Algorithms for Lie Algebras of Algebraic Groups

A catalogue record is available from the Eindhoven University of Technology Library.
ISBN: 978-90-386-2176-0

Printed by Printservice Technische Universiteit Eindhoven.

Cover: The extended Dynkin diagram of type E_7 and its automorphism, and the root system of type G_2. Design in cooperation with Verspaget & Bruinink.

Algorithms for Lie Algebras of 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 donderdag 18 maart 2010 om 16.00 uur

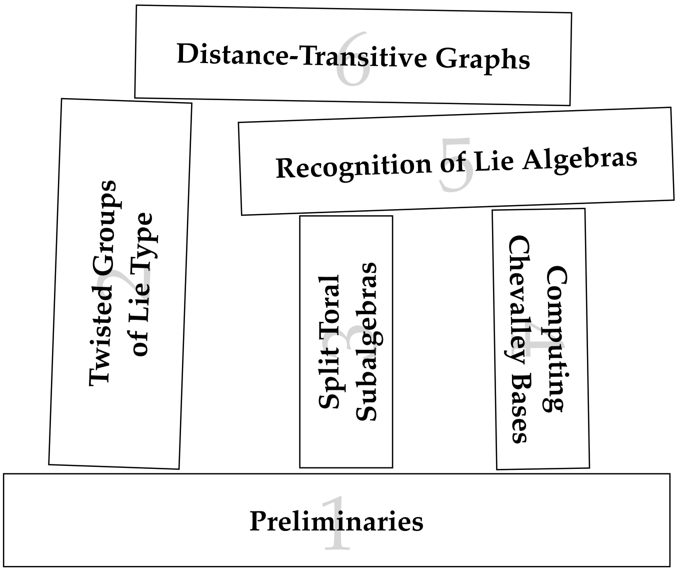
door

Danker Adriaan Roozemond

geboren te Leiden

Dit proefschrift is goedgekeurd door de promotor:

prof.dr. A.M. Cohen


Distance-Transitive Graphs
6
Twisted Groups of Lie Type
2
Recognition of Lie Algebras
5
Split Toral Subalgebras
3
Computing Chevalley Bases
4
Preliminaries
1

Contents

Introduction

Lie algebras are called after Sophus Lie (1842 – 1899), a Norwegian nineteenth century mathematician who realized that continuous transformation groups could be studied by linearizing them, obtaining what he called the *infinitesimal group*. These objects are what we now call *Lie algebras*.

Independently, Wilhelm Killing (1847 – 1923) introduced Lie algebras, and he proved that (at least over the complex numbers) only certain finite-dimensional simple Lie algebras could exist: the four *infinite series* and the five *exceptional Lie algebras* that are well known today. To this end, he introduced the concepts of root system, Cartan subalgebra, and Cartan matrix. These last two concepts now carry the name of Élie Cartan (1869 – 1951), whose major contribution was to prove that the five exceptional Lie algebras Killing had found actually exist. A later major contributor to this area was Claude Chevalley (1909–1984), who wrote the *Theory of Lie Groups*, a book in three volumes that systematically treats the theory of groups of Lie type and Lie algebras. (The biographical information presented here may be found in the excellent MacTutor History of Mathematics archive [OR09].)

Work by Chevalley and Leonard Dickson showed that the Lie algebras that Killing and Cartan found, commonly called *the classical Lie algebras*, also exist over finite fields, but there is more. Research by Nathan Jacobson, Aleksei Kostrikin, Ernst Witt, Igor Šafarevič, and Hans Zassenhaus produced the so-called *Cartan type Lie algebras*, and Hayk Melikyan found a new family of simple Lie algebras over fields of characteristic 5. Over the past 15 years, Alexander Premet and Helmut Strade have shown that over algebraically closed fields of characteristic at least 5 every simple Lie algebra belongs to one of these three classes. For characteristic 3 such a result has not been proved, and the characteristic 2 case is still far from settled: as recently as 2006 Michael Vaughan-Lee found two new simple Lie algebras over the field with two elements.

A brief overview of the classification of the simple Lie algebras over finite fields can be found in an unpublished note by Strade [Str06]. The existence of several classes of simple Lie algebras over finite fields leads to the problem of recognizing these: given a simple Lie algebra, find out which class it belongs to. In particular: decide whether a given simple Lie algebra is classical or not.

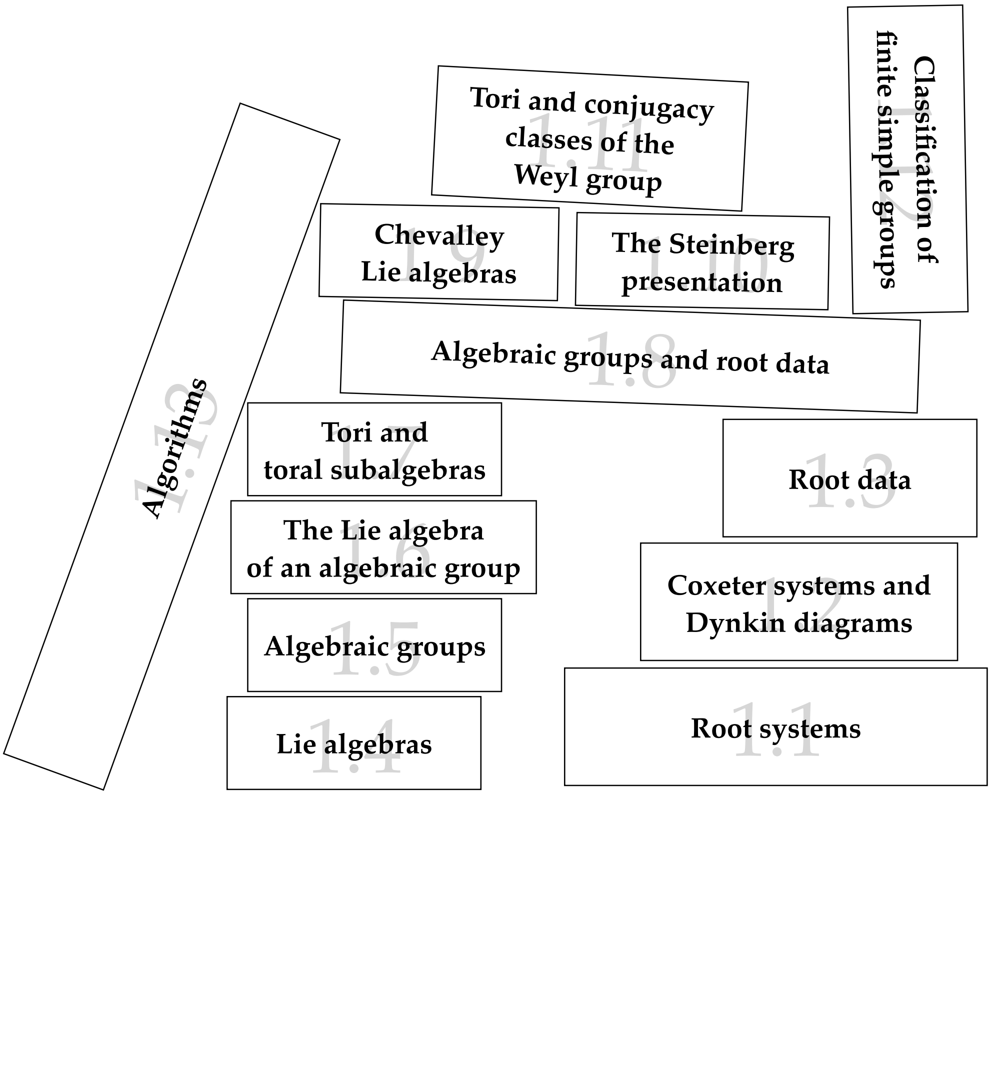
The new results in this thesis are set within the classical Lie algebras: the four infinite series A_n, B_n, C_n, D_n and the five exceptional Lie algebras E_6, E_7, E_8, F_4, G_2. These Lie algebras occur in two ways: as Lie algebras of algebraic groups (in the manner that Lie himself envisioned) and as the main objects that the *simple* *groups of Lie type* act on. The *classification of finite simple groups*, a major effort by the mathematical community in the twentieth century, shows that the simple groups of Lie type form a significant class of finite simple groups. A not too technical introduction to this classification is a short article by Ron Solomon [Sol95] that appeared in the notices of the AMS.

In recent years significant progress has been made to effectively calculate with and in these groups and algebras on the computer, including implementations in, for example, the GAP and MAGMA computer algebra systems. This research is partly stimulated by the matrix group recognition project: an international project whose main aim is solving problems with matrix groups over finite fields. We build in particular on work by Arjeh Cohen, Willem de Graaf, Sergei Haller, Scott Murray, and Don Taylor. Many algorithms that have been previously developed in this branch of research, however, apply only to groups and algebras over fields of characteristic 0 or at least 5. In this thesis we focus mainly on the characteristic 2 and 3 cases.

Reading guide

Chapter 1 covers the basic notions in the research area of Lie theory. Since this field has existed for quite some time now, the notions are rather numerous and the chapter accordingly elaborate. Chapter 2 contains a digression to the twisted groups of Lie type. In particular we explicitly construct the automorphisms needed to construct groups of type ${}^2B_2$, ${}^2F_4$, and ${}^2G_2$, and we exhibit these automorphisms as endomorphisms of Lie algebras as well. In Chapter 3 we investigate the computation of split maximal toral subalgebras over fields of characteristic 2, show why existing methods will not always work, and present a heuristic algorithm for this purpose. Chapter 4 shows how to construct Chevalley bases of the classical Lie algebras over any characteristic, including 2 and 3. We prove that the algorithm runs in time polynomial in the input. In Chapter 5 the results of Chapters 3 and 4 are used to produce algorithms for recognition of Lie algebras. In Chapter 6 we apply the algorithms described and their implementation to obtain a computer aided proof that there is no graph on which a certain group acts distance transitively.

If you are an expert in the subject area of this thesis, it is probably best to skip Chapter 1, and start reading in Chapter 2 (if you want to freshen up your knowledge of these extraordinary twisted groups) or Chapter 3 (if you are primarily interested in the results). If you are no expert in this area, but you are a mathematician, it is probably best to simply start with Chapter 1 and go from there. If you are not a mathematician or you have no desire to learn about Lie theory, skip to the abstract (or the samenvatting), possibly read the acknowledgements, and then get a copy of the excellent book *Finding Moonshine* (or *Het Symmetriemonster*) by Marcus du Sautoy to learn about the beauty of symmetry.


1.11 Tori and conjugacy classes of the Weyl group
1.12 Classification of finite simple groups
1.9 Chevalley Lie algebras
1.10 The Steinberg presentation
1.8 Algebraic groups and root data
1.13 Algorithms
1.7 Tori and toral subalgebras
1.3 Root data
1.6 The Lie algebra of an algebraic group
1.2 Coxeter systems and Dynkin diagrams
1.5 Algebraic groups
1.4 Lie algebras
1.1 Root systems

1 Preliminaries

This chapter covers the basic notions relevant to this thesis, such as root data, algebraic groups, and Lie algebras. Our treatment of algebraic groups and the corresponding Lie algebras rests on the theory developed mainly by Chevalley and available in textbooks Borel [Bor91], Carter [Car72], Humphreys [Hum72, Hum75], Jacobson [Jac62], and Springer [Spr98]. The interested reader is encouraged to consult any of these excellent books for more details.

Almost all proofs have been omitted, except some that are particularly short, elegant, or enlightening. If a result from a particular source is given along with a proof, that proof has been taken from that same source unless otherwise mentioned.

1.1 Root systems

The *root system* is a combinatorial object fundamental to many of the mathematical structures that are the topic of this thesis.

Let V be a Euclidian space of finite dimension n and let (v, w) denote the inner product of v and w. For each non-zero vector $\alpha \in V$ we denote by s_α the reflection in the hyperplane orthogonal to α, i.e., the linear map defined by

$$s_\alpha : \beta \mapsto \beta - \frac{2(\beta, \alpha)}{(\alpha, \alpha)}\alpha.$$

We define, for $\alpha \in V$:

$$\alpha^\vee = \frac{2\alpha}{(\alpha, \alpha)}$$

and we write $\langle \beta, \alpha^\vee \rangle$ instead of $(\beta, \alpha^\vee)$ (for consistency of notation when we arrive at root data) so that the definition of s_α simplifies to $s_\alpha : \beta \mapsto \beta - \langle \beta, \alpha^\vee \rangle \alpha$.

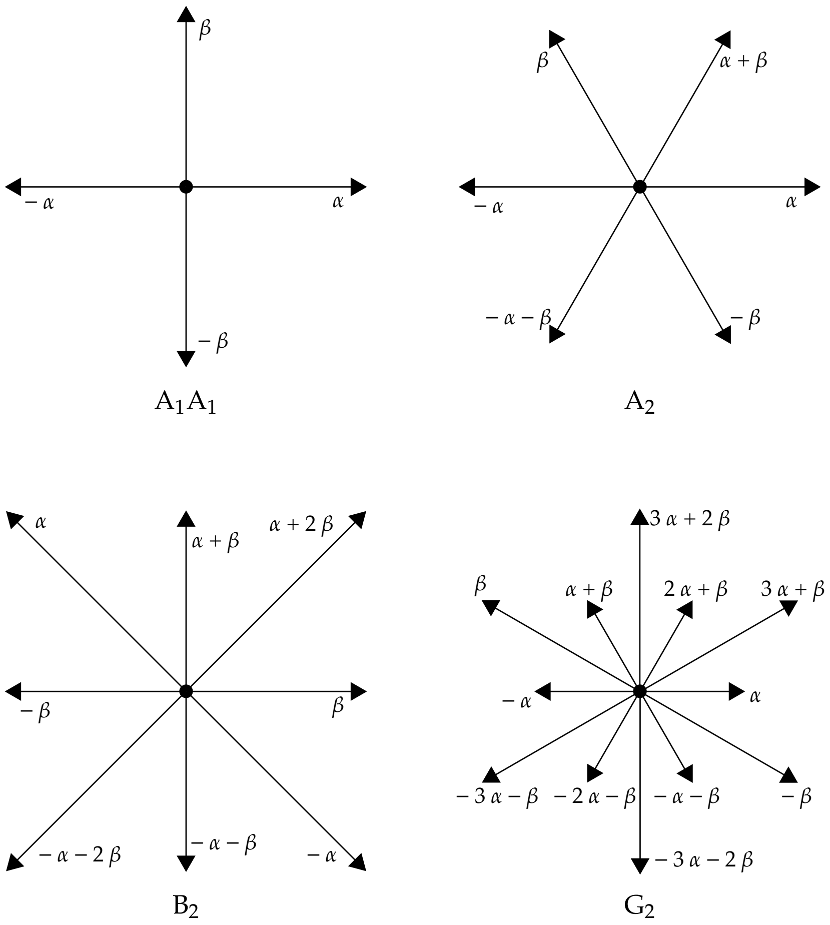
Definition 1.2 (Root System)**.** A subset Φ of V is called a *root system in V* if the following axioms are satisfied:

(i) Φ is a finite set of non-zero vectors.

(ii) Φ spans V.

(iii) If $\alpha, \beta \in \Phi$ then $s_\alpha(\beta) \in \Phi$.

(iv) If $\alpha, \beta \in \Phi$ then $\langle \beta, \alpha^\vee \rangle \in \mathbb{Z}$.



A_1A_1 A_2 B_2 G_2

Figure 1.1: All root systems of rank two

(v) If $\alpha, t\alpha \in \Phi$, where $t \in \mathbb{R}$, then $t = \pm 1$.

Observe that from (iii) it follows that $-\alpha \in \Phi$ whenever $\alpha \in \Phi$. Sometimes (v) is omitted, defining a so-called *nonreduced root system*. In this thesis, however, a root system is taken to be reduced unless otherwise specified.

The elements of a root system Φ are called its *roots*. The *rank* of Φ is defined to be $\dim(V)$ and denoted $\operatorname{rk}(\Phi)$. A subset $\Delta \subseteq \Phi$ is called a *set of fundamental roots* (or a *set of simple roots*) if $\Delta = \{\alpha_1, \ldots, \alpha_n\}$ is a basis of V relative to which each $\alpha \in \Phi$ has a unique expression $\alpha = \sum c_i \alpha_i$, where the c_i are integers and the c_i are either all nonnegative or all nonpositive. Such sets of fundamental roots exist (cf. [Car72, Proposition 2.1.3]). The roots for which all c_i are nonnegative (resp. nonpositive) are called the *positive* (resp. *negative*) roots, and the set of positive (resp. negative) roots is denoted Φ^+ (resp. Φ^-).

A root system Ψ is said to be *isomorphic* to a root system Φ if there is an isometry of their Euclidian spaces that maps Ψ to Φ.

The *length* of a root $\alpha \in \Phi$ is simply its length in V. It will follow from the classification of root systems that at most two different lengths occur in a given root system, justifying the division of the set of roots into *short roots* and *long roots* in case different lengths occur.

A root system is called *irreducible* if it cannot be partitioned into the union of two mutually orthogonal proper subsets.

1.1.1 The Weyl group

Let Φ be a root system. We denote by $W(\Phi)$ the group generated by the reflections $\{s_\alpha \mid \alpha \in \Phi\}$. The group $W(\Phi)$ is called the *Weyl group* of Φ. It is a group of orthogonal transformations of V, and by axiom (iii) of Definition 1.2 it transforms Φ into itself. By (ii) it acts faithfully on Φ. Therefore, since Φ is a finite set, $W(\Phi)$ is a finite group.

1.1.2 Irreducible root systems

It follows immediately from Definition 1.2(v) that, up to isomorphism, there is only one root system of rank one. The irreducible root systems of higher rank have been classified, and an important tool to come to that classification are the root systems of rank two. So suppose $\operatorname{rk}(\Phi) = 2$ and take α, β to be two simple roots.

Lemma 1.3 ([Spr98, Lemma 7.5.1])**.** *We have the following properties for $\langle \alpha, \beta^\vee \rangle$:*

(i) $\langle \alpha, \beta^\vee \rangle \langle \beta, \alpha^\vee \rangle$ is one of $0, 1, 2, 3$.

(ii) If $|\langle \alpha, \beta^\vee \rangle| > 1$ then $|\langle \beta, \alpha^\vee \rangle| = 1$.

(iii) In the four cases of (i), the order of $s_\alpha s_\beta$ is $2, 3, 4, 6$, respectively.

(iv) If $\langle \alpha, \beta^\vee \rangle = 0$, then $\langle \beta, \alpha^\vee \rangle = 0$.

Proof Note that s_α and s_β stabilize the two dimensional subspace of Φ spanned by α and β. On the basis $\{\alpha, \beta\}$ of that space, $s_\alpha s_\beta$ is represented by the matrix

$$M = \begin{pmatrix} \langle \alpha, \beta^\vee \rangle \langle \beta, \alpha^\vee \rangle - 1 & \langle \beta, \alpha^\vee \rangle \\ -\langle \alpha, \beta^\vee \rangle & -1 \end{pmatrix}.$$

Now, as the Weyl group is finite, $s_\alpha s_\beta$ has finite order, so the eigenvalues of M are two conjugate roots of unity and $|\langle \alpha, \beta^\vee \rangle \langle \beta, \alpha^\vee \rangle - 2| = |\mathrm{tr}(M)| = |\lambda + \overline{\lambda}| \leq |\lambda| + |\overline{\lambda}| = 2|\lambda| \leq 2$ since $\lambda^n = 1$. As M cannot be the identity matrix, the eigenvalues cannot both be 1, so (i) and (ii) follow. By straightforward calculations, (iii) also follows. If $\langle \alpha, \beta^\vee \rangle = 0$, then M is a triangular matrix with the same value in each diagonal entry, so it can only have finite order if it is diagonal. This implies that then also $\langle \beta, \alpha^\vee \rangle = 0$. □

In Figure 1.1 the four possible reduced root systems of rank two are shown, corresponding to the cases in Lemma 1.3(iii). For general rank, the irreducible root systems are described in Cartan's notation A_n $(n \geq 1)$, B_n $(n \geq 2)$, C_n $(n \geq 3)$, D_n $(n \geq 4)$, E_n $(n \in \{6, 7, 8\})$, F_4, and G_2.

1.1.3 Weights and the fundamental group

A vector $w \in V$ is called a *weight* if $\langle w, \alpha^\vee \rangle \in \mathbb{Z}$ for all $\alpha \in \Phi$. These weights form a lattice Λ called the *weight lattice* in which the lattice Λ_Φ spanned by Φ is a sublattice of finite index. If $\Delta = \{\alpha_1, \ldots, \alpha_n\}$ is a set of fundamental roots for Φ, then Λ has a corresponding basis of *fundamental weights* $\{\lambda_1, \ldots, \lambda_n\}$ such that $\langle \lambda_i, \alpha_j^\vee \rangle = \delta_{ij}$. The quotient Λ / Λ_Φ is called the *fundamental group*.

The fundamental group has the following structure for the irreducible root systems (see for example [Hum72, Section 13].) For A_n, it is $\mathbb{Z}/(n+1)\mathbb{Z}$, for B_n, C_n, and E_7 it is $\mathbb{Z}/2\mathbb{Z}$, for D_n it is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (if n is even) or $\mathbb{Z}/4\mathbb{Z}$ (if n is odd), for E_6 it is $\mathbb{Z}/3\mathbb{Z}$, and for E_8, F_4, and G_2 it is trivial.

1.2 Coxeter systems and Dynkin diagrams

Let Φ be a root system, $W = W(\Phi)$ its Weyl group, and $\{\alpha_1, \ldots, \alpha_n\}$ a set of fundamental roots. The pair (W, S), where $S = \{s_{\alpha_1}, \ldots, s_{\alpha_n}\}$, is called a *Coxeter system*. The *Cartan matrix* C of R is the $n \times n$ matrix whose (i, j) entry is $\langle \alpha_i, \alpha_j^\vee \rangle$. The matrix C is related to the Coxeter type of (W, S) as follows: $s_{\alpha_i} s_{\alpha_j}$ has order m_{ij} where

$$\cos \left(\frac{\pi}{m_{ij}} \right)^2 = \frac{\langle \alpha_i, \alpha_j^\vee \rangle \langle \alpha_j, \alpha_i^\vee \rangle}{4}.$$

The *Coxeter matrix* is $(m_{ij})_{1 \leq i,j \leq n}$ and the *Coxeter diagram* is a graph-theoretic representation thereof: it is a graph with vertex set $\{1, \ldots, n\}$ whose edges are the pairs $\{i, j\}$ with $m_{ij} > 2$; such an edge is labeled m_{ij}. The Cartan matrix C determines the Dynkin diagram (and vice versa). For, the *Dynkin diagram* is the Coxeter diagram with the following extra information about root lengths: $\langle \alpha_i, \alpha_j^\vee \rangle < \langle \alpha_j, \alpha_i^\vee \rangle$ if and

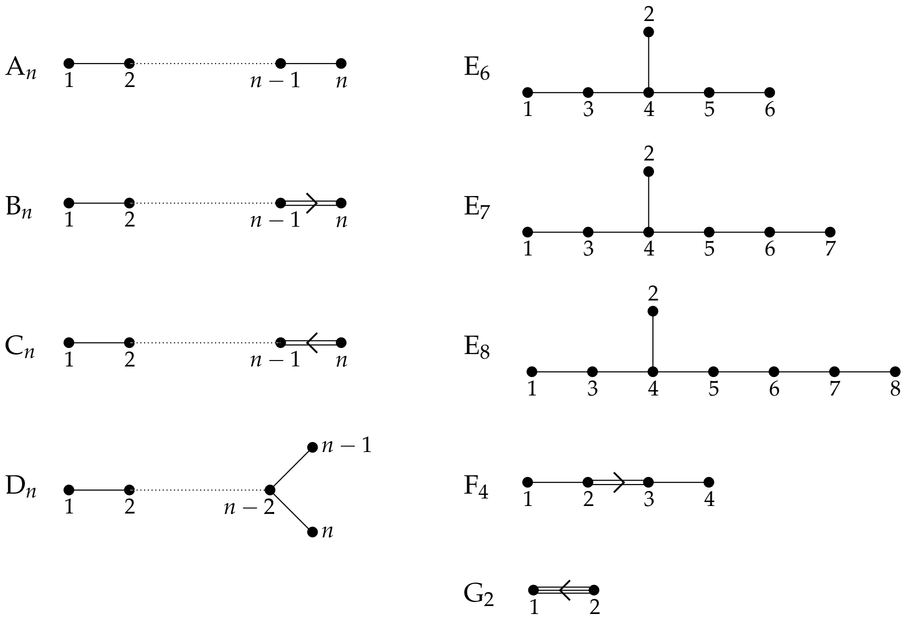


Figure 1.4: Dynkin diagrams

only if the Coxeter diagram edge $\{i, j\}$ (labelled m_{ij}) is replaced by the directed edge (i, j) in the Dynkin diagram (so that the arrow head serves as a mnemonic for the inequality sign indicating that the root length of α_i is larger than the root length of α_j).

The *Dynkin diagrams* of irreducible root systems are well known, and they are depicted in Figure 1.4, where the nodes are labeled as in [Bou81].

1.3 Root data

A slightly more general notion than root system is that of a *root datum*, an important tool in the theory of algebraic groups. It will turn out that connected reductive algebraic groups are classified by their root datum (cf. Theorem 1.43). Also, Chevalley Lie algebras (introduced in Section 1.9) will be parametrized by root data.

Definition 1.5 (Root datum)**.** A *root datum* is a quadruple $R = (X, \Phi, Y, \Phi^\vee)$, where

(i) X and Y are dual free $\mathbb{Z}$-modules of finite rank.

(ii) $\langle \cdot, \cdot \rangle : X \times Y \to \mathbb{Z}$ is a bilinear pairing putting X and Y into duality.

(iii) Φ is a finite subset of X and $\Phi^\vee$ a finite subset of Y.

(iv) There is a one-to-one correspondence $^\vee : \Phi \to \Phi^\vee$.

For $\alpha \in \Phi$ we define endomorphisms $s_\alpha : X \to X$ and $s_{\alpha^\vee} : Y \to Y$ by

$$s_\alpha(x) = x - \langle x, \alpha^\vee \rangle \alpha, \;\; s_{\alpha^\vee}(y) = y - \langle \alpha, y \rangle \alpha^\vee.$$

The following axioms are imposed:

(v) $\langle \alpha, \alpha^\vee \rangle = 2$, for all $\alpha \in \Phi$.

(vi) $s_\alpha(\Phi) = \Phi$ and $s_{\alpha^\vee}(\Phi^\vee) = \Phi^\vee$, for all $\alpha \in \Phi$.

(vii) If $\alpha, t\alpha \in \Phi$, where $t \in \mathbb{R}$, then $t = \pm 1$.

Denote by $\langle \Phi \rangle_X$ the submodule of X generated by Φ and put $V = \langle \Phi \rangle_X \otimes \mathbb{R}$. It follows immediately that Φ is a root system in V, provided it is nonempty. Similarly, $\Phi^\vee$ is a root system in $\langle \Phi^\vee \rangle_Y \otimes \mathbb{R}$.

Conversely, suppose Φ is a root system in some Euclidian space V with inner product $(\cdot, \cdot)$. Recall from Section 1.1 that $\alpha^\vee = 2\alpha/(\alpha, \alpha)$ and define $\Phi^\vee = \{\alpha^\vee \mid \alpha \in \Phi\}$. Choose the lattice X to be equal to $\mathbb{Z}\Phi$, take the lattice $Y = \{y \in V \mid (x, y) \in \mathbb{Z}$ for all $x \in X\}$, and define $\langle x, y^\vee \rangle = (x, y^\vee)$ for $x \in X$ and $y \in Y$. Then $R = (X, \Phi, Y, \Phi^\vee)$ is a root datum.

Example 1.6. Take Φ to be a root system of type B_2 in $\mathbb{R}^2$, e.g., $\alpha = (-1, 1)$, $\beta = (1, 0)$, and $\Phi = \{\pm\alpha, \pm\beta, \pm(\alpha + \beta), \pm(\alpha + 2\beta)\}$. Then $\alpha^\vee = (-1, 1)$ and $\beta^\vee = (2, 0)$, so that the vectors $(1, 0)$ and $(0, 1)$ form a basis for $\mathbb{Z}\Phi$ and the vectors $(-1, 1)$ and $(1, 1)$ form a basis for $\mathbb{Z}\Phi^\vee$.

We take $X = Y = \mathbb{Z}\Phi$ so that $R = (X, \Phi, Y, \Phi^\vee)$ is indeed a root datum.

The *rank* of a root datum is defined to be the dimension of $X \otimes \mathbb{R}$ (and therefore that of $Y \otimes \mathbb{R}$), and the *semisimple rank* is defined to be the dimension of $\mathbb{Z}\Phi \otimes \mathbb{R}$. The roots of Φ are called the *roots* of the root datum and the roots of $\Phi^\vee$ are called the *coroots* of the root datum. A root datum is called *irreducible* if Φ is. A root datum is called *semisimple* if its rank is equal to its semisimple rank. Each semisimple root datum can be decomposed uniquely into irreducible root data.

A root datum $R = (X, \Phi, Y, \Phi^\vee)$ is said to be *isomorphic* to a root datum $R' = (X', \Phi', Y', \Phi^{\vee\prime})$ if there are isomorphisms between X and X' and between Y and Y', both denoted φ, such that their restrictions to Φ and $\Phi^\vee$ are isomorphisms of root systems (as defined in Section 1.1). Furthermore, φ must satisfy $\langle \varphi x, \varphi y \rangle = \langle x, y \rangle$, for all $x \in \Phi, y \in \Phi^\vee$.

By the definition of reflections in root systems, we not only have the map $s_\alpha : X \to X$ for all $\alpha \in \Phi$, but also $s_{\alpha^\vee} : Y \to Y$ for all $\alpha^\vee \in \Phi^\vee$. The group $W(\Phi^\vee)$ generated by $\{s_{\alpha^\vee} \mid \alpha^\vee \in \Phi^\vee\}$ is isomorphic to $W(\Phi)$ (see [Bou81, Chapter VI.1] for more details).

Recall from Section 1.1.3 that a weight is a vector w in the Euclidian space $X \otimes \mathbb{R}$, such that $\langle w, \alpha^\vee \rangle \in \mathbb{Z}$ for all $\alpha \in \Phi$. These weights form a weight lattice, and that the fundamental group is the quotient of this lattice by the root lattice $\mathbb{Z}\Phi$. This fundamental group dictates the possible semisimple root data with a given root system Φ via the quotient $X/\mathbb{Z}\Phi$.

We will use this observation to introduce the *isogeny type* of a root datum. If $X/\mathbb{Z}\Phi$ is the trivial group, R is said to be of *adjoint* isogeny type, or *the adjoint root* *datum of type* Φ. If $X/\mathbb{Z}\Phi$ on the other hand is the full fundamental group, R is said to be of *simply connected* isogeny type, or *the simply connected root datum of type* Φ. If neither of these holds, R is said to be of *intermediate* isogeny type. Note that the last case only occurs for root systems of type A_n (and then only if $n+1$ is not prime) and D_n.

We denote an irreducible adjoint root datum of type X_n by ${X_n}^{\mathrm{ad}}$, and the corresponding simply connected root datum by ${X_n}^{\mathrm{sc}}$. Intermediate root data of type A_n will be denoted by $\mathrm{A}_n^{(k)}$, where $k|(n+1)$. Intermediate root data of type D_n will be denoted by $\mathrm{D}_n^{(1)}$ if n is odd, and by $\mathrm{D}_n^{(1)}$, $\mathrm{D}_n^{(n-1)}$, and $\mathrm{D}_n^{(n)}$ if n is even.

1.3.1 Computational conventions

In order to work with these objects on a computer, we let n be the rank of R and l the semisimple rank, we fix $X = Y = \mathbb{Z}^n$, and we set $\langle x, y \rangle = xy^\top$, which is an element of $\mathbb{Z}$ since x and y are row vectors. Now take A to be the integral $l \times n$ matrix containing the simple roots as row vectors; this matrix is called the *root matrix* of R. Similarly, let B be the $l \times n$ matrix containing the simple coroots in the corresponding order; this matrix is called the *coroot matrix* of R. Then the Cartan matrix C is equal to $AB^\top$ and $\mathbb{Z}\Phi = \mathbb{Z}A$ and $\mathbb{Z}\Phi^\vee = \mathbb{Z}B$. For $\alpha \in \Phi$ we define c^α to be the $\mathbb{Z}$-valued size l row vector satisfying $\alpha = c^\alpha A$.

In the greater part of this thesis we will deal with semisimple root data, so $l = n$. In the case of semisimple root data the definition of the adjoint isogeny type implies that for the adjoint root datum we may take A to be the $n \times n$ identity matrix and B to be $C^\top$. Similarly, for the simply connected root datum we may take $A = C$ and $B = I$.

1.3.2 Root data of rank one

In this section we classify the semisimple root data of rank one. Recall that there is only one root *system* of rank one (up to isomorphism). This root system, whose only roots are α and $-\alpha$, is called A_1.

There are, however, two non-isomorphic semisimple root *data* of rank one: *adjoint* and *simply connected* (denoted ${\mathrm{A}_1}^{\mathrm{ad}}$ and ${\mathrm{A}_1}^{\mathrm{sc}}$, respectively). The difference is clearest exposed if we adopt the computational conventions set out in Section 1.3.1. We fix the root lattice $X = \mathbb{Z}$ and the coroot lattice $Y = \mathbb{Z}$, so that the pairing is simply multiplication: $\langle x, y \rangle = xy$. The Cartan matrix C is equal to $(\langle \alpha, \alpha^\vee \rangle) = (2)$. We should then define an integral 1×1 matrix A containing the roots as row vectors and an integral 1×1 matrix B containing the coroots as row vectors, such that $AB^\top = C$. Now it becomes clear that there are two choices:

- $A = (1), B = (2)$: giving the *adjoint* root datum, and
- $A = (2), B = (1)$: giving the *simply connected* root datum.

These choices are non-isomorphic since the determinants of the root matrices A differ.

	Cartan matrix	Root matrix	Coroot matrix
$A_1{}^{\mathrm{ad}}A_1{}^{\mathrm{ad}}$	$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$
$A_1{}^{\mathrm{ad}}A_1{}^{\mathrm{sc}}$	$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$	$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$
$A_1{}^{\mathrm{sc}}A_1{}^{\mathrm{sc}}$	$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$	$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
$A_2{}^{\mathrm{ad}}$	$\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$
$A_2{}^{\mathrm{sc}}$	$\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$	$\begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
$B_2{}^{\mathrm{ad}}$	$\begin{pmatrix} 2 & -2 \\ -1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 2 & -1 \\ -2 & 2 \end{pmatrix}$
$B_2{}^{\mathrm{sc}}$	$\begin{pmatrix} 2 & -2 \\ -1 & 2 \end{pmatrix}$	$\begin{pmatrix} 2 & -2 \\ -1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
G_2	$\begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$\begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix}$

Table 1.7: Root data of rank two

1.3.3 Root data of rank two

In this section we classify the semisimple root data of rank two. Recall from Section 1.1.2 that there are only 4 root systems of rank two: $\mathrm{A}_1\mathrm{A}_1$, A_2, B_2, and G_2. Recall furthermore from Section 1.1.3 that the fundamental group of A_n is $\mathbb{Z}/(n+1)\mathbb{Z}$, the fundamental group of B_n is $\mathbb{Z}/2\mathbb{Z}$, and the fundamental group of G_2 is trivial. We again adopt the computational conventions from Section 1.3.1 and enumerate the possibilities in Table 1.7. The choices for the root and coroot matrices are unique up to multiplication with elements of $\mathrm{SL}(2,\mathbb{Z})$: if $m \in \mathrm{SL}(2,\mathbb{Z})$ then $AB^\top = (Am)(Bm^{-\top})^\top$, $\det(A) = \det(Am)$, and $\det(B) = \det(Bm)$.

1.4 Lie algebras

In this section we introduce Lie algebras, by giving the relevant definitions and providing some examples.

Definition 1.8 (Lie algebra)**.** A *Lie algebra* L is a vector space V over a field $\mathbb{F}$ equipped with an *alternating bilinear* product

$$[\cdot,\cdot] : L \times L \to L,$$

satisfying the *Jacobi identity*:

$$[x,[y,z]] + [y,[z,x]] + [z,[x,y]] = 0 \text{ for all } x,y,z \in L.$$

Note that it follows from the requirement that $[\cdot,\cdot]$ be alternating and bilinear that $[\cdot,\cdot]$ is *anti-symmetric*. Indeed, for all $x,y \in L$:

$$[x,y] = [x,y] - [x+y,x+y] = [x,y] - ([x,x]+[x,y]+[y,x]+[y,y]) = -[y,x].$$

If $\mathrm{char}(\mathbb{F}) \neq 2$ anti-symmetry of the product actually implies that it is alternating: suppose $[x,y] = -[y,x]$ for all $x,y \in L$ and observe that for every $z \in L$:

$$2[z,z] = [z,z] + [z,z] = [z,z] - [z,z] = 0,$$

so that $[z,z] = 0$.

The *dimension* of a Lie algebra (denoted $\dim(L)$) is simply the dimension $\dim(V)$ of its vector space. Furthermore, V is called the *underlying vector space* of L and the field $\mathbb{F}$ over which V is defined is called the *underlying field* of L.

Before proceeding, we give an elementary example.

Example 1.9. We show that any algebra A becomes a Lie algebra if we take

$$[a,b] := ab - ba.$$

Indeed, A is a vector space. To see that $[\cdot,\cdot]$ is alternating take $a \in A$ and observe:

$$[a,a] = aa - aa = 0.$$

To see that $[\cdot,\cdot]$ is bilinear take $a, b, c \in A$ and $\lambda, \mu \in \mathbb{F}$, where $\mathbb{F}$ is the field underlying A. By anti-symmetry we only need to verify one of the coordinates.

$$\begin{aligned}[\lambda a + \mu b, c] &= (\lambda a + \mu b)c - c(\lambda a + \mu b) \\ &= \lambda(ac - ca) + \mu(bc - cb) \\ &= \lambda[a, c] + \mu[b, c].\end{aligned}$$

To see that the Jacobi identity is satisfied take $a, b, c \in A$ and observe:

$$\begin{aligned}[a,[b,c]] + [b,[c,a]] + [c,[a,b]] &= [a, bc - cb] + [b, ca - ac] + [c, ab - ba] \\ &= (bc - cb)a - (bc - cb)a + b(ca - ac) \\ &\quad - (ca - ac)b + c(ab - ba) - (ab - ba)c \\ &= 0.\end{aligned}$$

For any vector space V we let $\mathfrak{gl}(V)$ be the endomorphisms $\mathrm{End}(V)$ viewed as a Lie algebra, i.e., $[x, y] = xy - yx$. This is called the *general linear algebra* (see also Example 1.16 in Section 1.5.2 and its continuation in Section 1.6.5).

1.4.1 Subalgebras and ideals

If X is a subset of L, its closure under the vector space operations (i.e., addition, subtraction, and multiplication with elements from $\mathbb{F}$) is denoted $\langle X \rangle_{\mathbb{F}}$. The closure of X under the Lie algebra operations (i.e., addition, subtraction, multiplication with elements from $\mathbb{F}$, and the Lie product $[\cdot,\cdot]$) is denoted $\langle X \rangle_L$.

A *subalgebra* of L is a subset X of L that is closed under the Lie algebra operations, i.e., $\langle X \rangle_L = X$. So, if M is a subalgebra of L, then M is a linear subspace of L and we have

$$[x, y] \in M \text{ for all } x, y \in M.$$

An *ideal* I of L is a subalgebra that has the following additional property:

$$[x, y] \in I \text{ for all } x \in I \text{ and all } y \in L.$$

We will denote the intersection of all ideals containing a subset X of V by $(X)_L$. Note that every ideal is a subalgebra, but the converse is not true.

A subalgebra (resp.!an ideal) S is called a *proper* subalgebra (resp. ideal) of L if $S \neq \{0\}$ and $S \neq L$. The *dimension* of a subalgebra (and of an ideal) is simply the dimension of the underlying subspace of L.

Example 1.10. In Example 1.9 we have seen that every matrix algebra gives rise to a Lie algebra. In this example, we take $L = \mathfrak{sl}(3, \mathbb{F})$, the Lie algebra of 3×3 matrices with trace 0 over the field $\mathbb{F}$ with multiplication $[a, b] := ab - ba$.

The dimension of L is clearly 8: We can freely fill all coordinates but $(3, 3)$, and that last one is uniquely determined by the requirement that the trace be 0.

First, we consider the subalgebra $M = \langle a, b\rangle_L$ of L, where

$$a = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad b = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

We claim $\dim(M) = 3$. Indeed:

$$[a, b] = ab - ba = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} - \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

It is straightforward to verify that taking products of elements in M does not yield further elements: $[a, [a, b]] = -2a$ and $[b, [a, b]] = 2b$. (We do not need to check further elements in view of anti-symmetry). So $M = \langle a, b, [a, b]\rangle_{\mathbb{F}}$ and indeed $\dim(M) = 3$.

Next, we consider the ideal $I = (h)_L$ of L, where

$$h = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -2 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

We claim that this is in general not a proper ideal. Assume for a moment that $\mathrm{char}(F) \neq 3$ and consider, as an example,

$$a = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in L$$

and observe that $[h, a] = 3a$ so that $a \in I$. More generally, write E_{kl} for the 3×3 matrix whose only non-zero entry is a 1 on the (k, l)-th coordinate. It is not hard to verify that $[h, E_{12}] = 3E_{12}$, $[h, E_{21}] = -3E_{12}$, $[h, E_{23}] = -3E_{23}$, and $[h, E_{32}] = 3E_{32}$, so that $E_{12}, E_{21}, E_{23}, E_{32} \in I$ (as $\mathrm{char}(F) \neq 3$). Moreover, since $[E_{12}, E_{23}] = E_{13}$ and $[E_{32}, E_{21}] = E_{31}$, we find $E_{13} \in I$ and $E_{31} \in I$. Now observe

$$[E_{12}, E_{21}] = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix},$$

which is a diagonal element that is not a multiple of h. Thus we have found that $\dim(I) \geq 8$, but as I is an ideal of L, we must have $L = I$, and indeed I is not a proper ideal of L.

To finish the example we drop the assumption that $\mathrm{char}(F) \neq 3$ and assume $\mathrm{char}(F) = 3$. Then h is the identity matrix, so that, for every $a \in L$,

$$[h, a] = ha - ah = a - a = 0,$$

so that in fact $I = \langle h \rangle_{\mathbb{F}}$. Thus, in this case, $\dim(I) = 1$ and I is a proper ideal of L.

We end this section with some special subalgebras of a Lie algebra L. If S is a subset of L then the *centralizer of S in L* is

$$\mathrm{C}_L(S) = \{y \in L \mid [x,y] = 0 \text{ for all } x \in S\},$$

and for $x \in L$ we write $\mathrm{C}_L(x)$ instead of $\mathrm{C}_L(\{x\})$. It follows immediately from the Jacobi identity that $\mathrm{C}_L(S)$ is a subalgebra. The *center of L* is defined to be $\mathrm{C}_L(L)$ and denoted $\mathrm{Z}(L)$. Clearly, $\mathrm{Z}(L)$ is an ideal of L. (Note that in the previous example $I \subseteq \mathrm{Z}(L)$ if $\mathrm{char}(\mathbb{F}) = 3$.)

If S is a subalgebra of L then the *normalizer* of S in L is

$$\mathrm{N}_L(S) = \{y \in L \mid [x,y] \in S \text{ for all } x \in S\},$$

and for $x \in L$ we write $\mathrm{N}_L(x)$ instead of $\mathrm{N}_L(\langle x \rangle_L)$. Observe that, if I is an ideal of L, we have $\mathrm{N}_L(I) = L$. More generally, S is an ideal of $\mathrm{N}_L(S)$ for any subalgebra S of L.

If I is an ideal of L then the *quotient algebra L/I* has elements of the form $x + I$ (where $x \in L$) and multiplication is clearly well defined:

$$[x+I, y+I] = [x,y] + [x,I] + [I,y] + [I,I] = [x,y] + I.$$

1.4.2 Algebras defined by structure constants

Lie algebras may be presented in several ways, for example as matrices, or using generators and relations. A *matrix representation* of L is defined to be a homomorphism $\varphi : L \mapsto \mathfrak{gl}(V)$. For instance, every Lie algebra has a representation as $\dim(L) \times \dim(L)$ matrices, called the *adjoint representation* $x \mapsto \mathrm{ad}_x$, where

$$\mathrm{ad}_x : L \to L, y \mapsto [x,y].$$

Note, however, that this representation is not necessarily faithful, since $Z(L)$ is in its kernel.

Particularly suitable for our purposes, namely for working with Lie algebras on a computer, is the representation as an *algebra defined by structure constants*. Earlier work on this subject is due to Willem de Graaf [dG97, dG00], who introduced Lie algebras into the GAP and MAGMA computer algebra systems in this manner. For ease of notation we will assume finite dimensionality throughout this section, but that is not strictly necessary for the construction.

Assume we have a Lie algebra L with underlying vector space $V = \mathbb{F}^n$, and a basis $e_1, \ldots, e_n$ of V. The elements of L are represented as elements of V, and the Lie product $[\cdot,\cdot]$ is stored in a *multiplication table* T: An $n \times n$ table whose entries are $\mathbb{F}$-vectors of length n such that, for $i, j \in \{1, \ldots, n\}$,

$$[e_i, e_j] = \sum_{k=1}^{n} T_{ijk} e_k.$$

Example 1.10 (continued). We consider the 3-dimensional subalgebra M defined in Example 1.10. Observe that $\{a, b, [a, b]\}$ is a basis of M, so that $[\cdot, \cdot]$ on M is completely determined by the following table:

	a	b	$[a,b]$
a	0	$[a,b]$	$-2a$
b	$-[a,b]$	0	$2b$
$[a,b]$	$2a$	$-2b$	0

To see that this small table indeed determines the multiplication on the whole of M suppose we are given any two elements $x, y \in M$. Because $\{a, b, [a, b]\}$ is known to be a basis of M, there exist $x_1, x_2, x_3 \in \mathbb{F}$ and $y_1, y_2, y_3 \in \mathbb{F}$ such that $x = x_1a + x_2b + x_3[a, b]$ and $y = y_1a + y_2b + y_3[a, b]$. Now, by bilinearity of the Lie product,

$$\begin{aligned}[x, y] &= [x_1a + x_2b + x_3[a, b], y_1a + y_2b + y_3[a, b]]\\ &= x_1y_1[a, a] + x_1y_2[a, b] + \cdots + x_3y_3[[a, b], [a, b]],\end{aligned}$$

and these are all products of basis elements, that can be looked up in the multiplication table.

As an algebra defined by structure constants M looks as follows:

$$\begin{array}{ccc} (0\quad 0\quad 0) & (0\quad 0\quad 1) & (-2\quad 0\quad 0)\\ (0\quad 0\quad -1) & (0\quad 0\quad 1) & (0\quad 2\quad 0)\\ (2\quad 0\quad 0) & (0\quad -2\quad 0) & (0\quad 0\quad 0)\end{array}$$

On the other hand, a matrix representation for M is:

$$a = \begin{pmatrix} 0 & 1\\ 0 & 0\end{pmatrix}, b = \begin{pmatrix} 0 & 0\\ 1 & 0\end{pmatrix}, \text{ so that } [a, b] = \begin{pmatrix} 1 & 0\\ 0 & -1\end{pmatrix}.$$

Finally, M may also be represented using generators and relations: Take a and b as generators and require $[a, [a, b]] = -2a$ and $[b, [a, b]] = 2b$.

It is easy to see that the observation from this example easily generalizes, and that, given any two elements $v, w \in L$ as elements of V, we are able to compute $[v, w]$ using the multiplication table T.

In this thesis, almost all Lie algebras that we want to represent on a computer are represented in this fashion. There are several advantages of this approach over storing Lie algebra elements as matrices. The main reason is that many Lie algebras we study do not have a small dimensional matrix representation: the $\mathfrak{sl}$ example we gave being the exception to the rule. So generally storing elements as vectors is much cheaper than storing elements as matrices, as is the multiplication of two elements.

In practice, we try to force many of these structure constants to be zero, as multiplication of elements can be much more efficiently performed in that case. The Chevalley basis (see Section 1.9) in particular has this property.

Observe that in fact every algebra (and not just Lie algebras) can be represented as an algebra defined by structure constants. However, since most algebras we deal with in this thesis are Lie algebras we presented the construction for that class.

1.4.3 The Killing form

An important invariant of Lie algebras is the *Killing form*. Let L be a Lie algebra over an arbitrary field $\mathbb{F}$ and $x \mapsto \mathrm{ad}_x$ its adjoint representation, and define the Killing form κ by

$$\kappa : L \times L \mapsto \mathbb{F} : (x, y) \mapsto \mathrm{Tr}(\mathrm{ad}_x\, \mathrm{ad}_y).$$

This form is easily seen to be symmetric, bilinear, and associative. Its significance is stated in the following theorem.

Theorem 1.11 ([Hum72, Section 5.1])**.** *If the Killing form of L is non-degenerate, then L is semisimple. If* $\mathrm{char}(\mathbb{F}) = 0$ *then the converse also holds: L is semisimple if and only if its Killing form is non-degenerate.*

1.4.4 Restricted Lie algebras

Suppose throughout this section that L is a Lie algebra over a field $\mathbb{F}$ and let p denote the *characteristic exponent of* $\mathbb{F}$, i.e., $p = \mathrm{char}(\mathbb{F})$ if $\mathrm{char}(\mathbb{F}) > 0$, and $p = 1$ if $\mathrm{char}(\mathbb{F}) = 0$. The Lie algebra L is called *restricted* (or a *p-Lie algebra*) if there exists an operation $[p] : L \to L, x \mapsto x^{[p]}$ (called the *p-operation*) such that, for all $x, y \in L$ and all $t \in \mathbb{F}$ (where we write $\mathrm{ad}_x(y) = [x, y]$)

(i) $(tx)^{[p]} = t^p x^{[p]}$,

(ii) $\mathrm{ad}_{x^{[p]}} = (\mathrm{ad}_x)^p$, and

(iii) $(x + y)^{[p]} = x^{[p]} + y^{[p]} + \sum_{i=1}^{p-1} i^{-1} s_i(x, y)$, where $s_i(x, y)$ is the coefficient of t^i in $(\mathrm{ad}_{tx+y})^{p-1}(y)$ (this is called *Jacobson's formula*).

1.5 Algebraic groups

The notion of an algebraic group is a very general one, and a very extensive theory dealing with this concept has developed over the past six decades. This thesis is clearly not the right place to give a comprehensive overview of all the results and properties of these groups, so we will only give the basic definitions and properties. We refer to [Hum75] and [Spr98] for more details. Our main goal here will be to arrive at Theorem 1.42, which states that semisimple algebraic groups are determined, up to isomorphism, by their field of definition and their root datum.

1.5.1 Affine varieties

Throughout this section we let $\mathbb{F}$ be an arbitrary field. By an *affine variety defined over* $\mathbb{F}$ we will mean the set of common zeroes in some vector space over the algebraic closure $\overline{\mathbb{F}}$ of $\mathbb{F}$ of a finite collection of polynomials with coefficients in $\mathbb{F}$. We will denote the variety arising from a set of polynomials X by $\mathcal{V}(X)$.

First, notice that the ideal $(f_1, \ldots, f_k)$ in $\mathbb{F}[\mathbf{x}] = \mathbb{F}[x_1, \ldots, x_n]$ generated by the polynomials $f_1, \ldots, f_k$ has precisely the same common zeroes as the set $\{f_1, \ldots, f_k\}$. Moreover, the Hilbert Basis Theorem [Hum75, Theorem 0.1] asserts that each ideal in $\mathbb{F}[\mathbf{x}]$ has a finite set of generators, so that every ideal corresponds to an affine variety. Unfortunately, though, the correspondence is not one-to-one:

> **Example 1.12.** Let $I_1 = (x)$ be the ideal in $\mathbb{Q}[x]$ generated by $\{x\}$, and $I_2 = (x^2)$. Obviously, I_1 and I_2 have the same set of common zeroes, but the ideals are distinct.

Formally, we can assign to each ideal I in $\mathbb{F}[\mathbf{x}]$ the variety $\mathcal{V}(I)$ of its common zeroes, and to each subset $S \subseteq \mathbb{F}^n$ the collection $\mathcal{I}(S)$ of all polynomials vanishing on S. It is clear that $\mathcal{I}(S)$ is an ideal, and that we have inclusions $S \subseteq \mathcal{V}(\mathcal{I}(S))$ and $I \subseteq \mathcal{I}(\mathcal{V}(I))$. Neither of these needs to be an equality:

> **Example 1.13.** First, consider $S = \mathbb{F}^*$, the set of non-zero elements of $\mathbb{F}$. Then $\mathcal{I}(S) = \{ 0 \}$ so that $\mathcal{V}(\mathcal{I}(S)) = \mathbb{F} \supsetneq S$. (Observe that S is (as a variety) isomorphic to the variety of an ideal in a bivariate polynomial ring: $S \cong \mathcal{V}(\{(x,y) \in \mathbb{F}^2 \mid xy - 1 = 0\})$ by $x \leftrightarrow (x, 1/x)$.)
>
> Second, let $I = (x^2)$. Then $\mathcal{V}(I) = \{0\}$ so that $\mathcal{I}(\mathcal{V}(I)) = (x) \supsetneq I$.

By definition, the *radical* $\sqrt{I}$ of an ideal I is the ideal $\{f \in \mathbb{F}[\mathbf{x}] \mid f^r \in I \text{ for some } r \geq 0\}$. Clearly, $I \subseteq \sqrt{I} \subseteq \mathcal{I}(\mathcal{V}(I))$, refining the above inclusion. For some fields, however, the second inclusion is in fact an equality:

Theorem 1.14 (Hilbert's Nullstellensatz). *If $\mathbb{F}$ is algebraically closed and I is an ideal in $\mathbb{F}[\mathbf{x}]$ then $\sqrt{I} = \mathcal{I}(\mathcal{V}(I))$.*

If V is an affine variety then the polynomial functions of $\mathbb{F}[\mathbf{x}]$ restricted to V form an $\mathbb{F}$-algebra isomorphic to $S/\mathcal{I}(V)$. We denote this algebra by $\mathbb{F}[V]$.

We will finish this section with the definition of *Zariski topology*. Let $V = \overline{\mathbb{F}}^k$ be some vector space over the algebraic closure of the field $\mathbb{F}$. Observe that the function $I \mapsto \mathcal{V}(I)$ sending ideals to varieties has the following properties (cf. [Spr98, Definition 1.1.3]).

(i) $\mathcal{V}(\{0\}) = V$ and $\mathcal{V}(\overline{\mathbb{F}}[x_1, \ldots, x_k]) = \emptyset$.

(ii) If $I \subseteq J$ then $\mathcal{V}(J) \subseteq \mathcal{V}(I)$.

(iii) $\mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J)$.

(iv) If $(I_a)_{a \in A}$ is a family of ideals and $I = \sum_{a \in A} I_a$ is their sum, then $\mathcal{V}(I) = \bigcap_{a \in A} \mathcal{V}(I_a)$.

It follows from these observations that there is a topology on V whose closed sets are the $\mathcal{V}(I)$, for I an ideal of $\overline{\mathbb{F}}[x_1, \ldots, x_k]$. This is called the *Zariski topology on V*, and the induced topology on a subset V' of V is defined to be the Zariski topology of V. A closed set in V is called an *algebraic set*.

A non-empty topological space is called *reducible* if it is the union of two proper closed subsets and *irreducible* otherwise. A topological space is *connected* if it is not the union of two disjoint proper closed subsets. So an irreducible space is connected, but not all connected spaces are irreducible.

1.5.2 A group structure on a variety

Next let X and Y be affine varieties defined over $\mathbb{F}$. By a *morphism* $\varphi : X \to Y$ we mean a mapping of the form $\varphi(\mathbf{x}) = (\varphi_1(\mathbf{x}), \ldots, \varphi_m(\mathbf{x}))$, where $\varphi_i \in \mathbb{F}[\mathbf{x}]$. Now let G be an affine variety endowed with the structure of a group. If the two maps $\mu : G \times G \to G$ (where $\mu(x,y) = xy$) and $\iota : G \to G$ (where $\iota(x) = x^{-1}$) are morphisms of varieties, we call G an *algebraic group*.

Before giving additional examples, we try to clarify some of the subtleties that occur in definitions of algebraic groups. Suppose for a moment that G is an affine variety defined over $\mathbb{F}$ with suitable multiplication and inversion maps, denoted μ and ι, respectively. We may view the algebraic group G as a functor from fields to groups:

$$G : \mathbb{F}' \mapsto \mathbb{F}' \cap G,$$

where $\mathbb{F}'$ is a field containing $\mathbb{F}$. We call this *the $\mathbb{F}'$-rational points of G*, and denote it $G(\mathbb{F}')$. Consequently, $G(\mathbb{F})$ is the smallest group that can be constructed in this manner. An equivalent viewpoint is the following:

$$G : \mathbb{F}' \mapsto \{x \in G \text{ defined over } \overline{\mathbb{F}} \mid x^{\sigma} = x \text{ for all } \sigma \in \mathrm{Gal}(\overline{\mathbb{F}}/\mathbb{F}')\}.$$

Example 1.15. We consider the group $\mathbb{Z}/2\mathbb{Z}$ of order two, and show that it can be viewed as an algebraic group. Take G to be the variety over $\mathbb{Q}$ defined as the zeroes of the polynomial $x(x-1)$, take $\mu : G \times G \to G, (x,y) \mapsto (x-y)^2$ to be the multiplication morphism, and $\iota : G \to G, x \mapsto x$ the inversion morphism.

Indeed, if $x(x-1) = 0$ and $y(y-1) = 0$, then $(x-y)^2((x-y)^2 - 1) = 0$ and μ and ι are polynomial maps, so that μ and ι are morphisms of varieties and G is an algebraic group. To see that $G(\mathbb{F})$, for any $\mathbb{F} \supseteq \mathbb{Q}$, is isomorphic to $\mathbb{Z}/2\mathbb{Z}$, observe that its elements are simply 0 and 1, and that $\iota(0) = 0$, $\iota(1) = 1$, $\mu(0,0) = 0$, $\mu(1,0) = 1$, $\mu(0,1) = 1$, and $\mu(1,1) = 0$.

So G is an algebraic group defined over $\mathbb{Q}$, and $G(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$. In fact, also $G(\overline{\mathbb{Q}}) \cong \mathbb{Z}/2\mathbb{Z}$.

Example 1.16. $\mathrm{GL}(n, \mathbb{F})$, the *general linear group*, is the group of all invertible $n \times n$ matrices over $\mathbb{F}$. We will show that $\mathrm{GL}(n, \cdot) : \mathbb{F} \mapsto \mathrm{GL}(n, \mathbb{F})$ is in fact an algebraic group. Consider the polynomial ring $R = \mathbb{F}[x_{11}, x_{12}, \ldots, x_{nn}, t]$, let X be the matrix whose (i,j)-entry is x_{ij}, and write elements of R as (X, t).

We define the variety V to be the set of zeroes of $t \cdot \det(X) - 1$. The multiplication map $\mu : V \times V \to V$ is obviously defined by $\mu\left((X,t),(Y,u)\right) = (XY, tu)$, and the inversion map $\iota : V \to V$ by $\iota\left((X,t)\right) = (X^{-1}, \frac{1}{t})$. Indeed $tu \det(XY) - 1 = tu \det(X) \det(Y) - 1 = 0$, $\frac{1}{t} \det(X^{-1}) - 1 = \frac{1}{t} \det(X)^{-1} - 1 = 0$, and μ and ι are polynomial maps, so that they are morphisms of varieties and V is an algebraic group.

Example 1.17. The additive group $\mathrm{G}_a : \cdot \mapsto \mathbb{F}$ is the affine line $\mathbb{F}$ with group law $\mu(x,y) = x + y$, so that $\iota(x) = -x$ and $\mathrm{id} = 0$. The multiplicative group $\mathrm{G}_m : \cdot \mapsto \mathbb{F}^*$ is the affine open subset $\mathbb{F}^*$ with group law $\mu(x,y) = xy$, so that $\iota(x) = x^{-1}$ and $\mathrm{id} = 1$. Note that $\mathrm{G}_m = \mathrm{GL}(1, \cdot)$.

We remark that since we assume our varieties to be affine, the resulting algebraic groups are *linear algebraic groups*. The attribution "linear" is justified by the following proposition.

Proposition 1.18 ([Bor91, Proposition 1.10])**.** *Let G be an algebraic group defined over the field $\mathbb{F}$. Then G is $\mathbb{F}$-isomorphic to a closed subgroup of some* $\mathrm{GL}(n, \mathbb{F})$.

The observation that each subgroup of an algebraic group is again an algebraic group easily gives further examples, such as the group of upper triangular matrices or the group of diagonal matrices. Also, the *direct product* of two algebraic groups is again an algebraic group.

Now let X be a set on which G *acts*, i.e., there is a map $\varphi : G \times X \to X$, denoted for brevity by $\varphi(x,y) = x.y$, such that $x_1.(x_2.y) = (x_1x_2).y$ for $x_1, x_2 \in G$ and $y \in X$, and $\mathrm{id}.y = y$, for all $y \in Y$, where id is the identity of G. We denote by X^G the set of *fixed points*:

$$X^G := \{x \in X \mid g.x = x \text{ for all } g \in G\}.$$

Clearly, G acts on itself by sending y to $\mathrm{Int}_x(y) := x^{-1}yx$, also called the action by *inner automorphisms*.

The *stabilizer* of $y \in X$ is

$$G_y := \{g \in G \mid g.y = y\}.$$

Another useful notion is the *transporter*: let Y and Z be subsets of X. Then we define the transporter to be

$$\mathrm{Tran}_G(Y, Z) := \{g \in G \mid g.Y \subseteq Z\}.$$

The *centralizer* of a subset Y of X is defined to be

$$\mathrm{C}_G(Y) := \{g \in G \mid g.y = y \text{ for all } y \in Y\},$$

so that $\mathrm{C}_G(Y) = \bigcap_{y \in Y} G_y$ and the centralizer of a subgroup H of G (where G acts on H by inner automorphisms) is

$$\mathrm{C}_G(H) := \{g \in G \mid g^{-1}hg = h \text{ for all } h \in H\}.$$

The *normalizer* of a subgroup H of G is

$$\mathrm{N}_G(H) := \{g \in G \mid g^{-1}hg \in H \text{ for all } h \in H\}.$$

We give a few properties of the transporter, centralizer, and normalizer in the following lemma.

Lemma 1.19 ([Hum75, Section 8.2])**.** *Let the algebraic group G act on the variety X and let Y, Z be subsets of X, with Z closed. Let H be a subgroup of G.*

(i) $\mathrm{Tran}_G(Y, Z)$ *is a closed subset of G.*

(ii) For each $y \in X$, the stabilizer G_y is a closed subgroup of G.

(iii) The fixed point set of $x \in G$ is closed in X; in particular X^G is closed.

