{i=1}^n x_i = 0$ *and that* $x \in \mathbb{R}$ *has the property that* $x_i \leq x$ *for all* $i = 1, \ldots, n$. *Then* $\sum_{i=1}^n x_i^2 \leq n(n-1)x^2$.

We leave the proof of the lemma to the reader. The theorem says that Pic_F^0 can be covered with simplices Σ_I centered in the reduced divisors D. We use the theorem to estimate the volume of the Arakelov class group Pic_F^0 in terms of the number of reduced divisors.

COROLLARY 7.6. *Let* F *be a number field of degree* n *with* r_1 *real and* r_2 *complex infinite primes. We have*

$$\begin{aligned} \mathrm{vol}(\mathrm{Pic}_F^0) &\leq \frac{2^{-r_2/2} n^{-1/2}}{(r_1 + r_2 - 1)!} (\log \partial_F)^{r_1 + r_2} \#\mathrm{Red}_F \\ &\leq (\log |\Delta_F|)^n \#\mathrm{Red}_F. \end{aligned}$$

PROOF. Let $D = d(I) = (I, N(I)^{-1/n})$ be a reduced divisor. The set Σ_I is given by

$$\Big\{(I, N(I)^{-1/n}) + (O_F, v) : \log v_\sigma \le \frac{1}{n}\big(\log \partial_F + \log N(I)\big)\Big\}.$$

By Proposition 7.2(i) we have $N(I^{-1}) \le \partial_F$. This implies that the set Σ_I is a nonempty simplex of volume $\big(\frac{1}{n}\log(\partial_F\, N(I))\big)^{r_1+r_2}$ times the volume of the standard simplex

$$\big\{(y_\sigma) \in \textstyle\bigoplus_\sigma \mathbb{R} : \sum_\sigma y_\sigma = 0 \text{ and } y_\sigma \le 1 \text{ for each } \sigma\big\},$$

which one checks to be equal to $2^{-r_2/2} n^{r_1+r_2-1/2}/(r_1+r_2-1)!$. This leads to the inequality

$$\mathrm{vol}(\mathrm{Pic}^0_F) \;\le\; \frac{2^{-r_2/2} n^{r_1+r_2-1/2}}{(r_1+r_2-1)!} \sum_D \Big(\frac{1}{n}\log(\partial_F\, N(I))\Big)^{r_1+r_2}.$$

Here the sum runs over the reduced divisors $D = (I, N(I)^{-1/n})$ of F.

Since $N(I) \le 1$, the first estimate follows. The second inequality follows by a rather crude estimate from the first one. □

Next we prove a kind of converse to Theorem 7.4. The following theorem and its corollary say that the image of the set Red_F is rather *sparse* in the group $\widetilde{\mathrm{Pic}}^0_F$. Recall that $F^*_+ = \{x \in F^* : \sigma(x) > 0 \text{ for all real } \sigma\}$.

THEOREM 7.7. *Let F be a number field.*

(i) *Let D and D' be two reduced divisors in $\widetilde{\mathrm{Div}}^0_F$. If there exists an element $f \in F^*_+$ for which*

$$D - D' + (f) = (O_F, v),$$

with $|\log v_\sigma| < \log \frac{4}{3}$ for each σ, then $D = D'$ in $\widetilde{\mathrm{Div}}^0_F$. Similarly, if $\|v\|_{\widetilde{\mathrm{Pic}}} < \log \frac{4}{3}$, we have $D = D'$ in $\widetilde{\mathrm{Div}}^0_F$.

(ii) *The natural map from*

$$\bigcup_{D' \in \mathrm{Red}_F} \{D' + (O_F, v) :\; v \in (F^*_{\mathbb{R},\,\mathrm{conn}})^0 \text{ and } |\log v_\sigma| < \tfrac{1}{2}\log\tfrac{4}{3} \text{ for each } \sigma\}$$

to $\widetilde{\mathrm{Pic}}^0_F$ is injective.

PROOF. Suppose that $D = d(I)$ and $D' = d(I')$ are two reduced divisors with the property that $D - D' + (f) = (O_F, v)$ with $f \in F^*$ for which $\sigma(f) > 0$ for all real σ. By Proposition 5.3, the images of D and D' in $\widetilde{\mathrm{Pic}}^0_F$ lie on the same

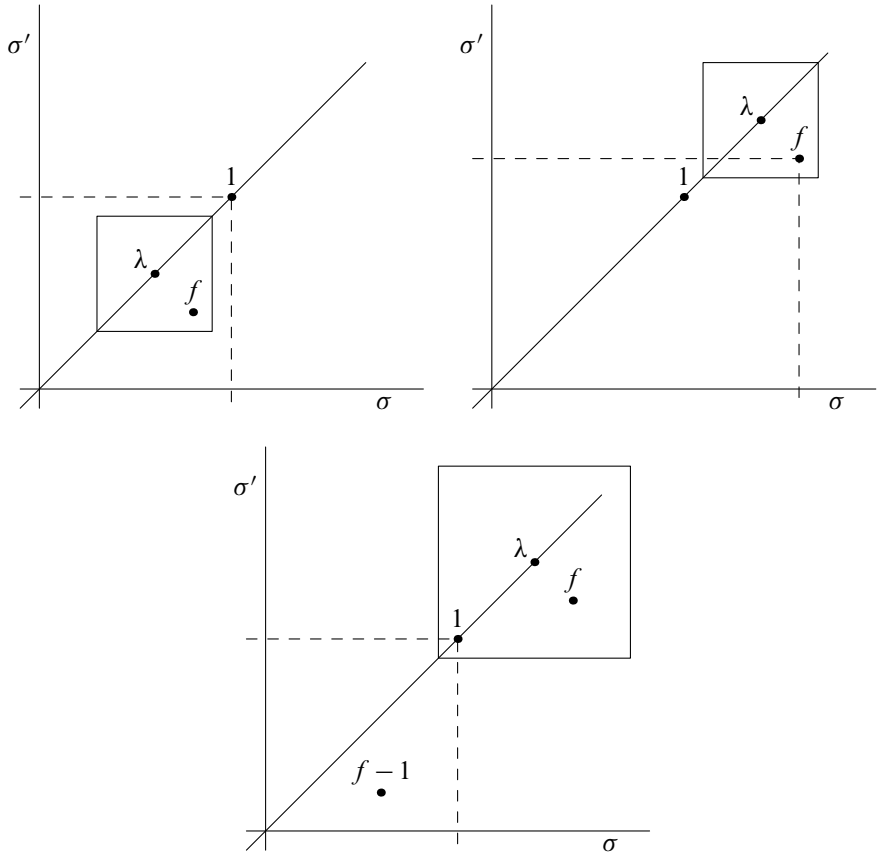

Figure 1. Top left: Since f is in the box of λ, it is in the box of 1. Top right: Since f is in the box of λ, 1 is in the box of f. Bottom: Since f is in the box of λ, $f-1$ is in the box of 1.

connected component of $\widetilde{\mathrm{Pic}}^0_F$. We put $\lambda = N(I/I')^{1/n}$. Then $\sigma(f)/\lambda = v_\sigma$. Since $|\log v_\sigma| < \log \frac{4}{3}$, we have

$$\begin{aligned}\left|\frac{\sigma(f)}{\lambda}-1\right| &= |v_\sigma - 1| \\ &= |\exp(\log v_\sigma)-1| \le \exp|\log(v_\sigma)|-1 < \exp(\log\tfrac{4}{3})-1 = \tfrac{1}{3},\end{aligned}$$

and hence

$$|\sigma(f)-\lambda| < \tfrac{1}{3}\lambda \quad \text{for every } \sigma.$$

Since D and D' are reduced, the element 1 is minimal in both I and I'. Therefore both 1 and f are minimal in $fI' = I$.

If λ is small, i.e., if $0 < \lambda < \frac{1}{2}$, we have $|\sigma(f)| \le |\sigma(f) - \lambda| + |\lambda| < \frac{1}{3}\lambda + \lambda < \frac{4}{3} \cdot \frac{1}{2} < 1$ for each σ. In other words, $|\sigma(f)| < |\sigma(1)|$ for all σ, contradicting the fact that $1 \in I$ is minimal. If λ is large, i.e., if $\lambda > \frac{3}{2}$, we have that $|\sigma(f)| \ge |\lambda| - |\sigma(f) - \lambda| \ge \lambda - \frac{1}{3}\lambda > \frac{2}{3} \cdot \frac{3}{2} = 1$ for each σ. In other words, $|\sigma(1)| < |\sigma(f)|$ for all σ, contradicting the fact that $f \in I$ is a minimal vector.

Therefore $\frac{1}{2} \le \lambda \le \frac{3}{2}$. This implies that the element $f-1 \in I$ satisfies

$$|\sigma(f-1)| \le |\sigma(f)-\lambda| + |\lambda-1| < \tfrac{1}{3}\lambda + |\lambda-1| \le \tfrac{1}{3} \cdot \tfrac{3}{2} + \tfrac{1}{2} = 1 = |\sigma(1)|$$

for all σ. Since $1 \in I$ is a minimal vector, this implies that $f - 1 = 0$. Therefore $I = I'$ and hence $D = D'$. This proves the first statement.

If that $\|v\|_{\widetilde{\mathrm{Pic}}} < \log \frac{4}{3}$, there is a totally positive unit ε with $|\log(\sigma(\varepsilon)v_\sigma)| < \log \frac{4}{3}$ for each σ. Replacing f by εf if necessary, we may then assume that $|\log(v_\sigma)| < \log \frac{4}{3}$ for each σ and we are back in the earlier situation. This proves (i).

Part (ii) follows, because (i) implies that the sets

$$\left\{D' + (O_F, v) : v \in (F^*_{\mathbb{R},\,\mathrm{conn}})^0 \text{ and } |\log(v_\sigma)| < \tfrac{1}{2}\log\tfrac{4}{3} \text{ for each } \sigma\right\}$$

map injectively to $\widetilde{\mathrm{Pic}}^0_F$ and that their images are mutually disjoint. This proves the theorem. □

COROLLARY 7.8. *There is a constant $c > 0$, so that for every number field F of degree n, the number of reduced divisors contained in a ball of radius 1 in* Pic^0_F *is at most* $(cn)^{n/2}$.

PROOF. The reduced divisors whose images in Pic^0_F are contained in a ball of radius 1 lie in a subset S of $\widetilde{\mathrm{Pic}}^0_F$ of volume $2^{r_1}(2\pi\sqrt{2})^{r_2}/w_F$ times the volume of a unit ball in Pic^0_F. By Theorem 7.7, the balls of radius $\frac{1}{2}\log\left(\frac{4}{3}\right)$ centered at reduced divisors are mutually disjoint in $\widetilde{\mathrm{Pic}}^0_F$. Comparing the volume of the union of the disjoint balls with the volume of S leads to the estimate. □

COROLLARY 7.9. *Let F be a number field of degree n. Then*

$$\#\mathrm{Red}_F \le \mathrm{vol}(\widetilde{\mathrm{Pic}}^0_F) \cdot 6^n.$$

PROOF. Theorem 7.7(ii) implies that the volume of $\widetilde{\mathrm{Pic}}^0_F$ is at least $\#\mathrm{Red}_F$ times the volume of the simplex $\{v \in ((F^*_{\mathbb{R},\,\mathrm{conn}})^0 : |\log(v_\sigma)| < \frac{1}{2}\log\frac{4}{3} \text{ for each } \sigma\}$, which is equal to

$$\frac{2^{-r_2/2} n^{r_1+r_2-1/2}}{(r_1+r_2-1)!}\left(\tfrac{1}{2}\log\tfrac{4}{3}\right)^{r_1+r_2}.$$

Since this is at least 6^{-n}, the result follows. □

COROLLARY 7.10. *Let F be a number field. Then*

$$(\log|\Delta_F|)^{-n} \;\le\; \frac{\#\mathrm{Red}_F}{\mathrm{vol}(\mathrm{Pic}^0_F)} \;\le\; 18^n.$$

PROOF. The volume of $\widetilde{\mathrm{Pic}}^0_F$ is $2^{r_1}(2\pi\sqrt{2})^{r_2}/w_F$ times the volume of Pic^0_F. Since $2^{r_1}(2\pi\sqrt{2})^{r_2}/w_F \le (2\pi\sqrt{2})^{n/2}$, the inequalities follow from Corollaries 7.6 and 7.9 respectively. □

We recall the following estimates for the volume of Pic^0_F. They say that in a sense the volume of Pic^0_F is approximately equal to $\sqrt{|\Delta_F|}$.

