Computing unit groups of orders

Gabriele Nebe

Lehrstuhl D für Mathematik

University of Pennsylvania, Philadelphia, 6. November 2015

RWTH AACHEN UNIVERSITY

Setup

- $\mathcal{A} = \mathcal{D}^{n\times n}$ simple $\mathbb{Q}$-algebra
- $\mathcal{D}$ division algebra with center K
- K an algebraic number field
- $\mathbb{Z}_K$ ring of integers in K
- V_∞ the infinite places of K
- $V_f := \{\wp \mid 0 \neq \wp \trianglelefteq_{prime} \mathbb{Z}_K\}$ the finite places of K
- $S_f = \{\wp_1, \ldots, \wp_s\} \subseteq V_f$
- $S := S_f \cup V_\infty$
- $\mathbb{Z}_{K,S} := \{a \in K \mid ||a||_\wp \leq 1 \text{ for all } \wp \notin S\}$ S-integers
- Λ a $\mathbb{Z}_K$-order in $\mathcal{A}$.
- $\Lambda_S := \mathbb{Z}_{K,S} \otimes \Lambda$

Theorem (Borel, Serre, 1962-1975)

The unit group of Λ_S is finitely presented.

The proof of Borel and Serre

$\mathcal{A}$ a simple $\mathbb{Q}$-algebra
Λ order in $\mathcal{A}$
$S = \{\wp_1 \ldots, \wp_s\} \cup V_\infty$

Theorem (Borel, Serre 1962-1975)

The unit group of Λ_S is finitely presented.

- The unit group Λ_S^* acts on the locally finite cell complex
- $\mathcal{X} = \mathcal{X}_\infty \times \mathcal{X}_{\wp_1} \times \ldots \times \mathcal{X}_{\wp_s}$
- with finite stabilisers of points

The proof of Borel and Serre

$\mathcal{A}$ a simple $\mathbb{Q}$-algebra
Λ order in $\mathcal{A}$
$S = \{\wp_1 \ldots, \wp_s\} \cup V_\infty$

Theorem (Borel, Serre 1962-1975)

The unit group of Λ_S is finitely presented.

- The unit group Λ_S^* acts on the locally finite cell complex
- $\mathcal{X} = \mathcal{X}_\infty \times \mathcal{X}_{\wp_1} \times \ldots \times \mathcal{X}_{\wp_s}$
- with finite stabilisers of points
- $\mathcal{X}_{\wp_i} =$ Bruhat-Tits building of the $\wp_i$-adic group $\mathrm{SL}(\mathcal{A}_{\wp_i})$.
- $\mathcal{X}$ homogeneous space with point stabiliser the maximal compact subgroup of $\mathrm{SL}(\mathcal{A}_\infty)$
- General Theory: One may compute a finite presentation using this action.

Examples

- $\mathcal{A} = K$ algebraic number field $\Lambda = \mathbb{Z}_K$, $S_f = \emptyset$,
  $\Lambda^* = \mathbb{Z}_K^* \cong \mu_K \times \mathbb{Z}^{r+s-1}$ (Dirichlet's unit theorem)

Examples

- $\mathcal{A} = K$ algebraic number field $\Lambda = \mathbb{Z}_K$, $S_f = \emptyset$, $\Lambda^* = \mathbb{Z}_K^* \cong \mu_K \times \mathbb{Z}^{r+s-1}$ (Dirichlet's unit theorem)
- $\mathcal{A} = \mathcal{D} = \left(\frac{-1,-1}{\mathbb{Q}}\right) = \langle 1, i, j, k = ij \mid i^2 = j^2 = k^2 = -1 \rangle_{\mathbb{Q}}$ definite rational quaternion algebra, $\Lambda = \langle 1, i, j, k \rangle_{\mathbb{Z}}$. $S_f = \emptyset \Rightarrow \Lambda^* = \langle i, j \rangle \cong Q_8$ finite.

Examples

- $\mathcal{A} = K$ algebraic number field $\Lambda = \mathbb{Z}_K$, $S_f = \emptyset$,
  $\Lambda^* = \mathbb{Z}_K^* \cong \mu_K \times \mathbb{Z}^{r+s-1}$ (Dirichlet's unit theorem)
- $\mathcal{A} = \mathcal{D} = \left(\frac{-1,-1}{\mathbb{Q}}\right) = \langle 1, i, j, k = ij \mid i^2 = j^2 = k^2 = -1 \rangle_{\mathbb{Q}}$
  definite rational quaternion algebra, $\Lambda = \langle 1, i, j, k \rangle_{\mathbb{Z}}$.
  $S_f = \emptyset \Rightarrow \Lambda^* = \langle i, j \rangle \cong Q_8$ finite.
  $S_f \neq \emptyset \Rightarrow$ Chinburg etal: congruence subgroup problem.

Examples

- $\mathcal{A} = K$ algebraic number field $\Lambda = \mathbb{Z}_K$, $S_f = \emptyset$,
  $\Lambda^* = \mathbb{Z}_K^* \cong \mu_K \times \mathbb{Z}^{r+s-1}$ (Dirichlet's unit theorem)
- $\mathcal{A} = \mathcal{D} = \left(\frac{-1,-1}{\mathbb{Q}}\right) = \langle 1, i, j, k = ij \mid i^2 = j^2 = k^2 = -1 \rangle_{\mathbb{Q}}$
  definite rational quaternion algebra, $\Lambda = \langle 1, i, j, k \rangle_{\mathbb{Z}}$.
  $S_f = \emptyset \Rightarrow \Lambda^* = \langle i, j \rangle \cong Q_8$ finite.
  $S_f \neq \emptyset \Rightarrow$ Chinburg etal: congruence subgroup problem.
- $\mathcal{A} = \mathbb{Q}^{2\times 2}$.

$$\mathrm{SL}_2(\mathbb{Z}) = \langle S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mid S^2 = (ST)^3 = -1 \rangle$$

