# Abstract Infrastructures of Unit Rank Two

University of Zurich

**Felix Fontein**

Institut für Mathematik, Universität Zürich

## 1. Why Infrastructures?

- Infrastructures can be used for **computation of fundamental units** and regulator (see below);
- Infrastructures can be used for **public key cryptography**, for example for key exchange [JSS07].

In the following, we will describe what an infrastructure is (in general) and describe Voronoĭ's algorithm for computing fundamental units (in unit rank two).

## 2. Infrastructures from Global Fields

Let $K$ be a **global field**:

- either $K$ is a number field; in that case, let $S$ denote the set of archimedean places of $K$;
- or $K$ is a function field with a finite field of constants $\mathbb{F}_q$; in that case, write $K = \mathbb{F}_q(x, y)$ with $K/\mathbb{F}_q(x)$ being a finite separable extension and let $S$ be the set of poles of $x$.

Write $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$. For every place $\mathfrak{p} \in S$, we have its **degree** $\deg \mathfrak{p}$ and an associated **absolute value** $|\bullet|_\mathfrak{p}$:

- if $\mathfrak{p}$ is an archimedean place, let $\sigma : K \to \mathbb{C}$ be an associated embedding. Then

$$\deg \mathfrak{p} = \begin{cases} 1 & \text{if } \sigma(K) \subseteq \mathbb{R}, \\ 2 & \text{otherwise,} \end{cases} \quad \text{and} \quad |f|_\mathfrak{p} = |\sigma(f)|;$$

- if $\mathfrak{p}$ is a non-archimedean place, let $\nu_\mathfrak{p} : K^* \to \mathbb{Z}$ denote the normalized valuation for $\mathfrak{p}$, $\mathcal{O}_\mathfrak{p}$ the valuation ring and $\mathfrak{m}_\mathfrak{p}$ the valuation ideal. Then

$$\deg \mathfrak{p} = [\mathcal{O}_\mathfrak{p}/\mathfrak{m}_\mathfrak{p} : \mathbb{F}_q] \quad \text{and} \quad |f|_\mathfrak{p} = q^{-\nu_\mathfrak{p}(f) \cdot \deg \mathfrak{p}}.$$

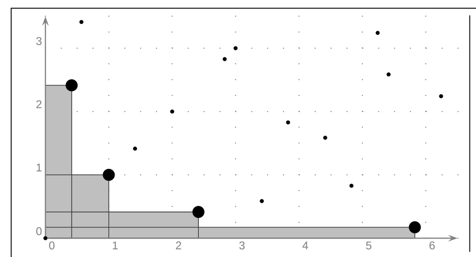
Let $\mathcal{O}$ denote the ring of integers (i.e. the integral closure of $\mathbb{Z}$ resp. $\mathbb{F}_q(x)$); then its **unit group** $\mathcal{O}^*$ is the direct product of the group of roots of unity, denoted by $k^*$, and a free abelian group of rank $|S| - 1$. Consider the map

$$\Phi : K \to \mathbb{R}^n_{\geq 0}, \qquad f \mapsto (|f|_{\mathfrak{p}_i})_i.$$

The image of $\mathcal{O}$ under this map is a discrete set. We say that an element $\mu \in \mathcal{O} \setminus \{0\}$ is a **minimum** of $\mathcal{O}$ if, for every $f \in \mathcal{O}$,

$$|f|_\mathfrak{p} \leq |\mu|_\mathfrak{p} \text{ for all } \mathfrak{p} \in S$$

implies $f = 0$ or $|f|_\mathfrak{p} = |\mu|_\mathfrak{p}$ for all $\mathfrak{p} \in S$.



Here, $K = \mathbb{Q}(\sqrt{2})$. The big dots mark the visible minima of $\mathcal{O} = \mathbb{Z}[\sqrt{2}]$.

Let $\mathcal{E}(\mathcal{O})$ denote the set of all minima and let $\sim$ denote the equivalence relation

$$\mu \sim \mu' :\Longleftrightarrow \forall \mathfrak{p} \in S : |\mu|_\mathfrak{p} = |\mu'|_\mathfrak{p}.$$

Let $[\mu]_\sim \in \mathcal{E}(\mathcal{O})/\sim$ and $\mathfrak{p} \in S$. Then we define the **baby step** of $[\mu]_\sim$ in $\mathfrak{p}$-direction as follows: consider the set

$$X = \left\{ f \in \mathcal{O} \;\middle|\; \begin{array}{l} \forall \mathfrak{q} \in S \setminus \{\mathfrak{p}\} : |f|_\mathfrak{q} \leq |\mu|_\mathfrak{q} \\ \exists \mathfrak{q} \in S \setminus \{\mathfrak{p}\} : |f|_\mathfrak{q} < |\mu|_\mathfrak{q} \end{array} \right\}.$$