(iv) The centralizer $\mathrm{C}_G(H)$ *and the normalizer* $\mathrm{N}_G(H)$ *are closed subgroups.*

1.5.3 Reductive algebraic groups

Clearly, $\mathrm{C}_G(H)$ is an algebraic group, since it is given by equations. Furthermore, $\mathrm{N}_G(H)$ is an algebraic group because closed subgroups are algebraic. A subgroup is called *solvable* if the *derived series* terminates in the identity id. This series is defined inductively by $\mathcal{D}^0G = G$, $\mathcal{D}^{i+1}G = (\mathcal{D}^iG, \mathcal{D}^iG)$.

Before giving the four classical examples we introduce the key notions of semisimple and reductive group. By Proposition 1.18 we may view algebraic groups as groups of matrices. An element $x \in G$ is called *semisimple* if the roots of its minimal polynomial are all distinct (this is equivalent to x being diagonalizable). An element $x \in G$ is called *unipotent* if its sole eigenvalue is 1.

It follows from the observation that if A and B are normal solvable subgroups then AB is, that every algebraic group G possesses a unique largest normal solvable subgroup, which is automatically closed. Its identity component (more precisely: the unique connected component containing the identity) G° is then the largest connected normal solvable subgroup of G, and it is called the *radical* of G and denoted $\mathrm{Rad}(G)$. The subgroup of $\mathrm{Rad}(G)$ consisting of its unipotent elements is normal in G and called the *unipotent radical* of G and denoted $\mathrm{Rad}_u(G)$. It is the largest connected normal unipotent subgroup of G.

If G is connected, $G \neq \mathrm{id}$, and $\mathrm{Rad}(G)$ is trivial, we call G *semisimple*. If G is connected, $G \neq \mathrm{id}$, and $\mathrm{Rad}_u(G)$ is trivial, we call G *reductive*. Starting with an arbitrary connected algebraic group G, we get a semisimple group $G/\mathrm{Rad}(G)$ and a reductive group $G/\mathrm{Rad}_u(G)$, unless of course $G = \mathrm{Rad}(G)$ or $G = \mathrm{Rad}_u(G)$.

Because of these observations, the study of algebraic groups reduces to some extent to the study of the reductive group $G/\mathrm{Rad}_u(G)$. Techniques for computing in unipotent groups, and applications thereof in computing in reductive algebraic groups, are described in [CHM08].

1.5.4 Classical examples

We finish this section with four examples: the *classical groups*. In each case the parameter n is the dimension of the subgroup of diagonal matrices in the group under discussion.

Example 1.20. $\mathrm{A}_n{}^{\mathrm{sc}}(\mathbb{F})$ for any field $\mathbb{F}$ is the *special linear group* $\mathrm{SL}(n+1,\mathbb{F})$ consisting of the matrices of determinant 1 in $\mathrm{GL}(n+1,\mathbb{F})$. It is clearly a closed subgroup of $\mathrm{GL}(n+1,\mathbb{F})$, and since it is defined by a single polynomial it is a hypersurface in $\mathrm{M}(n+1,\mathbb{F})$, so its dimension is $(n+1)^2-1$.

Example 1.21. $\mathrm{C}_n{}^{\mathrm{sc}}(\mathbb{F})$ for any field $\mathbb{F}$ is the *symplectic group* $\mathrm{Sp}(2n,\mathbb{F})$, consisting of all $x \in \mathrm{GL}(2n,\mathbb{F})$ satisfying

$$x^T s x = s, \text{ where } s = \begin{pmatrix} 0 & J \\ -J & 0 \end{pmatrix}, \text{ where } J = \begin{pmatrix} & & 1 \\ & \iddots & \\ 1 & & \end{pmatrix}.$$

It is easily checked that it is a closed subgroup of $\mathrm{GL}(2n,\mathbb{F})$, but the dimension is not as easy to compute as in the previous case.

Example 1.22. $\mathrm{B}_n{}^{\mathrm{sc}}(\mathbb{F})$ is the *special orthogonal group* $\mathrm{SO}(2n+1,\mathbb{F})$. If $\mathrm{char}(\mathbb{F})$ is distinct from 2 it is defined to be all $x \in \mathrm{SL}(2n+1,\mathbb{F})$ satisfying

$$x^T s x = s, \text{ where } s = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & J \\ 0 & J & 0 \end{pmatrix},$$

and J as in Example 1.21. Again, it is easily checked that is is a closed subgroup of $\mathrm{SL}(2n+1,\mathbb{F})$.

Example 1.23. $\mathrm{D}_n^{(n)}(\mathbb{F})$ is another special orthogonal group, $\mathrm{SO}(2n,\mathbb{F})$. If $\mathrm{char}(\mathbb{F})$ is distinct from 2 it is defined to be all $x \in \mathrm{SL}(2n,\mathbb{F})$ satisfying

$$x^T s x = s, \text{ where } s = \begin{pmatrix} 0 & J \\ J & 0 \end{pmatrix}.$$

Again, it is easily checked that it is a closed subgroup of $\mathrm{SL}(2n,\mathbb{F})$.

Example 1.24. Over fields $\mathbb{F}$ of characteristic 2, the groups $\mathrm{SO}(n,\mathbb{F})$ (and by that B_n and D_n) are defined in a rather different manner.

First, note that if $\mathbb{F}$ is a field of characteristic different from 2 and $B(x,y)$ is a symmetric scalar product on a vector space V over $\mathbb{F}$, the corresponding quadratic form f is defined by $f(x) = B(x,x)$, and therefore satisfies

$$f(\lambda x + \mu y) = \lambda^2 f(x) + \mu^2 f(y) + 2\lambda\mu B(x,y),$$

for all $\lambda, \mu \in \mathbb{F}$. A quadratic form on a vector space V over $\mathbb{F}$ is defined to be a function $f : \mathbb{F} \to \mathbb{F}$ satisfying the condition

$$f(\lambda x + \mu y) = \lambda^2 f(x) + \mu^2 f(y) + 2\lambda\mu B(x, y),$$

for all $\lambda, \mu \in \mathbb{F}$, where $B(x, y)$ is some symmetric bilinear scalar product on V.

Now let $\mathbb{F}$ be a field of characteristic 2 for the remainder of this example. In particular, putting $\mu = 0$ we have $f(\lambda x) = \lambda^2 f(x)$ and putting $\lambda = \mu = 1$ we find $B(x, x) = 0$ and $B(x, y) = B(y, x)$. Thus $B(x, y)$ may be regarded as a symplectic scalar product on V. By a suitable choice of basis for V it can be represented by a matrix of the form

$$\begin{pmatrix}
0 & 1 & & & & & & & & & \\
1 & 0 & & & & & & & & & \\
 & & 0 & 1 & & & & & 0 & & \\
 & & 1 & 0 & & & & & & & \\
 & & & & \ddots & & & & & & \\
 & & & & & 0 & 1 & & & & \\
 & & & & & 1 & 0 & & & & \\
 & & & & & & & 0 & & & \\
 & & & & 0 & & & & 0 & & \\
 & & & & & & & & & \ddots & \\
 & & & & & & & & & & 0
\end{pmatrix}.$$

Let n be the dimension of V and $2l$ the rank of the above matrix. Let V_0 be the set $\{x \in V \mid B(x, y) = 0 \text{ for all } y \in V\}$, so that V_0 is a subspace of V of dimension $d = n - 2l$. On this subspace V_0 the quadratic form f clearly satisfies

$$f(\lambda x + \mu y) = \lambda^2 f(x) + \mu^2 f(y)$$

for all $\lambda, \mu \in \mathbb{F}$, and f is said to be *non-degenerate* if no non-zero vector $x \in V_0$ satisfies $f(x) = 0$.

The non-singular linear transformations T of V which satisfy the condition $f(Tx) = f(x)$ form the *orthogonal group* $\mathrm{O}(n, \mathbb{F}, f)$. Since $B(x, y) = f(x + y) + f(x) + f(y)$ it is clear that $B(Tx, Ty) = B(x, y)$, so that each element of $\mathrm{O}(n, \mathbb{F}, f)$ is an isometry of the scalar product $B(x, y)$.

The *special orthogonal group* $\mathrm{SO}(n, \mathbb{F}, f)$ now consists of the transformations in $\mathrm{O}(n, \mathbb{F}, f)$ whose determinant is 1.

When we allow algebraic groups over fields that are not algebraically closed, interesting things occur.

Example 1.25. We consider $V = \{(x, y) \in \mathbb{C}^2 \mid xy = 1\}$ and show that it produces two distinct varieties over $\mathbb{R}^2$. Note that the Galois group $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ consists of two elements: the identity and complex conjugation $\tau : z \mapsto \bar{z}$.

Now first consider the points of V fixed under $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$, i.e., those fixed under τ. This is the set $(a+bi, c+di) \in V$ for which $(a+bi, c+di) = (a-bi, c-di)$, i.e., $V_\tau = \{(a,c) \in \mathbb{R}^2 \mid ac = 1\}$.

On the other hand, $\delta : \mathbb{C}^2 \to \mathbb{C}^2$, $(x,y) \mapsto (y,x)$ is clearly an automorphism of $\mathbb{C}^2$, so to obtain a real variety from V we could just as well take the points of V fixed under the composition $\tau\delta$. This is the set $(a+bi, c+di) \in V$ for which $(a+bi, c+di) = (c-di, a-bi)$, which straightforwardly reduces to the variety $V_{\tau\delta} = \{(a,b) \in \mathbb{R}^2 \mid a^2+b^2 = 1\}$.

Clearly, V_τ and $V_{\tau\delta}$ are nonisomorphic varieties in $\mathbb{R}^2$, even though they arise from the same variety in $\mathbb{C}^2$. In particular, V has the structure of $\mathbb{C}^*$, V_τ has the structure of $\mathbb{R}^*$, and $V_{\tau\delta}$ has the structure of $U_1(\mathbb{C})$, the complex unitary group of rank 1.

1.6 The Lie algebra of an algebraic group

For the definition of the Lie algebra of an algebraic group we follow Springer's approach [Spr98, Chapter 4]. We first introduce the concept of derivations (Section 1.6.1), and then we define tangent spaces, both heuristically and formally (Section 1.6.2). After introducing the module of differentials (Section 1.6.3) we introduce the Lie algebra $\mathrm{Lie}(G)$ of an algebraic group G defined over $\mathbb{F}$ as the derivations on $\mathbb{F}[G]$ that commute with all left translations (Section 1.6.4). The most important proposition in this section is Proposition 1.32, where $\mathrm{Lie}(G)$ is identified with the tangent space of G at the identity. Finally, in Section 1.6.5 we provide some examples where we explicitly compute the Lie algebra of a number of algebraic groups.

1.6.1 Derivations

Let R be a commutative ring, A an R-algebra, and M a left A-module. An *R-derivation of A in M* is an R-linear map $D : A \to M$ such that, for $a, b \in A$, we have

$$D(ab) = a.D(b) + b.D(a).$$

It is immediate that $D(r.1) = 0$ for all $r \in A$. The set $\mathrm{Der}_R(A, M)$ of such derivations is a left A-module, where the module structure is given by $(D+E)a = Da + Ea$ and $(b.D)a = b.D(a)$, for $D, E \in \mathrm{Der}_R(A, M)$ and $a, b \in A$.

The elements of $\mathrm{Der}_R(A, A)$ are the derivations of A. If B is another R-algebra, N is a left B-module, and $\varphi : A \to B$ is a homomorphism of R-algebras then N is an A-module in the following way. If $D \in \mathrm{Der}_R(B, N)$ then $D \circ \varphi$ is a derivation of A in N and the map $D \mapsto D \circ \varphi$ defines a homomorphism of A-modules $\varphi_0 : \mathrm{Der}_R(B, N) \to \mathrm{Der}_R(A, N)$ whose kernel is $\mathrm{Der}_A(B, N)$.

1.6.2 Tangent spaces

We first give a heuristic introduction to the concept of tangent spaces, and we give a formal definition at the end of this section.

Let X be a closed subvariety of the affine variety $\mathbb{F}^n$, where $\mathbb{F}$ is an algebraically closed field. Let I be the ideal of polynomial functions vanishing on X, and let $f_1, \ldots, f_k$ be generators of I. We identify the algebra of regular functions $\mathbb{F}[X]$ with $\mathbb{F}[\mathbf{x}] = \mathbb{F}[x_1, \ldots, x_n]/I$.

Now let $x \in X$ and let L be a line in $\mathbb{F}^n$ through x, so that the points on L can be written as $x + tv$, where $v = (v_1, \ldots, v_n)$ is a direction vector and t runs through $\mathbb{F}$. The t-values of the points on L that lie in X are found by solving

$$f_i(x + tv) = 0 \text{ for all } i = 1, \ldots, k. \tag{1.26}$$

Clearly, $t = 0$ is a solution, but there may be more.

Let D_j be partial derivation in $\mathbb{F}[\mathbf{x}]$ with respect to x_j, so that

$$f_i(x + tv) = t \sum_{j=1}^{n} v_j (D_j f_i)(x) + t^2(\ldots). \tag{1.27}$$

Then $t = 0$ is a multiple root of the set of equations (1.26) if and only if

$$\sum_{j=1}^{n} (D_j f_i)(x) = 0 \text{ for all } i = 1, \ldots, k. \tag{1.28}$$

If this is the case, we call L a *tangent line* and v a *tangent vector of X in x*.

We define $D' = \sum_{j=1}^{n} v_j D_j$, so that D' is an $\mathbb{F}$-derivation of $\mathbb{F}[\mathbf{x}]$, and (1.28) is equivalent to $D' f_i(x) = 0$ for all $i = 1, \ldots, k$. We let M_x be the maximal ideal in $\mathbb{F}[\mathbf{x}]$ of functions vanishing at x, and it follows that $D'I \subseteq M_x$ (recall that I is the ideal of polynomial functions vanishing on X).

The linear map $f \mapsto (D'f)(x)$ gives a linear map $D : \mathbb{F}[X] \to \mathbb{F} = \mathbb{F}[X]/M_x$. We view $\mathbb{F}$ as an $\mathbb{F}[X]$-module (called $\mathbb{F}_x$) via the homomorphism $f \mapsto f(x)$, and note that D is an $\mathbb{F}$-derivation of $\mathbb{F}[X]$ in $\mathbb{F}_x$. Conversely, any element of $\mathrm{Der}_{\mathbb{F}}(\mathbb{F}[X], \mathbb{F}_x)$ can be obtained in this manner from a derivation D' of $\mathbb{F}[\mathbf{x}]$ satisfying $D'I \subseteq M_x$. Hence there is a bijection of the set of tangent vectors v such that (1.28) has a multiple root $t = 0$, onto $\mathrm{Der}_{\mathbb{F}}(\mathbb{F}[X], \mathbb{F}_x)$.

We will now formalize the above intuition. Let X be an affine variety, let $x \in X$, and define the *tangent space of X at x* (denoted $T_x X$) to be the $\mathbb{F}$-vector space $\mathrm{Der}_{\mathbb{F}}(\mathbb{F}[X], \mathbb{F}_x)$, where $\mathbb{F}_x$ is as above.

Let $\varphi : X \to Y$ be a morphism of varieties with corresponding algebra homomorphism $\varphi^* : \mathbb{F}[Y] \mapsto \mathbb{F}[X]$. The induced linear map φ_0^* is a linear map of tangent spaces

$$d\varphi_x : T_x X \to T_{\varphi x} Y,$$

called the *differential of φ at x* or the *tangent map at x*.

We give two alternative descriptions of the tangent space $T_x X$. Firstly, let $M_x \subseteq \mathbb{F}[X]$ be the maximal ideal of functions vanishing in x. If $D \in T_x X$ then D maps the elements of M_x^2 to 0, so D defines a linear function $\lambda(D) : M_x/M_x^2 \to \mathbb{F}$. It turns out that λ is an isomorphism of $T_x X$ onto the dual of M_x/M_x^2 (cf. [Spr98, Lemma 4.1.4]).

For the second description of the tangent space let $\mathcal{O}_x$ be the ring of functions regular in x (i.e., functions defined and regular in some open neighborhood of x). It is an $\mathbb{F}$-algebra with a unique maximal ideal $\mathcal{M}_x$, which consists of the functions vanishing in x, and we have that $\mathcal{O}_x/\mathcal{M}_x \cong \mathbb{F}$. Consequently, we may view $\mathbb{F}$ as an $\mathcal{O}_x$-module and we have an algebra homomorphism $\alpha : \mathbb{F}[X] \to \mathcal{O}_x$, inducing a linear map $\alpha_0 : \mathrm{Der}_{\mathbb{F}}(\mathcal{O}_x, \mathbb{F}) \to \mathrm{Der}_{\mathbb{F}}(\mathbb{F}[X], \mathbb{F}_x)$. It turns out that the map α_0 is bijective (cf. [Spr98, Lemma 4.1.5]).

1.6.3 The module of differentials

In this section we introduce a number of results on derivations that we will need later on. Let R be a commutative ring and A a commutative R-algebra, denote by $\mu : A \otimes_R A \to A$ the product morphism, and let $I = \mathrm{Ker}(\mu)$. This ideal I of $A \otimes A$ is generated by the elements $a \otimes 1 - 1 \otimes a$, for $a \in A$. The quotient algebra $(A \otimes A)/I$ is isomorphic to A.

The *module of differentials* $\Omega_{A/R}$ of the R-algebra A is defined by $\Omega_{A/R} = I/I^2$. This is an $(A \otimes A)$-module, but since it is annihilated by I and $(A \otimes A)/I \cong A$, we may view it as an A-module.

By $d_{A/R}a$ (or da if no confusion is imminent) we denote the image of $a \otimes 1 - 1 \otimes a$ in $\Omega_{A/R}$. The map d is an R-derivation of A in $\Omega_{A/R}$ and the da ($a \in A$) generate the A-module $\Omega_{A/R}$. The following theorem shows the connection between $\Omega_{A/R}$ and derivations of A.

Theorem 1.29 ([Spr98, Theorem 4.2.2(i)]). *For every A-module M the map Φ from* $\mathrm{Hom}_A(\Omega_{A/R}, M)$ *into* $\mathrm{Der}_R(A, M)$ *defined by $\varphi \mapsto \varphi \circ d$ is an isomorphism of A-modules.*

1.6.4 Derivations in algebraic groups

For the remainder of this section we let G be a linear algebraic group defined over $\mathbb{F}$. We denote by λ and ρ the representation of G in $\mathbb{F}[G]$ by left and right translations:

$$\lambda : G \to \mathbb{F}[G], \ (\lambda_g f)(x) = f(g^{-1}x),$$
$$\rho : G \to \mathbb{F}[G], \ (\rho_g f)(x) = f(xg),$$

where $g, x \in G$ and $f \in \mathbb{F}[G]$.

We view $\mathbb{F}[G] \otimes_{\mathbb{F}} \mathbb{F}[G]$ as the algebra of regular functions $\mathbb{F}[G \times G]$ and let $\mu : \mathbb{F}[G] \otimes \mathbb{F}[G] \to \mathbb{F}[G]$ be the multiplication map in $\mathbb{F}[G]$. Then, for $f \in \mathbb{F}[G \times G]$ we have $(\mu f)(x) = f(x, x)$. The ideal $I = \mathrm{Ker}(\mu)$ is the ideal of functions vanishing on the diagonal. Clearly, for $g \in G$, the automorphisms $\lambda_g \times \lambda_g$ and $\rho_g \times \rho_g$ stabilize I and I^2, so they induce automorphisms of $\Omega_G = I/I^2$. We will denote these automorphisms also by λ_g and ρ_g. We thus have representations λ and ρ of G in Ω_G, and the derivation $d : \mathbb{F}[G] \to \Omega_G$ (as defined in the previous section) commutes with all λ_g and ρ_g.

Recall the inner automorphism Int of G from Section 1.5.2 defined by $\mathrm{Int}_x(y) = xyx^{-1}$. It induces linear automorphisms $\mathrm{Ad}\, x$ of the tangent space $T_{\mathrm{id}}G$ of G at the identity id, and $(\mathrm{Ad}\, x)^*$ of the cotangent space $(T_{\mathrm{id}}G)^*$. Thus, for $u \in (T_{\mathrm{id}}G)^*$,

$x \in G$, and $X \in (T_{\mathrm{id}}G)^*$ we have

$$((\mathrm{Ad}\,x)^* u)X = u(\mathrm{Ad}(x^{-1})X).$$

Now let M_{id} be the maximal ideal of $\mathbb{F}[G]$ of functions vanishing at id. As in Section 1.6.2 the cotangent space $(T_{\mathrm{id}}G)^*$ can be identified with $M_{\mathrm{id}}/M_{\mathrm{id}}^2$, and for $f \in \mathbb{F}[G]$ we denote the element $f - f(\mathrm{id}) + M_{\mathrm{id}}^2$ of $(T_{\mathrm{id}}G)^*$ by δf. It satisfies $(\delta f)(X) = Xf$, for $X \in T_{\mathrm{id}}G = \mathrm{Der}_{\mathbb{F}}(\mathbb{F}[G], \mathbb{F}_{\mathrm{id}})$.

The relation between Ω_G and $(T_{\mathrm{id}}G)^*$ becomes apparent in the following proposition.

Proposition 1.30 ([Spr98, Proposition 4.4.2])**.** *There is an isomorphism of $\mathbb{F}[G]$-modules*

$$\Phi : \Omega_G \to \mathbb{F}[G] \otimes_{\mathbb{F}} (T_{\mathrm{id}}G)^*,$$

the module structure on the right hand side being given by the first factor, satisfying

(i) For $g \in G$ we have $\Phi \circ \lambda_g \circ \Phi^{-1} = \lambda_g \otimes \mathrm{id}$, and $\Phi \circ \rho_g \circ \Phi^{-1} = \rho_g \otimes (\mathrm{Ad}\,g)^*$.

(ii) For $f \in \mathbb{F}[G]$ and $\Delta f = \sum_i f_i \otimes g_i$ we have $\Phi(df) = -\sum_i f_i \otimes \delta g_i$ (where Δ is the comultiplication, i.e., $(\Delta f)(x, y) = f(xy)$.)

The space $\mathcal{D}_G = \mathrm{Der}_{\mathbb{F}}(\mathbb{F}[G], \mathbb{F}[G])$ has a Lie algebra structure given by $[D, E] = D \circ E - E \circ D$. Recall the automorphisms λ and ρ of G and define representations of G in $\mathcal{D}_G$ (denoted by the same symbols) by

$$\lambda_g D = \lambda_g \circ D \circ \lambda_g{}^{-1}, \quad \rho_g D = \rho_g \circ D \circ \rho_g{}^{-1},$$

for $g \in G$ and $D \in \mathcal{D}_G$. The *Lie algebra of G* (denoted $\mathrm{Lie}(G)$) is defined to be the set of $D \in \mathcal{D}_G$ commuting with all λ_g (for $g \in G$). Since left and right translations commute, all ρ_g stabilize $\mathrm{Lie}(G)$ and we denote the induced linear maps also by ρ_g.

Recall from Section 1.4.4 that a Lie algebra is called restricted if there exists an operation $[p] : L \to L$ with certain properties. It is straightforward to verify (see also [Spr98, Section 4.4.3]) that $\mathrm{Lie}(G)$ is restricted with p-operation $D^{[p]} = D^p$, since we have for all $D \in \mathrm{Lie}(G)$ and all $x, y \in \mathbb{F}[G]$:

$$D^p(ab) = \sum_{i=0}^{p} \binom{p}{i} (D^i x)(D^{p-i} y) = x(D^p y) + (D^p x)y,$$

so that $D^p \in \mathrm{Lie}(G)$.

We have a result on $\mathcal{D}_G$ similar to Proposition 1.30.

Proposition 1.31 ([Spr98, Corollary 4.4.4])**.** *There is an isomorphism of $\mathbb{F}[G]$-modules*

$$\Psi : \mathcal{D}_G \to \mathbb{F}[G] \otimes_{\mathbb{F}} T_{\mathrm{id}}G,$$

the module structure on the right hand side again being given by the first factor, satisfying

(i) For $g \in G$ we have $\Psi \circ \lambda_g \circ \Psi^{-1} = \lambda_g \otimes \mathrm{id}$ and $\Psi \circ \rho_g \circ \Psi^{-1} = \rho_g \otimes \mathrm{Ad}\,g$.

(ii) For $X \in T_{\mathrm{id}}G$ and $f \in \mathbb{F}[G]$ with $\Delta f = \sum_i f_i \otimes g_i$ we have $\Psi^{-1}(1 \otimes X)(f) = -\sum_i f_i(Xg_i)$.

Finally, we arrive at the equivalence of $\mathrm{Lie}(G)$ and $T_{\mathrm{id}}G$.

Proposition 1.32 ([Spr98, Proposition 4.4.5])**.** *Let $\alpha_G : \mathcal{D}_G \to T_{\mathrm{id}}G$ be the linear map $(\alpha_G D)f = (Df)(\mathrm{id})$.*

(i) α induces an isomorphism of vector spaces $\mathrm{Lie}(G) \cong T_{\mathrm{id}}G$.

(ii) We have, for $g \in G$, that $\alpha \circ \rho_g \circ \alpha^{-1} = \mathrm{Ad}\, g$.

(iii) Ad is a rational representation of G in $T_{\mathrm{id}}G$ (called the adjoint representation*).*

1.6.5 Examples

In this section we give some elementary examples, using the *ε-trick*: the elements of the tangent space $T_{\mathrm{id}}G$ (and therefore those of the Lie algebra $\mathrm{Lie}(G)$) are those x such that for all ε with $\varepsilon^2 = 0$ we have $\mathrm{id} + \varepsilon x \in G$.

Example 1.15 (continued). We compute the Lie algebra of the algebraic group G isomorphic to $\mathbb{Z}/2\mathbb{Z}$:

$$\begin{aligned} 1 + \varepsilon x \in G &\Leftrightarrow (1+\varepsilon x)(1+\varepsilon x - 1) = 0 \\ &\Leftrightarrow (1+\varepsilon x)\varepsilon x = 0 \\ &\Leftrightarrow \varepsilon x = 0 \\ &\Leftrightarrow x = 0, \end{aligned}$$

showing that $\mathrm{Lie}(G)$ is trivial.

Example 1.16 (continued). Similarly, we compute the Lie algebra of the algebraic group $G = \mathrm{GL}(n, \mathbb{F})$. Recall that the elements of G are pairs (X, t), with X an $n \times n$ matrix over $\mathbb{F}$ and $t \in \mathbb{F}$ such that $t \det(X) = 1$. It is clear that the identity id of G is $(I, 1)$, where I is the $n \times n$ identity matrix. So $\mathrm{Lie}(G)$ are those (X, t) such that for all ε with $\varepsilon^2 = 0$ we have $\mathrm{id} + \varepsilon(X, t) \in G$:

$$\begin{aligned} (I,1) + \varepsilon(X,t) \in G &\Leftrightarrow (I + \varepsilon X, 1 + \varepsilon t) \in G \\ &\Leftrightarrow (1+\varepsilon t)\det(I + \varepsilon X) = 1 \\ &\Leftrightarrow (1+\varepsilon t)(1 + \varepsilon\,\mathrm{Tr}(X)) = 1 \\ &\Leftrightarrow 1 + \varepsilon(t + \mathrm{Tr}(X)) = 1 \\ &\Leftrightarrow t = -\mathrm{Tr}(X). \end{aligned}$$

But this means that $\mathrm{Lie}(G) = \mathfrak{gl}(n, \mathbb{F})$ consists of all $n \times n$ matrices over $\mathbb{F}$.

Example 1.20 (continued). As a final example, we compute the Lie algebra of the algebraic group $G = \mathrm{A}_{n-1}{}^{\mathrm{sc}}(\mathbb{F}) = \mathrm{SL}(n, \mathbb{F})$. Recall that the elements of G are

$n \times n$ matrices X for which $\det(X) = 1$. Now we have

$$\begin{aligned} I + \varepsilon X \in G &\Leftrightarrow \det(I + \varepsilon X) = 1 \\ &\Leftrightarrow 1 + \varepsilon \operatorname{Tr}(X) = 1 \\ &\Leftrightarrow \operatorname{Tr}(X) = 0, \end{aligned}$$

so that $\operatorname{Lie}(G) = \mathfrak{sl}(n, \mathbb{F})$ consists of all $n \times n$ matrices over $\mathbb{F}$ whose trace is 0.

1.7 Tori and toral subalgebras

An algebraic group G defined over an arbitrary field $\mathbb{F}$ is called *diagonalizable* if it is isomorphic to a subgroup of the *diagonal group* $\mathrm{D}(n, \mathbb{F})$ of diagonal $n \times n$ matrices over $\mathbb{F}$. In this case G is obviously commutative and consists of semisimple elements. A diagonalizable group T defined over the field $\mathbb{F}$ is also called an $\mathbb{F}$-*torus*, or simply a *torus*.

A *linear character* is by definition any morphism of algebraic groups $\chi : G \to \mathrm{G}_m$. If χ, ψ are linear characters of G then clearly $\chi + \psi$ is if we define $(\chi + \psi)(g) = \chi(g)\psi(g)$. In this manner we obtain an abelian group called the *character group* of G, denoted $\mathrm{X}(G)$.

Let T be a torus of G defined over $\mathbb{F}$ and let $\mathrm{X}(T)$ be its character group, and $\mathrm{X}(T)_{\mathbb{F}}$ the subgroup of the additive group $\mathrm{X}(T)$ consisting of the characters that are $\mathbb{F}$-morphisms. We call T *split over* $\mathbb{F}$ (or $\mathbb{F}$-*split*) if $\mathrm{X}(T)_{\mathbb{F}}$ spans $\mathbb{F}[T]$. Equivalently, T is $\mathbb{F}$-isomorphic to $\dim(T)$ copies of the multiplicative group, i.e., $T(\mathbb{F}) \cong \mathbb{F}^* \times \cdots \times \mathbb{F}^*$. At the other extreme, T is called $\mathbb{F}$-*anisotropic* if $\mathrm{X}(T)_{\mathbb{F}} = 0$.

Example 1.33. Consider the algebraic group $T : \mathbb{F} \mapsto \{(x, y) \in \mathbb{F}^2 \mid x^2 + y^2 = 1\}$ defined over $\mathbb{Z}$. For multiplication and inversion we define $\mu((x_1, y_1), (x_2, y_2))$ to be $(x_1x_2 - y_1y_2, x_1y_2 + y_1x_2)$ and $\iota((x, y)) = (x, -y)$, respectively (think of (x, y) as the complex number $x + iy$). We let $R = \mathbb{Z}[T] = \mathbb{Z}[x, y]/(x^2 + y^2 - 1)$.

Furthermore, let $T' : \mathbb{F} \mapsto \{(u, v) \in \mathbb{F}^2 \mid xy = 1\}$, also defined over $\mathbb{Z}$, with pairwise multiplication and $\iota((u, v)) = (v, u)$ as inversion. We let $R' = \mathbb{Z}[T'] = \mathbb{Z}[u, v]/(uv - 1)$.

First, we investigate what $\mathbb{C}$-morphisms exist from T to T'. Such morphisms $T \to T'$ correspond to homomorphisms $R' \otimes \mathbb{C} \to R \otimes \mathbb{C}$ of $\mathbb{C}$-algebras, and since invertible elements should be mapped to invertible elements, we consider invertible elements of $R \otimes \mathbb{C}$ (those of $R' \otimes \mathbb{C}$ are easily seen to be cu^av^b, for $c \in \mathbb{C}$ and $a, b \in \mathbb{N}$). The invertible elements of $R \otimes \mathbb{C}$ are $c(x + iy)^a$, for $c \in \mathbb{C}^*$ and $a \in \mathbb{Z}$, where we interpret $(x + iy)^a$ as $(x - iy)^{-a}$ if $a < 0$. Consequently, homomorphisms from $R' \otimes \mathbb{C}$ to $R \otimes \mathbb{C}$ are of the form $u \mapsto c(x + iy)^a$ and $v \mapsto \frac{1}{c}(x - iy)^a$.

Since $T' \cong \mathrm{G}_m$ and $X(T)$ consists by definition of the $\mathbb{C}$-homomorphisms from T to G_m, the characters of T are of the form $\chi_a : (x, y) \mapsto (x + iy)^a$, for $a \in \mathbb{Z}$. This means $X(T)_{\mathbb{C}} \cong \mathbb{Z}$, and $X(T)_{\mathbb{Z}}$ spans $\mathbb{C}[T]$, so that T is $\mathbb{C}$-split. Observe that indeed $T(\mathbb{C}) \cong \mathbb{C}^*$.

It is, however, easy to see that the only invertible elements of $R \otimes \mathbb{Q}$ are 1 and -1, which by the same reasoning as above leads to the observation that $X(T)_{\mathbb{Q}} = \{1\}$. Consequently, T is not $\mathbb{Q}$-split.

The example demonstrates that there is a notion dual to character: any morphism of algebraic groups $\varphi : \mathrm{G}_m \to G$ is called a *one parameter multiplicative subgroup* of G. The set of these is denoted by $\mathrm{Y}(G)$. There is an obvious duality between $\mathrm{X}(G)$ and $\mathrm{Y}(G)$ that will be denoted by $^\vee$: $\chi \in \mathrm{X}(G) \leftrightarrow \chi^\vee \in \mathrm{Y}(G)$. We give a useful theorem due to Borel on the structure of tori of algebraic groups.

Theorem 1.34 ([Hum75, Section 34.3])**.** *Let T be an $\mathbb{F}$-torus.*

(i) There exists a finite Galois extension of $\mathbb{F}$ over which T becomes split.

(ii) There exist unique subtori T', T'' of T defined over $\mathbb{F}$ such that $T = T'T''$, where T' is $\mathbb{F}$-split, and T'' is $\mathbb{F}$-anisotropic. Moreover, T' is the largest $\mathbb{F}$-split subtorus of T and T'' is its largest $\mathbb{F}$-anisotropic subtorus.

An algebraic group is called *split* if it has a split maximal torus. A *Borel subgroup* of G is a closed connected solvable subgroup properly included in no other. The following theorems show the significance of these subgroups and (split) tori.

Theorem 1.35 ([Hum75, Section 21.3])**.** *Let B be any Borel subgroup of G. Then G/B is a projective variety, and all Borel subgroups are conjugate to B.*

A direct consequence of this theorem is the following:

Corollary 1.36 ([Hum75, Section 21.3])**.** *The maximal tori (resp. maximal connected unipotent subgroups) of G are those of the Borel subgroups of G, and are all conjugate.*

We take $\mathbb{F}$ to be any field and consider tori in $G(\mathbb{F})$, the rational points of G.

Theorem 1.37 ([Hum75, Section 34.4])**.** *Let G be a connected algebraic group defined over the field $\mathbb{F}$.*

(i) G has a maximal torus defined over $\mathbb{F}$.

(ii) If G is reductive, then G splits over a finite Galois extension of $\mathbb{F}$.

(iii) If G is reductive and S is an $\mathbb{F}$-torus, then $\mathrm{C}_G(S)$ is reductive and defined over $\mathbb{F}$. Moreover, S is contained in some maximal torus defined over $\mathbb{F}$.

The following result, originally due to Borel and Tits, is the equivalent of Corollary 1.36 for split tori.

Theorem 1.38 ([Spr98, Theorem 15.2.6])**.** *Let G be a connected algebraic group defined over the field $\mathbb{F}$. Two maximal $\mathbb{F}$-split $\mathbb{F}$-tori are conjugate by an element of $G(\mathbb{F})$.*

1.7.1 Toral subalgebras

In the Lie algebra of an algebraic group notions similar to (split) tori exist. Suppose L is a Lie algebra over an arbitrary field $\mathbb{F}$, and suppose $\mathrm{ad} : L \to \mathrm{End}(\mathbb{F}^d)$ (where $d = \dim(L)$) is its adjoint representation. An element $x \in L$ is called *semisimple* if the roots of the minimal polynomial of $\mathrm{ad}(x)$ over $\mathbb{F}$ are all distinct. (If $\mathbb{F}$ is algebraically closed this is equivalent to $\mathrm{ad}(x)$ being diagonalizable.) An element $x \in L$ is called *nilpotent* if $\mathrm{ad}(x)$ is. In the special cases where $\mathbb{F}$ is algebraically closed or L is restricted, an arbitrary element $x \in L$ has a *Jordan-Chevalley decomposition* (or simply *Jordan decomposition*) $x = x_s + x_n$, where x_s is semisimple, x_n is nilpotent, and $[x_s, x_n] = 0$.

Let H be a subalgebra of the Lie algebra L. Then H is called *toral* if it is abelian and consists solely of semisimple elements. A toral subalgebra is called *maximal* if it is not properly contained in any other. A toral subalgebra H is called *split* if the characteristic roots of every ad_h (for $h \in H$) are in the base field. A Lie algebra is called *split* if it has a split maximal toral subalgebra.

The relation between tori and toral subalgebras becomes apparent in the following lemma, which is an accumulation of several results by Humphreys [Hum67, Proposition 13.2, Theorem 13.3, Corollaries 13.5, 13.6] and a result by Seligman [Sel67, Theorem 9].

Lemma 1.39. *Let G be a connected algebraic group defined over $\mathbb{F}$ and $L = \mathrm{Lie}(G)$ its Lie algebra.*

(i) If T is a maximal torus of G, then $\mathrm{Lie}(T)$ is a maximal toral subalgebra of L.

(ii) If H is a maximal toral subalgebra of L then $H = \mathrm{Lie}(T)$ for some maximal torus T of G.

(iii) The maximal toral subalgebras of L are all conjugate under the adjoint action of G on L.

(iv) If $\mathrm{char}(\mathbb{F}) \neq 2$ then there is a one-to-one correspondence between maximal tori of G and maximal toral subalgebras of L given by $T \leftrightarrow \mathrm{Lie}(T)$.

(v) If $\mathrm{char}(\mathbb{F}) \neq 2$ then split *maximal tori correspond to* split *maximal toral subalgebras in the correspondence from (iv).*

The concept of maximal toral subalgebra is closely related to that of Cartan subalgebras. A subalgebra H of a Lie algebra L is called a *Cartan subalgebra* if it is nilpotent and $H = \mathrm{N}_L(H)$.

Lemma 1.40 ([Hum67, Propositions 15.1, 15.2, Corollary 15.3])**.** *Let G be a connected algebraic group defined over $\mathbb{F}$ and $L = \mathrm{Lie}(G)$ its Lie algebra.*

(i) If T is a maximal toral subalgebra of L, then $H = \mathrm{C}_L(T)$ is a Cartan subalgebra of L.

(ii) If H is a Cartan subalgebra of L, then $H = \mathrm{C}_L(T)$ for some maximal toral subalgebra $T \subseteq L$. The subalgebra T is in fact uniquely determined as the set of semisimple elements of H.

(iii) The Cartan subalgebras of L are all conjugate under the adjoint action of G on L.

Example 1.41. Over fields of characteristic 2 a split maximal toral subalgebra can be strictly contained in a Cartan subalgebra, as can be seen by considering the Lie algebra L of type $\mathrm{A}_1{}^{\mathrm{sc}}$. (See Section 1.9 for more details on how this Lie algebra is constructed). Over an arbitrary field $\mathbb{F}$, the Lie algebra L has basis elements h, X_α and $X_{-\alpha}$, and its multiplication table is as follows:

	X_α	$X_{-\alpha}$	h
X_α	0	$-h$	$2X_\alpha$
$X_{-\alpha}$	h	0	$-2X_{-\alpha}$
h	$-2X_\alpha$	$2X_{-\alpha}$	0

but if $\mathbb{F}$ is taken to be a field of characteristic 2 this specializes to

	X_α	$X_{-\alpha}$	h
X_α	0	$-h$	0
$X_{-\alpha}$	h	0	0
h	0	0	0

Now $H = \langle h \rangle_{\mathbb{F}}$ is a split toral subalgebra over any field, and it is even maximal. Furthermore, if $\mathrm{char}(\mathbb{F}) \neq 2$ then H is a Cartan subalgebra (it is clearly nilpotent and $\mathrm{N}_L(H) = H$). If $\mathrm{char}(\mathbb{F}) = 2$, however, $\mathrm{N}_L(H) = L$, so that H is no longer a Cartan subalgebra. On the other hand, L is nilpotent and $\mathrm{N}_L(L) = L$, so that L itself is a Cartan subalgebra. L is, however, not split: the minimal polynomial of ad_{X_α} is x^2 rather than x.

1.8 Algebraic groups and root data

Throughout this section we let G be a split algebraic group and we fix a split maximal torus T of G. We call $W(G,T) = \mathrm{N}_G(T)/\,\mathrm{C}_G(T)$ the *Weyl group of G relative to T*. Because of the rigidity of tori, it is a finite group. Moreover, since all maximal tori are conjugate (cf. Corollary 1.36), all their Weyl groups are isomorphic, so such a group will be called simply *the Weyl group of* G, denoted by $W(G)$.

Recall from Section 1.7 that $\mathrm{X}(T)$ is the character group of T, that $\mathrm{Y}(T)$ is the set of one parameter multiplicative subgroups of T, and that the *roots* of G relative to T are the nontrivial weights of $\mathrm{Ad}\,T$ in $T_{\mathrm{id}}G$:

$$T_{\mathrm{id}}G = \mathrm{C}_{T_{\mathrm{id}}G}(T) \oplus \bigoplus_{\alpha \in \Phi} (T_{\mathrm{id}}G)_\alpha,$$

where $(T_{\mathrm{id}}G)_\alpha = \{x \in (T_{\mathrm{id}}G) \mid \mathrm{Ad}\,t(x) = \alpha(t)x \text{ for all } t \in T\}$, and $\alpha \in X(T)$. We will denote the set of such non-zero roots by $\Phi(G,T)$. The elements of the subset $\{\alpha^\vee \mid \alpha \in \Phi(G,T)\} \subseteq \mathrm{Y}(G)$ are called the *coroots* of G and denoted by $\Phi^\vee(G,T)$. An important result in this field is the following theorem due to Chevalley.

Theorem 1.42 ([Spr98, Section 7.4.3])**.** *Let G be a connected linear algebraic group, T a maximal torus of G, $\Phi = \Phi(G,T)$, $W = W(G)$, $X = \mathrm{X}(T)$, $Y = \mathrm{Y}(T)$, and $\Phi^\vee =$*

$\Phi^\vee(G,T)$. *Then* $R = (X, \Phi, Y, \Phi^\vee)$ *is a root datum whose rank is* $\mathrm{rk}(G)$ *and whose Weyl group is isomorphic to* W. *The root datum* R *is called* the root datum of G.

The following theorem asserts that simple algebraic groups are classified by their root datum:

Theorem 1.43 ([Spr98, Theorem 9.6.2]). *If* G, G' *are connected reductive linear algebraic groups having isomorphic root data, then* G *and* G' *are isomorphic as algebraic groups.*

1.9 Chevalley Lie algebras

We now show an alternative construction of the Lie algebra of a reductive algebraic group: not as tangent space at the identity, but explicitly by the root datum of the group. Equivalence of these constructions is stated in Theorem 1.44.

Given a root datum $R = (X, \Phi, Y, \Phi^\vee)$ we consider the free $\mathbb{Z}$-module

$$L_{\mathbb{Z}}(R) = Y \oplus \bigoplus_{\alpha \in \Phi} \mathbb{Z} X_\alpha,$$

where the X_α are formal basis elements. The rank of $L_{\mathbb{Z}}(R)$ is $n + |\Phi|$. We denote by $[\cdot, \cdot]$ the alternating bilinear map $L_{\mathbb{Z}}(R) \times L_{\mathbb{Z}}(R) \to L_{\mathbb{Z}}(R)$ determined by the following rules:

$$[y, z] = 0, \tag{CB$\mathbb{Z}$1}$$

$$[X_\alpha, y] = \langle \alpha, y \rangle X_\alpha, \tag{CB$\mathbb{Z}$2}$$

$$[X_{-\alpha}, X_\alpha] = \alpha^\vee, \tag{CB$\mathbb{Z}$3}$$

$$[X_\alpha, X_\beta] = \begin{cases} N_{\alpha,\beta} X_{\alpha+\beta} & \text{if } \alpha + \beta \in \Phi, \\ 0 & \text{otherwise,} \end{cases} \tag{CB$\mathbb{Z}$4}$$

where $y, z \in Y$ and $\alpha, \beta \in \Phi$ such that $\alpha \neq \pm\beta$. The $N_{\alpha,\beta}$ are integral structure constants chosen to be $\pm(p_{\alpha,\beta} + 1)$, where $p_{\alpha,\beta}$ is the biggest number such that $-p_{\alpha,\beta}\alpha + \beta$ is a root and the signs are chosen (once and for all) so as to satisfy the Jacobi identity. It is easily verified that $N_{\alpha,\beta} = -N_{-\alpha,-\beta}$ and it is a well-known result (see for example [Car72, Section 4.2]) that such a product exists. $L_{\mathbb{Z}}(R)$ is called a *Chevalley Lie algebra*.

A basis of $L_{\mathbb{Z}}(R)$ that consists of a basis of Y and the formal elements X_α and satisfies (CB$\mathbb{Z}$1) – (CB$\mathbb{Z}$4) is called a *Chevalley basis of the Lie algebra* $L_{\mathbb{Z}}(R)$ *with respect to the split maximal toral subalgebra* Y *and the root datum* R. If no confusion is imminent we just call this a *Chevalley basis of* $L_{\mathbb{Z}}(R)$.

Note that, because $L_{\mathbb{Z}}(R)$ is defined over the integers, tensoring $L_{\mathbb{Z}}(R)$ with an arbitrary field $\mathbb{F}$ yields a Lie algebra over $\mathbb{F}$. We will denote this Lie algebra $L_{\mathbb{F}}(R)$. The toral subalgebra Y of each Chevalley Lie algebra $L_{\mathbb{F}}(R)$ is split. These Lie algebras are also commonly called *classical Lie algebras* (cf. [Str04, Section 4.1]).

The following result due to Chevalley states that this Lie algebra is in fact the Lie algebra of the split algebraic group defined over $\mathbb{F}$ whose root datum is R.

Theorem 1.44 (Chevalley [Che58]). *Suppose that* G *is a split simple algebraic group defined over the field* $\mathbb{F}$ *with root datum* $R = (X, \Phi, Y, \Phi^\vee)$. *Suppose furthermore that*

$L = \mathrm{Lie}(G)$ *and that* H *is a split maximal toral subalgebra of* L*. Then* $L \cong L_{\mathbb{F}}(R)$ *and so it has a Chevalley basis with respect to* H *and* R*.*

1.9.1 Roots in Lie algebras

Let p be zero or a prime and suppose that $\mathbb{F}$ is a (not necessarily algebraically closed) field of characteristic p. We fix a root datum $R = (X, \Phi, Y, \Phi^\vee)$ and write $L = L_{\mathbb{F}}(R)$. We define roots and their multiplicities in L as follows. A *root of* H *on* L is the function

$$\overline{\alpha} : h \mapsto \sum_{i=1}^{n} \langle \alpha, y_i \rangle t_i, \quad \text{where } h = \sum_{i=1}^{n} y_i \otimes t_i = \sum_{i=1}^{n} t_i h_i,$$

for some $\alpha \in \Phi$ (where $h_i = y_i \otimes 1_{\mathbb{F}}$); here $\langle \alpha, y_i \rangle$ is interpreted in $\mathbb{Z}$ (if $p = 0$) or $\mathbb{Z}/p\mathbb{Z}$ (if $p \neq 0$). Note that this implies that $\langle \alpha, h \rangle := \overline{\alpha}(h)$ because $h \in H$ is completely determined by the values $\langle \alpha, y_i \rangle$, $i = 1, \ldots, n$. We write $\Phi(L, H)$ for the set of roots of H on L.

For $\overline{\alpha} \in \Phi(L, H)$ we define the *root space corresponding to* $\overline{\alpha}$ to be

$$L_{\overline{\alpha}} = \bigcap_{i=1}^{n} \mathrm{Ker}(\mathrm{ad}_{h_i} - \overline{\alpha}(h_i)).$$

It is immediate that L is a direct sum of $L_0 = \mathrm{C}_L(H)$ and $\{L_{\overline{\alpha}} \mid \alpha \in \Phi, \overline{\alpha} \neq 0\}$. If $\overline{\alpha} \neq 0$ for all $\alpha \in \Phi$ then even $C_L(H) = H$.

Given a root α, we define the *multiplicity of* α *in* L to be the number of $\beta \in \Phi$ such that $\overline{\alpha} = \overline{\beta}$. Observe that if $\overline{\alpha} \neq 0$ the multiplicity of $\overline{\alpha} \in \Phi(L, H)$ is equal to $\dim(L_{\overline{\alpha}})$. If $\overline{\alpha} = 0$ this multiplicity is equal to $\dim(L_0) - n$. Note that $\alpha \mapsto \overline{\alpha}$ is a surjective map $\Phi \to \Phi(L, H)$, so in what follows we abbreviate $\Phi(L, H)$ to $\overline{\Phi}$.

If $p = 0$, the fact that $\langle \cdot, \cdot \rangle$ puts X and Y into duality implies that $\overline{\alpha}$ and $\overline{\beta}$ are different whenever $\alpha \neq \beta$. Indeed, suppose $\overline{\alpha} \equiv \overline{\beta}$, then $(\overline{\alpha - \beta})(h) \equiv 0$ for all $h \in H$, implying in particular $\langle \alpha - \beta, y \rangle \equiv 0$ for all $y \in Y$. But this means $\alpha - \beta = 0$ in Φ, hence $\alpha = \beta$. This means that the multiplicity of α in L is 1 for all $\alpha \in \Phi$.

If $p \neq 0$, however, this is not necessarily the case. Indeed, suppose $p = 2$ and observe that, since we interpret $\langle \alpha, y_i \rangle$ in $\mathbb{Z}/2\mathbb{Z}$, we have that $\overline{\alpha} \equiv \overline{-\alpha}$ for all $\alpha \in \Phi$. This means that, if $p = 2$, the multiplicity of α in L is at least 2 for all $\alpha \in \Phi$.

1.9.2 Computational conventions

Let $L_{\mathbb{Z}}(R)$ be a Chevalley Lie algebra with root datum R, fix $X = Y = \mathbb{Z}^n$, a basis of row vectors $e_1, \ldots, e_n$ of X, and a basis of row vectors $f_1, \ldots, f_n$ of Y dual to $e_1, \ldots, e_n$ with respect to the pairing $\langle \cdot, \cdot \rangle$. Moreover, we let $\mathbb{F}$ be a field, we set $h_i = f_i \otimes 1$, $i = 1, \ldots, n$, and $H = Y \otimes \mathbb{F}$. Now tensoring $L_{\mathbb{Z}}(R)$ with $\mathbb{F}$ yields a Lie algebra over $\mathbb{F}$, denoted $L_{\mathbb{F}}(R)$, and the integral Chevalley basis relations (CB$\mathbb{Z}$1) – (CB$\mathbb{Z}$4) can

	$A_1{}^{\mathrm{ad}}$	$A_1{}^{\mathrm{sc}}$
Root lattice	Root lattice $X = \mathbb{Z}$; $e_1 = (1)$	
Coroot lattice	Coroot lattice $Y = \mathbb{Z}$; $f_1 = (1)$	
Basis elements	$X_\alpha, X_{-\alpha}, h$	
Roots	$\alpha = (1), -\alpha = (-1)$	$\alpha = (2), -\alpha = (-2)$
Coroots	$\alpha^\vee = (2), -\alpha^\vee = (-2)$	$\alpha^\vee = (1), -\alpha^\vee = (-1)$
$\langle \cdot, \cdot \rangle$	$\langle \alpha, f_1 \rangle = 1$	$\langle \alpha, f_1 \rangle = 2$
	$\langle e_1, \alpha^\vee \rangle = 2$	$\langle e_1, \alpha^\vee \rangle = 1$
Mult. table	$\begin{array}{cccc} & X_\alpha & X_{-\alpha} & h \\ \hline X_\alpha & 0 & -2h & X_\alpha \\ X_{-\alpha} & 2h & 0 & -X_{-\alpha} \\ h & -X_\alpha & X_{-\alpha} & 0 \end{array}$	$\begin{array}{cccc} & X_\alpha & X_{-\alpha} & h \\ \hline X_\alpha & 0 & -h & 2X_\alpha \\ X_{-\alpha} & h & 0 & -2X_{-\alpha} \\ h & -2X_\alpha & 2X_{-\alpha} & 0 \end{array}$

Table 1.45: Chevalley Lie algebras of rank one

be rephrased as:

$$[h_i, h_j] = 0, \tag{CB1}$$

$$[X_\alpha, h_i] = \langle \alpha, f_i \rangle X_\alpha, \tag{CB2}$$

$$[X_{-\alpha}, X_\alpha] = \sum_{i=1}^{n} \langle e_i, \alpha^\vee \rangle h_i, \tag{CB3}$$

$$[X_\alpha, X_\beta] = \begin{cases} N_{\alpha,\beta} X_{\alpha+\beta} & \text{if } \alpha + \beta \in \Phi, \\ 0 & \text{otherwise,} \end{cases} \tag{CB4}$$

where $i, j \in \{1, \ldots, n\}$ and $\alpha, \beta \in \Phi$ such that $\alpha \neq \pm\beta$.

Note that this definition gives rise to a multiplication table as defined in Section 1.4.2, and that such a multiplication table will contain many zeroes.

1.9.3 Chevalley Lie algebras of rank one

In Table 1.45 we present the two possible Chevalley Lie algebras over $\mathbb{Z}$ of rank one, following the conventions from Sections 1.3.1 and 1.9.2. Values that are by definition equal for both cases are centered over the two columns.

1.10 The Steinberg presentation

Theorems 1.42 and 1.43 show that the structure of split simple algebraic groups is completely determined by their root datum. The following presentation exhibits this structure very clearly.

Definition 1.46 (Group of Lie type)**.** Suppose $R = (X, \Phi, Y, \Phi^\vee)$ is a root datum and $\mathbb{F}$ an arbitrary field. Then the *group of Lie type* with root datum R and base field $\mathbb{F}$ is defined to be the group whose generators are $x_\alpha(a)$ (for $\alpha \in \Phi$ and $a \in \mathbb{F}$) and

$y \otimes t$ (for $y \in Y$ and $t \in \mathbb{F}^*$), and whose relations are:

$$\begin{aligned}
(y \otimes t)(y \otimes u) &= y \otimes (tu), && \text{(ST1)}\\
(y \otimes t)(z \otimes t) &= (y+z) \otimes t, && \text{(ST2)}\\
(\alpha^\vee \otimes t) &= n_\alpha(-1)n_\alpha(t), && \text{(ST3)}\\
(y \otimes t)^{n_\alpha} &= s_{\alpha^\vee}(y) \otimes t, && \text{(ST4)}\\
x_\alpha(a)x_\alpha(b) &= x_\alpha(a+b), && \text{(ST5)}\\
[x_\alpha(a), x_\beta(b)] &= \prod_{i,j>0} x_{i\alpha+j\beta}\left(C_{ij\alpha\beta}a^i b^j\right), && \text{(ST6)}\\
x_\alpha(a)^{x_{-\alpha}(b)} &= x_{-\alpha}(-b^2a)^{x_\alpha(b^{-1})}, && \text{(ST7)}
\end{aligned}$$

for $y, z \in \Phi^\vee$, $t, u \in \mathbb{F}^*$, $\alpha, \beta \in \Phi$ (such that $\alpha \neq \pm\beta$) and $a, b \in \mathbb{F}$. Here $n_\alpha(t) = x_\alpha(t)x_{-\alpha}(-t^{-1})x_\alpha(t)$, $n_\alpha(1)$ is abbreviated to n_α, and the $C_{ij\alpha\beta}$ are structure constants defined in Section 1.10.1. The order of the terms in the product is taken such that $i+j$ increases (this does not uniquely determine the order, but in the ambiguous cases the terms commute).

The following theorem provides the connection between algebraic groups and groups of Lie type.

Theorem 1.47 ([Spr98, Theorem 9.4.3])**.** *Let G be a connected reductive linear algebraic group defined over $\mathbb{F}$, let R be the root datum of G, and let $\mathbb{F}' \supseteq \mathbb{F}$. Moreover, let G' be the group of Lie type with root datum R and base field $\mathbb{F}'$. Then $G(\mathbb{F}')$ and G' are isomorphic as abstract groups.*

This presentation of an algebraic group is called the *Steinberg presentation*. The usual important subgroups arise naturally: A split maximal torus T is generated by $y \otimes t$, the subgroup N is generated by T and the n_α (where $\alpha \in \Phi$), the unipotent subgroup U is generated by $\{x_\alpha(a) \mid \alpha \in \Phi^+, a \in \mathbb{F}\}$, and a Borel subgroup is $B = TU$.

Moreover, for every $w \in W$ there is a corresponding element $\dot{w}$ of G: Take a reduced expression $w = s_{\beta_1} \cdots s_{\beta_l}$, then $\dot{w} = n_{\beta_1} \cdots n_{\beta_l}$. This is well-defined by [Spr98, Proposition 9.3.2]. There is an isomorphism between N/T and W given by $T\dot{w} \leftrightarrow w$. We write $\dot{W}' = \{\dot{w} \mid w \in W'\}$ if $W' \subseteq W$. Moreover, the double cosets of B correspond (bijectively) to the elements of W by $B\dot{w}B \leftrightarrow w$.

We prove some additional properties of the elements of a group of Lie type that we will need in Chapter 2.

Lemma 1.48. *For $\alpha \in \Phi$, $t, u \in \mathbb{F}^*$, and x an arbitrary element of G the following relations hold:*

$$\begin{aligned}
\alpha^\vee \otimes 1 &= \mathrm{id}, && \text{(ST8)}\\
x_\alpha(0) &= \mathrm{id}, && \text{(ST9)}\\
n_\alpha(t)^{-1} &= n_\alpha(-t), && \text{(ST10)}\\
n_\alpha(t)n_\alpha(u) &= \alpha^\vee \otimes -\frac{u}{t}. && \text{(ST11)}
\end{aligned}$$

Proof The first three statements are trivial to verify. For the fourth, we have

$$\begin{aligned} n_\alpha(t)n_\alpha(u) &= n_\alpha(t)n_\alpha(1)n_\alpha(-1)n_\alpha(u) \\ &= n_\alpha(-t)^{-1}n_\alpha(-1)^{-1}n_\alpha(-1)n_\alpha(u) \\ &= (\alpha^\vee \otimes -t)^{-1}(\alpha^\vee \otimes u) = \alpha^\vee \otimes -\frac{u}{t}. \end{aligned}$$

□

1.10.1 The structure constants

We now turn to the constants $N_{\alpha,\beta}$ in order to arrive at the definition of the constants $C_{ij\alpha\beta}$. Throughout this section, let Φ be a root system, Δ a set of fundamental roots, and Φ^+ (resp. Φ^-) the corresponding set of positive (resp. negative) roots. Recall from Section 1.9 that the $N_{\alpha,\beta}$ are integral structure constants such that $N_{\alpha,\beta} = \pm(p_{\alpha,\beta}+1)$, where $p_{\alpha,\beta}$ is the biggest number such that $-p_{\alpha,\beta}\alpha + \beta$ is a root. Similarly, we define $q_{\alpha,\beta}$ to be the biggest number such that $q_{\alpha,\beta}\alpha + \beta$ is a root.

The fact that the relations (CB$\mathbb{Z}$1) – (CB$\mathbb{Z}$4) should produce a Lie algebra imposes several restrictions on these constants. In particular

Lemma 1.49 ([Car72, Theorem 4.1.2]). *For $\alpha, \beta \in \Phi$, the constants $N_{\alpha,\beta}$ satisfy:*

(i) $N_{\beta,\alpha} = -N_{\alpha,\beta}$, *and*

(ii) $N_{-\alpha,-\beta} = -N_{\alpha,\beta}$.

Additionally, for $\alpha, \beta, \gamma \in \Phi$ such that $\alpha + \beta + \gamma = 0$, we have

(iii) $\frac{N_{\alpha,\beta}}{(\gamma,\gamma)} = \frac{N_{\beta,\gamma}}{(\alpha,\alpha)} = \frac{N_{\gamma,\alpha}}{(\beta,\beta)}$,

and for $\alpha, \beta, \gamma, \delta \in \Phi$ such that $\alpha + \beta + \gamma + \delta = 0$ and no two of these roots are opposite we have

(iv) $\frac{N_{\alpha,\beta}N_{\gamma,\delta}}{(\alpha+\beta,\alpha+\beta)} + \frac{N_{\beta,\gamma}N_{\alpha,\delta}}{(\beta+\gamma,\beta+\gamma)} + \frac{N_{\gamma,\alpha}N_{\beta,\delta}}{(\alpha+\gamma,\alpha+\gamma)} = 0.$

These relations obviously impose a number of restrictions on the choices available for $N_{\alpha,\beta}$. It turns out that the possible choices are parametrized by so-called *extraspecial pairs*, that are defined as follows. Suppose we are given a total ordering on the space containing the roots (for instance one extending the partial ordering $\alpha \succ \beta$ whenever $\alpha - \beta \in \Phi^+$). An ordered pair of roots (α, β) is called a *special pair* if $\alpha + \beta \in \Phi$ and $0 \prec \alpha \prec \beta$. An ordered pair of roots (α, β) is called an *extraspecial pair* if it is a special pair and if for all special pairs (α', β') for which $\alpha + \beta = \alpha' + \beta'$ we have $\alpha \preceq \alpha'$. This definition easily leads to the observation that every root in Φ^+ which is the sum of two roots in Φ^+ is the sum of precisely one extraspecial pair. Since every non-simple positive root is the sum of two roots in Φ^+, there is a 1-1 correspondence between $\Phi^+\backslash\Delta$ and the set of extraspecial pairs.

The significance of these extraspecial pairs becomes apparent in the following lemma.

	α_1	α_2	$\alpha_1+\alpha_2$	$2\alpha_1+\alpha_2$	$3\alpha_1+\alpha_2$	$3\alpha_1+2\alpha_2$	$\dots$
α_1	0	ε_1	$2\varepsilon_2$	$3\varepsilon_3$	0	0	
α_2	$-\varepsilon_1$	0	0	0	ε_4	0	
$\alpha_1+\alpha_2$	$-2\varepsilon_2$	0	0	$-3\varepsilon_1\varepsilon_3\varepsilon_4$	0	0	
$2\alpha_1+\alpha_2$	$-3\varepsilon_3$	0	$3\varepsilon_1\varepsilon_3\varepsilon_4$	0	0	0	
$3\alpha_1+\alpha_2$	0	$-\varepsilon_4$	0	0	0	0	
$3\alpha_1+2\alpha_2$	0	0	0	0	0	0	
$-\alpha_1$	0	0	$3\varepsilon_1$	$2\varepsilon_2$	ε_3	0	
$-\alpha_2$	0	0	$-\varepsilon_1$	0	0	ε_4	
$-\alpha_1-\alpha_2$	$3\varepsilon_1$	$-\varepsilon_1$	0	$-2\varepsilon_2$	0	$-\varepsilon_1\varepsilon_3\varepsilon_4$	
$-2\alpha_1-\alpha_2$	$2\varepsilon_2$	0	$-2\varepsilon_2$	0	$-\varepsilon_3$	$\varepsilon_1\varepsilon_3\varepsilon_4$	
$-3\alpha_1-\alpha_2$	ε_3	0	0	$-\varepsilon_3$	0	$-\varepsilon_4$	
$-3\alpha_1-2\alpha_2$	0	ε_4	$-\varepsilon_1\varepsilon_3\varepsilon_4$	$\varepsilon_1\varepsilon_3\varepsilon_4$	$-\varepsilon_4$	0	

Table 1.51: Structure constants $N_{\alpha,\beta}$ for the root system of type G_2

Lemma 1.50 ([Car72, Proposition 4.2.2]). *The signs of the structure constants $N_{\alpha,\beta}$ may be chosen arbitrarily for extraspecial pairs (α,β), and then the structure constants for all pairs are uniquely determined by the requirement that $L_{\mathbb{Z}}(R)$ be a Lie algebra.*

The signs so chosen are commonly called *extraspecial signs*.

