Computing Galois cohomology and forms of linear algebraic groups

Proefschrift

Sergei Haller

CIP-DATA LIBRARY TECHNISCHE UNIVERSITEIT EINDHOVEN

Haller, Sergei

Computing Galois cohomology and forms of linear algebraic groups /
Haller, Sergei – Eindhoven: Technische Universiteit Eindhoven, 2005.
Proefschrift – ISBN 90-386-0664-8

NUR 921

Subject headings : group theory / linear algebraic groups / cohomology /
computer algebra
2000 Mathematics Subject Classification: 20G15, 20G40, 11E72, 20G10, 20J06.

Printed by Universiteitsdrukkerij Technische Universiteit Eindhoven
Cover by Jan-Willem Luiten, JWL Producties

Computing Galois cohomology and forms of linear algebraic groups

Proefschrift

ter verkrijging van de graad van doctor aan de Technische Universiteit Eindhoven, op gezag van de Rector Magnificus, prof.dr.ir. C.J. van Duijn, voor een commissie aangewezen door het College voor Promoties in het openbaar te verdedigen op woensdag 12 oktober 2005 om 16.00 uur

door

Sergei Haller

geboren te Krasnoturinsk, Rusland

Dit proefschrift is goedgekeurd door de promotoren:

prof.dr. A.M. Cohen
en
prof. Dr. F.G. Timmesfeld

Contents

Notation

Here, we describe some common notation used throughout this work. Given elements g and h of the group G, we write

$$g^h := h^{-1}gh \quad \text{and} \quad {}^h g := hgh^{-1}$$

for right and left conjugation. For a subgroup H of G, we write $C_G(H)$ for the centralizer of H in G, $N_G(H)$ for normalizer of H in G, and $Z(G)$ for the center of G.

For a given field k, we denote its multiplicative group by k^*. $\mathrm{M}_n(k)$ is the set of all $n \times n$ matrices with entries in k. We denote the algebraic and separable closures of k by $\bar{k}$ and k_{sep}, respectively.

We finish complete proofs with $\square$ and incomplete proofs with $\blacksquare$. In the latter case, a reference to a complete proof is given. Known results are indicated as such by giving a reference after the statement.

Chapter 1

Introduction

Computations with large finite or infinite groups are usually very tedious and time consuming. In many cases the computations carried out are very mechanical and error prone when carried out by hand. Such computations can often be carried out more easily by computer. For more complicated tasks one needs to design and implement new algorithms. For groups in particular, this includes operations with group elements (multiplication, inversion, conjugation, etc.) or other important properties (subgroup structure, conjugacy classes, etc.). The first problem is deciding how elements should be represented in the computer. Often a group is defined *intrinsically*, that is, defined implicitly by requiring some properties on the elements (e.g., the fixed point subgroup of another group). For computations with group elements, such a definition is not very useful, since it provides no group elements other than the identity. In such cases one needs an *extrinsic* definition for the group, such as a presentation or a matrix representation.

We design and implement algorithms for computation with groups of Lie type. Algorithms for element arithmetic in the Steinberg presentation of untwisted groups of Lie type, and for conversion between this presentation and linear representations, were given in [12] (building on work of [15] and [26]). We extend this work to twisted groups, including groups that are not quasisplit.

A twisted group of Lie type is the group of rational points of a twisted form of a reductive linear algebraic group. These forms are classified by Galois cohomology. In order to compute the Galois cohomology, we develop a method for computing the cohomology of a finitely presented group Γ on a finite group A. This method is of interest in its own right. We then extend this method to the Galois cohomology of reductive linear algebraic groups.

Let G be a reductive linear algebraic group defined over a field k. A twisted group of Lie type $G_{\boldsymbol{\alpha}}(k)$ is uniquely determined by the cocycle $\boldsymbol{\alpha}$ of the Galois group of K on $A := \mathrm{Aut}_K(G)$, the group of K-algebraic automorphisms where

K is a finite Galois extension of k. We give algorithms for computing the relative root system of $G_{\boldsymbol{\alpha}}(k)$, the root subgroups, and the root elements, as well as algorithms for the computing of relations between root elements. This enables us to compute inside the normal subgroup $G_{\boldsymbol{\alpha}}(k)^{\dagger}$ of $G_{\boldsymbol{\alpha}}(k)$ generated by the root elements. We apply our algorithms to several examples, including ${}^{2}\mathrm{E}_{6,1}(k)$ and ${}^{3,6}\mathrm{D}_{4,1}(k)$. In this application, the field k need not be specified, one only needs to assume some properties of k.

As an application, we develop an algorithm for computing all twisted maximal tori of a finite group of Lie type. The order of such a torus is computed as a polynomial in q, the order of the field k. We also compute the orders of the factors in a decomposition of the torus as a direct product of cyclic subgroups. For a given field k, we compute the maximal tori of $G_{\boldsymbol{\beta}}(k)$ as subgroups of $G_{\boldsymbol{\beta}}(K)$ over some extension field K, and then use the effective version of Lang's Theorem [11] to conjugate the torus to a k-torus, which is a subgroup of $G_{\boldsymbol{\beta}}(k)$.

Using this information on the maximal tori, we provide an algorithm for computing all Sylow subgroups of a finite group of Lie type. If p is not the characteristic of the field, the Sylow subgroup is computed as a subgroup of the normaliser of a k-torus.

All algorithms presented here have been implemented by the author in MAGMA [5].

Chapter 2

Nonabelian cohomology of finite groups

We are primarily interested in the twisted forms of linear algebraic groups, which are classified via the Galois cohomology. In the present chapter, we introduce the first cohomology of nonabelian groups and develop a new technique for computing cohomology $H^1(\Gamma, A)$ for a finitely presented group Γ and a finite group A. In Chapter 3, we extend this technique to Galois cohomology. We also introduce the concept of twisting in Section 2.3.

2.1 Definitions and first properties

Let Γ be a group. A Γ-*set* A is a set with a (right) Γ-action. If A is a group and Γ acts by group automorphisms, then A is called a Γ-*group*. A subset (subgroup) of the Γ-set (Γ-group) A that is normalised by the action of Γ, is called a Γ-*subset* (Γ-*subgroup*) of A. Given a Γ-set A, define

$$H^0(\Gamma, A) := \{a \in A \mid a^\sigma = a \text{ for all } \sigma \in \Gamma\}.$$

If A is a Γ-group, then $H^0(\Gamma, A)$ is a subgroup of A.

Now let A be a Γ-group. A 1-*cocycle of* Γ *on* A is a map

$$\boldsymbol{\alpha} : \Gamma \to A, \quad \sigma \mapsto \boldsymbol{\alpha}_\sigma,$$

such that

$$\boldsymbol{\alpha}_{\sigma\tau} = (\boldsymbol{\alpha}_\sigma)^\tau \boldsymbol{\alpha}_\tau \qquad \text{for all } \sigma, \tau \in \Gamma. \tag{2.1}$$

We denote by $Z^1(\Gamma, A)$ the set of all 1-cocycles of Γ on A. The constant map $\mathbf{1} : \sigma \mapsto 1$ is a distinguished element of $Z^1(\Gamma, A)$, called the *trivial* 1-*cocycle*.

Applying (2.1) to $\boldsymbol{\alpha}_{\sigma\cdot 1}$ and $\boldsymbol{\alpha}_{\sigma\sigma^{-1}}$ respectively, we immediately obtain the following important properties:

$$\boldsymbol{\alpha}_1 = 1, \tag{2.2}$$
$$\boldsymbol{\alpha}_{\sigma^{-1}} = (\boldsymbol{\alpha}_\sigma)^{-\sigma^{-1}} \quad \text{for all } \sigma \in \Gamma. \tag{2.3}$$

Given a 1-cocycle $\boldsymbol{\alpha} \in Z^1(\Gamma, A)$ and an element $a \in A$, the map

$$\boldsymbol{\beta} : \Gamma \to A, \qquad \sigma \mapsto \boldsymbol{\beta}_\sigma := a^{-\sigma} \cdot \boldsymbol{\alpha}_\sigma \cdot a \tag{2.4}$$

is also in $Z^1(\Gamma, A)$, since

$$\begin{aligned}\boldsymbol{\beta}_{\sigma\tau} &= a^{-\sigma\tau}\boldsymbol{\alpha}_{\sigma\tau}a = a^{-\sigma\tau}(\boldsymbol{\alpha}_\sigma)^\tau\boldsymbol{\alpha}_\tau a \\ &= (a^{-\sigma}\boldsymbol{\alpha}_\sigma a)^\tau(a^{-\tau}\boldsymbol{\alpha}_\tau a) = (\boldsymbol{\beta}_\sigma)^\tau\boldsymbol{\beta}_\tau.\end{aligned}$$

If there exists $a \in A$ such that $\boldsymbol{\beta}_\sigma = a^{-\sigma} \cdot \boldsymbol{\alpha}_\sigma \cdot a$ for all $\sigma \in \Gamma$, we write $\boldsymbol{\beta} \sim \boldsymbol{\alpha}$. We call $\boldsymbol{\beta}$ and $\boldsymbol{\alpha}$ *cohomologous with respect to* a, and denote $\boldsymbol{\beta}$ by $\boldsymbol{\alpha}^{(a)}$. A 1-cocycle cohomologous to the trivial cocycle is called a *coboundary*. Note that $\sim$ is an equivalence relation. We denote the equivalence class of $\boldsymbol{\alpha}$ by $[\boldsymbol{\alpha}]$ and the set of equivalence classes of 1-cocycles by $H^1(\Gamma, A)$. A *pointed set* is a set with a distinguished element. Both $Z^1(\Gamma, A)$ and $H^1(\Gamma, A)$ are pointed sets with distinguished elements being the trivial cocycle and the class of coboundaries, respectively. If A is abelian, then $Z^1(\Gamma, A)$ and $H^1(\Gamma, A)$ are groups and agree with the usual definition of group cohomology (see, for example, [1]). In general, however, $Z^1(\Gamma, A)$ and $H^1(\Gamma, A)$ do not have a group structure.

Given two cohomologous cocycles $\boldsymbol{\alpha}, \boldsymbol{\beta} \in Z^1(\Gamma, A)$, it is a non-trivial problem to find the intertwining element $a \in A$ such that $\boldsymbol{\beta} = \boldsymbol{\alpha}^{(a)}$. For example, if $\Gamma = \langle\sigma\rangle$ is cyclic and $\boldsymbol{\alpha} = \mathbf{1}$, it amounts to solving

$$\boldsymbol{\beta}_\sigma = a^{-\sigma} \cdot \mathbf{1}_\sigma \cdot a = a^{-\sigma} \cdot a \quad \text{for } a \in A.$$

For connected algebraic groups over finite fields, Lang's Theorem (Theorem 3.17) gives a nonconstructive proof of the existence of a solution (in other words, it shows that the cohomology is trivial). Solving this equation constructively for reductive groups is addressed in [11].

In order to compute the first cohomology more efficiently (Section 2.6), we sometimes use the second cohomology of abelian groups. Let A be an abelian Γ-group. Then a map $\boldsymbol{\alpha} : \Gamma \times \Gamma \to A$ satisfying

$$\boldsymbol{\alpha}_{\sigma\tau,\rho}\boldsymbol{\alpha}^\rho_{\sigma,\tau} = \boldsymbol{\alpha}_{\sigma,\tau\rho}\boldsymbol{\alpha}_{\tau,\rho} \quad \text{for all } \sigma, \tau, \rho \in \Gamma \tag{2.5}$$

is called a 2-*cocycle*. The set of all 2-cocycles is denoted by $Z^2(\Gamma, A)$. Two 2-cocycles $\boldsymbol{\alpha}, \boldsymbol{\beta} \in Z^2(\Gamma, A)$ are called *cohomologous* if there is a map $\varphi : \Gamma \mapsto A$ satisfying

$$\boldsymbol{\beta}_{\sigma,\tau} = \boldsymbol{\alpha}_{\sigma,\tau}\varphi^\tau_\sigma\varphi_\tau\varphi^{-1}_{\sigma\tau} \quad \text{for all } \sigma, \tau \in \Gamma. \tag{2.6}$$

This is an equivalence relation, whose set of equivalence classes is denoted $H^2(\Gamma, A)$. Once again, there is a trivial 2-cocycle, denoted $\mathbf{1}$.

Let M, N be two pointed sets. A map $\varphi : M \to N$ is called a *morphism of pointed sets* if it maps the distinguished element of M to the distinguished element of N. Let A and B be Γ-groups and let $\phi : A \to B$ be a group homomorphism. We call ϕ a Γ*-homomorphism* if it respects the Γ-action, i.e.,

$$(a^\sigma)^\phi = \left(a^\phi\right)^\sigma \qquad \text{for all } \sigma \in \Gamma \text{ and } a \in A.$$

If $\phi : A \to B$ is a Γ-homomorphism, it is immediate from the definitions that there are induced maps

$$\begin{aligned} \phi^i &: Z^i(\Gamma, A) \to Z^i(\Gamma, B) \qquad && (i = 1), \\ \phi^i &: H^i(\Gamma, A) \to H^i(\Gamma, B) \qquad && (i = 0, 1). \end{aligned}$$

Note that we use the same name ϕ^1 for the maps $Z^1(\Gamma, A) \to Z^1(\Gamma, B)$ and $H^1(\Gamma, A) \to H^1(\Gamma, B)$, since it is obvious from context which one is intended. Moreover, ϕ^0 is a group homomorphism and ϕ^1 is a morphism of pointed sets. If A and B are abelian Γ-groups, there are also induced maps ϕ^2, and the maps ϕ^1 and ϕ^2 are group homomorphisms. If $\psi : B \to C$ is another Γ-homomorphism, then the *functorial property*

$$(\phi\psi)^i = \phi^i \psi^i$$

holds for all $i = 0, 1, 2$ whenever the maps are defined.

2.2 Finitely presented groups

A 1-cocycle $\boldsymbol{\alpha} \in Z^1(\Gamma, A)$ is uniquely determined by the images of a fixed set of generators of Γ, since it can be extended by properties (2.1) and (2.3) to all elements of Γ. In other words, if $\Gamma = \langle \gamma_1, \ldots, \gamma_k \rangle$, then the cocycle $\boldsymbol{\alpha} \in Z^1(\Gamma, A)$ is uniquely determined by the map $f = \boldsymbol{\alpha}|_{\{\gamma_1, \ldots, \gamma_k\}}$. Note that an arbitrary map $f : \{\gamma_1, \ldots, \gamma_k\} \to A$ does not always define a valid cocycle, but the following theorem provides a necessary and sufficient condition in case Γ is a finitely presented group.

Let Γ be a finitely-presented group with generators $\gamma_1, \ldots, \gamma_k$ and relators $r_1, \ldots, r_\ell$. Let F be the free group on the letters $x_1, \ldots, x_k$. Let $\mu : F \to \Gamma$ be the universal epimorphism with $\mu(x_i) = \gamma_i$. Then Γ is identified with F/N where $N := \ker \mu = \langle r_j^F \mid j = 1, \ldots, \ell \rangle$. Note that A is also an F-group with the action induced by μ and, in this case, every map $f : \{x_1, \ldots, x_k\} \to A$ defines a cocycle in $Z^1(F, A)$.

2.1 Theorem (Recognizing 1-cocycles).
Let Γ be a finitely-presented group with generators $\gamma_1, \ldots, \gamma_k$ and relators

$r_1, \ldots, r_\ell$. Let F be the free group on the letters $x_1, \ldots, x_k$. Let $\mu : F \to \Gamma$ be the universal epimorphism with $\mu(x_i) = \gamma_i$ and let $N = \ker \mu$. Let A be a Γ-group. Choose arbitrary $a_1, \ldots, a_k \in A$ and let $\boldsymbol{\beta}$ be the cocycle in $Z^1(F, A)$ defined by the map $x_i \mapsto a_i$. Then the map $\gamma_i \mapsto a_i$ defines a cocycle in $Z^1(\Gamma, A)$ if, and only if, $\boldsymbol{\beta}_{r_j} = 1$ for $j = 1, \ldots, \ell$.

Proof. First, since A is a Γ-group, it is also an F-group with the action induced by μ and $\boldsymbol{\beta}$ is a cocycle in $Z^1(F, A)$.

If $\boldsymbol{\alpha}$ is a cocycle of Γ on A with $\boldsymbol{\alpha}_{\gamma_i} = a_i$, then $\boldsymbol{\beta}_{r_j} = \boldsymbol{\alpha}_{\mu(r_j)} = \boldsymbol{\alpha}_1 = 1$ for $j = 1, \ldots, \ell$.

Conversely assume that $\boldsymbol{\beta}_{r_j} = 1$ for $j = 1, \ldots, \ell$. First we show that $\boldsymbol{\beta}_n = 1$ for all $n \in N$. Let $1 \neq n \in N$. Then $n = \prod_{i=1}^{m} r_{j_i}^{y_i}$ for some $m \in \mathbb{N}$, $j_i \in \{1, \ldots, \ell\}$ and $y_i \in F$. In the case $m = 1$, we have

$$\boldsymbol{\beta}_n = \boldsymbol{\beta}_{y^{-1} r_j y} = \boldsymbol{\beta}_{y^{-1}}^{r_j y} \boldsymbol{\beta}_{r_j}^{y} \boldsymbol{\beta}_y = \boldsymbol{\beta}_{y^{-1}}^{\mu(r_j) y} \boldsymbol{\beta}_y = \boldsymbol{\beta}_{y^{-1}}^{y} \boldsymbol{\beta}_y = \boldsymbol{\beta}_{y^{-1} y} = 1.$$

Otherwise, let $y := y_m$ and $j := j_m$, so that

$$\boldsymbol{\beta}_n = \boldsymbol{\beta}_{n' r_j^y} = \boldsymbol{\beta}_{n'}^{r_j^y} \boldsymbol{\beta}_{r_j^y} = 1$$

with $n' = \prod_{i=1}^{m-1} r_{j_i}^{y_i}$ by induction.

Now let $x, y \in F$ with $\mu(x) = \mu(y)$. Then $x = ny$ for some $n \in N$. Hence

$$\boldsymbol{\beta}_x = \boldsymbol{\beta}_{ny} = \boldsymbol{\beta}_n^y \boldsymbol{\beta}_y = \boldsymbol{\beta}_y$$

and the following map is well defined:

$$\boldsymbol{\rho} : \Gamma \to A; \quad \boldsymbol{\rho}_\gamma := \boldsymbol{\beta}_x \quad \text{for some } x \in \mu^{-1}(\gamma).$$

Now $\boldsymbol{\rho}_1 = \boldsymbol{\beta}_1 = 1$ and for $\sigma, \tau \in \Gamma$ and $x \in \mu^{-1}(\sigma)$, $y \in \mu^{-1}(\tau)$ we have:

$$\boldsymbol{\rho}_{\sigma\tau} = \boldsymbol{\beta}_{xy} = \boldsymbol{\beta}_x^y \boldsymbol{\beta}_y = \boldsymbol{\rho}_\sigma^y \boldsymbol{\rho}_\tau = \boldsymbol{\rho}_\sigma^{\mu(y)} \boldsymbol{\rho}_\tau = \boldsymbol{\rho}_\sigma^\tau \boldsymbol{\rho}_\tau.$$

This shows that $\boldsymbol{\rho}$ is a cocycle in $Z^1(\Gamma, A)$ with $\boldsymbol{\rho}_{\gamma_i} = \boldsymbol{\beta}_{x_i} = a_i$. $\square$

Let A be a Γ-group with a finitely presented group Γ and a fixed set $\gamma_1, \ldots, \gamma_k$ of generators of Γ. If a map $\gamma_i \mapsto a_i$ defines a valid cocycle, we denote this cocycle by $[\![a_1, \ldots, a_n]\!]$.

2.3 Twisted forms

In this section, we introduce twisting by a cocycle and twisted forms. Let B be a Γ-set, and let A be a Γ-group with an action on B that commutes with the action of Γ, i.e.,

$$(b^a)^\sigma = (b^\sigma)^{a^\sigma} \quad \text{for all } b \in B,\ a \in A,\ \sigma \in \Gamma.$$

Now fix an arbitrary 1-cocycle $\boldsymbol{\alpha} \in Z^1(\Gamma, A)$ and define

$$b * \sigma := b^{\sigma \boldsymbol{\alpha}_\sigma} \qquad \text{for } \sigma \in \Gamma \text{ and } b \in B.$$

This is a new action of Γ on B since

$$b * (\sigma\tau) = b^{\sigma\tau\boldsymbol{\alpha}_{\sigma\tau}} = b^{\sigma\tau\boldsymbol{\alpha}_\sigma^\tau\boldsymbol{\alpha}_\tau} = b^{\sigma\boldsymbol{\alpha}_\sigma\tau\boldsymbol{\alpha}_\tau} = (b * \sigma) * \tau.$$

We call this the $*$*-action with respect to* $\boldsymbol{\alpha}$. The set B with the $*$-action is again a Γ-set, denoted $B_{\boldsymbol{\alpha}}$ and called a *twisted form* of B. We say that $B_{\boldsymbol{\alpha}}$ is obtained by *twisting* B by the 1-cocycle $\boldsymbol{\alpha}$.

The most common example is when B is a Γ-group and $A = \operatorname{Aut}(B)$, the group of automorphisms of B. Then there is an action of Γ on A given by

$$a^\sigma = \sigma^{-1} \circ a \circ \sigma \qquad \text{for } \sigma \in \Gamma,\ a \in A, \tag{2.7}$$

where $\circ$ is composition of maps on B. The subgroup $H^0(\Gamma, \operatorname{Aut}(B))$ is exactly the set of Γ-automorphisms of B.

The following well-known proposition essentially shows that we get nothing new by looking at the twisted forms of a twisted form, for which we give an elementary proof.

2.2 Proposition ([30, Proposition 35bis]).
Let A be a Γ-group and $\boldsymbol{\alpha} \in Z^1(\Gamma, A)$. Then the map

$$\theta_{\boldsymbol{\alpha}} : H^1(\Gamma, A_{\boldsymbol{\alpha}}) \to H^1(\Gamma, A), \quad [\boldsymbol{\gamma}] \mapsto [\boldsymbol{\alpha}\boldsymbol{\gamma}],$$

where $\boldsymbol{\alpha}\boldsymbol{\gamma}$ denotes the map $\sigma \mapsto \boldsymbol{\alpha}_\sigma\boldsymbol{\gamma}_\sigma$, is a well defined bijection, which takes the trivial class in $H^1(\Gamma, A_{\boldsymbol{\alpha}})$ to the class of $\boldsymbol{\alpha}$ in $H^1(\Gamma, A)$.

Proof. Let $\boldsymbol{\gamma} \in Z^1(\Gamma, A_{\boldsymbol{\alpha}})$. Then

$$\boldsymbol{\alpha}_{\sigma\tau}\boldsymbol{\gamma}_{\sigma\tau} = \boldsymbol{\alpha}_\sigma^\tau\boldsymbol{\alpha}_\tau(\boldsymbol{\gamma}_\sigma * \tau)\boldsymbol{\gamma}_\tau = \boldsymbol{\alpha}_\sigma^\tau\boldsymbol{\alpha}_\tau(\boldsymbol{\gamma}_\sigma^\tau)^{\boldsymbol{\alpha}_\tau}\boldsymbol{\gamma}_\tau = (\boldsymbol{\alpha}_\sigma\boldsymbol{\gamma}_\sigma)^\tau\boldsymbol{\alpha}_\tau\boldsymbol{\gamma}_\tau$$

and thus $\boldsymbol{\alpha}\boldsymbol{\gamma} \in Z^1(\Gamma, A)$. Let $\boldsymbol{\gamma}'$ be cohomologous to $\boldsymbol{\gamma}$ with respect to $a \in A_{\boldsymbol{\alpha}}$. That is, $\boldsymbol{\gamma}'_\sigma = (a^{-1} * \sigma)\boldsymbol{\gamma}_\sigma a$ for all $\sigma \in \Gamma$. Then we have

$$\boldsymbol{\alpha}_\sigma\boldsymbol{\gamma}'_\sigma = \boldsymbol{\alpha}_\sigma(a^{-1} * \sigma)\boldsymbol{\gamma}_\sigma a = \boldsymbol{\alpha}_\sigma(a^{-\sigma})^{\boldsymbol{\alpha}_\sigma}\boldsymbol{\gamma}_\sigma a = a^{-\sigma}(\boldsymbol{\alpha}_\sigma\boldsymbol{\gamma}_\sigma)a,$$

and so $\boldsymbol{\alpha}\boldsymbol{\gamma}$ is cohomologous to $\boldsymbol{\alpha}\boldsymbol{\gamma}'$. Hence the map $\theta_{\boldsymbol{\alpha}}$ is well defined. Now $\boldsymbol{\rho} : \sigma \mapsto (\boldsymbol{\alpha}_\sigma)^{-1}$ is a cocycle in $Z^1(\Gamma, A_{\boldsymbol{\alpha}})$:

$$\begin{aligned}\boldsymbol{\rho}_{\sigma\tau} &= (\boldsymbol{\alpha}_{\sigma\tau})^{-1} = (\boldsymbol{\alpha}_\sigma^\tau\boldsymbol{\alpha}_\tau)^{-1} = \boldsymbol{\alpha}_\tau^{-1}\boldsymbol{\alpha}_\sigma^{-\tau}\boldsymbol{\alpha}_\tau\boldsymbol{\alpha}_\tau^{-1} \\ &= (\boldsymbol{\alpha}_\sigma^{-1} * \tau)\boldsymbol{\alpha}_\tau^{-1} = (\boldsymbol{\rho}_\sigma * \tau)\boldsymbol{\rho}_\tau.\end{aligned}$$

The induced map $\theta_{\boldsymbol{\rho}} : H^1(\Gamma, A) \to H^1(\Gamma, A_{\boldsymbol{\alpha}})$ is the inverse of $\theta_{\boldsymbol{\alpha}}$. $\square$

2.4 Exact sequences

In this section, we prove a fundamental result for the study of cohomology.

First we need some basic terminology for pointed sets. The *kernel* $\ker(\mu)$ of a morphism of pointed sets $\mu : M \to N$ is the set of all elements in M mapped to the distinguished point of N. A sequence of morphisms of pointed sets

$$L \xrightarrow{\nu} M \xrightarrow{\mu} N$$

is called *exact* at M if $\operatorname{im}(\nu) = \ker(\mu)$. Thus, the sequence $M \xrightarrow{\mu} N \to 1$ is exact if, and only if, μ is surjective, and the sequence $1 \to M \xrightarrow{\mu} N$ is exact if, and only if, $\ker(\mu)$ contains only the distinguished point of M. Note that this does not necessarily imply that μ is injective.

The following proposition is well known. Since this proposition is of a fundamental nature, we give a detailed proof.

2.3 Proposition ([30, Propositions 36, 38, 43]).
Let A be a Γ-group and let B be a Γ-subgroup of A. Let $i : B \to A$ be the inclusion map. Then A/B is a Γ-set with the natural action of Γ on cosets, and it is a Γ-group if B is normal. Let $\pi : A \to A/B$ be the canonical projection map.

(i) Define
$$\delta^0 : H^0(\Gamma, A/B) \to H^1(\Gamma, B), \quad aB \mapsto [\boldsymbol{\alpha}],$$
where $\boldsymbol{\alpha}$ is the cocycle defined by $\boldsymbol{\alpha}_\sigma := a^{-\sigma}a$. Then δ^0 is a map of pointed sets and the sequence
$$1 \to H^0(\Gamma, B) \xrightarrow{i^0} H^0(\Gamma, A) \xrightarrow{\pi^0} H^0(\Gamma, A/B) \xrightarrow{\delta^0} H^1(\Gamma, B) \xrightarrow{i^1} H^1(\Gamma, A)$$
is exact.

(ii) If B is normal, the sequence obtained from the sequence in (i) by adding
$$\ldots \xrightarrow{\pi^1} H^1(\Gamma, A/B)$$
on the right is exact.

(iii) Suppose B is a subgroup of the center of A. Given $\boldsymbol{\gamma} \in Z^1(\Gamma, A/B)$, choose a map $t : \Gamma \to A$ with $t_\sigma \in \boldsymbol{\gamma}_\sigma$ for every $\sigma \in \Gamma$. Set $\boldsymbol{\alpha}_{\sigma,\tau} := t_\sigma^\tau t_\tau t_{\sigma\tau}^{-1}$. Then
$$\delta^1 : H^1(\Gamma, A/B) \to H^2(\Gamma, B), \quad [\boldsymbol{\gamma}] \mapsto [\boldsymbol{\alpha}]$$
is a map of pointed sets and the sequence obtained from the sequence in (ii) by adding
$$\ldots \xrightarrow{\delta^1} H^2(\Gamma, B)$$
on the right is exact.

