Relative Springer isomorphisms and the conjugacy classes in Sylow p-subgroups of Chevalley groups

by

Simon Mark Goodwin

A thesis submitted to
The University of Birmingham
for the degree of
Doctor of Philosophy

School of Mathematics and Statistics
The University of Birmingham
December 8, 2004

Abstract

Let G be a simple linear algebraic group over the algebraically closed field k. Assume $p = \operatorname{char} k > 0$ is good for G and that G is defined and split over the prime field $\mathbb{F}_p$. For a power q of p, we write $G(q)$ for the Chevalley group consisting of the $\mathbb{F}_q$-rational points of G. Let $F : G \to G$ be the standard Frobenius morphism such that $G^F = G(q)$. Let B be an F-stable Borel subgroup of G; write U for the unipotent radical of B and $\mathfrak{u}$ for its Lie algebra. We note that U and $\mathfrak{u}$ are F-stable and that $U(q)$ is a Sylow p-subgroup of $G(q)$.

We study the adjoint orbits of U and show that the conjugacy classes of $U(q)$ are in correspondence with the F-stable adjoint orbits of U. This allows us to deduce results about the conjugacy classes of $U(q)$. We are also interested in the adjoint orbits of B in $\mathfrak{u}$ and the $B(q)$-conjugacy classes in $U(q)$. In particular, we consider the question of when B acts on a B-submodule of $\mathfrak{u}$ with a Zariski dense orbit.

For our study of the adjoint orbits of U we require the existence of B-equivariant isomorphisms of varieties $U/M \to \mathfrak{u}/\mathfrak{m}$, where M is a unipotent normal subgroup of B and $\mathfrak{m} = \operatorname{Lie} M$. We define *relative Springer isomorphisms* which are certain maps of the above form and prove that they exist for all M.

Acknowledgements

First and foremost I thank my supervisor Gerhard Röhrle. His knowledge and advice have been invaluable and his enthusiasm an inspiration.

I am also grateful to Chris Parker and Robert Wilson for their support and I thank Geoff Robinson for conversations about §5.3 of this thesis.

I thank my cohabitants of office 203: Ahmed Alghamdi, John Bradley, Murray Clelland and Stuart Hendren.

I am particularly grateful to my girlfriend Lucy Partridge for all her support and encouragement.

Finally, I acknowledge the financial support of the Engineering and Physical Sciences Research Council.

Contents

Introduction

Let G be a reductive algebraic group over the algebraically closed field k. We write $\mathfrak{g}$ for the Lie algebra of G and $\mathcal{N}$ for the nilpotent variety of $\mathfrak{g}$.

There has been a lot of interest in the nilpotent orbits of G, i.e. the adjoint orbits of G in $\mathcal{N}$. One of the first results in this direction says that if $\operatorname{char} k$ is zero or good for G, then there are only finitely many orbits of G in $\mathcal{N}$ – this was proved by R.W. Richardson in [56]. This finiteness result was generalized to arbitrary characteristic by D. Holt and N. Spaltenstein, see [36].

There has also been interest in classifying the nilpotent G-orbits. The Dynkin–Kostant classification which is based on the Jacobson–Morozov theory is valid for $\operatorname{char} k$ zero or "sufficiently large" and associates to each nilpotent orbit a weighted Dynkin diagram. This classification was proved for $\operatorname{char} k = 0$ by B. Kostant in [48] using work of E.B. Dynkin from [21]. The classification was shown to be valid for $\operatorname{char} k$ "sufficiently large" by T.A. Springer and R. Steinberg in [67] (see also [17, 5.6]).

The more well-known classification of the nilpotent G-orbits is the Bala–Carter theory. This says that the nilpotent orbits correspond to G-conjugacy classes of distinguished parabolic subgroups of Levi subgroups of G. It was proved for $\operatorname{char} k$ zero or "sufficiently large" by P. Bala and R.W. Carter in [9]. K. Pommerening extended the classification to $\operatorname{char} k$ good for G, see [51] and [52]. Recently, A. Premet gave a more conceptual proof of the Bala–Carter theory, see [54].

The adjoint orbits of a parabolic subgroup P of G in the Lie algebra of its unipotent radical, which we denote by $\mathfrak{p}_u$, are also of interest. One of the first papers about these orbits, considered the case where $\mathfrak{p}_u$ is abelian; R. Richardson, G. Röhrle and R. Steinberg showed that in this case P acts on $\mathfrak{p}_u$ with finitely many orbits, see [58]. In [60] this result was generalized by Röhrle, where he proves that, for P arbitrary, P acts on an abelian P-submodule of $\mathfrak{p}_u$ with finitely many orbits.

There has been recent interest in the question of when P acts on $\mathfrak{p}_u$ with finitely many orbits. In [43] V.V. Kashin classified all instances when a Borel subgroup B of G acts on the Lie algebra of its unipotent radical with finitely many orbits. This classification was extended to minimal parabolic subgroups by V. Popov and G. Röhrle in [53]. Then in [33] and [34] L. Hille and G. Röhrle classified all instances when P acts on $\mathfrak{p}_u$ with finitely many orbits, for G of classical type. By computer calculations U. Jürgens and G. Röhrle extended this classification to the exceptional groups in [42].

The question of when P acts on terms $\mathfrak{p}_u^{(l)}$ of the descending central series of $\mathfrak{p}_u$ with finitely many orbits has also been considered. There is a classification of all such instances for G of classical type due to T. Brüstle, L. Hille and G. Röhrle, see [14] and [15]. This classification was extended to G of type F_4 and E_6 by G. Röhrle and the author in [28]. The case G of type G_2 is straightforward and follows from work of V. Popov and G. Röhrle in [53].

Part of Richardson's dense orbit theorem ([57]) implies that P always acts on $\mathfrak{p}_u$ with a dense orbit. There has also been interest in the question of when $\mathfrak{p}_u^{(l)}$ is a prehomogeneous space for P, for $l \geq 1$. This question was first considered by L. Hille and G. Röhrle in [35]. For certain parabolic subgroups (including Borel subgroups) of $\mathrm{GL}_n(k)$ they showed this is true for all $l \geq 0$. However, it is possible to find parabolic subgroups P of $\mathrm{GL}_n(k)$ such that P fails to admit a dense orbit in $\mathfrak{p}_u^{(1)}$ (see [31] or [35]). Hille considered the case $G = \mathrm{GL}_n(k)$ further in [32].

There has been particular interest in the special case when $P = B$ is a Borel subgroup of G. In [16] H. Bürgstein and W.H. Hesselink considered the adjoint orbits of B in $\mathfrak{u} = \mathfrak{b}_u$; they were motivated by the problem of describing the component configuration of the variety $\mathcal{B}_X = \{B' \in \mathcal{B} : X \in \mathrm{Lie}\, B'\}$, where $\mathcal{B}$ denotes the variety of Borel subgroups of G and $X \in \mathfrak{g}$ is nilpotent. This variety seems important for the representation theory of the Weyl group of G and its associated Hecke algebra, see [45, 6.3].

There has been a lot of interest in the conjugacy classes of the unitriangular group $\mathrm{U}_n(q) = \{(x_{ij}) \in \mathrm{GL}_n(q) : x_{ij} = 0 \text{ for } i > j \text{ and } x_{ii} = 1\}$, $q = p^s$ for some $s \in \mathbb{Z}_{\geq 1}$. Both G. Higman and J. Thompson have been interested in the number $k(\mathrm{U}_n(q))$ of conjugacy classes of $\mathrm{U}_n(q)$. For instance, see the paper of Higman [30] and the preprint of Thompson [71]. In particular, it is conjectured that $k(\mathrm{U}_n(q))$ is a polynomial in q with integer coefficients.

The conjugacy classes of $\mathrm{U}_n(q)$ have also been considered by A. Vera-López and J.M. Arregi, see [72]–[79]. In particular, in [78], they showed that $k(\mathrm{U}_n(q))$ is a polynomial in q with integer coefficients for $n \leq 13$ by computer calculation.

G.R. Robinson also considered the conjugacy classes of $\mathrm{U}_n(q)$ and certain subgroups of $\mathrm{U}_n(q)$ in [59]. The main result in *loc. cit.* implies that the zeta function

$$\zeta_{\mathrm{U}_n}(t) = \exp\left(\sum_{s=1}^{\infty} \frac{k(\mathrm{U}_n(p^s))}{s} t^s\right)$$

(in $\mathbb{C}[[t]]$) is a rational function in t whose numerator and denominator may be assumed to be elements of $1 + t\mathbb{Z}[t]$. This implies that once $k(\mathrm{U}_n(p^s))$ is known for a certain finite number of values of s, it can be calculated for all s.

Further, I.M. Isaacs and D. Karagueuzian considered the conjugacy classes and irreducible complex characters of $\mathrm{U}_n(q)$. In [39] they showed that not all elements of $\mathrm{U}_n(2)$ are conjugate to their inverses, implying that not all characters of $\mathrm{U}_n(2)$ are real valued. They also discussed analogous phenomena for odd primes.

Assume that p is good for G and G is defined and split over the prime field $\mathbb{F}_p$. For a power q of p, we write $G(q)$ for the Chevalley group consisting of $\mathbb{F}_q$-rational points of G. Let $F : G \to G$ be the Frobenius morphism such that $G(q) = G^F = \{g \in G : F(g) = g\}$. Let B be an F-stable Borel subgroup of G and U the unipotent radical of B. Then U is F-stable and $U(q)$ is a Sylow p-subgroup of $G(q)$.

In the special case $G = \mathrm{GL}_n(k)$, we may take B to be the group of upper triangular matrices, then $U = \mathrm{U}_n(k)$. Therefore, the study of the conjugacy classes of $U(q)$ generalizes the study of the conjugacy classes of $\mathrm{U}_n(q)$.

In Chapter 3 of this thesis we show that we have the correspondence

$$F\text{-stable adjoint orbits of } U \longleftrightarrow \text{conjugacy classes of } U(q).$$

Therefore, one can study the conjugacy classes of $U(q)$ through the adjoint orbits of U in $\mathfrak{u}$, and vice-versa.

Consider the commuting variety of $\mathfrak{u}$

$$\mathcal{C}(\mathfrak{u}) = \{(x, y) \in \mathfrak{u} \times \mathfrak{u} : [x, y] = 0\}.$$

The geometry of this variety is closely linked to the adjoint orbits of U in $\mathfrak{u}$ – we choose not to discuss this relationship here. For G of small rank $\mathcal{C}(\mathfrak{u})$ has been studied by A.G. Keeton in his PhD thesis [46]. In [55], A. Premet proved that the commuting variety $\mathcal{C}(\mathcal{N})$ of $\mathcal{N}$ is equidimensional.

There has also been interest in the coadjoint orbits of B in $\mathfrak{u}^*$. For example, C. André has considered the coadjoint orbits of $\mathrm{U}_n(q)$ and their relationship with the complex characters of $\mathrm{U}_n(q)$, see [1]–[7]. It is known that, for $\operatorname{char} k$ "sufficiently large", the irreducible characters of U are in correspondence with the coadjoint orbits of U in $\mathfrak{u}^*$ and there is a method for calculating a character from a given coadjoint orbit, see [47] and [44]. In [23] the author considered the coadjoint action of B on $\mathfrak{u}^*$ and showed that B always acts on $\mathfrak{u}^*$ with a dense orbit. This generalized a result of A. Joseph ([41]) from characteristic zero to arbitrary characteristic.

We now give an outline of the structure of this thesis. In this outline, G is a simple algebraic group defined and split over $\mathbb{F}(q)$, $F : G \to G$ the Frobenius morphism such that $G(q) = G^F$, B a Borel subgroup of G, U the unipotent radical of B and $\mathfrak{u}$ the Lie algebra of U. In Chapter 1 we give a brief introduction to the theory of algebraic groups, then in Chapter 2 we consider Springer isomorphisms and relative Springer isomorphisms. We discuss Springer isomorphisms in §2.1 and then in §2.2 we define and prove existence of relative Springer isomorphisms. In Chapter 3 we study the adjoint orbits of U in $\mathfrak{u}$. In particular, we show that any U-orbit in $\mathfrak{u}$ contains a so-called minimal representative and present an algorithm for calculating all such representatives. Next in Chapter 4 we consider the adjoint orbits of B in $\mathfrak{u}$. In §4.1 and §4.2 we prove analogues of the results in Chapter 3 for the adjoint action of B on $\mathfrak{u}$. We describe an algorithm which determines whether B acts on a B-submodule of $\mathfrak{u}$ with a dense orbit in §4.3, then in §4.4 we give a classification of all instances when B acts on a term of the descending central series of $\mathfrak{u}$ with a dense orbit. In the final chapter we use our results for the adjoint actions of U and B, from Chapters 3 and 4, to consider the conjugacy classes of $U(q)$ and the conjugacy classes of $B(q)$ in $U(q)$. Lastly in §5.3 we generalize a result of G.R. Robinson mentioned above.

Some of the results of this thesis are contained in the four articles [27], [24], [25] and [26]. More specifically, the results of §2.2 are contained in [25] and [26]. Chapter 3 contains results from [25]. In §4.1 and §4.2, we present some further results from [25]. The results in §4.3 are contained in [24] and the results of §4.4 are from [27]. Finally, §5.1 and §5.2 contain further results from [25].

Notation

We make the following conventions in this thesis.

- An algebraic group means a linear algebraic group.
- By a subgroup of an algebraic group we mean a closed subgroup.
- An action of an algebraic group means a morphic action.
- A representation of an algebraic group means a rational representation.

We fix some notation which we use in Chapters 2 to 5.

Let G be a simple algebraic group over the algebraically closed field k. Assume $\operatorname{char} k = p > 0$ is good for G and that G is defined and split over the prime field $\mathbb{F}_p$. We denote the Lie algebra of G by $\mathfrak{g} = \operatorname{Lie} G$; likewise for closed subgroups of G. Lower case Roman letters are used to denote elements of G and upper case Roman letters are used to denote elements of $\mathfrak{g}$. We write $r = \operatorname{rank} G$ for the rank of G and h for the Coxeter number of G. The unipotent variety of G is denoted by $\mathcal{U}$ and the nilpotent variety of $\mathfrak{g}$ is denoted by $\mathcal{N}$.

Let q be a power of p. We denote by $G(q)$ the group of $\mathbb{F}_q$-rational points in G and write F for the Frobenius morphism such that $G^F = G(q)$. By an abuse of notation we also write F for the map induced on $\mathfrak{g}$ by F. Let B be an F-stable Borel subgroup of G and let $T \subseteq B$ be an F-stable maximal torus of G. We write U for the unipotent radical of B and $\mathfrak{u}$ for the Lie algebra of U. Let Ψ be the root system of G with respect to T, Ψ^+ the system of positive roots determined by B, Π the corresponding set of simple roots and $N = |\Psi^+| = \dim U$. For a root $\beta \in \Psi$ we choose a parametrization $u_\beta : k \longrightarrow U_\beta$ of the root subgroup U_β, then $e_\beta = du_\beta(1)$ is a generator for the corresponding root subspace $\mathfrak{g}_\beta$ of $\mathfrak{g}$.

We make the assumptions that $\operatorname{char} k > 0$ and that G is simple for convenience. We note that our results are true for $\operatorname{char} k = 0$ whenever they make sense, i.e. do not involve the Frobenius morphism. Further, our results remain true for reductive G with an appropriate restatement; they can be proved by a reduction to the simple components of G.

Let R be an algebraic group and let V be an R-variety. For $r \in R$ and $v \in V$ we write $r \cdot v$ for the image of v under r, $R \cdot v = \{r \cdot v : r \in R\}$ for the R-orbit of v in V and $C_R(v) = \{r \in R : r \cdot v = v\}$ for the stabilizer of v in R.

Now let V be an R-module. Then V is also a module for $\mathfrak{r} = \operatorname{Lie} R$. For $Y \in \mathfrak{r}$ and $v \in V$, we write $Y \cdot v$ for the image of v under Y, $\mathfrak{r} \cdot v = \{Y \cdot v : Y \in \mathfrak{r}\}$ and $\mathfrak{c}_{\mathfrak{r}}(v) = \{Y \in \mathfrak{r} : Y \cdot v = 0\}$.

Chapter 1
Preliminaries

In this chapter we give a brief introduction to the theory of linear algebraic groups and prove some general results on algebraic groups. We assume the reader is familiar with elementary group theory, algebraic geometry, Lie algebras and root systems; we give [8], [29], [37] and [13] as respective references. As a general reference for the theory of algebraic groups we refer the reader to the books of Borel [11] and Springer [66]. The material in §1.1– 1.6 is standard so we do not include references for the results we state.

We now give two pieces of terminology from algebraic geometry which we use in the sequel. Given an algebraically closed field k, we write $\mathbb{A}^n$ for affine n-space over k and for a variety V over k we write $k[V]$ for its ring of regular functions.

1.1 Linear algebraic groups

Let k be an algebraically closed field. A *linear algebraic group* over k is an affine algebraic variety G over k which is simultaneously an abstract group such that the maps defining the group structure, $\mu : G \times G \to G$ with $\mu(x, y) = xy$ and $\iota : G \to G$ with $\iota(x) = x^{-1}$, are morphisms of algebraic varieties. In the sequel we refer to linear algebraic groups over k simply as algebraic groups.

A *homomorphism* of algebraic groups is a map from one algebraic group to another which is both a morphism of algebraic varieties and a homomorphism of abstract groups. One can easily define the notions of isomorphism, automorphism, etc. In the sequel a homomorphism means a homomorphism of algebraic groups unless otherwise stated. Given two algebraic groups G and H we write $\mathrm{Hom}(G, H)$ for the set of homomorphisms $G \to H$.

A *closed subgroup* of G is a subgroup of G which is closed in the Zariski topology. The algebraic group structure on G induces a structure of an algebraic group on H so that the inclusion $H \to G$ is a homomorphism of algebraic groups. When we talk about subgroups of algebraic groups in the sequel we always mean closed subgroups.

Given algebraic groups G and H, we can form their direct product $G \times H$ – this is an algebraic group.

Let G be an algebraic group. As an affine variety G can be decomposed into its irreducible components. There is a unique irreducible component G^0 of G that contains the identity element 1 called the *identity component* of G. It is a normal subgroup of G with finite index. The cosets of G^0 in G are the other irreducible components of G. Therefore, the irreducible components of G coincide with the connected components of G. So when working with algebraic groups, we may use the words irreducible and connected interchangeably, we choose to use connected.

Perhaps the most important example of an algebraic group is the general linear group $\mathrm{GL}_n(k)$ of invertible $n \times n$ matrices over k. This may be considered as an affine variety by identifying it with the closed subset of k^{n^2+1} defined by the vanishing of $\det(T_{ij})S - 1$, where we write the polynomials in $n^2 + 1$ variables as $k[T_{ij}, S]$ $(1 \leq i, j \leq n)$. In the special case $n = 1$, we have $\mathrm{GL}_1(k) = \mathbb{G}_m$ is the multiplicative group of the field k.

We now give some important subgroups of $\mathrm{GL}_n(k)$. We have the group of upper triangular matrices $\mathrm{B}_n(k) = \{(x_{ij} \in \mathrm{GL}_n(k) : x_{ij} = 0 \text{ if } i > j\}$ which has the group of unitriangular matrices $\mathrm{U}_n(k) = \{(x_{ij} \in \mathrm{GL}_n(k) : x_{ij} = 0 \text{ if } i > j \text{ and } x_{ii} = 1\}$ as a normal subgroup. The field k is an algebraic group under addition, we denote this group by $\mathbb{G}_a$ and have an isomorphism $\mathrm{U}_2(k) \cong \mathbb{G}_a$.

It may seem more natural for linear algebraic groups to be called "affine algebraic groups". The chosen adjective "linear" is justified by the following standard proposition.

Proposition 1.1.1 *A linear algebraic group is isomorphic to a subgroup of* $\mathrm{GL}_n(k)$ *for some* $n \in \mathbb{Z}_{\geq 1}$.

Let G be an algebraic group and V an algebraic variety. We say that G *acts morphically* on V if G acts on V as an abstract group and the map $\nu : G \times V \to V$ with $\nu(g, v) = g \cdot v$ is a morphism of varieties. In the sequel when we consider an action of an algebraic group we always mean a morphic action. A variety on which G acts morphically is called a G-variety. Let V and W be G-varieties. A map $\phi : V \to W$ is a morphism of G-varieties if it is a morphism of algebraic varieties and $\phi(g \cdot v) = g \cdot \phi(v)$ for all $g \in G$ and $v \in V$. We sometimes call a morphism of G-varieties, a G-equivariant morphism. Given $v \in V$ we write $C_G(v) = \{g \in G : g \cdot v = v\}$ for the stabilizer of v in G and $G \cdot v = \{g \cdot v : g \in G\}$ for the G-orbit of v.

Now suppose V is a vector space over k of dimension $n < \infty$. The group $\mathrm{GL}(V)$ can be given the structure of an algebraic group by fixing a basis of V and identifying $\mathrm{GL}(V)$ with $\mathrm{GL}_n(k)$. A homomorphism $\rho : G \to \mathrm{GL}(V)$ is called a *rational representation* of G. In the sequel we refer to rational representations simply as representations. A representation $\rho : G \to \mathrm{GL}(V)$ gives rise to an action of G on V defined by $g \cdot v = \rho(g)v$. The notion of a representation of G is equivalent to that of a G-module. A *G-module* is a finite dimensional vector space V over k on which G acts as linear transformations.

Let G be an algebraic group and H a subgroup of G. The coset space G/H can be given the structure of an algebraic variety so that the natural map $\pi : G \to G/H$ is a surjective morphism of varieties. If H is a normal subgroup of G, then G/H is an affine variety and the structure of G/H as an abstract group gives G/H the structure of an algebraic group.

Let G be an algebraic group, H a subgroup of G and V a G-module. Then V has a natural structure of an H-module. A *G-submodule* of V is a G-stable vector subspace of V. Given a submodule W of V, the quotient space V/W has a natural structure of a G-module. Suppose H is a normal subgroup of G, W is a submodule of V and $h \cdot v - v \in W$ for all $h \in H$ and $v \in V$. Then the action of G on V/W factors through G/H, giving V/W the structure of a G/H-module.

1.2 The Lie algebra of an algebraic group

Let G be an algebraic group. We may associate to G a Lie algebra $\mathfrak{g} = \mathrm{Lie}(G)$; we explain this briefly below.

We recall that a k-derivation of a k-algebra A is a k-linear map $\delta : A \to A$ such that $\delta(ab) = \delta(a)b + a\delta(b)$ and we write $\mathrm{Der}(A)$ for the space of all k-derivations of A. We recall that G acts on $k[G]$ as k-algebra isomorphisms by $(g \cdot f)(x) = f(g^{-1}x)$. We define $\mathfrak{g}$ to be the subspace of $\mathrm{Der}(k[G])$ consisting of k-derivations δ of $k[G]$ such that $g \cdot (\delta(f)) = \delta(g \cdot f)$ for all $g \in G$. The space $\mathrm{Der}(k[G])$ has a natural structure as a Lie algebra and $\mathfrak{g}$ is a Lie subalgebra.

One can show that there is a vector space isomorphism from $\mathfrak{g}$ to $T_1(G)$ (the tangent space of G at the identity), obtained by evaluation at the identity. Therefore, we may identify $\mathfrak{g}$ with $T_1(G)$.

Let $\phi : G \to H$ be a homomorphism of algebraic groups and let $\mathfrak{g}$ and $\mathfrak{h}$ be the Lie algebras of G and H respectively. Then ϕ is a morphism of algebraic varieties so, by identifying $\mathfrak{g}$ and $\mathfrak{h}$ with $T_1(G)$ and $T_1(H)$, we can take the derivative of ϕ at the identity to get a linear map $d\phi_1 : \mathfrak{g} \to \mathfrak{h}$. We write $d\phi = d\phi_1$ and call it the *derivative of ϕ*. The derivative of ϕ is a homomorphism of Lie algebras.

Let G be an algebraic group and let H be a subgroup of G. Then $\mathfrak{h}$ is a Lie subalgebra of $\mathfrak{g}$ and if H is a normal subgroup of G, then $\mathfrak{h}$ is an ideal of $\mathfrak{g}$ and $\mathrm{Lie}(G/H) \cong \mathfrak{g}/\mathfrak{h}$.

We note that the Lie algebra of $\mathrm{GL}_n(k)$ is $\mathfrak{gl}_n(k)$ so if G is a subgroup of $\mathrm{GL}_n(k)$, then

$\mathfrak{g}$ is a Lie subalgebra of $\mathfrak{gl}_n(k)$. Also for a finite dimensional vector space V over k, we may identify $\operatorname{Lie}\mathrm{GL}(V)$ with $\mathfrak{gl}(V)$.

Let $\rho : G \to \mathrm{GL}(V)$ be a representation of G. Then $d\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ is a representation of the Lie algebra $\mathfrak{g}$. In particular, the action of G on V induces an action of $\mathfrak{g}$ on V. Suppose V is a G-module so that it is also a $\mathfrak{g}$-module. For $X \in \mathfrak{g}$ and $v \in V$ we write $X \cdot v$ for the image of v under X, $\mathfrak{c}_{\mathfrak{g}}(v) = \{X \in \mathfrak{g} : X \cdot v = 0\}$ and $\mathfrak{g} \cdot v = \{X \cdot v : X \in \mathfrak{g}\}$.

1.3 The conjugation and adjoint actions

Let G be an algebraic group and let $\mathfrak{g}$ be the Lie algebra of G. We recall that G acts on itself by conjugation; for $x \in G$ we define $\operatorname{Int} x : G \to G$ by $\operatorname{Int} x(y) = xyx^{-1}$ and we write $x \cdot y$ for $\operatorname{Int} x(y)$. The derivative of $\operatorname{Int} y$ is denoted by $\operatorname{Ad} x : \mathfrak{g} \to \mathfrak{g}$. We can define a map $\operatorname{Ad} : G \to \mathrm{GL}(\mathfrak{g})$; this is a representation of G called the *adjoint representation* and we call the associated action of G the *adjoint action*. We note that if G is a subgroup of $\mathrm{GL}_n(k)$ (so $\mathfrak{g}$ is a Lie subalgebra of $\mathfrak{gl}_n(k)$), then the adjoint action of G is given by $\operatorname{Ad} x(Y) = xYx^{-1}$, where the product on the right hand side is matrix multiplication. We can take the derivative of Ad and we get the adjoint representation $\operatorname{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$.

Let M and N be normal subgroups of G and write $\mathfrak{m} = \operatorname{Lie} M$ and $\mathfrak{n} = \operatorname{Lie} N$. The conjugation action of G on itself induces an action of G on G/M. Suppose this action factors through G/N. The adjoint action of G on $\mathfrak{g}$ induces an action of G on $\mathfrak{g}/\mathfrak{m}$ and this action factors through G/N. Further, the action of G/N on $\mathfrak{g}/\mathfrak{m}$ induces an action of $\mathfrak{g}/\mathfrak{n}$ on $\mathfrak{g}/\mathfrak{m}$ – this action is the one induced by the adjoint action of $\mathfrak{g}$ on itself. Therefore, objects such as $(G/N) \cdot (X + \mathfrak{m})$, $\mathfrak{c}_{\mathfrak{g}/\mathfrak{n}}(X + \mathfrak{m})$ (for $X \in \mathfrak{g}$) are defined as in §1.1 and §1.2.

Let $x \in G$ and let $\varphi_x : G \to G \cdot x$ be the orbit map in the conjugation action. The map $y \to \varphi_x(y)y^{-1} = (x, y) = xyx^{-1}y^{-1}$ from G to itself has derivative given by $\operatorname{Ad} x - \mathrm{id} : \mathfrak{g} \to \mathfrak{g}$. Therefore, its kernel is $\mathfrak{c}_{\mathfrak{g}}(x) = \{Y \in \mathfrak{g} : x \cdot Y = Y\}$. Since translation is an isomorphism, we conclude that $\ker(d\varphi_x)_1 = \mathfrak{c}_{\mathfrak{g}}(x)$.

Let $X \in \mathfrak{g}$ and let $\varphi_X : G \to G \cdot X$ be the orbit map in the adjoint action. The derivative of φ_X at the identity is given by $(d\varphi_X)_1(Y) = [Y, X]$. Therefore, $\ker(d\varphi_X)_1 = \mathfrak{c}_{\mathfrak{g}}(X)$.

