MATHEMATICS OF COMPUTATION
Volume 80, Number 276, October 2011, Pages 2325–2357
S 0025-5718(2011)02490-7
Article electronically published on April 26, 2011

THE INFRASTRUCTURE OF A GLOBAL FIELD OF ARBITRARY UNIT RANK

FELIX FONTEIN

Abstract. In this paper, we show a general way to interpret the infrastructure of a global field of arbitrary unit rank. This interpretation generalizes the prior concepts of the giant-step operation and f-representations, and makes it possible to relate the infrastructure to the (Arakelov) divisor class group of the global field. In the case of global function fields, we present results that establish that effective implementation of the presented methods is indeed possible, and we show how Shanks' baby-step giant-step method can be generalized to this situation.

1. Introduction

The infrastructure of a global field, i.e., of a number field or a function field over a finite field, is a group-like algebraic structure. It is a crucial ingredient in the computation of the regulator, a system of fundamental units, and the order and structure of the ideal class group. In the case of a one-dimensional infrastructure, which occurs in fields of unit rank one, this group-like structure was first used by D. Shanks to compute the regulator of a real quadratic number field via a baby-step giant-step algorithm.

In this paper, we present a framework of infrastructure that unifies number fields and function fields. The crucial tool to accomplish this is f-representations; these represent a group well suited for computations into which the infrastructure embeds. Using f-representations, we obtain giant steps, which are an important tool in algorithms of baby-step giant-step type. We establish that f-representations require little storage and lend themselves very well to computation. They can be efficiently used for determining a system of fundamental units of a global function field. We provide evidence for this by presenting preliminary implementation results as well as non-trivial numerical examples.

The idea behind f-representations was described in [Fon08] in the one-dimensional case, i.e., for infrastructures obtained from global fields of unit rank one. The concept of f-representations goes back to (f,p)-representations, which were introduced in the context of cryptography in real quadratic number fields by D. Hühnlein and S. Paulus [HP01] and M. J. Jacobson, Jr., R. Scheidler and H. C. Williams [JSW01].

Received by the editor January 26, 2009 and, in revised form, October 7, 2010.
2010 *Mathematics Subject Classification.* Primary 11Y40; Secondary 14H05, 11R27, 11R65.
Key words and phrases. Infrastructures, giant steps, number fields, function fields, Riemann-Roch spaces, fundamental units.
This work was supported in part by the Swiss National Science Foundation under grant no. 107887.

Infrastructures of number fields and, more recently, of function fields have been studied for some time. Their investigation has its roots in C. F. Gauß' study of the composition of binary quadratic forms, as well as J.-L. Lagrange's continued fraction algorithm. The infrastructure first appeared explicitly in the context of generalizing continued fraction expansion. In his PhD dissertation, G. Voronoĭ found a generalization of continued fraction expansion by minima of lattices and formulated an algorithm to find a system of fundamental units of a cubic number field [DF64].

The set of minima of a global field was studied, for example, in [Ber63, HP87], and was used for computing fundamental units in number fields, for example, in [PZ77, Ste77, AO82, PZ82, PWZ82]. J. A. Buchmann generalized Voronoĭ's algorithm to number fields of unit rank one and two [Buc85]. Subsequently, he presented a generalization of Lagrange's algorithm for computing fundamental units in arbitrary number fields in $\mathcal{O}(R \cdot |\Delta|^{\varepsilon})$ binary operations; here $\varepsilon > 0$ is arbitrary, R is the regulator and Δ the discriminant of the number field [Buc87a]. Note that $R = \mathcal{O}(|\Delta|^{1/2+\varepsilon})$ for any $\varepsilon > 0$.

In 1972, D. Shanks [Sha72] discovered that the principal infrastructure of a real quadratic number field supports a group-like structure. With every element of the principal infrastructure is associated a distance which imposes an ordering on this set. The infrastructure supports two operations: a *baby step*, which proceeds cyclically from one element to the next in this ordering, and a *giant step*, which is akin to multiplication in a cyclic group and under which distances behave almost additively. As a result, the principal infrastructure is almost an abelian group under giant steps that only slightly fails associativity. Using this group-like behavior, Shanks was able to compute the regulator and therefore the absolute value of a fundamental unit of a real quadratic number field in $\mathcal{O}(\sqrt{R})$ steps instead of the $\mathcal{O}(R)$ steps required by the classical algorithm of Lagrange. Note that writing down a system of fundamental units requires $\mathcal{O}(R)$ binary operations, whence no algorithm can compute a system of fundamental units in time faster than $\mathcal{O}(R)$. However, the logarithm of an absolute value of a fundamental unit can be computed faster. Shanks' method was further analyzed and refined by H. W. Lenstra, R. Schoof, H. C. Williams and M. C. Wunderlich in [Len82, Sch82, Wil85, WW87], and finally generalized to all number fields of unit rank one by Buchmann and Williams [BW88].

Shanks' method was first extended to function fields in works of A. Stein and H. G. Zimmer [Ste92, SZ91], Stein and Williams [SW98, SW99] and Scheidler and Stein [SS98, Sch01]. The relationship between the infrastructure in real elliptic and hyperelliptic function fields and the divisor class group in their imaginary counterparts was investigated by Stein in [Ste97], and by S. Paulus and H.-G. Rück in [PR99].

Shanks' discovery of the infrastructure also led to a number of cryptographic applications. The first of these was a Diffie-Hellman-like key exchange protocol described by Buchmann and Williams, and later by Scheidler, Buchmann and Williams in [BW90, SBW94]. This was extended in several ways, and additional encryption and signature schemes were proposed; some of these are described in [BBT94, SSW96, JSW06, JSS07]. The security of these systems is argued to be based on the hardness of computing distances or computing the regulator; the hardness of these problems is analyzed, for example, in [MST99, Jac99, Mau00, Vol03].

All efficient algorithms and cryptosystems based on the infrastructure crucially require the giant-step operation. This raises the question of whether a giant step can be defined and used efficiently in all global fields, not just of unit rank one. In the number field case, Buchmann showed in his habilitation thesis [Buc87b] that there is in fact such a giant step, and that this giant step can be used to compute the absolute values of fundamental units in $\mathcal{O}(\sqrt{R}\cdot|\Delta|^{\varepsilon})$ binary operations. Unfortunately, this algorithm was only published in Buchmann's thesis, which was written in German and is not easily accessible. Later, Schoof presented a modern treatment of the general number field case using Arakelov divisor theory [Sch08]. This is so far the most general treatment of infrastructure. It includes the concept of a giant step, even though Schoof does not give a baby-step giant-step algorithm like Buchmann's. Both Buchmann's and Schoof's giant steps rely on a simple reduction strategy: the infrastructure is in both cases a subset of the set of fractional ideals, whose elements are called "reduced ideals", and the giant step roughly corresponds to multiplying two such ideals. The result is in general not inside this set, but after finding a "short" element in the product and dividing by it, the resulting ideal will lie in this set. This process of chosing the short element is called *reduction*.

In this paper, we present for the first time a unified treatment of number fields and function fields and define infrastructure for any unit rank. Moreover, we provide a connection between the infrastructure and the (Arakelov) divisor class group and relate the arithmetic in these two objects. The key point is a more sophisticated reduction strategy, mimicking the reduction described by F. Heß for arithmetic in the divisor class groups of global function fields [Heß02]. For that, we have to use a slightly different embedding of the reduced ideals into the Arakelov divisor class group than the one used by Schoof. We also do not use the oriented Arakelov divisor class group, but instead an equivalence relation on reduced ideals in case when there is no real embedding of the number field. This allows us to unify arithmetic in the (Arakelov) divisor class group of both number fields and function fields. Moreover, in contrast to Schoof's work, we "parameterize" the Arakelov divisor class group using equivalence classes of reduced divisors together with a finite set of real numbers, and can describe explicit arithmetic using this representation. This parameterization generalizes the aforementioned result by Paulus and Rück [PR99] on hyperelliptic function fields, and, since it extends Heß' approach, it also generalizes known arithmetic in imaginary hyperelliptic and superelliptic function fields [CFA+06, GPS02].

To increase readability of the paper, we moved most proofs to the appendix. All proofs relevant for understanding or constructive proofs which result in algorithms for arithmetic are left in the main body of the paper.

2. Arithmetic in function fields and number fields

Let K be a global field, i.e., either a function field over a finite field of constants k, or an algebraic number field. In the latter case, denote by k^* the roots of unity of K and set $k := k^* \cup \{0\}$.

If K is an algebraic function field, we assume that k is the exact field of constants of K. Let $x \in K$ be transcendental over k.[1] Let $\mathcal{O}_K$ denote the integral closure of $k[x]$ in K and S the set of places of K/k which do not correspond to prime ideals of $\mathcal{O}_K$, i.e., the places of K lying over the infinite place of $k(x)$. Note that for any

[1] Note that we do not assume that $K/k(x)$ is separable.

non-empty finite choice of S, one can find such an x so that S is the set of places lying over the infinite place of $k(x)$. We assume that x and S are fixed throughout this paper. In the number field case, let $\mathcal{O}_K$ denote the integral closure of $\mathbb{Z}$ in K and S the set of all archimedean places of K. In both cases, we denote by $\mathcal{P}_K$ the set of all places of K. If $\mathfrak{p} \in \mathcal{P}_K$ is a non-archimedean place, let $\nu_\mathfrak{p}$ be its normalized discrete valuation, $\mathcal{O}_\mathfrak{p}$ its valuation ring and $\mathfrak{m}_\mathfrak{p}$ its valuation ideal. All places in S are called *infinite*, and all others *finite*. All finite places are non-archimedean.

In the function field case, the group of divisors $\mathrm{Div}(K)$ is the free abelian group generated by $\mathcal{P}_K$. For a divisor $D = \sum_{\mathfrak{p}\in\mathcal{P}_K} n_\mathfrak{p}\mathfrak{p}$, the degree is defined as $\deg D := \sum_{\mathfrak{p}\in\mathcal{P}_K} n_\mathfrak{p} \deg \mathfrak{p}$. The divisors of degree zero form a subgroup of $\mathrm{Div}(K)$, denoted by $\mathrm{Div}^0(K)$. For an element $f \in K^*$, the principal divisor of f is defined by $(f) := \sum_{\mathfrak{p}\in\mathcal{P}_K} \nu_\mathfrak{p}(f)\mathfrak{p} \in \mathrm{Div}^0(K)$; the set of all such divisors forms the group $\mathrm{Princ}(K)$, and the quotient group $\mathrm{Pic}^0(K) := \mathrm{Div}^0(K)/\mathrm{Princ}(K)$ is called the (degree zero) divisor class group of K. Moreover, we have the quotient $\mathrm{Pic}(K) := \mathrm{Div}(K)/\mathrm{Princ}(K)$ together with the exact sequence $0 \longrightarrow \mathrm{Pic}^0(K) \longrightarrow \mathrm{Pic}(K) \xrightarrow{\deg} \mathbb{Z}$. Note that the last map (after restricting the codomain to the image) splits across this exact sequence, whence we have $\mathrm{Pic}(K) \cong \mathrm{Pic}^0(K) \times \mathbb{Z}$.

In the number field case, the group of divisors $\mathrm{Div}(K)$ is the direct product of the free abelian group generated by all places outside S and the abelian group $\mathbb{R}^S$ of all tuples $(n_\mathfrak{p})_{\mathfrak{p}\in S}$ of real numbers with pointwise addition. We write elements $(n_\mathfrak{p})_{\mathfrak{p}\in S} \in \mathbb{R}^S$ additively as $\sum_{\mathfrak{p}\in S} n_\mathfrak{p}\mathfrak{p}$. For $\mathfrak{p} \in S$, let $\sigma : K \to \mathbb{C}$ be a corresponding embedding; define $\deg \mathfrak{p} := 1$ if $\sigma(K) \subseteq \mathbb{R}$ and $\deg \mathfrak{p} := 2$ elsewhere. Also define $\nu_\mathfrak{p}(f) := -\log|\sigma(f)|$ for any $f \in K^*$. If $\mathfrak{p}$ is a finite place, i.e., $\mathfrak{p} \notin S$, define $\deg \mathfrak{p} := \log|\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p}|$. Here, log denotes the natural logarithm. The definition of the degree of a divisor and of a principal divisor is analogous to the function field case, as is the definition of $\mathrm{Pic}^0(K)$ and $\mathrm{Pic}(K)$, and we get $\mathrm{Pic}(K) \cong \mathrm{Pic}^0(K) \times \mathbb{R}$ in the same way as above.

If $D = \sum_{\mathfrak{p}\in\mathcal{P}_K} n_\mathfrak{p}\mathfrak{p}$ is a divisor, the places $\mathfrak{p} \in \mathcal{P}_K$ with $n_\mathfrak{p} \neq 0$ form the *support* of D. If K is a global function field, let $q = |k| < \infty$. For non-global function fields, let $q > 1$ be arbitrary. For number fields, let $q = e = \exp(1)$. Then define the absolute value with respect to a place $\mathfrak{p} \in \mathcal{P}_K$ by $|f|_\mathfrak{p} := q^{-\nu_\mathfrak{p}(f)\deg\mathfrak{p}}$ for $f \in K^*$ and $|0|_\mathfrak{p} := 0$. The fact that principal divisors have degree zero translates to the product formula $\prod_{\mathfrak{p}\in\mathcal{P}_K} |f|_\mathfrak{p} = 1$ for $f \in K^*$.

In both number fields and function fields, a finitely generated $\mathcal{O}_K$-submodule of K is called a fractional ideal. Throughout this paper, we will often say "ideal" when we mean "non-zero fractional ideal". The set of non-zero fractional ideals $\mathrm{Id}(\mathcal{O}_K)$ forms a free abelian group under multiplication, with the set of non-zero prime ideals of $\mathcal{O}_K$ as a basis. These prime ideals correspond to the places of K outside S: if $\mathfrak{p}$ is such a place, $\mathfrak{m}_\mathfrak{p} \cap \mathcal{O}_K$ is the corresponding prime ideal of $\mathcal{O}_K$. Moreover, we have a natural homomorphism $\mathrm{Div}(K) \to \mathrm{Id}(\mathcal{O}_K)$ defined by $\sum n_\mathfrak{p}\mathfrak{p} \mapsto \prod_{\mathfrak{p}\notin S}(\mathfrak{m}_\mathfrak{p} \cap \mathcal{O}_K)^{-n_\mathfrak{p}}$. This homomorphism extends to a map $\mathrm{Pic}^0(K) \to \mathrm{Pic}(\mathcal{O}_K)$, where $\mathrm{Pic}(\mathcal{O}_K) := \mathrm{Id}(\mathcal{O}_K)/\mathrm{Princ}(\mathcal{O}_K)$ is the ideal class group of $\mathcal{O}_K$, i.e., the quotient of $\mathrm{Id}(\mathcal{O}_K)$ with the subgroup $\mathrm{Princ}(\mathcal{O}_K) = \{\frac{1}{f}\mathcal{O}_K \mid f \in K^*\}$ of non-zero principal fractional ideals.

Note that forming principal divisors or principal ideals give homomorphisms $K^* \to \mathrm{Princ}(K) \subseteq \mathrm{Div}^0(K)$, $f \mapsto (f)$ and $K^* \to \mathrm{Princ}(\mathcal{O}_K) \subseteq \mathrm{Id}(\mathcal{O}_K)$, $f \mapsto \frac{1}{f}\mathcal{O}_K$.

Finally, denote by $\mathrm{Div}^0_\infty(K)$ the set of divisors in $\mathrm{Div}^0(K)$ that are only supported at places in S. All the aforementioned maps give rise to the following commuting diagram with exact rows and columns:

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & \mathcal{O}_K^*/k^* & \longrightarrow & \mathrm{Div}^0_\infty(K) & \longrightarrow & T & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K^*/k^* & \longrightarrow & \mathrm{Div}^0(K) & \longrightarrow & \mathrm{Pic}^0(K) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & K^*/\mathcal{O}_K^* & \longrightarrow & \mathrm{Id}(\mathcal{O}_K) & \longrightarrow & \mathrm{Pic}(\mathcal{O}_K) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & H & \xrightarrow{\cong} & H' & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 0 & & 0 & &
\end{array}$$

Here, T, H and H' are suitable groups that are discussed in more detail below.

If K is a number field, $\mathrm{Div}^0_\infty(K) \cong \mathbb{R}^{|S|-1}$, the image of $\mathcal{O}_K^*/k^*$ is a lattice of full rank in $\mathbb{R}^{|S|-1}$ and hence T is an $(|S|-1)$-dimensional torus. Moreover, $H = 0$ and $H' = 0$. If K is a function field, then $\mathrm{Div}^0_\infty(K) \cong \mathbb{Z}^{|S|-1}$. If k is finite, then T is finite by an analogue of Dirichlet's Unit Theorem [Ros02, p. 243, Proposition 14.2]. In case k is infinite, T can be finite or infinite, and both possibilities occur; see [HP87, Section 4] for examples with $k = \mathbb{Q}$. We have $H = 0 = H'$ if and only if $(\deg \mathfrak{p} \mid \mathfrak{p} \in S) = (\deg \mathfrak{p} \mid \mathfrak{p} \in \mathcal{P}_K)$, as $H \cong (\deg \mathfrak{p} \mid \mathfrak{p} \in \mathcal{P}_K)/(\deg \mathfrak{p} \mid \mathfrak{p} \in S)$. Here, $(\deg \mathfrak{p} \mid \mathfrak{p} \in S)$ is the ideal in $\mathbb{Z}$ generated by $\{\deg \mathfrak{p} \mid \mathfrak{p} \in S\}$; $(\deg \mathfrak{p} \mid \mathfrak{p} \in S)$ is defined analogously.

For both number fields and function fields, the rank of $\mathcal{O}_K^*/k^*$ is called the *unit rank* of K. In case K is a number field or T is finite, the rank equals $|S|-1$. Note that we assumed x to be fixed in the function field case. If the unit rank equals $n = |S| - 1$, let $\mathfrak{p}_1, \ldots, \mathfrak{p}_n \in S$ be n distinct places, and $\varepsilon_1, \ldots, \varepsilon_n$ a system of fundamental units of $\mathcal{O}_K$, i.e., a set of units whose residue classes in $\mathcal{O}_K^*/k^*$ are a basis of $\mathcal{O}_K^*/k^*$. Define

$$R := \left| \det\Big(\nu_{\mathfrak{p}_i}(\varepsilon_j) \deg \mathfrak{p}_i \Big)_{1 \le i,j \le n} \right| \in \mathbb{R}_{\ge 0};$$

this number is the *regulator* of K (after fixing x in the function field case) and is independent of the choice of the $\mathfrak{p}_i$ and of the choice of the ε_j.

3. One-dimensional infrastructures

A one-dimensional infrastructure can be interpreted as a circle with a finite set of points on it. This interpretation goes back to Lenstra's work in [Len82]. See also [Fon08] for an earlier treatment of (abstract) one-dimensional infrastructures.

Definition 3.1. A *one-dimensional infrastructure* (X, d) of *circumference* $R > 0$ is a finite set $X \neq \emptyset$ together with an injective map $d : X \to \mathbb{R}/R\mathbb{Z}$.

This can be visualized as follows; see also Figure 1(a). One can interpret $\mathbb{R}/R\mathbb{Z}$ as a circle of circumference R, with a fixed point $0 \in \mathbb{R}/R\mathbb{Z}$. Then $d(X)$ is a finite set of points on this circle, and for every $x \in X$, the residue class $d(x)$ can be interpreted as the *distance* of the point $d(x)$ on the circle to 0.

