Berechnung von Einheitengruppen von Ordnungen

Gabriele Nebe

Lehrstuhl D für Mathematik

Baer Kolloquium, Würzburg, 30.05.2015

Setup

- $\mathcal{A} = \mathcal{D}^{n \times n}$ einfache $\mathbb{Q}$-Algebra
- $\mathcal{D}$ Divisionsalgebra mit Zentrum K
- K ein algebraischer Zahlkörper
- $\mathbb{Z}_K$ Ring der ganzen Zahlen in K
- V_∞ die unendlichen Stellen von K
- $V_f := \{\wp \mid 0 \neq \wp \trianglelefteq_{prim} \mathbb{Z}_K\}$ die endlichen Stellen von K
- $S_f = \{\wp_1, \ldots, \wp_s\} \subseteq V_f$
- $S := S_f \cup V_\infty$
- $\mathbb{Z}_{K,S} := \{a \in K \mid ||a||_\wp \leq 1$ für alle $\wp \notin S\}$ S-ganze Zahlen
- Λ eine $\mathbb{Z}_K$-Ordnung in $\mathcal{A}$.
- $\Lambda_S := \mathbb{Z}_{K,S} \otimes \Lambda$

Satz (Borel, Serre, 1962-1975)

Die Einheitengruppe von Λ_S ist endlich präsentierbar.

Der Beweis von Borel und Serre

Satz (Borel, Serre 1962-1975)

Die Einheitengruppe von Λ_S ist endlich präsentierbar.

- Die Einheitengruppe Λ_S^* operiert auf lokal endlichem zellulären Komplex
- $\mathfrak{X} = \mathfrak{X}_\infty \times \mathfrak{X}_{\wp_1} \times \ldots \times \mathfrak{X}_{\wp_s}$
- mit endlichem Punktstabilisator

Der Beweis von Borel und Serre

Satz (Borel, Serre 1962-1975)

Die Einheitengruppe von Λ_S ist endlich präsentierbar.

- Die Einheitengruppe Λ_S^* operiert auf lokal endlichem zellulären Komplex
- $\mathcal{X} = \mathcal{X}_\infty \times \mathcal{X}_{\wp_1} \times \ldots \times \mathcal{X}_{\wp_s}$
- mit endlichem Punktstabilisator
- $\mathcal{X}_{\wp_i} =$ Bruhat-Tits Gebäude der $\wp_i$-adischen Gruppe $\mathrm{SL}(\mathcal{A}_{\wp_i})$.
- $\mathcal{X}$ konstruiert als homogener Raum nach der maximal kompakten Untergruppe von $\mathrm{SL}(\mathcal{A}_\infty)$
- Allgemeine Theorie: Endliche Präsentation aus dieser Operation berechenbar.

Beispiele

- $\mathcal{A} = K$ algebraischer Zahlkörper, $\Lambda = \mathbb{Z}_K$, $S_f = \emptyset$,
  $\Lambda^* = \mathbb{Z}_K^* \cong \mu_K \times \mathbb{Z}^{r+s-1}$ (Dirichletscher Einheitensatz)

Beispiele

- $\mathcal{A} = K$ algebraischer Zahlkörper, $\Lambda = \mathbb{Z}_K$, $S_f = \emptyset$, $\Lambda^* = \mathbb{Z}_K^* \cong \mu_K \times \mathbb{Z}^{r+s-1}$ (Dirichletscher Einheitensatz)
- $\mathcal{A} = \mathcal{D} = \left(\frac{-1,-1}{\mathbb{Q}}\right) = \langle 1, i, j, k = ij \mid i^2 = j^2 = k^2 = -1 \rangle_{\mathbb{Q}}$ definite rationale Quaternionenalgebra, $\Lambda = \langle 1, i, j, k \rangle_{\mathbb{Z}}$. $S_f = \emptyset \Rightarrow \Lambda^* = \langle i, j \rangle \cong Q_8$ endlich.

Beispiele

- $\mathcal{A} = K$ algebraischer Zahlkörper, $\Lambda = \mathbb{Z}_K$, $S_f = \emptyset$,
  $\Lambda^* = \mathbb{Z}_K^* \cong \mu_K \times \mathbb{Z}^{r+s-1}$ (Dirichletscher Einheitensatz)
- $\mathcal{A} = \mathcal{D} = \left(\frac{-1,-1}{\mathbb{Q}}\right) = \langle 1, i, j, k = ij \mid i^2 = j^2 = k^2 = -1 \rangle_{\mathbb{Q}}$
  definite rationale Quaternionenalgebra, $\Lambda = \langle 1, i, j, k \rangle_{\mathbb{Z}}$.
  $S_f = \emptyset \Rightarrow \Lambda^* = \langle i, j \rangle \cong Q_8$ endlich.
  $S_f \neq \emptyset \Rightarrow$ Chinburg etal: Kongruenzuntergruppenproblem

Beispiele

- $\mathcal{A} = K$ algebraischer Zahlkörper, $\Lambda = \mathbb{Z}_K$, $S_f = \emptyset$,
  $\Lambda^* = \mathbb{Z}_K^* \cong \mu_K \times \mathbb{Z}^{r+s-1}$ (Dirichletscher Einheitensatz)
- $\mathcal{A} = \mathcal{D} = \left(\frac{-1,-1}{\mathbb{Q}}\right) = \langle 1, i, j, k = ij \mid i^2 = j^2 = k^2 = -1 \rangle_{\mathbb{Q}}$
  definite rationale Quaternionenalgebra, $\Lambda = \langle 1, i, j, k \rangle_{\mathbb{Z}}$.
  $S_f = \emptyset \Rightarrow \Lambda^* = \langle i, j \rangle \cong Q_8$ endlich.
  $S_f \neq \emptyset \Rightarrow$ Chinburg etal: Kongruenzuntergruppenproblem
- $\mathcal{A} = \mathbb{Q}^{2\times 2}$.