Now let $\mathfrak{m}$ be a G-submodule of $\mathfrak{g}$ and consider the action of G on $\mathfrak{g}/\mathfrak{m}$ induced by the adjoint action of G on $\mathfrak{g}$. Let $\pi : \mathfrak{g} \to \mathfrak{g}/\mathfrak{m}$ be the natural map. For any $Y \in \mathfrak{g}$ we can identify $T_Y(\mathfrak{g}) = \mathfrak{g}$ and $T_{Y+\mathfrak{m}}(\mathfrak{g}/\mathfrak{m}) = \mathfrak{g}/\mathfrak{m}$. Then we have $d\pi_Y = \pi$. Let $X \in \mathfrak{g}$ and let $\varphi_{X+\mathfrak{m}} : G \to G \cdot (X + \mathfrak{m})$ be the orbit map of $X + \mathfrak{m} \in \mathfrak{g}/\mathfrak{m}$. We have the factorization $\varphi_{X+\mathfrak{m}} = \pi\varphi_X$, which gives rise to the factorization $(d\varphi_{X+\mathfrak{m}})_1 = \pi(d\varphi_X)_1$. Therefore, we have $(d\varphi_{X+\mathfrak{m}})_1(Y) = [Y, X] + \mathfrak{m}$ and $\ker(d\varphi_{X+\mathfrak{m}})_1 = \mathfrak{c}_{\mathfrak{g}}(X + \mathfrak{m})$.

1.4 More on algebraic groups

Let V be a finite dimensional vector space over k and let $f : V \to V$ be an endomorphism of V. We recall that f is said to be *semisimple* if V has a basis of eigenvectors of f. We say f is *nilpotent* if $f^m = 0$ for some $m \in \mathbb{Z}_{\geq 1}$ and we say f is *unipotent* if $f - 1$ is nilpotent.

Let G be an algebraic group. An element $x \in G$ is said to be *semisimple* if $\rho(x)$ is semisimple for any representation $\rho : G \to \mathrm{GL}(V)$. Similarly, x is said to be *unipotent* if $\rho(x)$ is unipotent for any representation $\rho : G \to \mathrm{GL}(V)$.

An element X of the Lie algebra of G is said to be *semisimple* if $d\rho(X)$ is semisimple for any representation $\rho : G \to \mathrm{GL}(V)$. Similarly, X is said to be *nilpotent* if $d\rho(X)$ is nilpotent for any representation $\rho : G \to \mathrm{GL}(V)$.

We say that G is a *torus* if it is isomorphic to a direct product of copies of $\mathbb{G}_m$. If $G \cong \mathbb{G}_m \times \cdots \times \mathbb{G}_m = \mathbb{G}_m^r$ is a torus, then the *rank* of G is defined to be r. We note that all elements of a torus are semisimple. Let V be a module for a torus G. Then we have a decomposition $V = \bigoplus_{\gamma \in \Gamma} V_\gamma$, where Γ is a finite subset of $\mathrm{Hom}(G, \mathbb{G}_m)$ whose elements are called the *weights* of G on V and $V_\gamma = \{v \in V : g \cdot v = \gamma(g)v \text{ for all } g \in G\}$.

Now let G be any algebraic group. A *maximal torus* of G is a subgroup of G which is maximal subject to being a torus. All maximal tori of G are conjugate in G. The *rank* of G, denoted by $\operatorname{rank} G$, is the rank of a maximal torus of G.

Given subgroups H and K of G the commutator subgroup (H, K) is the subgroup of G generated by commutators $(h, k) = hkh^{-1}k^{-1}$, where $h \in H$ and $k \in K$. The derived series of G is defined as usual and we say G is *solvable* if the derived series terminates. The descending central series of G is defined by

$$G^{(0)} = G \text{ and } G^{(i+1)} = (G^{(i)}, G) \text{ for } i \geq 0$$

and we say G is *nilpotent* if $G^{(m)} = \{1\}$ for some $m \in \mathbb{Z}_{\geq 1}$.

Let $\mathfrak{g}$ be the Lie algebra of G. The descending central series of $\mathfrak{g}$ is defined by

$$\mathfrak{g}^{(0)} = \mathfrak{g} \text{ and } \mathfrak{g}^{(i+1)} = [\mathfrak{g}^{(i)}, \mathfrak{g}] \text{ for } i \geq 0$$

and we say $\mathfrak{g}$ is *nilpotent* if $\mathfrak{g}^{(m)} = \{0\}$ for some $m \in \mathbb{Z}_{\geq 1}$. We note that if G is nilpotent, then $\mathfrak{g}$ is nilpotent.

A *Borel subgroup* of G is a maximal connected solvable subgroup of G. All Borel subgroups of G are conjugate in G. A *parabolic subgroup* of G is a subgroup which contains a Borel subgroup.

We say that G is *unipotent* if every element of G is unipotent. It is known that if G is unipotent, then G is nilpotent. The *unipotent radical* $R_u(G)$ of G is the maximal normal connected unipotent subgroup of G. We say that G is *reductive* if $R_u(G) = \{1\}$. We note that $G/R_u(G)$ is reductive for any G.

We say that G is *simple* if it has no non-trivial proper connected normal subgroups.

1.5 The classification of simple algebraic groups

In this section, we give a brief outline of the classification of the simple algebraic groups. They are classified by their root system and fundamental group; we discuss this below.

Let G be a simple algebraic group and T a maximal torus of G. The set $\Xi = \mathrm{Hom}(T, \mathbb{G}_m)$ has the structure of an abelian group, where addition is defined by $(\chi + \chi')(t) = \chi(t)\chi'(t)$; it is called the *character group* of T and is isomorphic to $\mathbb{Z}^r$, where r is the rank of G. We may therefore consider the real vector space $E = \Xi \otimes_{\mathbb{Z}} \mathbb{R}$.

The adjoint action of G on its Lie algebra $\mathfrak{g}$ induces an action of T on $\mathfrak{g}$. Since T is a torus we get a decomposition $\mathfrak{g} = \mathfrak{c}_{\mathfrak{g}}(T) \oplus \bigoplus_{\beta \in \Psi} \mathfrak{g}_\beta$, where $\mathfrak{c}_{\mathfrak{g}}(T) = \{X \in \mathfrak{g} : t \cdot X = X \text{ for all } t \in T\}$, $\Psi \subseteq \Xi$ and $\mathfrak{g}_\beta = \{X \in \mathfrak{g} : t \cdot X = \beta(t)X \text{ for all } t \in T\}$. It turns out that $\mathfrak{c}_{\mathfrak{g}}(T) = \mathfrak{t} = \mathrm{Lie}\, T$ and that $\Psi \subseteq \Xi$ is a root system, which we call the *root system of* G with respect to T. We note that Ψ depends on the choice of T; however, this dependence does not effect the isomorphism class of Ψ because all maximal tori of G are conjugate in G.

We denote the weight lattice of Ψ by Λ and the root lattice of Ψ by Λ_r. We have the inclusions $\Lambda_r \subseteq \Xi \subseteq \Lambda$ and Λ/Λ_r is a finite abelian group. The *fundamental group* of G is defined to be $\pi(G) = \Lambda/\Xi$. There are only finitely many possibilities for the fundamental group of G.

Now we may state the classification of simple algebraic groups.

Theorem 1.5.1 *Let G and G' be simple algebraic groups having isomorphic root systems and isomorphic fundamental groups. Then G and G' are isomorphic, unless the root system is of type D_r and the fundamental group has order 2, in which case there may be two isomorphism types.*

Further, given an irreducible root system Ψ and a quotient π of Λ/Λ_r, there exists a simple algebraic group G with root system Ψ and fundamental group π.

Let G be a simple algebraic group, T a maximal torus of G and Ψ the root system of G with respect to T. Let $B \supseteq T$ be a Borel subgroup of G. The Lie algebra $\mathfrak{b}$ of B is a Borel subalgebra of $\mathfrak{g}$ and we have $\mathfrak{b} = \mathfrak{t} \oplus \bigoplus_{\beta \in \Psi^+} \mathfrak{g}_\beta$, where $\Psi^+ \subseteq \Psi$ is a system of positive roots of Ψ. Let Π be the corresponding set of simple roots.

We recall the *height* of a root $\beta = \sum_{\alpha \in \Pi} b_\alpha \alpha \in \Psi^+$ is given by $\mathrm{ht}(\beta) = \sum_{\alpha \in \Pi} b_\alpha$. The standard (strict) partial order $\prec$ on Ψ^+ is defined by: $\alpha \prec \beta$ if $\beta - \alpha$ is a sum of positive roots. Write $\varrho = \sum_{\alpha \in \Pi} c_\alpha \alpha$ for the highest root of Ψ. Then we say that $p = \operatorname{char} k > 0$ is *bad* for G if p divides c_α for some $\alpha \in \Pi$. We say that p is *good* for G if it is not bad for G. The *Coxeter number* of G is $h = \mathrm{ht}(\varrho) + 1$.

Let G be a simple algebraic group, the isomorphism class of its root system is called the *type* of G. Therefore, the simple algebraic groups G and G' are said to be of the *same type* if they have isomorphic root systems. An *isogeny* $\sigma : G \to G'$ is an epimorphism with finite kernel. If $\sigma : G \to G'$ is an isogeny, then G and G' have the same type and $\ker \sigma$ is contained in the centre $Z(G)$ of G.

If G is a simple algebraic group and the fundamental group of G is trivial, then G is said to be *simply connected*. If G and G' are simple algebraic groups of the same type with G' simply connected, then there is an isogeny $\sigma : G' \to G$ called the *covering map* of G'. If the fundamental group of G is Λ/Λ_r, then G is called *adjoint*.

We now describe the various possibilities for a simple algebraic group G, when p is zero or good for G. If G is of type A, B, C or D, then we say G is *classical* and if G is of type E, F or G, then we say G is *exceptional*. We note that if G is not of type A and G' is a simply connected simple algebraic group of the same type as G, then the covering map $G' \to G$ is separable, so that $\mathfrak{g}' \cong \mathfrak{g}$.

For G of type A_r, the fundamental group is Z_{r+1} – the cyclic group of order $r+1$. The simply connected group is the special linear group $\mathrm{SL}_{r+1}(k)$ and the adjoint group is $\mathrm{PGL}_{r+1}(k)$. There may be other possibilities for G which are neither simply connected nor adjoint. We recall that the Lie algebra of $\mathrm{SL}_n(k)$ is given by $\mathfrak{sl}_n(k) = \{X \in \mathfrak{gl}_n(k) : \operatorname{tr} X = 0\}$, where $\operatorname{tr} X$ denotes the trace of X. Let G be a simple group of type A_r. We note that if p does not divide $r+1$, then the covering map $\mathrm{SL}_{r+1}(k) \to G$ is separable so that $\mathfrak{g} = \mathfrak{sl}_n(k)$. If p divides $r+1$, then the covering map may not be separable and $\mathfrak{g}$ may be different from $\mathfrak{sl}_n(k)$.

If G is of type B_r, then p is good unless $p = 2$ and the fundamental group of G is Z_2. If G is simply connected, then it is the spin group $\mathrm{Spin}_{2r+1}(k)$ and if G is adjoint, then it is the special orthogonal group $\mathrm{SO}_{2r+1}(k)$. For $n \in \mathbb{Z}_{\geq 1}$ we consider the orthogonal group $\mathrm{O}_n(k) = \{x \in \mathrm{GL}_n(k) : xJx^t = J\}$, where x^t denotes the transpose of x, and J is the matrix whose (i,j)th entry is 1 if $i + j = n + 1$ and 0 otherwise. We consider $\mathrm{SO}_n(k) = \mathrm{O}_n(k) \cap \mathrm{SL}_n(k)$. The Lie algebra of $\mathrm{SO}_n(k)$ is given by $\mathfrak{so}_n(k) = \{X \in \mathfrak{gl}_n(k) : xJ = -Jx^t\}$.

When G is of type C_r, $p = 2$ is the only bad prime for G and the fundamental group of G is Z_2. The symplectic group $\mathrm{Sp}_{2r}(k)$ is the simply connected possibility for G and the projective symplectic group $\mathrm{PSp}_{2r}(k)$ is the adjoint possibility for G. For $n \in \mathbb{Z}_{\geq 1}$ we consider the symplectic group $\mathrm{Sp}_{2n}(k) = \{x \in \mathrm{GL}_{2n}(k) : xJx^t = J\}$, where J is the matrix whose (i,j)th entry is 1 if $i+j = 2n+1$ and $i \leq n$, -1 if $i+j = 2n+1$ and $i \geq n+1$, and 0 otherwise. The Lie algebra of $\mathrm{Sp}_{2n}(k)$ is given by $\mathfrak{sp}_{2n}(k) = \{X \in \mathfrak{gl}_{2n}(k) : xJ = -Jx^t\}$.

If G is of type D_r, then p is good for G unless $p = 2$. The fundamental group of G is of order 4; if r is odd, then it is isomorphic to Z_4 and if r is even, then it is isomorphic to $Z_2 \times Z_2$. If r is odd there are three possibilities for G. If G is simply connected, then it is the spin group $\mathrm{Spin}_{2r}(k)$, if G is neither simply connected nor adjoint, then it is the special orthogonal group $\mathrm{SO}_{2r}(k)$ and if G is adjoint, then it is the projective special orthogonal group $\mathrm{PSO}_{2r}(k)$. If r is even the there is one further possibility for G which is neither simply connected nor adjoint – namely the half spin group $\mathrm{HSpin}_{2r}(k)$.

Now consider G of exceptional type. If G is of type E_6, then 2 and 3 are the bad primes for G and the fundamental group of G is Z_3 so G is either simply connected or adjoint. If G is of type E_7, then 2 and 3 are the bad primes for G and the fundamental group of G is Z_2 so G is either simply connected or adjoint. If G is of type E_8, then 2, 3 and 5 are the bad primes for G and the fundamental group of G is trivial so there is only one possibility for G. If G is of type F_4 or G_2, then 2 and 3 are the bad primes for G and the fundamental group of G is trivial so there is only one possibility for G.

1.6 More on simple algebraic groups

Let G be a simple algebraic group, let T be a maximal torus of G and let Ψ be the root system of G with respect to T.

Let H be a subgroup of G. We say H is (T-)*regular* if it is normalized by T. In this case the adjoint action of G on $\mathfrak{g}$ induces an action of T on $\mathfrak{h}$. Then we have $\mathfrak{h} = (\mathfrak{t} \cap \mathfrak{h}) \oplus \bigoplus_{\beta \in \Psi(H)} \mathfrak{g}_\beta$, where $\Psi(H) \subseteq \Psi$. We call $\Psi(H)$ the *set of roots of* H with respect to T. Similarly, a subalgebra of $\mathfrak{g}$ is called *regular* if it is normalized by T. If $\mathfrak{h}$ is a regular subalgebra of $\mathfrak{g}$, then we have $\mathfrak{h} = (\mathfrak{t} \cap \mathfrak{h}) \oplus \bigoplus_{\beta \in \Psi(\mathfrak{h})} \mathfrak{g}_\beta$, where $\Psi(\mathfrak{h}) \subseteq \Psi$ is called *the set of roots of* $\mathfrak{h}$ with respect to T. Clearly, if H is a regular subgroup of G, then $\mathfrak{h} = \operatorname{Lie} H$ is a regular subalgebra of $\mathfrak{g}$ and $\Psi(H) = \Psi(\mathfrak{h})$. In fact, if $\operatorname{char} k$ is zero or good for G, then any regular subalgebra of $\mathfrak{g}$ is the Lie algebra of a regular subgroup of G.

Let $B \supseteq T$ be a Borel subgroup of G and write U for the unipotent radical of B. We have that $\Psi^+ = \Psi(B) = \Psi(U)$ is a set of positive roots of Ψ. Also we have a semidirect product decomposition $B = UT$.

For $\beta \in \Psi$ we have the *root subgroup* U_β of G; this is a one dimensional subgroup of G with an isomorphism $u_\beta : \mathbb{G}_a \to U_\beta$ such that $tu_\beta(s)t^{-1} = u_\beta(\beta(t)s)$ for all $t \in T$. We recall the Chevalley commutator relations in G. For $\beta \neq \pm\gamma$:

$$(u_\beta(s), u_\gamma(t)) = \prod_{i\beta+j\gamma\in\Psi:i,j>0} u_\delta(c_{\beta,\gamma,i,j}s^i t^j) \tag{1.6.1}$$

where $c_{\beta,\gamma,i,j} \in k$. For each $\beta \in \Psi$ we choose a generator e_β for the root subspace $\mathfrak{g}_\beta$. We recall the following relations for the adjoint action. For $\beta \neq \pm\gamma$:

$$u_\beta(t) \cdot e_\gamma = e_\gamma + \sum_{\gamma+i\beta:i>0} b_{\beta,\gamma,i} t^i e_{\gamma+i\beta} \tag{1.6.2}$$

where $b_{\beta,\gamma,i} \in k$. Finally, we recall the Chevalley commutator relations in $\mathfrak{g}$. For $\beta \neq \pm\gamma$, if $\beta + \gamma \in \Psi$, then

$$[e_\beta, e_\gamma] = a_{\beta,\gamma} e_{\beta+\gamma}, \tag{1.6.3}$$

where $a_{\beta,\gamma} \in k$ and if $\beta + \gamma \notin \Psi$, then $[e_\beta, e_\gamma] = 0$. Further, if $\gamma - a\beta, \dots, \gamma + b\beta$ is the β string through γ, then we can choose the e_β so that $a_{\beta,\gamma} = \pm(a+1)$.

The Chevalley commutator relations imply that if $\operatorname{char} k$ is zero or good for G, then

$$U^{(l)} = \prod_{\mathrm{ht}(\beta)>l} U_\beta,$$

so that, for $l < m$, we may identify $U^{(l)}/U^{(m)}$ as a variety with

$$\prod_{l<\mathrm{ht}(\beta)\leq m} U_\beta.$$

The terms of the descending central series of $\mathfrak{u}$ have an analogous description.

Now let G be a connected reductive algebraic group. Then G can be decomposed as a commuting product $G = Z(G)G_1 \cdots G_s$ such that each G_i is simple and $G_i \cap \prod_{j\neq i} G_j$ is finite for each i, and $Z(G)$ is the centre of G. The G_i are the minimal non-trivial connected normal subgroups of (G, G) so the above decomposition of G is unique and we call the G_i the *simple components of* G. Given a maximal torus T of G we may form the root system Ψ of G as in the case where G is simple. The irreducible components Ψ_i of Ψ are the root systems of G_i with respect to $T \cap G_i$.

In the sequel we consider a simple algebraic group G. We note here that all our results could be given an appropriate restatement with G reductive; they can be proved by a reduction to the simple components.

Let P be a parabolic subgroup of G containing the Borel subgroup B of G. Let Ψ^+ be the system of positive roots of Ψ determined by B and Π the corresponding set of simple roots. We write P_u for the unipotent radical of P. Let $J = \{\alpha \in \Pi : -\alpha \in \Psi(P)\}$ and let $\Psi_J = \mathbb{Z}J \cap \Psi$. Then Ψ_J is the root system of the reductive group P/P_u. In particular, the rank of each of the simple components of P/P_u is less than $\operatorname{rank} G$.

1.7 Some general results on actions of algebraic groups

In this section we give some general results that we shall require later in the thesis.

Let G be an algebraic group G, suppose G acts on the variety V and let $v \in V$. The following formula is a consequence of [11, Thm. AG.10.1].

$$\dim G \cdot v + \dim C_G(v) = \dim G. \tag{1.7.1}$$

The proposition below follows easily from [11, Prop. 6.7].

Proposition 1.7.1 *Let $v \in V$ and let $\varphi_v : G \to G \cdot v$ be the orbit map. The following are equivalent:*

(i) *φ_v is separable, i.e. $(d\varphi_v)_1 : \mathfrak{g} \to T_v(G \cdot v)$ is surjective.*

(ii) *The kernel of $(d\varphi_v)_1$ is contained the Lie algebra of $C_G(v)$.*

Further, the latter condition holds if and only if $\dim \ker(d\varphi_v)_1 = \dim C_G(v)$.

Proof: The equivalence follows immediately from [11, Prop. 6.7]. The final statement in the proposition is true, because the kernel of $(d\varphi_v)_1$ always contains $\operatorname{Lie} C_G(v)$. □

Now we apply Proposition 1.7.1 to the action of G on itself by conjugation. Let $x \in G$, and let $\varphi_x : G \to G \cdot x$ be the orbit map. We recall from §1.3 that we have $\ker(d\varphi_x)_1 = \mathfrak{c}_{\mathfrak{g}}(x)$.

Proposition 1.7.2 *Let $x \in G$. The following are equivalent:*

(i) *φ_x is separable.*

(ii) $\mathfrak{c}_{\mathfrak{g}}(x) = \operatorname{Lie} C_G(x)$.

Further, the latter condition holds if and only if $\dim \mathfrak{c}_{\mathfrak{g}}(x) = \dim C_G(x)$.

Next we apply Proposition 1.7.1 to the action of G on $\mathfrak{g}/\mathfrak{m}$, where $\mathfrak{m}$ is a G-submodule of $\mathfrak{g}$. Let $X \in \mathfrak{g}$, and let $\varphi_{X+\mathfrak{m}} : G \to G \cdot (X + \mathfrak{m})$ be the orbit map. We recall from §1.3 that we have $(d\varphi_X)_1(\mathfrak{g}) = [\mathfrak{g}, X] + \mathfrak{m}$ and $\ker(d\varphi_x)_1 = \mathfrak{c}_{\mathfrak{g}}(X + \mathfrak{m})$. Therefore, we have

Proposition 1.7.3 *Let $\mathfrak{m}$ be a G-submodule of $\mathfrak{g}$ and let $X \in \mathfrak{g}$. The following are equivalent:*

(i) $\varphi_{X+\mathfrak{m}}$ *is separable, i.e.* $[\mathfrak{g}, X] + \mathfrak{m} = T_X(G \cdot (X + \mathfrak{m}))$.

(ii) $\mathfrak{c}_{\mathfrak{g}}(X + \mathfrak{m}) = \operatorname{Lie} C_G(X + \mathfrak{m})$.

Further, the latter condition holds if and only if $\dim \mathfrak{c}_{\mathfrak{g}}(X + \mathfrak{m}) = \dim C_G(X + \mathfrak{m})$.

The following lemma about a module for a torus is easy to prove.

Lemma 1.7.4 *Suppose G is a torus and let V be a module for G. Let $\lambda_1, \ldots, \lambda_l$ be linearly independent weights of G on V. Let $v_1, \ldots, v_l$ be eigenvectors of G with weights $\lambda_1, \ldots, \lambda_l$ respectively and let $x = v_1 + \cdots + v_l$. Then $G \cdot x = \{t_1 v_1 + \cdots + t_l v_l : t_1, \ldots, t_l \in k^\times\}$. In particular,* $\dim G \cdot x = l$.

Let G be an algebraic group and V a variety on which G acts. The subvarieties V_i ($i \in \mathbb{Z}_{\geq 0}$) of V are defined by $V_i = \{v \in V : \dim G \cdot v = i\}$. The irreducible components of the V_i are called the *sheets* of G on V. There are finitely many sheets of G on V and if G acts on V with finitely many orbits, then the sheets coincide with the orbits. The reader is referred to [12] for more information on sheets. We can prove the following rigidity result about the sheets of G on V. This result generalizes the lemma in [62].

Proposition 1.7.5 *Let G be a connected algebraic group and let V and W be G-varieties. Let Z be an irreducible algebraic variety and $\Phi : Z \times V \to W$ a morphism such that for every $z \in Z$, the map $v \mapsto \Phi(z, v)$ is an isomorphism of G-varieties. Then for every sheet S of V the image $\Phi(z, S)$ is independent of $z \in Z$.*

Proof: It is clear that for every $z \in Z$ the isomorphism $\Phi_z : v \to \Phi(z, v)$ maps V_i to W_i. Therefore, we may assume that $V = V_i$ and $W = W_i$. Moreover, the irreducibility of Z implies that the Φ_zs map a given irreducible component of V into the same irreducible component of W. Therefore, we may assume that V and W are irreducible. The result now follows. □

1.8 Algebraic groups over finite fields

In this section we assume $\operatorname{char} k = p > 0$ and recall some results about algebraic groups defined over finite fields. We refer the reader to [19, §3] as a general reference for algebraic groups defined over finite fields and to [11, 18.6 and 18.7] for information about split groups.

Let G be an algebraic group over k and assume that G is defined and split over the finite field of p elements $\mathbb{F}_p$. We recall that G being split over $\mathbb{F}_p$ means that there exists a maximal torus T of G defined over $\mathbb{F}_p$ and such that isomorphism $T \cong \mathbb{G}_m^r$ ($r = \operatorname{rank} G$) is defined over $\mathbb{F}_p$. Let q be a power of p and denote by $G(q)$ the finite group consisting of $\mathbb{F}_q$-rational points of G. The groups constructed by Chevalley in [18], known as *Chevalley groups* are of this form; for this reason $G(q)$ is also called a Chevalley group. We write F for the Frobenius morphism such that $G(q) = G^F = \{g \in G : F(g) = g\}$. The Frobenius morphism induces a map on $\mathfrak{g}$, which by an abuse of notation we also denote by F.

By Proposition 1.1.1 we may assume G is a closed subgroup of $\mathrm{GL}_n(k)$. Then we may further assume that F is given by $F(x_{ij}) = (x_{ij}^q)$ so that $G(q)$ consists of the matrices in G with entries in $\mathbb{F}_q$.

We recall that a subvariety S of G or $\mathfrak{g}$ is F-stable if and only if it is defined over $\mathbb{F}_q$, [19, Prop. 3.3]. If S is F-stable we write $S^F = \{s \in S : F(s) = s\}$ this is equal to the $\mathbb{F}_q$-rational points of S, which we denote by $S(q)$.

Let B be an F-stable Borel subgroup of G – such B exists by [19, 3.15]. Then the unipotent radical U of B and its Lie algebra $\mathfrak{u}$ are F-stable and $U(q)$ is a Sylow p-subgroup of $G(q)$.

Let $T \subseteq B$ be an F-stable maximal torus of G and write Ψ for the root system of G with respect to T. Since T is split (as it is contained in an F-stable Borel subgroup), we may choose the isomorphisms $u_\beta : k \to U_\beta$ so that the action of F is given by $F(u_\beta(t)) = u_\beta(t^q)$, for each $\beta \in \Psi$. Then F acts on $\mathfrak{g}_\beta$ and this action is given by $F(ae_\beta) = a^q e_\beta$.

Let H be an F-stable subgroup of G and M an F-stable normal subgroup of H. Then F acts on both H/M and $\mathfrak{h}/\mathfrak{m}$ in a natural way. Let $X \in \mathfrak{h}$. We recall that the set $H^1(F, C_H(X+\mathfrak{m}))$ is defined to be the set of equivalence classes of $C_H(X+\mathfrak{m})$ under the relation $\sim$, where $x \sim y$ if there exists $z \in C_H(X+\mathfrak{m})$ such that $x = zyF(z)^{-1}$. The following proposition combines parts of [67, I, 2.7 and 2.8].

Proposition 1.8.1

(i) *The orbits of $H(q)$ in $(H \cdot (X+\mathfrak{m}))^F$ are in correspondence with the elements of the set $H^1(F, C_H(X+\mathfrak{m}))$.*

(ii) *There is a bijection between $H^1(F, C_H(X+\mathfrak{m}))$ and $H^1(F, C_H(X+\mathfrak{m})/C_H(X+\mathfrak{m})^0)$.*

In particular, if $C_H(X+\mathfrak{m})$ is connected, then $(H \cdot (X+\mathfrak{m}))^F$ is a single $H(q)$-orbit.

1.9 The unipotent and nilpotent varieties

Let G be a simple algebraic group with $r = \operatorname{rank} G$ and let $\mathfrak{g}$ be the Lie algebra of G. Assume that $\operatorname{char} k$ is zero or good for G. The *unipotent variety* $\mathcal{U}$ of G is defined to be the variety of all unipotent elements of G and the *nilpotent variety* $\mathcal{N}$ of $\mathfrak{g}$ is defined to be the variety of all nilpotent elements of $\mathfrak{g}$. Both $\mathcal{U}$ and $\mathcal{N}$ are irreducible varieties.

