Twisted forms of linear algebraic groups: Relative root subgroups

Sergei Haller

Sergei.Haller@math.uni-giessen.de

Magma Workshop on Group Theory and Algebraic Geometry

University of Warwick, Coventry, UK

August 22–26, 2005

The Project

- Main goal: algorithms for computation in linear algebraic groups
- Joint with Arjeh M. Cohen, Scott H. Murray and Don E. Taylor
- Implementation in Magma

Preliminary remarks

- Classification of finite simple groups
  - Chevallley groups (“untwisted”)
  - Twisted Chevallley groups (unitary, Ree, Suzuki, . . .)

Preliminary remarks

- Classification of finite simple groups
  - Chevallley groups (“untwisted”)
  - Twisted Chevallley groups (unitary, Ree, Suzuki, . . .)

- Computation in “untwisted” groups possible for arbitrary fields
  - Steinberg presentation
  - Unique decomposition of elements

Preliminary remarks

- Classification of finite simple groups
  - Chevallley groups (“untwisted”)
  - Twisted Chevallley groups (unitary, Ree, Suzuki, . . .)
- Computation in “untwisted” groups possible for arbitrary fields
  - Steinberg presentation
  - Unique decomposition of elements
- Computation in “twisted” groups is not possible
- More twisted groups for arbitrary fields

Linear Algebraic Groups

- F is an algebraically closed field

- Linear algebraic groups are
  - subgroups of GL_n for some n
  - defined by polynomial equations (over F)

- Examples:

$$\mathrm{GL}_n = \{ \ (A, t) \in F^{n \times n+1} \mid \det(A)t = 1 \ \}$$

$$\mathrm{SL}_n = \{ \ A \in F^{n \times n} \mid \det(A) = 1 \ \}$$

$$\mathrm{SU}_n = (\mathrm{SL}_n)_{\boldsymbol{\alpha}}$$

Field of Definition

- F is an algebraically closed field
- G is a linear algebraic group

- G is <u>defined over</u> the subfield $k \subseteq F$ if
  the polynomials involved in the definition of G are over k

- Examples:
  GL_n and SL_n are defined over the prime field of F

Groups of Lie type

- For a Galois extension $k \subseteq K \subseteq k_{sep}$ and $\Gamma = \mathrm{Gal}(k_{sep} : K)$

$$G(K) = \{\, g \in G \mid g^\gamma = g \quad \forall \gamma \in \Gamma \,\}$$

(here Γ acts componentwise on the entries)

Cocycles

- A is a group,
  Γ is a group acting on A (on the right)

Cocycles

- A is a group,
  Γ is a group acting on A (on the right)

- A <u>cocycle</u> is a map $\boldsymbol{\alpha} : \Gamma \to A$, $\boldsymbol{\alpha} : \gamma \mapsto \boldsymbol{\alpha}_\gamma$ s.t.

$$\boldsymbol{\alpha}_{\sigma\tau} = (\boldsymbol{\alpha}_\sigma)^\tau \cdot \boldsymbol{\alpha}_\tau \quad \forall \sigma, \tau \in \Gamma$$

Cocycles

- A is a group,
  Γ is a group acting on A (on the right)

- A cocycle is a map $\boldsymbol{\alpha} : \Gamma \to A$, $\boldsymbol{\alpha} : \gamma \mapsto \boldsymbol{\alpha}_\gamma$ s.t.

$$\boldsymbol{\alpha}_{\sigma\tau} = (\boldsymbol{\alpha}_\sigma)^\tau \cdot \boldsymbol{\alpha}_\tau \quad \forall \sigma, \tau \in \Gamma$$

- G is a reductive linear algebraic group defined over k
  K is a Galois extension of k

$$\Gamma := \mathrm{Gal}(K : k) \qquad A := \mathrm{Aut}_K(G)$$

Twisted Groups

- For a cocycle $\boldsymbol{\alpha}$:

$$G_{\boldsymbol{\alpha}}(k) = \{\ g \in G(K) \mid g^{\gamma \boldsymbol{\alpha}_\gamma} = g \quad \forall \gamma \in \Gamma\ \} \leq G(K)$$

  is a “twisted” group of Lie type

Twisted Groups

- For a cocycle $\boldsymbol{\alpha}$:

$$G_{\boldsymbol{\alpha}}(k) = \{ \; g \in G(K) \mid g^{\gamma \boldsymbol{\alpha}_\gamma} = g \quad \forall \gamma \in \Gamma \; \} \leq G(K)$$

  is a “twisted” group of Lie type

- “Untwisted” groups of Lie type given by the trivial cocycle:

$$G_{\mathbf{1}}(k) = \{ \; g \in G(K) \mid g^{\gamma} = g \quad \forall \gamma \in \Gamma \; \} = G(k)$$

