Computing Unit Groups of Orders

Gabriele Nebe, Oliver Braun, Sebastian Schönnenbeck

Lehrstuhl D für Mathematik

Bad Boll, March 5, 2014

RWTH AACHEN UNIVERSITY

The classical Voronoi Algorithm

- Around 1900 Korkine, Zolotareff, and Voronoi developed a reduction theory for quadratic forms.
- The aim was to classify the densest lattice sphere packings in n-dimensional Euclidean space.
- lattice $L = \mathbb{Z}^{1\times n}$, Euclidean structure on L given by some some positive definite $F \in \mathbb{R}^{n\times n}_{sym}$, $(x,y) = xFy^{tr}$.
- Voronoi described an algorithm to find all local maxima of the density function on the space of all n-dimensional positive definite F.
- They are perfect forms (as will be defined below).
- There are only finitely many perfect forms up to the action of $\mathrm{GL}_n(\mathbb{Z})$, the unit group of the order $\mathbb{Z}^{n\times n}$.
- Later, Voronoi's algorithm has been used to compute generators and relations for $\mathrm{GL}_n(\mathbb{Z})$ but also its integral homology groups.
- It has been generalised to other situations: compute integral normalizer, the automorphism group of hyperbolic lattices and
- more general unit groups of orders.

Unit groups of orders

- A separable $\mathbb{Q}$-algebra, so $A \cong \bigoplus_{i=1}^{s} D_i^{n_i \times n_i}$, is a direct sum of matrix rings over division algebras.
- An order Λ in A is a subring that is finitely generated as a $\mathbb{Z}$-module and such that $\langle \Lambda \rangle_{\mathbb{Q}} = A$.
- Its unit group is $\Lambda^* := \{u \in \Lambda \mid \exists v \in \Lambda, uv = 1\}$.
- Know in general: Λ^* is finitely generated.
- Example: $A = K$ a number field, $\Lambda = O_K$, its ring of integers. Then Dirichlet's unit theorem says that $\Lambda^* \cong \mu_K \times \mathbb{Z}^{r+s-1}$.
- Example: $\Lambda = \langle 1, i, j, ij \rangle_{\mathbb{Z}}$ with $i^2 = j^2 = (ij)^2 = -1$. Then $\Lambda^* = \langle i, j \rangle$ the quaternion group of order 8.
- Example: $A = \mathbb{Q}G$ for some finite group G, $\Lambda = \mathbb{Z}G$.
- Example: A a division algebra with $\dim_{Z(A)}(A) = d^2 > 4$. Not much known about the structure of Λ^*.
- Voronoi's algorithm may be used to compute generators and relations for Λ^* and to solve the word problem.
- Seems to be practical for "small" A and for $d = 3$.

The classical Voronoi Algorithm

Korkine, Zolotareff, Voronoi, $\sim$ 1900.

Definition

- $\mathcal{V} := \{X \in \mathbb{R}^{n\times n} \mid X = X^{tr}\}$ space of symmetric matrices
- $\sigma : \mathcal{V} \times \mathcal{V} \to \mathbb{R}$, $\sigma(A,B) := \mathrm{trace}(AB)$ Euclidean inner product on $\mathcal{V}$.
- for $F \in \mathcal{V}$, $x \in \mathbb{R}^{1\times n}$ define $F[x] := xFx^{tr} = \sigma(F, x^{tr}x)$
- $\mathcal{V}^{>0} := \{F \in \mathcal{V} \mid F$ positive definite $\}$
- for $F \in \mathcal{V}^{>0}$ define the minimum $\mu(F) := \min\{F[x] : 0 \neq x \in \mathbb{Z}^{1\times n}\}$ and $\mathcal{M}(F) := \{x \in \mathbb{Z}^{1\times n} \mid F[x] = \mu(F)\}$
- $\mathrm{Vor}(F) := \{\sum_{x\in\mathcal{M}(F)} a_x x^{tr} x \mid a_x \geq 0\}$ the Voronoi domain
- F is called perfect $\Leftrightarrow \dim(\mathrm{Vor}(F)) = \dim(\mathcal{V}) = \frac{n(n+1)}{2}$.

Remark

$\mathrm{GL}_n(\mathbb{Z})$ acts on $\mathcal{V}^{>0}$ by $(F,g) \mapsto g^{-1}Fg^{-tr}$. Then

$$\begin{aligned} \mathcal{M}(g^{-1}Fg^{-tr}) &= \{xg \mid x \in \mathcal{M}(F)\} \\ \mathrm{Vor}(g^{-1}Fg^{-tr}) &= g^{tr}\,\mathrm{Vor}(F)g \end{aligned}$$

The classical Voronoi Algorithm

Korkine, Zolotareff, Voronoi, $\sim$ 1900.

Definition

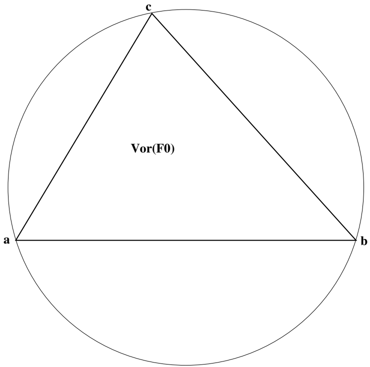
- $\mathcal{V} := \{X \in \mathbb{R}^{n\times n} \mid X = X^{tr}\}$ space of symmetric matrices
- $\sigma : \mathcal{V} \times \mathcal{V} \to \mathbb{R}$, $\sigma(A,B) := \mathrm{trace}(AB)$ Euclidean inner product on $\mathcal{V}$.
- for $F \in \mathcal{V}$, $x \in \mathbb{R}^{1\times n}$ define $F[x] := xFx^{tr} = \sigma(F, x^{tr}x)$
- $\mathcal{V}^{>0} := \{F \in \mathcal{V} \mid F$ positive definite $\}$
- for $F \in \mathcal{V}^{>0}$ define the minimum $\mu(F) := \min\{F[x] : 0 \neq x \in \mathbb{Z}^{1\times n}\}$ and $\mathcal{M}(F) := \{x \in \mathbb{Z}^{1\times n} \mid F[x] = \mu(F)\}$
- $\mathrm{Vor}(F) := \{\sum_{x\in\mathcal{M}(F)} a_x x^{tr} x \mid a_x \geq 0\}$ the Voronoi domain
- F is called perfect $\Leftrightarrow \dim(\mathrm{Vor}(F)) = \dim(\mathcal{V}) = \frac{n(n+1)}{2}$.

Theorem (Voronoi)

(a) $\mathcal{T} := \{\mathrm{Vor}(F) \mid F \in \mathcal{V}^{>0},$ perfect $\}$ forms a face to face tesselation of $\mathcal{V}^{\geq 0}$.
(b) $\mathrm{GL}_n(\mathbb{Z})$ acts on $\mathcal{T}$ with finitely many orbits that may be computed algorithmically.