R.W. Richardson proved in [56] that $\mathcal{U}$ splits up into finitely many G-orbits. Since $\mathcal{U}$ is irreducible, it follows from the general theory of algebraic groups that one of the G-orbits is open in $\mathcal{U}$. This open orbit $\mathcal{U}^r$ is called the *regular unipotent orbit* and $x \in \mathcal{U}^r$ is called *regular unipotent*.

Similarly, G acts on $\mathcal{N}$ with finitely many orbits ([56]) and therefore, with an open orbit $\mathcal{N}^r$. We call $\mathcal{N}^r$ the *regular nilpotent orbit* and $X \in \mathcal{N}^r$ is called *regular nilpotent*.

Let B be a Borel subgroup of G with unipotent radical U. We write $\mathfrak{u}$ for the Lie algebra of U. Let Ψ^+ be the system of positive roots determined by B and Π the corresponding set of simple roots.

It follows from the results in [57] that $\mathcal{U}^r \cap U$ is a single B-orbit which is open in U. For $x \in \mathcal{U}^r \cap U$ we have that $\dim C_G(x) = r$ and $\dim C_B(x) = r$. An element $x = \prod_{\beta \in \Psi^+} u_\beta(\lambda_\beta) \in U$ is regular unipotent if and only if $\lambda_\alpha \neq 0$ for all $\alpha \in \Pi$, see [68] or [67, III, 1.13].

We also have that $\mathcal{N}^r \cap \mathfrak{u}$ is a single B-orbit which is open in $\mathfrak{u}$. If $X \in \mathfrak{u}$ is regular nilpotent, then $\dim C_G(X) = \dim C_B(X) = r$. Further, by [70, 3.7] B is the unique Borel subgroup of G with $X \in \mathfrak{b}$. Finally, we note that $X = \sum_{\beta \in \Psi^+} a_\beta e_\beta \in \mathfrak{u}$ is regular nilpotent if and only if $a_\alpha \neq 0$ for all $\alpha \in \Pi$ see [64] or [67, III, 3.5].

1.10 Unipotent normal subgroups of B

Let G be a simple algebraic group, let B be a Borel subgroup of G and $T \subseteq B$ a maximal torus of G. Let U be the unipotent radical of B and $\mathfrak{u}$ its Lie algebra. Write Ψ for the root system of G with respect to T and Ψ^+ for the system of positive roots determined by B. We recall Ψ^+ is partially ordered by $\prec$ as defined in §1.5.

A subset I of Ψ^+ is called an *ideal* if $\alpha \in I$, $\beta \in \Psi^+$ and $\alpha + \beta \in \Psi^+$ implies $\alpha + \beta \in I$. Given an ideal I of Ψ^+ an element $\alpha \in I$ is called a *generator* if it is a minimal element of I with respect to $\prec$. We write $\Gamma(I)$ for the set of generators of I; $\Gamma(I)$ forms an *anti-chain* in Ψ^+, that is $\alpha \not\prec \beta$ for all $\alpha, \beta \in \Gamma(I)$. Further, the map $I \mapsto \Gamma(I)$ is a bijection between the set of all ideals of Ψ^+ and the set of anti-chains in Ψ^+. We refer the reader to [50, §1 and §2] for a more detailed account of ideals, anti-chains, etc.

Let N be a unipotent normal subgroup of B. Then N is determined by the ideal

$\Psi(N)$ of Ψ^+. The set of generators of $\Psi(N)$ is given by $\Gamma(\Psi(N)) = \Psi(N) \setminus \Psi((U, N))$. Conversely, an ideal I of Ψ^+ gives rise to the unipotent normal subgroup $N_I = \prod_{\beta \in I} U_\beta$ of B. Therefore, the sets of unipotent normal subgroups of B, ideals of Ψ^+ and antichains in Ψ^+ are in bijective correspondence.

Any B-submodule of $\mathfrak{u}$ is the Lie algebra of a unipotent normal subgroup of B. Therefore, we have a correspondence between B-submodules of $\mathfrak{u}$, ideals of Ψ^+ and antichains in Ψ^+ given by the maps

$$\mathfrak{n} \mapsto \Psi(\mathfrak{n}) \mapsto \Gamma(\Psi(\mathfrak{n})) = \Psi(\mathfrak{n}) \setminus \Psi([\mathfrak{u}, \mathfrak{n}]).$$

1.11 Calculating $\dim \mathfrak{c}_\mathfrak{u}(X + \mathfrak{m})$

Let G be a simple algebraic group, B a Borel subgroup of G, U the unipotent radical of B and $\mathfrak{u}$ the Lie algebra of U. In this section we discuss a method for calculating the dimension of the centralizer $\mathfrak{c}_\mathfrak{u}(X + \mathfrak{m})$ where $X \in \mathfrak{u}$ and $\mathfrak{m}$ is a B-submodule of $\mathfrak{u}$.

Let $T \subseteq B$ be a maximal torus of G, let Ψ be the root system of G with respect to T and let Ψ^+ be the system of positive roots determined by B. We choose generators e_β of the root spaces $\mathfrak{g}_\beta$ so that if $\beta, \gamma \in \Psi$ with $\beta \neq \pm\gamma$, $\beta + \gamma \in \Psi$ and $\gamma - a\beta, \dots, \gamma + b\beta$ is the β-string through γ, then $[e_\beta, e_\gamma] = \pm(a+1)e_{\beta+\gamma}$ (see the discussion after (1.6.3)). By using these relations we reduce the calculation of $\dim \mathfrak{c}_\mathfrak{u}(X + \mathfrak{m})$ to linear algebra, as explained below.

Let $\mathfrak{m}$ be a B-submodule of $\mathfrak{u}$ and let $X \in \mathfrak{u}$. An arbitrary element $Y \in \mathfrak{u}$ can be written as $Y = \sum_{\beta \in \Psi^+} y_\beta e_\beta$. Write $X + \mathfrak{m} = \sum_{\beta \in \Psi^+ \setminus \Psi(\mathfrak{m})} x_\beta e_\beta + \mathfrak{m}$. Using the Chevalley commutator relations (1.6.3), we may calculate $[Y, X] + \mathfrak{m} = \sum_{\beta \in \Psi^+ \setminus \Psi(\mathfrak{m})} z_\beta(y_\gamma) e_\beta + \mathfrak{m}$, where z_β is linear in the y_γ. Therefore, we see that $\dim \mathfrak{c}_\mathfrak{u}(X + \mathfrak{m})$ is equal to the dimension of the solution space of the system of linear equations $z_\beta = 0$, for $\beta \in \Psi^+ \setminus \Psi(\mathfrak{m})$. Let E be the $(\dim \mathfrak{u} - \dim \mathfrak{m}) \times \dim \mathfrak{u}$ matrix corresponding to this system of equations. Then $\dim \mathfrak{c}_\mathfrak{u}(X + \mathfrak{m})$ is equal to the rank of E; this rank is easily calculated by row reducing E.

Now suppose we have a sequence $\mathfrak{u} = \mathfrak{m}_0 \supseteq \cdots \supseteq \mathfrak{m}_N = \{0\}$ of B-submodules of $\mathfrak{u}$ with $\dim \mathfrak{m}_{i+1} = \dim \mathfrak{m}_i - 1$ and we want to calculate $\dim \mathfrak{c}_\mathfrak{u}(X + \mathfrak{m}_i)$ for each $i = 1, \dots, N$. For each i we can find the matrix $E_i = E$ as above. To reduce the amount of computation one can row reduce each E_i in turn, using the row reduced matrix obtained from E_{i-1} to calculate a row reduced matrix from E_i.

Now suppose $X = \sum_{\beta \in \Delta} e_\beta$ ($\Delta \subseteq \Psi^+$) is a sum of root vectors. Then we can consider $X \in \mathfrak{u}$ for any field k. It is clear from the discussion above that the dimension of $\mathfrak{c}_\mathfrak{u}(X + \mathfrak{m})$ depends only on the characteristic of k and not on the specific field k. We use the notation $\dim_p \mathfrak{c}_\mathfrak{u}(X + \mathfrak{m})$ to denote the dimension of $\mathfrak{c}_\mathfrak{u}(X + \mathfrak{m})$ if $\operatorname{char} k = p$. We now explain how one can try to work out $\dim_p \mathfrak{c}_{\mathfrak{u}}(X+\mathfrak{m})$ for $p>0$ from $\dim_0 \mathfrak{c}_{\mathfrak{u}}(X+\mathfrak{m})$. It is clear that we have $\dim_p \mathfrak{c}_{\mathfrak{u}}(X+\mathfrak{m}) \leq \dim_0 \mathfrak{c}_{\mathfrak{u}}(X+\mathfrak{m})$ and we have equality if we do not "divide" by p when row reducing the matrix E (as above) in characteristic zero. Therefore, by row reducing E in characteristic zero and keeping track of which primes we "divide" by during this reduction, we can deduce $\dim_p \mathfrak{c}_{\mathfrak{u}}(X+\mathfrak{m}) = \dim_0 \mathfrak{c}_{\mathfrak{u}}(X+\mathfrak{m})$ for all but finitely many values of p.

1.12 Semisimple automorphisms

Let G be an algebraic group. In this section, we define what it means for an automorphism of G to be semisimple. We also give some examples which will be important in §4.4.

Let Θ be an automorphism of G. We write θ for the derivative of Θ at the identity. For a Θ-stable subset S of G, we denote the fixed points of Θ in S by $S^\Theta = \{x \in S : \Theta(x) = x\}$. Similarly, for θ-stable $S \subseteq \mathfrak{g}$, we write $S^\theta = \{X \in S : \theta(X) = X\}$.

Let Θ be an automorphism of G. We say Θ is a *semisimple automorphism* if there is an embedding $G \hookrightarrow \mathrm{GL}_n(k)$ (for some n) such that Θ is induced from conjugation by a diagonal matrix in $\mathrm{GL}_n(k)$.

We note that if Θ is a semisimple automorphism of G with finite order $|\Theta|$, then $\operatorname{char} k$ does not divide $|\Theta|$.

In the following paragraph we assume that $\operatorname{char} k \neq 2$ and give three semisimple automorphisms that we shall require in §4.4. We refer the reader to [69, §11, pp. 169] for more details. For the reader's convenience we give explicit descriptions of the derivatives of these automorphisms.

There exists a semisimple automorphism Θ of $\mathrm{GL}_n(k)$ with $\mathrm{GL}_n(k)^\Theta = \mathrm{O}_n(k)$, its derivative θ is given by $\theta(x_{ij}) = (-x_{n+1-j,n+1-i})$. There is a semisimple automorphism Θ of $\mathrm{GL}_{2n}(k)$ such that $\mathrm{GL}_{2n}(k)^\Theta = \mathrm{Sp}_{2n}(k)$, its derivative θ is given by $\theta(x_{ij}) = (\epsilon x_{n+1-j,n+1-i})$ where $\epsilon = (-1)^{\lfloor \frac{|i-j|}{n} \rfloor + 1}$. Further there exists a semisimple automorphism Φ of $\mathrm{O}_{2n}(k)$ such that $\mathrm{O}_{2n}(k)^\Phi = \mathrm{O}_{2n-1}(k)$, its derivative ϕ is given by $\phi(x_{ij}) = (y_{ij})$, where $y_{ij} = x_{in}$ if $j = n+1$, $y_{ij} = x_{i,n+1}$ if $j = n$, $y_{ij} = x_{nj}$ if $i = n+1$, $y_{ij} = x_{n+1,j}$ if $j = n$ and $y_{ij} = x_{ij}$ otherwise.

1.13 Prehomogeneous spaces

Let G be an algebraic group and V a G-module. We say V is a *prehomogeneous space* for G provided G acts on V with a dense orbit.

We now give two results about prehomogeneous spaces. The first is elementary and sometimes used without reference.

Lemma 1.13.1 *Let G be an algebraic group and H a normal subgroup of G. Let V be a G-module and W a G-submodule of V. Suppose $h \cdot v - v \in W$ for all $h \in H, v \in V$ (so that the action of G on V/W factors through G/H). Suppose V is a prehomogeneous space for G. Then V/W is a prehomogeneous space for G/H.*

Proof: If $v \in V$ is a representative of a dense G-orbit in V, then $v + W \in V/W$ is a representative of a dense G-orbit in V/W and thus a representative of a dense (G/H)-orbit in V/W. $\square$

We use the following result in §4.4.

Theorem 1.13.2 *Let G be an algebraic group, Θ a semisimple automorphism of G with finite order and $\mathfrak{n}$ a θ-stable G-submodule of $\mathfrak{g}$. Suppose there exists $X \in \mathfrak{n}^\theta$ such that $G \cdot X$ is dense in $\mathfrak{n}$ and the orbit map $G \to G \cdot X$ is separable. Then $G^\Theta \cdot X$ is dense in $\mathfrak{n}^\theta$ and the orbit map $G^\Theta \to G^\Theta \cdot X$ is separable.*

Proof: It follows from Proposition 1.7.3 that the separability of the orbit map $G \to G \cdot X$ implies that $T_X(G \cdot X) = [\mathfrak{g}, X]$. We prove the following series of inclusions

$$T_X(G^\Theta \cdot X) \subseteq T_X((G \cdot X)^\theta) \subseteq (T_X(G \cdot X))^\theta = [\mathfrak{g}, X]^\theta \subseteq [\mathfrak{g}^\theta, X] \subseteq T_X(G^\Theta \cdot X).$$

The last inclusion is clear. To show $[\mathfrak{g}, X]^\theta \subseteq [\mathfrak{g}^\theta, X]$ we let $[Y, X] \in [\mathfrak{g}, X]^\theta$. One easily checks that if $Z = \frac{1}{|\Theta|} \sum_{i=0}^{|\Theta|-1} \theta^i(Y)$, then $\theta(Z) = Z$ and $[Y, X] = [Z, X] \in [\mathfrak{g}^\theta, X]$. From $T_X(G \cdot X) = [\mathfrak{g}, X]$ it follows immediately that $(T_X(G \cdot X))^\theta = [\mathfrak{g}, X]^\theta$. Since $(G \cdot X)^\theta \subseteq G \cdot X$ we get that $T_X((G \cdot X)^\theta) \subseteq T_X(G \cdot X)$. Therefore, to show $T_X((G \cdot X)^\theta) \subseteq (T_X(G \cdot X))^\theta$ it suffices to show that $T_X((G \cdot X)^\theta)$ is fixed by θ. But $(G \cdot X)^\theta \subseteq \mathfrak{n}^\theta$, so $T_X((G \cdot X)^\theta) \subseteq T_X(\mathfrak{n}^\theta) = \mathfrak{n}^\theta$. Since $\mathfrak{n}^\theta$ is G^Θ-stable, we have that $G^\Theta \cdot X \subseteq (G \cdot X)^\theta$ which implies the first inclusion.

Since $G \cdot X$ is dense in $\mathfrak{n}$ we have $T_X(G \cdot X) = \mathfrak{n}$. The series of inclusions above then implies that $T_X(G^\Theta \cdot X) = \mathfrak{n}^\theta$ and thus that $G^\Theta \cdot X$ is dense in $\mathfrak{n}^\theta$. The series of inclusions also implies that $T_X(G^\Theta \cdot X) = [\mathfrak{g}^\theta, X]$ which by Proposition 1.7.3 implies the orbit map $G^\Theta \to G^\Theta \cdot X$ is separable. $\square$

Let G be an algebraic group, $\mathfrak{g}$ the Lie algebra of G and $\mathfrak{n}$ a G-submodule of $\mathfrak{g}$. Below we give a basic strategy for showing that $\mathfrak{n}$ is a prehomogeneous space for G.

Using (1.7.1), we see that it suffices to show that $\dim C_G(X) = \dim G - \dim \mathfrak{n}$ for some $X \in \mathfrak{n}$. Since $\operatorname{Lie} C_G(X) \subseteq \mathfrak{c}_\mathfrak{g}(X)$, it suffices to show $\dim \mathfrak{c}_\mathfrak{g}(X) = \dim \mathfrak{g} - \dim \mathfrak{n}$ for some $X \in \mathfrak{n}$.

Remark 1.13.3 We make the observation that if we can find such an X, then we have $\dim \mathfrak{c}_{\mathfrak{g}}(X) = \dim C_G(X)$. Then by Proposition 1.7.3, the orbit map $g \mapsto g \cdot X$ from G to $G \cdot X$ is separable.

Choose a faithful representation $\mathfrak{g} \to \mathfrak{gl}_n(k)$ for some n. We choose this representation so that we have natural vector space isomorphisms $\mathfrak{g} \cong k^{\dim \mathfrak{g}}$; so there is some $A \subseteq \{1, \dots, n\} \times \{1, \dots, n\}$ such that the map $(y_{ij}) \to (y_a : a \in A)$ is an isomorphism. Then we consider $\mathfrak{g} \subseteq \mathfrak{gl}_n(k)$. Let $X \in \mathfrak{n}$, to find $\mathfrak{c}_{\mathfrak{g}}(X)$ we need to look at those $Y \in \mathfrak{g}$ for which $[Y, X] = 0$. Let $Y = (y_{ij}) \in \mathfrak{g} \subseteq \mathfrak{gl}_n(k)$ and consider the y_{ij} (for $(i, j) \in A$) as variables. We see that the condition $[Y, X] = 0$ is equivalent to a system of $\dim \mathfrak{n}$ linear equations in the $\dim \mathfrak{g}$ variables y_{ij}. The dimension of their solution space is $\dim \mathfrak{c}_{\mathfrak{g}}(X)$. To prove that G admits a dense orbit in $\mathfrak{n}$, it therefore suffices to find X for which these equations are independent.

Chapter 2
Relative Springer isomorphisms

In this chapter we define and prove the existence of relative Springer isomorphisms; this is done in §2.2. First in §2.1 we discuss Springer isomorphisms. We remind the reader that in this chapter we use the notation given in the introduction.

2.1 Springer isomorphisms

For char $k > 2h-2$ we have a logarithm map from $\mathcal{U}$ to $\mathcal{N}$, i.e. we may identify $\mathcal{U}$ and $\mathcal{N}$ with their images under the respective adjoint representations of G and $\mathfrak{g}$ and $\log : \mathcal{U} \to \mathcal{N}$ can be defined formally by its power series expansion, see for example [49, §5.7]. This logarithm map and its inverse $\exp : \mathcal{N} \to \mathcal{U}$ are inverse G-equivariant isomorphisms of varieties.

For char $k \leq 2h-2$ the situation is not so straightforward. For char $k \geq h$ a "logarithm map" still exists. A statement of this result can be found in [61, Prop. 5.2], the proof is attributed to J.-P. Serre. In [65] T.A. Springer proved that if G is simply connected, then there exists a G-equivariant morphism of varieties $\mathcal{U} \to \mathcal{N}$ which is a homeomorphism on the underlying topological spaces. This has subsequently been strengthened to the following result (see [10, Cor. 9.5.4] or [38, 6.20]).

Theorem 2.1.1 *If G is of type A assume the covering map $\mathrm{SL}_n(k) \to G$ is separable.*

(i) *There exists a G-equivariant isomorphism of varieties $\phi : \mathcal{U} \to \mathcal{N}$.*

(ii) *ϕ can be chosen to commute with F.*

An isomorphism as in Theorem 2.1.1 is called a *Springer isomorphism* and gives a good substitute for the logarithm map for small p.

We now give a brief discussion of how one can prove Springer isomorphisms exist. We note that the proof given by P. Bardsley and R.W. Richardson in [10] uses a different argument. Assume for now that G is not of type A – we note that for Propositions 2.1.2

and 2.1.3, we can drop this assumption. Let $\hat{G}$ be an adjoint group of the same type as G and let $\sigma : G \to \hat{G}$ be the covering map. One can check that σ induces an isomorphism of varieties from the unipotent variety $\mathcal{U}$ of G to the unipotent variety $\hat{\mathcal{U}}$ of $\hat{G}$. Since G is not of type A, σ is separable, so $d\sigma : \mathfrak{g} \to \hat{\mathfrak{g}}$ is an isomorphism of Lie algebras and therefore induces an isomorphism of varieties from the nilpotent variety $\mathcal{N}$ of G to the nilpotent variety $\hat{\mathcal{N}}$ of $\hat{\mathfrak{g}}$. It is therefore easy to see that there exists a G-equivariant isomorphism of varieties $\mathcal{U} \to \mathcal{N}$ if and only if there exists a $\hat{G}$-equivariant isomorphism of varieties $\hat{\mathcal{U}} \to \hat{\mathcal{N}}$. So we may assume that G is adjoint. We now have the following result of Springer from [63].

Proposition 2.1.2 *Assume G is adjoint.*

(i) *Let $x \in U$ be regular unipotent. Then $C_G(x) = C_U(x)$ is connected.*

(ii) *Let $X \in \mathfrak{u}$ be regular nilpotent. Then $C_G(X) = C_U(X)$ is connected.*

One can use this to prove the following, see [63].

Proposition 2.1.3 *Assume G is adjoint. Let $x \in \mathcal{U}$ be regular unipotent. There exists a regular nilpotent element $X \in \operatorname{Lie} C_G(x)$ and for any such X we have that $C_G(x) = C_G(X)$.*

Therefore, given x and X as in Proposition 2.1.3 we may define an isomorphism of varieties. $\phi : G \cdot x \to G \cdot X$. It is known that the codimension of the complement of $G \cdot x$ in $\mathcal{U}$ is 2 see [68]; similarly the codimension of the complement of $G \cdot X$ in $\mathcal{N}$ is 2 ([63] and [68]). It is known that $\mathcal{U}$ is a normal variety, see [67, III, 2.7]. It is also known that, under our assumptions, $\mathcal{N}$ is a normal variety, see [40, 8.5] – this was proved for char 0 by B. Kostant, then extended to most p by F.D. Veldkamp and these restrictions on p were removed by M. Demazure. Therefore, the isomorphism $\phi : G \cdot x \to G \cdot X$ extends to an isomorphism $\phi : \mathcal{U} \to \mathcal{N}$, see for example [40, Corollary 8.3].

For G of type A, if the covering map $\mathrm{SL}_n(k) \to G$ is separable, then we may assume that $G = \mathrm{SL}_n(k)$. One can easily check that the map $y \mapsto y - 1$ is a Springer isomorphism.

Recall that U is the unipotent radical of an F-stable Borel subgroup B of G. Suppose $x \in U$ is regular nilpotent and let ϕ be a Springer isomorphism. By G-equivariance of ϕ we have that $\phi(x)$ is regular nilpotent. Now $C_G(x)^0 \subseteq B$, therefore, by G-equivariance of ϕ, we have that $C_G(\phi(x))^0 \subseteq B$. Therefore, by the discussion at the end of §1.9 we see that $\phi(x) \in \mathfrak{u}$ and thus $B \cdot \phi(x)$ is dense in $\mathfrak{u}$. Thus, we have the following standard corollary of Theorem 2.1.1.

Corollary 2.1.4

(i) *There exists a B-equivariant isomorphism $\phi : U \to \mathfrak{u}$.*

(ii) *ϕ can be taken to commute with F.*

Proof: The above discussion implies that a Springer isomorphism $\phi : \mathcal{U} \to \mathcal{N}$ induces a B-equivariant isomorphism $\phi : U \to \mathfrak{u}$.

We can remove the assumption on G of type A because the covering map $\mathrm{SL}_n(k) \to G$ induces an isomorphism from $\mathrm{U}_n(k)$ onto its image. $\square$

Let $x \in U$ be regular. Then any B-equivariant isomorphism $\phi : U \to \mathfrak{u}$ is determined by $\phi(x)$. One can check that $\phi(x)$ must be a regular nilpotent element of $\operatorname{Lie} C_B(x) = \operatorname{Lie} C_G(x)$. Therefore, we see that ϕ is the restriction of a Springer isomorphism $\phi : \mathcal{U} \to \mathcal{N}$. In light of the above discussion, an isomorphism as in Corollary 2.1.4 is also called a Springer isomorphism.

The proof of the existence of Springer isomorphisms shows that they are not unique. We now discuss a parametrization of Springer isomorphisms due to J.-P. Serre. Given a subvariety V of G (respectively $\mathfrak{g}$) we write V^r for the variety of regular unipotent elements (respectively regular nilpotent elements) in V.

Let $x \in \mathcal{U}^r$ and fix $X \in (\operatorname{Lie} C_G(x))^r$. It is clear from the proof of the existence of Springer isomorphisms that for each $y \in C_U(x)^r$ there is a unique Springer isomorphism $\phi_{y,X} : \mathcal{U} \to \mathfrak{u}$ with $\phi_{y,X}(y) = X$. Moreover, every Springer isomorphism is of the form $\phi_{y,X}$ for some $y \in C_G(x)^r$. Therefore, the Springer isomorphisms are parameterized by $C_G(x)^r$. In [62] J.-P. Serre proved that this parametrization is algebraic in the following sense.

Proposition 2.1.5 *There exists an algebraic morphism $\Phi : C_G(x)^r \times \mathcal{U} \to \mathcal{N}$ such that $\Phi(y, z) = \phi_{y,X}(z)$ for all $y \in C_G(x)^r$ and $z \in \mathcal{U}$.*

Serre then uses a lemma less general than Proposition 1.7.5 to deduce.

Corollary 2.1.6 *The bijection*

$$G\text{-classes of } \mathcal{U} \to G\text{-classes of } \mathcal{N}$$

given by a Springer isomorphism ϕ is independent of the choice of ϕ.

In the two examples below we describe all Springer isomorphisms when G is of classical type.

Example 2.1.7 Consider the case $G = \mathrm{SL}_n(k)$. Let $a = (a_1, \ldots, a_{n-1}) \in k^{n-1}$ with $a_1 \neq 0$ and define a map $\psi : \mathcal{N} \to \mathcal{U}$ by $\psi(Y) = 1 + a_1 Y + \ldots a_{n-1} Y^{n-1}$. One can check that ψ^{-1} is a Springer isomorphism and that any Springer isomorphism is of this form.

Example 2.1.8 Let $G = \{x \in \mathrm{SL}_n(k) : xJx^t = J\}$ be a simple group of type B, C or D as described in §1.5. Let $\tilde{G} = \mathrm{SL}_n(k)$ and let $\tilde{\mathcal{U}}$ and $\tilde{\mathcal{N}}$ denote the unipotent variety of $\tilde{G}$ and nilpotent variety of $\tilde{\mathfrak{g}}$ respectively. We consider which Springer isomorphisms $\tilde{\mathcal{U}} \to \tilde{\mathcal{N}}$ restrict to a Springer isomorphism $\mathcal{U} \to \mathcal{N}$.

Let $\psi : \tilde{\mathcal{N}} \to \tilde{\mathcal{U}}$, defined by $\psi(Y) = 1 + a_1 Y + \ldots a_{n-1} Y^{n-1}$ where $a = (a_1, \ldots, a_{n-1}) \in k^{n-1}$ with $a_1 \neq 0$, (as in the previous example). For ψ to induce a G-equivariant isomorphism $\mathcal{N} \to \mathcal{U}$ we require that:

$$\text{if } YJ = -JY^t, \quad \text{then} \quad \psi(Y)J\psi(Y)^t = J. \tag{2.1.1}$$

Now we see that if $YJ = -JY^t$, then $Y^i J = (-1)^i J (Y^t)^i$ for any i. Therefore, (2.1.1) is equivalent to

$$\left(1 + \sum_{i=1}^{N-1} a_i Y^i\right)\left(1 + \sum_{i=1}^{N-1} (-1)^i a_i Y^i\right) = 1. \tag{2.1.2}$$

We see that the conditions imposed by (2.1.2) allow a free choice for a_i if i is odd and, for i even, determine the value of a_i from the values of a_j for $j < i$.

One can check that if a satisfies (2.1.2), then ψ^{-1} does restrict to a Springer isomorphism $\mathcal{U} \to \mathcal{N}$ and also that all Springer isomorphisms are of this form.

As a concrete example of such ψ we may take the Cayley map which is defined by $\psi(Y) = (1 - Y)(1 + Y)^{-1}$, see [67, III, 3.14].