Proof.

(i) Given a coset aB in A/B, the cocycles defined by $\boldsymbol{\alpha}_\sigma := a^{-\sigma}a$ and $\boldsymbol{\beta}_\sigma := (ab)^{-\sigma}(ab)$ are obviously cohomologous, thus δ^0 is well defined. Moreover, $\delta^0(A) = [\mathbf{1}]$.

Exactness at $H^0(\Gamma, B)$ is obvious since i^0 is just the inclusion map. For exactness at $H^0(\Gamma, A)$, suppose $a \in \ker(\pi^0)$. Then $\pi^0(a) = B$ and $a \in B$. If, on the other hand, $a \in B$, then a obviously lies in the kernel of π^0.

For exactness at $H^0(\Gamma, A/B)$, suppose that the cocycle $\boldsymbol{\alpha}_\sigma = a^{-\sigma}a$ is trivial in $H^1(\Gamma, B)$. That is, $\boldsymbol{\alpha} \sim \mathbf{1}$ and $\boldsymbol{\alpha}_\sigma = b^{-\sigma}b$ for some $b \in B$. Then $ab^{-1} \in H^0(\Gamma, A)$ and $aB = (ab^{-1})B = \pi^0(ab^{-1}) \in \operatorname{im}(\pi^0)$.

Finally, let $[\boldsymbol{\alpha}] \in \ker(i^1)$. Then $\boldsymbol{\alpha} \in Z^1(\Gamma, B)$ and $\boldsymbol{\alpha}$ is cohomologous to $\mathbf{1} \in Z^1(\Gamma, A)$: $\boldsymbol{\alpha}_\sigma = a^{-\sigma}a$ for some $a \in A$. But this implies $(aB)^\sigma = a^\sigma B = (a(\boldsymbol{\alpha}_\sigma)^{-1})B = aB$, thus $aB \in H^0(\Gamma, A/B)$ and $\delta^0(aB) = [\boldsymbol{\alpha}]$. If, on the other hand, $[\boldsymbol{\alpha}] = \delta^0(aB)$ for some $a \in A$, then $\boldsymbol{\alpha}_\sigma = a^{-\sigma}a$ is cohomologous to $\mathbf{1} \in Z^1(\Gamma, A)$ and $[\boldsymbol{\alpha}] \in \ker(i^1)$.

(ii) Now let $\boldsymbol{\alpha} \in Z^1(\Gamma, A)$ with $[\boldsymbol{\alpha}] \in \ker(\pi^1)$. That means $[\pi^1(\boldsymbol{\alpha})] = [\mathbf{1}] \in H^1(\Gamma, A/B)$:

$$\boldsymbol{\alpha}_\sigma B = (aB)^{-\sigma}B(aB) = a^{-\sigma}aB = a^{-\sigma}Ba \quad \text{for some } a \in A.$$

Hence for all $\sigma \in \Gamma$ we have $\boldsymbol{\alpha}_\sigma = a^{-\sigma}b_\sigma a$ for some $b_\sigma \in B$. Now the map $b : \Gamma \to B$ defined by $\sigma \mapsto b_\sigma$ turns out to be a cocycle on B: $b_\sigma = a^\sigma \boldsymbol{\alpha}_\sigma a^{-1}$. Thus $[\boldsymbol{\alpha}] = [b] \in H^1(\Gamma, A)$ is the image of $[b] \in H^1(\Gamma, B)$ under the map i^1.

(iii) First we show that $\boldsymbol{\alpha} \in Z^2(\Gamma, B)$:

$$(t_\sigma^\tau t_\tau t_{\sigma\tau}^{-1})B = t_\sigma^\tau B t_\tau B t_{\sigma\tau}^{-1} B = \boldsymbol{\gamma}_\sigma^\tau \boldsymbol{\gamma}_\tau \boldsymbol{\gamma}_{\sigma\tau}^{-1} = 1_{A/B} = B$$

and thus $\boldsymbol{\alpha}_{\sigma,\tau} \in B$ for all $\sigma, \tau \in \Gamma$. Now we prove the cocycle condition (note that expressions in parenthesis are in B and thus commute with all elements):

$$\begin{aligned}
\boldsymbol{\alpha}_{\sigma\tau,\rho}\boldsymbol{\alpha}_{\sigma,\tau}^\rho &= (t_{\sigma\tau}^\rho t_\rho t_{\sigma\tau\rho}^{-1})(t_\sigma^{\tau\rho} t_\tau^\rho t_{\sigma\tau}^{-\rho}) = (t_\sigma^{\tau\rho} t_\tau^\rho t_{\sigma\tau}^{-\rho})(t_{\sigma\tau}^\rho t_\rho t_{\sigma\tau\rho}^{-1}) \\
&= t_\sigma^{\tau\rho} t_\tau^\rho t_\rho t_{\sigma\tau\rho}^{-1} = t_\sigma^{\tau\rho}(t_\tau^\rho t_\rho t_{\tau\rho}^{-1}) t_{\tau\rho} t_{\sigma\tau\rho}^{-1} = t_\sigma^{\tau\rho} t_{\tau\rho} t_{\sigma\tau\rho}^{-1}(t_\tau^\rho t_\rho t_{\tau\rho}^{-1}) \\
&= \boldsymbol{\alpha}_{\sigma,\tau\rho}\boldsymbol{\alpha}_{\tau,\rho}.
\end{aligned}$$

Moreover, if we choose a different map $t' : \Gamma \to A$ with $t'_\sigma \in \boldsymbol{\gamma}_\sigma$ for every $\sigma \in \Gamma$, then $t'_\sigma = t_\sigma b_\sigma$ for some $b_\sigma \in B$ and the obtained 2-cocycle $\boldsymbol{\alpha}'$ is cohomologous to $\boldsymbol{\alpha}$:

$$\boldsymbol{\alpha}'_{\sigma,\tau} = (t'_\sigma)^\tau t'_\tau (t'_{\sigma\tau})^{-1} = (t_\sigma^\tau b_\sigma^\tau)(t_\tau b_\tau)(t_{\sigma\tau}^{-1} b_{\sigma\tau}^{-1}) = \boldsymbol{\alpha}_{\sigma,\tau} b_\sigma^\tau b_\tau b_{\sigma\tau}^{-1}.$$

And finally if $\boldsymbol{\gamma}, \boldsymbol{\gamma}' \in Z^1(\Gamma, A/B)$ are cohomologous, then so are the corresponding 2-cocycles $\boldsymbol{\alpha}$ and $\boldsymbol{\alpha}'$. For, let $a \in A$ have the property $\boldsymbol{\gamma}'_\sigma = (aB)^{-\sigma}\boldsymbol{\gamma}_\sigma(aB) = (a^{-\sigma}t_\sigma a)B$. Now we just set $t'_\sigma := a^{-\sigma}t_\sigma a$ and obtain:

$$\boldsymbol{\alpha}'_{\sigma,\tau} = (a^{-\sigma}t_\sigma a)^\tau(a^{-\tau}t_\tau a)(a^{-\sigma\tau}t_{\sigma\tau}a)^{-1} = a^{-\sigma\tau}\boldsymbol{\alpha}_{\sigma,\tau}a^{\sigma\tau} = \boldsymbol{\alpha}_{\sigma,\tau}.$$

Hence $[\boldsymbol{\alpha}] \in H^2(\Gamma, B)$ does not depend on the choice of t nor on the choice of the cocycle in $[\boldsymbol{\gamma}]$.

For exactness of the sequence, choose $\boldsymbol{\gamma} \in Z^1(\Gamma, A/B)$, whose cohomology class lies in the kernel of δ^1. Let t and $\boldsymbol{\alpha}_{\sigma,\tau} = t_\sigma^\tau t_\tau t_{\sigma\tau}^{-1}$ be as above. Then $\boldsymbol{\alpha}$ is cohomologous to the trivial 2-cocycle and thus there is a map $\varphi : \Gamma \mapsto B$ satisfying

$$\boldsymbol{\alpha}_{\sigma,\tau} = \mathbf{1}_{\sigma,\tau}\varphi_\sigma^\tau\varphi_\tau\varphi_{\sigma\tau}^{-1} = \varphi_\sigma^\tau\varphi_\tau\varphi_{\sigma\tau}^{-1}.$$

Now the map $\boldsymbol{\beta} : \Gamma \mapsto A$ defined by $\boldsymbol{\beta}_\sigma := t_\sigma\varphi_\sigma^{-1}$ turns out to be a 1-cocycle:

$$\boldsymbol{\beta}_{\sigma\tau} = t_{\sigma\tau}\varphi_{\sigma\tau}^{-1} = (t_\sigma^\tau t_\tau\varphi_\sigma^{-\tau}\varphi_\tau^{-1}\varphi_{\sigma\tau})\varphi_{\sigma\tau}^{-1} = (t_\sigma\varphi_\sigma^{-1})^\tau(t_\tau\varphi_\tau^{-1}) = \boldsymbol{\beta}_\sigma^\tau\boldsymbol{\beta}_\tau.$$

Moreover, $\boldsymbol{\gamma}$ is the image of $\boldsymbol{\beta}$:

$$(\pi^1(\boldsymbol{\beta}))_\sigma = \boldsymbol{\beta}_\sigma B = t_\sigma\varphi_\sigma^{-1}B = t_\sigma B = \boldsymbol{\gamma}_\sigma.$$

Conversely, if $\boldsymbol{\gamma} = \pi^1(\boldsymbol{\beta})$ for some $\boldsymbol{\beta} \in Z^1(\Gamma, A)$, then we can choose $t := \boldsymbol{\beta}$ and obtain

$$\boldsymbol{\alpha}_{\sigma,\tau} = \boldsymbol{\beta}_\sigma^\tau\boldsymbol{\beta}_\tau\boldsymbol{\beta}_{\sigma\tau}^{-1} = \boldsymbol{\beta}_{\sigma\tau}\boldsymbol{\beta}_{\sigma\tau}^{-1} = 1.$$

This completes the proof. □

From the definition of exact sequences, it is immediately clear that the kernel of π^1 is trivial if $H^1(\Gamma, B) = 1$. This does not immediately imply that π^1 is injective, since first cohomologies of nonabelian groups do not have a group structure in general. We use twisting to prove injectivity. For $f : M \to N$ and $n \in N$ we call $f^{-1}(n) := \{m \in M \mid f(m) = n\}$ a *fibre* of f.

2.4 Proposition.
Let A be a Γ-group, let B be a normal Γ-subgroup of A, and let $\pi : A \to A/B$ be the canonical projection map. Then all non-empty fibres of π^1 have the same order, which is at most $|H^1(\Gamma, B)|$.

Proof. In this proof, we write π for π^1 and i for i^1 to simplify the notation. Let $\boldsymbol{\alpha} \in Z^1(\Gamma, A)$. Then we obtain $A_{\boldsymbol{\alpha}}$, $B_{\boldsymbol{\alpha}}$ and $(A/B)_{\boldsymbol{\alpha}}$ as in Section 2.3, and an exact sequence:

$$\ldots \to H^1(\Gamma, B_{\boldsymbol{\alpha}}) \xrightarrow{i'} H^1(\Gamma, A_{\boldsymbol{\alpha}}) \xrightarrow{\pi'} H^1(\Gamma, (A/B)_{\boldsymbol{\alpha}}).$$

The map $\theta_{\boldsymbol{\alpha}}$ of Proposition 2.2 induces a bijection between the kernel of π' and $\pi^{-1}(\pi([\boldsymbol{\alpha}]))$, since

$$\begin{aligned}[\boldsymbol{\beta}] \in \ker(\pi') &\iff \pi'([\boldsymbol{\beta}]) = \pi'([\mathbf{1}]) \\ &\iff \pi(\theta_{\boldsymbol{\alpha}}([\boldsymbol{\beta}])) = \pi(\theta_{\boldsymbol{\alpha}}([\mathbf{1}])) \\ &\iff \theta_{\boldsymbol{\alpha}}([\boldsymbol{\beta}]) \in \pi^{-1}(\pi([\boldsymbol{\alpha}])).\end{aligned}$$

This shows that every non-empty fibre of π has the same order.

Of course, the order of such a fibre cannot exceed $|H^1(\Gamma, B)|$. $\square$

2.5 Corollary.
If $H^1(\Gamma, B) = 1$, then π^1 is injective.

The upper bound on the size of the fibres given by Proposition 2.4 is used for the computation of cohomology in Section 2.6.

2.5 Extending 1-cocycles

In this section, we show how to compute the cocycles on a group from the cocycles on a quotient. Let A be a Γ-group and let B be a normal Γ-subgroup of A. Let $\pi : A \to A/B$ be the standard projection. Denote images under the maps π and π^1 by $\overline{a}$ and $\overline{\boldsymbol{\alpha}}$ for $a \in A$ and $\boldsymbol{\alpha} \in Z^1(\Gamma, A)$.

Let $\boldsymbol{\alpha}, \boldsymbol{\beta} \in Z^1(\Gamma, A)$ be cohomologous with respect to some $a \in A$. Then $\overline{\boldsymbol{\beta}}$ is cohomologous to $\overline{\boldsymbol{\alpha}}$ with respect to $\overline{a}$:

$$\overline{\boldsymbol{\beta}}_\gamma = \overline{\boldsymbol{\beta}_\gamma} = \overline{a^{-\gamma} \cdot \boldsymbol{\alpha}_\gamma \cdot a} = \overline{a^{-\gamma}} \cdot \overline{\boldsymbol{\alpha}_\gamma} \cdot \overline{a} = \overline{a}^{-\gamma} \cdot \overline{\boldsymbol{\alpha}}_\gamma \cdot \overline{a} = \overline{\boldsymbol{\alpha}}_\gamma^{(\overline{a})}.$$

Given a cocycle $\boldsymbol{\alpha} \in Z^1(\Gamma, A/B)$, we call a cocycle $\boldsymbol{\beta} \in Z^1(\Gamma, A)$ such that $\overline{\boldsymbol{\beta}} = \boldsymbol{\alpha}$ an *extension* of $\boldsymbol{\alpha}$. Two questions now arise:

1. Can every 1-cocycle on A/B be extended to a 1-cocycle on A?
2. Can every 1-cocycle on A be constructed by such an extension?

The answer to the second question is obviously yes. The answer to the first question is no in general (a counterexample is given at the end of the section). The following theorem provides a necessary and sufficient condition for a cocycle to be extendable and an algorithm for finding the extensions. Recall the $[\![\ ]\!]$ notation from the end of Section 2.2.

2.6 Theorem.
Let $\boldsymbol{\alpha} \in Z^1(\Gamma, A/B)$ and let Γ have a finite presentation with generators $\gamma_1, \ldots, \gamma_k$ and relators $r_1, \ldots, r_\ell$. Fix a set $T = \{t(x) \mid x \in A/B\}$ of coset representatives. Now follow the following procedure:

1. Let $b(\gamma_1), \dots, b(\gamma_k), b(\gamma_1^{-1}), \dots, b(\gamma_k^{-1})$ be indeterminates over B.
2. For $r \in \{r_1, \dots, r_\ell\}$, compute

$$b(r) := \prod_{i=1}^{m} \left(\left(t(\boldsymbol{\alpha}_{\sigma_i}) b(\sigma_i) \right)^{\prod_{j=i+1}^{m} \sigma_j} \right) \tag{2.8}$$

   where $r = \prod_{i=1}^{m} \sigma_i$ with each $\sigma_i \in \{\gamma_1, \dots, \gamma_k, \gamma_1^{-1}, \dots, \gamma_k^{-1}\}$.
3. Consider the system of equations

$$\{b(r_j) = 1\}_{j=1}^{\ell} \tag{2.9}$$

   for $b(\gamma_1), \dots, b(\gamma_k) \in B$.

Then

(a) The system (2.9) is solvable if, and only if, $\boldsymbol{\alpha}$ can be extended to a cocycle on A.

(b) For every solution of this system,

$$[\![t(\boldsymbol{\alpha}_{\gamma_1}) \cdot b(\gamma_1), \dots, t(\boldsymbol{\alpha}_{\gamma_k}) \cdot b(\gamma_k)]\!]$$

defines a 1-cocycle $\boldsymbol{\beta}$ on A such that $\overline{\boldsymbol{\beta}} = \boldsymbol{\alpha}$.

(c) Every cocycle $\boldsymbol{\beta} \in Z^1(\Gamma, A)$ with $\overline{\boldsymbol{\beta}} = \boldsymbol{\alpha}$ can be constructed this way.

Proof.

(a) By Theorem 2.1,

$$\boldsymbol{\beta} := [\![t(\boldsymbol{\alpha}_{\gamma_1}) \cdot b(\gamma_1), \dots, t(\boldsymbol{\alpha}_{\gamma_k}) \cdot b(\gamma_k)]\!]$$

is a cocycle if, and only if, $\boldsymbol{\beta}_r = 1$ for all $r \in \{r_1, \dots, r_\ell\}$. Now let $r = \prod_{i=1}^{m} \sigma_i$ be one of these relators. Then

$$\boldsymbol{\beta}_r = \prod_{i=1}^{m} \left(\left(t(\boldsymbol{\alpha}_{\sigma_i}) b(\sigma_i) \right)^{\prod_{j=i+1}^{m} \sigma_j} \right) = b(r)$$

and hence $\boldsymbol{\beta}_r = 1$ if, and only if, $b(r) = 1$.

(b) For $i = 1, \dots, k$, we have

$$\overline{\boldsymbol{\beta}}_{\gamma_i} = \overline{t(\boldsymbol{\alpha}_{\gamma_i}) b(\gamma_i)} = t(\boldsymbol{\alpha}_{\gamma_i}) b(\gamma_i) B = t(\boldsymbol{\alpha}_{\gamma_i}) B = \boldsymbol{\alpha}_{\gamma_i}$$

and so $\overline{\boldsymbol{\beta}} = \boldsymbol{\alpha}$.

(c) If $\boldsymbol{\beta} \in Z^1(\Gamma, A)$ with $\overline{\boldsymbol{\beta}} = \boldsymbol{\alpha}$, then $\overline{\boldsymbol{\beta}}_\gamma = \boldsymbol{\alpha}_\gamma$ and $\boldsymbol{\beta}_\gamma \in t(\boldsymbol{\alpha}_\gamma)B$. Set

$$b(\gamma) := t(\boldsymbol{\alpha}_\gamma)^{-1}\boldsymbol{\beta}_\gamma \quad \text{for } \gamma \in \{\gamma_1, \dots, \gamma_k, \gamma_1^{-1}, \dots, \gamma_k^{-1}\}.$$

Then $b(\gamma_1), \dots, b(\gamma_k), b(\gamma_1^{-1}), \dots, b(\gamma_k^{-1})$ is a solution of the system (2.9):

$$b(r) = \prod_{i=1}^{m} \Big(\big(t(\boldsymbol{\alpha}_{\sigma_i})b(\sigma_i)\big)^{\prod_{j=i+1}^{m}\sigma_j} \Big) = \prod_{i=1}^{m} \Big(\boldsymbol{\beta}_{\sigma_i}{}^{\prod_{j=i+1}^{m}\sigma_j} \Big) = \boldsymbol{\beta}_r = 1$$

for all $r \in \{r_1, \dots, r_\ell\}$.

□

Note that if Γ acts by conjugation, formula (2.8) reduces to

$$b(r) = \prod_{i=1}^{m} \big(\sigma_i t(\boldsymbol{\alpha}_{\sigma_i}) b(\sigma_i)\big). \tag{2.8$'$}$$

We now give a small example demonstrating how Theorem 2.6 is applied to extend cocycles.

2.7 Example.
Let $\Gamma = \Sigma_3$ be the symmetric group on three letters. Then

$$\Gamma = \langle \gamma_1, \gamma_2 \mid \gamma_1^2 = \gamma_2^3 = (\gamma_1\gamma_2)^2 = 1 \rangle$$

with $\gamma_1 = (1,2)$ and $\gamma_2 = (1,2,3)$. Let $A := \Sigma_4$ be a Γ-group with Γ acting by conjugation. The alternating group $B := A_4$ is a normal Γ-subgroup of A. We fix the set $T := \{1, (1,2)\}$ of representatives for the elements of $A/B \simeq C_2$.

Since $\operatorname{Aut}(C_2) = 1$, the induced action of Γ on A/B is trivial. First, we compute the cohomology set $H^1(\Gamma, A/B)$. Let $\boldsymbol{\alpha} \in Z^1(\Gamma, A/B)$, $a \in A/B$, and $\gamma \in \Gamma$. Then

$$a^{-\gamma}\boldsymbol{\alpha}_\gamma a = a^{-1}\boldsymbol{\alpha}_\gamma a = a^{-1}a\boldsymbol{\alpha}_\gamma = \boldsymbol{\alpha}_\gamma.$$

Thus, every cohomology class in $H^1(\Gamma, A/B)$ consists of exactly one cocycle. Since $\boldsymbol{\alpha}_{\gamma\delta} = \boldsymbol{\alpha}_\gamma^\delta \boldsymbol{\alpha}_\delta = \boldsymbol{\alpha}_\gamma\boldsymbol{\alpha}_\delta$, the order of $\boldsymbol{\alpha}_{\gamma_1}$ must be a divisor of 2 and the order of $\boldsymbol{\alpha}_{\gamma_2}$ must be a divisor of 3. Thus, $\boldsymbol{\alpha}_{\gamma_2} = 1_{A/B}$. Both possible choices for $\boldsymbol{\alpha}_{\gamma_1}$ in A/B give rise to cocycles. Hence we have $Z^1(\Gamma, A/B) = \big\{\mathbf{1}, [\![\overline{(1,2)}, \overline{1}]\!]\big\}$.

Now consider indeterminates $b(\gamma_1)$ and $b(\gamma_2)$ and write down the equations from (2.8′):

$$\begin{aligned}
1 = b\big(\gamma_1^2\big) &= \big(\gamma_1 \cdot t(\boldsymbol{\alpha}_{\gamma_1}) \cdot b(\gamma_1)\big)^2, \\
1 = b\big(\gamma_2^3\big) &= \big(\gamma_2 \cdot t(\boldsymbol{\alpha}_{\gamma_2}) \cdot b(\gamma_2)\big)^3, \\
1 = b\big((\gamma_1\gamma_2)^2\big) &= \big(\gamma_1 \cdot t(\boldsymbol{\alpha}_{\gamma_1}) \cdot b(\gamma_1) \cdot \gamma_2 \cdot t(\boldsymbol{\alpha}_{\gamma_2}) \cdot b(\gamma_2)\big)^2.
\end{aligned}$$

We now extend these cocycles on A/B to cocycles on A:

$\boldsymbol{\alpha} = \mathbf{1} \in Z^1(\Gamma, A/B)$.

In this case, the equations reduce to

$$\begin{aligned} 1 &= \big(\gamma_1 \cdot b(\gamma_1)\big)^2, \\ 1 &= \big(\gamma_2 \cdot b(\gamma_2)\big)^3, \\ 1 &= \big(\gamma_1 \cdot b(\gamma_1) \cdot \gamma_2 \cdot b(\gamma_2)\big)^2. \end{aligned}$$

One solution can be seen immediately (and could have been guessed), namely $b(\gamma_1) = b(\gamma_2) = 1$. In this case, the extended cocycle is the trivial cocycle $\mathbf{1}$. But there are other solutions. The solution $b(\gamma_1) = 1, b(\gamma_2) = \gamma_2^{-1}$ provides a cocycle $\boldsymbol{\beta}'$, which is not cohomologous to the trivial one. All other solutions of this system produce cocycles cohomologous to either $\mathbf{1}$ or $\boldsymbol{\beta}'$.

$\boldsymbol{\alpha} = [\![\overline{(1,2)}, \overline{1}]\!] \in Z^1(\Gamma, A/B)$.

In this case, the equations reduce to

$$\begin{aligned} 1 &= b(\gamma_1)^2, \\ 1 &= \big(\gamma_2 \cdot b(\gamma_2)\big)^3, \\ 1 &= \big(b(\gamma_1) \cdot \gamma_2 \cdot b(\gamma_2)\big)^2. \end{aligned}$$

We present two solutions here, which give rise to non-cohomologous cocycles:

- $b(\gamma_1) = 1$, $b(\gamma_2) = \gamma_2^{-1}$ gives extended cocycle $\boldsymbol{\beta}'' = [\![\gamma_1, \gamma_2^{-1}]\!]$.
- $b(\gamma_1) = (1,2)(3,4)$, $b(\gamma_2) = \gamma_2^{-1}$ gives extended cocycle $\boldsymbol{\beta}''' = [\![(3,4), \gamma_2^{-1}]\!]$.

All other solutions of this system produce cocycles cohomologous to either $\boldsymbol{\beta}''$ or $\boldsymbol{\beta}'''$.

By Theorem 2.6(c), the cocycles $\mathbf{1}, \boldsymbol{\beta}', \boldsymbol{\beta}'', \boldsymbol{\beta}'''$ represent all cohomology classes in $H^1(\Gamma, A)$.

The following example demonstrates the existence of non-extendable cocycles.

2.8 Example.

Let $A = \Gamma = D_8$ be the symmetry group of a square, with the Coxeter presentation

$$\Gamma = \big\langle \gamma_1, \gamma_2 \mid \gamma_1^2, \gamma_2^2, (\gamma_1\gamma_2)^4 \big\rangle.$$

The group Γ acts on A by conjugation. We label the vertices of the square by $1, \ldots, 4$ and write elements of Γ as permutations on the vertices. Let $B = Z(A) = \langle (1,3)(2,4) \rangle \simeq C_2$ be the center of A.

Now $\boldsymbol{\alpha} := [\![\overline{\gamma_1}, \overline{\gamma_1}]\!]$ is a cocycle in $Z^1(\Gamma, A/B)$. Define the map $t : \Gamma \to A$ by $t_\sigma := \gamma_1^{\ell(\sigma)}$, where ℓ is the Coxeter length of σ (see for example [19] for the definition of the Coxeter length). It satisfies the condition $t_\sigma \in \boldsymbol{\alpha}_\sigma$. Now recall the map δ^1 of Proposition 2.3: $\delta^1([\boldsymbol{\alpha}]) = [\boldsymbol{\beta}] \in H^2(\Gamma, B)$, where $\boldsymbol{\beta}_{\sigma,\tau} := t_\sigma^\tau t_\tau t_{\sigma\tau}^{-1}$. But $\boldsymbol{\beta}$ is not cohomologous to the trivial 2-cocycle (this can be proven either by trying all 256 possibilities for a map $\varphi : \Gamma \to B$ in Equation (2.6) or by using Derek Holt's algorithms [17]). Hence there are no extensions of $\boldsymbol{\alpha}$, by Proposition 2.3(iii).

Note that, by extending only one representative of $[\boldsymbol{\alpha}] \in H^1(\Gamma, A/B)$, we do not necessarily obtain all cohomology classes $[\boldsymbol{\beta}] \in H^1(\Gamma, A)$ that are mapped onto $[\boldsymbol{\alpha}]$ by π^1. In general, we have to extend all elements of $[\boldsymbol{\alpha}]$ in all possible ways.

2.6 Computing finite cohomology

In this section, we describe algorithms for the computation of the first cohomology of a finite group. Let A be a finite Γ-group as before. If A is abelian, the first cohomology $H^1(\Gamma, A)$ can be computed efficiently using algorithms of Derek Holt [17], which are implemented in Magma. Here we describe algorithms for dealing with the computation in case A is nonabelian.

2.6.1 Groups with a normal subgroup

Suppose B is a normal Γ-subgroup of A. Then we compute the cohomology $H^1(\Gamma, A/B)$ and lift the cocycles of every cohomology class in $H^1(\Gamma, A/B)$ to a cocycle on A as in Section 2.5.

It may happen that unnecessary computations are carried out in the following two situations:

1. Constructing extensions in $Z^1(\Gamma, A)$ that are cohomologous to the cocycles we already know (see Example 2.7).
2. Trying to construct an extension of a cocycle in $Z^1(\Gamma, A/B)$ that has no extensions (see Example 2.8).