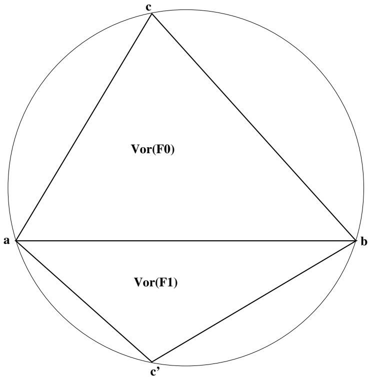
Example, generators for $\mathrm{GL}_2(\mathbb{Z})$

- $n = 2$, $\dim(\mathcal{V}) = 3$, $\dim(\mathcal{V}^{>0}/\mathbb{R}_{>0}) = 2$
- compute in affine section of the projective space
- $\mathcal{A}^{\geq 0} = \{F \in \mathcal{V}^{\geq 0} \mid \mathrm{trace}(F) = 1\}$
- $F_0 = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$, $\mu(F_0) = 2$, $\mathcal{M}(F_0) = \{\pm(1,0), \pm(0,1), \pm(1,1)\}$
- $\mathcal{A}^{\geq 0} \cap \mathrm{Vor}(F_0) = \mathrm{conv}(a = \begin{pmatrix} 10 \\ 00 \end{pmatrix}, b = \begin{pmatrix} 00 \\ 01 \end{pmatrix}, c = \frac{1}{2}\begin{pmatrix} 11 \\ 11 \end{pmatrix})$



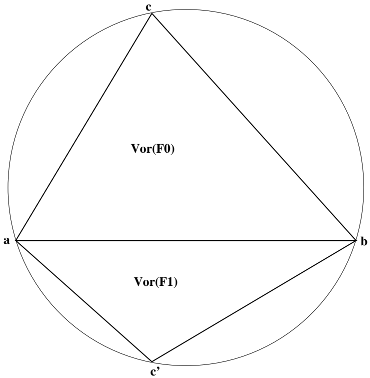
Example, generators for $\mathrm{GL}_2(\mathbb{Z})$

- $n = 2$, $\dim(\mathcal{V}) = 3$, $\dim(\mathcal{V}^{>0}/\mathbb{R}_{>0}) = 2$
- compute in affine section of the projective space
- $\mathcal{A}^{\geq 0} = \{F \in \mathcal{V}^{\geq 0} \mid \mathrm{trace}(F) = 1\}$
- $F_0 = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$, $\mu(F_0) = 2$, $\mathcal{M}(F_0) = \{\pm(1,0), \pm(0,1), \pm(1,1)\}$
- $\mathcal{A}^{\geq 0} \cap \mathrm{Vor}(F_0) = \mathrm{conv}(a = \begin{pmatrix} 10 \\ 00 \end{pmatrix}, b = \begin{pmatrix} 00 \\ 01 \end{pmatrix}, c = \frac{1}{2}\begin{pmatrix} 11 \\ 11 \end{pmatrix})$



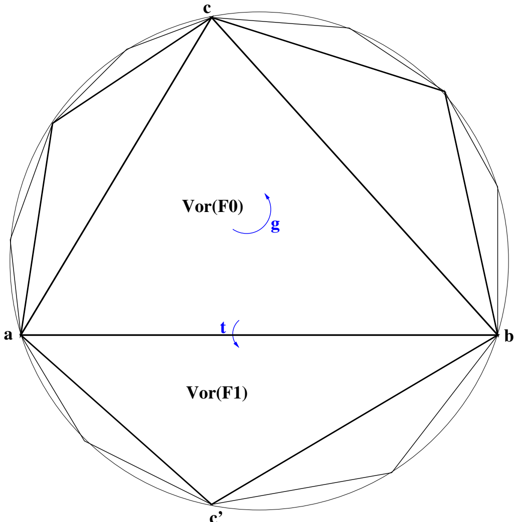
Example, generators for $\mathrm{GL}_2(\mathbb{Z})$

- Compute neighbor: $F_1 \in \mathcal{V}^{>0}$ so that $\mathrm{Vor}(F_1) = \mathrm{conv}(a, b, c')$.
- linear equation on F_1: $\mathrm{trace}(F_1 a) = \mathrm{trace}(F_1 b) = 2$ and $\mathrm{trace}(F_1 c) > 2$,
- so $F_1 = F_0 + sX$ where $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ generates $\langle a, b\rangle^{\perp}$.
- For $s = 2$ the matrix $F_1 = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ has again 6 minimal vectors
- $\mathcal{M}(F_1) = \{\pm(1,0), \pm(0,1), \pm(1,-1)\}$
- $\mathcal{A}^{\geq 0} \cap \mathrm{Vor}(F_1) = \mathrm{conv}(a, b, c' := \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix})$



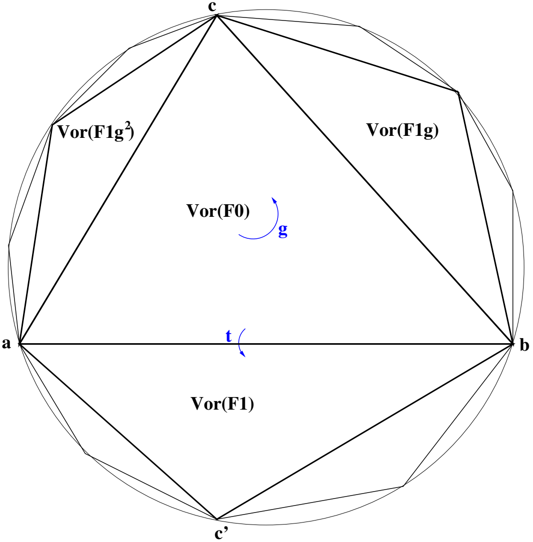
Example, generators for $\mathrm{GL}_2(\mathbb{Z})$

- $\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(F_0) = \langle g = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, h = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rangle$
- $(a, b) \cdot g = (b, c)$, $(b, c) \cdot g = (c, a)$
- Compute isometry $t = \mathrm{diag}(1, -1) \in \mathrm{GL}_2(\mathbb{Z})$, so $t^{-1} F_0 t^{-tr} = F_1$.
- Then $\mathrm{GL}_2(\mathbb{Z}) = \langle g, h, t \rangle$.



$\mathrm{GL}_2(\mathbb{Z}) = \langle g, h, t \rangle$.

- $\mathrm{Stab}_{\mathrm{GL}_2(\mathbb{Z})}(F_0) = \langle g = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}, h = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \rangle$
- $(a, b) \cdot g = (b, c)$, $(b, c) \cdot g = (c, a)$
- Compute isometry $t = \mathrm{diag}(1, -1) \in \mathrm{GL}_2(\mathbb{Z})$, so $t^{-1} F_0 t^{-tr} = F_1$.



Variations of Voronoi's algorithm

- Many authors used this algorithm to compute integral homology groups of $\mathrm{SL}_n(\mathbb{Z})$ and related groups, as developed C. Soulé in 1978.
- Max Köcher developed a general Voronoi Theory for pairs of dual cones in the 1950s.
  $\sigma : \mathcal{V}_1 \times \mathcal{V}_2 \to \mathbb{R}$ non degenerate and positive on the cones $\mathcal{V}_1^{>0} \times \mathcal{V}_2^{>0}$.
  discrete admissible set $D \subset \mathcal{V}_2^{>0}$ used to define minimal vectors and perfection for $F \in \mathcal{V}_1^{>0}$ and $\mathrm{Vor}_D(F) \subset \mathcal{V}_2{}^{>0}$.
- J. Opgenorth (2001) used Köcher's theory to compute the integral normalizer $N_{\mathrm{GL}_n(\mathbb{Z})}(G)$ for a finite unimodular group G.
- M. Mertens (Masterthesis, 2012) applied Köcher's theory to compute automorphism groups of hyperbolic lattices.
- This talk will explain how to apply it to obtain generators and relations for **unit group of orders** in semi-simple rational algebras and an algorithm to solve the word problem in these generators.

Orders in semi-simple rational algebras.

The positive cone

- K some rational division algebra, $A = K^{n \times n}$
- $A_{\mathbb{R}} := A \otimes_{\mathbb{Q}} \mathbb{R}$ semi-simple real algebra
- so $A_{\mathbb{R}}$ is isomorphic to a direct sum of matrix rings over of $\mathbb{H}$, $\mathbb{R}$ or $\mathbb{C}$.
- $A_{\mathbb{R}}$ carries a "canonical" involution † (depending on the choice of the isomorphism) that we use to define symmetric elements:
- $\mathcal{V} := \mathrm{Sym}(A_{\mathbb{R}}) := \{F \in A_{\mathbb{R}} \mid F^{\dagger} = F\}$
- $\sigma(F_1, F_2) := \mathrm{trace}(F_1 F_2)$ defines a Euclidean inner product on $\mathcal{V}$.
- In general the involution † will not fix the set A.

The simple A-module.