2.2 Relative Springer isomorphisms

The principal result of this section is

Theorem 2.2.1 *Let $\phi : U \to \mathfrak{u}$ be a Springer isomorphism and let M be a unipotent normal subgroup of B. Then there exists a B-equivariant isomorphism $\tilde{\phi} : U/M \to \mathfrak{u}/\mathfrak{m}$ such that the diagram*

$$\begin{array}{ccc} U & \xrightarrow{\phi} & \mathfrak{u} \\ \big\downarrow{\scriptstyle \pi_M} & & \big\downarrow{\scriptstyle \pi_{\mathfrak{m}}} \\ U/M & \xrightarrow{\tilde{\phi}} & \mathfrak{u}/\mathfrak{m} \end{array}$$

commutes, where π_M, $\pi_{\mathfrak{m}}$ denote the natural maps.

We call a map $\tilde{\phi}$ as in Theorem 2.2.1 a *relative Springer isomorphism*. This terminology is justified by the commutative diagram above. We note that if $\tilde{\phi} : U/M \to \mathfrak{u}/\mathfrak{m}$ is an isomorphism such that the above diagram commutes, then $\tilde{\phi}$ is B-equivariant so we could drop this requirement in the statement. The existence of relative Springer isomorphisms is crucial for Chapters 3 and 4 where we consider the adjoint orbits of U and B in $\mathfrak{u}$.

We now present some results which we require to prove Theorem 2.2.1. Some of our results concern the action of U on itself by conjugation and have natural analogues for the adjoint action of U on $\mathfrak{u}$. We do not state (or prove) these analogous results but do refer to them later in this section. We refer to these results by adding a $'$ after the number – so for example, the analogous result to Proposition 2.2.5 is referred to as Proposition 2.2.5$'$.

We begin with the following lemma.

Lemma 2.2.2 *Let M, N be unipotent normal subgroups of B and suppose the action of U on U/M factors through U/N. Then for $y \in U$, $C_U(yM)$ is connected if and only if $C_{U/N}(yM)$ is connected.*

Proof: Let $\pi_N : U \to U/N$ be the natural map. It is clear that $\pi_N(C_U(yM)) = C_{U/N}(yM)$. Therefore, π_N induces a bijection between the subgroups of $C_U(yM)$ containing N and the subgroups of $C_{U/N}(yM)$. It follows that

$$|C_U(yM) : C_U(yM)^0| = |C_{U/N}(yM) : C_{U/N}(yM)^0|$$

and the result follows. □

We now consider the centralizer in U and B of a regular unipotent element. The following two easy lemmas are used to prove Proposition 2.2.5.

Lemma 2.2.3 *Let $x = \prod_{\alpha\in\Pi} u_\alpha(1) \in U$ and let M be a unipotent normal subgroup of B. Then we have the factorization*

$$C_B(xM) = C_T(xM)C_U(xM).$$

Proof: Let $b \in C_B(xM)$ and write $b = tu$ with $t \in T$ and $u \in U$. The Chevalley commutator relations (1.6.1) imply that

$$u \cdot xM = x \prod_{\mathrm{ht}(\gamma)\geq 2} u_\gamma(\lambda_\gamma)M$$

where $\lambda_\gamma \in k$. Then
$$b \cdot xM = (t \cdot x) \prod_{\mathrm{ht}(\gamma)\geq 2} u_\gamma(\gamma(t)\lambda_\gamma)M.$$
Since $b \in C_B(xM)$, we have $\gamma(t)\lambda_\gamma = 0$ for all $\gamma \in \Psi^+$ with $\mathrm{ht}(\gamma) \geq 2$, which implies $\lambda_\gamma = 0$, so that $u \in C_U(xM)$. □

Lemma 2.2.4 *Assume G is adjoint. Let $x = \prod_{\alpha\in\Pi} u_\alpha(1) \in U$ and let M be a unipotent normal subgroup of B. Then $C_T(xM)$ is connected.*

Proof: We work by induction on $\dim M$. If $\Psi(M) \cap \Pi = \varnothing$, then one can see that $C_T(xM) = C_T(x) = \{1\}$, the latter equality holds, because $x \in U$ is regular unipotent so $C_G(x) \subseteq U$ (by 2.1.2). So suppose $|\Psi(M) \cap \Pi| \geq 1$. Let $N \subseteq M$ be a unipotent normal subgroup of B with codimension 1 in M. If $|\Psi(M) \cap \Pi| = |\Psi(N) \cap \Pi|$, then we see that $C_T(xM) = C_T(xN)$. So suppose $|\Psi(M) \cap \Pi| = |\Psi(N) \cap \Pi| + 1$ and let $\beta \in (\Psi(M) \setminus \Psi(N)) \cap \Pi$. Consider the subgroup $S = \{y \in T : y \cdot u_\alpha(1) = u_\alpha(1) \text{ for all } \alpha \in \Pi \setminus \{\beta\}\}$. One can check that S is a torus of rank 1 and that $C_T(xM) = C_T(xN)S$. Hence $C_T(xM)$ is connected. □

It follows from the discussion in §1.9 that $x \in U$ as in Lemmas 2.2.3 and 2.2.4 is regular unipotent. Therefore, we get

Proposition 2.2.5 *Assume G is adjoint. Let $x \in U$ be regular unipotent and let M be a unipotent normal subgroup of B. If $C_U(xM)$ is connected, then $C_B(xM)$ is connected.*

Lemma 2.2.6 below says that the existence of relative Springer isomorphisms is independent of the isogeny class of G. We now introduce the notation required for its statement.

Let $\sigma : G \to \hat{G}$ be an isogeny. We write $d\sigma : \mathfrak{g} \to \hat{\mathfrak{g}}$ for the derivative of σ at the identity. For a subgroup H of G we write $\hat{H}$ for the image of H under σ; likewise we write $\hat{\mathfrak{h}} = d\sigma(\mathfrak{h})$. We note that for a unipotent normal subgroup M of B, σ induces an isomorphism between M and $\hat{M}$. Similarly, $d\sigma$ induces an isomorphism between $\mathfrak{m}$ and $\hat{\mathfrak{m}}$.

Let $\phi : U \to \mathfrak{u}$ be a Springer isomorphism and define
$$\hat{\phi} = (d\sigma)\phi\sigma^{-1} : \hat{U} \to \hat{\mathfrak{u}}.$$

Then one can see $\hat{\phi}$ is a Springer isomorphism. Assume we have a relative Springer isomorphism $\tilde{\phi} : U/M \to \mathfrak{u}/\mathfrak{m}$. Then we may define

$$\tilde{\hat{\phi}} = (d\sigma)\tilde{\phi}\sigma^{-1} : \hat{U}/\hat{M} \to \hat{\mathfrak{u}}/\hat{\mathfrak{m}}$$

where by an abuse of notation $\sigma : U/M \to \hat{U}/\hat{M}$ is the isomorphism induced from σ. One can check that $\tilde{\hat{\phi}}$ is a relative Springer isomorphism.

We have proved one direction of the following lemma and the converse is similar.

Lemma 2.2.6 *Let $\phi : U \to \mathfrak{u}$ be a Springer isomorphism and let M be a unipotent normal subgroup of B. Then ϕ induces a relative Springer isomorphism $\tilde{\phi} : U/M \to \mathfrak{u}/\mathfrak{m}$ if and only if $\hat{\phi}$ induces a relative Springer isomorphism $\tilde{\hat{\phi}} : \hat{U}/\hat{M} \to \hat{\mathfrak{u}}/\hat{\mathfrak{m}}$.*

We show in Corollary 2.2.13 that for a unipotent normal subgroup M of B, the existence of a relative Springer isomorphism $U/M \to \mathfrak{u}/\mathfrak{m}$ is equivalent to $C_U(xM)$ and $C_U(X + \mathfrak{m})$ being connected, where $x \in U$ is regular unipotent and $X \in \mathfrak{u}$ is regular nilpotent. We require the following two propositions.

Proposition 2.2.7 *Let M be a unipotent normal subgroup of B and let $y \in B$. Then $C_{B/M}(yM)$ contains an abelian subgroup of dimension $r = \mathrm{rank}(G)$.*

Proof: Since G is simple, $C_G(T) = T$, thus $C_B(T) = T$. Therefore, by [11, 11.10], $\bigcup_{b\in B} bTb^{-1}$ is dense in B, i.e. the semisimple elements of B are dense in B.

Consider the natural map $\pi_M : B \to B/M$. It is clear that, if $z \in B$ is semisimple, then $zM \in B/M$ is semisimple. It follows that the semisimple elements of B/M are dense in B/M.

Any semisimple element $zM \in B/M$ lies in some maximal torus S of B/M. Therefore, $C_{B/M}(zM)$ contains an abelian subgroup of dimension r – namely S.

Now we adapt Springer's proof that $C_G(y)$ contains an abelian subgroup of dimension r from [63] (see also [38, Thm. 1.14]) to give the result.

Put $R = B/M$ and let S be a maximal torus of R. Set $V_n = R/S \times S^n$ and define a morphism $f_n : V_n \to R^n$ by

$$f_n(xS, s_1, \ldots, s_n) = (xs_1x^{-1}, \ldots, xs_nx^{-1}).$$

The image Y_n of f_n consists of n-tuples of elements belonging to a common maximal torus. Since these elements commute pairwise the same is seen to be true of any n-tuple belonging to the closure Z_n of Y_n. Since R and S are irreducible so is V_n and therefore so are Y_n and Z_n.

In the case $n = 1$, we have that Y_1 is the just the set of semisimple elements of R. We said above that the semisimple elements of R are dense in R so we have that $Z_1 = R$.

Now define a projection $p_n : R^n \to R^{n-1}$ by $p_n(x_1, \dots, x_n) = (x_1, \dots, x_{n-1})$ and a section $s_n : R^{n-1} \to R^n$ by $s_n(x_1, \dots, x_{n-1}) = (x_1, \dots, x_{n-1}, 1)$, where 1 denotes the identity of R. Clearly $s_n(Y_{n-1}) \subseteq Y_n$ which forces $s_n(Z_{n-1}) \subseteq Z_n$. It is also clear that $p_n(Y_n) \subseteq Y_{n-1}$ forcing $p_n(Z_n) \subseteq Z_{n-1}$. In fact we have equality here because $Z_{n-1} = p_n(s_n(Z_{n-1})) \subseteq p_n(Z_n)$.

Therefore, we have constructed irreducible varieties Z_n together with surjective morphisms $p_n : Z_n \to Z_{n-1}$. If $(x_1, \dots, x_{n-1}) \in Y_{n-1}$ these elements lie in a common maximal torus S', so we see that the variety of n-tuples of the form $(x_1, \dots, x_{n-1}, x)$ with $x \in S'$ are in the fibre $p_n^{-1}(x_1, \dots, x_{n-1})$. It now follows from [11, AG Thm. 10.1] that each fibre of p_n has dimension at least r.

Now let $x \in R$ be arbitrary and consider all possible n-tuples $(x_1, \dots, x_n)$ $(n \geq 0)$ for which $(x, x_1, \dots, x_n) \in Z_{n+1}$. Such n-tuples exist: for $n = 0$ we can take the empty tuple and use the fact that $Z_1 = R$. Choose such an n-tuple with the centralizer C in $C_R(x)$ of the set $\{x_1, \dots, x_n\}$ minimal. Now we let z be such that $(x, x_1, \dots, x_n, z) \in Z_{n+2}$. Clearly, $C \supseteq C_G(x, x_1, \dots, x_n, z)$ This means $z \in C$ and C centralizes z. The variety of all such z corresponds to the fibre $p_{n+1}^{-1}(x, x_1, \dots, x_n)$ which has dimension at least r and is included in the abelian subgroup $Z(C)$ of $C_R(x)$. $\square$

Corollary 2.2.8 *Let M be a unipotent normal subgroup of B and let $x \in U$ be regular unipotent. Then $C_{B/M}(xM)^0$ is abelian and* $\dim C_{B/M}(xM) = r$.

Proof: The action of B on U/M factors through B/M and if $x \in U$ is regular, then $B\cdot(xM) = (B/M)\cdot(xM)$ is dense in U/M. Therefore, using (1.7.1) we see that $C_{B/M}(xM)$ has dimension r. By Proposition 2.2.7, $C_{B/M}(xM)$ has an abelian subgroup of dimension r. It follows that $C_{B/M}(xM)^0$ is abelian. $\square$

Proposition 2.2.9 *Assume G is adjoint. Let $x \in U$ be regular unipotent, let $X \in$* $\operatorname{Lie} C_B(x)$ *be regular nilpotent and let M be a unipotent normal subgroup of B. Assume $C_U(xM)$ and $C_U(X + \mathfrak{m})$ are connected. Then $C_B(xM) = C_B(X + \mathfrak{m})$.*

Proof: Since $C_{B/M}(xM)$ is abelian, by Corollary 2.2.8, Lemma 2.2.2, Proposition 2.2.5 and the assumption that $C_U(xM)$ is connected, the adjoint action of B/M on its Lie algebra is trivial. Since $X \in \operatorname{Lie} C_B(x)$, which implies $X + \mathfrak{m} \in \operatorname{Lie} C_{B/M}$, we get

$$C_{B/M}(xM) \subseteq C_{B/M}(X + \mathfrak{m}).$$

Now $C_U(X+\mathfrak{m})$ is connected by assumption, so $C_B(X+\mathfrak{m})$ is connected by Proposition 2.2.5. Thus $C_{B/M}(X+\mathfrak{m})$ is also connected by Lemma 2.2.2$'$. Also

$$\dim C_{B/M}(xM) = \dim C_{B/M}(X+\mathfrak{m}) = r$$

(by Corollaries 2.2.8 and 2.2.8$'$), so we have that

$$C_{B/M}(xM) = C_{B/M}(X+\mathfrak{m}).$$

Hence, we get $C_B(xM) = C_B(X+\mathfrak{m})$. □

We now prove

Proposition 2.2.10 *Let $\phi : U \to \mathfrak{u}$ be a Springer isomorphism, let $x \in U$ be regular unipotent, let M be a unipotent normal subgroup of B and set $X = \phi(x)$. Assume $C_B(xM) = C_B(X+\mathfrak{m})$. Then there exists a relative Springer isomorphism $\tilde{\phi} : U/M \to \mathfrak{u}/\mathfrak{m}$.*

Proof: We have $C_B(x) = C_B(X)$ and our sketch of a proof of Theorem 2.1.1 implies that the isomorphism $\phi : B\cdot x \to B\cdot X$ extends to an isomorphism $\phi : U \to \mathfrak{u}$. By assumption $C_B(xM) = C_B(X+\mathfrak{m})$, so we have an isomorphism $\tilde{\phi} : B\cdot(xM) \to B\cdot(X+\mathfrak{m})$.

We write

$$\Lambda = k[U] = k[T_\beta : \beta \in \Psi^+]$$

for the ring of regular functions of U. By an abuse of notation we also write $\Lambda = k[\mathfrak{u}]$ for the ring of regular functions of $\mathfrak{u}$. Then we have

$$\Lambda' = k[B\cdot x] = \Lambda[T_\alpha^{-1} : \alpha \in \Pi]$$

and by another abuse of notation we write $\Lambda' = k[B\cdot X]$.

The isomorphism $\phi : B\cdot x \to B\cdot X$ induces an isomorphism of k-algebras $\phi^* : \Lambda' \to \Lambda'$. The fact that ϕ extends to $\phi : U \to \mathfrak{u}$ means that ϕ^* sends Λ onto Λ.

We also have

$$\Lambda_M = k[U/M] = k[T_\beta : \beta \in \Psi^+ \setminus \Psi(\mathfrak{m})]$$

and $\Lambda_M = k[\mathfrak{u}/\mathfrak{m}]$. Then

$$\Lambda'_M = k[B\cdot(xM)] = \Lambda_M[T_\alpha^{-1} : \alpha \in \Pi \setminus \Psi(\mathfrak{m})]$$

and $\Lambda'_M = k[B \cdot (X + \mathfrak{m})]$. The isomorphism $\tilde{\phi} : B \cdot (xM) \to B \cdot (X + \mathfrak{m})$ induces an isomorphism of k-algebras $\tilde{\phi}^* : \Lambda'_M \to \Lambda'_M$. We get the commutative diagram

$$\begin{array}{ccc} \Lambda' & \xrightarrow{\phi^*} & \Lambda' \\ \uparrow{\scriptstyle i} & & \uparrow{\scriptstyle i} \\ \Lambda'_M & \xrightarrow{\tilde{\phi}^*} & \Lambda'_M \end{array}$$

where i denotes the natural inclusion. Therefore, as ϕ^* sends Λ onto Λ, it follows that $\tilde{\phi}^*$ sends Λ_M onto Λ_M and thus induces an isomorphism $\Lambda_M \to \Lambda_M$. Hence, we see that $\tilde{\phi}$ extends to an isomorphism $\tilde{\phi} : U/M \to \mathfrak{u}/\mathfrak{m}$. $\square$

We need the notation introduced in Definition 2.2.11 below for the proof of Proposition 2.2.12.

Definition 2.2.11 Let $\phi : U \to \mathfrak{u}$ be a Springer isomorphism. For $y \in U$ and $t \in k$ we define

$$y^t_\phi = \phi^{-1}(t\phi(y)).$$

Let M be a unipotent normal subgroup of B and suppose $\tilde{\phi} : U/M \to \mathfrak{u}/\mathfrak{m}$ is a relative Springer isomorphism. For $y \in U$ and $t \in k$ we define

$$(yM)^t_{\tilde{\phi}} = \tilde{\phi}^{-1}(t\tilde{\phi}(yM)).$$

We note that in the notation of Definition 2.2.11 we have $(yM)^t_{\tilde{\phi}} = y^t_\phi M$.

Proposition 2.2.12 *Let M be a unipotent normal subgroup of B and let $\phi : U \to \mathfrak{u}$ be a Springer isomorphism. Assume there exists a relative Springer isomorphism $\tilde{\phi} : U/M \to \mathfrak{u}/\mathfrak{m}$. Then, $C_U(yM)$ is connected for all $y \in U$ and $C_U(Y + \mathfrak{m})$ is connected for all $Y \in \mathfrak{u}$.*

Proof: For $zM \in U/M$ and $t \in k$, if $zM \in C_{U/M}(yM)$, then the B-equivariance (and therefore U/M-equivariance) of $\tilde{\phi}$ implies that $(zM)^t_{\tilde{\phi}} \in C_{U/M}(yM)$ for any $t \in k$. For $t = 0$ we have $(zM)^0_{\tilde{\phi}} = M$ and for $t = 1$ we have $(zM)^1_{\tilde{\phi}} = zM$. So $M, zM \in \{(zM)^t_{\tilde{\phi}} : t \in k\}$, also $\{(zM)^t_{\tilde{\phi}} : t \in k\}$ is isomorphic to $\mathbb{A}^1$ as an algebraic variety. Therefore, as $\mathbb{A}^1$ is connected, we see that $zM \in C_{U/M}(yM)^0$ and hence that $C_{U/M}(yM)$ is connected. Thus by Lemma 2.2.2 we see that $C_U(yM)$ is connected and we have proved the first part.

The second part of the proposition now follows from the first applied to $\tilde{\phi}^{-1}(Y + \mathfrak{m})$, noting that $C_U(Y + \mathfrak{m}) = C_U(\tilde{\phi}^{-1}(Y + \mathfrak{m}))$ by B-equivariance of $\tilde{\phi}$. $\square$

Using Propositions 2.2.9, 2.2.10 and 2.2.12 we can now easily deduce

Corollary 2.2.13 *Let $x \in U$ be regular unipotent, $X \in \mathfrak{u}$ be regular nilpotent, M a unipotent normal subgroup of B and $\phi : U \to \mathfrak{u}$ a Springer isomorphism. There exists a relative Springer isomorphism $\tilde{\phi} : U/M \to \mathfrak{u}/\mathfrak{m}$ if and only if $C_U(xM)$ and $C_U(X + \mathfrak{m})$ are connected.*

We now introduce a class of unipotent normal subgroups M of B, called QNT-subgroups, for which we can show that $C_U(xM)$ and $C_U(X + \mathfrak{m})$ are connected for x regular unipotent and X regular nilpotent.

Definition 2.2.14 An enumeration $\beta_1, \ldots, \beta_N$ of Ψ^+, such that

(i) $\beta_j \not\prec \beta_i$ for $i < j$,

(ii) $\{\beta_1, \ldots, \beta_r\} = \Pi$ and

(iii) $\mathrm{ht}(\beta_i) < 2\,\mathrm{ht}(\beta_j) - 1$ for $r < i < j$

is called a *QNT-enumeration.*

Given a QNT-enumeration $\beta_1, \ldots, \beta_N$ of Ψ^+ we may form a sequence of subgroups

$$M_i = \prod_{j=i+1}^{N} U_{\beta_j}.$$

Property (i) of Definition 2.2.14 ensures that M_i is a unipotent normal subgroup of B for all i. The importance of property (ii) will become apparent in the proof of Theorem 2.2.18. We have

$$\mathfrak{m}_i = \mathrm{Lie}\, M_i = \bigoplus_{j=i+1}^{N} \mathfrak{g}_{\beta_j}.$$

Definition 2.2.15 Given a QNT-enumeration of Ψ^+ the sequence of subgroup M_i as defined above is called a *QNT-sequence* of subgroups. A subgroup M of U is called a *QNT-subgroup* if it lies in a QNT-sequence of subgroups.

Remark 2.2.16 We give an explanation of the terminology QNT-subgroup. In [25, Defn. 4.1] NT-subgroups were defined. An enumeration $\beta_1, \ldots, \beta_N$ of Ψ^+ is called an *NT-enumeration* if $\mathrm{ht}(\beta_i) \leq \mathrm{ht}(\beta_{i+1})$ for $i = 1, \ldots, N-1$. The sequence of subgroups M_i as defined above is then called an *NT-sequence*. A subgroup M of U is called an *NT-subgroup* if it lies in some NT-sequence of subgroups. One easily sees that if M is an NT-subgroup, then M is a QNT-subgroup. The terminology NT-subgroup introduced in

[25] was chosen, because in the case $G = \mathrm{SL}_n(k)$ and $U = \mathrm{U}_n(k)$, NT-subgroups look "Near Triangular". The "Q" in QNT was chosen to mean "Quite".

In Theorem 2.2.18 we prove that $C_U(xM)$ is connected for $x \in U$ regular unipotent if M is a QNT-subgroup of U. Our starting point is Proposition 2.1.2. First we prove the following technical lemma.

Lemma 2.2.17 *Let $x \in U$ be regular unipotent. Then*

$$\dim C_{U^{(l)}}(x) = |\{\gamma \in \Psi^+ : \mathrm{ht}(\gamma) = l + 1\}|.$$

Proof: Using Corollary 2.1.4 we note that it suffices to show that

$$\dim C_{U^{(l)}}(X) = |\{\gamma \in \Psi^+ : \mathrm{ht}(\gamma) = l + 1\}|$$

for $X \in \mathfrak{u}$ regular nilpotent. We note that

$$U^{(l)} \cdot X \subseteq \{Y \in \mathfrak{u} : Y - X \in \mathfrak{u}^{(l+1)}\}.$$

The variety on the right hand side of the above expression has dimension $|\{\gamma \in \Psi^+ : \mathrm{ht}(\gamma) \geq l + 2\}|$ and $\dim U^{(l)} = |\{\gamma \in \Psi^+ : \mathrm{ht}(\gamma) \geq l + 1\}|$. Therefore, using (1.7.1) we see that

$$\dim C_{U^{(l)}}(X) \geq |\{\gamma \in \Psi^+ : \mathrm{ht}(\gamma) = l + 1\}|.$$

It follows from 1.7.3 that $\dim \mathfrak{c}_{\mathfrak{u}^{(l)}}(X) \geq \dim C_{U^{(l)}}(X)$. Therefore, it suffices to show that

$$\dim \mathfrak{c}_{\mathfrak{u}^{(l)}}(X) = |\{\gamma \in \Psi^+ : \mathrm{ht}(\gamma) = l + 1\}|.$$

This is contained in [64, §2]. □

Theorem 2.2.18 *Let $x \in U$ be regular unipotent and let M be a QNT-subgroup of U. Then $C_U(xM)$ is connected.*

Proof: We may assume $x = \prod_{\alpha \in \Pi} u_\alpha(1)$. Let $U = M_0 \supseteq \cdots \supseteq M_N = \{1\}$ be a QNT-sequence of subgroups of U and suppose that $M = M_i$. We work by (reverse) induction on i to show that $C_B(xM_i)$ is connected, the base case $i = N$ being Proposition 2.1.2.

So suppose $0 \leq i < N$ and $C_U(xM_{i+1})$ is connected, let $\beta = \beta_{i+1}$ and suppose $\mathrm{ht}(\beta) = l$. If $l = 1$, then one can see that $C_U(xM_i) = C_U(xM_{i+1})$, so assume that $l \geq 2$.

By considering the Chevalley commutator relations (see [66, Prop. 8.2.3]) and condition (ii) for a QNT-enumeration we see that the action of U on U/M_i factors through $U/U^{(2l-3)}$. Then by Lemma 2.2.2 we have that $C_{U/U^{(2l-3)}}(xM_{i+1})$ is connected.

The Chevalley commutator relations imply that

$$U^{(l-2)} \cdot x \subseteq \left\{ y \in U : y = x \prod_{\mathrm{ht}(\gamma) \geq l} u_\gamma(\lambda_\gamma) \ , \ \lambda_\gamma \in k \right\}.$$

We denote the variety on the right hand side of the above expression by $\mathcal{A}_l$; it is a closed, irreducible subset of U. Clearly we have

$$\dim \mathcal{A}_l = |\{\gamma \in \Psi^+ : \mathrm{ht}(\gamma) \geq l\}|$$

and we also have

$$\dim U^{(l-2)} = |\{\gamma \in \Psi^+ : \mathrm{ht}(\gamma) \geq l-1\}|.$$

Therefore, by Lemma 2.2.17 and (1.7.1) we see that

$$\dim U^{(l-2)} \cdot x = \dim \mathcal{A}_l.$$

Since $U^{(l-2)}$ is a unipotent group $U^{(l-2)} \cdot x$ is closed in $\mathcal{A}_l$ by [11, Prop. 4.10]. Thus, the irreducibility of $\mathcal{A}_l$ implies that

$$U^{(l-2)} \cdot x = \mathcal{A}_l.$$

Therefore, we may find

$$v = \prod_{l-1 \leq \mathrm{ht}(\gamma) \leq 2l-3} u_\gamma(\mu_\gamma) \in U^{(l-2)}$$

such that

$$v \cdot xU^{(2l-2)} = xu_\beta(1)U^{(2l-2)}.$$

For $t \in k$ define

$$v(t) = \prod_{l-1 \leq \mathrm{ht}(\gamma) \leq 2l-3} u_\gamma(\mu_\gamma t).$$

Since $U^{(l-2)}/U^{(2l-3)}$ is abelian,

$$V = \{v(t)U^{(2l-3)} : t \in k\}$$

is a subgroup of $U^{(l-2)}/U^{(2l-3)}$ isomorphic to $\mathbb{G}_a$. We note that the action of $U^{(l-2)}$

on $U/U^{(2l-2)}$ factors through $U^{(l-2)}/U^{(2l-3)}$ By considering the Chevalley commutator relations we see that

$$V \cdot xU^{(2l-2)} = \{yU^{(2l-2)} : y = xu_\beta(\lambda), \lambda \in k\}.$$

Let $yU^{(2l-3)} \in C_{U/U^{(2l-3)}}(xM_i)$. Then

$$y \cdot xM_{i+1} = xu_\beta(\mu)M_{i+1}$$

for some $\mu \in k$. There exists $w \in V$ such that

$$w \cdot xu_\beta(\mu)M_{i+1} = xM_{i+1}.$$

So that

$$wyU^{(2l-3)} \in C_{U/U^{(2l-3)}}(xM_{i+1}).$$

Therefore,

$$C_{U/U^{(2l-3)}}(xM_i) \subseteq VC_{U/U^{(2l-3)}}(xM_{i+1}).$$

Hence, as $V, C_{U/U^{(l-1)}}(xM_{i+1}) \subseteq C_{U/U^{(l-1)}}(xM_i)$ are connected, we see that

$$C_{U/U^{(2l-3)}}(xM_i) = VC_{U/U^{(2l-3)}}(xM_{i+1})$$

is connected. Thus, by Lemma 2.2.2 $C_U(xM_i)$ is connected. $\square$

Using Theorems 2.2.18 and 2.2.18′, and Corollary 2.2.13 we can easily deduce

Corollary 2.2.19 *Let $\phi : U \to \mathfrak{u}$ be a Springer isomorphism and let M be a QNT-subgroup of U. There exists a relative Springer isomorphism $\tilde{\phi} : U/M \to \mathfrak{u}/\mathfrak{m}$.*

In Remark 2.2.20 and Proposition 2.2.21 we give methods for deducing the existence of a relative Springer isomorphism from the existence of other relative Springer isomorphisms.