Examples

- $\mathcal{A} = K$ algebraic number field $\Lambda = \mathbb{Z}_K$, $S_f = \emptyset$,
  $\Lambda^* = \mathbb{Z}_K^* \cong \mu_K \times \mathbb{Z}^{r+s-1}$ (Dirichlet's unit theorem)
- $\mathcal{A} = \mathcal{D} = \left(\frac{-1,-1}{\mathbb{Q}}\right) = \langle 1, i, j, k = ij \mid i^2 = j^2 = k^2 = -1 \rangle_{\mathbb{Q}}$
  definite rational quaternion algebra, $\Lambda = \langle 1, i, j, k \rangle_{\mathbb{Z}}$.
  $S_f = \emptyset \Rightarrow \Lambda^* = \langle i, j \rangle \cong Q_8$ finite.
  $S_f \neq \emptyset \Rightarrow$ Chinburg etal: congruence subgroup problem.
- $\mathcal{A} = \mathbb{Q}^{2\times 2}$.

$$\mathrm{SL}_2(\mathbb{Z}) = \langle S = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \mid S^2 = (ST)^3 = -1 \rangle$$

- $\mathcal{A} = \mathcal{D} = \mathcal{Q}_{2,3} = \left(\frac{2,3}{\mathbb{Q}}\right) = \langle 1, i, j, k = ij \mid i^2 = 2, j^2 = 3 \rangle_{\mathbb{Q}}$,
  $\Lambda = \langle 1, i, \frac{1}{2}(1 + i + ij), \frac{1}{2}(j + ij) \rangle_{\mathbb{Z}}$ maximal order.

$$a = \frac{1}{2}\begin{pmatrix} 1 & \sqrt{2}+1 \\ 3-3\sqrt{2} & 1 \end{pmatrix}, b = \begin{pmatrix} \sqrt{2} & \sqrt{2}+1 \\ 3-3\sqrt{2} & -\sqrt{2} \end{pmatrix}, t = b - a + 1.$$

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

The congruence subgroup problem

- $n \in \mathbb{N}$
- $\Lambda_S[n] \hookrightarrow \Lambda_S^* \to (\Lambda_S/n\Lambda_S)^*$ (finite group)
- $\Lambda_S[n]$ is normal in Λ_S^* of finite index.

The congruence subgroup problem

- $n \in \mathbb{N}$
- $\Lambda_S[n] \hookrightarrow \Lambda_S^* \to (\Lambda_S/n\Lambda_S)^*$ (finite group)
- $\Lambda_S[n]$ is normal in Λ_S^* of finite index.

Definition

$U \leq \Lambda_S^*$ is called congruence subgroup, if there is some $n \in \mathbb{N}$ such that $\Lambda_S[n] \subseteq U$.
The algebra $\mathcal{A}$ has the congruence subgroup property for S, if all subgroups U of finite index in Λ_S^* are congruence subgroups.

The congruence subgroup problem

- $n \in \mathbb{N}$
- $\Lambda_S[n] \hookrightarrow \Lambda_S^* \to (\Lambda_S/n\Lambda_S)^*$ (finite group)
- $\Lambda_S[n]$ is normal in Λ_S^* of finite index.

Definition

$U \leq \Lambda_S^*$ is called congruence subgroup, if there is some $n \in \mathbb{N}$ such that $\Lambda_S[n] \subseteq U$.
The algebra $\mathcal{A}$ has the congruence subgroup property for S, if all subgroups U of finite index in Λ_S^* are congruence subgroups.

Conjecture (Serre, 1970)

$\mathcal{A}$ has the congruence subgroup property for S if and only if

$$\mathrm{Rk}_S(\mathrm{SL}(\mathcal{A})) := \sum_{i=1}^{s} \mathrm{Rk}(\mathrm{SL}(\mathcal{A}_{\wp_i})) + \sum_{v \in V_\infty} \mathrm{Rk}(\mathrm{SL}(\mathcal{A}_v)) \geq 2$$

and $\mathrm{Rk}(\mathrm{SL}(\mathcal{A}_{\wp_i})) > 0$ for all i.

$\mathbb{Q}^{2\times 2}$ has not the congruence subgroup property

Idea

G finite simple group, not an epimorphic image of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

$$1 \to N \hookrightarrow \mathrm{SL}_2(\mathbb{Z}) \overset{\varphi}{\twoheadrightarrow} G \to 1$$

Then N is not a congruence subgroup.

$\mathbb{Q}^{2\times 2}$ has not the congruence subgroup property

Idea

G finite simple group, not an epimorphic image of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

$$1 \to N \hookrightarrow \mathrm{SL}_2(\mathbb{Z}) \stackrel{\varphi}{\twoheadrightarrow} G \to 1$$

Then N is not a congruence subgroup.

$$\mathrm{SL}_2(\mathbb{Z}) = \langle S, ST \mid S^2 = (ST)^3 = -1 \rangle$$

$G = \langle x, y \rangle$ so that $x^2 = y^3 = 1$.
$\varphi : \mathrm{SL}_2(\mathbb{Z}) \to G, S \mapsto x, (ST) \mapsto y$ epimorphism. $N :=$Ker(φ) no congruence subgroup.
There are many such groups G.
E.g. $G = J_1$ has standard generators of order 2 and 3.

$S = \{\infty\}$, $\mathrm{Rk}_S(\mathrm{SL}_2(\mathbb{Q})) = \mathrm{Rk}(\mathrm{SL}_2(\mathbb{R})) = 1 < 2$

So the example confirms Serre's conjecture.

$\mathcal{Q}_{2,3}$ has not the congruence subgroup property

Idea

G finite simple group, not an epimorphic image of $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

$$1 \to N \hookrightarrow \mathrm{SL}_2(\mathbb{Z}) \stackrel{\varphi}{\twoheadrightarrow} G \to 1$$

Then N is not a congruence subgroup.

Λ maximal order in $\mathcal{Q}_{2,3}$. $\Lambda^* = \langle a, b, t \mid a^3 = b^2 = atbt = -1 \rangle$

Theorem

Choose $G = J_1 = \langle x, y \rangle$ with $x^2 = y^3 = 1$. Put $z := (xy)^3 x$. Then z is the unique element such that $yzxz = 1$.

$$\varphi : \Lambda^* \twoheadrightarrow J_1, a \mapsto y, b \mapsto x, t \mapsto z$$

epimorphisms. Ker(φ) no congruence subgroup.