Knowing *a priori* that a cocycle is extendable is crucial for the efficiency of the algorithm provided by Theorem 2.6. Here Proposition 2.4 is very useful: It provides an upper bound for the number of extensions and also the exact number of extensions once one cocycle is extended in all possible ways.

2.6.2 Groups with a nontrivial center

Now suppose B is central. In this case, we proceed as in the previous subsection. But this time we know by Proposition 2.3(iii) that only those cocycles in

$Z^1(\Gamma, A/B)$ with cohomology classes in $\ker(\delta^1)$ need be extended.

If A is nilpotent and so has a central series, we can proceed recursively. The number of steps required is equal to the nilpotency class.

2.6.3 Other finite groups

We use brute force otherwise. Though, for an implementation, the cohomology of these groups could be computed once and stored in a database.

Basically we use Theorem 2.1 to recognise 1-cocycles and compute $Z^1(\Gamma, A)$ in the first step, and then we split it into cohomology classes in the second. Since a 1-cocycle is uniquely determined by its images on generators of Γ, all $k^{|A|}$ sequences $[\![a_1, \ldots, a_k]\!]$ must be considered, where k is the number of generators of Γ, and up to ℓ relations must be verified for every sequence. Thus it is vital to have the smallest possible generating set for Γ and important to have short relations on these generators. Even so, this method is only feasible for very small groups.

2.6.4 Timings

We have implemented this algorithm in Magma. The times in Table 2.1 are given in CPU-seconds for an AMD Opteron 246 (2GHz). In this table we denote the alternating and the symmetric groups on n letters by A_n and Σ_n, the cyclic group of order n by C_n, the dihedral group of the n-gon by D_{2n}, and the Coxeter group of type X by $W(X)$.

Table 2.1: Timings for computation of $H^1(\Gamma, A)$.

A	Γ	action	$\lvert H^1(\Gamma, A)\rvert$	time
D_{16}	$N_{\Sigma_8}(D_{16})$	conjugation	38	2.880
A_4	Σ_4	conjugation	5	0.150
A_5	Σ_5	conjugation	3	1.140
A_6	Σ_6	conjugation	6	56.990
$W(\mathrm{A}_5)$	C_2	trivial	4	0.340
$W(\mathrm{D}_5)$	C_2	trivial	6	0.730
$W(\mathrm{E}_6)$	C_2	trivial	5	24.530
$W(\mathrm{D}_4)$	C_3	trivial	2	0.120

2.7 Classical interpretation of group cohomology

In this section, we give a classical group-theoretic interpretation of the first cohomology in terms of complements of A in the semidirect product of Γ and A. Let A be a Γ-group and define the *semidirect product*

$$\Gamma \ltimes A = \{(\gamma, a) \mid \gamma \in \Gamma, a \in A\}$$

with multiplication

$$(\gamma_1, a_1)(\gamma_2, a_2) = (\gamma_1\gamma_2, a_1^{\gamma_2} a_2).$$

Identify A with $\{(1, a) \mid a \in A\} \leq \Gamma \ltimes A$. For $\boldsymbol{\alpha} \in Z^1(\Gamma, A)$, define a subgroup of $\Gamma \ltimes A$ by $K_{\boldsymbol{\alpha}} := \{(\gamma, \boldsymbol{\alpha}_\gamma) \mid \gamma \in \Gamma\}$. Then the set

$$\{K_{\boldsymbol{\alpha}} \mid \boldsymbol{\alpha} \in Z^1(\Gamma, A)\}$$

is the set of all complements of A in $\Gamma \ltimes A$. Two complements $K_{\boldsymbol{\alpha}}$ and $K_{\boldsymbol{\beta}}$ are conjugate in $\Gamma \ltimes A$ if, and only if, $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are cohomologous. Thus, if we choose a set R of representatives of cohomology classes in $H^1(\Gamma, A)$, then

$$\{K_{\boldsymbol{\alpha}} \mid \boldsymbol{\alpha} \in R\}$$

is the set of conjugacy class representatives of the complements. Furthermore,

$$\begin{aligned} \Gamma \ltimes A_{\boldsymbol{\alpha}} &\to \Gamma \ltimes A \\ (\gamma, a) &\mapsto (\gamma, \boldsymbol{\alpha}_\gamma a) \end{aligned}$$

is a group isomorphism, where in $\Gamma \ltimes A_{\boldsymbol{\alpha}}$ the group Γ acts on A by the $*$-action as described in Section 2.3.

The problem of computing the conjugacy classes of complements has been considered for cases where $\Gamma \ltimes A$ is soluble and A is abelian by, for example, Celler, Neubüser and Wright [10] or Holt [17]. There are more recent results for the case where A is nonsoluble, for example in Cannon and Holt [7]. There is also a faster method to compute a "large subset" of the first cohomology due to Archer [3].

Chapter 3

Algebraic groups

Our aim is to describe the twisted forms of a linear algebraic group. In the first sections of the present chapter, we introduce linear algebraic groups and associated terminology. We state some well-known results which we need in the sequel. We follow the notation of Springer [32] and Humphreys [18].

In Section 3.4, we recall the classification of the twisted forms via Galois cohomology. The rest of this chapter is devoted to methods for computing the Galois cohomology. See Chapter 4 on the problem of describing the twisted form corresponding to a given cocycle.

3.1 Definitions and basic properties

We start with a definition of affine algebraic groups without going into a deep discussion of the theory of affine algebraic varieties. Let L be an algebraically closed field. We denote by L^n the set of all n-tuples of elements of L, called the n-dimensional *affine space* over L. For a subfield K of L, let $P_K^n = K[x_1, \ldots, x_n]$ be the polynomial ring in n variables over K. We can interpret the elements of P_K^n as functions from L^n to L. For a subset T of P_L^n, we define the *zero set* of T to be the set of common zeros of all elements of T, namely

$$Z(T) := \{a \in L^n \mid f(a) = 0 \text{ for all } f \in T\}.$$

Such a zero set is called an *affine algebraic variety.* If $X \subseteq L^n$ and $Y \subseteq L^m$ are varieties, a map $\varphi : X \to Y$ is called a *morphism of varieties* if it is given by polynomials over L, that is, there are polynomials $p_1, \ldots, p_m \in P_L^n$ such that

$$\varphi(x) = \big(p_1(x), \ldots, p_m(x)\big)$$

for $x = (x_1, \ldots, x_n) \in X$.

The subset T generates an ideal of P_L^n and, since P_L^n is Noetherian, this ideal has a finite generating set. Thus $Z(T)$ is the zero set of some *finite* set of polynomials.

If $Z(T)$ is a group such that the multiplication map and the inverse map are both morphisms of varieties, then $Z(T)$ is called an *affine algebraic group*. A simple example is

$$\{(x,y)\in L^2 \mid xy-1=0\}$$

with multiplication given by $(x_1,y_1)\cdot(x_2,y_2) := (x_1x_2, y_1y_2)$. The identity element is $(1,1)$ and the inverse of (x,y) is (y,x). This group is isomorphic to the multiplicative group of L and is denoted $\mathrm{G_m}$.

For the definition of the *dimension* of an affine variety, we refer to [32, 1.8.1]. Basically, it is the number of algebraically independent coordinates. For example, $\mathrm{G_m}$ has dimension 1.

A subset of an affine algebraic group G is called *closed* if it is the zero set of some polynomials in P^n_L. A closed subgroup of G is also an affine algebraic group. This defines a topology on G, called the *Zarisski topology*.

Let G be an affine algebraic group and let k be a subfield of L. If there is a subset T of P^n_k such that $G = Z(T)$, and the multiplication and inverse maps are given by polynomials over k, then the algebraic group G is said to be *defined over* k. Note that if G is defined over k then it is defined over K whenever $k\subseteq K\subseteq L$, and G is always defined over L. The group $\mathrm{G_m}$ in the above example is defined over the prime field of L.

From now on, L is assumed to be the algebraic closure $\bar{k}$ of the field k, and G is assumed to be defined over k. Let G be an affine algebraic group defined over k. Let k_{sep} be the separable closure of k. It is a Galois extension of k with Galois group $\Gamma_{\mathrm{sep}} := \mathrm{Gal}(k_{\mathrm{sep}}\colon k)$. The action of Γ_{sep} on k_{sep} extends uniquely to an action on $\bar{k}$. Then the group Γ_{sep} acts on G componentwise:

$$(x_1,\dots,x_n)\mapsto(x_1,\dots,x_n)^\gamma=(x_1^\gamma,\dots,x_n^\gamma) \tag{3.1}$$

for $\gamma\in\Gamma_{\mathrm{sep}}$. This action is continuous with respect to the profinite topology on Γ_{sep} (cf. [20, Chapter VII]) and the Zarisski topology on G. Let K be a Galois extension of k contained in $\bar{k}$; then K is contained in k_{sep}. The set of *K-rational points* of G is

$$G(K) := \{g\in G \mid g^\gamma = g \text{ for all } \gamma\in\mathrm{Gal}(k_{\mathrm{sep}}\colon K)\}. \tag{3.2}$$

$G(K)$ is a group, since it is a fixed point subgroup of G, although it is not necessarily algebraic. Let T be a finite set of polynomials over k such that $G = Z(T)$. Obviously, $G(K)$ is the set of zeros of T contained in K^n, i.e.,

$$G(K) = G\cap K^n. \tag{3.3}$$

From this, one can see immediately that $\mathrm{Gal}(K\colon k)$ acts componentwise (as in (3.1)) on $G(K)$.

Let G and H be affine algebraic groups defined over the field k. A group homomorphism $\alpha : G \to H$ is *algebraic over* k or k-*algebraic* if it is given by polynomials over k. A group isomorphism $\alpha : G \to H$ is called *algebraic over* k or k-*algebraic* if α and α^{-1} are both k-algebraic homomorphisms. A k-algebraic isomorphism from G to G is a k-*algebraic automorphism.* If $k = \bar{k}$, then we omit k from the notation and speak just of algebraic homomorphisms, isomorphisms, and automorphisms.

3.1 Example.
Let k be a prime field and let $L := \bar{k}$ be its algebraic closure. The general linear group GL_n is the group of invertible $n \times n$ matrices with entries in L. This group is affine algebraic when considered as a zero set in L^{n^2+1} as follows:

$$\mathrm{GL}_n \simeq \{(A, t) \mid A \in \mathrm{M}_n(L),\ t \in L,\ t \det A = 1\}.$$

As a consequence, every closed subgroup of GL_n is again an affine algebraic group. Clearly, GL_n is defined over k.

A closed subgroup of GL_n for some n is called a *linear algebraic group.* The following theorem shows that the notions of affine and linear algebraic groups coincide. We speak, as is more common, of linear algebraic groups in the sequel.

3.2 Theorem ([32, 2.3.7]).
Let G be an affine algebraic group. Then G is isomorphic to a closed subgroup of some GL_n. ■

The affine variety $X \subseteq L^n$ is called *irreducible* if it is nonempty and cannot be expressed as the union $X = Y_1 \cup Y_2$ of two proper closed subsets. By [18, Proposition 1.3B], every zero set is a union of finitely many irreducible closed subsets. These are called the *irreducible components* of $Z(T)$.

The affine variety $X \subseteq L^n$ is called *connected* if it cannot be expressed as the union $X = Y_1 \cup Y_2$ of two *disjoint* proper closed subsets. It follows immediately that irreducible affine varieties are connected. The converse isn't necessarily true, as can be seen from the example $\{(x, y) \in L^2 \mid xy = 0\}$.

The following proposition shows that the notions of irreducibility and connectedness coincide for linear algebraic groups. Following the usual convention, we speak of connected algebraic groups rather than irreducible ones.

3.3 Proposition ([32, 2.2.1]).
Let G be a linear algebraic group.

1. There is a unique irreducible component G° of G that contains the identity element 1. It is a closed normal subgroup of finite index.

2. G° is also the unique connected component of G that contains 1.

3. Any closed subgroup of finite index in G contains G°. ■

We call G° the *identity component* of G. If G is defined over k, then G° is also defined over k by [32, 12.1.1].

A matrix x is *unipotent* if $(x-1)^s = 0$ for some integer $s \geq 1$. A matrix is *semisimple* if it is diagonalizable, i.e., similar to a diagonal matrix over $\bar{k}$. An element x of a linear algebraic group is *unipotent* (respectively *semisimple*) if $\phi(x)$ is unipotent (respectively *semisimple*) for some algebraic isomorphism ϕ of G onto a closed subgroup of GL_n. By [32, 2.4.9], these definitions are independent of n and ϕ. We also have the well-known

3.4 Theorem (Jordan decomposition, [32, 2.4.8(i)]).
Let G be a linear algebraic group and $g \in G$. Then there are unique elements $g_s, g_u \in G$ such that g_s is semisimple, g_u is unipotent, and $g = g_s g_u = g_u g_s$. ■

The elements g_u and g_s are called the *unipotent part* and the *semisimple part* of g, respectively. A linear algebraic group G is called *unipotent* if all its elements are unipotent.

3.5 Proposition ([32, 2.4.13]).
A unipotent linear algebraic group is nilpotent. ■

A *torus* T is an algebraic group that is algebraically isomorphic to $(\mathrm{G_m})^d$. The torus T is a *k-torus* if it is defined over k. Note that, even for a k-torus T, the isomorphism $T \simeq (\mathrm{G_m})^d$ need not be defined over k. If it is, the torus is said to be *k-split*. A k-torus is called *k-anisotropic* if it doesn't have any proper k-split subtori.

A *subtorus* of a linear algebraic group G is an algebraic subgroup of G that is a torus. A *maximal torus* of G is a subtorus of G that is not strictly contained in another subtorus.

3.6 Theorem ([32, 6.4.1]).
Two maximal tori of a connected linear algebraic group G are conjugate in G. ■

This theorem justifies the definition of the *rank* of a connected linear algebraic group G as the dimension of a maximal torus of G. A *Cartan subgroup* of G is the identity component of the centralizer of a maximal torus. (In fact, such a centralizer is connected, see the next lemma.)

3.7 Lemma.
Let G be a connected linear algebraic group.

(i) If S is a subtorus of G, then $C_G(S)$ is connected.

(ii) If T is a maximal torus of G, then $C_G(T)$ is a Cartan subgroup of G.

Proof. (i) is [32, Theorem 6.4.7(i)] and (ii) follows immediately from (i) and the definition of Cartan subgroup. ∎

3.8 Lemma ([32, 13.2.4]).
Every k-torus T has k-subtori T_s and T_a, which are k-split and k-anisotropic, respectively, such that $T = T_a T_s$ and $T_a \cap T_s$ is finite. ∎

A connected linear algebraic group G defined over k has a maximal torus $T \subseteq G$, which is also defined over k. If there exists a maximal k-torus that is k-split, then G is called *k-split*.

By [18, Corollary 7.4, Lemma 17.3(c)], every linear algebraic group G has a unique maximal solvable normal subgroup, which is automatically closed. Its identity component is then the largest connected solvable normal subgroup of G. We call this the *radical* of G and denote it $R(G)$. The subset of unipotent elements in $R(G)$ is also a normal subgroup in G. We call it the *unipotent radical* of G, denoted by $R_u(G)$. It is the largest connected normal unipotent subgroup of G.

If G is connected, we call it *semisimple* if $R(G)$ is trivial and *reductive* if $R_u(G)$ is trivial. The ranks of $G/R(G)$ and $G/R_u(G)$ are called the *semisimple* and *reductive ranks* of G, respectively.

3.9 Lemma ([32, 7.6.4(ii)]).
If G is a reductive linear algebraic group and T is a maximal torus of G, then $T = C_G(T)$. ∎

3.10 Theorem ([32, 5.5.10, 12.2.2]).
Let G be a linear algebraic group and let H be a closed normal subgroup of G. Then the quotient G/H is also a linear algebraic group. If G and H are defined over the field k, then G/H is also defined over k. ∎

3.2 Root data and the Steinberg presentation

Reductive linear algebraic groups are classified using root data, which we introduce in this section. We start with a brief description of root data using the notation of [12]. More details on root data can be found in [32].

Consider a quadruple $\mathcal{R} = (X, \Phi, Y, \Phi^\star)$, where

- X and Y are free $\mathbb{Z}$-modules of finite rank d with a bilinear pairing $\langle \cdot, \cdot \rangle : X \times Y \to \mathbb{Z}$ putting them in duality.

- Φ and $\Phi^\star$ are finite subsets of X and Y, and we have a bijective map $r \mapsto r^\star$ of Φ onto $\Phi^\star$. We call the elements of Φ *roots* and the elements of $\Phi^\star$ *coroots*.

Assume we have a basis $e_1, \ldots, e_d$ for X and a dual basis $f_1, \ldots, f_d$ for Y, that is $\langle e_i, f_j \rangle = \delta_{ij}$. Given a root r, we define linear maps $s_r : X \to X$ and $s_r^\star : Y \to Y$ by

$$xs_r = x - \langle x, r^\star \rangle r \quad \text{and} \quad ys_r^\star = y - \langle r, y \rangle r^\star.$$

These maps are called *reflections* if $\langle r, r^\star \rangle = 2$.

The quadruple $\mathcal{R} = (X, \Phi, Y, \Phi^\star)$ is called a *root datum* if the following axioms are satisfied for every $r \in \Phi$:

(RD1) s_r and $s_r^\star$ are reflections,

(RD2) Φ is closed under the action of s_r and $\Phi^\star$ is closed under the action of $s_r^\star$.

Note that if we let Q denote the submodule of X generated by Φ and let $V := \mathbb{R} \otimes Q$, then Φ is a root system in V in the sense of Bourbaki [6, Chapter VI]. In a similar way, $\Phi^\star$ is a root system.

A root datum is called *reduced* if r and $-r$ are the only roots in Φ of the form cr with $c \in \mathbb{Q}$, for every $r \in \Phi$. If a root datum is not reduced and $r, cr \in \Phi$ for $c \in \mathbb{Q}$, then $c \in \{\pm\frac{1}{2}, \pm 1, \pm 2\}$, see for example [6, Chapter VI]. A root datum is called *irreducible* if the root system Φ is not a disjoint union of two proper root subsystems.

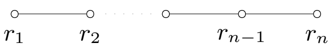
The *Weyl group* $W(\mathcal{R})$ is the group generated by the reflections s_r. We refer to Bourbaki [6, Chapter VI] for the definitions of positive roots, negative roots, fundamental systems, and length of a root.

A *Dynkin diagram* $\mathcal{D}$ of a root datum $\mathcal{R} = (X, \Phi, Y, \Phi^\star)$ is a graph with the vertex set labeled by the fundamental roots. Two distinct vertices r_i and r_j are connected by $\langle r_i, r_j^\star \rangle \langle r_j, r_i^\star \rangle$ edges. If the the number of edges between r_i and r_j is at least 2, then one of the roots r_i and r_j is shorter than the other. We indicate that by placing a less-than sign over the edges. The root data are classified (see for example [6, Chapter VI]) and Table 3.1 shows all Dynkin diagrams for a reduced irreducible root datum. The Dynkin diagram of a reducible root datum is the disjoint union of the Dynkin diagrams of its irreducible components.

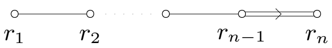
Let G be a reductive linear algebraic group and fix a maximal torus T in G, then a reduced root datum $\mathcal{R} = \mathcal{R}(G, T)$ can be constructed (see [32] for details). Further, $W = W(\mathcal{R})$ is isomorphic to $N_G(T)/T$. By the Isomorphism Theorem [32, 9.6.2], the group G is uniquely determined up to algebraic isomorphism by its root datum and $\bar{k}$.

Table 3.1: Dynkin diagrams of reduced irreducible root data.

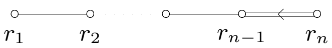
A_n



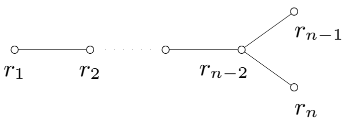
B_n $n \geq 2$



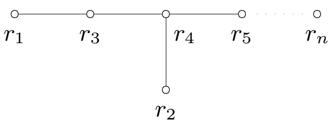
C_n $n \geq 3$



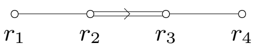
D_n $n \geq 4$



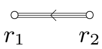
E_n $n \in \{6, 7, 8\}$



F_4



G_2



Let G be a reductive linear algebraic group defined over k, and let G be k-split. Then the group of k-rational points $G(k)$ is called an (untwisted) *group of Lie type*. (Another common way to introduce groups of Lie type is as groups of automorphisms of buildings, as in [35, II.§5].)

There is an important presentation for the group $G(k)$, called the *Steinberg presentation*. Let $\mathcal{R} = (X, \Phi, Y, \Phi^\star)$ be the root datum of G with respect to a k-split maximal torus T. The generators are $x_r(a)$, for r a root and $a \in k$, and $y \otimes t$, for $y \in Y$ and $t \in k^*$. We also define auxiliary generators

$$n_r(t) := x_r(t)x_{-r}(-t^{-1})x_r(t) \quad \text{and} \quad n_r := n_r(1).$$

The relations are

$$\begin{aligned}
(y \otimes t)(y \otimes u) &= y \otimes (tu), \\
(y \otimes t)(z \otimes t) &= (y + z) \otimes t, \\
r^\star \otimes t &= n_r(-1)n_r(t), \\
(y \otimes t)^{n_r} &= y s_r^\star \otimes t, \\
x_r(a)x_r(b) &= x_r(a+b), \\
x_r(a)^{x_{r'}(b)} &= x_r(a) \prod_{i,j>0} x_{ir+jr'}(C_{ijrr'}a^i b^j), \\
x_r(a)^{x_{-r}(t)} &= x_{-r}(-t^2 a)^{x_r(t^{-1})},
\end{aligned} \tag{3.4}$$

where r and r' are linearly independent roots, $y, z \in Y$, $a, b \in k$ and $t, u \in k^*$. The product on the right-hand side of (3.4) runs over roots of the form $ir + jr'$ (for i and j positive integers) in a fixed order. See [12] or [15] for a description of this order and the definition of $C_{ijr\beta}$. The last relation is redundant except when the rank is one. Note that $h_r(t) = r^\star \otimes t$ is another common notation. The generators of the form $x_r(a)$ for $a \neq 0$ are called *root elements*.

We can recover the following important subgroups of $G(k)$ from the Steinberg presentation:

- $T(k)$, the k-rational points of the torus T, is generated by the elements $y \otimes t$.
- $N(k)$, the k-rational points of the normalizer $N := N_G(T)$, is generated by $T(k)$ and the terms n_r.

  For w in the Weyl group W, take the lexicographically smallest reduced expression $w = s_{\beta_1} \cdots s_{\beta_l}$ and set $\dot{w} = n_{\beta_1} \cdots n_{\beta_l}$. There is an isomorphism between $N(k)/T(k)$ and W given by $T(k)\dot{w} \leftrightarrow w$.
- The group of k-rational points $U(k)$ of the standard maximal unipotent subgroup is generated by the elements $x_r(a)$ for r a positive root and $a \in k$.

- $X_r(k) := \{x_r(t) \mid t \in k\}$ is the *root subgroup* of $G(k)$ corresponding to the root $r \in \Phi$.

3.3 Automorphisms

In this section, we give a short overview of algebraic and nonalgebraic automorphisms of reductive algebraic groups.

Let $\mathrm{Aut}(G)$ denote the group of algebraic automorphisms of G, let $\mathrm{Aut}_K(G)$ denote the algebraic automorphisms of G that are defined over K, and let $\mathrm{Aut}(G(K))$ denote the group of automorphisms of $G(K)$ as an abstract group. Note that $\mathrm{Aut}_K(G)$ is the group of K-rational points of $\mathrm{Aut}(G)$.

3.11 Lemma ([18, Theorem 27.4]).
If G is a semisimple linear algebraic group, then $\mathrm{Aut}(G)$ is a linear algebraic group. ■

Although this theorem is only stated for semisimple groups, it can be extended to reductive groups as well.

We consider the following four types of automorphisms on G: A *field automorphism* is an automorphism on G induced by an element of Γ_{sep}. A *inner automorphism* is conjugation by an element of G. A *diagram automorphism* is an automorphism induced by a symmetry of the Dynkin diagram of G. Note further that in types, where all roots have the same length, a diagram automorphism corresponding to a Dynkin diagram symmetry τ is uniquely determined by

$$x_r(t) \mapsto x_{r^\tau}(\lambda_r t),$$

where each λ_r is either 1 or -1 and all these signs are uniquely determined by λ_r for $r \in \Pi$. Further, the signs may be chosen to be 1 for all $r \in \Pi$ (see, for example, [9, Proposition 12.2.3]), in which case we denote the diagram automorphism of G by $\dot{\tau}$.

Field automorphisms are not algebraic, but inner and diagram automorphisms are.

3.12 Lemma ([9, Proposition 12.2.3]).
Let G be a k-split reductive linear algebraic group and T a k-split maximal torus. Denote the group of symmetries of the Dynkin diagram of G by $D := \mathrm{Aut}(\mathcal{D})$ and the group of diagram automorphisms by D'. Then $D'T/T = D$. ■

3.4 Classification of twisted forms

Let G be a linear algebraic group defined over the field k and let K be a Galois extension of k contained in the algebraic closure $\bar{k}$. Since K is separable, it is contained in k_{sep}. Let $\Gamma_{\text{sep}} := \text{Gal}(k_{\text{sep}} : k)$ and $\Gamma := \text{Gal}(K : k)$. Then Γ_{sep} acts continuously on G, as described in Section 3.1, and so Γ_{sep} also acts continuously on $\text{Aut}(G)$, the group of algebraic automorphisms of G as in (2.7) of Chapter 2. Furthermore, actions of Γ on $G(K)$ and on $\text{Aut}_K(G)$ are induced by the actions of Γ_{sep} on G and $\text{Aut}(G)$. The first cohomology $H^1\big(\Gamma_{\text{sep}}, \text{Aut}(G)\big)$ is called the *Galois cohomology* of G. Note that $H^1\big(\Gamma_{\text{sep}}, G\big)$ and $H^1\big(\Gamma_{\text{sep}}, \text{Aut}(G)\big)$ are often denoted $H^1\big(k, G\big)$ and $H^1\big(k, \text{Aut}(G)\big)$ in the literature.

Given $\boldsymbol{\alpha} \in Z^1(\Gamma_{\text{sep}}, \text{Aut}(G))$, we define the $*$-*action* of Γ_{sep} on G with respect to $\boldsymbol{\alpha}$ as in Section 2.3:

$$g * \gamma := g^{\gamma \boldsymbol{\alpha}_\gamma} \qquad \text{for } \gamma \in \Gamma \text{ and } g \in G,$$

and define $G_{\boldsymbol{\alpha}}$ to be the group G with the $*$-action instead of the natural action of Γ_{sep} on G. The group $G_{\boldsymbol{\alpha}}$ is called the *twisted form* of G induced by $\boldsymbol{\alpha}$.

Although G and $G_{\boldsymbol{\alpha}}$ are the same as abstract groups, they have different groups of rational points. Let K be a Galois extension of k contained in $\bar{k}$. Then

$$\begin{aligned} G_{\boldsymbol{\alpha}}(K) &= \{g \in G \mid g * \gamma = g \text{ for all } \gamma \in \text{Gal}(k_{\text{sep}} : K)\} \\ &= \{g \in G \mid g^{\gamma \boldsymbol{\alpha}_\gamma} = g \text{ for all } \gamma \in \text{Gal}(k_{\text{sep}} : K)\}. \end{aligned} \tag{3.5}$$

Note that this agrees with the definition of $G(K)$ in Section 3.1 if we take $\boldsymbol{\alpha}$ to be the trivial cocycle:

$$\begin{aligned} G_{\mathbf{1}}(K) &= \{g \in G \mid g^{\gamma \mathbf{1}_\gamma} = g \text{ for all } \gamma \in \text{Gal}(k_{\text{sep}} : K)\} \\ &= \{g \in G \mid g^{\gamma} = g \text{ for all } \gamma \in \text{Gal}(k_{\text{sep}} : K)\} = G(K). \end{aligned}$$

If G is reductive, then a group of rational points of $G_{\boldsymbol{\alpha}}$ is called a *twisted group of Lie type*.

The following proposition, when applied to $L = k_{\text{sep}}$, states that groups of rational points of two twisted forms are conjugate in $\text{Aut}(G)$ if, and only if, their cocycles are cohomologous. That is, twisted forms of G are classified by $H^1(\Gamma_{\text{sep}}, \text{Aut}(G))$.