The infrastructure essentially offers two operations:

- *baby steps*: given $x \in X$, the baby step $\mathrm{bs}(x)$ denotes the preimage of the element in $d(X)$ on the circle "following" $d(x)$;
- *giant steps*: given $x, y \in X$, the giant step $\mathrm{gs}(x, y)$ denotes the preimage of the element in $d(X)$ on the circle "before" $d(x) + d(y)$.

We want to make this more precise. If $|X| = 1$, there is only one way to define $\mathrm{bs} : X \to X$ and $\mathrm{gs} : X \times X \to X$ by $\mathrm{bs}(x) = x$, $\mathrm{gs}(x, x) = x$ if $X = \{x\}$. If $|X| > 1$, then we can define these two maps as follows.

For $s = a + R\mathbb{Z}$ and $t = b + R\mathbb{Z}$ with $a \leq b < a + R$, we denote by $[s, t]$ the set $\{x + R\mathbb{Z} \mid a \leq x \leq b\}$. If we interpret $\mathbb{R}/R\mathbb{Z}$ as a circle, $[s, t]$ will be the circle segment starting at s and ending at t in positive direction. See also Figure 1(b).

Then for $x \in X$, we can define $\mathrm{bs}(x)$ as the unique element of $X \setminus \{x\}$ satisfying

$$\{d(x), d(\mathrm{bs}(x))\} = d(X) \cap [d(x), d(\mathrm{bs}(x))],$$

i.e., the only two points in $d(X)$ lying on the circle segment $[d(x), d(\mathrm{bs}(x))]$ are $d(x)$ and $d(\mathrm{bs}(x))$; see Figure 1(c). For $x, y \in X$, we can define $\mathrm{gs}(x, y)$ as the unique element of X satisfying

$$\{d(\mathrm{gs}(x, y))\} = d(X) \cap [d(\mathrm{gs}(x, y)), d(x) + d(y)],$$

i.e., the only point in $d(X)$ lying on the circle segment $[d(\mathrm{gs}(x, y)), d(x) + d(y)]$ is $d(\mathrm{gs}(x, y))$; see Figure 1(d).

The simplest example of one-dimensional infrastructures, which is nevertheless important, is given by finite cyclic groups:

Example 3.2. Let $G = \langle g \rangle$ be a finite cyclic group of order R. Then we have a canonical isomorphism $\varphi : \mathbb{Z}/R\mathbb{Z} \to G$, $n \mapsto g^n$. Concatenating its inverse with the inclusion $\mathbb{Z}/R\mathbb{Z} \subset \mathbb{R}/R\mathbb{Z}$, we obtain an injective map $d : G \to \mathbb{R}/R\mathbb{Z}$, making (G, d) a one-dimensional infrastructure. This map is the *discrete logarithm* map with base g, i.e., it satisfies $g^{d(h)} = h$ for every $h \in G$.

Let $h \in G$ and $d(h) = n + R\mathbb{Z}$. Then for $h' = g^{n'}$ with $n \leq n' < n + R$, we have $[d(h), d(h')] \cap d(X) = \{d(g^n), d(g^{n+1}), \ldots, d(g^{n'-1}), d(g^{n'})\}$. This shows that if this set contains exactly two elements, then $n' = n + 1$. But this translates to $\mathrm{bs}(h) = gh$, so baby steps on G are simply multiplication by the generator g of G.

Similarly, if $h = g^n$ and $h' = g^{n'}$, we see that $d(X) \cap [d(g^m), d(h) + d(h')] = \{d(g^m), d(g^{m+1}), \ldots, d(g^{n+n'-1}), d(g^{n+n'})\}$ if $m \leq n + n' < m + R$. This shows that $\mathrm{gs}(h, h') = g^{n+n'} = hh'$, so giant steps on G amount to group multiplication.

In this paper, we will concentrate on giant steps as they are needed to obtain algorithms of square root type, which compute the absolute values of a system of

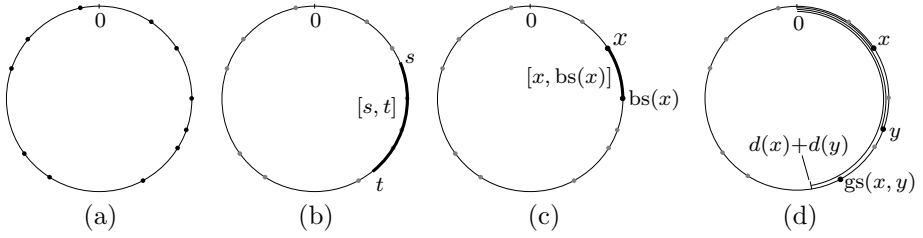

FIGURE 1. Illustrating a one-dimensional infrastructure using a circle

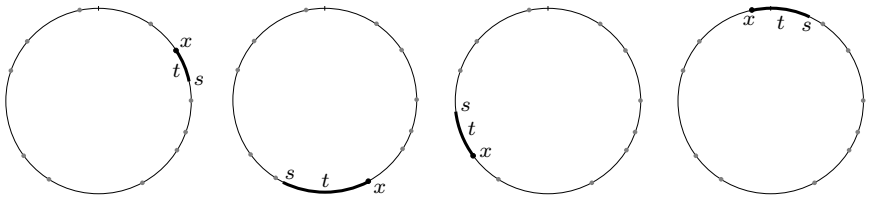

FIGURE 2. Illustrating f-representations in a one-dimensional infrastructure

fundamental units in $\mathcal{O}(\sqrt{R})$ infrastructure operations, where R is the regulator of the field.

The giant step is a binary operation on the finite set X which is not necessarily associative. For certain applications, such as using the infrastructure in cryptography, one is interested in having associative operations: the Diffie-Hellman key exchange protocol depends on the fact that $(x^a)^b = (x^b)^a$ for all $a, b \in \mathbb{N}$. More precisely, it is not obvious how to define x^a without having an associative operation.

In the infrastructure case, one could define x^a as an element $y \in X$ such that $a \cdot d(x) \approx d(y)$; but then it is not necessarily true that $(x^a)^b$ is equal to $(x^b)^a$. One only knows that $d((x^a)^b) \approx a \cdot b \cdot d(x) \approx d((x^b)^a)$, but the error here can be up to a or b times larger than in $a \cdot d(x) \approx d(y)$. In Example 3.2 above, where we start with a finite cyclic group G, this error is always 0 since G is of course associative, and we recover the original Diffie-Hellman key exchange protocol, whose security is based on the fact that computing the map $d : G \to \mathbb{R}/R\mathbb{Z}$ is hard for random elements of G.

Note that while the giant-step operation is in general not associative, it is *almost* associative: it is so up to a "small error", which can be bounded by $d_{\max} := \max\{d(\mathrm{bs}(x)) - d(x) \mid x \in X\}$, where we identify $d(\mathrm{bs}(x)) - d(x)$ with the smallest non-negative real number lying in the residue class modulo R. Namely, we have

$$d(\mathrm{gs}(x, y)) = d(x) + d(y) - \varepsilon_{x,y} \qquad \text{with } 0 \le \varepsilon_{x,y} < d_{\max}.$$

In terms of Figure 1, $d_{\max}$ is the maximal distance between two adjacent points on the circle. In Example 3.2 above, we have $d_{\max} = 1$, even though the error $\varepsilon_{x,y}$ will always be zero.

One can ask whether this gap towards an associative operation can be closed. One solution is to embed infrastructures into groups. Obviously, $\mathbb{R}/R\mathbb{Z}$ is a group under addition. Unfortunately, as seen in Example 3.2, the embedding d is in general not very helpful, since it is often hard to evaluate; in the example, evaluating it is equivalent to compute a discrete logarithm, which, depending on the group G, can be a hard problem; see for example [CFA+06]. We want a group suitable for effective computations, into which X embeds by an easily computable embedding. In order to achieve that, we require f-representations:

Definition 3.3. An element $(x, t) \in X \times \mathbb{R}$ is called an *f-representation* if $0 \le t < R$ and

$$\{d(x)\} = [d(x), d(x) + t] \cap d(X).$$

Denote the set of all f-representations by $\mathrm{Rep}^f(X, d)$.

The f-representation (x, t) *represents* the element $s := d(x) + t \in \mathbb{R}/R\mathbb{Z}$. The condition on t implies that t is minimal for such a representation: it is the smallest

distance from the point $s = d(x) + t$ on the circle backwards to a point in $d(X)$ (namely $d(x)$). In other words, t is small enough that no image under d of any element in $X \setminus \{x\}$ lies in the circle segment $[d(x), d(x) + t]$. The simplest f-representations are the ones of the form $(x, 0)$, where $x \in X$; this shows that we can embed X into $\mathrm{Rep}^f(X, d)$ by $x \mapsto (x, 0)$.

In Example 3.2, we have $\mathrm{Rep}^f(G, d) = G \times [0, 1)$. Moreover, the f-representations of various elements of the example in Figure 1 are shown in Figure 2.

We obtain the following result which shows that the set of f-representations can be identified with the group $(\mathbb{R}/R\mathbb{Z}, +)$.

Proposition 3.4. *The map*

$$\hat{d} : \mathrm{Rep}^f(X, d) \to \mathbb{R}/R\mathbb{Z}, \qquad (x, t) \mapsto d(x) + t$$

is a bijection. □

This allows us to pull the group operation of $\mathbb{R}/R\mathbb{Z}$ back to the set $\mathrm{Rep}^f(X, d)$, giving an operation $+$ on $\mathrm{Rep}^f(X, d)$ by $(x, t) + (x', t') := \hat{d}^{-1}(\hat{d}(x, t) + \hat{d}(x', t'))$. The following remark describes an algorithm which computes the group operation on $\mathrm{Rep}^f(X, d)$ using baby and giant steps.

Remark 3.5. For $(x, t), (x', t') \in \mathrm{Rep}^f(X, d)$, consider

$$(x'', t'') := (\mathrm{gs}(x, x'), t + t' + (d(x) + d(x') - d(\mathrm{gs}(x, x')))) \in X \times \mathbb{R};$$

this ensures that $d(x'') + t'' = \hat{d}(x, t) + \hat{d}(x', t')$. In general, $(x'', t'') \notin \mathrm{Rep}^f(X, d)$, but $t'' \geq 0$ is not too big; more precisely, $t'' < 3d_{\max}$. The idea of the algorithm for realizing the group operation on $\mathrm{Rep}^f(X, d)$ is to decrease t'' using baby steps, while preserving the invariant $d(x'') + t'' = \hat{d}(x, t) + \hat{d}(x', t')$, until $(x'', t'') \in \mathrm{Rep}^f(X, d)$.

For that, note that for $t'' \geq 0$, we have $(x'', t'') \in \mathrm{Rep}^f(X, d)$ if and only if $t'' < d(\mathrm{bs}(x'')) - d(x'')$, i.e., if t'' is smaller than the distance from x to $\mathrm{bs}(x)$. Hence, we iteratively replace (x'', t'') by $(\mathrm{bs}(x''), t'' - (d(\mathrm{bs}(x'')) - d(x'')))$ as long as $t'' \geq 0$ is satisfied.

The smallest non-negative t'' yields $(x'', t'') \in \mathrm{Rep}^f(X, d)$ with $\hat{d}(x'', t'') = \hat{d}(x, t) + \hat{d}(x', t')$, and therefore (x'', t'') is the sum of (x, t) and (x', t') in $\mathrm{Rep}^f(X, d)$.

Finally, if we define $d_{\min} := \min\{d(\mathrm{bs}(x)) - d(x) \mid x \in X\}$, we see that this process requires at most $\frac{3d_{\max}}{d_{\min}}$ baby-step computations and one giant-step computation.

The algorithm first uses giant steps to compute a pair $(x'', t'') \in X \times \mathbb{R}$ with $d(x'') + t'' = \hat{d}(x, t) + \hat{d}(x', t')$, where t'' is "small", and then "reduces" (x'', t'') to an element of $\mathrm{Rep}^f(X, d)$. To make this more precise, we need to introduce a *reduction map* $\mathrm{red}_{(X,d)} : \mathbb{R}/R\mathbb{Z} \to X$. For a point s on the circle $\mathbb{R}/R\mathbb{Z}$, we want $\mathrm{red}_{(X,d)}(s)$ to be the preimage of the element in $d(X)$ "before" s. More precisely, we want $\mathrm{red}_{(X,d)}(s)$ to be the unique element in X such that

$$\{d(\mathrm{red}_{(X,d)}(s))\} = d(X) \cap [d(\mathrm{red}_{(X,d)}(s)), s],$$

i.e., $d(\mathrm{red}_{(X,d)}(s))$ is the only point in $d(X)$ lying on the circle segment $[d(\mathrm{red}_{(X,d)}(s)),\ s]$. Hence, $\mathrm{red}_{(X,d)}$ assigns to each $s \in \mathbb{R}/R\mathbb{Z}$ some $x \in X$ such that $d(x) \approx s$, and satisfies $\mathrm{red}_{(X,d)}(d(x)) = x$. The algorithm in Remark 3.5 computes $\mathrm{red}(d(x'') + t'')$ for $t'' \geq 0$; one can easily adjust it to work for $t'' < 0$ as well.

If one compares the definition of $\mathrm{red}_{(X,d)}$ to Figure 2, one quickly sees that if $(x,t) \in \mathrm{Rep}^f(X,d)$ represents s, i.e., if $d(x)+t=s$, then $\mathrm{red}_{(X,d)}(s)=x$. Hence, if $\pi : X \times \mathbb{R} \to X$ denotes the projection onto the first component, we see that

$$\mathrm{red}_{(X,d)}(s) = \pi_1(\hat{d}^{-1}(s)).$$

In the context of Example 3.2, where we obtained a one-dimensional infrastructure (G,d) from a finite cyclic group $G=\langle g\rangle$, we see that $\mathrm{red}(s+R\mathbb{Z}) = g^{\lfloor s \rfloor}$ for $s \in \mathbb{R}$. This directly follows from the fact that $\mathrm{Rep}^f(G,d) = G \times [0,1)$.

Moreover, one can see that the reduction map $\mathrm{red}_{(X,d)}$ can be used to define $\mathrm{Rep}^f(X,d)$ and giant steps, as

$$\begin{aligned} \mathrm{Rep}^f(X,d) &= \{(x,t) \in X \times \mathbb{R} \mid \mathrm{red}_{(X,d)}(d(x)+t) = x\} \\ \text{and} \qquad \mathrm{gs}(x,y) &= \mathrm{red}_{(X,d)}(d(x)+d(y)) \qquad \text{for all } x,y \in X. \end{aligned}$$

It is obvious that our choice of $\mathrm{red}_{(X,d)}$ is not the only one possible. One could choose $\mathrm{red}_{(X,d)}$ such that $d(\mathrm{red}_{(X,d)}(s))$ is closest to s, with a rule to break ties; such a reduction map is, for example, used in [GHM08] in the case of infrastructures obtained from real quadratic function fields. The advantage of such a reduction map is that it reduces the number of baby steps in Remark 3.5 to at most $\frac{3d_{\max}}{2d_{\min}}$. Using a different reduction map would result in different f-representations and possibly also different giant steps. We will investigate this relationship between reduction maps and f-representations in more detail in the next section.

An interesting question is where and how infrastructures occur in practice. The first known non-associative instance was the infrastructure of a real quadratic number field, which was discovered in 1972 by Shanks. It was originally described in terms of binary quadratic forms, but an alternative and more accessible description uses ideals; see, for example, [Wil85]. We will use the language of ideals since it is available in all number fields and function fields. See Section 5 on how the infrastructure can be realized in detail; for the moment, we want to give a simpler example: the infrastructure of a real quadratic number field.

Example 3.6 (compare [Wil85])**.** Let $K=\mathbb{Q}(\sqrt{D})$ be a real quadratic number field, where $D>1$ is a squarefree integer. Note that there are two embeddings $K \to \mathbb{R}$, one is the identity, and the other one maps $\sqrt{D}$ to $-\sqrt{D}$. Denote the first embedding by σ_1 and the second one by σ_2; then we have $S=\{\mathfrak{p}_1,\mathfrak{p}_2\}$ with $|h|_{\mathfrak{p}_i} = |\sigma_i(h)|$ for $h \in K$.

We say that a fractional ideal $\mathfrak{a} \in \mathrm{Id}(\mathcal{O}_K)$ is *reduced* if $1 \in \mathfrak{a}$, and for every $\mu \in \mathfrak{a}$ satisfying $|\mu|_1 \le 1$ and $|\mu|_2 \le 1$ we have $\mu \in \{-1,0,1\}$. Using the Minkowski embedding $\Phi : K \to K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^2$, given by $h \mapsto (\sigma_1(h),\sigma_2(h))$, we can visualize $\mathfrak{a}$ as a lattice $\Phi(\mathfrak{a})$ of rank two in $\mathbb{R}^2$. The condition that $\mathfrak{a}$ is reduced is equivalent to the property that the square $[-1,1]^2$ contains exactly the three points $(-1,-1)$, $(0,0)$ and $(1,1)$ of $\Phi(\mathfrak{a})$. The unit ideal $\mathcal{O}_K$ is always reduced. See Figure 3 for an example.

Let $\varepsilon \in \mathcal{O}_K$ be the fundamental unit with $\varepsilon > 1$. We have $\mathcal{O}_K^* = \{\pm\varepsilon^n \mid n \in \mathbb{Z}\}$. Set $R := \log \varepsilon$; then R is the regulator of K. If $\mathfrak{a} = \frac{1}{\mu}\mathcal{O}_K$ is a reduced fractional ideal, the elements in $\mu\mathcal{O}_K^*$ are exactly the elements μ' such that $\mathfrak{a} = \frac{1}{\mu'}\mathcal{O}_K$, whence $\{-\log|\mu'| \mid \mathfrak{a} = \frac{1}{\mu'}\mathcal{O}_K\} = -\log|\mu| + R\mathbb{Z}$. Define $d(\frac{1}{\mu}\mathcal{O}_K) := -\log|\mu| + R\mathbb{Z}$; then d is a map from the set X of reduced principal ideals to $\mathbb{R}/R\mathbb{Z}$. One can show that

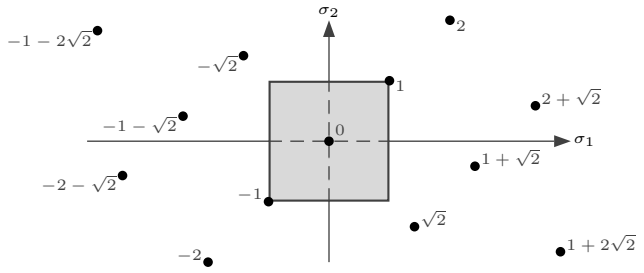

FIGURE 3. The Minkowski embedding (σ_1, σ_2) of $\mathcal{O}_K$ in the real quadratic number field $K = \mathbb{Q}(\sqrt{2})$. The grey square is $[-1, 1]^2$.

X is finite and that d is injective.[2] Then (X, d) is a one-dimensional infrastructure: in fact, this is the infrastructure used by Shanks in [Sha72], translated into the language of ideals.