On $X/\sim$ with $\mathfrak{p} = \mathfrak{p}_i$, consider the total order

$$[f]_\sim \leq_i [g]_\sim :\Longleftrightarrow \begin{array}{r} (|f|_{\mathfrak{p}_i}, \dots, |f|_{\mathfrak{p}_n}, |f|_{\mathfrak{p}_1}, \dots, |f|_{\mathfrak{p}_{i-1}}) \\ \leq_{\ell ex} (|g|_{\mathfrak{p}_i}, \dots, |g|_{\mathfrak{p}_n}, |g|_{\mathfrak{p}_1}, \dots, |g|_{\mathfrak{p}_{i-1}}), \end{array}$$

where $\leq_{\ell ex}$ is the usual lexicographic order on $\mathbb{R}^n$. One has that $X/\sim$ contains a minimum with respect to $\leq_i$; we denote this minimum by $\mathrm{bs}_\mathfrak{p}([\mu]_\sim)$ and call it the **baby step of $[\mu]_\sim$ in $\mathfrak{p}$-direction**.

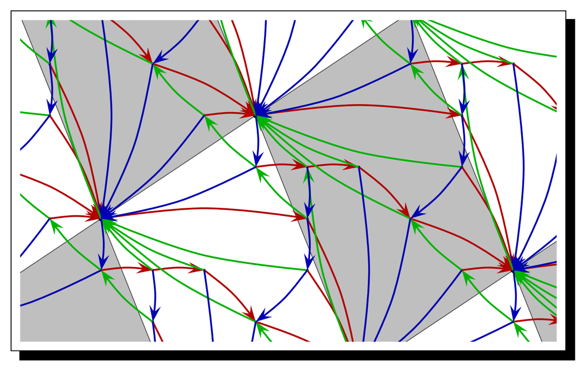
The set $\mathcal{E}(\mathcal{O})$ together with the function $\Phi$, the equivalence relation $\sim$, the action of $\mathcal{O}^*$, and the baby steps $\mathrm{bs}_\mathfrak{p}$, $\mathfrak{p} \in S$, is called the **infrastructure** of $K$.

**Proposition.** *(See, for example, [Fon08b, Fon08a].)*

1. *Assume that $\deg \mathfrak{p} = 1$ for some $\mathfrak{p} \in S$. Then, for all $\mu, \mu' \in \mathcal{E}(\mathcal{O})$, $\mu \sim \mu'$ if, and only if, $\frac{\mu}{\mu'} \in k^*$.*
2. *The unit group $\mathcal{O}^*$ acts on $\mathcal{E}(\mathcal{O})$ by multiplication, and the number of orbits is finite.*
3. *The map $\mu \mapsto \frac{1}{\mu}\mathcal{O}$ induces a bijection between $\mathcal{E}(\mathcal{O})/\mathcal{O}^*$ and the set of **reduced principal ideals**.*

In the following, we will visualize $\mathcal{E}(\mathcal{O})/\sim$, $\mathcal{O}^*$ and the baby steps as follows. If $S = \{\mathfrak{p}_1, \dots, \mathfrak{p}_n\}$, consider the map

$$\Psi : K^* \to \mathbb{R}^{n-1}, \qquad f \mapsto (\log |f|_{\mathfrak{p}_1}, \dots, \log |f|_{\mathfrak{p}_{n-1}}).$$