$S = \{\infty\}$, $\mathrm{Rk}_S(\mathrm{SL}_2(\mathbb{Q})) = \mathrm{Rk}(\mathrm{SL}_2(\mathbb{R})) = 1 < 2$

So also this example confirms Serre's conjecture. To find a counterexample, need to choose $S_f \neq \emptyset$.

Compute presentation of Λ_S^*

Part I for $S_f = \emptyset$, Braun, Coulangeon, N., Schönnenbeck (2015)

- Action of $\mathcal{A}^*$ on $\mathcal{X}_\infty$.
- computes generators and relations for Λ^*.
- solves word problem in these generators
- uses Voronoi algorithm to enumerate perfect forms.
- Implementation is good for $\dim_{\mathbb{Q}}(\mathcal{A}) \leq 9$.
- For quaternion algebras we are better than Magma (5 min. versus 1 day)
- For division algebras of degree 3 this is the first available algorithm.

Compute presentation of Λ_S^*

Part I for $S_f = \emptyset$, Braun, Coulangeon, N., Schönnenbeck (2015)

- Action of $\mathcal{A}^*$ on $\mathcal{X}_\infty$.
- computes generators and relations for Λ^*.
- solves word problem in these generators
- uses Voronoi algorithm to enumerate perfect forms.
- Implementation is good for $\dim_{\mathbb{Q}}(\mathcal{A}) \leq 9$.
- For quaternion algebras we are better than Magma (5 min. versus 1 day)
- For division algebras of degree 3 this is the first available algorithm.

Part II for $S_f = \{\wp_1, \ldots, \wp_s\}$, Coulangeon, N. (in preparation)

- Action of $\mathcal{A}^*$ on $\mathcal{X}_{\wp_1} \times \ldots \times \mathcal{X}_{\wp_s}$.
- Stabilisers Λ^* for suitable orders Λ.
- Idea: Chinburg et al (2014):
  $\mathcal{A} = \left(\frac{-1,-1}{\mathbb{Q}}\right) \Rightarrow \mathrm{Rk}_S(\mathcal{A}) = |S_f - \{2\}|$
  $\mathcal{X}_p$ is tree, stabilisers finite.

Part I for $S_f = \emptyset$: Voronoi

- $\mathcal{A} = \mathcal{D}^{n \times n}$ simple $\mathbb{Q}$-algebra
- $\mathcal{A} \hookrightarrow \mathcal{A}_{\mathbb{R}} := \mathcal{A} \otimes_{\mathbb{Q}} \mathbb{R}$ real semisimple algebra, so isomorphic to direct sum of matrix rings over $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$.
- $\mathcal{A}_{\mathbb{R}}$ has "canonical involution". $x \mapsto x^{\dagger}$

Part I for $S_f = \emptyset$: Voronoi

- $\mathcal{A} = \mathcal{D}^{n \times n}$ simple $\mathbb{Q}$-algebra
- $\mathcal{A} \hookrightarrow \mathcal{A}_{\mathbb{R}} := \mathcal{A} \otimes_{\mathbb{Q}} \mathbb{R}$ real semisimple algebra, so isomorphic to direct sum of matrix rings over $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$.
- $\mathcal{A}_{\mathbb{R}}$ has "canonical involution". $x \mapsto x^{\dagger}$
- $\Sigma := \mathrm{Sym}(\mathcal{A}_{\mathbb{R}}) := \left\{ F \in \mathcal{A}_{\mathbb{R}} \mid F^{\dagger} = F \right\}$ symmetric elements.
- $(-,-) : \Sigma \times \Sigma \to \mathbb{R}$, $(F_1, F_2) := \mathrm{trace}(F_1 F_2^{\dagger})$.
- $(\Sigma, (-,-))$ euclidean space.
- Note: in general $\mathcal{A}^{\dagger} \neq \mathcal{A}$.

Part I for $S_f = \emptyset$: Voronoi

- $\mathcal{A} = \mathcal{D}^{n\times n}$ simple $\mathbb{Q}$-algebra
- $\mathcal{A} \hookrightarrow \mathcal{A}_{\mathbb{R}} := \mathcal{A} \otimes_{\mathbb{Q}} \mathbb{R}$ real semisimple algebra, so isomorphic to direct sum of matrix rings over $\mathbb{R}$, $\mathbb{C}$ and $\mathbb{H}$.
- $\mathcal{A}_{\mathbb{R}}$ has "canonical involution". $x \mapsto x^\dagger$
- $\Sigma := \mathrm{Sym}(\mathcal{A}_{\mathbb{R}}) := \left\{F \in \mathcal{A}_{\mathbb{R}} \mid F^\dagger = F\right\}$ symmetric elements.
- $(-,-) : \Sigma \times \Sigma \to \mathbb{R}$, $(F_1, F_2) := \mathrm{trace}(F_1 F_2^\dagger)$.
- $(\Sigma, (-,-))$ euclidean space.
- Note: in general $\mathcal{A}^\dagger \neq \mathcal{A}$.

Positive forms

- Let $V = \mathcal{D}^{1\times n}$ the simple right $\mathcal{A}$-module, $V_{\mathbb{R}} = V \otimes_{\mathbb{Q}} \mathbb{R}$.
- $x \in V_{\mathbb{R}} \Rightarrow x^\dagger x \in \Sigma$.
- $F \in \Sigma$ positive if $F[x] > 0$ for all $0 \neq x \in V_{\mathbb{R}}$.

$$F[x] := (F, x^\dagger x) = \mathrm{trace}(F x^\dagger x) = \mathrm{trace}(x F x^\dagger) > 0$$

- construct $\mathcal{X}_\infty$ in the cone $\Sigma^{>0} = \{F \in \Sigma \mid F \text{ positive } \}$

Lattices and perfect forms

- Let $\mathcal{O}$ be a $\mathbb{Z}_K$-order in $\mathcal{D}$ and L an $\mathcal{O}$-lattice in the simple $\mathcal{A}$ module V.
- $\Lambda := \mathrm{End}_{\mathcal{O}}(L)$ is $\mathbb{Z}_K$-order in $\mathcal{A}$ with unit group $\Lambda^* := \mathrm{GL}(L) = \{a \in \mathcal{A} \mid aL = L\}$.

