Computing in arithmetic groups with Voronoï's algorithm

Renaud Coulangeon[1], Gabriele Nebe[2], Oliver Braun[3], and Sebastian Schönnenbeck[4]

[1]Univ. Bordeaux, IMB, UMR 5251,F-33400 Talence, France, CNRS, IMB, UMR 5251, F-33400 Talence, France, renaud.coulangeon@math.u-bordeaux1.fr
[2,3,4]Lehrstuhl D für Mathematik, RWTH Aachen University, 52056 Aachen, Germany, nebe@math.rwth-aachen.de

January 7, 2015

Abstract

We describe an algorithm, meant to be very general, to compute a presentation of the group of units of an order in a (semi)simple algebra over $\mathbb{Q}$. Our method is based on a generalisation of Voronoï's algorithm for computing perfect forms, combined with Bass-Serre theory. It differs essentially from previously known methods to deal with such questions, *e.g.* for units in quaternion algebras. We illustrate this new algorithm by a series of examples where the computations are carried out completely.

KEYWORDS: unit groups of orders; generators; presentation; word problem; lattices; Voronoï's algorithm;

1 Introduction

Let Λ be an order in a (semi-)simple finite dimensional algebra A over $\mathbb{Q}$. By definition, this means that Λ is a subring of A and that, additively, it is a free abelian group generated by a basis of A over $\mathbb{Q}$. Its unit group $\Lambda^\times$, that is the set of elements of Λ that have a multiplicative inverse in Λ, is the most basic example of an arithmetic group. However, a large variety of arithmetic groups can be obtained in this way (for instance, units of group rings over $\mathbb{Z}$ belong to this category). The study of such groups is consequently of major interest .

The easiest and most classical case, where $A = K$ a number field, is fully understood due to *Dirichlet's unit theorem*: in that case, $\Lambda^\times$ is, up to its torsion part, a finitely generated free abelian group, and efficient algorithms exist to compute a set of its generators. In the non-commutative case, the determination of $\Lambda^\times$ is a very difficult task, both from the theoretical and computational point of view, and many questions remain open, as regards structural results and algorithms. We refer the reader to Ernst Kleinert's survey [Kle94] for more details.

In this paper we propose a method, meant to be very general, to compute a presentation of $\Lambda^\times$. This method is based on a combination of Voronoï theory of perfect quadratic forms and Bass-Serre theory of graphs of groups. The latter is well-known to provide a very versatile tool for computing a presentation of a group Γ acting on a connected graph X. In such a situation, a good knowledge of the quotient graph $\Gamma\backslash X$ yields virtually all the information on Γ. To be more precise, one has the following fundamental exact sequence ([Bas93, Theorem 3.6])

$$1 \longrightarrow \pi_1(X) \longrightarrow \pi_1(\Gamma\backslash\backslash X) \longrightarrow \Gamma \longrightarrow 1 \tag{1}$$

where $\pi_1(X)$ (resp. $\pi_1(\Gamma\backslash\backslash X)$) denotes the fundamental group of the graph X (resp. of the quotient graph of groups $\Gamma\backslash\backslash X$), see *loc. cit.* for precise definitions. From this exact sequence, one can derive, at least in principle, a presentation of the group Γ. Of course, to be of any practical interest, the exact sequence (1) must be applied in a context where the fundamental groups $\pi_1(X)$ and $\pi_1(\Gamma\backslash\backslash X)$ are computable as easily as possible, without too much prior knowledge of the structure of Γ. The idea of using Bass-Serre theory in this context dates back to Swan's fundamental paper [Swa71], where he develops an algorithm to compute generators and relations for Bianchi groups using the action on binary Hermitian forms. From a more computational point of view a similar method has been implemented by Riley [Ril83] in Fortran to obtain presentations of 30 Bianchi groups.

The graph on which we will let $\Gamma = \Lambda^\times$ act is built as a neighbouring graph of "perfect forms", where we use a suitable refinement of the original notion of perfect forms in [Vor07]. The action on perfect forms was first applied by Soulé in [Sou78] to derive the explicit structure of $SL_3(\mathbb{Z})$ as an amalgamated product of small finite groups. Later, Opgenorth [Opg01] applied the same kind of ideas to compute the integral normalizer Γ of a finite unimodular group, where he only used the surjectivity of the map $\pi_1(\Gamma\backslash\backslash X) \longrightarrow \Gamma$, which already allows for the computation of a generating set of Γ. Opgenorth's methods have been applied in [Brü98] to compute generators for unit groups $\Gamma = \mathbb{Z}G^\times$ of integral group rings for small groups G. Yasaki [Yas10] used similar ideas, combined with Macbeath theorem [Mac64] to obtain a presentation of some Bianchi groups. Here, we propose to use the full strength of (1) to actually get a presentation of Γ. From the exact sequence (1), we see that this amounts essentially to computing the fundamental group of the neighbouring graph of perfect forms, which is non-trivial in general (the graph is not a tree). There are several ways to do this. We choose to view the neighboring relation on perfect forms not only as a graph but as the 1-skeleton of a CW-complex (the well-rounded retract W, see Section 3). For groups acting on such complexes, there is a slightly refined version of Bass-Serre theory, due to K.-S. Brown (see [Bro84]), which allows one to obtain a presentation of the group which involves only the 2-skeleton of W. Beside the geometry of this complex, our algorithm only involves the computation of the stabilizers of some vertices or edges as well as "side-pairing" transformations. All these computations essentially reduce to isometry testing of lattices and do not require any a priori knowledge of $\Lambda^\times$. Most of them are performed using the Plesken-Souvignier algorithm [PS97] implemented in MAGMA [BCP97].

For sake of simplicity, we chose to develop the theory for simple algebras over $\mathbb{Q}$. The case of semisimple algebras requires only slight modifications.

In some special cases, *e.g.* Bianchi groups or units of quaternion algebras, there are well-known methods based on an action of the relevant group on some *hyperbolic space* (see *e.g.* [CJLdR04]) for computing presentations. Our method applies in these cases too, and should be compared to the aforementioned ones, from which they differ essentially in that we use an action on a *Euclidean space*. The action on hyperbolic space has the advantage that the group respects the metric and hence the volume of a fundamental domain is well defined. Experiments show that our method seems to be faster and therefore allows the computation of more complicated examples. More important: our method applies to more general finite dimensional rational algebras, such as division algebras of degree 3, where no methods to compute Λ^* have been known before ([Kle00, Chapter 7]).

The paper is structured as follows: in Sections 2 and 3, we define a certain space of "quadratic forms" acted on by the unit group $\Gamma = \Lambda^\times$ we want to study, and review some rather classical material about Voronoï's algorithm and the *"well-rounded retract"* in this context. In Section 4 we explain how to use Bass-Serre theory to obtain a presentation of Γ. We also show in Section 5 how the previous idea can be used to solve the word problem in Γ. In Section 6, a selection of examples of applications of our method is presented. The final section provides an outline of the implementation of the algorithm.

2 Preliminaries

2.1 Lattices

Let $A = M_n(K)$ be a finitely generated simple algebra over $\mathbb{Q}$, where K is a skew field with center k and $M_n(K)$ denotes the set of $n \times n$-matrices. Let $V = K^n$ be the simple left A-module. Then $K = \mathrm{End}_A(V)$ and we view V as a right K-module.

Let Λ be an order in A, and $\Lambda^\times$ its group of units. We fix some left Λ-lattice L in V and let $\mathcal{O} := \mathrm{End}_\Lambda(L)$. Then $\mathcal{O}$ is an order in K and L is a right $\mathcal{O}$-lattice. Put

$$\mathfrak{M} := \mathrm{End}_{\mathcal{O}}(L) = \{M \in M_n(K) \mid ML \subset L\}.$$

If $\mathcal{O}$ is a maximal order, then also $\mathfrak{M}$ is maximal, but for arbitrary orders Λ in division algebras $A = K$, one may always choose $L = \Lambda$ to achieve $\mathcal{O} = \Lambda$ and $\Lambda = \mathfrak{M} = \mathrm{End}_\Lambda(\Lambda)$. In general $\Lambda \subseteq \mathfrak{M}$ is of finite index and also its unit group

$$\Lambda^\times = \mathrm{Stab}_{\mathfrak{M}^\times} \Lambda = \{a \in \mathfrak{M}^\times \mid a\Lambda = \Lambda\}.$$

has finite index in

$$\mathfrak{M}^\times = \mathrm{GL}(L) = \{a \in M_n(K) \mid aL = L\}.$$

As the Voronoï algorithm is designed to work with endomorphism rings of lattices, it is more efficient to compute $\mathfrak{M}^\times$ first and retrieve $\Lambda^\times$ by orbit stabiliser routines. Nevertheless we try to develop the theory, as much as possible, without the assumption that Λ is the endomorphism ring of a lattice.

2.2 Forms

As explained in the introduction, we want to let the group $\Lambda^\times$ act on a space of "forms" associated to the algebra A. To that end, we first extend the scalars to $\mathbb{R}$, and obtain a semi-simple real algebra

$$A_{\mathbb{R}} := A \otimes_{\mathbb{Q}} \mathbb{R} = M_n(K_{\mathbb{R}}).$$

Let d denote the degree of K, so $d^2 = \dim_k(K)$, and let

$\iota_1, \ldots, \iota_s$	be the real places of k that ramify in K,
$\sigma_1, \ldots, \sigma_r$	the real places of k that do not ramify in K
$\tau_1, \ldots, \tau_t$	the complex places of k.