Computation of baby steps and giant steps is done by continued fraction expansion. Let $\mathfrak{a}$ be a principal fractional ideal with $\mathfrak{a} \cap \mathbb{Q} = \mathbb{Z}$; any reduced ideal satisfies this. We can then write $\mathfrak{a} = \mathbb{Z} \oplus \phi\mathbb{Z}$ with $\phi = (P + \sqrt{D})/Q$, and compute the continued fraction expansion of $\phi = \phi_0$. If ϕ_i is the i-th complete quotient, we can write $\phi_i = (P_i + \sqrt{D})/Q_i$ with $P_i, Q_i \in \mathbb{Z}$, and it turns out that $\mathfrak{a}_i := \mathbb{Z} \oplus \phi_i\mathbb{Z}$ is a principal fractional ideal. There exists some $i_0 \in \mathbb{N}$, depending on $\mathfrak{a}$, such that for all $i \geq i_0$, $\mathfrak{a}_i$ is reduced. In fact, $\{\mathfrak{a}_i \mid i \geq i_0\}$ is the set of *all* reduced principal ideals X. If $\mathfrak{a}_i$ is reduced, $\mathrm{bs}(\mathfrak{a}_i) = \mathfrak{a}_{i+1}$. Moreover, if one defines $\mathrm{red}(\mathfrak{a}) = \mathfrak{a}_n$ if $n \geq 0$ is chosen minimal under the condition that $\mathfrak{a}_n$ is reduced, then $\mathrm{gs}(\mathfrak{a}_i, \mathfrak{a}_j) = \mathrm{red}(\mathfrak{a}_i\mathfrak{a}_j)$ is the giant-step operation used by Shanks in [Sha72].

One can use this to define a reduction map on a dense subset of $\mathbb{R}/R\mathbb{Z}$. For that, note that the map $\Psi : \mathrm{PId}(K) \to \mathbb{R}/R\mathbb{Z}$, $\frac{1}{\mu}\mathcal{O}_K \mapsto -\log|\mu| + R\mathbb{Z}$ is injective as argued in footnote 2. The set $\Psi(\mathrm{PId}(K))$ is a dense subgroup of $\mathbb{R}/R\mathbb{Z}$, and if $s \in \mathbb{R}/R\mathbb{Z}$ lies in the image of Ψ, one can define $\mathrm{red}(s) := \mathrm{red}(\Psi^{-1}(s))$. This was in fact done by Lenstra in [Len82], and Lenstra called the image of Ψ a "circular group" since it is a dense subset of the circle $\mathbb{R}/R\mathbb{Z}$. (Note that Lenstra uses a distance map that is different from the one introduced by Shanks.)

4. n-Dimensional infrastructures

In this section, we want to define an abstract n-dimensional infrastructure. We want this definition to share most properties of one-dimensional infrastructures. Unfortunately, it is not as clear as in the one-dimensional case how baby steps, giant steps and f-representations can be defined. We will see that as outlined in the discussion of the one-dimensional case in the previous section, f-representations and reduction maps are equivalent, and both yield giant steps. As a consequence of the additional freedom gained in the n-dimensional case, we are forced to include more information on the infrastructure in the definition, namely a reduction map.

[2]This is a special case of Proposition 5.5 with $X = \mathrm{Red}(\mathcal{O}_K)$ and $d = d^{\mathcal{O}_K}$, when we identify an equivalence class $[\mathfrak{a}]_\sim$ with $\mathfrak{a}$, since by Corollary 5.3 every class contains exactly one ideal. In this special case, at least the injectivity of d is rather obvious, since $h \mapsto \log|h|$ is a group homomorphism $(K^*, \cdot) \to (\mathbb{R}, +)$ with kernel $\{-1, 1\} = k^* \subseteq \mathcal{O}_K^*$.

Note that we will ignore baby steps for the rest of this paper. For n-dimensional infrastructures obtained from global fields one can define $n+1$ baby-step functions; see, for example, [Buc85], [LSY03] or [Fon09, Section 3.5]. These definitions come from the relation of the infrastructure to the set of minima of an ideal, but there is no reason an abstract n-dimensional infrastructure arises from such a structure. Moreover, such baby steps do not always behave as expected, as it might happen that certain minima cannot be reached by baby steps. So far, it is unknown whether there is a usable definition of baby steps for abstract n-dimensional infrastructures when $n > 1$.

We want to make the definition on an n-dimensional infrastructure slightly more general by allowing to restrict to a suitable subgroup $\mathbb{G}$ of $\mathbb{R}$. For example, for infrastructures obtained from function fields, the natural subgroup to restrict to is $\mathbb{Z}$, since all valuations of a function field are discrete. In the case of Example 3.6, one could restrict to the subgroup $\{\log|\mu| \mid \mu \in K^*\}$; then the function red from the example will no longer be partially defined, and one essentially obtains the group (though not the distance function) of Lenstra [Len82].

Throughout this section, fix a suitable non-zero subgroup $\mathbb{G}$ of $\mathbb{R}$. The similarity to Section 3 is clearer if one assumes $\mathbb{G} = \mathbb{R}$. In the following sections, we will restrict to $\mathbb{G} = \mathbb{Z}$ in the function field case and $\mathbb{G} = \mathbb{R}$ in the number field case.

The natural analogue to a circle $\mathbb{R}/R\mathbb{Z}$ in n dimensions is an n-dimensional *torus* $\mathbb{R}^n/\Lambda$, where Λ is a lattice of full rank. Since we want to restrict to $\mathbb{G}$, we assume that $\Lambda \subseteq \mathbb{G}^n$. Moreover, we abuse terminology by calling $\mathbb{G}^n/\Lambda$ a torus, even though we can in general only embed it canonically into the torus $\mathbb{R}^n/\Lambda$. Note that both the circle $\mathbb{R}/R\mathbb{Z}$ and the torus $\mathbb{G}^n/\Lambda$ have a fixed point 0.

A natural generalization of a one-dimensional infrastructure would be a finite set $X \neq \emptyset$ together with an injective map $d : X \to \mathbb{G}^n/\Lambda$. Unfortunately, the situation is not as simple as in the one-dimensional case. The problem lies in the definition of f-representations and the giant-step function, not to mention the baby-step function(s). In the one-dimensional case, one has essentially two directions on the circle: one can go clockwise and counterclockwise. In fact, our circle $\mathbb{R}/R\mathbb{Z}$ has a distinguished direction corresponding to the positive direction on the real line. This allows us to define baby steps as going "forward", and we can define giant steps, f-representations and the reduction map by taking an element of $d(X)$ "before" a point on the circle.

As soon as $n > 1$, the torus $\mathbb{G}^n/\Lambda$ has infinitely many directions, none of them more distinguished than others. This gives many more choices for giant steps, f-representations and reduction maps, not to mention baby steps. We will be forced to include a particular choice in the definition of an n-dimensional infrastructure. Before we do that, let us formalize the notions of reduction maps and f-representations and discuss their relationship.

Let X be a non-empty finite set and let $d : X \to \mathbb{G}^n/\Lambda$ be a injective map.

Definition 4.1.

(a) a *reduction map* (for (X, d)) is a map $\mathrm{red} : \mathbb{G}^n/\Lambda \to X$ satisfying $\mathrm{red}(d(x)) = x$ for every $x \in X$;

(b) *f-representations* (for (X, d)) are a subset $\mathrm{Rep}^f \subseteq X \times \mathbb{G}^n$ satisfying $X \times \{0\} \subseteq \mathrm{Rep}^f$ such that the following map is a bijection:

$$\Phi : \mathrm{Rep}^f \to \mathbb{G}^n/\Lambda, \qquad (x, t) \mapsto d(x) + t.$$

If (X, d) is a one-dimensional infrastructure, then the definition of $\mathrm{red}_{(X,d)}$ as in Section 3 yields a reduction map in the sense of (a), and Definition 3.3 and Proposition 3.4 yield f-representations in the sense of (b).

Note that the condition $\mathrm{red}(d(x)) = x$ for reduction maps ensures that the only fixed points under the map $d \circ \mathrm{red} : \mathbb{G}^n/\Lambda \to \mathbb{G}^n/\Lambda$ are the elements in $d(X)$; i.e., these elements can be interpreted as *reduced* elements: other elements of $\mathbb{G}^n/\Lambda$ will be mapped to a reduced element when applying red, while reduced elements are left unchanged under this map.

We begin by outlining the relationship between reduction maps and f-representations in the sense of Definition 4.1. This is analogous to the relationship in the one-dimensional case in Section 3.

If red is a reduction map, then we obtain a set of f-representations by

$$\mathrm{Rep}^f := \{(x, t) \in X \times \mathbb{G}^n \mid \mathrm{red}(d(x) + t) = x\}.$$

Here, we choose pairs (x, t) such that $d(x) + t \in \mathbb{G}^n/\Lambda$ will reduce to x. If red satisfies $d(\mathrm{red}(s)) \approx s$ for all $s \in \mathbb{G}^n/\Lambda$, then the permissible t values in the f-representations will be "small". Moreover, the condition $\mathrm{red}(d(x) + t) = x$ ensures that there is a *unique* f-representation (x, t) for every $s \in \mathbb{G}^n/\Lambda$.

Conversely, if Rep^f is a set of f-representations with induced bijection $\Phi : \mathrm{Rep}^f \to \mathbb{G}^n/\Lambda$, then we get a reduction map by

$$\mathrm{red} : \mathbb{G}^n/\Lambda \to X, \qquad s \mapsto \pi_1(\Phi^{-1}(s)),$$

where $\pi_1 : X \times \mathbb{G}^n \to X$ is the projection onto the first component. This is the direct generalization of the map $\mathrm{red}_{(X,d)}$ in the one-dimensional case: given a point s on the torus $\mathbb{G}^n/\Lambda$, we consider the f-representation $(x, t) = \Phi^{-1}(s)$ representing that point, and return $x = \pi_1(x, t)$.

Therefore, as in the one-dimensional case, the concepts of reduction maps and of f-representations are equivalent. We can continue as in the one-dimensional case and define giant steps using these two notions. If $\mathrm{red} : \mathbb{G}^n/\Lambda \to X$ is a reduction map, we define

$$\mathrm{gs}(x, y) := \mathrm{red}(d(x) + d(y))$$

for all $x, y \in X$; if Rep^f are f-representations with induced bijection $\Phi : \mathrm{Rep}^f \to \mathbb{G}^n/\Lambda$, we define

$$\mathrm{gs}(x, y) := \pi_1(\Phi^{-1}(\Phi(x, 0) + \Phi(y, 0)))$$

for all $x, y \in X$. Both definitions yield the same giant-step operation on X.

This discussion gives rise to the following definition of an abstract n-dimensional infrastructure:

Definition 4.2. Let $\Lambda \subseteq \mathbb{G}^n$ be a lattice of full rank.

(a) An *n-dimensional infrastructure* is a triple (X, d, red), where $X \neq \emptyset$ is a non-empty finite set, $d : X \to \mathbb{G}^n/\Lambda$ an injective map and $\mathrm{red} : \mathbb{G}^n/\Lambda \to X$ a reduction map for (X, d).

(b) If (X, d, red) is an n-dimensional infrastructure, then set

$$\mathrm{Rep}^f(X, d, \mathrm{red}) := \{(x, t) \in X \times \mathbb{G}^n \mid \mathrm{red}(d(x) + t) = x\}$$

and

$$\mathrm{gs}(x, x') := \mathrm{red}(d(x) + d(y)) \qquad \text{for } x, x' \in X.$$

Since $R\mathbb{Z}$ is a lattice in $\mathbb{R}^1$ of full rank, we see that a one-dimensional infrastructure (X, d) in the sense of Definition 3.1 is a 1-dimensional infrastructure $(X, d, \mathrm{red}_{(X,d)})$ in the sense of Definition 4.2, whose giant steps and f-representations coincide. This shows that our new definition is indeed a generalization of the notion of a one-dimensional infrastructure as in Section 3 or [Fon08].

We conclude this section with an example, which shows that n-dimensional infrastructures can be seen as a generalization of finite abelian groups. Recall that Example 3.2 showed how a finite cyclic group can be interpreted as a one-dimensional infrastructure, where the distance map was essentially the discrete logarithm map.

Example 4.3. Assume that $\mathbb{Z} \subseteq \mathbb{G}$. Let $G = \langle g_1, \dots, g_n \rangle$ be a finite abelian group, and let

$$\Lambda := \left\{ (e_1, \dots, e_n) \in \mathbb{Z}^n \;\middle|\; \prod_{i=1}^{n} g_i^{e_i} = 1 \right\}$$

be the relation lattice of $g_1, \dots, g_n$; this is the kernel of the epimorphism $\mathbb{Z}^n \to G$, $(e_1, \dots, e_n) \mapsto \prod_{i=1}^n g_i^{e_i}$, whence $G \cong \mathbb{Z}^n/\Lambda$.

Concatenating the inverse of this isomorphism with the inclusion $\mathbb{Z}^n/\Lambda \subseteq \mathbb{G}^n/\Lambda$, we obtain an injective map $d : G \to \mathbb{G}^n/\Lambda$. This map is the *generalized discrete logarithm* map with base $g := (g_1, \dots, g_n)$, i.e., it satisfies[3] $g^{d(h)} = h$ for every $h \in G$.

It is easy to see that $\mathrm{Rep}^f := G \times (\mathbb{G} \cap [0, 1))^n$ is a set of f-representations for (G, d); the corresponding reduction map maps $s \in \mathbb{G}^n/\Lambda$ to $\mathrm{red}(s) := \prod_{i=1}^n g_i^{\lfloor e_i \rfloor}$, if $s = (e_i)_i + \Lambda$. Therefore, (G, d, red) is an n-dimensional infrastructure. The induced giant-step map is given by

$$\mathrm{gs}(h, h') = \mathrm{red}(d(h) + d(h')) = hh'$$

for $h, h' \in G$, since $d(h) + d(h') = (e_1, \dots, e_n) + \Lambda$ with $e_i \in \mathbb{Z}$ and $g_1^{e_1} \cdots g_n^{e_n} = hh'$.

This shows that giant steps generalize the group operation in this case as well. In particular, in this case, the giant-step operation is associative, as opposed to general n-dimensional infrastructures.

5. Reduced ideals

Now that we have obtained a definition of an abstract n-dimensional infrastructure, we want to construct such an infrastructure from a global field K. The aim of this section is to construct the lattice $\Lambda \subset \mathbb{G}^n$, the finite set X as well as the injective map $d : X \to \mathbb{G}^n/\Lambda$. In the next section, we will add a reduction map red for (X, d) such that (X, d, red) is an n-dimensional infrastructure.

For the rest of the paper, let $\mathbb{G}$ denote $\mathbb{Z}$ if K is a function field and $\mathbb{R}$ if K is a number field.

In order to construct the underlying set X, we require the notion of a reduced (fractional) ideal[4] in analogy to Example 3.6. In case K is a function field, reduced ideals correspond to certain reduced divisors in the sense of [Heß02].

The notion of a reduced ideal is rather geometric. To describe it, we define the notion of a *box*, which is the set of elements of an ideal (interpreted as a lattice) in a bounded area. An ideal will be reduced if a certain box contains elements only

[3] For $g = (g_1, \dots, g_n) \in G^n$ and $v = (v_1, \dots, v_n) \in \mathbb{Z}^n$, define $g^v := \prod_{i=1}^n g_i^{v_i}$.

[4] Recall that we always mean "non-zero fractional ideal" when we write "ideal", if not explicitly said otherwise.

at very specific positions. Write $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_{n+1}\}$, where $n = |S| - 1$; then recall that the absolute value of an element $h \in K$ with respect to a place $\mathfrak{p}$ is defined as $|h|_{\mathfrak{p}} = q^{-\nu_{\mathfrak{p}}(h) \deg \mathfrak{p}}$, where $q > 1$ is a constant.

For $t_1, \dots, t_{n+1} \in \mathbb{G}$ and an ideal $\mathfrak{a} \in \mathrm{Id}(\mathcal{O}_K)$, we define

$$B(\mathfrak{a}, (t_1, \dots, t_{n+1})) := \{h \in \mathfrak{a} \mid \forall i \in \{1, \dots, n+1\} : |h|_{\mathfrak{p}_i} \leq q^{t_i \deg \mathfrak{p}_i}\}.$$

The motivation of this definition comes from the number field case; in that scenario, $\mathfrak{a}$ is a lattice of full rank under the Minkowski embedding $K \hookrightarrow K \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{R}^d$, where $d = [K : \mathbb{Q}]$. The box $B(\mathfrak{a}, (t_1, \dots, t_{n+1}))$ is the set of lattice points lying in the symmetric compact convex set described by $(t_1, \dots, t_{n+1})$. If K is totally real, this convex set is a hyperrectangle (box) with side lengths $2e^{t_1}, \dots, 2e^{t_{n+1}}$, and if K is totally imaginary, this convex set is the direct product of $n+1$ closed discs of radii $e^{t_1}, \dots, e^{t_{n+1}}$. If K is neither totally real nor totally complex, the convex set features both properties; for example, if K has one real embedding corresponding to $\mathfrak{p}_1$ and two complex conjugate embeddings corresponding to $\mathfrak{p}_2$, the convex set is a cylinder of length $2e^{t_1}$ and radius e^{t_2}. Figure 3 displays the box with parameters $t_1 = t_2 = 0$ in the real quadratic number field $K = \mathbb{Q}(\sqrt{2})$ as the grey square in the center.

If $\mu \in K^*$, we define the abbreviation

$$B(\mathfrak{a}, \mu) := B(\mathfrak{a}, (-\nu_{\mathfrak{p}_1}(\mu), \dots, -\nu_{\mathfrak{p}_{n+1}}(\mu))).$$

This is the smallest box which would contain μ if $\mu \in \mathfrak{a}$. With this, we are able to define reduced ideals:

Definition 5.1.

(a) An element $\mu \in \mathfrak{a} \setminus \{0\}$ is said to be a *minimum* of $\mathfrak{a}$ if for every $h \in B(\mathfrak{a}, \mu)$ we either have $h = 0$ or $|h|_{\mathfrak{p}} = |\mu|_{\mathfrak{p}}$ for all $\mathfrak{p} \in S$. Denote the set of all minima of $\mathfrak{a}$ by $\mathcal{E}(\mathfrak{a})$.

(b) An ideal $\mathfrak{a}$ is said to be *reduced* if $1 \in \mathfrak{a}$ is a minimum of $\mathfrak{a}$.

The notation of $\mathcal{E}(\mathfrak{a})$ for the set of minima goes back to Y. Hellegouarch and R. Paysant-Le Roux [HP85].

The property that μ is a minimum of $\mathfrak{a}$ means simply that the box $B(\mathfrak{a}, \mu)$ is empty, up to a few elements which always need to belong to $B(\mathfrak{a}, \mu)$: 0 is always contained in $B(\mathfrak{a}, \mu)$, as well as μ and $\varepsilon\mu$ for all $\varepsilon \in k^*$, since all absolute values of elements in k^* are 1. Hence, we ask that all elements in $B(\mathfrak{a}, \mu)$ are either 0 or have the same infinite absolute values as μ. For example, in Figure 3, 1 and $1 + \sqrt{2}$ are minima of $\mathcal{O}_K$, while $\sqrt{2}$ is not, since $1 \in B(\mathcal{O}_K, \sqrt{2}) \setminus \{0\}$ has different absolute values than $\sqrt{2}$.

Under certain circumstances, there can be elements in $\mathfrak{a}$ with the same infinite absolute values as μ other than $\varepsilon\mu$, $\varepsilon \in k^*$, and these elements thus belong to $B(\mathfrak{a}, \mu)$ as well. These elements are the reason why the aforementioned equivalence relation is needed: if $\mu \in \mathfrak{a}$ is such an element, then $\frac{1}{\mu}\mathfrak{a}$ is a reduced ideal different from $\mathfrak{a}$ which will be mapped to the same element by our distance map. For that reason, we have to identify any two such ideals if such elements can exist.

The following proposition shows that in many important situations, such elements cannot occur. This includes, in particular, the case when an infinite place of degree one exists. For number fields K, this is always the case unless K is totally imaginary, and for function fields one can always move to a constant field extension

by a splitting field for one of the infinite places. Many treatments of the infrastructure and of arithmetic in function fields require such a place of degree one, sometimes explicitly as for Heß' arithmetic [Heß02] and sometimes implicitly by restricting to certain classes of fields; for example, every real quadratic field has exactly two infinite places of degree one, and a cubic number field always has a real embedding.