PROPOSITION 7.11. *Let $n \ge 1$. For every number field F of degree n we have:*

(i) $$\mathrm{vol}(\mathrm{Pic}^0_F) \le \sqrt{|\Delta_F|}\,(\log|\Delta_F|)^{n-1}\,;$$

(ii) (GRH) *there exists a constant $c > 0$ only depending on the degree n so that*

$$\mathrm{vol}(\mathrm{Pic}^0_F) \ge c\sqrt{|\Delta_F|}/\log\log|\Delta_F|.$$

PROOF. Part (i) follows from Corollary 7.7, the fact that for every reduced divisor $d(I)$ the ideal I^{-1} is integral and has norm at most $(2/\pi)^{r_2}\sqrt{|\Delta_F|}$ and the estimate for the number of O_F-ideals of bounded norm provided in [Lenstra 1992, Theorem 6.5]. Under assumption of the generalized Riemann Hypothesis (GRH) for the zeta function of the normal closure of F, Buchmann and Williams [1989, (3.2)] obtained the estimate in (ii). □

8. Quadratic fields

Since the class group of $\mathbb{Q}$ is trivial and $\mathbb{Z}^* = \{\pm 1\}$, the group $\mathrm{Pic}^0_{\mathbb{Q}}$ is trivial and the degree map induces an isomorphism $\mathrm{Pic}_{\mathbb{Q}} \cong \mathbb{R}$. The narrow class group of $\mathbb{Q}$ is also trivial and it follows from Definition 5.1 that $\widetilde{\mathrm{Pic}}^0_{\mathbb{Q}} = 0$ and that $\widetilde{\mathrm{Pic}}_{\mathbb{Q}}$ is isomorphic to $\mathbb{R}^*_+$.

This is the whole story as far as $\mathbb{Q}$ is concerned. We now briefly work out the theory of the previous sections for quadratic number fields. For these fields the language of binary quadratic forms is often used [Lenstra 1982; Shanks 1972].

EXAMPLE 8.1. For complex quadratic fields F, the torus T^0 of Section 2 is trivial, so that the group Pic^0_F is canonically isomorphic to the class group Cl_F of F. The group $\widetilde{\mathrm{Pic}}^0_F$ is an extension of Cl_F by a circle group of length $2\pi\sqrt{2}/w_F$. Here $w_F = 2$ except when $F = \mathbb{Q}(i)$ or $\mathbb{Q}((1+\sqrt{-3})/2)$, in which case $w_F = 4$ or 6 respectively.

We describe the reduced Arakelov divisors of F. Let $D = (I, N(I)^{-1/2})$ be reduced. The fact that 1 is a minimal element of I simply means that it is a shortest vector in the corresponding lattice in $F_{\mathbb{R}} \cong \mathbb{C}$. We write $I = \mathbb{Z} + f\mathbb{Z}$

for some f in the upper half-plane $\{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$. Since $O_F \cdot I \subset I$, we have $f = (b + \sqrt{\Delta_F})/(2a)$ for certain $a, b \in \mathbb{Z}$, $a > 0$ and $b^2 - 4ac = \Delta_F$ for some $c \in \mathbb{Z}$ with $\gcd(a, b, c) = 1$. The O_F-ideal I^{-1} is generated by a and $\frac{1}{2}(b - \sqrt{\Delta_F})$ and has norm a. For complex quadratic fields the simplices Σ_I introduced in Section 6 are simply points.

Since f is unique up to addition of an integer, the $\mathrm{SL}_2(\mathbb{Z})$-equivalence class of the binary quadratic form $N(X + fY)/N(I) = aX^2 + bXY + cY^2$ is well defined. The form has discriminant Δ_F. If we choose f to lie in the usual fundamental domain for the action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half-plane, the corresponding quadratic form is reduced in the sense of Gauss. There is a slight ambiguity here. If $|f| = 1$, the reduced Arakelov divisors $d(\mathbb{Z} + f\mathbb{Z})$ and $d(\mathbb{Z} + \bar{f}\mathbb{Z})$ give rise to the quadratic forms $aX^2 + bXY + aY^2$ and $aX^2 - bXY + aY^2$ respectively. If f is not a root of unity, the Arakelov divisors are distinct, but the two quadratic forms are $\mathrm{SL}_2(\mathbb{Z})$-equivalent and only one of them is reduced. Apart from this ambiguity, the map that associates to a reduced Arakelov divisor its associated reduced quadratic form, is a bijection.

EXAMPLE 8.2. Any real quadratic field F can be written as $\mathbb{Q}(\sqrt{\Delta_F})$, where Δ_F denotes its discriminant. The group Pic^0_F is an extension of the class group by a circle group and the group $\widetilde{\mathrm{Pic}}^0_F$ is an extension of the *narrow* class group by a circle group. We describe the reduced Arakelov divisors of F. Let σ and σ' denote the two infinite primes of F. To be definite, we let σ denote the embedding that maps $\sqrt{\Delta_F}$ to the positive square root of Δ_F in $\mathbb{R}$. Let $D = d(I) = (I, N(I)^{-1/2})$ be reduced. The fact that $1 \in I$ is minimal implies that we can write $I = \mathbb{Z} + f\mathbb{Z}$ for a unique f satisfying $\sigma(f) > 1$ and $-1 < \sigma'(f) < 0$. The fact that $O_F \cdot I \subset I$ implies that $f = (b + \sqrt{\Delta_F})/(2a)$ where $\Delta_F = b^2 - 4ac$ for some $c \in \mathbb{Z}$ with $\gcd(a, b, c) = 1$. The conditions on $\sigma(f)$ and $\sigma'(f)$ say that $a > 0$ and $|\sqrt{\Delta_F} - 2a| < b < \sqrt{\Delta_F}$. The O_F-ideal I^{-1} is generated by a and $\frac{1}{2}(b - \sqrt{\Delta_F})$. Its norm is a. The simplex Σ_I of Section 6 is an interval of length $\sqrt{2}\,\log(\sqrt{\Delta_F}/a)$ centered in D.

The map that associates the quadratic form $aX^2 + bXY + cY^2$ to the reduced divisor $D = (I, N(I)^{-1/2})$, is a bijection between the set of reduced Arakelov divisors of F and the set of reduced binary quadratic forms of discriminant Δ_F with $a > 0$.

The element $1 \in I$ is a shortest vector precisely when both $\|f\|$ and $\|f - 1\|$ are at least $\|1\| = \sqrt{2}$. This condition is not always satisfied. Drawing a picture, one sees that it is if $\sigma(f) - \sigma'(f) \geq 2$, or equivalently if $a < \frac{1}{2}\sqrt{\Delta_F}$, but this is not a necessary condition.

When $D = d(I)$ and $I = \mathbb{Z} + f\mathbb{Z}$ as above, the vector f is a minimal element of I. Therefore $D' = d(f^{-1}I)$ is a reduced Arakelov divisor. We have $D = D' + (f) + (O_F, v)$, where $v \in F^*_{\mathbb{R}} \cong \mathbb{R}^* \times \mathbb{R}^*$ is the vector

$(|\sigma'(f)/\sigma(f)|^{1/2}, -|\sigma(f)/\sigma'(f)|^{1/2})$. The distance between the images of D and D' in Pic_F^0 is equal to $\|v\|_{\mathrm{Pic}}$. Since $f = (b + \sqrt{\Delta})/(2a)$, we have $\|v\|_{\mathrm{Pic}} = 2^{-3/2} \log \left|(b+\sqrt{\Delta_F})/(b-\sqrt{\Delta_F})\right|$. In this way we recover Lenstra's distance formula [Lenstra 1982, (11.1)]. The divisor D' is the 'successor' of D in its component, in the sense that there are no reduced divisors on the circle between D and D'. In order to obtain D's 'predecessor', take g the shortest minimum such that $|\sigma(g)| < |\sigma'(g)|$. Then the Arakelov divisor $d(g^{-1}I)$ is the predecessor of D.

Lenstra's group $\mathcal{F}$, or rather its topological completion $\overline{\mathcal{F}}$, is closely related to the oriented Arakelov class group of the real quadratic field F, and several of the results in [Lenstra 1982] are special cases of the ones in this paper. The group $\overline{\mathcal{F}}$ is not quite *equal* to $\widetilde{\mathrm{Pic}}_F^0$ but it admits a degree 2 cover onto it. More generally, for a number field F we let Pic_F^+ denote the group $\widetilde{\mathrm{Div}}_F^0$ modulo its subgroup $\pm F_+^*$. When F is totally complex, i.e., when $r_1 = 0$, this is simply $\widetilde{\mathrm{Pic}}_F^0$. When $r_1 > 0$ however, there is an exact sequence

$$0 \longrightarrow \{\pm 1\}^{r_1}/\{\pm 1\} \longrightarrow \mathrm{Pic}_F^+ \longrightarrow \widetilde{\mathrm{Pic}}_F^0 \longrightarrow 0.$$

Let $(F_{\mathbb{R}}^*)^0 = \{u \in F_{\mathbb{R}} : |N(u)| = 1\}$. The topological structure of Pic_F^+ can be seen from the exact sequence

$$0 \longrightarrow (F_{\mathbb{R}}^*)^0/\pm O_{F,+}^* \longrightarrow \mathrm{Pic}_F^+ \longrightarrow Cl_{F,+} \longrightarrow 0,$$

realizing Pic_F^+ as an extension of the narrow class group $Cl_{F,+}$ by a 2^{r_1-1}-component Lie group. When F is real quadratic, the group Pic_F^+ is equal to Lenstra's group $\overline{\mathcal{F}}$.

9. Reduced Arakelov divisors; examples and counterexamples

Let F be a number field of degree n and discriminant Δ_F. Theorems 7.4 and 7.7 say that the image of the set Red_F of reduced Arakelov divisors is, in a precise sense, rather regularly distributed in the groups Pic_F^0 and $\widetilde{\mathrm{Pic}}_F^0$. In this section we discuss these results and we consider variations in the definition of the set of reduced divisors.

Theorem 7.4 says that the image of Red_F is rather 'dense' in Pic_F^0. After a first draft of this paper was written, a similar result was obtained for the larger group $\widetilde{\mathrm{Pic}}_F^0$.

PROPOSITION 9.1 (BUHLER ET AL.[1]). *Let $L \subset \mathbb{R}^n$ be a lattice and suppose that all nonzero vectors of L have all their coordinates different from zero. Then there exists a minimal vector $(x_i) \in L$ with $x_i > 0$ for all i.*

[1] Personal communication from Joe Buhler describing discussions between Buhler, Randy Dougherty, Chris Freiling, Dan Mauldin, Nghi Nguyen, Peter Ostapenko, and Ken Zeger.