Example 1.52. As an example, we consider the root system of type G_2, and calculate $N_{\alpha,\beta}$ for all $\alpha,\beta \in \Phi$. The result is shown in Table 1.51, where the missing entries (i.e., $N_{\alpha,\beta}$ for β a negative root) can easily be reconstructed using Lemma 1.49(ii).

We choose a total ordering on the roots extending $\alpha \succ \beta$ whenever $\alpha - \beta \in \Phi^+$, so that the extraspecial pairs are (α_1,α_2), $(\alpha_1,\alpha_1+\alpha_2)$, $(\alpha_1, 2\alpha_1+\alpha_2)$, and $(\alpha_2, 3\alpha_1+\alpha_2)$. Suppose we choose as extraspecial signs for these extraspecial pairs $\varepsilon_1,\varepsilon_2,\varepsilon_3$, and ε_4, respectively ($\varepsilon_i \in \{-1,1\}$). This implies for instance that $N_{\alpha_1,\alpha_2} = \varepsilon_1(p_{\alpha_1,\alpha_2}+1) = \varepsilon_1$ (since $-\alpha_1+\alpha_2$ is not a root and therefore $p_{\alpha_1,\alpha_2} = 0$). Similarly, $-\alpha_1 + (\alpha_1+\alpha_2) = \alpha_2$ is a root, but $-2\alpha_1 + (\alpha_1+\alpha_2)$ is not, so that $p_{\alpha_1,\alpha_1+\alpha_2} = 1$ and $N_{\alpha_1,\alpha_1+\alpha_2} = \varepsilon_2(1+1) = 2\varepsilon_2$.

Now to compute for instance $N_{-\alpha_2,2\alpha_1+\alpha_2}$ observe that $-\alpha_1-\alpha_2+(\alpha_1+\alpha_2) = 0$ so that, by Lemma 1.49(iii)

$$\frac{N_{-\alpha_1,-\alpha_2}}{(\alpha_1+\alpha_2,\alpha_1+\alpha_2)} = \frac{N_{-\alpha_2,\alpha_1+\alpha_2}}{(-\alpha_1,-\alpha_1)},$$

implying $N_{-\alpha_2,\alpha_1+\alpha_2} = N_{-\alpha_1,-\alpha_2} = -N_{\alpha_1,\alpha_2} = -\varepsilon_1$ using Lemma 1.49(ii) and the fact that these three roots are all short. Similarly, using $(-3\alpha_1-\alpha_2)+(2\alpha_1+\alpha_2)+\alpha_1 = 0$ we find

$$\frac{N_{-3\alpha_1-\alpha_2,2\alpha_1+\alpha_2}}{(\alpha_1,\alpha_1)} = \frac{N_{2\alpha_1+\alpha_2,\alpha_1}}{(-3\alpha_1-\alpha_2,-3\alpha_1-\alpha_2)},$$

implying $N_{-3\alpha_1-\alpha_2,2\alpha_1+\alpha_2} = -\frac{1}{3}N_{\alpha_1,2\alpha_1+\alpha_2} = -\varepsilon_3$.

As a final example, we compute $N_{\alpha_1+\alpha_2,2\alpha_1+\alpha_2}$. Observe $(\alpha_1+\alpha_2)+(2\alpha_1+\alpha_2)+(-\alpha_2)+(-3\alpha_1-\alpha_2)=0$, and (since no two of these are opposite roots) by Lemma 1.49(iv):

$$\frac{N_{\alpha_1+\alpha_2,2\alpha_1+\alpha_2}N_{-\alpha_2,-3\alpha_1-\alpha_2}}{(3\alpha_1+2\alpha_2,3\alpha_1+2\alpha_2)}+\frac{N_{2\alpha_1+\alpha_2,-\alpha_2}N_{\alpha_1+\alpha_2,-3\alpha_1-\alpha_2}}{(2\alpha_1,2\alpha_1)} \\ +\frac{N_{-\alpha_2,\alpha_1+\alpha_2}N_{2\alpha_1+\alpha_2,-3\alpha_1-\alpha_2}}{(\alpha_1,\alpha_1)}=0.$$

Using the values computed earlier, this reduces to

$$\frac{N_{\alpha_1+\alpha_2,2\alpha_1+\alpha_2}\cdot-\varepsilon_4}{3}+0+\frac{-\varepsilon_1\cdot\varepsilon_3}{1}=0,$$

implying $N_{\alpha_1+\alpha_2,2\alpha_1+\alpha_2} = -3\varepsilon_1\varepsilon_3\varepsilon_4$. All the other entries of the table are easily computed using the same techniques.

We end this section with the definition of $M_{\alpha,\beta,i}$ and $C_{\alpha,\beta,i,j}$. We write

$$M_{\alpha,\beta,i}=\frac{1}{i!}N_{\alpha,\beta}N_{\alpha,\alpha+\beta}\cdots N_{\alpha,(i-1)\alpha+\beta},$$

adopting the convention that $M_{\alpha,\beta,0}=1$. Using $N_{\alpha,\beta}=\pm(p_{\alpha,\beta}+1)$ we readily see

$$M_{\alpha,\beta,i}=\pm\frac{(p_{\alpha,\beta}+1)(p_{\alpha,\beta}+2)\cdots(p_{\alpha,\beta}+i)}{i!}=\pm\binom{p_{\alpha,\beta}+i}{i},$$

in particular $M_{\alpha,\beta,i}$ is integral. Now the $C_{ij\alpha\beta}$ are defined as follows:

$$\begin{aligned} C_{i1\alpha\beta}&=-M_{\alpha,\beta,i},\\ C_{1j\alpha\beta}&=M_{\beta,\alpha,j},\\ C_{32\alpha\beta}&=-\frac{2}{3}M_{\alpha+\beta,\alpha,2},\\ C_{23\alpha\beta}&=-\frac{1}{3}M_{\alpha+\beta,\beta,2}. \end{aligned}$$

Also the $C_{ij\alpha\beta}$ are integral. Indeed, for $C_{i1\alpha\beta}$ and $C_{1j\alpha\beta}$ this is trivial; for $C_{32\alpha\beta}$ observe

$$C_{32\alpha\beta}=-\frac{2}{3}M_{\alpha+\beta,\alpha,2}=-\frac{2}{3}\frac{1}{2}N_{\alpha+\beta,\alpha}N_{\alpha+\beta,2\alpha+\beta},$$

which either is equal to zero (if $3\alpha+2\beta$ is not a root), or $3\alpha+2\beta$ is a root. Then $-(\alpha+\beta)+\alpha=-\beta$ is a root (and $-2(\alpha+\beta)+\alpha=-\alpha-2\beta$ is not, for root chains of such length do not exist), implying $p_{\alpha+\beta,\alpha}=1$, and both $-(\alpha+\beta)+2\alpha+\beta=\alpha$ and $-2(\alpha+\beta)+2\alpha+\beta=-\beta$ are roots, so that $p_{\alpha+\beta,2\alpha+\beta}=2$. This implies $N_{\alpha+\beta,\alpha}=\pm2$ and $N_{\alpha+\beta,2\alpha+\beta}=\pm3$, so that $C_{32\alpha\beta}$ is indeed integral. A similar reasoning leads to the observation that $C_{23\alpha\beta}$ is integral.

1.10.2 The action of G on $\mathrm{Lie}(G)$

In this section we combine the results of the previous two sections and exhibit the action of an algebraic group on its Lie algebra. So let G be a split simple algebraic group defined over the field $\mathbb{F}$, R its root datum, and $L = \mathrm{Lie}(G)$ its Lie algebra. By Theorem 1.47 G has a Steinberg presentation, and by Theorem 1.44 the Lie algebra L has a Chevalley basis (cf. Equations CB1 – CB4).

The action of G on L is then given by the following relations:

$$\begin{aligned} (y \otimes t)h_i &= h_i, & x_\alpha(a)h_i &= h_i + \langle \alpha, f_i \rangle a X_\alpha, \\ (y \otimes t)X_\beta &= t^{\langle \beta, y \rangle} X_\beta, & x_\alpha(a)X_\beta &= \textstyle\sum_{i=0}^{q_{\alpha\beta}} C_{i1\alpha\beta} a^i X_{i\alpha+\beta}. \end{aligned}$$

1.11 Tori and conjugacy classes of the Weyl group

In this section we let G be a split group of Lie type defined over an arbitrary field $\mathbb{F}$, we let T_0 be a split maximal torus of G, and we let W be the Weyl group of G (see Section 1.8 for some additional details). We claim conjugacy classes of maximal tori of G over $\mathbb{F}$ are parametrized by conjugacy classes of W.

For suppose T is a torus defined over $\mathbb{F}$, but not necessarily split. There is a $g \in G(\overline{\mathbb{F}})$ such that $T = T_0^g$, and $T_0^g \leq G(\mathbb{F})$ if and only if $t^{g^F} = t^g$ for all $t \in T_0$, where F is the Frobenius automorphism of the field $\mathbb{F}$. But this holds if and only if $t^{g^F g^{-1}} = t$, which holds if and only if $t^{F g^F g^{-1}} = t$ for all $t \in T_0$. Now we write $w = g^F g^{-1}$, and observe that $(t^F)^w = t$, so that $w \in N_G(T_0) = W$ since both $t \in T_0$ and $t^F \in T_0$. So there exists a correspondence between conjugacy classes of tori and conjugacy classes of the Weyl group, and it is given by $g \leftrightarrow g^F g^{-1}$.

Example 1.53. We determine all tori of $G = \mathrm{SL}_2$ defined over GF(3). The standard split torus T_0 consists of the diagonal matrices in G and $T_0(\mathrm{GF}(3))$ consists of the GF(3)-rational points of T_0, i.e.

$$T_0(\mathrm{GF}(3)) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \right\}.$$

The set of tori of G is by definition

$$\mathcal{T} = \{ T_0^g \mid g \in \overline{G}, \text{ satisfying } t^F = t \text{ for all } t \in T_0^g \}.$$

In this case it suffices to consider only the GF(3^2)-rational points of G. We let ξ be a generating element of GF(3^2) such that $\xi^2 = \xi + 1$. By explicit computations we find 4 elements of $\mathcal{T}$, namely $T_0(\mathrm{GF}(3))$,

$$T_1 = \left\{ \begin{pmatrix} -1 & -1 \\ -1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \right\},$$

$$T_2 = \left\{ \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}, \begin{pmatrix} -1 & 1 \\ 1 & 1 \end{pmatrix} \right\},$$

$$T_3 = \left\{ \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}.$$

Example elements $g \in \overline{G}$ giving rise to these tori are

$$g_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, g_1 = \begin{pmatrix} 1 & \xi \\ \xi^6 & \xi \end{pmatrix}, g_2 = \begin{pmatrix} 1 & \xi^5 \\ \xi^2 & \xi \end{pmatrix}, \text{ and } g_3 = \begin{pmatrix} \xi^2 & 1 \\ 1 & \xi^2 \end{pmatrix}.$$

Now $w_i = g_i^F g_i^{-1}$ (for $i = 1, \dots, 4$) should be an element of the normalizer of the torus of $\overline{G}$. Indeed,

$$w_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, w_1 = \begin{pmatrix} 0 & \xi^2 \\ \xi^2 & 0 \end{pmatrix}, \text{ and } w_2 = w_3 = \begin{pmatrix} 0 & \xi^6 \\ \xi^6 & 0 \end{pmatrix}.$$

The fact that w_1, w_2, and w_3 are the same (up to elements of the torus: observe $w_1 T_0 = w_2 T_0$) indicates that the tori T_1, T_2, and T_3 should be conjugate in $G(\mathrm{GF}(3))$. Indeed, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ sends T_2 to T_1 and $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ sends T_3 to T_1.

One last observation is that T_0 is a split torus, and T_1 is nonsplit ($x^2 + 1$ is the minimal polynomial of two of its elements).

We may find the g corresponding to a given w, i.e., a g such that $w = g^F g^{-1}$, using Lang's theorem:

Theorem 1.54 (Lang's Theorem, [Lan56])**.** *If G is a connected algebraic group defined over the finite field $\mathbb{F}$ with Frobenius map F, then the map $G \to G$, $x \mapsto x^{-F}x$ is onto.*

An algorithm for Lang's theorem has been described by Cohen and Murray [CM09], and we execute the algorithm in the following example.

Example 1.55. Let $\mathbb{F}$ be the field with 3^4 elements and $\mathbb{F}' \subseteq \mathbb{F}$ the field with 3 elements, let ξ be a primitive element of $\mathbb{F}$, let F be the Frobenius automorphism $i \mapsto i^3$, let R be the root datum of type $\mathrm{A_2}^{\mathrm{sc}}$, let $G = \mathrm{SL}_3$ defined over $\mathbb{F}$, and let $L = \mathfrak{sl}_3(\mathbb{F})$ be the corresponding Lie algebra. An advantage of this convention is that the action of $g \in G$ on L is simply $x \mapsto (g^{-1} x^\top g)^\top$.

Let $w = n_{\alpha_1}$ be the element of G corresponding to the first fundamental reflection s_{α_1} in the root system of type A_2:

$$w = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

We search for a $g \in G$ such that $w = g^F g^{-1}$. To that end, we let L' be the subalgebra of L consisting of those elements that are invariant under wF, viewed as a Lie algebra over the smaller field $\mathbb{F}'$. Simply solving linear equations gives us an $\mathbb{F}'$-basis of L', and using techniques from [CM09] we find a split maximal toral subalgebra and a Chevalley basis (again with respect to R) for L'. It consists of the following elements:

$$X_{\alpha_1} = \begin{pmatrix} 0 & 0 & \xi^{55} \\ 0 & 0 & \xi^{45} \\ 0 & 0 & 0 \end{pmatrix}, X_{\alpha_2} = \begin{pmatrix} \xi^{60} & \xi^{70} & 0 \\ \xi^{10} & \xi^{20} & 0 \\ 0 & 0 & 0 \end{pmatrix}, X_{\alpha_1+\alpha_2} = \begin{pmatrix} 0 & 0 & \xi^{35} \\ 0 & 0 & \xi^{65} \\ 0 & 0 & 0 \end{pmatrix},$$
$$X_{-\alpha_1} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ \xi^{65} & \xi^{75} & 0 \end{pmatrix}, X_{-\alpha_2} = \begin{pmatrix} \xi^{20} & \xi^{70} & 0 \\ \xi^{10} & \xi^{60} & 0 \\ 0 & 0 & 0 \end{pmatrix}, X_{-\alpha_1-\alpha_2} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ \xi^{5} & \xi^{55} & 0 \end{pmatrix},$$
$$h_1 = \begin{pmatrix} 1 & \xi^{10} & 0 \\ \xi^{70} & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, h_2 = \begin{pmatrix} 0 & \xi^{10} & 0 \\ \xi^{70} & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Now, since maps between Chevalley bases are automorphisms of L, we find a $g \in G$ that sends this new Chevalley basis to the original Chevalley basis of L:

$$g = \begin{pmatrix} 0 & \xi^{15} & \xi^{35} \\ 0 & \xi^{5} & \xi^{65} \\ -1 & 0 & 0 \end{pmatrix},$$

and it happens that $g \in G$. (This is not automatically the case, as $\mathrm{Aut}(L)$ is strictly bigger than G). It is now easily verified that $g^F g^{-1} = w$.

1.12 Classification of finite simple groups

A major effort of discrete mathematicians in the twentieth century has been towards finding all possible finite simple groups. This resulted ultimately in the classification of finite simple groups:

Theorem 1.56 ([Gor85]). *Every finite simple group is, up to isomorphism, one of* 26 *sporadic simple groups or belongs to at least one of the following three infinite families:*

(i) The cyclic groups of prime order;

(ii) The alternating groups of degree at least 5;

(iii) The simple groups of Lie type, including the four classical series of Lie groups, (denoted A_n *(*$n \geq 1$*),* B_n *(*$n \geq 2$*),* C_n *(*$n \geq 3$*),* D_n *(*$n \geq 4$*)), the exceptional Lie groups (*E_6*,* E_7*,* E_8*,* F_4*,* G_2*), the twisted groups of Lie type (*${}^2\mathrm{A}_n$ *(*$n \geq 1$*),* ${}^2\mathrm{D}_n$ *(*$n \geq 4$*),* ${}^3\mathrm{D}_4$*,* ${}^2\mathrm{E}_6$*,* ${}^2\mathrm{B}_2(2^{2m+1})$*,* ${}^2\mathrm{F}_4(2^{2m+1})$*, and* ${}^2\mathrm{G}_2(3^{2m+1})$*) and the Tits group (*${}^2\mathrm{F}_4(2)'$*).*

This theorem implies in particular that the groups under consideration in this thesis represent a significant portion of all finite simple groups. A large amount of information about these groups has been collected in the famous *Atlas of Finite Groups* [CCN+85].

We refer to Section 1.10 for the Steinberg presentation of the finite simple groups of Lie type in terms of generators and relations. In Chapter 2 we describe the construction of the twisted groups of Lie type, focusing on those of type ${}^2\mathrm{B}_2$, ${}^2\mathrm{F}_4$, and ${}^2\mathrm{G}_2$.

1.13 Algorithms

Since the main focus of this thesis is working with algebraic groups and their Lie algebras on a computer, we introduce some of the required notions regarding algorithms. We will take $O^{\sim}(N)$ to mean $O(N(\log N)^c)$ for some constant c. Recall (e.g., from [Shp99, Introduction]) that arithmetic operations in a field $\mathbb{F}$ are understood to be addition, subtraction, multiplication, division, and equality testing.

We will call a field *effective* if its elements can be described on a computer, equality between two elements can be tested by means of an algorithm, its arithmetic operations can be performed by means of algorithms, and the solutions of linear equations can be found algorithmically.

Finite fields are effective. In particular, in a field $\mathbb{F}$ of size q the arithmetic operations all take $O^{\sim}(\log(q))$ elementary operations [Shp99, Introduction]. We will assume that performing standard linear algebra arithmetic, that is, operations on matrices of size m, like multiplication, determinant, and kernel (solving linear equations), takes $O(m^3)$ arithmetic operations [Shp99, Section 4.4].

Algorithms may be *randomized*. Two important classes of randomized algorithms are *Monte Carlo* and *Las Vegas* [Ser06, Section 2]. A randomized algorithm is called Monte Carlo if there is a chance of an incorrect output, but an upper bound for the probability of error can be prescribed by the user. However, in most cases the runtime increases when that error probability is decreased. On the contrary, a Las Vegas algorithm never returns an incorrect answer but it may report failure with probability bounded by the user. Again, in most cases the runtime increases when the user requires a lower probability for failure.

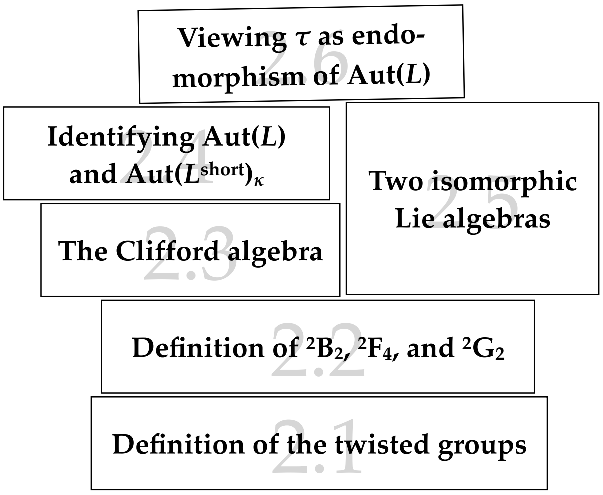
An example of a Las Vegas algorithm is the *Meat-axe* algorithm [Hol98, HEO05], which is generally used to compute submodules of modules over finite fields. Finding an ideal I of a given Lie algebra L is equivalent to finding the submodule I of the A-module L, where A is the associative subalgebra of $\mathrm{End}(L)$ generated by all ad_x for x running over a basis of L. Consequently, such an ideal I can be found by application of the Meat-axe to the A-module L. For finite fields, the Meat-axe algorithm is analysed in [Rón90], [Hol98, Section 2] and [IL00]: irreducible submodules of a finite L-module of dimension m over $\mathrm{GF}(q)$ can be found in Las Vegas time $O^{\sim}(m^3\log(q))$. For infinite fields, Meat-axe procedures are known; however, we know of no proof of polynomiality in the literature.

Many basic algorithms for computing with Lie algebras (e.g., computing subalgebras, centers, ideals, etc) were designed by De Graaf [dG00] and have been implemented in GAP and Magma.

Regarding the computation of split maximal toral subalgebras of Lie algebras of classical type, Cohen and Murray present an algorithm for computing split maximal toral subalgebras [CM09, Section 5]. However, in this case it is also assumed that the characteristic of the field is not 2 or 3 (in fact, the algorithm will often work if the characteristic is 3, but it will not work for characteristic 2). This algorithm has been implemented in Magma. Independently, Ryba developed an algorithm for computing split Cartan subalgebras [Ryb07]. However, this algorithm similarly requires the field to not be of characteristic 2. In Chapter 3 we present a heuristic algorithm that yields good results in the characteristic 2 case. This algorithm may fail if certain unfortunate random choices occur, but if it returns a result, that result is correct. However, we provide no estimates on the failure probability, hence the algorithm is not a Las Vegas algorithm in the sense defined above.

Regarding the computation of Chevalley bases, De Graaf describes an algorithm called CanonicalGenerators that produces "a canonical set of generators" of a Lie algebra, given a simple system of the root system of L. This returns in fact a Chevalley basis up to scalars [dG00, Section 5.11], but the required scaling can be accomplished by straightforwardly solving linear equations. Furthermore, in [CM09, Section 5] Cohen and Murray give an algorithm StandardChevalleyBasis that produces a Chevalley basis, given only the Lie algebra L. A split maximal toral subalgebra of L and an appropriate root system are computed in the first two steps. The drawback of both these algorithms is the assumption on the characteristic of the field underlying the Lie algebra. The former assumes this characteristic is 0 (although the algorithm will often work if the characteristic is at least 5), and the latter assumes the characteristic of the field is not 2 or 3. In Chapter 4 we present an algorithm that works even in characteristics 2 and 3.

We apply these algorithms in Chapter 5 to produce algorithms for recognition of Lie algebras of algebraic groups, and in Chapter 6 to prove the non-existence of a graph on which a certain group acts distance transitively.


Viewing τ as endomorphism of Aut(L)
2.6
Identifying Aut(L) and Aut(L^{short})$_\kappa$
2.4
Two isomorphic Lie algebras
2.5
The Clifford algebra
2.3
Definition of ${}^2B_2$, ${}^2F_4$, and ${}^2G_2$
2.2
Definition of the twisted groups
2.1

2 Twisted Groups of Lie Type

The twisted groups of Lie type were discovered independently by Steinberg, Tits, and Hertzig. They are well known today and for example described by Steinberg [Ste67, Section 11] and Carter [Car72, Chapters 12 – 14]. This chapter focuses on a construction of the twisted groups by use of Lie algebras. It is joint work with Arjeh M. Cohen, and these results will also appear in [BC].

We first briefly describe the general construction for finite fields in Section 2.1, and then focus on types ${}^2\mathrm{B}_2$, ${}^2\mathrm{F}_4$, and ${}^2\mathrm{G}_2$ as these are the most complicated cases. The construction of the automorphism of the group in these cases (described in Section 2.2) is known, and described in some detail in [Car72, Sections 12.3, 12.4]. In Sections 2.3 – 2.6 we describe how to find a corresponding endomorphism of Lie algebras (Proposition 2.10), and thus show that the automorphism used to construct the twisted groups has a geometrical interpretation (Corollary 2.12).

To increase legibility we will mostly use action from the left in this chapter, e.g., $x \mapsto g(x)$. Field automorphisms, however, will act from the right, e.g., $t \mapsto t^F$.

2.1 Definition of the twisted groups

Let G be a simple algebraic group defined over the field $\mathbb{F}$ (see Section 1.5) whose Dynkin diagram has a non-trivial symmetry δ, and let R be its root datum. Let τ be an automorphism of G corresponding to δ, and F be a non-trivial automorphism of $\mathbb{F}$ (that extends to an automorphism of G denoted by the same symbol) chosen so that $\sigma = \tau F$ satisfies $\sigma^n = 1$, where n is the order of δ. The subgroup of $G(\mathbb{F})$ consisting of all elements that are fixed under σ is called the *twisted group of Lie type* of type ${}^nR$.

The same procedure can be applied to the corresponding Lie algebra: let $L = L_{\mathbb{F}}(R)$ be the Chevalley Lie algebra of type R over the finite field $\mathbb{F}$. The automorphism δ induces an endomorphism τ of the algebraic group G, and therefore an endomorphism $\mathrm{d}\tau$ of $L \cong \mathrm{Lie}(G)$. Moreover, since the field automorphism F naturally acts on L, we find an endomorphism $\sigma = (\mathrm{d}\tau)F$ of L. If $\mathrm{d}\tau$ is an automorphism of L, then σ again satisfies $\sigma^n = 1$. In that case, the subalgebra of L consisting of all elements fixed under σ is called the *twisted Lie algebra* of type ${}^nR$.

Consider the irreducible Dynkin diagrams, shown in Figure 1.4. "Obvious" automorphisms exist for the cases A_l (of order two for $l \geq 2$), D_l (of order two for $l \geq 4$ and of order three for $l = 4$), and E_6: see Figure 2.1. For these four cases, $\mathbb{F}$

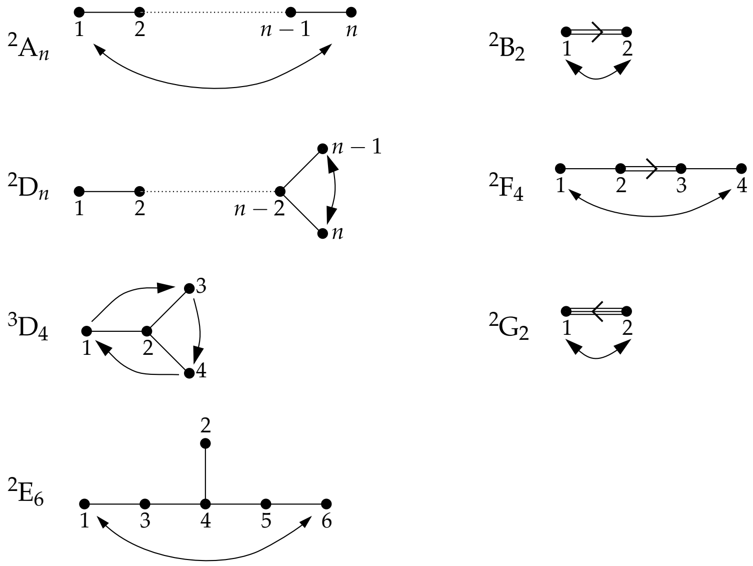


Figure 2.1: Automorphisms of Dynkin diagrams

must be a field that admits an automorphism whose order is equal to the order of δ. Therefore, in the finite case, $\mathbb{F} = \mathrm{GF}(q^2)$ for some prime power q for the twisted groups ^2A_l, ^2D_l, and $^2E_6$, and $\mathbb{F} = \mathrm{GF}(q^3)$ for some prime power q for the case $^3D_4$.

The cases B_2, F_4, and G_2 are significantly different: Indeed, the graph automorphisms depicted interchange the short roots and the long roots (see Figure 2.1). For $^2B_2$ and $^2F_4$ the field $\mathbb{F}$ must be of characteristic 2 and admit an automorphism ϑ such that $2\vartheta^2 = 1$, i.e., for all $x \in \mathbb{F}$ we have $x^{2\vartheta^2} = x$. Similarly, for $^2G_2$ the field $\mathbb{F}$ must be of characteristic 3 and admit an automorphism ϑ such that $3\vartheta^2 = 1$. The following lemma determines which finite fields have that property.

Lemma 2.2 ([Car72, Lemma 14.1.1]). *Let $\mathbb{F} = \mathrm{GF}(p^k)$ be a finite field of characteristic p admitting an automorphism ϑ satisfying $p\vartheta^2 = 1$. Then k is odd and ϑ is of the form*

$$x^\vartheta = x^{p^m},$$

where m is such that $k = 2m+1$.

Proof We have $x^\vartheta = x^{p^r}$ for some r, so $x = x^{p\vartheta^2} = x^{p^{2r+1}}$, so that $x^{p^{2r+1}} = x$ for all $x \in \mathbb{F}$. Thus $\mathbb{F}$ is contained in $\mathrm{GF}(p^{2r+1})$, and therefore k divides $2r+1$. It follows that k is odd, so we write $k = 2m+1$, where $m \in \mathbb{N}$. Now let $(2r+1) = (2m+1)(2s+1)$. Then $r = s(2m+1)+m$ and $x^{p^r} = x^{p^{(2m+1)s+m}} = x^{p^{(2m+1)s}p^m} = (x^{p^{(2m+1)s}})^{p^m}$. But since $x^{p^{2m+1}} = x^{p^k} = x$, so that $x^{p^{(2m+1)s}} = x$, it follows that $x^{p^r} = x^{p^m}$. Hence $x^\vartheta = x^{p^m}$, as required. □

This gives rise to the following twisted groups:

$$\begin{array}{ll} {}^2\mathrm{A}_n(q^2), & n \geq 2 \\ {}^2\mathrm{D}_n(q^2), & n \geq 4 \\ {}^3\mathrm{D}_4(q^3), & \\ {}^2\mathrm{E}_6(q^2), & \\ {}^2\mathrm{B}_2(2^{2m+1}), & \\ {}^2\mathrm{F}_4(2^{2m+1}), & \\ {}^2\mathrm{G}_2(3^{2m+1}). & \end{array}$$

The fact that automorphisms of groups of Lie type are the product of an inner automorphism, a so-called diagonal automorphism, a graph automorphism, and a field automorphism, shows that these groups are uniquely determined in the case where $\mathbb{F}$ is a finite field, for then the field automorphism is unique up to conjugation. (In the case where $\mathbb{F}$ is not finite this procedure may produce non-isomorphic groups for different choices of the field automorphism.) Note also that these twisted groups are isomorphic to certain classical groups: $^2\mathrm{A}_n(q^2)$ is isomorphic to the unitary group $\mathrm{PSU}_{n+1}(\mathrm{GF}(q^2), f)$ for some Hermitian form f, and $^2\mathrm{D}_n(q^2)$ is isomorphic to the orthogonal group $\mathrm{P}\Omega_{2n}(\mathrm{GF}(q), f)$, for some quadratic form f (cf. [Car72, Theorems 14.5.1, 14.5.2]).

In Chapter 6 we consider the twisted group of type ^{2}A$_7$, but in a special setting where it is inside the group of type E$_7$. In this chapter we concentrate on ^{2}B$_2$, ^{2}F$_4$, and ^{2}G$_2$, for the following reason. Recall from the above that τ is an automorphism of the algebraic group, so that there exists an endomorphism $\mathrm{d}\tau$ of $\mathrm{Lie}(G)$. It turns out that $\mathrm{d}\tau$ is bijective in the case of ^{2}A$_n$, ^{2}D$_n$, ^{3}D$_4$, and ^{2}E$_6$, but $\mathrm{d}\tau$ has a substantial kernel in the case of ^{2}B$_2$, ^{2}F$_4$, and ^{2}G$_2$. However, in Proposition 2.10 we will show that the automorphism τ of G corresponds to an endomorphism of $\mathrm{Aut}(L)$. Moreover, τ induces a duality on the Lie incidence geometry related to G (cf. Corollary 2.12).

2.2 Definition of ^{2}B$_2$, ^{2}F$_4$, and ^{2}G$_2$

In this section we will consider the diagram automorphisms of B$_2$, F$_4$, and G$_2$ and show (in Proposition 2.5) that they extend to endomorphisms of the corresponding groups of Lie type.

Let Φ be a root system of type B$_2$, F$_4$, or G$_2$, and take $\delta : \Phi \to \Phi$ to be the Dynkin diagram automorphism. For $\Phi = \mathrm{B}_2$ and $\Phi = \mathrm{G}_2$ this automorphism is obtained by reflecting in the line bisecting α and β, as shown in Figure 2.3, followed by the appropriate scaling to ensure that the image is again a root. For $\Phi = \mathrm{F}_4$ the procedure is similar and naturally extends the automorphism construction for B$_2$.

For $\Phi = \mathrm{B}_2$ (taking as fundamental roots α_1, α_2, such that α_1 is long and α_2 is short) the automorphism δ acts as follows:

$$\begin{array}{rlrl} \alpha_1 & \leftrightarrow \alpha_2, & -\alpha_1 & \leftrightarrow -\alpha_2, \\ \alpha_1 + 2\alpha_2 & \leftrightarrow \alpha_1 + \alpha_2, & -\alpha_1 - 2\alpha_2 & \leftrightarrow -\alpha_1 - \alpha_2. \end{array}$$

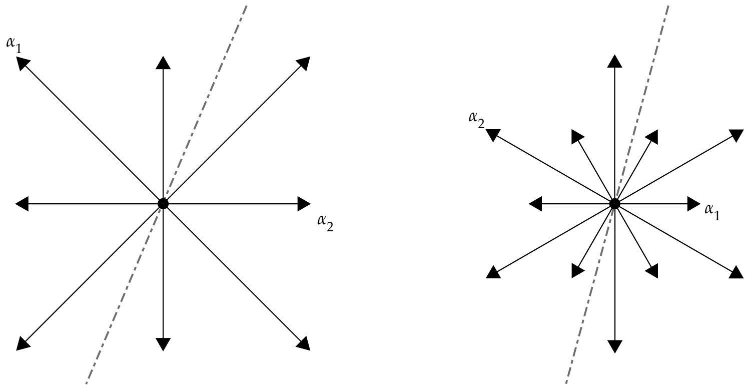


Figure 2.3: Automorphisms inducing ${}^2B_2$ and ${}^2G_2$

For $\Phi = G_2$ (taking as fundamental roots α_1, α_2, such that α_1 is short and α_2 is long) the automorphism δ acts as follows:

$$\begin{aligned} \alpha_1 &\leftrightarrow \alpha_2, \\ \alpha_1 + \alpha_2 &\leftrightarrow 3\alpha_1 + \alpha_2, \\ 2\alpha_1 + \alpha_2 &\leftrightarrow 3\alpha_1 + 2\alpha_2, \end{aligned}$$

and the equivalent action on the negative roots.

For $\Phi = F_4$ (taking as fundamental roots $\alpha_1, \dots, \alpha_4$, such that α_1 and α_2 are long and α_3 and α_4 are short) the automorphism δ acts as follows:

$$\begin{aligned} \alpha_1 &\leftrightarrow \alpha_4, \\ \alpha_2 &\leftrightarrow \alpha_3, \\ \alpha_1 + \alpha_2 &\leftrightarrow \alpha_3 + \alpha_4, \\ \alpha_2 + \alpha_3 &\leftrightarrow \alpha_2 + 2\alpha_3, \\ \alpha_1 + \alpha_2 + \alpha_3 &\leftrightarrow \alpha_2 + 2\alpha_3 + 2\alpha_4, \\ \alpha_2 + \alpha_3 + \alpha_4 &\leftrightarrow \alpha_1 + \alpha_2 + 2\alpha_3, \\ \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 &\leftrightarrow \alpha_1 + \alpha_2 + 2\alpha_3 + 2\alpha_4, \\ \alpha_2 + 2\alpha_3 + \alpha_4 &\leftrightarrow \alpha_1 + 2\alpha_2 + 2\alpha_3, \\ \alpha_1 + \alpha_2 + 2\alpha_3 + \alpha_4 &\leftrightarrow \alpha_1 + 2\alpha_2 + 2\alpha_3 + 2\alpha_4, \\ \alpha_1 + 2\alpha_2 + 2\alpha_3 + \alpha_4 &\leftrightarrow \alpha_1 + 2\alpha_2 + 4\alpha_3 + 2\alpha_4, \\ \alpha_1 + 2\alpha_2 + 3\alpha_3 + \alpha_4 &\leftrightarrow \alpha_1 + 3\alpha_2 + 4\alpha_3 + 2\alpha_4, \\ \alpha_1 + 2\alpha_2 + 3\alpha_3 + 2\alpha_4 &\leftrightarrow 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 2\alpha_4, \end{aligned}$$

and the equivalent action on the negative roots.

Note that in each case δ interchanges the long and the short roots, but leaves the set of positive roots (and the set of negative roots) invariant. We let δ act on $\Phi^\vee$ in correspondence with the way it acts on Φ, by taking $\delta(\alpha^\vee) = (\delta\alpha)^\vee$. We introduce signs $\varepsilon : \Phi \to \{1, -1\}$, needed in order to be able to extend δ to an automorphism of G. If $\Phi = \mathrm{B}_2$ or $\Phi = \mathrm{F}_4$ we take $\varepsilon \equiv 1$. For $\Phi = \mathrm{G}_2$, we fix extraspecial signs $\varepsilon_1, \dots, \varepsilon_4$ in advance (cf. Example 1.52) and let

$$\varepsilon_\alpha = \begin{cases} \eta_1 & \text{if } \alpha = \pm\alpha_1 \text{ or } \alpha = \pm\alpha_2, \\ \eta_2 & \text{if } \alpha = \pm(\alpha_1 + \alpha_2) \text{ or } \alpha = \pm(3\alpha_1 + \alpha_2), \\ \eta_3 & \text{if } \alpha = \pm(2\alpha_1 + \alpha_2) \text{ or } \alpha = \pm(3\alpha_1 + 2\alpha_2), \end{cases}$$

where we demand η_1, η_2, η_3 be such that

$$\eta_2 = -\varepsilon_2\varepsilon_3 \text{ and } \eta_1\eta_3 = \varepsilon_3\varepsilon_4.$$

Classical choices here are $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4) = (1, 1, 1, 1)$ and $(\eta_1, \eta_2, \eta_3) = (1, -1, 1)$ (due to Steinberg [Ste67, Section 11]) and $(\varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4) = (-1, -1, 1, 1)$ and $(\eta_1, \eta_2, \eta_3) = (1, 1, 1)$ (due to Carter [Car72, Section 12.4]).

We write Φ^{short} for the set of short roots and Φ^{long} for the set of long roots in Φ, and we prove various properties of δ and ε.

Lemma 2.4. *Let $\delta : \Phi \to \Phi$ and $\varepsilon : \Phi \to \{-1, 1\}$ be as defined above.*

(i) $\varepsilon_{-\alpha} = \varepsilon_\alpha$ and $\varepsilon_\alpha = \varepsilon_{\delta\alpha}$, for all $\alpha \in \Phi$.

(ii) For $\alpha, \beta \in \Phi^{\mathrm{short}}$ such that $\alpha + \beta \in \Phi^{\mathrm{short}}$, we have $\varepsilon_\alpha\varepsilon_\beta N_{\delta\alpha,\delta\beta} = \varepsilon_{\alpha+\beta}N_{\alpha,\beta}$.

(iii) If $\alpha, \beta \in \Phi$ such that $\alpha + \beta \notin \Phi$ then either $\delta(\alpha) + \delta(\beta) \notin \Phi$, or $N_{\delta(\alpha),\delta(\beta)} \equiv 0 \mod p$ (where $p = 2$ if $\Phi = \mathrm{B}_2$ or $\Phi = \mathrm{F}_4$, and $p = 3$ if $\Phi = \mathrm{G}_2$).

(iv) For $\alpha, \beta \in \Phi^{\mathrm{short}}$, $\alpha \neq \pm\beta$, we have:

(a) If $\alpha + \beta \in \Phi^{\mathrm{short}}$, then $\delta(\alpha) + \delta(\beta) = \delta(\alpha + \beta) \in \Phi^{\mathrm{long}}$.

(b) If $\alpha + \beta \in \Phi^{\mathrm{long}}$, then $\delta(\alpha) + \delta(\beta) \notin \Phi$.

(v) For $\alpha, \beta \in \Phi^{\mathrm{long}}$ such that $\alpha + \beta \in \Phi$ we have $\alpha + \beta \in \Phi^{\mathrm{long}}$, $\delta(\alpha + \beta) = \delta(\alpha) + \delta(\beta)$, $2\alpha + \beta \notin \Phi$, and $3\alpha + \beta \notin \Phi$.

(vi) For $\alpha \in \Phi^{\mathrm{short}}$ and $\beta \in \Phi^{\mathrm{long}}$ such that $\alpha + \beta \in \Phi$, we have

(a) If $\Phi = \mathrm{B}_2$ or $\Phi = \mathrm{F}_4$ and $\alpha + \beta \in \Phi$ then $\alpha + \beta \in \Phi^{\mathrm{short}}$, $2\alpha + \beta \in \Phi^{\mathrm{long}}$, and $3\alpha + \beta \notin \Phi$.

(b) If $\Phi = \mathrm{G}_2$ then $\alpha + \beta \in \Phi^{\mathrm{short}}$, $2\alpha + \beta \in \Phi^{\mathrm{short}}$, and $3\alpha + \beta \in \Phi^{\mathrm{long}}$.

Proof (i) follows immediately from the definition of ε, and (ii) is easily verified. For example, for $\Phi = \mathrm{G}_2$, $\alpha = \alpha_1$ and $\beta = \alpha_1 + \alpha_2$ we see:

$$\begin{aligned} \varepsilon_\alpha\varepsilon_\beta N_{\delta\alpha,\delta\beta} &= \varepsilon_{\alpha_1}\varepsilon_{\alpha_1+\alpha_2}N_{\alpha_2,3\alpha_1+\alpha_2} = \eta_1\eta_2\varepsilon_4 = \eta_3 \cdot 2\varepsilon_2 \\ &= \varepsilon_{2\alpha_1+\alpha_2}N_{\alpha_1,\alpha_1+\alpha_2} = \varepsilon_{\alpha+\beta}N_{\alpha,\beta}, \end{aligned}$$

using $\eta_1\eta_2\eta_3 = -\varepsilon_2\varepsilon_3^2\varepsilon_4 = -\varepsilon_2\varepsilon_4$ and the fact that $\mathrm{char}(\mathbb{F}) = 3$. Properties (iii) – (vi) are straightforward to check. □

Now to extend the automorphism δ of the root system to an endomorphism of the group of Lie type let $R = (X, \Phi, Y, \Phi^\vee)$ be a root datum of type $\mathrm{B}_2{}^{\mathrm{ad}}$, F_4, or G_2, let $\mathbb{F}$ be a perfect field of size 2^{2m+1} for some $m \in \mathbb{N}$ (for B_2 and F_4) or of size 3^{2m+1} for some $m \in \mathbb{N}$ (for G_2), and let G be the corresponding group of Lie type. Furthermore, we write $p = \mathrm{char}(\mathbb{F})$ and we let F be an automorphism of $\mathbb{F}$ of the same order as δ.

Proposition 2.5. *The automorphism δ of the root system extends to an endomorphism τ of G determined by*

$$x_\alpha(t) \mapsto \begin{cases} x_{\delta(\alpha)}(\varepsilon_\alpha t) & \text{if } \alpha \text{ is a long root,} \\ x_{\delta(\alpha)}(\varepsilon_\alpha t^p) & \text{if } \alpha \text{ is a short root,} \end{cases}$$
$$y \otimes t \mapsto \begin{cases} \delta(y) \otimes t & \text{if } y \text{ is a long coroot,} \\ \delta(y) \otimes t^p & \text{if } y \text{ is a short coroot,} \end{cases}$$

and $\tau^2 = \mathrm{F}$. If $\omega \in \mathrm{Aut}(\mathbb{F})$ satisfies $\omega^2 = \mathrm{F}$, then the endomorphism $\tau^* = \tau\omega^{-1}$ is an involution.

Proof To see that τ is indeed an endomorphism of G we verify that τ preserves the Steinberg relations (ST1)–(ST7) defined in Section 1.10. Throughout the proof, we let $y, z \in \Phi^\vee$, $t, u \in \mathbb{F}^*$, $\alpha, \beta \in \Phi$ such that $\alpha \neq \pm\beta$, and $a, b \in \mathbb{F}$. Moreover, we let

$$\lambda : \Phi \to \mathbb{F}, \lambda(\alpha) = \begin{cases} p & \text{if } \alpha \in \Phi^{\text{short}}, \\ 1 & \text{if } \alpha \in \Phi^{\text{long}}, \end{cases}$$

and $\lambda(\alpha^\vee) = \lambda(\alpha)$, so that $\tau(x_\alpha(t)) = x_{\delta(\alpha)}(\varepsilon_\alpha t^{\lambda(\alpha)})$ and $\tau(y \otimes t) = \delta(y) \otimes t^{\lambda(y)}$. We abbreviate $\delta(\alpha)$ to $\delta\alpha$ and $\lambda(\alpha)$ to $\lambda\alpha$ for ease of reading.

Observe first that the action of τ on $n_\alpha(t)$ follows from the action on $x_\alpha(t)$:

$$\begin{aligned} \tau(n_\alpha(t)) &= \tau x_\alpha(t) \tau x_{-\alpha}(-t^{-1}) \tau x_\alpha(t) \\ &= x_{\delta\alpha}(\varepsilon_\alpha t^{\lambda\alpha}) x_{\delta(-\alpha)}(\varepsilon_\alpha(-t^{-1})^{\lambda\alpha}) x_{\delta\alpha}(\varepsilon_\alpha t^{\lambda\alpha}) \\ &= x_{\delta\alpha}(\varepsilon_\alpha t^{\lambda\alpha}) x_{-\delta\alpha}(-\left((\varepsilon_\alpha t)^{\lambda\alpha}\right)^{-1}) x_{\delta\alpha}(\varepsilon_\alpha t^{\lambda\alpha}) \\ &= n_{\delta\alpha}(\varepsilon_\alpha t^{\lambda\alpha}), \end{aligned}$$

using the fact that $\delta(-\alpha) = -\delta(\alpha)$. We will now deal with each of the relations (ST1)–(ST7) (see Section 1.10) separately.

For (ST1), observe

$$\tau(y \otimes t)\tau(y \otimes u) = (\delta y \otimes t^{\lambda y})(\delta y \otimes u^{\lambda y}) = \delta y \otimes (tu)^{\lambda y} = \tau(y \otimes (tu)).$$

The invariance of (ST2) follows immediately from the definition of $\tau(y \otimes t)$.

For (ST3), observe

$$\begin{aligned} \tau(\alpha^\vee \otimes t) &= (\delta\alpha)^\vee \otimes t^{\lambda\alpha} = n_{\delta\alpha}(-1) n_{\delta\alpha}(t^{\lambda\alpha}) \\ &= n_{\delta\alpha}(-\varepsilon_\alpha) n_{\delta\alpha}(\varepsilon_\alpha t^{\lambda\alpha}) = \tau n_\alpha(-1) \tau n_\alpha(t), \end{aligned}$$

where we use (ST11) to introduce the two ε_α.

For (ST4), observe

$$\begin{aligned}
\tau((y \otimes t)^{n_\alpha}) &= \tau(n_\alpha(-1))\tau(y \otimes t)\tau(n_\alpha(1)) \\
&= n_{\delta\alpha}(-\varepsilon_\alpha)(\delta y \otimes t^{\lambda y})n_{\delta\alpha}(\varepsilon_\alpha) \\
&= n_{\delta\alpha}(-1)(\delta y \otimes t^{\lambda y})n_{\delta\alpha}(1) \\
&= (\delta y) \otimes t^{\lambda y})^{n_{\delta\alpha}} \\
&= s_{\alpha^\vee}(\delta y) \otimes t^{\lambda y} \\
&= \delta(s_{\alpha^\vee}(y)) \otimes t^{\lambda(s_\alpha^\vee(y))} \\
&= \tau(s_{\alpha^\vee}(y) \otimes t),
\end{aligned}$$

where we use the fact that δ is an automorphism of the root system, $s_{\alpha^\vee}$ is a reflection, so it maps y to a coroot of equal length, and again (ST11).

Relation (ST5) is trivially verified:

$$\begin{aligned}
\tau x_\alpha(a)\tau x_\alpha(b) &= x_{\delta\alpha}(\varepsilon_\alpha a^{\lambda\alpha})x_{\delta\alpha}(\varepsilon_\alpha b^{\lambda\alpha}) \\
&= x_{\delta\alpha}(\varepsilon_\alpha a^{\lambda\alpha} + \varepsilon_\alpha b^{\lambda\alpha}) \\
&= x_{\delta\alpha}(\varepsilon_\alpha(a+b)^{\lambda\alpha}) = \tau x_\alpha(a+b),
\end{aligned}$$

where we explicitly need the fact that $\lambda\alpha$ is either 1 or char$(\mathbb{F})$.

Before considering (ST6), which is the most involved case, we deal with (ST7).

$$\begin{aligned}
\tau\left(x_\alpha(a)^{x_{-\alpha}(b)}\right) &= x_{\delta\alpha}(\varepsilon_\alpha a^{\lambda\alpha})^{x_{\delta(-\alpha)}(\varepsilon_{-\alpha} b^{\lambda\alpha})} \\
&= x_{\delta\alpha}(\varepsilon_\alpha a^{\lambda\alpha})^{x_{-\delta\alpha}(\varepsilon_\alpha b^{\lambda\alpha})} \\
&= x_{-\delta\alpha}(-\varepsilon_\alpha^2(b^{\lambda\alpha})^2\varepsilon_\alpha a^{\lambda\alpha})^{x_{\delta\alpha}((\varepsilon_\alpha b^{\lambda\alpha})^{-1})} \\
&= x_{-\delta\alpha}(-\varepsilon_\alpha(b^2a)^{\lambda\alpha})^{x_{\delta\alpha}(\varepsilon_\alpha b^{-\lambda\alpha})} \\
&= x_{\delta(-\alpha)}(-\varepsilon_{-\alpha}(b^2a)^{\lambda(-\alpha)})^{x_{\delta\alpha}(\varepsilon_\alpha b^{-\lambda\alpha})} \\
&= \tau\left(x_{-\alpha}(-b^2a)^{x_\alpha(b^{-1})}\right).
\end{aligned}$$

For (ST6) we distinguish five cases, depending on the type of subsystem α and β generate: A subsystem of type A$_2$ (then α and β are of equal length and inclined at $2\pi/3$), a subsystem of type B$_2$ (only if $\Phi = \mathrm{B}_2$ or $\Phi = \mathrm{F}_4$, then either α and β are both short and inclined at $\pi/2$, or α is short, β is long, and they are inclined at $3\pi/4$), or a subsystem of type G$_2$ (only if $\Phi = \mathrm{G}_2$, then either α and β are both short and inclined at $\pi/3$, or α is short, β is long, and they are inclined at $5\pi/6$).

If α and β are of equal length and inclined at $2\pi/3$, observe

$$\begin{aligned}\tau[x_\alpha(a), x_\beta(b)] &= [x_{\delta\alpha}(\varepsilon_\alpha t^{\lambda\alpha}), x_{\delta\beta}(\varepsilon_\beta t^{\lambda\beta})]\\ &= x_{\delta\alpha+\delta\beta}(-\varepsilon_\alpha \varepsilon\beta N_{\delta\alpha,\delta\beta} a^{\lambda\alpha} b^{\lambda\beta})\\ &= x_{\delta(\alpha+\beta)}(-\varepsilon_{\alpha+\beta} N_{\alpha\beta}(ab)^{\lambda(\alpha+\beta)})\\ &= \tau x_{\alpha+\beta}(-N\alpha\beta ab)\\ &= \tau x_{\alpha+\beta}(C_{11\alpha\beta}ab),\end{aligned}$$

using Lemma 2.4(ii), (iv), and (v), the fact that α, β, $\alpha+\beta$ are all of the same length, and the fact that $N_{\alpha\beta} = \pm 1$, and therefore non-zero mod p.

If $\Phi = \mathrm{B}_2$ or F_4 and α and β are both short and inclined at $\pi/2$, we are in the case that $\mathrm{char}(\mathbb{F}) = 2$ so we ignore the ε_α. Moreover, $\alpha+\beta \in \Phi^{\mathrm{long}}$, so $\delta(\alpha)+\delta(\beta) \notin \Phi$ by Lemma 2.4(iv). Also, since $-\alpha+\beta$ is a root and $-2\alpha+\beta$ is not, we have $p_{\alpha\beta} = 1$ and therefore $N_{\alpha\beta} = \pm 2 \equiv 0 \mod p$, so that

$$\tau([x_\alpha(a), x_\beta(b)]) = [x_{\delta\alpha}(a^2), x_{\delta\beta}(b^2)] = \mathrm{id} = x_{\delta(\alpha+\beta)}(-N_{\alpha\beta}ab) = \tau x_{\alpha+\beta}(C_{11\alpha\beta}ab).$$

If $\Phi = \mathrm{B}_2$ or F_4 and α is short, β is long, and they are inclined at $3\pi/4$, we have $N_{\alpha\beta} = \pm 1$, $M_{\alpha\beta 2} = \pm 1$, and also $N_{\delta\alpha,\delta\beta} = \pm 1$, $M_{\delta\alpha,\delta\beta,2} = \pm 1$. It follows that

$$\begin{aligned}\tau([x_\alpha(a), x_\beta(b)]) &= [x_{\delta\alpha}(a^2), x_{\delta\beta}(b^2)]\\ &= x_{\delta\alpha+\delta\beta}(-N_{\delta\alpha,\delta\beta}a^2b)x_{\delta\alpha+2\delta\beta}(M_{\delta\beta,\delta\alpha,2}a^2b^2)\\ &= x_{\delta\alpha+\delta\beta}(a^2b)x_{\delta\alpha+2\delta\beta}(a^2b^2)\\ &= x_{\delta\alpha+2\delta\beta}(a^2b^2)x_{\delta\alpha+\delta\beta}(a^2b)\\ &= x_{\delta\alpha+2\delta\beta}(-N_{\alpha\beta}a^2b^2)x_{\delta\alpha+\delta\beta}(M_{\alpha,\beta,2}a^2b)\\ &= x_{\delta(\alpha+\beta)}(-N_{\alpha\beta}(ab)^2)x_{\delta(2\alpha+\beta)}(M_{\alpha,\beta,2}a^2b)\\ &= \tau x_{\alpha+\beta}(-N_{\alpha\beta}ab)\tau x_{2\alpha+\beta}(M_{\alpha,\beta,2}a^2b),\end{aligned}$$

using the observation that $\delta(\alpha+\beta) = \delta\alpha + 2\delta\beta$ and $\delta(2\alpha+\beta) = \delta\alpha+\delta\beta$. Moreover, $x_{\delta\alpha+\delta\beta}(a^2b)$ and $x_{\delta\alpha+2\delta\beta}(a^2b^2)$ commute since $(\delta\alpha+\delta\beta)+(\delta\alpha+2\delta\beta)$ is not a root.

If $\Phi = \mathrm{G}_2$ and α and β are both short and inclined at $\pi/3$, we are in the case that $\mathrm{char}(\mathbb{F}) = 3$ and $\alpha+\beta \in \Phi^{\mathrm{long}}$ so that $\delta\alpha+\delta\beta \notin \Phi$ (cf. Lemma 2.4(iv)). Furthermore, since $-2\alpha+\beta$ is a root and $-3\alpha+\beta$ is not, we have $p_{\alpha\beta} = 2$ and therefore $N_{\alpha\beta} = \pm 3 \equiv 0 \mod p$, so that

$$\begin{aligned}\tau([x_\alpha(a), x_\beta(b)]) &= [x_{\varepsilon_\alpha\delta\alpha}(a^3), x_{\varepsilon_\beta\delta\beta}(b^3)] = \mathrm{id}\\ &= x_{\delta(\alpha+\beta)}(-N_{\alpha\beta}\varepsilon_{\alpha+\beta}ab) = \tau x_{\alpha+\beta}(C_{11\alpha\beta}ab).\end{aligned}$$

If $\Phi = \mathrm{G}_2$ and α is short, β is long, and they are inclined at $5\pi/6$, then $\delta\alpha = \beta$ and $\delta\beta = \alpha$. We compute, using Table 1.51, $C_{11\alpha\beta} = -\varepsilon_1$, $C_{21\alpha\beta} = -\varepsilon_1\varepsilon_2$, $C_{31\alpha\beta} =$

$-\varepsilon_1\varepsilon_2\varepsilon_3$, $C_{32\alpha\beta} = \varepsilon_1\varepsilon_2\varepsilon_3\varepsilon_4$. This means

$$\begin{aligned}[x_\alpha(a), x_\beta(b)] = {} & x_{\alpha+\beta}(-\varepsilon_1 ab) \cdot x_{2\alpha+\beta}(-\varepsilon_1\varepsilon_2 a^2 b) \\ & \cdot x_{3\alpha+\beta}(-\varepsilon_1\varepsilon_2\varepsilon_3 a^3 b) \cdot x_{3\alpha+2\beta}(\varepsilon_1\varepsilon_2\varepsilon_3\varepsilon_4 a^3 b^2).\end{aligned}$$

Furthermore, we observe that $x_{3\alpha+\beta}(\cdot)$ and $x_{3\alpha+2\beta}(\cdot)$ commute since $(3\alpha+\beta)+(3\alpha+2\beta)$ is not a root, and $x_{\alpha+\beta}(\cdot)$ and $x_{2\alpha+\beta}(\cdot)$ commute since $-2(\alpha+\beta)+(2\alpha+\beta) = -\beta$ is a root and therefore $N_{\alpha+\beta,2\alpha+\beta} = \pm 3 \equiv 0 \mod p$. Now observe

$$\begin{aligned}\tau[x_\alpha(a), x_\beta(b)] &= [x_{\delta\alpha}(\varepsilon_\alpha a^3), x_{\delta\beta}(\varepsilon_\beta b)] = [x_\beta(\eta_1 a^3), x_\alpha(\eta_1 b)] \\ &= \Big([x_\alpha(\eta_1 b), x_\beta(\eta_1 a^3)]\Big)^{-1} \\ &= x_{3\alpha+2\beta}(-\eta_1^5\varepsilon_1\varepsilon_2\varepsilon_3\varepsilon_4 b^3 a^6) \cdot x_{3\alpha+\beta}(\eta_1^4\varepsilon_1\varepsilon_2\varepsilon_3 b^3 a^3) \\ &\quad \cdot x_{2\alpha+\beta}(\eta_1^3\varepsilon_1\varepsilon_2 b^2 a^3) \cdot x_{\alpha+\beta}(\eta_1^2\varepsilon_1 b a^3) \\ &= x_{3\alpha+\beta}(\varepsilon_1\varepsilon_2\varepsilon_3 b^3 a^3) \cdot x_{3\alpha+2\beta}(-\eta_1\varepsilon_1\varepsilon_2\varepsilon_3\varepsilon_4 b^3 a^6) \\ &\quad \cdot x_{\alpha+\beta}(\varepsilon_1 b a^3) \cdot x_{2\alpha+\beta}(\eta_1\varepsilon_1\varepsilon_2 b^2 a^3) \\ &= x_{\delta(\alpha+\beta)}(-\eta_2\varepsilon_1 b^3 a^3) \cdot x_{\delta(2\alpha+\beta)}(-\eta_3\varepsilon_1\varepsilon_2 b^3 a^6) \\ &\quad \cdot x_{\delta(3\alpha+\beta)}(-\eta_2\varepsilon_1\varepsilon_2\varepsilon_3 b a^3) \cdot x_{\delta(3\alpha+2\beta)}(\eta_3\varepsilon_1\varepsilon_2\varepsilon_3\varepsilon_4 b^2 a^3) \\ &= \tau x_{\alpha+\beta}(C_{11\alpha\beta} ab) \cdot \tau x_{2\alpha+\beta}(C_{21\alpha\beta} a^2 b) \\ &\quad \cdot \tau x_{3\alpha+\beta}(C_{31\alpha\beta} a^3 b) \cdot \tau x_{3\alpha+2\beta}(C_{32\alpha\beta} a^3 b^2),\end{aligned}$$

where we explicitly used the requirements that $\eta_1\eta_3 = \varepsilon_3\varepsilon_4$ and $\eta_2 = -\varepsilon_2\varepsilon_3$. This proves that τ is indeed an endomorphism of G.

To see that, for $\omega \in \mathrm{Aut}(\mathbb{F})$ such that $\omega^2 = \mathrm{F}$, the composition $\tau\omega^{-1}$ is an involution observe that ω and τ commute:

$$\omega\tau(x_\alpha(t)) = \omega(x_{\delta\alpha}(t^{\lambda(\alpha)})) = x_{\delta\alpha}(\omega(t)\lambda(\alpha)) = \tau(x_\alpha(\omega(t))) = \tau\omega(x_\alpha(t)).$$

This implies $(\tau^*)^2 = \tau^2\omega^{-2} = \mathrm{F}\,\omega^{-2} = \mathrm{id}$, proving the claim. □

Consequently, the automorphism $\sigma = \tau F$, as in the definition of twisted group, behaves as follows on the Steinberg presentation of G:

$$x_\alpha(t) \mapsto \begin{cases} x_{\delta(\alpha)}(\varepsilon_\alpha t^p) & \text{if } \alpha \text{ is a long root,} \\ x_{\delta(\alpha)}(\varepsilon_\alpha t^{p^2}) & \text{if } \alpha \text{ is a short root.} \end{cases}$$

$$y \otimes t \mapsto \begin{cases} \delta(y) \otimes t^p & \text{if } y \text{ is a long coroot,} \\ \delta(y) \otimes t^{p^2} & \text{if } y \text{ is a short coroot.} \end{cases}$$

2.3 The Clifford algebra

In this section, we introduce a procedure for creating a Lie algebra from a *Clifford algebra*. Let V be a vector space over an arbitrary field $\mathbb{F}$. The *tensor algebra* (denoted $T(V)$) consists of all tensor powers of V, including the one-dimensional zeroth power, which is defined to be $\mathbb{F}$. The algebra multiplication is simply tensor composition. $T(V)$ is an associative non-commutative algebra over $\mathbb{F}$, with unit $1 \in \mathbb{F}$. The *Clifford algebra*, denoted $\mathrm{Cl}(V)$, of the vector space V supplied with a quadratic form κ is the quotient of $T(V)$ by the two-sided ideal generated by all $x^2 - \kappa(x)$ for $x \in V$.

Let B denote the bilinear form on V associated with κ:

$$B(x,y) = \kappa(x+y) - \kappa(x) + \kappa(y).$$

This immediately implies $B(x,y) = (x+y)^2 - x^2 - y^2 = xy + yx$ for all $x, y \in \mathrm{Cl}(V)$. Now let $e_1, \dots, e_m$ be a basis of V. Then the products $e_J := \prod_{j \in J} e_j$, with the order of the factors given by increasing index, for J running over all subsets of $\{1, \dots, m\}$, is a basis of $\mathrm{Cl}(V)$. In particular, $\dim(\mathrm{Cl}(V)) = 2^m$.