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

Beispiele

- $\mathcal{A} = K$ algebraischer Zahlkörper, $\Lambda = \mathbb{Z}_K$, $S_f = \emptyset$,
  $\Lambda^* = \mathbb{Z}_K^* \cong \mu_K \times \mathbb{Z}^{r+s-1}$ (Dirichletscher Einheitensatz)
- $\mathcal{A} = \mathcal{D} = \left(\frac{-1,-1}{\mathbb{Q}}\right) = \langle 1, i, j, k = ij \mid i^2 = j^2 = k^2 = -1\rangle_{\mathbb{Q}}$
  definite rationale Quaternionenalgebra, $\Lambda = \langle 1, i, j, k\rangle_{\mathbb{Z}}$.
  $S_f = \emptyset \Rightarrow \Lambda^* = \langle i, j\rangle \cong Q_8$ endlich.
  $S_f \neq \emptyset \Rightarrow$ Chinburg etal: Kongruenzuntergruppenproblem
- $\mathcal{A} = \mathbb{Q}^{2\times 2}$.

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

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

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

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

Das Kongruenzuntergruppenproblem

- $n \in \mathbb{N}$
- $\Lambda_S[n] \hookrightarrow \Lambda_S^* \to (\Lambda_S/n\Lambda_S)^*$ (endliche Gruppe)
- $\Lambda_S[n]$ ist ein Normalteiler in Λ_S^* von endlichem Index

Das Kongruenzuntergruppenproblem

- $n \in \mathbb{N}$
- $\Lambda_S[n] \hookrightarrow \Lambda_S^* \to (\Lambda_S/n\Lambda_S)^*$ (endliche Gruppe)
- $\Lambda_S[n]$ ist ein Normalteiler in Λ_S^* von endlichem Index

Definition

Eine Untergruppe U von Λ_S^* heißt Kongruenzuntergruppe, falls es ein $n \in \mathbb{N}$ gibt mit $\Lambda_S[n] \subseteq U$.
Die Algebra $\mathcal{A}$ hat die Kongruenzuntergruppeneigenschaft für S, genau dann wenn jede Untergruppe U von endlichem Index in Λ_S^* eine Kongruenzuntergruppe ist.

Das Kongruenzuntergruppenproblem

- $n \in \mathbb{N}$
- $\Lambda_S[n] \hookrightarrow \Lambda_S^* \to (\Lambda_S/n\Lambda_S)^*$ (endliche Gruppe)
- $\Lambda_S[n]$ ist ein Normalteiler in Λ_S^* von endlichem Index

Definition

Eine Untergruppe U von Λ_S^* heißt Kongruenzuntergruppe, falls es ein $n \in \mathbb{N}$ gibt mit $\Lambda_S[n] \subseteq U$.
Die Algebra $\mathcal{A}$ hat die Kongruenzuntergruppeneigenschaft für S, genau dann wenn jede Untergruppe U von endlichem Index in Λ_S^* eine Kongruenzuntergruppe ist.

Vermutung (Serre, 1970)

$\mathcal{A}$ hat die Kongruenzuntergruppeneigenschaft für S genau dann wenn

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

und $\mathrm{Rk}(\mathrm{SL}(\mathcal{A}_{\wp_i})) > 0$ für alle i.

$\mathbb{Q}^{2\times 2}$ hat nicht die Kongruenzuntergruppeneigenschaft

Idee

G endliche einfache Gruppe, keine Faktorgruppe von $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

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

Dann ist N keine Kongruenzuntergruppe.

$\mathbb{Q}^{2\times 2}$ hat nicht die Kongruenzuntergruppeneigenschaft

Idee

G endliche einfache Gruppe, keine Faktorgruppe von $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

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

Dann ist N keine Kongruenzuntergruppe.

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

$G = \langle x, y \rangle$ mit $x^2 = y^3 = 1$.
$\varphi : \mathrm{SL}_2(\mathbb{Z}) \to G, S \mapsto x, (ST) \mapsto y$ Gruppenepimorphismus. N :=Kern(φ) keine Kongruenzuntergruppe.
Es gibt viele solche endliche Gruppen G.
Z.B. $G = J_1$ hat Standarderzeuger der Ordnung 2 und 3.

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

Das Beispiel bestätigt also Serre's Vermutung.

$\mathcal{Q}_{2,3}$ hat nicht die Kongruenzuntergruppeneigenschaft

Idee

G endliche einfache Gruppe, keine Faktorgruppe von $\mathrm{SL}_2(\mathbb{Z}/n\mathbb{Z})$.

$$1 \to N \hookrightarrow \Lambda^* \overset{\varphi}{\twoheadrightarrow} G \to 1$$

Dann ist N keine Kongruenzuntergruppe.

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

Satz

Wähle $G = J_1 = \langle x, y \rangle$ mit $x^2 = y^3 = 1$. Setze $z := (xy)^3 x$. Dann ist z das einzige Element von J_1 mit $yzxz = 1$.

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

Gruppenepimorphismus. Kern(φ) keine Kongruenzuntergruppe.

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

Das Beispiel bestätigt also Serre's Vermutung. Um ein Gegenbeispiel mit dieser Algebra zu finden, müssen wir also $S_f \neq \emptyset$ wählen.

Berechne Präsentation von Λ_S^*

Teil I für $S_f = \emptyset$, Braun, Coulangeon, N., Schönnenbeck (2015)

- Operation von $\mathcal{A}^*$ auf $\mathcal{X}_\infty$.
- Berechnet Präsentation von Λ^*.
- Löst Wortproblem in gegebenen Erzeugern.
- Benutzt Voronois Algorithmus zum Berechnen lokal dichtester Gitter.
- Läuft gut für kleine Beispiele, $\dim_{\mathbb{Q}}(\mathcal{A}) \leq 9$.
- Für Quaternionenalgebren besser als Magma (5 Min. versus 1 Tag)
- Erster verfügbarer Algorithmus für Divisionsalgebren vom Index 3.