PROOF. Let $\boldsymbol{x} \in \mathbb{R}^n$ be an *extreme* point of the convex hull of the set

$$S = \{(x_i) \in L : x_i > 0 \text{ for all } i\}.$$

This means that no open line segment inside the convex hull of S contains $\boldsymbol{x}$. It follows that $\boldsymbol{x}$ is contained in L. If $\boldsymbol{x}$ were not a minimal vector of L, there would be a non-zero vector $\boldsymbol{y} = (y_i)$ in L for which $-x_i < y_i < x_i$ for all i, so that both vectors $\boldsymbol{x} - \boldsymbol{y}$ and $\boldsymbol{x} + \boldsymbol{y}$ are in S. Since $\boldsymbol{x}$ is contained in the line segment connecting $\boldsymbol{x} - \boldsymbol{y}$ and $\boldsymbol{x} + \boldsymbol{y}$, this contradicts the fact that $\boldsymbol{x}$ is an extreme point. It follows that $\boldsymbol{x}$ is minimal. □

This result easily implies that all components of the oriented Arakelov class group $\widetilde{\mathrm{Pic}}^0_F$ contain reduced Arakelov divisors. In addition, Joe Buhler and his collaborators obtain a bound for the length of the shortest vector $(x_i) \in L$ with $x_i > 0$ for all i. It leads to an analogue of Theorem 7.4 for $\widetilde{\mathrm{Pic}}^0_F$. The dependence on n is a little worse. I do not know how to compute these vectors efficiently.

In the other direction, Theorem 7.7 implies that the image of Red_F in $\widetilde{\mathrm{Pic}}^0_F$ is rather 'sparse'. When we replace $\widetilde{\mathrm{Pic}}^0_F$ by Pic^0_F, the theorem is no longer true. First of all the map $\mathrm{Red}_F \longrightarrow \mathrm{Pic}_F$ is in general not injective. In addition, it may happen that distinct reduced divisors have images in Pic^0_F that are much closer to one another than the bound $\log\left(\frac{4}{3}\right)$ of Theorem 7.7. However, by Corollary 7.9, the *number* of reduced divisors in a ball in Pic^0_F of radius 1 is bounded by a constant depending only on the degree of F.

LEMMA 9.2. *Let F be a number field of degree n, let $D = (I, u)$ be an Arakelov divisor and suppose $f \in I$.*

(i) *$d(f^{-1}I) = d(I)$ in Div^0_F if and only if f is a unit of O_F.*
(ii) *The classes of $d(f^{-1}I)$ and $d(I)$ in Pic^0_F are equal if and only if f is the product of a unit and an element $g \in F^*$ all of whose absolute values $|\sigma(g)|$ are equal.*
(iii) $\|d(I) - d(f^{-1}I)\|_{\mathrm{Pic}} < 2\sqrt{n}\max_\sigma \left|\log|\sigma(f)|\right|$.

PROOF. Part (i) follows from the fact that $I = f^{-1}I$ if and only if $f \in O_F^*$. Since

$$d(f^{-1}I) - d(I) = (f^{-1}O_F, |N(f)|^{1/n}),$$

the class of this divisor is trivial in Pic^0_F if and only if there is $g \in F^*$ for which $f = \varepsilon g$ for some unit $\varepsilon \in O_F^*$ and $|\sigma(g)|^{-1} = |N(f)|^{-1/n}$ for all σ. Since $|N(g)| = |N(f)|$, the second relation is equivalent to the fact that the $|\sigma(g)|$ are all equal. This proves (ii).

To prove (iii) we note that

$$\|d(I) - d(f^{-1}I)\|_{\mathrm{Pic}} \leq \sqrt{n}\max_\sigma \left|\log|\sigma(f)/N(f)^{1/n}|\right|,$$

which is at most $\sqrt{n}$ times $\max_\sigma \left|\log|\sigma(f)|\right| + \frac{1}{n}\sum_\sigma \deg(\sigma)\log|\sigma(f)|$. The estimate follows easily.

This implies that f is a root of unity. □

Proposition 7.2(iii) says that the natural map from the set of reduced divisors Red_F to the oriented Arakelov class group $\widetilde{\mathrm{Pic}}^0_F$ is injective. The following example shows that, in general, the map $\mathrm{Red}_F \longrightarrow \mathrm{Pic}^0_F$ is *not*.

EXAMPLE 9.3. Let $a > b \geq 1$ and put $\Delta = b^2 - 4a^2$. Suppose that Δ is squarefree and let F denote the complex quadratic number field $\mathbb{Q}(\sqrt{\Delta})$. Let I denote the fractional O_F-ideal $\mathbb{Z} + f\mathbb{Z}$, where $f = (b + \sqrt{\Delta})/(2a)$. Then $1 \in I$ is minimal. Let $\sigma : F \longrightarrow \mathbb{C}$ denote the unique infinite prime. Since $\sigma(f)$ has absolute value 1, the element f is also minimal. Since f is not a unit of O_F, Lemma 9.2 implies that the reduced divisors $d(I)$ and $d(f^{-1}I)$ are distinct, but that their classes in Pic^0_F are equal.

Theorem 7.7 says that the distance between the images of the reduced divisors in $\widetilde{\mathrm{Pic}}^0_F$ is bounded from below by an absolute constant. The following example shows that this is false for the Arakelov class group Pic^0_F.

EXAMPLE 9.4. Let n be a large even integer such that $\Delta = n^2 + 1$ is squarefree and consider the field $F = \mathbb{Q}(\sqrt{\Delta})$. Let $f = (1 + \sqrt{\Delta})/n \in F$. Then 1 is a minimal element in $I = \mathbb{Z} + f\mathbb{Z}$. The conjugates $\sigma(f)$ are close to 1 and -1 respectively. Indeed, we have $\left|\log|\sigma(f)|\right| \approx \Delta^{-1/2}$ for each infinite prime σ. It follows from Lemma 9.2(iii) that the classes of the reduced divisors $d(I)$ and $d(f^{-1}I)$ are at distance at most $2\sqrt{2}\,\Delta^{-1/2}$ in Pic^0_F.

The definition of the set Red_F is rather delicate, as we'll see now by considering slight variations of it. We let Red'_F denote the set of divisors $d(I)$ for which $1 \in I$ is a *shortest* rather than a *minimal* vector and write Red''_F for the set of divisors $d(I)$ for which we have $N(I^{-1}) \leq \partial_F = (2/\pi)^{r_2}\sqrt{|\Delta_F|}$ and for which $1 \in I$ is merely *primitive*, i.e., not divisible by an integer $d \geq 2$. Since *shortest* implies *minimal* and *minimal* implies *primitive*, we have the inclusions

$$\mathrm{Red}'_F \quad \subset \quad \mathrm{Red}_F \quad \subset \quad \mathrm{Red}''_F$$

of finite sets. Theorem 7.4 says that the set Red_F is rather 'dense' in the Arakelov divisor class group. It is not clear whether the set Red'_F has the same property. The proof of Theorem 7.4, showing that every $D = (I, u)$ of degree 0 is close to a reduced divisor $D' \in \mathrm{Red}_F$, does not work for Red'_F. Indeed, tracing the steps of the proof of Theorem 7.4, we see that if $f \in I$ is a shortest vector, it is also minimal and hence the element $1 \in f^{-1}I$ is *minimal*. It follows that the divisor $d(f^{-1}I)$ is in Red_F. However, 1 need not be a *shortest* vector in $f^{-1}I$ so that $d(f^{-1}I)$ may not be contained in Red'_F.

The following example shows that this phenomenon actually occurs. It shows that the set Red'_F is, at least in this sense, too small.

EXAMPLE 9.5. We present examples of reduced Arakelov divisors $D = d(I)$ with the property that the element $1 \in I$ is *not* a shortest vector of the lattice I associated to (I, u) for *any* $u \in F_{\mathbb{R}}^*$. This implies that D is not equal to $d(f^{-1}J)$ for any divisor $D' = (J, v)$ and a shortest element $f \in J$. Indeed, if that were the case, 1 would be shortest vector in the lattice associated to the Arakelov divisor $(I, f^{-1}v)$.

Let F be a real quadratic number field of discriminant Δ. Then $F = \mathbb{Q}(\sqrt{\Delta})$. Suppose that $d(I)$ is a reduced Arakelov divisor. We write $I = \mathbb{Z} + f\mathbb{Z}$ where $f > 0$ and $-1 < \bar{f} < 0$. Here we identify F with its image in $\mathbb{R}$ through one of its embeddings and we write $f \mapsto \bar{f}$ for the other embedding.

CLAIM. *If* $N(f - \frac{1}{2}) > -\frac{3}{4}$, *then* 1 *is not a shortest element of* I *for any Arakelov divisor* (I, u) *of degree zero.*

PROOF. Suppose that $D = (I, u)$ has degree 0. Then we have

$$u = \left(\frac{v}{\sqrt{N(I)}}, \frac{v^{-1}}{\sqrt{N(I)}} \right)$$

for some $v \in \mathbb{R}^*_{>0}$. Suppose that $1 \in I$ is a shortest vector in the lattice associated to D. This implies in particular that $\|1\|_D \leq \|f\|_D$ and $\|1\|_D \leq \|f - 1\|_D$. This means that $v^{-2} + v^2 \leq v^{-2} f^2 + v^2 \bar{f}^2$ and that $v^{-2} + v^2 \leq v^{-2}(f - 1)^2 + v^2(\bar{f} - 1)^2$. In other words we have that $v^4 \leq (f^2 - 1)/(1 - \bar{f}^2)$ and $v^4 \geq (2f - f^2)/(\bar{f}^2 - 2\bar{f})$ respectively. Therefore, if the upper bound for v^4 is smaller than the lower bound, there cannot exist such an v. This happens precisely when $(f - \bar{f})(2f\bar{f} - f - \bar{f} + 2) > 0$. Since $f - \bar{f}$ is positive, this means that $2f\bar{f} - f - \bar{f} + 2 > 0$ which is equivalent to $N(f - \frac{1}{2}) > -\frac{3}{4}$. This proves the claim. □

When $f = (b + \sqrt{\Delta})/(2a)$ as in Section 8, a sufficient condition for the inequality of the claim to hold is that $a \geq \sqrt{\Delta/3}$. As an explicit example, take the field $\mathbb{Q}(\sqrt{21})$ and the reduced divisor $d(I)$ associated to $I = \mathbb{Z} + f\mathbb{Z}$, with $f = (3 + \sqrt{21})/6$.

In the other direction, it may happen that the image of Red''_F is very dense in $\widetilde{\mathrm{Pic}}^0_F$, so that an analogue of Theorem 7.7 does not hold for this set. We present two examples, due to H. W. Lenstra, showing that for some number fields certain small open balls in $\widetilde{\mathrm{Pic}}^0_F$ contain the images of very many $D \in \mathrm{Red}''_F$. Both examples exploit the existence of certain 'very small' elements in F. In the first example these are contained in a proper subfield, but this is not the case in the second example.

EXAMPLE 9.6. Let F be a number field of degree n containing $\mathbb{Q}(i)$. Let $m, m' \in \mathbb{Z}$ satisfy $\frac{1}{2}|\Delta_F|^{1/2n} < m,\ m' < |\Delta_F|^{1/2n} - 1$. Let I and I' denote the inverses of the O_F-ideals generated by $m-i$ and $m'-i$ respectively. Then 1 is primitive in both I and I' and the norms of I^{-1} and I'^{-1} do not exceed $\partial_F = (2/\pi)^{r_2}\,|\Delta_F|^{1/2}$. It follows that $d(I)$ and $d(I')$ are in Red''_F. If the images of $d(I)$ and $d(I')$ in $\widetilde{\mathrm{Pic}}^0_F$ are equal, Proposition 6.4 implies that $I = mI'$ for some $m \in \mathbb{Q}^*$. Since 1 is primitive in both I and I', it follows that $m = \pm 1$. This implies that $I = I'$ and hence that $N(I) = m^2 + 1$ is equal to $N(I') = m'^2 + 1$, so that $m = m'$. Therefore $d(I)$ and $d(I')$ are distinct in $\widetilde{\mathrm{Pic}}^0_F$, whenever m and m' are.