Now let L be the Lie algebra of $\mathrm{Cl}(V)$ (in the sense of Example 1.9): The elements of L are the elements of $\mathrm{Cl}(V)$ and the Lie multiplication is given by $[x,y] = xy - yx$. Let $M \subseteq L$ be given by $M = \langle e_J \mid |J| \in \{0,2\} \rangle_{\mathbb{F}}$. We claim M is a subalgebra of L. Let $x, y \in M$. If either x or y corresponds to $e_\emptyset$ the assertion that $[x,y] \in M$ is trivial, so assume $x = ab$ and $y = cd$, for some $a, b, c, d \in V$. Then

$$\begin{aligned}
[x,y] = [ab, cd] &= abcd - cdab \\
&= -acbd + aB(b,c)d + cadb - cB(d,a)b \\
&= acdb - acB(b,d) + cadb + B(b,c)ad - B(d,a)cb \\
&= B(a,c)db - B(b,d)ac + B(b,c)ad - B(a,d)cb \in M.
\end{aligned}$$

So indeed M is a subalgebra of L. Clearly, $\dim(M) = 1 + \binom{m}{2}$. Consider the linear functional Tr on M given by $\mathrm{Tr}(1) = 2$ and $\mathrm{Tr}(xy) = B(x,y)$. It is well defined since

$$\mathrm{Tr}(x^2 - \kappa(x)) = \mathrm{Tr}(x^2) - \mathrm{Tr}(\kappa(x)) = B(x,x) - \mathrm{Tr}(\kappa(x)) = 2\kappa(x) - 2\kappa(x) = 0,$$

for all $x \in V$. The kernel of Tr on M is a codimension 1 subspace, which we denote by $P(V, \kappa)$. Observe that

$$\begin{aligned}
\mathrm{Tr}([ab,cd]) &= B(a,c)\,\mathrm{Tr}(db) - B(b,d)\,\mathrm{Tr}(ac) + B(b,c)\,\mathrm{Tr}(ad) - B(a,d)\,\mathrm{Tr}(cb) \\
&= B(a,c)B(d,b) - B(b,d)B(a,c) + B(b,c)B(a,d) - B(a,d)B(b,c) = 0,
\end{aligned}$$

so that every commutator of elements of M is in the kernel of Tr, and hence in $P(V, \kappa)$.

Example 2.6. We explicitly compute $P = P(V, \kappa)$, for $V = \mathbb{F}^5$, with $\mathbb{F}$ a field of characteristic 2 and $\kappa(v) = v_1 + v_2 v_4 + v_3 v_5$. We claim P is a Lie algebra of type B_2, and a suitable Chevalley basis is given by

$$\begin{aligned}
&X_{\alpha_1} = e_4 e_5,\ X_{\alpha_2} = e_1 e_3,\ X_{\alpha_1+\alpha_2} = e_1 e_4,\ X_{\alpha_1+2\alpha_2} = e_3 e_4, \\
&X_{-\alpha_1} = e_2 e_3,\ X_{-\alpha_2} = e_1 e_5,\ X_{-(\alpha_1+\alpha_2)} = e_1 e_2,\ X_{\alpha_1+2\alpha_2} = e_2 e_5, \\
&h_1 = e_2 e_4 + e_3 e_5 + 1,\ h_2 = 1.
\end{aligned}$$

To see this, the multiplication rules (CB1)–(CB4) should be verified. For example,

$$\begin{aligned}[X_{\alpha_1}, X_{\alpha_2}] &= [e_4e_5, e_1e_3] \\ &= B(e_4, e_1)e_3e_1 - B(e_5, e_3)e_4e_1 + B(e_5, e_1)e_4e_3 - B(e_4, e_3)e_1e_5 \\ &= 0 * e_3e_1 - (-1) * e_4e_1 + 0 * e_4e_3 - 0 * e_1e_5 \\ &= e_4e_1 = -e_1e_4 + B(e_1, e_4) = X_{\alpha_1+\alpha_2},\end{aligned}$$

as required.

2.4 Identifying $\mathrm{Aut}(L)$ and $\mathrm{Aut}(L^{\text{short}})_\kappa$

So far, we have seen the automorphism $\sigma = \tau F$ (the product of a diagram automorphism and a field automorphism) merely as an automorphism of the group of Lie type in its Steinberg presentation. In the remainder of this chapter we show how to see δ as an endomorphism of $\mathrm{Aut}(L)$, the main result being Proposition 2.10. To that end, we first identify $\mathrm{Aut}(L)$ and $\mathrm{Aut}(L^{\text{short}})_\kappa$ (this section), then show that L^{short} and L/L^{short} are isomorphic (Section 2.5), and finally come to the proof of Proposition 2.10 in Section 2.6.

So, for the remainder of this chapter, let $R = (X, \Phi, Y, \Phi^\vee)$ be a root datum of type $\mathrm{B_2}^{\text{sc}}$, $\mathrm{F_4}$, or $\mathrm{G_2}$, let $\mathbb{F}$ be a perfect field of characteristic 2, 2, or 3, respectively, and let L be the corresponding Lie algebra. Observe that for the $\mathrm{B_2}$ case we let the Lie algebra be of type $\mathrm{B_2}^{\text{sc}}$ (in order for L^{short} below to be generated by root elements), but we let the corresponding group be of type $\mathrm{B_2}^{\text{ad}}$ (because its action on the Lie algebra is more natural).

The Lie algebra L has an ideal generated by the short roots:

$$L^{\text{short}} = \left(X_\alpha \;\middle|\; \alpha \in \Phi^{\text{short}} \right)_L,$$

and $\dim(L^{\text{short}}) = \frac{1}{2}\dim(L)$ (i.e., 5, 26, or 7, for $\mathrm{B_2}$, $\mathrm{F_4}$, $\mathrm{G_2}$, respectively), because $\alpha^\vee = [X_{-\alpha}, X_\alpha] \in L^{\text{short}}$ whenever $\alpha \in \Phi^{\text{short}}$. The verification that L^{short} is in fact an ideal is straightforward, but needs the fact that $\mathbb{F}$ has the appropriate characteristic. For example, for the case where $\Phi = \mathrm{B_2}$,

$$[X_{\alpha_2}, X_{\alpha_1+\alpha_2}] = \pm(p_{\alpha_2,\alpha_1+\alpha_2} + 1)X_{\alpha_1+2\alpha_2} = \pm 2X_{\alpha_1+2\alpha_2},$$

which is only in L^{short} if $2 = 0$. (So L^{short} is not even a subalgebra otherwise).

Example 2.7. To appreciate the difficulties of various Lie algebras over fields of characteristic 2, consider the Lie algebra $L = \mathfrak{sl}_2(\mathbb{F})$, where $\mathrm{char}(\mathbb{F}) = 2$. This algebra can also be constructed as the Chevalley Lie algebra of type A_1^{sc} over $\mathbb{F}$ (cf. Section 1.9).

The Lie algebra structure on $L = \mathbb{F}e + \mathbb{F}f + \mathbb{F}h$ is determined by a symmetric bilinear form B on L with radical h that satisfies $[x, y] = B(x, y)h$ (for all $x, y \in L$). An interesting consequence of this observation is that apparently the automorphism group of L coincides with the symplectic group on the vector space L.

Here $Z(L) = \mathbb{F}h$ and $L/Z(L)$ is an abelian Lie algebra of dimension 2, so that $\mathrm{Aut}(L/Z(L)) \cong \mathrm{GL}(\mathbb{F}^2)$.

However, the image of $\mathrm{Aut}(L)$ in $\mathrm{Aut}(L/Z(L))$ is isomorphic to $\mathrm{SL}(\mathbb{F}^2)$. The kernel of the natural map $\mathrm{Aut}(L) \to \mathrm{Aut}(L/Z(L))$ consists of linear transformations g of L mapping h to νh and $x \in \mathbb{F}e + \mathbb{F}f$ to $x + \lambda(x)h$, where $\nu \in \mathbb{F}, \nu \neq 0$ and λ is an arbitrary linear functional on $\mathbb{F}e + \mathbb{F}f$. A natural way to rid ourselves of this kernel is to impose that automorphisms preserve the quadratic form κ on L given by

$$\kappa : L \to \mathbb{F}, \qquad \lambda_e e + \lambda_f f + \lambda_h h \mapsto \lambda_e \lambda_f + \lambda_h^2.$$

Note that B is the bilinear form associated to κ, via $B(x, y) = \kappa(x + y) - \kappa(x) - \kappa(y)$. Indeed, the generating long root transformations leave κ invariant and, if $x \in \mathbb{F}e + \mathbb{F}f$, then

$$\kappa(gx) = \kappa(x + \lambda(x)h) = \kappa(x) + \lambda(x)^2\kappa(h) = \kappa(x) + \lambda(x)^2,$$

so that $\lambda(x) = 0$, and

$$\kappa(gh) = \kappa(\nu h) = \nu^2,$$

so that $\nu = 0$. Hence, an element g of the kernel fixes κ if and only if it is the identity. In other words, $\mathrm{Aut}(L/Z(L))_\kappa$ is isomorphic to $\mathrm{SL}(\mathbb{F}^2)$ and hence to $\mathrm{Aut}(L)$.

We finish this example by pointing out that the choice for κ we made is a natural one. The quadratic form arising from the Killing form of $\mathfrak{sl}_2(\mathbb{Z})$ is given by

$$\lambda_e e + \lambda_f f + \lambda_h h \mapsto 8(\lambda_e + \lambda_f + \lambda_h^2),$$

so that $\frac{1}{8}$ of this form is still integral and hence still defined after tensoring with $\mathrm{GF}(2)$, giving the quadratic form κ.

The same phenomenon occurs for B_2, so it is natural to consider $\mathrm{Aut}(L^{\mathrm{short}})_\kappa$, albeit for a different κ. We define $\kappa = 0$ if $\Phi = \mathrm{F}_4$ or $\Phi = \mathrm{G}_2$ and let κ_L be the quadratic form on L defined in Example 2.6, and κ the restriction of κ_L to L^{short}, if $\Phi = \mathrm{B}_2$.

We claim that the action of $\mathrm{Aut}(L)$ can actually be seen on L^{short}.

Lemma 2.8. *Restriction to L^{short} is a group isomorphism $\rho : \mathrm{Aut}(L) \to \mathrm{Aut}(L^{\mathrm{short}})_\kappa$.*

Proof Let $g \in \mathrm{Aut}(L)$. Then g preserves the quadratic form κ_L and κ is its restriction to L^{short}, so the restriction of g to L^{short} lies in $\mathrm{Aut}(L^{\mathrm{short}})_\kappa$. This shows that the homomorphism ρ is well defined, so it remains to prove that ρ is an isomorphism.

To see that ρ is injective, suppose that the restriction of some $g \in G$ to L^{short} is the identity. Then, for all $x \in L$ and $y \in L^{\mathrm{short}}$ we have (since $[x, y] \in L^{\mathrm{short}}$)

$$[x, y] = g[x, y] = [gx, gy] = [gx, y],$$

so $gx - x$ is centralized by each element of L^{short}. Therefore, $gx = x + \lambda_x z$ for some $\lambda_x \in \mathbb{F}$, where $z \in L^{\mathrm{short}}$ spans the center. But now

$$\kappa(x) = \kappa(gx) = \kappa(x + \lambda_x z) = \kappa(x) + (\lambda_x)^2\kappa(z),$$

forcing $\lambda_x = 0$. This means $gx = x$ and thus g is the identity, and ρ is injective.

To see that ρ is surjective, take $h \in \mathrm{Aut}(L^{\mathrm{short}})_\kappa$. The automorphism h induces a unique automorphism $d(h)$ of $\mathrm{Der}(L^{\mathrm{short}})$, given by $d(h)D = h^{-1}Dh$. Let $\mathrm{InnDer}(L^{\mathrm{short}})$ be the inner derivations of L^{short}, i.e., those elements of $\mathrm{Der}(L^{\mathrm{short}})$ that are elements of L^{short}. Clearly, $\mathrm{InnDer}(L^{\mathrm{short}})$ embeds into $\mathrm{Der}(L^{\mathrm{short}})$, and $d(h)$ respects this embedding. Since κ is invariant under h, the bilinear form B is as well. In particular, the Lie algebra

$$\mathrm{Der}(L^{\mathrm{short}})_\kappa = \mathfrak{o}(L^{\mathrm{short}}, B) \cap \mathrm{Der}(L^{\mathrm{short}})_B$$

of elements $D \in \mathrm{Der}(L^{\mathrm{short}})$ with $B(Dx, x) \equiv 0$ is preserved by h. Indeed, for $D \in \mathrm{Der}(L^{\mathrm{short}})_\kappa$ we have, for all $x \in L^{\mathrm{short}}$,

$$B(d(h)Dx, x) = B(h^{-1}Dhx, x) = B(Dhx, hx) = 0,$$

so that $d(h)D \in \mathrm{Der}(L^{\mathrm{short}})_\kappa$. Also, the zeros of B in this algebra are h-invariant, because it is the only codimension one ideal in $\mathrm{Der}(L^{\mathrm{short}})_\kappa$. Hence $d(h)$ leaves invariant a subalgebra of $\mathrm{Der}(L^{\mathrm{short}})_\kappa$ isomorphic to $L/Z(L)$.

Now $d(h)$ pulls back to a unique automorphism of L by a similar argument to the above: the homomorphism assigning to $\vartheta \in \mathrm{Aut}(L)$ the automorphism $\overline{\vartheta} \in \mathrm{Aut}(L/Z(L))$ induced by ϑ is faithful. Indeed, if $\overline{\vartheta}$ is the identity on $L/Z(L)$ then for each $x \in L$ there is a $\lambda_x \in \mathbb{F}$ such that $\vartheta(x) = x + \lambda_x z$. But then

$$\kappa_L(x) = \kappa_L(\vartheta x) = \kappa_L(x + \lambda_x z) = \kappa_L(x) + \lambda_x^2 \kappa_L(z) + \lambda_x B(x, z) = \kappa_L(x) + \lambda_x^2,$$

so that $\lambda_x = 0$, proving ϑ is the identity on L.

This shows that $h \in \mathrm{Aut}(L^{\mathrm{short}})$ induces a unique automorphism of $\mathrm{Der}(L^{\mathrm{short}})$, which we will denote by $d(h)$. Now $d(h)$ induces an automorphism of $L/Z(L)$, and this corresponds to a unique automorphism of L. This proves ρ is surjective on $\mathrm{Aut}(L^{\mathrm{short}})_\kappa$, and thus finishing the proof of the lemma. □

2.5 Two isomorphic Lie algebras

We define $L^{\mathrm{long}} = L/L^{\mathrm{short}}$, so that $\dim(L^{\mathrm{long}}) = 5, 26, 7$ for $\Phi = \mathrm{B}_2, \mathrm{F}_4, \mathrm{G}_2$, respectively. In this section we prove that L^{long} and L^{short} are isomorphic.

To that end, we define a map π from L^{short} to L^{long}, which acts on the basis elements of L^{short} as follows:

$$\pi : L^{\mathrm{short}} \to L^{\mathrm{long}}, \qquad \left\{ \begin{array}{lll} X_\alpha & \mapsto & \varepsilon_\alpha X_{\delta\alpha} + L^{\mathrm{short}} \\ \alpha^\vee & \mapsto & \delta\alpha^\vee + L^{\mathrm{short}} \end{array} \right. ,$$

and is linearly extended to act on the whole of L^{short}. Note that π is the inverse of the map $\mathrm{d}\tau : \mathrm{Lie}(G) \to \mathrm{Lie}(G)$, in the sense that $\mathrm{Im}(\mathrm{d}\tau) = L^{\mathrm{short}}$ and $\mathrm{Ker}(\mathrm{d}\tau) = L^{\mathrm{short}}$, so that $\mathrm{d}\tau$ induces a bijection $L^{\mathrm{long}} \to L^{\mathrm{short}}$.

Lemma 2.9. *The map π is bijective.*

Proof It is immediate that π is injective and surjective, but it is less clear that it is a valid morphism of Lie algebras. So we verify, for α, β short roots:

$$\begin{aligned}[\pi\alpha^\vee, \pi X_\beta] &= \varepsilon_\beta[(\delta\alpha^\vee), X_{\delta\beta}] + L^{\text{short}} \\ &= \varepsilon_\beta\langle\delta\beta, \delta\alpha^\vee\rangle X_{\delta\beta} + L^{\text{short}} \\ &= \varepsilon_\beta\langle\beta, \alpha^\vee\rangle X_{\delta\beta} + L^{\text{short}} \\ &= \pi(\langle\beta, \alpha^\vee\rangle X_\beta) \\ &= \pi[\alpha^\vee, X_\beta].\end{aligned}$$

If $\alpha + \beta$ is not a root then, by Lemma 2.4(iii), neither is $\delta(\alpha) + \delta(\beta)$, so that

$$[\pi X_\alpha, \pi X_\beta] = \varepsilon_\alpha\varepsilon_\beta[X_{\delta\alpha}, X_{\delta\beta}] + L^{\text{short}} = 0 + L^{\text{short}} = \pi(0) = \pi([X_\alpha, X_\beta]).$$

If on the other hand $\alpha + \beta \in \Phi^{\text{long}}$ then $\delta(\alpha + \beta) \in \Phi^{\text{short}}$ and $\delta(\alpha) + \delta(\beta)$ is no root by Lemma 2.4(iv), so that

$$\begin{aligned}[\pi X_\alpha, \pi X_\beta] &= \varepsilon_\alpha\varepsilon_\beta[X_{\delta\alpha}, X_{\delta\beta}] + L^{\text{short}} = 0 + L^{\text{short}} \\ &= \varepsilon_{\alpha+\beta}N_{\alpha,\beta}X_{\delta(\alpha+\beta)} + L^{\text{short}} = \pi([X_\alpha, X_\beta]).\end{aligned}$$

Finally, if $\alpha + \beta \in \Phi^{\text{short}}$ then $\delta(\alpha) + \delta(\beta) = \delta(\alpha + \beta)$ by Lemma 2.4(iv) and

$$\begin{aligned}[\pi X_\alpha, \pi X_\beta] &= \varepsilon_\alpha\varepsilon_\beta[X_{\delta\alpha}, X_{\delta\beta}] + L^{\text{short}} \\ &= \varepsilon_\alpha\varepsilon_\beta N_{\delta\alpha,\delta\beta}X_{\delta\alpha+\delta\beta} + L^{\text{short}} \\ &= \varepsilon_{\alpha+\beta}N_{\alpha,\beta}X_{\delta(\alpha+\beta)} + L^{\text{short}} \\ &= \pi(N_{\alpha,\beta}X_{\alpha+\beta}) \\ &= \pi([X_\alpha, X_\beta]),\end{aligned}$$

using Lemma 2.4(ii). So indeed π is an isomorphism between L^{short} and L^{long}. □

2.6 Viewing τ as endomorphism of $\mathrm{Aut}(L)$

The main result of this chapter is the following proposition, which shows that the automorphism τ of G corresponds to an endomorphism of $\mathrm{Aut}(L)$. Moreover, τ induces a duality on the Lie incidence geometry related to G. The existence of this duality is well known, but we show how it can be understood in terms of the Lie algebra of G (cf. Corollary 2.12).

Proposition 2.10. *Let Φ be a root system of type B_2, F_4, or G_2, and let $\mathbb{F}$ be a perfect field of characteristic 2, 2, or 3, respectively. Let G be the group of Lie type of type ${\mathrm{B}_2}^{\mathrm{ad}}$, F_4, G_2, resp., over $\mathbb{F}$, and let L be the Lie algebra of type ${\mathrm{B}_2}^{\mathrm{sc}}$, F_4, G_2, resp., over $\mathbb{F}$, so that $G < \mathrm{Aut}(L)$. Recall the automorphism $\tau : G \to G$ introduced in Proposition 2.5, the restriction map $\rho : \mathrm{Aut}(L) \to \mathrm{Aut}(L^{\text{short}})_\kappa$ proved to be a group isomorphism in Lemma 2.8, and the homomorphism $\pi : L^{\text{short}} \to L^{\text{long}} = L/L^{\text{short}}$ proved to be bijective in Lemma 2.9.*

The automorphism τ coincides with the endomorphism $g \mapsto \rho^{-1}(\pi^{-1}\overline{g}\pi)$ of G, where $\overline{g}$ denotes the element of $\mathrm{Aut}(L/L^{\mathrm{short}})$ *induced by g.*

Proof Let $g \in G$. We prove that $\rho(\tau(g)) = \pi^{-1}\overline{g}\pi$.

Let α be an arbitrary root and β a short root. We verify that $\pi^{-1}\overline{x_\alpha(t)}\pi X_\beta = \tau(x_\alpha(t))X_\beta$. This suffices to prove the proposition since L^{short} is generated by such X_β by definition and $g \in G$ is determined by its action on L^{short} by Lemma 2.8.

First, we rule out the case where $\alpha = \pm\delta\beta$. If $\alpha = \delta\beta$ then

$$\begin{aligned}\pi^{-1}\overline{x_\alpha(t)}\pi X_\beta &= \pi^{-1}\overline{x_\alpha(t)}(\varepsilon_\beta X_\alpha + L^{\mathrm{short}})\\ &= \pi^{-1}(\varepsilon_\beta X_\alpha + L^{\mathrm{short}})\\ &= \varepsilon_\beta\varepsilon_\alpha X_\beta\\ &= X_\beta\\ &= x_\beta(\varepsilon_\alpha t)X_\beta = \tau x_\alpha(t)X_\beta,\end{aligned}$$

where we use the fact that $\varepsilon_\beta\varepsilon_\alpha = \varepsilon_\beta\varepsilon_{\delta\beta} = 1$ (see Lemma 2.4(i)). If $\alpha = -\delta\beta$ then

$$\begin{aligned}\pi^{-1}\overline{x_\alpha(t)}\pi X_\beta &= \pi^{-1}\overline{x_\alpha(t)}(\varepsilon_\beta X_{-\alpha} + L^{\mathrm{short}})\\ &= \varepsilon_\beta\pi^{-1}(X_{-\alpha} - t\alpha^\vee - t^2X_\alpha + L^{\mathrm{short}})\\ &= \varepsilon_\beta(\varepsilon_{-\alpha}X_\beta + t\beta^\vee - t^2\varepsilon_\alpha X_{\delta\alpha})\\ &= X_\beta + (\varepsilon_\beta t)\beta^\vee - t^2X_{-\beta}\\ &= X_\beta + (\varepsilon_\alpha t)\beta^\vee - (\varepsilon_\alpha t)^2X_{-\beta}\\ &= x_{-\beta}(\varepsilon_\alpha t)X_\beta\\ &= \tau x_\alpha(t)X_\beta,\end{aligned}$$

where we use $\varepsilon_\alpha^2 = \varepsilon_\beta^2 = 1$ and the fact that $\varepsilon_\beta = \varepsilon_{-\delta\beta} = \varepsilon_{-\alpha} = \varepsilon_\alpha$, again by repeatedly applying Lemma 2.4(i).

So assume for the remainder of the proof that $\alpha \neq \pm\delta\beta$ and observe

$$\begin{aligned}\pi^{-1}\overline{x_\alpha(t)}\pi X_\beta &= \pi^{-1}\overline{x_\alpha(t)}\pi\varepsilon_\beta X_{\delta\beta}\\ &= \pi^{-1}\varepsilon_\beta\Big(X_{\delta\beta} + tM^{\#}{}_{\alpha,\delta\beta,1}X_{\alpha+\delta\beta} + t^2M^{\#}{}_{\alpha,\delta\beta,2}X_{2\alpha+\delta\beta}\\ &\quad + t^3M^{\#}{}_{\alpha,\delta\beta,3}X_{3\alpha+\delta\beta} + L^{\mathrm{short}}\Big)\\ &= X_\beta + \varepsilon_\beta\varepsilon_{\alpha+\delta\beta}tM^{\#}{}_{\alpha,\delta\beta,1}X_{\delta(\alpha+\delta\beta)} + \varepsilon_\beta\varepsilon_{2\alpha+\delta\beta}t^2M^{\#}{}_{\alpha,\delta\beta,2}X_{\delta(2\alpha+\delta\beta)}\\ &\quad + \varepsilon_\beta\varepsilon_{3\alpha+\delta\beta}t^3M^{\#}{}_{\alpha,\delta\beta,3}X_{\delta(3\alpha+\delta\beta)},\end{aligned} \tag{2.11}$$

where we take $M^{\#}{}_{\alpha,\beta,j} = M_{\alpha,\beta,j}$ if $j\alpha + \beta$ is a short root, and 0 otherwise, so that in the last expression the contribution of a term to the sum is only counted if the subscripted root γ of the root element X_γ exists and is short.

We first cover the case where $\alpha + \delta\beta$ is not a root. Firstly, note that if $\delta\alpha + \beta$ is not a root either then (2.11) reduces to

$$\pi^{-1}\overline{x_\alpha(t)}\pi X_\beta = X_\beta = \tau x_\alpha(t) X_\beta,$$

since $x_{\delta\alpha}(t)$ acts trivially on X_β. If on the other hand $\delta\alpha+\beta$ is a root, then $N_{\delta\alpha,\beta} \equiv 0 \mod \operatorname{char}(\mathbb{F})$ by Lemma 2.4(iii), so that

$$\begin{aligned}\pi^{-1}\overline{x_\alpha(t)}\pi X_\beta &= X_\beta \\ &= X_\beta + N_{\delta\alpha,\beta} t X_{\delta\alpha+\beta} \\ &= x_{\delta\alpha}(t) X_\beta = \tau x_\alpha(t) X_\beta,\end{aligned}$$

finishing the case where $\alpha+\delta\beta$ is not a root.

Thus the only remaining cases are those where $\alpha+\delta\beta \in \Phi$. We finish the proof by case distinction on $\operatorname{char}(\mathbb{F})$ and on the length of α.

If $\operatorname{char}(\mathbb{F}) = 2$ (implying $\varepsilon \equiv 1$) and α is short then $\alpha+\delta\beta$ is short (so that $M^{\#}{}_{\alpha,\delta\beta,1} = 0$), $2\alpha+\delta\beta$ is long, and $3\alpha+\delta\beta$ is never a root (see Lemma 2.4(vi)). Without loss of generality we reduce to the case where $\beta = \alpha_2$ and α is either α_2 or $-(\alpha_1+\alpha_2)$, which shows that $M_{\alpha,\delta\beta,2} = 1 = N_{\delta\alpha,\beta}$ and $\delta(2\alpha+\delta\beta) = \delta(2\alpha_2+\alpha_1) = \alpha_1+\alpha_2 = \delta\alpha+\beta$. Now (2.11) reduces to

$$\begin{aligned}\pi^{-1}\overline{x_\alpha(t)}\pi X_\beta &= X_\beta + 0 + t^2 M_{\alpha,\delta\beta,2} X_{\delta(2\alpha+\delta\beta)} \\ &= X_\beta + t^2 N_{\delta\alpha,\beta} X_{\delta\alpha+\beta} \\ &= x_{\delta\alpha}(t^2) X_\beta = \tau x_\alpha(t) X_\beta,\end{aligned}$$

as required.

If $\operatorname{char}(\mathbb{F}) = 2$ and α is long then (2.11) implies

$$\begin{aligned}\pi^{-1}\overline{x_\alpha(t)}\pi X_\beta &= X_\beta + t N_{\alpha,\delta\beta} X_{\delta(\alpha+\delta\beta)} \\ &= X_\beta + t N_{\delta\alpha,\beta} X_{\delta\alpha+\beta)} \\ &= x_{\delta\alpha}(t) X_\beta = \tau x_\alpha(t) X_\beta,\end{aligned}$$

by Lemma 2.4(v). This concludes the proof for the case where $\operatorname{char}(\mathbb{F}) = 2$.

If $\operatorname{char}(\mathbb{F}) = 3$ and α is short then $\alpha+\delta\beta \in \Phi^{\text{short}}$, $2\alpha+\delta\beta \in \Phi^{\text{short}}$, and $3\alpha+\delta\beta \in \Phi^{\text{long}}$ (see Lemma 2.4(vi)). Without loss of generality, fix $\beta = \alpha_1$. Then $\alpha = \alpha_1$ or $\alpha = -(\alpha_1+\alpha_2)$. For the case where $\alpha = \beta = \alpha_1$, observe

$$\begin{aligned}\varepsilon_\beta \varepsilon_{3\alpha+\delta\beta} M_{\alpha,\delta\beta,3} &= \varepsilon_{\alpha_1}\varepsilon_{3\alpha_1+\alpha_2} \cdot \frac{1}{6} N_{\alpha_1,\alpha_2} N_{\alpha_1,\alpha_1+\alpha_2} N_{\alpha_1,2\alpha_1+\alpha_2} \\ &= \eta_1\eta_2 \cdot \frac{1}{6}\varepsilon_1 \cdot 2\varepsilon_2 \cdot 3\varepsilon_3 \\ &= \eta_1(-\varepsilon_2\varepsilon_3) \cdot \varepsilon_1\varepsilon_2\varepsilon_3 \\ &= \eta_1 \cdot -\varepsilon_1 \\ &= \varepsilon_\alpha N_{\alpha_2,\alpha_1} = \varepsilon_\alpha N_{\delta\alpha,\beta}.\end{aligned}$$

(See Table 1.51 for the values of N.) For the case where $\beta = \alpha_1$ and $\alpha = -\alpha_1-\alpha_2$, we similarly observe that

$$\begin{aligned}
\varepsilon_\beta \varepsilon_{3\alpha+\delta\beta} M_{\alpha,\delta\beta,3} &= \varepsilon_{\alpha_1}\varepsilon_{-\alpha_1-\alpha_2} \cdot \frac{1}{6} N_{-\alpha_1-\alpha_2,\alpha_2} N_{-\alpha_1-\alpha_2,-\alpha_1} N_{-\alpha_1-\alpha_2,-2\alpha_1-\alpha_2} \\
&= \eta_1\eta_3 \cdot \frac{1}{6} - \varepsilon_1 \cdot 2\varepsilon_2 \cdot 3\varepsilon_1\varepsilon_3\varepsilon_4 \\
&= \varepsilon_3\varepsilon_4 \cdot -\varepsilon_2\varepsilon_3\varepsilon_4 \\
&= -\varepsilon_2\varepsilon_3\varepsilon_3 \\
&= \eta_2\varepsilon_3 = \varepsilon_\alpha N_{\alpha_2,\alpha_1} = \varepsilon_\alpha N_{\delta\alpha,\beta}.
\end{aligned}$$

So both for $\alpha = \alpha_1$ and $\alpha = -\alpha_1 - \alpha_2$ we find that (2.11) reduces to

$$\begin{aligned}
\pi^{-1}\overline{x_\alpha(t)}\pi X_\beta &= X_\beta + 0 + 0 + \varepsilon_\beta\varepsilon_{3\alpha+\delta\beta} t^3 M_{\alpha,\delta\beta,3} X_{\delta(3\alpha+\delta\beta)} \\
&= X_\beta + \varepsilon_\alpha t^3 N_{\delta\alpha,\beta} X_{\delta(3\alpha+\delta\beta)} \\
&= x_{\delta\alpha}(\varepsilon_\alpha t^3) X_\beta = \tau x_\alpha(t) X_\beta,
\end{aligned}$$

finishing the case where char($\mathbb{F}$) $= 3$ and α is short.

If char($\mathbb{F}$) $= 3$ and α is long then first assume $\alpha + \delta\beta$ is not a root. Then both $\pi^{-1}\overline{x_\alpha(t)}\pi$ and $x_{\delta\alpha}(t)$ fix X_β. So assume $\alpha + \delta\beta$ is a root. Then it is a long root, and $2\alpha + \delta\beta$ and $3\alpha + \delta\beta$ are not roots by Lemma 2.4(v). Without loss of generality we may assume $\beta = \alpha_1$, so that $\alpha = 3\alpha_1 + \alpha_2$ or $\alpha = -3\alpha_1 - 2\alpha_2$. If $\alpha = 3\alpha_1 + \alpha_2$, observe

$$\begin{aligned}
\varepsilon_\beta\varepsilon_{\alpha+\delta\beta} M_{\alpha,\delta\beta,1} &= \varepsilon_{\alpha_1}\varepsilon_{3\alpha_1+2\alpha_2} N_{3\alpha_1+\alpha_2,\alpha_2} \\
&= \eta_1\eta_3 \cdot -\varepsilon_4 \\
&= -\varepsilon_2\varepsilon_3 \cdot \varepsilon_2 \\
&= \eta_2 \cdot -\frac{1}{2} N_{\alpha_1+\alpha_2,\alpha_1} \\
&= \varepsilon_\alpha N_{\delta\alpha,\beta},
\end{aligned}$$

where the last equation uses that char($\mathbb{F}$) $= 3$. Similarly, if $\alpha = -3\alpha_1 - 2\alpha_2$, observe

$$\begin{aligned}
\varepsilon_\beta\varepsilon_{\alpha+\delta\beta} M_{\alpha,\delta\beta,1} &= \varepsilon_{\alpha_1}\varepsilon_{-3\alpha_1-\alpha_2} N_{-3\alpha_1-2\alpha_2,\alpha_2} \\
&= \eta_1 \cdot \eta_2 \cdot \varepsilon_4 \\
&= \eta_3\varepsilon_3\varepsilon_4 \cdot -\varepsilon_2\varepsilon_3 \cdot \varepsilon_4 \\
&= \eta_3 \cdot 2\varepsilon_2 \\
&= \varepsilon_\alpha \cdot N_{-2\alpha_1-\alpha_2,\alpha_1} = \varepsilon_\alpha \cdot N_{\delta\alpha,\beta},
\end{aligned}$$

again explicitly using that char($\mathbb{F}$) $= 3$.

So both for $\alpha = 3\alpha_1 + \alpha_2$ and $\alpha = -3\alpha_1 - 2\alpha_2$ this implies that (2.11) reduces to

$$\begin{aligned}\pi^{-1}\overline{x_\alpha(t)}\pi X_\beta &= X_\beta + \varepsilon_\beta \varepsilon_{\alpha+\delta\beta} t M_{\alpha,\delta\beta,1} X_{\delta(\alpha+\delta\beta)} \\ &= X_\beta + \varepsilon_\alpha t N_{\delta\alpha,\beta} X_{\delta\alpha+\beta} \\ &= x_{\delta\alpha}(\varepsilon_\alpha t) X_\beta = \tau x_\alpha(t) X_\beta,\end{aligned}$$

concluding the case where $\mathrm{char}(\mathbb{F}) = 3$ and α is long, and therefore the proof of the proposition. □

We conclude from this proposition that the following sequence is exact:

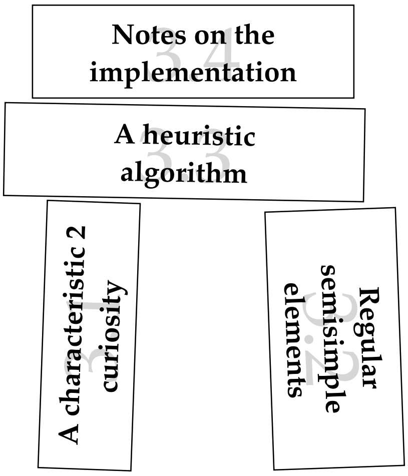
$$0 \longrightarrow L^{\text{short}} \longrightarrow L \longrightarrow L^{\text{short}} \longrightarrow 0,$$

where the second arrow is simply the embedding of L^{short} into L, and the third arrow is $\mathrm{d}\tau$.

Finally, we observe that the elements of L form a geometry in the following manner. We define $\mathcal{P} = \{\mathbb{F}X_\alpha \mid \alpha \in \Phi^{\text{short}}\}^G$ and $\mathcal{L} = \{\mathbb{F}X_\beta \mid \beta \in \Phi^{\text{long}}\}^G$. (In the case where $\Phi = \mathrm{B}_2$ or $\Phi = \mathrm{G}_2$, the elements of $\mathcal{P}$ correspond to points and those of $\mathcal{L}$ to lines.) For $p_\alpha = \mathbb{F}X_\alpha \in \mathcal{P}$ and $l_\beta = \mathbb{F}X_\beta \in \mathcal{L}$, we take p_α incident with l_β (denoted by $p_\alpha * l_\beta$) if and only if $X_\alpha \in [X_\beta, L^{\text{short}}]$.

Corollary 2.12. *The automorphism τ of G induces a duality of $(\mathcal{P}, \mathcal{L})$.*

Proof In Proposition 2.10 we have established that τ acts on the entirety of $\mathcal{P}$ and $\mathcal{L}$. The fact that the incidence is invariant under τ follows easily by inspection of the appropriate root systems. □


Notes on the implementation
3.4
A heuristic algorithm
3.3
A characteristic 2 curiosity
3.1
Regular semisimple elements
3.2

3 Split Toral Subalgebras

Recall from Section 1.7.1 that a toral subalgebra of a Lie algebra over a field $\mathbb{F}$ is an abelian subalgebra containing only semisimple elements, and it is called split if the characteristic roots of all its elements are in $\mathbb{F}$. Furthermore, a subalgebra H of a Lie algebra L is called a *Cartan subalgebra* if it is nilpotent and $H = \mathrm{N}_L(H)$. Recall from Lemma 1.40 that toral subalgebras and Cartan subalgebras are very closely related. In this chapter we study the problem of computing split toral subalgebras of Lie algebras of split simple algebraic groups over a finite field $\mathbb{F}$.

In the case that $\mathbb{F}$ is not of characteristic 2 or 3 a Las Vegas algorithm exists, due to Cohen and Murray [CM09, Lemma 5.7]. Independently, Ryba developed a Las Vegas algorithm for computing split Cartan subalgebras [Ryb07]. Unfortunately, Ryba also excludes characteristic 2 and, if the Lie algebra is of type A_2 or G_2, characteristic 3. It is, however, claimed that the algorithm may work in some cases in characteristic 2, but not in all cases (cf. [Ryb07, Section 9.3]). These two algorithms employ a similar recursive procedure: they descend into Lie algebras of type A_1 and lift split toral subalgebras of those Lie algebras to the original Lie algebra.

We first remark that the troublesome characteristic 3 cases that Ryba excludes are precisely those occurring in Table 4.4 in the next chapter. The problems arising there may be remedied by some minor modifications to his algorithms. This modification is based on the observation that the product of two random elements of opposite 3-dimensional eigenspaces is often a split semisimple element. We will not go into this problem any further.

In this chapter we consider the problem of finding split toral subalgebras over fields of characteristic 2. In Section 3.1 we investigate a special instance where a split toral subalgebra is not contained in a split toral subalgebra of maximal dimension. In Section 3.2 we study the presence of regular semisimple elements in Lie algebras over fields of characteristic 2, showing that the Las Vegas algorithm by Cohen and Murray cannot easily be applied in those cases. In Sections 3.3 and 3.4 we describe a heuristic algorithm to find split maximal toral subalgebras in Lie algebras over fields of characteristic 2, inspired by the algorithm by Cohen and Murray.

3.1 A characteristic 2 curiosity

For the development of a recursive algorithm for finding split maximal toral subalgebras it would be very useful to know that every split toral subalgebra is contained in a split maximal toral subalgebra (i.e., a toral subalgebra of maximal dimension that is split). The algorithm by Cohen and Murray relies on a similar (but weaker) assertion (cf. [CM09, Proposition 5.8]). This is, however, not in general true in characteristic 2, as we will show in the following example.

We consider the Chevalley Lie algebra L of type $\mathrm{C}_4^{\mathrm{sc}}$ over $\mathrm{GF}(2)$, with root datum $R = (X, \Phi, Y, \Phi^\vee)$ and Chevalley basis elements $\{X_\alpha, h_i \mid \alpha \in \Phi, i \in \{1, \dots, 4\}\}$. Furthermore, we denote the simple roots of Φ by $\alpha_1, \dots, \alpha_4$, so that its non-simple positive roots are

$$\begin{aligned} \alpha_5 = (1,1,0,0), \alpha_6 = (0,1,1,0), \alpha_7 = (0,0,1,1), \alpha_8 = (1,1,1,0),\\ \alpha_9 = (0,1,1,1), \alpha_{10} = (0,0,2,1), \alpha_{11} = (1,1,1,1), \alpha_{12} = (0,1,2,1),\\ \alpha_{13} = (1,1,2,1), \alpha_{14} = (0,2,2,1), \alpha_{15} = (1,2,2,1), \alpha_{16} = (2,2,2,1), \end{aligned}$$

where (c_1, c_2, c_3, c_4) denotes $c_1\alpha_1 + c_2\alpha_2 + c_3\alpha_3 + c_4\alpha_4$ and the negative roots are defined accordingly. Now let

$$\begin{aligned} y_1 &= h_1 + h_3 \in \mathrm{Z}(L),\\ y_2 &= h_1 + X_{\alpha_{12}} + X_{-\alpha_8},\\ y_3 &= h_2 + X_{\alpha_3} + X_{-\alpha_3} + X_{\alpha_{15}} + X_{-\alpha_{15}}, \end{aligned}$$

and $H = \langle y_1, y_2, y_3 \rangle_L$.

Proposition 3.1. *The subalgebra H is a 3-dimensional split toral subalgebra of L. However, there does not exist a split toral subalgebra H' of L of dimension 4 such that $H \subsetneq H'$.*

Proof It is straightforward to verify that H is a split toral subalgebra of L: on diagonalization of H in the adjoint representation we obtain 3 eigenspaces of dimension 8 (corresponding to roots $(0,1,0)$, $(0,0,1)$, and $(0,1,1)$) and an eigenspace L_0 of dimension 12 (corresponding to the root $(0,0,0)$ and H itself).

Now suppose there exists a split toral subalgebra H' of dimension 4 containing H. This would imply the existence of a $y \in H'$ such that $y \notin H$ and $[y, H] = 0$. Furthermore, by the structure of the root spaces of L (proved in Proposition 4.2 in the next Chapter, see Table 4.4), diagonalization with respect to H' would give 6 eigenspaces of dimension 4, and one eigenspace L_0' of dimension 12 (where $H' \subseteq L_0'$). This means in particular that $L_0 = L_0'$ and that y should have a unique eigenvalue on L_0. Since $[y, H] = 0$ and $H \subseteq L_0$, the eigenvalue of y on L_0 must be 0, and thus $y \in \mathrm{C}_{H'}(L_0)$, implying $y \in \mathrm{C}_L(L_0)$.

However, $\mathrm{C}_L(L_0)$ is 4-dimensional and $y_1, y_2, y_3 \in \mathrm{C}_L(L_0)$, so that (modulo linear combinations of y_1, y_2, y_3, and up to scalar multiples) there is only one choice for y:

$$y = h_3 + h_4 + X_{\alpha_3} + X_{\alpha_9} + X_{\alpha_{12}} + X_{-\alpha_3} + X_{-\alpha_5}.$$

Because the characteristic polynomial of ad_y is equal to $x^{16}(x+1)^4(x^2+x+1)^8$, we see that y is not split, and that therefore H' is not a split toral subalgebra: a contradiction. □

In the standard representation of L in terms of 8×8 matrices in $\mathfrak{sp}_8(\mathrm{GF}(2))$, we have (the entries equal to 0 have been omitted in order to expose the structure of the matrices more clearly):

$$y_1 = \begin{pmatrix} 1 &&&&&&& \\ & 1 &&&&&& \\ && 1 &&&&& \\ &&& 1 &&&& \\ &&&& 1 &&& \\ &&&&& 1 && \\ &&&&&& 1 & \\ &&&&&&& 1 \end{pmatrix}, \quad y_2 = \begin{pmatrix} 1 &&& 1 &&&& \\ & 1 &&&&&& \\ &&&&&&& \\ &&&&&&& \\ &&&&&&& 1 \\ & 1 &&&&&& \\ && 1 &&&& 1 & \\ &&&&&&& 1 \end{pmatrix},$$

$$y_3 = \begin{pmatrix} &&&&&& 1 & \\ & 1 &&&&&& 1 \\ && 1 & 1 &&&& \\ && 1 &&&&& \\ &&&&& 1 && \\ &&&& 1 & 1 && \\ 1 &&&&&& 1 & \\ & 1 &&&&&& \end{pmatrix}.$$

Their characteristic polynomials are $(x+1)^8$, $x^4(x+1)^4$, and $(x^2+x+1)^4$, respectively. In the adjoint representation, however, their characteristic polynomials are x^{36}, $x^{20}(x+1)^{16}$, and $x^{20}(x+1)^{16}$, respectively. This leaves us in the interesting situation where no field extension is needed to diagonalize H in the adjoint representation, but a quadratic field extension is needed to diagonalize H in $\mathfrak{sp}_8$.

We note that H is inside a 4-dimensional split toral subalgebra of L over a quadratic extension of $\mathbb{F}$. Let ξ be a primitive element of $\mathrm{GF}(2^2)$, and take $H' = \langle y_1, y_2, y_3, y \rangle_L$ (where y is as in the proof of Proposition 3.1). Now H' is a split toral subalgebra of L, so that we can compute a Chevalley basis with respect to H'. Furthermore, we can find (using generalized row reduction [CMT04]) an element τ of the corresponding group of Lie type that maps the original Chevalley basis to this new one:

$$\begin{aligned} \tau = {} & x_4(\xi)x_7(\xi)x_9(\xi^2)x_{12}(1)x_{15}(\xi^2)x_3(\xi^2) \cdot (1,1,1,\xi^2) \cdot \\ & n_1n_2n_3n_2n_1n_4n_3n_2n_1n_4n_3n_2n_4n_3 \cdot x_9(\xi^2)x_{11}(1)x_{13}(1)x_1(\xi^2). \end{aligned}$$

3.2 Regular semisimple elements

In [CM09] Cohen and Murray describe an algorithm for Lang's theorem, which needs an algorithm to find split maximal toral subalgebras of Lie algebras. Although they do not claim their algorithm is valid in the characteristic 2 case, some propositions are. We shall first introduce the concept of regular semisimple elements in order to expose some of the difficulties in characteristic 2.

An element x of a Lie algebra L is called *regular semisimple* if its centralizer $\mathrm{C}_L(x)$ is a maximal toral subalgebra. We denote the set of regular semisimple elements of L by L_{rss}. Moreover, if L is the Lie algebra of a group of Lie type with root datum R we let $L_{\mathrm{rss},w}$ be the set of elements $x \in L_{\mathrm{rss}}$ for which there exists a $g \in G$ such

	GF(2)		GF(2^2)		GF(2^3)		GF(3)		GF(5)		GF(7)	
	$\|H\|$	$\|H_{\text{rss}}\|$	$\|H\|$	$\|H_{\text{rss}}\|$	$\|H\|$	$\|H_{\text{rss}}\|$	$\|H\|$	$\|H_{\text{rss}}\|$	$\|H\|$	$\|H_{\text{rss}}\|$	$\|H\|$	$\|H_{\text{rss}}\|$
$\mathrm{A_1}^{\mathrm{sc}}$	2	0	4	0	8	0	3	2	5	4	7	6
$\mathrm{A_1}^{\mathrm{ad}}$	2	1	4	3	8	7	3	2	5	4	7	6
$\mathrm{A_2}^{\mathrm{sc}}$	4	0	16	6	64	42	9	6	25	12	49	30
$\mathrm{A_2}^{\mathrm{ad}}$	4	0	16	6	64	42	9	2	25	12	49	30
$\mathrm{A_3}^{\mathrm{sc}}$	8	0	64	24	512	336	27	0	125	24	343	120
$\mathrm{A}_3^{(2)}$	8	0	64	24	512	336	27	0	125	24	343	120
$\mathrm{A_3}^{\mathrm{ad}}$	8	0	64	6	512	210	27	0	125	24	343	120
$\mathrm{A_4}^{\mathrm{sc}}$	16	0	256	0	4096	840	81	0	625	120	2401	360
$\mathrm{A_4}^{\mathrm{ad}}$	16	0	256	0	4096	840	81	0	625	24	2401	360
$\mathrm{B_2}^{\mathrm{sc}}$	4	0	16	0	64	0	9	0	25	8	49	24
$\mathrm{B_2}^{\mathrm{ad}}$	4	0	16	6	64	42	9	0	25	8	49	24
$\mathrm{B_3}^{\mathrm{sc}}$	8	0	64	24	512	336	27	0	125	0	343	48
$\mathrm{B_3}^{\mathrm{ad}}$	8	0	64	6	512	210	27	0	125	0	343	48
$\mathrm{B_4}^{\mathrm{sc}}$	16	0	256	0	4096	1344	81	0	625	0	2401	0
$\mathrm{B_4}^{\mathrm{ad}}$	16	0	256	0	4096	840	81	0	625	0	2401	0
$\mathrm{C_3}^{\mathrm{sc}}$	8	0	64	0	512	0	27	0	125	0	343	48
$\mathrm{C_3}^{\mathrm{ad}}$	8	0	64	0	512	168	27	0	125	0	343	48
$\mathrm{C_4}^{\mathrm{sc}}$	16	0	256	0	4096	0	81	0	625	0	2401	0
$\mathrm{C_4}^{\mathrm{ad}}$	16	0	256	0	4096	336	81	0	625	0	2401	0
$\mathrm{D_4}^{\mathrm{ad}}$	16	0	256	6	4096	546	81	0	625	0	2401	192
$\mathrm{D_4}^{\mathrm{sc}}$	16	0	256	96	4096	2688	81	0	625	0	2401	192
$\mathrm{F_4}^{\mathrm{ad}}$	16	0	256	0	4096	0	81	0	625	0	2401	0
$\mathrm{G_2}^{\mathrm{ad}}$	4	0	16	6	64	42	9	0	25	0	49	12

Table 3.2: Counting regular semisimple elements in split maximal toral subalgebras

that $\mathrm{C}_L(x) = H_0^g$ and $g^F g^{-1} \in T_0 \dot{w}$, where T_0 is the standard split maximal torus and $H_0 = \mathrm{Lie}(T_0)$ the corresponding split maximal toral subalgebra. In this section we are primarily interested in split toral subalgebras, hence in $L_{\mathrm{rss,id}}$.

The time analysis in [CM09] uses the fact that a significant fraction of the elements in the Lie algebra is regular semisimple. In the following proposition we show that this is not always true over fields of characteristic 2.

Proposition 3.3. *Let $\mathbb{F}$ be a field of characteristic* 2*, let R be a root datum of type* $\mathrm{A}_1{}^{\mathrm{sc}}$*,* $\mathrm{B}_2{}^{\mathrm{sc}}$*, or* $\mathrm{C}_n{}^{\mathrm{sc}}$ *(where $n \geq 3$), and let L be the Lie algebra of type R over $\mathbb{F}$. There exist no regular semisimple elements in L.*

Proof We refer to Proposition 4.2 and Table 4.4 in the next chapter, were it is shown that in the cases mentioned the 0-eigenspace of a split toral subalgebra contains some of the root spaces. This in particular implies that if H is a split maximal toral subalgebra of L then $H \subsetneq \mathrm{C}_L(H)$.

So suppose $x \in L_{\mathrm{rss,id}}$, so that $\mathrm{C}_L(x) = H$, for some split maximal toral subalgebra H of L. However, $x \in H$ since $x \in \mathrm{C}_L(x)$, so that $\mathrm{C}_L(x) \supseteq \mathrm{C}_L(H) \supsetneq H$, a contradiction. □

This shows that in some cases in characteristic 2 there is a complete absence of regular semisimple elements. In other cases in characteristic 2, however, regular semisimple elements are scarce as well. In Table 3.2 we show the results of explicitly counting regular semisimple elements. For each of 23 Chevalley Lie algebras L, and each of 6 fields $\mathbb{F}$, this table shows in the first column the number of elements in a split maximal toral subalgebra H, and in the second column the number of those that are regular semisimple.

From Table 3.2 we conclude that over the field with 2 elements there are almost no semisimple elements, regardless of the type of the Lie algebra. Moreover, even over small fields of odd characteristic the number of regular semisimple elements with a split centralizer may be small, or even 0.

3.3 A heuristic algorithm

Proposition 3.3 indicates that the approach for finding split maximal toral subalgebras described by Cohen and Murray [CM09, Section 5] will not in general work in the cases covered by the proposition: there do not exist enough regular semisimple elements in the Lie algebra. Moreover, that algorithm strongly relies on the fact that root spaces are 1-dimensional, something that is not true over characteristic 2 as shown in Proposition 4.2 (in Section 4.2).

Ryba explicitly notes [Ryb07, Section 9] that the algorithm he describes is not easily extended to work over fields of characteristic 2, largely because of similar problems. Finally, the counterexample in Section 3.1 suggests that algorithms for finding split maximal toral subalgebras run the risk of descending into a split toral subalgebra that is not in a split toral subalgebra of maximal dimension.

In this section we describe a heuristic Las Vegas type algorithm for finding split maximal toral subalgebras in characteristic 2. Unfortunately, we have no bound

```
FindSplitSemisimpleElt
in:     An eigenspace $V$ of a semisimple element of the Lie algebra $M \subseteq L$,
out:    A split semisimple element $h \in M$, or fail.
begin
  let $S = \langle V \rangle_M$ be the subalgebra of $M$ generated by $V$,
  let $I = (V)_M$ be the ideal of $M$ generated by $V$,
  if $\dim([S,S]) = 1$ then
    /* Case (A) */
    let $h \in [S,S]$ be such that $[S,S] = \langle h \rangle_{\mathbb{F}}$.
  else if $[I,I] = I$ and $\dim([S,S]) \in \{2,3\}$ then
    /* Case (B) */
    let $h$ be a random non-zero element of $[S,S]$.
  else if $\dim(I) \neq 0$ and $\dim(I)$ is even and $\dim([I,I]) = 0$
    and $\dim([S,S]) = 0$ then
    /* Case (C) */
    find an $h \in M$ such that $[h,e] = e$ for all $e \in I$.
  else if $\dim(S) = 6$ and $[I,I] = S$ and $\dim([S,S]) = 2$ then
    /* Case (D) */
    let $h$ be a random non-zero element of $[S,S]$.
  else if $\dim(I) \neq 0$ and $\dim(I)$ is even and $\dim([I,I]) \neq 0$
    and $\dim([S,S]) = 0$ then
    /* Case (E) */
    find an $h \in I$ such that $[h,e] = e$ for all $e \in S$.
  else if $\dim(V)$ is even and $\dim([S,S]) \neq 0$ then
    /* Case (F) */
    let $h$ be a random non-zero element of $[S,S]$
  end if,
  if $h$ is defined and $h$ pulls back to split semisimple elements in $L$ then
    return h.
  else
    return fail.
  end if.
end
```

Algorithm 3.4: Finding a split semisimple element in an eigenspace

```
SplitMaximalToralSubalgebra
in:     A Lie algebra $L$ over a finite field $\mathbb{F}$ of characteristic 2,
out:    A split maximal toral subalgebra $H$ of $L$.
begin
  let $M = L$, $H = 0$,
  while $M \neq 0$ do
    if $\dim(Z(M)) > 0$ then
      /* Take out the center */
      if $Z(M)$ is split semisimple then let $H = H \cup Z(M)$.
      let $M = M/Z(M)$.
    else
      /* Try to find a new element of $H$ */
      let $h'$ be a random non-zero semisimple element of $M$,
      if $h'$ is split semisimple in $L$ then
        let $h = h'$.
      else
        /* Use this $h'$ as input for FindSSElt */
        for each eigenvalue $v$ of $h'$ do
          let $V$ be the $v$-eigenspace of $h'$,
          let $h =$ FindSplitSemisimpleElt($V$, $M$, $L$),
          if $h \neq$ fail then break.
        end for,
      end if,
      if $h \neq$ fail then
        let $H = H \cup h$,
        let $M = C_M(h)/(h)_M$.
      end if.
    end if.
  end while.
end
```

Algorithm 3.5: Finding a split maximal toral subalgebra

on the probability that it completes successfully, and therefore no estimate of the runtime. However, we do provide the intuition behind the design of the algorithm (in the remainder of this section) and we show that the implementation is successful (we give timings in Section 3.4).

For the remainder of this section we let L be the Lie algebra of a split simple algebraic group defined over a finite field $\mathbb{F}$ of characteristic 2, and we assume L to be given as a structure constant algebra. The goal of the algorithm described is to find a split maximal toral subalgebra H of L.

The general principle is given in Algorithm 3.5. This algorithm repeatedly tries to find a split semisimple element $h \in M$ (initially $M = L$), and then recursively continues the search in $\mathrm{C}_M(h)/(h)_M$. It attempts to find such split semisimple elements by taking a random non-zero semisimple element h', and producing a random split semisimple element using suitable eigenspaces of h'. The latter process is described in Algorithm 3.4.

In order to clarify Algorithm 3.4 we let R be an irreducible root datum, $\mathbb{F}$ a field of characteristic 2, and L the Lie algebra of type R over $\mathbb{F}$. Furthermore, we let H be the standard split maximal toral subalgebra of L, and recall the definition of *roots of H on L* from Section 1.9.1. Observe first of all that, since $\mathrm{char}(\mathbb{F}) = 2$, the root spaces L_α and $L_{-\alpha}$ coincide for all $\alpha \in \Phi$. This implies that $\alpha^\vee \in [L_\alpha, L_\alpha]$, prompting us to consider $[S, S]$ in line 4 of Algorithm 3.4.

We justify the choices for the various other cases in this algorithm using the data in Table 3.6. In the first column that table contains the root data R that we will prove have multidimensional root spaces over fields of characteristic 2 (see Proposition 4.2 in the following chapter). For each of these the dimensions and multiplicities, in the same notation used in Table 4.4, are shown in the second column labeled Mult. To clarify the other columns we let V be one of the eigenspaces mentioned (e.g., for the eighth line of the table $L = \mathrm{B}_n{}^{\mathrm{ad}}(\mathbb{F})$ and V is one of the 4-dimensional (long) root spaces). Then we let $S = \langle V \rangle_L$ be the subalgebra generated by V and $I = (V)_L$ the ideal generated by V. Now the third column contains the dimension of S, the fourth column the dimension of $[S, S]$ and the fifth the dimension of $[S, S] \cap H$. The sixth column contains the dimension of I, or "L" if $I = L$, or "$L - 1$" if I is a codimension one ideal of L, and the seventh column contains the dimension of $[I, I]$, or "I" if $[I, I] = I$. Finally, the eighth column shows which of the cases of Algorithm 3.4 is based on this type of root space.

The case distinction in Algorithm 3.4 is based on the observations in Table 3.6 in the following manner.

(A) In each of the cases where $\dim([S, S]) = 1$ we have $[S, S] \subseteq H$, prompting us to take h to be a basis element of $[S, S]$. Note that this case also applies if V corresponds to the direct sum of several Lie algebras of type $\mathrm{A}_1{}^{\mathrm{sc}}$.

(B) In the cases where $[I, I] = I$ and $\dim([S, S]) \in \{2, 3\}$ we also have $[S, S] \subseteq H$, so that a random non-zero element of $[S, S]$ seems a good candidate.

(C) In the cases where $\dim([I, I]) = \dim([S, S]) = 0$ the best candidate we can find is an element $h \in M$ that acts on I as a split semisimple element should. Note that this case also applies if V corresponds to the direct sum of several Lie algebras of type $\mathrm{A}_1{}^{\mathrm{ad}}$.

R	Mult	S	$[S,S]$	$[S,S]\cap H$	I	$[I,I]$	Soln
$\mathrm{A_1}^{\mathrm{ad}}$	2	2	0	0	2	2	(C)
$\mathrm{A_1}^{\mathrm{sc}}$	**2**	3	1	1	3	1	(A)
$\mathrm{A_3}^{\mathrm{sc}}$	4^3	6	2	2	L	I	(B)
$\mathrm{A}_3^{(2)}$	4^3	5	1	1	$L-1$	I	(A)
$\mathrm{B_2}^{\mathrm{ad}}$	2^2	2	0	0	4	0	(C)
$\lfloor$	4	5	1	1	9	5	(A)
$\mathrm{B}_n{}^{\mathrm{ad}}$ $(n \geq 3)$	2^n	2	0	0	$2n$	0	(C)
$\lfloor$	$4^{\binom{n}{2}}$	5	1	1	$L-1$	I	(A)
$\mathrm{B_2}^{\mathrm{sc}}$	**4**	6	2	2	L	6	(D)
$\lfloor$	4	5	1	1	5	1	(A)
$\mathrm{B_3}^{\mathrm{sc}}$	6^3	8	2	2	L	I	(B)
$\mathrm{B_4}^{\mathrm{sc}}$	2^4	3	1	1	9	1	(A)
$\lfloor$	8^3	11	3	3	L	I	(B)
$\mathrm{B}_n{}^{\mathrm{sc}}$ $(n \geq 5)$	2^n	3	1	1	$2n+1$	1	(A)
$\lfloor$	$4^{\binom{n}{2}}$	6	2	2	L	I	(B)
$\mathrm{C}_n{}^{\mathrm{ad}}$ $(n \geq 3)$	$2n$	$3n-1$	$n-1$	$n-1$	L		(F)
$\lfloor$	$2^{n(n-1)}$	3	1	1		I	(A)
$\mathrm{C}_n{}^{\mathrm{sc}}$ $(n \geq 3)$	**2n**	$3n$	n	n	L		(F)
$\lfloor$	$4^{\binom{n}{2}}$	5	1	1		I	(A)
$\mathrm{D_4}^{\mathrm{sc}}$	8^3	11	3	3	L	I	(B)
$\mathrm{D}_4^{(1),(n),(n-1)}$	4^6	5	1	1	$L-1$	I	(A)
$\mathrm{D}_n{}^{\mathrm{sc}}$ $(n \geq 5)$	$4^{\binom{n}{2}}$	6	2	2	L	I	(B)
$\mathrm{D}_n^{(1)}$ $(n \geq 5)$	$4^{\binom{n}{2}}$	5	1	1	$L-1$	I	(A)
$\mathrm{F_4}$	2^{12}	3	1	1	26	I	(A)
$\lfloor$	8^3	11	3	3	L	I	(B)
$\mathrm{G_2}$	4^3	5	1	1	L	I	(A)

Table 3.6: Eigenspaces, their subalgebras, and their ideals in characteristic 2

(D) In the cases where $\dim(S) = 6$ (prime example being the long roots in ${B_2}^{sc}$) we also pick a random non-zero element of $[S, S]$ as candidate.

(E) This case is special since it does not occur in Table 3.6. It is however needed to successfully complete the search for a split maximal toral subalgebra if L is of type ${C_n}^{sc}$. The solution is similar to that of case (C).

(F) This case is needed for Lie algebras of type C_n, where again $[S, S] \subseteq H$, but the dimension of $[S, S]$ can be as large as $\dim(H)$. Again, we pick a random non-zero element of $[S, S]$ as candidate.

3.4 Notes on the implementation

From the manner in which Algorithm 3.5 is specified we can conclude that SplitMaximalToralSubalgebra may run for an infinite time. Indeed, M only decreases in dimension if a new split semisimple element is found and such an element does not always exist, as shown in Section 3.1. Also, in many cases the algorithm FindSplitSemisimpleElt, used by SplitMaximalToralSubalgebra, will fail to return a split semisimple h, due to the simple fact that S is not of a suitable type or the candidate h turns out not to be split. In the implementation of this algorithm these problems are remedied by limiting the number of random tries allowed for each M in line 7 of SplitMaximalToralSubalgebra to some finite number. If after that number of tries no new H was found, the algorithm terminates and reports failure.

The influence of the size of the field on the performance of the algorithm is twofold. Firstly, the smaller the field, the higher the probability of finding split semisimple elements in Algorithm 3.4. On the other hand, the bigger the field, the higher the probability that the random semisimple elements picked in Algorithm 3.5 have eigenspaces of small dimension. This dichotomy yields an algorithm whose performance is acceptable both over small and over larger fields.