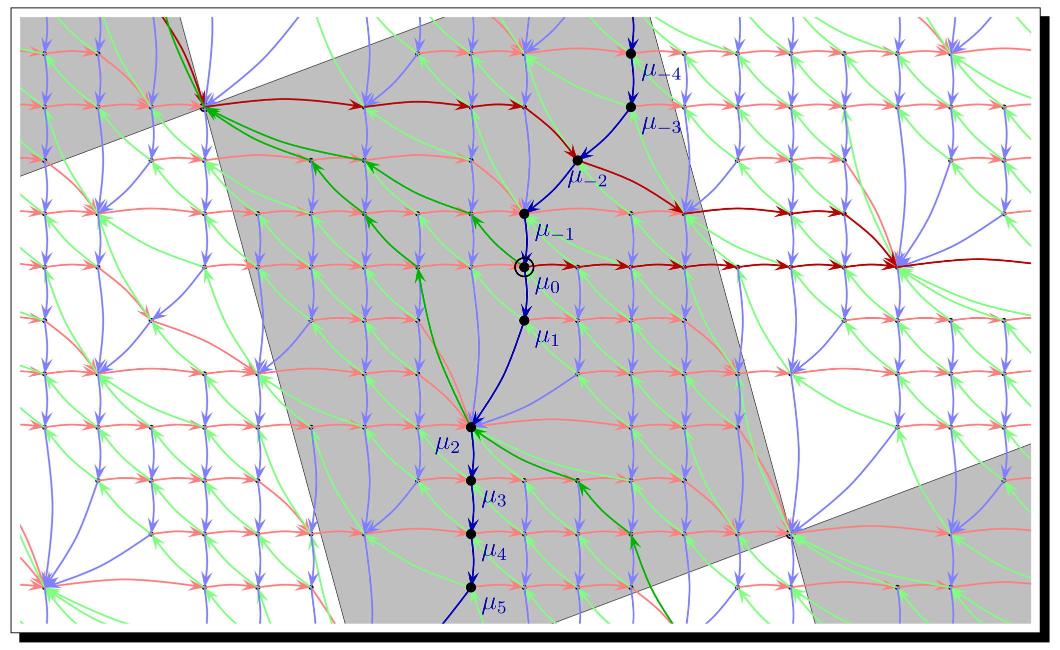
We have that $\Psi(\mathcal{O}^*) \subseteq \mathbb{R}^{n-1}$ is a lattice and that $\Psi$ is injective on $\mathcal{E}(\mathcal{O})/\sim$. In the following, we will always display $\Psi(\mathcal{E}(\mathcal{O}))$ together with $\Psi(\mathcal{O}^*)$, where every second translate of the fundamental mesh of $\Psi(\mathcal{O}^*)$ is marked. Moreover, the baby steps in the different directions will be drawn with different colors. In the example displayed here, $|S| = 3$. The arrows denote baby steps: red baby steps go in the $\mathfrak{p}_1$-direction, green baby steps in the $\mathfrak{p}_2$-direction, and blue baby steps in the $\mathfrak{p}_3$-direction.

## 3. Voronoĭ's Algorithm

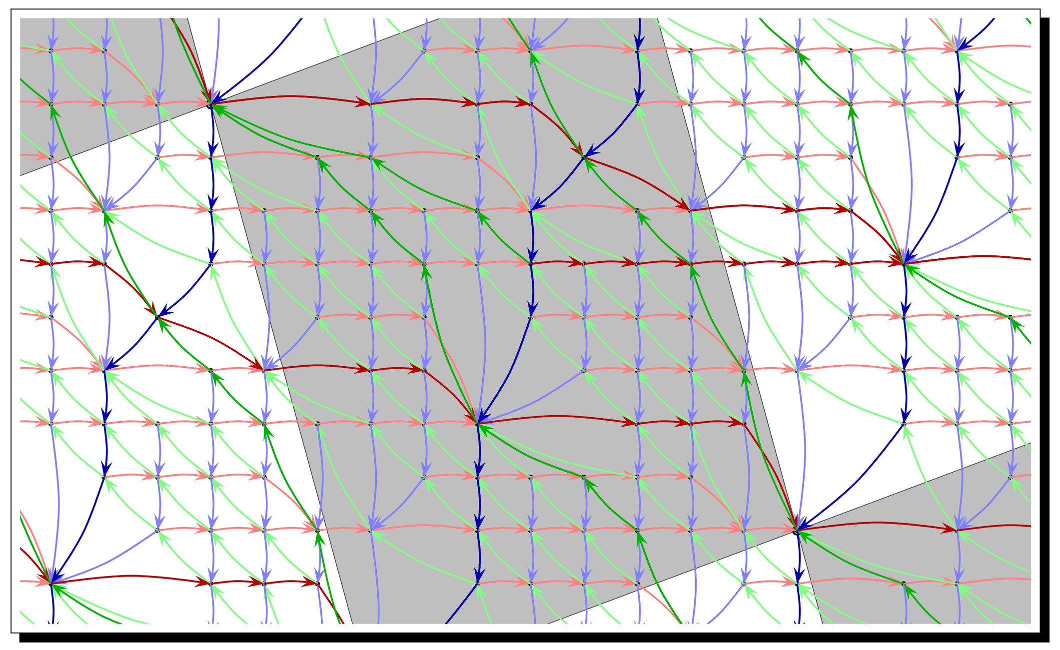
In this section, we will explain Voronoĭ's algorithm, as it has been described in [Buc85] and [LSY03]. **We assume that** $|S| = 3$. Then $\mathcal{O}^* = k^* \oplus \langle \varepsilon_1, \varepsilon_2 \rangle$ for two non-constant independent units $\varepsilon_1, \varepsilon_2 \in \mathcal{O}^*$. The aim is to compute $\varepsilon_1$ and $\varepsilon_2$. Moreover, we assume that $\deg \mathfrak{p}' = 1$ for some $\mathfrak{p}' \in S$ for simplicity.