Lattices and perfect forms

- Let $\mathcal{O}$ be a $\mathbb{Z}_K$-order in $\mathcal{D}$ and L an $\mathcal{O}$-lattice in the simple $\mathcal{A}$ module V.
- $\Lambda := \mathrm{End}_{\mathcal{O}}(L)$ is $\mathbb{Z}_K$-order in $\mathcal{A}$ with unit group $\Lambda^* := \mathrm{GL}(L) = \{a \in \mathcal{A} \mid aL = L\}$.

L-minimal vectors

Choose $F \in \Sigma^{>0}$ (positive form).

- $\mu(F) := \mu_L(F) = \min\{F[\ell] \mid 0 \neq \ell \in L\}$ the L-minimum of F
- $\mathcal{M}_L(F) := \{\ell \in L \mid F[\ell] = \mu_L(F)\}$ set of L-minimal vectors

Lattices and perfect forms

- Let $\mathcal{O}$ be a $\mathbb{Z}_K$-order in $\mathcal{D}$ and L an $\mathcal{O}$-lattice in the simple $\mathcal{A}$ module V.
- $\Lambda := \mathrm{End}_{\mathcal{O}}(L)$ is $\mathbb{Z}_K$-order in $\mathcal{A}$ with unit group $\Lambda^* := \mathrm{GL}(L) = \{a \in \mathcal{A} \mid aL = L\}$.

L-minimal vectors

Choose $F \in \Sigma^{>0}$ (positive form).

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

Lattices and perfect forms

- Let $\mathcal{O}$ be a $\mathbb{Z}_K$-order in $\mathcal{D}$ and L an $\mathcal{O}$-lattice in the simple $\mathcal{A}$ module V.
- $\Lambda := \mathrm{End}_{\mathcal{O}}(L)$ is $\mathbb{Z}_K$-order in $\mathcal{A}$ with unit group $\Lambda^* := \mathrm{GL}(L) = \{a \in \mathcal{A} \mid aL = L\}$.

L-minimal vectors

Choose $F \in \Sigma^{>0}$ (positive form).

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

Main theorem

$$\mathcal{T} := \{\mathrm{Vor}_L(F) \mid F \in \Sigma^{>0},\ \text{L-perfect}\ \}$$

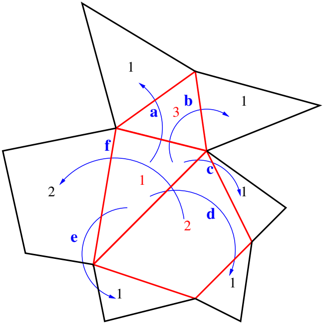
is an exact locally finite polyhedral tiling of the cone $\Sigma^{\geq 0}$.
Λ^* acts on $\mathcal{T}$ with finitely many orbits.

Generators for Λ^*

- Representatives $\mathfrak{R} := \{F_1, \ldots, F_s\}$ of the Λ^*-orbits of L-perfect forms.
- for all neighbors F of the F_i (codim($\mathrm{Vor}(F) \cap \mathrm{Vor}(F_i)$)$= 1$) find some $g_F \in \Lambda^*$ with $g_F \cdot F \in \mathfrak{R}$ (isometry of lattices)
- Then $\Lambda^* = \langle \mathrm{Aut}(F_i), g_F \mid F_i \in \mathfrak{R}, F$ neighbor of some $F_j \in \mathfrak{R}\rangle$.

Generators for Λ^*

- Representatives $\mathfrak{R} := \{F_1, \ldots, F_s\}$ of the Λ^*-orbits of L-perfect forms.
- for all neighbors F of the F_i (codim($\mathrm{Vor}(F) \cap \mathrm{Vor}(F_i)$)$= 1$) find some $g_F \in \Lambda^*$ with $g_F \cdot F \in \mathfrak{R}$ (isometry of lattices)
- Then $\Lambda^* = \langle \mathrm{Aut}(F_i), g_F \mid F_i \in \mathfrak{R}, F$ neighbor of some $F_j \in \mathfrak{R} \rangle$.



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

An example: $\mathcal{Q}_{2,3}$.

- $\mathcal{A} = \mathcal{D} = \mathcal{Q}_{2,3} = \left(\frac{2,3}{\mathbb{Q}}\right) = \langle i, j \mid i^2 = 2, j^2 = 3, ij = -ji \rangle_{\mathbb{Q}}$
- maximal order $\Lambda = \langle 1, i, \frac{1}{2}(1 + i + ij), \frac{1}{2}(j + ij) \rangle_{\mathbb{Z}}$
- $V = \mathcal{A}$, $L = \Lambda$, $\Lambda = \mathrm{End}_{\Lambda}(\Lambda)$.
- $\mathcal{A} \hookrightarrow \mathcal{A}_{\mathbb{R}} = \mathbb{R}^{2\times 2}$ by

$$i \mapsto \mathrm{diag}(\sqrt{2}, -\sqrt{2}),\ j \mapsto \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}$$

An example: $\mathcal{Q}_{2,3}$.