We present timings of runs of the SplitMaximalToralSubalgebra algorithm on Lie algebras of split simple algebraic groups over fields of characteristic 2. In every case the algorithm was run repeatedly until successful completion. In Table 3.7 and in Figure 3.8, the algorithm was run for Lie algebras up to rank 8, over fields of size 2, 2^6, and 2^{10}. In Figure 3.9 the algorithm was run for the Lie algebras of 7 different root data, varying the size of the field between 2 and 2^{20}. All timings are in seconds and were created using Magma 2.15 [BC08] on a Quad-Core Intel Xeon running at 3 GHz with 16GB of memory available, although only one core and less than 2GB of memory were used.

R	GF(2)	GF(2^6)	GF(2^{10})
A_1^{SC}	0.1	0.0	0.0
A_1^{Ad}	0.0	0.0	0.0
A_2^{SC}	0.0	0.0	0.0
A_2^{Ad}	0.0	0.0	0.0
A_3^{SC}	0.0	0.1	0.1
$A_3^{(2)}$	0.0	0.1	0.1
A_3^{Ad}	0.0	0.1	0.1
A_4^{SC}	0.2	0.6	0.3
A_4^{Ad}	0.4	0.4	0.4
A_5^{SC}	0.9	2.0	5.2
$A_5^{(3)}$	0.7	1.8	2.2
$A_5^{(2)}$	1.3	5.1	2.5
A_5^{Ad}	0.9	1.9	2.5
A_6^{SC}	3.6	10	8.9
A_6^{Ad}	4.0	12	10
A_7^{SC}	22	109	52
$A_7^{(4)}$	19	45	88
$A_7^{(2)}$	19	82	86
A_7^{Ad}	18	38	53
A_8^{SC}	67	278	390
$A_8^{(3)}$	68	134	163
A_8^{Ad}	69	151	227
B_2^{SC}	0.1	0.1	0.1
B_2^{Ad}	0.0	0.0	0.0
B_3^{SC}	0.1	0.2	0.1
B_3^{Ad}	0.2	0.2	0.2
B_4^{SC}	0.8	1.2	2.0
B_4^{Ad}	1.2	1.4	1.0
B_5^{SC}	8.3	8.4	8.5
B_5^{Ad}	3.1	8.8	8.4
B_6^{SC}	85	39	67
B_6^{Ad}	17	55	81
B_7^{SC}	120	212	272
B_7^{Ad}	93	206	203
B_8^{SC}	772	991	1123
B_8^{Ad}	544	1060	1631
C_3^{SC}	0.6	1.1	1.4
C_3^{Ad}	0.1	0.1	0.2
C_4^{SC}	8.6	9.3	11
C_4^{Ad}	2.7	2.9	1.8
C_5^{SC}	37	70	137
C_5^{Ad}	10	12	30
C_6^{SC}	221	386	682
C_6^{Ad}	63	84	152
C_7^{SC}	890	7630	12201
C_7^{Ad}	170	327	722
C_8^{Ad}	765	1626	23109
C_8^{SC}	3907	23383	34536
D_4^{SC}	0.3	0.6	0.6
$D_4^{(2a)}$	0.3	0.6	0.6
$D_4^{(2b)}$	6.7	0.6	0.7
$D_4^{(2c)}$	0.9	1.0	0.7
D_4^{Ad}	1.7	0.5	0.9
D_5^{SC}	1.9	4.7	5.0
$D_5^{(2)}$	2.8	4.0	4.4
D_5^{Ad}	8.1	5.1	15
D_6^{SC}	16	37	68
$D_6^{(2a)}$	12	28	36
$D_6^{(2b)}$	14	102	126
$D_6^{(2c)}$	19	27	59
D_6^{Ad}	13	29	48
D_7^{SC}	64	125	165
$D_7^{(2)}$	105	129	175
D_7^{Ad}	1217	299	464
D_8^{SC}	607	577	2036
$D_8^{(2a)}$	367	719	958
$D_8^{(2b)}$	5067	2162	7613
$D_8^{(2c)}$	3055	1364	3192
D_8^{Ad}	1716	2700	1305
E_6^{SC}	34	52	80
E_6^{Ad}	36	43	66
E_7^{SC}	985	6523	3212
E_7^{Ad}	254	1609	1663
E_8	2511	81835	17628
F_4	2.4	9.7	6.2
G_2	0.0	0.0	0.0

Table 3.7: Runtimes for SplitMaximalToralSubalgebra

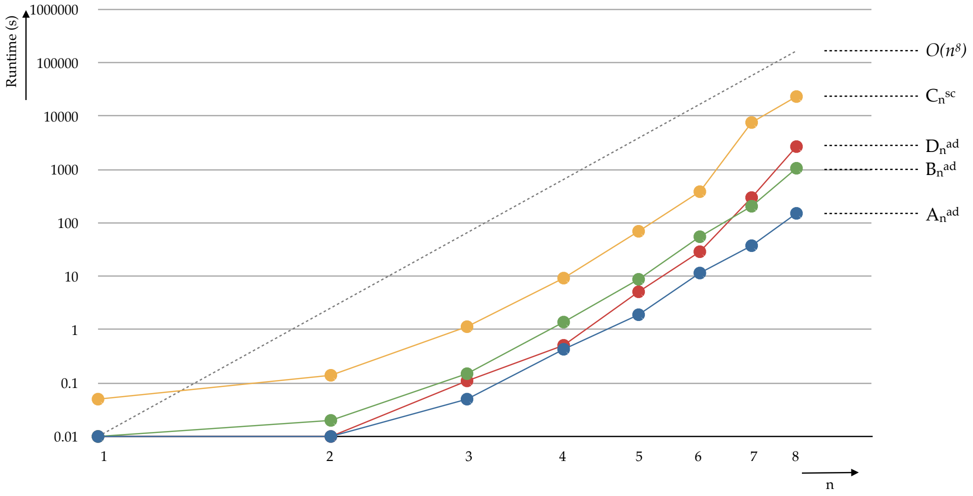


Figure 3.8: Runtimes for SplitMaximalToralSubalgebra for $\mathbb{F} = GF(2^6)$

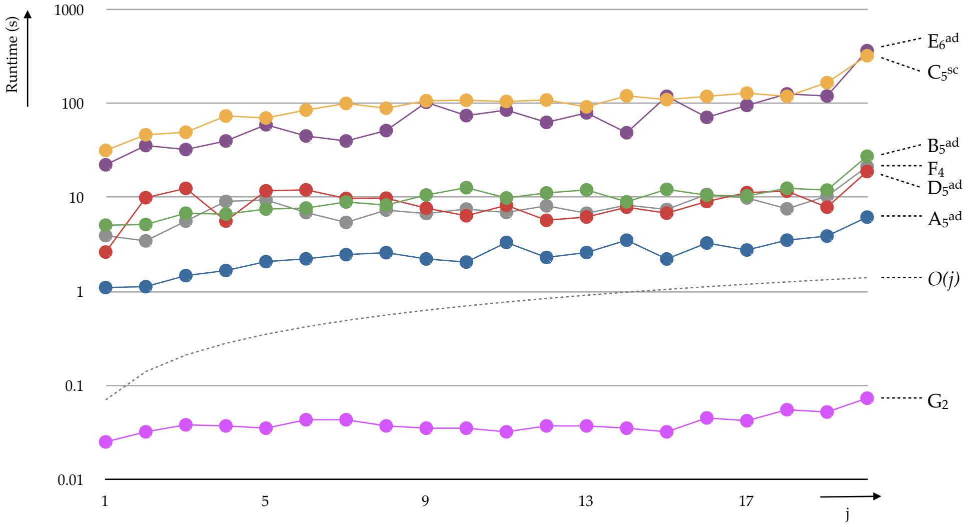
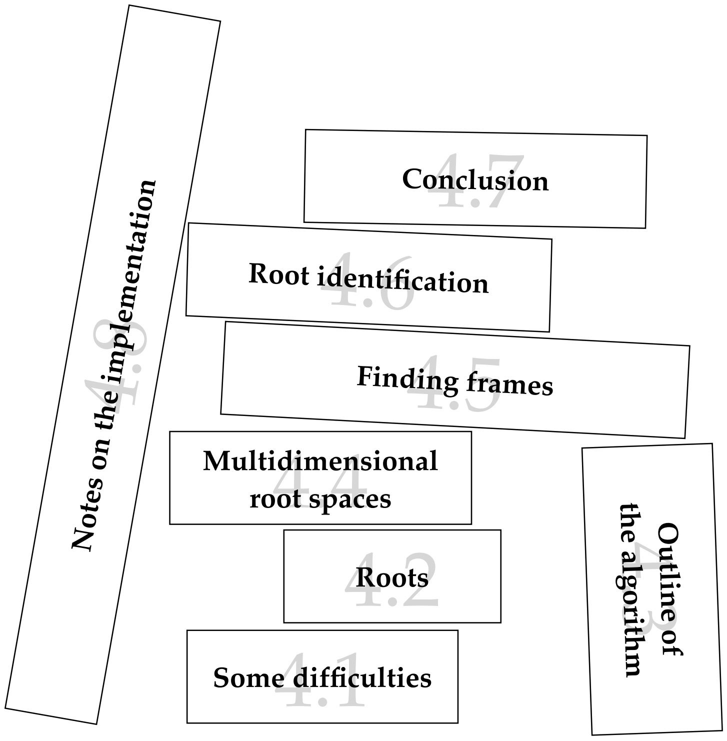


Figure 3.9: Runtimes for SplitMaximalToralSubalgebra for $\mathbb{F} = GF(2^j)$


Conclusion
4.7
Root identification
4.6
Finding frames
4.5
Multidimensional root spaces
4.4
Roots
4.2
Some difficulties
4.1
Outline of the algorithm
4.3
Notes on the implementation
4.8

4 Computing Chevalley Bases

In this chapter we show how to compute a Chevalley basis for a Lie algebra of a split simple algebraic group. For the definition of Chevalley basis we refer to Section 1.9, where in particular the theorem due to Chevalley is mentioned: The Lie algebra of a split simple algebraic group has a Chevalley basis. Existing algorithms (due to De Graaf [dG00, Section 5.11] and Cohen and Murray [CM09, Section 5]) assume that the field of definition of the Lie algebra under consideration has characteristic distinct from 2 and 3.

We discuss the considerably difficulties encountered in these excluded characteristics in Section 4.1. The main difficulty, namely roots with a multiplicity greater than 1, is described in Proposition 4.2 (see Section 4.2). The proof of this proposition is Section 4.4. We give an outline of our algorithm in Section 4.3, and describe the algorithm in more detail in Sections 4.5 and 4.6. In Section 4.7, we finish the proof of Theorem 4.1 and discuss some further problems for which our algorithm may be of use. Finally, in Section 4.8 we analyse the performance of our algorithm in practice.

This chapter is based on the paper titled *Computing Chevalley bases in small characteristics* by Arjeh M. Cohen and the author of this thesis [CR09]. The main result of this chapter is the following theorem:

Theorem 4.1. *Let L be the Lie algebra of a split simple algebraic group with root datum R of rank n defined over an effective field $\mathbb{F}$. Suppose that H is an $\mathbb{F}$-split maximal toral subalgebra of L. If L is given as a structure constant Lie algebra and H is given by means of a spanning set, then there is a Las Vegas algorithm that finds a Chevalley basis of L with respect to H and R. If $\mathbb{F} = \mathrm{GF}(q)$, this algorithm needs at most $O^{\sim}(n^{10}(\log q)^4)$ elementary operations.*

Better estimates than those of the theorem are conceivable. However, our primary goal will be to establish that the algorithm is polynomial in $n \log(q)$. Moreover, in comparison to the dimension $O(n^2)$ of L or the estimate $O(n^6)$ for arithmetic operations needed for multiplying two elements of L, the high exponent of n in the timing looks more reasonable than it may seem at first sight.

The proof of Theorem 4.1 rests on Algorithm 4.3, which is really an outline of an algorithm further specified in the course of this chapter. The algorithm is implemented in Magma [BC08].

The algorithm is mostly deterministic. However, in some instances where $\mathbb{F}$ is of characteristic 2 (such as Method [$\mathrm{B}_2{}^{\mathrm{sc}}$] and the case where L is of type D_4; see Sections 4.5.3, 4.5.5, and 4.5.6) we use the Meat-axe (see Section 1.13) for finding a particular submodule of a given module. We will apply the Meat-axe only to modules of bounded dimension, so that the factor $\dim(L)^3 = O(n^6)$ in the estimate for the Meat-axe running time when $\mathbb{F} = \mathrm{GF}(q)$ plays no role in the asymptotic time analysis.

Algorithm 4.3 assumes that besides L and H the root datum R of the underlying group is known. However, in Section 5.1 we show that this root datum can be determined by running the algorithm a small number of times.

4.1 Some difficulties

Thanks to the characterization of Lie algebras of split reductive algebraic groups described in Theorem 1.44 (see Section 1.9) we can view the Lie algebras in Theorem 4.1 as Chevalley Lie algebras.

So we will deal with the construction of a Chevalley basis for a Chevalley Lie algebra L over a field $\mathbb{F}$, given only a split maximal toral subalgebra H and a root datum R. The output of our algorithm is an ordered basis $\{X_\alpha, h_i \mid \alpha \in \Phi, i \in \{1, \ldots, n\}\}$ of L (based on some ordering of the elements of Φ) satisfying (CB1)–(CB4).

If we consider Lie algebras of simple algebraic groups over a field $\mathbb{F}$ of characteristic 2 or 3, the current algorithms (mostly designed for characteristic 0; see Section 1.13) break down in several places. Firstly, the root spaces (joint eigenspaces) of the split maximal toral subalgebra H acting on L are no longer necessarily one-dimensional. This means that we will have to take extra measures in order to identify which vectors in these root spaces are root elements. This problem will be dealt with in Section 4.5. Secondly, we can no longer always use root chains to compute Cartan integers $\langle \alpha, \beta^\vee \rangle$, which are the most important piece of information for the root identification algorithm in the general case. We will deal with this problem in Section 4.6. Thirdly, when computing the Chevalley basis elements for non-simple roots, we cannot always obtain $X_{\alpha+\beta}$ from (CB4) by $X_{\alpha+\beta} = \frac{1}{N_{\alpha,\beta}}[X_\alpha, X_\beta]$ as $N_{\alpha,\beta}$ may be a multiple of $\mathrm{char}(\mathbb{F})$. This problem, however, is easily dealt with by using a different order in which we fix the scalar multiples of the roots, so we will not discuss this any further.

4.2 Roots

Recall from Section 1.9.1 that a root of H on L is a function

$$\overline{\alpha} : h \mapsto \sum_{i=1}^{n} \langle \alpha, y_i \rangle t_i, \quad \text{where } h = \sum_{i=1}^{n} y_i \otimes t_i = \sum_{i=1}^{n} t_i h_i,$$

for some $\alpha \in \Phi$, where $\langle \alpha, y_i \rangle$ is interpreted in $\mathbb{Z}$ (if $p = 0$) or $\mathbb{Z}/p\mathbb{Z}$ (if $p \neq 0$), and that the multiplicity of α in L is the number of $\beta \in \Phi$ such that $\overline{\alpha} = \overline{\beta}$.

If each root has multiplicity 1, there is a bijection between $\overline{\Phi}$ and Φ. Our first order of business is to decide in which cases higher multiplicities occur. Observe that $\overline{\alpha} = 0$ if and only if $\overline{-\alpha} = 0$ so the multiplicity of the 0-root space is never 1.

```
ChevalleyBasis
in:     The Lie algebra $L$ over a field $\mathbb{F}$ of a split reductive algebraic group,
        a split maximal toral subalgebra $H$ of $L$, and
        a root datum $R = (X, \Phi, Y, \Phi^\vee)$.
out:    A Chevalley basis $B$ for $L$ with respect to $H$ and $R$.
begin
    let $E, \overline{\Phi}$ = FindRootSpaces($L$, $H$),
    let $\mathcal{X}$ = FindFrame($L$, $H$, $R$, $\overline{\Phi}$, $E$),
    let $\iota$ = IdentifyRoots($L$, $H$, $R$, $\overline{\Phi}$, $\mathcal{X}$),
    let $X^0, H^0$ = ScaleToBasis($L$, $H$, $R$, $\mathcal{X}$, $\iota$),
    return $X^0, H^0$.
end
```

Algorithm 4.3: Finding a Chevalley Basis

If $\mathrm{char}(\mathbb{F}) = 2$, then all non-zero multiplicities are at least 2 as $\overline{\alpha}$ and $\overline{-\alpha}$ coincide. Steinberg [Ste61, Proposition 7.4] studied part of the classification of Chevalley Lie algebras L for which higher multiplicities occur (namely the simply connected case with Dynkin type A_n, D_n, $\mathrm{E}_{6,7,8}$) in a search for all Lie algebras L with $\mathrm{Aut}(L/Z(L))$ strictly larger than G. In Section 4.4 of this paper we prove the following proposition, which generalizes Steinberg's result to arbitrary root data. The study of multiplicities of roots can easily be reduced to the case where G is simple, since the multiplicity of a root of H on the Lie algebra L of a central product of split reductive linear algebraic groups is equal to the minimum over all multiplicities of its restrictions to summands of the corresponding central sum decomposition of L.

Proposition 4.2. *Let L be the Lie algebra of a split simple algebraic group over a field $\mathbb{F}$ of characteristic p with root datum $R = (X, \Phi, Y, \Phi^\vee)$. Then the multiplicities of the roots in $\overline{\Phi}$ are either all 1 or as indicated in Table 4.4.*

In Table 4.4, the Dynkin type R of L and the characteristic p of $\mathbb{F}$ are indicated by $R(p)$ in the first column. The isogeny type of R appearing as a superscript on $R(p)$ is explained in the beginning of Section 4.4. The multiplicities of the root spaces appear in the second column under Mults. Those shown in bold correspond to the root 0. For instance, for $\mathrm{B}_2{}^{\mathrm{sc}}(2)$ we have $\dim(\mathrm{C}_L(H)) = 6$, so the multiplicity equals $6 - 2 = 4$. The third column, with header Soln, indicates the method chosen by our algorithm. Further details appear later, in Section 4.5.

4.3 Outline of the algorithm

In this section we give a brief overview of the inner workings of Algorithm 4.3. It is assumed that L is isomorphic to $L_{\mathbb{F}}(R)$. The FindRootSpaces algorithm consists of simultaneous diagonalization of L with respect to $\mathrm{ad}_{h_1}, \ldots, \mathrm{ad}_{h_n}$, where $\{h_1, \ldots, h_n\}$ is a basis of H. Its output is a basis E of H-eigenvectors of L and the set $\overline{\Phi}$ of roots of H on L. This is feasible over $\mathbb{F}$ because the elements are semisimple and H is

$R(p)$	Mults	Soln	$R(p)$	Mults	Soln
$\mathrm{A}_2{}^{\mathrm{sc}}(3)$	3^2	[Der]	$\mathrm{C}_n{}^{\mathrm{ad}}(2)$ $(n \geq 3)$	$2n, 2^{n(n-1)}$	[C]
$\mathrm{G}_2(3)$	$1^6, 3^2$	[C]	$\mathrm{C}_n{}^{\mathrm{sc}}(2)$ $(n \geq 3)$	$\mathbf{2n}, 4^{\binom{n}{2}}$	[$\mathrm{B}_2{}^{\mathrm{sc}}$]
$\mathrm{A}_1{}^{\mathrm{sc}}(2)$	$\mathbf{2}$	[$\mathrm{A}_1{}^{\mathrm{sc}}$]	$\mathrm{D}_4^{(1),(n-1),(n)}(2)$	4^6	[Der]
$\mathrm{A}_3^{\mathrm{sc},(2)}(2)$	4^3	[Der]	$\mathrm{D}_4{}^{\mathrm{sc}}(2)$	8^3	[Der]
$\mathrm{B}_2{}^{\mathrm{ad}}(2)$	$2^2, 4$	[C]	$\mathrm{D}_n^{(1)}(2)$ $(n \geq 5)$	$4^{\binom{n}{2}}$	[Der]
$\mathrm{B}_n{}^{\mathrm{ad}}(2)$ $(n \geq 3)$	$2^n, 4^{\binom{n}{2}}$	[C]	$\mathrm{D}_n{}^{\mathrm{sc}}(2)$ $(n \geq 5)$	$4^{\binom{n}{2}}$	[Der]
$\mathrm{B}_2{}^{\mathrm{sc}}(2)$	$\mathbf{4}, 4$	[$\mathrm{B}_2{}^{\mathrm{sc}}$]	$\mathrm{F}_4(2)$	$2^{12}, 8^3$	[C]
$\mathrm{B}_3{}^{\mathrm{sc}}(2)$	6^3	[Der]	$\mathrm{G}_2(2)$	4^3	[Der]
$\mathrm{B}_4{}^{\mathrm{sc}}(2)$	$2^4, 8^3$	[Der]	all remaining(2)	$2^{\lvert\Phi^+\rvert}$	[A_2]
$\mathrm{B}_n{}^{\mathrm{sc}}(2)$ $(n \geq 5)$	$2^n, 4^{\binom{n}{2}}$	[C]			

Table 4.4: Multidimensional root spaces

split. As $\dim(L) = O(n^2)$, these operations need time $O^{\sim}(n^6 \log q)$ for each basis element of H, so the total cost is $O^{\sim}(n^7 \log q)$ elementary operations.

The algorithm called FindFrame is more involved, and solves the difficulties mentioned in Section 4.1 by various methods. The output $\mathcal{X}$ is a *Chevalley frame*, that is, a set of the form $\{\mathbb{F}X_\alpha \mid \alpha \in \Phi\}$, where X_α $(\alpha \in \Phi)$ belong to a Chevalley basis of L with respect to H and R. If all multiplicities are 1 then FindFrame is trivial, meaning that $\mathcal{X} = \{\mathbb{F}x \mid x \in E \setminus H\}$ is the required result. The remaining cases are identified by Proposition 4.2, and the algorithms for these cases are indicated by [A_2], [C], [Der], [$\mathrm{B}_2{}^{\mathrm{sc}}$] in Table 4.4 and explained in Section 4.5.

In IdentifyRoots we compute Cartan integers and use these to make the identification ι between the root system Φ of R and the Chevalley frame $\mathcal{X}$ computed previously. This identification is again made on a case-by-case basis depending on the root datum R. See Section 4.6 for details.

The algorithm ends with ScaleToBasis where the vectors X_α $(\alpha \in \Phi)$ belonging to members of the Chevalley frame $\mathcal{X}$ are picked in such a way that $X^0 = (X_\alpha)_{\alpha \in \Phi}$ is part of a Chevalley basis with respect to H and R, and a suitable basis $H^0 = \{h_1, \ldots, h_n\}$ of H is computed, so that they satisfy the Chevalley basis multiplication rules. This step involves the solving of several systems of linear equations, similar to the procedure explained in [CM09, Algorithm 9], which takes time $O^{\sim}(n^8 \log q)$.

4.4 Multidimensional root spaces

In this section we prove Proposition 4.2, but first we explain the notation in Table 4.4. As already mentioned, the first column contains the root datum R specified by means of the Dynkin type with a superscript for the isogeny type, as well as (between parentheses) the characteristic p. A root datum of type A_3 can have any of three isogeny types: adjoint, simply connected, or an intermediate one, corresponding to the subgroup of order 1, 4, and 2 of its fundamental group $\mathbb{Z}/4\mathbb{Z}$, respectively (see Section 1.1.3). We denote the intermediate type by $\mathrm{A}_3^{(2)}$. For computations we fix root and coroot matrices for each isomorphism class of root data, as indicated in Section 1.3. For A_3, for example, the Cartan matrix is

$$C = \begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix}.$$

For the adjoint isogeny type $\mathrm{A}_3{}^{\mathrm{ad}}$ we take the root matrix A to be equal to the identity matrix I and the coroot matrix B to be equal to C. Similarly, for $\mathrm{A}_3{}^{\mathrm{sc}}$ we have $A = C$ and $B = I$. For the intermediate case $\mathrm{A}_3^{(2)}$ for instance, we take

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 1 & 0 & 2 \end{pmatrix} \text{ and } B = \begin{pmatrix} 2 & -1 & -1 \\ -1 & 2 & 0 \\ 0 & -1 & 1 \end{pmatrix}.$$

It is straightforward to check that indeed $\det(A) = 2 = \det(B)$ and $AB^\top = C$. We refer to Section 1.3 for the possible isogeny types of irreducible root data and their notation.

Assume the setting of Proposition 4.2. By Theorem 1.44 there is an irreducible root datum $R = (X, \Phi, Y, \Phi^\vee)$ such that $L = \mathrm{Lie}(G)$ satisfies $L \cong L_{\mathbb{F}}(R)$. Also, all split maximal toral subalgebras H of L are conjugate under G, so the multiplicities of $L_{\mathbb{F}}(R)$ do not depend on the choice of H. For the proof of the proposition, there is no harm in identifying L with $L_{\mathbb{F}}(R)$ and H with the Lie algebra of a given split maximal torus of G.

As all multiplicities are known to be 1 if $\mathrm{char}(\mathbb{F}) = 0$, we will assume that $p = \mathrm{char}(\mathbb{F})$ is a prime. We will write $\equiv$ for equality mod p. (To prevent confusion we will sometimes add: mod p.) We begin with two lemmas.

Lemma 4.5. *Let $\alpha, \beta \in \Phi$. Then $\overline{\alpha} = \overline{\beta}$ if and only if $(c^\alpha - c^\beta)A \equiv 0$.*

Proof For $h \in H$, by definition, $\langle \alpha, h \rangle = \langle c^\alpha A, h \rangle = c^\alpha A h^\top$. This implies that $\overline{\alpha} = \overline{\beta}$ if and only if $c^\alpha A h^\top \equiv c^\beta A h^\top$ for all $h \in H$, which is equivalent to $(c^\alpha - c^\beta)A \equiv 0$. □

Lemma 4.6. *Let R_1, R_2 be irreducible root data of the same rank and with the same Cartan matrix C and denote their root matrices by A_1 and A_2, respectively.*

(i) If $\det(A_2)$ strictly divides $\det(A_1)$, then the multiplicities in $L_{\mathbb{F}}(R_1)$ are greater than or equal to those in $L_{\mathbb{F}}(R_2)$.

(ii) If $p \not| \det(C)$, then the multiplicities of $L_{\mathbb{F}}(R_1)$ and $L_{\mathbb{F}}(R_2)$ are the same.

Proof (i). Without loss of generality, we identify the ambient lattices X and Y with $\mathbb{Z}^n$ and choose the same bilinear pairing (as in Section 1.3) for each of the two root data R_1 and R_2. The condition that $\det(A_2)$ strictly divides $\det(A_1)$ then implies that the columns of A_1 belong to the lattice spanned by the columns of A_2. Hence

$A_1 = A_2 M$ for a certain integral $n \times n$ matrix M. Thus $(c^\alpha - c^\beta)A_2 \equiv 0$ implies $(c^\alpha - c^\beta)A_1 \equiv (c^\alpha - c^\beta)A_2 M \equiv 0$, proving the lemma in view of Lemma 4.5.

(ii). As $\det(C) \not\equiv 0$, the determinants of the coroot matrices B_1 and B_2 are non-zero modulo p, and $A_1 = A_2(B_2 B_1^{-1})$ and $A_2 = A_1(B_1 B_2^{-1})$. It follows that $(c^\alpha - c^\beta)A_2 \equiv 0$ is equivalent to $(c^\alpha - c^\beta)A_1 \equiv 0$. □

A typical case where part (i) of this lemma can be applied is when the adjoint and simply connected case have the same multiplicities, for then every intermediate type will have those multiplicities as well. It immediately follows from Lemma 4.6 that the root space dimensions are biggest in the simply connected case, and least in the adjoint case. Thus considering root data of the adjoint and simply connected isogeny types often suffices to understand the intermediate cases. Part (ii) indicates that in many cases even one isogeny type will do.

The proof of Proposition 4.2 follows a division of cases according to the different Dynkin types of the root datum R. For each type, we need to determine when distinct roots α, β exist in Φ such that $\overline{\alpha} = \overline{\beta}$. By Lemma 4.6(ii), there are deviations from the adjoint case only if p divides $\det(C)$.

As the Weyl group W embeds in $N_G(H)/T$, and acts equivariantly on Φ and $\overline{\Phi} = \Phi(L, H)$, the multiplicity of a root $\overline{\alpha} \in \overline{\Phi}$ only depends on the W-orbit of $\alpha \in \Phi$. By transitivity of the Weyl group on roots of the same length in Φ, it suffices to consider only $\alpha = \alpha_1$ in the cases where all roots in Φ have the same length ($\mathrm{A}_n, \mathrm{D}_n, \mathrm{E}_{6,7,8}$) and $\alpha = \alpha_1$ or α_n if there are multiple root lengths ($\mathrm{B}_n, \mathrm{C}_n, \mathrm{F}_4, \mathrm{G}_2$).

In the adjoint cases, the simple roots $\alpha_1, \dots, \alpha_n$ are the standard basis vectors $e_1, \dots, e_n$, since then the root matrix A and the coroot matrix B are I and $C^\top$, respectively. Similarly, in the simply connected cases, the simple roots $\alpha_1, \dots, \alpha_n$ are the rows of the Cartan matrix C, since then $A = C$ and $B = I$. We write $c = c^\beta$ so $\beta = cA$ and either all $c_i \in \mathbb{N}$ or all $c_i \in -\mathbb{N}$.

4.4.1 A_n $(n \geq 1)$

The root datum of type A_n has Cartan matrix

$$C = \begin{pmatrix} 2 & -1 & 0 & \dots & 0 \\ -1 & 2 & -1 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & -1 & 2 & -1 \\ 0 & \dots & 0 & -1 & 2 \end{pmatrix},$$

and the roots are

$$\pm(\alpha_j + \dots + \alpha_k), \quad 1 \leq j \leq k \leq n,$$

where $\{\alpha_1, \dots, \alpha_n\}$ are the simple roots, thus giving a total of $2 \cdot \frac{1}{2}n(n+1)$ roots.

For the adjoint case, suppose $\overline{\alpha_1} = \overline{\beta}$. Observe that all $c_i \in \{0, \pm 1\}$. Since $A = I$, we must have $c_1 \equiv 1$ and $c_j \equiv 0$ ($j = 2, \dots, n$), which implies either $p \neq 2$, $c_1 = 1$, and $c_2 = \dots = c_n = 0$, or $p = 2$, $c_1 = \pm 1$, and $c_2 = \dots = c_n = 0$. Since we assumed $\beta \neq \alpha_1$ we find $p = 2$ and $\beta = -\alpha_1$, giving $\frac{n^2+n}{2}$ root spaces of dimension 2.

In the simply connected case the simple roots are equal to the rows of C, so that $\overline{\alpha_1} = \overline{\beta}$ implies $2c_1 - c_2 \equiv 2$, $-c_1 + 2c_2 - c_3 \equiv -1$, $-c_{j-2} + 2c_{j-1} - c_j \equiv 0$ for $j = 4, \ldots, n$, and $-c_{n-1} + 2c_n \equiv 0$. We will deal with the case $n = 1$ separately below.

We distinguish three possibilities: $c_1 = 1$, $c_1 = 0$, and $c_1 = -1$. If $c_1 = 1$, then $c_2 \equiv 0$, so $c_2 = 0$. As $c_1\alpha_1 + \cdots + c_n\alpha_n$ must be a root, this implies $c_3 = \cdots = c_n = 0$, forcing $\overline{\beta} = \overline{\alpha_1}$, a contradiction.

If $c_1 = 0$, then $-c_2 \equiv 2$, so that either $p = 2$ and $c_2 = 0$, or $p = 3$ and $c_2 = 1$. In the first case, we find $c_3 \equiv 1$, giving a contradiction if $n \geq 5$ (because then $c_4 \equiv 0$ and $c_5 \equiv 1$), a contradiction if $n = 4$ (because then the last relation becomes $0 = -c_3 + 2c_4$, which is not satisfied). Consequently, $n = 3$ and $p = 2$; the resulting case is discussed below. In the second case, where $p = 3$ and $c_2 = 1$, we find $-1 \equiv 2 - c_3$, so that $c_3 \equiv 0$, giving a contradiction if $n \geq 4$ (because then $c_4 \equiv 1$), a contradiction if $n = 3$ (because then the last relation becomes $0 = -c_2 + 2c_3$, which is not satisfied). It follows that $n = 2$ and $p = 3$; this case is also discussed below.

If $c_1 = -1$, then $-c_2 \equiv 4$, so that either $p = 2$ and $c_2 = 0$, or $p = 3$ and $c_2 = -1$. In the first case, we find $c_3 = \cdots = c_n = 0$, so $\beta = -\alpha_1$. In the second case, we find that either $n = 2$ (the special case below), or $c_3 = 0$, which leads to a contradiction if $n \geq 4$ (because then $c_3 = 0$ but $c_4 \neq 0$), and also if $n = 3$ (because then the last equation becomes $0 = -c_2 + 2c_3$).

We next determine the multiplicities in the three cases found to occur for $\mathrm{A}_n{}^{\mathrm{sc}}$. For $n = 1$ we have

$$A = C = \begin{pmatrix} 2 \end{pmatrix},$$

so that multiple roots can only occur if $\overline{-\alpha_1} = \overline{\alpha_1}$, i.e., if $p = 2$. Note that if that is the case $\overline{-\alpha_1} = \overline{\alpha_1} \equiv 0$, giving the bold-faced 2 in the entry corresponding to $\mathrm{A}_1{}^{\mathrm{sc}}$ in Table 4.4.

For $n = 3$ and $p = 2$ we have

$$A = C = \begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -1 \\ 0 & -1 & 2 \end{pmatrix} \equiv \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \mod 2.$$

This gives $\overline{\alpha_1} = \overline{\alpha_3}$, as well as $\overline{\alpha_1 + \alpha_2} = \overline{\alpha_2 + \alpha_3}$ and $\overline{\alpha_2} = \overline{\alpha_1 + \alpha_2 + \alpha_3}$, accounting for 3 root spaces of dimension 4.

For $n = 2$ and $p = 3$ we have

$$A = C = \begin{pmatrix} 2 & -1 \\ -1 & 2 \end{pmatrix} \equiv \begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix} \mod 3,$$

which implies $\overline{\alpha_1} = \overline{\alpha_2}$ and $\overline{\alpha_1} = \overline{-(\alpha_1 + \alpha_2)}$. Similarly, $\overline{-\alpha_1} = \overline{-\alpha_2} = \overline{\alpha_1 + \alpha_2}$, giving 2 root spaces of dimension 3.

For the intermediate cases observe that by Lemma 4.6(i) we need only consider $(n, p) = (2, 3)$ and $(3, 2)$. But the former case has no intermediate isogeny types, and the latter case is readily checked to be as stated. This finishes the proof for the A_n case.

4.4.2 B_n $(n \geq 2)$

The root datum of type B_n has Cartan matrix

$$C = \begin{pmatrix} 2 & -1 & 0 & \dots & 0 \\ -1 & 2 & -1 & \dots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & -1 & 2 & -2 \\ 0 & \dots & 0 & -1 & 2 \end{pmatrix},$$

and the roots are

$$\begin{array}{ll} \pm(\alpha_j + \cdots + \alpha_l), & 1 \leq j \leq l \leq n, \\ \pm(\alpha_j + \cdots + \alpha_{l-1} + 2\alpha_l + \cdots + 2\alpha_n), & 1 \leq j < l \leq n, \end{array}$$

giving a total of $2 \cdot \frac{1}{2}n(n+1) + 2 \cdot \frac{1}{2}n(n-1) = 2n^2$ roots.

In the adjoint case we have $A = I$. For the long roots, suppose $\overline{\alpha_1} = \overline{\beta}$, so $c_1 \equiv 1$ and $c_2 \equiv \cdots \equiv c_n \equiv 0$. If $c_1 = 1$, then $c_2 \neq 0$ (for otherwise $\beta = \alpha_1$), which implies $p = 2$ and $\beta = \alpha_1 + 2\alpha_2 + \cdots + 2\alpha_n$. If $c_1 = -1$, then $p = 2$, and either $c_2 = 0$, which gives $\beta = -\alpha_1$, or $c_2 \neq 0$, which implies $\beta = -\alpha_1 - 2\alpha_2 - \cdots - 2\alpha_n$. In this case the long roots have multiplicities 4.

In the adjoint case, for the short roots, suppose $\overline{\alpha_n} = \overline{\beta}$, so $c_n \equiv 1$ and $c_1 \equiv \cdots \equiv c_{n-1} \equiv 0$. This yields three possibilities for c_n: If $c_n = -2$, then $p = 3$, implying c_{n-1} is either 0 or -3, neither of which give rise to roots. If $c_n = -1$, then $p = 2$; now either $c_{n-1} = 0$ (yielding $\beta = -\alpha_n$), or $c_{n-1} = -2$ (not giving any roots). If $c_n = 1$ we must have $c_{n-1} = \cdots = c_1 = 0$, giving the contradiction $\beta = \alpha_n$. This shows that $p = 2$ and all multiplicities are 2.

In the simply connected case we have $A = C$. By Lemma 4.6(ii), we may assume $p = 2$. We will consider $n \geq 5$ first, and then treat $n = 2, 3, 4$ separately.

For the long roots, suppose $\overline{\alpha_1} = \overline{\beta}$, so $c_2 \equiv 0$, $c_1 + c_3 \equiv 1$, and $c_{j-2} + c_j \equiv 0$ $(j = 4, \dots, n)$. This forces $c_4 \equiv 0$. If $c_1 \equiv 0$ then $c_1 = 0$ and hence $c_2 = 0$, so $c_3 = \pm 1$. replacing β by β if needed, we may assume $c_3 = 1$. As $c_4 \equiv 0$ and $c_5 \equiv 1$, we must have $c_4 = 2$ and $c + 5 = 1$, which is never satisfied by a root. If on the other hand $c_1 \equiv 1$ then $c_3 \equiv c_4 \equiv \cdots \equiv c_n \equiv 0$, so $\beta = -\alpha_1$ or $\beta = \pm(\alpha_1 + 2\alpha_2 + \cdots + 2\alpha_n)$. This shows that, for $n \geq 5$, the multiplicities of $\overline{\beta}$ for β a long root are 4.

For the short roots, suppose $\overline{\alpha_n} = \overline{\beta}$, so $c_2 \equiv 0$, $c_{j-2} + c_j \equiv 0$ $(j = 3, \dots, n-1)$, and $c_{n-2} + c_n \equiv 1$. If $c_1 \equiv 1$ then $c_3 \equiv 1$, but since $c_2 \equiv 0$ this contradicts that β is a root. If on the other hand $c_1 \equiv 0$, then $c_2 \equiv c_3 \equiv \cdots \equiv c_{n-1} \equiv 0$, so $c_n \equiv 1$ and we find $\beta = -\alpha_n$. Hence, for $n \geq 5$, the multiplicities of $\overline{\beta}$ for β a short root are 2.

If $n = 2$ then

$$C = \begin{pmatrix} 2 & -2 \\ -1 & 2 \end{pmatrix} \equiv \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

If $\overline{\alpha_1} = \overline{\beta}$ we have $c_2 \equiv 0$. Since $-2 \leq c_2 \leq 2$ we must have either $c_2 = 0$ (hence $\beta = -\alpha_1$), or $c_2 = \pm 2$ (hence $c_1 = \pm 1$), giving $\beta = \pm\alpha_1$ or $\beta = \pm(\alpha_1 + 2\alpha_2)$. If on the other hand $\overline{\alpha_2} = \overline{\beta}$ we find $c_2 \equiv 1$ hence $\beta = \pm\alpha_2$ or $\beta = \pm(\alpha_1 + \alpha_2)$. This shows that ${B_2}^{\mathrm{sc}}$ has 2 root spaces of dimension 4 if $p = 2$.

If $n = 3$ then

$$C = \begin{pmatrix} 2 & -1 & 0 \\ -1 & 2 & -2 \\ 0 & -1 & 2 \end{pmatrix} \equiv \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

From a straightforward case distinction on the roots of B_3 and the fact that $\overline{\alpha_1} = \overline{\alpha_3}$ we immediately see that $\overline{\alpha_1} = \overline{\alpha_3} = \overline{\alpha_1 + 2\alpha_2 + 2\alpha_3}$, $\overline{\alpha_2} = \overline{\alpha_1 + \alpha_2 + \alpha_3} = \overline{\alpha_2 + 2\alpha_3}$, and $\overline{\alpha_1 + \alpha_2} = \overline{\alpha_2 + \alpha_3} = \overline{\alpha_1 + \alpha_2 + 2\alpha_3}$. This gives the 3 required root spaces of dimension 6.

If $n = 4$ then

$$C = \begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -1 & 0 \\ 0 & -1 & 2 & -2 \\ 0 & 0 & -1 & 2 \end{pmatrix} \equiv \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

From a straightforward case distinction on the roots of B_4 and the fact that $\overline{\alpha_1} = \overline{\alpha_3}$, we find $\overline{\alpha_1} = \overline{\alpha_3} = \overline{\alpha_3 + 2\alpha_4} = \overline{\alpha_1 + 2\alpha_2 + 2\alpha_3 + 2\alpha_4}$, as well as $\overline{\alpha_2} = \overline{\alpha_1 + \alpha_2 + \alpha_3} = \overline{\alpha_1 + \alpha_2 + \alpha_3 + 2\alpha_4} = \overline{\alpha_2 + 2\alpha_3 + 2\alpha_4}$ and $\overline{\alpha_1 + \alpha_2} = \overline{\alpha_2 + \alpha_3} = \overline{\alpha_2 + 2\alpha_3 + 2\alpha_4} = \overline{\alpha_1 + \alpha_2 + 2\alpha_3 + 2\alpha_4}$. The remaining $32 - 24 = 8$ roots $(\pm(\alpha_j + \cdots + \alpha_n), j = 1, \ldots, 4)$ are in 2-dimensional spaces, giving $2^4, 8^3$, as required.

4.4.3 C_n $(n \geq 3)$

The root datum of type C_n has Cartan matrix

$$C = \begin{pmatrix} 2 & -1 & 0 & \ldots & 0 \\ -1 & 2 & -1 & \ldots & 0 \\ \vdots & & & & \vdots \\ 0 & \ldots & -1 & 2 & -1 \\ 0 & \ldots & 0 & -2 & 2 \end{pmatrix},$$

and the roots are

$$\begin{array}{lll} \text{(a)} & \pm(\alpha_j + \cdots + \alpha_l), & 1 \leq j \leq l \leq n, \\ \text{(b)} & \pm(\alpha_j + \cdots + \alpha_{l-1} + 2\alpha_l + \cdots + 2\alpha_{n-1} + \alpha_n), & 1 \leq j \leq l \leq n-1, \end{array}$$

giving a total of $2 \cdot \frac{1}{2}n(n+1) + 2 \cdot \frac{1}{2}n(n-1) = 2n^2$ roots.

In the adjoint case, for the short roots, suppose $\overline{\alpha_1} = \overline{\beta}$, so $c_1 \equiv 1$ and $c_2 \equiv \cdots \equiv c_n \equiv 0$. If $c_1 = 1$, then either $c_2 = 0$, giving $\beta = \alpha_1$ or $p = 2$ and $c_2 = 2$, implying $c_3 = \cdots = c_{n-1} = 2$ and $c_n = 1$, which is a contradiction with $c_n \equiv 0$. If $c_1 = -1$, then $p = 2$, similarly giving either $c_2 = 0$ (hence $\beta = -\alpha 1$) or $c_2 = -2$ and $c_3 = \cdots = c_{n-1} = 2$, $c_n = 1$, which is a contradiction. If $c_1 = -2$ then $p = 3$, but this does not give rise to any roots. This shows that the multiplicities of $\overline{\beta}$ for β a short root are 2.

For the long roots, suppose $\overline{\alpha_n} = \overline{\beta}$, so $c_1 \equiv 1$ and $c_2 \equiv \cdots \equiv c_n \equiv 0$. If $c_n = 1$, we find either $c_{n-1} = 0$ (hence $\beta = \alpha_n$) or $c_{n-2} = 2$ and $p = 2$, giving $\beta =$

$2\alpha_j + \ldots + 2\alpha_{n-1}$, for any $j \in \{1, \ldots, n-1\}$. If $c_n = -1$, we must have $p = 2$, and we find either $c_{n-1} = 0$ (hence $\beta = -\alpha_n$) or $c_{n-2} = -2$, giving $\beta = -(2\alpha_j + \ldots + 2\alpha_{n-1})$, for any $j \in \{1, \ldots, n-1\}$. This shows that the long roots are in one eigenspace of dimension $2n$.

In the simply connected case we have $A = C$. By Lemma 4.6(ii), we may assume $p = 2$. For the short roots, suppose $\overline{\alpha_1} = \overline{\beta}$, so $c_2 \equiv 0$, $c_1 + c_3 \equiv 1$, $c_{j-2} + c_j \equiv 0$ ($j = 4, \ldots, n-1$), $c_{n-2} \equiv 0$, and $c_{n-1} \equiv 0$.

If $c_1 = 2$, we must have $c_1 = \cdots = c_{n-1} = 2$, $c_n = 1$, but this is not a solution to the equations. If $c_1 = 1$ then either $c_2 = 0$ (hence $\beta = \alpha_1$) or $c_2 = 2$ (hence $c_3 = \cdots = c_{n-1} = 2$, $c_n = 1$, giving $\beta = \alpha_1 + 2\alpha_2 + \cdots + 2\alpha_{n-1} + \alpha_n$). If $c_1 = 0$ we have $c_3 \equiv 1$, but this never gives a solution to the equations. If $c_1 = -1$ then either $c_2 = 0$ (hence $\beta = -\alpha_1$) or $c_2 = -2$ (hence $\beta = -(\alpha_1 + 2\alpha_2 + \cdots + 2\alpha_{n-1} + \alpha_n)$. If $c_1 = -2$ we must have $c_3 = -2$ but this contradicts $c_1 + c_3 \equiv 1$. In conclusion, the cases where $c_1 = \pm 1$ give the 4-dimensional eigenspaces mentioned in Table 4.4.

For the long roots, suppose $\overline{\alpha_n} = \overline{\beta}$ so $c_2 \equiv 0$, $c_{j-2} + c_j \equiv 0$ ($j = 3, \ldots, n-2$), $c_{n-2} \equiv 0$, and $c_{n-1} \equiv 0$. If $c_n = 1$ either $c_{n-1} = 0$ (giving $\beta = \alpha_n$) or $c_{n-1} = 2$ (giving $\beta = 2\alpha_j + \cdots + 2\alpha_{n-1} + \alpha_n$, for any $j \in \{1, \ldots, n-1\}$). If $c_n = 0$ we must have $c_{n-1} = 0$ (otherwise β would not be a root), but it follows from the relations that $c_j = 0$ for $j = 1, \ldots, n-2$, which does not give a root either. If $c_n = -1$ either $c_{n-1} = 0$ (giving $\beta = -\alpha_n$) or $c_{n-1} = -2$ (giving $\beta = -(2\alpha_j + \cdots + 2\alpha_{n-1} + \alpha_n)$, for any $j \in \{1, \ldots, n-1\}$). In conclusion, the cases where $c_n = \pm 1$ give one $2n$-dimensional eigenspaces containing all the long roots.

This completes the proof for C_n, giving multiplicities not equal to 1 in characteristic 2 only. In that case, the multiplicities are either $2n, 2^{n(n-1)}$ (for the adjoint isogeny type) or $2n, 4^{\binom{n}{2}}$ (for the simply connected isogeny type).

4.4.4 D_n ($n \geq 4$)

The root datum of type D_n has Cartan matrix

$$C = \begin{pmatrix} 2 & -1 & 0 & \ldots & 0 \\ -1 & 2 & -1 & \ldots & 0 \\ \vdots & & & & \vdots \\ 0 & \ldots & 2 & -1 & -1 \\ 0 & \ldots & -1 & 2 & 0 \\ 0 & \ldots & -1 & 0 & 2 \end{pmatrix},$$

and the roots are

(a)	$\pm(\alpha_j + \cdots + \alpha_l)$,	$1 \leq j \leq l \leq n-2$,
(b)	$\pm\alpha_{n-1}, \pm\alpha_n$	
(c)	$\pm(\alpha_j + \cdots + \alpha_{n-2} + \alpha_{n-1})$,	$1 \leq j \leq n-2$,
(d)	$\pm(\alpha_j + \cdots + \alpha_{n-2} + \alpha_n)$,	$1 \leq j \leq n-2$,
(e)	$\pm(\alpha_j + \cdots + \alpha_{n-2} + \alpha_{n-1} + \alpha_n)$,	$1 \leq j \leq n-2$,
(f)	$\pm(\alpha_j + \cdots + \alpha_{l-1} + 2\alpha_l + \cdots + 2\alpha_{n-2} + \alpha_{n-1} + \alpha_n)$,	$1 \leq j < l \leq n-2$,

giving a total of $\frac{1}{2}(n-1)(n-2)+2+3(n-1)+\frac{1}{2}(n-2)(n-3)=n^2-n$ positive roots, so $2n^2-2n=4\binom{n}{2}$ roots in total.

In the adjoint case, suppose $\overline{\alpha_1}=\overline{\beta}$. If β is of type (a), we find $p=2$ and $\beta=-\alpha_1$. It is easy to see that if β is not of type (a), $\overline{\alpha_1}\neq\overline{\beta}$ unless $\alpha_1=\beta$. This yields $2\binom{n}{2}$ eigenspaces of dimension 2.

For the simply connected case we may assume $p=2$ by Lemma 4.6(ii), since $\det(C)=4$. We first consider $n=4$.

$$A=C=\begin{pmatrix}2&-1&0&0\\-1&2&-1&-1\\0&-1&2&0\\0&-1&0&2\end{pmatrix}\equiv\begin{pmatrix}0&1&0&0\\1&0&1&1\\0&1&0&0\\0&1&0&0\end{pmatrix}$$

giving $\overline{\alpha_1}=\overline{\alpha_3}=\overline{\alpha_4}=\overline{2\alpha_1+2\alpha_2+\alpha_3+\alpha_4}$, i.e., an 8-dimensional eigenspace. Similarly, $\overline{\alpha_2}=\overline{\alpha_1+\alpha_2+\alpha_3}=\overline{\alpha_1+\alpha_2+\alpha_4}=\overline{\alpha_2+\alpha_3+\alpha_4}$ and $\overline{\alpha_1+\alpha_2}=\overline{\alpha_2+\alpha_3}=\overline{\alpha_2+\alpha_4}=\overline{\alpha_1+\alpha_2+\alpha_3+\alpha_4}$, yielding 3 eigenspaces of dimension 8 in total. For $n>4$, suppose $\overline{\alpha_1}=\overline{\beta}$, so that $c_2\equiv 0$, $c_1+c_3\equiv 1$, $c_{j-2}+c_j\equiv 0$, $(j=4,\dots,n-2)$, $c_{n-3}+c_{n-1}+c_n\equiv 0$, $c_{n-2}\equiv 0$, and $c_{n-2}\equiv 0$.

If $c_1=1$ then either $c_2=0$ (giving $\beta=-\alpha_1$), or $c_2=-2$ (giving $\beta=-\alpha_1-2\alpha_2-\dots-2\alpha_{n-2}-\alpha_{n-1}-\alpha_n$). If $c_1=0$ then $c_3\equiv 1$ and $c_4\equiv 0$, giving a contradiction as well. If $c_1=1$ then either $c_2=0$ (hence $\beta=\alpha_1$) or $c_2=2$ (hence $\beta=\alpha_1+2\alpha_2+\dots+2\alpha_{n-2}+\alpha_{n-1}+\alpha_n$). This shows that we find $\binom{n}{2}$ eigenspaces of dimension 4 if $n\geq 5$.

For the intermediate case, recall that the fundamental group for type D_n is $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ (if n is even) or $\mathbb{Z}/4\mathbb{Z}$ (if n is odd). We again assume $p=2$ and first consider $n=4$. Note that, due to the threefold symmetry of the Dynkin diagram the three intermediate isogenies are all equivalent, so that we only need to consider one:

$$A=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&1&2\end{pmatrix},$$

giving $\overline{\alpha_1}=\overline{\alpha_1+2\alpha_2+\alpha_3+\alpha_4}$. It is not hard to see that if β is not of type (f) then $\overline{\alpha_1}\neq\overline{\beta}$ unless $\alpha_1=\pm\beta$, proving that we indeed find 6 eigenspaces of dimension 4.

For $n>4$, we can always choose

$$A=\begin{pmatrix}&&&&0\\&I&&&\vdots\\&&&&0\\0&\cdots&0&1&2\end{pmatrix},$$

where I denotes the $(n-1)\times(n-1)$ identity matrix. If n is odd this corresponds to the only intermediate isogeny, if n is even this corresponds to one of the intermediate isogenies. Following the same reasoning as in the $n=4$ case, we see $\overline{\alpha_1}=\overline{\alpha_1+2\alpha_2+\cdots 2\alpha_{n-2}+\alpha_{n-1}+\alpha_n}$, accounting for $\binom{n}{2}$ eigenspaces of dimension 4.

Finally, if $n > 4$ and n is even there are two intermediate isogenies left but, again, they are equivalent due to the symmetry of the Dynkin diagram. We consider

$$A = \begin{pmatrix} & & & & & & 0 \\ & & & I & & & \vdots \\ & & & & & & 0 \\ 1 & 0 & \cdots & 1 & 0 & 0 & 2 \end{pmatrix},$$

where the omitted entries of the last row alternate between 0 and 1 and I again denotes the $(n-1) \times (n-1)$ identity matrix. Again assume $\overline{\alpha_1} = \overline{\beta}$, so that $c_1 + c_n \equiv 1$, $c_{2i} \equiv 0$ (for $i = 1, \ldots, \frac{n}{2} - 1$), $c_{2i+1} + c_n \equiv 0$ (for $i = 1, \ldots, \frac{n}{2} - 1$), and $2c_n \equiv 0$. If $c_1 \equiv 1$ then $c_n \equiv 0$ and $c_{n-1} \equiv 0$, forcing $c_2 = \cdots = c_n = 0$ and hence $\alpha_1 = \pm\beta$. If on the other hand $c_1 \equiv 0$ then $c_2 \equiv 0$ and $c_n \equiv 1$ and therefore $c_3 \equiv 1$, a contradiction. This proves that in this case all eigenspaces are of dimension 2.

4.4.5 E_n $(n = 6, 7, 8)$

We first prove the theorem for E_8, from which the cases E_6 and E_7 of adjoint type follow since they are subsystems of E_8. Then we prove E_6 and E_7 of simply connected type separately.

Note that for the E_8 case we have to consider only the adjoint type, since the simply connected type is equal to the adjoint type. So suppose $\overline{\alpha_1} = \overline{\beta}$, so that $c_1 \equiv 1$ and $c_j \equiv 0$, $j = 2, \ldots, 8$.

If $p \geq 5$, we have $c_1 = 1$, which means $c_2 = 0$, and we find $\beta = \alpha_1$. If $p = 3$ then $c_1 \in \{1, -2\}$. If $c_1 = 1$ then c_2 must be either 0 (giving $\beta = \alpha_1$) or 3 (where the root system implies $c_3 = 3$ and $c_4 = 5$, a contradiction). If on the other hand $c_1 = -2$, then $c_2 = -3$ and $c_3 = -4$, which is a contradiction as well. Finally, if $p = 2$ then $c_1 \in \{1, -1\}$. If $c_1 = 1$ then either $c_2 = 0$ (giving $\beta = \alpha_1$) or $c_2 = 2$ (giving no roots satisfying the equations). If $c_1 = -1$ then either $c_2 = 0$ (giving $\beta = -\alpha_1$) or $c_2 = -2$ (again giving no roots satisfying the equations).

This shows that multidimensional eigenspaces occur in adjoint E_6, E_7, E_8 only if $p = 2$, and then all eigenspaces are of dimension 2.

We consider E_6 of simply connected type.

$$A = C = \begin{pmatrix} 2 & 0 & -1 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 0 \\ -1 & 0 & 2 & -1 & 0 & 0 \\ 0 & -1 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}$$

If $p \neq 3$ the situation is as in the adjoint case by Lemma 4.6(ii) because $\det(C) = 3$. So we assume $p = 3$ and suppose $\overline{\alpha_1} = \overline{\beta}$. Now $c_1 + c_3 \equiv 1$, $c_2 + c_4 \equiv 0$, $c_1 + c_3 + c_4 \equiv 1$, $c_2 + c_3 + c_4 + c_5 \equiv 0$, $c_4 + c_5 + c_6 \equiv 0$, and $c_5 + c_6 \equiv 0$.

If $c_1 = 1$ we have $c_3 \equiv 0$, implying $\beta = \alpha_1$. If $c_1 = 0$ we find $c_3 \equiv 1$ so that $c_3 = 1$ (implying $c_4 = 0$, $c_2 = 0$, $c_5 = 2$, a contradiction). If $c_1 = -1$ we find $c_3 \equiv -1$

so that $c_3 = -1$ which implies $c_4 \equiv 0$, giving a contradiction for both $c_4 = 0$ and $c_4 = -3$.

This shows that the root multiplicities for E_6 of simply connected type are equal to those for E_6 of adjoint type: All roots have multiplicity 2.

We consider E_7 of simply connected type.

$$A = C = \begin{pmatrix} 2 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & -1 & 0 & 0 & 0 \\ -1 & 0 & 2 & -1 & 0 & 0 & 0 \\ 0 & -1 & -1 & 2 & -1 & 0 & 0 \\ 0 & 0 & 0 & -1 & 2 & -1 & 0 \\ 0 & 0 & 0 & 0 & -1 & 2 & -1 \\ 0 & 0 & 0 & 0 & 0 & -1 & 2 \end{pmatrix}$$

Since $\det(C) = 2$ we assume $p = 2$ (again by Lemma 4.6(ii)). In this case it is more convenient to consider $\overline{\alpha_7} = \overline{\beta}$, which is allowed by the action of the Weyl group. So $c_3 \equiv 0$, $c_4 \equiv 0$, $c_1 + c_4 \equiv 0$, $c_2 + c_3 + c_5 \equiv 0$, $c_4 + c_6 \equiv 0$, $c_5 + c_7 \equiv 1$, and $c_6 \equiv 0$.

If $c_7 = \pm 1$ we find $c_6 \equiv \cdots \equiv c_1 \equiv 0$, which only gives $\beta = \pm\alpha_7$. If $c_7 = 0$ we have $c_6 = 0$ and $c_5 \equiv 1$, $c_4 \equiv c_3 \equiv c_1 \equiv 0$ and $c_2 \equiv 1$. Observing all the roots of E_7, however, shows that this can never be a root.

This shows that the root multiplicities for E_7 of simply connected type are equal to those for E_7 of adjoint type: All roots have multiplicity 2.

4.4.6 F_4

The root datum of type F_4 has Cartan matrix

$$C = \begin{pmatrix} 2 & -1 & 0 & 0 \\ -1 & 2 & -2 & 0 \\ 0 & -1 & 2 & -1 \\ 0 & 0 & -1 & 2 \end{pmatrix},$$

and the roots are

(a) $\pm(\alpha_j + \cdots + \alpha_l)$, $1 \leq j \leq l \leq 4$,
(b) $\pm(\alpha_2 + 2\alpha_3), \pm(\alpha_1 + \alpha_2 + 2\alpha_3), \pm(\alpha_2 + 2\alpha_3 + \alpha_4), \pm(\alpha_1 + \alpha_2 + 2\alpha_3 + \alpha_4)$,
(c) $\pm(\alpha_1 + 2\alpha_2 + 2\alpha_3), \pm(\alpha_2 + 2\alpha_3 + 2\alpha_4), \pm(\alpha_1 + 2\alpha_2 + 2\alpha_3 + \alpha_4)$,
$\pm(\alpha_1 + \alpha_2 + 2\alpha_3 + 2\alpha_4)$,
(d) $\pm(\alpha_1 + 2\alpha_2 + 2\alpha_3 + 2\alpha_4)$,
(e) $\pm(\alpha_1 + 2\alpha_2 + 3\alpha_3 + \alpha_4)$,
(f) $\pm(\alpha_1 + 2\alpha_2 + 3\alpha_3 + 2\alpha_4)$,
(g) $\pm(\alpha_1 + 2\alpha_2 + 4\alpha_3 + 2\alpha_4)$,
(h) $\pm(\alpha_1 + 3\alpha_2 + 4\alpha_3 + 2\alpha_4)$,
(i) $\pm(2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 2\alpha_4)$,

giving a total of $2(10 + 4 + 4 + 6 \cdot 1) = 48$ roots.

We consider the case where $A = I$, since for F_4 the adjoint and simply connected case are identical. We first consider the case where $p = 2$. Then:

$$\begin{aligned}
&\overline{\alpha_1+2\alpha_2+4\alpha_3+2\alpha_4}^{(\mathrm{g})} = \overline{\alpha_1}^{(\mathrm{a})} = \overline{\alpha_1+2\alpha_2+2\alpha_3}^{(\mathrm{c})} = \overline{\alpha_1+2\alpha_2+2\alpha_3+2\alpha_4}^{(\mathrm{d})},\\
&\overline{\alpha_1+3\alpha_2+4\alpha_3+2\alpha_4}^{(\mathrm{h})} = \overline{\alpha_1+\alpha_2}^{(\mathrm{a})} = \overline{\alpha_1+\alpha_2+2\alpha_3}^{(\mathrm{b})} = \overline{\alpha_1+\alpha_2+2\alpha_3+2\alpha_4}^{(\mathrm{c})},\\
&\overline{2\alpha_1+3\alpha_2+4\alpha_3+2\alpha_4}^{(\mathrm{i})} = \overline{\alpha_2}^{(\mathrm{a})} = \overline{\alpha_2+2\alpha_3+2\alpha_4}^{(\mathrm{c})} = \overline{\alpha_2+2\alpha_3}^{(\mathrm{b})},
\end{aligned}$$

giving 3 eigenspaces of dimension 8. The remaining 7 positive roots of type (a), 2 of type (b), and 1 each of type (c), (e) and (f) give 12 eigenspaces of dimension 2. This shows the $2^{12}, 8^3$ given in Table 4.4 for F_4 and $p = 2$.

Now suppose $p \neq 2$ and $\overline{\alpha_1} = \overline{\beta}$, giving $c_1 \equiv 1$ and $c_2 \equiv c_3 \equiv c_4 \equiv 0$. Since $c_1 \in \{-2, -1, 0, 1, 2\}$ and $p \neq 2$ we must have $c_1 = -2$ and $p = 3$, but the only root satisfying this is $-2\alpha_1 - 3\alpha_2 - 4\alpha_3 - 2\alpha_4$, which does not satisfy the equations. Next, suppose $p \neq 2$ and $\overline{\alpha_4} = \overline{\beta}$, giving $c_4 \equiv 1$ and $c_1 \equiv c_2 \equiv c_3 \equiv 0$. Since $c_4 \in \{-2, -1, 0, 1, 2\}$ and $p \neq 2$ we must have $c_4 = -2$ and $p = 3$, but then no roots satisfying the equations exist. This shows that F_4 has multidimensional eigenspaces only if $p = 2$.