- Let $V = K^{1 \times n}$ denote the simple right A-module, $V_{\mathbb{R}} = V \otimes_{\mathbb{Q}} \mathbb{R}$.
- For $x \in V$ we have $x^{\dagger} x \in \mathcal{V}$.
- $F \in \mathcal{V}$ is called positive if

$$F[x] := \sigma(F, x^{\dagger} x) > 0 \text{ for all } 0 \neq x \in V_{\mathbb{R}}.$$

Minimal vectors.

The discrete admissible set

- $\mathcal{O}$ maximal order in K, L some $\mathcal{O}$-lattice in the simple A-module V
- $\Lambda := \mathrm{End}_{\mathcal{O}}(L)$ is a maximal order in A with unit group $\Lambda^* := \mathrm{GL}(L) = \{a \in A \mid aL = L\}$.

L-minimal vectors

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

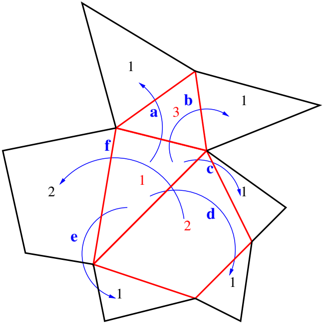
- $\mu(F) := \mu_L(F) = \min\{F[\ell] \mid 0 \neq \ell \in L\}$ the L-minimum of F.
- $\mathcal{M}_L(F) := \{\ell \in L \mid F[\ell] = \mu_L(F)\}$ the finite set of L-minimal vectors.
- $\mathrm{Vor}_L(F) := \{\sum_{x \in \mathcal{M}_L(F)} a_x x^{\dagger} x \mid a_x \geq 0\} \subset \mathcal{V}^{\geq 0}$ Voronoi domain of F.
- F is called L-perfect $\Leftrightarrow \dim(\mathrm{Vor}_L(F)) = \dim(\mathcal{V})$.

Theorem

$\mathcal{T} := \{\mathrm{Vor}_L(F) \mid F \in \mathcal{V}^{>0},$ L-perfect $\}$ forms a face to face tesselation of $\mathcal{V}^{\geq 0}$.
Λ^* acts on $\mathcal{T}$ with finitely many orbits.

Generators for Λ^*

- Compute $\mathcal{R} := \{F_1, \dots, F_s\}$ set of representatives of Λ^*-orbits on the L-perfect forms, such that their Voronoi-graph is connected.
- For all neighbors F of one of these F_i (so $\mathrm{Vor}(F) \cap \mathrm{Vor}(F_i)$ has codimension 1) compute some $g_F \in \Lambda^*$ such that $g_F \cdot F \in \mathcal{R}$.
- Then $\Lambda^* = \langle \mathrm{Aut}(F_i), g_F \mid F_i \in \mathcal{R}, F \text{ neighbor of some } F_j \in \mathcal{R} \rangle$.



so here $\Lambda^* = \langle \mathrm{Aut}(F_1), \mathrm{Aut}(F_2), \mathrm{Aut}(F_3), a, b, c, d, e, f \rangle$.

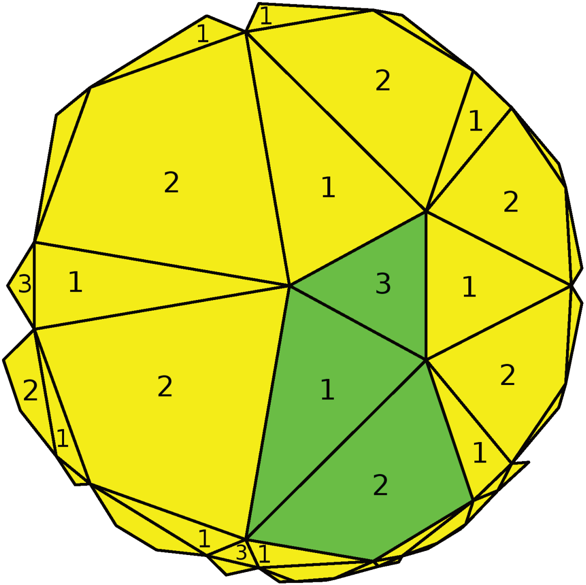
Example $\mathcal{Q}_{2,3}$.

- Take the rational quaternion algebra ramified at 2 and 3,

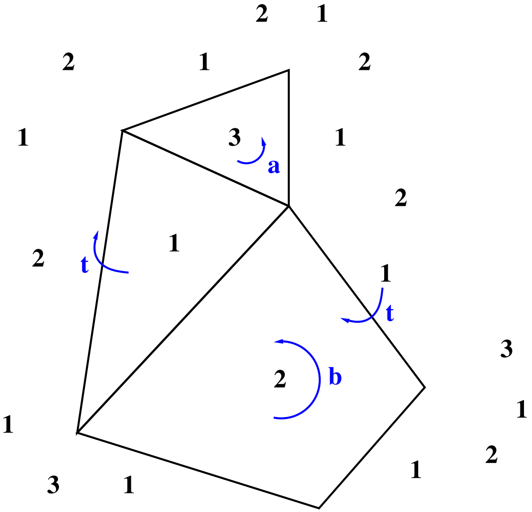
  $$\mathcal{Q}_{2,3} = \langle i, j \mid i^2 = 2, j^2 = 3, ij = -ji \rangle = \langle \mathrm{diag}(\sqrt{2}, -\sqrt{2}), \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix} \rangle$$

  Maximal order $\Lambda = \langle 1, i, \frac{1}{2}(1 + i + ij), \frac{1}{2}(j + ij) \rangle$
- $V = A = \mathcal{Q}_{2,3}$, $A_{\mathbb{R}} = \mathbb{R}^{2\times 2}$, $L = \Lambda$
- Embed A into $A_{\mathbb{R}}$ using the maximal subfield $\mathbb{Q}[\sqrt{2}]$.
- Get three perfect forms:
- $F_1 = \begin{pmatrix} 1 & 2-\sqrt{2} \\ 2-\sqrt{2} & 1 \end{pmatrix}, F_2 = \begin{pmatrix} 6-3\sqrt{2} & 2 \\ 2 & 2+\sqrt{2} \end{pmatrix}$
- $F_3 = \mathrm{diag}(-3\sqrt{2} + 9, 3\sqrt{2} + 5)$

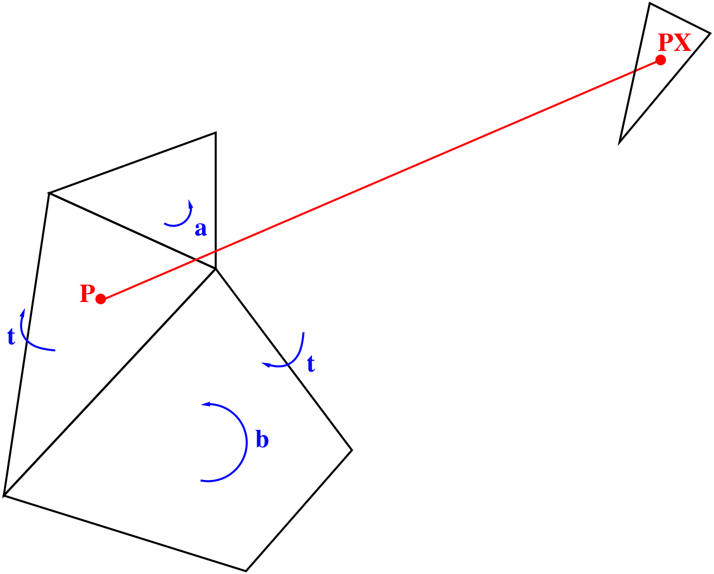
The tesselation for $\mathcal{Q}_{2,3} \hookrightarrow \mathbb{Q}[\sqrt{2}]^{2\times 2}$.