Proposition 5.2. *Assume that* $\deg \mathfrak{p} = 1$ *for some* $\mathfrak{p} \in S$. *Let* $\mathfrak{b}$ *be a reduced ideal. Then* $B(\mathfrak{b}, (0, \dots, 0)) = k$.

Before we proceed with the proof, we need to introduce a right inverse $\operatorname{div} : \operatorname{Id}(\mathcal{O}_K) \to \operatorname{Div}(K)$ to the natural map $\operatorname{Div}(K) \to \operatorname{Id}(\mathcal{O}_K)$ described in Section 2. For a fractional ideal $\mathfrak{b} = \prod_{\mathfrak{p} \notin S} (\mathfrak{m}_\mathfrak{p} \cap \mathcal{O}_K)^{n_\mathfrak{p}}$, define $\operatorname{div}(\mathfrak{b}) := -\sum_{\mathfrak{p} \notin S} n_\mathfrak{p} \mathfrak{p}$. This allows us to relate boxes to *Riemann-Roch spaces*: we have

$$B(\mathfrak{a}, (t_1, \dots, t_{n+1})) = L\left(\operatorname{div}(\mathfrak{a}) + \sum_{i=1}^{n+1} t_i \mathfrak{p}_i\right);$$

here, $L(D) := \{f \in K^* \mid (f) \geq -D\} \cup \{0\}$ for $D \in \operatorname{Div}(K)$ is the Riemann-Roch space of D.

Proof of Proposition 5.2. If K is a number field, then $\deg \mathfrak{p} = 1$ means that $\mathfrak{p}$ corresponds to a real embedding; hence, $|h|_\mathfrak{p} = |h'|_\mathfrak{p}$ for $h, h' \in K$ if and only if $h = \pm h'$. Thus, if $\mathfrak{b}$ is reduced, $B(\mathfrak{b}, (0, \dots, 0)) = k = \{-1, 0, 1\}$.

If K is a function field, then $B(\mathfrak{b}, (0, \dots, 0)) = L(\operatorname{div}(\mathfrak{b})) \supseteq k$, and $L(\operatorname{div}(\mathfrak{b}) - \mathfrak{p}) = 0$; but by [Sti93, Lemma I.4.8],

$$\begin{aligned} 0 = \dim_k L(\operatorname{div}(\mathfrak{b}) - \mathfrak{p}) &\leq \dim_k L(\operatorname{div}(\mathfrak{b})) \\ &\leq \dim_k L(\operatorname{div}(\mathfrak{b}) - \mathfrak{p}) + \deg \mathfrak{p} = 1, \end{aligned}$$

whence $B(\mathfrak{b}, (0, \dots, 0)) = k$. □

For the rest of the section, we fix an ideal $\mathfrak{a} \in \operatorname{Id}(\mathcal{O}_K)$. There is a close relationship between the set of minima of an ideal and the set of reduced ideals in the ideal class of that ideal. First note that the unit group $\mathcal{O}_K^*$ of $\mathcal{O}_K$ operates on $\mathcal{E}(\mathfrak{a})$ by multiplication: if $\mu \in \mathcal{E}(\mathfrak{a})$ and $\varepsilon \in \mathcal{O}_K^*$, then $\varepsilon\mu \in \mathcal{E}(\mathfrak{a})$. This shows that the map

$$\mathcal{E}(\mathfrak{a})/\mathcal{O}_K^* \to \operatorname{Id}(\mathcal{O}_K), \qquad \mu\mathcal{O}_K^* \mapsto \tfrac{1}{\mu}\mathfrak{a}$$

is well defined and injective. The image of this map is exactly the set of reduced ideals in the ideal class of $\mathfrak{a}$. Denote this set by $\operatorname{Red}(\mathfrak{a})$. This set, modulo the aforementioned equivalence relation, will be our set X.

Note that in case K is a function field with $\deg \mathfrak{p}_i = 1$ for some i, the reduced ideals $\mathfrak{b} \in \operatorname{Red}(K)$, where

$$\operatorname{Red}(K) := \bigcup_{\mathfrak{a} \in \operatorname{Id}(\mathcal{O})} \operatorname{Red}(\mathfrak{a}),$$

correspond exactly to the divisors $D \in \operatorname{Div}(K)$ that are reduced with respect to $\mathfrak{p}_i$ in the sense of Heß [Heß02] and satisfy $\nu_{\mathfrak{p}_j}(D) = 0$ for $j \in \{1, \dots, n+1\}$. This is due to the relationship between boxes and Riemann-Roch spaces sketched above, and the correspondence is given by $\mathfrak{b} \mapsto \operatorname{div}(\mathfrak{b})$.

Next, we want to construct the distance map d. In the process of constructing d, we obtain the lattice Λ and derive the equivalence relation needed to define X. We begin with the map

$$\Psi : K^* \to \mathbb{G}^n, \qquad h \mapsto (-\nu_{\mathfrak{p}_1}(h), \dots, -\nu_{\mathfrak{p}_n}(h)),$$

which maps $(K^*, \cdot)$ homomorphically into $(\mathbb{G}^n, +)$. This map plays a crucial role in constructing the distance map. The image of $\mathcal{O}_K^*$ under Ψ is a lattice in $\mathbb{G}^n \subseteq \mathbb{R}^n$; it is called the *unit lattice* of $\mathcal{O}_K$ and is denoted by Λ. For number fields K, Λ always has full rank; this is a consequence of Dirichlet's Unit Theorem. For function fields, Λ has full rank if and only if T is finite. In case Λ has full rank, we have

$$\det \Lambda = \frac{R}{\prod_{i=1}^{n} \deg \mathfrak{p}_i}.$$

In case $\mathcal{O}_K^*$ has full rank, $\mathbb{G}^n/\Lambda \subseteq \mathbb{R}^n/\Lambda$ is an n-dimensional torus that will be the codomain of our distance map d.

Note that $\frac{1}{h}\mathfrak{a} = \frac{1}{h'}\mathfrak{a}$ if and only if $h'h^{-1} \in \mathcal{O}_K^*$, and this implies $\Psi(h) - \Psi(h') \in \Lambda$. Therefore, the map $\frac{1}{h}\mathfrak{a} \mapsto \Psi(h) + \Lambda$ is well defined. Ideally, this map will represent our distance map. Unfortunately, it is in general not injective on $\mathrm{Red}(\mathfrak{a})$, whence we need to identify elements in $\mathrm{Red}(\mathfrak{a})$ which are mapped onto the same element of $\mathbb{G}^n/\Lambda$ under the map $\frac{1}{h}\mathfrak{a} \mapsto \Psi(h) + \Lambda$. We will define an equivalence relation $\sim$, study it in more detail, and then show in Proposition 5.5 that it indeed makes this map injective.

If $\mathfrak{b}, \mathfrak{b}'$ are ideals in the ideal class of $\mathfrak{a}$ such that $\mathfrak{b} = h\mathfrak{b}'$ with $|h|_{\mathfrak{p}} = 1$ for all $\mathfrak{p} \in S$, then $\mathfrak{b}$ and $\mathfrak{b}'$ are mapped to the same element of $\mathbb{G}^n/\Lambda$. Hence, we can define the equivalence relation $\sim$ on $\mathrm{Id}(\mathcal{O}_K)$ by

$$\mathfrak{b} \sim \mathfrak{b}' :\iff \exists h \in K^* : \mathfrak{b} = h\mathfrak{b}' \wedge \forall \mathfrak{p} \in S : |h|_{\mathfrak{p}} = 1.$$

We thus see that the map $\mathrm{Red}(\mathfrak{a})/_\sim \to \mathbb{G}^n/\Lambda$ via $[\frac{1}{\mu}\mathfrak{a}]_\sim \mapsto \Psi(h) + \Lambda$ is well defined, but we are left to show that it is injective. Note that the above equivalence relation $\sim$ is *not* the equivalence relation on ideals used to define the ideal class group $\mathrm{Pic}(\mathcal{O}_K)$: we impose the additional condition that $|h|_{\mathfrak{p}} = 1$ for all $\mathfrak{p} \in S$.

We can deduce from Proposition 5.2 that this equivalence relation $\sim$ is trivial in case an infinite place of degree one exists:

Corollary 5.3. *Assume that* $\deg \mathfrak{p} = 1$ *for some* $\mathfrak{p} \in S$. *Let* $\mathfrak{b}$ *and* $\mathfrak{b}'$ *be two reduced ideals. Then* $\mathfrak{b} \sim \mathfrak{b}'$ *if and only if* $\mathfrak{b} = \mathfrak{b}'$.

Proof. If $\mathfrak{b} = h\mathfrak{b}'$ with $|h|_{\mathfrak{p}} = 1$ for all $\mathfrak{p} \in S$, we get $h \in B(\mathfrak{b}, (0, \dots, 0))$ and thus, by Proposition 5.2, $h \in k^* \subseteq \mathcal{O}_K^*$. □

In the general case, testing $\sim$ is more complicated. The following proposition shows how this can be done:

Proposition 5.4. *Let* $\mathfrak{b}$ *and* $\mathfrak{b}'$ *be two reduced ideals. Then* $\mathfrak{b} \sim \mathfrak{b}'$ *if and only if* $B(\mathfrak{b}(\mathfrak{b}')^{-1}, (0, \dots, 0)) \neq \{0\}$ *and* $\deg \mathrm{div}(\mathfrak{b}) = \deg \mathrm{div}(\mathfrak{b}')$.

Note that in case K is a number field, $\deg \mathrm{div}(\mathfrak{b}) = -\log \mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{b})$, and in case K is a function field, $\deg \mathrm{div}(\mathfrak{b}) = -\deg \mathrm{Norm}_{K/k(x)}(\mathfrak{b})$. A proof of Proposition 5.4 can be found in Appendix A.

We have now obtained a well-defined map $[\frac{1}{h}\mathfrak{a}]_\sim \mapsto \Psi(h) + \Lambda$, and we are able to test whether $\mathfrak{b} \sim \mathfrak{b}'$ for ideals $\mathfrak{b}, \mathfrak{b}' \in \mathrm{Red}(K)$. The next statement shows that this

map is injective when restricted to the non-empty set $\mathrm{Red}(\mathfrak{a})/_\sim$, and that $\mathrm{Red}(\mathfrak{a})/_\sim$ is finite for all global fields and some non-global function fields.

Proposition 5.5. *The map*

$$d^{\mathfrak{a}} : \mathrm{Red}(\mathfrak{a})/_\sim \to \mathbb{G}^n/\Lambda, \qquad [\tfrac{1}{\mu}\mathfrak{a}]_\sim \to \Psi(\mu) + \Lambda$$

is injective. In case K is a number field, or K is a function field and T is finite, the set $\mathrm{Red}(\mathfrak{a})/_\sim$ *is finite. In any case, it is non-empty. In case K is a global field,* $\mathrm{Red}(\mathfrak{a})$ *itself is finite as well.*

Recall that when K is a function field with finite constant field, then T is always finite. A proof of Proposition 5.5 can be found in Appendix A. Note that the injectivity of $d^{\mathfrak{a}}$ for number fields is also shown by Schoof in [Sch08, Lemma 9.2 (ii)]. The finiteness result for global fields is well known; see for example [HP85, Theorems 3 and 4].

Assume that K is a global field. If we define $X^{\mathfrak{a}} := \mathrm{Red}(\mathfrak{a})/_\sim$, we obtain the first ingredients of an n-dimensional infrastructure: a finite set $X^{\mathfrak{a}}$, a lattice $\Lambda \subseteq \mathbb{G}^n$ of full rank, and an injective map $d^{\mathfrak{a}} : X^{\mathfrak{a}} \to \mathbb{G}^n/\Lambda$.

The map $d^{\mathfrak{a}}$ takes the equivalence class of a reduced ideal $\mathfrak{b}$ in the ideal class of $\mathfrak{a}$, say $\mathfrak{b} = \frac{1}{\mu}\mathfrak{a}$, and maps it to its "distance" $\Psi(\mu)$, which is well defined up to elements of Λ. Choosing the logarithmic absolute value vector of the relative generator μ as the distance generalizes Shanks' original definition of distance in infrastructures [Sha72], and is used in most treatments of the infrastructure, for example in the works of Buchmann and Williams. A notable difference is Lenstra's distance function [Len82]. In the case of function fields, this is also the common measure used to define distances, at least in the case of unit rank one [PR99, Sch01, Lan09].

In this section, we obtained for every $\mathfrak{a} \in \mathrm{Id}(\mathcal{O})$ a finite set $X^{\mathfrak{a}}$, a lattice of full rank $\Lambda \subseteq \mathbb{G}^n$, as well as an injective map $d^{\mathfrak{a}} : X^{\mathfrak{a}} \to \mathbb{G}^n/\Lambda$. Here, we needed to assume that K is a global field to ensure that $X^{\mathfrak{a}}$ is finite and Λ is of full rank, though this can also be true for certain function fields with infinite constant fields. In fact, for arbitrary function fields, $X^{\mathfrak{a}}$ is finite if, and only if, Λ is of full rank. The ingredient this is still missing in order to obtain an n-dimensional infrastructure in the sense of Definition 4.2, namely, a reduction map, will be defined in the next section.

6. f-Representations in global fields

In this section we introduce f-representations $\mathrm{Rep}^f(\mathfrak{a})$ for $(\mathrm{Red}(\mathfrak{a})/_\sim, d^{\mathfrak{a}})$. Using the equivalence of f-representations and reduction maps discussed in Section 4, this yields a reduction map $\mathrm{red}^{\mathfrak{a}} : \mathbb{G}^n/\Lambda \to X^{\mathfrak{a}} = \mathrm{Red}(\mathfrak{a})/_\sim$, so that $(X^{\mathfrak{a}}, d^{\mathfrak{a}}, \mathrm{red}^{\mathfrak{a}})$ is an n-dimensional infrastructure in the sense of Definition 4.2.

Before we define f-representations for arbitrary number fields and function fields, we want to consider a special case, namely $\deg \mathfrak{p}_{n+1} = 1$. In this case, the definition of an f-representation can be drastically simplified and stated with a lot less technical involvement. We distinguish the simpler scenario from the general case by appending an asterisk to the f in f-representations. By Corollary 5.3, we can replace $\mathrm{Red}(\mathfrak{a})/_\sim$ by $\mathrm{Red}(\mathfrak{a})$ itself, as every equivalence class $[\mathfrak{b}]_\sim$ contains exactly one reduced ideal. Recall that in this case, an ideal $\mathfrak{b} \in \mathrm{Id}(\mathcal{O}_K)$ is reduced if $B(\mathfrak{b}, (0, \ldots, 0)) = k$ by Proposition 5.2. An f-representation should be a reduced

ideal $\mathfrak{b}$ together with numbers $t_1, \dots, t_n \geq 0$ which determine how far the box $B(\mathfrak{b}, (0, \dots, 0))$ can be enlarged in the directions of $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ without containing anything but k. More precisely:

Definition 6.1. An *$f*$-representation* is a tuple $(\mathfrak{b}, (t_1, \dots, t_n)) \in \mathrm{Red}(\mathfrak{a}) \times \mathbb{G}^n$ such that $B(\mathfrak{b}, (t_1, \dots, t_n, 0)) = k$. Denote the set of all $f*$-representations in $\mathrm{Red}(\mathfrak{a}) \times \mathbb{G}^n$ by $\mathrm{Rep}^{f*}(\mathfrak{a})$.

We say that $(\mathfrak{b}, t) \in \mathrm{Rep}^{f*}(\mathfrak{a})$ *represents* $d^{\mathfrak{a}}([\mathfrak{b}]_\sim) + t \in \mathbb{G}^n/\Lambda$.

Remark 6.2.

(a) If $\mathfrak{b} \in \mathrm{Red}(\mathfrak{a})$, then always $(\mathfrak{b}, (0, \dots, 0)) \in \mathrm{Rep}^{f*}(\mathfrak{a})$.
(b) If $\mathfrak{b} = \frac{1}{\mu}\mathfrak{a}$ for some $\mu \in K^*$, and if $t_1, \dots, t_n \in \mathbb{G}$ are elements such that $B(\mathfrak{b}, (t_1, \dots, t_n, 0)) = k$, then $(\mathfrak{b}, (t_1, \dots, t_n)) \in \mathrm{Rep}^{f*}(\mathfrak{a})$. In particular, $\mathfrak{b} \in \mathrm{Red}(\mathfrak{a})$. This shows that the assumption that $\mathfrak{b} \in \mathrm{Red}(\mathfrak{a})$ in the definition is not actually needed.

Now we drop the assumption that $\deg \mathfrak{p}_{n+1} = 1$. We have to introduce certain technicalities to ensure that f-representations are well defined. First, as in the case of reduced ideals, we will only have $k \subseteq B(\mathfrak{b}, (t_1, \dots, t_n, 0))$. To ensure that this set does not contain too many elements, we need to introduce a technical tool, namely a total preorder[5] on K^*. For $h, h' \in K^*$, define

$$h \leq h' :\Longleftrightarrow (|h|_{\mathfrak{p}_{n+1}}, |h|_{\mathfrak{p}_1}, \dots, |h|_{\mathfrak{p}_n}) \leq_{\ell ex} (|h'|_{\mathfrak{p}_{n+1}}, |h'|_{\mathfrak{p}_1}, \dots, |h'|_{\mathfrak{p}_n}),$$

where $\leq_{\ell ex}$ is the usual lexicographical order on $\mathbb{R}^{n+1}$. Using this notion, we define f-representations as follows:

Definition 6.3. An *f-representation* is a tuple $([\mathfrak{b}]_\sim, (t_1, \dots, t_n)) \in \mathrm{Red}(\mathfrak{a})/_\sim \times \mathbb{G}^n$ such that $1 \in B(\mathfrak{b}, (t_1, \dots, t_n, 0)) \setminus \{0\}$ is a smallest element with respect to $\leq$. Denote the set of all f-representations in $\mathrm{Red}(\mathfrak{a})/_\sim \times \mathbb{G}^n$ by $\mathrm{Rep}^{f}(\mathfrak{a})$.

As above, we say that $([\mathfrak{b}]_\sim, t) \in \mathrm{Rep}^{f}(\mathfrak{a})$ *represents* $d^{\mathfrak{a}}([\mathfrak{b}]_\sim) + t \in \mathbb{G}^n/\Lambda$.

The condition that 1 is a smallest element with respect to $\leq$ ensures that all elements $h \in B(\mathfrak{b}, (t_1, \dots, t_n, 0)) \setminus \{0\}$ satisfy $|h|_{\mathfrak{p}_{n+1}} = 1$. Moreover, it ensures that $\mathfrak{b}$ is reduced, since any element in $B(\mathfrak{b}, (0, \dots, 0)) \setminus \{0\}$ whose absolute values are not equal to 1 would be strictly less than 1 with respect to this order.

In fact, the choice of $\leq$ is somewhat arbitrary. One could replace $\leq$ with any other preorder on K^* such that:

(a) if $h, h' \in K^*$ satisfy $|h|_{\mathfrak{p}_{n+1}} < |h'|_{\mathfrak{p}_{n+1}}$, then $h < h'$;
(b) if $h, h', h'' \in K^*$ satisfy $h' \leq h''$, then $hh' \leq hh''$;
(c) for every ideal $\mathfrak{b}$ and any $t_1, \dots, t_{n+1} \in \mathbb{G}$, the set $B(\mathfrak{b}, (t_1, \dots, t_{n+1})) \setminus \{0\}$ has a smallest element with respect to $\leq$ if it is non-empty, and this element happens to be a minimum of $\mathfrak{b}$ in the sense of Definition 5.1;
(d) if $h \leq h'$ and $h' \leq h$ for $h, h' \in K^*$, we have $|h|_{\mathfrak{p}} = |h'|_{\mathfrak{p}}$ for every $\mathfrak{p} \in S$.