Then

$$K_{\mathbb{R}} := K \otimes_{\mathbb{Q}} \mathbb{R} \cong \bigoplus_{i=1}^{s} M_{d/2}(\mathbb{H}) \oplus \bigoplus_{i=1}^{r} M_d(\mathbb{R}) \oplus \bigoplus_{i=1}^{t} M_d(\mathbb{C})$$

and

$$A_{\mathbb{R}} \cong \bigoplus_{i=1}^{s} M_{nd/2}(\mathbb{H}) \oplus \bigoplus_{i=1}^{r} M_{nd}(\mathbb{R}) \oplus \bigoplus_{i=1}^{t} M_{nd}(\mathbb{C}). \tag{2}$$

Note that d is even whenever $s > 0$. The case of Bianchi groups corresponds to $d = 1$, $n = 2$, $s = r = 0$ and $t = 1$, so $K = k$ is an imaginary quadratic field and $A = M_2(K)$. The “canonical” involution * (depending on the choice of this isomorphism) is defined on any simple summand of $K_{\mathbb{R}}$ to be transposition for $M_d(\mathbb{R})$, transposition and complex (respectively quaternionic) conjugation for $M_d(\mathbb{C})$ and $M_{d/2}(\mathbb{H})$. The resulting involution on $K_{\mathbb{R}}$ is again denoted by *. As usual it defines a mapping $^\dagger : M_{m,n}(K_{\mathbb{R}}) \to M_{n,m}(K_{\mathbb{R}})$ by applying * to the entries and then transposing the $m \times n$-matrices. In particular this defines an involution † on $A_{\mathbb{R}} = M_n(K_{\mathbb{R}})$. Though in certain cases (e.g. for Bianchi groups or certain quaternion algebras over totally complex fields) we may choose † such that $A^\dagger = A$, this will not be the case in general.

Definition 2.1. $\Sigma := \mathrm{Sym}(A_{\mathbb{R}}) := \left\{F \in A_{\mathbb{R}} \mid F^\dagger = F\right\}$ is the $\mathbb{R}$-linear subspace of symmetric elements of $A_{\mathbb{R}}$. It supports the positive definite inner product

$$\langle F_1, F_2 \rangle := \mathrm{tr}(F_1 F_2)$$

where $\mathrm{tr} = \mathrm{tr}_{A_{\mathbb{R}}/\mathbb{R}}$ is the reduced trace of the semi-simple $\mathbb{R}$-algebra $A_{\mathbb{R}}$. Each element of Σ can be identified, via (2), with a tuple $(q_1, \ldots, q_s, f_1, \ldots, f_r, h_1, \ldots, h_t)$ of symmetric (resp hermitian) matrices. Then, one can define the open real cone $\mathscr{P}$ of positive elements in Σ as

$$\mathscr{P} = \mathrm{Sym}(A_{\mathbb{R}})_{>0} := \left\{(q_1, \ldots, q_s, f_1, \ldots, f_r, h_1, \ldots, h_t) \in \Sigma \mid q_i, f_j, h_k \text{ pos. def.}\right\}.$$

The closure of $\mathscr{P}$ in Σ is denoted by $\overline{\mathscr{P}}$.

Recall that $V = K^n$ is the simple left A-module. Any $F \in \Sigma$ defines a quadratic form on $V_{\mathbb{R}}$ by

$$F[x] := \langle F, xx^\dagger \rangle \in \mathbb{R} \text{ for all } x \in V_{\mathbb{R}}.$$

This quadratic form is positive definite (resp. positive semidefinite) if and only if $F \in \mathscr{P}$ (resp. $F \in \overline{\mathscr{P}}$).

The group $\mathrm{GL}_n(K)$ acts on Σ by

$$(F, g) \mapsto g^\dagger F g \tag{3}$$

where we embed A into $A_\mathbb{R}$ to define the multiplication. This action preserves the cone $\mathscr{P}$.

2.3 Minimal vectors and Voronoï domains

As before we choose a left Λ-lattice L in the simple A-module $V = K^n$ and put $\mathfrak{M} := \mathrm{End}_\mathscr{O}(L)$ (where $\mathscr{O} := \mathrm{End}_\Lambda(L)$). Then $\mathfrak{M}$ is an order in A that contains Λ of finite index.

The L-minimum of a form $F \in \mathscr{P}$ is defined as

$$\min_L(F) := \min_{\ell \in L - \{0\}} F[\ell]$$

and the set of L-minimal vectors of F as

$$S_L(F) := \{\ell \in L \mid F[\ell] = \min_L(F)\}.$$

The L-Voronoï domain of F (or simply Voronoï domain of F, if there is no ambiguity on the underlying lattice L) is defined as

$$D_F := \left\{ \sum_{x \in S_L(F)} \lambda_x x x^\dagger, \lambda_x \geq 0 \right\} \subset \overline{\mathscr{P}},$$

the closed convex hull of the rays $\mathbb{R}_{\geq 0} x x^\dagger$ as x ranges over $S_L(F)$.

The Voronoï polyhedron Ω is defined as the closed convex hull of the rays $\mathbb{R}_{\geq 0} x x^\dagger$ as x ranges over V.

Definition 2.2. A form $F \in \mathscr{P}$ is L-perfect (or simply perfect if there is no ambiguity on the underlying lattice) if one the following equivalent conditions holds

1. The forms $xx^\dagger$, where x ranges over $S_L(F)$, span the whole space Σ.

2. The L-Voronoï domain of F has non-empty interior.

The Voronoï domain D_F of a perfect form $F \in \mathscr{P}$ is thus an N-dimensional polyhedral cone in the Euclidean space Σ, where $N = \dfrac{nd}{2}\,(nd\,[k:\mathbb{Q}] + r - s)$ is the dimension of Σ. It has finitely many facets, i.e. codimension 1 faces. To each facet $\mathscr{F}$ one associates a *direction* H, that is a normal facet vector, pointing towards the interior of D_F. In other words, $0 \neq H \in \Sigma$ is a direction of D_F if:

- $\langle H, xx^\dagger \rangle \geq 0$ for all $x \in S_L(F)$,

- the forms $xx^\dagger$, as x ranges over the set of minimal vectors of L such that $\langle H, xx^\dagger \rangle = 0$, generate a hyperplane of Σ .

The following lemma is at the core of Voronoï theory :

Lemma 2.3. *Let F be a perfect form $F \in \mathscr{P}$, and H a direction of its Voronoï domain. Then there exists a well-defined positive real number λ such that $F + \lambda H$ is perfect, and the Voronoï domains of F and $F + \lambda H$ share a common facet.*

Proof. This follows from [Opg01, Proposition 1.8] and its proof. In particular, the real number λ can be defined as

$$\lambda = \sup\{\theta \in \mathbb{R}_{>0} \mid F + \theta H \in \mathscr{P} \text{ and } \min_L(F + \theta H) = \min_L(F)\}. \tag{4}$$

The only thing to check is that $\lambda < +\infty$, which amounts to proving that $H \notin \overline{\mathscr{P}}$ (see [Mar03, Proposition 13.1.8] or the discussion following [Opg01, Proposition 1.8]). Assume by way of contradiction that H is positive. Then its kernel (the set of $x \in V_{\mathbb{R}}$ such that $Hx = 0$) coincides with its radical (the set of $x \in V_{\mathbb{R}}$ such that $H[x] = 0$), and contains the set $S(\mathscr{F})$ of minimal vectors $x \in L$ whose image $xx^\dagger$ in Σ generate the facet $\mathscr{F}$ corresponding to H. So these vectors span a K-subspace of dimension at most $n-1$ of K^n, since otherwise H would be zero, which means that there exists $0 \neq y \in K^n$ such that

$$y^\dagger x = 0 \text{ for all } x \in S(\mathscr{F}). \tag{5}$$

This implies, in particular, that n is at least 2 (there is at least one element in the set of minimal vectors belonging to this facet). Finally, the matrices $xx^\dagger$, $x \in S(\mathscr{F})$, generate a subset of dimension at most $N - n$ of Σ : indeed each of the n columns of

$$xx^\dagger = \begin{pmatrix} x_1 x_1^* & x_1 x_2^* & \cdots & x_1 x_n^* \\ x_2 x_1^* & x_2 x_2^* & \cdots & x_2 x_n^* \\ \vdots & \vdots & & \vdots \\ x_n x_1^* & x_n x_2^* & \cdots & x_n x_n^* \end{pmatrix}$$

lies in the hyperplane determined by (5). This yields a contradiction since $N - n < N - 1$. □

With the notation above, the form $F + \lambda H$ is called the *neighbour* of F in the direction H.

2.4 Voronoï algorithm

Roughly speaking, Voronoï theory, or its variants, says that the Voronoï polyhedron Ω may be tiled by the cones D_F as F ranges over the set of *perfect* forms (see below for a more precise statement). There is also a dual formulation, in terms of minimal classes, which will provide the graph on which to apply Bass-Serre theory.

Theorem 2.4. *The L-Voronoï domains of perfect forms constitute a locally finite exact tessellation of $\mathscr{P}$, that is :*

1. $\mathscr{P} \subset \bigcup_{F \text{ perfect}} D_F$,

2. *for any two perfect forms F and F' one has $\mathring{D}_F \cap D_{F'} \neq \emptyset$ if and only if $F = \lambda F'$ for some $\lambda \in \mathbb{R}_{>0}$,*

3. *each facet of the Voronoï domain D_F of a perfect form F is a common facet of exactly two Voronoï domains D_F and $D_{F'}$ of perfect forms F and F',*

4. *the Voronoï domain of a perfect form F intersects only finitely many Voronoï domains of perfect forms.*

Moreover this tessellation is finite up to the action of $\Lambda^\times$, in the following sense:

5. *There are finitely many $\Lambda^\times$-inequivalent perfect forms of minimum* 1.

