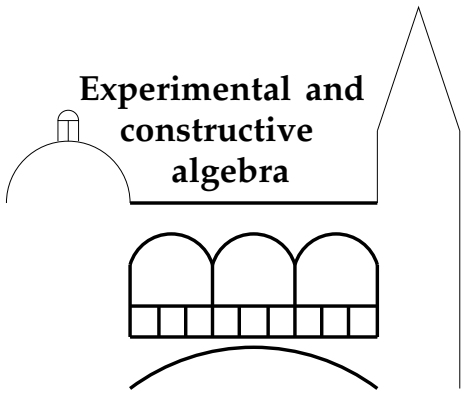
# Computing in unit groups of orders with Voronoi's algorithm

Luxembourg Number Theory Seminar

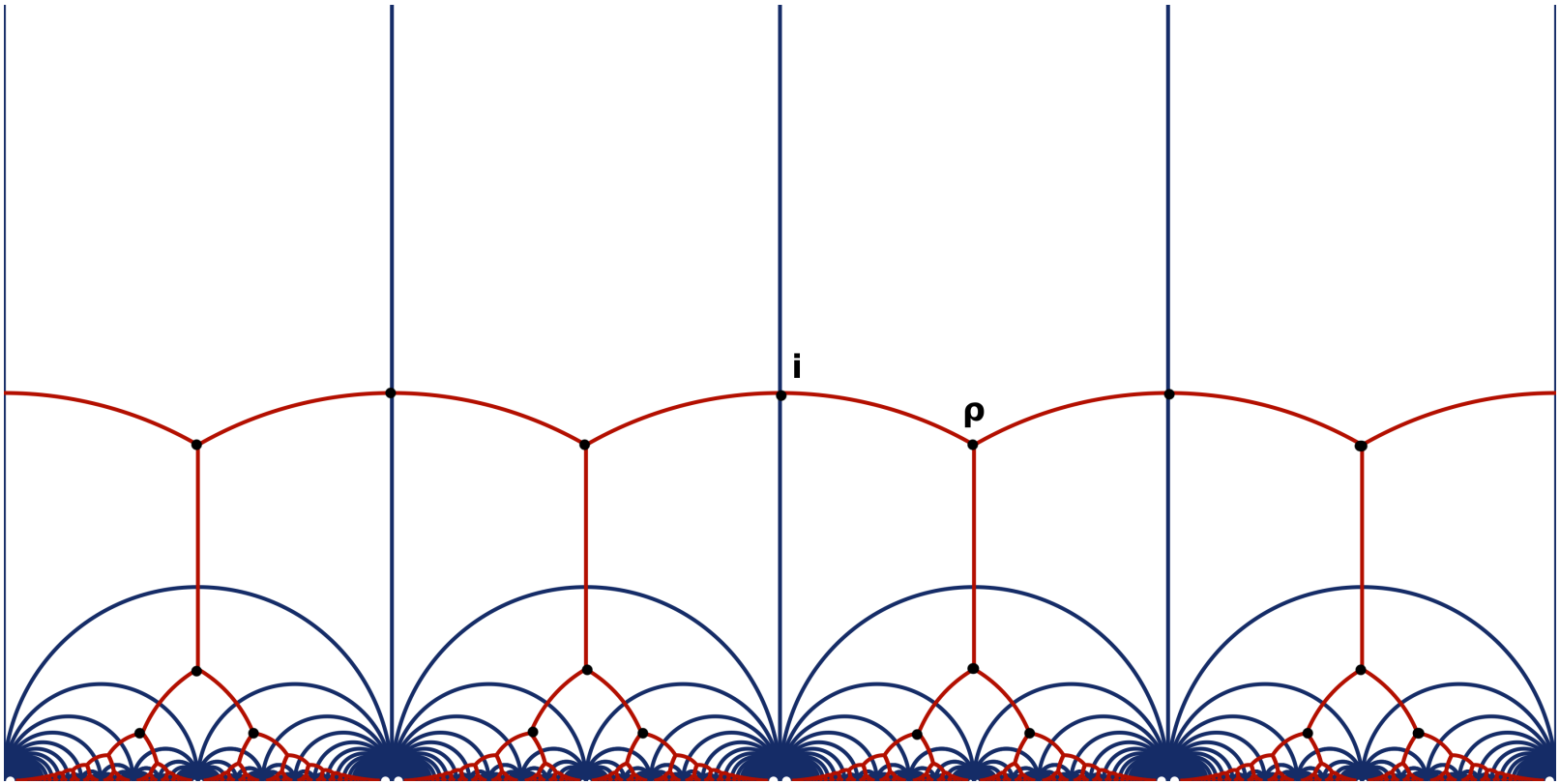
Sebastian Schönnenbeck
joint work with O. Braun, R. Coulangeon, and G. Nebe
December 7, 2016




RWTH AACHEN UNIVERSITY

# Motivation

The well known isomorphism $\Gamma = \mathrm{SL}_2(\mathbb{Z}) \cong C_4 *_{C_2} C_6$ (or $\mathrm{GL}_2(\mathbb{Z}) \cong D_8 *_{C_2} D_{12}$) is obtained by studying the action of $\Gamma$ on a tree in the upper half plane:




## Question

Can this approach be generalized to other groups that are “similar” to $\mathrm{SL}_2(\mathbb{Z})$?