The choice of $\leq$ as the lexicographical order on vectors of absolute values is a convenient choice satisfying these conditions, in particular, since it is well suited for computations.

[5]A total preorder $\leq$ on a set X is a binary relation which is reflexive and transitive such that for every $x, y \in X$, we have $x \leq y$ or $y \leq x$.

In the case $\deg \mathfrak{p}_{n+1} = 1$, f-representations and the simpler $f*$-representations coincide; this is shown in Proposition 6.5. Before we establish this, we state a few more remarks.

Remark 6.4.

(a) The definition of an f-representation depends only on the equivalence class $[\mathfrak{b}]_\sim$ of $\mathfrak{b}$: if $\mathfrak{b}, \mathfrak{b}'$ are two reduced ideals with $\mathfrak{b} \sim \mathfrak{b}'$, an element with given absolute values in $B(\mathfrak{b}, (t_1, \dots, t_n, 0))$ exists if and only if an element with the same absolute values exists in $B(\mathfrak{b}', (t_1, \dots, t_n, 0))$. Therefore, $\mathrm{Rep}^f(\mathfrak{a})$ is well defined.

(b) If $(\mathfrak{b}, (t_1, \dots, t_n)) \in \mathrm{Rep}^{f*}(\mathfrak{a})$, then $([\mathfrak{b}]_\sim, (t_1, \dots, t_n)) \in \mathrm{Rep}^f(\mathfrak{a})$.

(c) If $\mathfrak{b} \in \mathrm{Red}(\mathfrak{a})$, then always $([\mathfrak{b}]_\sim, (0, \dots, 0)) \in \mathrm{Rep}^f(\mathfrak{a})$. That is, the reduced ideals in the ideal class of $\mathfrak{a}$, modulo the equivalence relation $\sim$, can be embedded into $\mathrm{Rep}^f(\mathfrak{a})$.

(d) If $\mathfrak{b} = \frac{1}{\mu}\mathfrak{a}$ for some $\mu \in K^*$, and if $t_1, \dots, t_n \in \mathbb{G}$ are elements such that $1 \in B(\mathfrak{b}, (t_1, \dots, t_n, 0)) \setminus \{0\}$ is a smallest element with respect to $\leq$, then $([\mathfrak{b}]_\sim, (t_1, \dots, t_n)) \in \mathrm{Rep}^f(\mathfrak{a})$. In particular, $\mathfrak{b} \in \mathrm{Red}(\mathfrak{a})$. This shows that the assumption that $[\mathfrak{b}]_\sim \in \mathrm{Red}(\mathfrak{a})/_\sim$ in the definition is not actually needed.

As mentioned before, in the case of $\deg \mathfrak{p}_{n+1} = 1$, f-representations are equivalent to the simpler $f*$-representations introduced first:

Proposition 6.5. *The map*

$$\mathrm{Rep}^{f*}(\mathfrak{a}) \to \mathrm{Rep}^f(\mathfrak{a}), \qquad (\mathfrak{b}, (t_1, \dots, t_n)) \mapsto ([\mathfrak{b}]_\sim, (t_1, \dots, t_n))$$

is always an injection. Furthermore, if $\deg \mathfrak{p}_{n+1} = 1$*, it is a bijection.*

The proof can be found in Appendix A. The injectivity part is rather straightforward. The proof for the surjectivity is similar to the proof of Proposition 5.2.

Before we show that $\mathrm{Rep}^f(\mathfrak{a})$ is indeed a set of f-representations for $(\mathrm{Red}(\mathfrak{a})/_\sim, d^{\mathfrak{a}})$ in the sense of Definition 4.1, we show the following two lemmas, which illustrate how f-representations can be obtained ("reduction") and in which way they are unique. These lemmas are crucial to prove that the induced map $\mathrm{Rep}^f(\mathfrak{a}) \to \mathbb{G}^n/\Lambda$, $(x, t) \mapsto d^{\mathfrak{a}}(x) + t$ is a bijection: the Reduction Lemma shows that the map is surjective, and the Uniqueness Lemma shows that the map is injective.

The first result, the Reduction Lemma, shows that any tuple $(\mathfrak{b}, (t_1, \dots, t_n)) \in \mathrm{Id}(\mathcal{O}_K) \times \mathbb{G}^n$ can be *reduced* to an f-representation. Similar to reducing an ideal, this procedure divides by a minimum μ of the ideal. The t_i have to be adjusted by the valuations of μ. In particular, this result shows that for every ideal $\mathfrak{a}$, the set $\mathrm{Red}(\mathfrak{a})$ is not empty, hence giving another proof of the non-emptiness result in Proposition 5.5. In fact, the proof is very similar to the proof of that proposition, except that here, we divide by a very specific minimum of $\mathfrak{b}$.

Lemma 6.6 (Existence and Reduction)**.** *Let* $\mathfrak{b}$ *be any ideal equivalent to* $\mathfrak{a}$*, and let* $t_1, \dots, t_n \in \mathbb{G}$*. Then there exists a smallest* $\ell \in \mathbb{G}$ *such that* $B_\ell := B(\mathfrak{b}, (t_1, \dots, t_n, \ell)) \setminus \{0\}$ *is non-empty. If* $\mu \in B_\ell$ *is a smallest element with respect to* $\leq$*, then*

$$([\tfrac{1}{\mu}\mathfrak{b}]_\sim, (t_1 + \nu_{\mathfrak{p}_1}(\mu), \dots, t_n + \nu_{\mathfrak{p}_n}(\mu))) \in \mathrm{Rep}^f(\mathfrak{a}).$$

The proof of Lemma 6.6 shows why ℓ and μ exist, as claimed in the statement of the lemma. Since this lemma yields a reduction procedure, we include the proof here, rather than in the appendix.

Before we prove this result, we want to discuss it in the function field case. Let $D = \operatorname{div}(\mathfrak{b}) + \sum_{i=1}^{n} t_i \mathfrak{p}_i$; then $B_\ell = L(D + \ell\mathfrak{p}_{n+1}) \setminus \{0\}$. In the case of function fields with $\deg \mathfrak{p}_{n+1} = 1$, Heß' reduction method as described in [Heß02] works by minimizing ℓ with $L(D + \ell\mathfrak{p}_{n+1}) \neq \{0\}$, then choosing an element $\mu \in L(D + \ell\mathfrak{p}_{n+1}) \setminus \{0\}$ and replacing D by

$$D + \ell\mathfrak{p}_{n+1} + (\mu) = \operatorname{div}\left(\tfrac{1}{\mu}\mathfrak{b}\right) + \sum_{i=1}^{n} (t_i + \nu_{\mathfrak{p}_i}(\mu))\mathfrak{p}_i.$$

Since $\deg \mathfrak{p}_{n+1} = 1$, $\dim_k L(D + \ell\mathfrak{p}_{n+1}) = 1$, so the choice of $\leq$ does not matter: any other element μ' of B_ℓ will yield the same reduced divisor $D + (\mu')$.

If $\deg \mathfrak{p}_{n+1} > 1$, the condition that μ is a smallest element in B_ℓ with respect to $\leq$ ensures that μ is indeed a minimum of $\mathfrak{b}$, i.e., that $\frac{1}{\mu}\mathfrak{b}$ is reduced in the sense of Definition 5.1. This shows that the procedure described in the lemma generalizes Heß' reduction.

Note that if we consider the set $X = \bigcup_{\ell \in \mathbb{G}} B_\ell$, then X has a smallest element with respect to $\leq$, and every such smallest element μ will satisfy that $\ell = -\nu_{\mathfrak{p}_{n+1}}(\mu)$ is minimal with $B_\ell \neq \emptyset$: this is ensured by the choice of $\leq$, which "prefers" elements with smaller absolute value $|\bullet|_{\mathfrak{p}_{n+1}}$. Hence, we could relax the lemma by not requiring that ℓ be minimal, but just that $B_\ell \neq \emptyset$.

Proof of Lemma 6.6. If $\ell \ll 0$, we have $B_\ell = \emptyset$ by the Product Formula.[6] For $\ell \gg 0$, we get that $B_\ell \neq \emptyset$ by Riemann's Inequality, respectively, Minkowski's Lattice Point Theorem. Choose $\ell \in \mathbb{G}$ minimal such that $B_\ell \neq \emptyset$; in the number field case, this is possible since B_ℓ is a finite set: hence, if ℓ' is chosen such that $B_{\ell'}$ is non-empty, we can choose $\ell = -\max\{\nu_{\mathfrak{p}_{n+1}}(x) \mid x \in B_{\ell'}\}$.

If K is a number field, then B_ℓ is a finite set, whence a minimal element with respect to $\leq$ clearly exists as well. If K is a function field, then the infinite valuations $\nu_{\mathfrak{p}}$ for $\mathfrak{p} \in S$ take on only finitely many values on B_ℓ since $B_\ell \cup \{0\}$ is a finite-dimensional vector space, whence the existence of μ is also clear.

If ℓ is minimal, we have $-\nu_{\mathfrak{p}_{n+1}}(\mu) = \ell$ by choice of μ. Moreover,

$$B(\tfrac{1}{\mu}\mathfrak{b}, (t_1 + \nu_{\mathfrak{p}_1}(\mu), \dots, t_n + \nu_{\mathfrak{p}_n}(\mu), 0)) = \tfrac{1}{\mu} B(\mathfrak{b}, (t_1, \dots, t_n, \ell))$$

and, by choice of μ, we have that $1 = \frac{\mu}{\mu}$ lies in this set and is minimal among the non-zero elements with respect to $\leq$. Hence, by Remark 6.4 (c), the claim follows. □

The second result, uniqueness, shows that reducing an f-representation will always yield the same f-representation. This will be utilized in showing that the map $\operatorname{Rep}^f(\mathfrak{a}) \to \mathbb{G}^n/\Lambda$ is injective: in the proof of Theorem 6.8, we will show that if two f-representations are mapped onto the same element of $\mathbb{G}^n/\Lambda$, then one is a reduction in the sense of the Reduction Lemma 6.6 of the other.

Lemma 6.7 (Uniqueness)**.** *Let* $A := ([\mathfrak{b}]_\sim, (t_1, \dots, t_n)) \in \operatorname{Rep}^f(\mathfrak{a})$ *and let* $\mu \in K^*$ *such that* $B := ([\frac{1}{\mu}\mathfrak{b}]_\sim, (t_1 + \nu_{\mathfrak{p}_1}(\mu), \dots, t_n + \nu_{\mathfrak{p}_n}(\mu))) \in \operatorname{Rep}^f(\mathfrak{a})$. *Then* $|\mu|_{\mathfrak{p}} = 1$ *for all* $\mathfrak{p} \in S$*, and hence* $A = B$.

[6] Here, a statement being true for $x \ll 0$ (respectively, $x \gg 0$) means that there exists some N such that the statement holds for all $x \leq N$ (respectively, $x \geq N$).

The proof can be found in Appendix A. The main part is to show that since $A, B \in \mathrm{Rep}^f(K)$, we have $1 \leq \mu$ and $\mu \leq 1$, which, by the definition of $\leq$, shows that $|\mu|_{\mathfrak{p}} = 1$ for all $\mathfrak{p} \in S$.

Now we will state our main result in this section, which asserts that the set $\mathrm{Rep}^f(\mathfrak{a})$ as given in Definition 6.3 indeed defines a set of f-representations for $(X^{\mathfrak{a}}, d^{\mathfrak{a}})$ in the sense of Definition 4.1. This can be seen as generalizing Proposition 3.4 for the one-dimensional infrastructure case. Note that the set $X^{\mathfrak{a}} = \mathrm{Red}(\mathfrak{a})/_{\sim}$ is possibly infinite if K is a function field and k is not finite.

Theorem 6.8 (Infrastructure, Part I: Correspondence between f-representations and $\mathbb{G}^n/\Lambda$)**.** *The map*

$$\Phi^{\mathfrak{a}} : \mathrm{Rep}^f(\mathfrak{a}) \to \mathbb{G}^n/\Lambda, \qquad ([\mathfrak{b}]_{\sim}, t) \mapsto d^{\mathfrak{a}}(\mathfrak{b}) + t$$

is a bijection, and $([\mathfrak{b}]_{\sim}, (0, \ldots, 0)) \in \mathrm{Rep}^f(\mathfrak{a})$ *for every* $[\mathfrak{b}]_{\sim} \in \mathrm{Red}(\mathfrak{a})/_{\sim}$.

A proof can be found in Appendix A. Note that this result generalizes the injectivity of $d^{\mathfrak{a}}$ in Proposition 5.5: for that result, it suffices to note that the map $\mathrm{Red}(\mathfrak{a})/_{\sim} \to \mathrm{Rep}^f(\mathfrak{a})$, $[\mathfrak{b}]_{\sim} \mapsto ([\mathfrak{b}]_{\sim}, (0, \ldots, 0))$ is an injection.

So far, we have obtained a set $X^{\mathfrak{a}} = \mathrm{Red}(\mathfrak{a})/_{\sim}$ of classes of reduced ideals equivalent to $\mathfrak{a}$, together with a distance map $d^{\mathfrak{a}} : X^{\mathfrak{a}} \to \mathbb{G}^n/\Lambda$ and a set of f-representations $\mathrm{Rep}^f(\mathfrak{a}) \subset X^{\mathfrak{a}} \times \mathbb{G}^n/\Lambda$ for $(X^{\mathfrak{a}}, d^{\mathfrak{a}})$. This means that the map

$$\Phi^{\mathfrak{a}} : \mathrm{Rep}^f(\mathfrak{a}) \to \mathbb{G}^n/\Lambda, \qquad (x, t) \mapsto d^{\mathfrak{a}}(x) + t$$

is a bijection, and we know that $(x, 0) \in \mathrm{Rep}^f(\mathfrak{a})$ for all $x \in X^{\mathfrak{a}}$. This allows us to define a reduction map

$$\mathrm{red}^{\mathfrak{a}} : \mathbb{G}^n/\Lambda \to X^{\mathfrak{a}}$$

for $(X^{\mathfrak{a}}, d^{\mathfrak{a}})$ as in the previous section, by taking $\mathrm{red}^{\mathfrak{a}}(v)$ to be the first component of $(\Phi^{\mathfrak{a}})^{-1}(v) \in \mathrm{Rep}^f(\mathfrak{a})$. Therefore, assuming K is a global field, $(X^{\mathfrak{a}}, d^{\mathfrak{a}}, \mathrm{red}^{\mathfrak{a}})$ is an *n-dimensional infrastructure*, and we obtain a giant step

$$\mathrm{gs}^{\mathfrak{a}}(x, x') := \mathrm{red}^{\mathfrak{a}}(d^{\mathfrak{a}}(x) + d^{\mathfrak{a}}(x')), \qquad x, x' \in X^{\mathfrak{a}}.$$

Moreover, as in the one-dimensional case, we can use $\Phi^{\mathfrak{a}}$ to turn $\mathrm{Rep}^f(\mathfrak{a})$ into an abelian group by pulling back the group operation from $\mathbb{G}^n/\Lambda$: for $A, B \in \mathrm{Rep}^f(\mathfrak{a})$, define

$$A \oplus_{\mathfrak{a}} B := (\Phi^{\mathfrak{a}})^{-1}(\Phi^{\mathfrak{a}}(A) + \Phi^{\mathfrak{a}}(B)).$$

Then $(\mathrm{Rep}^f(\mathfrak{a}), \oplus_{\mathfrak{a}})$ is an abelian group isomorphic to $\mathbb{G}^n/\Lambda$ via $\Phi^{\mathfrak{a}}$. We denote this group operation by $\oplus_{\mathfrak{a}}$ and not by $+$ since in the next section, we will equip $\bigcup_{\mathfrak{a} \in \mathrm{Id}(\mathcal{O}_K)} \mathrm{Rep}^f(\mathfrak{a})$ with a group operation named $+$ which is related to the (Arakelov) divisor class group of K. Now $(\mathrm{Rep}^f(\mathcal{O}_K), \oplus_{\mathcal{O}_K})$ will be a subgroup of $\bigcup_{\mathfrak{a} \in \mathrm{Id}(\mathcal{O}_K)} \mathrm{Rep}^f(\mathfrak{a})$, but no other $(\mathrm{Rep}^f(\mathfrak{a}), \oplus_{\mathfrak{a}})$ will be a subgroup. Therefore, we reserve the symbol $+$ for the operation defined in the next section.

If $\mathfrak{a} = \mathcal{O}_K$, then the results in the next section allow us to explicitly describe the group operation on $\mathrm{Rep}^f(\mathcal{O}_K)$. It is essentially ideal multiplication, followed by a reduction: if $A = ([\mathfrak{b}]_{\sim}, (t_1, \ldots, t_n)), B = ([\mathfrak{b}']_{\sim}, (t'_1, \ldots, t'_n)) \in \mathrm{Rep}^f(\mathcal{O}_K)$, we can apply the Reduction Lemma 6.6 to $(\mathfrak{b}\mathfrak{b}', (t_1 + t'_1, \ldots, t_n + t'_n))$. In case $\mathfrak{a} \neq \mathcal{O}_K$, one can still describe the group operation $\oplus_{\mathfrak{a}}$ on $\mathrm{Rep}^f(\mathfrak{a})$, but one cannot use simple ideal multiplication since $\mathfrak{b}\mathfrak{b}'$ will not be in the ideal class of $\mathfrak{a}$ as soon as $\mathfrak{a}$ is not a principal ideal; and even if $\mathfrak{a}$ is principal, distances will be added incorrectly. The correct formula is given as follows:

Proposition 6.9. *Let* $A = ([\mathfrak{b}]_\sim, (t_1, \ldots, t_n)), B = ([\mathfrak{b}']_\sim, (t'_1, \ldots, t'_n)) \in \mathrm{Rep}^f(\mathfrak{a})$. *Apply the Reduction Lemma* 6.6 *to* $(\mathfrak{b}\mathfrak{b}'\mathfrak{a}^{-1}, (t_1 + t'_1, \ldots, t_n + t'_n))$, *and denote the result by* C. *Then* $C \in \mathrm{Rep}^f(\mathfrak{a})$ *and* $A \oplus_\mathfrak{a} B = C$.

This result is similar to Remark 3.5 and Example 3.6 in the one-dimensional case: the reduced ideals are multiplied and the product is then reduced. In case $\mathfrak{a} \neq \mathcal{O}_K$, a correction factor needs to be multiplied to the product of the ideals. A proof of this result can be found in Appendix A.

In this section, we saw how to construct a set of f-representations $\mathrm{Rep}^f(\mathfrak{a})$ and, therefore, a reduction map $\mathrm{red}^\mathfrak{a}$ for $(X^\mathfrak{a}, d^\mathfrak{a}) = (\mathrm{Red}(\mathfrak{a})/_\sim, d^\mathfrak{a})$, thereby turning this pair into an n-dimensional infrastructure $(X^\mathfrak{a}, d^\mathfrak{a}, \mathrm{red}^\mathfrak{a})$. We also saw how to explicitly compute the group operation induced by the bijection $\mathrm{Rep}^f(\mathfrak{a}) \to \mathbb{G}^n/\Lambda$ in terms of ideal multiplication followed by reduction. This also shows how the giant-step operation $\mathrm{gs}([\mathfrak{b}]_\sim, [\mathfrak{b}']_\sim)$ can be computed, by ignoring the t-part of the resulting f-representation $([\mathfrak{b}]_\sim, 0) \oplus_\mathfrak{a} ([\mathfrak{b}']_\sim, 0)$. This operation generalizes Shanks' original approach as sketched in Example 3.6.