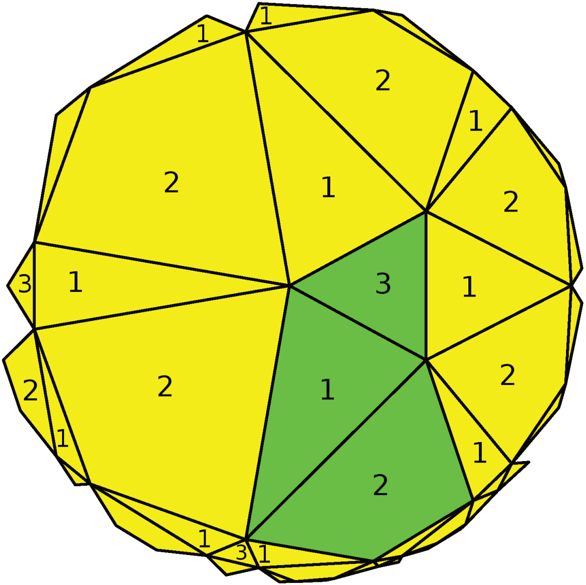
- $\mathcal{A} = \mathcal{D} = \mathcal{Q}_{2,3} = \left(\frac{2,3}{\mathbb{Q}}\right) = \langle i, j \mid i^2 = 2, j^2 = 3, ij = -ji\rangle_{\mathbb{Q}}$
- maximal order $\Lambda = \langle 1, i, \frac{1}{2}(1 + i + ij), \frac{1}{2}(j + ij)\rangle_{\mathbb{Z}}$
- $V = \mathcal{A}$, $L = \Lambda$, $\Lambda = \mathrm{End}_{\Lambda}(\Lambda)$.
- $\mathcal{A} \hookrightarrow \mathcal{A}_{\mathbb{R}} = \mathbb{R}^{2\times 2}$ by

$$i \mapsto \mathrm{diag}(\sqrt{2}, -\sqrt{2}),\ j \mapsto \begin{pmatrix} 0 & 1 \\ 3 & 0 \end{pmatrix}$$

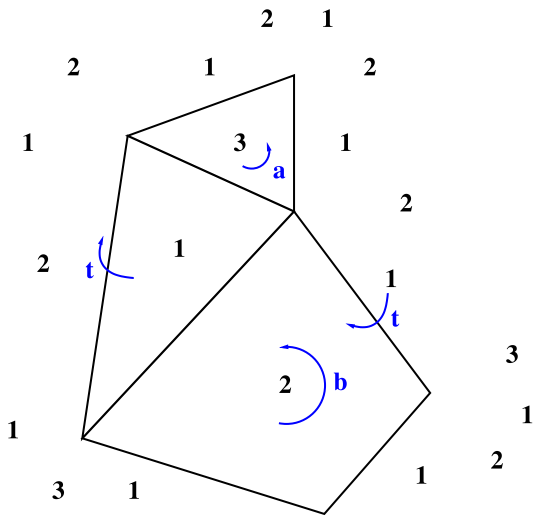
Three perfect forms

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

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



$\Lambda^*/\langle \pm 1\rangle = \langle a, b, t \mid a^3, b^2, atbt\rangle$, $\mathcal{A} \cong \mathcal{Q}_{2,3}$

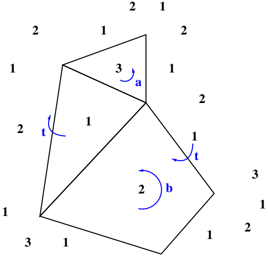


$\Lambda^* = \langle a, b, t \mid a^3 = b^2 = atbt = -1 \rangle$, $\mathcal{A} \cong \mathcal{Q}_{2,3}$

$$a = \frac{1}{2}\begin{pmatrix} 1 & \sqrt{2}+1 \\ 3-3\sqrt{2} & 1 \end{pmatrix}$$

$$b = \begin{pmatrix} \sqrt{2} & \sqrt{2}+1 \\ 3-3\sqrt{2} & -\sqrt{2} \end{pmatrix}$$

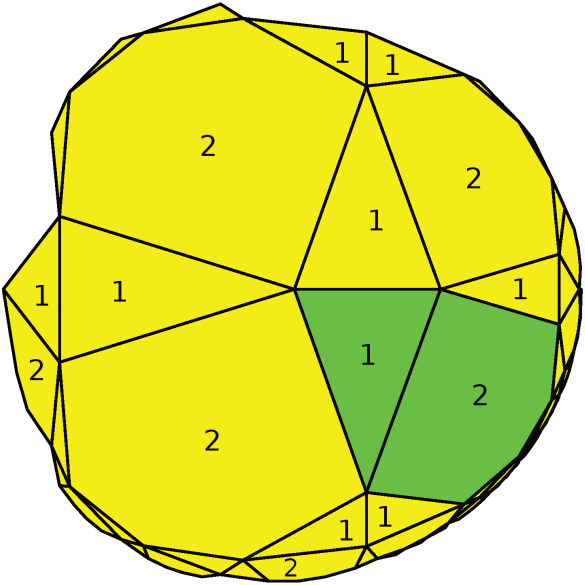
$$t = \frac{1}{2}\begin{pmatrix} 2\sqrt{2}+1 & \sqrt{2}+1 \\ 3-3\sqrt{2} & 1-2\sqrt{2} \end{pmatrix}$$



Then

- $t = b - a + 1$ has minimal polynomial $\mu_t = x^2 + x - 1$
- $\langle a, b \rangle / \langle \pm 1 \rangle \cong C_3 * C_2 \cong \mathrm{PSL}_2(\mathbb{Z})$

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



A rational division algebra of index 3

- $\vartheta = \zeta_9 + \zeta_9^{-1}$, $\langle\sigma\rangle = \mathrm{Gal}(\mathbb{Q}(\vartheta)/\mathbb{Q})$,
- $\mathcal{A}$ the $\mathbb{Q}$-algebra generated by
- $Z := \begin{pmatrix} \vartheta & & \\ & \sigma(\vartheta) & \\ & & \sigma^2(\vartheta) \end{pmatrix}$ and $\Pi := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix}$.
- $\mathcal{A}$ division algebra with center $\mathbb{Q}$, Hasse invariants $\frac{1}{3}$ at 2 and $\frac{2}{3}$ at 3.
- Λ maximal order in $\mathcal{A}$
- $\Gamma := \Lambda^\times$ has 431 orbits of perfect forms and presentation
- $$\begin{aligned}\Gamma \cong \langle a, b \mid \quad & b^2a^2(b^{-1}a^{-1})^2,\ b^{-2}(a^{-1}b^{-1})^2ab^{-2}a^2b^{-3}, \\ & ab^2a^{-1}b^3a^{-2}bab^3,\ a^2bab^{-2}ab^{-1}(a^{-2}b)^2, \\ & a^{-1}b^2a^{-1}b^{-1}a^{-5}b^{-2}a^{-3}, \\ & b^{-2}a^{-2}b^{-1}a^{-1}b^{-1}a^{-2}b^{-1}a^{-1}b^{-2}(a^{-1}b^{-1})^3\rangle\end{aligned}$$
- $a = \frac{1}{3}((1-3Z-Z^2)+(2+Z^2)\Pi+(1-Z^2)\Pi^2)$,
  $b = \frac{1}{3}((-3-2Z+Z^2)+(1-2Z)\Pi+(1-Z^2)\Pi^2)$.