Remark 2.2.20 Let P be a parabolic subgroup of G containing B. We denote the unipotent radical of P by P_u and write $\mathfrak{p}_u$ for the Lie algebra of P_u. We write $\pi : P \to P/P_u$ for the natural map and $d\pi : \mathfrak{p} \to \mathfrak{p}/\mathfrak{p}_u$ for its derivative. The image $\hat{B} = \pi(B)$ is a Borel subgroup of the reductive group $\hat{P} = \pi(P)$ and $\hat{U} = \pi(U)$ is the unipotent radical of $\hat{B}$. For a unipotent normal subgroup M of B containing P_u we write $\hat{M} = \pi(M)$ and $\hat{\mathfrak{m}} = d\pi(\mathfrak{m})$.

Let $\psi : \hat{U} \to \hat{\mathfrak{u}}$ be a Springer isomorphism, let M be a unipotent normal subgroup of B and suppose there exists a relative Springer isomorphism $\tilde{\psi} : \hat{U}/\hat{M} \to \hat{\mathfrak{u}}/\hat{\mathfrak{m}}$. We have isomorphisms

$$\hat{U}/\hat{M} \cong U/M \quad \text{and} \quad \hat{\mathfrak{u}}/\hat{\mathfrak{m}} \cong \mathfrak{u}/\mathfrak{m}.$$

So we get a B-equivariant isomorphism of varieties $U/M \to \mathfrak{u}/\mathfrak{m}$. Now one can deduce (using a strengthened version of Proposition 2.2.12, which can be proved in the same way) that $C_U(xM)$ and $C_U(X+\mathfrak{m})$ are connected. Hence, by Corollary 2.2.13 given a Springer isomorphism $\phi : U \to \mathfrak{u}$ we get a relative Springer isomorphism $U/M \to \mathfrak{u}/\mathfrak{m}$.

Since the rank of each of the simple components $\hat{P}$ is less than the rank of G, the above discussion leads to an inductive method for proving the existence of relative Springer isomorphisms.

Proposition 2.2.21 *Let $\phi : U \to \mathfrak{u}$ be a Springer isomorphism and let M_1, M_2 be unipotent normal subgroups of B. Suppose there exist relative Springer isomorphisms $\tilde{\phi}_i : U/M_i \to \mathfrak{u}/\mathfrak{m}_i$ (for $i = 1,2$). Then there exists a relative Springer isomorphism $\tilde{\phi} : U/(M_1 \cap M_2) \to \mathfrak{u}/(\mathfrak{m}_1 \cap \mathfrak{m}_2)$.*

Proof: Let $x \in U$ be regular unipotent. It is easy to see that $C_B(x(M_1 \cap M_2)) = C_B(xM_1) \cap C_B(xM_2)$. Similarly, $C_B(X + (\mathfrak{m}_1 \cap \mathfrak{m}_2)) = C_B(X+\mathfrak{m}_1) \cap C_B(X+\mathfrak{m}_2)$, where $X = \phi(x)$. Since, $\tilde{\phi}_i : U/M_i \to \mathfrak{u}/\mathfrak{m}_i$ are relative Springer isomorphisms, for $i = 1,2$, we have $C_B(xM_i) = C_B(X+\mathfrak{m}_i)$, for $i = 1,2$. Hence, $C_B(x(M_1 \cap M_2)) = C_B(X + (\mathfrak{m}_1 \cap \mathfrak{m}_2))$. Therefore, there exists a relative Springer isomorphism $\tilde{\phi} : U/(M_1 \cap M_2) \to \mathfrak{u}/(\mathfrak{m}_1 \cap \mathfrak{m}_2)$, by Proposition 2.2.10. $\square$

We are now in a position to prove Theorem 2.2.1.

Proof of Theorem 2.2.1: First suppose G is of type A and let M be a unipotent normal subgroup of B. By Lemma 2.2.6 we may assume that $G = \mathrm{SL}_n(k)$ for some n. Then we may assume $U = \mathrm{U}_n(k)$. The map $x \to x - 1$ from U to $\mathfrak{u}$ is a Springer isomorphism which induces a relative Springer isomorphism for any unipotent normal subgroup of B. Therefore, by Corollary 2.2.13 we see that $C_U(xM)$ and $C_U(X+\mathfrak{m})$ are connected, where $x \in U$ is regular unipotent, $X \in \mathfrak{u}$ is regular nilpotent and M is a unipotent normal subgroup of B. Thus, given any Springer isomorphism $\phi : U \to \mathfrak{u}$, we may use Corollary 2.2.13 to deduce that there exists a relative Springer isomorphism $\tilde{\phi} : U/M \to \mathfrak{u}/\mathfrak{m}$.

Now suppose G is a classical group not of type A. By Lemma 2.2.6 we may assume $G = \mathrm{Sp}_n(k)$ or $G = \mathrm{SO}_n(k)$ for some n. Then we may consider $G \subseteq H = \mathrm{SL}_n(k)$ and $U = G \cap V$ where $V = \mathrm{U}_n(k)$. The Cayley map $X \mapsto (1-X)(1+X)^{-1}$ from $\mathfrak{u}$ to U is a

B-equivariant isomorphism of varieties (see [67, III, 3.14] or Example 2.1.8). Therefore, its inverse is a Springer isomorphism $\phi : U \to \mathfrak{u}$. Also the inverse of the Cayley map defines a Springer isomorphism $\psi : V \to \mathfrak{v}$ such that $\phi = \psi|_U$. Now let M be any unipotent normal subgroup of B. Then M be can written as $U \cap N$ for some unipotent normal subgroup N of $\mathrm{B}_n(k)$ – this can be checked using [69, §11]. By the first part of this proof, we have a relative Springer isomorphism $\tilde{\psi} : V/N \to \mathfrak{v}/\mathfrak{n}$. Also we have isomorphisms $U/M \to UN/N$ and $\mathfrak{u}/\mathfrak{m} \to (\mathfrak{u}+\mathfrak{n})/\mathfrak{n}$. Then we get the following commutative diagram

$$\begin{array}{ccc} UN/N & \xrightarrow{\tilde{\psi}} & (\mathfrak{u}+\mathfrak{n})/\mathfrak{n} \\ \uparrow & & \uparrow \\ U/M & \xrightarrow{\tilde{\phi}} & \mathfrak{u}/\mathfrak{m} \end{array}$$

where $\tilde{\phi}$ is induced from $\tilde{\psi}$. It is straightforward to check that $\tilde{\phi}$ is a relative Springer isomorphism. As in the type A case we may deduce that given any Springer isomorphism we get relative Springer isomorphisms for all unipotent normal subgroups M of B.

For G of exceptional type we made an (inductive) check that relative Springer isomorphisms $U/M \to \mathfrak{u}/\mathfrak{m}$ exist as described below.

Suppose P is a parabolic subgroup of G. Then P/P_u is a reductive group each of whose simple components has rank less than that of G. Therefore, the discussion in Remark 2.2.20 implies that we may inductively assume relative Springer isomorphisms exist if M contains P_u. By Corollary 2.2.19 we also have that relative Springer isomorphisms exist if M is a QNT-subgroup. This gives us a set of subgroups $\mathcal{S}$ for which relative Springer isomorphisms exist. Using Proposition 2.2.21, we may take intersections of subgroups in $\mathcal{S}$ to get subgroups for which relative Springer isomorphisms exist. By writing a procedure in the computer algebra language GAP4 [22] we checked that for G of exceptional type we get all unipotent normal subgroups of B in this way. Although this check was done by computer we demonstrate in Example 2.2.22 below that it would be possible to do this by hand. □

Example 2.2.22 In this example we demonstrate how one can show relative Springer isomorphisms exist. We consider an example in the case G is of type E_6. We use the notation from [13, Planche V] for the roots of the root system of type E_6. We recall the terminology of ideals of Ψ and generators from §1.10. Given a unipotent normal subgroup M of B we recall that $\Psi(M)$ is an ideal of Ψ and we write $\Gamma(\Psi(M))$ for its set of generators.

We consider the unipotent normal subgroup M of B where $\Gamma(\Psi(M)) = \{{}^{00110}_{\;\;1}, {}^{11100}_{\;\;1}\}$.

Clearly, M cannot be dealt with using Remark 2.2.20 and one sees that $\begin{smallmatrix}11111\\0\end{smallmatrix} \notin \Psi(M)$ so that M is not a QNT-subgroup. However, one can check that $M = M_1 \cap M_2$ where M_1 has one generator, namely $\begin{smallmatrix}00000\\1\end{smallmatrix}$ and M_2 has generators $\begin{smallmatrix}00110\\1\end{smallmatrix}$ and $\begin{smallmatrix}11100\\0\end{smallmatrix}$. We can use Remark 2.2.20 to deduce that (for a Springer isomorphism $\phi : U \to \mathfrak{u}$) we have a relative Springer isomorphism $\tilde{\phi}_1 : U/M_1 \to \mathfrak{u}/\mathfrak{m}_1$. We can check that M_2 is a QNT-subgroup so that we have a relative Springer isomorphism $\tilde{\phi}_2 : U/M_2 \to \mathfrak{u}/\mathfrak{m}_2$, by Corollary 2.2.19. Then we may use Proposition 2.2.21 to deduce that there is a relative Springer isomorphism $\tilde{\phi} : U/M \to \mathfrak{u}/\mathfrak{m}$.

By considering the commutative diagram in the statement of Theorem 2.2.1 we get the following corollary.

Corollary 2.2.23 *Let $\phi : U \to \mathfrak{u}$ be a Springer isomorphism and let M be a unipotent normal subgroup of B. Then $\phi(M) = \mathfrak{m}$.*

One can easily see that if $\phi : U \to \mathfrak{u}$ is a Springer isomorphism which commutes with F and M is a unipotent normal subgroup of B, then the relative Springer isomorphism $\tilde{\phi} : U/M \to \mathfrak{u}/\mathfrak{m}$ commutes with F. So we have:

Proposition 2.2.24 *Let M be a unipotent normal subgroup of B. There exist relative Springer isomorphisms $\tilde{\phi} : U/M \to \mathfrak{u}/\mathfrak{m}$ which commute with F.*

Corollary 2.1.6 states the bijection between the G-orbits in $\mathcal{U}$ and $\mathcal{N}$ induced by a Springer isomorphism is independent of the choice of Springer isomorphism. We now consider the analogous question for the bijection between the B-orbits in U/M and $\mathfrak{u}/\mathfrak{m}$ induced by a relative Springer isomorphism. In Theorem 2.2.26 below we show that the bijection between the sheets of B on U/M and $\mathfrak{u}/\mathfrak{m}$ induced by a relative Springer isomorphism is independent of the choice of relative Springer isomorphism. In particular, this applies to the case $M = \{1\}$.

Let $x \in \mathcal{U}^r$ and fix $X \in (\operatorname{Lie} C_G(x))^r$. We recall that for each $y \in C_U(x)^r$ there is a unique Springer isomorphism $\phi_{y,X} : \mathcal{U} \to \mathfrak{u}$ with $\phi_{y,X}(y) = X$ and every Springer isomorphism is of the form $\phi_{y,X}$ for some $y \in C_G(x)^r$. Given a Springer isomorphism $\phi_{y,X}$ and a unipotent normal subgroup M of U, we write $\tilde{\phi}_{y,X} : U/M \to \mathfrak{u}/\mathfrak{m}$ for the corresponding relative Springer isomorphism.

Proposition 2.2.25 *There exists a morphism of algebraic varieties $\tilde{\Phi} : C_U(x)^r \times U/M \to \mathfrak{u}/\mathfrak{m}$ such that $\tilde{\Phi}(y, zM) = \tilde{\phi}_{y,X}(zM)$ for every $y \in C_U(x)^r$ and $z \in U$.*

Proof: The proof that Φ (in Proposition 2.1.5) exists given in [62] shows that the map $(y, z) \mapsto \phi_{y,X}(z)$ from $C_G(x)^r \times G \cdot x$ to $G \cdot X$ extends to $\Phi : C_G(x)^r \times \mathcal{U} \to \mathcal{N}$. This means that the map $(y, z) \mapsto \phi_{y,X}(z)$ from $C_U(x)^r \times B \cdot x$ to $B \cdot X$ extends to $\Phi : C_U(x)^r \times U \to \mathfrak{u}$. Now we may apply arguments similar to those in the proof of Theorem 2.2.1 to show that the map $(y, z) \mapsto \tilde{\phi}_{y,X}(zM)$ from $C_U(x)^r \times B \cdot (xM)$ to $B \cdot (X + \mathfrak{m})$ extends to $\tilde{\Phi} : C_U(x)^r \times U/M \to \mathfrak{u}/\mathfrak{m}$. $\square$

We now easily deduce Theorem 2.2.26 from Propositions 2.2.25 and 1.7.5.

Theorem 2.2.26 *The bijection between the sheets of B on U/M and $\mathfrak{u}/\mathfrak{m}$ given by a relative Springer isomorphism $\tilde{\phi}$ is independent of the choice of $\tilde{\phi}$. In particular, if B acts on U/M with finitely many orbits, then the bijection between the orbits of B in U/M and $\mathfrak{u}/\mathfrak{m}$ induced by $\tilde{\phi}$ is independent of $\tilde{\phi}$.*

Remark 2.2.27 We do not know an example of two relative Springer isomorphism which induce different bijections on the B-orbits in U/M and $\mathfrak{u}/\mathfrak{m}$. Some calculations for small rank type A cases (where B acts with infinitely many orbits) show that the bijection of B-orbits is independent in these cases.

Chapter 3
The adjoint action of U on $\mathfrak{u}$

In this chapter we study the adjoint orbits of U in $\mathfrak{u}$. We show that any such orbit contains a unique so-called *minimal representative* and we present an algorithm for calculating all minimal representatives, which only requires linear algebra. We require the existence of relative Springer isomorphisms for Proposition 3.1.2, which is crucial in this chapter. We remind the reader that in this chapter we use the notation given in the introduction.

3.1 Orbit maps and centralizers

In this section we consider orbits and centralizers in the action of U on a quotient U/M of U and a quotient $\mathfrak{u}/\mathfrak{m}$ of $\mathfrak{u}$, where M is a unipotent normal subgroup of B.

We begin by giving the following immediate consequence of [11, Prop. 4.10].

Lemma 3.1.1 *Let M be a unipotent normal subgroup of B.*

(i) *For $y \in U$, the orbit $U \cdot (yM)$ is closed.*

(ii) *For $Y \in \mathfrak{u}$, the orbit $U \cdot (Y + \mathfrak{m})$ is closed.*

The following proposition strengthens Proposition 2.2.12; it follows from Corollary 2.2.13 and Theorem 2.2.1.

Proposition 3.1.2 *Let M be a unipotent normal subgroup of B.*

(i) *For $y \in U$, the centralizer $C_U(yM)$ is connected.*

(ii) *For $Y \in \mathfrak{u}$, the centralizer $C_U(Y + \mathfrak{m})$ is connected.*

In Proposition 3.1.4 below we show that the orbit map $U \to U \cdot (X + \mathfrak{m})$ is separable for any $X \in \mathfrak{u}$. We require Proposition 3.1.3 to prove Proposition 3.1.4. In the proofs of these two propositions we frequently use the equivalent conditions for the separability of an orbit map given in Propositions 1.7.2 and 1.7.3; this reference is not made in the proofs.

Proposition 3.1.3 *Let M be a unipotent normal subgroup of B and let $x \in U$. The orbit map $U/M \to (U/M) \cdot xM$ is separable.*

Proof: Let $\phi : U \to \mathfrak{u}$ be a Springer isomorphism and let $\tilde{\phi} : U/M \to \mathfrak{u}/\mathfrak{m}$ be the corresponding relative Springer isomorphism. We begin by showing that $\tilde{\phi}^{-1}(\mathfrak{c}_{\mathfrak{u}/\mathfrak{m}}(xM)) = C_{U/M}(xM)$. Let $Y + \mathfrak{m} \in \mathfrak{c}_{\mathfrak{u}/\mathfrak{m}}(xM)$. Then $xM \in C_{U/M}(Y + \mathfrak{m}) = C_{U/M}(\tilde{\phi}^{-1}(Y + \mathfrak{m}))$ by U/M-equivariance of $\tilde{\phi}$. Therefore, $\tilde{\phi}^{-1}(Y + \mathfrak{m}) \in C_{U/M}(xM)$, which implies the inclusion $\tilde{\phi}^{-1}(\mathfrak{c}_{\mathfrak{u}/\mathfrak{m}}(xM)) \subseteq C_{U/M}(xM)$. A similar argument gives the reverse inclusion. In particular, we have $\dim \mathfrak{c}_{\mathfrak{u}/\mathfrak{m}}(xM) = \dim C_{U/M}(xM)$ so that the orbit map $U/M \to (U/M) \cdot xM$ is separable. □

Proposition 3.1.4 *Let M be a unipotent normal subgroup of B.*

(i) *Let $x \in U$. The orbit map $U \to U \cdot (xM)$ is separable.*

(ii) *Let $X \in \mathfrak{u}$. The orbit map $U \to U \cdot (X + \mathfrak{m})$ is separable.*

Proof: Let $x \in U$. By Proposition 3.1.3, $\dim C_{U/M}(xM) = \dim \mathfrak{c}_{\mathfrak{u}/\mathfrak{m}}(xM)$. It is clear that $\dim C_U(xM) = \dim C_{U/M}(xM) + \dim M$ and $\dim \mathfrak{c}_{\mathfrak{u}}(xM) = \dim \mathfrak{c}_{\mathfrak{u}/\mathfrak{m}}(xM) + \dim M$. Thus $\dim C_U(xM) = \dim \mathfrak{c}_{\mathfrak{u}}(xM)$ and the orbit map $U \to U \cdot (xM)$ is separable, which proves part (i).

Let $\phi : U \to \mathfrak{u}$ be a Springer isomorphism and let $\tilde{\phi} : U/M \to \mathfrak{u}/\mathfrak{m}$ be the corresponding relative Springer isomorphism. Let $X \in \mathfrak{u}$. The isomorphism $\tilde{\phi}$ transforms the orbit map $U \to U \cdot \tilde{\phi}^{-1}(X + \mathfrak{m})$ to the orbit map $U \to U \cdot (X + \mathfrak{m})$. Since the former map is separable, so is the latter map. □

The following corollary is proved using arguments from the proof of Proposition 3.1.3.

Corollary 3.1.5 *Let $\phi : U \to \mathfrak{u}$ be a Springer isomorphism and M a unipotent normal subgroup of B.*

(i) *Let $x \in U$. Then $\phi(C_U(xM)) = \mathfrak{c}_{\mathfrak{u}}(xM)$.*

(ii) *Let $X \in \mathfrak{u}$. Then $\phi(C_U(X + \mathfrak{m})) = \mathfrak{c}_{\mathfrak{u}}(X + \mathfrak{m})$.*

Proof: Part (i) follows from arguments in the proof of Proposition 3.1.3.

For part (ii) set $x = \phi^{-1}(X)$. Proposition 3.1.4 implies $\operatorname{Lie} C_U(xM) = \mathfrak{c}_{\mathfrak{u}}(xM)$ and $\operatorname{Lie} C_U(X + \mathfrak{m}) = \mathfrak{c}_{\mathfrak{u}}(X + \mathfrak{m})$. Hence,

$$\phi(C_U(X + \mathfrak{m})) = \phi(C_U(xM)) = \mathfrak{c}_{\mathfrak{u}}(xM) = \operatorname{Lie} C_U(xM) = \operatorname{Lie} C_U(X + \mathfrak{m}) = \mathfrak{c}_{\mathfrak{u}}(X + \mathfrak{m}),$$

the first and fourth equalities holding by U-equivariance of ϕ and the second from part (i). □

3.2 Minimal representatives

In this section we show that each U-orbit in $\mathfrak{u}$ contains a minimal representative. We note that some of the results in this section generalize results of A. Vera-López and J.M. Arregi from [74].

Fix an enumeration $\beta_1, \dots, \beta_N$ of Ψ^+ such that $\beta_j \not\preccurlyeq \beta_i$ for $i < j$ and define B-submodules of $\mathfrak{u}$ by

$$\mathfrak{m}_i = \bigoplus_{j=i+1}^{N} \mathfrak{g}_{\beta_j}.$$

for $i = 0, \dots, N$. Then we define $\mathfrak{u}_i = \mathfrak{u}/\mathfrak{m}_i$.

We study the orbits of U in $\mathfrak{u}$ by considering the action of U on successive $\mathfrak{u}_i$.

Remark 3.2.1 We note that we could consider the U-orbits in any B-submodule $\mathfrak{n}$ of $\mathfrak{u}$ in a similar way. One just chooses an enumeration of $\Psi(\mathfrak{n})$ rather than an enumeration of Ψ^+.

Suppose $X \in \mathfrak{u}$ and consider the variety

$$X + ke_{\beta_i} + \mathfrak{m}_i = \{X + \lambda e_{\beta_i} + \mathfrak{m}_i : \lambda \in k\} \subseteq \mathfrak{u}_i.$$

We consider which elements of $X + ke_{\beta_i} + \mathfrak{m}_i$ are U-conjugate in $\mathfrak{u}_i$. We have the following lemma, the existence of relative Springer isomorphisms and therefore Proposition 3.1.2 are crucial to its proof.

Lemma 3.2.2 *Let $X + \mathfrak{m}_{i-1} \in \mathfrak{u}_{i-1}$. Either*

(i) *all elements of $X + ke_{\beta_i} + \mathfrak{m}_i$ are U-conjugate or*

(ii) *no two elements of $X + ke_{\beta_i} + \mathfrak{m}_i$ are U-conjugate.*

Proof: Let $\lambda \in k$, and consider the orbit map

$$\psi_\lambda : C_U(X + \mathfrak{m}_{i-1}) \to C_U(X + \mathfrak{m}_{i-1}) \cdot (X + \lambda e_{\beta_i} + \mathfrak{m}_i) \subseteq X + ke_{\beta_i} + \mathfrak{m}_i.$$

By Proposition 3.1.2, $C_U(X + \mathfrak{m}_{i-1})$ is connected, thus the image of ψ_λ is connected. Further, the image of ψ_λ is closed by Lemma 3.1.1. Therefore, since $X + ke_{\beta_i} + \mathfrak{m}_i$ is isomorphic to $\mathbb{A}^1$ as an algebraic variety, we have that $\operatorname{im} \psi_\lambda$ is equal to either $\{X + \lambda e_{\beta_i} + \mathfrak{m}_i\}$ or $X + ke_{\beta_i} + \mathfrak{m}_i$. $\square$

Lemma 3.2.2 allows us to make the following definition.

Definition 3.2.3 Let $X \in \mathfrak{u}$.

(i) If Lemma 3.2.2(i) holds, then we say i is an *inert* point of X.

(ii) If Lemma 3.2.2(ii) holds, then we say i is a *ramification* point of X.

We now define a partial order $\leq_i$ $(i = 0, 1, \ldots, N)$ on $\mathfrak{u}_i$.

Definition 3.2.4 Let $X, Y \in \mathfrak{u}$ and let $X + \mathfrak{m}_i = \sum_{j=1}^{i} a_j e_{\beta_j} + \mathfrak{m}_i$ and $Y + \mathfrak{m}_i = \sum_{j=1}^{i} b_j e_{\beta_j} + \mathfrak{m}_i$. Then $X + \mathfrak{m}_i <_i Y + \mathfrak{m}_i$ provided there exists $l \leq i$ such that $a_j = b_j$ for $j < l$ and $a_l = 0$, $b_l \neq 0$.

The partial order $\leq_i$ induces a reflexive, transitive relation on $\mathfrak{u}$; we also write $\leq_i$ for this relation. If S is any subset of $\mathfrak{u}_i$, one can see that S contains $\leq_i$-minimal elements. A minimal element $\sum_{j \in J} a_j e_{\beta_j} + \mathfrak{m}_i \in S$ ($J \subseteq \{1, \ldots, i\}$, $a_j \neq 0$ for all $j \in J$) has as few as possible non-zero a_j, in the sense that there is no $Y + \mathfrak{m}_i \in S$, $i' \leq i$ and $J' \subsetneqq J \cap \{1, \ldots, i'\}$ such that $Y + \mathfrak{m}_{i'} = \sum_{j \in J'} a_j e_{\beta_j} + \mathfrak{m}_{i'}$. Similarly, a subset S of $\mathfrak{u}$ contains $\leq_i$-minimal elements, which have a description similar to the above.

We note that for $X, Y \in \mathfrak{u}$, if $j \leq i$ and $X \leq_i Y$, then $X \leq_j Y$. In particular, if S is a subset of $\mathfrak{u}$ (respectively $\mathfrak{u}_i$) and X (respectively $X + \mathfrak{m}_i$) is a $\leq_i$-minimal element of S, then X (respectively $X + \mathfrak{m}_j$) is a $\leq_j$-minimal element of S.

The next proposition implies that each U-orbit in $\mathfrak{u}$ contains a unique minimal element (with respect to the enumeration $\beta_1, \ldots, \beta_N$ of Ψ).

Proposition 3.2.5 *Let $U \cdot (Z + \mathfrak{m}_i)$ be an orbit of U in $\mathfrak{u}_i$. There exists a unique $\leq_i$-minimal element of $U \cdot (Z + \mathfrak{m}_i)$.*

Proof: We work by induction on i. If $i = 0$, then the result is trivial. So assume $i > 0$ and $U \cdot (Z + \mathfrak{m}_{i-1})$ contains a unique $\leq_{i-1}$-minimal element. Let $X = \sum_{j=1}^{i} a_j e_{\beta_j}$ and $Y = \sum_{j=1}^{i} b_j e_{\beta_j}$ be such that $X + \mathfrak{m}_i$ and $Y + \mathfrak{m}_i$ are $\leq_i$-minimal elements of $U \cdot (Z + \mathfrak{m}_i)$. Then $X + \mathfrak{m}_{i-1}$ and $Y + \mathfrak{m}_{i-1}$ are $\leq_{i-1}$-minimal elements of $U \cdot (Z + \mathfrak{m}_{i-1})$. Therefore, by induction $X + \mathfrak{m}_{i-1} = Y + \mathfrak{m}_{i-1}$ is the unique $\leq_{i-1}$-minimal representative of $U \cdot (Z + \mathfrak{m}_{i-1})$ and so $a_j = b_j$ for $j \leq i - 1$. Now if $a_i \neq b_i$, then i is an inert point of X so that $X' + \mathfrak{m}_i = \sum_{j=1}^{i-1} a_j e_{\beta_j} + \mathfrak{m}_i \in U \cdot (Z + \mathfrak{m}_i)$. Now $X' + \mathfrak{m}_i \leq_i X + \mathfrak{m}_i$ and $X' + \mathfrak{m}_i \leq_i Y + \mathfrak{m}_i$. Therefore, $\leq_i$-minimality of $X + \mathfrak{m}_i$ and $Y + \mathfrak{m}_i$ forces $X + \mathfrak{m}_i = X' + \mathfrak{m}_i = Y + \mathfrak{m}_i$. $\square$

We note that the minimal representatives of the U-orbits in $\mathfrak{u}_i$ do depend on the chosen order of Ψ^+. Also we note that, if $X + \mathfrak{m}_i$ is the minimal representative of its U-orbit in $\mathfrak{u}_i$, then $X + \mathfrak{m}_{i-1}$ is the minimal representative of its U-orbit in $\mathfrak{u}_{i-1}$.

We now describe when an element of $\mathfrak{u}_i$ is the $\leq_i$-minimal element of its U-orbit.

Lemma 3.2.6 *Let $X \in \mathfrak{u}$. Then $X + \mathfrak{m}_i = \sum_{j=1}^{i} a_j e_{\beta_j} + \mathfrak{m}_i$ is the unique $\leq_i$-minimal element of its U-orbit in $\mathfrak{u}_i$ if and only if $a_j = 0$ whenever j is an inert point of X.*

Proof: We work by induction on i to show that, if $X + \mathfrak{m}_i = \sum_{j=1}^{i} a_j e_{\beta_j} + \mathfrak{m}_i$ is the unique $\leq_i$-minimal element of its U-orbit in $\mathfrak{u}_i$, then $a_j = 0$ whenever j is an inert point of X. The case $i = 0$ is trivial.