4.4.7 G_2

The root datum of type G_2 has Cartan matrix

$$C = \begin{pmatrix} 2 & -1 \\ -3 & 2 \end{pmatrix},$$

and the roots are

$$\begin{aligned}
&\pm\alpha_1, \pm(\alpha_1+\alpha_2), \pm(2\alpha_1+\alpha_2), && \text{(6 short roots)}\\
&\pm\alpha_2, \pm(3\alpha_1+\alpha_2), \pm(3\alpha_1+2\alpha_2), && \text{(6 long roots)}
\end{aligned}$$

giving a total of 12 roots. As $\det(C) = 1$ we take $A = I$. All components of c are in $\{-3, \ldots, 3\}$, so all components of the differences $\alpha_1 - \beta$ and $\alpha_2 - \beta$ are in $\{-4, \ldots, 4\}$. Hence, if multidimensional root spaces occur, we must have $p \leq 3$.

If $p = 3$ we see $\overline{3\alpha_1+\alpha_2} = \overline{\alpha_2} = \overline{-(3\alpha_1+2\alpha_2)}$ and $\overline{-(3\alpha_1+\alpha_2)} = \overline{-\alpha_2} = \overline{3\alpha_1+2\alpha_2}$, and the remaining 6 roots all have distinct root spaces. If $p = 2$ we find $\overline{\alpha_1+\alpha_2} = \overline{3\alpha_1+\alpha_2}$, $\overline{\alpha_1} = \overline{3\alpha_1+2\alpha_2}$ and $\overline{\alpha_2} = \overline{2\alpha_1+\alpha_2}$, giving 3 root spaces of dimension 4.

This finishes the proof of Proposition 4.2.

4.5 Finding frames

Let L be a Chevalley Lie algebra over an effective field $\mathbb{F}$ with root datum R, a fixed split maximal toral subalgebra H, and given decomposition E into root spaces with respect to the set $\overline{\Phi} = \Phi(L, H)$ of roots of H on L. In this section we discuss the procedure of Algorithm 4.3 referred to as FINDFRAME. It determines the set $\mathcal{X} = \{\mathbb{F}X_\alpha \mid \alpha \in \Phi\}$, i.e., the one-dimensional root spaces with respect to Φ, to which we refer as the *Chevalley frame*. Note that we do not yet *identify* the root spaces: finding a suitable bijection between Φ and the Chevalley frame $\mathcal{X}$ is discussed in the next section. We set $p = \mathrm{char}(\mathbb{F})$.

We require that R be given, since we execute different algorithms depending on R, for example $\mathrm{B_2}^{\mathrm{ad}}$ needs [C] whereas $\mathrm{B_2}^{\mathrm{sc}}$ needs [$\mathrm{B_2}^{\mathrm{sc}}$].

For $p = 2$, we use the procedure described in Section 4.5.1 to find the frame once we have computed all spaces $\mathbb{F}X_\alpha + \mathbb{F}X_{-\alpha}$ for $\alpha \in \Phi$. We call this algorithm [$\mathrm{A_2}$]. As an auxiliary result, this procedure stores the unordered pairs $\{\{\alpha, -\alpha\} \mid \alpha \in \Phi^+\}$, to be used in the IdentifyRoots procedure discussed in Section 4.6 (notably, the proof of Lemma 4.12). The general method in characteristic 2 is to partition the root spaces of dimension greater than 2 into such 2-dimensional root spaces, and apply [$\mathrm{A_2}$].

For this purpose, and for the two cases of characteristic 3, we distinguish three general methods:

- [C]: Given two root spaces M, M' compute $C_M(M')$ to break down M. Often, but not always, $\dim(M') = 2$. An example of this method is given in Section 4.5.2.

- [Der]: Compute the Lie algebra $\mathrm{Der}(L)$ of derivations of L, and calculate in there. This is a useful approach if $\mathrm{Der}(L)$ is strictly larger than L, for then we can often extend H to a larger split maximal toral subalgebra, so we find new semisimple elements acting on the root spaces. Examples of this method are given in Sections 4.5.3 and 4.5.4.

- [$\mathrm{B_2}^{\mathrm{sc}}$]: The case where $R(p) = \mathrm{B_2}^{\mathrm{sc}}(2)$ is slightly more involved than the other cases because $\overline{\alpha} = 0$ for some $\alpha \in \Phi$. We use the Meat-axe to split the action of the long roots on the short roots. Examples of this method are given in Sections 4.5.5 and 4.5.6.

The case where $R = \mathrm{A_1}^{\mathrm{sc}}$ and $p = 2$ is dealt with separately:

- [$\mathrm{A_1}^{\mathrm{sc}}$]: Here, as in the case where $R(p) = \mathrm{B_2}^{\mathrm{sc}}(2)$, $\alpha = 0$ for some (in fact all) $\alpha \in \Phi$, but we will show that in this case there is enough freedom of choice. We clarify this method in Section 4.5.7.

The method chosen depends on the root datum R and the characteristic p, as indicated in the third column of Table 4.4.

4.5.1 $\mathrm{A_2}$ in characteristic 2

First, we consider the Lie algebras L with $R(p) = \mathrm{A_2}(2)$, as this procedure is used inside various other cases. It will become clear that we do not need to know the isogeny type of the root datum in order to carry out this procedure. For clarity, we write α, β for the two simple roots of the root system of type $\mathrm{A_2}$ (so that $\alpha \neq \pm\beta$).

As indicated in Table 4.4, we have 3 root spaces of dimension 2. They correspond to $\langle X_\gamma, X_{-\gamma} \rangle_{\mathbb{F}}$ for $\gamma \in \{\alpha, \beta, \alpha+\beta\}$. Without loss of generality we consider $L_{\overline{\alpha}} = \langle X_\alpha, X_{-\alpha} \rangle_{\mathbb{F}}$ and $L_{\overline{\beta}} = \langle X_\beta, X_{-\beta} \rangle_{\mathbb{F}}$. Observe that the squared adjoint action $\mathrm{ad}^2_{X_\alpha}$ of X_α sends any element of $L_{\overline{\beta}}$ to zero: $[X_\alpha, [X_\alpha, X_\beta]] = [X_\alpha, N_{\alpha,\beta} X_{\alpha+\beta}] = 0$ as $2\alpha + \beta \notin \Phi$, and $[X_\alpha, X_{-\beta}] = 0$ since $\alpha - \beta \notin \Phi$. Similarly, $\mathrm{ad}^2_{X_{-\alpha}}(L_{\overline{\beta}}) = 0$.

However, the quadratic action ad_x^2 of a general element $x = t_1X_\alpha + t_2X_{-\alpha}$ ($t_1, t_2 \in \mathbb{F}$, both non-zero) of $L_{\overline{\alpha}}$ does not centralize $L_{\overline{\beta}}$. Indeed:

$$\begin{aligned}[x,[x,X_\beta]] &= t_1t_2\left([X_{-\alpha},[X_\alpha,X_\beta]] + [X_\alpha,[X_{-\alpha},X_\beta]]\right)\\ &= t_1t_2N_{-\alpha,\alpha+\beta}N_{\alpha,\beta}X_\beta,\end{aligned}$$

which is non-zero since $N_{-\alpha,\alpha+\beta}$ and $N_{\alpha,\beta}$ are both equal to 1 modulo 2.

Recall that we are given $L_{\overline{\alpha}}$ and $L_{\overline{\beta}}$. Fix a basis r_1, r_2 of $L_{\overline{\alpha}}$ and consider the element $x = r_1 + tr_2$, where $t \in \mathbb{F}$. It follows from the above observations that $\mathrm{ad}_x^2(L_{\overline{\beta}}) = 0$ if and only if x is a scalar multiple of X_α or $X_{-\alpha}$, so in order to find the frame elements among the $\mathbb{F}x$ for $t \in \mathbb{F}$ we have to solve $0 = [x,[x,y]]$ for all $y \in L_{\overline{\beta}}$. This reduces to the following system of equations in the unknown t:

$$\begin{aligned}0 = [x,[x,y]] &= [r_1 + tr_2, [r_1 + tr_2, y]]\\ &= [r_1,[r_1,y]] + t\left([r_1,[r_2,y]] + [r_2,[r_1,y]]\right) + t^2[r_2,[r_2,y]].\end{aligned}$$

This system consists of at most $2 \cdot 3 = 6$ quadratic equations over $\mathbb{F}$ in t, since $\dim(L_{\overline{\beta}}) = 2$ (which gives 2 independent choices for y) and $[r_i,[r_j,y]]$ are in $\langle L_{\overline{\beta}}\rangle_L$, which is at most 3-dimensional. We know there is a solution as H is split. If $\mathbb{F} = \mathrm{GF}(q)$, solving such a quadratic equation is equivalent to solving $\log(q)$ equations in $\log(q)$ variables over $\mathrm{GF}(2)$ (as $p = 2$ is fixed), requiring $O^\sim((\log q)^3)$ arithmetic operations, or $O^\sim((\log q)^4)$ elementary operations.

For more general Lie algebras L, the solutions for Lie subalgebras of type A_2 normalized by H will be part of a Chevalley frame. These parts can be found inside any two-dimensional root space $V \in E$, provided there is at least one other two-dimensional root space $V' \in E$ such that $\langle V, V'\rangle_L$ is of type A_2. So, if all root spaces in E are 2-dimensional and $\mathbb{F} = \mathrm{GF}(q)$, this method needs $O(n^2)$ root spaces V to be analysed (at a cost of $O^\sim(n^8(\log q)^4)$ each), so that $\mathcal{X}$ will be found in $O^\sim(n^{10}(\log q)^4)$ elementary operations.

4.5.2 G_2 in characteristic 3

Secondly, we consider the Lie algebra $L = L_{\mathbb{F}}(\mathrm{G}_2)$ of the root datum of type G_2 over an effective field $\mathbb{F}$ of characteristic 3. By Proposition 4.2 there are 8 root spaces. It is readily verified that $\dim(L_{\overline{\alpha}}) = 1$ if α is a short root and $\dim(L_{\overline{\alpha}}) = 3$ if α is a long root of Φ. In particular, the short root spaces belong to $\mathcal{X}$ and it remains to split the two long root spaces.

Consider one of the two three-dimensional root spaces in E, say $V = \mathbb{F}X_{\alpha_2} + \mathbb{F}X_{3\alpha_1+\alpha_2} + \mathbb{F}X_{-3\alpha_1-2\alpha_2}$. The left multiplications on V by the short roots are easily obtained from (CB1)–(CB4); these are given in Table 4.7.

Although we have not yet identified the roots, we can identify the three pairs of one-dimensional root spaces $\{\mathbb{F}X_\alpha, \mathbb{F}X_{-\alpha}\}$, for $\alpha \in \Phi$ short, since $L_{\overline{-\alpha}}$ is the unique one-dimensional root space with root $-\overline{\alpha}$. From this observation and Table 4.7 it follows that we can obtain the triple $\mathbb{F}X_\beta$ ($\beta \in \{\alpha_2, 3\alpha_1 + \alpha_2, -3\alpha_1 + 2\alpha_2\}$) as

	X_{α_2}	$X_{3\alpha_1+\alpha_2}$	$X_{-3\alpha_1-2\alpha_2}$
X_{α_1}	$X_{\alpha_1+\alpha_2}$	0	0
$X_{-\alpha_1}$	0	$X_{2\alpha_1+\alpha_2}$	0
$X_{\alpha_1+\alpha_2}$	0	0	$X_{-2\alpha_1-\alpha_2}$
$X_{-\alpha_1-\alpha_2}$	$-X_{\alpha_1}$	0	0
$X_{2\alpha_1+\alpha_2}$	0	0	$-X_{-\alpha_1}$
$X_{-2\alpha_1-\alpha_2}$	0	$-X_{\alpha_1}$	0

Table 4.7: Part of the G_2 multiplication table

follows:

$$\begin{aligned}
\mathbb{F}X_{\alpha_2} &= C_V(L_{\overline{2\alpha_1+\alpha_2}} + L_{\overline{-2\alpha_1-\alpha_2}}),\\
\mathbb{F}X_{3\alpha_1+\alpha_2} &= C_V(L_{\overline{\alpha_1+\alpha_2}} + L_{\overline{-\alpha_1-\alpha_2}}),\\
\mathbb{F}X_{-3\alpha_1-2\alpha_2} &= C_V(L_{\overline{\alpha_1}} + L_{\overline{-\alpha_1}}).
\end{aligned}$$

For the other three-dimensional space, the same approach is used. This completes the search for the Chevalley frame $\mathcal{X}$.

4.5.3 D_4 in characteristic 2

Thirdly, we consider the Lie algebras with Dynkin diagram of type D_4 over an effective field $\mathbb{F}$ of characteristic 2. As mentioned in Section 4.4, there are three cases:

L^{ad}: the adjoint root datum (12 two-dimensional root spaces);

L^{sc}: the simply connected root datum (3 eight-dimensional root spaces);

$L^{(1)}, L^{(3)}, L^{(4)}$: the intermediate root data (6 four-dimensional root spaces).

The three intermediate root data all give rise to the same Lie algebra up to isomorphism (by triality), so we will restrict ourselves to the study of L^{ad}, L^{sc}, and $L^{(1)}$. It is straightforward to verify that L^{ad} has a 26-dimensional ideal I^{ad} (see [Hog82, Theorem 2.1], or [Hog78] for more details), linearly spanned by X_α ($\alpha \in \Phi$), $(\alpha_1^\vee + \alpha_3^\vee + \alpha_4^\vee) \otimes 1$, and $\alpha_2^\vee \otimes 1$. This ideal can be found, for example, by use of the Meat-axe.

Similarly, L^{sc} has a 2-dimensional ideal I (spanned by $(\alpha_1^\vee + \alpha_4^\vee) \otimes 1$ and $(\alpha_3^\vee + \alpha_4^\vee) \otimes 1$). Let $I^{\text{sc}} = L^{\text{sc}}/I$ be the 26-dimensional Lie algebra obtained by computing in L^{sc} modulo I. Finally, $L^{(1)}$ has a 1-dimensional ideal I (spanned by $\alpha_4 \otimes 1$), and a 27-dimensional ideal I' (spanned by $\alpha_4 \otimes 1$ and X_α, $\alpha \in \Phi$). We let $I^{(\text{a})} = I'/I$. Again, the 26-dimensional ideal is easily found by means of the Meat-axe.

Thus we have constructed three 26-dimensional Lie algebras: I^{ad}, I^{sc}, and $I^{(\text{a})}$. By results of Chevalley (cf. [Jan03, Part 2, Cor. 2.7]) they are isomorphic, so from now on we let I be one of these 26-dimensional Lie algebras. The Lie algebra I is simple. Its derivation algebra $\text{Der}(I)$ is a Lie algebra of type F_4, and thus has 12 two-dimensional root spaces and 3 eight-dimensional root spaces.

Using a procedure similar to the one for G_2 over characteristic 3 described in Section 4.5.2, we can break up the eight-dimensional spaces of E into two-dimensional spaces, giving us 24 two-dimensional spaces. These two-dimensional spaces may then be broken up into one-dimensional spaces by the procedure [A_2]. The last step in the process is "pulling back" the relevant one-dimensional spaces from $\mathrm{Der}(I)$ to I. But this is straightforward, since I is an ideal of $\mathrm{Der}(I)$ by construction.

4.5.4 G_2 in characteristic 2

As noted in [Ste61, Section 2.6], in the exceptional case $R(p) = G_2(2)$, the Lie algebra L is isomorphic to the unique 14-dimensional ideal of the Chevalley Lie algebra L^{A} of adjoint type A_3 over $\mathbb{F}$. In particular, $\mathrm{Der}(L)$ contains a copy of L^{A}. We use this fact by finding a split maximal toral subalgebra H' inside $C_{\mathrm{Der}(L)}(H)$ so that $H \subseteq H'$. For then we can calculate the Chevalley frame $\mathcal{X}^{A}$ inside the Lie subalgebra $\langle L, H'\rangle_{\mathrm{Der}(L)}$ of $\mathrm{Der}(L)$ with respect to H', which is of type A_3 by the above observation.

The Chevalley frame $\mathcal{X}$ of L is now simply the part of $\mathcal{X}^{A}$ that lies inside L.

4.5.5 ${B_2}^{sc}$ in characteristic 2

We consider the Chevalley Lie algebra L of type ${B_2}^{sc}$ over an effective field $\mathbb{F}$ of characteristic 2 with split maximal toral subalgebra $H = \mathbb{F}h_1 + \mathbb{F}h_2$. This is a particularly difficult case, as the automorphism group of L is quite big: $\mathrm{Aut}(L) = G \ltimes (\mathbb{F}^{+})^4$ [Hog78, Theorem 14.1], where G is the Chevalley group of adjoint type B_2 over $\mathbb{F}$ and $\mathbb{F}^{+}$ refers to the additive group of $\mathbb{F}$. As a consequence, there is more choice in finding the frame than in the previous cases.

To begin, we take L_0 to be the $(0,0)$-root space of H on L, and L_1 to be the $(1,0)$-root space of H on L. It is easily verified that $L_0 = \langle H, X_{\pm\alpha_1}, X_{\pm(\alpha_1+2\alpha_2)}\rangle_{\mathbb{F}}$ (that is, the linear span of H and the long root elements) and $L_1 = \langle X_{\pm\alpha_2}, X_{\pm(\alpha_1+\alpha_2)}\rangle_{\mathbb{F}}$ (the linear span of the short root elements). We proceed in three steps.

[$\mathbf{B_2}^{sc}$.**1**]. The subalgebra L_0 has Dynkin type $A_1 \oplus A_1$. We may split it (non-uniquely) into two subalgebras of type A_1 using a direct sum decomposition procedure. This is a procedure that can be carried out with standard linear algebra arithmetic for a fixed dimension (6, in this case); see e.g., [dG00, Section 1.15].

[$\mathbf{B_2}^{sc}$.**2**]. Let A be one of these subalgebras of L_0 of type A_1. Assume for the sake of reasoning that $A = \langle X_{\pm\alpha_1}\rangle_L$, the Lie subalgebra of L generated by X_{α_1} and $X_{-\alpha_1}$. Since $[A, L_1] = L_1$ we may view L_1 as a four-dimensional A-module, and hence apply the Meat-axe [Hol98, HEO05] to find a proper irreducible A-submodule M of L_1. This will be a submodule of the form

$$M = \langle t_1 X_{\alpha_2} + t_2 X_{-\alpha_1-\alpha_2}, t_1 X_{\alpha_1+\alpha_2} + t_2 X_{-\alpha_2}\rangle_{\mathbb{F}}, \quad t_1, t_2 \in \mathbb{F}.$$

We take b_1, b_2 to be a basis of M, and add $C_A(b_2)$ and $C_A(b_1)$ to $\mathcal{X}$. These two spaces are indeed one-dimensional and coincide with the original $\mathbb{F}X_{\pm\alpha_1}$ if $b_1 \in \mathbb{F}(t_1 X_{\alpha_2} + t_2 X_{-\alpha_1-\alpha_2})$ and $b_2 \in \mathbb{F}(t_1 X_{\alpha_1+\alpha_2} + t_2 X_{-\alpha_2})$. This exhibits part of the freedom of choice induced by the factor $(\mathbb{F}^{+})^4$ in $\mathrm{Aut}(L)$.

We repeat this procedure for both subalgebras of type A_1 found in the first step. The result is the part of the Chevalley frame $\mathcal{X}$ inside L_0. In fact, due to our method, we can make an identification of the long roots $\pm\alpha_1$, $\pm(\alpha_1+2\alpha_2)$ with the four elements of $\mathcal{X}$ found. In what follows we will work with such a choice so that we have the elements $\mathbb{F}X_{\alpha_1}$, $\mathbb{F}X_{-\alpha_1}$, $\mathbb{F}X_{\alpha_1+2\alpha_2}$, $\mathbb{F}X_{-\alpha_1-2\alpha_2}$ in $\mathcal{X}$ as well as the correspondence with the roots in Φ suggested by the subscripts.

[$\mathbf{B_2}^{\mathrm{sc}}$**.3**]. We find the part of $\mathcal{X}$ inside L_1 as follows. $\mathbb{F}X_{\alpha_1+\alpha_2}$ coincides with $C_{L_1}(\mathbb{F}X_{\alpha_1}, \mathbb{F}X_{\alpha_1+2\alpha_2})$. Having computed this element of $\mathcal{X}$, we finish by taking

$$\begin{aligned}\mathbb{F}X_{\alpha_2} &= [\mathbb{F}X_{\alpha_1+\alpha_2}, \mathbb{F}X_{-\alpha_1}],\\ \mathbb{F}X_{-\alpha_1-\alpha_2} &= [\mathbb{F}X_{\alpha_2}, \mathbb{F}X_{-\alpha_1-2\alpha_2}],\\ \mathbb{F}X_{-\alpha_2} &= [\mathbb{F}X_{\alpha_1-\alpha_2}, \mathbb{F}X_{\alpha_1}].\end{aligned}$$

This completes the search for $\mathcal{X}$ in the case $B_2{}^{\mathrm{sc}}(2)$ and establishes that its running time is $O^{\sim}(\log q)$.

4.5.6 $C_n{}^{\mathrm{sc}}$ in characteristic 2

We consider the Chevalley Lie algebra L of type $C_n{}^{\mathrm{sc}}$ over an effective field $\mathbb{F}$ of characteristic 2. Here $n \geq 3$, so that the multiplicity of $\overline{0}$ is strictly larger than 4. Let h_z be a basis of the 1-dimensional center of L, inside the split maximal toral subalgebra H of L. This case is a generalisation of the $B_2{}^{\mathrm{sc}}$ case described in Section 4.5.5. We again take L_0 to be the 0-root space of H on L, so that L_0 is $3n$-dimensional and consists of H and the root spaces corresponding to the long roots. Similar to the previous case, $L_0 \cong A_1 \oplus \cdots \oplus A_1$ (n constituents), and again the decomposition is not unique. We describe how to find such a decomposition.

We let $\mathcal{F}$ be the set of $\binom{n}{2}$ four-dimensional root spaces (cf. Table 4.4). In the root system of type C_n each of these corresponds to the four roots $\pm\varepsilon_i \pm \varepsilon_j$ for some $i, j \in \{1, \ldots, n\}$ with $i \neq j$. Our first task is to split L_0 into subalgebras of type A_1 in a way compatible with $\mathcal{F}$. To this end, we let Γ be the graph with vertex set $\mathcal{F}$, and edges $f \sim g$ whenever $f \neq g$ and $[f, g] \neq 0$.

Let Δ be a maximal coclique of Γ of size $n-1$, so that Δ consists of $n-1$ elements of $\mathcal{F}$ such that $[f, g] = 0$ for all $f, g \in \Delta$. This means that, for a particular $i \in \{1, \ldots, n\}$, the set $\Delta \subseteq \mathcal{F}$ corresponds to those four-spaces in $\mathcal{F}$ that arise from the roots $\pm\varepsilon_i \pm \varepsilon_j$, where $j \in \{1, \ldots, n\} \setminus \{i\}$. Let $\overline{\Delta} = \Gamma - \Delta$, so that $\overline{\Delta}$ contains precisely the four-dimensional spaces corresponding to $\pm\varepsilon_k \pm \varepsilon_l$ with $k, l \neq i$.

Now compute the centralizer A in L_0 of all spaces in $\overline{\Delta}$. Then A coincides with $\langle X_{\pm\gamma}, \gamma^\vee \otimes 1, h_z\rangle_{\mathbb{F}}$ for the long root $\gamma = 2\varepsilon_i$. Using a direct sum decomposition procedure we find the Lie subalgebra A' of A such that $A = A' \oplus \mathbb{F}h_z$, where $A' = \langle X_{\pm\gamma}, \gamma^\vee \otimes 1\rangle_{\mathbb{F}}$. The subalgebra A' is one of the type A_1 constituents of L_0 we are after. Thus, by repeating this procedure for each maximal coclique of Γ of size $n-1$, we obtain a decomposition of L_0 into n subalgebras of type A_1. We will denote by $\mathcal{A}$ the set of these n subalgebras.

Now we continue as in the $B_2{}^{\mathrm{sc}}$ case: For each element of $\mathcal{A}$ we use the procedure labelled [$B_2{}^{\mathrm{sc}}$.2] to find suitable elements $\mathbb{F}X_{\pm\gamma}$ for $\mathcal{X}$. For each four-dimensional space $K \in \mathcal{F}$ we then use distinct $S_1, S_2 \in \mathcal{A}$ satisfying $[K, S_1] \neq 0$, $[K, S_2] \neq 0$ and these $\mathbb{F}X_{\pm\gamma}$ to execute a [$B_2{}^{\mathrm{sc}}$.3] procedure. Thus, we find the part of the frame inside K.

If $n = 3$ splitting L_0 has to be done in a slightly different way, but as this is only a slight modification of the algorithm we will not go into details here. This completes the Chevalley frame finding in the case $\mathrm{C}_n{}^{\mathrm{sc}}(2)$. Its running time involves $O(n^2)$ executions of parts of the algorithm of Section 4.5.5, which is however dominated by the time $O^{\sim}(n^{10}(\log q)^4)$ needed for method [A$_2$].

4.5.7 $\mathrm{A}_1{}^{\mathrm{sc}}$ in characteristic 2

We consider the Chevalley Lie algebra L of type $\mathrm{A}_1{}^{\mathrm{sc}}$ over an effective field $\mathbb{F}$ of characteristic 2, consisting of basis elements X_α, $X_{-\alpha}$, and h, where $\langle h \rangle_{\mathbb{F}} = H$. It follows immediately from the structure of the root datum of type $\mathrm{A}_1{}^{\mathrm{sc}}$ that $[X_\alpha, h] = [X_{-\alpha}, h] = 0$ and $[X_\alpha, X_{-\alpha}] = h$ (see also Section 1.9.3).

Now let x, y be two elements of L, so $x = x_1 X_\alpha + x_2 X_{-\alpha} + x_3 h$ and $y = y_1 X_\alpha + y_2 X_{-\alpha} + y_3 h$ (where $x_i, y_i \in \mathbb{F}$) and observe:

$$[x, y] = [x_1 X_\alpha + x_2 X_{-\alpha} + x_3 h, y_1 X_\alpha + y_2 X_{-\alpha} + y_3] = (x_1 y_2 + x_2 y_1) h,$$

so that $\mathcal{X} = \{x, y\}$ satisfies the requirements for a Chevalley frame as long as $\langle x, y, h \rangle_{\mathbb{F}} = L$ and $[x, y] \neq 0$. However, this is equivalent to demanding that

$$\det \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix} \neq 0,$$

which happens for a random choice of x and y in a fraction of $(q^2 - 1)(q^2 - q)/q^4$ of the cases. Observe that, for $q = 2$, this fraction is equal to $\frac{3}{8}$. This implies via straightforward calculation in particular that in order to have a failure probability smaller than ε, the required number N_ε of random choices satisfies $N_\varepsilon > -\log(\varepsilon)/\log(\frac{3}{8})$.

If on the other hand $q > 2$ the probability of success is equal to

$$\frac{(q^2-1)(q^2-q)}{q^4} > \frac{(q^2-q)^2}{q^4} = \frac{q^2 - 2q + 1}{q^2} > 1 - \frac{2}{q}.$$

This straightforwardly reduces to the requirement that $N_\varepsilon > -\log(\varepsilon)/\log(\frac{q}{2})$.

We summarize the results of this section.

Proposition 4.8. *Given L, H, R, the set $\overline{\Phi}$ of roots of H on L, and the root spaces E, the Las Vegas procedure* FindFrame *finds a Chevalley frame. For $\mathbb{F} = \mathrm{GF}(q)$, it runs in time $O^{\sim}(n^{10}(\log q)^4)$.*

Proof As mentioned in Section 4.3 this procedure is trivial in all cases except those mentioned in Table 4.4, and for each of the cases in Table 4.4 we have presented a solution. Recall that $|\Phi| \leq \dim(L) = O(n^2)$.

The timing of method [A$_2$] is dealt with in Section 4.5.1, which produces the bound stated in the proposition.

```
IdentifyRoots
in:    The Lie algebra $L$ over an effective field $\mathbb{F}$ of a split reductive algebraic
       group, a split maximal toral subalgebra $H$ of $L$,
       a root datum $R = (X, \Phi, Y, \Phi^\vee)$, and a Chevalley frame $\mathcal{X}$.
out:   A bijection $\iota : \Phi \to \mathcal{X}$.
begin
  if $R(p) \in \{\mathrm{B}_n(2), \mathrm{C}_n(2), \mathrm{F}_4(2), \mathrm{G}_2(2), \mathrm{G}_2(3)\}$ then
    find $\iota$ using a specialized procedure.
  else
    /* Find fundamental roots */
    let $\zeta : \mathcal{X} \times \mathcal{X} \to \mathbb{Z}$ be the Cartan integers computing using Lemma 4.12,
    let $\mathcal{X}^\mathrm{F}$ = FindFundamentals$(L, \Phi, \mathcal{X}, \zeta)$,
    let $\iota$ = IdentifyByFundamentals$(L, \Phi, \mathcal{X}, \zeta, \mathcal{X}^\mathrm{F})$.
  end if,
  return $\iota$.
end
```

Algorithm 4.9: Identifying the roots

Method [C] concerns $O(n^2)$ instances of standard linear algebra arithmetic on spaces of bounded dimension, and so its running time is dominated again by the time spent on the [A$_2$] method.

Method [Der] involves the computation of parts of the Lie algebra of derivations. Computing the full Lie algebra of derivations in instances like $D_n{}^{\mathrm{sc}}(2)$ would take running time $O^{\sim}(n^{12} \log q)$. However, we only carry out this procedure for Lie algebras of bounded dimension (the bound being 28, which occurs for type D$_4$) or compute the part of $\mathrm{Der}(L)$ that leaves invariant H and the corresponding decomposition into root spaces (which reduces the running time to $O^{\sim}(n^8 \log q)$). Therefore, the stated bound suffices.

The timing of method [A$_1{}^{\mathrm{sc}}$] is dealt with in Section 4.5.7.

Finally, according to Table 4.4, Method [B$_2{}^{\mathrm{sc}}$] with unbounded n only occurs in the cases treated in Section 4.5.6, where the time analysis is already given. □

4.6 Root identification

In this section we clarify Step 3 of the ChevalleyBasis algorithm 4.3. We first describe the general principle to compute the Cartan integers in Lemmas 4.11 and 4.12, and describe how the roots may be identified using these integers in Algorithms 4.13–4.20. The cases not covered by Lemma 4.12 are dealt with in Section 4.6.3.

The routine IdentifyRoots takes as input a Chevalley Lie algebra L, a split maximal toral subalgebra H of L, the root datum R, the set of roots $\overline{\Phi} = \Phi(L, H)$, and the Chevalley frame $\mathcal{X}$ found in the previous step (Section 4.5). It returns a bijection $\iota : \Phi \to \mathcal{X}$ so that, up to scaling, $(\iota(\alpha))_{\alpha \in \Phi}$ will be the root element part of a Chevalley basis.

An important tool to make this identification are the Cartan integers $\langle \alpha, \beta^\vee \rangle$. Cartan integers may be computed using root chains.

Lemma 4.10 ([Car72, Section 3.3])**.** *Let $\alpha, \beta \in \Phi$. Suppose p and q are the largest non-negative integers such that $-p\alpha + \beta \in \Phi$ and $q\alpha + \beta \in \Phi$. Then $\langle \beta, \alpha^\vee \rangle = p - q$.*

We use this lemma by computing such a chain in the set of roots $\overline{\Phi}$ corresponding to the Chevalley frame $\mathcal{X} = \{\mathbb{F}X_\alpha \mid \alpha \in \Phi\}$. However, as these roots are computed from the Lie algebra L over $\mathbb{F}$ itself, they are elements of $\mathbb{F}^n$ rather than $\mathbb{Z}^n$.

A straightforward verification of cases for Chevalley Lie algebras arising from root systems of rank 2 shows that the chain can simply be computed in terms of the root spaces (which are defined over $\mathbb{F}^n$), except if the characteristic is 2 or 3. So in those cases, a different method for computing $\langle \alpha, \beta^\vee \rangle$ is needed.

Lemma 4.11. *Suppose that $L = L_{\mathbb{F}}(R)$ is a Chevalley Lie algebra with respect to an irreducible root datum $R = (X, \Phi, Y, \Phi^\vee)$ over the field $\mathbb{F}$ of characteristic 2 or 3. Let H be the standard split maximal toral subalgebra of L. Suppose furthermore that $X_\alpha, X_{-\alpha}, X_\beta, X_{-\beta}$ are four vectors spanning root spaces corresponding to $\alpha, -\alpha, \beta, -\beta \in \Phi$, respectively, and $\alpha \neq \pm\beta$.*

If Φ is simply laced, then $\langle \beta, \alpha^\vee \rangle = P - Q$, where

$$P = \begin{cases} 0 & \text{if } [X_{-\alpha}, X_\beta] = 0 \\ 1 & \text{if } [X_{-\alpha}, X_\beta] \neq 0 \end{cases}, \quad Q = \begin{cases} 0 & \text{if } [X_\alpha, X_\beta] = 0 \\ 1 & \text{if } [X_\alpha, X_\beta] \neq 0 \end{cases}.$$

If Φ is doubly laced and $\mathrm{char}(\mathbb{F}) \neq 2$, *then $\langle \beta, \alpha^\vee \rangle = P - Q$, where*

$$\begin{aligned} P &= \begin{cases} 0 & \text{if } [X_{-\alpha}, X_\beta] = 0 \\ 1 & \text{if } [X_{-\alpha}, X_\beta] \neq 0, [X_{-\alpha}, [X_{-\alpha}, X_\beta]] = 0 \\ 2 & \text{if } [X_{-\alpha}, [X_{-\alpha}, X_\beta]] \neq 0 \end{cases} \\ Q &= \begin{cases} 0 & \text{if } [X_\alpha, X_\beta] = 0 \\ 1 & \text{if } [X_\alpha, X_\beta] \neq 0, [X_\alpha, [X_\alpha, X_\beta]] = 0 \\ 2 & \text{if } [X_\alpha, [X_\alpha, X_\beta]] \neq 0 \end{cases} \end{aligned}$$

Proof For any $\gamma, \delta \in \Phi$, let $p_{\gamma\delta}$ and $q_{\gamma\delta}$ be the biggest non-negative integers such that $-p_{\gamma\delta}\gamma + \delta \in \Phi$ and $q_{\gamma\delta}\gamma + \delta \in \Phi$. Recall from (CB4) that, if $\gamma + \delta \in \Phi$, then $[X_\gamma, X_\delta] = N_{\gamma,\delta} X_{\gamma+\delta}$, where $N_{\gamma,\delta} = \pm(p_{\gamma\delta} + 1)$.

If Φ is simply laced, the subsystem of Φ generated by $\pm\alpha, \pm\beta$ is of type $\mathrm{A}_1\mathrm{A}_1$ or of type A_2. Then $\alpha + \beta \in \Phi$ implies $\alpha - \beta \notin \Phi$, so $N_{\alpha,\beta} = \pm 1$ and $N_{\beta,\alpha} = \pm 1$. This means that, regardless of the characteristic, we can reconstruct $p_{\alpha\beta}$ and $q_{\alpha\beta}$ by the procedure described in the lemma, and thus compute $\langle \beta, \alpha^\vee \rangle = p_{\alpha\beta} - q_{\alpha\beta}$ by Lemma 4.10.

If Φ is doubly laced and $\mathrm{char}(\mathbb{F}) \neq 2$, the subsystem of Φ generated by $\pm\alpha, \pm\beta$ is of type $\mathrm{A}_1\mathrm{A}_1$, A_2, or B_2. (Note that G_2 never occurs inside a bigger root system.) In the first two cases the previous argument applies, so assume $\pm\alpha, \pm\beta$ generate a subsystem of Φ of type B_2. Similarly to the previous case, if $\alpha + \beta \in \Phi$ then $\alpha - 2\beta \notin \Phi$, so that $N_{\alpha,\beta}, N_{\beta,\alpha} \in \{\pm 1, \pm 2\}$. In particular, since $\mathrm{char}(\mathbb{F}) \neq 2$, we find that both $N_{\alpha,\beta}$ and $N_{\beta,\alpha}$ are non-zero, so that we can reconstruct $p_{\alpha\beta}$ and $q_{\alpha\beta}$ by the procedure described in the theorem, and thus compute $\langle \beta, \alpha^\vee \rangle = p_{\alpha\beta} - q_{\alpha\beta}$ by Lemma 4.10. □

Lemma 4.12. *Suppose that L is a Chevalley Lie algebra over $\mathbb{F}$ with respect to an irreducible root datum $R = (X, \Phi, Y, \Phi^\vee)$, H the split maximal toral subalgebra of L, and X_α and X_β are two root elements whose roots with respect to H are $\overline{\alpha}$ and $\overline{\beta}$ for certain $\overline{\alpha}, \overline{\beta} \in \overline{\Phi}$. Suppose, furthermore, that at least one of the following statements holds.*

(i) $\mathrm{char}(\mathbb{F}) \notin \{2, 3\}$*;*

(ii) Φ *is simply laced;*

(iii) Φ *is doubly laced and* $\mathrm{char}(\mathbb{F}) \neq 2$.

The Cartan integer $\langle \alpha, \beta^\vee \rangle$ can be computed from the available data in $O^\sim(n^{10} \log q)$ elementary operations.

Proof Observe first of all that the case where $\alpha = \beta$ is easily caught, for example by computing $\dim(\langle \mathbb{F}X_\alpha, \mathbb{F}X_\beta \rangle_{\mathbb{F}})$. Obviously then $\langle \alpha, \beta^\vee \rangle = 2$.

Moreover, we can distinguish the case where $\alpha = -\beta$ as follows. If $\mathrm{char}(\mathbb{F}) \neq 2$ we may simply test whether $\overline{\alpha} = -\overline{\beta}$. If on the other hand $\mathrm{char}(\mathbb{F}) = 2$, we find the sets $\{\{\gamma, -\gamma\} \mid \gamma \in \Phi^+\}$ as an auxiliary result of the algorithm FindFrame described in introduction of Section 4.5.1. If $\alpha = -\beta$, then of course $\langle \alpha, \beta^\vee \rangle = -2$.

So assume $\alpha \neq \pm\beta$. Now if (i) holds we compute $\langle \alpha, \beta^\vee \rangle$ from the roots $\overline{\alpha}$ and $\overline{\beta}$ using Lemma 4.10, as mentioned earlier. Suppose, therefore, (ii) or (iii) holds. We can find $\mathbb{F}X_{-\alpha}$ and $\mathbb{F}X_{-\beta}$ either simply by considering $\{\overline{\gamma} \mid \gamma \in \Phi\}$ (if $\mathrm{char}(\mathbb{F}) \neq 2$) or as an auxiliary result of FindFrame (if $\mathrm{char}(\mathbb{F}) = 2$). This leaves us in a position where we may apply Lemma 4.11, and thus find $\langle \alpha, \beta^\vee \rangle$.

Finally, the time needed does not exceed the time needed for standard linear algebra arithmetic for each pair of roots, that is, $O^\sim(n^4 \cdot n^6 \log q)$. □

4.6.1 Selecting a set of fundamental roots

We restrict to the cases assumed in Lemma 4.12, so that we obtain Cartan integers as a map $\zeta : \mathcal{X} \times \mathcal{X} \to \mathbb{Z}$. (The other cases are dealt with in Section 4.6.3.) We claim that ζ provides a root system structure of $\mathcal{X}$. Indeed, if we let $N = |\mathcal{X}|$ and we fix any order of elements of $\mathcal{X}$, i.e., $\mathcal{X} = \{x_1, \ldots, x_N\}$, we find a new map $\zeta : \mathcal{X} \to \mathbb{Z}^N$ defined by

$$\zeta(x) = (\zeta(x, x_1), \ldots, \zeta(x, x_N)).$$

Since the Cartan integers are elements of $\mathbb{Z}$ rather than $\mathbb{F}$, the vectors $\zeta(x) \in \mathbb{Z}^N$ reflect the structure of the root system Φ that exists in $\mathcal{X}$ much better than $\mathcal{X}$ itself does. We may now first find a set of positive roots, and then a set of fundamental roots, using the procedure described in Algorithm 4.13. See [Car72, Section 2.1] for the justification of this procedure.

4.6.2 Identifying the roots

The previous section, in particular Algorithm 4.13, gives us a set of fundamental roots. In Algorithm 4.14 we map these onto the standard fundamental roots of Φ,

```
FindFundamentals
in:   $L, \Phi, \mathcal{X}$ as in Algorithm 4.9, Cartan integers $\zeta : \mathcal{X} \times \mathcal{X} \to \mathbb{Z}$,
out:  A set $\mathcal{X}^{\mathrm{F}} \subseteq \mathcal{X}$ of fundamental roots.
begin
    fix an ordering on $\mathcal{X}$, so that $\mathcal{X} = \{x_1, \ldots, x_N\}$,
    let $\zeta : \mathcal{X} \to \mathbb{Z}^N$ be defined by $\zeta(x) = (\zeta(x, x_1), \ldots, \zeta(x, x_N))$,
    /* Identify a positive half */
    let $p(x)$, for $x \in \mathcal{X}$, be the assertion that

        $\zeta(x)_i > 0, \text{ where } i = \min\{j \in \{1, \ldots, N\} \mid \zeta(x)_j \neq 0\}$

    i.e., the first non-zero entry of $\zeta(x)$ is positive,
    let $\mathcal{X}^+ = \{x \in \mathcal{X} \mid p(x)\}$,
    /* Exclude non-fundamentals */
    let $N = \{x \in \mathcal{X}^+ \mid \exists y, z \in \mathcal{X}^+ \text{ such that } \zeta(x) = \zeta(y) + \zeta(z)\}$,
    return $\mathcal{X}^+ \backslash N$.
end
```

Algorithm 4.13: Finding a set of fundamental roots

using algorithms depending on the type of root datum, and subsequently extend this identification to the other elements of the Chevalley frame.

4.6.3 The remaining cases

Lemma 4.12 enables us to compute Cartan integers and obtain an identification ι in many cases. For the cases not covered by this lemma we proceed as follows to construct ι directly.

- $\mathrm{B}_n(2)$: The short root spaces generate an ideal, I say, of L found by the Meataxe, and the root eigenspaces of H that do not lie in I belong to long roots. The latter root spaces generate a subalgebra of type D_n. This Lie algebra is simply laced, so the root identification problem can be solved within this subalgebra. This identifies the long root spaces. Now, for $i = 1, \ldots, n$, let the short root γ_i be $\alpha_i + \alpha_{i+1} + \cdots + \alpha_n$ and let $\alpha_0 = \alpha_1 + 2\alpha_2 + 2\alpha_3 + \cdots + 2\alpha_n$ be the (long) highest root. Observe then that $[X_{\alpha_0}, X_{-\gamma_1}] = X_{\gamma_2}$ and $[X_{\alpha_0}, X_{-\gamma_2}] = X_{\gamma_1}$, and $X_{-\gamma_1}$ and $X_{-\gamma_2}$ are the only short root elements that do not commute with X_{α_0}. This fact, together with the set of pairs $\{\{\gamma, -\gamma\} \mid \gamma \in \Phi^+\}$ obtained in FindFrame, allows us to find $X_{\pm\gamma_1}$ and $X_{\pm\gamma_2}$. Note that we have to execute this procedure at most twice, since there are only elements of $\mathcal{X}$ that could be identified with $X_{-\gamma_1}$, and the other short root elements are fixed once $X_{-\gamma_1}$ is fixed. The other short root elements can now be found by using relations such as $[X_{\gamma_i}, X_{-\alpha_i}] = X_{\gamma_{i+1}}$.

- $\mathrm{C}_n(2)$: The short root spaces generate an ideal of L of type D_n, so we execute a similar procedure as in the previous case.

```
IdentifyByFundamentals
in:     $L, \Phi, \mathcal{X}$ as in Algorithm 4.9, a set of fundamental roots $\Delta \subseteq \Phi$,
        Cartan integers $\zeta : \mathcal{X} \times \mathcal{X} \to \mathbb{Z}$, and
        a set $\mathcal{X}^{\mathrm{F}} \subseteq \mathcal{X}$ of fundamental roots.
out:    A bijection $\iota : \Phi \to \mathcal{X}$ such that $\zeta(\iota(\alpha), \iota(\beta)) = \langle \alpha, \beta^\vee \rangle$ for all $\alpha, \beta \in \Phi$,
begin
  recall the ordering on $\mathcal{X}$ and $\zeta : \mathcal{X} \to \mathbb{Z}^N$ from Algorithm 4.13,
  /* Identify fundamental roots */
  find $\iota : \Delta \to \mathcal{X}^{\mathrm{F}}$ using one of Algorithms 4.15-4.20,
  /* Extend to the non-fundamental roots */
  for $\gamma \in \Phi \backslash \Delta$ do
    let $c_\alpha$, for $\alpha \in \Delta$, be such that $\gamma = \sum_{\alpha \in \Delta} c_\alpha \alpha$,
    find $x \in \mathcal{X}$ satisfying $\zeta(x) = \sum_{\alpha \in \Delta} c_\alpha \zeta(\iota(\alpha))$,
    set $\iota(\gamma) = x$.
  end for,
  return $\iota$.
end
```

Algorithm 4.14: Identifying the roots given the fundamentals

```
IdentifyRootsAn
in:     all input of Algorithm 4.14,
out:    A map $\iota : \Delta \to \mathcal{X}^{\mathrm{F}}$ such that $\zeta(\iota(\alpha), \iota(\beta)) = \langle \alpha, \beta^\vee \rangle$ for all $\alpha, \beta \in \Delta$,
        provided $\Phi$ is of type $\mathrm{A}_n$,
begin
  let $\alpha_1, \ldots, \alpha_{\mathrm{rk}(\Phi)}$ be the fundamental roots, numbered as in Figure 1.4,
  /* Find one of the endpoints */
  find $x \in \mathcal{X}^{\mathrm{F}}$ such that $\left|\{y \in \mathcal{X}^{\mathrm{F}} \mid \zeta(x, y) = -1\}\right| = 1$,
  set $\iota(\alpha_1) = x$,
  /* Find the intermediate points, and the other endpoint */
  for $i = 2, \ldots, \mathrm{rk}(\Phi)$ do
    find $y \in \mathcal{X}^{\mathrm{F}} \backslash \{\iota(\alpha_1), \ldots, \iota(\alpha_{i-1})\}$ such that $\zeta(\iota(\alpha_{i-1}), y) = -1$,
    set $\iota(\alpha_i) = y$.
  end for,
  return $\iota$.
end
```

Algorithm 4.15: Identifying the fundamental roots (A_n case)

```
IdentifyRootsDn
in:   all input of Algorithm 4.14,
out:  A map $\iota : \Delta \to \mathcal{X}^{\mathrm{F}}$ such that $\zeta(\iota(\alpha), \iota(\beta)) = \langle \alpha, \beta^\vee \rangle$ for all $\alpha, \beta \in \Delta$,
      provided $\Phi$ is of type $\mathrm{D}_n$,
begin
  let $\alpha_1, \ldots, \alpha_{\mathrm{rk}(\Phi)}$ be the fundamental roots, numbered as in Figure 1.4,
  /* Find the point of degree 3 */
  find $t \in \mathcal{X}^{\mathrm{F}}$ such that $\left|\{y \in \mathcal{X}^{\mathrm{F}} \mid \zeta(t, y) = -1\}\right| = 3$,
  let $\iota(\alpha_{\mathrm{rk}(\Phi)-2}) = t$,
  /* Find the two endpoints */
  find distinct $x_1, x_2 \in \mathcal{X}^{\mathrm{F}}$ satisfying
    $\left|\{y \in \mathcal{X}^{\mathrm{F}} \mid \zeta(x_i, y) = -1\}\right| = 1$ and $\zeta(x_i, t) = -1$,
  set $\iota(\alpha_{\mathrm{rk}(\Phi)-1}) = x_1$ and $\iota(\alpha_{\mathrm{rk}(\Phi)}) = x_2$,
  /* Find the other points */
  for $i = \mathrm{rk}(\Phi) - 3, \ldots, 1$ do
    find $y \in \mathcal{X}^{\mathrm{F}} \backslash \{\iota(\alpha_{i+1}), \ldots, \iota(\alpha_{\mathrm{rk}(\Phi)})\}$ such that $\zeta(\iota(\alpha_{i+1}), y) = -1$,
    set $\iota(\alpha_i) = y$.
  end for,
  return $\iota$.
end
```

Algorithm 4.16: Identifying the fundamental roots (D_n case)

- $\mathrm{F}_4(2)$: The short roots generate generate an ideal of L of dimension 26 which together with the maximal toral subalgebra H gives a 28-dimensional subalgebra of type D_4, allowing the same procedure as before.

- $\mathrm{G}_2(3)$: Similarly to the previous cases, we use the fact that the short roots generate an ideal of L of type A_2, which is again simply laced.

- $\mathrm{G}_2(2)$: As described in Section 4.5.4, the manner in which the root spaces in L^{A} correspond to those in L is fixed. Therefore, we may use the roots identified in L^{A}, which is simply laced, to identify the roots in L.

4.6.4 Runtime analysis

The methods described lead to the following conclusion.

Proposition 4.21. *Given L over $\mathbb{F}$, H, $R = (X, \Phi, Y, \Phi^\vee)$, the set $\overline{\Phi}$ of roots of H on L, and a Chevalley frame $\mathcal{X}$, the routine* IdentifyRoots *finds a bijection $\iota : \Phi \to \mathcal{X}$ such that for all $\alpha, \beta \in \Phi$, $\alpha \neq \pm\beta$,*

$$[\iota(\alpha), \iota(\beta)] = \begin{cases} \iota(\alpha + \beta) & \text{if } \alpha + \beta \in \Phi \text{ and } N_{\alpha,\beta} \not\equiv 0 \pmod{p}, \\ \{0\} & \text{otherwise.} \end{cases}$$

For $\mathbb{F} = \mathrm{GF}(q)$, the routine needs $O^{\sim}(n^{10} \log q)$ elementary operations.

```
IdentifyRootsEn
in:     all input of Algorithm 4.14,
out:    A map $\iota : \Delta \to \mathcal{X}^{\mathrm{F}}$ such that $\zeta(\iota(\alpha), \iota(\beta)) = \langle \alpha, \beta^\vee \rangle$ for all $\alpha, \beta \in \Delta$,
        provided $\Phi$ is of type $\mathrm{E}_6$, $\mathrm{E}_7$, or $\mathrm{E}_8$,
begin
  let $\alpha_1, \ldots, \alpha_{\mathrm{rk}(\Phi)}$ be the fundamental roots, numbered as in Figure 1.4,
  /* Find the point of degree 3 */
  find $t \in \mathcal{X}^{\mathrm{F}}$ such that $\left|\{y \in \mathcal{X}^{\mathrm{F}} \mid \zeta(t, y) = -1\}\right| = 3$,
  set $\iota(\alpha_4) = t$,
  /* Find endpoint */
  find $u \in \mathcal{X}^{\mathrm{F}}$ such that $\left|\{y \in \mathcal{X}^{\mathrm{F}} \mid \zeta(x, y) = -1\}\right| = 1$ and $\zeta(x, t) = -1$,
  set $\iota(\alpha_2) = u$,
  /* Identify chains in two directions */
  find distinct $x_1, x_2 \in \mathcal{X}^{\mathrm{F}}$ such that $x_1, x_2 \neq u$, and $\zeta(x_1, t) = \zeta(x_2, t) = -1$,
  for $i = 1, 2$ do
    set the sequence $S_i = [t, x_i]$, the boolean $b =$ true, $m = 2$,
    while $b$ do
      if $y \in \mathcal{X}^{\mathrm{F}} \backslash S_i$ exists such that $\zeta(S_i[m], y) = -1$ then
        set $S_i[m+1] = y$ and $m = m + 1$.
      else
        let $b =$ false.
      end if.
    end while.
  end for,
  /* Map these chains onto the root system */
  if $|S_1| > |S_2|$ then swap $S_1$ and $S_2$.
  set $\iota(\alpha_1) = S_1[2]$, $\iota(\alpha_3) = S_1[3]$,
  for $i = 5, \ldots, \mathrm{rk}(\Phi)$ set $\iota(\alpha_i) = S_2[i-3]$,
  return $\iota$.
end
```

Algorithm 4.17: Identifying the fundamental roots (E_n case)

```
IdentifyRootsBCn
in:   all input of Algorithm 4.14,
out:  A map $\iota : \Delta \to \mathcal{X}^{\mathrm{F}}$ such that $\zeta(\iota(\alpha), \iota(\beta)) = \langle \alpha, \beta^\vee \rangle$ for all $\alpha, \beta \in \Delta$,
      provided $\Phi$ is of type $\mathrm{B}_n$ or of type $\mathrm{C}_n$,
begin
  let $\alpha_1, \ldots, \alpha_{\mathrm{rk}(\Phi)}$ be the fundamental roots, numbered as in Figure 1.4,
  /* Find the double bond */
  find $x, y \in \mathcal{X}^{\mathrm{F}}$ such that $\zeta(x, y) = -2$,
  if $R$ is of type $B$ then
    set $\iota(\alpha_{\mathrm{rk}(\Phi)-1}) = x$, $\iota(\alpha_{\mathrm{rk}(\Phi)}) = y$,
    let $t = x$.
  else if $R$ is of type $C$ then
    let $\iota(\alpha_{\mathrm{rk}(\Phi)-1}) = y$, $\iota(\alpha_{\mathrm{rk}(\Phi)}) = x$,
    let $t = y$.
  end if,
  /* Find the other points */
  for $i = \mathrm{rk}(\Phi) - 2, \ldots, 1$ do
    find $z \in \mathcal{X}^{\mathrm{F}} \backslash \{\iota(\alpha_{i+1}), \ldots, \iota(\alpha_{\mathrm{rk}(\Phi)})\}$ such that $\zeta(\iota(\alpha_{i+1}), z) = -1$,
    set $\iota(\alpha_i) = z$.
  end for,
  return $\iota$.
end
```

Algorithm 4.18: Identifying the fundamental roots (B_n / C_n case)

```
IdentifyRootsF4
in:   all input of Algorithm 4.14,
out:  A map $\iota : \Delta \to \mathcal{X}^{\mathrm{F}}$ such that $\zeta(\iota(\alpha), \iota(\beta)) = \langle \alpha, \beta^\vee \rangle$ for all $\alpha, \beta \in \Delta$,
      provided $\Phi$ is of type $\mathrm{F}_4$,
begin
  let $\alpha_1, \ldots, \alpha_{\mathrm{rk}(\Phi)}$ be the fundamental roots, numbered as in Figure 1.4,
  /* Find the double bond */
  find $x, y \in \mathcal{X}^{\mathrm{F}}$ such that $\zeta(x, y) = -2$,
  set $\iota(\alpha_2) = x$, $\iota(\alpha_3) = y$,
  /* Find the other two points */
  find $z \in \mathcal{X}^{\mathrm{F}}$ such that $\zeta(z, x) = -1$, and set $\iota(\alpha_1) = z$,
  find $z \in \mathcal{X}^{\mathrm{F}}$ such that $\zeta(z, y) = -1$, and set $\iota(\alpha_4) = z$,
  return $\iota$.
end
```

Algorithm 4.19: Identifying the fundamental roots (F_4 case)

```
IdentifyRootsG2
in:    all input of Algorithm 4.14,
out:   A map $\iota : \Delta \to \mathcal{X}^{\mathrm{F}}$ such that $\zeta(\iota(\alpha), \iota(\beta)) = \langle \alpha, \beta^\vee \rangle$ for all $\alpha, \beta \in \Delta$,
       provided $\Phi$ is of type $\mathrm{G}_2$,
begin
    let $\alpha_1, \dots, \alpha_{\mathrm{rk}(\Phi)}$ be the fundamental roots, numbered as in Figure 1.4,
    /* Find the triple bond */
    find $x, y \in \mathcal{X}^{\mathrm{F}}$ such that $\zeta(x, y) = -3$,
    set $\iota(\alpha_1) = x$, $\iota(\alpha_2) = y$,
    return $\iota$.
end
```

Algorithm 4.20: Identifying the fundamental roots (G_2 case)

Proof (of Proposition 4.21) Lemma 4.12 shows that in many cases we can compute Cartan integers. To this end, we need to compute $\langle \alpha, \beta^\vee \rangle$ for all $O(n^4)$ pairs of roots, and every computation of this type involves at most 6 multiplications in L, requiring a total of $O^\sim(n^{4+6} \log q)$ elementary operations. Once these numbers are computed, it takes $O(n^4)$ steps to select a set of simple roots and subsequently complete the bijection between Φ and $\mathcal{X}$ using Algorithms 4.13 and 4.14. This proves that we can make the required bijection in $O^\sim(n^{10} \log q)$ time for the cases covered by Lemma 4.12.

For the remainder of the proof, we can restrict ourselves to the cases not covered by Lemma 4.12. Here the procedure described provides ι directly, so we only need prove the last assertion of the proposition. As $\mathrm{G}_2(2)$ is directly reduced to a case already treated, it needs no further consideration. In each of the remaining cases, we need to compute a subalgebra or an ideal of L. Although this is hard in general, the fact that we have already found the Chevalley frame $\mathcal{X}$ and the fact that the subalgebra or ideal is a sum of elements from $\mathcal{X}$ imply that the computations take $O^\sim(n^{10} \log q)$ elementary operations. A bijection ι' from the relevant subsystem of Φ to the subset of $\mathcal{X}$ of root spaces lying in the ideal may then be identified in time $O^\sim(n^{10} \log q)$. Finally, extending ι' to the entirety of Φ is a straightforward task, requiring only standard linear algebra in L.

This shows that we can find the required bijection in the time stated for all cases. □

4.7 Conclusion

As discussed in Section 4.3 the more difficult steps of Algorithm 4.3 are FindFrame and IdentifyRoots. In Sections 4.5 (Proposition 4.8) and 4.6 (Proposition 4.21) we established that these steps can be dealt with in time $O^\sim(n^{10} (\log q)^4)$. This proves Theorem 4.1. We emphasize that this estimate is only asymptotic and refer to Section 4.8 for timings.

A primary goal in writing the Chevalley basis algorithm is to use it for conjugacy questions in simple algebraic groups G or finite groups $G(\mathrm{GF}(q))$ of rational points over $\mathrm{GF}(q)$. One of the complications in this application is the fact that the group $\mathrm{Aut}(L)$ may be larger than $G(\mathrm{GF}(q))$ (cf. [Hog78, Section 14]). To deal with this complication, a method is needed to write an arbitrary automorphism of L as a product of an element from $G(\mathrm{GF}(q))$ and a particular coset representative of $G(\mathrm{GF}(q))$ in $\mathrm{Aut}(L)$. Such a method is in [CMT04] and is also used in [CM09].

4.8 Notes on the implementation

The timings in Table 4.22 were created using Magma 2.15 [BC08] on an Intel Core 2 Quad CPU running at 2.4 GHz with 8GB of memory available, although only one core and 2.7GB of memory were used. The values in the table denote the time (in seconds) it takes to compute a Chevalley basis for a Lie algebra L, given a maximal toral subalgebra H and the corresponding root datum R. The Lie algebra L and its subalgebra H are given as structure constant algebras, and a homomorphism from H into L is given as well. Although L is initially constructed as a Chevalley Lie algebra, a basis transformation τ has been applied, where τ keeps the eigenspaces of L with respect to H invariant but acts randomly within those eigenspaces.

In addition to the theoretical analysis leading to the $O^{\sim}(n^{10}(\log q)^4)$ bound on the runtime of the ChevalleyBasis algorithm, Figures 4.23 – 4.27 provide some insight in the performance of the implementation in practice. In Figure 4.23 we fix a particular root datum (one of the intermediate isogenies for type D_6), chosen because it is one of the more difficult cases in characteristic 2, and run the algorithm for varying sizes of the underlying field. In figures 4.24 – 4.27 we fix the field, but let the Lie algebra vary over each of the four classical series, for rank up to 9.

Figure 4.23 indicates that the size of the field has a much smaller influence than $O^{\sim}((\log q)^4)$. For smaller fields, this could be explained by the fact that many computer algebra systems, Magma among them, cache field operations when creating finite fields. Even for bigger fields, however, $O^{\sim}((\log q)^4)$ seems to be an overestimate.

On the other hand Figure 4.24 indicates that in characteristic 2 the $O^{\sim}(n^{10})$ estimate on the runtime is appropriate for root data of type B_n, C_n, and D_n, but for root data of type A_n the runtime seems closer to $O^{\sim}(n^6)$. Surprisingly, in the cases where the characteristic is not 2 (Figures 4.25, 4.26, and 4.27) a runtime estimate of $O^{\sim}(n^8)$ seems more appropriate.