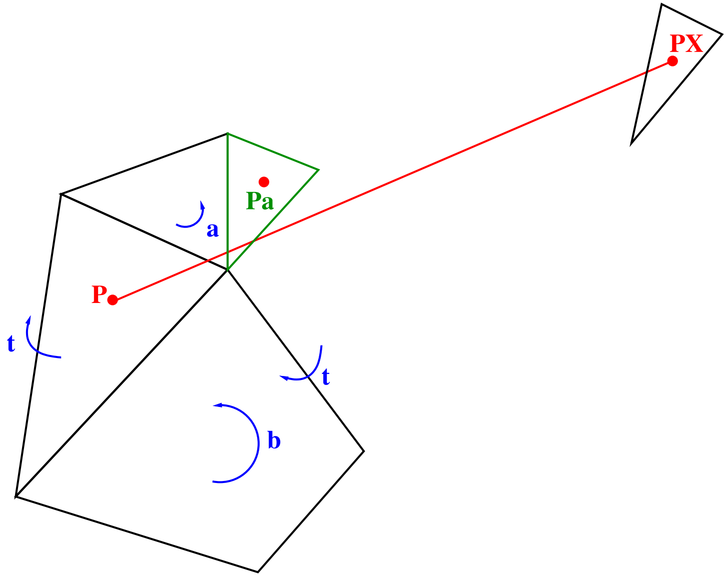
$\Lambda^*/\langle\pm 1\rangle = \langle a, b, t \mid a^3, b^2, atbt\rangle$



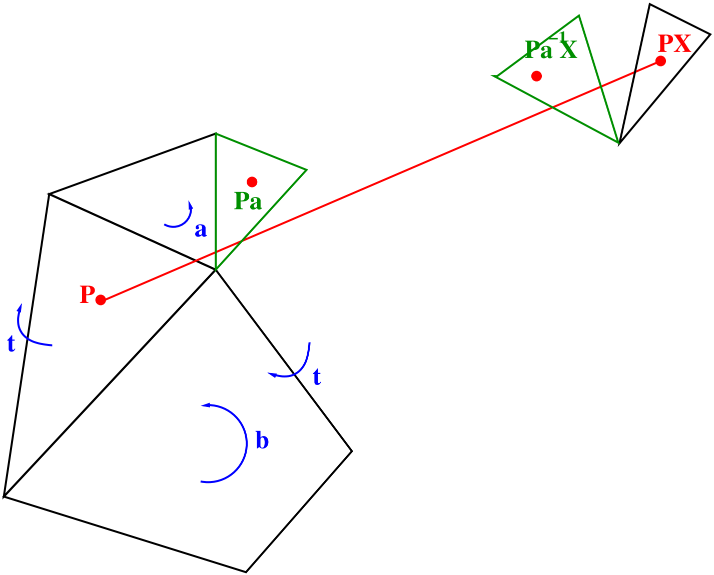
Easy solution of the word problem



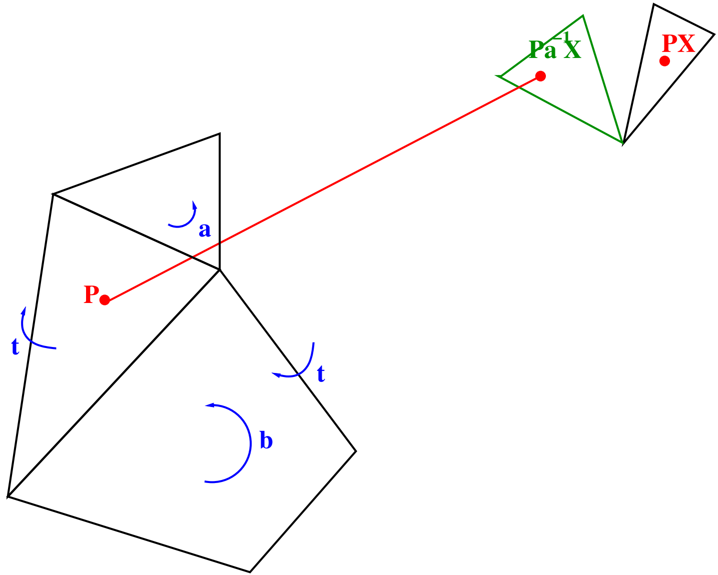
Easy solution of the word problem



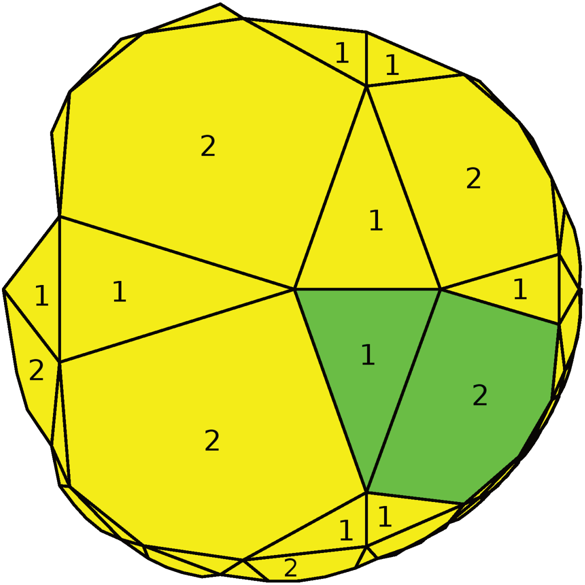
Easy solution of the word problem



Easy solution of the word problem



The tesselation for $\mathcal{Q}_{2,3} \hookrightarrow \mathbb{Q}[\sqrt{3}]^{2\times 2}$.



Conclusion

- Algorithm works quite well for indefinite quaternion algebras over the rationals
- Obtain presentation and algorithm to solve the word problem
- For $\mathcal{Q}_{19,37}$ our algorithm computes the presentation within 5 minutes (288 perfect forms, 88 generators) whereas the $\textsc{Magma}$ implementation "FuchsianGroup" does not return a result after four hours
- Reasonably fast for quaternion algebras with imaginary quadratic center or matrix rings of degree 2 over imaginary quadratic fields
- For the rational division algebra of degree 3 ramified at 2 and 3 compute presentation of Λ^*, 431 perfect forms, 50 generators in about 10 minutes.
- Quaternion algebra with center $\mathbb{Q}[\zeta_5]$: > 40.000 perfect forms.
- Masterthesis by Oliver Braun: The tesselation $\mathcal{T}$ can be used to compute the maximal finite subgroups of Λ^*.
- Masterthesis by Sebastian Schönnenbeck: Compute integral homology of Λ^*.

Calculating maximal finite subgroups

Minimal classes

Definition

Let $A, B \in \mathcal{V}^{>0}$. A and B are **minimally equivalent** if $\mathcal{M}_L(A) = \mathcal{M}_L(B)$. $C := \mathrm{Cl}_L(A) = \{X \in \mathcal{V}^{>0} \mid \mathcal{M}_L(X) = \mathcal{M}_L(A)\}$ is the **minimal class** of A. In this case $\mathcal{M}_L(C) := \mathcal{M}_L(A)$. Call C **well-rounded** if $\mathcal{M}_L(C)$ contains a K-basis of $V = K^{1\times n}$.

Remark

$A \in \mathcal{V}^{>0}$ is L-perfect if and only if $\mathrm{Cl}_L(A) = \{\alpha A \mid \alpha \in \mathbb{R}_{>0}\}$.

Calculating maximal finite subgroups
Minimal classes

Definition

Let $A, B \in \mathcal{V}^{>0}$. A and B are **minimally equivalent** if $\mathcal{M}_L(A) = \mathcal{M}_L(B)$. $C := \mathrm{Cl}_L(A) = \{X \in \mathcal{V}^{>0} \mid \mathcal{M}_L(X) = \mathcal{M}_L(A)\}$ is the **minimal class** of A. In this case $\mathcal{M}_L(C) := \mathcal{M}_L(A)$. Call C **well-rounded** if $\mathcal{M}_L(C)$ contains a K-basis of $V = K^{1\times n}$.

Remark

$A \in \mathcal{V}^{>0}$ is L-perfect if and only if $\mathrm{Cl}_L(A) = \{\alpha A \mid \alpha \in \mathbb{R}_{>0}\}$.

