Units in semisimple algebras over $\mathbf{Q}$ and Voronoï algorithm

Renaud Coulangeon, Université Bordeaux

based on a joint work with Gabriele Nebe, RWTH Aachen

Patagonia, December 2013

Introduction

Let

$$\begin{array}{ccl} A & = & M_n(D) \text{ a finitely generated simple algebra over } \mathbb{Q} \\ \cup & & (\ D = \text{ skew field, with center } K\ ) \\ \Lambda & & \text{ a maximal order} \end{array}$$

Introduction

Let

$$\begin{array}{lcl} A & = & M_n(D) \text{ a finitely generated simple algebra over } \mathbb{Q} \\ \cup & & (\ D = \text{ skew field, with center } K\ ) \\ \Lambda & & \text{ a maximal order} \end{array}$$

Let $\Lambda^\times$ be the group of units in Λ.

Introduction

Let

$$\begin{array}{lcl} A & = & M_n(D) \text{ a finitely generated simple algebra over } \mathbb{Q} \\ \cup & & (D = \text{ skew field, with center } K) \\ \Lambda & & \text{ a maximal order} \end{array}$$

Let $\Lambda^\times$ be the group of units in Λ.

Questions :

Introduction

Let

$$\begin{array}{lcl} A & = & M_n(D) \text{ a finitely generated simple algebra over } \mathbb{Q} \\ \cup & & (\ D = \text{ skew field, with center } K\ ) \\ \Lambda & & \text{ a maximal order} \end{array}$$

Let $\Lambda^\times$ be the group of units in Λ.

Questions :

- structure ?

Introduction

Let

$$\begin{array}{lcl} A & = & M_n(D) \text{ a finitely generated simple algebra over } \mathbb{Q} \\ \cup & & (\ D = \text{ skew field, with center } K\ ) \\ \Lambda & & \text{ a maximal order} \end{array}$$

Let $\Lambda^\times$ be the group of units in Λ.

Questions :

- structure ?
- computation ?

Introduction

Let

$$\begin{array}{lcl} A & = & M_n(D) \text{ a finitely generated simple algebra over } \mathbb{Q} \\ \cup & & (\ D = \text{ skew field, with center } K\ ) \\ \Lambda & & \text{a maximal order} \end{array}$$

Let $\Lambda^\times$ be the group of units in Λ.

Questions :

- structure ?
- computation ?
- $\Lambda_1^\times \simeq \Lambda_2^\times$?

Introduction

Let

$$\begin{array}{rcl} A & = & M_n(D) \text{ a finitely generated simple algebra over } \mathbb{Q} \\ \cup & & (\ D = \text{ skew field, with center } K\ ) \\ \Lambda & & \text{ a maximal order} \end{array}$$

Let $\Lambda^\times$ be the group of units in Λ.

Questions :

- structure ?
- computation ?
- $\Lambda_1^\times \simeq \Lambda_2^\times$?
- maximal finite subgroups ?

General method : let $\Gamma = \Lambda^{\times}$ act on a connected graph X.

General method : let $\Gamma = \Lambda^{\times}$ act on a connected graph X.

"*A good knowledge of the quotient graph* $\Gamma \backslash X$ *yields virtually all the information on* Γ."

General method : let $\Gamma = \Lambda^\times$ act on a connected graph X.

"*A good knowledge of the quotient graph* $\Gamma\backslash X$ *yields virtually all the information on* Γ."

Explicitely, one can use the following fundamental exact sequence from Bass-Serre theory to get a *presentation* of Γ (*i.e.* generators and relations)

$$1 \longrightarrow \pi_1(X) \longrightarrow \pi_1(\Gamma\backslash\backslash X) \longrightarrow \Gamma \longrightarrow 1$$

(this idea dates back to Opgenorth 2001)

General method : let $\Gamma = \Lambda^{\times}$ act on a connected graph X.

"*A good knowledge of the quotient graph* $\Gamma \backslash X$ *yields virtually all the information on* Γ."

Explicitely, one can use the following fundamental exact sequence from Bass-Serre theory to get a *presentation* of Γ (*i.e.* generators and relations)

$$1 \longrightarrow \pi_1(X) \longrightarrow \pi_1(\Gamma \backslash\backslash X) \longrightarrow \Gamma \longrightarrow 1$$

(this idea dates back to Opgenorth 2001)
Question : how can one get such a graph X ?

General method : let $\Gamma = \Lambda^\times$ act on a connected graph X.

"*A good knowledge of the quotient graph* $\Gamma \backslash X$ *yields virtually all the information on* Γ."