Problem description

- Which elements are inside $G_{\boldsymbol{\alpha}}(k)$?
  - easy to decide for a given element
  - hard to find new elements

Steinberg presentation and Root datum

- Consider the Steinberg presentation for $G(k)$ with respect to
  - the root datum $\mathcal{R} = (X, \Phi, Y, \Phi^*)$
  - and the fundamental system Π

Steinberg presentation and Root datum

- Consider the Steinberg presentation for $G(k)$ with respect to
  - the root datum $\mathcal{R} = (X, \Phi, Y, \Phi^*)$
  - and the fundamental system Π
- Generators: $x_r(t)$ with $r \in \Phi$ and $t \in k$

Steinberg presentation and Root datum

- Consider the Steinberg presentation for $G(k)$ with respect to
  - the root datum $\mathcal{R} = (X, \Phi, Y, \Phi^*)$
  - and the fundamental system Π
- Generators: $x_r(t)$ with $r \in \Phi$ and $t \in k$
- Relations:

$$x_r(t)x_r(u) = x_r(t+u)$$

$$[x_r(t), x_s(u)] = \prod_{i,j>0} x_{ir+js}(C_{rsij}t^i u^j)$$

$$\dots$$

$$\dots$$

Γ-action on the root system

- Each α_γ can be assumed to be of the form

$$\tau \dot{w} h$$

  - τ is Diagram automorphism
  - w is Weyl element
  - h is torus element

Γ-action on the root system

- Each $\boldsymbol{\alpha}_\gamma$ can be assumed to be of the form

$$\tau \dot{w} h$$

- Γ acts on the root system Φ by

$$\boldsymbol{\alpha}_\gamma : r \mapsto r^{\tau w}$$

Γ-action on the root system

- Each $\boldsymbol{\alpha}_\gamma$ can be assumed to be of the form

$$\tau \dot{w} h$$

- Γ acts on the root system Φ by

$$\boldsymbol{\alpha}_\gamma : r \mapsto r^{\tau w}$$

- Each orbit $\mathcal{O}_{\boldsymbol{\alpha}}(r)$ has one of the following properties:

$$\sum_{s \in \mathcal{O}_{\boldsymbol{\alpha}}(r)} s = 0$$

$$\mathcal{O}_{\boldsymbol{\alpha}}(r) \subseteq \Phi^+$$

Γ-action on the root system

- Each $\boldsymbol{\alpha}_\gamma$ can be assumed to be of the form

$$\tau \dot{w} h$$

- Γ acts on the root system Φ by

$$\boldsymbol{\alpha}_\gamma : r \mapsto r^{\tau w}$$

- Each orbit $\mathcal{O}_{\boldsymbol{\alpha}}(r)$ has one of the following properties:

$$\sum_{s \in \mathcal{O}_{\boldsymbol{\alpha}}(r)} s = 0$$

$$\mathcal{O}_{\boldsymbol{\alpha}}(r) \subseteq \Phi^+, \qquad \mathcal{O}_{\boldsymbol{\alpha}}(r) \subseteq \Phi^-$$

Relative root system

- Put

$$X_0 := \{\chi \in X \mid \sum_{\gamma \in \Gamma} \chi^{\boldsymbol{\alpha}_\gamma} = 0\}$$

Relative root system

- Put
$$X_0 := \{\chi \in X \mid \sum_{\gamma \in \Gamma} \chi^{\boldsymbol{\alpha}_\gamma} = 0\}$$
- Let $\bar{X} := X/X_0$ and $\pi : X \to \bar{X}$
- π is morphism of $\mathbb{Z}$-modules

Relative root system

- Put

$$X_0 := \{\chi \in X \mid \sum_{\gamma \in \Gamma} \chi^{\boldsymbol{\alpha}_\gamma} = 0\}$$

- Let $\bar{X} := X/X_0$ and $\pi : X \to \bar{X}$
- π is morphism of $\mathbb{Z}$-modules

- $\Psi := \pi(\Phi \setminus \Phi_0)$ is a root system
- $\Delta := \pi(\Pi \setminus \Pi_0)$ is a fundamental system for Ψ
- Ψ not necessarily irreducible nor reduced (even if Φ is)

Relative root system

- Put
$$X_0 := \{\chi \in X \mid \sum_{\gamma \in \Gamma} \chi^{\boldsymbol{\alpha}_\gamma} = 0\}$$
- Let $\bar{X} := X/X_0$ and $\pi : X \to \bar{X}$
- π is morphism of $\mathbb{Z}$-modules

