COMPUTING WITH ROOT SUBGROUPS OF TWISTED REDUCTIVE GROUPS

ARJEH M. COHEN, SERGEI HALLER, AND SCOTT H. MURRAY

Abstract. We present algorithms to compute with relative root subgroups of twisted reductive groups. Given a Galois cocycle specifying a twisted form, we can find the relative root datum and Tits index, and carry out operations involving root elements. We can also find a presentation of the unipotent subgroup. Given a Tits index and the anisotropic subgroup, we can determine a cocycle with that index, if one exists.

1. Introduction

In this paper, we describe algorithms for computing with relative root elements in twisted reductive groups over arbitrary perfect fields, as described in [BT65]. This builds on the algorithms for element arithmetic in the Steinberg presentation of untwisted groups of Lie type given in [CMT04, CHM08]. These forms are classified by Galois cohomology, as in [Spr98, Ser02]. Here we assume that the Galois cocycle is provided by the user, but algorithms for computing Galois cohomology can be found in [Hal05], extending the work of [Hol85]. All algorithms presented here have been implemented by the second author in Magma [BC97].

The following notation is used throughout the paper. Let G be a split reductive linear algebraic group defined over the perfect field k. We consider twisted forms of G which are split over a given finite Galois extension K of k. Since every twisted form of G splits over some such extension, we do not lose any generality. Let $A := \mathrm{Aut}(G)$ be the group of algebraic automorphisms of G and let $\Gamma := \mathrm{Gal}(K\colon k)$. The twisted forms of G splitting over K are now classified by the Galois cohomology $H^1(\Gamma, A)$. For a given cocycle $\boldsymbol{\alpha} \in Z^1(\Gamma, A)$, the twisted form is written $G_{\boldsymbol{\alpha}}$ and its group of k-rational points is

$$G_{\boldsymbol{\alpha}}(k) = \{g \in G(K) \mid g^{\gamma \boldsymbol{\alpha}_\gamma} = g \text{ for all } \gamma \in \Gamma\}.$$

Recall that the Steinberg presentation for G determines a standard maximal torus T and standard unipotent subgroup U. We can assume that our cocycle stabilizes T by Springer's Lemma [Ser02].

From the definition, it is easy to test if an element of $G(K)$ is in $G_{\boldsymbol{\alpha}}(k)$. We call this an *extrinsic* description of the twisted group, since it is given in terms of a larger group. This paper is part of a program to determine computationally effective BN-pairs and presentations for $G_\alpha(k)$, ie, an *intrinsic* description. In this paper we make some progress towards this by giving algorithms for the *relative root elements*. Our main result is:

Date: January 17, 2009.

This paper was written during a stay of the second author at the Magma group at the University of Sydney.

Main Theorem. *Let k be a perfect field with finite Galois extension K, and let $\Gamma = \mathrm{Gal}(K\colon k)$. Let G be a split reductive algebraic group over k described by its Steinberg presentation. Let T be the standard maximal torus and let U be the standard unipotent subgroup. Given a cocycle $\boldsymbol{\alpha} \in Z^1(\Gamma, \mathrm{Aut}(G))$ normalizing T we can compute:*

1. *the relative root system and Tits index of G_α with respect to T;*
2. *the relative root subgroups of G_α with respect to T, given as parametrised subgroups of $G(K)$; and*
3. *an explicit presentation for $U_{\boldsymbol{\alpha}}(k) := G_\alpha(k) \cap U(K)$.*

We apply our algorithms to several examples: ${}^2\mathrm{E}_{6,1}^{35}(k)$, ${}^3\mathrm{D}_{4,1}^{9}(k)$, and ${}^6\mathrm{D}_{4,1}^{9}(k)$. In these examples, the field k need not be specified beforehand. In fact, given a Tits index for G and an intrinsic description of the anisotropic kernel, we can give explicit conditions on k for the cocycle to exist, as well as a method for constructing it. Another application, given in [Hal05], is to compute twisted maximal tori of reductive groups, and then use them to compute all Sylow subgroups of a finite group of Lie type.

In Section 2 we describe algorithms for extended root data, relative root data, and Tits indices. In Section 3 we describe relative root elements and relative root subgroups, as well as relations between them. Finally in Section 4 we apply our techniques to several important examples, some of which have not been explicitly described before now, to the best of our knowledge.

Note that the methods presented here do not work for types ${}^2\mathrm{B}_2$, ${}^2\mathrm{G}_2$, and ${}^2\mathrm{F}_4$, since the map induced by the Dynkin diagram symmetry on the full root lattice X is not linear. We expect though that our method will work if we replace the $\mathbb{Z}$-module X by a $(\mathbb{Z}+\mathbb{Z}\sqrt{2})$-module in cases ${}^2\mathrm{B}_2$ and ${}^2\mathrm{F}_4$ or a $(\mathbb{Z}+\mathbb{Z}\sqrt{3})$-module in the case ${}^2\mathrm{G}_2$. This construction is given for groups over finite fields in [BM92].

2. The relative root datum and Tits index

In this section we describe the extended root datum, relative root datum, and Tits index for the twisted reductive group $G_{\boldsymbol{\alpha}}$. We also outline algorithms for these structures. See [Dem65] on the theory of root data and see [CMT04] for computational methods. Our description of relative root data is based on [Sat71] and [Sch69].

Let $\mathcal{R} = (X, \Phi, Y, \Phi^\star)$ be the root datum of G. Let Π be a fundamental system of Φ and define the positive roots Φ^+ accordingly. Recall that an algebraic group can be identified with its elements defined over $\bar{k}$, the algebraic closure of k. The Steinberg presentation of G has generators $x_r(a)$, for $r \in \Phi$ a root and $a \in \bar{k}$, and $y \otimes t$, for $y \in Y$ and $t \in \bar{k}^\times$. The relations are given in [CMT04, Section 4.1] and the action of a field automorphism γ is given by $x_r(a)^\gamma = x_r(a^\gamma)$ and $(y \otimes t)^\gamma = y \otimes t^\gamma$. The *standard torus* $T = Y \otimes \bar{k}^\times$ is now the subgroup generated by the elements $y \otimes t$, for $y \in Y$ and $t \in \bar{k}^\times$. The *standard unipotent subgroup* U is generated by the elements $x_r(a)$ for $r \in \Phi^+$ and $a \in \bar{k}$. Finally the *root subgroup* of the root r is $X_r = \{x_r(a) \mid a \in \bar{k}\} \cong \bar{k}^+$.

As usual, set $A := \mathrm{Aut}(G)$, $\Gamma := \mathrm{Gal}(K\colon k)$, and let $\boldsymbol{\alpha} \in Z^1(\Gamma, A)$ be a fixed cocycle normalising T. A cocycle is determined by the images of the generators of Γ, and we use this fact to represent our cocycle computationally. Given a fixed generating set $\gamma_1, \ldots, \gamma_m$ for Γ, we write $[\![a_1, \ldots, a_m]\!]$ to denote the cocycle $\boldsymbol{\alpha}$ with

$\boldsymbol{\alpha}_{\gamma_i} = a_i$ for each i. The cocycle determines a twisted action on $G_{\boldsymbol{\alpha}}$ where $\gamma \in \Gamma$ acts by $g \mapsto g^{\gamma \boldsymbol{\alpha}_\gamma}$.

The automorphism group of $\mathcal{R}$ is a semidirect product DW, where the Weyl group $W := N_G(T)/T$ is normal and D is the group of automorphisms of the Dynkin diagram of $\mathcal{R}$. Now $N_A(T)$ is a semidirect product $(DW)T$ with T normal. For $\tau \in D$ or $w \in W$ there is an easily computed T-coset representative denoted $\dot{\tau}$ or $\dot{w}$ (see [CMT04]). Since $\boldsymbol{\alpha}$ normalizes T, for each $\gamma \in \Gamma$ we have $\boldsymbol{\alpha}_\gamma = \dot{\tau}\dot{w}t$ for some $\tau \in D$, $w \in W$, $t \in T$. The action of γ on $\mathcal{R}$ is now given by τw. This is the Γ-action in [Sch69]. The root datum $\mathcal{R}$ together with the action of Γ on $\mathcal{R}$ induced by the cocycle $\boldsymbol{\alpha}$ is called an *extended root datum* and denoted by $\mathcal{R}_{\boldsymbol{\alpha}}$.