Explicitely, one can use the following fundamental exact sequence from Bass-Serre theory to get a *presentation* of Γ (*i.e.* generators and relations)

$$1 \longrightarrow \pi_1(X) \longrightarrow \pi_1(\Gamma \backslash\backslash X) \longrightarrow \Gamma \longrightarrow 1$$

(this idea dates back to Opgenorth 2001)
Question : how can one get such a graph X ?
Answer : Voronoi theory, graph of perfect "forms".

Lattices

$A = M_n(D)$, $\mathcal{O}$ a **fixed** maximal order in D.

Lattices

$A = M_n(D)$, $\mathcal{O}$ a **fixed** maximal order in D.

$\Lambda \subset A$ maximal order $\Leftrightarrow \exists$ an $\mathcal{O}$-lattice $L \subset D^n$ such that

$$\Lambda = \mathrm{End}(L) = \{M \in M_n(D) \mid ML \subset L\}$$

Lattices

$A = M_n(D)$, $\mathcal{O}$ a **fixed** maximal order in D.

$\Lambda \subset A$ maximal order $\Leftrightarrow \exists$ an $\mathcal{O}$-lattice $L \subset D^n$ such that

$$\Lambda = \mathrm{End}(L) = \{M \in M_n(D) \mid ML \subset L\}$$

$\Longrightarrow \Lambda^\times = \mathrm{GL}(L) = \{a \in M_n(D) \mid aL = L\}$.

Lattices

$A = M_n(D)$, $\mathcal{O}$ a **fixed** maximal order in D.

$\Lambda \subset A$ maximal order $\Leftrightarrow \exists$ an $\mathcal{O}$-lattice $L \subset D^n$ such that
$$\Lambda = \mathrm{End}(L) = \{M \in M_n(D) \mid ML \subset L\}$$

$\Longrightarrow \Lambda^\times = \mathrm{GL}(L) = \{a \in M_n(D) \mid aL = L\}$.

Classification of $\mathcal{O}$-lattices (*Steinitz class*) $\Longrightarrow \Lambda$ conjugated in $\mathrm{GL}_n(D)$ to

$$\Lambda(\mathfrak{a}) := \begin{pmatrix} \mathcal{O} & \dots & \mathcal{O} & \mathfrak{a}^{-1} \\ \vdots & \dots & \vdots & \vdots \\ \mathcal{O} & \dots & \mathcal{O} & \mathfrak{a}^{-1} \\ \mathfrak{a} & \dots & \mathfrak{a} & \mathcal{O}' \end{pmatrix}$$

where $\mathcal{O}' = O_l(\mathfrak{a}) = \{x \in K \mid x\mathfrak{a} \subseteq \mathfrak{a}\}$.

Forms

$$A = M_n(D) \quad \rightsquigarrow \quad A_{\mathbb{R}} := A \otimes_{\mathbb{Q}} \mathbb{R} = M_n(D_{\mathbb{R}})$$

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

where $K = Z(D)$, d is the degree of D (so that $d^2 = \dim_K D$),

$\iota_1, \ldots, \iota_s$	are the real places of $K := Z(D)$ that ramify in D,
$\sigma_1, \ldots, \sigma_r$	the real places of K that do not ramify in D
$\tau_1, \ldots, \tau_t$	the complex places of K.

Forms

$$A = M_n(D) \qquad \rightsquigarrow \qquad A_{\mathbb{R}} := A \otimes_{\mathbb{Q}} \mathbb{R} = M_n(D_{\mathbb{R}})$$

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

where $K = Z(D)$, d is the degree of D (so that $d^2 = \dim_K D$),

$\iota_1, \ldots, \iota_s$	are the real places of $K := Z(D)$ that ramify in D,
$\sigma_1, \ldots, \sigma_r$	the real places of K that do not ramify in D
$\tau_1, \ldots, \tau_t$	the complex places of K.

$\rightsquigarrow$ a well-defined involution * on $D_{\mathbb{R}}$ ("*transconjugation*"), which induces an involution † on $A_{\mathbb{R}}$ (* on the entries + transposition of the matrix)

Remark : in general $A \subset A_{\mathbb{R}}$ is not sable under †.

Forms

$$A = M_n(D) \qquad \rightsquigarrow \qquad A_{\mathbb{R}} := A \otimes_{\mathbb{Q}} \mathbb{R} = M_n(D_{\mathbb{R}})$$

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

where $K = Z(D)$, d is the degree of D (so that $d^2 = \dim_K D$),

$\iota_1, \ldots, \iota_s$	are the real places of $K := Z(D)$ that ramify in D,
$\sigma_1, \ldots, \sigma_r$	the real places of K that do not ramify in D
$\tau_1, \ldots, \tau_t$	the complex places of K.