7. Relation to the divisor class group

In this section, we want to relate the set of all f-representations,

$$\mathrm{Rep}^f(K) := \bigcup_{\mathfrak{a} \in \mathrm{Id}(\mathcal{O}_K)} \mathrm{Rep}^f(\mathfrak{a}),$$

to the (Arakelov) divisor class group $\mathrm{Pic}^0(K)$. In case K is a number field, or in case K is a function field and $\deg \mathfrak{p}_{n+1} = 1$, we obtain an isomorphism $\mathrm{Rep}^f(K) \to \mathrm{Pic}^0(K)$. In case K is a function field and $\deg \mathfrak{p}_{n+1} > 1$, we can identify a subset of $\mathrm{Rep}^f(K)$ with $\mathrm{Pic}^0(K)$. We show that we can then extend $\mathrm{Pic}^0(K)$ to obtain a group which is isomorphic to $\mathrm{Rep}^f(K)$. Finally, we show how to perform effective arithmetic in $\mathrm{Rep}^f(K)$.

To motivate the fact that there is a relationship between our infrastructures $(X^\mathfrak{a}, d^\mathfrak{a}, \mathrm{red}^\mathfrak{a})$ together with $\mathrm{Rep}^f(\mathfrak{a})$ and the (Arakelov) divisor class group $\mathrm{Pic}^0(K)$, we first consider the aforementioned special case. Assume for a moment that $\deg \mathfrak{p}_{n+1} = 1$, or that K is a number field. In this case, we have the short exact sequence

$$0 \longrightarrow T \longrightarrow \mathrm{Pic}^0(K) \longrightarrow \mathrm{Pic}(\mathcal{O}_K) \longrightarrow 0,$$

and we have $T \cong \mathbb{G}^n/\Lambda$. Moreover, we have a representation of $\mathbb{G}^n/\Lambda$ by $\mathrm{Rep}^f(\mathfrak{a})$ for every $\mathfrak{a} \in \mathrm{Id}(\mathcal{O}_K)$, which consists of all f-representations whose reduced ideals range over all reduced ideals in the ideal class of $\mathfrak{a}$. By the short exact sequence, clearly the (Arakelov) divisor class group $\mathrm{Pic}^0(K)$ is covered by $|\mathrm{Pic}(\mathcal{O}_K)|$ copies of $\mathbb{G}^n/\Lambda$, whence one might hope that $\mathrm{Pic}^0(K)$ can be described in a nice way using $\mathrm{Rep}^f(K) = \bigcup_{\mathfrak{a} \in \mathrm{Id}(\mathcal{O}_K)} \mathrm{Rep}^f(\mathfrak{a})$. This turns out to be the case. In fact, Paulus and Rück already showed this for the special case of the infrastructure obtained from a real hyperelliptic curve in [PR99].

In the general case, i.e., if $\deg \mathfrak{p}_{n+1}$ is not necessarily 1, T can be embedded into $\mathbb{G}^n/\Lambda$, but might not cover the entire set, and the map $\mathrm{Pic}^0(K) \to \mathrm{Pic}(\mathcal{O}_K)$ might not be surjective. This can only happen in the function field case. It would be desirable to have a short exact sequence

$$(*) \qquad 0 \longrightarrow \mathbb{G}^n/\Lambda \longrightarrow ? \longrightarrow \mathrm{Pic}(\mathcal{O}_K) \longrightarrow 0$$

for all function fields, into which the exact sequence

$$(**) \qquad 0 \longrightarrow T \longrightarrow \mathrm{Pic}^0(K) \longrightarrow \mathrm{Pic}(\mathcal{O}_K)$$

embeds in a natural way. If D is a divisor with $\deg D \neq 0$, one obtains an exact sequence

$$0 \longrightarrow \mathrm{Pic}^0(K) \longrightarrow \mathrm{Pic}(K)/\langle [D] \rangle \longrightarrow (\deg \mathfrak{p} \mid \mathfrak{p} \in \mathcal{P}_K)\mathbb{Z}/(\deg D)\mathbb{Z} \longrightarrow 0.$$

For the right choice of D, we obtain that $\mathrm{Pic}(K)/\langle [D] \rangle$ is the right replacement for the "?" in equation $(*)$. The exact relationship between the exact sequences in equations $(*)$ and $(**)$ will be described later in Proposition 7.2.

We now state the main result for this section, which identifies the set of f-representations with the Arakelov divisor class group, or with an extension of $\mathrm{Pic}^0(K)$.

Theorem 7.1 (Infrastructure, Part II: Relating f-representations to the divisor class group)**.**

(a) *Let K be a number field. Then the following map is a bijection:*

$$\Phi : \mathrm{Rep}^f(K) \to \mathrm{Pic}^0(K),$$
$$([\mathfrak{b}]_\sim, (t_1, \ldots, t_n)) \mapsto \left[\mathrm{div}(\mathfrak{b}) + \sum_{i=1}^{n} t_i \mathfrak{p}_i - \tfrac{\deg \mathrm{div}(\mathfrak{b}) + \sum_{i=1}^{n} t_i \deg \mathfrak{p}_i}{\deg \mathfrak{p}_{n+1}} \mathfrak{p}_{n+1}\right].$$

(b) *Let K be a function field. Then the following map is a bijection:*

$$\Phi : \mathrm{Rep}^f(K) \to \mathrm{Pic}(K)/\langle [\mathfrak{p}_{n+1}] \rangle,$$
$$([\mathfrak{b}]_\sim, (t_1, \ldots, t_n)) \mapsto \left[\mathrm{div}(\mathfrak{b}) + \sum_{i=1}^{n} t_i \mathfrak{p}_i\right] + \langle [\mathfrak{p}_{n+1}] \rangle.$$

The proof can be found in Appendix A.

Note that this gives, in particular, an embedding of $\mathrm{Red}(K)/_\sim$ into $\mathrm{Pic}^0(K)$, respectively, $\mathrm{Pic}(K)/\langle [\mathfrak{p}_{n+1}] \rangle$, where $\mathrm{Red}(K) = \bigcup_{\mathfrak{a} \in \mathrm{Id}(\mathcal{O}_K)} \mathrm{Red}(\mathfrak{a})$. In the case of number fields, Schoof gave a similar embedding in [Sch08]; more precisely, he embedded $\mathrm{Red}(K)$ in the *oriented* Arakelov divisor class group $\widetilde{\mathrm{Pic}}^0(K)$, which is a cover of $\mathrm{Pic}^0(K)$. Moreover, his embedding assigns different valuations for the infinite places. Our embedding has the advantage that it works in a very similar way for both number fields and function fields. In the case of real hyperelliptic function fields, our embedding is the same as the one by Paulus and Rück [PR99, Theorem 4.2]. Moreover, in part (b) of the theorem, the divisor whose class is taken is reduced along $\mathfrak{p}_{n+1}$ in the sense of Heß [Heß02]. In case $\deg \mathfrak{p}_{n+1} = 1$, this shows that f-representations directly correspond to *arbitrary* reduced divisors in the sense of Heß which are reduced along $\mathfrak{p}_{n+1}$.

Finally, note that if we denote by $\mathbb{G}[\mathfrak{p}_{n+1}]$ the 1-parameter subgroup $\{[g\mathfrak{p}_{n+1}] \mid g \in \mathbb{G}\}$ of $\mathrm{Pic}(K)$ in case K is a number field, then we can identify $\mathrm{Pic}^0(K)$ with $\mathrm{Pic}(K)/\mathbb{G}[\mathfrak{p}_{n+1}]$. Hence, we can write Φ as

$$\Phi : \mathrm{Rep}^f(K) \to \mathrm{Pic}(K)/\mathbb{G}[\mathfrak{p}_{n+1}],$$
$$([\mathfrak{b}]_\sim, (t_1, \ldots, t_n)) \mapsto \left[\mathrm{div}(\mathfrak{b}) + \sum_{i=1}^{n} t_i \mathfrak{p}_i\right] + \mathbb{G}[\mathfrak{p}_{n+1}]$$

for both number fields and function fields. Thus, Theorem 7.1 completely unifies the number field and function field scenarios.

Before describing how the group operation on $\mathrm{Rep}^f(K)$ induced by the one on $\mathrm{Pic}(K)/\mathbb{G}[\mathfrak{p}_{n+1}]$ can be computed, we want to state a result on the interrelations between all aforementioned groups. For that, we first make clear how the map $T \to \mathbb{G}^n/\Lambda$ is defined. Assume that $T = \mathrm{Div}^0_\infty(K)/(\mathcal{O}_K^*/k^*)$, where $\mathcal{O}_K^*/k^*$ is embedded into $\mathrm{Div}^0_\infty(K)$ by forming principal divisors. Then we obtain a map $T \hookrightarrow \mathbb{G}^n/\Lambda$ by mapping the class of $\sum_{\mathfrak{p}\in S} t_\mathfrak{p}\mathfrak{p}$ to $(t_{\mathfrak{p}_1}, \dots, t_{\mathfrak{p}_n}) + \Lambda$. This map is clearly injective. In case K is a number field or if $\deg \mathfrak{p}_{n+1} = 1$, it is surjective as well.

Proposition 7.2. *The diagram*

$$\begin{array}{ccccccc}
0 & \longrightarrow & T & \longrightarrow & \mathrm{Pic}^0(K) & \longrightarrow & \mathrm{Pic}(\mathcal{O}_K) \\
 & & \downarrow & & \downarrow & & \| \\
 & & \mathbb{G}^n/\Lambda & & \mathrm{Pic}(K)/\mathbb{G}[\mathfrak{p}_{n+1}] & & \| \\
 & & \cong\downarrow{\scriptstyle (\Phi^\mathfrak{a})^{-1}} & & \cong\downarrow{\scriptstyle \Phi^{-1}} & & \| \\
0 & \longrightarrow & \mathrm{Rep}^f(\mathcal{O}_K) & \longrightarrow & \mathrm{Rep}^f(K) & \longrightarrow & \mathrm{Pic}(\mathcal{O}_K) \longrightarrow 0
\end{array}$$

commutes. In case K is a function field, the image of T in $\mathbb{G}^n/\Lambda$ is the set

$$\left\{ (t_i)_i + \Lambda \in \mathbb{G}^n/\Lambda \;\middle|\; \deg \mathfrak{p}_{n+1} \text{ divides } \sum_{i=1}^n t_i \deg \mathfrak{p}_i \right\},$$

and the image of $\mathrm{Pic}^0(K)$ in $\mathrm{Rep}^f(K)$ is the set

$$\left\{ ([\mathfrak{a}]_\sim, (t_1, \dots, t_n)) \in \mathrm{Rep}^f(K) \;\middle|\; \deg \mathfrak{p}_{n+1} \text{ divides } \deg \mathrm{div}(\mathfrak{a}) + \sum_{i=1}^n t_i \deg \mathfrak{p}_i \right\}.$$

The proof consists of diagram chasing using the definitions of the relevant objects. It does not give any new insight, and can be found in Appendix A for reference.

Proposition 7.2 shows, in particular, that the group operation $\oplus_{\mathcal{O}_K}$ on $\mathrm{Rep}^f(\mathcal{O}_K)$ defined in the last section is identical to the group operation $+$ obtained from the group operation on $\mathrm{Pic}(K)/\mathbb{G}[\mathfrak{p}_{n+1}]$ restricted to the subset $\mathrm{Rep}^f(\mathcal{O}_K)$. Hence, we are able to relate two group operations which were defined quite differently: $\oplus_{\mathcal{O}_K}$ is defined by pulling back the addition from $\mathbb{G}^n/\Lambda$, and $+$ is defined by pulling back the addition from $\mathrm{Pic}(K)/\mathbb{G}[\mathfrak{p}_{n+1}]$.

It turns out that the group operations in $\mathrm{Pic}^0(K)$, respectively, $\mathrm{Pic}(K)/\langle[\mathfrak{p}_{n+1}]\rangle$, can be described in a nice way using f-representations. This directly generalizes the arithmetic in $(\mathrm{Rep}^f(\mathcal{O}_K), \oplus_{\mathcal{O}_K})$ as described in Proposition 6.9. Note that this is *not* related to the arithmetic in $(\mathrm{Rep}^f(\mathfrak{a}), \oplus_\mathfrak{a})$ for $\mathfrak{a} \neq \mathcal{O}_K$.

The following theorem describes how the group operations on $\mathrm{Rep}^f(K)$ can be effectively computed.

Theorem 7.3 (Infrastructure, Part III: Computing the group operation)**.** *Let $A = ([\mathfrak{b}]_\sim, (t_1, \dots, t_n))$, $A' = ([\mathfrak{b}']_\sim, (t'_1, \dots, t'_n)) \in \mathrm{Rep}^f(K)$.*

(a) *There exists a minimal $\ell \in \mathbb{G}$ such that $B_\ell := B(\mathfrak{b}\mathfrak{b}', (t_1 + t'_1, \dots, t_n + t'_n, \ell)) \setminus \{0\}$ is non-empty; if μ is a smallest element with respect to $\leq$ in B_ℓ, we get $B := ([\frac{1}{\mu}\mathfrak{b}\mathfrak{b}']_\sim, (t_1 + t'_1 + \nu_{\mathfrak{p}_1}(\mu), \dots, t_n + t'_n + \nu_{\mathfrak{p}_n}(\mu))) \in \mathrm{Rep}^f(K)$ and $\Phi(A) + \Phi(A') = \Phi(B)$.*

(b) *There exists a minimal* $\ell \in \mathbb{G}$ *such that* $B_\ell := B(\mathfrak{b}^{-1}, (-t_1, \ldots, -t_n, \ell)) \setminus \{0\}$ *is non-empty; if* μ *is a smallest element with respect to* $\leq$ *in* B_ℓ*, we get* $C := ([\frac{1}{\mu}\mathfrak{b}^{-1}]_\sim, (-t_1 + \nu_{\mathfrak{p}_1}(\mu), \ldots, -t_n + \nu_{\mathfrak{p}_n}(\mu))) \in \mathrm{Rep}^f(K)$ *and* $-\Phi(A) = \Phi(C)$.

The main parts of this lemma were already shown in Lemma 6.6, namely that B and C are indeed f-representations. The claims $\Phi(A) + \Phi(A') = \Phi(B)$ and $-\Phi(A) = \Phi(C)$ follow from the fact that $\mathrm{div} : \mathrm{Id}(\mathcal{O}_K) \to \mathrm{Div}(K)$ is a group homomorphism as well as from the definitions of Φ and of the group operation on $\mathrm{Pic}^0(K)$, respectively, $\mathrm{Pic}(K)/\langle[\mathfrak{p}_{n+1}]\rangle$.

Note that this "reduction" step, namely minimizing ℓ, and then minimizing μ with respect to $\leq$ if necessary, is essentially the same that is used for arithmetic on hyperelliptic and superelliptic curves [GPS02], and for Heß' arithmetic in function fields with $\deg \mathfrak{p}_{n+1} = 1$ [Heß02]; compare the discussion following the Reduction Lemma 6.6. This is not very surprising, since as we already mentioned, f-representations are another representation of divisors reduced along $\mathfrak{p}_{n+1}$.

We have seen that all infrastructures $(\mathrm{Red}(\mathfrak{a})/_\sim, d^{\mathfrak{a}})$ in K, and their corresponding f-representations $\mathrm{Rep}^f(\mathfrak{a})$, can be combined to the set of *all* f-representations $\mathrm{Rep}^f(K)$, which parameterizes the (Arakelov) divisor class group $\mathrm{Pic}(K)/\mathbb{G}[\mathfrak{p}_{n+1}] \supseteq \mathrm{Pic}^0(K)$ using the bijection Φ. Moreover, we have seen how the group structure on $\mathrm{Rep}^f(K)$ induced by the one on the (Arakelov) divisor class group can be computed in terms of f-representations only; this is essentially ideal multiplication followed by reduction, hence generalizing Shanks' giant steps. Using Corollary 5.3 and Proposition 5.4 we are able to compare f-representations. Therefore, we can represent the (Arakelov) divisor class group using f-representations and use them to perform effective arithmetic.

8. Computations using f-representations

Infrastructures not only represent an interesting algebraic concept, but f-representations lend themselves very well to computation and lead to efficient algorithms for computing fundamental units in global function fields. They require only limited storage and allow for efficient giant-step computation, as documented in this section. Further evidence supporting the suitability of f-representations for computation is provided with three non-trivial numerical examples. Proofs of these results and a more detailed discussion of implementation go beyond the scope of this work and are the subject of a forthcoming paper.

We begin with a result on the size of f-representations, which in the function field case is identical to a result by Heß in [Heß02, Section 8]. In the number field case, it generalizes a result by Schoof [Sch08, Proposition 7.2 (i)] to f-representations; his result is slightly stronger than the well-known inequality $1 \leq \mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{a}^{-1}) \leq \sqrt{|\Delta|}$ for $\mathfrak{a} \in \mathrm{Red}(K)$, where Δ is the discriminant of K.

Remember that $\deg \mathrm{div}(\mathfrak{a}) = -\log \mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{a})$ if K is a number field, and $\deg \mathrm{div}(\mathfrak{a}) = -\deg \mathrm{Norm}_{K/k(x)}(\mathfrak{a})$ if K is a function field.

Proposition 8.1. *Let* $([\mathfrak{a}]_\sim, (t_i)_i) \in \mathrm{Rep}^f(K)$. *Then* $\mathrm{div}(\mathfrak{a}) \geq 0$ *and* $t_i \geq 0$ *for* $1 \leq i \leq n$. *If* K *is a function field, let* g *be its genus, and if* K *is a number field, let* Δ *be its discriminant and* $2s$ *its number of complex embeddings. Then*

$$0 \leq \deg \operatorname{div}(\mathfrak{a}) + \sum_{i=1}^{n} t_i \deg \mathfrak{p}_i \leq \begin{cases} g + (\deg \mathfrak{p}_{n+1} - 1) & \text{if } K \text{ is a function field,} \\ \frac{1}{2} \log |\Delta| - s \log \frac{\pi}{2} & \text{if } K \text{ is a number field.} \end{cases}$$

We included a proof of this result in Appendix A.

This shows that not only the norm of the integral ideal $\mathfrak{a}^{-1}$ as well as the positive integers t_i are bounded, but a linear combination of these values with positive coefficients is bounded. As shown by Paulus and Rück [PR99], this bound is sharp in the case of real quadratic function fields.

To represent a reduced ideal, one can use a Hermite normal form representation with respect to a fixed integral basis as described in [Coh96]. This allows us to represent a fractional ideal with a unique binary representation. In the number field case, C. Thiel showed in [Thi95, Corollary 3.7] that one can represent a reduced ideal in a number field of degree d and discriminant Δ with at most $(d^2+1) \log_2 \sqrt{|\Delta|}$ bits. For function fields, we obtain:

Proposition 8.2. *Let K be a function field. Assume that elements of k can be represented by $\mathcal{O}(\log q)$ bits. Then f-representations can be represented by $\mathcal{O}\big(d^2(g + \deg \mathfrak{p}_{n+1} - 1) \log q\big)$ bits.* □

We will provide a more precise statement as well as a proof in a subsequent paper.