Assume in addition that $|m - m'| < |\Delta_F|^{1/3n}$ and that $|\Delta_F| > 4^{6n}$. Then the distance between m and m' is much smaller than m and m' themselves. The distance between the Arakelov divisors $d(I)$ and $d(I')$ in $\widetilde{\mathrm{Pic}}^0_F$ is at most $\sqrt{n}\,|\log((m-i)/(m'-i))|$. This does not exceed

$$\begin{aligned}\sqrt{n}\,|m-m'|/(|m-i|-|m-m'|) &\le \sqrt{n}|\Delta_F|^{1/3n}/\left(\tfrac{1}{2}|\Delta_F|^{1/2n} - |\Delta_F|^{1/3n}\right)\\ &\le 4\sqrt{n}|\Delta_F|^{-1/6n}.\end{aligned}$$

In this way we obtain $|\Delta_F|^{1/3n}$ elements of Red''_F whose images in $\widetilde{\mathrm{Pic}}^0_F$ are distinct, but are as close as $4\sqrt{n}\,|\Delta_F|^{-1/6n}$ to one another. By varying F over degree $n/2$ extensions of $\mathbb{Q}(i)$, we can make $|\Delta_F|$ as large as we like. One may replace $\mathbb{Q}(i)$ by any number field and proceed similarly.

EXAMPLE 9.7. Let $n \ge 4$ and $a \in \mathbb{Z}$ be such that the polynomial $X^n - a$ is irreducible over $\mathbb{Q}$. Let α denote a zero and put $F = \mathbb{Q}(\alpha)$. Suppose that the ring of integers of F is equal to $\mathbb{Z}[\alpha]$. There are infinitely many such integers a. Then $|\Delta_F| = n^n|a|^{n-1}$ and $|\sigma(\alpha)| = |a|^{1/n}$ for every infinite prime σ. Let $m, m' \in \mathbb{Z}$ satisfy $\frac{1}{2}|a|^{1/2-1/2n} + |a|^{1/n} < m, m' < |a|^{1/2-1/2n}$ and $|m - m'| \le |a|^{1/4}$. Consider two Arakelov divisors $d(I)$ and $d(J)$ given by $I^{-1} = (m-\alpha)O_F$ and $J^{-1} = (m'-\alpha)O_F$. The norms of I^{-1} and J^{-1} are at most ∂_F. Since both I and J contain 1 as a primitive element, we have $d(I), d(J) \in \mathrm{Red}''_F$. The argument used in Example 9.6 shows that the images of $d(I)$ and $d(J)$ in $\widetilde{\mathrm{Pic}}^0_F$ are distinct when $m \ne m'$. The difference between $d(I)$ and $d(J)$ is equal to $(IJ^{-1}, N(IJ^{-1})^{1/n})$, which is equivalent to (O_F, v), where

$$v = \frac{m-\sigma(\alpha)}{m'-\sigma(\alpha)}\left|N\left(\frac{m'-\alpha}{m-\alpha}\right)\right|^{1/n}.$$

It follows that $\|d(I) - d(J)\|_{\widetilde{\mathrm{Pic}}}$ is at most

$$2\sqrt{n}\,\max_\sigma \left|\log\left(\frac{m-\sigma(\alpha)}{m'-\sigma(\alpha)}\right)\right|.$$

Since $(m-\sigma(\alpha))/(m'-\sigma(\alpha)) = 1 + (m-m')/(m'-\sigma(\alpha))$ and since $|m'-\sigma(\alpha)| \geq m' - |\sigma(\alpha)| \geq \frac{1}{2}|a|^{1/2-1/2n}$, the absolute value of the logarithm of $(m-\sigma(\alpha))/(m'-\sigma(\alpha))$ is at most $4|m-m'|/|a|^{1/2-1/2n}$ for each σ. It follows that $\|d(I)-d(J)\|_{\widetilde{\text{Pic}}}$ is at most $4\sqrt{n}|a|^{-1/4+1/2n}$, which becomes arbitrarily small as $|a|$ grows.

10. Computations with reduced Arakelov divisors

In this section we discuss the set of reduced Arakelov divisors from a computational point of view. Our presentation is informal; in particular, we do not say much about the accuracy of the approximations required to perform the computations with the real and complex numbers involved. (See [Thiel 1995] for a more rigorous approach.) Since Arakelov divisors can be represented as lattices in the Euclidean space $F_{\mathbb{R}}$, lattice reduction algorithms play an important role. When the degree n of the number field is large, the celebrated Lenstra–Lenstra–Lovász (LLL) reduction algorithm [Lenstra et al. 1982; Lenstra 2008] is an important tool.

We suppose that the number field F is given as $\mathbb{Q}(\alpha)$, where α is the zero of some irreducible monic polynomial $\varphi(X) \in \mathbb{Z}[X]$. We assume that we have already computed an LLL-reduced basis $\{\omega_1, \ldots, \omega_n\}$ for the ring of integers O_F embedded in $F_{\mathbb{R}}$. In other words, we have an explicit lattice

$$O_F = \omega_1\mathbb{Z} + \ldots + \omega_n\mathbb{Z} \subset F_{\mathbb{R}},$$

with, say, an LLL-reduced basis $\{\omega_1, \ldots, \omega_n\}$. Such a basis can be computed as explained in [Lenstra 1992, Section 4] or [Cohen 1993, Section 6.1] combined with a basis reduction algorithm. We have also computed a multiplication table i.e., coefficients $\lambda_{ijk} \in \mathbb{Z}$ for which $\omega_i\omega_j = \sum_k \lambda_{ijk}\omega_k$. The discriminant Δ_F of F is the integer given by $\Delta_F = \det(\mathrm{Tr}(\omega_i\omega_j))$. By [Lenstra 1992, Section 2.10] we have $\lambda_{ijk} = |\Delta_F|^{O(n)}$. We view the degree n of F as fixed and estimate the running times of the algorithms in terms of $|\Delta_F|$.

An Arakelov divisor or oriented Arakelov divisor $D = (I, u)$ is determined by its associated ideal I and the vector $u \in F_{\mathbb{R}}^* \cong \prod_\sigma F_\sigma^*$. It can be represented by an $n \times n$ matrix λ_{ij} having the property that the vectors $\sum_{ij} \lambda_{ij}\omega_j$ form an LLL-reduced basis for the lattice $I \subset F_{\mathbb{R}}$, together with a sufficiently accurate approximation of the vector $u = (u_\sigma)_\sigma$. We have $\lambda_{ij} = O(N(I))$ (see [Thiel 1995]). In practice, one might want to take logarithms and work with the vectors $(\log u_\sigma)_\sigma$. There are efficient algorithms to multiply ideals, to compute inverses and to test for equality. See [Cohen 1993, sections 4.6–4.8]. Using these one can compute efficiently in the group Div_F. The algorithms have been implemented in LiDIA, MAGMA and PARI.

Rather than the Arakelov divisor group, we are interested in computing in the *Arakelov class group* Pic_F^0. We do calculations in this group by means of the set Red_F of *reduced* divisors in Div_F^0. By Theorems 7.4 and 7.7, the image of the finite set Red_F is in a certain sense regularly distributed in the compact groups Pic_F^0 and $\widetilde{\mathrm{Pic}}_F^0$. Reduced divisors have one further property that is important for our application: a reduced divisor D is of the form $D = d(I) = (I, N(I)^{-1/n})$ where I^{-1} is and integral ideal of norm at most $\partial_F = (2/\pi)^{r_2}|\Delta_F|^{1/2}$. Therefore D can be represented using only $(\log|\Delta_F|)^{O(n)}$ bits.

Before describing the algorithms, we formulate a lemma concerning the LLL algorithm.

LEMMA 10.1. *Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be an LLL-reduced basis of a real vector space V. Then for every vector $\mathbf{x} = \sum_{i=1}^n m_i\mathbf{b}_i$ of V we have*

$$|m_i|\|\mathbf{b}_i^*\| \;\le\; \Big(\frac{3}{\sqrt{2}}\Big)^{n-i}\|\mathbf{x}\| \quad \textit{for } 1 \le i \le n.$$

Here $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ denotes the Gram–Schmidt orthogonalization of the basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$.

For the proof, see [Lenstra 2008].

COROLLARY 10.2. *Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be an LLL-reduced basis of a real vector space V. Then we have for any vector $\mathbf{x} = \sum_{i=1}^n m_i\mathbf{b}_i$ in V that*

$$|m_i| \;\le\; 2^{(i-1)/2}\Big(\frac{3}{\sqrt{2}}\Big)^{n-i}\frac{\|\mathbf{x}\|}{\|\mathbf{b}_1\|} \quad \textit{for } 1 \le i \le n.$$

PROOF. The LLL conditions imply that $\|\mathbf{b}_1^*\| \le 2^{(i-1)/2}\|\mathbf{b}_i^*\|$ for every $i = 1, 2, \ldots, n$. Since $\mathbf{b}_1 = \mathbf{b}_1^*$, the result follows from Lemma 10.1. □

We have the following basic algorithms at our disposal. For number fields of fixed degree n, each runs in time polynomial in $\log|\Delta_F|$.

ALGORITHM 10.3 (REDUCTION ALGORITHM). Given an Arakelov divisor $D = (I, u) \in \mathrm{Div}_F^0$,

– check whether it is reduced or not;
– compute a reduced divisor D' that is close to D in Pic_F^0.

Description. We compute an LLL-reduced basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ of the lattice $uI \subset F_{\mathbb{R}}$. Then we compute a shortest vector $\mathbf{x}$ in uI as follows. Any shortest vector $\mathbf{x} = \sum_{i=1}^n m_i\mathbf{b}_i$ in the lattice satisfies $\|\mathbf{x}\|/\|\mathbf{b}_1\| \le 1$. Therefore Corollary 10.2 implies that the coordinates $m_i \in \mathbb{Z}$ are bounded independent of the discriminant of F. To compute a shortest vector in the lattice in time polynomial in $\log|\Delta_F|$, we may therefore just try all possible m_i.

To find a reduced divisor D' that is close to D in Pic_F^0, we compute a shortest vector f in the lattice I associated to D. The divisor $D' = d(f^{-1}I)$ is then reduced. Moreover, by Theorem 7.4 or rather its proof, the divisor D' has the property that $\|D - D'\|_{\mathrm{Pic}} \leq \log \partial_F$, so that D' is close to D.

In a similar way one can check that a given divisor $D = (I, u)$ is reduced. First of all we must have that $u = N(I)^{-1/n}$. Then we check that 1 is contained in I. To see whether 1 is a *minimal* element of I, we need to make sure that the box

$$B = \{(y_\sigma) \in F_{\mathbb{R}} : \ |y_\sigma| < 1 \text{ for all } \sigma.\}.$$

contains no nonzero points of the lattice $I \subset F_{\mathbb{R}}$. The box B contains all vectors of length at most 1. On the other hand, every vector in B has length at most $\sqrt{n}$.

If the first vector $\mathbf{b}_1$ of the LLL-reduced basis has length less than 1, it is contained in B and the element $1 \in I$ is *not* minimal. In this case we are done. Suppose therefore that we have $\|\mathbf{b}_1\| \geq 1$. It suffices now to compute all vectors $\mathbf{x}$ in the lattice that have length less than $\sqrt{n}$ and see whether they are in the box B or not. By Corollary 10.2, the vectors $\mathbf{x} = \sum_{i=1}^n m_i \mathbf{b}_i$ of length at most $\sqrt{n}$ have the property that

$$|m_i| \ \leq \ 2^{(i-1)/2} \left(\frac{3}{\sqrt{2}}\right)^{n-i} \frac{\|\mathbf{x}\|}{\|\mathbf{b}_1\|} \ \leq \ 2^{(n-1)/2} \left(\frac{3}{2}\right)^{n-i} \sqrt{n}.$$

So, the number of vectors to be checked is bounded independently of the discriminant of F. This completes the description of the algorithm. Both algorithms run in time polynomial in $\log |\Delta_F|$, $\log \|u\|$ and the logarithmic height of $N(I)$.