Berechne Präsentation von Λ_S^*

Teil I für $S_f = \emptyset$, Braun, Coulangeon, N., Schönnenbeck (2015)

- Operation von $\mathcal{A}^*$ auf $\mathcal{X}_\infty$.
- Berechnet Präsentation von Λ^*.
- Löst Wortproblem in gegebenen Erzeugern.
- Benutzt Voronois Algorithmus zum Berechnen lokal dichtester Gitter.
- Läuft gut für kleine Beispiele, $\dim_{\mathbb{Q}}(\mathcal{A}) \leq 9$.
- Für Quaternionenalgebren besser als Magma (5 Min. versus 1 Tag)
- Erster verfügbarer Algorithmus für Divisionsalgebren vom Index 3.

Teil II für $S_f = \{\wp_1, \ldots, \wp_s\}$, Coulangeon, N. (in Vorbereitung)

- Operation von $\mathcal{A}^*$ auf $\mathcal{X}_{\wp_1} \times \ldots \times \mathcal{X}_{\wp_s}$.
- Punktstabilisatoren Λ^* für geeignete Ordnungen Λ.
- Idee: Chinburg et al (2014):
  $\mathcal{A} = \left(\frac{-1,-1}{\mathbb{Q}}\right) \Rightarrow \mathrm{Rk}_S(\mathcal{A}) = |S_f - \{2\}|$
  $\mathcal{X}_p$ ist Baum, Stabilisatoren endlich.

Teil I für $S_f = \emptyset$: Voronoitheorie

- $\mathcal{A} = \mathcal{D}^{n \times n}$ einfache $\mathbb{Q}$-Algebra
- $\mathcal{A} \hookrightarrow \mathcal{A}_{\mathbb{R}} := \mathcal{A} \otimes_{\mathbb{Q}} \mathbb{R}$ ist halbeinfache reelle Algebra, also isomorph zu direkter Summe von Matrixringen über $\mathbb{R}$, $\mathbb{C}$ und $\mathbb{H}$.
- Also trägt $\mathcal{A}_{\mathbb{R}}$ eine "kanonische" Involution $x \mapsto x^{\dagger}$

Teil I für $S_f = \emptyset$: Voronoitheorie

- $\mathcal{A} = \mathcal{D}^{n\times n}$ einfache $\mathbb{Q}$-Algebra
- $\mathcal{A} \hookrightarrow \mathcal{A}_{\mathbb{R}} := \mathcal{A} \otimes_{\mathbb{Q}} \mathbb{R}$ ist halbeinfache reelle Algebra, also isomorph zu direkter Summe von Matrixringen über $\mathbb{R}$, $\mathbb{C}$ und $\mathbb{H}$.
- Also trägt $\mathcal{A}_{\mathbb{R}}$ eine "kanonische" Involution $x \mapsto x^{\dagger}$
- $\Sigma := \mathrm{Sym}(\mathcal{A}_{\mathbb{R}}) := \left\{F \in \mathcal{A}_{\mathbb{R}} \mid F^{\dagger} = F\right\}$ symmetrische Elemente.
- $(-,-) : \Sigma \times \Sigma \to \mathbb{R}$, $(F_1, F_2) := \mathrm{trace}(F_1 F_2^{\dagger})$.
- $(\Sigma, (-,-))$ Euklidischer Raum.
- Achtung: Im Allgemeinen ist $\mathcal{A}^{\dagger} \neq \mathcal{A}$.

Teil I für $S_f = \emptyset$: Voronoitheorie

- $\mathcal{A} = \mathcal{D}^{n\times n}$ einfache $\mathbb{Q}$-Algebra
- $\mathcal{A} \hookrightarrow \mathcal{A}_{\mathbb{R}} := \mathcal{A} \otimes_{\mathbb{Q}} \mathbb{R}$ ist halbeinfache reelle Algebra, also isomorph zu direkter Summe von Matrixringen über $\mathbb{R}$, $\mathbb{C}$ und $\mathbb{H}$.
- Also trägt $\mathcal{A}_{\mathbb{R}}$ eine "kanonische" Involution $x \mapsto x^\dagger$
- $\Sigma := \mathrm{Sym}(\mathcal{A}_{\mathbb{R}}) := \left\{F \in \mathcal{A}_{\mathbb{R}} \mid F^\dagger = F\right\}$ symmetrische Elemente.
- $(-,-) : \Sigma \times \Sigma \to \mathbb{R}$, $(F_1, F_2) := \mathrm{trace}(F_1 F_2^\dagger)$.
- $(\Sigma, (-,-))$ Euklidischer Raum.
- Achtung: Im Allgemeinen ist $\mathcal{A}^\dagger \neq \mathcal{A}$.

Positive Formen

- Sei $V = \mathcal{D}^{1\times n}$ der einfache $\mathcal{A}$-Rechtsmodul, $V_{\mathbb{R}} = V \otimes_{\mathbb{Q}} \mathbb{R}$.
- $x \in V_{\mathbb{R}} \Rightarrow x^\dagger x \in \Sigma$.
- $F \in \Sigma$ heißt positiv falls $F[x] > 0$ für alle $0 \neq x \in V_{\mathbb{R}}$.

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

- $\mathcal{X}_\infty$ lebt auf $\Sigma^{>0} = \{F \in \Sigma \mid F \text{ positiv } \}$

Gitter und perfekte Formen

- Sei $\mathcal{O}$ eine $\mathbb{Z}_K$-Ordnung in $\mathcal{D}$ und L ein $\mathcal{O}$-Gitter in dem einfachen $\mathcal{A}$ Modul V.
- $\Lambda := \mathrm{End}_{\mathcal{O}}(L)$ ist eine $\mathbb{Z}_K$-Ordnung in $\mathcal{A}$ mit Einheitengruppe $\Lambda^* := \mathrm{GL}(L) = \{a \in \mathcal{A} \mid aL = L\}$.