3.13 Proposition.
Let G be a linear algebraic group defined over k. Let L be a Galois extension of k contained in $\bar{k}$ and let K be a Galois extension of k contained in L. Let $\Gamma = \text{Gal}(L : K)$. Let $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ be in $Z^1(\Gamma, \text{Aut}_L(G))$. The cocycles $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are cohomologous with respect to $a \in \text{Aut}_L(G)$ (that is, $\boldsymbol{\beta} = \boldsymbol{\alpha}^{(a)}$) if, and only if, $G_{\boldsymbol{\alpha}}(K)^a = G_{\boldsymbol{\beta}}(K)$.

Proof. First suppose we have $a \in \text{Aut}_L(G)$ such that $\boldsymbol{\beta}_\gamma = a^{-\gamma} \boldsymbol{\alpha}_\gamma a$ for all $\gamma \in \Gamma$. Then $g \in G_{\boldsymbol{\beta}}(K)$ if, and only if, $g^{a^{-1}} \in G_{\boldsymbol{\alpha}}(K)$, since

$$g^{a^{-1}} = \big(g^{\gamma \boldsymbol{\beta}_\gamma}\big)^{a^{-1}} = g^{\gamma (a^{-\gamma} \boldsymbol{\alpha}_\gamma a) a^{-1}} = g^{a^{-1} \gamma \boldsymbol{\alpha}_\gamma}$$

for all $\gamma \in \Gamma$. Hence, $G_{\boldsymbol{\alpha}}(K)^a = G_{\boldsymbol{\beta}}(K)$.

Now suppose $G_{\boldsymbol{\alpha}}(K)^a = G_{\boldsymbol{\beta}}(K)$. Then for every $g \in G_{\boldsymbol{\beta}}(K)$ there is an $h \in G_{\boldsymbol{\alpha}}(K)$ with $g = h^a$ and

$$g^{\gamma \boldsymbol{\beta}_\gamma} = g = h^a = \left(h^{\gamma \boldsymbol{\alpha}_\gamma}\right)^a = h^{a a^{-1} \gamma \boldsymbol{\alpha}_\gamma a} = g^{a^{-1} \gamma \boldsymbol{\alpha}_\gamma a} = g^{\gamma a^{-\gamma} \boldsymbol{\alpha}_\gamma a}$$

for all $\gamma \in \Gamma$. Hence, $g^{\boldsymbol{\beta}_\gamma} = g^{a^{-\gamma} \boldsymbol{\alpha}_\gamma a}$ for all $g \in G_{\boldsymbol{\beta}}(K)$, and so $\boldsymbol{\beta}_\gamma = a^{-\gamma} \boldsymbol{\alpha}_\gamma a$. Thus, $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are cohomologous. $\square$

Finally, we state the analogue of the Proposition 2.3 for linear algebraic groups. This is a well-known result.

3.14 Proposition ([32, 12.3.4]).
Let G be a linear algebraic group and let H be a closed normal subgroup, both defined over the field k. Let $\Gamma_{\text{sep}} := \text{Gal}(k_{\text{sep}} \colon k)$. Let $i : H \to G$ be the inclusion map and $\pi : G \to G/H$ the canonical projection map. Let δ^0 and δ^1 be defined as in Proposition 2.3. Then the sequence

$$\begin{gathered} 1 \to H^0(\Gamma, H) \xrightarrow{i^0} H^0(\Gamma, G) \xrightarrow{\pi^0} H^0(\Gamma, G/H) \xrightarrow{\delta^0} \\ \xrightarrow{\delta^0} H^1(\Gamma, H) \xrightarrow{i^1} H^1(\Gamma, G) \xrightarrow{\pi^1} H^1(\Gamma, G/H) \end{gathered}$$

is exact and, if H is a subgroup of the center of G, the sequence obtained by adding

$$\ldots \xrightarrow{\delta^1} H^2(\Gamma, H)$$

on the right is also exact.

Proof. By Theorem 3.10, the quotient G/H is a linear algebraic group defined over k, and G, H, and G/H are Γ-groups as described above. The rest of the proof is analogous to the proof of Proposition 2.3. $\square$

3.5 Computation of the Galois cohomology

In this section, we describe how the Galois cohomology of reductive linear algebraic groups can be computed. In the first step, we compute the cohomology of a finite quotient of the automorphism group $A := \text{Aut}_K(G)$. Then we extend the cocycles to the group A using methods from Section 2.5.

3.5.1 Preliminary results

In this section, we present well known results used in the subsequent sections to compute Galois cohomology.

3.15 Theorem (Springer's Lemma, [30, Lemma III.6]).
Let C be a Cartan subgroup of a linear algebraic group G defined over k, and let $N := N_G(C)$ be the normalizer of C in G. Let $\Gamma_{\text{sep}} := \text{Gal}(k_{\text{sep}}\colon k)$. The canonical map $H^1(\Gamma_{\text{sep}}, N) \to H^1(\Gamma_{\text{sep}}, G)$ is surjective. ■

As in [32, 17.10.1], we say that a field k has *cohomological dimension* ≤ 1 if there are no nontrivial central division algebras over k. Examples include finite fields and the field of rational functions $\mathbb{C}(t)$.

3.16 Theorem ([30, Corollary 3 of Theorem III.3]).
Let G be a linear algebraic group defined over a perfect field k of dimension ≤ 1, let G° be its identity component, and let $\pi : G \to G/G^\circ$ be the standard projection. Then

$$\pi^1 : H^1(\Gamma_{\text{sep}}, G) \to H^1(\Gamma_{\text{sep}}, G/G^\circ)$$

is bijective. ■

The importance of this result for the computation of the Galois cohomology is evident: it reduces the computation of the cohomology on G to the computation of the cohomology on a finite group. An important special case of this theorem is:

3.17 Theorem (Lang's Theorem).
If G is a connected linear algebraic group defined over a finite field k, then

$$H^1(\Gamma_{\text{sep}}, G) = 1.$$ ■

This theorem is often stated in the following, obviously equivalent, form:

3.18 Theorem (Lang's Theorem).
Let G be a connected linear algebraic group defined over a finite field k with $|k| = q$, and let $F : G \to G$ be the field automorphism induced by

$$\bar{k} \to \bar{k}, \quad x \mapsto x^q.$$

Then the map

$$L : G \to G, \quad h \mapsto h^{-F}h$$

is surjective. ■

3.5.2 Cohomology of DW

Let G be k-split reductive linear algebraic group. We use Springer's Lemma 3.15 to compute Galois cohomology. First we compute the cohomology of Γ_{sep} on DW, where W is the Weyl group and D is the symmetry group of the Dynkin diagram of G. This is used to find the Galois cohomology of $\mathrm{Aut}(G)$ in Section 3.5.3.

We start with a general lemma:

3.19 Lemma.
Let A be a Γ'-group with the trivial action. Let Δ be a normal subgroup of Γ' and let $\Gamma := \Gamma'/\Delta$. Then the map

$$i_\Gamma : Z^1(\Gamma, A) \to Z^1(\Gamma', A),$$

defined by

$$i_\Gamma(\boldsymbol{\alpha}) : \gamma \mapsto \boldsymbol{\alpha}_{\gamma\Delta} \quad \text{for } \boldsymbol{\alpha} \in Z^1(\Gamma, A) \text{ and } \gamma \in \Gamma'$$

is an inclusion of pointed sets.

Proof. To avoid large subscripts, we write $\boldsymbol{\alpha}(\gamma)$ instead of $\boldsymbol{\alpha}_\gamma$ in this proof.

Since Γ' acts trivially on A, all cocycles considered here are group homomorphisms. Let $\boldsymbol{\alpha} \in Z^1(\Gamma, A)$ be a cocycle. Set $\boldsymbol{\beta} := i_\Gamma(\boldsymbol{\alpha})$. Then

$$\boldsymbol{\beta}(\gamma_1\gamma_2) = \boldsymbol{\alpha}(\gamma_1\gamma_2\Delta) = \boldsymbol{\alpha}(\gamma_1\Delta\gamma_2\Delta) = \boldsymbol{\alpha}(\gamma_1\Delta)\boldsymbol{\alpha}(\gamma_2\Delta) = \boldsymbol{\beta}(\gamma_1)\boldsymbol{\beta}(\gamma_2)$$

for all $\gamma_1, \gamma_2 \in \Gamma'$. Thus $\boldsymbol{\beta} \in Z^1(\Gamma', A)$. It is also easily seen that $i_\Gamma(\mathbf{1}) = \mathbf{1} \in Z^1(\Gamma', A)$. Thus, i_Γ is a morphism of pointed sets.

For injectivity let $\boldsymbol{\alpha}, \boldsymbol{\alpha}' \in Z^1(\Gamma, A)$ and set $\boldsymbol{\beta} := i_\Gamma(\boldsymbol{\alpha})$ and $\boldsymbol{\beta}' := i_\Gamma(\boldsymbol{\alpha}')$. Suppose $\boldsymbol{\beta} = \boldsymbol{\beta}'$, then we have for all $\gamma \in \Gamma'$:

$$\boldsymbol{\alpha}(\gamma\Delta) = \boldsymbol{\beta}(\gamma) = \boldsymbol{\beta}'(\gamma) = \boldsymbol{\alpha}'(\gamma\Delta).$$

Hence i_Γ is injective. □

We fix some notation: Let T be a k-split maximal torus of G. Let $\mathcal{R} = (X, \Phi, Y, \Phi^\star)$ be the root datum of G with respect to T and Π fundamental system. Write elements of G as words in the Steinberg presentation, as described in Section 3.2. Let N be the normaliser of T in G. Then the Weyl group W is isomorphic to N/T. We have standard representatives $\dot{w}$ for $w \in W$, which are fixed by all field automorphisms, so are contained in $G(k)$. Let $D = \mathrm{Aut}(\mathcal{D})$ be the automorphism group of the Dynkin diagram $\mathcal{D}$ of G. We also identify elements of D with the corresponding automorphisms induced on the root datum $\mathcal{R}$ of G.

Set $\mathrm{Aut}(\mathcal{R})$ to be the set of automorphisms of X preserving Φ. Then $\mathrm{Aut}(\mathcal{R}) = DW$. Indeed, if $s \in \mathrm{Aut}(\mathcal{R})$ leaves Π invariant, it is an element of D. If it does not, Π^s is another fundamental system for Φ and there is a $w \in W$ such that $\Pi^w = \Pi^s$, hence sw^{-1} leaves Π invariant, so is an element of D.

If H is an arbitrary group and $\mathcal{R}$ is a root datum, then a group homomorphism $\varphi : H \to \mathrm{Aut}(\mathcal{R})$ is called a *representation* of H on $\mathcal{R}$. Two representations φ

and ψ of H on $\mathcal{R}$ are *equivalent* if there is an automorphism $a \in \mathrm{Aut}(\mathcal{R})$, such that $\varphi(h) = a^{-1}\psi(h)a$ for all $h \in H$.

3.20 Proposition.
Let Γ_{sep} be the Galois group $\mathrm{Gal}(k_{\mathrm{sep}} : k)$ of the separable closure k_{sep} of k. Then a set of representatives of $H^1(\Gamma_{\mathrm{sep}}, DW)$ is given by

$$\bigcup_{\Gamma} i_\Gamma\big(R(\Gamma)\big),$$

where the union is taken over all subgroups Γ of DW that occur as Galois groups of a Galois extension of k, i_Γ is as in the previous lemma, and $R(\Gamma)$ is a set of representatives of equivalence classes of faithful representations of Γ on $\mathcal{R}$.

Proof. The Galois group Γ_{sep} acts trivially on DW and thus $Z^1(\Gamma_{\mathrm{sep}}, DW)$ is the set of homomorphisms from Γ_{sep} to DW.

Since $DW = \mathrm{Aut}(\mathcal{R})$, each $\boldsymbol{\alpha} \in Z^1(\Gamma_{\mathrm{sep}}, DW)$ gives a representation of Γ_{sep} on $\mathcal{R}$. Moreover, two cocycles $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are cohomologous if, and only if, they are equivalent as representations of Γ_{sep} on $\mathcal{R}$. Thus $H^1(\Gamma_{\mathrm{sep}}, DW)$ is the set of equivalence classes of representations of Γ_{sep} on $\mathcal{R}$.

Assume $\boldsymbol{\alpha} \in Z^1(\Gamma_{\mathrm{sep}}, DW)$ is not injective. Then k has a Galois extension $K \subseteq \bar{k}$ with $\Delta := \ker \boldsymbol{\alpha} = \mathrm{Gal}(k_{\mathrm{sep}} : K)$ and $\Gamma := \Gamma_{\mathrm{sep}}/\Delta \simeq \mathrm{Gal}(K : k)$ by the Fundamental Theorem of Galois theory. Moreover, $\boldsymbol{\alpha} = i_\Gamma(\boldsymbol{\beta})$ for some $\boldsymbol{\beta} \in Z^1(\Gamma, DW)$ by Lemma 3.19 and $\boldsymbol{\beta}$ is a faithful representation.

Hence it is sufficient to consider only faithful representations of Γ on $\mathcal{R}$ for subgroups Γ of DW that occur as Galois groups of a Galois extension of k. $\square$

An immediate consequence of this proposition is that $|DW|$ is a bound on the degree of field extensions that need to be considered.

Note that $H^1(\Gamma, DW)$ can be computed by the methods of Theorem 2.6.

3.5.3 Extension of an induced 1-cocycle

In this section, we extend Theorem 2.6 to $H^1(\Gamma, \mathrm{Aut}_K(G))$, replacing the group equations by polynomial equations. We fix some notation for the rest of this section: Let G be a reductive linear algebraic group defined over the field k and let K be a finite Galois extension of k with Galois group Γ. Let W be the Weyl group of G and let $D := \mathrm{Aut}(\mathcal{D})$ the group of symmetries of the Dynkin diagram $\mathcal{D}$ of G. Let $A := \mathrm{Aut}_K(G)$ and let T be a maximal torus of A. Let $C := C_A(T)$ be a Cartan subgroup of A and let $N := N_A(C)$ be the normaliser of C in A.

3.21 Lemma.
Suppose $T = C$. Then $N = D' \cdot T \cdot N_G(T \cap G)$, where D' is the subgroup of A generated by the diagram automorphisms. Further, $N^\circ = T$ and $N/N^\circ \simeq DW$.

Proof. N is the normaliser of the maximal torus T, hence consists of all diagonal and diagram automorphisms, all conjugations by a Weyl or a torus element of G, and their products. The connected component N° consists of all diagonal automorphisms. Finally,

$$N/N^\circ = D'TN_G(T \cap G)/T \simeq DW. \qquad \square$$

Using the previous lemma and Section 3.5.2 we can compute the cohomology on N/N°. Next we have to extend the cocycles on N/N° to cocycles on N. This is done using methods of Section 2.5. Since the group N is in general not finite, solving group equations directly is not feasible. We therefore replace group equations over N by polynomial equations in several steps.

First we describe how to replace group equations over N by equations over W and equations over T. Let $\boldsymbol{\alpha} \in Z^1(\Gamma, N/N^\circ)$. Recall the notation of Theorem 2.6: Let $\Gamma = \langle \gamma_1, \ldots, \gamma_k \mid r_1, \ldots, r_\ell \rangle$. Since Γ is finite, we may take r_i to be words in $\gamma_1, \ldots, \gamma_k$ not involving inverses. We fix a set $\{t(x) \in N \mid x \in N/N^\circ\}$ of coset representatives and introduce indeterminates $b(\gamma_1), \ldots, b(\gamma_k)$ over N°.

Decompose the coset representatives $t(\boldsymbol{\alpha}_{\gamma_i}) = \dot{\tau}_{\gamma_i} t_{\gamma_i} \dot{w}_{\gamma_i}$ with $\tau_{\gamma_i} \in D$, $t_{\gamma_i} \in T$, and $w_{\gamma_i} \in W$. Decompose the indeterminates $b(\gamma_i) = s_{\gamma_i} \dot{v}_{\gamma_i}$ into new indeterminates $s_{\gamma_i} \in T$ and $v_{\gamma_i} \in W$. Then, for every relator $r = \prod_{i=1}^m \sigma_i$, the equation

$$\prod_{i=1}^m \left(\left(t(\boldsymbol{\alpha}_{\sigma_i}) b(\sigma_i) \right)^{\prod_{j=i+1}^m \sigma_j} \right) = 1, \tag{3.6}$$

corresponding to (2.8) and (2.9), is equivalent to equation

$$\prod_{i=1}^m \tau_{\sigma_i} w_{\sigma_i} v_{\sigma_i} = 1 \tag{3.7}$$

in DW with indeterminates v_{γ_i}, and, for each given solution of (3.7), the equation

$$\prod_{i=1}^m \dot{\tau}_{\sigma_i} \dot{w}_{\sigma_i} \dot{v}_{\sigma_i} \prod_{i=1}^m (t_{\sigma_i}^{\dot{w}_{\sigma_i}} s_{\sigma_i})^{X_i} = 1 \tag{3.8}$$

in T with indeterminates s_{γ_i}, where

$$X_i = \dot{v}_{\sigma_i} \prod_{j=i+1}^m \dot{\tau}_{\sigma_j} \dot{w}_{\sigma_j} \dot{v}_{\sigma_j} \sigma_j.$$

To see this, we use the simple fact that $xy = yx^y$ for elements of a group and that all $\dot{\tau}_{\sigma_i}, \dot{w}_{\sigma_i}$, and $\dot{v}_{\sigma_i}$ commute with field automorphisms, we obtain (3.8) from (3.6). Now

$$\prod_{i=1}^m \dot{\tau}_{\sigma_i} \dot{w}_{\sigma_i} \dot{v}_{\sigma_i} = \left(\prod_{i=1}^m (t_{\sigma_i}^{\dot{w}_{\sigma_i}} s_{\sigma_i})^{X_i} \right)^{-1} \in T$$

and thus

$$\prod_{i=1}^{m} \tau_{\sigma_i} w_{\sigma_i} v_{\sigma_i} = 1.$$

Note that the right hand side of (3.8) is $1_A = \mathrm{id}_G$, and hence is conjugation by an element from $Z(G)$.

Let $K[x_1, \dots, x_\ell]$ be a polynomial ring. A formal sum

$$p = \sum_{i=0}^{n} a_i \prod_{j=1}^{m_i} y_j^{\alpha_{ij}},$$

where n and m_i are nonnegative integers, $a_i \in K$, $\alpha_{ij} \in \Gamma$, and $y_j \in \{x_1, \dots, x_\ell\}$, is called a *(multivariate) polynomial over K with field automorphisms*. The *total degree* of p is $\max\{m_0, \dots, m_n\}$.

Fix a solution $v_{\gamma_i} \in W$ of (3.7). We now show that the group equation (3.8) is equivalent to a polynomial equation with field automorphisms. The left hand side of the equation

$$\prod_{i=1}^{m} (t_{\sigma_i}^{\dot{w}_{\sigma_i}} s_{\sigma_i})^{X_i} = \Big(\prod_{i=1}^{m} \dot{\tau}_{\sigma_i} \dot{w}_{\sigma_i} \dot{v}_{\sigma_i} \Big)^{-1}$$

is a torus element involving indeterminates. The right hand side is a known torus element. Now we replace every indeterminate s_{σ_i} over T by a d-tuple of indeterminates over K, using the isomorphism $T \simeq \mathrm{G_m}^d$. Then the left hand side becomes a d-tuple of polynomials with field automorphisms and the equation is now equivalent to d polynomial equations with field automorphisms.

We now describe how to replace polynomials with a field automorphism by ordinary polynomials. Let p be a polynomial with field automorphisms over K in ℓ variables of total degree n. Let $r := [K : k]$ and let $(b_1, \dots, b_r)$ be a basis of K as a vector space over k. Substitute the formal sum $\sum_{j=1}^{r} b_j x_{ij}$ for every indeterminate x_i of p, where $x_{i1}, \dots, x_{ir}$ are new indeterminates over the field k. Then p becomes an ordinary polynomial s over K of the same total degree n with $r\ell$ variables. The map

$$\big(a_{ij} \in k \mid i = 1, \dots, \ell,\ j = 1, \dots, r\big) \mapsto \Big(\sum_{j=1}^{r} b_j a_{ij} \mid i = 1, \dots, \ell\Big)$$

is a bijection between the set of zeros of s in $k^{r\ell}$ and the set of zeros of p in K^ℓ.

A simpler approach is available when K is a finite field: Every $\gamma \in \Gamma$ has the form $\gamma : x \mapsto x^{q^m}$ for some m, where q is the size of k. Substituting x^{q^m} for x^γ provides an ordinary polynomial s' of degree at most $q^m n$ in the same number of variables. The zero sets of p and s' are the same. The systems of polynomial

Table 3.2: Timings for computation of Gröbner Bases.

Group	$[K : k]$	time
$\mathrm{A}_6(5)$	2	6.250
$\mathrm{A}_7(5)$	2	66.980
$\mathrm{E}_6(5)$	2	2.070
$\mathrm{D}_4(5)$	6	157.980
$\mathrm{D}_5(5)$	2	0.700

equations obtained by this method can be solved relatively easily by the Walk method [13] for Gröbner Basis computation, as can be seen from the Table 3.2

We have now proved the following proposition:

3.22 Proposition.
Let $\boldsymbol{\alpha} \in Z^1(\Gamma, N/N^\circ)$ and suppose $T = C$. Let v_{γ_i} be indeterminates over W for $\gamma_1, \dots, \gamma_k$ and let $s_{\gamma_i,j}$ be indeterminates over K for $\gamma_1, \dots, \gamma_k$ and $j = 1, \dots, d$, where d is the dimension of T. Set $s_{\gamma_i} = (s_{\gamma_i,1}, \dots, s_{\gamma_i,d}) \in T$. Consider the system of equations given by (3.7) and (3.8) for every relator $r = \prod_{i=1}^m \sigma_i$.

(a) This system is solvable if, and only if, $\boldsymbol{\alpha}$ can be extended to a cocycle on N.

(b) For every solution of this system,

$$\boldsymbol{\beta} := [\![t(\boldsymbol{\alpha}_{\gamma_1}) \cdot s_{\gamma_1} \dot{v}_{\gamma_1},\ \dots,\ t(\boldsymbol{\alpha}_{\gamma_k}) \cdot s_{\gamma_k} \dot{v}_{\gamma_k}]\!]$$

is a 1-cocycle on N, such that $\overline{\boldsymbol{\beta}} = \boldsymbol{\alpha}$.

(c) Every cocycle $\boldsymbol{\beta} \in Z^1(\Gamma, N)$ with $\overline{\boldsymbol{\beta}} = \boldsymbol{\alpha}$ can be constructed this way.

(d) A representative of every class $[\boldsymbol{\beta}] \in H^1(\Gamma, A)$ can be constructed this way.

□

If A is reductive, then $T = C$ and Proposition 3.22 can be applied.

3.5.4 Conclusion

We now give some general remarks on the presented algorithms. We know N/N° from Lemma 3.21 and compute the finite cohomology $H^1\big(\Gamma, N/N^\circ\big)$ as described in Section 2.6 and extend its representatives to cocycles on $\mathrm{Aut}_K(G)$ using Proposition 3.22. We solve the system (3.7) of group equations over the

Weyl group W and the corresponding system (3.8) of polynomial equations. The polynomial equations are solved using methods for Gröbner bases.

In general, all solutions of these systems of equations must be found. The importance of Lemma 3.16 is that, whenever it holds, only one solution for each system of equations is required.

We now discuss the cases where Lemma 3.16 cannot be applied. If the field k is not perfect or not of dimension ≤ 1, then one of the following can happen:

1. The same cocycle from $Z^1(\Gamma, N/N^\circ)$ can be extended to (at least) two non-cohomologous cocycles in $Z^1(\Gamma, N)$.

   For example, $A = \mathrm{Aut}(\mathrm{SL}_2) \simeq \mathrm{PGL}_2$ is connected, thus $A/A^\circ \simeq 1$ and there is only the trivial cocycle to extend. This lifts to the trivial cocycle and to $[\![c_h]\!]$ with $h = \left(\begin{smallmatrix} & 1 \\ c & \end{smallmatrix}\right)$ and $c \notin N_k^K(K)$. (See Case 1 after the proof of Proposition 4.12 in Section 4.5.1.)

2. Some cocycles in $Z^1(\Gamma, N/N^\circ)$ may have no extensions in $Z^1(\Gamma, N)$.

   In this case Gröbner basis methods would show that there are no solutions.

3.6 Example: GL_1

In this section, we explicitly compute the cocycles and twisted forms of GL_1. See Section 4.5 for more examples. Recall the group $G := \mathrm{G_m} = \mathrm{GL}_1$ defined in the Section 3.1:

$$G = \{(x, y) \in \bar{k}^2 \mid xy - 1 = 0\}$$

with the multiplication $(x_1, y_1) \cdot (x_2, y_2) := (x_1 x_2, y_1 y_2)$.

For any Galois extension K of k contained in $\bar{k}$, the group of rational points is

$$\begin{aligned} G(K) &= \{(x, y) \in K^2 \mid xy = 1\} \\ &= \{(x, y) \in K^2 \mid y = x^{-1}, x \neq 0\} \simeq K^* \end{aligned}$$

By considering polynomials in the variables x and y, which define group automorphisms, we see that the group of algebraic automorphisms of G is

$$\mathrm{Aut}(G) = \langle \tau \rangle$$

with $\tau : (x, y) \mapsto (y, x)$. Note that $\tau^2 = 1$ and $\mathrm{Aut}(G) = \mathrm{Aut}_K(G)$ for every K.

Now suppose K is an extension of degree 2 and set $\Gamma := \mathrm{Gal}(K : k) = \langle \gamma \rangle$. Consider $\boldsymbol{\alpha} \in Z^1\big(\Gamma, \mathrm{Aut}_K(G)\big)$. Since every cocycle in $Z^1\big(\Gamma, \mathrm{Aut}_K(G)\big)$ is uniquely determined by the image of γ, we have two cases:

Case 1: The trivial cocycle $\mathbf{1}$. Then $G_{\mathbf{1}}(k) = G(k) \simeq k^*$.

Case 2: $\boldsymbol{\alpha} = [\![\tau]\!]$. Then

$$\begin{aligned}
G_{\boldsymbol{\alpha}}(k) &= \{g \in G(K) \mid g^{\gamma \boldsymbol{\alpha}_\gamma} = g\} \\
&= \{(x,y) \in K^2 \mid xy = 1 \text{ and } (x,y)^{\gamma\tau} = (x,y)\} \\
&= \{(x,y) \in K^2 \mid xy = 1 \text{ and } y = x^\gamma\} \\
&= \{(x,y) \in K^2 \mid xx^\gamma = 1 \text{ and } y = x^\gamma\} \\
&\simeq \{x \in K \mid xx^\gamma = 1\}.
\end{aligned}$$

That is, $G_{\boldsymbol{\alpha}}(k)$ is the set of norm 1 elements of K. In other words, $G_{\boldsymbol{\alpha}}(k)$ is the subgroup of unitary matrices of GL_1.

In the case $k = \mathbb{F}_q$, we have $K = \mathbb{F}_{q^2}$, $\gamma : x \mapsto x^q$,

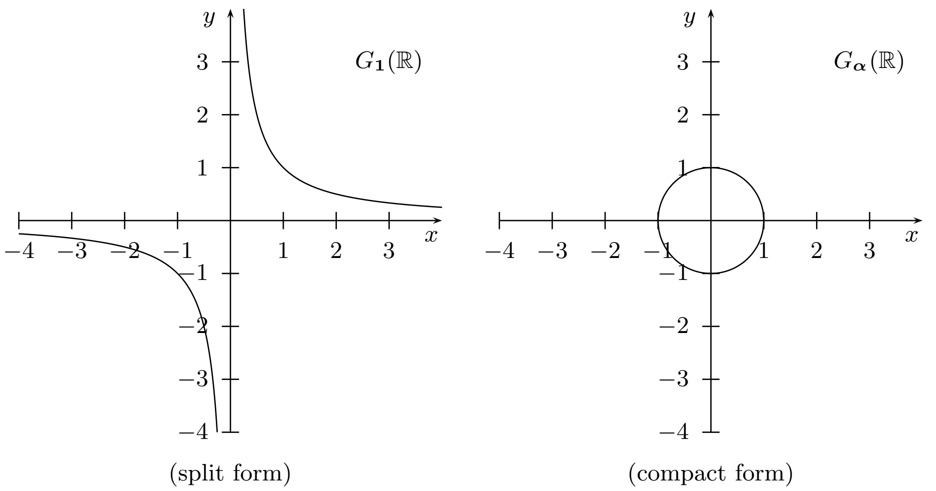
$$\begin{aligned}
G_{\mathbf{1}}(k) &\simeq \{x \in K \mid x^{q-1} = 1\}, \qquad \text{and} \\
G_{\boldsymbol{\alpha}}(k) &\simeq \{x \in K \mid x^{q+1} = 1\}.
\end{aligned}$$

In the case $k = \mathbb{R}$ and $K = \mathbb{C}$, we have $\gamma : a + ib \mapsto a - ib$,

$$\begin{aligned}
G_{\mathbf{1}}(k) &\simeq \{(x,y) \in k^2 \mid xy = 1\} \qquad \text{and} \\
G_{\boldsymbol{\alpha}}(k) &\simeq \{x \in K \mid xx^\gamma = 1\} \\
&\simeq \{(a,b) \in k^2 \mid a^2 + b^2 = 1\}.
\end{aligned}$$

The groups of $\mathbb{R}$-rational points of $G_{\mathbf{1}}$ and $G_{\boldsymbol{\alpha}}$ are shown in Figure 3.1.