ALGORITHM 10.4 (COMPOSITION ALGORITHM). Given two reduced Arakelov divisors $D = d(I)$ and $D' = d(J)$, compute a reduced divisor that is close to the sum $D + D'$ in Pic_F^0.

Description. One first adds D and D' as divisors. Since $N(I^{-1}), N(J^{-1}) \leq \partial_F$, the result $(IJ, N(IJ)^{-1/n})$ can be computed in time polynomial in $\log |\Delta_F|$. Then one reduces the result by means of Algorithm 10.3. The resulting reduced divisor is then close to $D + D'$. Since $N(IJ)^{-1} \leq \partial_F^2$, the running time of this second step is also polynomial in $\log |\Delta_F|$.

ALGORITHM 10.5 (INVERSION ALGORITHM). Given a reduced Arakelov divisor $D = d(I)$, compute a reduced divisor that is close to $-D$ in Pic_F^0.

Description. One just computes the inverse ideal I^{-1} and reduces the divisor $d(I^{-1})$ by means of Algorithm 10.3. Since $N(I^{-1}) \leq \partial_F$, the running time of this algorithm is also polynomial in $\log |\Delta_F|$.

I owe the next algorithm to Hendrik Lenstra. See [Buchmann 1987a; 1987c; Thiel 1995] for a different approach. We first prove a lemma.

LEMMA 10.6. *Let $D = (I, u)$ be an Arakelov divisor of degree 0 and let $\varepsilon > 0$. Then every reduced divisor at distance at most ε from D is of the form $d(I\mu^{-1})$ where μ is a minimal element of I satisfying*

$$\|\mu\|_D < \sqrt{n}\, e^{2\varepsilon} \|y\|_D \quad \text{for all nonzero } y \in I.$$

In particular, the inequality holds for a nonzero $y \in I$ that is shortest with respect to the metric of D.

PROOF. Let D' be a reduced divisor for which we have $\|D - D'\|_{\mathrm{Pic}} < \varepsilon$. Then we have $D' = d(I\mu^{-1})$ for some minimal element $\mu \in I$. By Proposition 6.2 there is a unit η so that for $D'' = D + (\mu) + (O_F, |\eta|)$ we have

$$e^{-\|D'-D''\|_{\mathrm{Pic}}} \;\le\; \frac{\|x\|_{D'}}{\|x\|_{D''}} \;\le\; e^{\|D'-D''\|_{\mathrm{Pic}}} \quad \text{for every } x \in I\mu^{-1}.$$

We multiply μ by η. Then μ remains a minimal element of I and the divisor D' does not change. But now D'' is equal to $D + (\mu)$. Since $\|D - D'\|_{\mathrm{Pic}} = \|D' - D''\|_{\mathrm{Pic}}$, the inequality above and Proposition 7.1 imply that

$$\begin{aligned}\|\mu\|_D = \|1\|_{D+(\mu)} &\le e^{\varepsilon} \|1\|_{D'} \\ &\le e^{\varepsilon}\sqrt{n}\|x\|_{D'} \le e^{2\varepsilon}\sqrt{n}\|x\|_{D+(\mu)} = e^{2\varepsilon}\sqrt{n}\|x\mu\|_D,\end{aligned}$$

for any nonzero $x \in I\mu^{-1}$. Hence $\|\mu\|_D \le \sqrt{n}e^{2\varepsilon}\|y\|_D$ for all non-zero $y \in I$. □

ALGORITHM 10.7 (SCAN ALGORITHM). Let $D = (I, u)$ be an Arakelov divisor of degree 0. Compute all reduced Arakelov divisors in a ball in the Arakelov class group Pic^0_F of radius 1 and center D in time polynomial in $\log|\Delta_F|$.

Description. Choose $\varepsilon, \varepsilon' \in \mathbb{R}$ such that $0 < \varepsilon' < \varepsilon < 1$. Inside the open ball of divisors in Pic^0_F having distance at most $1 + \varepsilon$ from D, we compute a *web* of regularly distributed points. The points P in the web are at most ε and at least ε' apart. By Theorem 7.4 every P is the class of a divisor of the form $D' + (O_F, v)$ for some reduced divisor $D' = d(J)$ and a totally positive $v \in F^*_{\mathbb{R}}$ satisfying $\|v\|_{\mathrm{Pic}} < \log \partial_F$. Therefore an LLL-reduced basis for the lattice associated to each P can be computed in time polynomial in $\log|\Delta_F|$.

By Lemma 10.6, the reduced divisors we are looking for are among the divisors of the form $d(J\mu^{-1})$ where $D' = d(J)$ is reduced, $P = D' + (O_F, v)$ is in the web and $\mu \in J$ is a *minimal* element for which $\|\mu\|_P$ is at most $e^{2\varepsilon}\sqrt{n}$ times the length of a nonzero element $y \in J$ that is shortest with respect to the metric induced by P. So, it suffices to compute the elements μ for all P in the web. For a given P, Corollary 10.2 says that the number of vectors $\mu \in J$ of length at most $e^{2\varepsilon}\sqrt{n}$ times the length of the shortest nonzero vector, is bounded independently of P and even of the discriminant of F. They can be computed

in time polynomial in $\log|\Delta_F|$. Minimality of the elements μ can be tested by means of Algorithm 10.3. Finally, since the divisors P are at least ε' apart, the number of points in the web is proportional to the volume of the ball.

ALGORITHM 10.8 (JUMP ALGORITHM). Given a divisor

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

of degree 0, compute a reduced Arakelov divisor whose image in Pic_F^0 has distance less than $\log \partial_F$ from D.

Description. We assume that at most $O(\log|\Delta_F|)$ coefficients of D are non-zero, that the coefficients themselves have size $|\Delta_F|^{O(1)}$ and that $N(\mathfrak{p})$ has size $|\Delta_F|^{O(1)}$ for the prime ideals $\mathfrak{p}$ with $n_{\mathfrak{p}} \neq 0$. Directly applying the reduction algorithm to $D = (I, v)$ with $I = \prod_{\mathfrak{p}} \mathfrak{p}^{n_{\mathfrak{p}}}$ and $v = \exp(x_\sigma)_\sigma$, is not a very good idea, since the LLL-algorithm and therefore the reduction algorithm run in time polynomial in the coefficients $|x_\sigma|$, which is *exponential* in terms of $\log|\Delta_F|$. Therefore we proceed differently.

We have $D = (I, 1) + (O_F, v)$. We compute reduced divisors close to $(I, 1)$ and to (O_F, v). Adding these as in Algorithm 10.4, we may then compute a reduced divisor close to D, in the sense that its distance to D is at most $\log \partial_F$. For each prime ideal $\mathfrak{p}$ with $n_{\mathfrak{p}} \neq 0$ we use Algorithm 10.3 to compute a reduced divisor $D_{\mathfrak{p}}$ close to $(\mathfrak{p}, 1)$. We compute a reduced divisor close to $\sum_{\mathfrak{p}} n_{\mathfrak{p}} D_{\mathfrak{p}}$ by composing and reducing as in Algorithm 10.4. The result is a reduced divisor close to $(I, 1)$.

Next we explain how to compute efficiently a reduced divisor close to the divisor (O_F, v). Let $t \geq 0$ be the smallest integer for which the vector $y = (y_\sigma)_\sigma$ given by $y_\sigma = 2^{-t} x_\sigma$ satisfies $n|y_\sigma| < \log \partial_F$ for all σ. Then $t \in O(\log|\Delta_F|)$. Put $w = \exp(y_\sigma)_\sigma$. We have $w^{2^t} = v$. We inductively compute reduced Arakelov divisors $D_i = d(I_i)$ for which

$$\|D_i - (O_F, w^{2^i})\|_{\mathrm{Pic}} < \log \partial_F, \qquad \text{for } i = 0, 1, \ldots, t,$$

as follows. We put $D_0 = (O_F, 1)$. We compute D_{i+1} from D_i by doubling. More precisely, by induction we have $D_i = (O_F, w^{2^i}) + (O_F, w_i)$ in Pic_F^0 for some $w_i \in F_{\mathbb{R}}^*$ with $\|w_i\|_{\mathrm{Pic}} < \log \partial_F$. Let D_{i+1} be a reduced divisor whose distance to $2D_i - (O_F, w_i^2)$ is at most $\log \partial_F$. Then we have

$$D_{i+1} - (O_F, w^{2^{i+1}}) = (O_F, w_{i+1})$$

in Pic_F^0 for some $w_{i+1} \in F_{\mathbb{R}}$ satisfying $\|w_{i+1}\|_{\mathrm{Pic}} < \log \partial_F$. Using Algorithm 10.3, we see that D_{i+1} is of the form $d(I_{i+1})$ where $I_{i+1} = I_i^2/(x)$ for some element $x \in I_i^2$ that has the property that $w_i^{-2} x$ is a shortest vector in the

lattice $w_i^{-2} I_i^2 \subset F_{\mathbb{R}}$. Since $\|w_i\|_{\mathrm{Pic}} < \log \partial_F$ and since $D_i = d(I_i)$ is reduced, the computation of D_{i+1} can be performed in time polynomial in $\log |\Delta_F|$. This completes the description of the algorithm.

Mutatis mutandis, we have the same algorithms for the group $\widetilde{\mathrm{Div}}_F^0$ of *oriented* divisors and for the oriented Arakelov class group $\widetilde{\mathrm{Pic}}_F^0$. The only difference is that the unit u of an oriented Arakelov divisor $D = (I, u)$ is a complex rather than a positive real number. The image of the set of reduced Arakelov divisors in this group is probably also reasonably dense in $\widetilde{\mathrm{Pic}}_F^0$ and that's all we need for the Jump algorithm to work. See Proposition 9.1.

APPLICATION 10.9. We present an algorithm to compute the function $h^0(D)$, introduced in [Van der Geer and Schoof 2000]. For an Arakelov divisor $D = (I, u)$, the number $h^0(D)$ should be viewed as the arithmetic analogue of the dimension of the space of global sections of a divisor D on an algebraic curve. The number $h^0(D)$ depends only on the class of D in Pic_F^0 and is defined as

$$h^0(D) = \log \sum_{f \in I} \exp(-\pi \|f\|_D^2).$$

See Section 4 for the close relation between the function $h^0(D)$ and the Hermite constant $\gamma(D)$ of the ideal lattice associated to D. Since the short vectors $f \in I$ contribute the most to this exponentially quickly converging sum, the function $h^0(D)$ can be evaluated most efficiently when we know a good, i.e., a reasonably orthogonal basis for I. As we explained above, a direct application of a lattice reduction algorithm to D may be very time consuming. Therefore we apply the *Jump algorithm*. We jump to a reduced divisor $D' = d(J)$ close to D in Pic_F^0. Then D is equivalent to $D' + (O_F, v)$ for some short $v \in F_{\mathbb{R}}^*$ and

$$\begin{aligned} h^0(D) = h^0(D' + (O_F, v)) &= \log \sum_{f \in J} \exp\bigl(-\pi \|f\|_{D'+(O_F,v)}^2\bigr) \\ &= \log \sum_{f \in J} \exp\biggl(-\pi N(J)^{-2/n} \sum_{\sigma} \deg(\sigma) |\sigma(f)|^2 v_\sigma^2\biggr). \end{aligned}$$

Since D' is reduced and the vector $v = (v_\sigma)_\sigma$ is short, an LLL reduced basis for the lattice associated to $D' + (O_F, v)$ can be computed efficiently. This is because J^{-1} is an integral ideal of norm at most $|\Delta_F|^{1/2}$. This completes the description of the algorithm to compute $h^0(D)$.