In Magma, we generally use a representation of Galois cocycles which explicitly stores the action of Γ on $\mathcal{R}$. If $\boldsymbol{\alpha}_\gamma$ is just given as a map $G(K) \to G(K)$, we need to compute this action. If G is semisimple, we can proceed as follows:

1. Take a generating set $\gamma_1, \dots, \gamma_m$ for Γ, and let $\Pi = \{r_1, \dots, r_\ell\}$.
2. For each γ_i and r_j compute $x_{r_j}(1)^{\boldsymbol{\alpha}_{\gamma_i}}$. This has the form $x_s(\lambda)$ for $s = r^{\boldsymbol{\alpha}_\gamma}$ and some $\lambda \in k$.
3. We now have the action of $\boldsymbol{\alpha}_\gamma$ on the roots, so we can compute its action on X by linear algebra over $\mathbb{Q}$. The action on Y is the dual of this action.

If G is not semisimple, we need to look at the action on toral elements: Let $f_1, \dots, f_n$ be a basis of Y and suppose $f_j^{\boldsymbol{\alpha}_{\gamma_i}} = \sum_m a_m f_m$. Then we have, for $t \in K$,

$$(f_j \otimes t)^{\boldsymbol{\alpha}_{\gamma_i}} = \prod_m f_m \otimes t^{a_m}.$$

If necessary we can find the a_m by a Gröbner basis computation. For many fields there is a faster method however: For example, if K is finite we can use discrete logarithms, or if K is a number field we can use the algorithm of [FdG08]. Once again the action on X is the dual.

Let $\mathcal{O}_{\boldsymbol{\alpha}}(\chi)$ denote the orbit of $\chi \in X$ under the Γ-action corresponding to the cocycle $\boldsymbol{\alpha}$. For $r \in \Phi$, [Sch69, (16)] shows that either $\mathcal{O}_{\boldsymbol{\alpha}}(r)$ is contained in Φ^+, or it is contained in Φ^-, or the sum of the roots of $\mathcal{O}_{\boldsymbol{\alpha}}(r)$ is zero. In the latter case, we have $\sum_{\gamma \in \Gamma} r^{\boldsymbol{\alpha}_\gamma} = 0$, which is equivalent to

$$\sum_{s \in \mathcal{O}_{\boldsymbol{\alpha}}(r)} s = 0, \tag{1}$$

since $\sum_{\gamma \in \Gamma} r^{\boldsymbol{\alpha}_\gamma} = m \sum_{s \in \mathcal{O}_{\boldsymbol{\alpha}}(r)} s$, where m is the order of the stabilizer of r in Γ. Put

$$X_0 := \{\chi \in X \mid \sum_{\gamma \in \Gamma} \chi^{\boldsymbol{\alpha}_\gamma} = 0\}. \tag{2}$$

Let $\Phi_0 := \Phi \cap X_0$ and $\Pi_0 := \Pi \cap X_0$. Then, by [Sch69, Section 1], X_0 is a submodule of X, Φ_0 is a subsystem of Φ, and Π_0 is a fundamental system of Φ_0. Note that Π_0 is not necessarily a basis of X_0 (a counterexample is given in Example 2.1).

Set $\bar{X} := X/X_0$ and let $\pi_X : X \to \bar{X}$ be the standard projection. Then $\bar{X}$ is a free $\mathbb{Z}$-module. Let Ψ and Δ be the images under π_X of $\Phi \setminus \Phi_0$ and $\Pi \setminus \Pi_0$, respectively. Write π for the restriction of π_X to Φ. Dually we can define $\bar{Y}$ and $\Psi^\star$. Then $\mathcal{S} = (\bar{X}, \Psi, \bar{Y}, \Psi^\star)$ is a root datum and Δ is a fundamental system of it. We call Ψ the *relative root datum* and Δ the *relative fundamental system*. Note that Ψ need not be irreducible nor reduced even if Φ is. The *relative rank* of $\mathcal{R}_{\boldsymbol{\alpha}}$ is $|\Delta|$, whereas the *absolute rank* is $|\Pi|$. Let Ψ^+ and Ψ^- denote the images under π

of $\Phi^+ \setminus \Phi_0$ and $\Phi^- \setminus \Phi_0$. When $X_0 = X$, the relative root system is an empty set and the twisted form $G_{\boldsymbol{\alpha}}$ is called *anisotropic*.

Let $\delta \in \Psi^+$ be a relative root. We fix a set of representatives of the orbits $\mathcal{O}_{\boldsymbol{\alpha}}(r)$ with the property $\pi(r) = \delta$ and call this set J_δ. Then, by [Sch69, Section 2],

$$\pi^{-1}(\delta) = \dot{\bigcup_{r \in J_\delta}} \mathcal{O}_{\boldsymbol{\alpha}}(r). \tag{3}$$

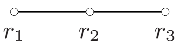
Once the action of Γ on X and Y is known, the other properties of an extended root datum can be computed from the definitions. The action of Γ on X can be found as an integral matrix group. Now X_0 is the intersection of the nullspaces of the generators, and π can be computed by linear algebra. The action on Φ can be found as a permutation group The orbits can be calculated by the standard orbit algorithm, and the representative sets J_δ can be chosen arbitrarily. We can also compute basic properties of the relative root datum. For example, the Cartan matrix can be found by looking at root strings. In type A_{20}, all of these computations take less than 2 seconds on a Pentium 1.6 GHz.

We now construct an action of Γ on Π induced by the action on Φ. Let $\gamma \in \Gamma$ and recall that $\boldsymbol{\alpha}_\gamma$ acts on $\mathcal{R}$ as τw for some $\tau \in D$, $w \in W$. Then γ acts on Π by $r \mapsto r^\tau$. This is the $[\Gamma]$-action of [Sch69]. The cocycle $\boldsymbol{\alpha}$ and the corresponding twisted form $G_{\boldsymbol{\alpha}}$ are called *inner* if the $[\Gamma]$-action is trivial and *outer* otherwise. Let $[\mathcal{O}]_{\boldsymbol{\alpha}}(r)$ be the orbit of $r \in \Pi$ under this action. Then, by [Sch69, Proposition 3.5],

$$[\mathcal{O}]_{\boldsymbol{\alpha}}(r) = \Pi \cap \pi^{-1}(\pi(r)).$$

In order to compute the $[\Gamma]$-action on the Dynkin diagram, first consider the Γ-action as a permutation group on Φ. Then D is the subgroup normalising the set Π, which can be found by standard permutation group algorithms.

Example 2.1. We illustrate this by a small example. Let Φ be a root system of type A_3 and let $\Pi = \{r_1, r_2, r_3\}$ be a fundamental root system of Φ with the Dynkin diagram:



Then the Weyl group W is generated by fundamental reflections s_1, s_2, and s_3. Let $\Gamma = \langle \gamma \rangle$ be of order 2. Choose the cocycle $\boldsymbol{\alpha} = [\![\dot{\tau}\dot{s}_2]\!]$, where τ is the non-trivial Dynkin diagram symmetry. Then

$$X_0 = \langle r_2, r_1 - r_3 \rangle, \quad \Phi_0 = \{\pm r_2\}, \quad \text{and} \quad \Pi_0 = \{r_2\}.$$