Figure 3.1: $\mathbb{R}$-rational points of $G_{\mathbf{1}}$ and $G_{\boldsymbol{\alpha}}$.



Chapter 4

Twisted forms

In this chapter, we study twisted forms of reductive linear algebraic groups. That is, we are given a reductive k-split linear algebraic group G defined over a field k and a cocycle $\boldsymbol{\alpha} \in H^1(\Gamma_{\mathrm{sep}}, \mathrm{Aut}(G))$, where $\Gamma_{\mathrm{sep}} := \mathrm{Gal}(k_{\mathrm{sep}}\colon k)$ is the Galois group of the separable closure of k. Using Springer's Lemma 3.15, we can assume that $\boldsymbol{\alpha}$ stabilizes the standard k-split torus T. Then, as in Section 3.4, the group of k-rational points of the twisted form $G_{\boldsymbol{\alpha}}$ is

$$G_{\boldsymbol{\alpha}}(k) = \{g \in G \mid g^{\gamma \boldsymbol{\alpha}_\gamma} = g \ \forall \gamma \in \Gamma_{\mathrm{sep}}\}.$$

One can easily determine if a given element $g \in G$ lies in $G_{\boldsymbol{\alpha}}(k)$ or not. This is not satisfactory for computing with $G_{\boldsymbol{\alpha}}(k)$ however, since this definition gives us no nontrivial elements to work with. To this end, we develop algorithms for computing the normal subgroup $G_{\boldsymbol{\alpha}}(k)^\dagger$ of $G_{\boldsymbol{\alpha}}(k)$ generated by the root elements. This also provides a presentation for $G_{\boldsymbol{\alpha}}(k)^\dagger$.

The quotient $G_{\boldsymbol{\alpha}}(k)/G_{\boldsymbol{\alpha}}(k)^\dagger$ is called the *Whitehead group*, see for example [38]. The determination of the Whitehead group is very hard in general. In [23, Chapter 9], a general overview is given and, among other results, the Whitehead group is proven to be trivial for algebraic number fields in all types other than ${}^2\mathrm{E}_6$. We expect that our methods will be useful for determining the Whitehead group.

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 root lattice X is not a linear map. We expect though, that our method will work if we replace X, which is a $\mathbb{Z}$-module spanned by the fundamental system Π, 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 ${}^2\mathrm{G}_2$.

4.1 Relative root system

Just as the Steinberg presentation for $G(k)$ is based on a root datum, the presentation for $G_{\boldsymbol{\alpha}}(k)^{\dagger}$ is based on a relative root system, which we describe in this section. Our description is based on Satake [27] and Schattschneider [28].

First we make the connection between our notation and the notation in [28]. As usual, set $A := \mathrm{Aut}(G)$, $\Gamma := \Gamma_{\mathrm{sep}} = \mathrm{Gal}(k_{\mathrm{sep}} \colon k)$, and let $\boldsymbol{\alpha} \in Z^1(\Gamma, N_A(T))$ be a fixed cocycle. Let $\mathcal{R} = (X, \Phi, Y, \Phi^{\star})$ be the root datum of G with fundamental system Π.

As shown in Section 3.5.2, $H^1(\Gamma, N_A(T)/(N_A(T))^{\circ}) \simeq H^1(\Gamma, DW)$ and cocycles of DW are homomorphisms from Γ to DW. Since $DW \simeq \mathrm{Aut}(\mathcal{R})$, a cocycle determines an action of Γ on $\mathcal{R}$ and thus a permutation action on the root system Φ. This is the Γ-action in [28].

Let $\mathcal{O}_{\boldsymbol{\alpha}}(\chi)$ denote the orbit of $\chi \in X$ under the Γ-action corresponding to the cocycle $\boldsymbol{\alpha}$. By [28, (16)], 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

$$\sum_{s \in \mathcal{O}_{\boldsymbol{\alpha}}(r)} s = 0, \tag{4.1}$$

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

$$X_0 := \{\chi \in X \mid \sum_{\gamma \in \Gamma} \chi^{\boldsymbol{\alpha}_\gamma} = 0\} \qquad \text{and} \tag{4.2}$$

$$X^{\Gamma} := \{\chi \in X \mid \chi^{\boldsymbol{\alpha}_\gamma} = \chi \text{ for all } \gamma \in \Gamma\} \tag{4.3}$$

Let $\Phi_0 := \Phi \cap X_0$ and $\Pi_0 := \Pi \cap X_0$. Then, by [28, §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 4.1).

Set $\bar{X} := X/X_0$ and let $\pi : X \to \bar{X}$ be the standard projection. Then $\bar{X}$ is a free $\mathbb{Z}$-module and π is a homomorphism of modules. Let Ψ and Δ be the images under π of $\Phi \setminus \Phi_0$ and $\Pi \setminus \Pi_0$, respectively. Then Ψ is a root system and Δ is a fundamental system of it. We call Ψ the *relative root system* and Δ the *relative fundamental system*. Note that Ψ need not be irreducible nor reduced even if Φ is. The rank of the relative system is $|\Delta|$ and is called the *relative* *rank* of $G_{\boldsymbol{\alpha}}$, whereas the rank $|\Pi|$ of Φ is called the *absolute rank*. 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 form 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 [28, §2],

$$\pi^{-1}(\delta) = \dot{\bigcup_{r \in J_\delta}} \mathcal{O}_{\boldsymbol{\alpha}}(r) \subseteq \Phi^+ \setminus \Phi_0. \tag{4.4}$$

We now construct an action of Γ on Π induced by the action on Φ. Remember that $\boldsymbol{\alpha}_\gamma = \tau w$ for some $\tau \in D$, $w \in W$. Then γ acts on Π by

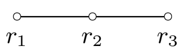
$$r \mapsto r^\tau.$$

This is the $[\Gamma]$-action of [28]. 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 [28, Proposition 3.5],

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

Computation of the actions of Γ on Φ and on Π, as well as the orbits of both actions, is straightforward using the definitions, and is very fast. For example, in type A_{20}, the computation takes less than 2 seconds on a Pentium 1.6 GHz.

4.1 Example.
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 $\boldsymbol{\alpha} = [\![\tau s_2]\!]$, 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

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

Finally, we state several basic results that are used in Section 4.3

4.2 Lemma.
Let r and s be positive roots with $r \in \Phi^+ \setminus \Phi_0$. If $r+s \in \Phi$ then $r+s \in \Phi^+ \setminus \Phi_0$.

Proof. Every positive root is a unique linear combination of roots in Π with non-negative coefficients. 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. But then the coefficient of this fundamental root in the linear combination of $r + s$ is also positive. □

For the next lemma, recall that the only scalar multiples of a root r in a (not necessarily reduced) root system are $\pm\frac{1}{2}r$, $\pm r$ and $\pm 2r$.

4.3 Lemma.
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. By the previous lemma, $ir+js \in \Phi^+\setminus\Phi_0$, and, since π 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. □

Recall from Section 3.2 the notation for the maximal unipotent subgroup $U(K)$ of $G(K)$ and the root subgroups.

4.4 Corollary.
Suppose $\delta \in \Psi^+$ but $2\delta \notin \Psi$ and let $r, s \in \pi^{-1}(\delta)$. Then $[X_r, X_s] = 1$.

Proof. By Equation (3.4) in Section 3.2, $[x_r(u), x_s(v)]$ is a product of root elements corresponding to roots in Φ^+ that have the form $ir + js$ for positive integers i and j. But if $ir + js$ is a root for some positive integers i and j, then $i = j = 1$ and $\pi(r + s) = 2\delta \in \Psi$ by Lemma 4.3, a contradiction to $2\delta \notin \Psi$. □

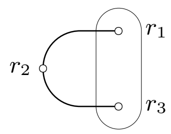
4.5 Corollary.
Suppose $\delta, 2\delta \in \Psi^+$ and let $r \in \pi^{-1}(\delta)$, $s \in \pi^{-1}(2\delta)$. Then $[X_r, X_s] = 1$.

Proof. The commutator $[x_r(u), x_s(v)]$ is a product of root elements corresponding to roots in Φ^+ that have the form $ir+js$ with positive integers i and j. But if $ir+js$ is a root for some positive integers i and j, then $\pi(ir+js) = (i+2j)\delta \in \Psi$ by Lemma 4.3 and $i + 2j \geq 3$, a contradiction. □

4.2 Tits indices

In this section, we describe a graphic notation for relative root systems called the *Tits index* (see e.g., [37]). It is the Dynkin diagram of the absolute root system of G together with additional data. We call a vertex of the Dynkin diagram *distinguished* if the corresponding fundamental root r is not contained 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.

We use the same terminology for the Tits indices as in [37]: A Tits index is denoted by ${}^{g}M^{t}_{n,\ell}$, 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. To emphasize the difference in the notation, t is put in parenthesis 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.

Note that the computations of the previous section also allow the Tits index to be computed from the cocycle $\boldsymbol{\alpha}$.

To compute a cocycle of the linear algebraic group corresponding to a given Tits index, one first has to read the action on Π off the diagram and then find Weyl group elements such that $[\![\tau_1 w_1, \ldots, \tau_n w_n]\!]$ is a cocycle of Γ on DW. Then a cocycle on G is given by $\boldsymbol{\alpha} = [\![\dot{\tau}_1 \dot{w}_1 h_1, \ldots, \dot{\tau}_n \dot{w}_n h_n]\!]$, where $h_1, \ldots, h_n$ are torus elements that need to be chosen according to Proposition 3.22, that is, by solving a system of polynomial equations.

Note that different h_i may give noncohomologous cocycles. The corresponding forms, however, only differ on the anisotropic kernel.

4.3 Root subgroups

The *(standard) unipotent subgroup* of $G_{\boldsymbol{\alpha}}(k)$ is $U_{\boldsymbol{\alpha}}(k) := U(K) \cap G_{\boldsymbol{\alpha}}(k)$. We now describe the root elements and root subgroups of $U_{\boldsymbol{\alpha}}(k)$. Let $\gamma \in \Gamma$, let $\boldsymbol{\alpha}_\gamma = \tau n$ for $n \in N$, and let $w \in W$ be the image of n under the natural homomorphism. Then 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

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

where $\lambda_{r\gamma}$ is a constant that depends on the root r and, for a fixed cocycle $\boldsymbol{\alpha}$, on γ. Let $\delta \in \Psi$ be a relative root. Its preimages are, as described by (4.4),

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

Symbolically construct a K-vector space V_δ with basis J_δ and denote by t_r the coefficient of $r \in J_\delta$ in the linear combination of $t \in V_\delta$. For $t \in V_\delta$ set

$$u_\delta(t) = \prod_{r \in J_\delta} \prod_{\gamma \in \Gamma} x_r(t_r)^{\gamma\boldsymbol{\alpha}_\gamma}, \tag{4.5}$$

where the whole product is taken in the ordering of the roots fixed for the unique decomposition of U in Section 3.2, and set

$$U_\delta = \{u_\delta(t) \mid t \in V_\delta\}. \tag{4.6}$$

Then $u_\delta(t)^{\gamma\boldsymbol{\alpha}_\gamma}$ is the product of the same terms taken in a different order, since

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

and so $u_\delta(t)^{\gamma\boldsymbol{\alpha}_\gamma} = u_\delta(t)c_\gamma(t)$. In other words, we set $c_\gamma(t) := u_\delta(t)^{-1}u_\delta(t)^{\gamma\boldsymbol{\alpha}_\gamma}$. The following lemma provides a description of $c_\gamma(t)$. If $\delta, 2\delta \in \Psi$, set

$$Y_{2\delta} := \prod_{r \in \pi^{-1}(2\delta)} X_r(K).$$

4.6 Lemma.
If $2\delta \notin \Psi$, then $c_\gamma(t) = 1$ for all $\gamma \in \Gamma$. Otherwise $c_\gamma(t) \in Y_{2\delta}$.

Proof. If 2δ is not a relative root, then all root elements in the product (4.5) commute by Corollary 4.5.

If $2\delta \in \Psi$, then $c_\gamma(t)$ is a product of commutators of pairs of root elements from the product (4.5). Let $r, s \in \pi^{-1}(\delta)$ be two roots. By Lemma 4.3, the commutator of root elements corresponding to these roots is a single root element corresponding to the root $r + s \in \pi^{-1}(2\delta)$. □

Let $\delta \in \Psi$ be a relative root. First we consider the case $2\delta \notin \Psi$. In this case we define the *relative root elements* to be

$$x_\delta(t) := u_\delta(t) \tag{4.7}$$

for $t \in V_\delta$ and the *relative root subgroups* $X_\delta := U_\delta$. Indeed, X_δ is an (abstract) abelian group by Lemma 4.6 with relations

$$\begin{aligned} x_\delta(t) \cdot x_\delta(s) &= x_\delta(t+s), \\ x_\delta(t)^{-1} &= x_\delta(-t), \\ \big[x_\delta(t), x_\delta(s)\big] &= 1 \end{aligned}$$

for $t, s \in V_\delta$.

Now consider the case where 2δ is also a relative root. Choose an arbitrary $u := u_\delta(t)$ and compute $c_\gamma(t) := u^{-1}u^{\gamma\boldsymbol{\alpha}_\gamma}$ for all $\gamma \in \Gamma$. We need a correction term $v \in U(K)$ such that

$$uv = (uv)^{\gamma\boldsymbol{\alpha}_\gamma} = u^{\gamma\boldsymbol{\alpha}_\gamma} v^{\gamma\boldsymbol{\alpha}_\gamma} = uc_\gamma(t)v^{\gamma\boldsymbol{\alpha}_\gamma} \quad \text{for all } \gamma \in \Gamma,$$

which is equivalent to

$$c_\gamma(t) = vv^{-\gamma\boldsymbol{\alpha}_\gamma} \qquad \text{for all } \gamma \in \Gamma.$$

4.7 Lemma.

(a) For a given t, the map $\boldsymbol{\rho} : \gamma \mapsto c_\gamma(t)$ is a cocycle in $Z^1(\Gamma, Y_{2\delta})$.

(b) There is a solution v for the system of equations

$$c_\gamma(t) = vv^{-\gamma\boldsymbol{\alpha}_\gamma}, \quad \gamma \in \Gamma. \tag{4.8}$$

Proof. To show that $\boldsymbol{\rho}$ is a cocycle, we compute

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

Hence, $c_{\gamma\gamma'}(t) = c_\gamma(t)^{\gamma'\boldsymbol{\alpha}_{\gamma'}}c_{\gamma'}(t)$. But $Y_{2\delta}$ is unipotent, thus $H^1(\Gamma, Y_{2\delta}) = 1$ and the constructed cocycle is cohomologous to the trivial one, that is, there is an element $v \in Y_{2\delta}$ such that $c_\gamma(t) = vv^{-\gamma\boldsymbol{\alpha}_\gamma}$ for all $\gamma \in \Gamma$. □

A method to construct such a solution v for given elements $c_\gamma(t)$ is discussed in the Section 4.4 below.

4.8 Lemma.
For given $c_\gamma(t)$, $\gamma \in \Gamma$, the set of solutions $v \in Y_{2\delta}$ for (4.8) is the coset $v_1X_{2\delta}$, where v_1 is any particular solution for this equation system.

Proof. Let v be a solution of (4.8) and $x \in X_{2\delta}$, then $vx \in Y_{2\delta}$ and

$$(vx)(vx)^{-\gamma\boldsymbol{\alpha}_\gamma} = vxx^{-\gamma\boldsymbol{\alpha}_\gamma}v^{-\gamma\boldsymbol{\alpha}_\gamma} = vxx^{-1}v^{-\gamma\boldsymbol{\alpha}_\gamma} = vv^{-\gamma\boldsymbol{\alpha}_\gamma} = c_\gamma(t)$$

for all $\gamma \in \Gamma$. Let on the other hand, v_1 and v_2 be two solutions for (4.8), then

$$v_2v_2^{-\gamma\boldsymbol{\alpha}_\gamma} = c_\gamma(t) = v_1v_1^{-\gamma\boldsymbol{\alpha}_\gamma} \;\Rightarrow\; v_1^{-1}v_2 = v_1^{-\gamma\boldsymbol{\alpha}_\gamma}v_2^{\gamma\boldsymbol{\alpha}_\gamma} = (v_1^{-1}v_2)^{\gamma\boldsymbol{\alpha}_\gamma},$$

for all $\gamma \in \Gamma$, thus $v_1^{-1}v_2 \in X_{2\delta}$. □

Now we can define the *relative root elements* in the case $\delta \in \Psi$ with $2\delta \in \Psi$ to be

$$x_\delta(t) := u_\delta(t)v(t) \tag{4.9}$$

for $t \in V_\delta$, where $v(t) \in Y_{2\delta}$ is an arbitrary fixed solution for (4.8). Define the *relative root subgroups* to be

$$X_\delta := \big\langle X_{2\delta};\; x_\delta(t) \mid t \in V_\delta \big\rangle.$$

Note that, by Lemma 4.8, the definition of X_δ does not depend on the choice of the elements $v(t)$ in (4.9).

4.9 Lemma.

(a) $X_{2\delta}$ is a central subgroup of X_δ and $X_\delta = \big\langle x_\delta(t) \mid t \in V_\delta \big\rangle X_{2\delta}$.

(b) $X_\delta = \big\{ x_\delta(t)x_{2\delta}(s) \mid t \in V_\delta, s \in V_{2\delta} \big\}$

Proof. (a) follows from the fact that elements $x_\delta(t)$ and $x_{2\delta}(s)$ commute for any $t \in V_\delta$, $s \in V_{2\delta}$ by Corollary 4.5.

For (b), the inclusion of the right hand side in X_δ is trivial. For the other inclusion, let $x_\delta(t) = u_\delta(t)v(t)$ and $x_\delta(s) = u_\delta(s)v(s)$ for $t, s \in V_\delta$. Then

$$\begin{aligned} x_\delta(t)x_\delta(s) &= u_\delta(t)v(t)u_\delta(s)v(s) = u_\delta(t)u_\delta(s)v(t)v(s) \\ &= u_\delta(t+s)y(t,s)v(t)v(s), \end{aligned}$$

where $y(t,s)$ is a product of root elements corresponding to roots in $\pi^{-1}(2\delta)$, and depends on t and s.

Now the element $x_\delta(t)x_\delta(s)$ is fixed by $\gamma\boldsymbol{\alpha}_\gamma$ and we have

$$\begin{aligned} u_\delta(t+s)y(t,s)v(t)v(s) &= \big(u_\delta(t+s)y(t,s)v(t)v(s)\big)^{\gamma\boldsymbol{\alpha}_\gamma} \\ &= u_\delta(t+s)^{\gamma\boldsymbol{\alpha}_\gamma}\big(y(t,s)v(t)v(s)\big)^{\gamma\boldsymbol{\alpha}_\gamma} \\ &= u_\delta(t+s)c_\gamma(t+s)\big(y(t,s)v(t)v(s)\big)^{\gamma\boldsymbol{\alpha}_\gamma}, \end{aligned}$$

where $c_\gamma(t+s)$ is as before and

$$c_\gamma(t+s) = \big(y(t,s)v(t)v(s)\big)\big(y(t,s)v(t)v(s)\big)^{-\gamma\boldsymbol{\alpha}_\gamma}.$$

Hence $y(t,s)v(t)v(s) \in v(t+s)X_{2\delta}$ by Lemma 4.8 and

$$x_\delta(t)x_\delta(s) = u_\delta(t+s)y(t,s)v(t)v(s) \in x_\delta(t+s)X_{2\delta}. \qquad \square$$

Finally

$$x_\delta(t)x_\delta(s) \in x_\delta(t+s)X_{2\delta}, \tag{4.10}$$
$$x_\delta(t)^{-1} \in x_\delta(-t)X_{2\delta}, \tag{4.11}$$
$$\big[x_\delta(t), x_\delta(s)\big] \in X_{2\delta}. \tag{4.12}$$

In particular, X_δ is nilpotent of nilpotency class 2. The exact relations between relative root elements of this form can be easily computed inside the original untwisted group of Lie type. For each group, we compute them for generic relative root elements once, so we can use them for computations.

4.10 Proposition.

$$U_{\boldsymbol{\alpha}}(k) = \langle X_\delta \mid \delta \in \Psi^+\rangle.$$

Proof. Let $u \in U_{\boldsymbol{\alpha}}(k)$ be an arbitrary element. Write the unique decomposition of u as a product of root elements. Let $x_r(v)$ be the first nontrivial root element occurring in the decomposition, that is, r is the first root with coefficient $v \neq 0$.

Since $x_r(v)$ occurs in this product, $x_r(v)^{\gamma\boldsymbol{\alpha}_\gamma}$ 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 $t_r = v$ 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, $u \in \langle X_\delta \mid \delta \in \Psi^+\rangle$ by induction. $\square$

The relative root elements and relative root subgroups for negative relative roots are defined in the similar way. Now we define a normal subgroup of $G_{\boldsymbol{\alpha}}(k)$:

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

The quotient $G_{\boldsymbol{\alpha}}(k)/G_{\boldsymbol{\alpha}}(k)^\dagger$ is called the *Whitehead group*. Its description is a hard problem and is of interest for the study of $G_{\boldsymbol{\alpha}}(k)$.

4.4 Cohomology of unipotent subgroups

Suppose we have a reductive algebraic group G defined over k and U is its standard maximal unipotent subgroup. Let K be a Galois extension of k and let $\Gamma := \mathrm{Gal}(K{:}\,k)$. In this section, we describe how to find an element $v \in U(K)$ with the property

$$c_\gamma = vv^{-\gamma\boldsymbol{\alpha}_\gamma}, \quad \text{for all } \gamma \in \Gamma$$

for a given cocycle $c \in Z^1(\Gamma, Y_{2\delta})$, and $\boldsymbol{\alpha} \in Z^1(\Gamma, N_A(U(K)))$.

By [32, 14.3.10], there are no twisted forms of unipotent groups if k is perfect. That is, the above equation always has a solution. To obtain the solution, we repeatedly use the following proposition:

4.11 Proposition ([30, Proposition II.1]).
For every Galois extension K over a field k and $\Gamma := \mathrm{Gal}(K{:}\,k)$, we have

$$H^1(\Gamma, \mathrm{G_a}(K)) = 1,$$

where $\mathrm{G_a}(K)$ is the additive group of K. ∎

We first describe how this proposition is applied in case $\boldsymbol{\alpha} = \mathbf{1}$: We recall that c_γ can be written as a product of root elements in a certain ordering respecting the heights of the roots, [15, 12]. We write $c_\gamma = x_r(t_{r,\gamma})d_\gamma$, where d_γ is a product of root elements corresponding to roots which are larger than r with respect to this ordering. Now we use the above proposition to find an element $s_{r,\gamma} \in K$ with the property $s_{r,\gamma} - s_{r,\gamma}^\gamma = t_{r,\gamma}$ and obtain

$$\begin{aligned} x_r(s_{r,\gamma})^{-1} c_\gamma x_r(s_{r,\gamma})^\gamma &= x_r(-s_{r,\gamma}) x_r(t_{r,\gamma}) d_\gamma x_r(s_{r,\gamma}^\gamma) \\ &= x_r(-s_{r,\gamma}) x_r(t_{r,\gamma}) x_r(s^\gamma) d'_\gamma \\ &= x_r(-s_{r,\gamma} + t_{r,\gamma} + s_{r,\gamma}^\gamma) d'_\gamma = d'_\gamma, \end{aligned}$$

where d'_γ is also a product of root elements corresponding to roots which are all larger than r. Since there is only a finite number of roots, by induction we can find an element $b \in U(K)$ with the property $d'_\gamma = bb^{-\gamma}$. Now we obtain

$$\begin{aligned} c_\gamma &= x_r(s_{r,\gamma}) d'_\gamma x_r(s_{r,\gamma})^{-\gamma} \\ &= x_r(s_{r,\gamma}) bb^{-\gamma} x_r(s_{r,\gamma})^{-\gamma} = \big(x_r(s_{r,\gamma})b\big)\big(x_r(s_{r,\gamma})b\big)^{-\gamma}. \end{aligned}$$

For $\boldsymbol{\alpha} \neq \mathbf{1}$, the situation is slightly more difficult. But we only need the solution in a special case: The elements c_γ and the solution v are contained in $Y_{2\delta}$, and this group is commutative. Recall that

$$c_\gamma = \prod_{r \in \pi^{-1}(2\delta)} x_r(s_r) \quad \text{and} \quad v = \prod_{r \in \pi^{-1}(2\delta)} x_r(u_r).$$

Thus

$$v^{-\gamma \boldsymbol{\alpha}_\gamma} = \prod x_{r^{\boldsymbol{\alpha}_\gamma}}(-\lambda_{r\gamma} u_r^\gamma).$$

Now

$$v v^{-\gamma \boldsymbol{\alpha}_\gamma} = \prod x_{r^{\boldsymbol{\alpha}_\gamma}}(u_{r^{\boldsymbol{\alpha}_\gamma}} - \lambda_{r\gamma} u_r^\gamma)$$

and we obtain the following system of equations over K from the equation $c_\gamma = v v^{-\gamma \boldsymbol{\alpha}_\gamma}$:

$$s_{r^{\boldsymbol{\alpha}_\gamma}} = u_{r^{\boldsymbol{\alpha}_\gamma}} - \lambda_{r\gamma} u_r^\gamma \quad \text{for } r \in \pi^{-1}(2\delta). \tag{4.13}$$

We recall that the elements s_r and $\lambda_{r\gamma}$ are known and the elements u_r are the indeterminates. The next step is done for every $\gamma \in \Gamma$, we write λ_r instead of $\lambda_{r\gamma}$ to simplify the notation. Now we fix a root $r \in \pi^{-1}(\delta)$ and get the equation for

$$s_r + \lambda_{r\boldsymbol{\alpha}_\gamma^{-1}}(s_{r\boldsymbol{\alpha}_\gamma^{-1}})^\gamma + \lambda_{r\boldsymbol{\alpha}_\gamma^{-1}}\lambda_{r\boldsymbol{\alpha}_\gamma^{-2}}(s_{r\boldsymbol{\alpha}_\gamma^{-2}})^{\gamma^2} + \cdots = u_r - \prod_{i=1}^{o}\lambda_{r(\boldsymbol{\alpha}_\gamma^{-i})}u_r^{\gamma^o} \quad (4.14)$$

where o is the order of the orbit of r under $\boldsymbol{\alpha}_\gamma$. This is best shown on a small example: Suppose $\pi^{-1}(2\delta)$ consists of three roots: r_1, r_2 and r_3, and $\boldsymbol{\alpha}_\gamma$ acts on them as a permutation (r_1, r_2, r_3). Then the System of equations (4.13) is

$$\begin{aligned} s_{r_1} &= u_{r_1} - \lambda_{r_3}u_{r_3}^\gamma, \\ s_{r_2} &= u_{r_2} - \lambda_{r_1}u_{r_1}^\gamma, \\ s_{r_3} &= u_{r_3} - \lambda_{r_2}u_{r_2}^\gamma. \end{aligned}$$

Now we build the equation

$$\begin{aligned} &s_{r_1} + \lambda_{r_3}s_{r_3}^\gamma + \lambda_{r_3}\lambda_{r_2}s_{r_2}^{\gamma^2} \\ &\quad = u_{r_1} - \lambda_{r_3}u_{r_3}^\gamma + \lambda_{r_3}(u_{r_3} - \lambda_{r_2}u_{r_2}^\gamma)^\gamma + \lambda_{r_3}\lambda_{r_2}(u_{r_2} - \lambda_{r_1}u_{r_1}^\gamma)^{\gamma^2} \\ &\quad = u_{r_1} - \lambda_{r_3}\lambda_{r_2}\lambda_{r_1}u_{r_1}^{\gamma^3}. \end{aligned}$$

The single Equation (4.14) can be solved in the field k using the proposition above. The other indeterminates can now be computed using the equations from the system (4.13). In the above example,

$$\begin{aligned} u_{r_2} &= \lambda_{r_1}u_{r_1}^\gamma - s_{r_2}, \\ u_{r_3} &= \lambda_{r_2}u_{r_2}^\gamma - s_{r_3}. \end{aligned}$$

4.5 Important Examples

In this section, we present several important examples. For the group SL_2, we compute the Galois cohomology and the corresponding twisted forms explicitly. We compute the subgroup generated by the root subgroups for twisted groups of Lie type ${}^2\mathrm{E}_{6,1}(k)$, ${}^3\mathrm{D}_{4,1}(k)$ and ${}^6\mathrm{D}_{4,1}(k)$. Finally, we present an embedding of the twisted group of Lie type ${}^2\mathrm{A}_7(k)$ into $\mathrm{E}_7(k)$ for finite fields.