Gitter und perfekte Formen

- Sei $\mathcal{O}$ eine $\mathbb{Z}_K$-Ordnung in $\mathcal{D}$ und L ein $\mathcal{O}$-Gitter in dem einfachen $\mathcal{A}$ Modul V.
- $\Lambda := \mathrm{End}_{\mathcal{O}}(L)$ ist eine $\mathbb{Z}_K$-Ordnung in $\mathcal{A}$ mit Einheitengruppe $\Lambda^* := \mathrm{GL}(L) = \{a \in \mathcal{A} \mid aL = L\}$.

L-minimale Vektoren

Sei $F \in \Sigma^{>0}$ (positive Form).

- $\mu(F) := \mu_L(F) = \min\{F[\ell] \mid 0 \neq \ell \in L\}$ heißt das L-Minimum von F
- $\mathcal{M}_L(F) := \{\ell \in L \mid F[\ell] = \mu_L(F)\}$ die Menge der L-minimalen Vektoren

Gitter und perfekte Formen

- Sei $\mathcal{O}$ eine $\mathbb{Z}_K$-Ordnung in $\mathcal{D}$ und L ein $\mathcal{O}$-Gitter in dem einfachen $\mathcal{A}$ Modul V.
- $\Lambda := \mathrm{End}_{\mathcal{O}}(L)$ ist eine $\mathbb{Z}_K$-Ordnung in $\mathcal{A}$ mit Einheitengruppe $\Lambda^* := \mathrm{GL}(L) = \{a \in \mathcal{A} \mid aL = L\}$.

L-minimale Vektoren

Sei $F \in \Sigma^{>0}$ (positive Form).

- $\mu(F) := \mu_L(F) = \min\{F[\ell] \mid 0 \neq \ell \in L\}$ heißt das L-Minimum von F
- $\mathcal{M}_L(F) := \{\ell \in L \mid F[\ell] = \mu_L(F)\}$ die Menge der L-minimalen Vektoren
- $\mathrm{Vor}_L(F) := \{\sum_{x \in \mathcal{M}_L(F)} a_x x^{\dagger} x \mid a_x \geq 0\} \subset \Sigma^{\geq 0}$ Voronoi Bereich
- F heißt L-perfekt $\Leftrightarrow \dim(\mathrm{Vor}_L(F)) = \dim(\Sigma)$.

Gitter und perfekte Formen

- Sei $\mathcal{O}$ eine $\mathbb{Z}_K$-Ordnung in $\mathcal{D}$ und L ein $\mathcal{O}$-Gitter in dem einfachen $\mathcal{A}$ Modul V.
- $\Lambda := \mathrm{End}_{\mathcal{O}}(L)$ ist eine $\mathbb{Z}_K$-Ordnung in $\mathcal{A}$ mit Einheitengruppe $\Lambda^* := \mathrm{GL}(L) = \{a \in \mathcal{A} \mid aL = L\}$.

L-minimale Vektoren

Sei $F \in \Sigma^{>0}$ (positive Form).

- $\mu(F) := \mu_L(F) = \min\{F[\ell] \mid 0 \neq \ell \in L\}$ heißt das L-Minimum von F
- $\mathcal{M}_L(F) := \{\ell \in L \mid F[\ell] = \mu_L(F)\}$ die Menge der L-minimalen Vektoren
- $\mathrm{Vor}_L(F) := \{\sum_{x \in \mathcal{M}_L(F)} a_x x^\dagger x \mid a_x \geq 0\} \subset \Sigma^{\geq 0}$ Voronoi Bereich
- F heißt L-perfekt $\Leftrightarrow \dim(\mathrm{Vor}_L(F)) = \dim(\Sigma)$.

Hauptsatz

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

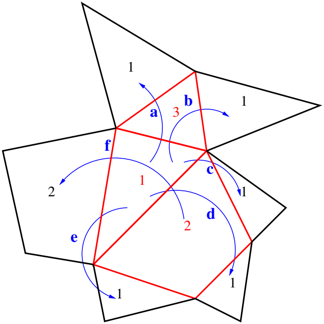
ist eine exakte lokal endliche polyedrische Pflasterung des Kegels $\Sigma^{\geq 0}$.
Λ^* operiert auf $\mathcal{T}$ mit endlich vielen Bahnen.

Erzeuger für Λ^*

- Vertretersystem $\mathfrak{R} := \{F_1, \ldots, F_s\}$ der Λ^*-Bahnen L-perfekter Formen.
- Für alle Nachbarn F der F_i (codim($\mathrm{Vor}(F) \cap \mathrm{Vor}(F_i)$)$= 1$) berechne $g_F \in \Lambda^*$ mit $g_F \cdot F \in \mathfrak{R}$.
- Dann $\Lambda^* = \langle \mathrm{Aut}(F_i), g_F \mid F_i \in \mathfrak{R}, F$ Nachbar eines $F_j \in \mathfrak{R} \rangle$.

Erzeuger für Λ^*

- Vertretersystem $\mathfrak{R} := \{F_1, \ldots, F_s\}$ der Λ^*-Bahnen L-perfekter Formen.
- Für alle Nachbarn F der F_i ($\mathrm{codim}(\mathrm{Vor}(F) \cap \mathrm{Vor}(F_i)) = 1$) berechne $g_F \in \Lambda^*$ mit $g_F \cdot F \in \mathfrak{R}$.
- Dann $\Lambda^* = \langle \mathrm{Aut}(F_i), g_F \mid F_i \in \mathfrak{R}, F$ Nachbar eines $F_j \in \mathfrak{R} \rangle$.



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

Ein Beispiel $\mathcal{Q}_{2,3}$.