# Motivation II

## Groups

There are plenty of algorithms readily available for dealing with finite groups in various guises (permutation groups, matrix groups, black box groups,...). However, there are only very few computational methods for infinite groups.

## Aim

What would like to be able to do?

- Compute a system of generators.
- Compute the defining relations.
- Perform constructive membership in these generators.
- Classify finite subgroups.
- ...

## Idea

For certain classes of groups find a general construction of a space with a suitable action and exploit this to solve these problems.

# Unit groups of orders

What groups can we deal with?

## Situation

$A$ a semisimple $\mathbb{Q}$-algebra $\rightsquigarrow A \cong \bigoplus_i D_i^{n_i \times n_i}$ (each $D_i$ a division algebra).
$\Lambda \subset A$ a $\mathbb{Z}$-order in $A$ (i.e. a subring of $A$ that is finitely generated as an $\mathbb{Z}$-module and contains a basis of $A$). We want to answer our questions for $\Lambda^\times$.

## Examples

- $A = \mathbb{Q}^{n\times n}, \Lambda = \mathbb{Z}^{n\times n}, \Lambda^\times = \mathrm{GL}_n(\mathbb{Z})$.
- $A$ an algebraic number field with ring of integers $\Lambda$ and corresponding unit group $\Lambda^\times \cong \mathbb{Z}^{r+s-1}$ (Dirichlet).
- $G$ a finite group, $A = \mathbb{Q}G$, and $\Lambda = \mathbb{Z}G$.
- $A = \left(\frac{-1,-1}{\mathbb{Q}}\right) = \langle 1, i, j, ij\rangle_{\mathbb{Q}}$ quaternion algebra, $\Lambda = \langle 1, i, j, ij\rangle_{\mathbb{Z}}$, $\Lambda^\times = \langle i, j\rangle \cong Q_8$.
- $A$ a division algebra of dimension greater than $4$ over its center. Next to nothing is known about $\Lambda^\times$.