4.5.1 Example: SL_2

Let k be a field and let G be the linear algebraic group SL_2, defined over k. Let K be a quadratic extension of k. So $\Gamma := \mathrm{Gal}(K{:}\,k) = \langle\sigma\rangle$ is of order 2. Write $\overline{x} := x^\sigma$. For $X = (x_{ij}) \in \mathrm{SL}_2(K)$, write $\overline{X} := (\overline{x_{ij}})$. Let $N : K \to k$ be the norm map defined by $x \mapsto x\overline{x}$. We denote by c_g the conjugation automorphism $x \mapsto x^g$ induced by $g \in \mathrm{GL}_2(K)$.

Let $A := \mathrm{Aut}_K(G) \simeq \mathrm{PGL}_2(K)$. Then Γ acts on A as in Section 2.3: $\varphi^\sigma = \sigma^{-1}\varphi\sigma = \sigma\varphi\sigma$ for $\varphi \in A$. But now $\varphi = c_g$ for some $g \in \mathrm{GL}_2(K)$, so

$$\varphi^\sigma = c_g^\sigma = c_{\overline{g}}.$$

4.12 Proposition.
Let $\boldsymbol{\alpha} \in Z^1(\Gamma, A)$. Then $\boldsymbol{\alpha}_\sigma = c_h$ for some $h \in \mathrm{GL}_2(K)$ with the following properties:

1. $\overline{h}h = xI_2$ for some $x \in k^*$; and
2. either $h = \left(\begin{smallmatrix} 0 & 1 \\ c & 0 \end{smallmatrix}\right)$ for $c \in k^*$ (in this case is $x = c$); or $h = \left(\begin{smallmatrix} a & b \\ c & 1 \end{smallmatrix}\right)$ for $a, b, c \in K$ with $a = -c\overline{c}^{-1} = -b\overline{b}^{-1}$ (in this case $a\overline{a} = 1$ and $x = \overline{c}b + 1$).

Proof. Since $\boldsymbol{\alpha}$ is a cocycle, $\boldsymbol{\alpha}_\sigma \in \mathrm{Aut}_K(G)$ and $\boldsymbol{\alpha}_\sigma = c_h$ for some $h \in \mathrm{GL}_2(K)$. Thus, $\mathrm{id}_G = \boldsymbol{\alpha}_{\sigma^2} = \boldsymbol{\alpha}_\sigma^\sigma \cdot \boldsymbol{\alpha}_\sigma = c_{\overline{h}h}$. Hence, $\overline{h}h = xI_2$ for some $x \in K^*$. Now let $h = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$.

Case $d = 0$: Then $b \neq 0$ and we can assume $b = 1$ (otherwise replace h by $b^{-1}h$). Now $xI_2 = \overline{h}h = \left(\begin{smallmatrix} \overline{a}a+c & \overline{a} \\ \overline{c}a & \overline{c} \end{smallmatrix}\right)$. Thus $a = 0$ and $x = c = \overline{c} \in k^*$.

Case $d \neq 0$: Here we can assume $d = 1$ (otherwise replace h by $d^{-1}h$). Now $xI_2 = \overline{h}h = \left(\begin{smallmatrix} \overline{a}a+\overline{b}c & \overline{a}b+\overline{b} \\ \overline{c}a+c & \overline{c}b+1 \end{smallmatrix}\right)$. And it follows that $c = -\overline{c}a$ and $\overline{b} = -\overline{a}b$. Further, $x = \overline{c}b + 1$. □

We wish to determine which cocycles $\boldsymbol{\alpha} = [\![c_h]\!] \in Z^1(\Gamma, A)$ are cohomologous to the trivial cocycle and find the intertwining elements for them. A cocycle $\boldsymbol{\alpha}$ is cohomologous to $\mathbf{1}$ if, and only if, $\boldsymbol{\alpha}_\sigma = \varphi^{-\sigma}\varphi$ for some $\varphi = c_g \in A$ and this is true if, and only if, there is a $y \in K^*$ with $y\overline{g}h = g$. Now the problem is to find such g and y. Set $g := (g_{ij})$.

Case 1: $h = \left(\begin{smallmatrix} & 1 \\ c & \end{smallmatrix}\right)$, $c \in k^*$.

Then $g = y\overline{g}h = \left(\begin{smallmatrix} yc\overline{g}_{12} & y\overline{g}_{11} \\ yc\overline{g}_{22} & y\overline{g}_{21} \end{smallmatrix}\right)$. Thus we get five equations:

$$\begin{aligned} g_{11} &= yc\overline{g}_{12}, & g_{12} &= y\overline{g}_{11}, & \det g &\neq 0, \\ g_{21} &= yc\overline{g}_{22}, & g_{22} &= y\overline{g}_{21}, \end{aligned}$$

and these are equivalent to

$$\begin{aligned} N(y) &= c^{-1}, & g_{12} &= y\overline{g}_{11}, & \det g &\neq 0, \\ & & g_{22} &= y\overline{g}_{21}. \end{aligned}$$

Hence $\boldsymbol{\alpha}$ is cohomologous to the trivial cocycle if, and only if, c is in the image of the norm map. If it is, $\varphi = c_g$ with $g = \left(\begin{smallmatrix} 1 & y \\ i & y\overline{i} \end{smallmatrix}\right)$, where

$y \in N^{-1}(c^{-1})$ and $i \in K \backslash k$. By Proposition 3.13, φ is an isomorphism from $G(k) = \mathrm{SL}_2(k)$ to $G_{\boldsymbol{\alpha}}(k)$.

If, on the other hand, c is not in the image of the norm map, then $G(k)$ is not conjugate to $G_{\boldsymbol{\alpha}}(k)$.

Case 2: $h = \left(\begin{smallmatrix} a & b \\ c & 1 \end{smallmatrix}\right)$.

If $b \neq 0$, then set $x = \left(\begin{smallmatrix} 1 & 0 \\ b^{-\sigma} & 1 \end{smallmatrix}\right)$, and $\boldsymbol{\alpha}^{(c_x)}$ was handled in Case 1. If $c \neq 0$, then set $y = \left(\begin{smallmatrix} 1 & -c^{-1} \\ 0 & 1 \end{smallmatrix}\right)$ and $\boldsymbol{\alpha}^{(c_y)}$ was handled in Case 1. From now on we assume that $b = c = 0$ and $h = \left(\begin{smallmatrix} a & \\ & 1 \end{smallmatrix}\right)$ and (by the above proposition) that a has norm 1.

We show that $\boldsymbol{\alpha}$ is cohomologous to $\mathbf{1}$ if, and only if, we can find a $\lambda \in K^*$ with $\lambda^{-\sigma}\lambda = a$. In this case conjugation by $\left(\begin{smallmatrix} \lambda^{-1} & \\ & 1 \end{smallmatrix}\right)$ is the intertwining element in A. In particular, a cocycle of this form is always a coboundary if k is a finite field (by Hilbert's Theorem 90) or whenever $H^1(\Gamma, K^*)$ is trivial.

By the above computation, $\boldsymbol{\alpha}$ is cohomologous to $\mathbf{1}$ if, and only if, we can find $g \in \mathrm{GL}_2(K)$ and $y \in K^*$, such that $y\overline{g}h = g$. This amounts to solving the following system of equations:

$$\begin{aligned} g_{11} &= y\overline{g}_{11}a, & g_{12} &= y\overline{g}_{12}, & \det g &\neq 0, \\ g_{21} &= y\overline{g}_{21}a, & g_{22} &= y\overline{g}_{22}, \end{aligned}$$

which is equivalent to finding a $\lambda \in K^*$, such that

$$\lambda^{-\sigma}\lambda = a.$$

Indeed, if we can find such a λ, then $g = \left(\begin{smallmatrix} \lambda & \\ & 1 \end{smallmatrix}\right)$, $y = 1$ is a solution for the above system; if we can find a solution for the above system, then at least one of $g_{11}g_{22}$, $g_{12}g_{21}$ is not equal to zero and

$$\lambda := \begin{cases} g_{11}\, g_{22}^{-1} & \text{if } g_{11}g_{22} \neq 0, \\ g_{21}\, g_{12}^{-1} & \text{if } g_{12}g_{21} \neq 0 \end{cases}$$

is a solution for the last equation above.

Finally, we compute the twisted groups explicitly. Let $\pi = \left(\begin{smallmatrix} & 1 \\ -1 & \end{smallmatrix}\right)$ and $M := \pi^{-1}h$, where h has either form $\left(\begin{smallmatrix} & 1 \\ c & \end{smallmatrix}\right)$, as in Case 1, or the form $\left(\begin{smallmatrix} a & \\ & 1 \end{smallmatrix}\right)$, as in Case 2. Then the map $f_M : K^2 \times K^2 \to K$, defined by $f_M : (v, w) \mapsto vM\overline{w}^t$ is a

Hermitian form and $(\mathrm{SL}_2)_{\boldsymbol{\alpha}}(k) = \mathrm{SU}_2(K, f_M)$:

$$\begin{aligned}
g \in (\mathrm{SL}_2)_{\boldsymbol{\alpha}}(k) &\Leftrightarrow g^{\sigma \boldsymbol{\alpha}_\sigma} = g \\
&\Leftrightarrow h^{-1}\overline{g}h = g \\
&\Leftrightarrow h^{-1}\pi\pi^{-1}\overline{g}\pi\pi^{-1}h = g \\
&\Leftrightarrow M^{-1}\overline{g}^{-t}M = g \\
&\Leftrightarrow gM\overline{g}^t = M \\
&\Leftrightarrow f_M(vg, wg) = vgM\overline{g}^t\overline{w}^t = vM\overline{w}^t = f_M(v,w) \\
&\qquad\qquad\qquad\qquad\qquad \text{for all } v, w \in K^2 \\
&\Leftrightarrow g \in \mathrm{SU}_2(K, f_M).
\end{aligned}$$

Recall that $\mathrm{SL}_2(k)$ is isomorphic to $(\mathrm{SL}_2)_{\boldsymbol{\alpha}}(k) = \mathrm{SU}_2(K, f_M)$ if, and only if, the cocycle defined by h is a coboundary.

We now present a different point of view for $h = \left(\begin{smallmatrix} & 1 \\ c & \end{smallmatrix}\right)$, as in Case 1:

$$\begin{aligned}
(\mathrm{SL}_2)_{\boldsymbol{\alpha}}(k) &= \left\{ g \in \mathrm{SL}_2(K) \mid g = g^{\sigma\boldsymbol{\alpha}_\sigma} = g^{\sigma h} \right\} \\
&= \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathrm{SL}_2(K) \mid \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} = \begin{pmatrix} \overline{a}_{22} & c^{-1}\overline{a}_{21} \\ c\overline{a}_{12} & \overline{a}_{11} \end{pmatrix} \right\} \\
&= \left\{ \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathrm{SL}_2(K) \mid a_{22} = \overline{a}_{11},\ a_{21} = c\overline{a}_{12} \right\} \\
&= \left\{ \begin{pmatrix} a_{11} & a_{12} \\ c\overline{a}_{12} & \overline{a}_{11} \end{pmatrix} \in \mathrm{SL}_2(K) \right\}.
\end{aligned}$$

We can describe this group in terms of quaternion algebras:

Choose $c \in k^*$. Then the set of all 2×2 matrices over K of the form

$$\begin{pmatrix} a & b \\ c\overline{b} & \overline{a} \end{pmatrix}$$

form a quaternion algebra $Q = Q(K/k, c)$ over k (cf. [39, Section 9]). If we identify K with its image in Q under the map $a \mapsto \mathrm{diag}(a, \overline{a})$ and set $\lambda := \left(\begin{smallmatrix} & 1 \\ c & \end{smallmatrix}\right)$, then we can write every element of Q as $a + b\lambda$. There is a unique extension of σ to an involution (antiautomorphism of order 2) of Q, such that $\overline{\lambda} = -\lambda$. The norm of an element in Q is given by

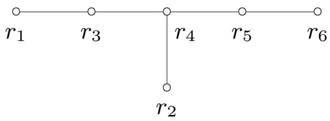
$$N(a + b\lambda) = (a + b\lambda)\overline{(a + b\lambda)} = (a + b\lambda)(\overline{a} - \overline{b}\lambda) = a\overline{a} - cb\overline{b}.$$

Hence $(\mathrm{SL}_2)_{\boldsymbol{\alpha}}(k)$ is the set of all elements of the quaternion algebra Q with norm 1, i.e., $(\mathrm{SL}_2)_{\boldsymbol{\alpha}}(k) = \mathrm{SL}_1(Q)$.

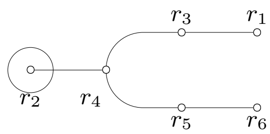
The quaternion algebra is a division algebra if, and only if, $c \notin N(K)$. If $c \in N(K)$, then $Q \simeq M_{2\times 2}(k)$. This leads to the two cases: $\mathrm{SL}_1(Q)$, Q a quaternion division algebra and $\mathrm{SL}_1(M_{2\times 2}(k)) \simeq \mathrm{SL}_2(k)$.

4.5.2 A twisted form of E_6 of rank 1: ${}^2\mathrm{E}_{6,1}^{35}(k)$

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 $\mathcal{D}$:



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 ${}^2\mathrm{E}_{6,1}^{35}(k)$:



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 [29]). We compute ${}^2\mathrm{E}_{6,1}^{35}(k)^\dagger$ as a subgroup of $\mathrm{E}_6(K)$, where K is a quadratic extension of k. Denote by γ the non-trivial automorphism in $\Gamma := \mathrm{Gal}(K{:}\, k)$.

The cocycle

First we compute a cocycle of Γ on $\mathrm{Aut}_K(G)$ defining a twisted form corresponding to the above index. As described in Section 4.2, this amounts to find 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 3.3. 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 $\Pi_0 = \{r_1, r_3, \ldots, r_6\}$ and Φ_0 is the subsystem of Φ spanned by Π_0 of type A_5. The Weyl element $w = w_0(\Phi_0)$ 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

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

where $J_\delta = \{ {}^{00000}_{\ \ 1}, {}^{00100}_{\ \ 1}, {}^{01100}_{\ \ 1}, {}^{00110}_{\ \ 1}, {}^{11100}_{\ \ 1} \}$. 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 actions of Γ on Φ and Π, we have to choose a torus element $h = \prod_{i=1}^{6} h_{\alpha_i}(s_i)$, where $s_i \in k^*$. For $\boldsymbol{\alpha}$ to be a cocycle, $\gamma\boldsymbol{\alpha}_\gamma$ must have order 2, which is true if, and only if,

$$s_2^2 s_3^2 s_4^3 s_5^2 s_6 = -1.$$

Hence s_1 is determined by $s_2, \dots, s_6$:

$$s_1 = -(s_2^2 s_3^2 s_4^3 s_5^2 s_6)^{-1}.$$

By construction, σ 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 σ to this subgroup is also an algebraic automorphism defining a cocycle.

Further we assume the existence of $s_1, s_2, s_3, \dots, s_6 \in k^*$, 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 $\prod_{i\in I} h_{\alpha_i}(s_i)$ in $\mathrm{SL}_6(K)$ defines an anisotropic unitary form q on K^6 and $(\mathrm{A}_5)_{\boldsymbol{\alpha}}(k) \simeq \mathrm{SU}_6(k,q)$.

Relative root elements

We use methods from Section 4.3. By (4.5) and (4.7), we have

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

For the root δ, we first compute

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

and $c(t)$ can be computed, but we omit the details. To compute $v(t)$, we introduce constants

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

Then for $t \in K$:

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

In characteristic not 2, we introduce a k-valued bilinear form $g : V_\delta \times V_\delta \to k$:

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

Then a solution $v(t)$ for the equation (4.8) is

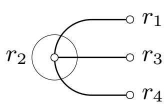
$$v(t) = -\tfrac{1}{2} g(t,t)$$

and the relative root element is

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

4.5.3 The groups ${}^3\mathrm{D}_{4,1}(k)$ and ${}^6\mathrm{D}_{4,1}(k)$

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 ${}^3\mathrm{D}_{4,1}$ and ${}^6\mathrm{D}_{4,1}$, both corresponding to the following figure:



Both these groups were of recent interest, see for example [24].

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 4.1. 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 3.3.

Type ${}^3\mathrm{D}_{4,1}$

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

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

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 $\langle\gamma^3\rangle$ and the order of the quotient is 3. Thus the index is of type ${}^3\mathrm{D}_{4,1}$.

The cocycle $\boldsymbol{\alpha} \in Z^1(\Gamma, N_A(T))$ now has the form $[\![\dot{\tau}_3 n_1 n_3 n_4 h]\!]$, where h is conjugation by a torus element. The torus element $h_1(-1)h_3(-1)h_4(-1)$ makes $\boldsymbol{\alpha}$ is a cocycle. By (4.5) and (4.7), we have

$$\begin{aligned}
x_{2\delta}(t) = u_{2\delta}(t) &= \prod x_{r_*}(t_{r_*})^{\gamma\boldsymbol{\alpha}_\gamma}\\
&= x_{r_*}(t_{r_*} - t_{r_*}^{\gamma} + t_{r_*}^{\gamma^2} - t_{r_*}^{\gamma^3} + t_{r_*}^{\gamma^4} - t_{r_*}^{\gamma^5}).
\end{aligned}$$

For the root δ, we first compute

$$\begin{aligned}
u_\delta(t) &= \prod_{r\in J_\delta}\prod x_r(t_r)^{\gamma\boldsymbol{\alpha}_\gamma},\\
c(t) &= x_{r_*}(t_{r_2}t_{r_2}^{\gamma} + t_{r_2}t_{r_2}^{\gamma^3} + t_{r_2}t_{r_2}^{\gamma^5} - t_{r_5}t_{r_5}^{\gamma^3}).
\end{aligned}$$

In characteristic not 2, a solution $v(t)$ for the equation (4.8) is

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

and the relative root element is

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

Type $^6\mathrm{D}_{4,1}$

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 $^3\mathrm{D}_{4,1}$, 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 $^6\mathrm{D}_{4,1}$.

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 $h' = h_1(-1)h_3(-1)h_4(-1)$ make $\boldsymbol{\alpha}$ a cocycle. By (4.5) and (4.7), we have

$$\begin{aligned} x_{2\delta}(t) = u_{2\delta}(t) &= \prod x_{r_*}(t_{r_*})^{\gamma\boldsymbol{\alpha}_\gamma} \\ &= x_{r_*}(t_* - t_*^{\gamma_2} - t_*^{\gamma_2\gamma_3} - t_*^{\gamma_3\gamma_2} + t_*^{\gamma_3} + t_*^{\gamma_3\gamma_3}). \end{aligned}$$

For the root δ, we first compute

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

and two terms $c(t)$ for the two generators of Γ:

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

In characteristic not 2, a simultaneous solution $v(t)$ for the equation system

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

is

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

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

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

4.5.4 $^2\mathrm{A}_7(k)$ inside $\mathrm{E}_7(k)$

This section is devoted to the construction of a subgroup of $\mathrm{E}_7(k)$, which is isomorphic to the twisted group of Lie type $^2\mathrm{A}_7(k)$. This subgroup is an open case in [21, Section 4.1]

Consider the usual embedding $\mathrm{A}_7(k) \subseteq \mathrm{E}_7(k)$, that is, the map

$$\begin{aligned} y_1(t) &\mapsto x_{-r_*}(t) & y_2(t) &\mapsto x_1(t) \\ y_i(t) &\mapsto x_i(t) \quad \text{for } i = 3, \dots, 7, \end{aligned}$$

where $y_i(t)$ are root elements of $\mathrm{A}_7(k)$, $x_i(t)$ the ones of $\mathrm{E}_7(k)$ and r_* is the highest root in the root system of type E_7. Denote by $w_0(\mathrm{A}_7)$ and $w_0(\mathrm{E}_7)$ the longest elements of the Weyl groups of $\mathrm{A}_7(k)$ and $\mathrm{E}_7(k)$, respectively, and set $w := w_0(\mathrm{A}_7)w_0(\mathrm{E}_7)$.

Then conjugation by $\dot{w}$ induces the standard diagram automorphism on $\mathrm{A}_7(k)$ and $\boldsymbol{\alpha} = [\![\dot{w}]\!]$ is an inner cocycle on $\mathrm{E}_7(k)$ but an outer cocycle on $\mathrm{A}_7(k)$ and ${}^2\mathrm{A}_7(k) = (\mathrm{A}_7)_{\boldsymbol{\alpha}}(k)$.

Using Galois cohomology we have

$${}^2\mathrm{A}_7(k) = (\mathrm{A}_7)_{\boldsymbol{\alpha}}(k) \subseteq (\mathrm{E}_7)_{\boldsymbol{\alpha}}(k) \simeq \mathrm{E}_7(k),$$

where the last isomorphism is a conjugation given by Lang's Theorem 3.17 and Proposition 3.13. Since $\dot{w}$ is always defined over the prime field, and has order 4, a conjugating element a can always be found in $E_7(k^4)$ by [11, Proposition 2.1], due to the author and Scott Murray.

For $k = \mathbb{F}_5$, the element a given in Figure 4.1 was computed by Scott Murray using methods from [11]. The same method would work for other finite fields of characteristic > 3.

Figure 4.1: Element conjugating $(\mathrm{E}_7)_{\boldsymbol{\alpha}}(\mathbb{F}_5)$ to $\mathrm{E}_7(\mathbb{F}_5)$.

$$
\begin{gathered}
x_1(\xi^{416})x_2(\xi^{494})x_3(\xi^{234})x_4(\xi^{286})x_5(\xi^{78})x_6(\xi^{234})x_7(\xi^{598})x_8(3)x_9(3)\\
x_{10}(\xi^{104})x_{11}(\xi^{130})x_{12}(\xi^{598})x_{13}(\xi^{182})x_{14}(\xi^{234})x_{15}(\xi^{520})x_{17}(\xi^{260})x_{18}(\xi^{234})\\
x_{20}(\xi^{286})x_{22}(2)x_{23}(\xi^{130})x_{24}(\xi^{572})x_{25}(4)x_{26}(\xi^{26})x_{27}(1)x_{28}(\xi^{234})x_{29}(\xi^{286})\\
x_{30}(\xi^{130})x_{31}(\xi^{338})x_{32}(\xi^{546})x_{33}(\xi^{182})x_{34}(3)x_{35}(\xi^{104})x_{36}(\xi^{390})x_{37}(\xi^{572})\\
x_{38}(1)x_{39}(\xi^{494})x_{40}(\xi^{52})x_{41}(\xi^{260})x_{42}(\xi^{598})x_{43}(2)x_{44}(\xi^{78})x_{45}(\xi^{494})x_{46}(\xi^{286})\\
x_{48}(3)x_{50}(2)x_{51}(1)x_{52}(\xi^{390})x_{53}(\xi^{390})x_{54}(\xi^{208})x_{55}(\xi^{416})x_{56}(\xi^{494})x_{57}(\xi^{494})\\
x_{58}(\xi^{234})x_{59}(\xi^{442})x_{60}(1)x_{61}(\xi^{208})x_{62}(\xi^{442})x_{63}(\xi^{520})\\
h_1(\xi^{260})h_2(\xi^{91})h_3(\xi^{390})h_4(\xi^{260})h_5(\xi^{221})h_7(\xi^{117})\\
n_1n_2n_3n_1n_4n_2n_3n_1n_4n_3n_5n_4n_2n_3n_1n_4n_3n_5n_4n_2n_6n_5n_4n_2n_3n_1n_4n_3n_5n_4n_2\\
n_6n_5n_4n_3n_1n_7n_6n_5n_4n_2n_3n_1n_4n_3n_5n_4n_2n_6n_5n_4n_3n_1n_7n_6n_5n_4n_2n_3n_4n_5n_6n_7\\
x_1(\xi^{494})x_2(\xi^{104})x_3(\xi^{390})x_4(\xi^{208})x_5(\xi^{234})x_6(\xi^{572})x_7(\xi^{182})x_8(\xi^{338})x_9(\xi^{572})\\
x_{10}(\xi^{286})x_{11}(\xi^{52})x_{12}(\xi^{546})x_{13}(\xi^{234})x_{14}(\xi^{104})x_{15}(\xi^{546})x_{16}(\xi^{78})x_{17}(\xi^{572})\\
x_{18}(\xi^{130})x_{19}(\xi^{416})x_{20}(\xi^{78})x_{21}(2)x_{22}(\xi^{572})x_{23}(\xi^{260})x_{24}(\xi^{520})x_{25}(\xi^{182})\\
x_{26}(\xi^{52})x_{27}(\xi^{390})x_{28}(\xi^{208})x_{29}(\xi^{390})x_{30}(\xi^{520})x_{31}(\xi^{52})x_{32}(\xi^{364})x_{33}(\xi^{234})\\
x_{34}(\xi^{338})x_{35}(\xi^{208})x_{36}(\xi^{208})x_{37}(\xi^{182})x_{38}(\xi^{104})x_{39}(3)x_{40}(4)x_{41}(\xi^{78})x_{42}(3)\\
x_{43}(\xi^{520})x_{44}(\xi^{182})x_{45}(\xi^{338})x_{46}(\xi^{104})x_{47}(\xi^{494})x_{48}(\xi^{260})x_{49}(\xi^{78})x_{50}(\xi^{338})\\
x_{51}(\xi^{78})x_{52}(\xi^{494})x_{53}(\xi^{182})x_{54}(\xi^{260})x_{55}(\xi^{260})x_{56}(\xi^{494})x_{57}(\xi^{130})x_{58}(\xi^{260})\\
x_{59}(\xi^{104})x_{60}(1)x_{61}(\xi^{26})x_{62}(\xi^{520})x_{63}(\xi^{260})
\end{gathered}
$$

The element is given as a word in Steinberg presentation, written in the unique Bruhat decomposition, ξ being a primitive element of $\mathbb{F}_{5^4}$.

Chapter 5

Maximal tori and Sylow subgroups

Let G be a reductive algebraic group defined over the field k and $\Gamma_{\mathrm{sep}} := \mathrm{Gal}(k_{\mathrm{sep}}\colon k)$. A *twisted torus* of G is a twisted form $T_{\boldsymbol{\alpha}}$ of the standard maximal torus $T \subseteq G$, where $\boldsymbol{\alpha} \in Z^1(\Gamma_{\mathrm{sep}}, N_{\mathrm{Aut}(G)}(T))$. In this section, we give a classification of all twisted tori of G using the methods of the previous chapters. In case k is finite, we compute them explicitly. For this computation, we need a set of conjugacy class representatives of the Weyl group of $G_{\boldsymbol{\beta}}$ for $\boldsymbol{\beta} \in Z^1(\Gamma_{\mathrm{sep}}, N_{\mathrm{Aut}(G)}(T))$. The conjugacy classes of Weyl groups are known (see, for example, [22, 8]) and, in [14], algorithms for their computation are described.

5.1 Twisted maximal tori

In this section, we provide a classification of all twisted tori of $G(k)$ and, for finite fields k, we compute them explicitly. It is well known that all the maximal tori of G are conjugate in G (Theorem 3.6). We are interested the $G(k)$-conjugacy classes of the groups of k-rational points of maximal k-tori of G.