R	$\mathbb{Q}$	GF(17)	GF(3^3)	GF(2^6)
A_1^{SC}	0.0	0.0	0.0	0.0
A_1^{Ad}	0.0	0.0	0.0	0.0
A_2^{SC}	0.0	0.0	0.0	0.0
A_2^{Ad}	0.0	0.0	0.0	0.0
A_3^{SC}	0.0	0.0	0.0	0.1
$A_3^{(2)}$	0.0	0.0	0.0	0.7
A_3^{Ad}	0.0	0.0	0.0	0.0
A_4^{SC}	0.1	0.0	0.1	0.1
A_4^{Ad}	0.1	0.0	0.1	0.1
A_5^{SC}	0.1	0.1	0.1	0.2
$A_5^{(3)}$	0.1	0.1	0.1	0.2
$A_5^{(2)}$	0.1	0.1	0.1	0.2
A_5^{Ad}	0.1	0.1	0.1	0.2
A_6^{SC}	0.3	0.2	0.3	0.6
A_6^{Ad}	0.3	0.2	0.4	0.6
A_7^{SC}	0.6	0.5	0.9	1.2
$A_7^{(4)}$	0.6	0.5	0.9	1.3
$A_7^{(2)}$	0.6	0.5	0.9	1.3
A_7^{Ad}	0.6	0.5	0.9	1.5
A_8^{SC}	1.4	1.0	1.4	3.5
$A_8^{(3)}$	1.4	1.0	1.4	3.5
A_8^{Ad}	1.4	1.0	2.0	3.6
B_2^{SC}	0.0	0.0	0.0	0.0
B_2^{Ad}	0.0	0.0	0.0	0.0
B_3^{SC}	0.0	0.0	0.1	0.4
B_3^{Ad}	0.0	0.0	0.0	0.1
B_4^{SC}	0.1	0.1	0.2	1.8
B_4^{Ad}	0.1	0.1	0.2	0.8
B_5^{SC}	0.3	0.2	0.9	4.8
B_5^{Ad}	0.3	0.2	0.9	4.5
B_6^{SC}	0.9	0.6	3.2	20
B_6^{Ad}	0.9	0.6	3.2	12
B_7^{SC}	2.2	1.6	10	50
B_7^{Ad}	2.2	1.6	10	54
B_8^{SC}	5.1	3.9	27	144
B_8^{Ad}	5.2	3.9	27	142
C_3^{SC}	0.0	0.0	0.0	0.1
C_3^{Ad}	0.0	0.0	0.0	0.1
C_4^{SC}	0.1	0.1	0.2	0.9
C_4^{Ad}	0.1	0.1	0.2	1.0
C_5^{SC}	0.3	0.2	0.9	5.8
C_5^{Ad}	0.3	0.2	0.9	10
C_6^{SC}	0.8	0.6	3.2	33
C_6^{Ad}	0.9	0.6	3.2	40
C_7^{SC}	2.2	1.6	10	111
C_7^{Ad}	2.2	1.6	10	148
C_8^{SC}	5.2	3.9	27	423
C_8^{Ad}	5.2	3.9	27	646
D_4^{SC}	0.1	0.0	0.1	1.0
$D_4^{(2a)}$	0.1	0.1	0.1	3.2
$D_4^{(2b)}$	0.1	0.1	0.1	2.8
$D_4^{(2c)}$	0.1	0.0	0.1	2.9
D_4^{Ad}	0.1	0.1	0.1	0.1
D_5^{SC}	0.2	0.1	0.3	1.9
$D_5^{(2)}$	0.2	0.1	0.3	22
D_5^{Ad}	0.2	0.1	0.3	0.5
D_6^{SC}	0.6	0.4	0.9	6.8
$D_6^{(2a)}$	0.6	0.4	0.9	121
$D_6^{(2b)}$	0.6	0.4	0.9	1.7
$D_6^{(2c)}$	0.6	0.4	0.9	1.8
D_6^{Ad}	0.6	0.4	0.9	1.7
D_7^{SC}	1.5	1.1	2.8	21
$D_7^{(2)}$	1.5	1.1	2.8	545
D_7^{Ad}	1.5	1.1	2.8	5.7
D_8^{SC}	3.7	2.8	7.7	57
$D_8^{(2a)}$	3.7	2.8	7.7	1994
$D_8^{(2b)}$	3.8	2.8	7.7	16
$D_8^{(2c)}$	3.8	2.8	7.7	16
D_8^{Ad}	3.8	2.8	7.7	17
E_6^{SC}	0.9	0.6	1.3	3.2
E_6^{Ad}	0.9	0.6	1.6	3.3
E_7^{SC}	4.1	3.0	11	25
E_7^{Ad}	4.1	3.0	11	27
E_8	28	21	112	397
F_4	0.2	0.2	0.7	2.8
G_2	0.0	0.0	0.0	0.3

Table 4.22: Runtimes of ChevalleyBasis

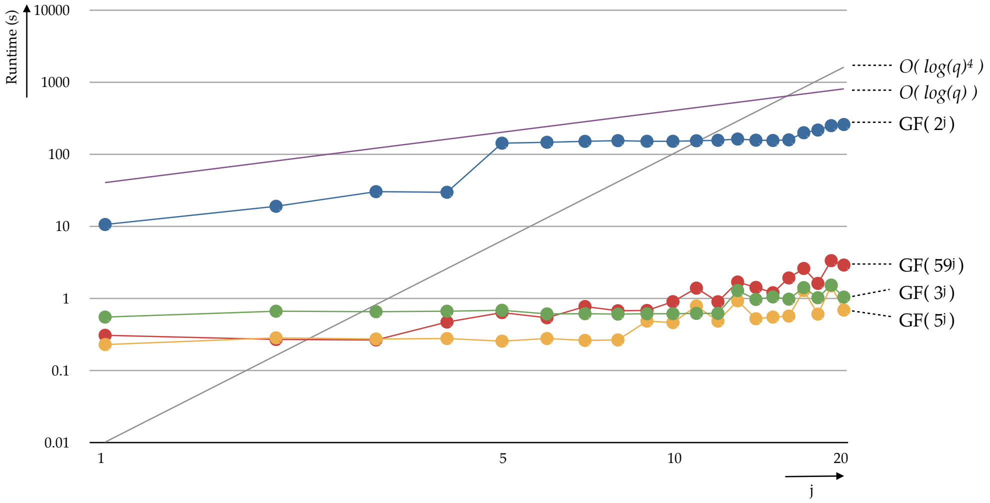


Figure 4.23: Runtimes of ChevalleyBasis for $L = D_6^{(2a)}$

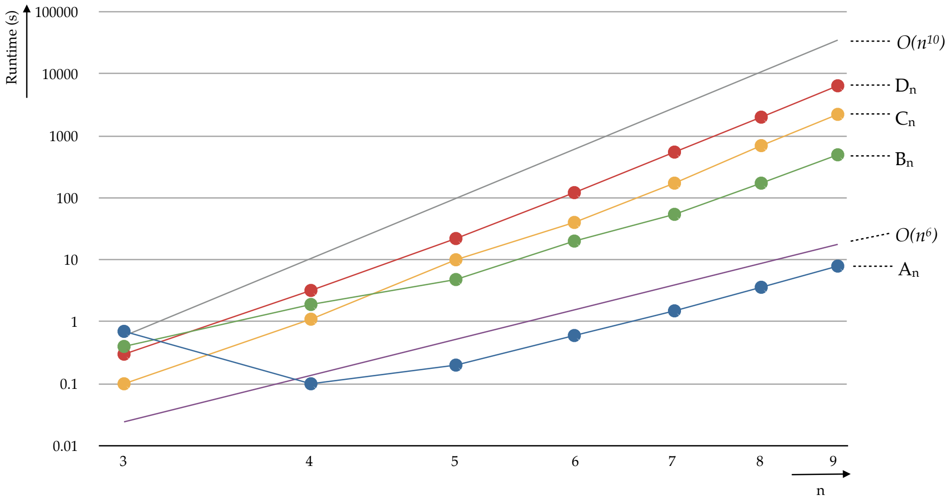


Figure 4.24: Runtimes of ChevalleyBasis for $\mathbb{F} = \mathrm{GF}(2^6)$

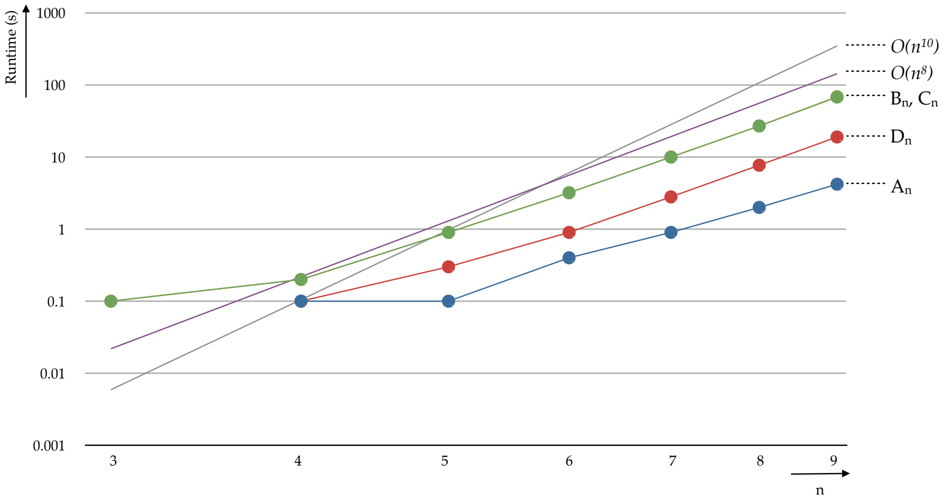


Figure 4.25: Runtimes of ChevalleyBasis for $\mathbb{F} = \mathrm{GF}(3^3)$

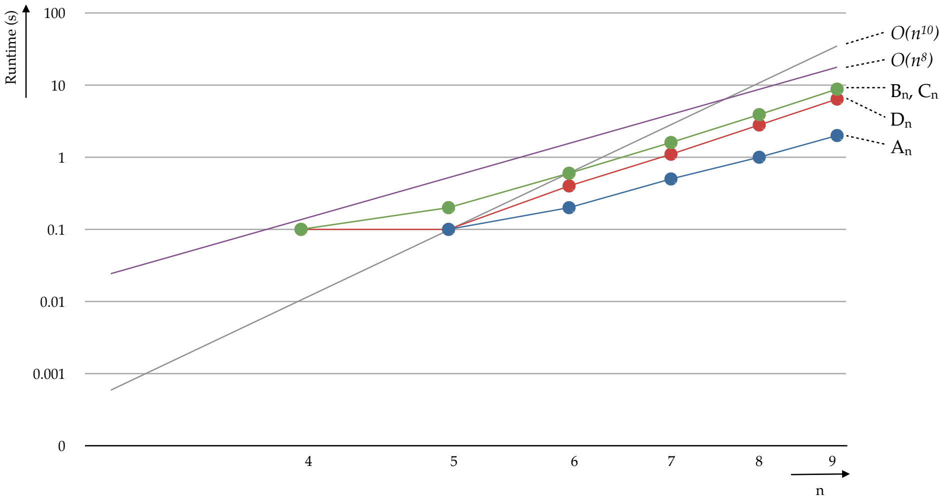


Figure 4.26: Runtimes of ChevalleyBasis for $\mathbb{F} = \mathrm{GF}(17)$

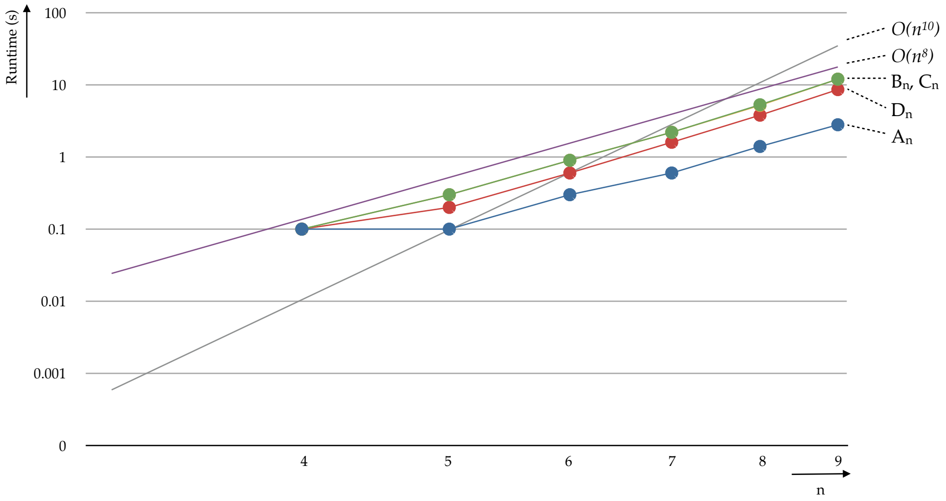
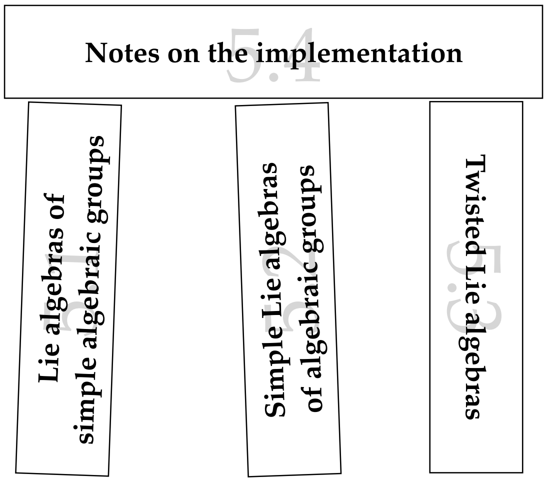


Figure 4.27: Runtimes of ChevalleyBasis for $\mathbb{F} = \mathbb{Q}$


5.4
Notes on the implementation
5.1
Lie algebras of simple algebraic groups
5.2
Simple Lie algebras of algebraic groups
5.3
Twisted Lie algebras

5 Recognition of Lie Algebras

In this chapter we apply the results of Chapters 3 and 4 to create an algorithm that recognizes certain Lie algebras. First, in Section 5.1 we show how to recognize Lie algebras of split simple algebraic groups. Second, in Section 5.2 we show how to recognize certain simple Lie algebras that occur inside Lie algebras of split simple algebraic groups. Third, in Section 5.3 we investigate the problem of recognizing twisted Lie algebras, as defined in Section 2.1. Finally, in Section 5.4 we briefly comment on the implementation of the algorithms presented in this chapter.

5.1 Lie algebras of simple algebraic groups

In this section we consider the problem of recognizing the Lie algebra of a simple algebraic group. These Lie algebras are precisely the ones we dealt with in Chapter 4. We assume we are given a Lie algebra L as a structure constant algebra.

If the characteristic is distinct from 2, we may use the algorithm described by Cohen and Murray in [CM09, Section 5] to produce a split maximal toral subalgebra H; if the characteristic is equal to 2 we use the procedure described in Chapter 3. This means that in order to be able to run the ChevalleyBasis algorithm we only need to find a suitable root datum R.

We claim such a root datum can easily be found. Note first that, because we have found H, and the underlying algebraic group is assumed to be simple, we may use $\dim(H) = \mathrm{rk}(R)$, the dimension of L, and the classification of simple Lie algebras to narrow down the root system to one or two possibilities (or three, but only if $\dim(L) = 78$ and $\dim(H) = 6$).

Second, given a root system, the number of possible root data is small as well. If the root system is not of type A_n or D_n, the number of possible isogeny types is at most 2. If the root system is of type D_n the number of possible isogeny types is at most 5, as explained in Section 1.3. So suppose Φ is of type A_n, and fix $p = \mathrm{char}(\mathbb{F})$. Note that the fundamental group is $\mathbb{Z}/(n+1)\mathbb{Z}$. Since two root data for A_n lead to isomorphic Lie algebras if both have the same exponent p in $X/\mathbb{Z}\Phi$, we need consider at most $\log_p(n+1) + 1 = O(\log n)$ different isogeny types. Thus, in order to recognize the correct root datum, we run Algorithm 4.3 a sufficient but small number of times for the bound given in Theorem 4.1 to remain intact.

We formalize this algorithm as Algorithm 5.1 and provide timings in Section 5.4. An important observation is that once the algorithm completes successfully we

```
RecognizeLieAlgebraOfSimpleAlgebraicGroup
in:   A structure constant Lie algebra $L$ over an effective field $\mathbb{F}$,
      and a split maximal toral subalgebra $H$ of $L$.
out:  A root datum $R$ and a Chevalley basis $B$ for $L$ with respect to $H$ and $R$
      if $L$ is the Lie algebra of a split reductive algebraic group,
      fail otherwise.
begin
  /* Find candidate root data */
  let $n = \dim(H)$,
  let $\mathcal{R}^0 = \{\}$,
  if $\dim(L) = (n+1)^2 - 1$ then let $\mathcal{R}^0 = \mathcal{R}^0 \cup \{\mathrm{A}_n\}$,
  if $\dim(L) = 2n^2 + n$ then let $\mathcal{R}^0 = \mathcal{R}^0 \cup \{\mathrm{B}_n, \mathrm{C}_n\}$,
  if $\dim(L) = 2n^2 - n$ then let $\mathcal{R}^0 = \mathcal{R}^0 \cup \{\mathrm{D}_n\}$,
  if $n = 6$ and $\dim(L) = 78$ then let $\mathcal{R}^0 = \mathcal{R}^0 \cup \{\mathrm{E}_6\}$,
  if $n = 7$ and $\dim(L) = 133$ then let $\mathcal{R}^0 = \mathcal{R}^0 \cup \{\mathrm{E}_7\}$,
  if $n = 8$ and $\dim(L) = 248$ then let $\mathcal{R}^0 = \mathcal{R}^0 \cup \{\mathrm{E}_8\}$,
  if $n = 4$ and $\dim(L) = 52$ then let $\mathcal{R}^0 = \mathcal{R}^0 \cup \{\mathrm{F}_4\}$,
  if $n = 2$ and $\dim(L) = 14$ then let $\mathcal{R}^0 = \mathcal{R}^0 \cup \{\mathrm{G}_2\}$,
  let $\mathcal{R} = \bigcup_{\Phi \in \mathcal{R}^0} \{\Phi^\iota \mid \iota$ is a possible isogeny type for $\Phi\}$,
  /* Compute Chevalley bases */
  for $R \in \mathcal{R}$ do
    try
      let $B = $ ChevalleyBasis$(L, H, R)$,
      return $R, B$.
    end try.
  end for,
  return fail.
end
```

Algorithm 5.1: Recognizing the Lie algebra of a simple algebraic group

$\Phi(p)$	$\dim(L)$	$\dim(H)$
$\mathrm{A}_n(p)$ $(n \geq 3, p \mid n+1)$	$(n+1)^2 - 2$	$n-1$
$\mathrm{D}_n(2)$ $(n \geq 4, n$ even$)$	$2n^2 - n - 2$	$n-2$
$\mathrm{D}_n(2)$ $(n \geq 4, n$ odd$)$	$2n^2 - n - 1$	$n-1$
$\mathrm{E}_6(3)$	77	5
$\mathrm{E}_7(2)$	132	6

Table 5.2: Some simple Lie algebras

have a certificate for a Lie algebra to be of type R: when presented with a candidate Chevalley basis X^0, H^0, we only need to carry out the straightforward and quick task of verifying that X^0, H^0 is indeed a Chevalley basis for L with respect to H and R.

5.2 Simple Lie algebras of algebraic groups

The class of Lie algebras considered in the previous section is to some extent artificial since, if the characteristic of the field is not 0, the Lie algebra of a simple algebraic group is not necessarily simple. In particular, simple algebraic groups and their Lie algebras over fields of characteristic 2 provide a large number of examples where the Lie algebra is non-simple.

Prime examples for this are the 80-dimensional Lie algebras of type A_8 over a field $\mathbb{F}$ of characteristic 3. Namely, for ${\mathrm{A}_8}^{\mathrm{ad}}$, there is a unique 79-dimensional ideal I such that I contains X_α for all $\alpha \in \Phi$, and $\dim(H \cap I) = 7$; for ${\mathrm{A}_8}^{\mathrm{sc}}$, the Lie algebra has a 1-dimensional center; and for $L = L_{\mathbb{F}}(\mathrm{A}_8^{(3)})$ we have $L \cong L' \oplus K$, where L' is 79-dimensional and K is the one-dimensional trivial Lie algebra. One could therefore argue that in characteristic 3 the 80-dimensional Lie algebra occurring in all three situations is "the" simple Lie algebra of type A_8 over fields of characteristic 3.

We investigate for which root data phenomena of this type occur. These observations are well known, and for example described by Hogeweij in [Hog82, Theorem 2.1], and in more detail in [Hog78].

- For root data R of type A_n, where $n \geq 3$, the Lie algebra $L = L_{\mathbb{F}}(R)$ is non-simple whenever $\mathrm{char}(\mathbb{F})$ divides $n+1$. If that is the case, we see behaviour similar to the A_8 example described above: For the adjoint isogeny type there exists a unique ideal of codimension 1, and for the simply connected isogeny type there is a 1-dimensional center. Moreover, if $p^2 | (n+1)$, for the intermediate isogeny type, we have $L = L' \oplus K$, where K is the one-dimensional trivial Lie algebra and L' has dimension $\dim(L) - 1$.

- For root data R of type B_n and fields $\mathbb{F}$ of characteristic 2, the Lie algebra $L = L_{\mathbb{F}}(R)$ has an ideal I generated by the short root elements. If R is ${\mathrm{B}_n}^{\mathrm{ad}}$, we have $\dim(I) = 2n$ and I is abelian; if R is ${\mathrm{B}_n}^{\mathrm{sc}}$, the dimension of I is $2n+1$, it has a 1-dimensional center $\langle h \rangle_{\mathbb{F}}$, and $I/\langle h \rangle_{\mathbb{F}}$ is abelian. Consequently, the quotient L/I is of dimension $2n^2 - n$, $2n^2 - n - 1$, respectively, and is equal to or is contained in a Lie algebra of type D_n.

- For root data R of type C_n and fields $\mathbb{F}$ of characteristic 2, the situation is dual to that of B_n. The Lie algebra $L = L_{\mathbb{F}}(R)$ contains an ideal I of type D_n generated by the short roots, and L/I (whose dimension is $2n+1$) either has a 1-dimensional center $\langle h \rangle_{\mathbb{F}}$ (and $(L/I)/\langle h \rangle_{\mathbb{F}}$ is abelian) or a $2n$-dimensional abelian ideal.

- For root data R of type D_4 over a field of characteristic 2 there are three distinct cases for $L = L_{\mathbb{F}}(R)$. Either there is a 26-dimensional ideal (for $\mathrm{D_4}^{\mathrm{ad}}$), there is a 2-dimensional center Z, yielding a 26-dimensional component as L/Z (for $\mathrm{D_4}^{\mathrm{sc}}$), or there is a 1-dimensional center Z and a codimension 1 ideal I, yielding a 26-dimensional Lie algebra I/Z (for the three intermediate isogeny types). We will call this 26-dimensional component "the" simple Lie algebra of type D_4 for fields of characteristic 2.

  For root data R of type D_n ($n \geq 5$) over a field $\mathbb{F}$ of characteristic 2 there are three distinct cases, but the details depend on whether n is odd or even. If n is odd, $L = L_{\mathbb{F}}(R)$ has a 1-dimensional center (for $\mathrm{D}_n{}^{\mathrm{sc}}$), a codimension 1 ideal (for $\mathrm{D}_n{}^{\mathrm{ad}}$), or $L = L' \oplus \langle h \rangle_{\mathbb{F}}$ (for $\mathrm{D}_n^{(1)}$). If n is even, $L = L_{\mathbb{F}}(R)$ has a 2-dimensional center (for $\mathrm{D}_n{}^{\mathrm{sc}}$), a codimension 1 ideal (for $\mathrm{D}_n{}^{\mathrm{ad}}$), or a 1-dimensional center Z and a codimension 1 ideal I. In conclusion, there always is a $2n^2 - n - 1$-dimensional (if n is odd) or $2n^2 - n - 2$-dimensional (if n is even) simple Lie algebra inside L. We will call this component "the" simple Lie algebra of type D_n for fields of characteristic 2.

- For root data R of type E_6 over fields $\mathbb{F}$ of characteristic 3, we find that $L = L_{\mathbb{F}}(R)$ either has a 1-dimensional center $\langle h \rangle_{\mathbb{F}}$ (for $\mathrm{E_6}^{\mathrm{sc}}$) or a codimension 1 ideal I (for $\mathrm{E_6}^{\mathrm{ad}}$). The simple Lie algebra, $L/\langle h \rangle_{\mathbb{F}}$ or I, is 77-dimensional. Similarly, for root data R of type E_7 over fields $\mathbb{F}$ of characteristic 2, we find that $L = L_{\mathbb{F}}(R)$ either has a 1-dimensional center $\langle h \rangle_{\mathbb{F}}$ (for $\mathrm{E_7}^{\mathrm{sc}}$) or a codimension 1 ideal I (for $\mathrm{E_7}^{\mathrm{ad}}$). The simple Lie algebra, $L/\langle h \rangle_{\mathbb{F}}$ or I, is 132-dimensional.

- For the root datum R of type F_4 and a field $\mathbb{F}$ of characteristic 2, $L = L_{\mathbb{F}}(R)$ has a 26-dimensional ideal I generated by the short root elements; it is the same 26-dimensional Lie algebra as "the" simple Lie algebra of type D_4. Moreover, $I \cong L/I$ (see Section 2.5).

- For the root datum R of type G_2 and a field $\mathbb{F}$ of characteristic 3, $L = L_{\mathbb{F}}(R)$ has a 7-dimensional ideal I generated by the short root elements; it is the same 7-dimensional Lie algebra as "the" simple Lie algebra of type A_2. Moreover, $I \cong L/I$ (see Section 2.5).

In this manner, we have found several simple Lie algebras that are not the Lie algebra of a simple algebraic group. They are shown in Table 5.2. Here the Dynkin type Φ of the Lie algebra L and the characteristic p of $\mathbb{F}$ are indicated by $\Phi(p)$ in the first column. The second column indicates the dimension of L and the third

```
RecognizeSimpleLieAlgebraOfAlgebraicGroup
in:     A structure constant Lie algebra $L$ over an effective field $\mathbb{F}$,
        and a split maximal toral subalgebra $H$ of $L$.
out:    A root datum $R$, a Lie algebra $L' \subseteq \mathrm{Der}(L)$
        and a split maximal toral subalgebra $H'$ of $L'$ such that $H \subseteq H'$,
        and a Chevalley basis $B$ for $L'$ with respect to $H'$ and $R$
        if $L$ is one of the Lie algebras occurring in Table 5.2,
        fail otherwise.
begin
    /* Find candidate root data */
    let $m = \dim(H)$,
    let $\mathcal{P} = \{\}$,
    if $m \geq 1$, $p \mid m+2$, and $\dim(L) = (m+2)^2 - 2$ then
        let $\mathcal{P} = \mathcal{P} \cup \{(\mathrm{A}_{m+1}, 1)\}$.
    end if,
    if $m \geq 2$, $m$ is even, $p = 2$, and $\dim(L) = 2(m+2)^2 - m - 4$ then
        let $\mathcal{P} = \mathcal{P} \cup \{(\mathrm{D}_{m+2}, 2)\}$.
    end if,
    if $m \geq 3$, $m$ is even, $p = 2$, and $\dim(L) = 2(m+1)^2 - m - 2$ then
        let $\mathcal{P} = \mathcal{P} \cup \{(\mathrm{D}_{m+1}, 1)\}$.
    end if,
    if $m = 5$, $p = 3$, and $\dim(L) = 77$ then let $\mathcal{P} = \mathcal{P} \cup \{(\mathrm{E}_6, 1)\}$.
    if $m = 6$, $p = 2$, and $\dim(L) = 132$ then let $\mathcal{P} = \mathcal{P} \cup \{(\mathrm{E}_7, 1)\}$.
    /* Compute Chevalley bases */
    compute the composition series of $\mathrm{Der}(L)$ using the Meat-Axe,
    for $(\Phi, d) \in \mathcal{P}$ do
        try
            let $L'$ be a $(\dim(L) + d)$-dimensional ideal of $\mathrm{Der}(L)$,
            let $H' \subseteq C_{L'}(H)$ be a split maximal toral subalgebra of $L'$,
            let $B = $ ChevalleyBasis$(L', H', \Phi^{\mathrm{ad}})$,
            return $\Phi^{\mathrm{ad}}, H, L', H', B$.
        end try.
    end for,
    return fail.
end
```

Algorithm 5.3: Recognizing the simple Lie algebra of an algebraic group

column contains the dimension of a maximal toral subalgebra H of L. These last two columns will be useful for identification purposes.

We may recognize the Lie algebras shown in Table 5.2 in the following manner, formalized in Algorithm 5.3. Suppose we encounter a Lie algebra L over a field of characteristic p, and we have computed a split maximal toral subalgebra H. Suppose Φ is a root system for which a suitable relation holds, e.g.,

$$\dim(L) = (\dim(H) + 2)^2 - 2 \text{ and } \; p \mid \dim(H) + 2$$

for $\Phi(p) = \mathrm{A}_n(p)$. We then compute the Lie algebra of derivations $\mathrm{Der}(L)$ and use the Meat-axe in an attempt to obtain a $(\dim(L) + d)$-dimensional ideal L' of $\mathrm{Der}(L)$, where $d = 2$ if $\Phi(p) = \mathrm{D}_n(2)$ and n is even, and $d = 1$ otherwise. We let $H' = \mathrm{C}_{L'}(H)$, which should yield a split maximal toral subalgebra of L', such that $\dim(H') = \mathrm{rk}(\Phi)$.

If this procedure succeeds and gives a Lie algebra L' and a split maximal toral subalgebra $H' \subseteq L'$ of the required dimensions, these may serve (with a root datum $R = \Phi^{\mathrm{ad}}$) as input for the ChevalleyBasis algorithm, and thus recognize L. If on the other hand something fails (e.g., L' cannot be extended as required), L was apparently not the simple Lie algebra of an algebraic group.

5.3 Twisted Lie algebras

In order to recognize twisted Lie algebras we introduce the notion of *twisted bases*. Suppose we are given a twisted Lie algebra L over the field $\mathbb{F}$ of type ${}^nR$, where $R = (X, \Phi, Y, \Phi^\vee)$, and δ is a degree n diagram automorphism of Φ. Fix an arbitrary basis $b_1, \ldots, b_k$ of L.

Let $\mathbb{F}'$ be a degree n field extension of $\mathbb{F}$, and F a degree n Frobenius automorphism of $\mathbb{F}$ such that $t^F = t$ for all $t \in \mathbb{F}$. Furthermore, let $L' = L \otimes \mathbb{F}'$ be the Lie algebra L with base field $\mathbb{F}'$ instead of $\mathbb{F}$ (this is well-defined since $\mathbb{F}' \supseteq \mathbb{F}$ and Lie multiplication is linear). The basis $b_1, \ldots, b_k$ of L is clearly also a basis of L'.

Since L' is defined over a suitable extension field of $\mathbb{F}$, it is a split Lie algebra, and therefore has a Chevalley basis. Suppose $\mathcal{B} = \{X_\alpha, h_i \mid \alpha \in \Phi, i = 1, \ldots, \mathrm{rk}(R)\}$ is such a basis. We may now write elements of L' (and thus also elements of L) as $\mathbb{F}'$ linear combinations of these basis elements: for all $x \in L'$ there exist $t_\alpha \in \mathbb{F}'$ ($\alpha \in \Phi$) and $t_i \in \mathbb{F}'$ ($i = 1, \ldots, \mathrm{rk}(R)$) such that

$$x = \sum_{\alpha \in \Phi} t_\alpha X_\alpha + \sum_{i=1}^{\mathrm{rk}(R)} t_i h_i.$$

We let the diagram automorphism δ act on L' in the usual manner, i.e., $X_\alpha^\delta = X_{\delta\alpha}$ for all $\alpha \in \Phi$ and $h_i^\delta = X_{\delta i}$ (where $\delta i = j$ precisely if $\delta(\alpha_i) = \alpha_j$; here α_k denotes the k-th fundamental root of Φ).

The field automorphism F now acts on L' in two distinct ways, corresponding to two canonical ways the elements of L' can be written in. First, with respect to the basis of L:

$$F_L : L' \to L', \qquad x = t_1 b_1 + \cdots + t_k b_k \mapsto t_1^F b_1 + \cdots + t_k^F b_k =: x^{F_L},$$

so that $x^{F_L} = x$ for all $x \in L$. Second, with respect to the Chevalley basis of L':

$$F_{\mathcal{B}} : L' \to L', \qquad x = \sum_{\alpha\in\Phi} t_\alpha X_\alpha + \sum_{i=1}^{\mathrm{rk}(R)} t_i h_i \mapsto \sum_{\alpha\in\Phi} t_\alpha^F X_\alpha + \sum_{i=1}^{\mathrm{rk}(R)} t_i^F h_i =: x^{F_{\mathcal{B}}},$$

so that $X_\alpha^{F_{\mathcal{B}}} = X_\alpha$ for all $\alpha \in \Phi$. The two actions of the field automorphism on L' are related in the following sense.

Lemma 5.4. *$x^{\delta F_{\mathcal{B}}} = x$ for all $x \in L$ if and only if $(X_\alpha)^{F_L} = X_{\delta\alpha}$ for all $\alpha \in \Phi$ and $(h_i)^{F_L} = h_{\delta i}$ for $i = 1, \ldots, \mathrm{rk}(R)$.*

Proof First observe that it follows immediately from the definition of F_L and $F_{\mathcal{B}}$ that $(tx)^{F_L} = t^F x^{F_L}$ and $(tx)^{F_{\mathcal{B}}} = t^F x^{F_{\mathcal{B}}}$ for all $t \in \mathbb{F}'$ and all $x \in L'$. Now suppose that $(X_\alpha)^{F_L} = X_{\delta\alpha}$ for all $\alpha \in \Phi$ and $(h_i)^{F_L} = h_{\delta i}$ for $i = 1, \ldots, \mathrm{rk}(R)$. Let $x \in L$, and let $t_\alpha \in \mathbb{F}'$ (where $\alpha \in \Phi$) and $t_i \in \mathbb{F}'$ (where $i = 1, \ldots, \mathrm{rk}(R)$) be such that

$$x = \sum_{\alpha\in\Phi} t_\alpha X_\alpha + \sum_{i=1}^{\mathrm{rk}(R)} t_i h_i,$$

so that

$$x = x^{F_L} = \sum_{\alpha\in\Phi} t_\alpha^F (X_\alpha)^{F_L} + \sum_{i=1}^{\mathrm{rk}(R)} t_i^F (h_i)^{F_L} = \sum_{\alpha\in\Phi} t_\alpha^F X_{\delta\alpha} + \sum_{i=1}^{\mathrm{rk}(R)} t_i^F h_{\delta i} = x^{\delta F_{\mathcal{B}}}.$$

This proves the "if"-direction. Suppose on the other hand that $x^{\delta F_{\mathcal{B}}} = x$ for all $x \in L$. Let $\alpha \in \Phi$ and $t_1, \ldots, t_k \in \mathbb{F}'$ be such that

$$X_\alpha = t_1 b_1 + \ldots + t_k b_k.$$

We calculate, similarly to the above,

$$X_{\delta\alpha} = X_{\delta\alpha}^{F_{\mathcal{B}}} = X_\alpha^{\delta F_{\mathcal{B}}} = t_1^F (b_1)^{\delta F_{\mathcal{B}}} + \cdots + t_k^F (b_k)^{\delta F_{\mathcal{B}}} = t_1^F b_1 + \cdots + t_k^F b_k = X_\alpha^{F_L}.$$

The assertion that $(h_i)^{F_L} = h_{\delta i}$ follows in precisely the same manner, finishing the proof of the lemma. □

Note that both the action of the diagram automorphism δ and that of the field automorphism $F_{\mathcal{B}}$ depend on the choice of a Chevalley basis $\mathcal{B}$. We call a Chevalley basis $\mathcal{B}$ a *twisted basis for L* if $x^{\delta F_{\mathcal{B}}} = x$ for all $x \in L$. It follows from the definition of twisted Lie algebras that such a twisted basis exists. Moreover, for an arbitrary Lie algebra L over $\mathbb{F}$ the existence of a twisted basis with respect to a certain root datum R and diagram automorphism of degree n proves that it is isomorphic to the twisted Lie algebra of type ${}^nR$.

In Algorithm 5.5 we present an algorithm for computing twisted bases.

```
TwistedBasis
in:     A structure constant Lie algebra $L$ over an effective field $\mathbb{F}$,
        a suitable split toral subalgebra $H$ of $L$,
        an irreducible root datum $R = (X, \Phi, Y, \Phi^\vee)$, and $n \in \{2, 3\}$.
out:    A twisted basis for $L$ if $L$ is of type ${}^nR$; fail otherwise.
begin
 1  let $\delta$ be the order $n$ automorphism of $\Phi$, and $\Delta$ a set of fundamental roots of $\Phi$,
 2  let $\mathbb{F}'$ a degree $n$ extension of $\mathbb{F}$, $L' = L \otimes \mathbb{F}'$, and $H_0' = H \otimes \mathbb{F}'$,
 3  try
 4    let $H' \supseteq H_0'$ be a split maximal toral subalgebra of $L'$,
 5    let $B = \{X_\alpha, h_i \mid \alpha \in \Phi, i = 1, \ldots, \mathrm{rk}(R)\} = \textsc{ChevalleyBasis}(L', H', R)$,
 6    let $w \in W(\Phi)$ such that $\mathbb{F}'\left(X_{w(\alpha)}^{F_L}\right) = \mathbb{F}'\left(X_{\delta(w(\alpha))}\right)$ for all $\alpha \in \Phi$,
 7    let $t_{w(\alpha)} \in (\mathbb{F}')^*$ such that $\left(t_{w(\alpha)} X_{w(\alpha)}\right)^{F_L} = t_{\delta(w(\alpha))} X_{\delta(w(\alpha))}$ for all $\alpha \in \Phi$,
 8    find $h_i'$ such that $B' = \{t_{w(\alpha)} X_{w(\alpha)}, h_i' \mid \alpha \in \Phi, i = 1, \ldots, \mathrm{rk}(R)\}$ is
      a Chevalley basis for $L'$ with respect to $H'$ and $R$,
 9    return $B'$.
10  end try,
11  return fail.
end
```

Algorithm 5.5: Computing a twisted basis

Proposition 5.6. *Let L' be the Chevalley Lie algebra with irreducible root datum $R = (X, \Phi, Y, \Phi^\vee)$ over the field $\mathbb{F}$, where Φ admits a degree n automorphism δ and $\mathbb{F}$ admits a degree n automorphism F (where $n \in \{2, 3\}$). Let H' be a split maximal toral subalgebra of L'. Let L (resp. H) be the fixed points of L' (resp. H') under the composition δF (such an H we call* suitable*). Upon input of L, H, R, and n, the algorithm* TwistedBasis *returns a twisted basis for L.*

Proof It follows immediately from Lemma 5.4 that if Algorithm 5.5 completes successfully it indeeds returns the required twisted basis. Now let $\mathbb{F}'$ be a degree n extension of $\mathbb{F}$, let G be the group of Lie type R over $\mathbb{F}'$, let W be the Weyl group of G, and let T be its split torus. Since by construction $L \otimes \mathbb{F}'$ is isomorphic to the split Chevalley Lie algebra of type R and since $\mathrm{N}_G(H') \cong WT$, the Weyl group element w in line 6 and the scalars t_α in line 7 must exist. Finally, the existence of the required h_i' is immediate; they may for instance be found from the $t_{w(\alpha)} X_{w(\alpha)}$ by elementary linear algebra. □

Note that in Proposition 5.6 we require the split toral subalgebra H that is input to the TwistedBasis algorithm to be of a special form. The question now naturally arises whether we can find such split toral subalgebras. Unfortunately, the existing algorithms [CM09, Ryb07] as discussed in Chapter 3 consider split toral subalgebras of split Chevalley Lie algebras: a class that the twisted Lie algebras do not fall into. Experiments with Magma, however, show that these algorithms find appropriate split toral subalgebras in many cases. Moreover, the heuristic algorithm for finding split maximal toral subalgebras in characteristic 2, described in Section 3.3,

```
RecognizeTwistedLieAlgebra
in:    A structure constant Lie algebra $L$ over an effective field $\mathbb{F}$,
       and a suitable split toral subalgebra $H$.
out:   An irreducible root datum $R = (X, \Phi, Y, \Phi^\vee)$, an $n \in \mathbb{Z}$,
       and a twisted basis for $L$ if $L$ is of type ${}^nR$ for some irreducible
       root datum $R$ and some $n \in \{2, 3\}$; fail otherwise.
begin
    /* Find candidate root data */
    let $\mathcal{P}^0 = \{\}$,
    if $\dim(L) = (k+1)^2 - 1$ for some $k \in \mathbb{Z}$ then let $\mathcal{P}^0 = \mathcal{P}^0 \cup \{(\mathrm{A}_k, 2)\}$,
    if $\dim(L) = 2 * k^2 - k$ for some $k \in \mathbb{Z}$ then let $\mathcal{P}^0 = \mathcal{P}^0 \cup \{(\mathrm{D}_k, 2)\}$,
    if $\dim(L) = 28$ then let $\mathcal{P}^0 = \mathcal{P}^0 \cup \{(\mathrm{D}_4, 3)\}$,
    if $\dim(L) = 78$ then let $\mathcal{P}^0 = \mathcal{P}^0 \cup \{(\mathrm{E}_6, 2)\}$,
    let $\mathcal{P} = \bigcup_{(\Phi,n) \in \mathcal{P}^0} \{(\Phi^\iota, n) \mid \iota$ is a possible isogeny type for $\Phi\}$,
    /* Compute twisted bases */
    for $(R, n) \in \mathcal{P}$ do
        try
            let $B = $ TwistedBasis$(L, H, R, n)$,
            return $R, n, B$.
        end try.
    end for,
    return fail.
end
```

Algorithm 5.7: Recognizing a twisted Lie algebra

performs quite well. There is, however, one notable exception to the rule. Consider a twisted Lie algebra of type ${}^2\mathrm{A}_l$ over a field $\mathbb{F}$ of characteristic 2, and adopt the notation from Proposition 5.6. It follows from the analysis of the twisted groups (cf. [GLS98, Proposition 2.3.2(d), Theorem 2.4.7(a)]) that $\dim(H')$ is $\frac{1}{2}l$ (if l is even) or $\frac{1}{2}(l+1)$ (if l is odd). In this particular case, however, $-\delta$ is an element of the Weyl group W and the (in odd characteristic non-split) maximal toral subalgebra of L corresponding to $-\delta$, is $\mathbb{F}$-split. Experiments show that in these cases our heuristic algorithm always returns such an $\mathbb{F}$-split toral subalgebra of dimension l.

The algorithm TwistedBasis for computing a twisted basis and the select set of root systems with a non-trivial automorphism immediately suggest a recognition algorithm for twisted Lie algebras arising from irreducible root data. This algorithm functions in a manner similar to Algorithms 5.1 and 5.3, and is presented in Algorithm 5.7. Note that we require the split toral subalgebra that is given as input to this algorithm to be *suitable*, as defined in Proposition 5.6.

5.4 Notes on the implementation

We have implemented the algorithms 5.1, 5.3, 5.5, and 5.7 in Magma, with one significant modification: instead of stopping as soon as the given Lie algebra has been identified, the implemented algorithm tests all candidates and returns all possible matches. Moreover, the three algorithms are combined into one algorithm that recognizes all three types of Lie algebras (Lie algebras of simple algebraic groups, the simple Lie algebras presented in Table 5.2, and twisted Lie algebras of simple algebraic groups). In particular, this means that for a Lie algebra L over $\mathbb{Q}$, the algorithm returns at least as many possibilities as there are isogeny types of the root datum of L.

In Tables 5.8a and 5.8b we give three values for every irreducible root datum of rank at most 8, and for each of four fields $\mathbb{F}$ (namely $\mathbb{Q}$, GF(17), GF(3^3), and GF(2^6)). First, under "#" the number of matches, i.e., $k_1 + k_2 + k_3$, where k_1 is the number of root data R such that the Lie algebra under consideration is isomorphic to $L_{\mathbb{F}}(R)$, and k_2 is 1 if L is isomorphic to one of the Lie algebras shown in Table 5.2, and $k_2 = 0$ otherwise. Finally, k_3 is the number of pairs (R, n), for a root datum R and an integer n, such that L is isomorphic to ${}^{n}R(\mathbb{F})$. The second value is the time in seconds it takes to find the first match (labeled "t_0"), and third the time it takes to find all matches (labeled "t").

In Table 5.8c the same values are given for each of the simple Lie algebras presented in Table 5.2, for the same fields, and again up to rank 8. In Tables 5.8d and 5.8e the same values are given for twisted Lie algebras of rank up to 8. Since the construction of twisted Lie algebras requires a finite field and the GF(2)-case is somewhat harder than the general characteristic 2 case, we ran the tests over GF(59), GF(17), GF(3^3), and GF(2). Furthermore, in some cases "n/a" is displayed in the table, indicating that the twisted Lie algebra of that particular type does not exist over that particular field. All timings are in seconds and were created using Magma 2.15 [BC08] on a Quad-Core Intel Xeon running at 3 GHz with 16GB of memory available, although only one core and less than 2GB of memory were used.

As in the timings produced for the ChevalleyBasis algorithm, the Lie algebra L and its subalgebra H are given as structure constant algebras, and a homomorphism from H into L is given as well. For the cases where L is split (Tables 5.8a–5.8c) we constructed L and H as a Chevalley Lie algebra, and have subsequently applied a random basis transformation τ, where τ is such that it keeps the eigenspaces of L with respect to H invariant but acts randomly within those eigenspaces. For the cases where L is twisted (Tables 5.8d–5.8e) we constructed L and H from their split counterparts, and then apply a fully random basis transformation. This ensures, by construction, that H is a suitable split toral subalgebra of L.

As expected, the timings in Tables 5.8a and 5.8b are of the same order of magnitude as the timings for computing Chevalley bases given in Section 4.8. The same is true for those in Table 5.8c. For Tables 5.8d and 5.8e, on the other hand, the algorithm performs significantly worse than might be expected from the corresponding Chevalley basis timings. This may largely be attributed to the computation of an additional split maximal toral subalgebra. Moreover, in this case we applied a fully random basis transformation, which significantly slows down the Lie algebra arithmetic, and we have not yet optimized the implementation for the computation of twisted bases or of split maximal toral subalgebras, whereas we have invested significant time and effort in the optimization of the code for the computation of Chevalley bases.

	$\mathbb{Q}$			GF(17)			GF(3^3)			GF(2^6)		
R	#	t_0	t	#	t_0	t	#	t_0	t	#	t_0	t
$\mathrm{A}_1^{\mathrm{SC}}$	2	0.0	0.0	2	0.0	0.0	2	0.0	0.0	1	0.0	0.0
$\mathrm{A}_1^{\mathrm{Ad}}$	2	0.0	0.0	2	0.0	0.0	2	0.0	0.0	1	0.0	0.0
$\mathrm{A}_2^{\mathrm{SC}}$	2	0.0	0.0	2	0.0	0.0	1	0.0	0.0	2	0.0	0.0
$\mathrm{A}_2^{\mathrm{Ad}}$	2	0.0	0.0	2	0.0	0.0	1	0.0	0.0	2	0.0	0.0
$\mathrm{A}_3^{\mathrm{SC}}$	3	0.0	0.1	3	0.0	0.0	3	0.0	0.1	1	0.1	0.2
$\mathrm{A}_3^{(2)}$	3	0.0	0.0	3	0.0	0.0	3	0.0	0.1	1	0.3	0.3
$\mathrm{A}_3^{\mathrm{Ad}}$	3	0.0	0.1	3	0.0	0.0	3	0.0	0.1	1	0.0	0.1
$\mathrm{A}_4^{\mathrm{SC}}$	2	0.0	0.1	2	0.0	0.1	2	0.1	0.2	2	0.1	0.2
$\mathrm{A}_4^{\mathrm{Ad}}$	2	0.1	0.1	2	0.0	0.1	2	0.1	0.1	2	0.1	0.2
$\mathrm{A}_5^{\mathrm{SC}}$	4	0.1	0.4	4	0.1	0.4	2	0.2	0.5	2	0.3	0.6
$\mathrm{A}_5^{(3)}$	4	0.1	0.5	4	0.1	0.4	2	0.2	0.5	2	0.2	0.7
$\mathrm{A}_5^{(2)}$	4	0.1	0.4	4	0.1	0.4	2	0.2	0.6	2	0.3	0.6
$\mathrm{A}_5^{\mathrm{Ad}}$	4	0.1	0.4	4	0.1	0.4	2	0.2	0.6	2	0.2	0.7
$\mathrm{A}_6^{\mathrm{SC}}$	2	0.2	0.4	2	0.2	0.4	2	0.3	0.6	2	0.3	0.7
$\mathrm{A}_6^{\mathrm{Ad}}$	2	0.2	0.4	2	0.2	0.3	2	0.3	0.6	2	0.4	0.7
$\mathrm{A}_7^{\mathrm{SC}}$	4	0.4	1.6	4	0.3	1.3	4	0.5	2.2	1	1.0	1.8
$\mathrm{A}_7^{(4)}$	4	0.4	1.6	4	0.3	1.3	4	0.6	2.2	2	1.4	2.0
$\mathrm{A}_7^{(2)}$	4	0.4	1.6	4	0.3	1.3	4	0.6	2.2	2	1.4	2.0
$\mathrm{A}_7^{\mathrm{Ad}}$	4	0.4	1.6	4	0.3	1.3	4	0.6	2.2	1	0.6	2.2
$\mathrm{A}_8^{\mathrm{SC}}$	3	0.7	2.1	3	0.5	1.4	1	1.3	1.9	3	1.0	3.2
$\mathrm{A}_8^{(3)}$	3	0.7	2.2	3	0.5	1.4	1	1.9	2.0	3	1.0	3.1
$\mathrm{A}_8^{\mathrm{Ad}}$	3	0.8	2.2	3	0.5	1.6	1	0.9	2.5	3	1.0	3.1
$\mathrm{B}_2^{\mathrm{SC}}$	2	0.0	0.0	2	0.0	0.0	2	0.0	0.0	1	0.0	0.0
$\mathrm{B}_2^{\mathrm{Ad}}$	2	0.0	0.0	2	0.0	0.0	2	0.0	0.0	1	0.0	0.1
$\mathrm{B}_3^{\mathrm{SC}}$	2	0.0	0.1	2	0.0	0.1	2	0.1	0.2	1	0.3	0.4
$\mathrm{B}_3^{\mathrm{Ad}}$	2	0.0	0.1	2	0.0	0.1	2	0.1	0.2	1	0.1	0.2
$\mathrm{B}_4^{\mathrm{SC}}$	2	0.1	0.3	2	0.1	0.3	2	0.2	0.5	1	1.1	1.2
$\mathrm{B}_4^{\mathrm{Ad}}$	2	0.1	0.3	2	0.1	0.3	2	0.2	0.5	1	0.3	0.8
$\mathrm{B}_5^{\mathrm{SC}}$	2	0.3	0.7	2	0.2	0.6	2	0.4	1.3	1	2.2	2.5
$\mathrm{B}_5^{\mathrm{Ad}}$	2	0.3	0.7	2	0.2	0.6	2	0.4	1.3	1	0.6	2.5
$\mathrm{B}_6^{\mathrm{SC}}$	2	0.5	2.1	2	0.5	1.9	2	0.9	3.3	1	6.1	7.1
$\mathrm{B}_6^{\mathrm{Ad}}$	2	0.6	2.5	2	0.4	1.6	2	0.9	3.3	1	1.5	7.2
$\mathrm{B}_7^{\mathrm{SC}}$	2	1.1	3.6	2	0.8	2.3	2	1.6	4.8	1	15	16
$\mathrm{B}_7^{\mathrm{Ad}}$	2	1.2	3.7	2	0.8	2.3	2	1.6	4.9	1	2.6	17
$\mathrm{B}_8^{\mathrm{SC}}$	2	2.2	7.3	2	1.4	4.1	2	2.8	8.6	1	36	38
$\mathrm{B}_8^{\mathrm{Ad}}$	2	2.1	6.6	2	1.3	4.0	2	2.8	8.6	1	4.5	39
$\mathrm{C}_3^{\mathrm{SC}}$	2	0.1	0.1	2	0.1	0.1	2	0.1	0.2	1	0.2	0.2
$\mathrm{C}_3^{\mathrm{Ad}}$	2	0.1	0.1	2	0.1	0.1	2	0.1	0.2	1	0.2	0.2

Table 5.8a: Recognition Timings (1/5)

	$\mathbb{Q}$			GF(17)			GF(3^3)			GF(2^6)		
R	#	t_0	t	#	t_0	t	#	t_0	t	#	t_0	t
C_4^{SC}	2	0.2	0.3	2	0.2	0.3	2	0.3	0.5	1	0.6	0.6
C_4^{Ad}	2	0.2	0.3	2	0.2	0.3	2	0.3	0.5	1	0.8	0.8
C_5^{SC}	2	0.5	0.8	2	0.4	0.6	2	0.8	1.3	1	1.2	1.2
C_5^{Ad}	2	0.5	0.8	2	0.4	0.6	2	0.8	1.3	1	2.5	2.6
C_6^{SC}	2	1.3	2.5	2	0.9	1.8	2	1.9	3.3	1	2.8	3.3
C_6^{Ad}	2	1.3	2.5	2	0.9	1.9	2	1.9	3.2	1	6.7	7.4
C_7^{SC}	2	2.5	3.6	2	1.4	2.3	2	3.2	4.8	1	6.3	6.4
C_7^{Ad}	2	2.5	3.7	2	1.5	2.3	2	3.2	4.9	1	17	18
C_8^{SC}	2	5.0	7.2	2	2.6	4.0	2	5.8	8.6	1	14	14
C_8^{Ad}	2	4.8	6.9	2	2.5	3.9	2	5.7	8.5	1	41	42
D_4^{SC}	5	0.1	0.4	5	0.1	0.3	5	0.1	0.5	1	0.7	0.8
$D_4^{(2a)}$	5	0.1	0.3	5	0.1	0.3	5	0.1	0.5	3	2.7	7.5
$D_4^{(2b)}$	5	0.1	0.3	5	0.1	0.3	5	0.1	0.5	3	2.6	7.6
$D_4^{(2c)}$	5	0.1	0.3	5	0.1	0.3	5	0.1	0.5	3	2.6	7.2
D_4^{Ad}	5	0.1	0.3	5	0.1	0.3	5	0.1	0.5	1	0.1	0.6
D_5^{SC}	3	0.2	0.5	3	0.1	0.4	3	0.3	0.8	1	1.3	7.4
$D_5^{(2)}$	3	0.2	0.5	3	0.1	0.4	3	0.3	0.8	1	21	21
D_5^{Ad}	3	0.2	0.5	3	0.1	0.4	3	0.3	0.8	1	0.3	0.8
D_6^{SC}	5	0.4	2.0	5	0.3	1.7	5	0.6	2.9	1	3.5	116
$D_6^{(2a)}$	5	0.4	2.2	5	0.3	1.7	5	0.6	2.9	1	106	310
$D_6^{(2b)}$	5	0.5	2.3	5	0.4	1.9	5	0.6	3.2	2	2.3	3.2
$D_6^{(2c)}$	5	0.5	2.2	5	0.4	1.8	5	0.7	3.3	2	2.3	3.2
D_6^{Ad}	5	0.4	2.2	5	0.4	1.9	5	0.7	3.3	1	0.8	3.5
D_7^{SC}	3	0.9	2.6	3	0.6	1.8	3	1.1	3.3	1	9.6	209
$D_7^{(2)}$	3	0.9	2.6	3	0.6	1.8	3	1.1	3.3	1	488	488
D_7^{Ad}	3	0.9	2.8	3	0.7	1.9	3	1.1	3.5	1	1.3	3.7
D_8^{SC}	5	1.7	8.3	5	1.0	5.2	5	2.0	9.9	1	23	2286
$D_8^{(2a)}$	5	1.8	8.9	5	1.0	5.2	5	2.0	10.0	1	1766	5359
$D_8^{(2b)}$	5	1.7	8.4	5	1.0	5.3	5	2.0	9.9	2	7.7	10
$D_8^{(2c)}$	5	1.6	8.2	5	1.0	5.2	5	2.0	9.9	2	7.6	10
D_8^{Ad}	5	1.6	7.9	5	1.0	5.2	5	2.0	9.9	1	2.5	12
E_6^{SC}	2	1.8	2.4	2	1.2	1.6	1	3.2	3.2	2	2.8	3.8
E_6^{Ad}	2	1.8	2.4	2	1.4	1.9	1	2.6	3.3	2	2.7	3.7
E_7^{SC}	2	1.9	3.8	2	1.3	2.6	2	2.4	5.0	1	5.3	5.4
E_7^{Ad}	2	1.9	3.9	2	1.2	2.6	2	2.4	5.0	1	3.2	5.9
E_8	1	8.0	8.0	1	5.0	5.2	1	10	11	1	14	14
F_4	1	0.2	0.2	1	0.2	0.2	1	0.4	0.4	1	0.9	0.9
G_2	1	0.0	0.0	1	0.0	0.0	1	0.1	0.1	2	0.2	0.3

Table 5.8b: Recognition Timings (2/5)

L	$\mathbb{F}$	#	t_0	t
7-dim simple Lie algebra in A_2	$GF(3^3)$	1	0.2	0.3
14-dim simple Lie algebra in A_3	$GF(2^6)$	2	0.2	0.3
34-dim simple Lie algebra in A_5	$GF(2^6)$	1	0.4	0.4
34-dim simple Lie algebra in A_5	$GF(3^3)$	1	0.5	0.5
62-dim simple Lie algebra in A_7	$GF(2^6)$	1	2.4	2.4
79-dim simple Lie algebra in A_8	$GF(3^3)$	1	4.9	4.9
26-dim simple Lie algebra in D_4	$GF(2^6)$	1	0.6	0.6
44-dim simple Lie algebra in D_5	$GF(2^6)$	1	1.2	1.2
64-dim simple Lie algebra in D_6	$GF(2^6)$	1	3.3	3.3
90-dim simple Lie algebra in D_7	$GF(2^6)$	1	9.9	9.9
118-dim simple Lie algebra in D_8	$GF(2^6)$	1	24	24
77-dim simple Lie algebra in E_6	$GF(3^3)$	1	4.2	4.2
132-dim simple Lie algebra in E_7	$GF(2^6)$	1	29	29

Table 5.8c: Recognition Timings (3/5)

	GF(59)			GF(17)			$GF(3^3)$			GF(2)		
R	#	t_0	t	#	t_0	t	#	t_0	t	#	t_0	t
${}^2A_2^{SC}$	2	0	0	2	0	0	1	0	0	1	0	0
${}^2A_2^{Ad}$	2	0	0	2	0	0	1	0	0	2	0	0
${}^2A_3^{SC}$	3	0.1	0.1	3	0.1	0.1	3	0.1	0.2	1	0.2	0.3
${}^2A_3^{(2)}$	3	0	0.1	3	0	0.1	3	0.1	0.2	1	0.2	0.5
${}^2A_3^{Ad}$	3	0	0.1	3	0	0.1	3	0.1	0.2	1	0.1	0.2
${}^2A_4^{SC}$	2	0.2	0.4	2	0.2	0.4	2	0.3	0.5	2	0.2	0.4
${}^2A_4^{Ad}$	2	0.1	0.2	2	0.2	0.3	2	0.2	0.5	2	0.2	0.4
${}^2A_5^{SC}$	4	0.8	2.9	4	0.8	3	2	1.4	2.8	2	1.2	2.3
${}^2A_5^{Ad}$	4	0.5	1.8	4	0.8	3	2	1.1	3.2	2	1	3.4
${}^2A_5^{(3)}$	4	0.7	2.9	4	0.8	3.1	2	1.4	2.8	2	1	3.4
${}^2A_5^{(2)}$	4	0.8	2.9	4	0.8	3	2	1	3.1	2	1.2	2.3
${}^2A_6^{SC}$	2	2.7	5.4	2	2.8	5.5	2	3.8	7.5	2	2.3	4.3
${}^2A_6^{Ad}$	2	2.7	5.5	2	2.8	5.7	2	3.7	7.4	2	2.3	4.3
${}^2A_7^{SC}$	4	10	40	4	9.9	39	4	13	53	1	16	30
${}^2A_7^{(4)}$	4	9.9	39	4	10	40	4	13	52	2	34	46
${}^2A_7^{(2)}$	4	9.6	38	4	10	41	4	13	53	2	34	46
${}^2A_7^{Ad}$	4	9.7	39	4	10	40	4	14	54	1	14	50

Table 5.8d: Recognition Timings (4/5)

	GF(59)			GF(17)			$GF(3^3)$			GF(2)		
R	#	t_0	t	#	t_0	t	#	t_0	t	#	t_0	t
${}^2\mathrm{A}_8^{\mathrm{SC}}$	3	30	90	3	31	91	1	52	65	3	29	84
${}^2\mathrm{A}_8^{(3)}$	3	30	89	3	30	90	1	65	65	3	30	87
${}^2\mathrm{A}_8^{\mathrm{Ad}}$	3	30	89	3	31	91	1	40	73	2	80	232
${}^2\mathrm{D}_4^{\mathrm{SC}}$	5	0.2	1	5	0.3	1.5	5	0.4	2.2	1	1.2	2.6
${}^2\mathrm{D}_4^{(2a)}$	5	0.3	1.5	5	0.3	1.5	5	0.5	2.2		n/a	
${}^2\mathrm{D}_4^{(2b)}$	5	0.3	1.5	5	0.3	1.5	5	0.5	2.2		n/a	
${}^2\mathrm{D}_4^{(2c)}$	5	0.3	1.5	5	0.3	1.5	5	0.5	2.2	3	0.8	7.7
${}^2\mathrm{D}_4^{\mathrm{Ad}}$	5	0.3	1.5	5	0.3	1.5	5	0.3	1.6	1	0.4	1.5
${}^2\mathrm{D}_5^{\mathrm{SC}}$	3	2.2	6.3	3	2.2	6.4	3	3	8.9	1	4.3	6.1
${}^2\mathrm{D}_5^{(2)}$	3	1.3	3.7	3	2.2	6.5	3	3	8.8	1	3.1	8.9
${}^2\mathrm{D}_5^{\mathrm{Ad}}$	3	2.1	6.2	3	2.2	6.4	3	3	8.9	1	1.7	4.4
${}^2\mathrm{D}_6^{\mathrm{SC}}$	5	12	57	5	12	58	5	16	79	1	26	54
${}^2\mathrm{D}_6^{(2a)}$	5	6.8	32	5	7.1	34	5	16	80	1	11	86
${}^2\mathrm{D}_6^{(2b)}$	5	11	56	5	12	58	5	16	79		n/a	
${}^2\mathrm{D}_6^{(2c)}$	5	12	57	5	12	58	5	16	79		n/a	
${}^2\mathrm{D}_6^{\mathrm{Ad}}$	5	12	57	5	12	57	5	16	80	1	8	33
${}^2\mathrm{D}_7^{\mathrm{SC}}$	3	30	88	3	57	166	3	75	222	1	74	115
${}^2\mathrm{D}_7^{(2)}$	3	57	165	3	32	92	3	77	225	2	34	153
${}^2\mathrm{D}_7^{\mathrm{Ad}}$	3	54	161	3	30	89	3	76	224	1	33	91
${}^2\mathrm{D}_8^{\mathrm{SC}}$	5	258	1244	5	259	1247	5	336	1631	1	354	868
${}^2\mathrm{D}_8^{(2a)}$	5	260	1250	5	263	1269	5	339	1641	2	117	1423
${}^2\mathrm{D}_8^{(2b)}$	5	259	1238	5	264	1260	5	338	1634		n/a	
${}^2\mathrm{D}_8^{(2c)}$	5	259	1231	5	121	562	5	340	1638		n/a	
${}^2\mathrm{D}_8^{\mathrm{Ad}}$	5	246	1211	5	257	1253	5	327	1603	1	130	612
${}^3\mathrm{D}_4^{\mathrm{SC}}$	5	0.5	2.4	5	0.3	1.6	5	0.5	2.2	1	2.1	2.6
${}^3\mathrm{D}_4^{(2a)}$	5	0.5	2.4	5	0.3	1.5	5	0.5	2.3		n/a	
${}^3\mathrm{D}_4^{(2b)}$	5	0.5	2.4	5	0.3	1.5	5	0.5	2.3		n/a	
${}^3\mathrm{D}_4^{(2c)}$	5	0.5	2.4	5	0.3	1.5	5	0.5	2.3		n/a	
${}^3\mathrm{D}_4^{\mathrm{Ad}}$	5	0.5	2.4	5	0.3	1.5	5	0.3	1.7	1	0.4	1.7
${}^2\mathrm{E}_6^{\mathrm{SC}}$	2	24	48	2	26	50	1	34	34	2	15	30
${}^2\mathrm{E}_6^{\mathrm{Ad}}$	2	25	49	2	26	50	1	34	48	2	15	30

Table 5.8e: Recognition Timings (5/5)

6 Distance-Transitive Graphs

In this chapter we apply the algorithms developed in Chapters 3 and 4 to prove the following theorem.

Theorem 6.1. *Let G be the group of Lie type $\mathrm{E}_7{}^{\mathrm{ad}}(2)$ and let H be a maximal subgroup of G isomorphic to ${}^2\mathrm{A}_7(2^2)$. The permutation character of the G-action on $H\backslash\backslash G$ is not multiplicity free.*

This theorem, combined with Proposition 6.8, implies the following corollary.