11. A deterministic algorithm

In this section we describe a *deterministic* algorithm to compute the Arakelov class group of a number field F of degree n and discriminant Δ_F. It runs in time proportional to $\sqrt{|\Delta_F|}$ times a power of $\log |\Delta_F|$.

LEMMA 11.1. *Let $B > 0$. Then any ideal $J \subset O_F$ with $N(J) < B$ is of the form $J = xI^{-1}$, where the Arakelov divisor $D = (I, N(I)^{-1/n})$ is reduced, the element $u = N(x)^{1/n}/|x|$ of $F_{\mathbb{R}}^*$ satisfies $\|u\|_{\mathrm{Pic}} < \log \partial_F$, and the element x is contained in I and satisfies $\|x\|_{D+(O_F,u)} < \sqrt{n} B^{1/n}$.*

PROOF. Suppose that $J \subset O_F$ satisfies $N(J) < B$. By Minkowski's Theorem there exists $y \in J^{-1}$, a shortest vector in $J^{-1} \subset F_{\mathbb{R}}$, satisfying $|\sigma(y)| < N(J)^{-1/n} \partial_F^{1/n}$ for every σ. We pick such an element y, put $x = 1/y$ and $I = xJ^{-1}$. Then the Arakelov divisor $D = (I, N(I)^{-1/n})$ is reduced. Moreover, since $xI^{-1} = J \subset O_F$, we have $x \in I$.

Writing $u = N(x)^{1/n}/|x|$, all coordinates of the vector $N(I)^{-1/n} ux$ have absolute value $N(I)^{-1/n} N(x)^{1/n} = N(J)^{1/n}$, so

$$\|x\|_{D+(O_F,u)} = \sqrt{n} N(J)^{1/n} < \sqrt{n} B^{1/n}.$$

Finally, we estimate $\|u\|_{\mathrm{Pic}}$. Since $N(I) \le 1$, we have

$$\begin{aligned} |u_\sigma| &= \frac{|N(x)|^{1/n}}{|\sigma(x)|} = |\sigma(y)||N(x)|^{1/n} \le N(J)^{-1/n} \partial_F^{1/n} |N(x)|^{1/n} \\ &= N(I)^{1/n} \partial_F^{1/n} \le \partial_F^{1/n}. \end{aligned}$$

Lemma 7.5 then implies $\|u\|_{\mathrm{Pic}} \le (1 - 1/n)^{1/2} \log \partial_F \le \log \partial_F$, as required. □

It is not hard to see that the lemma's converse also holds: any ideal $J \subset O_F$ for which the three conditions are satisfied automatically has norm at most B.

ALGORITHM 11.2. Suppose we have computed all reduced divisors in a connected component of the Arakelov class group Pic_F^0. In that component, detect all divisors that are of the form $(J^{-1}, N(J)^{1/n})$ with $J \subset O_F$ and $N(J) < \partial_F$.

Description. Let $\varepsilon, \varepsilon' \in \mathbb{R}$ be such that $0 < \varepsilon' < \varepsilon$. For each reduced divisor $D = (I, N(I)^{-1/n})$ in the given connected component, we make a web in the ball of center $D = (I, N(I)^{-1/n})$ and radius $\log \partial_F$, whose members $P = D + (O_F, v) = (I, N(I)^{-1/n} v)$ are at most ε and at least ε' apart. For each divisor $P = D + (O_F, v)$ in the web, we compute the vectors x for which we have $\|x\|_P \le \sqrt{n} e^{2\varepsilon} \partial_F^{1/n}$. This is done as follows. First we compute an LLL-reduced basis $\mathbf{b}_1, \ldots, \mathbf{b}_n$ for the lattice associated to the Arakelov divisor P. Let $\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*$ denote its Gram–Schmidt orthogonalization. By Lemma 10.1 we have for any vector $x = \sum_{i=1}^n m_i \mathbf{b}_i$ in the lattice for which $\|x\|_P$ is at most $\sqrt{n} e^{2\varepsilon} \partial_F^{1/n}$, that

$$|m_i| \|\mathbf{b}_i^*\| \le \left(\frac{3}{\sqrt{2}}\right)^{n-1} \sqrt{n} e^{2\varepsilon} \partial_F^{1/n}.$$

We simply try *all* coefficients m_i satisfying this inequality.

For each such element x we then compute the corresponding ideals $J = I^{-1}x$. The ideals J that we compute in this way are contained in O_F. Moreover, every ideal $J \subset O_F$ of norm at most ∂_F and for which the Arakelov divisor $(J^{-1}, N(J)^{1/n})$ lies on the given component, is obtained in this way. Indeed, if we have $N(J) < \partial_F$, Lemma 11.2 with $B = \partial_F$ implies that $J = xI^{-1}$ for some reduced divisor $d(I) = (I, N(I)^{-1/n})$ and some $x \in I$. Moreover, we have $\|x\|_{D+(O_F,u)} < \sqrt{n}\partial_F^{1/n}$ for some u satisfying $\|u\|_{\mathrm{Pic}} < \log \partial_F$. This means that the divisor $D + (O_F, u)$ is contained in the ball of center $D = (I, N(I)^{-1/n})$ and radius $\log \partial_F$. Therefore there is a member $P = D + (O_F, v)$ of the web at distance at most ε from $D + (O_F, u)$. Proposition 6.2 implies then that

$$\|x\|_P \leq e^{2\varepsilon}\sqrt{n}\partial_F^{1/n},$$

as required.

This shows that we encounter all ideals J that we are after. But we'll find many more and we'll find each ideal many times. Indeed, the vectors $x = \sum_{i=1}^{n} m_i \mathbf{b}_i$ that we consider in the computation above satisfy

$$|m_i|\|\mathbf{b}_i^*\| \leq \left(\frac{3}{\sqrt{2}}\right)^{n-1} \sqrt{n}e^{2\varepsilon}\partial_F^{1/n}$$

for each i and hence

$$\|x\|_P \leq n\left(\frac{3}{\sqrt{2}}\right)^{n-1} e^{2\varepsilon}\partial_F^{1/n}.$$

It follows from the arithmetic geometric mean inequality that for the ideal $J = xI^{-1}$ we have

$$N(J) = N(xI^{-1}) \leq n^{n/2}e^{2\varepsilon n}\left(\frac{3}{\sqrt{2}}\right)^{n(n-1)} \partial_F.$$

In order to estimate the running time of this algorithm, we estimate the number of ideals J that we compute, *and in addition* we estimate for how many divisors P in the web and how many vectors x, we obtain each ideal J. By [Lenstra 1992, Theorem 6.5], the number of ideals J is bounded by $\sqrt{|\Delta_F|}$ times a power of $\log|\Delta_F|$ times a constant that depends only on the degree n. Next we bound the number of times we find each ideal J.

First, suppose that for some divisor $P = (I, N(I)^{-1/n}) + (O_F, v)$ in the web, there are two elements $x, x' \in I^{-1}$ satisfying

$$\max(\|x\|_P, \|x'\|_P) \leq \sqrt{n}e^{2\varepsilon}\partial_F^{1/n},$$

for which the ideals xI^{-1} and $x'I^{-1}$ are the *same*. Then we have

$$|\sigma(x)N(I)^{-1/n}v_\sigma| \leq \sqrt{n}e^{2\varepsilon}\partial_F^{1/n}$$

for each σ. Since we have $|N(v)| = 1$, the product over σ satisfies

$$\prod_{\sigma} |\sigma(x)N(I)^{-1/n}v_\sigma|^{\deg(\sigma)} = N(xI^{-1}) \geq 1.$$

Therefore

$$-(n-1)\log(\sqrt{n}e^{2\varepsilon}\partial_F^{1/n}) \;\leq\; \log|\sigma(x)N(I)^{-1/n}v_\sigma| \;\leq\; \log(\sqrt{n}e^{2\varepsilon}\partial_F^{1/n})$$

for every σ. We have the same inequalities for x'. It follows that the unit $\eta = x'/x$ satisfies

$$\begin{aligned} -\log\partial_F - n\log(\sqrt{n}e^{2\varepsilon}) \;&\leq\; \log|\sigma(\eta)| = \log\left|\frac{\sigma(x')}{\sigma(x)}\right| \\ &\leq\; \log\partial_F + n\log(\sqrt{n}e^{2\varepsilon}), \end{aligned}$$

for every σ and hence we have

$$\|\log|\eta|\| \leq \sqrt{n}\log\partial_F + n^{3/2}\log(\sqrt{n}e^{2\varepsilon}).$$

By [Dobrowolski 1979], there exists an absolute constant $c > 0$ such that any unit $\eta \in O_F^*$ that is not a root of unity satisfies $\|\log|\eta|\| > cn^{-3/2}$. Since the number of roots of unity in F is $O(n\log n)$, the number of units satisfying the bounds above is bounded by some power of $\log\partial_F$. It follows that the number of distinct elements $x \in I$ for which the ideals xI^{-1} are equal to the same ideal $J \subset O_F$ is also bounded by some power of $\log\partial_F$.

Next, suppose that an ideal $J \subset O_F$ of norm at most ∂_F is of the form xI^{-1} where $D = (I, N(I)^{-1/n})$ is a reduced divisor and $x \in I$ satisfies $\|x\|_P \leq e^{2\varepsilon}\sqrt{n}\partial_F^{1/n}$ for some divisor $P = D + (O_F, v)$ in the web constructed. In particular, v satisfies $\|v\|_{\mathrm{Pic}} < \log\partial_F$. This implies that

$$\left|\frac{\sigma(x)}{N(x)^{1/n}}v_\sigma^{-1}\right| = \left|\sigma(x)N(I)^{1/n}v_\sigma^{-1}\right|\frac{1}{N(J)^{1/n}} < \frac{\sqrt{n}e^{2\varepsilon}\partial_F^{1/n}}{N(J)^{1/n}} \leq \sqrt{n}e^{2\varepsilon}\partial_F^{1/n}.$$

It follows that the Arakelov divisors P and $(J^{-1}, N(J)^{1/n})$ are rather close to one another in Pic_F^0. Indeed, we have

$$\|P - (J^{-1}, N(J)^{1/n})\|_{\mathrm{Pic}} = \|(O_F, |x|N(x)^{-1/n}v_\sigma^{-1})\|_{\mathrm{Pic}}.$$

Since we have $\log|\sigma(x)N(x)^{-1/n}v_\sigma^{-1}| < \log(\sqrt{n}e^{2\varepsilon}\partial_F^{1/n})$ for every infinite prime σ, it follows from Lemma 7.5 that we have

$$\|P - (J, N(J)^{1/n})\|_{\mathrm{Pic}} < \log(n^{2/n}e^{2\varepsilon/n}\partial_F).$$

By Corollary 7.9, the number of reduced divisors in a ball is bounded by some constant, depending only on the degree of the number field, times its volume.

Therefore the number of web members P for which we encounter a given ideal $J \subset O_F$, is bounded by a polynomial expression in $\log \partial_F$.

This completes the description and our analysis of the algorithm.

A deterministic algorithm. Finally we explain the deterministic algorithm to compute the Arakelov class group of a number field F. This algorithm seems to have been known to the experts. It was explained to me by Hendrik Lenstra. We start at the neutral element $(O_F, 1)$ of the Arakelov class group. We use Algorithm 10.3 to determine all reduced Arakelov divisors in the ball of radius $2 \log \partial_F$ and center $(O_F, 1)$. Then we do the same with the reduced divisors D we found: determine all reduced Arakelov divisors in the ball of radius $2 \log \partial_F$ and center D. Proceeding in a systematic way that is somewhat complicated to write down, we find in this way *all* reduced divisors in the connected component of identity. Keeping track of their positions in terms of the coordinates in $\prod_\sigma F_\sigma$ one computes in this way the absolute values of a set of generators of the unit group O_F^*. The running time is proportional to the volume of the connected component of identity and is polynomial in $\log |\Delta_F|$.