Let $i > 0$ and let $X + \mathfrak{m}_i = \sum_{j=1}^{i} a_j e_{\beta_j} + \mathfrak{m}_i \in \mathfrak{u}_i$ be the unique $\leq_i$-minimal element of its U-orbit in $\mathfrak{u}_i$. Then $X + \mathfrak{m}_{i-1}$ is the $\leq_{i-1}$-minimal representative of its U-orbit, so by induction, $a_j = 0$ whenever $j \leq i - 1$ is an inert point of X. If i is a ramification point of X, then trivially $a_j = 0$ whenever $j \leq i$ is an inert point of X. If i is an inert point of X, then $X + \mathfrak{m}_i$ is in the same U-orbit as $\sum_{j=1}^{i-1} a_j e_{\beta_j} + \mathfrak{m}_i$ and thus $\leq_i$-minimality of $X + \mathfrak{m}_i$ implies that $a_i = 0$.

We now work by induction on i to show that, if $X + \mathfrak{m}_i = \sum_{j=1}^{i} a_j e_{\beta_j} + \mathfrak{m}_i \in \mathfrak{u}_i$ satisfies $a_j = 0$ whenever $j \leq i$ is an inert point of X, then $X + \mathfrak{m}_i$ is the $\leq_i$-minimal representative of its U-orbit. The base case $i = 0$ is trivial.

Let $i > 0$ and suppose $X + \mathfrak{m}_i = \sum_{j=1}^{i} a_j e_{\beta_j} + \mathfrak{m}_i \in \mathfrak{u}_i$ satisfies $a_j = 0$ whenever $j \leq i$ is an inert point of X. Let $Y + \mathfrak{m}_i = \sum_{j=1}^{i} b_j e_{\beta_j} + \mathfrak{m}_i \in \mathfrak{u}_i$ be the $\leq_i$-minimal element of $U \cdot (X + \mathfrak{m}_i)$. Then $Y + \mathfrak{m}_{i-1}$ is $\leq_{i-1}$-minimal in $U \cdot (X + \mathfrak{m}_{i-1})$, so by induction $Y + \mathfrak{m}_{i-1} = X + \mathfrak{m}_{i-1}$. If $a_i \neq b_i$, then i must be an inert point of X and therefore $a_i = 0$ by assumption. Thus $\leq_i$-minimality of $Y + \mathfrak{m}_i$ implies $b_i = 0$ so $X + \mathfrak{m}_i = Y + \mathfrak{m}_i$ is $\leq_i$-minimal. $\square$

In Proposition 3.2.8 we describe the variety $U \cdot (X + \mathfrak{m}_i)$; in particular, we give its dimension. We use the following notation in the Proposition 3.2.8.

Definition 3.2.7 Let $X \in \mathfrak{u}$. The number of inert points of X less than or equal to i is denoted by $\mathrm{in}_i(X)$.

Proposition 3.2.8 *Let $X \in \mathfrak{u}$. Then $U \cdot (X + \mathfrak{m}_i)$ is isomorphic as a variety to $\mathbb{A}^{\mathrm{in}_i(X)}$. In particular, $\dim U \cdot (X + \mathfrak{m}_i) = \mathrm{in}_i(X)$ and $\dim C_U(X + \mathfrak{m}_i) = N - \mathrm{in}_i(X)$.*

Proof: We work by induction on i. If $i = 0$, then the result is trivial. Let $i > 0$ and let $\pi : \mathfrak{u}_i \to \mathfrak{u}_{i-1}$ be the natural map. We recall from the discussion at the end of §1.7 that for any $Y + \mathfrak{m}_i \in \mathfrak{u}_i$ we can identify $T_{Y+\mathfrak{m}_i}(\mathfrak{u}_i) = \mathfrak{u}_i$ and then we have $d\pi_{Y+\mathfrak{m}_i} = \pi$.

First suppose i is a ramification point of X. Then we see that the restriction $\pi : U \cdot (X + \mathfrak{m}_i) \to U \cdot (X + \mathfrak{m}_{i-1})$ is a bijective morphism. It follows from Proposition 3.1.4 that $T_{X+\mathfrak{m}_j}(U \cdot (X + \mathfrak{m}_j)) = [\mathfrak{u}, X] + \mathfrak{m}_j$ (for $j = i - 1, i$) and therefore that $d\pi_{X+\mathfrak{m}_i} = \pi : [\mathfrak{u}, X] + \mathfrak{m}_i \to [\mathfrak{u}, X] + \mathfrak{m}_{i-1}$ is surjective. Hence, $\pi : U \cdot (X + \mathfrak{m}_i) \to U \cdot (X + \mathfrak{m}_{i-1})$

is separable and thus an isomorphism, (this can be proved in the same way as [66, Thm. 5.3.2(iii)]) so that $U \cdot (X + \mathfrak{m}_i) \cong \mathbb{A}^{\mathrm{in}_i(X)}$.

So suppose i is an inert point of X. Then we can define a map

$$\theta : U \cdot (X + \mathfrak{m}_i) \to U \cdot (X + \mathfrak{m}_{i-1}) \times \mathbb{A}^1$$

by

$$\theta\left(\sum_{j=1}^{i-1} b_j e_{\beta_j} + c e_{\beta_i} + \mathfrak{m}_i\right) = \left(\sum_{j=1}^{i-1} b_j e_{\beta_j} + \mathfrak{m}_{i-1}, c\right).$$

We can see that θ is an isomorphism and it follows that $U \cdot (X + \mathfrak{m}_i) \cong \mathbb{A}^{\mathrm{in}_i(X)}$.

We now trivially have the equality $\dim U \cdot (X + \mathfrak{m}_i) = \mathrm{in}_i(X)$ and the equality $\dim C_U(X + \mathfrak{m}_i) = N - \mathrm{in}_i(X)$ follows from (1.7.1). $\square$

3.3 An algorithm for calculating minimal representatives

We retain the notation from the previous section. Our results of the previous section lead to an algorithm for determining the U-orbits in $\mathfrak{u}$, by finding all minimal representatives of the U-orbits in $\mathfrak{u}$. We outline this algorithm below.

0*th step*: There is one U-orbit in $\mathfrak{u}_0$, its $\leq_0$-minimal representative is $0 + \mathfrak{m}_0$.

i*th step*: Suppose we know the $\leq_{i-1}$-minimal representatives of all the U-orbits in $\mathfrak{u}_{i-1}$. We wish to determine the $\leq_i$-minimal representatives of all the U-orbits in $\mathfrak{u}_i$.

By Lemma 3.2.6, $X + \mathfrak{m}_i = \sum_{j=1}^{i} a_j e_{\beta_j} + \mathfrak{m}_i$ is the $\leq_i$-minimal representative of its U-orbit, if $X + \mathfrak{m}_{i-1}$ is the $\leq_{i-1}$-minimal representative of its U-orbit and $a_i = 0$ in case i is an inert point of X. Using Proposition 3.1.4 we see that we can determine whether i is an inert or ramification point of X by calculating $\dim \mathfrak{c}_{\mathfrak{u}}(X + \mathfrak{m}_i)$ – this can be reduced to linear algebra, as explained in §1.11.

Therefore, we can determine all the $\leq_i$-minimal representatives of U-orbits in $\mathfrak{u}_i$ by calculating $\dim \mathfrak{c}_{\mathfrak{u}}(X + \mathfrak{m}_i)$ for each X such that $X + \mathfrak{m}_{i-1}$ is a $\leq_{i-1}$ minimal representative of its U-orbit in $\mathfrak{u}_{i-1}$.

After the Nth step we will have calculated all the orbits of U in $\mathfrak{u}$.

We illustrate this algorithm when G is of type B_2 and A_3 in the examples below.

Example 3.3.1 We illustrate the calculation of the U-orbits in $\mathfrak{u}$ when G is of type B_2. We note that this example was given in [16, p. 29]. Since the structure of the U-orbits is quite simple in this case, the algorithm of Bürgstein and Hesellink (presented in [16]) gives the same result as our algorithm, see Remark 3.3.3. We consider $G = \mathrm{Sp}_4(k) = \{x \in \mathrm{GL}_4(k) : x^t Jx = J\}$, where

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

We take the upper triangular matrices in G to be the Borel subgroup B and T to be the diagonal matrices in G. Then $\mathfrak{u}$ consists of the strictly upper triangular matrices in $\mathfrak{g}$, i.e. matrices of the form

$$\begin{pmatrix} 0 & a & b & c \\ 0 & 0 & d & b \\ 0 & 0 & 0 & -a \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Using the notation of [13, Planche II] the positive roots of G are

$$\beta_1 = 01, \beta_2 = 10, \beta_3 = 11, \beta_4 = 12.$$

We use the above enumeration of Ψ^+. Then the $\mathfrak{m}_i$ are as depicted below where we only show the $(1,2)$th, $(1,3)$th, $(1,4)$th and the $(2,3)$th entries.

$$\mathfrak{m}_0 = \begin{matrix} k & k & k \\ & k & \end{matrix}, \quad \mathfrak{m}_1 = \begin{matrix} 0 & k & k \\ & k & \end{matrix}, \quad \mathfrak{m}_2 = \begin{matrix} 0 & k & k \\ & 0 & \end{matrix},$$

$$\mathfrak{m}_3 = \begin{matrix} 0 & 0 & k \\ & 0 & \end{matrix}, \quad \mathfrak{m}_4 = \begin{matrix} 0 & 0 & 0 \\ & 0 & \end{matrix}.$$

So for example, $\mathfrak{m}_2$ consists of matrices of the form

$$\begin{pmatrix} 0 & 0 & b & c \\ 0 & 0 & 0 & b \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

Figure 3.1 is a tree which illustrates the calculation of the U-orbits in $\mathfrak{u}$, using the algorithm described above. The ith row ($i = 0, 1, 2, 3, 4$) shows the minimal representatives of the U-orbits in $\mathfrak{u}_i$. We only show the $(1,2)$th, $(1,3)$th, $(1,4)$th and the $(2,3)$th entries of these minimal representatives. The entry $k^\times$ means that one can take any non-zero element of k and the entry $*$ means that the entry is factored out. An edge is drawn between minimal representatives of the form $X + \mathfrak{m}_{i-1}$ and $X + \mathfrak{m}_i$. So there are two edges coming from a minimal representative $X + \mathfrak{m}_{i-1}$ if i is a ramification point of X and one edge if i is an inert point of X.

The most interesting feature of the tree is that there are two edges coming from

$$\begin{array}{ccc} 0 & 0 & * \\ & k^\times & \end{array},$$

meaning that 4 is a ramification point of

$$\begin{array}{ccc} 0 & 0 & 0 \\ & \lambda & \end{array}$$

for any $\lambda \in k^\times$. This is because "U_{β_2} has been used to make the coefficient of e_{β_3} zero so it cannot also be used to make the coefficient of e_{β_4} zero".

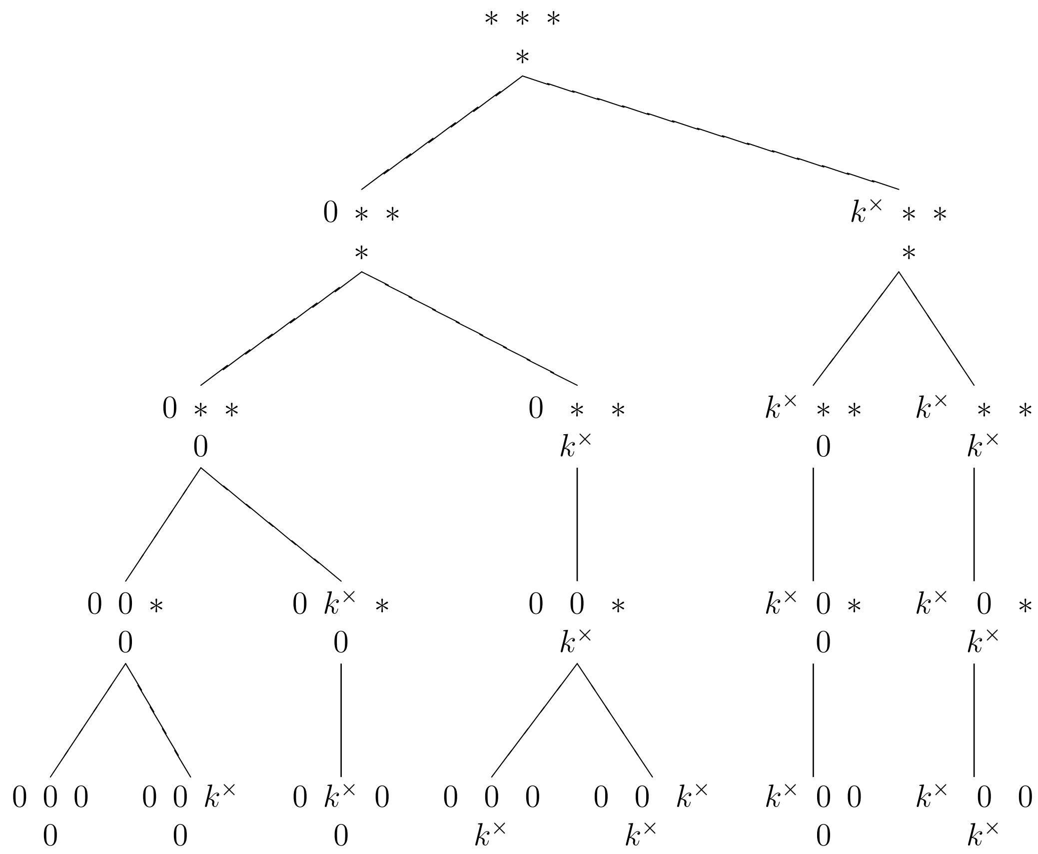

Figure 3.1: The U-orbits in $\mathfrak{u}$ for $G = \mathrm{Sp}_4(k)$

Example 3.3.2 We now give an example of part of the calculation of the U-orbits in $\mathfrak{u}$ in case G is of type A_3. We take $G = \mathrm{SL}_4(k)$, $U = \mathrm{U}_4(k)$ and T to consist of the diagonal matrices in G. Then $\mathfrak{u}$ consists of strictly upper triangular matrices in $\mathfrak{gl}_4(k)$. Using the notation from [13, Planche I] the positive roots of G are

$$\beta_1 = 100, \beta_2 = 010, \beta_3 = 001, \beta_4 = 110, \beta_5 = 011, \beta_6 = 111.$$

We use the above enumeration of Ψ^+. The submodules $\mathfrak{m}_i$ are then as depicted below where we show only the entries above the diagonal:

$$\mathfrak{m}_0 = \begin{matrix} k & k & k \\ & k & k \\ & & k \end{matrix}, \quad \mathfrak{m}_1 = \begin{matrix} 0 & k & k \\ & k & k \\ & & k \end{matrix}, \quad \mathfrak{m}_2 = \begin{matrix} 0 & k & k \\ & 0 & k \\ & & k \end{matrix}, \quad \mathfrak{m}_3 = \begin{matrix} 0 & k & k \\ & 0 & k \\ & & 0 \end{matrix},$$

$$\mathfrak{m}_4 = \begin{matrix} 0 & 0 & k \\ & 0 & k \\ & & 0 \end{matrix}, \quad \mathfrak{m}_5 = \begin{matrix} 0 & 0 & k \\ & 0 & 0 \\ & & 0 \end{matrix}, \quad \mathfrak{m}_6 = \begin{matrix} 0 & 0 & 0 \\ & 0 & 0 \\ & & 0 \end{matrix}.$$

Due to space restrictions we only show, in Figure 3.2 the branch of the tree illustrating the calculation of the U-orbits (as explained in the previous example) from the 2nd row of the tree beginning with

$$\begin{matrix} k^\times & * & * \\ & 0 & * \\ & & * \end{matrix}.$$

The most interesting point in the tree is at

$$\begin{matrix} k^\times & 0 & * \\ & 0 & * \\ & & k^\times \end{matrix},$$

where there are two edges, meaning that 5 is a ramification point of

$$\begin{matrix} \lambda & 0 & * \\ & 0 & 0 \\ & & \mu \end{matrix}$$

for any $\lambda, \mu \in k^\times$. This is because "$U_{\beta_2}$ has been used to make the coefficient of e_{β_4} zero so it cannot also be used to make the coefficient of e_{β_5} zero".

$$
\begin{tikzcd}[column sep=small]
 & & & \begin{matrix} k^\times & * & * \\ & 0 & * \\ & & * \end{matrix} \arrow[dll, dash] \arrow[drr, dash] & & & & \\
 & \begin{matrix} k^\times & * & * \\ & 0 & * \\ & & 0 \end{matrix} \arrow[d, dash] & & & & \begin{matrix} k^\times & * & * \\ & 0 & * \\ & & k^\times \end{matrix} \arrow[d, dash] & \\
 & \begin{matrix} k^\times & 0 & * \\ & 0 & * \\ & & 0 \end{matrix} \arrow[dl, dash] \arrow[dr, dash] & & & & \begin{matrix} k^\times & 0 & * \\ & 0 & * \\ & & k^\times \end{matrix} \arrow[dl, dash] \arrow[dr, dash] & \\
\begin{matrix} k^\times & 0 & * \\ & 0 & 0 \\ & & 0 \end{matrix} \arrow[d, dash] & & \begin{matrix} k^\times & 0 & * \\ & 0 & k^\times \\ & & 0 \end{matrix} \arrow[d, dash] & & \begin{matrix} k^\times & 0 & * \\ & 0 & 0 \\ & & k^\times \end{matrix} \arrow[d, dash] & & \begin{matrix} k^\times & 0 & * \\ & 0 & k^\times \\ & & k^\times \end{matrix} \arrow[d, dash] \\
\begin{matrix} k^\times & 0 & 0 \\ & 0 & 0 \\ & & 0 \end{matrix} & & \begin{matrix} k^\times & 0 & 0 \\ & 0 & k^\times \\ & & 0 \end{matrix} & & \begin{matrix} k^\times & 0 & 0 \\ & 0 & 0 \\ & & k^\times \end{matrix} & & \begin{matrix} k^\times & 0 & 0 \\ & 0 & k^\times \\ & & k^\times \end{matrix}
\end{tikzcd}
$$

Figure 3.2: Some of the U-orbits in $\mathfrak{u}$ for $G = \mathrm{SL}_4(k)$

Remark 3.3.3 We note that the orbits of U on $\mathfrak{u}$ are more complicated when the rank of G is large. There exist instances where there is a subset $J \subseteq \{1, \ldots, i-1\}$ and $a_j, b_j \in k^\times$ ($j \in J$) such that i is an inert point of $\sum_{j \in J} a_j e_{\beta_j}$ and a ramification point of $\sum_{j \in J} b_j e_{\beta_j}$, see [74, §3 Ex. 1].

Chapter 4
The adjoint action of B on $\mathfrak{u}$

In this chapter we discuss the adjoint B-orbits in $\mathfrak{u}$. We show as in the previous chapter, that each B-orbit contains a unique minimal representative and give an algorithm for calculating all such representatives. We also describe the geometry of a B-orbit in $\mathfrak{u}$. Further, we discuss an algorithm which determines whether B acts on a B-submodule of $\mathfrak{u}$ with a dense orbit. We also consider the question of when $\mathfrak{u}^{(l)}$ is a prehomogeneous space for B. We remind the reader that in this chapter we use the notation given in the introduction.

4.1 Minimal representatives

We choose an enumeration $\beta_1, \dots, \beta_N$ of Ψ^+ and define $\mathfrak{m}_i$ and $\mathfrak{u}_i$ as in §3.2. We study the B-orbits in $\mathfrak{u}$ by considering the B-orbits in successive $\mathfrak{u}_i$s.

Remark 4.1.1 As in Remark 3.2.1 we note that we could consider the B-orbits in any B-submodule $\mathfrak{n}$ of $\mathfrak{u}$ in a similar way.

We define a partial order $\leq_i^B$ on $\mathfrak{u}_i$ as follows.

Definition 4.1.2 Let $X, Y \in \mathfrak{u}$ and let $X + \mathfrak{m}_i = \sum_{j=1}^{i} a_j e_{\beta_j} + \mathfrak{m}_i$ and $Y + \mathfrak{m}_i = \sum_{j=1}^{i} b_j e_{\beta_j} + \mathfrak{m}_i$. Then $X + \mathfrak{m}_i <_i^B Y + \mathfrak{m}_i$ provided there exists $l \leq i$ such that $a_j = b_j$ for $j < l$, and $a_l = 0$, $b_l \neq 0$, or $a_l = 1$, $b_l \neq 0, 1$ and β_l is linearly independent of $\{\beta_j : j < l \text{ and } a_j \neq 0\}$.

This partial order is defined so that $X + \mathfrak{m}_i = \sum_{j=1}^{i} a_j e_{\beta_j} + \mathfrak{m}_i$ is $\leq_i^B$-minimal in its B-orbit in $\mathfrak{u}_i$ if it is $\leq_i$-minimal in its U-orbit and "as many as possible coefficients are normalized to 1". This means that if $a_l \neq 0$, and β_l is linearly independent of $\{\beta_j : j < l \text{ and } a_j \neq 0\}$ (so that a_l can be normalized to 1), then $a_l = 1$.

We can now prove the following analogue of Proposition 3.2.5.

Proposition 4.1.3 *Let $B \cdot (Z + \mathfrak{m}_i)$ be an orbit of B in $\mathfrak{u}_i$. There exists a unique $\leq_i^B$-minimal element of $B \cdot (Z + \mathfrak{m}_i)$.*

Proof: This can be proved by induction as for Proposition 3.2.5. We only need to note that if, in the induction step, i is a ramification point of X and $X + \mathfrak{m}_i = \sum_{j=1}^{i} a_j e_{\beta_j} + \mathfrak{m}_i$ is in the same B-orbit as $X + \lambda e_{\beta_i} + \mathfrak{m}_i$ (for some $\lambda \neq 0$), then β_i is linearly independent of $\{\beta_j : j < i \text{ and } a_j \neq 0\}$ and so we may assume $a_i = 1$, by Lemma 1.7.4. $\square$

In the next two results we consider the centralizer of a minimal representative of a B-orbit in $\mathfrak{u}_i$. We require the following definition.

Definition 4.1.4 Let $X = \sum_{\beta \in \Psi^+} a_\beta e_\beta$. The *support* of X is defined to be $\mathrm{supp}(X) = \{\beta \in \Psi^+ : a_\beta \neq 0\}$ and we write $\mathrm{supp}_i(X) = \mathrm{supp}(X) \cap \{\beta_1, \ldots, \beta_i\}$. We denote by $\mathrm{lir}_i(X)$ the maximal size of a linearly independent subset of $\mathrm{supp}_i(X)$.

Proposition 4.1.5 *Let $X + \mathfrak{m}_i \in \mathfrak{u}_i$ be the $\leq_i^B$-minimal representative of its B-orbit. Then we have the factorization $C_B(X + \mathfrak{m}_i) = C_U(X + \mathfrak{m}_i)C_T(X + \mathfrak{m}_i)$.*

Proof: Let $J = \{j : \beta_j \in \mathrm{supp}_i(X)\}$ and write $X + \mathfrak{m}_i = \sum_{j \in J} a_j e_{\beta_j} + \mathfrak{m}_i$. Let $b \in C_B(X + \mathfrak{m}_i)$. We may write $b = ut$ where $u \in U$ and $t \in T$. We have $t \cdot (X + \mathfrak{m}_i) = \sum_{j \in J} \beta_j(t) a_j e_{\beta_j} + \mathfrak{m}_i$. Suppose $t \notin C_T(X + \mathfrak{m}_i)$ and let $j \in J$ be minimal such that $\beta_j(t) \neq 1$. Since $a_j \neq 0$, j is a ramification point of X by Lemma 3.2.6. But

$$u \cdot (X + (\beta_j(t) - 1)a_j e_{\beta_j} + \mathfrak{m}_j) = X + \mathfrak{m}_j$$

which implies that j is an inert point of X. This contradiction means that $t \in C_T(X+\mathfrak{m}_i)$. Therefore, we also have $u \in C_U(X + \mathfrak{m}_i)$ and hence $b \in C_U(X + \mathfrak{m}_i)C_T(X + \mathfrak{m}_i)$. $\square$

Proposition 4.1.6 *Let $X + \mathfrak{m}_i \in \mathfrak{u}$ be the minimal representative of its B-orbit. Then $\dim C_B(X + \mathfrak{m}_i) = N + r - \mathrm{in}_i(X) - \mathrm{lir}_i(X)$ and $\dim B \cdot (X + \mathfrak{m}_i) = \mathrm{in}_i(X) + \mathrm{lir}_i(X)$.*

Proof: Given the factorization $C_B(X + \mathfrak{m}_i) = C_U(X + \mathfrak{m}_i)C_T(X + \mathfrak{m}_i)$, the equality $\dim C_B(X + \mathfrak{m}_i) = N + r - \mathrm{in}_i(X) - \mathrm{lir}_i(X)$ follows from Lemma 1.7.4 and Proposition 3.2.8. Then (1.7.1) implies that $\dim B \cdot (X + \mathfrak{m}_i) = \mathrm{in}_i(X) + \mathrm{lir}_i(X)$. $\square$

In Proposition 4.1.10 we describe the geometry of $B \cdot (X + \mathfrak{m}_i)$ for $X \in \mathfrak{u}$. We require a separability condition which we get from the next two lemmas.

Lemma 4.1.7 *Suppose for any linearly independent subset Δ of Ψ^+ we have $[\mathfrak{t}, Y] = \bigoplus_{\beta\in\Delta} \mathfrak{g}_\beta$, where $Y = \sum_{\beta\in\Delta} e_\beta$. Then for any $X \in \mathfrak{u}$ and $i = 1, \dots, N$, the orbit map $B \to B \cdot (X + \mathfrak{m}_i)$ is separable.*

Proof: Suppose the condition in the statement of the proposition holds and let $X \in \mathfrak{u}$. We may assume $X + \mathfrak{m}_i$ is the $\leq_i^B$-minimal representative of its B-orbit. Using Proposition 1.7.3 it suffices to prove that $\dim([\mathfrak{b}, X] + \mathfrak{m}_i) = \dim B \cdot (X + \mathfrak{m}_i)$. It is straightforward to prove the above equality of dimensions, using Proposition 4.1.6 and the proof of Proposition 3.2.8. □

We recall that the weight lattice of Ψ is denoted by Λ and the root lattice of Ψ is denoted by Λ_r. We refer the reader to [37, 13.1] for the cardinality of $|\Lambda/\Lambda_r|$.

Lemma 4.1.8 *Suppose p does not divide $|\Lambda/\Lambda_r|$. Let Δ be a linearly independent subset of Ψ and $Y = \sum_{\beta\in\Delta} e_\beta$. Then $[\mathfrak{t}, Y] = \bigoplus_{\beta\in\Delta} \mathfrak{g}_\beta$.*

Proof: The condition on p means that we may choose a basis $\{Z_\alpha : \alpha \in \Pi\}$ of $\mathfrak{t}$ such that $[Z_\alpha, e_\beta] = \delta_{\alpha,\beta} e_\beta$ for $\alpha, \beta \in \Pi$. It follows that the dimension of $[\mathfrak{t}, Y]$ is the dimension of the $\mathbb{F}_p$-vector space

$$\sum_{\beta\in\Delta} \mathbb{Z}\beta \otimes_{\mathbb{Z}} \mathbb{F}_p.$$

Since Δ is a linearly independent subset of Ψ and p is good for G, [67, 4.3] implies that the dimension of the above space is $|\Delta|$. The result now follows, because $[\mathfrak{t}, Y] \subseteq \bigoplus_{\beta\in\Delta} \mathfrak{g}_\beta$. □

Remark 4.1.9 We note that under the assumption that p is good for G, the only cases where p divides $|\Lambda/\Lambda_r|$ are when G is of type A_r and p divides $r + 1$. In this case we may replace G by $\mathrm{GL}_{r+1}(k)$ and B by $\mathrm{B}_{r+1}(k)$ without affecting $\mathfrak{u}$ or $B \cdot X$. With $B = \mathrm{B}_{r+1}(k)$, $X \in \mathfrak{u}$ and $\mathfrak{m}$ a B-submodule of $\mathfrak{u}$, we see that $C_B(X + \mathfrak{m})$ consists of the invertible elements of $\mathfrak{c}_{\mathfrak{b}}(X + \mathfrak{m})$. It follows from Proposition 1.7.3 that the orbit map $B \to B \cdot (X + \mathfrak{m})$ is separable.