$\rightsquigarrow$ a well-defined involution * on $D_{\mathbb{R}}$ ("*transconjugation*"), which induces an involution † on $A_{\mathbb{R}}$ (* on the entries + transposition of the matrix)

Remark : in general $A \subset A_{\mathbb{R}}$ is not sable under †.

Forms (2)

$$S_n(D_{\mathbb{R}}) = \left\{F \in A_{\mathbb{R}} \mid F^{\dagger} = F\right\} \quad \supset \quad P_n(D_{\mathbb{R}}) = S_n(D_{\mathbb{R}})_{>0}$$

To $F \in S_n(D_{\mathbb{R}})$ one can associate a quadratic form on the real vector space $D_{\mathbb{R}}^n$, defined as

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

which is positive definite if $F \in P_n(D_{\mathbb{R}})$.

Forms (2)

$$S_n(D_{\mathbb{R}}) = \left\{F \in A_{\mathbb{R}} \mid F^\dagger = F\right\} \quad \supset \quad P_n(D_{\mathbb{R}}) = S_n(D_{\mathbb{R}})_{>0}$$

To $F \in S_n(D_{\mathbb{R}})$ one can associate a quadratic form on the real vector space $D_{\mathbb{R}}^n$, defined as

$$F[x] := \text{trace}(Fxx^\dagger),$$

which is positive definite if $F \in P_n(D_{\mathbb{R}})$.

Definition

Let $L \subset D^n$ an $\mathcal{O}$-lattice, and $F \in P_n(D_{\mathbb{R}})$

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

Forms (2)

$$S_n(D_{\mathbb{R}}) = \left\{F \in A_{\mathbb{R}} \mid F^{\dagger} = F\right\} \quad \supset \quad P_n(D_{\mathbb{R}}) = S_n(D_{\mathbb{R}})_{>0}$$

To $F \in S_n(D_{\mathbb{R}})$ one can associate a quadratic form on the real vector space $D_{\mathbb{R}}^n$, defined as

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

which is positive definite if $F \in P_n(D_{\mathbb{R}})$.

Definition

Let $L \subset D^n$ an $\mathcal{O}$-lattice, and $F \in P_n(D_{\mathbb{R}})$

- $\min_L(F) = \min_{0 \neq \ell \in L} F[\ell]$,
- $S_L(F) = \{\ell \in L \mid F[\ell] = \min_L(F)\}$.

Forms (2)

$$S_n(D_{\mathbb{R}}) = \left\{F \in A_{\mathbb{R}} \mid F^{\dagger} = F\right\} \quad \supset \quad P_n(D_{\mathbb{R}}) = S_n(D_{\mathbb{R}})_{>0}$$

To $F \in S_n(D_{\mathbb{R}})$ one can associate a quadratic form on the real vector space $D_{\mathbb{R}}^n$, defined as

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

which is positive definite if $F \in P_n(D_{\mathbb{R}})$.

Definition

Let $L \subset D^n$ an $\mathcal{O}$-lattice, and $F \in P_n(D_{\mathbb{R}})$

- $\min_L(F) = \min_{0 \neq \ell \in L} F[\ell]$,
- $S_L(F) = \{\ell \in L \mid F[\ell] = \min_L(F)\}$.
- (*minimal classes*) $\mathrm{Cl}_L(F) := \{H \in P_n(D_{\mathbb{R}}) \mid S_L(H) = S_L(F)\}$.

A cell complex

The minimal classes w.r.t. a given lattices L form a cell complex ("Voronoi complex") on which $\Lambda^\times = \mathrm{GL}(L)$ acts

- $g \cdot F := g^\dagger F g$
  $\mathrm{Aut}_L(F) = \{g \in \mathrm{GL}(L) \mid g \cdot F = F\}$ finite group.
- $g \cdot \mathrm{Cl}_L(F) := \mathrm{Cl}_L(g \cdot F)$
  $\mathrm{Aut}_L(\mathrm{Cl}_L(F)) = \{g \in \mathrm{GL}(L) \mid g \cdot \mathrm{Cl}_L(F) = \mathrm{Cl}_L(F)\} \supset \mathrm{Aut}_L(F)$.

Definition

A form F is L**-perfect** if $\mathrm{Cl}_L(F) = \mathbb{R}_{>0} F$.

Voronoi theory $\Rightarrow$ this complex is finite $\mod \Lambda^\times$ and can be computed explicitely (Voronoi algorithm, neighbouring process).