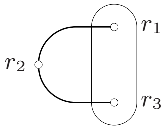
The orbits of the actions of Γ on Φ and Π are

$$\begin{aligned} \mathcal{O}_{\boldsymbol{\alpha}}(r_1) &= \{r_1, r_2 + r_3\}, & [\mathcal{O}]_{\boldsymbol{\alpha}}(r_1) &= \{r_1, r_3\}, \\ \mathcal{O}_{\boldsymbol{\alpha}}(r_2) &= \{r_2, -r_2\}, & [\mathcal{O}]_{\boldsymbol{\alpha}}(r_2) &= \{r_2\}, \\ \mathcal{O}_{\boldsymbol{\alpha}}(r_3) &= \{r_3, r_1 + r_2\}, & & \\ \mathcal{O}_{\boldsymbol{\alpha}}(r_1 + r_2 + r_3) &= \{r_1 + r_2 + r_3\}, & & \end{aligned}$$

together with the orbits lying entirely in Φ^-, which are determined by negating the orbits in Φ^+. The relative root system is $\Psi = \{\pm\delta_1, \pm 2\delta_1\}$ with $\delta_1 = \pi(r_1)$. This is a root system of type BC_1 with the fundamental system $\Delta = \{\delta_1\}$. Furthermore

$$\pi^{-1}(\delta_1) = \mathcal{O}_{\boldsymbol{\alpha}}(r_1) \,\dot{\cup}\, \mathcal{O}_{\boldsymbol{\alpha}}(r_3) \quad \text{and} \quad \pi^{-1}(2\delta_1) = \mathcal{O}_{\boldsymbol{\alpha}}(r_1 + r_2 + r_3).$$

Now we describe briefly the graphic notation for relative root systems called the *Tits index* [Tit66]. It is the Dynkin diagram of $\mathcal{R}$ with additional data describing the $[\Gamma]$-actions. We call a vertex of the Dynkin diagram *distinguished* if the corresponding fundamental root is not in Π_0. The vertices of the fundamental roots belonging to the same $[\Gamma]$-orbit are placed "next" to each other. If a vertex is distinguished, then all roots in its $[\Gamma]$-orbit are distinguished as well, and we circle the orbit. Thus, the example from the previous section has the Tits index



.

Let S be a maximal k-split torus contained in T. The commutator subgroup of the centraliser $C_G(S)$ is a semisimple k-anisotropic group and is called the *anisotropic kernel* of $G_{\boldsymbol{\alpha}}$. The anisotropic kernel is also a reductive group and the diagram of the anisotropic kernel is obtained from the index of $G_{\boldsymbol{\alpha}}$ by removing all distinguished vertices. Note that the anisotropic kernel is not completely determined by the Tits index, so different forms may have identical indices. The Tits index determines the extended root datum, up to isomorphism.

We use the same terminology for the Tits indices as in [Tit66]: A Tits index is denoted by ${}^gM^t_{n,\ell}$, where M_n is the Cartan type of the Dynkin diagram, g is the order of the quotient of Γ modulo the kernel of the $[\Gamma]$-action, n and ℓ are the absolute and the relative ranks, and t denotes the degree of a division algebra that occurs in the definition of the form in the case of classical types and it denotes the dimension of the anisotropic kernel in the case of exceptional types (including D_4). To emphasize the difference in the notation, t is put in parentheses for the classical types. The Tits index in the above example has type ${}^2\mathrm{A}^{(2)}_{3,1}$. We obviously have $g = 1$ for inner forms, in which case g is usually omitted. In the one case where t does not uniquely determine which index is intended, they are distinguished by primes: ${}^2\mathrm{E}^{16'}_{6,2}$ and ${}^2\mathrm{E}^{16''}_{6,2}$.

We have seen how to compute Φ_0 and the $[\Gamma]$-action. So, in order to compute the Tits index from a cocycle, it only remains to find the value of t. In the classical cases, t can computed from the action on the natural module for the group; in the exceptional cases, compute the dimension of the reductive Lie subalgebra corresponding to Φ_0. We have now proved part (1) of the Main Theorem.

Conversely, given a Tits index we can compute an extended root datum by extending the $[\Gamma]$ action linearly to all of Φ. A cocycle can also be computed provided that we have an intrinsic description of the anisotropic radical, as we see in Section 4.

3. ROOT SUBGROUPS

The *(standard) unipotent subgroup* of $G_{\boldsymbol{\alpha}}(k)$ is $U_{\boldsymbol{\alpha}}(k) := U(K) \cap G_{\boldsymbol{\alpha}}(k)$. In this section, we describe the relative root elements and relative root subgroups, and use them to compute a presentation of $U_{\boldsymbol{\alpha}}(k)$.

Recall that the only scalar multiples of a root δ in a (not necessarily reduced) root system are $\pm\frac{1}{2}\delta$, $\pm\delta$, and $\pm 2\delta$. We use the following lemma repeatedly:

Lemma 3.1. *Let* $\delta, \epsilon \in \Psi^+$ *and* $r \in \pi^{-1}(\delta)$, $s \in \pi^{-1}(\epsilon)$. *If* $ir + js \in \Phi$ *for positive integers* i *and* j, *then* $i\delta + j\epsilon \in \Psi^+$ *and* $\pi(ir+js) = i\delta + j\epsilon$. *In particular, if* $\delta = \epsilon$, *then we must have* $i = j = 1$ *and* $\pi(r+s) = 2\delta$.

Proof. Since $r \notin \Phi_0$, the coefficient of at least one fundamental root in $\Pi \setminus \Pi_0$ is positive in the linear combination of r. Hence the same coefficient in $ir + js$ is positive and so $ir + js \in \Phi^+ \setminus \Phi_0$. Since π_X is a homomorphism of $\mathbb{Z}$-modules, we have $\pi(ir+js) = i\pi(r) + j\pi(s) = i\delta + j\epsilon \in \Psi^+$.

If $\delta = \epsilon$, then $\pi(ir + js) = (i+j)\delta$. This can only be a root in Ψ if $i + j = 2$ since i and j are positive integers. $\square$

For $\delta \in \Psi^+$, define

$$U_\delta = \prod_{s \in \pi^{-1}(\delta)} X_s = \prod_{r \in J_\delta} \prod_{\gamma \in \Gamma} X_{r^{\boldsymbol{\alpha}_\gamma}},$$

with the whole product taken in the ordering of the roots fixed for the unique decomposition of U in [CHM08]. This is an algebraic subset of G, but not necessarily a subgroup. The *relative root subgroup* X_δ is now defined as the k-rational points of the subgroup of $G_{\boldsymbol{\alpha}}$ (algebraically) generated by U_δ. In other words,

$$X_\delta := \langle U_\delta \rangle_{\boldsymbol{\alpha}}(k).$$

First we consider the structure of the algebraic subgroup $\langle U_\delta \rangle$.

Lemma 3.2. *Let* $\delta \in \Psi^+$. *If* $2\delta \notin \Psi$, *then* $U_\delta = \langle U_\delta \rangle$ *is an abelian group. If* $2\delta \in \Psi$, *then* $\langle U_\delta \rangle = U_\delta U_{2\delta}$, *the centre of* $\langle U_\delta \rangle$ *is* $U_{2\delta}$, *and* $\langle U_\delta \rangle / U_{2\delta}$ *is abelian.*

Proof. If $a, b \in U_\delta$, then $a = \prod_{r \in \pi^{-1}(\delta)} x_r(a_r)$ and $b = \prod_{r \in \pi^{-1}(\delta)} x_r(b_r)$ with each $a_r, b_r \in \bar{k}$. By collection using the commutator relations, as in [CHM08], we can write

$$ab = \prod_{r \in \pi^{-1}(\delta)} x_r(a_r + b_r) \prod_s x_s(c_s)$$

where each $c_s \in \bar{k}$ and s runs over roots which are linear combinations of roots in $\pi^{-1}(\delta)$ with positive integral coefficients. By Lemma 3.1, it follows that $\prod_s x_s(c_s)$ is in $\langle U_{2\delta} \rangle$. If $2\delta \notin \Psi$, such roots s do not exist, and so U_δ is an abelian group. If $2\delta \in \Psi$, then $4\delta \notin \Psi$ and so $U_{2\delta}$ is an abelian group and must contain $\prod_s x_s(c_s)$. Hence $\langle U_\delta \rangle \subseteq U_\delta U_{2\delta}$ and $(U_\delta U_{2\delta})/U_{2\delta}$ is abelian.