In the statement of Proposition 4.1.10 we also use the notation $\mathbb{A}^1_0 = \mathbb{A}^1 \setminus \{0\}$ and $\mathbb{A}^n_0$ is the direct product of n copies of $\mathbb{A}^1_0$.

Proposition 4.1.10 *Let $X + \mathfrak{m}_i = \sum_{j=1}^{i} a_j e_{\beta_j} \in \mathfrak{u}_i$ be the $\leq_i^B$-minimal representative in it B-orbit. Then $B \cdot (X + \mathfrak{m}_i)$ is isomorphic as a variety to $\mathbb{A}^{\mathrm{in}_i(X)} \times \mathbb{A}_0^{\mathrm{lir}_i(X)}$.*

Proof: As discussed in Remark 4.1.9 if G is of type A_r and p divides $r+1$ we may replace B by $\mathrm{B}_{r+1}(k)$. Therefore, by Lemmas 4.1.7 and 4.1.8 and Remark 4.1.9, we may assume that the orbit maps $B \to B\cdot(X+\mathfrak{m}_j)$ are separable for $j = 1, \dots, i$. We work by induction on i. The base case $i = 0$ is trivial so assume $i \geq 1$ and the result holds for $i-1$. Let $\pi : \mathfrak{u}_i \to \mathfrak{u}_{i-1}$ be the natural map.

If i is an inert point of X or i is a ramification point of X and β_i is linearly dependent on $\mathrm{supp}_{i-1}(X)$, then the separability of the orbit maps $B \to B\cdot(X+\mathfrak{m}_j)$ means we may argue as in Proposition 3.2.8. Further, if i is a ramification point of X, and β_i is linearly independent of $\mathrm{supp}_{i-1}(X)$ and $a_i = 0$, then we can argue as in Proposition 3.2.8.

So suppose i is a ramification point of X, β_i is linearly independent of $\mathrm{supp}_{i-1}(X)$ and $a_i = 1$. Let $Y = \sum_{j=1}^{i-1} a_j e_{\beta_j}$. A consequence of the above discussion is that the restriction of π to $B\cdot(Y+\mathfrak{m}_i)$ is an isomorphism. This implies that there exists $f \in k[B\cdot(X+\mathfrak{m}_{i-1})]$ such that for any $\sum_{j=1}^{i} b_j e_{\beta_j} + \mathfrak{m}_i \in B\cdot(Y+\mathfrak{m}_i)$ we have $f(\sum_{j=1}^{i-1} b_j e_{\beta_j} + \mathfrak{m}_{i-1}) = b_i$. We can define a map

$$\theta : B\cdot(X+\mathfrak{m}_i) \to B\cdot(X+\mathfrak{m}_{i-1}) \times \mathbb{A}_0^1$$

by

$$\theta\left(\sum_{j=1}^{i-1} b_j e_{\beta_j} + c e_{\beta_i} + \mathfrak{m}_i\right) = \left(\sum_{j=1}^{i-1} b_j e_{\beta_j} + \mathfrak{m}_i, c - f(\sum_{j=1}^{i-1} b_j e_{\beta_j} + \mathfrak{m}_{i-1})\right).$$

One can check that this is an isomorphism so that $B\cdot(X+\mathfrak{m}_i) \cong \mathbb{A}^{\mathrm{in}_i(X)} \times \mathbb{A}_0^{\mathrm{lir}_i(X)}$. $\square$

4.2 An algorithm for calculating minimal representatives

The algorithm given in Section §3.2, to determine the adjoint U-orbits in $\mathfrak{u}$, has a natural modification to give an algorithm that calculates the minimal representatives of the B-orbits in $\mathfrak{u}$. We outline this algorithm below.

0*th step*: There is one B-orbit in $\mathfrak{u}_0$, its $\leq_0^B$-minimal representative is $0+\mathfrak{m}_0$.

i*th step*: Suppose we know the $\leq_{i-1}^B$-minimal representatives of all the B-orbits in $\mathfrak{u}_{i-1}$. We wish to determine the $\leq_i^B$-minimal representatives of all the B-orbits in $\mathfrak{u}_i$.

By Lemma 3.2.6, $X+\mathfrak{m}_i = \sum_{j=1}^{i} a_j e_{\beta_j} + \mathfrak{m}_i$ is the $\leq_i^B$-minimal representative of its B-orbit, if $X+\mathfrak{m}_{i-1}$ is the $\leq_{i-1}^B$-minimal representative of its B-orbit, $a_i = 0$ in case i is an inert point of X, and $a_i = 0, 1$ in case i is an ramification point of X and β_i is linearly independent of $\mathrm{supp}_{i-1}(X)$. Using Proposition 3.1.4 we see that we can determine whether i is an inert or ramification point of X by calculating $\dim \mathfrak{c}_{\mathfrak{u}}(X+\mathfrak{m}_i)$ – this can be reduced to linear algebra, as explained in §1.11. We can determine whether β_i is linearly independent of $\mathrm{supp}_{i-1}(X)$ by calculating the rank of the matrix whose rows correspond to the elements of $\mathrm{supp}_{i-1}(X) \cup \{\beta_i\}$.

Therefore, we can determine all the $\leq_i^B$-minimal representatives of U-orbits in $\mathfrak{u}_i$ by calculating $\dim \mathfrak{c}_{\mathfrak{u}}(X + \mathfrak{m}_i)$ and possibly the rank of the matrix whose rows correspond to a set of roots, for each X such that $X + \mathfrak{m}_{i-1}$ is a $\leq_{i-1}^B$ minimal representative of its B-orbit in $\mathfrak{u}_{i-1}$.

After the Nth step we will have calculated all the orbits of B in $\mathfrak{u}$.

Remark 4.2.1 It is easy to see how one can determine the minimal representatives of the U-orbits in $\mathfrak{u}$ from the minimal representatives of the B-orbits in $\mathfrak{u}$. It is therefore more efficient to calculate the minimal representatives of the B-orbits then determine the minimal representatives of the U-orbits, than to calculate the U-orbits directly.

In Example 3.3.1 we get the following minimal representatives of the 7 B-orbits. We use the same notation as in the example.

$$\begin{matrix}0&0&0\\&0&\end{matrix} \quad \begin{matrix}0&0&1\\&0&\end{matrix} \quad \begin{matrix}0&1&0\\&0&\end{matrix} \quad \begin{matrix}0&0&0\\&1&\end{matrix} \quad \begin{matrix}0&0&1\\&1&\end{matrix} \quad \begin{matrix}1&0&0\\&0&\end{matrix} \quad \begin{matrix}1&0&0\\&1&\end{matrix}$$

4.3 Algorithmic testing for dense orbits

In this section we describe an algorithm, called DOOBS (Dense Orbits of Borel Subgroups), which determines whether B acts on a B-submodule $\mathfrak{n}$ of $\mathfrak{u}$ with a dense orbit. We begin by introducing some notation.

Let $\mathfrak{n}$ be a B-submodule of $\mathfrak{u}$ and choose an enumeration $\beta_1, \dots, \beta_m$ of $\Psi(\mathfrak{n})$ ($m = \dim \mathfrak{n}$) so that $\beta_j \not\preceq \beta_i$ for $i < j$. We define B-submodules $\mathfrak{m}_i$ of $\mathfrak{n}$ by $\mathfrak{m}_i = \bigoplus_{j=i+1}^m \mathfrak{g}_{\beta_j}$ for $i = 0, \dots, m$. Then we define the quotients $\mathfrak{n}_i = \mathfrak{n}/\mathfrak{m}_i$.

DOOBS considers the action of B on successive $\mathfrak{n}_i$s; at each stage it finds a representative $X_i + \mathfrak{m}_i$ (with $\mathrm{supp}(X_i)$ linearly independent) of a dense B-orbit in $\mathfrak{n}_i$ or decides that $\mathfrak{n}_i$ is not a prehomogeneous space for B.

We note that Remarks 3.2.1 and 4.1.1 mean that we can apply the results of §3.2 and §4.1 in this setting.

We now give an outline of how DOOBS works. In this outline we do not justify why the algorithm makes the decisions it does; this is covered in Theorem 4.3.1 below.

0th step: DOOBS considers the action of B on $\mathfrak{n}_0 = \{0\}$. Trivially B acts on $\mathfrak{n}_0$ with a dense orbit, the algorithm chooses $0 + \mathfrak{m}_0$ as a representative of a dense orbit and therefore sets $X_0 = 0$.

ith step: DOOBS has chosen the representative $X_{i-1} + \mathfrak{m}_{i-1}$ of a dense B-orbit in $\mathfrak{n}_{i-1}$ with $\mathrm{supp}(X_{i-1})$ linearly independent. The algorithm considers the action of B on $\mathfrak{n}_i$.

- First DOOBS considers the U-orbit of $X_{i-1}+\mathfrak{m}_i$. It determines whether i is an inert point of X_{i-1} by calculating $\dim \mathfrak{c}_\mathfrak{u}(X_{i-1}+\mathfrak{m}_i)$. If this is the case, then it decides $B \cdot (X_{i-1} + \mathfrak{m}_i)$ is dense in $\mathfrak{n}_i$ and so sets $X_i = X_{i-1}$.
- If i is a ramification point of X_{i-1}, then DOOBS determines whether β_i is linearly independent of $\mathrm{supp}(X_{i-1})$. If this is the case, then it decides that $X_{i-1} + e_{\beta_i} + \mathfrak{m}_i$ is a representative of a dense B-orbit in $\mathfrak{n}_i$ and so sets $X_i = X_{i-1} + e_{\beta_i}$.
- If DOOBS decides that neither $B\cdot(X_{i-1}+\mathfrak{m}_i)$ nor $B\cdot(X_{i-1}+e_{\beta_i}+\mathfrak{m}_i)$ is dense in $\mathfrak{n}_i$, then it decides that B does not act on $\mathfrak{n}_i$ (and therefore on $\mathfrak{n}$) with a dense orbit and stops.

$(m+1)$th step: DOOBS has chosen a representative of a dense orbit in $\mathfrak{n}_m = \mathfrak{n}$ so it concludes that B does act on $\mathfrak{n}$ with a dense orbit and finishes.

In Theorem 4.3.1 below we justify that DOOBS does correctly decide whether B acts on $\mathfrak{n}$ with a dense orbit.

Theorem 4.3.1 DOOBS *correctly decides whether B acts on $\mathfrak{n}$ with a dense orbit. Moreover, if B does act on $\mathfrak{n}$ with a dense orbit, then* DOOBS *find a representative of this orbit.*

Proof: We prove, by induction on i, that if B acts on $\mathfrak{n}_i$ with a dense orbit, then DOOBS finds a representative X_i of this dense orbit.

The base case $i = 0$ is trivial so assume that $i \geq 1$ and the induction hypothesis holds for $i-1$. If B does not act on $\mathfrak{n}_{i-1}$ with a dense orbit, then clearly B does not act on $\mathfrak{n}_i$ with a dense orbit. Therefore, we may assume that DOOBS has found the representative X_{i-1} of a dense B-orbit in $\mathfrak{n}_{i-1}$. We note that if B does act on $\mathfrak{n}_i$ with a dense orbit, then there must be a representative of the form $X_{i-1} + \lambda e_{\beta_i} + \mathfrak{m}_i$ for some $\lambda \in k$.

If i is an inert point of X_{i-1}, then by Proposition 4.1.6 we have that

$$\dim(B \cdot (X_{i-1} + \mathfrak{m}_i)) = \dim(B \cdot (X_{i-1} + \mathfrak{m}_{i-1})) + 1.$$

So the B-orbit of $X_i + \mathfrak{m}_i = X_{i-1} + \mathfrak{m}_i$ is dense in $\mathfrak{n}_i$.

If i is a ramification point of X_{i-1} and β_i is linearly independent of $\mathrm{supp}(X_{i-1})$, then by Proposition 4.1.6 we have that

$$\dim(B \cdot (X_{i-1} + e_{\beta_i} + \mathfrak{m}_i)) = \dim(B \cdot (X_{i-1} + \mathfrak{m}_{i-1})) + 1.$$

Therefore, $X_i = X_{i-1} + e_{\beta_i}$ is a representative of a dense B-orbit in $\mathfrak{n}_i$.

Finally, suppose i is an ramification point of X_{i-1} and β_i is not linearly independent of $\operatorname{supp}(X_{i-1})$. Then $X_{i-1} + \lambda e_{\beta_i} + \mathfrak{m}_i$ is the $\leq_i^B$-minimal representative of its B-orbit for any $\lambda \in k$. Also, by Proposition 4.1.6 we have that

$$\dim(B \cdot (X_{i-1} + \lambda e_{\beta_i} + \mathfrak{m}_i)) = \dim(B \cdot (X_{i-1} + \mathfrak{m}_{i-1})) < \dim \mathfrak{n}_i$$

for any $\lambda \in k$. Hence, $\mathfrak{n}_i$ is not a prehomogeneous space for B. □

We now give the following corollary of Theorem 4.3.1.

Corollary 4.3.2 *Suppose $\mathfrak{n}$ is a prehomogeneous space for B. Then there is a linearly independent subset $\Delta \subseteq \Psi(\mathfrak{n})$ such that $X = \sum_{\beta \in \Delta} e_\beta$ is a representative of the dense B-orbit in $\mathfrak{n}$. Moreover we have*

(i) $\dim U \cdot X = \dim \mathfrak{n} - |\Delta|$;

(ii) $\dim T \cdot X = |\Delta|$;

(iii) $|U \cdot X \cap T \cdot X| = 1$.

Proof: Parts (i) and (ii) follow directly from the proof of Theorem 4.3.1. We see that the X found by DOOBS is the minimal representative of its B-orbit so that (iii) follows from Proposition 4.1.5. □

We have programmed DOOBS in the computer algebra language GAP4 ([22]). We briefly explain how this was achieved. The program is available on the author's website `http://web.mat.bham.ac.uk/S.M.Goodwin/DOOBS.html`.

The functions for Lie algebras in GAP4 are used to define the required mathematical objects. Checking if a set of roots is linearly independent is easily achieved by calculating the rank of the matrix whose rows correspond to these roots. The method for calculating the dimension of centralizers in $\mathfrak{u}$ is that described in §1.11. Using the language of §1.11, DOOBS calculates $\dim_0 \mathfrak{c}_\mathfrak{u}(X)$ and keeps track of the values of $p > 0$ for which we know $\dim_p \mathfrak{c}_\mathfrak{u}(X) = \dim_0 \mathfrak{c}_\mathfrak{u}(X)$. The values of p for which $\dim_p \mathfrak{c}_\mathfrak{u}(X) < \dim_0 \mathfrak{c}_\mathfrak{u}(X)$ are output at the end of the calculation as characteristic restrictions. Further, the algorithm was programmed to try to keep the entries in the matrices E_i (see §1.11) small.

We have used the version of DOOBS programmed in GAP4 to classify all instances when $\mathfrak{n}$ is a prehomogeneous space for B when $\operatorname{rank}(G) \leq 8$. The results are available at `http://web.mat.bham.ac.uk/S.M.Goodwin/DOOBS.html`. We explain how this was achieved and the format of the results obtained below.

We wrote a program in GAP4 which computes, for a given G, all B-submodules of $\mathfrak{u}$, then runs DOOBS on each submodule in turn. Our program outputs two files: the first is a LaTeX file which can be used to create a `dvi` or `pdf` file that can be read easily; the second is a text file which one can read into GAP4 and is then easy to search through. In all cases the only characteristic restrictions given by the program were a subset of the bad primes for G.

4.4 When $\mathfrak{u}^{(l)}$ is a prehomogeneous space for B

In this section we consider the question of when a term $\mathfrak{u}^{(l)}$ of the descending central series of $\mathfrak{u}$ is a prehomogeneous space for B. A classification of all instances when B acts on $\mathfrak{u}^{(l)}$ with a dense orbit is given in Theorem 4.4.7 below. We note that in this section we sometimes relax our assumption that G is simple by allowing $G = \mathrm{GL}_n(k)$ or $\mathrm{O}_n(k)$.

We begin by considering the case where G is of classical type; in Theorem 4.4.6 we show that in this case B always acts on $\mathfrak{u}^{(l)}$ with a dense orbit. We begin by introducing some notation that we require to prove a technical lemma, which we use to prove Theorem 4.4.6.

Let $G = \mathrm{GL}_{2n}(k)$, T the maximal torus of diagonal matrices and $B = \mathrm{B}_{2n}(k)$ the Borel subgroup of upper triangular matrices. Let Ψ be the root system of G with respect to T and Π the base of Ψ corresponding to B. Write $\Pi = \{\alpha_1, \dots, \alpha_{2n-1}\}$. For $i \leq j$, we denote $\alpha_i + \cdots + \alpha_j$ by ij. We describe B-submodules $\mathfrak{n}$ of $\mathfrak{u}$ by giving the set of generators $\Gamma(\Psi(\mathfrak{n}))$, see §1.10. For example $\mathfrak{u}$ is described by $\{11, \dots, (2n-1)(2n-1)\}$ and $\mathfrak{u}^{(l)}$ is described by $\{1(l+1), \dots, (2n-1-l)(2n-1)\}$.

For each $l \geq 0$, we define a B-submodule $\mathfrak{n}_l$ of $\mathfrak{u}$. For l even $\mathfrak{n}_l$ has generators

$$\begin{gathered}\{i(i+l) : 1 \leq i \leq n-l-1\} \\ \cup\{i(i+l+1) : n-l \leq i \leq n-1\} \\ \cup\{i(i+l) : n+1 \leq i \leq 2n-l-1\}.\end{gathered}$$

For example, for $n = 5$ and $l = 2$, $\mathfrak{n}_l$ consists of matrices of the form

$$\begin{pmatrix}
\cdot & \cdot & \cdot & * & * & * & * & * & * & * \\
\cdot & \cdot & \cdot & \cdot & * & * & * & * & * & * \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & * & * & * & * \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & * & * & * \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & * & * \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & * & * \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & * \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot
\end{pmatrix}.$$

For l odd $\mathfrak{n}_l$ has generators.

$$\{i(i+l) : 1 \leq i \leq n-l-1\}$$
$$\cup\{i(i+l+1) : n-l \leq i \leq n - \frac{l+3}{2}\}$$
$$\cup\{i(i+l+1) : n - \frac{l-1}{2} \leq i \leq n-1\}$$
$$\cup\{i(i+l) : n+1 \leq i \leq 2n-l-1\}.$$

For example, for $n = 7$ and $l = 3$, $\mathfrak{n}_l$ consists of matrices of the form

$$\begin{pmatrix}
\cdot & \cdot & \cdot & \cdot & * & * & * & * & * & * & * & * & * & * \\
\cdot & \cdot & \cdot & \cdot & \cdot & * & * & * & * & * & * & * & * & * \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & * & * & * & * & * & * & * & * \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & * & * & * & * & * & * \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & * & * & * & * \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & * & * & * & * \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & * & * & * \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & * & * & * \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & * & * \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & * \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\
\cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot
\end{pmatrix}.$$

Lemma 4.4.1 *Assume* $\operatorname{char} k \neq 2$. *Let* Θ *be the semisimple automorphism of* G *such that* $G^\Theta = \mathrm{O}_{2n}(k)$. *For each* $l \geq 0$, *there exists* $X \in \mathfrak{n}_l^\theta$ *such that* $\overline{B \cdot X} = \mathfrak{n}_l$ *and the orbit map* $B \to B \cdot X$ *is separable.*

Proof: Let $l \geq 0$. To simplify notation in this proof we write $a = n - l - 1$, $b = n + \frac{l+3}{2}$, $c = n - \frac{3l+3}{2}$, and $d = n - \frac{l+1}{2}$. We use the strategy described at the end of §4.4.

First we consider the case when l is even. We define $X = (x_{ij}) \in \mathfrak{n}_l$ as follows:

$$\begin{array}{ll} x_{i,i+l+1} = 1 & \text{if } 1 \leq i \leq a \\ x_{i,i+l+2} = 1 & \text{if } a \leq i \leq n \\ x_{i,i+l+1} = 1 & \text{if } n+1 \leq i \leq 2n-l-1 \\ x_{ij} = 0 & \text{otherwise.} \end{array}$$

For example, for $n = 5$ and $l = 2$ we have

$$X = \begin{pmatrix} \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix}.$$

We let $Y = (y_{ij}) \in \mathfrak{b}$ be arbitrary and consider the equations for the y_{ij} in $[Y, X] = 0$. We show that these equations are independent by induction on n the base case $n = 0$ being trivial.

First we consider the case where $n \leq l + 1$. We consider the occurrences of the y_{1j}s in the equations in $[Y, X] = 0$. They occur only in the top row and each entry of the top row of $[Y, X] = 0$ contains a distinct y_{1j}. Therefore, these equations must be independent of the other equations, so we may neglect the equations in the top row. By symmetry we may also neglect the equations in the rightmost column of $[Y, X] = 0$. The remaining equations are equivalent to the analogous equations we get when considering the corresponding case for $\mathrm{GL}_{2n-2}(k)$ which are independent by induction.

Now suppose $n \geq l + 2$. Again we consider the equations of the top row of $[Y, X] = 0$. Each such equation contains a y_{1j} but y_{1a} occurs twice. Further, the only occurrences of the y_{1j}s are in the top row. Now the occurrences of y_{1a} are as $y_{1a} - y_{l+2,n} = 0$ in the $(1, n)$th entry of $[Y, X] = 0$ and $y_{1a} - y_{l+2,n+1} = 0$ in the $(1, n+1)$th entry of $[Y, X] = 0$. The only other occurrence of $y_{l+2,n}$ and $y_{l+2,n+1}$ is in the $(l + 2, n + l + 2)$th entry of $[Y, X] = 0$ where we have $y_{l+2,n} + y_{l+2,n+1} - * = 0$ where $*$ does not involve $y_{l+2,n}$ or $y_{l+2,n+1}$. As $\operatorname{char} k \neq 2$, it follows that the equations on the top row of $[Y, X] = 0$ must be independent of the other equations and so we may neglect them. We may now apply induction as in the previous case.

Therefore, by induction the equations in $[Y,X]=0$ are independent.

Next we consider the case where l is odd. We define $X=(x_{ij})\in\mathfrak{n}_l$ as follows:

$$\begin{array}{ll}
x_{i,i+l+1}=1 & \text{if } 1\le i\le a\\
x_{i,i+l+2}=1 & \text{if } a\le i\le n-\frac{l+3}{2}\\
x_{i,i+l+2}=1 & \text{if } n-\frac{l-1}{2}\le i\le n\\
x_{i,i+l+1}=1 & \text{if } n+1\le i\le 2n-l-1\\
x_{cb}=1 & \\
x_{d,n+\frac{3l+5}{2}}=1 & \\
x_{ij}=0 & \text{otherwise.}
\end{array}$$

For example, for $n=7$ and $l=3$ we have

$$X=\begin{pmatrix}
\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot\\
\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot\\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&1&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot\\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot&\cdot&\cdot\\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1\\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot&\cdot\\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot\\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot&\cdot\\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1&\cdot\\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&1\\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot\\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot\\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot\\
\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot&\cdot
\end{pmatrix}.$$

We let $Y=(y_{ij})\in\mathfrak{b}$ be arbitrary and consider the equations for the y_{ij} in $[Y,X]=0$. As in the l even case, we show that these equations are independent by induction on n, the base case $n=0$ being trivial.

First we consider the case where $n\le l+1$. We look at the top row of $[Y,X]=0$. Apart from the $(1,b)$th entry each equation in the top row contains a y_{1j}. Moreover, there is only one occurrence of each y_{1j}. The $(1,b)$th entry is $y_{l+3,b}=0$ and this is the only occurrence of $y_{l+3,b}$ in $[Y,X]=0$. Therefore, we may neglect the equations in the top row and by symmetry those in the rightmost column of $[Y,X]=0$. Thus we may apply induction as in the proof of the l even case.

Now we consider the case $l+2\le n\le\frac{3l+3}{2}$. As in the previous case each equation in the top row of $[Y,X]=0$ contains a y_{1j} apart from the one in the $(1,b)$th entry. Again this entry is $y_{l+2,b}=0$ and this is the only occurrence of $y_{l+2,b}$. We see that y_{1a} occurs twice in the top row and each other y_{1j} occurs once. We may deal with the y_{1a} as in the proof of the l even case. Therefore, we may neglect the equations in the top row and rightmost column and apply induction.

Now we consider the case $n \geq \frac{3l+5}{2}$. We look at the equations in the top row of $[Y, X] = 0$, we see that each of these contains a y_{1j}. Both y_{1a} and y_{1c} occur twice. The y_{1a} can be dealt with as in the proof of the l even case. We see that y_{1c} occurs in the $(1, d)$th entry of $[Y, X] = 0$ as $y_{1c} - y_{l+2,d} = 0$ and in the $(1, b)$th entry as $y_{1c} - y_{l+2,b} = 0$. Now there is only one other occurrence of $y_{l+2,d}$ and $y_{l+2,b}$ in the $(l+2, n+\frac{3l+5}{2})$th entry of $[Y, X] = 0$ where they occur as $y_{l+2,d} + y_{l+2,b} - * = 0$ where $*$ does not involve $y_{l+2,d}$ or $y_{l+2,b}$. As $\operatorname{char} k \neq 2$ it follows that the equations on the top row of $[Y, X] = 0$ must be independent of the other equations and so we may neglect them. We may now apply induction.

Therefore, by induction the equations in $[Y, X] = 0$ are independent.

In both cases these arguments show that $\overline{B \cdot X} = \mathfrak{n}_l$ by the strategy described at the end of §4.4. We note that using the action of the maximal torus of diagonal matrices, we may assume $X \in \mathfrak{n}_l^\theta$. The separability of the orbit map follows from Remark 1.13.3. $\square$

Remark 4.4.2 Let Φ be the semisimple automorphism of $\mathrm{O}_{2n}(k)$ such that $\mathrm{O}_{2n}(k)^\Phi = \mathrm{O}_{2n-1}(k)$. We note the $X \in \mathfrak{n}_l^\theta$ we get from the proof of Lemma 4.4.1 are elements of $(\mathfrak{n}_l^\theta)^\phi$.

We also require the following easy lemma.

Lemma 4.4.3 *Let $G = \mathrm{GL}_n(k)$ and let B be a Borel subgroup of G. For each $l \geq 0$ there exists $X \in \mathfrak{u}^{(l)}$ with $\overline{B \cdot X} = \mathfrak{u}^{(l)}$ and such that the orbit map $B \to B \cdot X$ is separable.*

Proof: We take B to consist of the upper triangular matrices in G. From [35, Prop. 2.1], we know we can take $X = (x_{ij}) \in \mathfrak{u}^{(l)}$ defined by $x_{i,i+l+1} = 1$ for $1 \leq i \leq n-l-1$ and $x_{ij} = 0$ otherwise. The separability of the orbit map follows from considering $\mathfrak{c}_\mathfrak{b}(X)$ and Remark 1.13.3. $\square$

The following remarks are required in the proof of Theorem 4.4.6, X is as in the proof of Lemma 4.4.3.

Remark 4.4.4 We use the notation of the proof of Lemma 4.4.3. Assume $n = 2m$ is even and Θ is such that $G^\Theta = \mathrm{Sp}_{2m}(k)$. Then we may assume that $X \in (\mathfrak{u}^{(l)})^\theta$.

Remark 4.4.5 Let $H = \mathrm{O}_n(k)$, $G = \mathrm{SO}_n(k)$ and let C be a Borel subgroup of H, and $B = C \cap G$ a Borel subgroup of G. Write U for the unipotent radical of B and V for the unipotent radical of C. We have $\mathfrak{u}^{(l)} = \mathfrak{v}^{(l)}$ for each l, and B has index 2 in C. It follows that B acts on $\mathfrak{u}^{(l)}$ with a dense orbit if and only if C acts on $\mathfrak{v}^{(l)}$ with a dense orbit.