# $\mathrm{GL}_n(\mathbb{Z})$ and the classical Voronoi algorithm

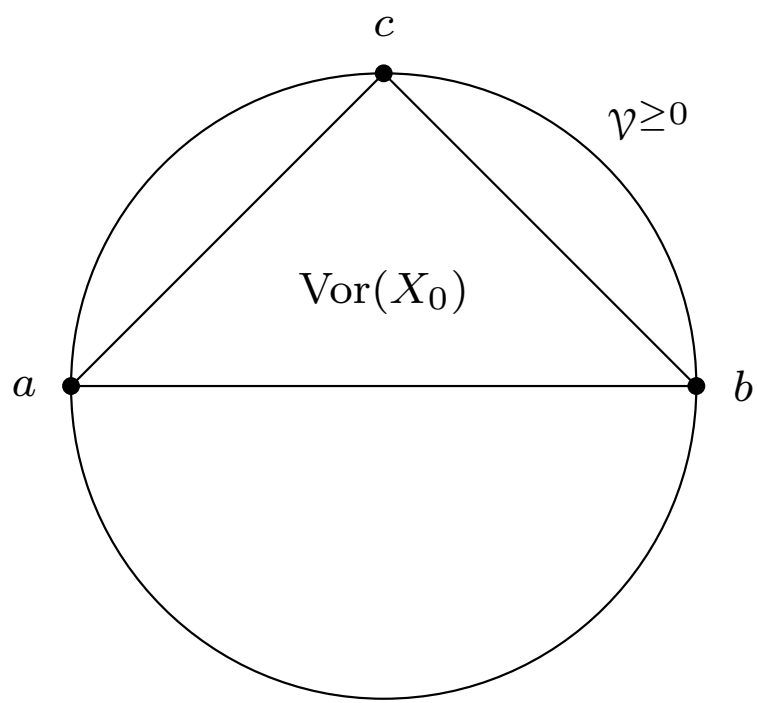
## Setup

- $\mathcal{V} = \{X \in \mathbb{R}^{n\times n} : X^{tr} = X\}$.
- $\mathcal{V}^{\geq 0}, \mathcal{V}^{>0} \subset \mathcal{V}$ the cone of positive (semi-)definite matrices.
- $X \in \mathcal{V}^{>0}$, $\mu(X) = \min\limits_{0\neq v\in\mathbb{Z}^n} vXv^{tr}$ the *minimum* of $X$.
- $\mathcal{M}(X) := \{v \in \mathbb{Z}^{1\times n} : vXv^{tr} = \mu(X)\}$ the *shortest vectors* of $X$.
- $\mathrm{Vor}(X) = \mathrm{cone}(\{v^{tr}v : v \in \mathcal{M}(X)\}) \subset \mathcal{V}^{\geq 0}$ the *Voronoi domain* of $X$.
- $X$ *perfect*, iff $\mathrm{Vor}(X)$ has non-empty interior, i.e. $\dim(\langle \mathrm{Vor}(X)\rangle) = \frac{n(n+1)}{2}$.

$\mathrm{GL}_n(\mathbb{Z})$ acts on $\mathcal{V}^{>0}$ with finitely many orbits on the set of perfect forms (up to rescaling). The Voronoi domains of perfect forms form a face-to-face tessellation of $\mathcal{V}^{\geq 0}$ that can be computed algorithmically.

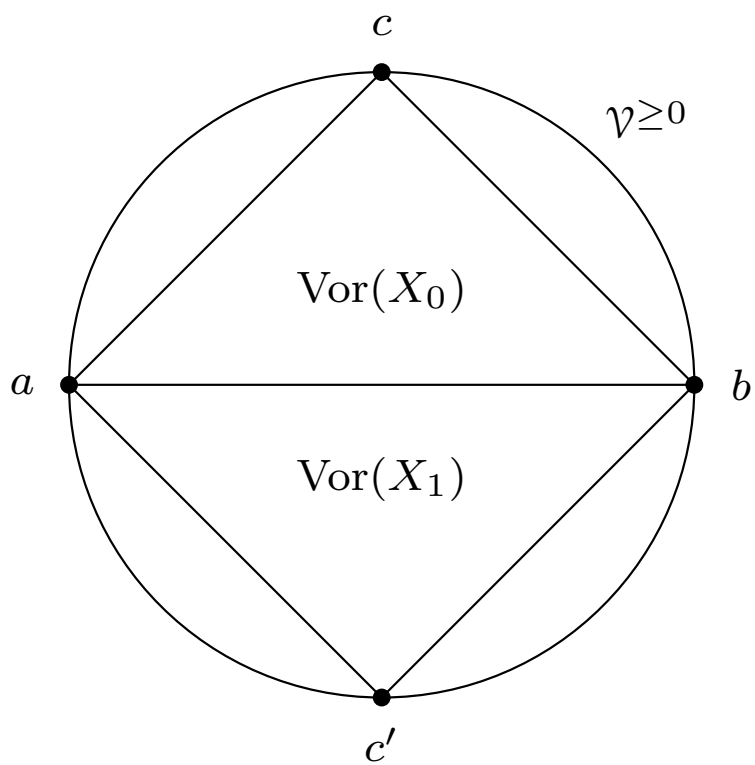
# The case $\mathrm{GL}_2(\mathbb{Z})$

- $n = 2$, $\dim(\mathcal{V}) = 3$, and $\dim(\mathcal{V}^{>0}/\mathbb{R}_{>0}) = 2$.
- We visualize $\mathcal{V}^{\geq 0}/\mathbb{R}_{>0}$ as $\mathcal{V}^{\geq 0} \cap \{X : \mathrm{Tr}(X) = 4\}$.
- $X_0 := \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$, $\mu(X_0) = 2$, $\mathcal{M}(X_0) = \{\pm e_1, \pm e_2, \pm(e_1 + e_2)\}$.
- $\mathrm{Vor}(X_0) = \mathrm{cone}\left(a = \begin{pmatrix} 4 & 0 \\ 0 & 0 \end{pmatrix}, b = \begin{pmatrix} 0 & 0 \\ 0 & 4 \end{pmatrix}, c = \begin{pmatrix} 2 & 2 \\ 2 & 2 \end{pmatrix}\right)$, $X_0$ is perfect.