Proof. The proof of the first four assertions is a direct application of [Opg01, Theorem 1.9] (with the terminology used there, one has to check that the image of L in $V_\mathbb{R}$ is a discrete admissible set, which is straightforward). The assertion regarding finiteness can be established using Mahler's compactness theorem and standard arguments from reduction theory. A quick alternative proof can be derived from results of Ash ([Ash84]) as follows: First, since $[\mathrm{GL}(L):\Lambda^\times]$ is finite, it is enough to prove that there are finitely many $\mathrm{GL}(L)$-inequivalent forms. Now the set $\mathcal{V}$ of L-perfect forms of minimum 1 is clearly a discrete and closed subset of $\mathscr{P}$. Moreover, it is contained in the set of well-rounded forms (see next section), whose quotient modulo $\mathrm{GL}(L)$ is compact (see [Ash84] main theorem, section 2). The conclusion follows. □

The radical $\mathrm{Rad}(F)$ of a form $F \in \overline{\mathscr{P}}$ is the set of $x \in V_\mathbb{R}$ such that $F[x] = 0$. We say that the radical of F is defined over K if there exists a K-subspace W of V such that $\mathrm{Rad}(F) = W \otimes_\mathbb{Q} \mathbb{R}$. The rational closure $\overline{\mathscr{P}}^K$ of $\mathscr{P}$ is the set of forms in $\overline{\mathscr{P}}$, the radical of which is defined over K. The following corollary is a straightforward generalization of [WYH13, Proposition 36] which was obtained under the restriction $d = 1$. Our proof is slightly shorter, since the most difficult part (the fact that $\mathscr{P}$ is contained in Ω) is now a simple consequence of Theorem 2.4.

Corollary 2.5. *The Voronoï polyhedron Ω coincides with the rational closure of $\mathscr{P}$. The Voronoï tessellation takes the final form*

$$\mathscr{P} \subset \bigcup_{F \text{ perfect}} D_F = \Omega = \overline{\mathscr{P}}^K \subset \overline{\mathscr{P}}. \tag{6}$$

Proof. The inclusions

$$\mathscr{P} \subset \bigcup_{F \text{ perfect}} D_F \subset \Omega$$

are clear (the first inclusion is a consequence of the previous theorem and the second is obvious from the definitions of Ω and D_F).

It is also easy to see that $\Omega \subset \overline{\mathscr{P}}^K$: Indeed, for any nonzero $F \in \Omega$, there exist vectors $x_1, \ldots, x_m$ in V and a family of positive real numbers $\lambda_1, \ldots, \lambda_m$ such that $F = \sum_{i=1}^m \lambda_i x_i x_i^\dagger$. The radical of such an F is the set of $y \in V_\mathbb{R}$ such that

$$0 = \sum_{i=1}^m \lambda_i \langle x_i x_i^\dagger, yy^\dagger \rangle = \sum_{i=1}^m \lambda_i \operatorname{tr}\left(x_i^\dagger y y^\dagger x_i\right) = \sum_{i=1}^m \lambda_i \operatorname{tr}_{K_\mathbb{R}/\mathbb{R}}\left(\left(x_i^\dagger y\right)\left(x_i^\dagger y\right)^*\right)$$

which means that $x_i^\dagger y = 0$ for all i, since the λ_is are positive, and $\mathrm{tr}_{K_\mathbb{R}/\mathbb{R}}(aa^*) > 0$ for any nonzero $a \in K_\mathbb{R}$. In other words, $\mathrm{Rad}(F)$ is the intersection of t hyperplanes in $V_\mathbb{R}$ which are clearly defined over K since the x_i are in V.

The reverse inclusion $\overline{\mathscr{P}}^K \subset \Omega$ can be established using the same argument as [WYH13, Proposition 36]. Consider a form $F \in \overline{\mathscr{P}}^K$. Assuming that $A = M_n(K)$, there exists a K-subspace W of $V = K^n$ of dimension $m \le n$ such that $\mathrm{Rad}(F) = W \otimes_\mathbb{Q} \mathbb{R}$. Consequently, F is $\mathrm{GL}_n(K)$-equivalent to a form of the shape

$$\begin{pmatrix} 0 & 0 \\ 0 & F_W \end{pmatrix}$$

with F_W in $\mathscr{P}_W = \mathrm{Sym}(B_\mathbb{R})_{>0}$, where $B = M_m(K) \cong \mathrm{End}_K(W)$. As already seen, this cone $\mathscr{P}_W$ is contained in the corresponding Voronoï cone, which means that there exists vectors $y_1, \dots, y_\ell$ in K^m and a family of positive real numbers $\lambda_1, \dots, \lambda_\ell$ such that $F_W = \sum_{i=1}^\ell \lambda_i y_i y_i^\dagger$. But then F is $\mathrm{GL}_n(K)$-equivalent to

$$\begin{pmatrix} 0 & 0 \\ 0 & F_W \end{pmatrix} = \sum_{i=1}^{\ell} \lambda_i \begin{pmatrix} 0 \\ y_i \end{pmatrix} \begin{pmatrix} 0 \\ y_i \end{pmatrix}^\dagger \in \Omega,$$

whence the conclusion.

The final step to prove (6) is to show that $\Omega \subset \bigcup_{F \text{ perfect}} D_F$. Let $Q = \sum_{i=1}^m \lambda_i x_i x_i^\dagger$ be a nonzero element in Ω. We may assume, without loss of generality, that all λ_is are > 0 and that the x_i are in $L \setminus \{0\}$. Let F_0 be a perfect form with L-minimum 1. If $Q \notin D_{F_0}$, then there exists a direction H of D_{F_0} such that $\langle H, Q\rangle < 0$. Consequently, if $F_1 = F_0 + \lambda H$ is the neighbour of F_0 in the direction H, then

$$\langle Q, F_1\rangle = \langle Q, F_0\rangle + \lambda\langle H, Q\rangle < \langle Q, F_0\rangle. \tag{7}$$

We can pursue this process as long as Q is not found to belong to the Voronoï domain of a perfect form, and build a sequence $(F_n)_{n\in\mathbb{N}}$ of perfect forms in $\mathscr{V}$, the set of perfect forms with L-minimum 1, such that the sequence $(\langle Q, F_n\rangle)_{n\in\mathbb{N}}$ is strictly decreasing. On the other hand, the sequence $(\langle Q, F_n\rangle)_{n\in\mathbb{N}}$ is easily seen to assume only finitely many values. Indeed, we have

$$\langle Q, F_0\rangle \ge \langle Q, F_n\rangle = \sum_{i=1}^{\ell} \lambda_i F_n[x_i] \tag{8}$$

and we know that for every positive definite form F and positive θ, the set $F[\theta] = \{F[x], x \in L\} \cap [0, \theta]$ is finite and depends on F only up to $\mathrm{GL}(L)$-conjugacy. Since $\mathscr{V}/\mathrm{GL}(L)$ is finite, the right-hand side of (8) can thus take only finitely many values. This shows that the process must terminate, and Q belongs to the Voronoï domain of a perfect form. □

3 A CW-complex

The Voronoï tessellation of Theorem 2.4 yields a cellular decomposition of $\mathscr{P}$. Dual to it, one has a natural CW-complex, acted on by $\Gamma = \Lambda^\times$, carried by the set of *well-rounded* forms (see definition below). This cell-complex has been studied by many authors, especially Avner Ash in [Ash84], to which we refer in what follows.

Definition 3.1. A form $F \in \mathscr{P}$ is *well-rounded* if its set of minimal vectors $S_L(F)$ contains a K-basis of V.

The cell structure on $\mathscr{P}$ is induced by the decomposition into minimal classes, which are defined as follows :

Definition 3.2. Two elements F_1 and $F_2 \in \mathscr{P}$ are called *minimally equivalent with respect to* L, if $S_L(F_1) = S_L(F_2)$. We denote by $\mathscr{C}\ell_L(F) := \{H \in \mathscr{P} \mid S_L(H) = S_L(F)\}$ the *minimal class* of F. If $C = \mathscr{C}\ell_L(F)$ is a minimal class then we define $S_L(C) = S_L(F)$ the associated set of minimal vectors. A minimal class $C = \mathscr{C}\ell_L(F)$ is called *well rounded* if the form F is.

One has the following equivalent characterizations of well-rounded forms (resp. classes):

Lemma 3.3. *Let $\mathring{D}_F$ denote the relative interior of the Voronoï domain of a form F (i.e. D_F deprived of its proper faces). Then, the following assertions are equivalent*

1. *$F \in \mathscr{P}$ is well-rounded,*

2. *$\mathring{D}_F \cap \mathscr{P} \neq \emptyset$,*

3. *$D_F \not\subset \partial\mathscr{P}$.*

Proof. Assume that F is well-rounded, and consider the form $H = \sum_{x \in S_L(F)} xx^\dagger \in \mathring{D}_F$. For any $y \in \mathrm{Rad}(H)$ one has

$$0 = H[y] = \sum_{x \in S_L(F)} \langle xx^\dagger, yy^\dagger \rangle = \sum_{x \in S_L(F)} \mathrm{tr}\left(x^\dagger yy^\dagger x\right) = \sum_{x \in S_L(F)} \mathrm{tr}_{K_{\mathbb{R}}/\mathbb{R}}\left(\left(x^\dagger y\right)\left(x^\dagger y\right)^*\right)$$

whence $x^\dagger y = 0$ for all $x \in S_L(F)$, hence $y = 0$ since $S_L(F)$ spans K^n. Thus $H \in \mathring{D}_F \cap \mathscr{P}$ which shows that (1) ⇒ (2). The implication (2) ⇒ (3) is obvious. As for (3) ⇒ (1), we note that if F is not well-rounded, then one can find a non zero $y \in K^n$ such that $y^\dagger x = 0$ for all $x \in S_L(F)$, whence we deduce that $xx^\dagger\left[y\right] = 0$ for all $x \in S_L(F)$, which implies that y belongs to the radical of every $H \in D_F$. Thus $D_F \subset \partial\mathscr{P}$. □

The action (3) of $\mathrm{GL}_n(K)$ on Σ, restricted to its subgroups $\Lambda^\times \subset \mathfrak{M}^\times = \mathrm{GL}(L)$, induces an action on the set of minimal classes.