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

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

Ein Beispiel $\mathcal{Q}_{2,3}$.

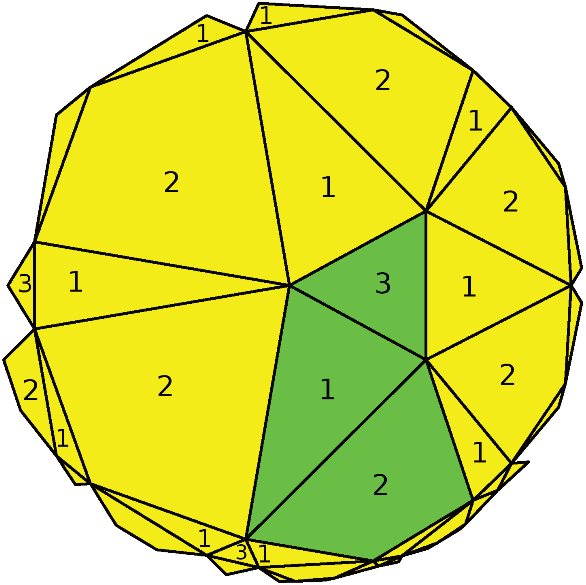
- $\mathcal{A} = \mathcal{D} = \mathcal{Q}_{2,3} = \left(\frac{2,3}{\mathbb{Q}}\right) = \langle i, j \mid i^2 = 2, j^2 = 3, ij = -ji \rangle_{\mathbb{Q}}$
- Maximalordnung $\Lambda = \langle 1, i, \frac{1}{2}(1+i+ij), \frac{1}{2}(j+ij)\rangle_{\mathbb{Z}}$
- $V = \mathcal{A}$, $L = \Lambda$, $\Lambda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

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

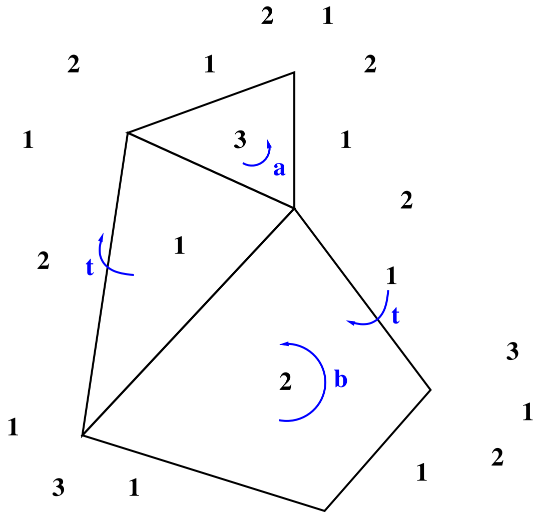
Drei perfekte Formen:

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

Die Pflasterung für $\mathcal{Q}_{2,3} \hookrightarrow \mathbb{Q}[\sqrt{2}]^{2\times 2}$.



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

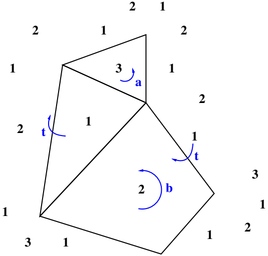


$\Lambda^* = \langle a, b, t \mid a^3 = b^2 = atbt = -1 \rangle$, $\mathcal{A} \cong \mathcal{Q}_{2,3}$

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

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

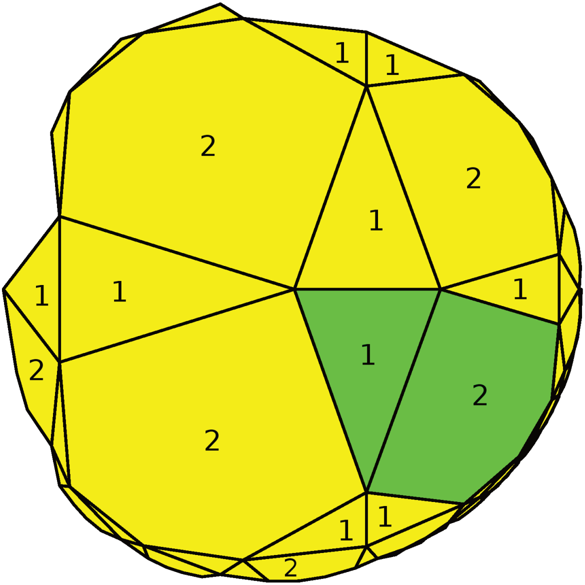
$$t = \frac{1}{2}\begin{pmatrix} 2\sqrt{2}+1 & \sqrt{2}+1 \\ 3-3\sqrt{2} & 1-2\sqrt{2} \end{pmatrix}$$



Es gilt

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

Die Pflasterung für $\mathcal{Q}_{2,3} \hookrightarrow \mathbb{Q}[\sqrt{3}]^{2\times 2}$.



Eine rationale Divisionsalgebra von Index 3

- $\vartheta = \zeta_9 + \zeta_9^{-1}$, $\langle\sigma\rangle = \mathrm{Gal}(\mathbb{Q}(\vartheta)/\mathbb{Q})$,
- $\mathcal{A}$ die $\mathbb{Q}$-Algebra erzeugt von
- $Z := \begin{pmatrix} \vartheta & & \\ & \sigma(\vartheta) & \\ & & \sigma^2(\vartheta) \end{pmatrix}$ und $\Pi := \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 2 & 0 & 0 \end{pmatrix}$.
- $\mathcal{A}$ Divisionsalgebra mit Hasse-Invarianten $\frac{1}{3}$ bei 2 und $\frac{2}{3}$ bei 3.
- Λ Maximalordnung in $\mathcal{A}$
- $\Gamma := \Lambda^\times$ hat 431 Bahnen von perfekten Formen und Präsentation
- $$\begin{aligned}\Gamma \cong \langle a, b \mid \quad & b^2a^2(b^{-1}a^{-1})^2,\ b^{-2}(a^{-1}b^{-1})^2ab^{-2}a^2b^{-3}, \\ & ab^2a^{-1}b^3a^{-2}bab^3,\ a^2bab^{-2}ab^{-1}(a^{-2}b)^2, \\ & a^{-1}b^2a^{-1}b^{-1}a^{-5}b^{-2}a^{-3}, \\ & b^{-2}a^{-2}b^{-1}a^{-1}b^{-1}a^{-2}b^{-1}a^{-1}b^{-2}(a^{-1}b^{-1})^3\rangle\end{aligned}$$
- $a = \frac{1}{3}((1-3Z-Z^2)+(2+Z^2)\Pi+(1-Z^2)\Pi^2)$,
  $b = \frac{1}{3}((-3-2Z+Z^2)+(1-2Z)\Pi+(1-Z^2)\Pi^2)$.