- $\Psi := \pi(\Phi \setminus \Phi_0)$ is a root system
- $\Delta := \pi(\Pi \setminus \Pi_0)$ is a fundamental system for Ψ
- Ψ not necessarily irreducible nor reduced (even if Φ is)

- Ψ is called relative root system

Relative roots

- For a relative root $\delta \in \Psi^+$ we have

$$\pi^{-1}(\delta) = \dot{\bigcup_{r \in J_\delta}} \mathcal{O}_{\boldsymbol{\alpha}}(r) \subseteq \Phi^+ \setminus \Phi_0.$$

- Here J_δ is a fixed set of representatives of involved orbits

Relative root elements

- For a relative root $\delta \in \Psi$ let
  - V_δ be the vector space over K with basis J_δ
  - write $t = \sum_{r \in J_\delta} t_r r$

Relative root elements

- For a relative root $\delta \in \Psi$ let
  - V_δ be the vector space over K with basis J_δ
  - write $t = \sum_{r \in J_\delta} t_r r$
  - For $t \in V_\delta$ set

$$u_\delta(t) = \prod_{r \in J_\delta} \prod_{\gamma \in \Gamma} x_r(t_r)^{\gamma \boldsymbol{\alpha}_\gamma}$$

Relative root elements

- For a relative root $\delta \in \Psi$ let
  - V_δ be the vector space over K with basis J_δ
  - write $t = \sum_{r \in J_\delta} t_r r$
  - For $t \in V_\delta$ set

$$u_\delta(t) = \prod_{r \in J_\delta} \prod_{\gamma \in \Gamma} x_r(t_r)^{\gamma \boldsymbol{\alpha}_\gamma}$$

  - Set

$$U_\delta = \left\{ u_\delta(t) \mid t \in V_\delta \right\}$$

Relative root elements

- For a relative root $\delta \in \Psi$ let
  - V_δ be the vector space over K with basis J_δ
  - write $t = \sum_{r \in J_\delta} t_r r$
  - For $t \in V_\delta$ set

$$u_\delta(t) = \prod_{r \in J_\delta} \prod_{\gamma \in \Gamma} x_r(t_r)^{\gamma \boldsymbol{\alpha}_\gamma}$$

  - Set

$$U_\delta = \left\{ u_\delta(t) \mid t \in V_\delta \right\}$$

- Two cases:

  - $2\delta \notin \Psi$
  - $2\delta \in \Psi$

Relative root elements: Case $2\delta \notin \Psi$

- In this case root elements are

$$x_\delta(t) := u_\delta(t)$$

- The root subgroup is abelian group

$$X_\delta = U_\delta$$

Relative root elements: Case $2\delta \in \Psi$

- The element $u_\delta(t)$ is not fixed under $\gamma\boldsymbol{\alpha}_\gamma$

Relative root elements: Case $2\delta \in \Psi$

- The element $u_\delta(t)$ is not fixed under $\gamma\boldsymbol{\alpha}_\gamma$
- BUT: product of the same terms, in a different order

Relative root elements: Case $2\delta \in \Psi$

- The element $u_\delta(t)$ is not fixed under $\gamma\boldsymbol{\alpha}_\gamma$
- BUT: product of the same terms, in a different order
- obtain $c(t)$ by reordering:

$$u_\delta(t)^{\gamma\boldsymbol{\alpha}_\gamma} = u_\delta(t)c(t)$$

Relative root elements: Case $2\delta \in \Psi$

- The element $u_\delta(t)$ is not fixed under $\gamma\boldsymbol{\alpha}_\gamma$
- BUT: product of the same terms, in a different order
- obtain $c(t)$ by reordering:

$$u_\delta(t)^{\gamma\boldsymbol{\alpha}_\gamma} = u_\delta(t)c(t)$$

- $c(t)$ is product of root elements corresponding to roots in $\pi^{-1}(2\delta)$

Relative root elements: Case $2\delta \in \Psi$

- Need a correction term: $v(t)$
  such that $u_\delta(t)v(t)$ is fixed under $\gamma\boldsymbol{\alpha}_\gamma$

Relative root elements: Case $2\delta \in \Psi$

- Need a correction term: $v(t)$
  such that $u_\delta(t)v(t)$ is fixed under $\gamma\boldsymbol{\alpha}_\gamma$

$$(u_\delta(t)v(t))^{\gamma\boldsymbol{\alpha}_\gamma} = u_\delta(t)v(t) \iff c(t) = v(t)v(t)^{-\gamma\boldsymbol{\alpha}_\gamma}$$