Clearly, because of positive definiteness, the stabilizer $\mathrm{Stab}_{\Lambda^\times}(F) := \left\{g \in \Lambda^\times \mid g^\dagger F g = F\right\}$ is always a finite subgroup of $\Lambda^\times$. We can define similarly the stabilizer of a minimal class as

$$\mathrm{Stab}_{\Lambda^\times}(C) = \left\{g \in \Lambda^\times \mid gS_L(C) = S_L(C)\right\}.$$

Lemma 3.4. *The stabilizer* $\mathrm{Stab}_{\Lambda^\times}(C)$ *of a well-rounded class is finite.*

Proof. It follows from [CN14, Lemma 5.3] that $\mathrm{Stab}_{\Lambda^\times}(C) = \mathrm{Stab}_{\Lambda^\times}(T_C^{-1})$ where $T_C := \sum_{x \in S_L(C)} xx^\dagger \in \mathscr{P}$ is the canonical form associated to C. So $\mathrm{Stab}_{\Lambda^\times}(C)$ is the stabilizer of some positive form and therefore a finite group. □

Positive real homotheties preserve minimal equivalence and the set of well-rounded forms. The quotient $\widetilde{W}$ of W by these homotheties inherits a well-defined CW-complex structure with the following properties.

Theorem 3.5 ([Ash84])**.** *Let W be the set of well-rounded forms in $\mathscr{P}$, and $\widetilde{W} = \mathbb{R}_{>0}\backslash W$. Then the correspondence*

$$\mathscr{C}\ell_L(F) \longleftrightarrow \mathring{D}_F \cap \mathscr{P}$$

is an inclusion-reversing bijection between the set of cells of $\widetilde{W}$, i.e. minimal classes*, and the set of open Voronoï domains not contained in the boundary of $\mathscr{P}$. In particular, 0-cells of $\widetilde{W}$ correspond to perfect forms in this bijection. The group $\Lambda^\times$ acts cellularly on $\widetilde{W}$, and the cells have finite stabilizers.*

Proof. If Λ is a maximal order, this is the main theorem of [Ash84]. The general case follows easily, since $\Lambda^\times$ is a finite index subgroup of the unit group of any of its maximal overorders. See also P. Gunnells' appendix to the book [Ste07] for a nice explanation of the duality between the Voronoï complex and the well-rounded retract, together with their cell decompositions. □

Remark 3.6. Scaling invariance allows to work within the set $\widetilde{\mathscr{P}} = \mathbb{R}_{>0}\backslash\mathscr{P}$, which we can identify with the set $\{F \in \mathscr{P} \mid \min_L(F) = 1\}$. Using a classical terminology, $\widetilde{\mathscr{P}}$ can thus be viewed as the boundary of a *Ryshkov polyhedron* ([Ryš70]), which is locally finite (see [Sch09b, Sch09a]). In particular, $\widetilde{\mathscr{P}}$ is a piecewise linear hypersurface, whose faces are the minimal classes. The bounded faces correspond to well-rounded classes and actually are polytopes.

4 Bass-Serre theory

In this section, we describe the theory underlying our algorithm for computing $\Gamma = \Lambda^\times$. Almost all the material here is borrowed, with hardly any change, from Brown's paper [Bro84].

Let $\widetilde{W}$ be equipped with its cell structure, as in the previous section. We denote by $\widetilde{W_i}$ its i-skeleton. We can see $\mathscr{G} := \widetilde{W_1}$ as a *graph* in the sense of [Ser77], with vertex set $\mathscr{V} := \widetilde{W_0}$ and edge set $\mathscr{E}$ consisting of 1-cells together with an orientation. Each edge e has an origin $o(e)$ and a terminus $t(e)$, corresponding to its orientation. For each such e, we define $\overline{e}$ as the same 1-cell, together with the reversed orientation ($o(\overline{e}) = t(e)$ and $t(\overline{e}) = o(e)$).

If there exists $g \in \Gamma$ such that $g(e) = \overline{e}$, one says that the edge e is inverted under the action of Γ. One technical difficulty when applying Bass-Serre theory in its original form is precisely that the definition of a graph adopted either in [Ser77] or in [Bas93] forbids action of groups reversing the orientation of edges, a condition which is not necessarily satisfied in practice. One can easily get around this problem e.g. using barycentric subdivision. Brown's paper deals with this in a slightly different way, although essentially equivalently, which we summarize in the following steps:

1. Choose an orientation on 1-cells, in such a way that the orientation of those that are not inverted by the action of Γ is preserved by this action.

2. Split the set of edges $\mathscr{E}$ into a disjoint union $\mathscr{E} = \mathscr{E}^+ \sqcup \mathscr{E}^-$, where $\mathscr{E}^+$ denotes the set of edges which are not inverted under the action of Γ, and $\mathscr{E}^-$ its complement. For $e \in \mathscr{E}$ let $\Gamma_{\{e,\overline{e}\}}$ be the stabilizer of the set $\{e, \overline{e}\}$ and Γ_e the stabilizer of e (together with its orientation). Clearly, Γ_e is a subgroup of $\Gamma_{\{e,\overline{e}\}}$, one has $\Gamma_e = \Gamma_{o(e)} \cap \Gamma_{t(e)}$ and
$$\left(\Gamma_{\{e,\overline{e}\}} : \Gamma_e\right) = \begin{cases} 1 \text{ if } e \in \mathscr{E}^+ \\ 2 \text{ if } e \in \mathscr{E}^-. \end{cases}$$

3. Fix a tree T of representatives of $\widetilde{W_1}$ mod Γ, that is a sub-tree such that the set V_T of its vertices is a set of representatives of $\widetilde{W_0}$ mod Γ, with the further assumption that all its edges are in $\mathscr{E}^+$. This implies in particular that its edges are pairwise inequivalent mod Γ.

4. Choose a set E^+ of representatives of $\mathscr{E}^+$ mod Γ such that $o(e) \in V_T$ for all $e \in E^+$, and a set E^- of representatives of $\mathscr{E}^-$ mod Γ such that $o(e) \in V_T$ for all $e \in E^-$.

5. For every $e \in E^+$, choose $g_e \in \Gamma$ such that $g_e^{-1}(t(e)) \in V_T$, with the convention that $g_e = 1$ whenever e is an edge of T.

6. For every $e \in E^-$, choose $g_e \in \Gamma_{\{e,\overline{e}\}} \setminus \Gamma_e$.

7. Choose a set F of representatives of the 2-cells of $\widetilde{W}$ mod Γ, and attach to every 2-cell τ in F a *combinatorial path α, i.e.* a sequence $(e_1, e_2, \ldots, e_m)$ of edges such that:

   - $\partial\tau = \cup_i \sigma_i$, where σ_i denotes the 1-cell underlying e_i,
   - $v_0 := o(e_1)$ is in V_T,
   - $t(e_i) = o(e_{i+1})$ for $1 \le i \le m-1$ and $t(e_m) = o(e_1)$,
   - $e_{i+1} \neq \overline{e_i}$ for $1 \le i \le m-1$ and $e_1 \neq \overline{e_m}$.

   To each edge of this path, one attaches (non-canonically) an element g_i of the subgroup generated by the various isotropy groups Γ_v ($v \in V_T$), $\Gamma_{\{e,\overline{e}\}}$ ($e \in E$) and the g_e ($e \in E^+$) chosen in step 5, such that the successive vertices belong to V_T, $g_1 V_T$, $g_1 g_2 V_T, \ldots, g_1 g_2 \cdots g_m V_T$ (see [Bro84, Section 1] for a precise description of g_i). In particular, one has $g_1 g_2 \cdots g_m \in \Gamma_{v_0}$. We call the sequence $(g_1, \cdots, g_m)$ the *cycle associated to* τ, and occasionally identify a cycle with the corresponding cell, when no confusion can ensue.

Altogether, the previous data lead to the following presentation of $\Gamma = \Lambda^\times$:

Theorem 4.1 ([Bro84] Theorem 1)**.** *Let $\Gamma = \Lambda^\times$ be the unit group of an order in a finitely generated simple algebra over $\mathbb{Q}$. Let W be the set of well-rounded forms in $\mathscr{P}$, and T, $E = E^+ \cup E^-$, F be chosen as above. Then Γ has the following structure:*
$$\Gamma = \left(\underset{v \in V_T}{*} \Gamma_v\right) * \left(\underset{e \in E^-}{*} \Gamma_{\{e,\overline{e}\}}\right) * F(E^+)/R \tag{9}$$
where $*$ stands for the free product, $F(E^+)$ denotes the free product on the set $\{g_e, e \in E^+\}$ and R is the normal subgroup generated by:

- *g_e, $e \in T$,*
- *$g_e^{-1} \cdot g \cdot g_e \left(g_e^{-1} g g_e\right)^{-1}$, $e \in E^+$, $g \in \Gamma_e \subset \Gamma_{o(e)}$,*
- *$g_1 \cdot g_2 \cdot \cdots \cdot g_{m-1} \cdot g_m \left(g_1 \cdots g_m\right)^{-1}$, $\left(g_1, \cdots, g_m\right) \in F$*

In other words, Γ is generated by the subgroups Γ_v ($v \in V_T$) and the elements g_e ($e \in E^+ \cup E^-$), subject to the following relations:

0. *The multiplication table of Γ_v ($v \in V_T$).*
1. *$g_e = 1$ if e is an edge of T.*
2. *$g_e^{-1} \cdot g \cdot g_e = g_e^{-1} g g_e \in \Gamma_{w(e)}$, for $e \in E^+$ and $g \in \Gamma_e \subset \Gamma_{o(e)}$.*
3. *$g_e \cdot g = g_e g$ and $g \cdot g_e = g g_e \in \Gamma_{o(e)}$, for $e \in E^-$ and $g \in \Gamma_e \subset \Gamma_{o(e)}$.*
4. *$g_1 \cdot g_2 \ldots g_{m-1} \cdot g_m = g_1 \cdots g_m$ for any cycle $\left(g_1, \cdots, g_m\right)$ associated to a 2-cell τ.*