Quaternionenalgebren über CM Körpern

K CM-Körper und $\mathcal{A} = \mathcal{Q} \otimes K$ mit $\mathcal{Q}$ definite rationale Quaternionenalgebra.

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

ist eine positive Involution auf $\mathcal{A}$.

$K = \mathbb{Q}\sqrt{-7}]$, Jespers, Corrales (2004)

- $\mathcal{A} = \left(\frac{-1,-1}{\mathbb{Q}[\sqrt{-7}]}\right) = \langle 1, i, j, k \rangle_{\mathbb{Q}[\sqrt{-7}]}$, Λ Maximalordnung
- nur eine Bahn perfekter Formen
- $\Lambda^\times = \langle a, b \mid b^3 = -1, (b^{-1}a^{-1}ba)^2 = -1, (b^2a^{-2})^3 = -1 \rangle$
- $a := \frac{1}{4}((1 + \sqrt{-7}) - (1 + \sqrt{-7})i + (1 + \sqrt{-7})j + (3 - \sqrt{-7})k)$,
- $b := \frac{1}{2}(1 + i - 3j + \sqrt{-7}k)$

Quaternionenalgebren über imaginär quadratischen Körpern

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

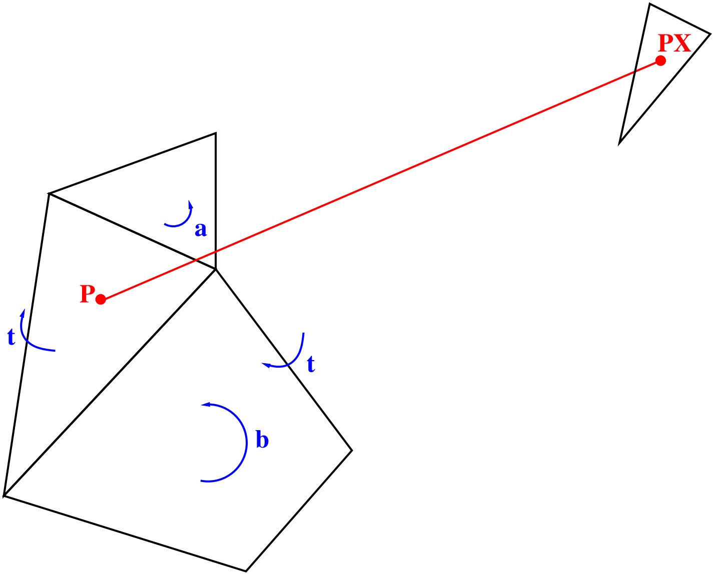
d	perfekte Formen	Laufzeit Voronoï	Laufzeit Präsentation	Anzahl Erzeuger
7	1	$1.24s$	$0.42s$	2
31	8	$6.16s$	$0.50s$	3
55	21	$14.69s$	$1.01s$	5
79	40	$28.74s$	$1.78s$	5
95	69	$53.78s$	$2.57s$	7
103	53	$38.39s$	$2.52s$	6
111	83	$66.16s$	$3.02s$	6
255	302	$323.93s$	$17.54s$	16

Quaternionenalgebren über $\mathbb{Q}(\sqrt{-7})$

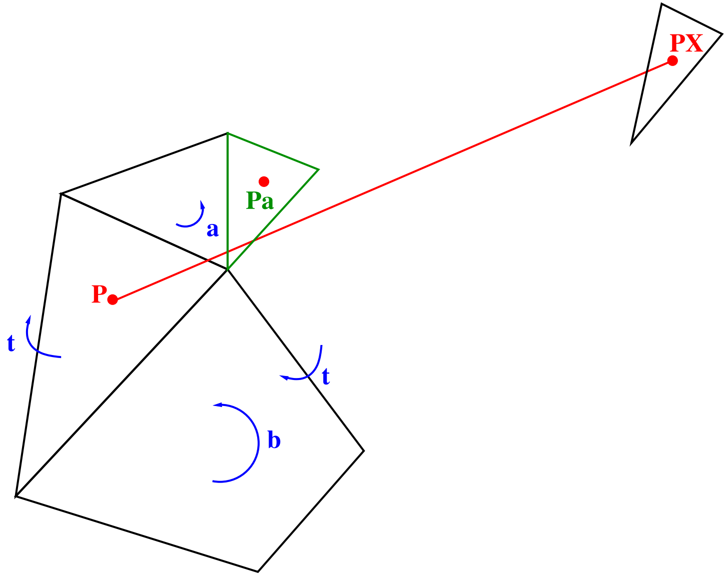
$$\mathcal{A} = \left(\frac{a, b}{\mathbb{Q}(\sqrt{-7})}\right)$$

a,b	perfekte Formen	Laufzeit Voronoï	Laufzeit Präsentation	Anzahl Erzeuger
$-1, -1$	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