If $\pi(t) = 2\delta$, then we must have $t = r + s$ for some $r, s \in \pi^{-1}(\delta)$. (Otherwise take a counterexample $t = \sum_i t_i r_i$ with $\sum_i t_i$ minimal. Then $t - r_i \in \Phi_0$ for some i, and hence $\pi(t) = \pi(r_1)$ which cannot be a double root.) Hence each $X_t = [X_r, X_s] \leq \langle U_\delta \rangle$, and so $U_{2\delta} \subseteq \langle U_\delta \rangle$.

Finally if $r \in \pi^{-1}(\delta)$, $s \in \pi^{-1}(2\delta)$ and $ir + js$ is a root for some positive integers i and j, then $\pi(ir+js) = (i+2j)\delta \in \Psi$ by Lemma 3.1 and $i + 2j \geq 3$, a contradiction. Hence $[X_r, X_s] = 1$, and so $U_{2\delta}$ is the centre. $\square$

Now we describe X_δ, consisting of the elements of $\langle U_\delta \rangle$ which are fixed by all $\gamma\boldsymbol{\alpha}_\gamma$. For $\delta \in \Psi$ let V_δ be the formal K-vector space with basis J_δ and let $t = \sum_{r \in J_\delta} t_r r \in V_\delta$. Define

$$u_\delta(t) = \prod_{r \in J_\delta} \prod_{\gamma \in \Gamma} x_r(t_r)^{\gamma\boldsymbol{\alpha}_\gamma}, \tag{4}$$

where the product is in the same order as above. The image under $\gamma\boldsymbol{\alpha}_\gamma$ of the root element $x_r(t_r)$ for $r \in \Phi$ and $t_r \in K$, is

$$x_r(t_r)^{\gamma\boldsymbol{\alpha}_\gamma} = x_{r^{\boldsymbol{\alpha}_\gamma}}(\lambda_{r\gamma} t_r^\gamma), \tag{5}$$

where $\lambda_{r\gamma} \in K$ is a constant that depends on the root r and on γ. Since

$$\left(x_r(t_r)^{\gamma'\boldsymbol{\alpha}_{\gamma'}}\right)^{\gamma\boldsymbol{\alpha}_\gamma} = x_r(t_r)^{\gamma'\gamma\boldsymbol{\alpha}_{\gamma'}^{\gamma}\boldsymbol{\alpha}_\gamma} = x_r(t_r)^{\gamma'\gamma\boldsymbol{\alpha}_{\gamma'\gamma}},$$

we have $u_\delta(t)^{\gamma\boldsymbol{\alpha}_\gamma}$ is the product of the same root elements as $u_\delta(t)$ taken in a different order.

If 2δ is not a relative root, then U_δ is an abelian group. Thus the order of terms in the product $u_\delta(t)$ is irrelevant and $u_\delta(t)^{\gamma\boldsymbol{\alpha}_\gamma} = u_\delta(t)$. Clearly $u_\delta : V_\delta \to U_\delta$ parametrizes the relative root group $X_\delta = \langle U_\delta \rangle_{\boldsymbol{\alpha}}(k)$.

If 2δ is a relative root, we define

$$c_{\delta\gamma}(t) = u_\delta(t)^{-1} u_\delta(t)^{\gamma\boldsymbol{\alpha}_\gamma} \quad \text{for } \gamma \in \Gamma. \tag{6}$$

By the same collection argument used in the proof of Lemma 3.2, $c_{\delta\gamma}(t)$ is contained in $U_{2\delta}$. Let $\boldsymbol{\rho} : \Gamma \to U_{2\delta}$ be defined by $\gamma \mapsto c_{\delta\gamma}(t)$. We compute

$$\begin{aligned} u_\delta(t) c_{\delta,\gamma\gamma'}(t) &= u_\delta(t)^{\gamma\gamma'\boldsymbol{\alpha}_{\gamma\gamma'}} = \left(u_\delta(t)^{\gamma\boldsymbol{\alpha}_\gamma}\right)^{\gamma'\boldsymbol{\alpha}_{\gamma'}} = \left(u_\delta(t) c_{\delta\gamma}(t)\right)^{\gamma'\boldsymbol{\alpha}_{\gamma'}} \\ &= u_\delta(t) c_{\delta\gamma'}(t) c_{\delta\gamma}(t)^{\gamma'\boldsymbol{\alpha}_{\gamma'}} = u_\delta(t) c_{\delta\gamma}(t)^{\gamma'\boldsymbol{\alpha}_{\gamma'}} c_{\delta\gamma'}(t) \end{aligned}$$

using equation (6) and the fact that $U_{2\delta}$ is central. Hence $c_{\delta,\gamma\gamma'}(t) = c_{\delta\gamma}(t)^{\gamma'\boldsymbol{\alpha}_{\gamma'}} c_{\delta\gamma'}(t)$ and so $\boldsymbol{\rho}$ is a cocycle in $Z^1(\Gamma, (U_{2\delta})_{\boldsymbol{\alpha}})$.

By [Spr98, Corollary 14.3.10], $H^1(\Gamma, U) = 1$ for every unipotent group U. Hence $\boldsymbol{\rho}$ is a coboundary, that is, there is a solution $v_\delta(t) \in U_{2\delta}(K)$ for the system of equations

$$c_{\delta\gamma}(t) = v_\delta(t) v_\delta(t)^{-\gamma\boldsymbol{\alpha}_\gamma}, \qquad \text{for all } \gamma \in \Gamma. \tag{7}$$

An algorithm for finding $v_\delta(t)$ is given at the end of this section.

Now fix a particular solution $v_\delta(t)$ for each $t \in V_\delta$ and define *relative root elements* by

$$x_\delta(t) = \begin{cases} u_\delta(t) & \text{if } 2\delta \notin \Psi\ , \\ u_\delta(t) v_\delta(t) & \text{if } 2\delta \in \Psi\ . \end{cases} \tag{8}$$

We will now show that

$$X_\delta = \begin{cases} \{x_\delta(t) \mid t \in V_\delta\} & \text{if } 2\delta \notin \Psi\ , \\ \{x_\delta(t) x_{2\delta}(s) \mid t \in V_\delta, s \in V_{2\delta}\} & \text{if } 2\delta \in \Psi\ . \end{cases} \tag{9}$$

If 2δ is a relative root, then

$$\begin{aligned} (x_\delta(t))^{\gamma\boldsymbol{\alpha}_\gamma} &= u_\delta(t)^{\gamma\boldsymbol{\alpha}_\gamma} v_\delta(t)^{\gamma\boldsymbol{\alpha}_\gamma} = u_\delta(t) c_{\delta,\gamma}(t) v_\delta(t)^{\gamma\boldsymbol{\alpha}_\gamma} \\ &= u_\delta(t) v_\delta(t) v_\delta(t)^{-\gamma\boldsymbol{\alpha}_\gamma} v_\delta(t)^{\gamma\boldsymbol{\alpha}_\gamma} = x_\delta(t), \end{aligned}$$

and so $x_\delta(t)$ is in X_δ. Clearly $X_{2\delta} \subseteq X_\delta$.