Quaternion algebras with imaginary quadratic fields

$$\mathcal{A} = \left(\frac{-1, -1}{k}\right), \quad k = \mathbb{Q}(\sqrt{-d})$$

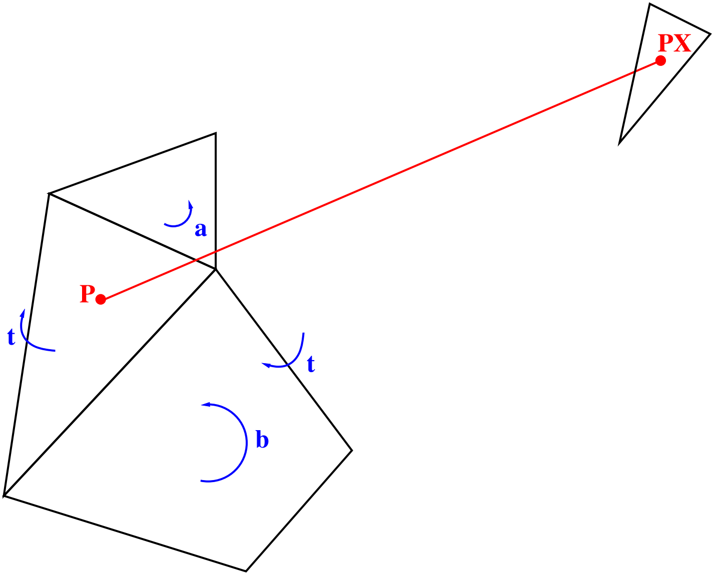
d	perfect forms	timing Voronoï	timing presentation	number of generators
7	1	$1.24s$	$0.42s$	2
31	8	$6.16s$	$0.50s$	3
55	21	$14.69s$	$1.01s$	5
79	40	$28.74s$	$1.78s$	5
95	69	$53.78s$	$2.57s$	7
103	53	$38.39s$	$2.52s$	6
111	83	$66.16s$	$3.02s$	6
255	302	$323.93s$	$17.54s$	16

Quaternion algebras with center $\mathbb{Q}(\sqrt{-7})$

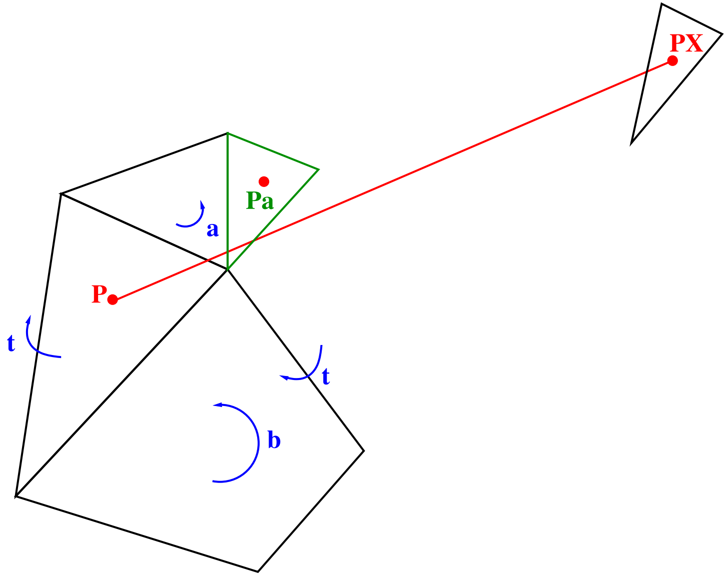
$$\mathcal{A} = \left(\frac{a,b}{\mathbb{Q}(\sqrt{-7})}\right)$$

a,b	perfect forms	timing Voronoï	timing presentation	number of generators
$-1,-1$	1	$1.24s$	$0.42s$	2
$-1,-11$	20	$21.61s$	$4.13s$	6
$-11,-14$	58	$51.46s$	$5.11s$	10
$-1,-23$	184	$179.23s$	$89.34s$	16