Let $\mu \in \mathcal{E}(\mathcal{O})$. Then, for $\mathfrak{p} \in S$ the sequence defined by $\mu_0 := \mu$ and $\mu_{n+1} := \mathrm{bs}_\mathfrak{p}(\mu_n)$, $n \in \mathbb{N}$ will get periodic in $\mathcal{E}(\mathcal{O})/\mathcal{O}^*$. The sequence is called a **(one-sided Voronoĭ) chain**. By working with the reduced principal ideals $\frac{1}{\mu_n}\mathcal{O}$ instead of $\mu_n$ and storing all of them until we found minimal $m, n \in \mathbb{N}$ with $0 \leq n < m$ and $\mu_n^{-1}\mathcal{O} = \mu_m^{-1}\mathcal{O}$, we obtain the pre-period $n$ and the period $m - n$ of the sequence $(\mathcal{O}^*\mu_i)_i$. Moreover, $\varepsilon_1 := \frac{\mu_m}{\mu_n} \in \mathcal{O}^*$.

If we replace $\mu$ by $\mu_n$, we get a chain with pre-period $n = 0$. In that case, we can extend $(\mu_i)_{i \in \mathbb{N}}$ to a **two-sided (Voronoĭ) chain** $(\mu_i)_{i \in \mathbb{Z}}$ by setting $\mu_{km+\ell} = \varepsilon^k \mu_\ell$ for $k \in \mathbb{Z}$, $\ell \in \{0, \dots, m-1\}$. Consider the following example:




The pre-period for the blue direction is trivial (i.e. zero), while the pre-period for the other two directions is non-trivial. If we plot the translates of the chains by the unit group $\mathcal{O}^*$, we obtain the following situation:



Then we begin with $\mu' := \mu_n$ and choose $\mathfrak{q} \in S \setminus \{\mathfrak{p}\}$ such that $|\varepsilon_1|_\mathfrak{q} \neq 1$; by the product formula, such an $\mathfrak{q}$ exists. In our example above, the unit obtained from the blue chain satisfies this both for $\mathfrak{q} = \mathfrak{p}_1$ and $\mathfrak{q} = \mathfrak{p}_2$.

We consider the one-sided chain $\mu'_0 := \mu'$, $\mu'_{i+1} := \mathrm{bs}_\mathfrak{q}(\mu'_i)$, $i \in \mathbb{N}$. If we find the minimal $j \in \mathbb{N}$, $j > 0$ such that $\mu'_j$ lies on a translate of the chain $(\mu_i)_{i \in \mathbb{N}}$, i.e. there exists a $k \in \{0, 1, \dots, m-1\}$ with $\mu_k^{-1}\mathcal{O} = (\mu'_j)^{-1}\mathcal{O}$, then $\varepsilon_2 := \mu'_j/\mu_k \in \mathcal{O}^*$ and $\mathcal{O}^* = k^* \oplus \langle \varepsilon_1, \varepsilon_2 \rangle$ (see [Buc85, LSY03]).

In our example, both for $\mathfrak{q} = \mathfrak{p}_1$ and $\mathfrak{q} = \mathfrak{p}_2$ the chain $(\mu'_i)_{i \in \mathbb{N}}$ eventually meets a translate of the blue chain, as one can see in the picture above.

## 4. Regulator, Runtime and Outlook

The **regulator** $R$ of $\mathcal{O}$ is (up to constants) the area of a fundamental mesh of $\Phi(\mathcal{O}^*)$. Hence, this algorithm has a running time of $\mathcal{O}(R)$ baby steps and needs a storage of $\mathcal{O}(R)$.

In the case $|S| = 2$, D. Shanks introduced **giant steps** and applied his baby step-giant step algorithm, which needs $\mathcal{O}(\sqrt{R})$ baby and giant steps and $\mathcal{O}(\sqrt{R})$ storage. Therefore, one can ask:

Q1) How can giant steps be generalized to the case $|S| > 2$?

And more generally:

Q2) Can one find an algorithm which computes $\mathcal{O}^*$ in $\mathcal{O}(\sqrt{R})$ steps and using $\mathcal{O}(\sqrt{R})$ storage for $|S| = 2$?

## References

[Buc85] J. A. Buchmann. A generalization of Voronoi's unit algorithm I, II. *J. Number Theory*, 20:177–209, 1985.

[Fon08a] F. Fontein. The infrastructure of a global field of arbitrary unit rank. In preparation.

[Fon08b] F. Fontein. The infrastructure of a global field of unit rank one, 2008. In preparation.

[JSS07] M. J. Jacobson, Jr., R. Scheidler, and A. Stein. Cryptographic protocols on real hyperelliptic curves. *Adv. Math. Commun.*, 1(2):197–221, 2007.

[LSY03] Y. Lee, R. Scheidler, and C. Yarrish. Computation of the fundamental units and the regulator of a cyclic cubic function field. *Exp. Math.*, 12:211–225, 2003.

Eighth Algorithmic Number Theory Symposium ANTS-VIII, May 17-22, 2008, Banff Centre, Banff, Alberta (Canada)