The fact that every element of X_δ is of the form $x_\delta(t) x_{2\delta}(s)$ follows immediately from:

Lemma 3.3. *For given $c_{\delta\gamma}(t)$, $\gamma \in \Gamma$, the set of solutions $v_\delta(t) \in U_{2\delta}$ for (7) is the coset $w_\delta(t) X_{2\delta}$, where $w_\delta(t)$ is any particular solution for this equation system.*

Proof. Let $w_\delta(t)$ be a solution of (7) and $x \in X_{2\delta}$. Then $w_\delta(t)x \in U_{2\delta}$ and

$$\begin{aligned}(w_\delta(t)x)(w_\delta(t)x)^{-\gamma\boldsymbol{\alpha}_\gamma} &= w_\delta(t)xx^{-\gamma\boldsymbol{\alpha}_\gamma}w_\delta(t)^{-\gamma\boldsymbol{\alpha}_\gamma}\\ &= w_\delta(t)xx^{-1}w_\delta(t)^{-\gamma\boldsymbol{\alpha}_\gamma} = w_\delta(t)w_\delta(t)^{-\gamma\boldsymbol{\alpha}_\gamma}\\ &= c_{\delta\gamma}(t)\end{aligned}$$

for all $\gamma \in \Gamma$. If on the other hand, $v_1, v_2 \in U_{2\delta}$ are two solutions for (7), then $v_2 v_2^{-\gamma\boldsymbol{\alpha}_\gamma} = c_{\delta\gamma}(t) = v_1 v_1^{-\gamma\boldsymbol{\alpha}_\gamma}$ and so $v_1^{-1}v_2 = v_1^{-\gamma\boldsymbol{\alpha}_\gamma} v_2^{\gamma\boldsymbol{\alpha}_\gamma} = (v_1^{-1}v_2)^{\gamma\boldsymbol{\alpha}_\gamma}$, for all $\gamma \in \Gamma$. Thus $v_1^{-1}v_2 \in X_{2\delta}$. □

Next we want to show that $U_{\boldsymbol{\alpha}}(k)$ is generated by the root subgroups. Let $u \in U_{\boldsymbol{\alpha}}(k)$ be an arbitrary element. Write u as a product of root elements with the roots in order of increasing height, as in [CHM08]. Let $x_r(a)$ be the first nontrivial root element occurring in this decomposition. Since $x_r(a)$ occurs in this product, $x_r(a)^{\gamma\boldsymbol{\alpha}_\gamma}$ must also occur in the product for each $\gamma \in \Gamma$, since u is fixed by $\gamma\boldsymbol{\alpha}_\gamma$. In particular, $\mathcal{O}_{\boldsymbol{\alpha}}(r)$ must be contained in Φ^+, hence $\delta := \pi(r) \in \Psi^+$. Now let $t \in V_\delta$ with $t_r = a$ and $t_s = 0$ for $r \neq s \in J_\delta$. Thus $u = x_\delta(t)u'$ and all root elements occurring in the decomposition of u' correspond to roots larger than r. Since the number of roots is finite, we conclude by induction that

$$U_{\boldsymbol{\alpha}}(k) = \prod_{\delta\in\Psi^+} X_\delta$$

where the ordering on the Ψ^+ is induced by the ordering on Φ^+.

We have now shown:

Theorem 3.4. *The relative root groups and root elements in $G_\alpha(k)$ satisfy the following properties:*

1. *For all $\delta \in \Psi$ and $t \in V_\delta$ we have $x_\delta(t) \in G_{\boldsymbol{\alpha}}(k)$.*
2. *If $2\delta \notin \Psi$, then X_δ is an abelian group isomorphic to the additive group of the vector space V_δ.*
3. *If $2\delta \in \Psi$, then X_δ is nilpotent of class 2, then $X_\delta = \{x_\delta(t)x_{2\delta}(s) \mid t \in V_\delta, s \in V_{2\delta}\}$, $X_{2\delta}$ is the centre of X_δ, and $X_\delta/X_{2\delta}$ is abelian.*
4. *$U_{\boldsymbol{\alpha}}(k) = \prod_{\delta\in\Psi^+} X_\delta$.*

Note that the relative root elements and relative root subgroups for negative relative roots can be constructed in a similar way.

Only one thing remains to finish our proof of part (2) of the Main Theorem. We need an algorithm for computing a solution $v_\delta(t) \in X_{2\delta}$ for the system of equations (7).

Recall the definition of $\lambda_{r,\gamma}$ from (5).

Lemma 3.5. *For any $\gamma \in \Gamma$ and any $s \in \Phi$, we have*

$$\prod_{j=1}^{|\gamma|-1} \lambda^{\gamma^{j-1}}_{s^{\boldsymbol{\alpha}_\gamma^{-j}},\gamma} = \lambda_{s,\gamma}^{-1}.$$

Proof. By induction we get for any $\gamma \in \Gamma$:

$$x_s(t_s)^{(\gamma\boldsymbol{\alpha}_\gamma)^{-|\gamma|}} = x_s\Big(\Big(\prod_{j=1}^{|\gamma|-1} \lambda^{\gamma^{j-1}}_{s^{\boldsymbol{\alpha}_\gamma^{-j}},\gamma}\Big)\lambda_{s,\gamma}t_s\Big).$$

On the other hand, $x_s(t_s)^{(\gamma\boldsymbol{\alpha}_\gamma)^{-|\gamma|}} = x_s(t_s)$. Now the lemma follows by comparing the coefficients. □

We can now give an algorithm for finding $v_\delta(t)$. Fix generators $\gamma_1, \ldots, \gamma_m$ for Γ. For $i := 1, \ldots, m$, write

$$c_{\delta\gamma_i}(t) := u_{2\delta}(c_i)$$

for $c_i \in V_{2\delta}$. So c_{ir} is the entry of the rth root element of $c_{\delta\gamma_i}(t)$ in the unique decomposition. Similarly write $v_\delta(t) = u_{2\delta}(v)$, where the v_r are to be found. Then

$$v_\delta(t)v_\delta(t)^{-\gamma\boldsymbol{\alpha}_\gamma} = \prod_{r\in\pi^{-1}(2\delta)} x_{r^{\boldsymbol{\alpha}_\gamma}}(v_{r^{\boldsymbol{\alpha}_\gamma}} - \lambda_{r\gamma}v_r^\gamma),$$

From the equations $c_{\delta\gamma_i}(t) = v_\delta(t)v_\delta(t)^{-\gamma_i\boldsymbol{\alpha}_{\gamma_i}}$ $(i = 1, \ldots, m)$ we obtain a system of equations over K:

$$c_{i,r^{\boldsymbol{\alpha}_{\gamma_i}}} = v_{r^{\boldsymbol{\alpha}_{\gamma_i}}} - \lambda_{r\gamma_i}v_r^{\gamma_i} \quad \text{for } r \in \pi^{-1}(2\delta),\ i = 1, \ldots, m. \tag{10}$$

Or equivalently

$$v_r = c_{i,r} + \lambda_{r^{\boldsymbol{\alpha}_{\gamma_i}^{-1}},\gamma_i} v^{\gamma_i}_{r^{\boldsymbol{\alpha}_{\gamma_i}^{-1}}} \quad \text{for } r \in \pi^{-1}(2\delta),\ i = 1, \ldots, m. \tag{11}$$

For each $s \in J_{2\delta}$, consider the subsystem of equations for $r \in \mathcal{O}_{\boldsymbol{\alpha}}(s)$. Then, applying (11) repeatedly starting with s, we get

$$\begin{aligned} v_s &= c_{i,s} + \lambda_{r^{\boldsymbol{\alpha}_{\gamma_i}^{-1}},\gamma_i} v^{\gamma_i}_{s^{\boldsymbol{\alpha}_{\gamma_i}^{-1}}} \\ &= c_{i,s} + \lambda_{s^{\boldsymbol{\alpha}_{\gamma_i}^{-1}},\gamma_i}(c_{i,s^{\boldsymbol{\alpha}_{\gamma_i}^{-1}}})^{\gamma_i} + \lambda_{s^{\boldsymbol{\alpha}_{\gamma_i}^{-1}},\gamma_i}\lambda^{\gamma_i}_{s^{\boldsymbol{\alpha}_{\gamma_i}^{-2}},\gamma_i}(c_{i,s^{\boldsymbol{\alpha}_{\gamma_i}^{-2}}})^{\gamma_i^2} + \cdots + \left(\prod_{j=1}^{|\gamma|-1} \lambda^{\gamma_i^{j-1}}_{s^{\boldsymbol{\alpha}_{\gamma_i}^{-j}},\gamma_i}\right) v_s^{\gamma_i^{-1}} \end{aligned}$$

Now we bring the last summand from the right hand side to the left hand side and replace the product in this summand by $\lambda_{s,\gamma_i}^{-1}$ using Lemma 3.5. What is left on the right hand side, we abbreviate by L_{is}. Note that it is known. We end up with

$$v_s - \lambda_{s,\gamma_i}^{-1} v_s^{\gamma_i^{-1}} = L_{is} \quad \text{for } s \in J_{2\delta},\ i = 1, \ldots, m \tag{12}$$

for each i and s. Our algorithm for finding $v_\delta(t)$ is:

1. Compute the constants L_{is} for each $i = 1, \ldots, m$ and $s \in J_{2\delta}$.
2. Solve the system of k-linear equations (12). We get a value v_s for each $s \in J_{2\delta}$.
3. Use Equation (11) to get v_r, $r \in \mathcal{O}_{\boldsymbol{\alpha}}(s)$ for each orbit representative s.