Proof. The description of Γ in the first part of the theorem is [Bro84, theorem 1'], applied to $\widetilde{W}$ (which is contractible, hence simply connected). More precisely, the free product

$$\left(\mathop{*}_{v \in V_T} \Gamma_v\right) * \left(\mathop{*}_{e \in E^-} \Gamma_{\{e, \overline{e}\}}\right) * F(E^+)$$

modulo the normal subgroup generated by

$$g_e, e \in T$$

and

$$g_e^{-1} \cdot g \cdot g_e \left(g_e^{-1} g g_e\right)^{-1}, e \in E^+, g \in \Gamma_e$$

is precisely the fundamental group of the barycentric subdivision $\mathscr{G}'$ of $\widetilde{W}_1$ acted on by Γ (see the discussion preceding [Bro84, theorem 1']). Finally, one has to mod out by the fundamental group of $\mathscr{G}'$, which is the normal closure of the cycles associated to the 2-cells in F. The second part of the theorem is just a rephrasing in terms of generators and relations. □

Remark 4.2. Let $\tilde{E} := \{e \in \mathscr{E} : o(e) \in V_T, t(e) \notin V_T\}$ be the set of edges coming out of T. For any $e \in \tilde{E}$ there is some element $f \in E$ with $o(f) = o(e)$. Choose some $h \in \Gamma_{o(e)}$ such that $h(f) = e$ (with the convention that $h = 1$ if $e = f$). The element $g_e = h g_f \in \Gamma$ then satisfies $g_e^{-1}(t(e)) \in V_T$. and is called the **side-transformation** corresponding to e.

Remark 4.3. In practical applications one usually does not fix an orientation on the edges of the graph X. The additional relations that we then need correspond to the so called "side-pairings" from the Poincaré-algorithm. Let $e \in E$ and g_e be as above, so that $g_e^{-1}(t(e)) = o(f) \in V_T$. We then call the edges e and $g_e^{-1}(e) = \overline{f}$ *paired.* Then $g_e(t(f)) = o(e) \in V_T$ because Γ acts on the graph and hence preserves edges. Also $g_f^{-1}(t(f)) \in V_T$ so these two vertices are in V_T and equivalent under Γ, which implies that $g_f^{-1}(t(f)) = o(e) \in V_T$ and $g_e^{-1} g_f \in \Gamma_v$. So if we do not choose an orientation and so do not restrict to those transformations g_e with $o(e) \in V_T$ we need to add these additional relations.

5 Solving the word problem

To solve the word problem we return to the tessellation by Voronoï domains D_F of the perfect forms. According to Corollary 2.5 this yields a locally finite exact tessellation of the Voronoï polyhedron Ω that contains the open cone $\mathscr{P}$. Recall that $\mathscr{P}$ is a cone in the Euclidean space Σ from Definition 2.1. Instead of working in projective space we take an affine section of $\mathscr{P}$,

$$\mathscr{P}' := \{F \in \mathscr{P} \mid \operatorname{tr}(F) = 1\}.$$

Lemma 5.1. *For $x, y \in \mathscr{P}'$ let $\mathscr{G} := \{x + s(x - y) \mid s \in [0,1]\} \subset \mathscr{P}'$ the Euclidean geodesic joining x and y. Then the set of all Voronoï domains of perfect forms that meet $\mathscr{G}$,*

$$\mathscr{V}(x, y) := \{D_F \mid D_F \cap \mathscr{G} \neq \emptyset\},$$

is finite. We call $d(x, y) := |\mathscr{V}(x, y)|$ the perfect-distance between x and y. Note that this distance is Γ-invariant, $d(x, y) = d(g(x), g(y))$ for all $g \in \Gamma$.

Proof. This is a general compactness argument: For any $z \in \mathscr{G}$ we may choose an open neighborhood U_z of z which intersects only finitely many Voronoï domains D_F, because of the local finiteness of the tessellation. As $\mathscr{G} \subset \cup_{z\in\mathscr{G}} U_z$ is an open covering of the compact set $\mathscr{G}$ there is a finite subset $Z \subseteq \mathscr{G}$ such that

$$\mathscr{G} \subset \bigcup_{z\in Z} U_z \subset \bigcup_{z\in Z} \bigcup_{D_F \cap U_z \neq \emptyset} D_F.$$

□

Theorem 5.2. *There is an algorithm to express a given $g \in \Lambda^\times$ as a word in the generators given in Theorem 4.1.*

Proof. For the proof we give an algorithm to find such a word in the set of all side-transformations as defined in Remark 4.2 followed by some element in $\cup_{v\in V_T}\Gamma_v$.

Let

$$F_T := \bigcup_{v\in V_T} D_v \cap \mathscr{P}'$$

be the union of all Voronoï domains of the perfect forms corresponding to the vertices of the tree T chosen in Section 4. Choose some inner point $x \in D_v \subset F_T$ and let $y := g(x)$ be its image under g and $\mathscr{G}$ be the geodesic between x and y. If $y \in D_w$ for some $w \in V_T$ then $w = v$ and $g \in \Gamma_v$. Otherwise $\mathscr{G}$ meets the boundary of F_T in some point $p \in \mathscr{P}'$. Let

$$M := \{D_F : F \in \mathscr{V} \setminus V_T, p \in D_F\}.$$

By Lemma 5.1 the set M is finite. If p is in the relative interior of some codimension 1 facet (which will be almost always the case) then $M = \{t(e)\}$ for some $e \in \tilde{E}$. Note that the perfect-distance $d(z, g(x))$ between any inner point z of $D_{t(e)}$ which lies on $\mathscr{G}$ and y is strictly smaller than $d(x, g(x))$. Let g_e be the corresponding side-transformation defined in Remark 4.2 Then $g_e^{-1}(t(e)) = w \in V_T$ and $g_e^{-1}(z) \in D_w$ with

$$d(g_e^{-1}(z), g_e^{-1}(g(x))) = d(z, g(x)) < d(x, g(x)).$$

Replace g by $g_e^{-1}g$, x by $g_e^{-1}(z)$ and y by $g_e^{-1}(y)$ and continue.

In the unlikely event that M contains more than one element (i.e. $\mathscr{G}$ meets the intersection of at least two distinct facets containing p) one chooses a different starting point x' in a small neighborhood of x which is still contained in D_v while keeping the endpoint y of $\mathscr{G}$ fixed. Since the intersection of two distinct facets is of codimension at least 2 it is (from a measure theoretic point of view) highly unlikely that $\mathscr{G}$ again meets more than one facet of the fundamental domain. Hence after a small number of modifications of x and $\mathscr{G}$ we are in the situation described above. □

6 Examples

In this section we list a few examples to illustrate the algorithm. Many more examples can be found in a database for unit groups of orders linked to the authors' homepages, where one will also find MAGMA implementations of the algorithms.

6.1 The rational quaternion algebra ramified at 2 and 3

To illustrate the theory of the previous sections we comment on a very easy example. Take the rational quaternion algebra ramified at 2 and 3,

$$\mathscr{Q}_{2,3} = \left(\frac{2,3}{\mathbb{Q}}\right) = \langle i,j \mid i^2 = 2, j^2 = 3, ij = -ji\rangle = \langle \operatorname{diag}(\sqrt{2}, -\sqrt{2}), \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}\rangle.$$

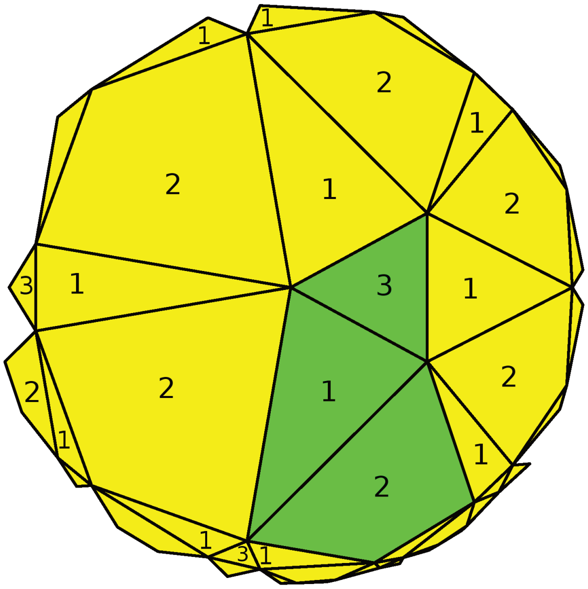
Then a maximal order is $\Lambda = \langle 1, i, \frac{1}{2}(1+i+ij), \frac{1}{2}(j+ij)\rangle$. So here $V = A = \mathscr{Q}_{2,3}$, $A_{\mathbb{R}} = M_2(\mathbb{R})$, $L = \Lambda$. If we embed A into $A_{\mathbb{R}}$ using the maximal subfield $\mathbb{Q}[\sqrt{2}]$ we find three perfect forms representing the $\Lambda^\times$-orbits on the set of all perfect forms:

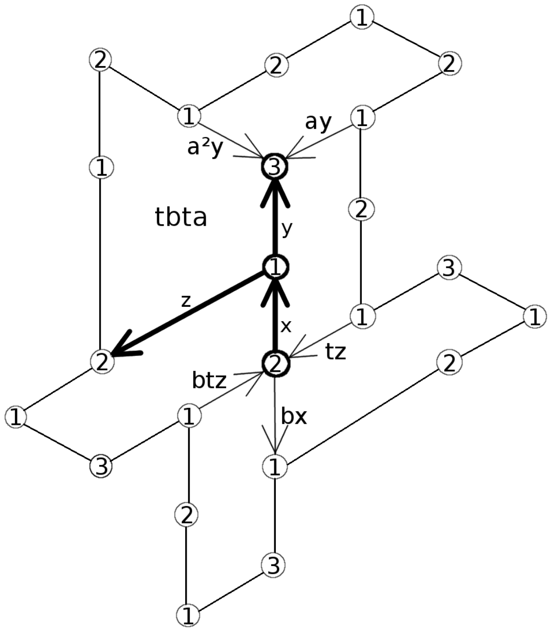
$$F_1 = \begin{pmatrix} 1 & 2-\sqrt{2} \\ 2-\sqrt{2} & 1 \end{pmatrix},\ F_2 = \begin{pmatrix} 6-3\sqrt{2} & 2 \\ 2 & 2+\sqrt{2} \end{pmatrix},\ F_3 = \operatorname{diag}(-3\sqrt{2}+9, 3\sqrt{2}+5)$$

with stabilizers

$$\operatorname{Stab}_{\Lambda^\times}(F_1) = \langle -1\rangle, \operatorname{Stab}_{\Lambda^\times}(F_2) = \langle \beta\rangle \cong C_4, \operatorname{Stab}_{\Lambda^\times}(F_3) = \langle \alpha\rangle \cong C_6.$$

The tessellation for $\mathscr{Q}_{2,3} \hookrightarrow M_2(\mathbb{Q}[\sqrt{2}])$ and the relevant part of the resulting graph (dual to the tessellation) is visualised in the following pictures.