Maximal finite subbgroups

Let G be a finite subgroup of $\Lambda^\times = \mathrm{GL}(L)$. Set

$$\mathcal{F}(G) = \{F \in S_n(\mathbb{D}_\mathbb{R}) \mid g \cdot F = F\}.$$

A form F is G-perfect w.r.t. L if $\mathrm{Cl}_L(F) \cap \mathcal{F}(G) = \mathbb{R}_{>0}F$.

Theorem

1. *Let G be a maximal finite subgroup of $\mathrm{GL}(L)$. Then, there exists a* ***well-rounded*** *(=compact) minimal class $\mathcal{C}$ such that $\mathcal{C} \cap \mathcal{F}(G) = \mathbb{R}_{>0}F$ for some form F, and $G = \mathrm{Aut}_L(\mathcal{C})$.*
2. *If G is a finite subgroup of $\mathrm{GL}(L)$, then the maximal finite subgroups of $\mathrm{GL}(L)$ containing it are of the form $H = \mathrm{Aut}_L(\mathcal{C}_G)$ where $\mathcal{C}_G$ is a G-minimal class.*

Example

Table: Well rounded minimal classes for $K = \mathbb{Q}[\sqrt{-15}]$

$L_0 = \mathcal{O}_K \oplus \mathcal{O}_K$				
C	$G = \mathrm{Aut}_L(C)$	$\dim(\pi_G(C))$	$\mathrm{Aut}_L(F)$	maximal
perf. corank = 0				
P_1	C_6	1	C_6	no
P_2	C_4	1	C_4	no
perf. corank = 1				
C_1	D_{12}	1	D_{12}	yes
C_2	D_{12}	1	D_{12}	yes
C_3	C_2	2		no
C_4	C_2	2		no
perf. corank = 2				
D_1	D_8	1	D_8	yes
D_2	D_8	1	D_8	yes
D_3	V_4	1	V_4	yes
D_4	V_4	1	V_4	yes

Example (continued)

Table: Well rounded minimal classes for $K = \mathbb{Q}[\sqrt{-15}]$

$L_1 = \mathcal{O}_K \oplus \mathfrak{p}_2$				
C	$G = \mathrm{Aut}_L(C)$	$\dim(\pi_G(C))$	$\mathrm{Aut}_L(F)$	maximal
perf. corank = 0				
P	$C_3 : C_4$	1	$C_3 : C_4$	yes
perf. corank = 1				
C_1	D_8	1	D_8	yes
C_2	D_8	1	D_8	yes
C_3	D_{12}	1	D_{12}	yes
perf. corank = 2				
D	V_4	1	V_4	yes

Example (continued)

Table: Well rounded minimal classes for $K = \mathbb{Q}[\sqrt{-15}]$

$L_1 = \mathcal{O}_K \oplus \mathfrak{p}_2$				
C	$G = \mathrm{Aut}_L(C)$	$\dim(\pi_G(C))$	$\mathrm{Aut}_L(F)$	maximal
perf. corank = 0				
P	$C_3 : C_4$	1	$C_3 : C_4$	yes
perf. corank = 1				
C_1	D_8	1	D_8	yes
C_2	D_8	1	D_8	yes
C_3	D_{12}	1	D_{12}	yes
perf. corank = 2				
D	V_4	1	V_4	yes

Corollary

$\mathrm{GL}_2(O_K) = \mathrm{GL}(L_0)$ *and* $\mathrm{GL}(L_1)$ *are not isomorphic.*

Number of conjugacy classes of maximal finite subgroups

	D_8	D_{12}	V_4	$SL_2(3)$	Q_8	$C_3 : C_4$
$K = \mathbb{Q}[\sqrt{-15}]$						
$St(L) = [O_K]$	2	2	2	-	-	-
$St(L) = [\wp_2]$	2	1	1	-	-	1
$K = \mathbb{Q}[\sqrt{-5}]$						
$St(L) = [O_K]$	3	2	1	-	1	-
$St(L) = [\wp_2]$	1	2	1	1	-	-
$K = \mathbb{Q}[\sqrt{-6}]$						
$St(L) = [O_K]$	3	2	1	1	-	-
$St(L) = [\wp_2]$	1	1	2	-	1	1
$K = \mathbb{Q}[\sqrt{-10}]$						
$St(L) = [O_K]$	3	2	1	-	1	-
$St(L) = [\wp_2]$	1	-	3	1	-	2
$K = \mathbb{Q}[\sqrt{-21}]$						
$St(L) = [O_K]$	6	4	2	-	-	2
$St(L) = [\wp_2]$	2	-	6	-	-	-
$St(L) = [\wp_3]$	-	2	6	2	-	-
$St(L) = [\wp_5]$	-	-	8	-	2	-