Note that we could have just solved the k-linear equations (10), but this method is more efficient.

This algorithm allows us to do more than just solve for $v_\delta(t)$ for a particular $t \in V_\delta$ however. Take E to be the polynomial ring over K with indeterminates t_r^γ and u_s^γ for $r \in J_\delta$, $s \in J_\epsilon$, $\gamma \in \Gamma$. Let Γ act on E in the obvious way, and call its elements Γ-*polynomials*. Then we can extend G and $\boldsymbol{\alpha}$ to E in Magma, and compute the solutions v_s above symbolically over E. So we have Γ-polynomials $v_r(t)$ such that

$$v_\delta(t) = \prod_{r\in\pi^{-1}(2\delta)} x_r(v_r(t)).$$

We have now computed parametrisations of the relative root subgroups, and so proved part (2) of the Main Theorem.

We can apply the same method to find commutator relations. Suppose that $\delta, \epsilon \in \Psi^+$. Then

$$x_\delta(t)x_\delta(u) = x_\delta(t+u)x_{2\delta}(f_\delta(t,u)), \text{ and} \tag{13}$$

$$[x_\delta(t), x_\epsilon(u)] = \prod x_{i\delta+j\epsilon}(g_{\delta\epsilon ij}(t,u)) \tag{14}$$

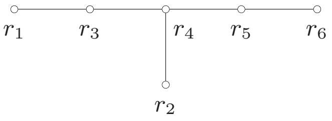
where i and j run over all nonegative positive integers, not both zero, such that $i\delta + j\epsilon$ is a relative root and the product is in the ordering described above. Here $f_\delta(t,u)$ and $g_{\delta\epsilon ij}(t,u)$ are Γ-polynomials, which are computed by collecting the roots elements in order of increasing height as in the proof of Theorem 3.4(4) given above. This finishes the proof of part (3) of the Main Theorem.

4. Important examples

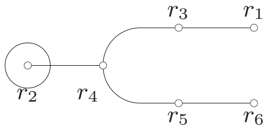
In this section, we present several important examples. We compute the subgroup generated by the root subgroups for twisted groups of Lie type ${}^2\mathrm{E}_{6,1}^{35}(k)$, ${}^3\mathrm{D}_{4,1}^{9}(k)$, and ${}^6\mathrm{D}_{4,1}^{9}(k)$. Another example ${}^2\mathrm{E}_{6,2}^{16'}$ is given in [HS05], including commutators between the two relative root subgroups.

In this section we assume that the characteristic of k is not 2.

4.1. **A twisted form of** E_6 **of rank 1:** ${}^2E_{6,1}^{35}(k)$**.** Let $\mathcal{R} = (X, \Phi, Y, \Phi^\star)$ be the adjoint root datum of type E_6 and $G(k) = \mathrm{E}_6(k)$ be given by the Steinberg presentation. Let Π be a fundamental system with the following Dynkin diagram:



Denote the highest root by r_*. We also use the notation $\substack{acdef\\b}$ for the root $ar_1+br_2+\cdots+fr_6$. In this section, we compute relative root elements and root subgroups for the twisted group of Lie type corresponding to the Tits index ${}^2E_{6,1}^{35}(k)$:



Note that 35 is the dimension of the anisotropic kernel of type A_5. This form is known not to exist over finite fields, over p-adic fields, or over $\mathbb{R}$. There are number fields k over which this form exists (see for example Selbach [Sel76]). We compute relative root subgroups of ${}^2E_{6,1}^{35}(k)$ as a subgroup of $\mathrm{E}_6(K)$, where K is a quadratic extension of k. Denote by γ the non-trivial automorphism in $\Gamma := \mathrm{Gal}(K\colon k)$.

4.1.1. *The cocycle.* First we compute a cocycle of Γ on $\mathrm{Aut}(G)$ defining a twisted form corresponding to the above index. As described in Section 2, this amounts to finding a Weyl group element w, such that τw has the needed action on Φ and Π, where τ is the non-trivial symmetry of $\mathcal{D}$. Recall the notation $\dot\tau$ from Section 2. Next we have to find a torus element h, such that

$$\boldsymbol{\alpha} := [\![\dot\tau\dot w h]\!]$$

is a cocycle.

We know from the Tits index that $\Pi_0 = \{r_1, r_3, \dots, r_6\}$ and Φ_0 is the subsystem of Φ spanned by Π_0 of type A_5. The longest word w for the subsystem Φ_0 has the required properties for the Γ-action on Φ. The orbits of Γ on Φ that sum up to 0 and those contained in Φ^+ are given by

$$\begin{aligned} \mathcal{O}_{\boldsymbol{\alpha}}(r) &= \{r, -r\} && \text{if } r \in \Phi_0, \\ \mathcal{O}_{\boldsymbol{\alpha}}(r_*) &= \{r_*\}, \\ \mathcal{O}_{\boldsymbol{\alpha}}(r) &= \{r, r_* - r\} && \text{if } r \in \Phi^+ \setminus \Phi_0 \text{ and } r \neq r^*. \end{aligned}$$

The relative root system $\Psi = \{\pm\delta, \pm 2\delta\}$ has type BC_1 with

$$\begin{aligned} \pi^{-1}(\delta) &= \dot{\bigcup_{r \in J_\delta}} \mathcal{O}_{\boldsymbol{\alpha}}(r), \\ \pi^{-1}(2\delta) &= \mathcal{O}_{\boldsymbol{\alpha}}(r_*) \end{aligned}$$

where $J_\delta = \{ \substack{00000\\1}, \substack{00100\\1}, \substack{01100\\1}, \substack{00110\\1}, \substack{11100\\1} \}$. We denote the elements of J_δ by $\beta_1, \dots, \beta_5$ and set $\beta_i := \beta_{i-5}^{\tau w}$ for $i = 6, \dots, 10$.

Now that we have the required action of Γ on Φ, we have to choose a torus element $h = \prod_{i=1}^{6} r_i^\star \otimes h_i$, where $h_i \in k^*$. For $\boldsymbol{\alpha}$ to be a cocycle, $\gamma\boldsymbol{\alpha}_\gamma$ must have order 2, which is true if, and only if,

$$h_1 h_2^2 h_3^2 h_4^3 h_5^2 h_6 = -1.$$

Hence h_1 is determined by $h_2, \dots, h_6$:

$$h_1 = -(h_2^2 h_3^2 h_4^3 h_5^2 h_6)^{-1}.$$

By construction, $\gamma\boldsymbol{\alpha}_\gamma$ leaves the subgroup $\mathrm{A}_5(K) := \langle X_r(K) \mid r \in \Phi_0 \rangle$ of $G(K)$ invariant and the restriction of the action to this subgroup is also an algebraic automorphism defining a cocycle.

Further we assume the existence of $h_1, h_2, h_3, \dots, h_6 \in k^*$, such that the group $(\mathrm{A}_5)_{\boldsymbol{\alpha}}(k)$ is an anisotropic twisted group of Lie type. Basically, this means that the standard representation of the torus element $\prod_i r_i^\star \otimes h_i$ in $\mathrm{SL}_6(K)$ defines an anisotropic unitary form q on K^6 and $(\mathrm{A}_5)_{\boldsymbol{\alpha}}(k) \simeq \mathrm{SU}_6(k, q)$.