Remark

$\dim_{\mathbb{R}}(\mathcal{V}) - \dim_{\mathbb{R}}(\langle x^\dagger x \mid x \in \mathcal{M}_L(A)\rangle)$, the **perfection corank**, is constant on $\mathrm{Cl}_L(A)$.

Calculating minimal classes

Theorem

Let $A \in \mathcal{V}^{>0}$ be L-perfect. Any codimension-k-face of $\mathrm{Vor}_L(A)$ corresponds to a minimal class of perfection corank k, represented by

$$A + \frac{1}{2k} \sum_{i=1}^{k} \rho_i R_i = \frac{1}{k} \sum_{i=1}^{k} \left(A + \frac{\rho_i}{2} R_i \right) \in \mathcal{V}^{>0}$$

with facet vectors R_i and $\rho_i \in \mathbb{R}_{>0}$ such that $A + \rho_i R_i$ is a perfect neighbour of A (and the codimension-k-face in question is the intersection is the intersection of the facets with facet vectors R_i).

Calculating minimal classes

Theorem

Let $A \in \mathcal{V}^{>0}$ be L-perfect. Any codimension-k-face of $\mathrm{Vor}_L(A)$ corresponds to a minimal class of perfection corank k, represented by

$$A + \frac{1}{2k}\sum_{i=1}^{k} \rho_i R_i = \frac{1}{k}\sum_{i=1}^{k}\left(A + \frac{\rho_i}{2}R_i\right) \in \mathcal{V}^{>0}$$

with facet vectors R_i and $\rho_i \in \mathbb{R}_{>0}$ such that $A + \rho_i R_i$ is a perfect neighbour of A (and the codimension-k-face in question is the intersection is the intersection of the facets with facet vectors R_i).

Example: The minimal classes in dimension 2 over $\mathbb{Z}$

$F_0 = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$, $\mathcal{M}(F_0) = \{\pm(1,0),\ \pm(0,1),\ \pm(1,1)\}$

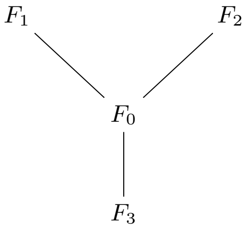
$\mathcal{A}^{\geq 0} \cap \mathrm{Vor}(F_0) = \mathrm{conv}\left(\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}\right)$

Facet vectors $R_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $R_2 = \begin{pmatrix} 2 & -1 \\ -1 & 0 \end{pmatrix}$, $R_3 = \begin{pmatrix} 0 & -1 \\ -1 & 2 \end{pmatrix}$

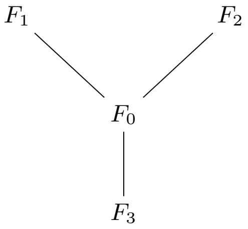
All perfect neighbours of F_0 are given by $F_0 + 2R_i$, so $\rho_i = 2$ for all $1 \leq i \leq 3$.

Now consider the dual of the tesselation of $\mathcal{T} = \{\mathrm{Vor}(F) \mid F \in \mathcal{V}^{>0} \text{ perfect}\}$.

Now consider the dual of the tesselation of $\mathcal{T} = \{\mathrm{Vor}(F) \mid F \in \mathcal{V}^{>0} \text{ perfect}\}$.



Now consider the dual of the tesselation of $\mathcal{T} = \{\mathrm{Vor}(F) \mid F \in \mathcal{V}^{>0} \text{ perfect}\}$.



- The well-rounded classes have perfection corank 0 or 1. The corank 0 class is the perfect class of F_0.
- The corank 1 classes are represented by

$$F_0 + R_1 = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$
$$F_0 + R_2 = \begin{pmatrix} 4 & -2 \\ -2 & 2 \end{pmatrix}$$
$$F_0 + R_3 = \begin{pmatrix} 2 & -2 \\ -2 & 4 \end{pmatrix}$$

- The minimal classes represented by these three matrices are in the same orbit under $\mathrm{GL}_2(\mathbb{Z})$. This is easily checked for well-rounded minimal classes using a theorem by A.-M. Bergé.
- The corank 2 class is represented by $\frac{1}{2}(2F_0 + R_1 + R_2) = \begin{pmatrix} 3 & -1 \\ -1 & 2 \end{pmatrix}$.

Maximal finite subgroups

Theorem (Coulangeon, Nebe (2013))

$G \leq \mathrm{GL}(L)$ maximal finite $\implies G = \mathrm{Aut}_L(C)$, where C is a well-rounded minimal class, such that $\dim(C \cap \mathcal{F}(G)) = 1$.
$\mathcal{F}(G) := \{A \in \mathcal{V} \mid A[g] = A \; \forall \; g \in G\}$

Remark

This theorem yields a finite set of finite subgroups of $\mathrm{GL}(L)$, containing a set of representatives of conjugacy classes of maximal finite subgroups of $\mathrm{GL}(L)$.

Maximal finite subgroups

Theorem (Coulangeon, Nebe (2013))

$G \leq \mathrm{GL}(L)$ maximal finite $\Longrightarrow G = \mathrm{Aut}_L(C)$, where C is a well-rounded minimal class, such that $\dim(C \cap \mathcal{F}(G)) = 1$.
$\mathcal{F}(G) := \{A \in \mathcal{V} \mid A[g] = A \; \forall \; g \in G\}$

Remark

This theorem yields a finite set of finite subgroups of $\mathrm{GL}(L)$, containing a set of representatives of conjugacy classes of maximal finite subgroups of $\mathrm{GL}(L)$.

- There are algorithmic methods to check if a finite subgroup is maximal finite and whether two maximal finite subgroups are conjugate.

Maximal finite subgroups

Theorem (Coulangeon, Nebe (2013))

$G \leq \mathrm{GL}(L)$ maximal finite $\Longrightarrow G = \mathrm{Aut}_L(C)$, where C is a well-rounded minimal class, such that $\dim(C \cap \mathcal{F}(G)) = 1$.
$\mathcal{F}(G) := \{A \in \mathcal{V} \mid A[g] = A \;\forall\; g \in G\}$

Remark

This theorem yields a finite set of finite subgroups of $\mathrm{GL}(L)$, containing a set of representatives of conjugacy classes of maximal finite subgroups of $\mathrm{GL}(L)$.

- There are algorithmic methods to check if a finite subgroup is maximal finite and whether two maximal finite subgroups are conjugate.
- Therefore in the previous example, we obtain two conjugacy classes of maximal finite subgroups:
  The stabilizer of the perfect form F_0, which is isomorphic to D_{12}.
  The stabilizer of the corank 1 class, which is isomorphic to D_8.
- These groups are indeed maximal finite.

Example: $\mathbb{Q}(\sqrt{-6})$

$\mathcal{O} = \mathbb{Z}[\sqrt{-6}]$, $L_0 = \mathcal{O} \oplus \mathcal{O}$, $L_1 = \mathcal{O} \oplus \mathfrak{p}$, where $\mathfrak{p} \mid (2)$.

Well-rounded minimal classes for $\mathbb{Q}(\sqrt{-6})$

$L = L_0$			$L = L_1$		
C	$G = \mathrm{Aut}_L(C)$	max.	C	$G = \mathrm{Aut}_L(C)$	max.
P_1	$\mathrm{SL}(2,3)$	yes	P_1	Q_8	yes
C_1	D_{12}	yes	P_2	$C_3 \rtimes C_4$	yes
C_2	D_{12}	yes	C_1	D_8	yes
C_3	C_4	no	C_2	C_4	no
C_4	D_8	yes	C_3	C_4	no
D_1	D_8	yes	C_4	D_{12}	yes
D_2	D_8	yes	D_1	$C_2 \times C_2$	yes
D_3	$C_2 \times C_2$	yes	D_2	$C_2 \times C_2$	yes

$$\Longrightarrow \mathrm{GL}(L_0) \ncong \mathrm{GL}(L_1)$$

Resolutions for Unit Groups of Orders

Setup: As before $A = K^{n \times n}$ for some rational division algebra K, $\mathcal{O}$ a maximal order in K and $\Lambda = \mathrm{End}_{\mathcal{O}}(L)$ for some $\mathcal{O}$-lattice L.