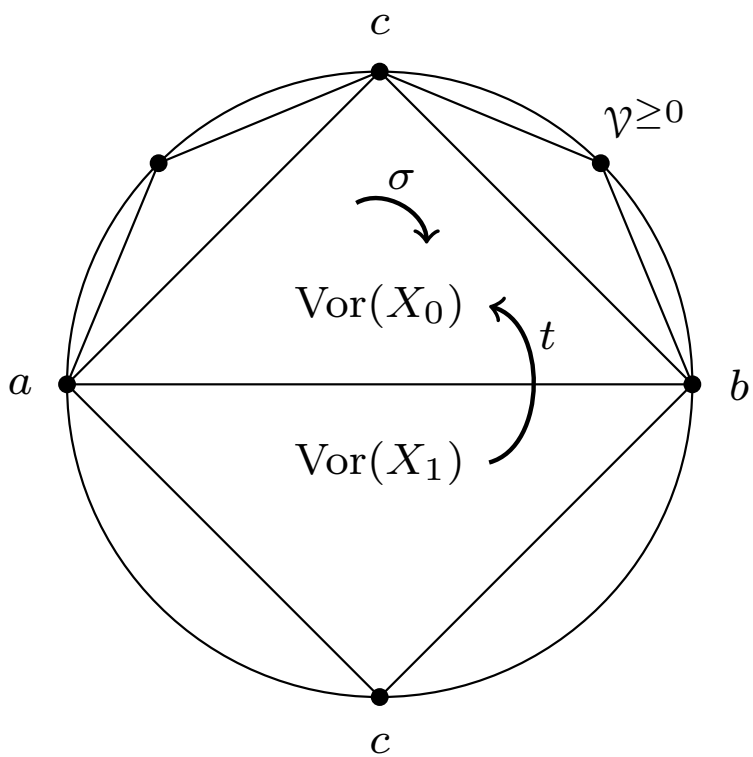
# The case $\mathrm{GL}_2(\mathbb{Z})$ (II)

- $X_1 = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ has $\mathcal{M}(X_1) = \{\pm e_1, \pm e_2, \pm(e_1 - e_2)\}$, and is again perfect.
- $\mathrm{Vor}(X_1) = \mathrm{cone}(a, b, c')$, where $c' = \begin{pmatrix} 2 & -2 \\ -2 & 2 \end{pmatrix}$.
- $X_1$ is in the $\mathrm{GL}_2(\mathbb{Z})$-orbit of $X_0$, $X_1 = tX_0t^{tr}$, where $t = \mathrm{diag}(1, -1)$.
- The same holds for the other two *neighbours* of $X_0$.



# Generators for $\mathrm{GL}_2(\mathbb{Z})$

- $\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(X_0) = \left\langle \sigma = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, \tau = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle \cong D_{12}$.
- $\sigma \cdot (b, c) = (a, b), \sigma(c, a) = (b, c)$ (i.e. the stabilizer is transitive on the neighbours).
- $\mathrm{GL}_2(\mathbb{Z})$ is generated by $\sigma, \tau$ and $t$.



# The Voronoi algorithm

## Some remarks

- Original idea due to Korkine, Zolotareff, and Voronoi ($\sim$1900).
- Perfect forms classify densest sphere packings (local maxima of the density function are perfect and eutactic).
- All perfect forms are known up to dimension $8$:

| Dim. | $2$ | $3$ | $4$ | $5$ | $6$ | $7$ | $8$ | $9$ |
|---|---|---|---|---|---|---|---|---|
| $\#$ | $1$ | $1$ | $2$ | $3$ | $7$ | $33$ | $10916$ | $> 500000$ |

- M. Koecher developed a generalization of Voronoi theory that applies to self-dual cones (e.g. the cone of positive definite matrices).
- J. Opgenorth employed this to compute integral normalizer of certain finite matrix groups.
- M. Mertens used the approach to compute automorphism groups of hyperbolic lattices.

# The general situation

## Symmetric elements

$D$ a $\mathbb{Q}$-division algebra, $A \cong D^{n\times n}$ a simple rational algebra.

- $A_{\mathbb{R}} := A \otimes_{\mathbb{Q}} \mathbb{R}$ is a semi-simple $\mathbb{R}$-algebra, hence a direct sum of matrix rings over $\mathbb{R}, \mathbb{C}$, and $\mathbb{H}$.
- $\mathbb{R}, \mathbb{C}$, and $\mathbb{H}$ carry a natural involution $\rightsquigarrow A_{\mathbb{R}}$ carries a natural involution $\dagger$ via transposition and applying the underlying involution entry-wise.
- $\mathcal{V} := A_{\mathbb{R}}^{\text{sym}} := \{F \in A_{\mathbb{R}} : F^\dagger = F\}$.
- $\sigma(X, Y) := \mathrm{Tr}(XY)$ is a Euclidean inner product on $\mathcal{V}$.

## The positive cone

Set $V := D^{1\times n}$ (the unique right $A$-module) and $V_{\mathbb{R}} := V \otimes_{\mathbb{Q}} \mathbb{R}$.