4.1.2. *Relative root elements.* We use methods from Section 3. By (4), we have

$$x_{2\delta}(t) = u_{2\delta}(t) = x_{r_*}(t_{r_*} - t_{r_*}^\gamma).$$

For the root δ, we first define $u_\delta(t)$ as in Equation (4) and $c_{\delta\gamma}(t)$ can be computed, but we omit the details. To compute $v_\delta(t)$, we introduce constants

$$c_r = \prod_{i=1}^{6} s_i^{\langle r, r_i^\star \rangle} \in k^*.$$

Then for $t \in K$:

$$\begin{aligned} x_r(t)^{\boldsymbol{\alpha}_\gamma} &= x_{r^{\tau w}}(N_{r, r^{\tau w}} c_r t), \\ x_{r_*}(t)^{\boldsymbol{\alpha}_\gamma} &= x_{r_*}(c_{r_*} \cdot t), \end{aligned}$$

where $N_{r, r^{\tau w}}$ is the structure constant defined in [CMT04]. We introduce a k-valued bilinear form $g : V_\delta \times V_\delta \to k$:

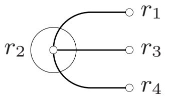
$$g(t, u) := \sum_{i=1}^{10} c_{\beta_i} t_{\beta_i} u_{\beta_i}^\gamma.$$

Since the characteristic is not 2, a solution $v_\delta(t)$ for the equation (7) is

$$v_\delta(t) = x_{r_*}(-\tfrac{1}{2}g(t,t))$$

and the relative root element is $x_\delta(t) = u_\delta(t)v_\delta(t)$. The commutator relation (13) has been computed but is too long to state here.

4.2. **The groups ${}^3\mathrm{D}^9_{4,1}(k)$ and ${}^6\mathrm{D}^9_{4,1}(k)$.** Let $\mathcal{R} = (X, \Phi, Y, \Phi^\star)$ be the adjoint root datum of type D_4. In this section, we compute the root elements of the twisted groups of Lie type corresponding to the Tits diagrams ${}^3\mathrm{D}^9_{4,1}$ and ${}^6\mathrm{D}^9_{4,1}$, both corresponding to the following figure:



Both of these groups were of recent interest, see for example [PRS04].

We start by computing the relative root systems and the root orbits under the actions of Γ on Φ and Π as described in Section 2. We use the notation of that section and denote the highest root by r_*.

The group of all its symmetries of the Dynkin diagram is $D = \langle \tau_3, \tau_2 \rangle$, where $\tau_3 = (r_1, r_3, r_4)$ and $\tau_2 = (r_3, r_4)$. Recall the notation $\dot\tau$ from Section 2.

4.2.1. *Type* ${}^3\mathrm{D}^9_{4,1}$. If Γ has order 3, then there is no cocycle in $Z^1(\Gamma, DW)$ with the properties

$$\mathcal{O}_{\boldsymbol\alpha}(r_2) \subset \Phi^+,$$
$$\sum_{\gamma\in\Gamma} r_i^\gamma = 0 \text{ for } i = 1, 3, 4.$$

The smallest possible field extension, for which such a cocycle exists, has cyclic Galois group of order 6, which we consider in the following construction. Let $\Gamma = \langle \gamma \rangle$.

Then the cocycle $\boldsymbol\alpha = [\![\tau_3 s_1 s_3 s_4]\!]$ admits the above Tits index. The Γ-orbits are:

$$\begin{aligned}
\mathcal{O}_{\boldsymbol\alpha}(r_1) &= \{\pm r_1, \pm r_3, \pm r_4\},\\
\mathcal{O}_{\boldsymbol\alpha}(r_2) &= \{r_2, r_1 + r_2 + r_3 + r_4\},\\
\mathcal{O}_{\boldsymbol\alpha}(r_1 + r_2) &= \{r_2 + r_1, r_2 + r_3, r_2 + r_4,\\
&\qquad r_2 + r_1 + r_3, r_2 + r_2 + r_4, r_2 + r_3 + r_4\},\\
\mathcal{O}_{\boldsymbol\alpha}(r_*) &= \{r_*\}.
\end{aligned}$$

The $[\Gamma]$-orbits are:

$$\begin{aligned}
[\mathcal{O}]_{\boldsymbol\alpha}(r_1) &= \{r_1, r_3, r_4\},\\
[\mathcal{O}]_{\boldsymbol\alpha}(r_2) &= \{r_2\},
\end{aligned}$$

of which only the latter is distinguished. We have

$$X_0 = \langle r_1, r_3, r_4 \rangle, \quad \Pi_0 = \{r_1, r_3, r_4\}, \quad \Phi_0 = \{\pm r_1, \pm r_3, \pm r_4\}.$$

Let $\delta = \pi(r_1)$. The relative root system is $\Psi = \{\pm\delta, \pm 2\delta\}$ of type BC_1 with the fundamental system $\Delta = \{\delta\}$. We set $J_\delta = \{r_*\}$ and $J_{2\delta} = \{r_2, r_1 + r_2\}$. Let $r_5 := r_1 + r_2$.

The $[\Gamma]$-action is not faithful. The kernel of the action is $\langle \gamma^2 \rangle$ and the order of the quotient is 3. The anisotropic kernel has type $\mathrm{A}_1\mathrm{A}_1\mathrm{A}_1$ and so its dimension is 9. Thus the index is of type ${}^3\mathrm{D}^9_{4,1}$.

The cocycle $\boldsymbol{\alpha} \in Z^1(\Gamma, N_A(T))$ now has the form $[\![\dot\tau_3 \dot w h]\!]$, where $w = s_1 s_3 s_4$ and h is conjugation by a torus element. The torus element $\prod_{i\in\{1,3,4\}} r_1^\star \otimes (-1)$ makes $\boldsymbol{\alpha}$ is a cocycle. By (4), we have

$$x_{2\delta}(t) = u_{2\delta}(t) = x_{r_*}(t_{r_*} - t_{r_*}^{\gamma} + t_{r_*}^{\gamma^2} - t_{r_*}^{\gamma^3} + t_{r_*}^{\gamma^4} - t_{r_*}^{\gamma^5}).$$

For the root δ, we first compute

$$c_{\delta\gamma}(t) = x_{r_*}(t_{r_2} t_{r_2}^{\gamma} + t_{r_2} t_{r_2}^{\gamma^3} + t_{r_2} t_{r_2}^{\gamma^5} - t_{r_5} t_{r_5}^{\gamma^3})$$

for t as in (4). In characteristic not 2, a solution $v_\delta(t)$ for the equation (7) is

$$\begin{aligned} v_\delta(t) = x_{r_*}\Bigg(\tfrac{1}{2}\Big(\sum_{i=0}^{2} (-1)^i (t_{r_2} t_{r_2}^{\gamma^3})^{\gamma^i} - \sum_{i=0}^{2} (-1)^i (t_{r_5} t_{r_5}^{\gamma^3})^{\gamma^i} \\ + \sum_{i=0}^{4} (-1)^i (t_{r_2} t_{r_2}^{\gamma})^{\gamma^i} + t_{r_2} t_{r_2}^{\gamma^5} \Big) \Bigg) \end{aligned}$$

and the relative root element is

$$x_\delta(t) = u_\delta(t) v_\delta(t).$$

Finally the commutator relation (13) holds with the Γ-polynomial

$$f_\delta(t,u) := -t_{01}^{\gamma} u_{01} - t_{11}^{\gamma} u_{11}^{\gamma^4} + t_{11}^{\gamma^3} u_{11} - t_{11}^{\gamma^5} u_{11}^{\gamma^2}.$$

where $t = t_{01} r_2 + t_{11}(r_1 + r_2)$ and $u = u_{01} r_2 + u_{11}(r_1 + r_2)$.