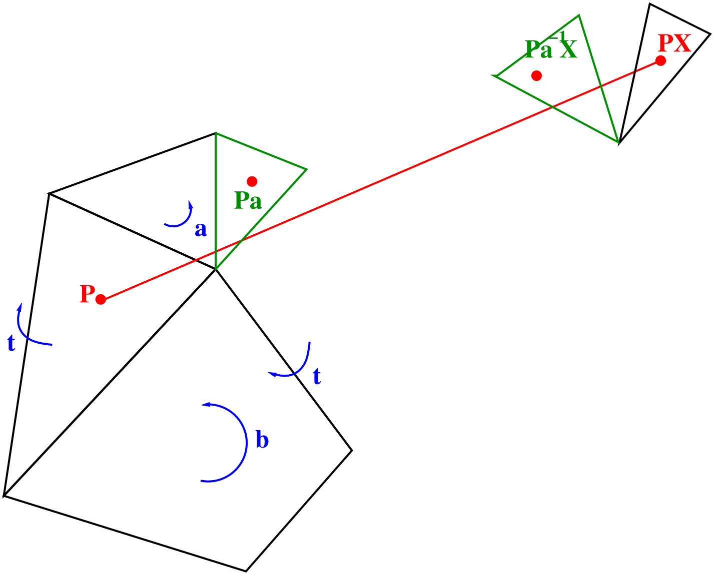
The word problem



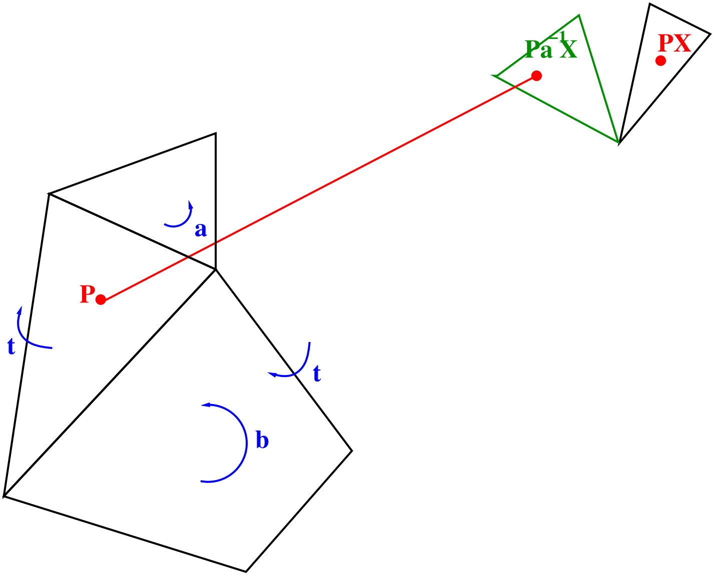
The word problem



The word problem



The word problem



Part II: $S_f \neq \emptyset$, buildings

$S = V_\infty \cup S_f$, $S_f = \{\wp_1, \ldots, \wp_s\}$.

Borel, Serre: Λ_S^* is finitely presented.

faithful action on locally finite polyhedral complex
$\mathcal{X} = \mathcal{X}_\infty \times \mathcal{X}_{\wp_1} \times \ldots \times \mathcal{X}_{\wp_s}$
$\mathcal{X}_\infty =$ Voronoi domains of L-perfect forms in $\Sigma^{>0}$.
$\mathcal{X}_{\wp_i} =$ Bruhat-Tits building of the $\wp_i$-adic group $\mathrm{SL}(\mathcal{A}_{\wp_i})$.

Part II: $S_f \neq \emptyset$, buildings

$S = V_\infty \cup S_f$, $S_f = \{\wp_1, \dots, \wp_s\}$.

Borel, Serre: Λ_S^* is finitely presented.

faithful action on locally finite polyhedral complex
$\mathcal{X} = \mathcal{X}_\infty \times \mathcal{X}_{\wp_1} \times \dots \times \mathcal{X}_{\wp_s}$
$\mathcal{X}_\infty$ = Voronoi domains of L-perfect forms in $\Sigma^{>0}$.
$\mathcal{X}_{\wp_i}$ = Bruhat-Tits building of the $\wp_i$-adic group $\mathrm{SL}(\mathcal{A}_{\wp_i})$.

Simplification

- $K = \mathbb{Q}$, $s = 1$, $\wp_1 = p\mathbb{Z}$, p unramified in $\mathcal{D}$.
- $\Lambda_S = \Lambda[\frac{1}{p}] = \{a \in \mathcal{A} \mid p^i a \in \Lambda \text{ for some } i\}$.
- Completion: $\mathcal{A}_p = \mathbb{Q}_p \otimes \mathcal{D}^{n\times n} = \mathbb{Q}_p^{nd\times nd}$.
- $\mathrm{SL}(\mathcal{A}_p) = \mathrm{SL}_{nd}(\mathbb{Q}_p)$.

The building of $\mathrm{SL}_m(\mathbb{Q}_p)$

- $V_p = \mathbb{Q}_p^m$ simple $\mathcal{A}_p$-module.
- L a $\mathbb{Z}_p$-lattice in V_p,
- $[L] := \{p^i L \mid i \in \mathbb{Z}\}$ homothetie class of L.
- $\mathcal{X}_p$: $m-1$-dimensional simplicial complex with
- vertices (0-simplices) $\mathcal{K} := \{[L] \mid L$ lattice in $V_p\}$
- $\{[L_1], \ldots, [L_k]\} \subset \mathcal{K}$ is a $k-1$ simplex, if there are $M_i \in [L_i]$ s.t. (after permutation)

$$\ldots \supset M_1 \supset M_2 \supset \ldots \supset M_k \supset pM_1 \supset \ldots$$

The building of $\mathrm{SL}_m(\mathbb{Q}_p)$

- $V_p = \mathbb{Q}_p^m$ simple $\mathcal{A}_p$-module.
- L a $\mathbb{Z}_p$-lattice in V_p,
- $[L] := \{p^i L \mid i \in \mathbb{Z}\}$ homothetie class of L.
- $\mathcal{X}_p$: $m-1$-dimensional simplicial complex with
- vertices (0-simplices) $\mathcal{K} := \{[L] \mid L \text{ lattice in } V_p\}$
- $\{[L_1], \ldots, [L_k]\} \subset \mathcal{K}$ is a $k-1$ simplex, if there are $M_i \in [L_i]$ s.t. (after permutation)

$$\ldots \supset M_1 \supset M_2 \supset \ldots \supset M_k \supset pM_1 \supset \ldots$$

- Choose basis $(b_1, \ldots, b_m)$ of V_p such that $L_0 := \bigoplus \mathbb{Z}_p b_i$ is Λ-invariant
- The Type of $[L]$ is $\nu_p(\det(B)) \in \mathbb{Z}/m\mathbb{Z}$ for any $B \in \mathrm{GL}_m(\mathbb{Q}_p)$ with $BL_0 = L$.
- $\mathrm{SL}_m(\mathbb{Q}_p)$ acts on $\mathcal{K}$ with Type as a separating invariant.