Resolutions for Unit Groups of Orders

Setup: As before $A = K^{n\times n}$ for some rational division algebra K, $\mathcal{O}$ a maximal order in K and $\Lambda = \mathrm{End}_{\mathcal{O}}(L)$ for some $\mathcal{O}$-lattice L.

Target

Compute a $\mathbb{Z}\Lambda^*$-free resolution of $\mathbb{Z}$ (which may then be used to compute e.g. the integral homology of Λ^*).

Resolutions for Unit Groups of Orders

Setup: As before $A = K^{n\times n}$ for some rational division algebra K, $\mathcal{O}$ a maximal order in K and $\Lambda = \mathrm{End}_{\mathcal{O}}(L)$ for some $\mathcal{O}$-lattice L.

Target

Compute a $\mathbb{Z}\Lambda^*$-free resolution of $\mathbb{Z}$ (which may then be used to compute e.g. the integral homology of Λ^*).

Basic idea

Find a cell complex with a suitable Λ^*-action and employ its cellular chain complex.

Resolutions for Unit Groups of Orders

Setup: As before $A = K^{n \times n}$ for some rational division algebra K, $\mathcal{O}$ a maximal order in K and $\Lambda = \mathrm{End}_{\mathcal{O}}(L)$ for some $\mathcal{O}$-lattice L.

Target

Compute a $\mathbb{Z}\Lambda^*$-free resolution of $\mathbb{Z}$ (which may then be used to compute e.g. the integral homology of Λ^*).

Basic idea

Find a cell complex with a suitable Λ^*-action and employ its cellular chain complex.

Reminder

$A_{\mathbb{R}} := A \otimes_{\mathbb{Q}} \mathbb{R}$ carries a "canonical" involution †, $\mathcal{V} := \{F \in A_{\mathbb{R}} \mid F^\dagger = F\}$.

Resolutions for Unit Groups of Orders

Setup: As before $A = K^{n\times n}$ for some rational division algebra K, $\mathcal{O}$ a maximal order in K and $\Lambda = \mathrm{End}_{\mathcal{O}}(L)$ for some $\mathcal{O}$-lattice L.

Target

Compute a $\mathbb{Z}\Lambda^*$-free resolution of $\mathbb{Z}$ (which may then be used to compute e.g. the integral homology of Λ^*).

Basic idea

Find a cell complex with a suitable Λ^*-action and employ its cellular chain complex.

Reminder

$A_{\mathbb{R}} := A \otimes_{\mathbb{Q}} \mathbb{R}$ carries a "canonical" involution †, $\mathcal{V} := \{F \in A_{\mathbb{R}} \mid F^\dagger = F\}$.
Λ^* acts on $\mathcal{V}^{>0}$ via $(g, F) \mapsto gFg^\dagger$.

The cell decomposition of $\mathcal{V}^{>0}$

Minimal classes

For $F \in \mathcal{V}^{>0}$ define $\mathrm{Cl}_L(F) := \{F' \in \mathcal{V}^{>0} \mid \mathcal{M}_L(F') = \mathcal{M}_L(F)\}$ the minimal class corresponding to F.

The cell decomposition of $\mathcal{V}^{>0}$

Minimal classes

For $F \in \mathcal{V}^{>0}$ define $\mathrm{Cl}_L(F) := \{F' \in \mathcal{V}^{>0} \mid \mathcal{M}_L(F') = \mathcal{M}_L(F)\}$ the minimal class corresponding to F.
$\mathcal{V}^{>0}$ decomposes into the disjoint union of all minimal classes.

The cell decomposition of $\mathcal{V}^{>0}$

Minimal classes

For $F \in \mathcal{V}^{>0}$ define $\mathrm{Cl}_L(F) := \{F' \in \mathcal{V}^{>0} \mid \mathcal{M}_L(F') = \mathcal{M}_L(F)\}$ the minimal class corresponding to F.
$\mathcal{V}^{>0}$ decomposes into the disjoint union of all minimal classes.

Properties of this decomposition:

- Partial ordering on the minimal classes: $C \preceq C' \Leftrightarrow \mathcal{M}_L(C) \subset \mathcal{M}_L(C')$.

The cell decomposition of $\mathcal{V}^{>0}$

Minimal classes

For $F \in \mathcal{V}^{>0}$ define $\mathrm{Cl}_L(F) := \{F' \in \mathcal{V}^{>0} \mid \mathcal{M}_L(F') = \mathcal{M}_L(F)\}$ the minimal class corresponding to F.
$\mathcal{V}^{>0}$ decomposes into the disjoint union of all minimal classes.

Properties of this decomposition:

- Partial ordering on the minimal classes: $C \preceq C' \Leftrightarrow \mathcal{M}_L(C) \subset \mathcal{M}_L(C')$.
- Each minimal class is a convex set in $\mathcal{V}$.

The cell decomposition of $\mathcal{V}^{>0}$

Minimal classes

For $F \in \mathcal{V}^{>0}$ define $\mathrm{Cl}_L(F) := \{F' \in \mathcal{V}^{>0} \mid \mathcal{M}_L(F') = \mathcal{M}_L(F)\}$ the minimal class corresponding to F.
$\mathcal{V}^{>0}$ decomposes into the disjoint union of all minimal classes.

Properties of this decomposition:

- Partial ordering on the minimal classes: $C \preceq C' \Leftrightarrow \mathcal{M}_L(C) \subset \mathcal{M}_L(C')$.
- Each minimal class is a convex set in $\mathcal{V}$.
- The decomposition as well as the partial ordering are compatible with the Λ^*-action.

The cell decomposition of $\mathcal{V}^{>0}$

Minimal classes

For $F \in \mathcal{V}^{>0}$ define $\mathrm{Cl}_L(F) := \{F' \in \mathcal{V}^{>0} \mid \mathcal{M}_L(F') = \mathcal{M}_L(F)\}$ the minimal class corresponding to F.
$\mathcal{V}^{>0}$ decomposes into the disjoint union of all minimal classes.

Properties of this decomposition:

- Partial ordering on the minimal classes: $C \preceq C' \Leftrightarrow \mathcal{M}_L(C) \subset \mathcal{M}_L(C')$.
- Each minimal class is a convex set in $\mathcal{V}$.
- The decomposition as well as the partial ordering are compatible with the Λ^*-action.
- We have $\overline{C} = \bigcup_{C \preceq C'} C'$.

The cell decomposition of $\mathcal{V}^{>0}$

Minimal classes

For $F \in \mathcal{V}^{>0}$ define $\mathrm{Cl}_L(F) := \{F' \in \mathcal{V}^{>0} \mid \mathcal{M}_L(F') = \mathcal{M}_L(F)\}$ the minimal class corresponding to F.
$\mathcal{V}^{>0}$ decomposes into the disjoint union of all minimal classes.

Properties of this decomposition:

- Partial ordering on the minimal classes: $C \preceq C' \Leftrightarrow \mathcal{M}_L(C) \subset \mathcal{M}_L(C')$.
- Each minimal class is a convex set in $\mathcal{V}$.
- The decomposition as well as the partial ordering are compatible with the Λ^*-action.
- We have $\overline{C} = \bigcup_{C \preceq C'} C'$.

The cellular chain complex

The decomposition yields an acyclic chain complex C, where C_n is the free Abelian group on the minimal classes in dimension n. C_n becomes a Λ^*-module by means of the Λ^*-action on $\mathcal{V}$.

Assembling the information

Problem 1: The modules C_n are not necessarily free.

Assembling the information

Problem 1: The modules C_n are not necessarily free.

Perturbations - C.T.C. Wall (1961)

There is an algorithm which takes as input the cellular chain complex and free resolutions of $\mathbb{Z}$ for the occuring stabilizers of cells and outputs a free resolution of $\mathbb{Z}$ for Λ^*.

Assembling the information

Problem 1: The modules C_n are not necessarily free.