4.2.2. *Type* ${}^6\mathrm{D}^9_{4,1}$. Consider a Galois extension K of k with Galois group isomorphic to Σ_3 and generators γ_3, γ_2 of orders 3 and 2 respectively. Then the cocycle $\boldsymbol{\alpha} = [\![\tau_3, \tau_2 s_1 s_3 s_4]\!]$ admits the above Tits index. The Γ- and $[\Gamma]$-orbits are the same as in the case of ${}^3\mathrm{D}^9_{4,1}$, as are X_0, Π_0, and Φ_0. The relative root system is $\Psi = \{\pm\delta, \pm 2\delta\}$ of type BC_1 with the fundamental system $\Delta = \{\delta\}$. We set $J_\delta = \{r_*\}$ and $J_{2\delta} = \{r_2, r_5\}$, as above.

This time the $[\Gamma]$-action is faithful, thus the index is of type ${}^6\mathrm{D}^9_{4,1}$.

The cocycle $\boldsymbol{\alpha} \in Z^1(\Gamma, N_A(T))$ now has the form $[\![\dot\tau_3 h, \dot\tau_2 n_1 n_3 n_4 h']\!]$, where h and h' are conjugations by torus elements. The torus elements $h = 1$ and $h' = \prod_{i\in\{1,3,4\}} r_i^\star \otimes (-1)$ make $\boldsymbol{\alpha}$ a cocycle. By (4) and (8), we have

$$x_{2\delta}(t) = u_{2\delta}(t) = x_{r_*}(t_* - t_*^{\gamma_2} - t_*^{\gamma_2\gamma_3} - t_*^{\gamma_3\gamma_2} + t_*^{\gamma_3} + t_*^{\gamma_3\gamma_3}).$$

where $t = t_* r_* \in V_{2\delta}$. For the root δ, we first compute

$$\begin{aligned} c_{\delta\gamma_2}(t) = x_{r_*}(& t_{r_2} t_{r_2}^{\gamma_2} - t_{r_2}^{\gamma_2\gamma_3} t_{r_2}^{\gamma_3} - t_{r_2}^{\gamma_2\gamma_3} t_{r_2}^{\gamma_3\gamma_3} - t_{r_2}^{\gamma_3\gamma_2} t_{r_2}^{\gamma_3} \\ & - t_{r_2}^{\gamma_3\gamma_2} t_{r_2}^{\gamma_3\gamma_3} - t_{r_5} t_{r_5}^{\gamma_2} + t_{r_5}^{\gamma_2\gamma_3} t_{r_5}^{\gamma_3} + t_{r_5}^{\gamma_3\gamma_2} t_{r_5}^{\gamma_3\gamma_3}), \\ c_{\delta\gamma_3}(t) = x_{r_*}(& t_{r_2} t_{r_2}^{\gamma_2} + t_{r_2} t_{r_2}^{\gamma_2\gamma_3} + t_{r_2} t_{r_2}^{\gamma_3\gamma_2} - t_{r_2}^{\gamma_2} t_{r_2}^{\gamma_3} - t_{r_2}^{\gamma_2\gamma_3} t_{r_2}^{\gamma_3} \\ & - t_{r_2}^{\gamma_3\gamma_2} t_{r_2}^{\gamma_3} - t_{r_5} t_{r_5}^{\gamma_2} + t_{r_5}^{\gamma_2\gamma_3} t_{r_5}^{\gamma_3}), \end{aligned}$$

for t as in (4). In characteristic not 2, a simultaneous solution $v_\delta(t)$ for the equation system

$$c_{\delta\gamma_2}(t) = v_\delta(t) v_\delta(t)^{-\gamma_2 \boldsymbol{\alpha}_{\gamma_2}}, \qquad c_{\delta\gamma_3}(t) = v_\delta(t) v_\delta(t)^{-\gamma_3 \boldsymbol{\alpha}_{\gamma_3}}$$

is

$$v_\delta(t) = x_{r_*}\Big(\tfrac{1}{2}\big(a - t_{r_2}^{\gamma_2} t_{r_2}^{\gamma_3^2} - t_{r_2}^{\gamma_2\gamma_3} t_{r_2}^{\gamma_3^2} - t_{r_2}^{\gamma_3\gamma_2} t_{r_2}^{\gamma_3^2} + t_{r_5}^{\gamma_3\gamma_2} t_{r_5}^{\gamma_3^2}\big)\Big),$$

where a is the field element occurring in $c_{\gamma_3}(t)$, and the relative root element is

$$x_\delta(t) = u_\delta(t)v_\delta(t).$$

References

[BC97] Wieb W. Bosma and J.J. Cannon, *The Magma Computational Algebra System*, Tech. report, School of Mathematics and Statistics, University of Sydney, 1997, `http://magma.maths.usyd.edu.au/`.

[BM92] Michel Broué and Gunter Malle, *Théorèmes de Sylow génériques pour les groupes réductifs sur les corps finis*, Math. Ann. **292** (1992), no. 2, 241–262.

[BT65] Armand Borel and Jacques Tits, *Groupes réductifs*, Inst. Hautes Études Sci. Publ. Math. (1965), no. 27, 55–150.

[CHM08] Arjeh M. Cohen, Sergei Haller, and Scott H. Murray, *Computing in unipotent and reductive algebraic groups*, LMS J. Comput. Math. **11** (2008), 343–366.

[CMT04] Arjeh M. Cohen, Scott H. Murray, and D. E. Taylor, *Computing in groups of Lie type*, Math. Comp. **73** (2004), 1477–1498.

[Dem65] M. Demazure, *Données radicielles*, Schémas en Groupes (Sém. Géométrie Algébrique, Inst. Hautes Études Sci., 1964), Fasc. 6, Exposé 21, Inst. Hautes Études Sci., Paris, 1965.

[FdG08] Claus Fieker and Willem de Graaf, *Constructing algebraic lie algebras*, Preprint, 2008.

[Hal05] Sergei Haller, *Computing Galois cohomology and forms of linear algebraic groups*, Dissertation, Technische Universiteit Eindhoven, Eindhoven, 2005.

[Hol85] D. F. Holt, *The mechanical computation of first and second cohomology groups*, J. Symbolic Comput. **1** (1985), no. 4, 351–361.

[HS05] Sergei Haller and Anja Steinbach, *An implementation of the root subgroups of an E_6-quadrangle in the Chevalley group $E_6(E)$*, Mitt. Math. Sem. Giessen (2005), no. 255, 65–79.

[PRS04] Gopal Prasad, Louis Rowen, and Yoav Segev, *Normal subgroups of Quaternion algebras and the Whitehead group of algebraic gtoups of type ${}^{3,6}D_4$*, Preprint, 2004.

[Sat71] I. Satake, *Classification theory of semi-simple algebraic groups*, Marcel Dekker Inc., New York, 1971, With an appendix by M. Sugiura, Notes prepared by Doris Schattschneider, Lecture Notes in Pure and Applied Mathematics, 3.

[Sch69] Doris J. Schattschneider, *On restricted roots of semi-simple algebraic groups*, J. Math. Soc. Japan **21** (1969), 94–115.

[Sel76] Martin Selbach, *Klassifikationstheorie halbeinfacher algebraischer Gruppen*, Mathematisches Institut der Universität Bonn, Bonn, 1976, Diplomarbeit, Univ. Bonn, Bonn, 1973, Bonner Mathematische Schriften, Nr. 83.

[Ser02] Jean-Pierre Serre, *Galois cohomology*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002.

[Spr98] Tonny A. Springer, *Linear algebraic groups*, Progress in Mathematics, vol. 9, Birkhäuser Boston Inc., Boston, MA, 1998.

[Tit66] Jacques Tits, *Classification of algebraic semisimple groups*, Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965), Amer. Math. Soc., Providence, R.I., 1966, pp. 33–62.

Department of Mathematics and Computer Science, Eindhoven University of Technology, PO Box 513, 5600 MB Eindhoven, Netherlands
E-mail address: `A.M.Cohen@tue.nl`

btexx business technologies GmbH, Rheinstrasse 4N, 55116 Mainz, Germany
E-mail address: `sergei@sergei-haller.de`

School of Mathematics and Statistics F07, Faculty of Science, University of Sydney, NSW 2006, Australia
E-mail address: `murray@maths.usyd.edu.au`