Corollary 6.2. *Let G be the group of Lie type $\mathrm{E}_7{}^{\mathrm{ad}}(2)$ and let H be a maximal subgroup of G isomorphic to ${}^2\mathrm{A}_7(2^2)$. There is no graph structure on the G-set $H\backslash\backslash G$ such that G acts distance transitively on it.*

This result fits in the effort by Cohen, Lawther, Liebeck, and Saxl to classify the graphs on which an almost simple group of exceptional Lie type acts distance transitively [CLS02]. Most general results regarding distance transitivity in this chapter have been taken from [BCN89, Chapters 4, 7] and [Coh04]. The structure of the proof of Theorem 6.1 is similar to [Kro03, Chapter 5], where it is proved that no distance-transitive graph exists with automorphism group $\mathrm{E}_7(q)$ and vertex stabilizer subgroup $\mathrm{A}_7(q).2$, for $q = 2$ or $q = 4$.

In Sections 6.1 and 6.2 the relevant notions are introduced and some of the elementary theorems we use are proved. In Section 6.3 we first explain how the subgroups required for the proof of Theorem 6.1 can be constructed on the computer, using the algorithms developed in the previous chapters. We finally explain why the 6 orbits depicted in Table 6.22 are sufficient to prove the theorem.

To increase legibility we will mostly use action from the right in this chapter, e.g., $x \mapsto x^\delta$.

6.1 Distance transitivity

We assume graphs to be without loops and without multiple bonds. Let $\Gamma_1 = (V_1, E_1)$ and $\Gamma_2 = (V_2, E_2)$ be two graphs, and denote adjacency of two vertices v and w by $v \sim w$. They are said to be *isomorphic* if there exists some bijection $\varphi : V_1 \to V_2$ such that $\varphi(v) \sim \varphi(w)$ if and only if $v \sim w$. The bijection φ is called a *graph isomorphism*. An isomorphism from a graph to itself is called an *automorphism*. The set of all automorphisms of a graph Γ forms a group with respect to composition of maps. This group is called the *automorphism group of* Γ, denoted by $\mathrm{Aut}(\Gamma)$.

Let $\Gamma = (V, E)$ be a graph and let $G \leq \mathrm{Aut}(\Gamma)$ be a group acting truthfully on Γ. The image of a vertex $v \in V$ under the action of $g \in G$ will be denoted by v^g, and the G-orbit of v will be denoted by v^G. Similarly, the image of an edge $e = \{v, w\} \in E$ under the action of $g \in G$ will be denoted by $e^g = \{v^g, w^g\}$, and its G-orbit by e^G. By G_v we denote the subgroup of G of elements that stabilize v:

$$G_v := \{g \in G \mid v^g = v\}.$$

The group G is called *vertex transitive on* Γ if $v^G = V$ for all $v \in V$ (i.e., if every vertex is mapped to every other vertex by G), and it is called *edge transitive* if all $e^G = E$ for all $e \in E$ (i.e., if every edge of Γ is mapped to every other edge by G).

We adopt the convention that $d(v, w) := \infty$ if the vertices v and w are in different components of Γ. We define a partition of the set $V \times V$ into *distance sets*:

$$\Gamma_i := \{(v, w) \in V \times V \mid d(v, w) = i\}.$$

Fixing a vertex $v \in V$ we can define a partition of V by

$$\Gamma_i(v) := \{w \in V \mid d(v, w) = i\}.$$

The group G is called *distance transitive on* Γ if it acts transitively on all distance sets of Γ, i.e., if for all $x, y, v, w \in V$ such that $d(v, w) = d(x, y)$, there exists a $g \in G$ such that $v^g = x$ and $w^g = y$. The graph Γ is called a *distance-transitive graph* if its automorphism group acts distance transitively on it.

We prove the following elementary lemma.

Lemma 6.3. *Let $\Gamma = (V, E)$ be a connected graph with diameter d and let G be a group of automorphisms of Γ. Then G is distance transitive on Γ if and only if G is vertex transitive on V and G_v is transitive on the set $\Gamma_i(v)$ for each $i = 1, \ldots, d$ and for all $v \in V$.*

Proof Suppose Γ is distance transitive. If $|V| = 1$ the claim is trivially true, so we assume $|V| > 1$. To see that G is vertex transitive pick $v, w \in V$, and take $v', w' \in V$ such that $d(v, v') = 1 = d(w, w')$ (which is possible since $|V| > 1$ and Γ is connected). By distance-transitivity there exists a $g \in G$ such that $v^g = w$ and $(v')^g = w'$, hence G is vertex transitive. Now pick $v \in V$, $i \in \{1, \ldots, d\}$, and $w, u \in \Gamma_i(v)$, so that $d(v, w) = d(v, u) = i$. By distance-transitivity of Γ there exists a $g \in G$ such that $v^g = v$ and $w^g = u$, proving G_v is transitive on $\Gamma_i(v)$.

Now suppose G is vertex transitive and G_v is transitive on the set $\Gamma_i(v)$ for each $i = 0, \ldots, d$ and for all $v \in V$. Take $v, w, x, y \in V$ such that $d(v, w) = d(x, y) = i$. Since G is vertex transitive there exists a $g \in G$ such that $v^g = x$, and since $G \leq \mathrm{Aut}(\Gamma)$ we have $d(x, w^g) = d(v^g, w^g) = i$. Because G_x is transitive on $\Gamma_i(x)$ there is an $h \in G_x$ such that $(w^g)^h = y$. Consequently, $v^{gh} = x^h = x$ and $w^{gh} = y$, proving Γ is distance transitive. □

Before proceeding, we give two examples.

Example 6.5. The automorphism group G of the graph Δ_1 depicted in Figure 6.4 has order 12 and is generated by the permutations $(1, 2, 3)(4, 5, 6)$, $(1, 4)(2, 5)(3, 6)$, and $(2, 3)(5, 6)$. Δ_1 is not distance transitive: even though $d(1, 2) = d(1, 4) = 1$,

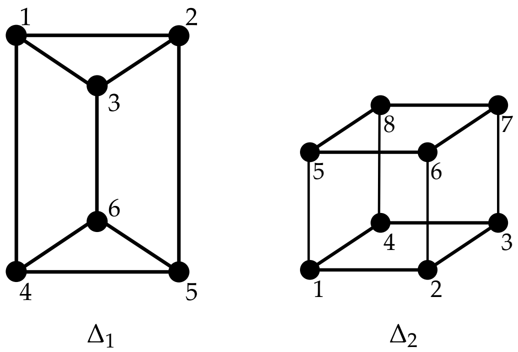


Figure 6.4: Examples of (non)-distance-transitive graphs

the edge $\{1,2\}$ will never be sent to the edge $\{1,4\}$ since the former is in a three-cycle and the latter is not.

It is on the other hand easy to see that G is vertex transitive. By Lemma 6.3 there should be a vertex stabilizer subgroup that does not act distance transitively. Indeed, consider the vertex stabilizer G_1 of 1. It does not act transitively on for example $(\Delta_1)_1(1)$: vertex 4 is never moved by G_1.

Example 6.6. The automorphism group G of the graph Δ_2 depicted in Figure 6.4 has order 48 and is generated by the permutations $(1,2)(3,4)(5,6)(7,8)$, $(2,4)(6,8)$, and $(3,6)(4,5)$.

We use Lemma 6.3 to see that Δ_2 is distance transitive. Firstly, it is immediately clear that G is vertex transitive, so that we only need to verify that G_1 is transitive on the set $\Gamma_i(1)$ for each $i = 0, \dots, 3$. Now indeed G_1 acts transitively on $(\Delta_2)_0(1) = \{1\}$, $(\Delta_2)_1(1) = \{2,4,5\}$, $(\Delta_2)_2(1) = \{3,8,6\}$, and on $(\Delta_2)_3(1) = \{7\}$ (observe the symmetries along the axis through vertices 1 and 7).

The following lemma and the proposition it implies will play an important role in our proof of Theorem 6.1.

Lemma 6.7 ([BCN89, 4.1B]). *The adjacency matrix of a distance-transitive graph Γ has precisely $d+1$ real distinct eigenvalues.*

The following proposition is straightforward, given this lemma.

Proposition 6.8 ([BCN89, Proposition 4.1.11]). *Let Γ be a distance-transitive graph with vertex set V and automorphism group G, and let π be the permutation character of the G-action on V. Firstly, $\langle \pi, \pi \rangle = d+1$, where d is the diameter of Γ. Secondly, the permutation character π of the G-action on V is multiplicity free.*

Proof Let d be the diameter of Γ and fix a vertex $v \in V$. There exists a partitioning of V into $d+1$ distance sets with respect to v. Since Γ is assumed to be distance transitive, the point stabilizer H in G of v acts transitively on each of the distance sets, hence they correspond to $d+1$ distinct H-orbits on V. Thus, using Frobenius reciprocity (cf. [Gor80, Theorem 4.5]), we see that

$$\langle \pi, \pi \rangle = \langle \pi, (1_H)^G \rangle = \langle \pi|_H, 1_H \rangle = d+1,$$

proving the first claim. For the second claim, let $\vartheta_0, \ldots, \vartheta_d$ be the eigenvalues of the adjacency matrix of Γ, which exist by Lemma 6.7. Since they are distinct, the corresponding $d+1$ eigenspaces in $\mathbb{R}^\Gamma$ are G-invariant, so that the (not necessarily distinct) characters $\chi_0, \ldots, \chi_d$ corresponding to these spaces are well defined. From $\pi = \sum_{i=0}^d \chi_i$ it follows that

$$d+1 = \langle \pi, \pi \rangle = \sum_{i=0}^{d} \sum_{j=0}^{d} \langle \chi_i, \chi_j \rangle \geq \sum_{i=0}^{d} \langle \chi_i, \chi_i \rangle \geq d+1,$$

showing that all characters $\chi_0, \ldots, \chi_d$ are distinct and irreducible. □

6.2 From groups to graphs

We have seen that for every graph we can construct a group that canonically belongs to it: its automorphism group. The question then arises whether we can reverse this process: given a group G, construct a graph Γ such that $\mathrm{Aut}(\Gamma) = G$.

Let G be a group, H a subgroup of G, and $r \in G$, $r \notin H$. We define $\Gamma(G, H, r)$ to be the graph whose vertex set is the set of left-cosets of H in G, denoted by $H\backslash\backslash G$, and whose adjacency is defined by $Hx \sim Hy \Leftrightarrow y \in HrHx$.

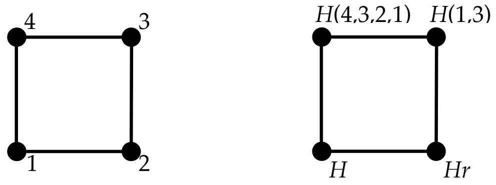
Lemma 6.9 ([Coh04, Theorem 3.1])**.** *Let $\Gamma = (V, E)$ be a distance-transitive graph and G its automorphism group. Fix a vertex $v \in V$, let $H = G_v$, and let $r \in G$ such that $v^r \in \Gamma_1(v)$. The graphs Γ and $\Gamma' = \Gamma(G, H, r)$ are isomorphic.*

Proof Recall that the vertex set of Γ' is $V' = H\backslash\backslash G$, and $Hx, Hy \in V'$ are connected if and only if $y \in HrHx$. First, every $w \in V$ is equal to v^g for some $g \in G$, giving a bijection between V and $V' = H\backslash\backslash G$ via $v^g \leftrightarrow Hg$. (The fact that this is a bijection follows immediately from the definition of H: indeed, suppose $w = v^g = v^h$ for some $g, h \in G$, $g \neq h$. Then $v^{gh^{-1}} = v$, so that $gh^{-1} \in G_v = H$ and therefore $Hg = Hh$. The reverse direction is easily proved along the same lines.)

Second, the set of neighbours of v is $\{v^{rh} \mid h \in H\}$, because H acts transitively on $\Gamma_1(v)$. For $Hx \in H\backslash\backslash G$, the set of neighbours of v^{Hx} is $\{v^{rhHx} \mid h \in H\} = v^{rHx}$. Therefore, $v^{Hx} \sim v^{Hy}$ if and only if $Hy = rHx$, which occurs if and only if $y \in HrHx$. This proves that $v^x \leftrightarrow Hx$ is indeed an isomorphism. □

Example 6.11. We consider the graph Δ_3 shown in Figure 6.10. Its automorphism group G has order 8 and is generated by $(1,2,3,4)$ and $(1,3)$, and Δ_3 is easily seen to be distance transitive.

We let $H = G_1 = \langle (2,4) \rangle$ and $r = (1,2,3,4)$ (so that $d(1, 1^r) = d(1,2) = 1$) and follow the procedure described above to construct $\Gamma(G, H, r)$. First, the vertex set is $H\backslash\backslash G$, so that there are 4 vertices:



Δ_3 $\Gamma(G, G_1, (1,2,3,4))$

Figure 6.10: A graph from a group

- $H = \{\text{id}, (2,4)\}$,
- $Hr = \{r = (1,2,3,4), (1,4)(2,3)\}$,
- $H(1,3) = \{(1,3), (1,3)(2,4)\}$, and
- $H(4,3,2,1) = \{(4,3,2,1), (1,2)(3,4)\}$.

Then, to find the edges, we compute

$$HrH = \{(1,2,3,4), (1,4)(2,3), (1,2)(3,4), (4,3,2,1)\} = Hr \cup H(4,3,2,1),$$

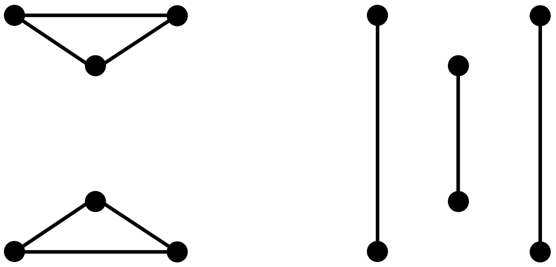
so that H is adjacent to Hr and $H(4,3,2,1)$. In the same fashion we find

- $HrHr = H(1,3) \cup H$,
- $HrH(1,3) = Hr \cup H(4,3,2,1)$, and
- $HrH(4,3,2,1) = H \cup H(1,3)$.

All in all, this gives the second graph in Figure 6.10.

Example 6.13. We investigate where the construction described above fails if the graph we start with is not vertex transitive or not edge transitive. So again consider Δ_1, depicted in Figure 6.4, and recall that $G = \langle (1,2,3)(4,5,6), (2,3)(5,6), (1,4)(2,5)(3,6) \rangle$ and $G_1 = \langle (2,3)(5,6) \rangle$. We take $r_1 = (1,2,3)(4,5,6)$ and $r_2 = (1,4)(2,5)(3,6)$, so that $r_i \in G$ but $r_i \notin H$ and we construct $\Gamma(G, G_1, r_i)$ (where $i = 1,2$).

The resulting graphs, shown in Figure 6.12, are clearly different from the graph Δ_1 we started with. This is a direct consequence of the fact that Δ_1 is not distance transitive, in particular of the fact that $\text{Aut}(\Delta_1)$ does not act transitively on the edges. This is exposed by the different choices for r: indeed, r_1 corresponds to the edge $\{1, 1^{r_1}\} = \{1,2\}$, whereas r_2 corresponds to the edge $\{1,4\}$.



$\Gamma(G, G_1, (1,2,3)(4,5,6))$ $\Gamma(G, G_1, (1,4)(2,5)(3,6))$

Figure 6.12: Two graphs from $\mathrm{Aut}(\Delta_1)$

Now the question that naturally arises is the following: "given a group G with a subgroup H, what are the conditions on G and H such that G acts distance transitively on $\Gamma(G, H, r)$ (for some $r \in G$)?" The following lemma limits the groups we need to consider in order to answer this question:

Lemma 6.14 ([Coh04, Theorem 3.2]). *Let G be a group, H a subgroup of G, and fix some $r \in G$. Consider $\Gamma = \Gamma(G, H, r)$.*

- *Γ is connected if and only if $\langle H, r\rangle = G$.*
- *Γ is undirected if and only if $HrH = Hr^{-1}H$.*

Proof The subgroup $\langle H, r\rangle$ is strictly smaller than G if and only if it does not work transitively on the set of right cosets of H in G. Thus if and only if it stabilizes some subset of $H\backslash\backslash G$. But that means that no vertex in this subset is connected to a vertex outside of the subset, hence that Γ is not connected. The second claim immediately follows from the observation that $x \sim y$ by definition if $y \in HrHx$, or equivalently if $x \in Hr^{-1}Hy$. □

In order to further limit the graphs under consideration, we introduce the notion of (im)primitivity. Let Γ be a graph of diameter d, let V be its vertices, and recall the partition of $V \times V$ into distance sets $\Gamma_i = \{(v, w) \in V \times V \mid d(v, w) = i\}$. The graph Γ is called *primitive* if Γ_i is connected for all i, and *imprimitive* otherwise. Two obvious examples of imprimitive graphs are the ones that are *bipartite* (where Γ_2 is disconnected) and the ones that are *antipodal* (where Γ_d is disconnected).

This notion is closely related to (im)primitivity in groups: A permutation group G on a set X is called *primitive* if the only G-invariant relations $\equiv$ on X are those defined by $x \equiv y$ if $x = y$ and by $x \equiv y$ for all $x, y \in X$. The permutation group G is called *imprimitive* otherwise. The following result is originally due to Smith [Smi71] (in fact, this result holds for the more general class of distance-regular graphs [BCN89, Theorems 4.1.10, 4.2.1], but we restrict to distance-transitive ones here).

$$\begin{tikzcd}
 & & \mathrm{E}_7(4) & & \\
 & \widetilde{\mathrm{E}_7(2)} \arrow[ur, phantom, sloped, "<"] \arrow[rr, bend right, "\tau"'] & & \mathrm{E}_7(2) \arrow[ul, phantom, sloped, ">"] & \\
{}^2\mathrm{A}_7(2^2) \arrow[ur, phantom, sloped, "<"] \arrow[rrrr, bend right, "\tau"'] & & & & \widetilde{{}^2\mathrm{A}_7(2^2)} \arrow[ul, phantom, sloped, ">"]
\end{tikzcd}$$

Figure 6.16: The groups involved

Lemma 6.15 ([Coh04, Corollary 5.2, Theorem 5.3]). *Suppose G acts distance-transitively on the connected graph Γ with diameter d. Then G is imprimitive if and only if Γ is; if this is the case then at least one of the following holds:*

(i) Γ is antipodal and G acts distance-transitively on the graph whose vertices are the equivalence classes $\Gamma_0 \cup \Gamma_d$, and where two vertices are adjacent if and only if they contain adjacent vertices in Γ.

(ii) Γ is bipartite and G acts distance-transitively on each of the two graphs obtained from Γ by taking the bipartite classes, where two vertices are adjacent if and only if they are at distance 2 in Γ.

This result prompts us to narrow the search for distance-transitive graphs to those that are primitive. Furthermore, if a group G acts transitively on the vertex set of a graph Γ, then Γ is primitive if and only if the vertex stabilizer subgroup G_v is a maximal subgroup of G for each vertex v of Γ (cf. [Rot95, Theorem 9.15]). So we restrict our study of distance transitivity to groups G and maximal subgroups $H < G$.

For example, $\mathrm{A}_7(q).2$ is a maximal subgroup of $\mathrm{E}_7(q)$. In [Kro03] it is proved that no distance-transitive graph exists with automorphism group $\mathrm{E}_7(q)$ and vertex stabilizer subgroup $\mathrm{A}_7(q).2$, for $q = 2$ or $q = 4$. An overview of the progress in the case where G is a finite exceptional group of Lie type is available online [CLS02]. Only a small number of cases is still open, due to bounds on the size of the subgroup H in relation to the overgroup G, general arguments on odd q, and explicit computations. In the next section we prove that no graph exists on which $\mathrm{E}_7{}^{\mathrm{ad}}(2)$ acts distance transitively with vertex stabilizer subgroup ${}^2\mathrm{A}_7(2^2)$.

6.3 ${}^2\mathrm{A}_7(2^2) < \mathrm{E}_7(2)$

The remainder of this section is devoted to the proof of Theorem 6.1. We let $R = (X, \Phi, Y, \Phi^\vee)$ be the adjoint root datum of type E_7, and we let $\mathrm{E}_7(4)$ be the corresponding group of Lie type over the field with 4 elements. This group is at the top of Figure 6.16. A subgroup of type $\mathrm{E}_7(2)$ is easy to construct on the computer:

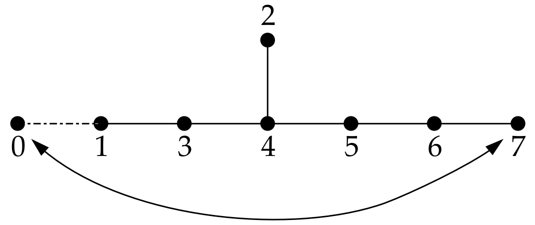


Figure 6.17: Extended Dynkin diagram of E_7 and the graph automorphism of A_7

we take the subgroup generated by $x_\alpha(a)$ (for $\alpha \in \Phi$ and $a \in GF(2)$) and $y \otimes t$ (for $y \in Y$ and $t \in GF(2)^*$). This group is denoted by $E_7(2)$ in Figure 6.16.

To make the other three subgroups featured in Figure 6.16 we explicitly follow the construction of ${}^2A_7(2^2)$ as described in Section 2.1. We introduce two involutions of $E_7(4)$. The first involution originates from the field automorphism of $GF(4)$, the Frobenius automorphism $i \mapsto i^2$ denoted by F. It extends to an automorphism of $E_7(4)$ by sending $x_\alpha(t)$ to $x_\alpha(t^2)$ and $y \otimes t$ to $y \otimes t^2$. The second involution is the nontrivial automorphism of the extended Dynkin diagram of E_7, sending α_0 to α_7, α_1 to α_6, etc. This involution will be denoted by δ. Since $\delta \in W(E_7)$ it corresponds to a $\dot{\delta} \in E_7(4)$ (see Section 1.10) and therefore it acts on $E_7(4)$ by conjugation: $g \mapsto g^{\dot{\delta}}$. Since it is clear from the context when we mean δ and when we mean $\dot{\delta}$, we will always write δ for ease of reading.

Now $E_7(4)_{\delta F}$ is by definition the subgroup of $E_7(4)$ consisting of the elements that are left invariant by δF. By Lang's theorem (cf. Theorem 1.54) it is isomorphic to the group $E_7(2)$ we constructed above. This subgroup $E_7(4)_{\delta F}$ is denoted by $\widetilde{E_7(2)}$ in Figure 6.16.

Observe that there exists a closed subsystem of type A_7 of extended E_7 that is left invariant by δ, thus inducing a subgroup $A_7(4)$ of $E_7(4)$. This implies that inside $\widetilde{E_7(2)}$ lives ${}^2A_7(2^2)$: those elements of the subgroup $A_7(4) < E_7(4)$ that are invariant under δF. This group is generated by $(\alpha_0 \otimes \xi)(\alpha_0 \otimes \xi)^{\delta F}$ and $x_{\alpha_0}(1)x_{\alpha_0}(1)^{\delta F}\dot{w}$, where ξ is a generator of $GF(4)^*$ and $w = s_{\alpha_0}s_{\alpha_7}s_{\alpha_1}s_{\alpha_6}s_{\alpha_3}s_{\alpha_5}s_{\alpha_4}$ (see [Ste62]).

By Lang's theorem there exists an isomorphism $\tau \in E_7(4)$ that sends $\widetilde{E_7(2)}$ to $E_7(2)$, and τ sends ${}^2A_7(2^2)$ to an isomorphic subgroup $\widetilde{{}^2A_7(2^2)} < E_7(2)$.

In the remainder of this section we show how $\widetilde{E_7(2)}$ and τ can be constructed as matrix groups in a computer algebra system. To that end, we let L be the Lie algebra $E_7(4)$ and let $b_1, \ldots, b_{133}$ be a basis for L. Now we consider L as a Lie algebra over the smaller field $GF(2)$. A basis is then $b_1, \ldots, b_{133}, \xi b_1, \ldots, \xi b_{133}$, where ξ is chosen such that $\xi \in GF(4)$ but $\xi \notin GF(2)$. We then compute the subalgebra M of L that is invariant under δF. Note that this is possible since F is a field automorphism and therefore acts on the Lie algebra just like it acts on the group and δ is an inner automorphism of $E_7(4)$, and therefore acts on the Lie algebra via the adjoint representation.

It is straightforward to see that M is defined over $GF(2)$ (in the sense that the structure constants that determine the multiplication are all in GF(2)). For suppose $a, b \in M$ and $[a,b] = (t\xi + u)c$, with $c \in M$ and $t, u \in \mathrm{GF}(2)$. Then $(t\xi + u)c = [a,b] = [a^{\delta F}, b^{\delta F}] = [a,b]^{\delta F} = ((t\xi+u)c)^{\delta F} = (t\xi^2 + u)c$, so that t must be equal to 0.

This means that $\widetilde{\mathrm{E}_7(2)}$ acts on M: To see this, suppose $g \in \widetilde{\mathrm{E}_7(2)}$ (so that then $g^{\delta F} = g$ by definition) and $x \in M$ (so that $x^{\delta F} = x$, again by definition). For clarity, we let ρ be the adjoint representation of $\mathrm{E}_7(4)$ acting on L. Since $\delta F = (\delta F)^{-1}$ we see that $(x^g)^{\delta F} = x \cdot \rho(g) \cdot \rho(\delta F) = x \cdot \rho(\delta F)) \cdot \rho((\delta F)^{-1}) \cdot \rho(g) \cdot \rho(\delta F) = x \cdot \rho(g^{\delta F}) = x^g$.

As mentioned earlier, because $\mathrm{E}_7(2) \cong \widetilde{\mathrm{E}_7(2)}$ there exists an isomorphism τ between the two, which can be found by computing a split maximal toral subalgebra and a Chevalley basis for $\widetilde{\mathrm{E}_7(2)}$. The isomorphism can then be determined by solving a system of linear equations, and we can verify that $\tau \in \mathrm{E}_7(4)$ using the "generalized row reduction" algorithm described in [CMT04]. This is the algorithm for Lang's theorem described in [CM09], but we need the algorithms developed in Chapters 3 and 4 since we are working over characteristic 2. We found the following expression for τ:

$$\begin{aligned}
\tau \;=\;& x_7(1)x_{13}(\xi^2)x_{19}(1)x_{25}(\xi^2)x_{31}(1)x_{36}(\xi^2)x_{45}(1)x_{49}(\xi)x_{39}(1)x_{44}(1)x_{48}(\xi^2)x_{52}(1)\\
& x_{51}(\xi^2)x_{54}(\xi)x_{57}(1)x_{56}(1)x_{60}(\xi^2)x_{61}(\xi)x_{62}(\xi^2)x_{63}(\xi^2)x_6(\xi^2)x_{12}(\xi^2)x_{18}(1)x_{24}(1)\\
& x_{23}(\xi)x_{33}(\xi^2)x_{35}(\xi^2)x_{38}(\xi^2)x_{40}(\xi^2)x_{43}(\xi^2)x_{42}(1)x_{50}(1)x_{53}(\xi^2)x_{16}(1)x_{21}(1)x_{26}(\xi)\\
& x_{28}(1)x_{32}(1)x_9(\xi)x_{15}(\xi)x_{14}(1)x_{20}(\xi^2)x_3(1)x_2(1)x_1(\xi) \quad (\xi^2,\xi^2,\xi^2,\xi,\xi^2,1,1) \quad n_1n_3n_1\\
& n_4n_2n_3n_1n_4n_3n_5n_4n_2n_3n_1n_4n_3n_5n_4n_2n_6n_5n_4n_2n_3n_1n_4n_3n_5n_4n_2n_6n_5n_4n_3n_1n_7n_6n_5n_4\\
& n_2n_3n_1n_4n_3n_5n_4n_2n_6n_5n_4n_3n_1n_7n_6n_5n_4n_2n_3n_4n_5n_6x_{25}(\xi^2)x_{31}(1)x_{30}(\xi^2)x_{36}(1)x_{41}(\xi)\\
& x_{45}(\xi)x_{49}(\xi^2)x_{34}(1)x_{39}(\xi)x_{44}(1)x_{48}(\xi)x_{47}(\xi^2)x_{51}(\xi)x_{54}(1)x_{56}(1)x_{58}(\xi)x_{59}(1)x_{60}(\xi)\\
& x_{61}(\xi^2)x_{62}(\xi)x_{63}(\xi)x_{12}(1)x_{18}(\xi)x_{24}(\xi^2)x_{27}(1)x_{23}(1)x_{29}(\xi^2)x_{33}(\xi^2)x_{35}(\xi^2)x_{38}(\xi^2)\\
& x_{40}(\xi^2)x_{43}(\xi)x_{42}(1)x_{46}(\xi)x_{50}(\xi)x_{53}(\xi)x_5(\xi^2)x_{11}(\xi^2)x_{17}(\xi)x_{22}(1)x_{21}(\xi)x_{28}(\xi^2)\\
& x_{32}(\xi^2)x_{37}(\xi)x_4(\xi)x_{10}(\xi^2)x_9(1)x_{15}(\xi^2)x_{14}(1)x_{20}(1)x_3(\xi)x_8(1)x_1(\xi^2),
\end{aligned}$$

where ξ is a generator of GF(4) satisfying $\xi^2 + \xi + 1 = 0$.

6.3.1 Towards the proof

We let $\mathbb{F} = \mathrm{GF}(2)$ and R the adjoint root datum of type E_7 with root system Φ. Moreover, we take $L = L_R(\mathbb{F})$ to be the corresponding Lie algebra, whose Chevalley basis is $\{X_\alpha, h_i \mid \alpha \in \Phi, i \in \{1, \ldots, 7\}$ and we take $v = h_2$.

We define $X = \{\mathbb{F}v^g \mid g \in H\backslash\backslash G\}$ and claim that as a G-set X is equal to $H\backslash\backslash G$. Indeed, G is transitive on X by construction and the stabilizer of $\mathbb{F}v$ in G contains H, and H is maximal in G. The elements of X can be expressed as elements of the Chevalley basis of L.

Now we define a second G-set $Y = \{\mathbb{F}(X_{\alpha_0})^g \mid g \in G\}$, let $P = \mathrm{C}_G(\mathbb{F}X_{\alpha_0})$ (so that $Y \cong P\backslash\backslash G$ as G-sets). We let ρ be the permutation character of the action of G on Y, so that $\rho = 1_P^G$. (We will study Y in more detail in Section 6.3.3 and show that it consists of extremal elements.)

Lemma 6.18. *ρ is multiplicity free of rank* 5.

Proof Let n be the number of P-orbits on Y. By Frobenius reciprocity we have

$$n = \langle \rho | P, 1_P \rangle = \langle \rho, (1_P)^G \rangle = \langle \rho, \rho \rangle.$$

Clearly, Y is in one-to-one correspondence to the set of right cosets $\{Pg \mid g \in G\}$ via $\mathbb{F}(X_{\alpha_0})^g \leftrightarrow Pg$, so that the number of P-orbits on Y is equal to the number of double cosets $P\backslash\backslash G/P$.

Since G is a Chevalley group, it has a (B, N) pair and, using the Bruhat decomposition, we have $G = BNB$. Because P is a parabolic subgroup of G of type D_6, we have $P = BN_{\mathrm{D}_6}B$ for some subgroup N_{D_6} of N, so that

$$P\backslash\backslash G/P = BN_{\mathrm{D}_6}B\backslash\backslash BNB/BN_{\mathrm{D}_6}B \cong W_{\mathrm{D}_6}\backslash\backslash W/W_{\mathrm{D}_6},$$

where W is the Weyl group of type E_7 and $W_{\mathrm{D}_6} < W$ the subgroup of type D_6.

With a computer algebra system it is easy to verify that $|W_{\mathrm{D}_6}\backslash\backslash W/W_{\mathrm{D}_6}| = 5$ and that the coset representatives, $g_1, \ldots, g_5$ say, are all involutions, so that $g_i^{-1} \in W_{\mathrm{D}_6}\backslash\backslash W/W_{\mathrm{D}_6}$ for all $i = 1, \ldots, 5$. Using the isomorphism of Y and $P\backslash\backslash G$, and the bijective correspondence between the G-orbits on $Y \times Y$ and $P\backslash\backslash G/P$, we find that this is equivalent to the fact that the G-orbits on $Y \times Y$ are all self-paired, by Lemma 6.14. But this implies that the permutation character ρ consists of 5 irreducible characters, hence it is multiplicity free. □

The following lemma hints at our strategy for the proof of Theorem 6.1.

Lemma 6.19. *If $\Gamma(G, H, r)$ is distance transitive then then number of H-orbits on Y is at most* 5.

Proof We let π be the permutation character of the action of G on X. Since X is equal to $H\backslash\backslash G$ its permutation character on X is 1_H, so that $\pi = 1_H^G$. It follows from Lemma 6.18 that there are 5 irreducible characters $\rho_1, \ldots, \rho_5$ such that $\rho = \sum_{i=1}^5 \rho_i$. We extend $\rho_1, \ldots, \rho_5$ to an orthonormal basis of irreducible characters $\rho_1, \ldots, \rho_k$ for the space of class functions, and we let $c_i \in \mathbb{N}$ be such that $\pi = \sum_{i=1}^k c_i\rho_i$. We find

$$\langle \pi, \rho \rangle = \sum_{i=1}^{k} \sum_{j=1}^{5} c_i \langle \rho_i, \rho_j \rangle = \sum_{i=1}^{5} c_i.$$

On the other hand, by applying Frobenius reciprocity, we find

$$\langle \pi, \rho \rangle = \langle (1_H)^G, \rho \rangle = \langle 1_H, \rho|_H \rangle = n,$$

where n is the number of H-orbits on Y. If $\Gamma(G, H, r)$ is distance transitive then π is multiplicity free by Proposition 6.8, so that the number of H-orbits on Y is at most 5. □

6.3.2 Distinguishing H-orbits

In this section we develop some tools to help us differentiate between different H-orbits on Y. Firstly, it is easily verified by computer calculations that the action of H on L decomposes into 3 irreducible modules: the 1-dimensional space $\mathbb{F}v$, which we will call S_1, a 62-dimensional subalgebra S_{62}, and a 70-dimensional subalgebra S_{70}. This is to be expected since H, a group of type ${}^2\mathrm{A}_7$, naturally acts on a Lie algebra M of type ${}^2\mathrm{A}_7$. The dimension of M is equal to 63, and it turns out that (because $\mathrm{char}(\mathbb{F}) = 2$) the Lie algebra M is a direct sum of $Z(M)$ and $[M, M]$, similar to the behaviour described for split Lie algebras of type A_7 in Section 5.2. This leaves $\dim(L) - 63 = 70$ dimensions for the third module, which is irreducible by maximality of H in G.

Lemma 6.20. *Let $S \in \{S_1, S_{62}, S_{70}\}$ and $y_1, y_2 \in Y$. If $\mathrm{C}_S(y_1) \not\cong \mathrm{C}_S(y_2)$ then y_1 and y_2 are in different H-orbits.*

Proof Observe that for $y \in Y$ and $g \in G$

$$\begin{aligned}
\mathrm{C}_S(y^g) &= \{s \in S \mid [s, y^g] = 0\} \\
&= \{s \in S \mid [s^{g^{-1}}, y]^g = 0\} \\
&= \{s \in S \mid [s^{g^{-1}}, y] = 0\} \\
&= \{(s^{g^{-1}})^g \in S \mid [s^{g^{-1}}, y] = 0\} \\
&= \left(\mathrm{C}_{S^{g^{-1}}}(y)\right)^g.
\end{aligned}$$

If $g \in H$ then $S^g = S$ so that the last line simplifies to $\mathrm{C}_S(y)^g$, showing that the structure of $\mathrm{C}_S(y)$ is an invariant for the action of H. □

6.3.3 Extremal Elements

In order to find suitable representatives of the orbits of H on L we introduce the concept of extremal elements.

Let L be a Lie algebra over a field $\mathbb{F}$. A non-zero element $x \in L$ is called *extremal* if there exists a linear map $g_x : L \to \mathbb{F}$ that satisfies the following *extremal identities* for all $y, z \in L$:

$$\begin{aligned}
[x, [x, y]] &= 2g_x(y)x, \\
[x, [y, [x, z]]] &= g_x([y, z])x - g_x(z)[x, y] - g_x(y)[x, z].
\end{aligned}$$

These identities go back to Premet, and they are also commonly called the *Premet identities*. We denote the set of extremal elements of L by $\mathcal{E}(L)$, or by $\mathcal{E}$ if no confusion is imminent. An extremal element x is called a *sandwich element* if g_x is identically zero.

Extremal elements were originally introduced by Chernousov [Che89] in his proof of the Hasse principle for E_8. Zel'manov and Kostrikin proved that, for every n, the universal Lie algebra L_n generated by a finite number of sandwich elements $x_1, \ldots, x_n$ is finite-dimensional [ZK90]. Cohen, Steinbach, Ushirobira, and Wales generalized this result and proved that, provided $\mathrm{char}(\mathbb{F}) \neq 2$, a Lie algebra generated by a finite number of extremal elements is finite dimensional. Moreover, they give an explicit lower bound on the number of extremal elements required to generate each of the classical Lie algebras [CSUW01]. Recently, In 't Panhuis, Postma, and the author of this thesis gave explicit presentations for Lie algebras of type A_n, B_n, C_n, and D_n, by means of minimal sets of extremal generators [itpPR09] (again excluding the case where $\mathrm{char}(\mathbb{F}) = 2$). Moreover, Draisma and In 't panhuis considered finite graphs and corresponding algebraic varieties whose points

$\dim(C_{S_{62}}(x)$	$x \in L$
29	x_{-63}
30	x_{-61}
33	x_{-53}
38	$x_{-59} + x_{-12}$
45	$x_3 + x_5 + x_6 + x_8 + x_{13} + x_{14} + x_{16} + x_{17} + x_{19} + x_{20} + x_{22} + x_{23} + x_{24} + x_{26} + x_{27} + x_{29} + x_{33} + x_{34} + x_{36} + x_{38} + x_{39} + x_{40} + x_{41} + x_{45} + x_{46} + x_{47} + x_{52} + x_{54} + x_{55} + x_{56} + x_{57} + x_{58} + x_{59} + x_{61} + x_{63} + x_{-1} + x_{-5} + x_{-6} + x_{-7} + x_{-10} + x_{-11} + x_{-14} + x_{-16} + x_{-21} + x_{-23} + x_{-25} + x_{-27} + x_{-28} + x_{-30} + x_{-31} + x_{-32} + x_{-35} + x_{-38} + x_{-41} + x_{-43} + x_{-44} + x_{-45} + x_{-48} + x_{-49} + x_{-50} + x_{-57} + x_{-59} + h_1 + h_3 + h_4 + h_6$
48	$x_3 + x_4 + x_5 + x_9 + x_{11} + x_{13} + x_{14} + x_{15} + x_{16} + x_{18} + x_{19} + x_{20} + x_{21} + x_{22} + x_{23} + x_{25} + x_{26} + x_{27} + x_{30} + x_{31} + x_{33} + x_{34} + x_{38} + x_{39} + x_{40} + x_{41} + x_{43} + x_{44} + x_{46} + x_{47} + x_{48} + x_{49} + x_{50} + x_{52} + x_{54} + x_{55} + x_{58} + x_{59} + x_{60} + x_{61} + x_{62} + x_{63} + x_{-1} + x_{-2} + x_{-6} + x_{-10} + x_{-12} + x_{-13} + x_{-15} + x_{-17} + x_{-18} + x_{-19} + x_{-22} + x_{-23} + x_{-25} + x_{-27} + x_{-30} + x_{-33} + x_{-34} + x_{-38} + x_{-39} + x_{-43} + x_{-57} + x_{-58} + x_{-59} + x_{-60} + h_2 + h_5$

Table 6.22: 6 different H-orbits on Y

parametrize Lie algebras generated by extremal elements. They proved in particular that if the graph is a simply laced Dynkin diagram of affine type, all points in an open dense subset of the affine variety parametrize Lie algebras isomorphic to the split finite-dimensional simple Lie algebra corresponding to the associated Dynkin diagram of finite type [Ditp08]. Furthermore, Cohen, Ivanyos, and the author of this thesis proved that if L is a Lie algebra over a field $\mathbb{F}$ (of characteristic distinct from 2 and 3) that has an extremal element that is not a sandwich, then L is generated by extremal elements, with one exception in characteristic 5 [CIR08]. The strong connection between extremal elements and geometries is further investigated in two papers by Cohen and Ivanyos [CI06, CI07], and in the Ph.D. theses by Postma and In 't panhuis [Pos07, itp09].

For the proof of Theorem 6.1 we will use the following lemma.

Lemma 6.21. *The group G acts transitively on the set $\mathcal{E}(L)$ of extremal elements of L.*

Proof An equivalent statement is that $\mathcal{E}(L)$ is equal to $X_{\alpha_0}^G$, since X_{α_0} is a long root element and therefore extremal. But by [CI06, Theorem 28] extremal elements correspond to abstract root subgroups, and Timmesfeld's study of abstract root subgroups forbids two distinct orbits in this case [Tim01, Theorem 2.14]. □

6.3.4 $\Gamma(E_7(2), {}^2A_7(2^2), r)$ is not multiplicity free

Recall we defined G to be the group of Lie type $E_7(2)$ and H a subgroup of G of type ${}^2A_7(2^2)$. Furthermore, we defined L to be the Chevalley Lie algebra of type E_7

over $\mathbb{F} = \mathrm{GF}(2)$, we let $X_{\alpha_0} \in L$ be the root element corresponding to the longest negative root, and we defined $Y = \{\mathbb{F}(X_{\alpha_0})^g \mid g \in G\}$.

In Table 6.22 we list 6 different orbits of H on Y, using the invariants defined in Section 6.3.2. The first column contains the dimension of $\mathrm{C}_{S_{62}}(x)$, where x is the element of L shown in the second column. These orbits were found using the computer algebra system MAGMA 2.15 [BC08], on a Quad-Core Intel Xeon running at 3 GHz, taking roughly 12 CPU hours.

Since the table contains 6 different values of $\mathrm{C}_{S_{62}}(x)$, this shows that the elements of L are in different H-orbits. It remains to show that they are in the same G-orbit, i.e., that they are elements of Y. For the first three rows it is immediate that $\mathbb{F}x = \mathbb{F}X^t_{\alpha_0}$ for some $t \in G$, since both x and X_{α_0} are long root elements and G acts transitively on long root elements. For the last three rows it is easily checked by machine that each of the given elements is extremal, so that it is in the G-orbit of $\mathbb{F}X^t_{\alpha_0}$ by Lemma 6.21.

This shows that there are more than 5 different H-orbits on Y, thus completing the proof of Theorem 6.1 by Lemma 6.19, and the proof of Corollary 6.2 by Proposition 6.8.

We have tried to apply the method described in this section to various other open cases, such as ${}^2\mathrm{A}_7(4^2) < \mathrm{E}_7(4)$ and ${}^2\mathrm{E}_6(q^2) < \mathrm{E}_7(q)$ for $q = 2, 4$. Unfortunately, although the groups relevant to these cases are easily constructed in MAGMA, the methods we used to find orbit representatives proved to be insufficient.

Samenvatting

Algoritmen voor Lie algebra’s van algebraïsche groepen

In dit proefschrift beschrijven we verschillende nieuwe algoritmen voor het werken met enkelvoudige algebraïsche groepen en de Lie algebra’s die daarmee samenhangen. Er is al veel onderzocht aan deze groepen en algebra’s, in eerste instantie vanuit een meer theoretische invalshoek en later met als doel berekeningen met deze objecten op de computer mogelijk te maken. Dit heeft geleid tot implementaties in computeralgebrasystemen zoals GAP en Magma. De resultaten in dit proefschrift bouwen in het bijzonder voort op werk van Arjeh Cohen, Willem de Graaf, Sergei Haller, Scott Murray en Don Taylor. Dit werk wordt gedeeltelijk gestimuleerd door het “matrix group recognition project”: een internationaal project waarin talloze wetenschappers werken aan de algoritmische analyse van allerlei problemen met matrixgroepen over eindige lichamen.

Een nadeel van veel algoritmen die in deze tak van onderzoek zijn ontwikkeld is dat ze alleen toepasbaar zijn op groepen en algebra’s gedefiniëerd over lichamen van karakteristiek 0 of tenminste 5. Recente algoritmes van Cohen en Murray, en onafhankelijk daarvan Ryba, voor het berekenen van gespleten maximale torale deelalgebra’s van een Lie algebra werken bijvoorbeeld in alle karakteristieken behalve 2 en (tot op zekere hoogte) 3. Evenzo is het bepalen van een Chevalley basis van een Lie algebra (gegeven een gespleten maximale torale deelalgebra) eenvoudig in vrijwel alle karakteristieken, en is dan ook geïmplementeerd in GAP en Magma. In karakteristiek 2 en 3 is het probleem echter veel moeilijker.

Het eerste deel van dit proefschrift is gewijd aan een uitgebreide introductie van de relevante wiskundige objecten, zoals root data, algebraïsche groepen, en Lie algebra’s. De nieuwe resultaten zijn een heuristisch algoritme voor het vinden van gespleten maximale torale deelalgebra’s van Lie algebra’s van gespleten enkelvoudige algebraïsche groepen over lichamen van karakteristiek 2, en een algoritme voor het vinden van Chevalley bases van Lie algebra’s van gespleten enkelvoudige algebraïsche groepen over willekeurige lichamen. Van het laatste algoritme bewijzen we dat het polynomiaal is wanneer het betreffende lichaam eindig is. Deze algoritmen worden toegepast bij het herkennen van dit type Lie algebra’s en ze helpen bij de analyse van de bijbehorende algebraïsche groepen. Bovendien passen we deze algoritmen toe bij het bewijzen, met behulp van de computer, dat er geen graaf is waarop een bepaalde groep afstands-transitief werkt.

Alle in dit proefschrift beschreven algoritmen zijn geïmplementeerd in het computeralgebrasysteem Magma.

Abstract

Algorithms for Lie Algebras of Algebraic Groups

In this thesis we present several new algorithms for dealing with simple algebraic groups and their Lie algebras. These groups and algebras have been studied for a long time, first in a theoretical sense and later with regards to effective calculations on the computer, including implementations in the GAP and MAGMA computer algebra systems. We build in particular on work by Arjeh Cohen, Willem de Graaf, Sergei Haller, Scott Murray, and Don Taylor. The work is partly stimulated by the matrix group recognition project: an international project which is aimed at the algorithmic analysis of problems with matrix groups over finite fields.

Many algorithms that have been previously developed in this branch of research, however, apply only to groups and algebras over fields of characteristic 0 or at least 5. For instance, Cohen and Murray, and, independently, Ryba recently gave an algorithm for computing a split maximal toral subalgebra of a Lie algebra in all characteristics except 2 and (to a certain extent) 3. Unfortunately, not only their proofs but also their algorithms do not work in the excluded cases. Similarly, the algorithm for computing a Chevalley basis of a Lie algebra, when given a split toral subalgebra, is straightforward in almost all characteristics, and has consequently been implemented in major computer algebra systems such as GAP and MAGMA. In characteristics 2 and 3, however, the algorithm is much more involved.

This thesis starts with an extensive introduction to the mathematical objects occurring in this thesis, such as root data, algebraic groups, and Lie algebras. The new results in this thesis are a heuristic algorithm for computing split maximal toral subalgebras of Lie algebras of split simple algebraic groups over fields of characteristic 2, and an algorithm for computing Chevalley bases of Lie algebras of split simple algebraic groups over any field. The latter algorithm is proved to be polynomial in the case where the field is finite. These algorithms are applied to the problem of recognizing these Lie algebras among all Lie algebras, and they help in the analysis of the associated algebraic groups. We also apply these algorithms in the computer aided proof that there is no graph on which a certain group acts distance transitively.

All of the algorithms presented in this thesis have been implemented in the MAGMA computer algebra system.

Acknowledgements

The booklet you have before you would not have been the same without the help of many, many people. Fortunately, this section exists to thank some of them.

Arjeh, zonder jou was dit proefschrift er niet geweest. Aan de ene kant ben je een uitstekende bron van ideeën; aan de andere kant ben je precies en doelgericht als zaken nodig op papier gezet moeten worden. Ik heb bewondering voor de manier waarop je tussen deze twee uitersten kunt manouvreren.

I would like to thank the other members of my defense committee: Jos Baeten, Andries Brouwer, Andrea Caranti, Hans Cuypers, Jan Draisma, Bill Kantor, and Gabriele Nebe for taking the time to read my thesis and travel to Eindhoven for the defense. I'm particularly grateful to Bill Kantor: the large number of questions you asked about the early draft and the large number of improvements you suggested really made this a better thesis.

Scott, thank you for all the useful discussions we had during my stay in Sydney and during your visits to Eindhoven.

My HG 9.50 office mates: Jos, je sarcastische opmerkingen werden gelukkig ruimschoots gecompenseerd met de aanvoer van frisdrank en rijstwafels. Çiçek, it's great to have your happy presence and your excellent cooking. Maxim, verfrissend vind ik de hoeveelheid energie waarmee je vecht tegen alles wat onrechtvaardig of slecht voor onze planeet is.

Rianne, het verveelt nooit om met je over boeken, reizen en van alles te praten. Ook is het heel prettig dat dingen die nu eenmaal geregeld moeten worden bij jou en Anita altijd in goede handen zijn. Jan, dankjewel dat je kamerdeur altijd open staat, zodat ik je met triviale vragen kan lastigvallen. Hans Sterk, ook jij bedankt voor je preciese lezing van mijn proefschrift, en voor wat je me geleerd hebt als het over lesgeven gaat. Shona, great fun to have an Aussie (/Kiwi/Chinese) girl in the group for a while, although I think our sleep-wake rhythms may be more in sync when you're still in Eindhoven and I'm in Sydney. Hopefully we meet again!

A thank you also to Aart, Bart, Hennie, Jan-Willem, Rikko, and Shoumin, and the members of the neighbouring Coding & Crypto, Combinatorial Optimization, and Security groups. All of you make the ninth (and occasionally eighth and tenth) floor a good place to be.

Peter Horn, thank you for the productive times we had working on the SCIEnce project, and the countless Skype chats on everything and nothing. It's great working with you. Erik, omdat we samen (eindelijk) een gepubliceerd artikel hebben, en voor jouw proefschrift waaruit ik niet alleen inspiratie heb opgedaan, maar ook talloze ideeën gestolen heb (zoals je gevarieerde notatie voor voortbrengers en je tweetalige acknowledgements).

Peter en Richard, ik vind het erg leuk dat jullie me als paranimfen bij mijn promotie morele ondersteuning zullen verlenen; in die tijd hadden we ook een slordige 85 rondjes bij Hezemans kunnen rijden.

Alle bananen en -aanhang, ik ga hier vanwege ruimtegebrek maar niet in detail in op onze vriendschap maar volsta met jullie namen te noemen: Richard & Paulien, Sander & Judy, Peter, Anette & Ronald, Maartje & Stijn, Pieter & Ellen, Marc & Lisanne, Esther & Peter, Mark, Mark, Wouter & Lieke, Finbar & Xiaoting, en jullie te bedanken voor alle leuke momenten die zijn geweest en ongetwijfeld nog komen gaan.

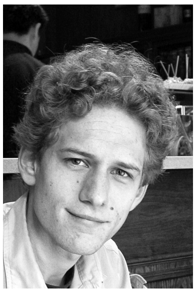
Fons, Liesbeth, Bennie, Brenda, Robbie: goed om te weten dat ik inmiddels zo geaccepteerd en geïntegreerd ben bij jullie dat ik Dommelsch mag gaan uitlaten als ik (onbedoeld!) jullie gasten beledig.

Arja en Cor, omdat jullie me hebben gemaakt tot wie ik ben en omdat jullie me altijd hebben aangemoedigd om te doen wat ik wilde doen. Zelfs als dat betekent dat we een tijd lang ruim 16000 km moeten reizen om elkaar te zien. Ik ben jullie dankbaar voor alles. Peter & Floor, veel sterkte met het compenseren van onze afwezigheid: jullie zullen twee keer zoveel eten moeten wegwerken bij jullie bezoeken aan Deventer.

Tot slot natuurlijk Marieke: dankjewel voor alle kleur die je aan mijn leven geeft!

Dan Roozemond
Eindhoven, February 2010

Curriculum Vitae



Dan Roozemond was born on January 3, 1982 in Leiden, the Netherlands. He finished his pre-university education at the Sint-Oelbertgymnasium in Oosterhout, and started his studies at the Technische Universiteit Eindhoven in September 2000.

After completing the first year in both mathematics and computer science, he continued in mathematics and received his Bachelor's of Science degree cum laude in August 2003. In the fall of 2003 he carried out an internship at the Technische Universität Berlin, working on automatic theorem proving in Cinderella, a popular interactive geometry software package. In August 2005, after writing his Master's thesis titled *Lie Algebras Generated by Extremal Elements*, Dan received his Master's of Science degree in Industrial and Applied Mathematics from the Technische Universiteit Eindhoven. This degree was awarded cum laude.

He then continued as a Ph.D. student in the Discrete Algebra and Geometry group in Eindhoven, under supervision of prof. dr. Arjeh M. Cohen. Apart from the research that found its way into this thesis, he was involved in the European SCIEnce project, focussing on the interaction between various computer algebra systems using the OpenMath standard. In 2006 he lived in Sydney for six months, working on the Lie theory aspects of the Magma computer algebra system. During his time in Eindhoven he was a member of the departmental council, first as a student (2003 – 2005) and later as a staff member (2006 – 2009). He was the vice-chairman of this council in 2008 and 2009.

His research focuses on the computational aspects of Lie theory. Apart from mathematics, Dan likes to travel and enjoys making photographs. Fortunately, these three activities are easily combined.

After his defense, Dan will work as a postdoctoral researcher at the University of Sydney.

Bibliography

[BC] F. Buekenhout and A.M. Cohen. Diagram geometry. In preparation.

[BC08] W. Bosma and J. J. Cannon, editors. *Handbook of Magma Functions, Edition 2.15*. School of Mathematics and Statistics, University of Sydney, 2008. http://magma.maths.usyd.edu.au/.

[BCN89] A.E. Brouwer, A.M. Cohen, and A. Neumaier. *Distance-Regular Graphs*. Springer, Berlin, 1989.

[Bor91] Armand Borel. *Linear Algebraic Groups*. Springer-Verlag, New York, second edition, 1991.

[Bou81] Nicolas Bourbaki. *Éléments de mathématique*. Masson, Paris, 1981. Groupes et algèbres de Lie. Chapitres 4, 5 et 6. [Lie groups and Lie algebras. Chapters 4, 5 and 6].

[Car72] Roger W. Carter. *Simple groups of Lie type*. Pure and Applied Mathematics (New York). John Wiley & Sons Inc., New York, 1972.

[CCN$^+$85] John Horton Conway, Robert Turner Curtis, Simon Phillips Norton, Richard A Parker, and Robert Arnott Wilson. *Atlas of Finite Groups: Maximal Subgroups and Ordinary Characters for Simple Groups*. Oxford University Press, 1985.

[Che58] C. Chevalley. *Classification des groupes de Lie algébriques*. Séminaire Ecole Normale Supérieure, Paris, 1956–1958.

[Che89] V. I. Chernousov. On the Hasse principle for groups of type E_8. *Dokl. Akad. Nauk SSSR*, 306, 25:1059–1063, 1989. Translation in Soviet Math. Dokl. 39, 592–596, 1989.

[CHM08] Arjeh M. Cohen, Sergei Haller, and Scott H. Murray. Computing in unipotent and reductive algebraic groups. *LMS Journal of Computational Mathematics*, 11:343–366, 2008.

[CI06] Arjeh M. Cohen and Gábor Ivanyos. Root filtration spaces from Lie algebras and abstract root groups. *J. Algebra*, 300(2):433–454, 2006.

[CI07] Arjeh M. Cohen and Gábor Ivanyos. Root shadow spaces. *European J. Combin.*, 28(5):1419–1441, 2007.

[CIR08] Arjeh M. Cohen, Gábor Ivanyos, and Dan A. Roozemond. Simple Lie algebras having extremal elements. *Indagationes Mathematicae*, 19(2):177–188, 2008.

[CLS02] A table of exceptional groups acting on possibly distance-transitive graphs, 2002. http://www.win.tue.nl/~amc/oz/dtg/tableCLS.html.

[CM09] Arjeh M. Cohen and Scott H. Murray. An algorithm for Lang's theorem. *Journal of Algebra*, 322:675–702, 2009.

[CMT04] Arjeh M. Cohen, Scott H. Murray, and D.E. Taylor. Computing in groups of Lie type. *Mathematics of Computation*, 73(247):1477–1498, 2004.

[Coh04] A.M. Cohen. Distance-transitive graphs. In L.W. Beineke and R.J. Wilson, editors, *Topics in Algebraic Graph Theory*, volume 102 of *Encyclopedia of Mathematics and Its Applications*, pages 222–249. Cambridge University Press, 2004.

[CR09] Arjeh M. Cohen and Dan Roozemond. Computing Chevalley bases in small characteristics. *J. Algebra*, 322(3):703–721, August 2009.

[CSUW01] Arjeh M. Cohen, Anja Steinbach, Rosane Ushirobira, and David Wales. Lie algebras generated by extremal elements. *J. Algebra*, 236(1):122–154, 2001.

[dG97] Willem A. de Graaf. *Algorithms for Finite-Dimensional Lie Algebras*. PhD thesis, Technische Universiteit Eindhoven, 1997.

[dG00] Willem A. de Graaf. *Lie Algebras: Theory and Algorithms*, volume 56 of *North Holland Mathematical Library*. Elsevier Science, 2000.

[Ditp08] Jan Draisma and Jos in 't panhuis. Constructing simply laced Lie algebras from extremal elements. *Algebra Number Theory*, 2(5):551–572, 2008.

[GLS98] Daniel Gorenstein, Richard Lyons, and Ronald Solomon. *The Classification of the Finite Simple Groups, Number 3*, volume 40 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, Rhode Island, 1998.

[Gor80] D. Gorenstein. *Finite Groups*. Chelsea, New York, 2nd edition, 1980.

[Gor85] Daniel Gorenstein. The enormous theorem. *Scientific American*, 253(6):104–115, 1985.

[HEO05] Derek F. Holt, Bettina Eick, and Eamonn A. O'Brien. *Handbook of computational group theory*. Discrete Mathematics and its Applications (Boca Raton). Chapman & Hall/CRC, Boca Raton, FL, 2005.

[Hog78] G.M.D. Hogeweij. *Ideals and Automorphisms of Almost-Classical Lie Algebras*. PhD thesis, Universiteit Utrecht, 1978.

[Hog82] G.M.D. Hogeweij. Almost-classical Lie algebras. I. *Nederl. Akad. Wetensch. Indag. Math.*, 44(4):441–452, 1982.

[Hol98] Derek F. Holt. *The atlas of finite groups: ten years on (Birmingham, 1995)*, volume 249 of *London Math. Soc. Lecture Note Ser.*, chapter The Meataxe as a tool in computational group theory, pages 74–81. Cambridge Univ. Press, Cambridge, 1998.

[Hum67] James E. Humphreys. *Algebraic groups and modular Lie algebras*, volume 71 of *Memoirs of the American Mathematical Society*. American Mathematical Society, Providence, Rhode Island, 1967.

[Hum72] James E. Humphreys. *Introduction to Lie Algebras and Representation Theory*. Graduate Texts in Methematics. Springer-Verlag New York, 1972.

[Hum75] James E. Humphreys. *Linear Algebraic Groups*. Graduate Texts in Methematics. Springer-Verlag New York, 1975.

[IL00] Gábor Ivanyos and Klaus Lux. Treating the exceptional cases of the MeatAxe. *Experiment. Math.*, 9(3):373–381, 2000.

[itp09] Jos C.H.W. in 't panhuis. *Lie algebras, extremal elements, and geometries*. PhD thesis, Technische Universiteit Eindhoven, 2009.

[itpPR09] Jos in 't panhuis, Erik Postma, and Dan Roozemond. Extremal presentations for classical Lie algebras. *J. Algebra*, 322(2):295–326, 2009.

[Jac62] N. Jacobson. *Lie Algebras*, volume 10 of *Interscience Tracts in Pure and Applied Mathematics*. Interscience Publishers, 1962.

[Jan03] Jens Carsten Jantzen. *Representations of algebraic groups*, volume 107 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, 2003.

[Kro03] C. Krook. Graphs related to $E_7(q)$: A quest for distance-transitivity. Master's thesis, Technische Universiteit Eindhoven, 2003.

[Lan56] S. Lang. Algebraic groups over finite fields. *American Journal of Mathematics*, 78:555–563, 1956.

[OR09] John J. O'Connor and Edmund F. Robertson. The MacTutor history of mathematics archive, 2009. http://www-history.mcs.st-and.ac.uk/.

[Pos07] Erik J. Postma. *From Lie algebras to geometry and back*. PhD thesis, Technische Universiteit Eindhoven, 2007.

[Rón90] Lajos Rónyai. Computing the structure of finite algebras. *Journal of Symbolic Computation*, 9:355–373, 1990.

[Rot95] Joseph J. Rotman. *An Introduction to the Theory of Groups*. Springer-Verlag, New York, 1995.

[Ryb07] Alexander J. E. Ryba. Computer construction of split Cartan subalgebras. *J. Algebra*, 309(2):455–483, 2007.

[Sel67] George B. Seligman. Some results on Lie p-algebras. *Bull. Amer. Math. Soc.*, 73:528–530, 1967.

[Ser06] Ákos Seress. A unified approach to computations with permutation and matrix groups. In *International Congress of Mathematicians. Vol. II*, pages 245–258. Eur. Math. Soc., Zürich, 2006.

[Shp99] Igor E. Shparlinski. *Finite fields: theory and computation*, volume 477 of *Mathematics and its Applications*. Kluwer Academic Publishers, Dordrecht, 1999.

[Smi71] D.H. Smith. Primitive and imprimitive graphs. *Quart. J. Math. Oxford (2)*, 22:551–557, 1971.

[Sol95] Ron Solomon. On finite simple groups and their classification. *Notices of the American Mathematical Society*, 1995. http://www.ams.org/notices/199502/solomon.pdf.

[Spr98] T.A. Springer. *Linear Algebraic Groups*, volume 9 of *Progress in Mathematics (Boston, Mass.)*. Birkhäuser, second edition, 1998.

[Ste61] Robert Steinberg. Automorphisms of classical Lie algebras. *Pacific J. Math.*, 11:1119–1129, 1961.

[Ste62] Robert Steinberg. Generators for simple groups. *Canad. J. Math.*, 14:277 – 283, 1962.

[Ste67] Robert Steinberg. *Lectures on Chevalley groups*. Yale University, 1967. Notes prepared by John Faulkner and Robert Wilson.

[Str04] Helmut Strade. *Simple Lie algebras over fields of positive characteristic. I*, volume 38 of *de Gruyter Expositions in Mathematics*. Walter de Gruyter & Co., Berlin, 2004. Structure theory.

[Str06] Helmut Strade. The classification of the simple modular Lie algebras. http://www.win.tue.nl/diamant/liealgebras/strade.pdf, 2006.

[Tim01] Franz Georg Timmesfeld. *Abstract Root Subgroups and Simple Groups of Lie-Type*, volume 95 of *Monographs in Mathematics*. Birkhäuser Verlag, 2001.

[ZK90] E.I. Zel′manov and A.I. Kostrikin. A theorem on sandwich algebras. *Trudy Mat. Inst. Steklov.*, 183:106–111, 225, 1990. Translated in Proc. Steklov Inst. Math. **1991**, no. 4, 121–126, Galois theory, rings, algebraic groups and their applications (Russian).

Index