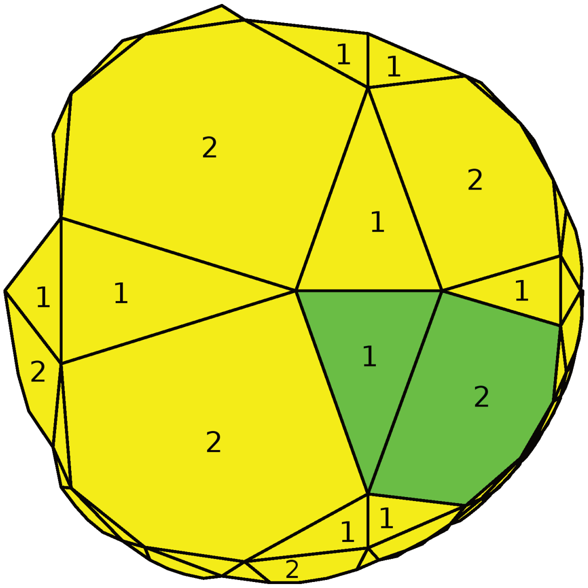
So $V = \{1,2,3\}$ is represented by the double circled vertices, and $E = E^+ = \{x, y, z\}$. We have $\Gamma_1 = 1$, $\Gamma_2 = \langle b\rangle \cong C_2$ and $\Gamma_3 = \langle a\rangle \cong C_3$ and put $g_z =: t$. Then

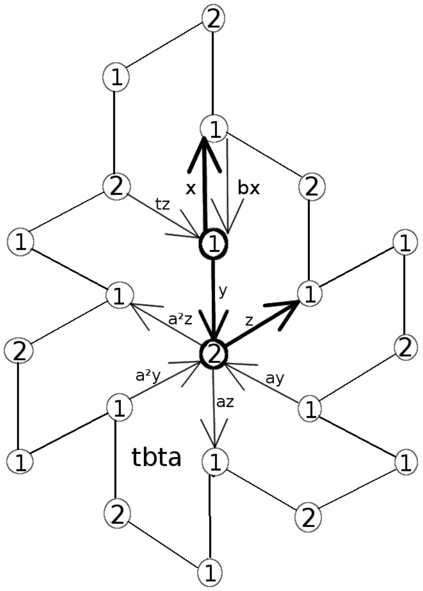
$$\Gamma = \Lambda^\times/\langle \pm 1\rangle = \langle a, b, t \mid a^3, b^2, atbt\rangle.$$

Note that all cycle relations are conjugate as there is just one $\Lambda^\times$-orbit on the minimal classes of perfection corank 2.

To illustrate that the resulting tessellation depends on the chosen maximal subfield we redo the computations for the maximal subfield $\mathbb{Q}[\sqrt{3}]$ instead of $\mathbb{Q}[\sqrt{2}]$.

The tessellation for $\mathcal{Q}_{2,3} \hookrightarrow M_2(\mathbb{Q}[\sqrt{3}])$ is as follows.





So here we obtain only 2 perfect forms, f_1 and f_2, say, with $\mathrm{Stab}_{\Lambda^\times}(f_1) = \langle -1 \rangle$, $\mathrm{Stab}_{\Lambda^\times}(f_2) = \langle \alpha \rangle \cong C_6$.

6.2 The rational quaternion algebra ramified at 19 and 37

This example illustrates the power of Voronoï's algorithm. Let Λ be a maximal order in the quaternion algebra $\left(\frac{19,37}{\mathbb{Q}}\right)$, the rational quaternion algebra ramified at 19 and 37. The Fuchsian Group package in Magma does not return a presentation of the unit group $\Lambda^\times$ in a reasonable time. Our algorithm takes about 5 minutes to compute $\Lambda^\times/\langle \pm 1 \rangle = \langle H_1, \ldots, H_{56} \rangle$ with the single relator

$$\begin{aligned}
&H_{21} H_{10}^{-1} H_{44}^{-1} H_{49}^{-1} H_{14}^{-1} H_{55}^{2} H_4 H_{42} H_{15}^{-1} H_{46} H_{19}^{-1} H_{52}^{-1} H_{20} H_{17}^{-1} H_9 H_{54} H_{39} H_{16}^{-1} H_{48} H_3^{-1} H_{44}^{-1} H_{38} \\
&H_2 H_{26}^{-1} H_{35}^{-1} H_{18} H_{12} H_{56}^{2} H_1 H_{20} H_{25} H_{24} H_{23} H_5 H_{50} H_8^{-1} H_{41} H_{35}^{-1} H_2 H_{15} H_{28}^{-1} H_5 H_{43} H_{53}^{-1} \\
&H_1^{-1} H_{34}^{-1} H_{52} H_{49}^{-1} H_{48} H_8^{-1} H_{33}^{-1} H_{14} H_3 H_{27} H_{36}^{-1} H_{40}^{-1} H_{47} H_9^{-1} H_{22} H_{13}^{-1} H_{53}^{-1} H_{39} H_{27} H_{51}^{-1} H_{13} H_{46} \\
&H_{47}^{-1} H_{43}^{-1} H_{17}^{-1} H_{37}^{-1} H_{40}^{-1} H_{21} H_{30} H_6 H_{12}^{-1} H_{32} H_{54}^{-1} H_{28}^{-1} H_{36} H_{22} H_{29}^{-1} H_7^{-1} H_{45}^{-1} H_{26}^{-1} H_{50}^{-1} H_{32}^{-1} H_{11}^{-1} \\
&H_{51}^{-1} H_{30} H_{18} H_{29} H_{16}^{-1} H_{33} H_{34} H_{41} H_{11} H_7 H_{37}^{-1} H_{42}^{-1} H_{10}^{-1} H_{23}^{-1} H_6 H_{31}^{-1} H_{45}^{-1} H_{19}^{-1} H_4 H_{25} H_{31} H_{38} H_{24}.
\end{aligned}$$

Remark 6.1. One might want to compare this result with the well known formula for the genus g of the associated Shimura curve (see e.g. [Shi65]). Note that $2g = \dim(\mathrm{Hom}(\Gamma, \mathbb{C}))$ where $\Gamma = \{g \in \Lambda^\times \mid \mathrm{nred}(g) = 1\}/\langle -1 \rangle$. From our presentation we obtain that $\Gamma/\Gamma' \cong \mathbb{Z}^{110}$, from which we get $110 = 2g = (19-1)(37-1)/6 + 2$ as predicted.

6.3 Quaternion algebras over imaginary quadratic fields

The number of perfect forms and hence the performance of our algorithm depends on the choice of the involution † on $A_{\mathbb{R}}$. For certain quaternion algebras A, there is a canonical way to choose such an involution † that preserves A:

Remark 6.2. Let k be a CM-field with complex conjugation $\overline{}$ and let $\mathcal{Q}$ be a definite rational quaternion algebra with canonical involution $\overline{}$. Then

$$\dagger : \mathcal{Q} \otimes k \to \mathcal{Q} \otimes k; a \otimes k \mapsto \overline{a} \otimes \overline{k}$$

defines a positive involution on $A = \mathcal{Q} \otimes k$.