- For $v \in V_{\mathbb{R}}$ we have $v^\dagger v \in \mathcal{V}$.
- $F \in \mathcal{V}$ defines a quadratic form on $V_{\mathbb{R}}$ via

$$F[v] = \sigma(F, v^\dagger v).$$

- $F \in \mathcal{V}$ is called positive if this form is positive definite (we write $\mathcal{V}^{>0}$).

# Minimal vectors

## The order

Let $\mathfrak{O} \subset D$ be a maximal $\mathbb{Z}$-order in $D$ and $L \subset V$ an $\mathfrak{O}$-lattice in $V$ (i.e. a finitely generated $\mathfrak{O}$-submodule of $V$ that contains a basis of $V$).

- $\Lambda := \mathrm{End}_{\mathfrak{O}}(L) = \{a \in A : La \subset L\}$ is a maximal order in $A$ (and each maximal order of $A$ is of this form).
- $\Lambda^\times = \mathrm{GL}(L) = \{a \in A : La = L\}$.

## $L$-minimal vectors

Let $X \in \mathcal{V}^{>0}$.

- $\mu(X) := \mu_L(X) := \min_{0 \neq v \in L} X[v]$ the *$L$-minimum* of $X$.
- $\mathcal{M}(X) := \mathcal{M}_L(X) := \{v \in L : X[v] = \mu(X)\}$ the *$L$-minimal vectors* of $X$.
- $\mathrm{Vor}(X) := \mathrm{Vor}_L(V) := \mathrm{cone}(\{v^\dagger v : v \in \mathcal{M}(X)\}) \subset \mathcal{V}^{\geq 0}$ the *Voronoi-domain* of $X$.
- $X$ is *$L$-perfect* if $\dim(\mathrm{Vor}(X)) = \dim(\mathcal{V})$.

## The tessellation

The set of Voronoi domains of perfect forms, $\{\mathrm{Vor}(X) : X\ L-\text{perfect}\}$, forms a face-to-face tessellation of $\mathcal{V}^{\geq 0}$ and $\Lambda^\times$ acts with finitely many orbits.

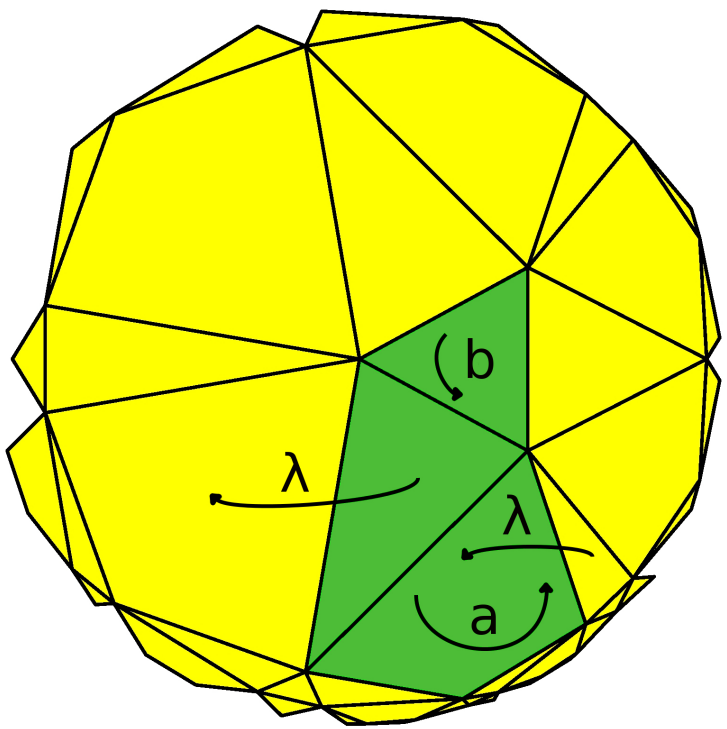
# Generators

## Finding a generating system for $\Lambda^\times$

- Compute a system of representatives $\{X_1, ..., X_r\}$ of $L$-perfect forms modulo $\Lambda^\times$.
- For each $X_i$ compute the finite group $\mathrm{Aut}(X_i) := \mathrm{Stab}_{\Lambda^\times}(X_i)$.
- For each neighbour $Y$ of the $X_i$ compute an element $\lambda_Y \in \Lambda_\times$ such that $\lambda_Y Y \in \{X_1, ..., X_r\}$.
- $\Lambda^\times$ is generated by the groups $\mathrm{Aut}(X_i)$ and the elements $\lambda_Y$.