Next we use Algorithm 11.2 and make a list $\mathfrak{L}$ of all integral ideals $J \subset O_F$ of norm at most ∂_F, for which $(J^{-1}, N(J)^{1/n})$ is on the connected component of identity. The amount of work is again proportional to the volume of the connected component of identity and polynomial in $\log |\Delta_F|$. By Minkowski's Theorem, the prime ideals of norm at most ∂_F generate the ideal class group of F. Therefore we check whether all prime ideals of norm at most ∂_F are in the list. This involves computing gcd's of the polynomial that defines the number field F with the polynomials $X^{p^i} - X$ for $i = 1, 2, \ldots, n$ for prime numbers p that are smaller than the Minkowski bound ∂_F. One reads off the degrees of the prime ideals over p and hence the number of primes of norm p^i for $i = 1, 2, \ldots$. The amount of work is linear in the length of the list and polynomial time in $\log p$ for each prime p. If all prime ideals of norm at most ∂_F are in the list $\mathfrak{L}$, then we are done. The class number is 1 and the Arakelov class group is connected.

However, if we do encounter a prime number p, for which a prime ideal $\mathfrak{p}$ of norm $p^i < \partial_F$ is missing, then we compute it. This involves factoring a polynomial of degree n modulo p. When we do this with a simple minded trial division algorithm, the amount of work is at most $p^i < \partial_F$ times a power of $\log |\Delta_F|$. By successive multiplications and reductions, we compute for $j = 1, 2, \ldots$ reduced divisor D_j in the connected components of the Arakelov class groups that contain divisors of the form $(\mathfrak{p}^j, u)$ for some u. Each time we check whether D_j is already in the list $\mathfrak{L}$. If it is, we stop computing divisors D_j.

Then we repeat the algorithm, but this time we work with the connected components of the divisors D_j rather than $(O_F, 1)$: we use Algorithm 10.3 to determine all reduced Arakelov divisors in the balls of radius $2 \log \partial_F$ and

center D_j. Then we do the same with the reduced divisors we found, and so on. Once we have computed all reduced divisors on the connected components of D_j, we use Algorithm 11.2 to compute all integral ideals $J \subset O_F$ of norm at most ∂_F, for which $(J^{-1}, N(J)^{1/n})$ is on the connected components of the divisors D_j and we add these to the list $\mathfrak{L}$.

When we are done with this, the list $\mathfrak{L}$ contains all integral ideals $J \subset O_F$ of norm at most ∂_F, whose classes are in the group generated by the ideal class of $\mathfrak{p}$. We check again whether all prime ideals of norm at most ∂_F are in the list. If this turns out to be the case, we are done. The ideal class group is cyclic, generated by the class of $\mathfrak{p}$. If, on the other hand, we do encounter a second prime number q, for which a prime ideal $\mathfrak{q}$ of norm $q^i < \partial_F$ is missing, then we compute it. We compute reduced divisors that are in the components of the powers of $\mathfrak{q}$ ... etc.

For each new prime that we find is *not* in the list $\mathfrak{L}$, we factor a polynomial and the amount of work to do this is at most ∂_F. However, since the ideal class group has order at most $\sqrt{|\Delta_F|}$ times power of $\log|\Delta_F|$, we need to do this at most $\log|\Delta_F|$ times. As a result this algorithm takes time at most $\sqrt{|\Delta_F|}$ times power of $\log|\Delta_F|$.

12. Buchmann's algorithm

In this section we briefly sketch Buchmann's algorithm [1990; 1991] for computing the Arakelov divisor class group and, as a corollary, the class group and regulator of a number field F. This algorithm combines the infrastructure idea with an algorithm for complex quadratic number fields presented by J. Hafner and K. McCurley [1989]. When we fix the degree of F, the algorithm is under reasonable assumptions subexponential in the discriminant of the number field F. A practical approach is described in [Cohen 1993, Section 6.5]. The algorithm has been implemented in LiDIA, MAGMA and PARI. See also [Thiel 1995].

Let F be a number field of degree n. The structure of Buchmann's algorithm is very simple. Our first description involves the Arakelov class group Pic_F^0 rather than the oriented group $\widetilde{\mathrm{Pic}}_F^0$.

Step 1: Estimate the volume of Pic_F^0. By Proposition 6.5 the volume of the compact Lie group Pic_F^0 is given by

$$\mathrm{vol}(\mathrm{Pic}_F^0) = \frac{w_F\sqrt{n}}{2^{r_1}(2\pi\sqrt{2})^{r_2}} \cdot |\Delta_F|^{1/2} \cdot \operatorname*{Res}_{s=1} \zeta_F(s).$$

The computation of r_1, r_2 and $w_F = \#\mu_F$ is easy. The discriminant is computed as a byproduct of the calculation of the ring of integers O_F. Approximating the

residue of the zeta function

$$\zeta_F(s) \;=\; \prod_{\mathfrak{p}} \left(1 - \frac{1}{N(\mathfrak{p})^s}\right)^{-1}$$

at $s = 1$ is done by dividing $\zeta_F(s)$ by the zeta function of $\mathbb{Q}$ and by directly evaluating a truncated Euler product

$$\prod_{p \le X} \frac{1 - 1/p}{\prod_{\mathfrak{p}|p}(1 - 1/N(\mathfrak{p}))}.$$

This involves factoring the ideals pO_F for all prime numbers $p < X$; for efficient methods to do this, see [Cohen 1993]. The Euler product converges rather slowly. Under assumption of the Generalized Riemann Hypothesis for the zeta function of F, using the primes $p < X$, the relative error is $O(X^{-1/2} \log |\Delta_F X|)$. Here the O-symbol only depends on the degree of the number field F. See [Buchmann and Williams 1989; Schoof 1982]. Therefore, there is a constant c only depending on the degree of F, so that if we truncate the Euler product at $X = c \log^2 |\Delta_F|$, the relative error in the approximation of $\mathrm{vol}(\mathrm{Pic}^0_F)$ is at most $1/2$.

Step 2: Compute a factor basis. We compute a factor base $\mathcal{B}$, that is, a list of prime ideals $\mathfrak{p}$ of O_F of norm less than Y for some $Y > 0$. Computing a factor basis involves factoring the ideals pO_F for various prime numbers p. It is convenient to do this alongside the computation of the Euler factors in Step 1. We add the infinite primes to our factor basis. By normalizing, we obtain in this way a factor basis of Arakelov divisors of degree 0. The factor basis should be so large that the natural homomorphism

$$\Big(\bigoplus_{\mathfrak{p} \in \mathcal{B}} \mathbb{Z} \times \bigoplus_{\sigma} \mathbb{R}\Big)^0 \quad \longrightarrow \quad \mathrm{Pic}^0_F$$

is surjective. By Proposition 2.2 this means that the classes of the primes in $\mathcal{B}$ must generate the ideal class group. Under assumption of the Generalized Riemann Hypothesis for the L-functions $L(s, \chi)$ associated to characters χ of the ideal class group Cl_F of F, this is the case for $Y > c' \log^2 |\Delta_F|$ for some constant $c' > 0$ that only depends on the degree of F. Taking $\mathcal{B}$ this big, we have

$$\mathrm{Pic}^0_F \;=\; \Big(\bigoplus_{\mathfrak{p} \in \mathcal{B}} \mathbb{Z} \times \bigoplus_{\sigma} \mathbb{R}\Big)^0 \Big/ H,$$

where H is the discrete subgroup of principal divisors of $\mathcal{B}$-units, i.e., the group of divisors (f) where $f \in F^*$ are elements whose prime factorizations involve only prime ideals $\mathfrak{p} \in \mathcal{B}$.

Step 3: Compute many elements in H. An Arakelov divisor $D = (I, u)$ is called $\mathcal{B}$-smooth if I is a product of powers of primes in $\mathcal{B}$. We need to find elements $f \in F^*$ for which (f) is $\mathcal{B}$-smooth and hence $(f) \in H$. This is achieved by repeatedly doing the following. For at most $O(\log |\Delta_F|)$ prime ideals $\mathfrak{p} \in \mathcal{B}$ pick random exponents $m_\mathfrak{p} \in \mathbb{Z}$ of absolute value not larger than $|\Delta_F|$. In addition, pick random $x_\sigma \in \mathbb{R}$ of absolute value not larger than $|\Delta_F|$. Replacing x_σ by $x_\sigma N(D)^{-1/n}$, scale the Arakelov divisor

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

so that it acquires degree zero. Then the class of D is a random element of Pic_F^0. We use the Jump Algorithm described in Section 10 and "jump to D". The result is a reduced divisor $D' = (I, N(I)^{-1/n})$ whose image in Pic_F^0 is not too far from the image of D. This means that

$$D = (f) + D' + (O_F, v)$$

for some $f \in F^*$ and $v = (v_\sigma) \in \left(\prod_\sigma \mathbb{R}_+^*\right)^0$ for which $\|v\|_{\mathrm{Pic}}$ is small, say at most $\log \partial_F$. There is no need to compute f, but when one applies the Jump Algorithm one should keep track of the infinite components and compute v or its logarithm.

Since the divisor D is random, it seems reasonable to think of the reduced divisor $D' = (I, N(I)^{-1/n})$ as being "random" as well. Next we attempt to factor the integral ideal I^{-1} into a product of prime ideals $\mathfrak{p} \in \mathcal{B}$. Since D' is random and since the norm of I^{-1} is at most $\partial_F = (2/\pi)^{r_2} |\Delta_F|^{1/2}$ and hence relatively small, we have a fair chance to succeed. If we do, then we have $D' = \sum_{\mathfrak{p} \in \mathcal{B}} n_\mathfrak{p} \mathfrak{p} + \sum_\sigma y_\sigma \sigma$ and hence $(f) \in H$. This factorization leads to a relation of the form

$$(f) = D - D' - (O_F, v) = \sum_{\mathfrak{p} \in \mathcal{B}} (m_\mathfrak{p} - n_\mathfrak{p}) \mathfrak{p} + \sum_\sigma (x_\sigma - y_\sigma + v_\sigma) \sigma.$$

In this way we have computed an explicit element in H.

Since we want to find many such relations, we need to be successful relatively often. In other words, the 'random' reduced divisors D' that we obtain, should be $\mathcal{B}$-*smooth* relatively often. This is the weakest point of our analysis of the algorithm. In Section 9 the set Red_F'' of Arakelov divisors $d(I)$ for which $1 \in I$ is primitive and $N(I^{-1}) \leq \sqrt{|\Delta_F|}$ was introduced. Under the assumption of the Generalized Riemann Hypothesis, Buchmann and Hollinger [1996] showed that when $Y \approx \exp(\sqrt{\log |\Delta_F|})$, the proportion of $\mathcal{B}$-smooth ideals J with $d(J^{-1}) \in \mathrm{Red}_F''$ is at least $\exp(-\sqrt{\log |\Delta_F|} \log \log |\Delta_F|)$. Here the Riemann Hypothesis for the zeta-function of the normal closure of F is used to guarantee the existence of sufficiently many prime ideals of norm at most $\sqrt{|\Delta_F|}$ and

degree 1. It is likely, but at present not known whether the proportion of $\mathcal{B}$-smooth ideals I for which $d(I)$ is contained in the subset Red_F rather than Red''_F, is *also* at least $\exp(-\sqrt{\log|\Delta_F|}\,\log\log|\Delta_F|)$. Even if this were the case, there is the problem that the divisor D' that comes out of the reduction algorithm is not a 'random' reduced divisor. Indeed, Example 9.5 provides examples of reduced divisors that are not the reduction of *any* Arakelov divisor. These reduced divisors will never show up in our calculations, since everything we compute is a result of the reduction algorithm. It would be of interest to know how many such reduced divisors there may be.