Presentation of the S-unit group

Main theorem

- $\Lambda_S^* = \Lambda[\frac{1}{p}]$ acts as simplicial automorphisms on $\mathcal{X}_p$ with finitely many orbits.
- $\mathbb{Z}_{K,S}^* = \mathbb{Z}[\frac{1}{p}]^* = \{1, -1\} \times \{p^i \mid i \in \mathbb{Z}\} = Z(\Lambda_S^*)$ is the kernel of this action.
- $\mathrm{Stab}_{\Lambda_S^*}(L_0) = \Lambda^*$.
- $\mathrm{Stab}_{\Lambda_S^*}([L_0]) = \Lambda^* \times \{p^i \mid i \in \mathbb{Z}\}$.

Presentation of the S-unit group

Main theorem

- $\Lambda_S^* = \Lambda[\frac{1}{p}]$ acts as simplicial automorphisms on $\mathcal{X}_p$ with finitely many orbits.
- $\mathbb{Z}_{K,S}^* = \mathbb{Z}[\frac{1}{p}]^* = \{1, -1\} \times \{p^i \mid i \in \mathbb{Z}\} = Z(\Lambda_S^*)$ is the kernel of this action.
- $\mathrm{Stab}_{\Lambda_S^*}(L_0) = \Lambda^*$.
- $\mathrm{Stab}_{\Lambda_S^*}([L_0]) = \Lambda^* \times \{p^i \mid i \in \mathbb{Z}\}$.

Presentation

- Representatives $\mathcal{R} := \{[L_1], \ldots, [L_s]\}$ of the Λ_S^*-orbits on $\mathcal{K}$
- For all adjacent vertices $[L]$ of some $[L_i]$ compute $g_L \in \Lambda_S^*$ such that $g_L \cdot [L] \in \mathcal{R}$.
- Then

$$\Lambda_S^* = \langle Z(\Lambda_S^*), \mathrm{Stab}_{\Lambda_S^*}(L_i), g_L \mid [L_i] \in \mathcal{R}, [L] \text{ adjacent to some } [L_j] \in \mathcal{R} \rangle.$$

- To get a presentation we need to solve the word problem in the point stabilisers ($\cong \Lambda^*$)

An example

$\mathcal{A} = \mathcal{D} = \mathcal{Q}_{2,3}$ and Λ as above

$$\Lambda^\times/\{\pm 1\} = \langle A, B \mid B^3, (A^2B)^2\rangle$$

Λ is right principal ideal domain

$$\Lambda[\frac{1}{p}]^*/\mathbb{Z}[\frac{1}{p}]^* = \langle A, B, C_p\rangle$$

with $C_p \in \Lambda$ of norm p.

An example

$\mathcal{A} = \mathcal{D} = \mathcal{Q}_{2,3}$ and Λ as above

$$\Lambda^\times/\{\pm 1\} = \langle A, B \mid B^3, (A^2B)^2 \rangle$$

Λ is right principal ideal domain

$$\Lambda[\frac{1}{p}]^*/\mathbb{Z}[\frac{1}{p}]^* = \langle A, B, C_p \rangle$$

with $C_p \in \Lambda$ of norm p.

$$\Lambda[\frac{1}{5}]^*/(\mathbb{Z}[\frac{1}{5}]^*) = \left\langle A, C \mid \begin{array}{l} (CA^{-2}C)^3, (C^{-1}A^2C^{-1}A^{-2})^2, \\ CA^{-1}C^{-1}A^2C^{-1}A^{-1}C^{-1}ACA^{-1}CA, \\ CA^3CA^{-1}C^{-1}A^2C^{-1}AC^{-1}A^2C^{-1}A^{-1}, \\ (CA^{-1}CACA^{-2}CA^{-1}C)^2 \end{array} \right\rangle$$

An example

$\mathcal{A} = \mathcal{D} = \mathcal{Q}_{2,3}$ and Λ as above

$$\Lambda^\times/\{\pm 1\} = \langle A, B \mid B^3, (A^2B)^2 \rangle$$

Λ is right principal ideal domain

$$\Lambda[\frac{1}{p}]^*/\mathbb{Z}[\frac{1}{p}]^* = \langle A, B, C_p \rangle$$

with $C_p \in \Lambda$ of norm p.

$$\Lambda[\frac{1}{5}]^*/(\mathbb{Z}[\frac{1}{5}]^*) = \left\langle A, C \;\middle|\; \begin{array}{l} (CA^{-2}C)^3, (C^{-1}A^2C^{-1}A^{-2})^2, \\ CA^{-1}C^{-1}A^2C^{-1}A^{-1}C^{-1}ACA^{-1}CA, \\ CA^3CA^{-1}C^{-1}A^2C^{-1}AC^{-1}A^2C^{-1}A^{-1}, \\ (CA^{-1}CACA^{-2}CA^{-1}C)^2 \end{array} \right\rangle$$

$$\Lambda[\frac{1}{7}]^*/(\mathbb{Z}[\frac{1}{7}]^*) = \left\langle A, B, C \;\middle|\; \begin{array}{l} B^3, (A^2B)^2, CBA^{-1}CAB^{-1}A^{-2}, \\ CA^2BA^{-2}CABA, CB^{-1}A^{-1}BABC^{-1}B^{-1}, \\ CB^{-1}AC^{-1}A^2B^{-1}AB \end{array} \right\rangle$$

Compute presentation of Λ_S^*

Part I: $S_f = \emptyset$, Braun, Coulangeon, N., Schönnenbeck (2015)

- Action $\mathcal{A}^*$ on $\mathcal{X}_\infty$.
- Voronoi-algorithm, perfect forms, isometries of lattices
- Presentation of Λ^*.
- Word problem in generators.
- Practicable for $\dim_{\mathbb{Q}}(\mathcal{A}) \leq 9$.
- For quaternion algebra better performance than Magma (5 min. versus 1 day)
- First available algorithms for division algebras of index ≥ 3.

Part II: $S_f = \{\wp_1, \ldots, \wp_s\}$, Coulangeon, N. (in preparation)

- Action of $\mathcal{A}^*$ on $\mathcal{X}_{\wp_1} \times \ldots \times \mathcal{X}_{\wp_s}$.
- Stabilisers Λ^* for certain orders Λ.
- Additional generators: suitable elements of Λ of norm dividing $\prod_{i=1}^s \wp_i^{a_i}$.