**Example:**

- $A = D = Q_{2,3} = \left(\frac{2,3}{\mathbb{Q}}\right)$.
- Maximal order $\Lambda = \langle 1, i, \frac{1}{2}(1 + i + ij), \frac{1}{2}(j + ij)\rangle$.
- $V = A, L = \Lambda, A_{\mathbb{R}} \cong \mathbb{R}^{2\times 2}$ (via embedding $A \hookrightarrow \mathbb{Q}(\sqrt{2})^{2\times 2}$)
- 3 perfect forms up to $\Lambda^\times$-action
- $\Lambda^\times = \langle a, b, \lambda\rangle$.



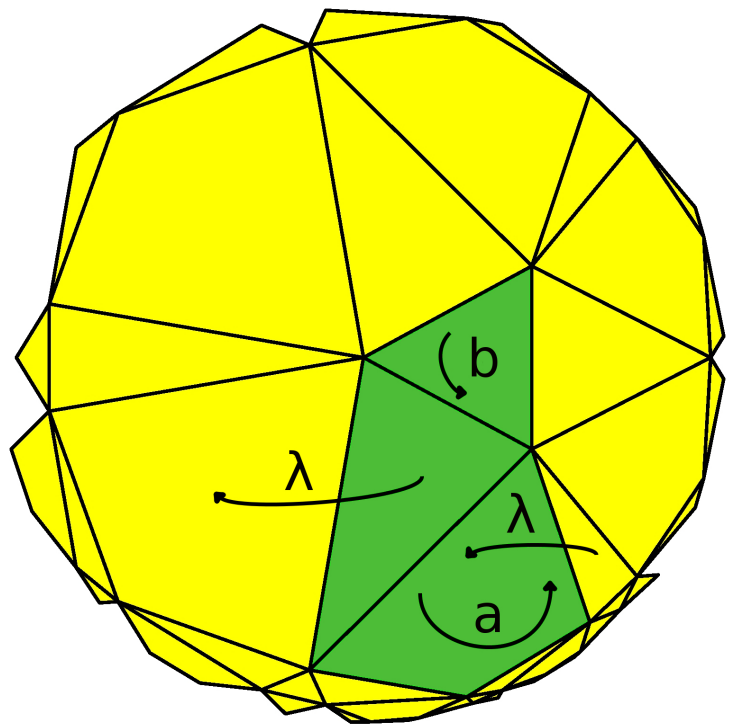
## Relations (Bass, Serre, Brown)

The defining relations between the generators from the last slide are:

- The multiplication table of the finite stabilizers.
- Relations from the action of the stabilizers on the neighbours.
- Relations from “running around” an edge (codimension-$2$ face).
- Poincaré relations from edges that are mapped to one another under the $\lambda_Y$.

**Example:**

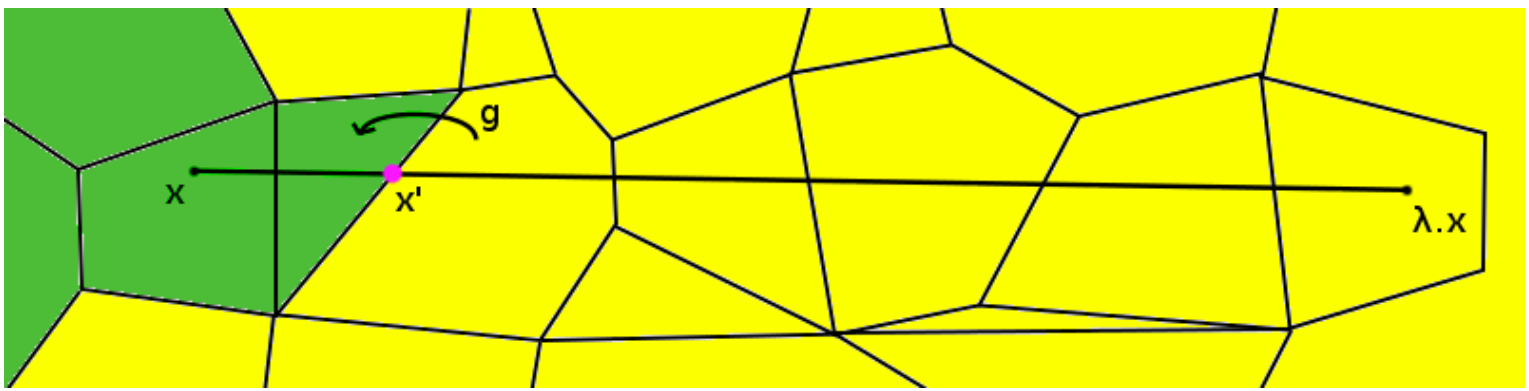
- As before $A = D = Q_{2,3} = \left(\frac{2,3}{\mathbb{Q}}\right)$ with maximal order $\Lambda$.
- Presentation: $\Lambda^\times/\langle -1\rangle \cong \langle a, b, \lambda | a^2, b^3, a\lambda b\lambda\rangle$.