For the next step we need to have computed approximately as many elements in H as the size of the factor base $\mathcal{B}$. This implies that we expect to have to repeat the computation explained above about $\exp\bigl(\sqrt{\log|\Delta_F|}\,\log\log|\Delta_F|\bigr)$ times. When the discriminant $|\Delta_F|$ is large, this is more work than we need to do in Steps 1, 2 and 4. Step 3 is in practice the dominating part of the algorithm. It follows that the algorithm is subexponential and runs in time

$$O\bigl(\exp(\sqrt{\log|\Delta_F|}\,\log\log|\Delta_F|)\bigr).$$

Step 4: Verify that the elements computed in Step 3 actually generate H. Let H' denote the subgroup of H generated by the divisors

$$(f)=\sum_{\mathfrak{p}\in\mathcal{B}} k_{\mathfrak{p}}\mathfrak{p}+\sum_{\sigma} y_\sigma\sigma$$

computed in Step 3. The quotient group $\bigl(\bigoplus_{\mathfrak{p}\in\mathcal{B}}\mathbb{Z}\times\bigoplus_\sigma\mathbb{R}\bigr)^0/H'$ admits a natural map onto Pic^0_F. Its volume is equal to the determinant of a square matrix of size $\#\mathcal{B}$ whose rows are the coefficients of a set of $\#\mathcal{B}$ independent principal divisors that generate H'. If the quotient of the volume by the estimate of $\mathrm{vol}(\mathrm{Pic}^0_F)$ computed in Step 1 is less than $1/2$, then $H'=H$ and $\bigl(\bigoplus_{\mathfrak{p}\in\mathcal{B}}\mathbb{Z}\times\bigoplus_\sigma\mathbb{R}\bigr)/H'$ is actually *isomorphic* to Pic^0_F and we are done.

In practice this means that once we have computed somewhat more divisors (f) in H than $\#\mathcal{B}$, we "reduce" the coefficient matrix. From the "reduced" matrix we can read off the structure of the ideal class group as well approximations to the logarithms of the absolute values of a set of units ε that generate the unit group O_F^*. This enables us to compute the regulator R_F.

This completes our description of Buchmann's algorithm. It seems difficult to compute approximations to the numbers $\sigma(\varepsilon)$ themselves from approximations to their absolute values $|\sigma(\varepsilon)|$. If one wants to obtain such approximations, one should apply the algorithm above to the *oriented* Arakelov class group. The computations are the same, but rather than real, one carries complex coordinates x_σ along. More precisely,

$$\widetilde{\mathrm{Pic}}^0_F \;=\; \Bigl(\bigoplus_{\mathfrak{p}\in\mathcal{B}}\mathbb{Z}\times\bigoplus_{\sigma}F_\sigma^*\Bigr)^0\Big/\widetilde{H}$$

for the discrete subgroup $\widetilde{H}$ that consists of elements $f \in F^*$ whose prime factorizations involve only prime ideals $\mathfrak{p} \in \mathcal{B}$. In this way one obtains approximations to $\sigma(\varepsilon_i)$ for a basis ε_i of the unit group O_F^*. In principle, once one has such approximations one may solve the linear system $\sigma(\varepsilon_i) = \sum_j \lambda_{ij}\sigma(\omega_j)$ and compute $\lambda_{ij} \in \mathbb{Z}$ so that $\varepsilon_i = \sum_j \lambda_{ij}\omega_j$ for $1 \le i \le r_1 + r_2 - 1$. However, it is well known that the size of the coefficients λ_{ij} may grow doubly exponentially quickly in $\log|\Delta_F|$ and it is therefore not reasonable to ask for an efficient algorithm that computes a set of generators of the unit group as linear combination of the basis ω_k of the additive group O_F.

What can be done efficiently, is to compute a *compact representation* of a set of generators of the unit group O_F^*. Briefly, this works as follows. Using the notation used in the description of the Jump Algorithm of Section 10, one finds for each fundamental unit ε_j integers m_{ij} such that $\prod_i v_i^{m_{ij}}$ is close to ε_j. The Arakelov divisors (O_F, v_i) are equivalent to reduced divisors $d(f_i^{-1})$. While jumping towards the fundamental unit, one keeps track of the principal ideals that are encountered on the way. For instance, if in the process one computes the sum of the divisors (O_F, v_i) and (O_F, v_j) and reduces the result by means of a shortest vector f, then the result is equivalent to the reduced divisor $d((f f_i f_j)^{-1})$. The size of the elements f_i, f_j and f ... etc. is bounded by $(\log|\Delta_F|)^{O(1)}$. With a good strategy one can jump reasonably close to the unit. The number of jumps we need to reach this point is also bounded by $(\log|\Delta_F|)^{O(1)}$. Using the approximations to the fundamental units and to the vectors f_i, f_j, f ... etc, we can approximate a small element $g \in F^*$, so that the difference between the divisor we jumped to and the fundamental unit is equivalent to a divisor of the form (O_F, g). Since g is small, we can compute it in time bounded by $\log|\Delta_F|^{O(1)}$ from its the approximations of the various $\sigma(g)$. From this we easily obtain the fundamental unit ε_j.

Acknowledgements

I thank the Clay Foundation for financial support during my stay at MSRI in the fall of 2000, Burcu Baran, Hendrik Lenstra, Sean Hallgren and Takao Watanabe for several useful remarks, Silvio Levy for the production of Figure 1 and YoungJu Choie for inviting me to lecture on 'infrastructure' at KIAS in June 2001.

References

[Bayer-Fluckiger 1999] E. Bayer-Fluckiger, "Lattices and number fields", pp. 69–84 in *Algebraic geometry: Hirzebruch 70* (Warsaw, 1998), edited by P. Pragacz et al., Contemp. Math. **241**, Amer. Math. Soc., Providence, RI, 1999.

[Buchmann 1987a] J. Buchmann, "On the computation of units and class numbers by a generalization of Lagrange's algorithm", *J. Number Theory* **26**:1 (1987), 8–30.

[Buchmann 1987b] J. Buchmann, "On the period length of the generalized Lagrange algorithm", *J. Number Theory* **26**:1 (1987), 31–37.

[Buchmann 1987c] J. Buchmann, *Zur Komplexität der Berechnung von Einheiten und Klassenzahlen algebraischer Zahlkörper*, Habilitationsschrift, Univ. Düsseldorf, 1987.

[Buchmann 1990] J. Buchmann, "A subexponential algorithm for the determination of class groups and regulators of algebraic number fields", pp. 27–41 in *Séminaire de Théorie des Nombres* (Paris, 1988–1989), edited by C. Goldstein, Progr. Math. **91**, Birkhäuser, Boston, 1990.

[Buchmann and Düllmann 1991] J. Buchmann and S. Düllmann, "A probabilistic class group and regulator algorithm and its implementation", pp. 53–72 in *Computational number theory* (Debrecen, 1989), edited by A. Pethö et al., de Gruyter, Berlin, 1991.

[Buchmann and Hollinger 1996] J. A. Buchmann and C. S. Hollinger, "On smooth ideals in number fields", *J. Number Theory* **59**:1 (1996), 82–87.

[Buchmann and Williams 1988] J. Buchmann and H. C. Williams, "On the infrastructure of the principal ideal class of an algebraic number field of unit rank one", *Math. Comp.* **50**:182 (1988), 569–579.

[Buchmann and Williams 1989] J. Buchmann and H. C. Williams, "On the computation of the class number of an algebraic number field", *Math. Comp.* **53**:188 (1989), 679–688.

[Cohen 1993] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics **138**, Springer, Berlin, 1993.

[Dobrowolski 1979] E. Dobrowolski, "On a question of Lehmer and the number of irreducible factors of a polynomial", *Acta Arith.* **34**:4 (1979), 391–401.

[Van der Geer and Schoof 2000] G. Van der Geer and R. Schoof, "Effectivity of Arakelov divisors and the theta divisor of a number field", *Selecta Math.* (*N.S.*) **6**:4 (2000), 377–398.

[Groenewegen 2001] R. P. Groenewegen, "An arithmetic analogue of Clifford's theorem", *J. Théor. Nombres Bordeaux* **13**:1 (2001), 143–156.

[Hafner and McCurley 1989] J. L. Hafner and K. S. McCurley, "A rigorous subexponential algorithm for computation of class groups", *J. Amer. Math. Soc.* **2**:4 (1989), 837–850.

[Lenstra 1982] H. W. Lenstra, Jr., "On the calculation of regulators and class numbers of quadratic fields", pp. 123–150 in *Journées Arithmétiques* (Exeter, 1980), edited by J. V. Armitage, London Math. Soc. Lecture Note Ser. **56**, Cambridge Univ. Press, Cambridge, 1982.

[Lenstra 1992] H. W. Lenstra, Jr., "Algorithms in algebraic number theory", *Bull. Amer. Math. Soc.* (*N.S.*) **26**:2 (1992), 211–244.

[Lenstra 2008] H. W. Lenstra, Jr., "Lattices", pp. 127–181 in *Surveys in algorithmic number theory*, edited by J. P. Buhler and P. Stevenhagen, Math. Sci. Res. Inst. Publ. **44**, Cambridge University Press, New York, 2008.

[Lenstra et al. 1982] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, "Factoring polynomials with rational coefficients", *Math. Ann.* **261**:4 (1982), 515–534.

[Marcus 1977] D. A. Marcus, *Number fields*, Springer, New York, 1977.

[Schoof 1982] R. J. Schoof, "Quadratic fields and factorization", pp. 235–286 in *Computational methods in number theory, Part II* (Amsterdam, 1982), edited by H. W. Lenstra, Jr. and R. Tijdeman, Math. Centre Tracts **155**, Math. Centrum, Amsterdam, 1982.

[Shanks 1972] D. Shanks, "The infrastructure of a real quadratic field and its applications", pp. 217–224 in *Proceedings of the Number Theory Conference* (Boulder, CO, 1972), Univ. Colorado, Boulder, 1972.

[Shanks 1976] D. Shanks, "A survey of quadratic, cubic and quartic algebraic number fields (from a computational point of view)", pp. 15–40. Congressus Numerantium, No. XVII in *Proceedings of the Seventh Southeastern Conference on Combinatorics, Graph Theory, and Computing* (Baton Rouge, LA, 1976), edited by F. Hoffman et al., Utilitas Math., Winnipeg, Man., 1976.

[Szpiro 1985] L. Szpiro, "Degrés, intersections, hauteurs", pp. 11–28 in *Séminaire sur les pinceaux arithmétiques: La conjecture de Mordell*, Astérisque **127**, Soc. math. de France, Paris, 1985.

[Szpiro 1987] L. Szpiro, "Présentation de la théorie d'Arakélov", pp. 279–293 in *Current trends in arithmetical algebraic geometry* (Arcata, CA, 1985), edited by K. Ribet, Contemp. Math. **67**, Amer. Math. Soc., Providence, RI, 1987.

[Thiel 1995] C. Thiel, *On the complexity of some problems in algorithmic algebraic number theory*, Ph.D. thesis, Universität des Saarlandes, Saarbrücken, 1995.

[Williams and Shanks 1979] H. C. Williams and D. Shanks, "A note on class-number one in pure cubic fields", *Math. Comp.* **33**:148 (1979), 1317–1320.

[Williams et al. 1983] H. C. Williams, G. W. Dueck, and B. K. Schmid, "A rapid method of evaluating the regulator and class number of a pure cubic field", *Math. Comp.* **41**:163 (1983), 235–286.

RENÉ SCHOOF
DIPARTIMENTO DI MATEMATICA
UNIVERSITÀ DI ROMA 2 "TOR VERGATA"
VIA DELLA RICERCA SCIENTIFICA
I-00133 ROMA
ITALY
schoof@mat.uniroma2.it, schoof@science.uva.nl