Using a technique similar to Heß' algorithm for computing Riemann-Roch spaces [Heß02], we implemented f-representations for function fields. We made the assumption that $\deg \mathfrak{p}_{n+1} = 1$ to ensure that we can quickly compare f-representations by their binary representation. We added to our implementation an algorithm by Buchmann and A. Schmidt [BS05] to compute the relation lattice Λ of the elements $(g_1, \ldots, g_n)$ in $\operatorname{Rep}^f(\mathcal{O}_K)$, where $g_i = (\Phi^{\mathcal{O}_K})^{-1}(e_i)$ if $e_i \in \mathbb{Z}^n$ is the i-th standard unit vector; note that this is a system of generators of $\operatorname{Rep}^f(\mathcal{O}_K)$. This lattice equals the unit lattice as defined in Section 5. Since the Buchmann-Schmidt algorithm is of baby-step giant-step type and requires $\mathcal{O}(n\sqrt{|\operatorname{Rep}^f(\mathcal{O}_K)|})$ group operations and $\mathcal{O}(\sqrt{|\operatorname{Rep}^f(\mathcal{O}_K)|})$ storage of group elements, we therefore implemented an algorithm which computes the unit lattice of a global function field with at least one infinite place of degree one in $\mathcal{O}(\sqrt{R})$ infrastructure operations using $\mathcal{O}(\sqrt{R})$ storage (assuming $[K : k(x)] = \mathcal{O}(1)$). This can be seen as a generalization of Shanks' baby-step giant-step algorithm for computing the unit lattice for a real quadratic number field [Sha72], or of Buchmann's baby-step giant-step algorithm for computing the unit lattice of an arbitrary number field [Buc87b].

Our algorithm was implemented in C++ using NTL. It currently relies on MAGMA for computation of integral bases and information on the infinite places. We present three numerical examples that were obtained using our algorithm. We compared the output of our program to MAGMA's built-in function `Regulator()`; this function apparently uses Heß' subexponential algorithm for computation of the divisor class group [Heß99]. We applied both our algorithm and MAGMA to the function fields of many curves. As an example, we want to present three curves:

(1) $y^3 = (x+1)y^2 - (123x^3 - 423x^2 + 948x - 1)y + (13x^2 + 3123x + 11)x^2$ over $\mathbb{F}_{1009}$; the function field has genus 3, two infinite places of degree 1 (so unit rank 1), and regulator 496 804 315;
(2) $y^8 = 81(x+2)^2(x-3)^3(x+1)^3$ over $\mathbb{F}_{1009}$; the function field has genus 3, eight infinite places of degree 1 (so unit rank 7), and regulator 62 322 365;

(3) $(2+\alpha)(y^4-y^2)+\frac{1-\alpha}{x}(y^3+y^2)+\frac{1}{1-(1+\alpha^2)x}y=12\frac{\alpha-x}{x}$ over $\mathbb{F}_{31^2}=\mathbb{F}_{31}[\alpha]$ with $\alpha^2+29\alpha+3=0$; the function field has genus 3, two infinite places of degree 1, one infinite place of degree 2 (so unit rank 2), and regulator 896 118 755.

These fields show that our implementation is not restricted to curves of special form, small unit rank, or prime fields. We also do not require all infinite places to have degree one.

For the first field, MAGMA ran 1.4 to 2.0 hours (in ten different runs) and required between 99 MB and 104 MB of memory to compute the regulator. For the second field, MAGMA's running time varied dramatically between 3.4 hours and 8.9 days in seven runs, with an average of 4.8 days; the memory consumption ranged between 119 MB and 127 MB, where usually the memory usage was around 120 MB, and only spiked up to 127 MB for the two runs which needed only a few hours. For the last field, MAGMA worked 2.4 minutes and required 110 MB of memory (with minimal variations in twelve runs). On the same machine, our implementation was able to compute the regulator in 13.6 minutes for the first field using 46 MB of memory, in 9.2 hours for the second field using 97 MB of memory, and in 11.6 hours for the last field using 313 MB of memory.

Note that our implementation is not very optimized and in a very general form. Nonetheless, this demonstrates that the techniques developed in this paper can be used for computation, and even outperform the built-in functions of MAGMA in certain cases. The latter is not surprising, since the algorithm MAGMA apparently uses is designed for small constant fields and characteristics, and for such function fields is in general much faster than our implementation.

9. Conclusion

We presented a concise interpretation of the infrastructure in a global field, by considering a finite set $X^{\mathfrak{a}}$, consisting of equivalence classes of reduced ideals in the ideal class of $\mathfrak{a}$, and a distance map $d^{\mathfrak{a}}: X^{\mathfrak{a}} \to \mathbb{G}^n/\Lambda$, where Λ is essentially $\mathcal{O}_K^*/k^*$. We have shown how one can find a reduction map $\mathrm{red}^{\mathfrak{a}}: \mathbb{G}^n/\Lambda \to X^{\mathfrak{a}}$ by providing a set of f-representations. This generalizes one-dimensional infrastructures, and in particular Shanks' original approach and its interpretation by Lenstra [Len82].

Considering all infrastructures $(X^{\mathfrak{a}}, d^{\mathfrak{a}}, \mathrm{red}^{\mathfrak{a}})$, $\mathfrak{a} \in \mathrm{Id}(\mathcal{O}_K)$ in K at the same time, we saw that the set of all f-representations, $\mathrm{Rep}^f(K)$, can be identified with the (Arakelov) divisor class group $\mathrm{Pic}(K)/\mathbb{G}[\mathfrak{p}_{n+1}]$ of K. This generalizes the result by Paulus and Rück [PR99] for hyperelliptic function fields, and is compatible with the arithmetic in $\mathrm{Pic}^0(K)$ described by Heß [Heß02]. Moreover, our embedding of $\mathrm{Rep}^f(K)$ into $\mathrm{Pic}^0(K)$ in the number field case is similar to Schoof's embedding of $\mathrm{Red}(K)$ into the Arakelov divisor class group $\mathrm{Pic}^0(K)$.

An important open question is how baby steps can be interpreted in our approach. One can interpret them as Buchmann in [Buc87b] as a tool which computes all reduced elements whose distance lies in a given parallelepiped, as this allows baby-step giant-step algorithms for arbitrary infrastructures. Unfortunately, no efficient method for computing these "baby steps" is known for number fields. Another open question is whether one can find an efficient unique representation of elements in $\mathrm{Pic}^0(K)$ in case no infinite place of degree one is available. Having a unique representation of an element in $\mathrm{Red}(K)/_\sim$ is required to do fast look-ups as in algorithms of baby-step giant-step type.

Acknowledgments

I would like to thank Michael J. Jacobson and Hugh C. Williams for introducing me to the subject of infrastructures, Andreas Stein for several discussions which gave me ideas, and Renate Scheidler and Mark Bauer for discussions on certain aspects. Moreover, I would like to thank the mathematical institutes at the Universität Oldenburg and the University of Calgary for their hospitality during my visits. Finally, I would like to thank Renate Scheidler and the anonymous referee for their helpful and extensive comments and Rachel Suri for proofreading.

Appendix A. Missing Proofs

This appendix contains the proofs we omitted in order to make the paper more readable. Most of the proofs are straightforward for experts. All proofs presented here should be accessible to interested readers.

Proof of Proposition 5.4. If $\mathfrak{b} \sim \mathfrak{b}'$, there exists $h \in K^*$ with $h\mathfrak{b}' = \mathfrak{b}$ such that $|h|_{\mathfrak{p}} = 1$ for all $\mathfrak{p} \in S$. Hence, $\mathfrak{b}(\mathfrak{b}')^{-1} = h\mathcal{O}_K$ and $h \in B(\mathfrak{b}(\mathfrak{b}')^{-1}, (0, \ldots, 0))$. Moreover, $\operatorname{div}(\mathfrak{b}(\mathfrak{b}')^{-1}) = (h^{-1})$ is principal, i.e., of degree zero, whence $\deg \operatorname{div}(\mathfrak{b}) = \deg \operatorname{div}(\mathfrak{b}')$.

Conversely, we see that $\operatorname{div}(\mathfrak{b}(\mathfrak{b}')^{-1})$ must be principal as $\deg \operatorname{div}(\mathfrak{b}(\mathfrak{b}')^{-1}) = 0$. Hence, there exists $h \in K^*$ with $\operatorname{div}(\mathfrak{b}(\mathfrak{b}')^{-1}) = (h^{-1})$; but then $\mathfrak{b}(\mathfrak{b}')^{-1} = h\mathcal{O}_K$ and $\nu_{\mathfrak{p}}(h) = 0$ for all $\mathfrak{p} \in S$, i.e., $\mathfrak{b} \sim \mathfrak{b}'$. □

Proof of Proposition 5.5. For injectivity, assume that $d^{\mathfrak{a}}(\frac{1}{\mu}\mathfrak{a}) = d^{\mathfrak{a}}(\frac{1}{\mu'}\mathfrak{a})$; this means that $\Psi(\mu) - \Psi(\mu') \in \Lambda$. If we choose $\varepsilon \in \mathcal{O}_K^*$ with $\Psi(\varepsilon) = \Psi(\mu) - \Psi(\mu')$, we obtain $|\mu|_{\mathfrak{p}} = |\varepsilon\mu'|_{\mathfrak{p}}$ for every $\mathfrak{p} \in S$. Therefore, $h := \frac{\mu}{\varepsilon\mu'}$ satisfies $|h|_{\mathfrak{p}} = 1$ for all $\mathfrak{p} \in S$, and $h \cdot \frac{1}{\mu}\mathfrak{a} = \frac{1}{\mu'}\varepsilon^{-1}\mathfrak{a} = \frac{1}{\mu'}\mathfrak{a}$, whence $\frac{1}{\mu}\mathfrak{a} \sim \frac{1}{\mu'}\mathfrak{a}$.

To see that $\operatorname{Red}(\mathfrak{a})$ is non-empty, it suffices to show that $\mathfrak{a}$ has at least one minimum. This can be done directly using Riemann's Inequality or Minkowski's Lattice Point Theorem, or one can use tools as the Reduction Lemma 6.6, applied to $(\mathfrak{a}, (0, \ldots, 0))$. It returns a tuple whose first component is the equivalence class of an element in $\operatorname{Red}(\mathfrak{a})$.

In case K is a function field and T is finite, the finiteness of $\operatorname{Red}(\mathfrak{a})/_{\sim}$ follows from the fact that $\mathbb{G}^n/\Lambda$ is finite, since T is isomorphic to a subgroup of $\mathbb{G}^n/\Lambda$ of finite index. If, moreover, k is finite, note that the equivalence class $[\mathfrak{b}]_{\sim}$ of $\mathfrak{b}$ is finite for every $\mathfrak{b}$ since $\mathfrak{b} = f\mathfrak{b}'$ with $|f|_{\mathfrak{p}} = 1$ for all $\mathfrak{p} \in S$ implies $f \in B(\mathfrak{b}, (0, \ldots, 0))$, which is a finite k-vector space and thus also a finite set. Therefore, $\operatorname{Red}(\mathfrak{b})$ is the union of finitely many finite sets.

Finally, in case K is a number field, Remark 6.4 (b) and Proposition 8.1 show that if $\mathfrak{b}$ is a reduced ideal, then $\mathfrak{b}^{-1}$ is an integral ideal with bounded norm. As there are only finitely many of these, $\operatorname{Red}(\mathfrak{a})$ itself is finite. □

Proof of Proposition 6.5. The map is well defined by Remark 6.4 (b). To see that it is injective, note that $k \subseteq B(\mathfrak{b}, (0, \ldots, 0)) \subseteq B(\mathfrak{b}, (t_1, \ldots, t_n, 0)) = k$ for $(\mathfrak{b}, (t_1, \ldots, t_n)) \in \operatorname{Rep}^{f*}(\mathfrak{a})$, whence $\mathfrak{b} \sim \mathfrak{b}'$ for $\mathfrak{b}' \in \operatorname{Red}(\mathfrak{a})$ implies $\mathfrak{b} = \mathfrak{b}'$. Therefore, $[\mathfrak{b}]_{\sim}$ contains exactly one element, whence $([\mathfrak{b}]_{\sim}, (t_1, \ldots, t_n))$ has exactly one preimage.

To see that the map is surjective in the case $\deg \mathfrak{p}_{n+1} = 1$, let $([\mathfrak{b}]_{\sim}, (t_1, \ldots, t_n)) \in \operatorname{Rep}^f(\mathfrak{a})$. Note that $|h|_{\mathfrak{p}_{n+1}} = 1$ for all $h \in B(\mathfrak{b}, (t_1, \ldots, t_n, 0)) \setminus \{0\}$. We can proceed

in a very similar manner as in the proof of Proposition 5.2. In case K is a number field, this shows that $B(\mathfrak{b},(t_1,\dots,t_n,0))=\{-1,0,1\}=k$.

In case K is a function field, $B(\mathfrak{b},(t_1,\dots,t_n,0))=L(D)$ with $D:=\operatorname{div}(\mathfrak{b})+\sum_{i=1}^n t_i\mathfrak{p}_i$, and we know that $L(D-\mathfrak{p}_{n+1})=\{0\}$. As in the proof of Proposition 5.2, we must have $\dim_k L(D)=1$, whence $1\in L(D)$ implies $L(D)=k$.

So in both cases, $B(\mathfrak{b},(t_1,\dots,t_n,0))=k$, whence $(\mathfrak{b},(t_1,\dots,t_n))\in \operatorname{Rep}^{f*}(\mathfrak{a})$ is a preimage of $([\mathfrak{b}]_\sim,(t_1,\dots,t_n))\in\operatorname{Rep}^f(\mathfrak{a})$. □

Proof of Lemma 6.7. As $1\in B(\frac{1}{\mu}\mathfrak{b},(t_1+\nu_{\mathfrak{p}_1}(\mu),\dots,t_n+\nu_{\mathfrak{p}_n}(\mu),0))$, we get $\mu=\mu\cdot 1\in\mu B(\frac{1}{\mu}\mathfrak{b},(t_1+\nu_{\mathfrak{p}_1}(\mu),\dots,t_n+\nu_{\mathfrak{p}_n}(\mu),0))\setminus\{0\}=B(\mathfrak{b},(t_1,\dots,t_n,-\nu_{\mathfrak{p}_{n+1}}(\mu)))\setminus\{0\}$. Hence, μ is minimal in $B(\mathfrak{b},(t_1,\dots,t_n,-\nu_{\mathfrak{p}_{n+1}}(\mu)))\setminus\{0\}$ with respect to $\le$. By the choice of $\le$, it is also minimal in $B(\mathfrak{b},(t_1,\dots,t_n,\max\{0,-\nu_{\mathfrak{p}_{n+1}}(\mu)\}))\setminus\{0\}$; but then, by the same argument, 1 is minimal with respect to $\le$ in the same set. Thus, we get $\mu\le 1\le\mu$, which shows that $|\mu|_{\mathfrak{p}}=1$ for every $\mathfrak{p}\in S$. □

Proof of Theorem 6.8. The second part is Remark 6.4 (b). For the injectivity of $\Phi^{\mathfrak{a}}$, let $A=([\mathfrak{b}]_\sim,(t_1,\dots,t_n)),A'=([\mathfrak{b}']_\sim,(t_1',\dots,t_n'))\in\operatorname{Rep}^f(\mathfrak{a})$ with $\Phi^{\mathfrak{a}}(A)=\Phi^{\mathfrak{a}}(A')$. Write $\mathfrak{b}=\frac{1}{\mu}\mathfrak{a}$ and $\mathfrak{b}'=\frac{1}{\mu'}\mathfrak{a}$. Then there exists $\varepsilon\in\mathcal{O}_K^*$ with $\Psi(\mu)+(t_1,\dots,t_n)=\Psi(\mu')+(t_1',\dots,t_n')+\Psi(\varepsilon)$. Define $\mu'':=\mu^{-1}\mu'\varepsilon$; then $t_i+\nu_{\mathfrak{p}_i}(\mu'')=t_i'$ and $\frac{1}{\mu''}\mathfrak{b}=\mathfrak{b}'$, whence by the Uniqueness Lemma 6.7, we get $A=A'$.

For the surjectivity of $\Phi^{\mathfrak{a}}$, let $(t_1,\dots,t_n)+\Lambda\in\mathbb{G}^n/\Lambda$. Then by the Reduction Lemma 6.6, there exists $\mu\in\mathfrak{a}$ such that $A''=([\frac{1}{\mu}\mathfrak{a}]_\sim,(t_1+\nu_{\mathfrak{p}_1}(\mu),\dots,t_n+\nu_{\mathfrak{p}_n}(\mu)))\in\operatorname{Rep}^f(\mathfrak{a})$. Now $\Phi^{\mathfrak{a}}(A'')=\Psi(\mu)+(t_1+\nu_{\mathfrak{p}_1}(\mu),\dots,t_n+\nu_{\mathfrak{p}_n}(\mu))+\Lambda=(t_1,\dots,t_n)+\Lambda$, as we wanted to show. □

Proof of Proposition 6.9. Write $\mathfrak{b}=\frac{1}{\mu}\mathfrak{a}$ and $\mathfrak{b}'=\frac{1}{\mu'}\mathfrak{a}$. Then $\mathfrak{b}\mathfrak{b}'\mathfrak{a}^{-1}=\frac{1}{\mu\mu'}\mathfrak{a}$ lies in the ideal class of $\mathfrak{a}$. We can now conclude with

$$\begin{aligned}\Phi^{\mathfrak{a}}(C)&=d^{\mathfrak{a}}(\mathfrak{b}\mathfrak{b}'\mathfrak{a}^{-1})+(t_1+t_1',\dots,t_n+t_n')\\&=d^{\mathfrak{a}}(\mathfrak{b})+(t_1,\dots,t_n)+d^{\mathfrak{a}}(\mathfrak{b}')+(t_1',\dots,t_n')=\Phi^{\mathfrak{a}}(A)+\Phi^{\mathfrak{a}}(B).\end{aligned}$$ □

Proof of Theorem 7.1. Clearly, the divisors in the definition of Φ in the number field case are all of degree zero. Hence, one can treat both cases at the same time by ignoring the valuations of the divisors at $\mathfrak{p}_{n+1}$. First, note that the maps are well defined, since if $\mathfrak{b}$ is replaced by $h\mathfrak{b}$ for some $h\in K^*$ with $|h|_{\mathfrak{p}}=1$ for all $\mathfrak{p}\in S$, then $\operatorname{div}(\mathfrak{b})$ is replaced by $\operatorname{div}(\mathfrak{b})-(h)=\operatorname{div}(h\mathfrak{b})$.

To show injectivity, let $A=([\mathfrak{b}]_\sim,(t_1,\dots,t_n))$ and $A'=([\mathfrak{b}']_\sim,(t_1',\dots,t_n'))\in\operatorname{Rep}^f(K)$ with $\Phi(A)=\Phi(A')$, i.e., let $h\in K^*$ and $\ell\in\mathbb{G}$ with

$$\operatorname{div}(\mathfrak{b})+\sum_{i=1}^n t_i\mathfrak{p}_i=\operatorname{div}(\mathfrak{b}')+\sum_{i=1}^n t_i'\mathfrak{p}_i+(h)+\ell\mathfrak{p}_{n+1}.$$

This gives $\frac{1}{h}\mathfrak{b}'=\mathfrak{b}$ and $t_i=t_i'+\nu_{\mathfrak{p}_i}(h)$. But then, $A=([\frac{1}{h}\mathfrak{b}'],(t_1'+\nu_{\mathfrak{p}_1}(h),\dots,t_n'+\nu_{\mathfrak{p}_n}(h)))$, whence by the Uniqueness Lemma 6.7 we get $|h|_{\mathfrak{p}}=1$ for every $\mathfrak{p}\in S$; but this implies $A=A'$. Therefore, Φ is injective.