# Constructive Membership

**Aim:** Write $\lambda \in \Lambda^\times$ as a word in our generators.

1. Choose $x$ in the interior of the Voronoi domain of $X_1$ and compute $\lambda x$.
2. Consider the geodesic $\mathcal{G}$ between $x$ and $\lambda x$.
3. $\mathcal{G}$ intersects the boundary of the fundamental domain in $x'$ (with corresponding neighbour $Y$ and generator $g = \lambda_Y$.
4. The geodesic between $x'$ and $\lambda x$ intersects fewer Voronoi domains
   Continue with $x \to gx'$, $\lambda x \to g\lambda x$, $\lambda \to g\lambda$.
5. After finitely many steps we are left with an element of the stabilizer of $X_1$.

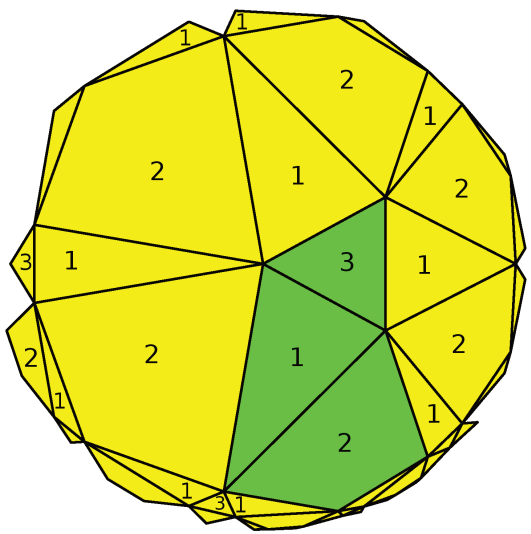


# Overview

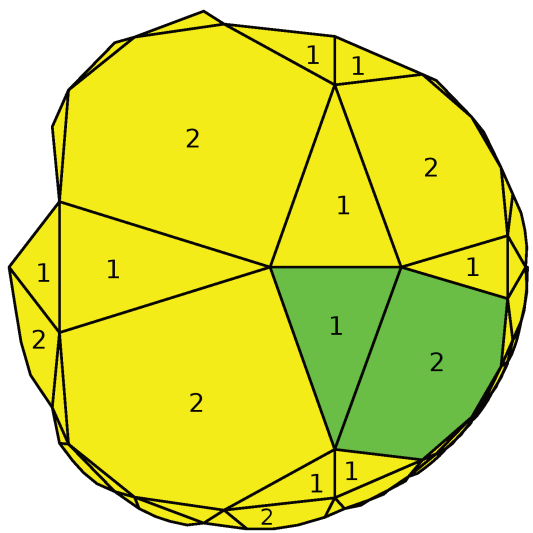
## Some remarks

- Perfect forms and the tessellation depend on the chosen isomorphism for $A_{\mathbb{R}}$.
- Applicability of the algorithm(s) limited in terms of $\dim_{\mathbb{Q}}(A)$ and $\mathrm{disc}(\Lambda)$ (Bottleneck: polytope computations).
- Computation of a presentation faster than previously known algorithms (e.g. $Q_{19,37}$ about 5 minutes (88 generators, 288 perfect forms), whereas MAGMA's `FuchsianGroup` does not produce a presentation within four hours).
- First known algorithm for most unit groups (e.g. division algebra of index $3$, quaternion algebras with CM-field of degree $\geq 4$ as a center,...).

$Q_{2,3} \hookrightarrow \mathbb{Q}(\sqrt{2})^{2\times 2}$:



$Q_{2,3} \hookrightarrow \mathbb{Q}(\sqrt{3})^{2\times 2}$:



# Minimal classes

For more advanced questions about $\Lambda^\times$ we need a refinement of the perfect form theory.

## Minimal classes

Let $X, Y \in \mathcal{V}^{>0}$.

- $X$ and $Y$ are *minimally equivalent* if $\mathcal{M}(X) = \mathcal{M}(Y)$.
- $C(X) := C(\mathcal{M}(X)) := \{X' \in \mathcal{V}^{>0} : X, X' \text{ minimally equivalent}\}$ is called the *minimal class* of $X$ (note $X$ is perfect iff $C(X) = \mathbb{R}_{>0} \cdot X$).
- $C(X)$ (or equivalently $X$ itself) is called *well-rounded* if $\mathcal{M}(X)$ contains a basis of $V$.