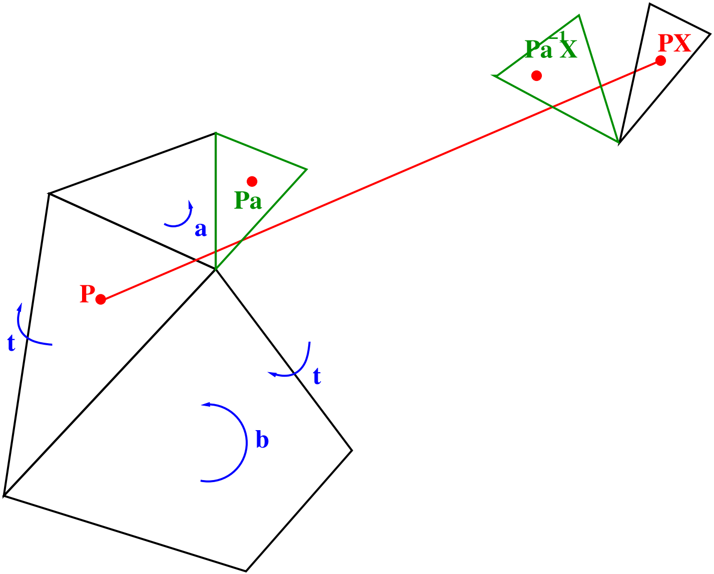
Das Wortproblem



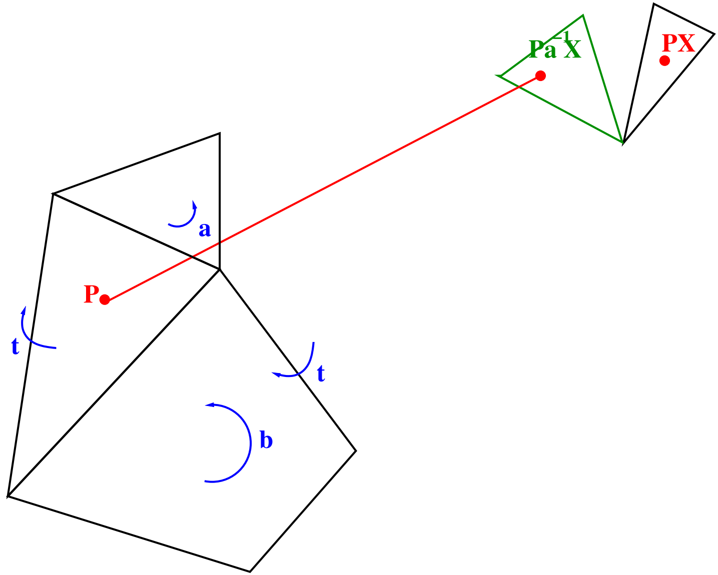
Das Wortproblem



Das Wortproblem



Das Wortproblem



Teil II: $S_f \neq \emptyset$, Gebäude

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

Borel, Serre: Λ_S^* ist endlich präsentiert.

Treue Operation auf lokal endlichem polyedrischen Komplex
$\mathcal{X} = \mathcal{X}_\infty \times \mathcal{X}_{\wp_1} \times \ldots \times \mathcal{X}_{\wp_s}$
$\mathcal{X}_\infty$ = Voronoikomplex L-perfekter Formen in $\Sigma^{>0}$.
$\mathcal{X}_{\wp_i}$ = Bruhat-Tits Gebäude der $\wp_i$-adischen Gruppe $\mathrm{SL}(\mathcal{A}_{\wp_i})$.

Teil II: $S_f \neq \emptyset$, Gebäude

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

Borel, Serre: Λ_S^* ist endlich präsentiert.

Treue Operation auf lokal endlichem polyedrischen Komplex
$\mathcal{X} = \mathcal{X}_\infty \times \mathcal{X}_{\wp_1} \times \ldots \times \mathcal{X}_{\wp_s}$
$\mathcal{X}_\infty =$ Voronoikomplex L-perfekter Formen in $\Sigma^{>0}$.
$\mathcal{X}_{\wp_i} =$ Bruhat-Tits Gebäude der $\wp_i$-adischen Gruppe $\mathrm{SL}(\mathcal{A}_{\wp_i})$.

Vereinfachende Annahme

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

Das Gebäude von $\mathrm{SL}_m(\mathbb{Q}_p)$

- $V_p = \mathbb{Q}_p^m$ einfacher $\mathcal{A}_p$-Modul.
- L ein $\mathbb{Z}_p$-Gitter in V_p,
- $[L] := \{p^i L \mid i \in \mathbb{Z}\}$ Homothetieklasse von L.
- $\mathcal{X}_p$: $m-1$-dimensionaler simplizialer Komplex mit
- Eckenmenge (0-Simplizes) $\mathcal{K} := \{[L] \mid L \text{ Gitter in } V_p\}$
- $([L_1], \ldots, [L_k]) \in \mathcal{K}^k$ bilden einen $k-1$ Simplex, genau dann wenn nach Umordnung Gitter $M_i \in [L_i]$ existieren mit

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

Das Gebäude von $\mathrm{SL}_m(\mathbb{Q}_p)$

- $V_p = \mathbb{Q}_p^m$ einfacher $\mathcal{A}_p$-Modul.
- L ein $\mathbb{Z}_p$-Gitter in V_p,
- $[L] := \{p^i L \mid i \in \mathbb{Z}\}$ Homothetieklasse von L.
- $\mathcal{X}_p$: $m-1$-dimensionaler simplizialer Komplex mit
- Eckenmenge (0-Simplizes) $\mathcal{K} := \{[L] \mid L \text{ Gitter in } V_p\}$
- $([L_1], \ldots, [L_k]) \in \mathcal{K}^k$ bilden einen $k-1$ Simplex, genau dann wenn nach Umordnung Gitter $M_i \in [L_i]$ existieren mit

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

Die Nachbarn von $[L]$ in $\mathcal{X}_p$ stehen in Bijektion zu den nicht-trivialen Teilräumen von $L/pL \cong \mathbb{F}_p^m$.