Using this involution we computed a few examples for imaginary quadratic fields k:
We first fix the quaternion algebra $\mathcal{Q} = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ and vary the imaginary quadratic field $k = \mathbb{Q}(\sqrt{-d})$, with $-d \equiv 1 \pmod 8$:

d	Number of perfect forms	Runtime Voronoï	Runtime Presentation	Number of generators
7	1	$1.24s$	$0.42s$	2
31	8	$6.16s$	$0.50s$	3
55	21	$14.69s$	$1.01s$	5
79	40	$28.74s$	$1.78s$	5
95	69	$53.78s$	$2.57s$	7
103	53	$38.39s$	$2.52s$	6
111	83	$66.16s$	$3.02s$	6
255	302	$323.93s$	$17.54s$	16

In the next example we fix the imaginary quadratic field k to be $\mathbb{Q}(\sqrt{-7})$ and vary the rational quaternion algebra $\mathcal{Q}$ to obtain $A = \left(\frac{a,b}{\mathbb{Q}(\sqrt{-7})}\right)$:

a,b	Norm of discriminant	Number of perfect forms	Runtime Voronoï	Runtime Presentation	Number of generators
$-1,-1$	4	1	$1.24s$	$0.42s$	2
$-1,-11$	121	20	$21.61s$	$4.13s$	6
$-11,-14$	484	58	$51.46s$	$5.11s$	10
$-1,-23$	529	184	$179.23s$	$89.34s$	16

6.4 A division algebra of index 3

Let $\vartheta = \zeta_9 + \zeta_9^{-1}$ be a real root of $x^3 - 3x + 1 \in \mathbb{Q}[x]$. Let A be the rational division algebra generated (as an algebra over $\mathbb{Q}$) by $Z := \operatorname{diag}(\vartheta, \sigma(\vartheta), \sigma^2(\vartheta))$ and $\Pi := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix}$ where σ generates the Galois group of $\mathbb{Q}[\vartheta]$ over $\mathbb{Q}$. As the minimal polynomial of ϑ (and hence of Z) is congruent modulo 2 to the minimal polynomial over $\mathbb{Q}_2$ of a seventh root of unity, $\Pi^3 = 2$ and $\Pi Z \Pi^{-1} - Z^2 = 2$, we see that the Hasse invariant of A is $\frac{1}{3}$ at the prime 2. We use [NeS09] to compute a maximal order Λ in A and its discriminant $2^6 3^6$. So the only other ramified prime in A is 3 and its Hasse invariant is $\frac{2}{3}$. Let $\Gamma := \operatorname{SL}(\Lambda) := \{g \in \Lambda^\times \mid \operatorname{nred}(g) = 1\}$, $L = \Lambda$, $A \hookrightarrow A_{\mathbb{R}}$ via one of the embeddings of $\mathbb{Q}[\vartheta] \hookrightarrow \mathbb{R}$. Then Γ has 431 orbits on the set of L-perfect forms in $\mathcal{P}$. After reducing the presentation obtained by the algorithm above with standard MAGMA programs we obtain that $\Gamma = \langle a, b \rangle$ where

$$a := \frac{1}{3} \begin{pmatrix} -\vartheta^2 - 3\vartheta + 1 & \vartheta^2 + 2 & -\vartheta^2 + 1 \\ 2\vartheta^2 + 2\vartheta - 6 & -2\vartheta^2 + \vartheta + 3 & -\vartheta^2 - \vartheta + 6 \\ 2\vartheta + 8 & -2\vartheta - 2 & 3\vartheta^2 + 2\vartheta - 7 \end{pmatrix},$$

$$b := \frac{1}{3} \begin{pmatrix} \vartheta^2 - 2\vartheta - 3 & -2\vartheta + 1 & -\vartheta^2 + 1 \\ 2\vartheta^2 + 2\vartheta - 6 & -3\vartheta^2 - \vartheta + 5 & -2\vartheta^2 + 5 \\ 4\vartheta^2 + 4\vartheta - 6 & -2\vartheta - 2 & 2\vartheta^2 + 3\vartheta - 5 \end{pmatrix}$$

with defining relators

$$\begin{aligned}
&b^2a^2(b^{-1}a^{-1})^2,\\
&b^{-2}(a^{-1}b^{-1})^2ab^{-2}a^2b^{-3},\\
&ab^2a^{-1}b^3a^{-2}bab^3,\\
&a^2bab^{-2}ab^{-1}(a^{-2}b)^2,\\
&a^{-1}b^2a^{-1}b^{-1}a^{-5}b^{-2}a^{-3},\\
&b^{-2}a^{-2}b^{-1}a^{-1}b^{-1}a^{-2}b^{-1}a^{-1}b^{-2}(a^{-1}b^{-1})^3.
\end{aligned}$$

Remark 6.3. Note that $A^{\mathrm{op}} = A^{\mathrm{Tr}}$ has Hasse invariant $\frac{2}{3}$ at 2 and $\frac{1}{3}$ at 3. As maximal orders of A and A^{op} correspond to each other by transposing matrices, also their unit groups are isomorphic (via $g \mapsto g^{-\mathrm{Tr}}$). Computing the Voronoï-tessellation for the transposed matrices, however, we find 410 perfect forms instead of 431, which shows that there is no direct correspondence on the level of perfect forms.

6.5 A matrix ring over a quaternion algebra

Consider the rational quaternion algebra $K = \left(\frac{-1,-3}{\mathbb{Q}}\right)$, ramified at 3 and the infinite place. Let $\mathscr{O}$ be the maximal order with $\mathbb{Z}$-basis $\left\{1,\ i,\ \frac{1}{2}(i+k),\ \frac{1}{2}(1+j)\right\}$ and let $A = M_2(K)$, $\Lambda = M_2(\mathscr{O})$. The algebra A is of interest as a direct summand of the rational group algebra of $\mathrm{SL}_2(5)$.

Our algorithm finds one perfect form with automorphism group of order 720 (isomorphic to $\mathrm{SL}_2(9)$) and a presentation of $\Lambda^\times$ on the two generators

$$\frac{1}{2}\begin{pmatrix} 2 & 0 \\ -1+i+j-k & -i-k \end{pmatrix},\ \frac{1}{2}\begin{pmatrix} i+k & -1+j \\ -2i & 2-i+k \end{pmatrix},$$

which have orders 4 and 6, respectively. These two generators satisfy a set of 64 relations, which is too large to be printed here. The commutator factor group $\Lambda^\times/(\Lambda^\times)'$ is cyclic of order 4.

7 Implementation

While many things in the implementation of our algorithms are straightforward, there are some tasks which do not have an obvious solution. We present these here.

7.1 Minimal vectors

Let $F \in \mathscr{P}$ be a form. In order to compute $S_L(F)$, the set of L-minimal vectors of F, we associate to F a $\mathbb{Z}$-lattice L_F and compute the minimal vectors of that lattice, e.g. using MAGMA [BCP97].

Let $\mathscr{B}$ be a $\mathbb{Z}$-basis of L. We associate to the form F the following bilinear form b_F on $V_{\mathbb{R}}$:

$$b_F\ :\ V_{\mathbb{R}} \times V_{\mathbb{R}} \to \mathbb{R},\ (x,y) \mapsto \frac{1}{2}\left(F[x+y]-F[x]-F[y]\right).$$

Clearly, b_F is positive definite since $F \in \mathscr{P}$. Now let L_F be the $\mathbb{Z}$-lattice which has as its Gram matrix the Gram matrix of b_F with respect to the basis $\mathscr{B}$. Then, since $F[\ell] = b_F(\ell,\ell)$ for all

$\ell \in L$, the minimal vectors of L_F are the coordinates of the minimal vectors of F with respect to the basis $\mathscr{B}$.

7.2 Isometry testing and automorphism groups

We want to decide algorithmically if two forms are in the same orbit under the action

$$\Lambda^\times \times \mathscr{P} \to \mathscr{P},\ (\lambda, F) \mapsto \lambda^\dagger F \lambda$$

of the unit group $\Lambda^\times$.

First, consider the case where $A = K$ is a division algebra. Then we choose $L = \Lambda$. In particular, the minimal vectors of our forms are elements of the order Λ.

Lemma 7.1. *Let $F_1, F_2 \in \mathscr{P}$, $\ell \in S_L(F_1)$. There is a $\lambda \in \Lambda^\times$ satisfying $\lambda^\dagger F_2 \lambda = F_1$ if and only if there is some $\ell_2 \in S_L(F_2)$ such that $(\ell_2\ell^{-1})^\dagger F_2 \ell_2 \ell^{-1} = F_1$ and $\ell_2\ell^{-1} \in \Lambda^\times$.*
Also, we have

$$\mathrm{Stab}_{\Lambda^\times}(F_1) = \{\ell_1\ell^{-1} \mid (\ell_1\ell^{-1})^\dagger F_1 \ell_1\ell^{-1} = F_1,\ \ell_1\ell^{-1} \in \Lambda^\times,\ \ell_1 \in S_L(F_1)\}.$$

Proof. If we have $\lambda^\dagger F_2 \lambda = F_1$, then $\lambda^{-1} S_L(F_2) = S_L(F_1)$, which is easily verified. This proves both claims. □

This lemma allows us to check for isometry and to compute automorphism groups of forms using only our knowledge of the finite sets of minimal vectors and without any a-priori knowledge of $\Lambda^\times$. The membership $\lambda \in \Lambda^\times$ is tested by checking that both λ and λ^{-1} are in the free abelian group Λ.

We now turn to the general case, where A is a simple algebra and $\mathfrak{M} = \mathrm{End}_{\mathscr{O}}(L)$ for some Λ-lattice L in V. We will only describe the computation of the automorphism group of a form $F \in \mathscr{P}$. Isometry testing is completely analogous. We use the notation from 7.1.

Consider the $\mathbb{Q}$-linear representation of A induced by the action of A on V with respect to the basis $\mathscr{B}$. If we compute the automorphism group of the $\mathbb{Z}$-lattice L_F with the Plesken-Souvignier algorithm [PS97], the result of this is a finite group of $|\mathscr{B}| \times |\mathscr{B}|$-matrices isomorphic to $\mathrm{Aut}_{\mathbb{Z}}(L_F)$. However, in general not all of these matrices will be contained in the image of $A \hookrightarrow \mathbb{Q}^{|\mathscr{B}|\times|\mathscr{B}|}$. In order to compute only those automorphisms which satisfy this additional condition we make use of the fact that the Plesken-Souvignier algorithm may be given an additional input, namely a list of matrices which is to be fixed by the resulting lattice automorphisms.