We use the cohomology of Γ_{sep} on DW, where D is the automorphism group of the Dynkin diagram and W the Weyl group of G. Therefore, we retain the notation of Section 3.5.2: Let T be a maximal k-split torus of G and let $\mathcal{R} = (X, \Phi, Y, \Phi^\star)$ be the root datum of G with respect to T. Write elements of G as words in the Steinberg generators, as described in Section 3.2. Let N be the normaliser of T in G. The Weyl group W is isomorphic to N/T. We have standard representatives $\dot{w} \in N$ for each $w \in W$, which are invariant under all field automorphisms, thus contained in $G(k)$. Let D be the automorphism group of the Dynkin diagram $\mathcal{D}$ of G and identify D with the group of automorphisms induced on the root datum $\mathcal{R}$ of G. Then $\mathrm{Aut}(\mathcal{R}) = DW$.

First we consider cocycles that have values in $N_{\mathrm{Aut}(G)}(T)$. Remember that, for a twisted form $G_{\boldsymbol{\beta}}$ of G, the cocycle $\boldsymbol{\beta}$ can be assumed to have values in $N_{\mathrm{Aut}(G)}(T)$ by Springer's Lemma 3.15. Thus, $T_{\boldsymbol{\beta}} \leq G_{\boldsymbol{\beta}}$ is a maximal torus of $G_{\boldsymbol{\beta}}$ and all its twisted forms are obtained by cocycles with values in $N_{\mathrm{Aut}(G)}(T)$. That is, we obtain in one step not only all twisted tori of G, but also all twisted tori of all twisted forms of G.

Note that in the following proposition we do not make any restrictions on the choice of k.

5.1 Proposition.
The set of representatives of $N_{\mathrm{Aut}(G)}(T)$-conjugacy classes of twisted tori of G is

$$\bigcup_{\Gamma} \{\ T_{\boldsymbol{\alpha}} \mid \boldsymbol{\alpha} \in i_\Gamma\big(R(\Gamma)\big)\ \},$$

where the union is taken over all subgroups of DW that occur as Galois groups of a Galois extension of k, i_Γ is as in Lemma 3.19, and $R(\Gamma)$ is a set of representatives of equivalence classes of faithful representations of Γ on $\mathcal{R}$.

Proof. The $N_{\mathrm{Aut}(G)}(T)$-conjugacy classes of twisted tori are classified by elements of $H^1(\Gamma_{\mathrm{sep}}, N_{\mathrm{Aut}(G)}(T))$.

Let N be the normaliser of T in G and $W = N/T$ be the Weyl group. If n_1, n_2 are two elements of N with $n_1 T = n_2 T$, then conjugation by n_1 and by n_2 give the same automorphism of T. Thus, $N_{\mathrm{Aut}(G)}(T)/C_{\mathrm{Aut}(G)}(T) \simeq D'N/T \simeq DW$, where D' is the group of diagram automorphisms.

Now Γ_{sep} acts trivially on $N_{\mathrm{Aut}(G)}(T)$, and so on DW, and thus

$$H^1(\Gamma_{\mathrm{sep}}, N_{\mathrm{Aut}(G)}(T)) = H^1(\Gamma_{\mathrm{sep}}, DW).$$

The rest follows from Proposition 3.20. □

Note that for non-isomorphic field extensions K_1 and K_2 of k that have isomorphic Galois groups $\Gamma := \mathrm{Gal}(K_1{:}\, k) \simeq \mathrm{Gal}(K_2{:}\, k)$, and for $\boldsymbol{\rho} \in i_\Gamma(R(\Gamma))$, the groups of rational points $T_{\boldsymbol{\rho}}(K_1)$ and $T_{\boldsymbol{\rho}}(K_2)$ are not isomorphic in general.

5.2 Corollary.
If k is finite, a set of representatives of the $N_{\mathrm{Aut}(G)}(T)$-conjugacy classes of twisted tori of G is given by

$$\{T_{\boldsymbol{\alpha}} \mid \boldsymbol{\alpha} = [\![w]\!], w \in R\},$$

where R is a set of conjugacy class representatives of elements of DW.

Proof. For finite fields, the finite Galois groups are always cyclic. Let $\Gamma = \langle\gamma\rangle$ be a cyclic group and $\boldsymbol{\alpha}, \boldsymbol{\beta} : \Gamma \to DW$ two faithful representations of Γ on

$\mathcal{R}$. Then $o(\boldsymbol{\alpha}_\gamma) = o(\gamma)$ and $\boldsymbol{\alpha}, \boldsymbol{\beta}$ are equivalent if, and only if, $\boldsymbol{\alpha}_\gamma$ and $\boldsymbol{\beta}_\gamma$ are conjugate in DW.

Thus, equivalence classes of faithful representations of Γ correspond to conjugacy classes of elements of DW of order $|\Gamma|$. And

$$\bigcup_{\Gamma} \{ \ T_{\boldsymbol{\alpha}} \mid \boldsymbol{\alpha} \in R(\Gamma) \ \} = \{ \ T_{\boldsymbol{\alpha}} \mid \boldsymbol{\alpha} = [\![w]\!], w \in R \ \},$$

where R is a set of conjugacy class representatives of elements of DW. □

If k is finite, we also write T_w instead of $T_{[\![w]\!]}$ for $w \in DW$.

5.2 Rational maximal tori

In this section, we describe the rational maximal tori of all twisted and untwisted forms $G_{\boldsymbol{\beta}}(k)$ of $G(k)$ and, over finite fields, we classify and compute them explicitly.

5.3 Lemma.
Let $\boldsymbol{\alpha}, \boldsymbol{\beta} \in i_\Gamma\big(R(\Gamma)\big)$, with the notation of Proposition 5.1. These cocycles naturally embed in $Z^1(\Gamma, \mathrm{Aut}_K(G))$. If they are cohomologous as cocycles in $Z^1(\Gamma, \mathrm{Aut}_K(G))$, then $T_{\boldsymbol{\alpha}}(k)$ is conjugate in $\mathrm{Aut}_K(G)$ to the group of rational points of a maximal torus of $G_{\boldsymbol{\beta}}(k)$.

Proof. Suppose, $\boldsymbol{\alpha}$ is cohomologous to $\boldsymbol{\beta}$. That is, there is an $a \in \mathrm{Aut}_K(G)$ such that $\boldsymbol{\alpha}_\gamma = a^{-\gamma}\boldsymbol{\beta}_\gamma a$ for all $\gamma \in \Gamma$. Then

$$T_{\boldsymbol{\alpha}}(k)^{a^{-1}} \subseteq G_{\boldsymbol{\alpha}}(k)^{a^{-1}} = G_{\boldsymbol{\beta}}(k)$$

by Proposition 3.13. □

If $a \in G(\bar{k})$ is as in this proof, then $T_{\boldsymbol{\alpha}}(k)^{a^{-1}}$ is called a *rational* maximal torus of $G_{\boldsymbol{\beta}}(k)$.

An important special case is given by the following lemma, which, together with Corollary 5.2, provides a classification of all rational maximal tori of twisted and untwisted finite groups of Lie type.

Denote the Weyl group of $G_{\boldsymbol{\beta}}$ by $W_{\boldsymbol{\beta}}$.

5.4 Lemma.
Let k be finite. Define cocycles $\boldsymbol{\beta} = [\![\tau]\!]$ for $\tau \in D$ and $\boldsymbol{\alpha} = [\![\tau w]\!]$ for some $w \in W_{\boldsymbol{\beta}}$ as in Corollary 5.2. Then $T_{\boldsymbol{\alpha}}(k)$ is conjugate in $G_{\boldsymbol{\beta}}(\bar{k})$ to a rational maximal torus of $G_{\boldsymbol{\beta}}(k)$.

Proof. We apply Lang's theorem to the group $G_{\boldsymbol{\beta}}$. By Lang's theorem, applied to the group $G_{\boldsymbol{\beta}}$, $[\![w]\!]$ is a coboundary in $Z^1(\Gamma, G_{\boldsymbol{\beta}})$; thus

$$\dot{w} = a^{-\gamma\boldsymbol{\beta}_\gamma} \cdot 1 \cdot a = \tau^{-1} a^{-\gamma} \tau a$$

and the intertwining element a is contained in $G_{\boldsymbol{\beta}}(\bar{k})$. Now $\boldsymbol{\alpha} = [\![\tau w]\!]$ is cohomologous to $\boldsymbol{\beta}$ as elements of $Z^1(\Gamma, \mathrm{Aut}(G))$ with the same intertwining element a. The result now follows from the previous lemma. □

Note that, the lemma remains true with $\bar{k}$ replaced by a finite extension of k. An algorithm for the construction of the conjugator a is given in [11].

Now we summarise Corollary 5.2 and Lemma 5.4 as

5.5 Corollary.
Let k be a finite field and let $\boldsymbol{\beta} = [\![\tau]\!]$ for some $\tau \in D$. A set of representatives of the $G_{\boldsymbol{\beta}}(k)$-conjugacy classes of groups of k-rational points of maximal tori of $G_{\boldsymbol{\beta}}$ is given by

$$\{T_{\boldsymbol{\alpha}}^{a_w}(k) \mid \boldsymbol{\alpha} = [\![\tau w]\!], w \in R\},$$

where R is a set of conjugacy class representatives in W_β, and a_w is the intertwining element from the previous lemma, i.e.,

$$\dot{w} = a_w^{-\gamma\tau} a_w.$$

5.3 Generators of twisted tori

In this section, we compute the generators of twisted tori explicitly in the case k is finite. Let the notation be as in the previous section. Denote by ℓ the semisimple rank of G. Note that methods from this and the next section do not apply for twisted groups of 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 root lattice is not a linear map.

5.6 Theorem.
Let w be an element of DW with order r. Let $q := |k|$, and let K be the field extension of k of degree r in $\bar{k}$. Let $\Gamma := \mathrm{Gal}(K{:}\,k) = \langle\gamma\rangle$. Set $m := |K^*| = q^r - 1$. Let M be the matrix of the action of $w^\star$ on Y and let ξ be a primitive element of K. Then

$$T_w(k) = \big\langle (\xi^{a_1}, \dots, \xi^{a_\ell}) \mid (a_1, \dots, a_\ell) \in \mathfrak{B} \big\rangle,$$

where $\mathfrak{B}$ is a generating set of the fixed-point space in $\mathbb{Z}_m^\ell$ of qM, interpreted as a matrix over $\mathbb{Z}_m$.

Proof. Let $t \in T(K)$. Then, in the notation of Section 3.2,

$$t = \prod_{i=1}^{\ell} \alpha_i^\star \otimes x_i$$

with $x_i \in K^*$. Moreover, for all $i = 1, \dots, \ell$ we have $x_i = \xi^{a_i}$ for some $a_i \in \mathbb{Z}_m$. By [12, 5.2]

$$t^{\dot{w}} = \prod_{j=1}^{\ell} \alpha_j^\star \otimes \Big(\prod_{i=1}^{\ell} x_i^{M_{ij}} \Big) = \prod_{j=1}^{\ell} \alpha_j^\star \otimes \Big(\prod_{i=1}^{\ell} \xi^{a_i M_{ij}} \Big).$$

Since $\gamma : x \mapsto x^q$ in our case,

$$t^{\gamma \dot{w}} = \prod_{j=1}^{\ell} \alpha_j^\star \otimes \Big(\prod_{i=1}^{\ell} \xi^{a_i q M_{ij}} \Big) = \prod_{j=1}^{\ell} \alpha_j^\star \otimes \xi^{\left(\sum_{i=1}^{\ell} a_i q M_{ij} \right)}.$$

Thus,

$$\begin{aligned} t^{\gamma \dot{w}} = t \quad &\iff \quad \sum_{i=1}^{\ell} a_i q M_{ij} = a_j \text{ for all } j = 1, \dots, \ell \\ &\iff \quad (a_1, \dots, a_\ell) q M = (a_1, \dots, a_\ell). \end{aligned}$$

That is,

$$T_w(k) = \big\{ (\xi^{a_1}, \dots, \xi^{a_\ell}) \mid (a_1, \dots, a_\ell) \in \mathbb{Z}_m^\ell, (a_1, \dots, a_\ell)(qM - I) = 0 \big\}. \quad (5.1)$$

□

Note that for different primitive elements of K this fixed-point space is the same: For, let ξ, ζ be two primitive elements in K and $t = (\xi^{a_1}, \dots, \xi^{a_\ell}) = (\zeta^{b_1}, \dots, \zeta^{b_\ell})$. Then $\zeta = \xi^c$ for some invertible $c \in \mathbb{Z}_m$ and the exponent vector $(a_1, \dots, a_\ell)$ is an eigenvector of qM to the eigenvalue 1 if, and only if, the exponent vector $(b_1, \dots, b_\ell)$ is one as well:

$$(b_1, \dots, b_\ell) q M = c(a_1, \dots, a_\ell) q M = c(a_1, \dots, a_\ell) = (b_1, \dots, b_\ell).$$

5.4 Computing orders of the maximal tori

Let the notation be as in the previous sections. The maximal tori of G are given by Corollary 5.2 and Theorem 5.6. The maximal tori are abelian groups which can be written as a direct product of cyclic subgroups. Given the type of the root datum of G and an element $w \in DW$, we now compute the orders of the cyclic factors of $T_w(k)$, as polynomials in q.

This is done in essentially the same way as in the proof of the Theorem 5.6. We interpret q, the order of k, as an indeterminate, so the Equation (5.1) becomes

$$\Big\{(\xi^{a_1},\dots,\xi^{a_\ell}) \;\Big|\; (a_1,\dots,a_\ell)\in\big(\mathbb{Z}[q]/(q^r-1)\big)^\ell, \\ (a_1,\dots,a_\ell)(qM-I)=0\Big\}.$$

Now $B := qM-I$ is a matrix over $\mathbb{Z}[q]/(q^r-1)$ and the order of the solution space of the equation $XB=0$ is exactly the order of $T_w(k)$, where $X\in\big(\mathbb{Z}[q]/(q^r-1)\big)^\ell$. We can view B as a matrix over $\mathbb{Q}[q]/(q^r-1)$. Using Magma we obtain the Smith form S of B by elementary matrix transformations. The order of the solution space of $XS=0$ is the same as the order of $T_w(k)$. The order of the solution space of $XS=0$ can now be read from the diagonal entries of S: Set

$$s_i := \begin{cases} q^r-1 & \text{if } S_{ii}=0,\\ S_{ii} & \text{otherwise}\end{cases}$$

and obtain

$$T_w(k)=\prod_{i=1}^{\ell} C_{s_i},$$

where s_i is the i-th diagonal entry of S and C_a is a cyclic group of order a.

A priori, the Smith form S is a diagonal matrix over $\mathbb{Q}[q]/(q^r-1)$. Every diagonal entry has the form $s_i=f_i/g_i$ with $f_i\in\mathbb{Z}[q]/(q^r-1)$ and $g_i\in\mathbb{Z}$. First we replace every zero on the diagonal by q^r-1 and then multiply the last row by $\prod_{i=1}^{\ell-1} g_i^{-1}$ and all other rows by g_i, thus preserving the determinant and making all but the last entry have integral coefficients. But the determinant of the matrix obtained is the same as the determinant of B, which is the characteristic polynomial of the matrix M, hence a polynomial with integral coefficients. Now the last entry also has integral coefficients. All diagonal entries of the matrix obtained are factors of the characteristic polynomial.

The results for exceptional types are given in Appendix A.

Raghunathan [25] uses similar techniques to describe the twisted tori, although only in the quasisplit case.

5.7 Example ($\mathrm{A}_1=\mathrm{SL}_2$)**.**
$G(k)=\mathrm{SL}_2(k)$, $k=GF(q)$, $W=\langle w\rangle\simeq C_2$. Standard torus:

$$T(k)=T_{\mathbf{1}}(k)=\{\left(\begin{smallmatrix} a & \\ & a^{-1}\end{smallmatrix}\right)\mid a\in k^*\}\simeq k^*\simeq C_{q-1}.$$

Twisted torus: $o(w)=2$, thus $K=GF(q^2)$, $\Gamma=\mathrm{Gal}(K\colon k)=\langle\gamma\rangle$. Now

$$\begin{aligned} T_w(k)&=\{t\in T(K)\mid t^{\gamma w}=t\}=\{\left(\begin{smallmatrix} a & \\ & a^{\gamma}\end{smallmatrix}\right)\in\mathrm{SL}_2(K)\}\\ &\simeq\{a\in K^*\mid aa^{\gamma}=1\}\simeq C_{q+1}.\end{aligned}$$

Examples for types G_2, F_4, E_6, E_7, E_8, ${}^2\mathrm{A}_5$, ${}^3\mathrm{D}_4$ and ${}^2\mathrm{E}_6$ are stated in Appendix A.

5.5 Computation of Sylow p-subgroups

We recall that G is a reductive linear algebraic group defined over the field k, which we assume to be finite of order q in this section. The aim of this section is to construct a "standard" Sylow p-subgroup of $G(k)$ for every prime p dividing the order of $G(k)$.

If the prime p is the characteristic of the field k, the maximal unipotent subgroups are precisely the Sylow p-subgroups and have order q^N, where N is the number of positive roots of the underlying root system. Using the Steinberg presentation, we already have a standard choice of a maximal unipotent subgroup: the subgroup $U(k)$.

From now on we assume that p is different from the characteristic of k. Let S be a Sylow p-subgroup of $G(k)$. Then S is nilpotent and each element of S is semisimple. Hence, by Corollary [31, 5.19],

$$S \le N_{G(k)}(T_w(k)) \tag{5.2}$$

for some (not necessarily unique) $w \in W$ and we have

$$N_{G(k)}(T_w(k))/T_w(k) \simeq C_W(w)$$

and

$$|N_{G(k)}(T_w(k))| = |T_w(k)| \cdot |C_W(w)|.$$

In case $p \nmid |C_W(w)|$, we have $S \le T_w(k)$ and we call the prime p *nice*.

5.8 Algorithm.
Note that when p is nice, steps 3 and 8 can be omitted.

0. Let $p^m := |G(k)|_p$. (A formula for $|G(k)|$ can be found, e.g., in [9])
1. Let R be a set of conjugacy class representatives of W.

   Using [14, Algorithm H] by Geck and Pfeiffer, each representative has the shortest length among all elements of its conjugacy class.
2. Replace R by the set

   $$\{w \in R \mid p^m \text{ divides } |N_{G(k)}(T_w(k))|\}. \tag{5.2'}$$

   (Otherwise a contradiction to (5.2).)

3. If p is not nice, select those Weyl elements for which $S \cap T_w(k)$ is largest. That is, set $u := \max_{w \in R}\{|T_w(k)|_p\}$ and replace R by the set
$$\{w \in R \big| |T_w(k)|_p = u\}.$$
4. Replace R by the set of elements $w \in R$ having the shortest length. (This leads to a "maximally split" torus.)
5. Let w be the lexicographically smallest element of R.
6. Compute $[s_1, \ldots, s_\ell]$ such that $T_w(k) = \prod_{i=1}^{\ell} C_{s_i}$ using the algorithms presented in Section 5.4.
7. For $i = 1, \ldots, \ell$, let g_i be a generator of C_{s_i} and $s_i = o_i \cdot p^{x_i}$ with $p \nmid o_i$. Then
$$S \cap T_w(k) = \langle\ g_i^{o_i} \mid i = 1, \ldots, \ell\ \rangle.$$
   If $S \subseteq T_w(k)$, we are done (this is always true if p is nice and in a few cases if p is not nice).
8. Suppose $S \not\subseteq T_w(k)$. To simplify notation, denote the order of a group element g by $|g|$.

   Let $p^o = |S|/|S \cap T_w(k)|$. Find a subgroup H of $C_W(w)$ of order p^o, which is contained in a p-Sylow subgroup of $C_W(w)$. Suppose H is generated by the set X. Set $q_x := |\dot{x}|/|x|$. By Tits [36], we have $q_x = 2^{\ell_x}$, where $\ell_x \geq 0$ is an integer.

   In case $p \neq 2$, replace $\dot{x}$ by $m_x := \dot{x}^{q_x}$. Then m_x has the same order as x and is a representative of x^{q_x}. But since $\gcd(|x|, q_x) = 1$, the elements x and x^{q_x} generate the same cyclic subgroup.

   In case $p = 2$, the order of the element $\dot{x}^{|x|}$ is a power of 2 and it is a torus element, thus contained in $|S \cap T_w(k)|$. Set $m_x := \dot{x}$ in this case.

Now $S = \langle (S \cap T_w(k)) \cup \{m_x \mid x \in X\} \rangle$. $\square$

Since we have standard representatives for every conjugacy class of W by using [14, Algorithm H], and by Steps 4 and 5, this algorithm constructs a "standard" Sylow subgroup.

Appendix A

Decomposition of orders of maximal tori

In this appendix we present the tables of the decomposed orders of maximal tori of twisted and untwisted reductive linear algebraic groups defined over finite fields. Note that the types ${}^2\mathrm{B}_2$, ${}^2\mathrm{G}_2$ and ${}^2\mathrm{F}_4$ are not included here, since the permutation on Φ induced by the Dynkin diagram symmetry is not a linear map and thus our method doesn't work.

A.1 How to read the tables

Each row contains the orders $o_1, \dots, o_n$ of cyclic components of the torus $T_w(q) \simeq C_{o_1} \times \cdots \times C_{o_n}$, where $w \in W$ is given as a word in the simple reflections. For example, in the last line of Table A.1, the Weyl element is

$$w := s_1 s_2 s_1 s_2 s_1 s_2,$$

where $W = \langle s_1, s_2 \rangle$ is the Weyl group of $\mathrm{G}_2(q)$ and

$$T_w(q) \simeq C_{q+1} \times C_{q+1}.$$

The generators of the Weyl groups are ordered as shown in the following Dynkin diagrams. The numbering of fundamental roots is as in Table 3.1.

Computation of the decompositions of all exceptional types takes a total of about 8 seconds on an Intel Pentium III 1.6GHz processor.

A.2 Tables

Table A.1: Maximal tori in $G_2(q)$

Orders	Weyl word
$q-1,\ q-1$	
q^2-1	1
q^2-1	2
q^2-q+1	12
q^2+q+1	1212
$q+1,\ q+1$	121212

Table A.2: Maximal tori in $F_4(q)$

Orders	Weyl word
$q-1,\ q-1,\ q-1,\ q-1$	
$q-1,\ q-1,\ q^2-1$	1
$q-1,\ q-1,\ q^2-1$	3
$q-1,\ q^3-1$	12
$q^2-1,\ q^2-1$	13
$q-1,\ q^3-q^2+q-1$	23
$q-1,\ q^3-1$	34
q^4-q^3+q-1	123
q^4+q^3-q-1	124
q^4+q^3-q-1	134
q^4-q^3+q-1	234
q^4-q^2+1	1234
$q^2-1,\ q-1,\ q+1$	2323
$q^2+1,\ q^2-1$	12323
$q^2+1,\ q^2-1$	23234
q^4+1	123234
$q^2-q+1,\ q^2-q+1$	12132343
$q+1,\ q+1,\ q^2-1$	121321323
$q+1,\ q+1,\ q^2-1$	232343234
$q+1,\ q^3+1$	1213213234
$q+1,\ q^3+1$	1232343234
$q^2+1,\ q^2+1$	121321343234
$q+1,\ q^3+q^2+q+1$	12132132343234
$q^2+q+1,\ q^2+q+1$	1213213432132343

Continued on next page

Table A.2 – *continued from previous page*

Orders	Weyl word
$q+1,\ q+1,\ q+1,\ q+1$	121321323432132343213234

Table A.3: Maximal tori in $\mathrm{E}_6(q)$

Orders	Weyl word
$q-1,\ q-1,\ q-1,\ q-1,\ q-1,\ q-1$	
$q-1,\ q-1,\ q-1,\ q-1,\ q^2-1$	1
$q-1,\ q-1,\ q^2-1,\ q^2-1$	12
$q-1,\ q-1,\ q-1,\ q^3-1$	13
$q-1,\ q-1,\ q^4+q^3-q-1$	123
$q^2-1,\ q^2-1,\ q^2-1$	125
$q-1,\ q-1,\ q^4-1$	134
$q-1,\ q^5-1$	1234
$q^2-1,\ q^4+q^3-q-1$	1235
$q^2-1,\ q^4-1$	1245
$q^3-1,\ q-1,\ q^2+q+1$	1356
$q^2-1,\ q^4-q^3+q-1$	2345
$q^6-q^4+q^2-1$	12345
q^6+q^5-q-1	12346
$q^2+q+1,\ q^4+q^3-q-1$	12356
$q^2+q+1,\ q^4-q^3+q-1$	13456
$q^6+q^5-q^3+q+1$	123456
$q^3-q^2+q-1,\ q^3-q^2+q-1$	234254
$q^6-q^5+q^4-q^2+q-1$	1234254
q^6+q^3+1	12342546
$q^2-q+1,\ q^4+q^2+1$	123142345465
$q+1,\ q+1,\ q^2-1,\ q^2-1$	234234542345
$q+1,\ q+1,\ q^4-1$	1234234542345
$q+1,\ q^5+q^4+q^3+q^2+q+1$	12342345423456
$q^2+q+1,\ q^2+q+1,\ q^2+q+1$	123142314542314565423456

Table A.4: Maximal tori in $\mathrm{E}_7(q)$

Orders	Weyl word
$q-1,\ q-1,\ q-1,\ q-1,\ q-1,\ q-1,\ q-1$	
$q-1,\ q-1,\ q-1,\ q-1,\ q-1,\ q^2-1$	1
$q-1,\ q-1,\ q-1,\ q^2-1,\ q^2-1$	12

Continued on next page

Table A.4 – *continued from previous page*

Orders	Weyl word
$q-1,\, q-1,\, q-1,\, q-1,\, q^3-1$	13
$q-1,\, q-1,\, q-1,\, q^4+q^3-q-1$	123
$q-1,\, q^2-1,\, q^2-1,\, q^2-1$	125
$q-1,\, q-1,\, q-1,\, q^4-1$	134
$q-1,\, q^2-1,\, q^2-1,\, q-1,\, q+1$	257
$q-1,\, q-1,\, q^5-1$	1234
$q-1,\, q^2-1,\, q^4+q^3-q-1$	1235
$q-1,\, q^2-1,\, q^4-1$	1245
$q+1,\, q^2-1,\, q^2-1,\, q^2-1$	1257
$q-1,\, q^3-1,\, q^3-1$	1356
$q-1,\, q^2-1,\, q^4-q^3+q-1$	2345
$q-1,\, q^4-1,\, q-1,\, q+1$	2457
$q-1,\, q^6-q^4+q^2-1$	12345
$q-1,\, q^6+q^5-q-1$	12346
$q^3-1,\, q^4+q^3-q-1$	12356
$q+1,\, q^2-1,\, q^4+q^3-q-1$	12357
$q+1,\, q^2-1,\, q^4-1$	12457
$q-1,\, q^6-1$	13456
$q-1,\, q^6+q^5+q^4-q^2-q-1$	13467
$q+1,\, q^2-1,\, q^4-q^3+q-1$	23457
$q-1,\, q^3-1,\, q^3+1$	24567
$q^7-q^5-q^4+q^3+q^2-1$	123456
$q+1,\, q^6-q^4+q^2-1$	123457
$q^7+q^6+q^5-q^2-q-1$	123467
$q+1,\, q^6+q^5+q^4-q^2-q-1$	123567
$q+1,\, q^6-1$	124567
q^7-1	134567
$q-1,\, q^3-q^2+q-1,\, q^3-q^2+q-1$	234254
$q+1,\, q^6-q^5+q-1$	234567
$q-1,\, q^6-q^5+q^4-q^2+q-1$	1234254
$q^7+q^6-q^4-q^3+q+1$	1234567
$q^3-q^2+q-1,\, q^2+1,\, q^2-1$	2342547
$q^7-q^6+q^4-q^3+q-1$	12342546
$q+1,\, q^6-q^5+q^4-q^2+q-1$	12342547
$q^2+1,\, q^5-q^4+q-1$	23425467
q^7+1	123425467
$q^3+1,\, q^4-q^3+q-1$	2342546547
$q^7-q^5+q^4+q^3-q^2+1$	12342546547