Perturbations - C.T.C. Wall (1961)

There is an algorithm which takes as input the cellular chain complex and free resolutions of $\mathbb{Z}$ for the occuring stabilizers of cells and outputs a free resolution of $\mathbb{Z}$ for Λ^*.

Problem 2: Some cells have infinite stabilisers.

Assembling the information

Problem 1: The modules C_n are not necessarily free.

Perturbations - C.T.C. Wall (1961)

There is an algorithm which takes as input the cellular chain complex and free resolutions of $\mathbb{Z}$ for the occuring stabilizers of cells and outputs a free resolution of $\mathbb{Z}$ for Λ^*.

Problem 2: Some cells have infinite stabilisers.
Solution: Consider only a certain retract of $\mathcal{V}^{>0}$.

Assembling the information

Problem 1: The modules C_n are not necessarily free.

Perturbations - C.T.C. Wall (1961)

There is an algorithm which takes as input the cellular chain complex and free resolutions of $\mathbb{Z}$ for the occuring stabilizers of cells and outputs a free resolution of $\mathbb{Z}$ for Λ^*.

Problem 2: Some cells have infinite stabilisers.
Solution: Consider only a certain retract of $\mathcal{V}^{>0}$.

The well-rounded retract

- $F \in \mathcal{V}^{>0}$ is called *well-rounded*, if $\mathcal{M}_L(F)$ contains a K-Basis of K^n.

Assembling the information

Problem 1: The modules C_n are not necessarily free.

Perturbations - C.T.C. Wall (1961)

There is an algorithm which takes as input the cellular chain complex and free resolutions of $\mathbb{Z}$ for the occuring stabilizers of cells and outputs a free resolution of $\mathbb{Z}$ for Λ^*.

Problem 2: Some cells have infinite stabilisers.
Solution: Consider only a certain retract of $\mathcal{V}^{>0}$.

The well-rounded retract

- $F \in \mathcal{V}^{>0}$ is called *well-rounded*, if $\mathcal{M}_L(F)$ contains a K-Basis of K^n.
- $\mathcal{V}_{=1}^{>0,wr} := \{F \in \mathcal{V}^{>0} \mid F \text{ well-rounded}, \mu_L(F) = 1\}$.

The well-rounded retract

Properties of the well-rounded retract

In $\mathcal{V}_{=1}^{>0,wr}$ we have:

The well-rounded retract

Properties of the well-rounded retract

In $\mathcal{V}_{=1}^{>0,wr}$ we have:

- There are only finitely many Λ^*-orbits in any dimension and every occuring stabiliser is finite.

The well-rounded retract

Properties of the well-rounded retract

In $\mathcal{V}_{=1}^{>0,wr}$ we have:

- There are only finitely many Λ^*-orbits in any dimension and every occuring stabiliser is finite.
- The topological closure of each cell is a polytope.

The well-rounded retract

Properties of the well-rounded retract

In $\mathcal{V}_{=1}^{>0,wr}$ we have:

- There are only finitely many Λ^*-orbits in any dimension and every occuring stabiliser is finite.
- The topological closure of each cell is a polytope.
- $\mathcal{V}_{=1}^{>0,wr}$ is a retract of $\mathcal{V}^{>0}$, especially we have that the cellular chain complex is again acyclic and $\mathrm{H}_0 \cong \mathbb{Z}$ (A. Ash, 1984).

The well-rounded retract

Properties of the well-rounded retract

In $\mathcal{V}_{=1}^{>0,wr}$ we have:

- There are only finitely many Λ^*-orbits in any dimension and every occuring stabiliser is finite.
- The topological closure of each cell is a polytope.
- $\mathcal{V}_{=1}^{>0,wr}$ is a retract of $\mathcal{V}^{>0}$, especially we have that the cellular chain complex is again acyclic and $\mathrm{H}_0 \cong \mathbb{Z}$ (A. Ash, 1984).

Summary

The well-rounded retract

Properties of the well-rounded retract

In $\mathcal{V}_{=1}^{>0,wr}$ we have:

- There are only finitely many Λ^*-orbits in any dimension and every occuring stabiliser is finite.
- The topological closure of each cell is a polytope.
- $\mathcal{V}_{=1}^{>0,wr}$ is a retract of $\mathcal{V}^{>0}$, especially we have that the cellular chain complex is again acyclic and $\mathrm{H}_0 \cong \mathbb{Z}$ (A. Ash, 1984).

Summary

- The group Λ^* acts on the space of positive definite forms.

Properties of the well-rounded retract

In $\mathcal{V}_{=1}^{>0,wr}$ we have:

- There are only finitely many Λ^*-orbits in any dimension and every occuring stabiliser is finite.
- The topological closure of each cell is a polytope.
- $\mathcal{V}_{=1}^{>0,wr}$ is a retract of $\mathcal{V}^{>0}$, especially we have that the cellular chain complex is again acyclic and $\mathrm{H}_0 \cong \mathbb{Z}$ (A. Ash, 1984).

Summary

- The group Λ^* acts on the space of positive definite forms.
- This space decomposes into cells in a Λ^*-compatible way.

The well-rounded retract

Properties of the well-rounded retract

In $\mathcal{V}_{=1}^{>0,wr}$ we have:

- There are only finitely many Λ^*-orbits in any dimension and every occuring stabiliser is finite.
- The topological closure of each cell is a polytope.
- $\mathcal{V}_{=1}^{>0,wr}$ is a retract of $\mathcal{V}^{>0}$, especially we have that the cellular chain complex is again acyclic and $\mathrm{H}_0 \cong \mathbb{Z}$ (A. Ash, 1984).

Summary

- The group Λ^* acts on the space of positive definite forms.
- This space decomposes into cells in a Λ^*-compatible way.
- There is a subspace such that each cell in it is a polytope and has finite stabiliser in Λ^*.

The well-rounded retract

Properties of the well-rounded retract

In $\mathcal{V}_{=1}^{>0,wr}$ we have:

- There are only finitely many Λ^*-orbits in any dimension and every occuring stabiliser is finite.
- The topological closure of each cell is a polytope.
- $\mathcal{V}_{=1}^{>0,wr}$ is a retract of $\mathcal{V}^{>0}$, especially we have that the cellular chain complex is again acyclic and $\mathrm{H}_0 \cong \mathbb{Z}$ (A. Ash, 1984).

Summary

- The group Λ^* acts on the space of positive definite forms.
- This space decomposes into cells in a Λ^*-compatible way.
- There is a subspace such that each cell in it is a polytope and has finite stabiliser in Λ^*.
- We may use this cellular decomposition and the *finite* stabilisers to construct a free $\mathbb{Z}\Lambda^*$-resolution of $\mathbb{Z}$.

Example 1: Linear Groups over Imaginary Quadratic Integers

$$\mathbb{Q}(\sqrt{-5})$$

Example 1: Linear Groups over Imaginary Quadratic Integers

$\mathbb{Q}(\sqrt{-5})$

$K := \mathbb{Q}(\sqrt{-5})$, $A := K^{2\times 2}$, $\mathcal{O} := \mathbb{Z}\left[\sqrt{-5}\right]$.
$\Lambda_i := \mathrm{End}_{\mathcal{O}}(L_i)$ where $L_1 := \mathcal{O}^2$ and $L_2 := \mathcal{O} \oplus \wp$ where $\wp^2 = (2)$.

Example 1: Linear Groups over Imaginary Quadratic Integers

$\mathbb{Q}(\sqrt{-5})$

$K := \mathbb{Q}(\sqrt{-5})$, $A := K^{2\times 2}$, $\mathcal{O} := \mathbb{Z}\left[\sqrt{-5}\right]$.
$\Lambda_i := \mathrm{End}_{\mathcal{O}}(L_i)$ where $L_1 := \mathcal{O}^2$ and $L_2 := \mathcal{O} \oplus \wp$ where $\wp^2 = (2)$.