## The cell decomposition

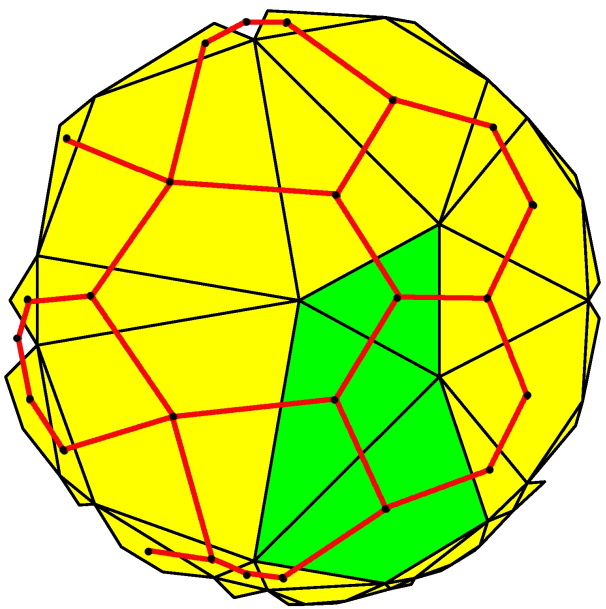
- The minimal classes yield a partition of $\mathcal{V}^{>0}$ (the corresponding tessellation is the dual of the Voronoi tessellation).
- The action of $\Lambda^\times$ respects this decomposition.
- $C(X)$ is convex and $\overline{C(X)} = \bigcup_{\mathcal{M}(X) \subset \mathcal{M}(Y)} C(Y)$ (topological closure).

# The well-rounded retract

## Well-rounded forms

- $\mathrm{Aut}(C(X)) := \mathrm{Stab}_{\Lambda^\times}(C(X))$ (as a set) is finite iff $C(X)$ is well-rounded.
- The set of well-rounded forms is a retract of $\mathcal{V}^{>0}$ (i.e. every forms can be continuously transformed into a well-rounded form).
- $X$ well-rounded implies $C(X)$ is the convex hull of the (finitely many) perfect forms in its boundary.
- There are only finitely many well-rounded classes up to $\Lambda^\times$ action.

The well-rounded complex of $Q_{2,3}$:



Well-rounded classes for $\mathrm{GL}_2(\mathbb{Z})$:

- One orbit of perfect forms (dimension $0$ minimal class), represented by $X_0 = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$.
- One orbit of dimension $1$ minimal classes, represented by $Y = \mathrm{diag}(2, 2)$.
- $C(Y)$ is the convex hull of $X_0$ and $X_1 = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$.

# Maximal finite subgroups

## Theorem (Coulangeon, Nebe)

Every maximal finite subgroup of $\Lambda^\times$ appears as a stabilizer of a well-rounded minimal class. Moreover it is possible to check if a finite subgroup is maximal finite using Voronoi theory.

## Example

$D = \mathbb{Q}(\sqrt{-6}), A = \mathbb{Q}^{2\times 2}, \mathcal{O} = \mathbb{Z}[\sqrt{-6}], L = \mathcal{O}^2.$

Well-rounded classes and stabilizers

| Class $C$ | $G = \mathrm{Aut}(C)$ | maximal? |
|---|---|---|
| $P_1$ | $\mathrm{SL}(2,3)$ | yes |
| $E_1$ | $D_{12}$ | yes |
| $E_2$ | $D_{12}$ | yes |
| $E_3$ | $C_4$ | no |
| $E_4$ | $D_8$ | yes |
| $C_1$ | $D_8$ | yes |
| $C_2$ | $D_8$ | yes |
| $C_3$ | $C_2 \times C_2$ | yes |

# Resolutions and (co)homology

## Theorem (Wall, Ash, Ellis,...)

The action of $\Lambda^\times$ on the well-rounded retract can also be used to construct a free resolution of $\mathbb{Z}$ (as a $\mathbb{Z}[\Lambda^\times]$-module), and thus to compute the (co)homology of $\Lambda^\times$.

## Examples

- $A = Q_{2,3}$ as before:

$$\mathrm{H}_n(\Lambda^\times, \mathbb{Z}) = \begin{cases} C_{24} & n \equiv 1 \pmod 2 \\ C_2 & n \equiv 0 \pmod 2 \end{cases}$$

- $A = \mathbb{Q}(\sqrt{-6})^{2\times 2}$, $\Lambda$ as before:

$$\mathrm{H}_n(\Lambda^\times, \mathbb{Z}) = \begin{cases} C_2^4 & n = 1 \\ C_4^2 \times C_{12} \times \mathbb{Z} & n = 2 \\ C_2^9 \times C_{24} & n = 3 \\ C_2^7 & n = 4 \end{cases}$$

Thank you for your attention.