For surjectivity, let $[D]\in\operatorname{Pic}^0(K)$, respectively, $[D]\in\operatorname{Pic}(K)/\langle[\mathfrak{p}_{n+1}]\rangle$. Write $D=\operatorname{div}(\mathfrak{a})+\sum_{i=1}^n t_i\mathfrak{p}_i+\ell\mathfrak{p}_{n+1}$ for $\mathfrak{a}\in\operatorname{Id}(\mathcal{O}_K)$, $t_1,\dots,t_n,\ell\in\mathbb{G}$. By Reduction Lemma 6.6, there exists a $\mu\in\mathfrak{b}$ such that $B=([\frac{1}{\mu}\mathfrak{a}]_\sim,(t_1+\nu_{\mathfrak{p}_1}(\mu),\dots,t_n+$

$\nu_{\mathfrak{p}_n}(\mu))) \in \mathrm{Rep}^f(K)$, and, up to $\mathfrak{p}_{n+1}$, the divisor in $\Phi(B)$ equals

$$\mathrm{div}\big(\tfrac{1}{\mu}\mathfrak{a}\big) + \sum_{i=1}^{n}(t_i + \nu_{\mathfrak{p}_i}(\mu))\mathfrak{p}_i = \mathrm{div}(\mathfrak{a}) + \sum_{i=1}^{n} t_i\mathfrak{p}_i + (\mu) - \nu_{\mathfrak{p}_{n+1}}(\mu)\mathfrak{p}_{n+1},$$

i.e., $\Phi(B) = [D]$. □

Proof of Proposition 7.2. We first show that the left square commutes. For that, we compare the maps $T \to \mathbb{G}^n/\Lambda \to \mathrm{Rep}^f(\mathcal{O}_K) \to \mathrm{Rep}^f(K) \to \mathrm{Pic}(K)/\mathbb{G}[\mathfrak{p}_{n+1}]$ with $T \to \mathrm{Pic}^0(K) \to \mathrm{Pic}(K)/\mathbb{G}[\mathfrak{p}_{n+1}]$. Let the class of $D = \sum_{i=1}^{n+1} t_i\mathfrak{p}_i$ be an element of T. Then it is mapped to $(t_1, \ldots, t_n) + \Lambda$ in $\mathbb{G}^n/\Lambda$ and to an f-representation $A = ([\frac{1}{\mu}\mathcal{O}_K]_\sim, (t_1', \ldots, t_n')) \in \mathrm{Rep}^f(\mathcal{O}_K)$ such that

$$(*) \qquad \Phi^{\mathcal{O}_K}(A) = \Psi(\mu) + (t_1', \ldots, t_n') + \Lambda = (t_1, \ldots, t_n) + \Lambda.$$

This in turn is mapped to the class of $\mathrm{div}(\frac{1}{\mu}\mathcal{O}_K) + \sum_{i=1}^{n} t_i'\mathfrak{p}_i$ in $\mathrm{Pic}(K)/\mathbb{G}[\mathfrak{p}_{n+1}]$. Hence, we evaluated the class of D along the first composition of maps.

Now D is rationally equivalent to $\sum_{i=1}^{n+1} t_i\mathfrak{p}_i + (\mu)$. The finite part of this divisor is $\mathrm{div}(\frac{1}{\mu}\mathcal{O}_K)$. The valuation of this divisor at $\mathfrak{p}_i$ is $t_i + \nu_{\mathfrak{p}_i}(\mu)$ for $1 \leq i \leq n$, and $(t_i + \nu_{\mathfrak{p}_i}(\mu))_i + \Lambda = (t_i')_i + \Lambda$ by $(*)$. But this means that $[D] = [D - \mu] = [\mathrm{div}(\mathfrak{a}) + \sum_{i=1}^{n} t_i'\mathfrak{p}_i + \ell\mathfrak{p}_{n+1}]$ in $\mathrm{Pic}^0(K)$ for suitable $\ell \in \mathbb{G}$, whence the first square commutes.

To see that the second square commutes, note that if $[D] \in \mathrm{Pic}^0(K)$ with $D = \mathrm{div}(\mathfrak{a}) + \sum_{i=1}^{n+1} t_i\mathfrak{p}_i$, then $[D]$ maps to the ideal class of $\mathfrak{a}$ in $\mathrm{Pic}(\mathcal{O}_K)$. Now the f-representation representing $[D] + \mathbb{G}[\mathfrak{p}_{n+1}]$ can be found by reducing $(\mathfrak{a}, (t_1, \ldots, t_n))$, yielding the ideal part $[\frac{1}{\mu}\mathfrak{a}]_\sim$ for some $\mu \in \mathcal{E}(\mathfrak{a})$. But the resulting f-representation is mapped to the ideal class of $\frac{1}{\mu}\mathfrak{a}$ in $\mathrm{Pic}(\mathcal{O}_K)$, which is the same as the ideal class of $\mathfrak{a}$. Therefore, the second square also commutes.

Finally, in case K is a function field, the equalities for the images of T in $\mathbb{G}^n/\Lambda$ and $\mathrm{Pic}^0(K)$ in $\mathrm{Rep}^f(K)$ follow from the fact that divisors representing elements of T and $\mathrm{Pic}^0(K)$ must have degree zero. □

Proof of Proposition 8.1. Let $D = \mathrm{div}(\mathfrak{a}) + \sum_{i=1}^{n} t_i\mathfrak{p}_i$. Then $B(\mathfrak{a}, (t_1, \ldots, t_n, 0)) = L(D)$ contains k and $L(D - \mathfrak{p}_{n+1}) = B(\mathfrak{a}, (t_1, \ldots, t_n, -\varepsilon)) = 0$ for every $\varepsilon > 0$, $\varepsilon \in \mathbb{G}$. The inclusion shows $D \geq 0$ as $1 \in k$, whence $\mathrm{div}(\mathfrak{a}) \geq 0$ and $t_i \geq 0$, $1 \leq i \leq n$.

If K is a function field of genus g, by Riemann's Inequality,

$$0 = \dim_k L(D - \mathfrak{p}_{n+1}) \geq 1 - g + \deg \mathrm{div}(\mathfrak{a}) + \sum_{i=1}^{n} t_i \deg \mathfrak{p}_i - \deg \mathfrak{p}_{n+1};$$

therefore, $\deg \mathrm{div}(\mathfrak{a}) + \sum_{i=1}^{n} t_i \deg \mathfrak{p}_i \leq g - 1 + \deg \mathfrak{p}_{n+1}$.

If K is a number field with $2s$ complex embeddings and discriminant Δ, we have $B(\mathfrak{a}, (t_1, \ldots, t_n, -\varepsilon)) \neq \{0\}$ for $\varepsilon > 0$ if

$$e^{-\varepsilon \deg \mathfrak{p}_{n+1}} \prod_{i=1}^{n} e^{t_i \deg \mathfrak{p}_i} > \big(\tfrac{2}{\pi}\big)^s \sqrt{|\Delta|}\, \mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{a})$$

by Minkowski's Lattice Point Theorem [Neu99, Theorem 5.3]. Hence, we must have

$$\exp\left(\sum_{i=1}^{n} t_i \deg \mathfrak{p}_i - \varepsilon \deg \mathfrak{p}_{n+1}\right) \leq \big(\tfrac{2}{\pi}\big)^s \sqrt{|\Delta|} e^{-\deg \mathrm{div}(\mathfrak{a})}.$$

Solving for $\deg \operatorname{div}(\mathfrak{a}) + \sum_{i=1}^{n} t_i \deg \mathfrak{p}_i$ and considering that this is true for all $\varepsilon > 0$ yields the claim. □

References

[AO82] H. Appelgate and H. Onishi, *Periodic expansion of modules and its relation to units*, J. Number Theory **15** (1982), no. 3, 283–294. MR680533 (84d:12005)

[BBT94] I. Biehl, J. A. Buchmann, and C. Thiel, *Cryptographic protocols based on discrete logarithms in real-quadratic orders*, Advances in Cryptology - CRYPTO '94, 14th Annual International Cryptology Conference, Santa Barbara, California, USA, August 21-25, 1994, Proceedings (Y. Desmedt, ed.), Lecture Notes in Computer Science, vol. 839, Springer, 1994, pp. 56–60. MR1316402 (95j:94002)

[Ber63] G. Bergmann, *Theorie der Netze*, Mathematische Annalen **149** (1963), 361–418. MR0157948 (28:1176)

[BS05] J. A. Buchmann and A. Schmidt, *Computing the structure of a finite abelian group*, Math. Comp. **74** (2005), no. 252, 2017–2026 (electronic). MR2164109 (2006c:20108)

[Buc85] J. A. Buchmann, *A generalization of Voronoĭ's unit algorithm. I, II*, J. Number Theory **20** (1985), no. 2, 177–209. MR790781 (86g:11062a)

[Buc87a] ———, *On the computation of units and class numbers by a generalization of Lagrange's algorithm*, J. Number Theory **26** (1987), no. 1, 8–30. MR883530 (89b:11104)

[Buc87b] ———, *Zur Komplexität der Berechnung von Einheiten und Klassenzahl algebraischer Zahlkörper*, Habilitationsschrift, October 1987.

[BW88] J. A. 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** (1988), no. 182, 569–579. MR929554 (89g:11098)

[BW90] ———, *A key exchange system based on real quadratic fields (extended abstract)*, Advances in cryptology—CRYPTO '89 (Santa Barbara, CA, 1989), Lecture Notes in Comput. Sci., vol. 435, Springer, New York, 1990, pp. 335–343. MR1062244 (91f:94014)

[CFA+06] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren (eds.), *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2006. MR2162716 (2007f:14020)

[Coh96] H. Cohen, *A course in computational algebraic number theory*, third corrected ed., Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1996. MR1228206 (94i:11105)

[DF64] B. N. Delone and D. K. Faddeev, *The theory of irrationalities of the third degree*, Translations of Mathematical Monographs, Vol. 10, American Mathematical Society, Providence, R.I., 1964. MR0160744 (28:3955)

[Fon08] F. Fontein, *Groups from cyclic infrastructures and Pohlig-Hellman in certain infrastructures*, Adv. Math. Commun. **2** (2008), no. 3, 293–307. MR2429459

[Fon09] F. Fontein, *The infrastructure of a global field and baby step-giant step algorithms*, Ph.D. thesis, Universität Zürich, March 2009, `http://user.math.uzh.ch/fontein/diss-fontein.pdf`.

[GHM08] S. D. Galbraith, M. Harrison, and D. J. Mireles Morales, *Efficient hyperelliptic arithmetic using balanced representation for divisors*, Algorithmic Number Theory, 8th International Symposium, ANTS-VIII, Banff, Canada, May 17-22, 2008 (Berlin) (A. J. van der Poorten and A. Stein, eds.), Lecture Notes in Computer Science, vol. 5011, Springer, 2008, pp. 342–356. MR2467851 (2010f:14024)

[GPS02] S. D. Galbraith, S. M. Paulus, and N. P. Smart, *Arithmetic on superelliptic curves*, Math. Comp. **71** (2002), no. 237, 393–405 (electronic). MR1863009 (2002h:14102)

[Heß99] F. Heß, *Zur Divisorklassengruppenberechnung in globalen funktionenkörpern*, Ph.D. thesis, Technische Universität Berlin, 1999.

[Heß02] F. Heß, *Computing Riemann-Roch spaces in algebraic function fields and related topics*, J. Symbolic Comput. **33** (2002), no. 4, 425–445. MR1890579 (2003j:14032)

[HP85] Y. Hellegouarch and R. Paysant-Le Roux, *Commas, points extrémaux et arêtes des corps possédant une formule du produit*, C. R. Math. Rep. Acad. Sci. Canada **7** (1985), no. 5, 291–296. MR813946 (87m:12011)

[HP87] ———, *Invariants arithmétiques des corps possédant une formule du produit; applications*, Astérisque (1987), no. 147-148, 291–300, 345, Journées arithmétiques de Besançon (Besançon, 1985). MR891435 (88k:11067)

[HP01] D. Hühnlein and S. M. Paulus, *On the implementation of cryptosystems based on real quadratic number fields (extended abstract)*, Selected areas in cryptography (Waterloo, ON, 2000), Lecture Notes in Comput. Sci., vol. 2012, Springer, Berlin, 2001, pp. 288–302. MR1895598

[Jac99] M. J. Jacobson, Jr., *Subexponential class group computation in quadratic orders*, Ph.D. thesis, Technische Universität Darmstadt, 1999.

[JSS07] M. J. Jacobson, Jr., R. Scheidler, and A. Stein, *Cryptographic protocols on real hyperelliptic curves*, Adv. Math. Commun. **1** (2007), no. 2, 197–221. MR2306309 (2008c:94024)

[JSW01] M. J. Jacobson, Jr., R. Scheidler, and H. C. Williams, *The efficiency and security of a real quadratic field based key exchange protocol*, Public-key cryptography and computational number theory (Warsaw, 2000), de Gruyter, Berlin, 2001, pp. 89–112. MR1881630 (2003f:94062)

[JSW06] ———, *An improved real-quadratic-field-based key exchange procedure*, Journal of Cryptology **19** (2006), no. 2, 211–239. MR2213407

[Lan09] E. Landquist, *Infrastructure, Arithmetic, and Class Number Computations in Purely Cubic Function Fields of Characteristic at Least* 5, Ph.D. thesis, University of Illinois at Urbana-Champaign, 2009, `http://www.math.uiuc.edu/~landquis/articles/landquist-thesis.pdf`.

[Len82] H. W. Lenstra, *On the computation of regulators and class numbers of quadratic fields*, Journées Arithmétiques 1980 (Exeter, 13th–19th April 1980) (Cambridge) (J. V. Armitage, ed.), London Mathematical Society Lecture Notes, no. 56, Cambridge University Press, 1982, pp. 123–150.

[LSY03] Y. Lee, R. Scheidler, and C. Yarrish, *Computation of the fundamental units and the regulator of a cyclic cubic function field*, Experiment. Math. **12** (2003), no. 2, 211–225. MR2016707 (2004j:11143)

[Mau00] M. Maurer, *Regulator approximation and fundamental unit computation for real-quadratic orders*, Ph.D. thesis, Technische Universität Darmstadt, 2000.

[MST99] V. Müller, A. Stein, and C. Thiel, *Computing discrete logarithms in real quadratic congruence function fields of large genus*, Math. Comp. **68** (1999), no. 226, 807–822. MR1620235 (99i:11119)

[Neu99] J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999. MR1697859 (2000m:11104)

[PR99] S. M. Paulus and H.-G. Rück, *Real and imaginary quadratic representations of hyperelliptic function fields*, Math. Comp. **68** (1999), no. 227, 1233–1241. MR1627817 (99i:11107)

[PWZ82] M. Pohst, P. Weiler, and H. Zassenhaus, *On effective computation of fundamental units. II*, Math. Comp. **38** (1982), no. 157, 293–329. MR637308 (83e:12005b)

[PZ77] M. Pohst and H. Zassenhaus, *An effective number geometric method of computing the fundamental units of an algebraic number field*, Math. Comp. **31** (1977), no. 139, 754–770. MR0498486 (58:16595)

[PZ82] ———, *On effective computation of fundamental units. I*, Math. Comp. **38** (1982), no. 157, 275–291. MR637307 (83e:12005a)

[Ros02] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002. MR1876657 (2003d:11171)

[SBW94] R. Scheidler, J. A. Buchmann, and H. C. Williams, *A key-exchange protocol using real quadratic fields*, J. Cryptology **7** (1994), no. 3, 171–199. MR1286662 (96e:94015)

[Sch82] R. J. Schoof, *Quadratic fields and factorization*, Computational methods in number theory, Part II, Math. Centre Tracts, vol. 155, Math. Centrum, Amsterdam, 1982, pp. 235–286. MR702519 (85g:11118b)

[Sch01] R. Scheidler, *Ideal arithmetic and infrastructure in purely cubic function fields*, J. Théor. Nombres Bordeaux **13** (2001), no. 2, 609–631. MR1879675 (2002k:11209)

[Sch08] R. J. Schoof, *Computing Arakelov class groups*, MSRI Publications, vol. 44, pp. 447–495, Cambridge University Press, Cambridge, 2008.

[Sha72] D. Shanks, *The infrastructure of a real quadratic field and its applications*, Proceedings of the Number Theory Conference (Univ. Colorado, Boulder, Colo., 1972) (Boulder, Colo.), Univ. Colorado, 1972, pp. 217–224. MR0389842 (52:10672)

[SS98] R. Scheidler and A. Stein, *Unit computation in purely cubic function fields of unit rank 1*, Algorithmic number theory (Portland, OR, 1998) (Berlin), Lecture Notes in Comput. Sci., vol. 1423, Springer, 1998, pp. 592–606. MR1726104 (2000k:11145)

[SSW96] R. Scheidler, A. Stein, and H. C. Williams, *Key-exchange in real quadratic congruence function fields*, Des. Codes Cryptogr. **7** (1996), no. 1-2, 153–174, Special issue dedicated to Gustavus J. Simmons. MR1377761 (97d:94009)

[Ste77] R. Steiner, *On the units in algebraic number fields*, Proceedings of the Sixth Manitoba Conference on Numerical Mathematics (Univ. Manitoba, Winnipeg, Man., 1976) (Winnipeg, Man.), Congress. Numer., XVIII, Utilitas Math., 1977, pp. 413–435. MR532716 (81b:12008)

[Ste92] A. Stein, *Baby step-giant step-Verfahren in reellquadratischen Kongruenzfunktionenkörpern mit Charakteristik ungleich 2*, Diplomarbeit, Universität des Saarlandes, Saarbrücken, 1992.

[Ste97] A. Stein, *Equivalences between elliptic curves and real quadratic congruence function fields*, J. Théor. Nombres Bordeaux **9** (1997), no. 1, 75–95. MR1469663 (98d:11144)

[Sti93] H. Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993. MR1251961 (94k:14016)

[SW98] A. Stein and H. C. Williams, *An improved method of computing the regulator of a real quadratic function field*, Algorithmic number theory (Portland, OR, 1998), Lecture Notes in Comput. Sci., vol. 1423, Springer, Berlin, 1998, pp. 607–620. MR1726105 (2000j:11201)

[SW99] ———, *Some methods for evaluating the regulator of a real quadratic function field*, Experiment. Math. **8** (1999), no. 2, 119–133. MR1700574 (2000f:11152)

[SZ91] A. Stein and H. G. Zimmer, *An algorithm for determining the regulator and the fundamental unit of hyperelliptic congruence function field*, Proceedings of the 1991 International Symposium on Symbolic and Algebraic Computation, ISSAC '91, Bonn, Germany, July 15-17, 1991, Association for Computing Machinery, 1991, pp. 183–184.

[Thi95] C. Thiel, *Short proofs using compact representations of algebraic integers*, J. Complexity **11** (1995), no. 3, 310–329. MR1349260 (96d:11142)

[Vol03] U. Vollmer, *Rigorously analyzed algorithms for the discrete logarithm problem in quadratic number fields*, Ph.D. thesis, Technische Universität Darmstadt, 2003.

[Wil85] H. C. Williams, *Continued fractions and number-theoretic computations*, Rocky Mountain J. Math. **15** (1985), no. 2, 621–655, Number theory (Winnipeg, Man., 1983). MR823273 (87h:11129)

[WW87] H. C. Williams and M. C. Wunderlich, *On the parallel generation of the residues for the continued fraction factoring algorithm*, Math. Comp. **48** (1987), no. 177, 405–423. MR866124 (88i:11099)

Department of Mathematics and Statistics, University of Calgary, 2500 University Drive NW, Calgary, Alberta, Canada T2N 1N4

Current address: Institut für Mathematik, Universität Zürich, Winterthurerstrasse 190, 8057 Zürich, Switzerland

E-mail address: felix.fontein@math.uzh.ch