1. $G_1 := \mathrm{GL}(L_1)$:

$$\mathrm{H}_n(G_1, \mathbb{Z}) = \begin{cases} C_2^5 & n = 1 \\ C_4^2 \times C_{12} \times \mathbb{Z} & n = 2 \\ C_2^8 \times C_{24} & n = 3 \\ C_2^7 & n = 4 \end{cases}$$

Example 1: Linear Groups over Imaginary Quadratic Integers

$\mathbb{Q}(\sqrt{-5})$

$K := \mathbb{Q}(\sqrt{-5})$, $A := K^{2\times 2}$, $\mathcal{O} := \mathbb{Z}\left[\sqrt{-5}\right]$.
$\Lambda_i := \mathrm{End}_{\mathcal{O}}(L_i)$ where $L_1 := \mathcal{O}^2$ and $L_2 := \mathcal{O} \oplus \wp$ where $\wp^2 = (2)$.

1. $G_1 := \mathrm{GL}(L_1)$:
$$\mathrm{H}_n(G_1, \mathbb{Z}) = \begin{cases} C_2^5 & n = 1 \\ C_4^2 \times C_{12} \times \mathbb{Z} & n = 2 \\ C_2^8 \times C_{24} & n = 3 \\ C_2^7 & n = 4 \end{cases}$$

2. $G_2 := \mathrm{GL}(L_2)$:
$$\mathrm{H}_n(G_2, \mathbb{Z}) = \begin{cases} C_2^3 & n = 1 \\ C_2^2 \times C_{12} \times \mathbb{Z} & n = 2 \\ C_2^8 \times C_{24} & n = 3 \\ C_2^7 & n = 4 \end{cases}$$

Example 1: Linear Groups over Imaginary Quadratic Integers

$\mathbb{Q}(\sqrt{-5})$

$K := \mathbb{Q}(\sqrt{-5})$, $A := K^{2\times 2}$, $\mathcal{O} := \mathbb{Z}\left[\sqrt{-5}\right]$.
$\Lambda_i := \mathrm{End}_{\mathcal{O}}(L_i)$ where $L_1 := \mathcal{O}^2$ and $L_2 := \mathcal{O} \oplus \wp$ where $\wp^2 = (2)$.

1. $G_1 := \mathrm{GL}(L_1)$:

$$\mathrm{H}_n(G_1, \mathbb{Z}) = \begin{cases} C_2^5 & n = 1 \\ C_4^2 \times C_{12} \times \mathbb{Z} & n = 2 \\ C_2^8 \times C_{24} & n = 3 \\ C_2^7 & n = 4 \end{cases}$$

2. $G_2 := \mathrm{GL}(L_2)$:

$$\mathrm{H}_n(G_2, \mathbb{Z}) = \begin{cases} C_2^3 & n = 1 \\ C_2^2 \times C_{12} \times \mathbb{Z} & n = 2 \\ C_2^8 \times C_{24} & n = 3 \\ C_2^7 & n = 4 \end{cases}$$

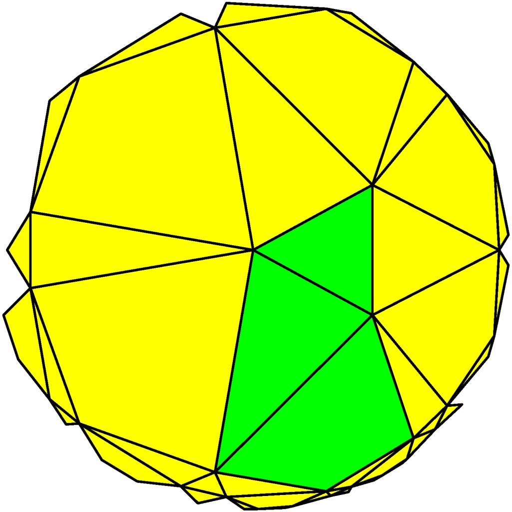
Especially: $G_1 \ncong G_2$.

Example 2: The well-rounded retract and the Voronoi domains

$$A = K = \left(\frac{2,3}{\mathbb{Q}}\right),\ \mathcal{O} = \Lambda = \langle 1, i, j, k \rangle_{\mathbb{Z}}$$

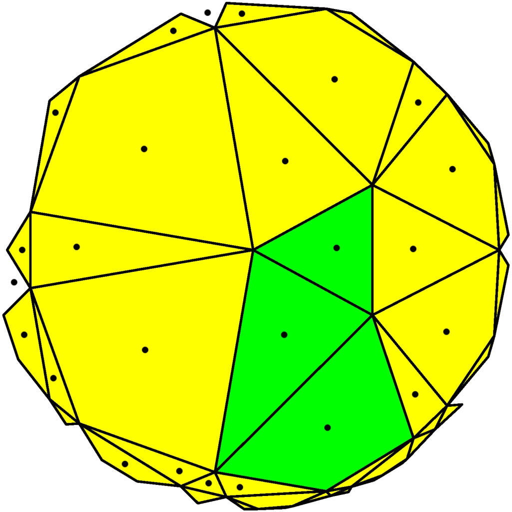
Example 2: The well-rounded retract and the Voronoi domains

$A = K = \left(\frac{2,3}{\mathbb{Q}}\right)$, $\mathcal{O} = \Lambda = \langle 1, i, j, k \rangle_{\mathbb{Z}}$



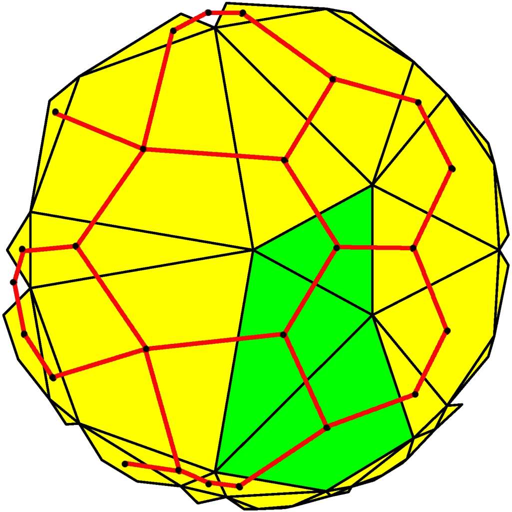
Example 2: The well-rounded retract and the Voronoi domains

$A = K = \left(\frac{2,3}{\mathbb{Q}}\right)$, $\mathcal{O} = \Lambda = \langle 1, i, j, k \rangle_{\mathbb{Z}}$



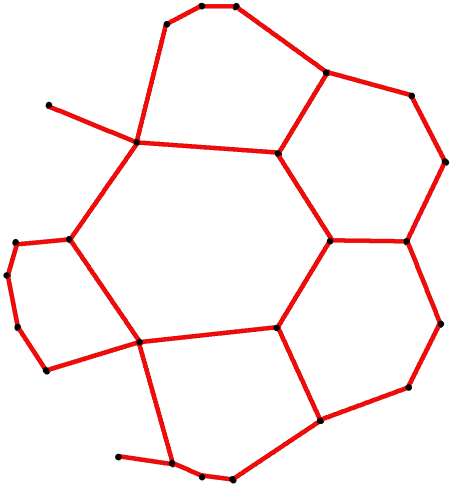
Example 2: The well-rounded retract and the Voronoi domains

$A = K = \left(\frac{2,3}{\mathbb{Q}}\right)$, $\mathcal{O} = \Lambda = \langle 1, i, j, k \rangle_{\mathbb{Z}}$



Example 2: The well-rounded retract and the Voronoi domains

$$A = K = \left(\frac{2,3}{\mathbb{Q}}\right),\ \mathcal{O} = \Lambda = \langle 1, i, j, k\rangle_{\mathbb{Z}}$$



References

A. Ash
Small-dimensional classifying spaces for arithmetic subgroups of general linear groups
Duke Mathematical Journal, 51, 1984.

Renaud Coulangeon, Gabriele Nebe
Maximal finite subgroups and minimal classes
arXiv:1304.2597 [math.NT], to appear in l'Ens. Math.

C.T.C. Wall
Resolutions for extensions of groups
Mathematical Proceedings of the Cambridge Philosophical Society, Cambridge Univ. Press, vol. 57, 1961