Relative root elements: Case $2\delta \in \Psi$

- Need a correction term: $v(t)$
  such that $u_\delta(t)v(t)$ is fixed under $\gamma\boldsymbol{\alpha}_\gamma$

$$(u_\delta(t)v(t))^{\gamma\boldsymbol{\alpha}_\gamma} = u_\delta(t)v(t) \iff c(t) = v(t)v(t)^{-\gamma\boldsymbol{\alpha}_\gamma}$$

- This equation is solvable and the set of solutions in

$$X = \prod_{r \in \pi^{-1}(2\delta)} X_r$$

is the coset $v(t)X_{2\delta}$ for any particular solution $v(t)$

Relative root elements: Case $2\delta \in \Psi$

- Need a correction term: $v(t)$
  such that $u_\delta(t)v(t)$ is fixed under $\gamma\boldsymbol{\alpha}_\gamma$

$$(u_\delta(t)v(t))^{\gamma\boldsymbol{\alpha}_\gamma} = u_\delta(t)v(t) \Longleftrightarrow c(t) = v(t)v(t)^{-\gamma\boldsymbol{\alpha}_\gamma}$$

- This equation is solvable and the set of solutions in

$$X = \prod_{r \in \pi^{-1}(2\delta)} X_r$$

  is the coset $v(t)X_{2\delta}$ for any particular solution $v(t)$

- Use modified version of additive Hilbert's Theorem 90

Relative root elements: Case $2\delta \in \Psi$

- Relative root elements are

$$x_\delta(t) := u_\delta(t)v(t)$$

for a fixed solution $v(t)$

Relative root elements: Case $2\delta \in \Psi$

- Relative root elements are

$$x_\delta(t) := u_\delta(t)v(t)$$

  for a fixed solution $v(t)$

- Relative root subgroup is

$$\begin{aligned} X_\delta &:= \langle X_{2\delta}, \{x_\delta(t) | t \in V_\delta\}\rangle \\ &= \langle x_\delta(t) | t \in V_\delta\rangle X_{2\delta} \end{aligned}$$

Relative root elements: Case $2\delta \in \Psi$

- Relative root elements are

$$x_\delta(t) := u_\delta(t)v(t)$$

  for a fixed solution $v(t)$

- Relative root subgroup is

$$\begin{aligned} X_\delta &:= \langle X_{2\delta}, \{x_\delta(t) | t \in V_\delta\}\rangle \\ &= \langle x_\delta(t) | t \in V_\delta\rangle X_{2\delta} \end{aligned}$$

- Note that the definition of X_δ is independent of the choice of elements $v(t)$

Groups generated by relative roots

- $$U_{\boldsymbol{\alpha}}(k) = U(K) \cap G_{\boldsymbol{\alpha}}(k) = \langle X_\delta \mid \delta \in \Psi^+ \rangle$$

Groups generated by relative roots

- $$U_{\boldsymbol{\alpha}}(k) = U(K) \cap G_{\boldsymbol{\alpha}}(k) = \langle X_\delta \mid \delta \in \Psi^+ \rangle$$

- $$G_{\boldsymbol{\alpha}}(k)^\dagger = \langle U_{\boldsymbol{\alpha}}(k)^g \mid g \in G_{\boldsymbol{\alpha}}(k) \rangle$$

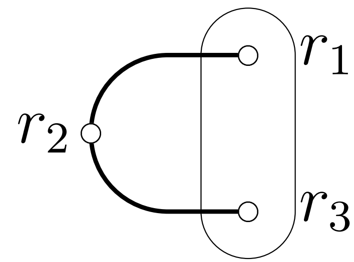
Groups generated by relative roots

- $$U_{\boldsymbol{\alpha}}(k) = U(K) \cap G_{\boldsymbol{\alpha}}(k) = \langle X_\delta \mid \delta \in \Psi^+ \rangle$$

- $$\begin{aligned} G_{\boldsymbol{\alpha}}(k)^\dagger &= \langle U_{\boldsymbol{\alpha}}(k)^g \mid g \in G_{\boldsymbol{\alpha}}(k) \rangle \\ &= \langle X_\delta \mid \delta \in \Psi \rangle \end{aligned}$$

Example

$^2A_{3,1}(k)$



$$\mathcal{O}_{\boldsymbol{\alpha}}(r_1) = \{r_1, r_2 + r_3\}$$

$$\mathcal{O}_{\boldsymbol{\alpha}}(r_2) = \{r_2, -r_2\}$$

$$\mathcal{O}_{\boldsymbol{\alpha}}(r_3) = \{r_3, r_1 + r_2\}$$

$$\mathcal{O}_{\boldsymbol{\alpha}}(r_*) = \{r_*\}$$