Continued on next page

Table A.4 – *continued from previous page*

Orders	Weyl word
$q^2-q+1,\ q^5-q^4+q^3-q^2+q-1$	123142345465
$q+1,\ q^2-1,\ q^2-1,\ q-1,\ q+1$	234234542345
$q^7-q^6+q^5+q^2-q+1$	1231423454657
$q+1,\ q^4-1,\ q-1,\ q+1$	1234234542345
$q+1,\ q+1,\ q+1,\ q^2-1,\ q^2-1$	2342345423457
$q+1,\ q^3-1,\ q^3+1$	12342345423456
$q+1,\ q+1,\ q+1,\ q^4-1$	12342345423457
$q+1,\ q+1,\ q+1,\ q^4-q^3+q-1$	23423454234567
$q+1,\ q+1,\ q^5+1$	123423454234567
$q^3+q^2+q+1,\ q^2+1,\ q^2-1$	2342345423456576
$q^2+1,\ q^5+q^4+q+1$	12342345423456576
$q^2-q+1,\ q^2-q+1,\ q^3+1$	123142314354234654765
$q+1,\ q^3+1,\ q^3+1$	12314231435423143546576
$q^2+q+1,\ q^2+q+1,\ q^3-1$	123142314542314565423456
$q^2+q+1,\ q^5+q^4+q^3+q^2+q+1$	123142314542314565423456 7
$q+1,\ q+1,\ q+1,\ q+1,\ q+1,\ q^2-1$	234234542345654234567654 234567
$q+1,\ q+1,\ q+1,\ q+1,\ q^3+1$	123423454234565423456765 4234567
$q+1,\ q^3+q^2+q+1,\ q^3+q^2+q+1$	123142345423145654234567 654234567
$q+1,\ q+1,\ q+1,\ q+1,\ q+1,\ q+1,\ q+1$	123142314354231435426542 314354265431765423143542 654317654234567

Table A.5: Maximal tori in $\mathrm{E}_8(q)$

Orders	Weyl word
$q-1,\ q-1,\ q-1,\ q-1,\ q-1,\ q-1,\ q-1,\ q-1$	
$q-1,\ q-1,\ q-1,\ q-1,\ q-1,\ q-1,\ q^2-1$	1
$q-1,\ q-1,\ q-1,\ q-1,\ q^2-1,\ q^2-1$	12
$q-1,\ q-1,\ q-1,\ q-1,\ q-1,\ q^3-1$	13
$q-1,\ q-1,\ q-1,\ q-1,\ q^4+q^3-q-1$	123

Continued on next page

Table A.5 – *continued from previous page*

Orders	Weyl word
$q-1,\ q-1,\ q^2-1,\ q^2-1,\ q^2-1$	125
$q-1,\ q-1,\ q-1,\ q-1,\ q^4-1$	134
$q-1,\ q-1,\ q-1,\ q^5-1$	1234
$q-1,\ q-1,\ q^2-1,\ q^4+q^3-q-1$	1235
$q-1,\ q-1,\ q^2-1,\ q^4-1$	1245
$q^2-1,\ q^2-1,\ q^2-1,\ q^2-1$	1257
$q-1,\ q-1,\ q^3-1,\ q^3-1$	1356
$q-1,\ q-1,\ q^2-1,\ q^4-q^3+q-1$	2345
$q-1,\ q-1,\ q^6-q^4+q^2-1$	12345
$q-1,\ q-1,\ q^6+q^5-q-1$	12346
$q-1,\ q^3-1,\ q^4+q^3-q-1$	12356
$q^2-1,\ q^2-1,\ q^4+q^3-q-1$	12357
$q^2-1,\ q^2-1,\ q^4-1$	12457
$q-1,\ q-1,\ q^6-1$	13456
$q-1,\ q-1,\ q^6+q^5+q^4-q^2-q-1$	13467
$q^2-1,\ q^2-1,\ q^4-q^3+q-1$	23457
$q-1,\ q^7-q^5-q^4+q^3+q^2-1$	123456
$q^2-1,\ q^6-q^4+q^2-1$	123457
$q-1,\ q^7+q^6+q^5-q^2-q-1$	123467
$q^2-1,\ q^6+q^5-q-1$	123468
$q^2-1,\ q^6+q^5+q^4-q^2-q-1$	123567
$q^4+q^3-q-1,\ q^4+q^3-q-1$	123568
$q^2-1,\ q^6-1$	124567
$q-1,\ q^7-1$	134567
$q^4-1,\ q^4-1$	134678
$q-1,\ q-1,\ q^3-q^2+q-1,\ q^3-q^2+q-1$	234254
$q^2-1,\ q^6-q^5+q-1$	234567
$q-1,\ q-1,\ q^6-q^5+q^4-q^2+q-1$	1234254
$q^8-q^6-q^5+q^3+q^2-1$	1234567
$q^8+q^7-q^6-2q^5+2q^3+q^2-q-1$	1234568
$q^8+q^7-q^5+q^3-q-1$	1234578
$q^8+q^7+q^6+q^5-q^3-q^2-q-1$	1234678
$q^8+2q^7+2q^6+q^5-q^3-2q^2-2q-1$	1235678
q^8+q^7-q-1	1245678
q^8-1	1345678
$q^3-q^2+q-1,\ q^2-1,\ q^3-q^2+q-1$	2342547
$q^8-q^6+q^2-1$	2345678

Continued on next page

Table A.5 – *continued from previous page*

Orders	Weyl word
$q-1,\ q^7-q^6+q^4-q^3+q-1$	12342546
$q^2-1,\ q^6-q^5+q^4-q^2+q-1$	12342547
$q^8+q^7-q^5-q^4-q^3+q+1$	12345678
$q^3-q^2+q-1,\ q^5-q^4+q-1$	23425467
q^8-q^7+q-1	123425467
$q^8-q^6+q^5-q^3+q^2-1$	123425468
$q^8+q^6-q^2-1$	123425478
$q^8-q^7+q^6-q^5+q^3-q^2+q-1$	234254678
$q^2-1,\ q^6-1$	1234254278
q^8-q^4+1	1234254678
$q^4-q^3+q-1,\ q^4-q^3+q-1$	2342546547
$q^8-q^7-q^6+2q^5-2q^3+q^2+q-1$	12342546547
$q^8-q^7+q^5-q^3+q-1$	23425465478
$q^3-2q^2+2q-1,\ q^5-q^4+q^3-q^2+q-1$	123142345465
$q^3-q^2+q-1,\ q^5+q^3-q^2-1$	123142345478
$q^8-q^6+q^4-q^2+1$	123425465478
$q^2-1,\ q^2-1,\ q-1,\ q+1,\ q-1,\ q+1$	234234542345
$q^8-2q^7+2q^6-q^5+q^3-2q^2+2q-1$	1231423454657
$q^2-q+1,\ q^2-q+1,\ q^4+q^3-q-1$	1231423454658
$q^4-1,\ q-1,\ q+1,\ q-1,\ q+1$	1234234542345
$q+1,\ q+1,\ q^2-1,\ q^2-1,\ q^2-1$	2342345423457
$q^2-q+1,\ q^6-q^3+1$	12314234546578
$q-1,\ q+1,\ q^3-1,\ q^3+1$	12342345423456
$q+1,\ q+1,\ q^2-1,\ q^4-1$	12342345423457
$q+1,\ q+1,\ q^2-1,\ q^4-q^3+q-1$	23423454234567
$q+1,\ q+1,\ q^6-q^5+q-1$	123423454234567
$q+1,\ q+1,\ q^6-1$	123423454234568
$q+1,\ q+1,\ q^6+q^5+q^4-q^2-q-1$	123423454234578
$q+1,\ q+1,\ q^6-q^4+q^2-1$	234234542345678
$q^8-q^7+q^5-q^4+q^3-q+1$	1231423454657658
$q+1,\ q^7+q^6-q^4-q^3+q+1$	1234234542345678
$q^2+1,\ q^2-1,\ q^2+1,\ q^2-1$	2342345423456576
$q^2+1,\ q^4+1,\ q^2-1$	12342345423456576
$q+1,\ q+1,\ q^6-q^5+q^4-q^2+q-1$	23423454234565768
$q+1,\ q^7+1$	123423454234565768
$q^4-q^2+1,\ q^4-q^2+1$	1231423454236547654 8

Continued on next page

Table A.5 – *continued from previous page*

Orders	Weyl word
$q^2-q+1,\ q^2-q+1,\ q^4-q^3+q-1$	1231423143542346547 65
$q^2+1,\ q^2+1,\ q^4-1$	234234542345654765876
$q+1,\ q+1,\ q^2-1,\ q^4+q^3-q-1$	1231423143542314354278
$q^2-q+1,\ q^6-q^5+q^3-q+1$	12314231435423465476 58
$q^2+1,\ q^6+1$	12342345423456547658 76
$q+1,\ q^3+1,\ q^4-q^3+q-1$	1231423143542314354 6576
$q+1,\ q^7-q^5+q^4+q^3-q^2+1$	1231423143542314354657 68
$q^2+q+1,\ q^3-1,\ q-1,\ q^2+q+1$	12314231454231456542 3456
$q^4-q^3+q^2-q+1,\ q^4-q^3+q^2-q+1$	1231423145423456547658 76
$q^2+q+1,\ q^2+q+1,\ q^4-q^3+q-1$	12314231454231456542 3456 7
$q^2+q+1,\ q^2+q+1,\ q^4+q^3-q-1$	12314231454231456542 3456 8
$q+1,\ q^7-q^6+q^5+q^2-q+1$	12314231454231435654765 8 76
$q^2+q+1,\ q^6+q^5-q^3+q+1$	12314231454231456542 3456 78
$q^2+q+1,\ q^6+q^3+1$	1231423145423145654234567687
$q^4+1,\ q^4+1$	1231423143542314654234765487 65
$q+1,\ q+1,\ q+1,\ q+1,\ q^2-1,\ q^2-1$	23423454234565423456765423456 7
$q+1,\ q+1,\ q+1,\ q+1,\ q^4-q^3+q-1$	123423454234565423456765423456 7
$q+1,\ q+1,\ q+1,\ q+1,\ q^4-1$	234234542345654234567654234567 8
$q+1,\ q+1,\ q+1,\ q^5+1$	1234234542345654234567654234567 8
$q^3+q^2+q+1,\ q^2-1,\ q^3+q^2+q+1$	1231423454231456542345676542345 67
$q^3+q^2+q+1,\ q^5+q^4+q+1$	1231423454231456542345676542345678
$q^2-q+1,\ q^2-q+1,\ q^2-q+1,\ q^2-q+1$	1231423143542314565423145676542345678765
$q^2-q+1,\ q^3+1,\ q+1,\ q^2-q+1$	12314231435423143542654231456765423 4567876
$q^4+q^2+1,\ q^4+q^2+1$	12314231435423143546542345676543187 654234567
$q+1,\ q+1,\ q^3+1,\ q^3+1$	1231423143542345654231456765423 1435 465768765
$q^3+q^2+q+1,\ q^5+q^3+q^2+1$	123142314354231456542314356765423 14 35465768765
$q^3+2q^2+2q+1,\ q^5+q^4+q^3+q^2+q+1$	123142314542314565423456765423456 78 76542345678
$q^4+q^3+q^2+q+1,\ q^4+q^3+q^2+q+1$	12314231454231456542314567654231456 7876542345678

Continued on next page

Table A.5 – *continued from previous page*

Orders	Weyl word
$q^2+1,\ q^2+1,\ q^2+1,\ q^2+1$	12314231435423143542654234576542314 3548765423143542654765876
$q+1,\ q+1,\ q+1,\ q+1,\ q+1,\ q+1,\ q^2-1$	12314231435423143542654231435426543 1765423143542654317654234567
$q+1,\ q+1,\ q+1,\ q+1,\ q+1,\ q^3+1$	12314231435423143542654231435426543 17654231435426543176542345678
$q+1,\ q+1,\ q^3+q^2+q+1,\ q^3+q^2+q+1$	12314231435423143542654231435426543 1765423143542654317876542345678
$q^2+q+1,\ q^2+q+1,\ q^2+q+1,\ q^2+q+1$	12314231435423143565423143542676542 31435426543178765423143542654317654 2345678765
$q+1,\ q+1,\ q+1,\ q+1,\ q+1,\ q+1,\ q+1,\ q+1$	12314231435423143542654231435426543 17654231435426543176542345678765423 14354265431765423456787654231435426 543176542345678

Table A.6: Maximal tori in ${}^2\mathrm{A}_5(q)$

Orders	Weyl word
$q-1,\ q^2-1,\ q^2-1$	
$q-1,\ q^2-1,\ q^2-1$	24
$q+1,\ q^2-1,\ q^2-1$	23432
$q^2-q+1,\ q^3+1$	32145
$q-1,\ q^4-1$	2343215
$q^5-q^4+q^3-q^2+q-1$	2321432154
$q+1,\ q^4-1$	123214354321
$q+1,\ q^2-1,\ q^2-1$	2132143215432
$q+1,\ q+1,\ q+1,\ q^2-1$	12132432154321
$q+1,\ q+1,\ q+1,\ q+1,\ q+1$	121321432154321

Table A.7: Maximal tori in ${}^3\mathrm{D}_4(q)$

Orders	Weyl word
$q-1,\ q^3-1$	
q^4-q^3+q-1	134
$q^2-q+1,\ q^2-q+1$	2134
$q^2+q+1,\ q^2+q+1$	21324213

Continued on next page

Table A.7 – *continued from previous page*

Orders	Weyl word
q^4+q^3-q-1	213242132
$q+1,\ q^3+1$	121321421324

Table A.8: Maximal tori in ${}^2\mathrm{E}_6(q)$

Orders	Weyl word
$q-1,\ q-1,\ q^2-1,\ q^2-1$	
$q-1,\ q^5-q^4+q^3-q^2+q-1$	3156
$q^2-q+1,\ q^4-q^3+q-1$	31546
$q-1,\ q-1,\ q^2-1,\ q^2-1$	243542
$q+1,\ q+1,\ q^2-1,\ q^2-1$	343543
$q-1,\ q-1,\ q^4-1$	1431565
$q^2-1,\ q^2-1,\ q^2-1$	423454234
$q^2-q+1,\ q^2-q+1,\ q^2-q+1$	134236542345
$q^2-1,\ q^4-1$	134315465431
$q^2-1,\ q^2-1,\ q^2-1$	3143154316543
$q+1,\ q+1,\ q+1,\ q+1,\ q^2-1$	131431543165431
$q^2-1,\ q^4+q^3-q-1$	1231454654231435
$q^2-1,\ q^4-q^3+q-1$	2342542314356542
$q^6-q^4+q^2-1$	34234542314356542
$q^3+q^2+q+1,\ q^3+q^2+q+1$	234315423143565431
$q^2-1,\ q^4+q^3-q-1$	2314254231435465423 1
$q+1,\ q+1,\ q^4-1$	342314542314354654231
$q^3+1,\ q+1,\ q^2-q+1$	3143542314356542314356
$q^2+q+1,\ q^4+q^2+1$	13423454365423143542654 3
$q^2-q+1,\ q^4+q^3-q-1$	231431542314356542314354 6
$q+1,\ q+1,\ q^4-1$	234231542314354654231435 4
$q+1,\ q+1,\ q+1,\ q^3+1$	234231454231435465423143 54
$q^6-q^5+q^3-q+1$	242314354231435654231435 46
$q+1,\ q+1,\ q^2-1,\ q^2-1$	242314354231435465423143 542654
$q+1,\ q+1,\ q+1,\ q+1,\ q+1,\ q+1$	123142314354231435426542 314354265431

Bibliography

[1] Alejandro Adem and R. James Milgram, *Cohomology of finite groups*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 309, Springer-Verlag, Berlin, 2004. MR 2004k:20109

[2] Shôrô Araki, *On root systems and an infinitesimal classification of irreducible symmetric spaces*, J. Math. Osaka City Univ. **13** (1962), 1–34. MR 27#3743

[3] Claude Archer, *Classification of group extensions*, Ph.D. thesis, Université Libre de Bruxelles, 2002.

[4] Armand Borel, *Linear algebraic groups*, Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991. MR 92d:20001

[5] 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/.

[6] Nicolas Bourbaki, *Lie groups and Lie algebras. Chapters 4–6*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 2002, Translated from the 1968 French original by Andrew Pressley. MR 1890629 (2003a:17001)

[7] John Cannon and Derek F. Holt, *Computing maximal subgroups of finite groups*, J. Symbolic Comput. **37** (2004), no. 5, 589–609. MR 2094616

[8] R. W. Carter, *Conjugacy classes in the Weyl group*, Compositio Math. **25** (1972), 1–59. MR 47#6884

[9] Roger W. Carter, *Simple groups of Lie type*, Wiley Classics Library, John Wiley & Sons Inc., New York, 1989, Reprint of the 1972 original, A Wiley-Interscience Publication. MR 90g:20001

[10] F. Celler, J. Neubüser, and C. R. B. Wright, *Some remarks on the computation of complements and normalizers in soluble groups*, Acta Appl. Math. **21** (1990), no. 1-2, 57–76. MR 1085773 (91m:20026)

[11] Arjeh M. Cohen and Scott H. Murray, *Algorithm for Lang's Theorem*, Preprint, http://arxiv.org/abs/math/0506068, 2005.

[12] Arjeh M. Cohen, Scott H. Murray, and D. E. Taylor, *Computing in groups of Lie type*, Math. Comp. **73** (2004), 1477–1498. MR 2 047 097

[13] S. Collart, M. Kalkbrener, and D. Mall, *Converting bases with the Gröbner walk*, J. Symbolic Comput. **24** (1997), no. 3-4, 465–469, Computational algebra and number theory (London, 1993). MR 1484492

[14] Meinolf Geck and Götz Pfeiffer, *Characters of finite Coxeter groups and Iwahori-Hecke algebras*, London Mathematical Society Monographs. New Series, vol. 21, The Clarendon Press, Oxford University Press, New York, 2000. MR 2002k:20017

[15] Sergei Haller, *Entwicklung und Implementierung eines Algorithmus zur Berechnung von Kommutatoren unipotenter Elemente in Chevalley-Gruppen*, Diplomarbeit, Justus-Liebig Universität Gießen, Gießen, April 2000.

[16] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977. MR 57#3116

[17] D. F. Holt, *The mechanical computation of first and second cohomology groups*, J. Symbolic Comput. **1** (1985), no. 4, 351–361. MR 87i:20005

[18] James E. Humphreys, *Linear algebraic groups*, Springer-Verlag, New York, 1975, Graduate Texts in Mathematics, No. 21. MR 53#633

[19] ———, *Reflection groups and Coxeter groups*, Cambridge Studies in Advanced Mathematics, vol. 29, Cambridge University Press, Cambridge, 1990. MR 1066460 (92h:20002)

[20] Max-Albert Knus, Alexander Merkurjev, Markus Rost, and Jean-Pierre Tignol, *The book of involutions*, American Mathematical Society Colloquium Publications, vol. 44, American Mathematical Society, Providence, RI, 1998. MR 2000a:16031

[21] C. Krook, *Graphs related to $E_7(q)$. A quest for distance-transitivity*, Master's thesis, Technische Universiteit Eindhoven, Eindhoven, January 2004.

[22] Roberto Pasqualucci, *The Conjugacy classes in the Weyl groups*, Master's thesis, "La Sapienza" University Roma, 1991–92.

[23] Vladimir Platonov and Andrei Rapinchuk, *Algebraic groups and number theory*, Pure and Applied Mathematics, vol. 139, Academic Press Inc., Boston, MA, 1994. MR 95b:11039

[24] 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.

[25] M. S. Raghunathan, *Tori in quasi-split-groups*, J. Ramanujan Math. Soc. **19** (2004), no. 4, 281–287. MR 2125504

[26] Remko Juriën Riebeek, *Computations in association schemes*, Thesis Publishers, Amsterdam, 1998, Dissertation, Technische Universiteit Eindhoven, Eindhoven, 1998. MR 99d:05089

[27] 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. MR 47#5135

[28] Doris J. Schattschneider, *On restricted roots of semi-simple algebraic groups*, J. Math. Soc. Japan **21** (1969), 94–115. MR 38 #4485

[29] Martin Selbach, *Klassifikationstheorie halbeinfacher algebraischer Gruppen*, Mathematisches Institut der Universität Bonn, Bonn, 1976, Diplomarbeit, Univ. Bonn, Bonn, 1973, Bonner Mathematische Schriften, Nr. 83. MR 55 #5759

[30] Jean-Pierre Serre, *Galois cohomology*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002. MR 2002i:12004

[31] T. A. Springer and R. Steinberg, *Conjugacy classes*, Seminar on Algebraic Groups and Related Finite Groups (The Institute for Advanced Study, Princeton, N.J., 1968/69), Lecture Notes in Mathematics, Vol. 131, Springer, Berlin, 1970, pp. 167–266. MR 42#3091

[32] Tonny A. Springer, *Linear algebraic groups*, Progress in Mathematics, vol. 9, Birkhäuser Boston Inc., Boston, MA, 1998. MR 99h:20075

[33] Helmut Strade, *Simple Lie algebras over fields of positive characteristic. I*, de Gruyter Expositions in Mathematics, vol. 38, Walter de Gruyter & Co., Berlin, 2004, Structure theory. MR 2 059 133

[34] Helmut Strade and Rolf Farnsteiner, *Modular Lie algebras and their representations*, Monographs and Textbooks in Pure and Applied Mathematics, vol. 116, Marcel Dekker Inc., New York, 1988. MR 89h:17021

[35] Franz Georg Timmesfeld, *Abstract root subgroups and simple groups of Lie type*, Monographs in Mathematics, vol. 95, Birkhäuser Verlag, Basel, 2001. MR 1852057 (2002f:20070)

[36] J. Tits, *Normalisateurs de tores. I. Groupes de Coxeter Étendus*, J. Algebra **4** (1966), 96–116. MR 34#5942

[37] 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. MR 37#309

[38] ______, *Groupes de Whitehead de groupes algébriques simples sur un corps (d'après V. P. Platonov et al.)*, Séminaire Bourbaki, 29e année (1976/77), Lecture Notes in Math., vol. 677, Springer, Berlin, 1978, pp. Exp. No. 505, pp. 218–236. MR 521771 (80d:12008)

[39] Jacques Tits and Richard M. Weiss, *Moufang polygons*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002. MR 2003m:51008

Index

V

W

Z

Samenvatting

Om op een efficiënte manier te rekenen met groepen is een geschikte voorstelling nodig van de groepselementen. Een groep heeft vaak een *intrinsieke* definitie, dat wil zeggen dat zij impliciet gedefinieerd wordt door een beschrijving van de eigenschappen van de elementen (bijv.: de vaste punt ondergroep van een groep). Een dergelijke definitie is voor berekeningen met groepselementen niet erg handig aangezien het, afgezien van de identiteit, geen construeerbare groepselementen geeft. In dergelijke gevallen dient men te beschikken over een extrinsieke definitie van de groep, zoals een voorstelling.

Wij ontwerpen en implementeren algoritmen voor berekeningen aan gedraaide groepen van Lie-type, waaronder begrepen zijn de groepen die niet quasi-gespleten zijn. Algoritmen voor het rekenen met elementen in de Steinberg voorstelling voor ongedraaide groepen van Lie-type en algoritmen voor de overgang tussen deze voorstelling en de lineaire representatie worden gegeven in [12] (gebaseerd op werk van [15] en [26]). Dit werk wordt in diverse richtingen uitgebreid.

De gedraaide groepen van Lie-type zijn groepen van rationale punten van gedraaide vormen van reductieve lineaire algebraïsche groepen. De gedraaide vormen zijn geclassificeerd door Galoiscohomologie. Ten einde de Galoiscohomologie te berekenen ontwerpen we een methode voor het berekenen van de cohomologie van een eindig voortgebrachte groep Γ op een groep A. Deze methode is op zichzelf van belang. De methode wordt toegepast op de berekening van de Galoiscohomologie van een reductieve lineaire algebraïsche groep.

Laat G een reductieve lineaire algebraïsche groep gedefinieerd over een lichaam k zijn. Een gedraaide groep van Lie-type $G_{\boldsymbol{\alpha}}(k)$ wordt uniek bepaald door de cocykel $\boldsymbol{\alpha}$ van de Galois groep van K op $\mathrm{Aut}_K(G)$, en de groep van K-algebraïsche automorfismen waar K de eindige Galoisuitbreiding over k is. Algoritmen voor de berekening van het relatieve wortelsysteem op $G_{\boldsymbol{\alpha}}(k)$, voor de wortelondergroepen en de wortelelementen worden gegeven. Daarnaast worden ook algoritmen voor de berekening van onderlinge relaties, zoals de commutatorrelaties en producten gegeven. Dit maakt het mogelijk om te rekenen binnen de normale ondergroep $G_{\boldsymbol{\alpha}}(k)^{\dagger}$ van $G_{\boldsymbol{\alpha}}(k)$ voortgebracht door de wortelelementen. We passen het algoritme toe op diverse voorbeelden, waaronder ${}^2\mathrm{E}_{6,1}(k)$ en ${}^{3,6}\mathrm{D}_{4,1}(k)$.

Een toepassing is een algoritme, ontworpen voor de berekening van alle gedraaide maximale tori van een eindige groep van Lie-type. De orde van zo'n torus wordt berekend als een polynoom in q, de orde van het lichaam k. Daarnaast berekenen we de ordes van de faktoren in de decompositie van de torus als een direkt product van cyklische ondergroepen.

Voor een gegeven lichaam k, worden de maximale tori van $G_{\boldsymbol{\beta}}(k)$ berekend als ondergroepen van $G_{\boldsymbol{\beta}}(K)$ over een uitbreidingslichaam K en daarna wordt de effectieve versie van Lang's Theorem [11] gebruikt om de torus te conjugeren tot een k-torus, wat een ondergroep van $G_{\boldsymbol{\beta}}(k)$ is.

Gebruikmakend van deze informatie over maximale tori, geven we een algoritme voor de berekening van alle Sylowondergroepen van de groep van Lie-type. Als p niet de karakteristiek van het lichaam is, wordt de Sylowondergroep berekend als een ondergroep van de normalisator van de k-torus.

Alle hier besproken algoritmen zijn geïmplementeerd in MAGMA [5].

Acknowledgments

There are many people I would like to thank for helping me (explicitly or implicitly) in this project. First and formost, I would like to express my thanks to both my supervisors, A.M. Cohen and F.G. Timmesfeld. Prof. Timmesfeld supervised me starting with my first year as an undergraduate student, during my diploma thesis and my Ph.D. project. I learned from him the affinity to abstract algebra and group theory. Prof. Cohen introduced me in the beautiful world of algebraic groups and guided me through my time as a Ph.D. student. Without their support and advices, this work would not be possible.

I would like to thank Scott Murray, whose role during my Ph.D. project comes close to the role of a copromotor. Especially my visit at the University of Sydney in 2004, where he was employed at that time, was a very important step in my research.

I would like to thank everybody who expressed interest in my work and inspired me to new ideas, without mentioning each name explicitly.

I would like to thank the Departments of Mathematics of the Justus-Liebig University of Gießen and the Technical University of Eindhoven, where I spent the last years of my research.

I thank all my friends for just being my friends, especially Nguyễn Văn Minh Mẫn, who was my office and apartment mate during my stays at the Eindhoven University in the last years.

I would like to thank my parents Nina and Andreas for their support through all my life.

I would like to thank my wife Natalia for her love.

Curriculum Vitae

Sergei Haller was born on March 4th, 1975 in Krasnoturinsk, Russia. He studied at School Number 9 in Krasnoturinsk from 1982 until 1990, with highest available marks in all subjects. He studied at Herderschule High School in Gießen, Germany, in 1990–1994.

After a year in the Bundeswehr, the German army, he started studying mathematics at the Justus-Liebig Universität Gießen in 1995. He obtained his diploma with a thesis entitled *Entwicklung und Implementierung eines Algorithmus zur Berechnung von Kommutatoren unipotenter Elemente in Chevalley-Gruppen* [15] (*Development and implementation of an algorithm for computing commutators of unipotent elements in Chevalley groups*), which obtained a mark of 1.0, in April 2000.

He has worked as a scientific assistant at the Mathematics Department of the Universität Gießen since May 2000. The present Ph.D. project was started in September 2002 and supervised by Prof. Arjeh M. Cohen from the Technische Universitait Eindhoven and Prof. Franz G. Timmesfeld from the Universität Gießen.