Das Gebäude von $\mathrm{SL}_m(\mathbb{Q}_p)$

- $V_p = \mathbb{Q}_p^m$ einfacher $\mathcal{A}_p$-Modul.
- L ein $\mathbb{Z}_p$-Gitter in V_p,
- $[L] := \{p^i L \mid i \in \mathbb{Z}\}$ Homothetieklasse von L.
- $\mathcal{X}_p$: $m-1$-dimensionaler simplizialer Komplex mit
- Eckenmenge (0-Simplizes) $\mathcal{K} := \{[L] \mid L \text{ Gitter in } V_p\}$
- $([L_1], \ldots, [L_k]) \in \mathcal{K}^k$ bilden einen $k-1$ Simplex, genau dann wenn nach Umordnung Gitter $M_i \in [L_i]$ existieren mit

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

Die Nachbarn von $[L]$ in $\mathcal{X}_p$ stehen in Bijektion zu den nicht-trivialen Teilräumen von $L/pL \cong \mathbb{F}_p^m$.

- Wähle Basis so dass $L_0 = \mathbb{Z}_p^m$ invariant unter Λ
- Ist $B \in \mathrm{GL}_m(\mathbb{Q}_p)$ mit $BL_0 = L$, so heißt $\nu_p(\det(B)) \in \mathbb{Z}/m\mathbb{Z}$ der Typ von $[L]$.
- $\mathrm{SL}_m(\mathbb{Q}_p)$ operiert auf $\mathcal{K}$ mit dem Typ als trennender Invariante.

Präsentation der S-Einheitengruppe

Hauptsatz

- $\Lambda_S^* = \Lambda[\frac{1}{p}]$ operiert simplizial auf $\mathcal{X}_p$ mit endlich vielen Bahnen.
- $\mathbb{Z}_{K,S}^* = \mathbb{Z}[\frac{1}{p}]^* = \{1, -1\} \times \{p^i \mid i \in \mathbb{Z}\} = Z(\Lambda_S^*)$ operiert trivial.
- $\mathrm{Stab}_{\Lambda_S^*}(L_0) = \Lambda^*$.
- $\mathrm{Stab}_{\Lambda_S^*}([L_0]) = \Lambda^* \times \{p^i \mid i \in \mathbb{Z}\}$.

Präsentation der S-Einheitengruppe

Hauptsatz

- $\Lambda_S^* = \Lambda[\frac{1}{p}]$ operiert simplizial auf $\mathcal{X}_p$ mit endlich vielen Bahnen.
- $\mathbb{Z}_{K,S}^* = \mathbb{Z}[\frac{1}{p}]^* = \{1, -1\} \times \{p^i \mid i \in \mathbb{Z}\} = Z(\Lambda_S^*)$ operiert trivial.
- $\mathrm{Stab}_{\Lambda_S^*}(L_0) = \Lambda^*$.
- $\mathrm{Stab}_{\Lambda_S^*}([L_0]) = \Lambda^* \times \{p^i \mid i \in \mathbb{Z}\}$.

Präsentation

- Vertretersystem $\mathcal{R} := \{[L_1], \dots, [L_s]\}$ der Λ_S^*-Bahnen auf $\mathcal{K}$
- Für alle Nachbarn $[L]$ der $[L_i]$ berechne $g_L \in \Lambda_S^*$ mit $g_L \cdot [L] \in \mathcal{R}$.
- Dann

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

- Präsentation, da wir in den Punktstabilisatoren Λ^* das Wortproblem lösen können.

Ein Beispiel

$\mathcal{A} = \mathcal{D} = \mathcal{Q}_{2,3}$ und Λ wie eben die bis auf Konjugation einzige Maximalordnung in $\mathcal{D}$.

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

Λ ist Rechts-Hauptidealbereich

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

wobei $C_p \in \Lambda$ ein Element der Norm p.

Ein Beispiel

$\mathcal{A} = \mathcal{D} = \mathcal{Q}_{2,3}$ und Λ wie eben die bis auf Konjugation einzige Maximalordnung in $\mathcal{D}$.

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

Λ ist Rechts-Hauptidealbereich

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

wobei $C_p \in \Lambda$ ein Element der Norm p.

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

Ein Beispiel

$\mathcal{A} = \mathcal{D} = \mathcal{Q}_{2,3}$ und Λ wie eben die bis auf Konjugation einzige Maximalordnung in $\mathcal{D}$.

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

Λ ist Rechts-Hauptidealbereich

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

wobei $C_p \in \Lambda$ ein Element der Norm p.

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

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

Berechne Präsentation von Λ_S^*

Teil I für $S_f = \emptyset$, Braun, Coulangeon, N., Schönnenbeck (2015)

- Operation von $\mathcal{A}^*$ auf $\mathcal{X}_\infty$.
- Voronoi-Algorithmus, perfekte Formen, Isometrien von Gittern
- Berechnet Präsentation von Λ^*.
- Löst Wortproblem in gegebenen Erzeugern.
- Läuft gut für kleine Beispiele, $\dim_{\mathbb{Q}}(\mathcal{A}) \leq 9$.
- Für Quaternionenalgebren besser als Magma (5 Min. versus 1 Tag)
- Erster verfügbarer Algorithmus für Divisionsalgebren vom Index 3.

Teil II für $S_f = \{\wp_1, \ldots, \wp_s\}$, Coulangeon, N. (in Vorbereitung)

- Operation von $\mathcal{A}^*$ auf $\mathcal{X}_{\wp_1} \times \ldots \times \mathcal{X}_{\wp_s}$.
- Punktstabilisatoren Λ^* für geeignete Ordnungen Λ.
- Zusätzliche Erzeuger: Elemente mit Norm $\prod_{i=1}^{s} \wp_i^{a_i}$ in Λ.