Lemma 7.2. *Let $\{b_1, \dots, b_\delta\}$ be a basis of the centralizer of the image $A \hookrightarrow \mathbb{Q}^{|\mathscr{B}|\times|\mathscr{B}|}$. The matrices $X \in \mathrm{GL}_{|\mathscr{B}|}(\mathbb{Z})$ stabilizing L_F and fixing $\mathrm{Gram}(L_F)\cdot b_1, \dots, \mathrm{Gram}(L_F)\cdot b_\delta$ are contained in the image of A.*

Proof. Let $G := \mathrm{Gram}(L_F)$ and consider $X \in \mathrm{GL}_{|\mathscr{B}|}(\mathbb{Z})$ as in the statement. Then we have $X^{tr}GX = G$ and consequently, for all $1 \le i \le \delta$, $X^{tr}Gb_iX = Gb_i = X^{tr}GXb_i$. This implies $b_iX = Xb_i$ for all i. It now follows from the double-centralizer theorem [Rei75, (7.11)] that X is contained in the image of the representation of A. □

Since $\mathfrak{M} = \mathrm{End}_{\mathcal{O}}(L)$, the matrices X from the previous lemma are actually contained in the image of $\mathfrak{M}$ under the representation we considered. Therefore, using this lemma, we can compute the stabilizer $\mathrm{Stab}_{\mathfrak{M}^\times}(F)$ and its intersection $\mathrm{Stab}_{\Lambda^*}(F) = \mathrm{Stab}_{\mathfrak{M}^\times}(F) \cap \Lambda$ without prior knowledge of $\Lambda^\times$.

7.3 Outline of an implementation

A detailed exposition of Voronoï's algorithm is beyond the scope of this paper, so we refer the reader to [Mar03, Opg01] for details on the theory of the algorithm. The purpose of this section is to provide an overview of the steps necessary to implement our algorithms.

First of all, it should be noted that one cannot carry out precise computations in $A_{\mathbb{R}} = A \otimes_{\mathbb{Q}} \mathbb{R}$. However in order to carry out the computations it is only necessary to embed A into a semisimple algebra $\mathscr{A}$ with positive involution. If, for example, A is a quaternion algebra with positive involution, we compute in A itself rather than in $A_{\mathbb{R}}$, which means that the computations of the polyhedral tessellation are exactly performed in MAGMA. Here we could also use polymake [GaJ00], allowing even exact computations with quadratic irrationalities. In the case of the example in Section 6.4 we use an embedding of A into $\mathscr{A} = M_3(\mathbb{Q}[\vartheta])$, the involution in that case being transposition. Then all perfect forms already lie in $\mathscr{A}$ and the number of perfect forms depends on the choice of this algebra $\mathscr{A}$. To compute the facets of the Voronoï domains we just determine all subsets of the vertices that define a codimension 1 subspace, which can be checked by computations in the rationals. To decide whether such a hyperplane is a facet, we only need to check whether the chosen real embeddings of the inner products of the corresponding direction (perpendicular to the facet) with all other vertices have the same sign.

Assuming the reader has a suitable version of Voronoï's algorithm at his disposal, we now move on to the computation of a presentation of $\Lambda^\times$. As a by-product of the algorithm, we already have the facets of the Voronoï domains. The codimension-2-faces are easily computed as intersections of facets. These codimension-2-faces (to which we will refer as "ridges" in what follows) correspond to the 2-cells of the CW-complex described in section 3 and for computational simplicity we perform our calculations using the faces.

Notice that the side transformations (*cf.* Remark 4.2) obtained by Voronoï's algorithm together with the stabilizers of the perfect forms generate $\Lambda^\times$. This is the set of generators we use in our implementation. However, this set of generators does not coincide with the generators described in Section 4.

Let $\mathcal{V}$ be a set of representatives of perfect forms obtained from Voronoï's algorithm. In order to compute the cycle relation corresponding to an ridge $\mathfrak{e}$ contained in the boundary of the Voronoï domain D_P of a perfect form $P = P_0 \in \mathcal{V}$ one should proceed as follows. Note that there is a finite sequence of perfect forms $P_i \in \mathscr{P}$, $0 \le i \le \ell$, such that D_{P_i} and $D_{P_{i+1}}$ meet precisely in a facet, $\mathfrak{e} \subset D_{P_i}$ for all i and $P_0 = P_\ell$. We now proceed iteratively: In the i^{th} step we construct an element $g \in \Lambda^\times$ as a product of side-transformation (i.e. generators of $\Lambda^\times$) such that $g^\dagger P_i g \in \mathcal{V}$. So in the ℓ^{th} step we will have $g^\dagger P_\ell g \in \mathcal{V}$, which means $g \in \mathrm{Stab}_{\Lambda^\times}(P)$, yielding a relation. Start this calculation by identifying a facet $\mathfrak{f}$ of D_P containing $\mathfrak{e}$, set P_1 to be the perfect form contiguous to P through the facet $\mathfrak{f}$, g_1 the corresponding side transformation and $g := g_1$. In the i^{th} step, identify the facet $\mathfrak{f}$ of the Voronoï domain of P_{i-1} containing $\mathfrak{e}$ and satisfying

$\mathfrak{f} \cap D_{P_{i-2}} \neq \mathfrak{f}$ (this can be done by computing in the Voronoï domain of $g^{\dagger} P_{i-1} g \in \mathcal{V}$), and let P_i be the perfect neighbour of P_{i-1} through $\mathfrak{f}$, g_i the side transformation corresponding to the facet $g^{-1}\mathfrak{f} g^{-\dagger}$ of $D_{g^{\dagger} P_{i-1} g}$ and replace by g by gg_i.

The remaining relations described in Section 4 are easily computed. Finally it is useful to employ a computer algebra system capable of handling finitely presented groups in order to simplify the presentation.

The implementation of the algorithm to solve the word problem is straightforward since it merely amounts to computing the intersection of an affine line with an affine polytope.

References

[Ash84] A. Ash, *Small-dimensional classifying spaces for arithmetic subgroups of general linear groups*, Duke Math. J. **51** (1984) 459–468.

[Bas93] H. Bass, *Covering theory for graphs of groups*, J. Pure Appl. Algebra **89** (1993) 3–47.

[BCP97] W.Bosma, J. Cannon, C. Playoust, *The Magma algebra system I: The user language*, Journal of Symbolic Computation 24.3 (1997) 235–265.

[Bro84] K. S. Brown, *Presentations for groups acting on simply-connected complexes*, J. Pure Appl. Algebra **32** (1984) 1–10.

[Brü98] H. Brückner, *Algorithmen für endliche auflösbare Gruppen und Anwendungen*, Thesis, RWTH Aachen University, 1998.

[CJLdR04] C.Corrales, E. Jespers, G. Leal, A. del Río, *Presentations of the unit group of an order in a non-split quaternion algebra*, Adv. Math. **186** (2004) 498–524.

[CN14] R. Coulangeon, G. Nebe, *Maximal finite subgroups and minimal classes*, to appear in Enseign. Math.

[GaJ00] Ewgenij Gawrilow and Michael Joswig. *polymake: a framework for analyzing convex polytopes. Polytopes—combinatorics and computation* (Oberwolfach, 1997), 43–73, DMV Sem., 29, Birkhäuser, Basel, 2000

[Kle00] E. Kleinert, *Units in skew fields*, Progress in Mathematics 186, Birkhäuser, Basel 2000

[Kle94] E. Kleinert, *Units of classical orders: a survey*, Enseign. Math. (2) **40** (1994) 205–248.

[Mac64] A. M. Macbeath, *Groups of homeomorphisms of a simply connected space*, Ann. of Math. (2) **79** (1964) 473–488.

[Mar03] J. Martinet, *Perfect lattices in Euclidean spaces*, Grundlehren der Mathematischen Wissenschaften 327, Springer-Verlag, Berlin, 2003.

[NeS09] G. Nebe, A. Steel, *Recognition of Division Algebras* J. Algebra 322 (2009) 903–909.

[Opg01] J. Opgenorth, *Dual cones and the Voronoi algorithm*, Experiment. Math. **10** (2001) 599–608.

[PS97] W. Plesken, B. Souvignier, *Computing isometries of lattices*, Journal of Symbolic Computation 24.3 (1997) 327–334.

[Rei75] I. Reiner, *Maximal orders*, Academic press, London, 1975.

[Ril83] R. Riley, *Applications of a computer implementation of Poincaré's theorem on fundamental polyhedra.* Math. Comp. 40 (1983) 607–632.

[Ryš70] S. S. Ryškov, *The polyhedron $\mu(m)$ and certain extremal problems of the geometry of numbers*, Dokl. Akad. Nauk SSSR **194** (1970) 514–517.

[Sch09a] A. Schürmann, *Computational geometry of positive definite quadratic forms*, University Lecture Series, vol. 48, AMS, Providence, RI, 2009, Polyhedral reduction theories, algorithms, and applications.

[Sch09b] ______, *Enumerating perfect forms*, Quadratic forms—algebra, arithmetic, and geometry, Contemp. Math. 493, AMS, Providence, RI, 2009, 359–377.

[Ser77] J.-P. Serre, *Arbres, amalgames,* SL_2, SMF, Paris, 1977, Astérisque, No. 46.

[Shi65] H. Shimizu, *On zeta functions of quaternion algebras.* Ann. of Math. 81 (1965) 166–193.

[Sou78] C. Soulé, *The cohomology of* $\mathrm{SL}_3(\mathbf{Z})$, Topology **17** (1978) 1–22.

[Ste07] W. Stein, *Modular forms, a computational approach*, Graduate Studies in Mathematics, vol. 79, AMS, Providence, RI, 2007, With an appendix by Paul E. Gunnells.

[Swa71] R.G. Swan, *Generators and relations for certain special linear groups.* Advances in Math. 6 (1971) 1–77.

[Vor07] G. F. Voronoï, *Nouvelles applications des paramètres continus à la théorie des formes quadratiques : 1 sur quelques propriétés des formes quadratiques parfaites*, J. Reine Angew. Math. **133** (1907) 97–178.

[WYH13] Takao Watanabe, Syouji Yano, and Takuma Hayashi, *Voronoï's reduction theory of GL_n over a totally real number field*, Diophantine methods, lattices, and arithmetic theory of quadratic forms, Contemp. Math. 587, AMS, Providence, RI, 2013, 213–232.

[Yas10] D. Yasaki, *Hyperbolic tessellations associated to Bianchi groups*, Algorithmic number theory, Lecture Notes in Comput. Sci. 6197, Springer, Berlin, 2010, 385–396.