Theorem 4.4.6 *Let G be a simple classical group. Then B admits a dense orbit in each member $\mathfrak{u}^{(l)}$ of the descending central series of $\mathfrak{u}$.*

Proof: The type A case follows from Lemma 4.4.3 and the fact that k is algebraically closed.

Next we consider the type C case. Let $G = \mathrm{Sp}_{2m}(k)$, $H = \mathrm{GL}_{2m}(k)$ and let Θ be the semisimple automorphism of H such that $H^\Theta = G$. Let C be a Borel subgroup of H consisting of the upper triangular matrices in H and $B = C^\Theta$ a Borel subgroup of G. We note that $(\mathfrak{v}^{(l)})^\theta = \mathfrak{u}^{(l)}$ for each l. We may now use Theorem 1.13.2 and Lemma 4.4.3 with Remark 4.4.4 to deduce that for each l there exists $X \in \mathfrak{u}^{(l)}$ such that $\overline{B \cdot X} = \mathfrak{u}^{(l)}$.

Now we consider the type D case. Let $G = \mathrm{O}_{2m}(k)$, $H = \mathrm{GL}_{2m}(k)$ and let Θ be the semisimple automorphism of H such that $H^\Theta = G$. Let C be a Borel subgroup of H consisting of the upper triangular matrices in H and $B = C^\Theta$ a Borel subgroup of G. We now require the technical Lemma 4.4.1. We emphasize that the C-submodules $\mathfrak{n}_l$ of $\mathfrak{c}_u$ from Lemma 4.4.1 are such that $\mathfrak{n}_l^\theta = \mathfrak{u}^{(l)}$ for each l. Therefore, using Lemma 4.4.1 and Theorem 1.13.2, we deduce that for each l there exists $X \in \mathfrak{u}^{(l)}$ such that $\overline{B \cdot X} = \mathfrak{u}^{(l)}$. Now using Remark 4.4.5 we pass from $\mathrm{O}_{2m}(k)$ to $\mathrm{SO}_{2m}(k)$.

Finally, we consider the type B case. Let $G = \mathrm{O}_{2m+1}(k)$, $H = \mathrm{O}_{2m+2}(k)$ and let Φ be the semisimple automorphism of H such that $H^\Phi = G$. Let C be a Borel subgroup of H consisting of the upper triangular matrices in H and $B = C^\Phi$ a Borel subgroup of G. We note that we have $(\mathfrak{v}^{(l)})^\phi = \mathfrak{u}^{(l)}$ for each l. From the proof of the type D case above and Remark 4.4.2 we see there is $X \in \mathfrak{u}^{(l)}$ such that $\overline{C \cdot X} = \mathfrak{v}^{(l)}$. Further using Theorem 1.13.2 we see that the orbit map $C \to C \cdot X$ is separable so we apply Theorem 1.13.2 to get $\overline{B \cdot X} = \mathfrak{u}^{(l)}$ as required. As in the type D case we pass from $\mathrm{O}_{2m+1}(k)$ to $\mathrm{SO}_{2m+1}(k)$ using Remark 4.4.5. $\square$

The computer calculations explained in §4.3 give five instances where $\mathfrak{u}^{(l)}$ is a not a prehomogeneous space for B for G of exceptional type, see also [35, Prop. 2.6] and [28, Thm. 8.1]. Therefore, we get

Theorem 4.4.7 *$\mathfrak{u}^{(l)}$ is a prehomogeneous space for B unless G is of type F_4, E_6 or E_7 and $l = 2$ or G is of type E_8 and $l = 2$ or 4.*

Chapter 5
Conjugacy classes in $U(q)$

In this chapter we use the results of Chapter 3 and 4 along with Proposition 1.8.1 to deduce results about the conjugacy classes of $U(q)$ and the conjugacy classes of $B(q)$ in $U(q)$. Also in §5.3 we prove a result about the number of conjugacy classes in a unipotent normal subgroup of B. We remind the reader that in this chapter we use the notation given in the introduction.

5.1 The $U(q)$-conjugacy classes

Using Propositions 1.8.1 and 3.1.2 we get

Proposition 5.1.1 *Let M be a unipotent normal subgroup of B. The orbits of $U(q)$ in $U(q)/M(q)$ are in correspondence with the F-stable orbits of U in $\mathfrak{u}/\mathfrak{m}$.*

In particular, the conjugacy classes of $U(q)$ are in correspondence with the F-stable adjoint orbits of U in $\mathfrak{u}$.

Proof: By Proposition 2.2.24 the $U(q)$-orbits in $U(q)/M(q)$ correspond to the orbits of $U(q)$ in $\mathfrak{u}(q)/\mathfrak{m}(q)$. Then, by Propositions 1.8.1 and 3.1.2, we see that the orbits of $U(q)$ in $\mathfrak{u}(q)/\mathfrak{m}(q)$ are in correspondence with the F-stable orbits of U in $\mathfrak{u}/\mathfrak{m}$.

The second part of the statement is the case where M is the trivial group. $\square$

As in §3.2, we choose an enumeration $\beta_1, \dots, \beta_N$ of Ψ^+ such that $\beta_j \not\prec \beta_i$ for $i < j$, we define B-submodules $\mathfrak{m}_i$ of $\mathfrak{u}$ by

$$\mathfrak{m}_i = \bigoplus_{j=i+1}^{N} \mathfrak{g}_{\beta_j}.$$

and set $\mathfrak{u}_i = \mathfrak{u}/\mathfrak{m}_i$, for $i = 0, \dots, N$.

We now consider the F-stable orbits of U in $\mathfrak{u}_i$.

Lemma 5.1.2 *Let $X + \mathfrak{m}_i \in \mathfrak{u}_i$ be the $\le_i$-minimal representative of its U-orbit in $\mathfrak{u}_i$. The orbit $U \cdot (X + \mathfrak{m}_i)$ is F-stable if and only if $X + \mathfrak{m}_i \in \mathfrak{u}_i(q)$.*

Proof: It is clear that if $X + \mathfrak{m}_i \in \mathfrak{u}_i(q)$, then $U \cdot (X + \mathfrak{m}_i)$ is F-stable.

If $X+\mathfrak{m}_i$ is $\le_i$-minimal in $U\cdot(X+\mathfrak{m}_i)$, then $F(X+\mathfrak{m}_i)$ is $\le_i$-minimal in $F(U\cdot(X+\mathfrak{m}_i))$. Therefore, if $U \cdot (X + \mathfrak{m}_i)$ is F-stable, then the uniqueness in Proposition 3.2.5 implies that $X + \mathfrak{m}_i \in \mathfrak{u}_i(q)$. $\square$

By Lemma 5.1.2, the conjugacy classes of $U(q)$ correspond to the minimal representatives of the U-orbits in $\mathfrak{u}$ of the form $\sum_{\beta\in\Psi^+} a_\beta e_\beta$ with $a_\beta \in \mathbb{F}_q$ for all $\beta \in \Psi^+$. For instance, in Example 3.3.1 (with $F(x_{ij}) = (x_{ij}^q)$) we have

$$1 + (q-1) + (q-1) + (q-1) + (q-1)^2 + (q-1) + (q-1)^2 = 2q^2 - 1$$

$U(q)$-conjugacy classes.

Our next proposition gives the size of a $U(q)$-orbit in $\mathfrak{u}(q)$.

Proposition 5.1.3 *Let $X + \mathfrak{m}_i \in \mathfrak{u}_i(q)$. Then we have $|U(q) \cdot (X + \mathfrak{m}_i)| = q^{\mathrm{in}_i(X)}$ and $|C_{U(q)}(X + \mathfrak{m}_i)| = q^{N-\mathrm{in}_i(X)}$.*

Proof: We work by induction on i, the base case $i = 0$ being trivial.

Assume by induction that $|U(q) \cdot (X + \mathfrak{m}_{i-1})| = q^{\mathrm{in}_{i-1}(X)}$. Consider the natural map $\pi : (U \cdot (X + \mathfrak{m}_i))^F \to (U \cdot (X + \mathfrak{m}_{i-1}))^F$. Let $Y + \mathfrak{m}_{i-1} \in (U \cdot (X + \mathfrak{m}_{i-1}))^F$ and consider its preimage $\pi^{-1}(Y + \mathfrak{m}_{i-1}) \subseteq (U \cdot (X + \mathfrak{m}_i))^F$. One can see that $|\pi^{-1}(Y + \mathfrak{m}_{i-1})| = q$ if i is an inert point of X and $|\pi^{-1}(Y + \mathfrak{m}_{i-1})| = 1$ if i is a ramification point of X. It follows that $|U(q) \cdot (X + \mathfrak{m}_i)| = q^{\mathrm{in}_i(X)}$.

An application of the formula $|C_{U(q)}(X)| = |U(q)|/|U(q) \cdot X|$ then gives the equality $|C_{U(q)}(X + \mathfrak{m}_i)| = q^{N-\mathrm{in}_i(X)}$. $\square$

5.2 The $B(q)$-conjugacy classes in $U(q)$

We choose an enumeration $\beta_1, \dots, \beta_N$ and define $\mathfrak{m}_i$ and $\mathfrak{u}_i$ as in the previous section.

We have the following analogue of Lemma 5.1.2 which can be proved in exactly the same way.

Lemma 5.2.1 *Let $X + \mathfrak{m}_i \in \mathfrak{u}_i$ be the $\le_i^B$-minimal representative of its U-orbit in $\mathfrak{u}_i$. The orbit $U \cdot (X + \mathfrak{m}_i)$ is F-stable if and only if $X + \mathfrak{m}_i \in \mathfrak{u}_i(q)$.*

It is not always the case that $C_B(X+\mathfrak{m}_i)$ is connected for $X \in \mathfrak{u}$ so it is not the case that the $B(q)$-conjugacy classes in $U(q)$ correspond to the F-stable B-orbits in $\mathfrak{u}$. However, the following proposition implies that, if $X + \mathfrak{m}_i \in \mathfrak{u}_i$ is the $\leq_i^B$-minimal representative of its B-orbit, then to decide how $(B \cdot (X + \mathfrak{m}_i))^F$ splits into $B(q)$-orbits one only needs to consider $C_T(X + \mathfrak{m}_i)$.

Proposition 5.2.2 *Let $X + \mathfrak{m}_i \in \mathfrak{u}_i(q)$ be the $\leq_i^B$-minimal representative of its B-orbit. Then the orbits of $B(q)$ in $(B \cdot (X + \mathfrak{m}_i))^F$ are in correspondence with the elements of $H^1(F, C_T(X + \mathfrak{m}_i)/C_T(X + \mathfrak{m}_i)^0)$.*

Proof: By Propositions 4.1.5 and 3.1.2, we see that

$$C_B(X + \mathfrak{m}_i)^0 = C_U(X + \mathfrak{m}_i)C_T(X + \mathfrak{m}_i)^0.$$

Therefore, we have an isomorphism $C_B(X+\mathfrak{m}_i)/C_B(X+\mathfrak{m}_i)^0 \cong C_T(X+\mathfrak{m}_i)/C_T(X+\mathfrak{m}_i)^0$. The result now follows from Proposition 1.8.1. $\square$

We give an example of when the F-stable points of the B-orbit of $X \in \mathfrak{u}$ do not form a single $B(q)$-orbit.

Example 5.2.3 Let $G = \mathrm{SL}_2(k)$ and assume $\operatorname{char} k \neq 2$. Let F be defined by $F(x_{ij}) = (x_{ij}^q)$, let B be the subgroup of upper triangular matrices in G and let T be the subgroup of diagonal matrices. Let

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

The B-orbit of X is $\{\lambda X : \lambda \in k^\times\}$ and the centralizer of X in T is $C_T(X) = \{\pm 1\}$. We also have $C_T(X)^0 = \{1\}$, so that $C_T(X)$ is disconnected.

One can see that $(B \cdot X)^F$ splits into two $B(q)$-orbits, namely

$$B(q) \cdot X = \{\lambda X : \lambda = \mu^2 \text{ for some } \mu \in \mathbb{F}_q^\times\}$$

and

$$B(q) \cdot \nu X = \{\lambda \nu X : \lambda = \mu^2 \text{ for some } \mu \in \mathbb{F}_q^\times\}$$

where $\nu \in \mathbb{F}_q$ is not a square.

We can also give the sizes of the $B(q)$-orbits in $\mathfrak{u}(q)$.

Proposition 5.2.4 *Let $X + \mathfrak{m}_i \in \mathfrak{u}_i(q)$ be the $\leq_i^B$-minimal representative of its B-orbit. Then*

$$|(B \cdot (X + \mathfrak{m}_i))^F| = (q-1)^{\mathrm{lir}_i(X)} q^{\mathrm{in}_i(X)}$$

and

$$|B(q) \cdot (X + \mathfrak{m}_i)| = (q-1)^{\mathrm{lir}_i(X)} q^{\mathrm{in}_i(X)} / |H^1(F, C_T(X + \mathfrak{m}_i))|.$$

Proof: We begin by proving the first equality by induction on i. The case $i = 0$ is trivial so assume $i \geq 1$ and the equality holds for $i - 1$.

If i is an inert point of X, or i is a ramification point of X and β_i is linearly dependent on $\mathrm{supp}_{i-1}(X)$, then we can argue as in Proposition 5.1.3. So suppose i is a ramification point of X and $\mathrm{lir}_i(X) = \mathrm{lir}_{i-1}(X) + 1$. We may assume the coefficient of e_{β_i} is non-zero otherwise we may again argue as in Proposition 5.1.3. Consider the natural map $\pi : (B \cdot (X + \mathfrak{m}_i))^F \to (B \cdot (X + \mathfrak{m}_{i-1}))^F$. It follows from Lemma 1.7.4 and Lemma 5.2.1 that the fibre of $X + \mathfrak{m}_{i-1}$ has size $q - 1$. Therefore, the fibre of $Y + \mathfrak{m}_{i-1}$ has size $q - 1$ for any Y with $Y + \mathfrak{m}_i$ in the same $B(q)$-orbit as $X + \mathfrak{m}_i$. Now suppose $Y + \mathfrak{m}_i \in (B \cdot (X + \mathfrak{m}_i))^F \setminus (B(q) \cdot (X + \mathfrak{m}_i))$. Then there exists $t \in T$ such that $t \cdot (Y + \mathfrak{m}_i) \in U \cdot (X + \mathfrak{m}_i)$. The factorization of $C_B(Y + \mathfrak{m}_i)$ given in Proposition 4.1.5 implies that $t \cdot (Y + \mathfrak{m}_i)$ is F-stable. It follows that t induces a bijection between the $B(q)$-orbits of $X + \mathfrak{m}_i$ and $Y + \mathfrak{m}_i$. Therefore, we have $|\pi^{-1}(Y + \mathfrak{m}_{i-1})| = q - 1$. Hence, by induction, we have

$$|(B \cdot (X + \mathfrak{m}_i))^F| = (q-1)^{\mathrm{lir}_i(X)} q^{\mathrm{in}_i(X)}.$$

The second equality in the statement of the proposition now follows from Proposition 5.2.2, and the argument above which said that if $Y + \mathfrak{m}_i \in (B \cdot (X + \mathfrak{m}_i))^F$ is not in the $B(q)$-orbit of $X + \mathfrak{m}_i$, then there is some $t \in T$ such that t induces a bijection between $B(q) \cdot (X + \mathfrak{m}_i)$ and $B(q) \cdot (Y + \mathfrak{m}_i)$. □

5.3 Counting conjugacy classes in $U(q)$

In this section we change notation by setting $q_0 = q$, i.e. under an identification $G \subseteq \mathrm{GL}_n(k)$, F is given by $F(x_{ij}) = (x_{ij}^{q_0})$. The reader should note that we will use q in this section to denote some power of q_0.

We consider the number of conjugacy classes of $N(q)$ where N is a subgroup of U normalized by T; by a mild abuse of notation we call such N a regular subgroup of U. We recall from §1.6 that

$$N = \prod_{\beta \in \Psi(N)} U_\beta.$$

We now introduce the notation we require. For each $s \in \mathbb{Z}_{\geq 1}$ we note that $F^s : G \to G$ is a Frobenius morphism. Given a regular subgroup N of U and a power $q = q_0^s$ of q_0 we have $N(q) = N^{F^s}$ and $\mathfrak{n}(q) = \mathfrak{n}^{F^s}$. Since N is a product of root subgroups (and $\mathfrak{n}$ is a direct sum of root subspaces), we note that $|N(q)| = |\mathfrak{n}(q)| = q^{\dim N}$. We denote by $k(N(q))$ the number of conjugacy classes of $N(q)$.

In [59] G.R. Robinson considered the number of conjugacy classes of *algebra subgroups* of $\mathrm{U}_n(q)$. The main result in *loc. cit.* implies that for any regular subgroup N of $\mathrm{U}_n(k)$ the zeta function

$$\zeta_N(t) = \exp\left(\sum_{s \in \mathbb{Z}_{\geq 0}} \frac{k(N(q_0^s))}{s} t^s\right)$$

(in $\mathbb{C}[[t]]$) is a rational function in t whose numerator and denominator may be assumed to be elements of $1 + t\mathbb{Z}[t]$. The main result of this section is the following generalization of Robinson's result.

Theorem 5.3.1 *Let N be a regular subgroup of U. The zeta function*

$$\zeta_N(t) = \exp\left(\sum_{s \in \mathbb{Z}_{\geq 0}} \frac{k(N(q_0^s))}{s} t^s\right)$$

(in $\mathbb{C}[[t]]$) is a rational function in t, whose numerator and denominator may be assumed to be elements of $1 + t\mathbb{Z}[t]$.

In particular, we can apply Theorem 5.3.1 in the case $N = U$.

Remark 5.3.2 As in the remark in [59] we note that $\zeta_N(t)$ being a rational function implies the existence of a recurrence relation for the values of $k(N(q))$. In particular, once $k(N(q))$ is known for a certain finite number of values of q it can be calculated for all q.

Remark 5.3.3 We note that our proof of Theorem 5.3.1 applies in more general settings. For example, if M and N are regular subgroups of U with N normalized by M, then we can prove an analogous result to Theorem 5.3.1 for the number of M-orbits in N.

In the remainder of this section we present a proof of Theorem 5.3.1; we begin by discussing a theorem of B. Dwork which we require for the proof.

Let V be a variety over k that is defined over $\mathbb{F}_{q_0}$. For a power q of q_0, we write $V(q)$ for the $\mathbb{F}_q$-rational points of V. In [20] Dwork proved

Theorem 5.3.4 *The zeta function*

$$\zeta(V;t) = \exp\left(\sum_{s=1}^{\infty} \frac{|V(q_0^s)|}{s} t^s\right)$$

is a rational function of t.

We now give an elementary argument using Theorem 5.3.4 to show that $\zeta_N(t)$ is a rational function of t. Then we show that the numerator and denominator of $\zeta_N(t)$ can be assumed to be elements of $1 + t\mathbb{Z}[t]$.

Consider the commuting variety of N

$$\mathcal{C}(N) = \{(x, y) \in N \times N : xy = yx\};$$

it is defined over $\mathbb{F}_q$ for any power $q = q_0^s$ of q_0 and its $\mathbb{F}_q$-rational points are

$$\mathcal{C}(N)(q) = \{(x, y) \in N(q) \times N(q) : xy = yx\}.$$

We have

$$|\mathcal{C}(N)(q)| = \sum_{x \in N(q)} |C_{N(q)}(x)|.$$

Also the Burnside formula gives

$$k(N(q)) = \frac{1}{|N(q)|} \left(\sum_{x \in N(q)} |C_{N(q)}(x)|\right). \tag{5.3.1}$$

Therefore, writing $c(q) = |\mathcal{C}(N)(q)|$, $k(q) = k(N(q))$ and $m = \dim N$ we have

$$k(q) = \frac{c(q)}{q^m}.$$

We can apply Theorem 5.3.4 to the variety $\mathcal{C}(N)$. Therefore,

$$\zeta(\mathcal{C}(N); t) = \exp\left(\sum_{s=1}^{\infty} \frac{c(q_0^s)}{s} t^s\right)$$

is a rational function of t. We have

$$\zeta_N(t) = \exp\left(\sum_{s=1}^{\infty} \frac{k(q_0^s)}{s} t^s\right) = \exp\left(\sum_{s=1}^{\infty} \frac{c(q_0^s)}{s} \left(\frac{t}{q_0^m}\right)^s\right) = \zeta\left(\mathcal{C}(N); \frac{t}{q_0^m}\right).$$

It follows immediately that $\zeta_N(t)$ is a rational function in t.

We now prove that we may assume the numerator and denominator of $\zeta_N(t)$ are elements of $1 + t\mathbb{Z}[t]$.

We may write

$$\zeta_N(t) = \frac{c\prod_{i=1}^{a}(1-\lambda_i t)^{m_i}}{d\prod_{j=1}^{b}(1-\mu_j t)^{n_j}}, \tag{5.3.2}$$

where c and d are non-zero complex numbers, the λ_i and μ_j are uniquely determined, pairwise distinct, complex numbers, and the m_i and n_j are positive integers. Evaluating both sides of the above expression for $\zeta_N(t)$ at $t = 0$ gives $c = d$, so we may suppose that $c = d = 1$.

Now

$$\begin{aligned}
\frac{\zeta_N'(t)}{\zeta_N(t)} &= \frac{d}{dt}\log\zeta_N(t) = \sum_{s=1}^{\infty} k(N(q_0^s))t^{s-1} \\
&= \frac{d}{dt}\left(\sum_{i=1}^{a} m_i \log(1-\lambda_i t)\right) - \frac{d}{dt}\left(\sum_{j=1}^{b} n_j \log(1-\mu_j t)\right) \\
&= \sum_{i=1}^{a} \frac{-m_i\lambda_i}{1-\lambda_i t} + \sum_{j=1}^{b} \frac{n_j\mu_j}{1-\mu_j t} \\
&= \sum_{i=1}^{a} -m_i\lambda_i\left(\sum_{l=0}^{\infty}\lambda_i^l t^l\right) + \sum_{j=1}^{b} n_j\mu_j\left(\sum_{l=0}^{\infty}\mu_j^l t^l\right) \\
&= \sum_{l=0}^{\infty}\left(\sum_{i=1}^{a} -m_i\lambda_i^{l+1} + \sum_{j=1}^{b} n_j\mu_j^{l+1}\right)t^l.
\end{aligned}$$

This series of equalities implies that

$$k(N(q_0^s)) = \sum_{i=1}^{a} -m_i\lambda_i^s + \sum_{j=1}^{b} n_j\mu_j^s. \tag{5.3.3}$$

for each integer s.

The next lemma is well-known, see for example [59, Lem. 2.2].

Lemma 5.3.5 *Let $\{\alpha_1, \ldots, \alpha_t\}$ be (distinct) elements of some Dedekind domain R, and let π be any ideal of R. Suppose that there are non-zero elements $m_1, \ldots, m_t$ of R such that for each $s \in \mathbb{Z}_{\geq 1}$ we have $\sum_{i=1}^{t} m_i\alpha_i^s \equiv 0 \mod \pi^s$. Then $\alpha_i \in \pi$ for each i.*

Now we prove:

Lemma 5.3.6 *Let $m_1, m_2, \ldots, m_n$ be non-zero integers, and let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be distinct non-zero complex numbers. Suppose that for each positive integer s, we have*

$$\sum_{i=1}^{n} m_i \alpha_i^s \in \mathbb{Z}.$$

Then the α_is are all algebraic integers, and $m_i = m_{i'}$ whenever α_i and $\alpha_{i'}$ are algebraically conjugate.

Proof: We first prove that the α_is are algebraic numbers. Let V be the Van der Monde matrix with (i,j) entry α_j^{i-1}. Let D be the diagonal matrix with ith diagonal entry α_i. Let $\underline{m}$ be the n-long column vector with ith entry m_i. For $s \geq 0$, let $\underline{x}_s$ be the vector $VD^s\underline{m}$, which is integral by hypothesis.

Since the m_is are non-zero (and the α_is are distinct), we see that $\{D^s\underline{m} : 0 \leq s \leq n-1\}$ is a basis for $\mathbb{C}^n$, hence so is $\{\underline{x}_s : 0 \leq s \leq n-1\}$. Since $\underline{x}_n$ is integral, and each $\underline{x}_s$ is integral, we see that $\underline{x}_n$ is a $\mathbb{Q}$-combination of $\{\underline{x}_s : 0 \leq s \leq n-1\}$. Set $T = VDV^{-1}$. Then $\{\underline{x}_s : 0 \leq s \leq n-1\}$ is a $\mathbb{Q}$-basis for $\mathbb{Q}^n$ with respect to which (the linear transformation represented by) T has a rational matrix. Its eigenvalues are therefore algebraic numbers. But the eigenvalues of T are $\{\alpha_i : 1 \leq i \leq n\}$, so the α_i are algebraic numbers, and are closed under algebraic conjugation.

Now there is a least positive integer h such that $h\alpha_i$ is an algebraic integer for each i. We note that $\sum_{i=1}^{n} m_i(h\alpha_i)^s$ is an integer multiple of h^s for each integer s, so by Lemma 5.3.5, we deduce that $h\alpha_i$ is an algebraic integer multiple of h for each i. Hence, each α_i is already an algebraic integer.

The final claim follows by induction on the minimal value of $|m_i|$ since $\{\alpha_i\}$ is closed under algebraic conjugation. $\square$

Lemma 5.3.6 implies that the λ_i and μ_j in (5.3.2) are algebraic integers. Elementary Galois theory then implies that we may assume the numerator and denominator of $\zeta_N(t)$ are elements of $1 + t\mathbb{Z}[t]$.

List of references

[1] C. A. M. André, *Basic characters of the unitriangular group*, J. Algebra **175** (1995), no. 1, 287–319.

[2] ———, *Basic sums of coadjoint orbits of the unitriangular group*, J. Algebra **176** (1995), no. 3, 959–1000.

[3] ———, *On the coadjoint orbits of the unitriangular group*, J. Algebra **180** (1996), no. 2, 587–630.

[4] ———, *The regular character of the unitriangular group*, J. Algebra **201** (1998), no. 1, 1–52.

[5] ———, *The basic character table of the unitriangular group*, J. Algebra **241** (2001), no. 1, 437–471.

[6] ———, *Basic characters of the unitriangular group (for arbitrary primes)*, Proc. Amer. Math. Soc. **130** (2002), no. 7, 1943–1954.

[7] ———, *Hecke algebras for the basic characters of the unitriangular group*, Proc. Amer. Math. Soc. **132** (2004), no. 4, 987–996.

[8] M. Aschbacher, *Finite group theory*, second ed., Cambridge Studies in Advanced Mathematics, vol. 10, Cambridge University Press, Cambridge, 2000.

[9] P. Bala and R. W. Carter, *The classification of unipotent and nilpotent elements*, Indag. Math. **36** (1974), 94–97.

[10] P. Bardsley and R. W. Richardson, *Étale slices for algebraic transformation groups in characteristic p*, Proc. London Math. Soc. (3) **51** (1985), no. 2, 295–317.

[11] A. Borel, *Linear algebraic groups*, second ed., Graduate Texts in Mathematics, vol. 126, Springer-Verlag, New York, 1991.

[12] W. Borho, *Über Schichten halbeinfacher Lie-Algebren*, Invent. Math. **65** (1981/82), no. 2, 283–317.

[13] N. Bourbaki, *Groupes et algèbres de Lie, chapitres 4, 5, et 6*, Hermann, Paris, 1975.

[14] T. Brüstle and L. Hille, *Finite, tame, and wild actions of parabolic subgroups in* GL(V) *on certain unipotent subgroups*, J. Algebra **226** (2000), no. 1, 347–360.

[15] T. Brüstle, L. Hille, and G. Röhrle, *Finiteness for parabolic group actions in classical groups*, Arch. Math. **76** (2001), no. 2, 81–87.

[16] H. Bürgstein and W. H. Hesselink, *Algorithmic orbit classification for some Borel group actions*, Compositio Math. **61** (1987), no. 1, 3–41.

[17] R. W. Carter, *Finite groups of Lie type*, Pure and Applied Mathematics, John Wiley & Sons Inc., New York, 1985.

[18] C. Chevalley, *Sur certains groupes simples*, Tôhoku Math. J. (2) **7** (1955), 14–66.

[19] F. Digne and J. Michel, *Representations of finite groups of Lie type*, London Mathematical Society Student Texts, vol. 21, Cambridge University Press, Cambridge, 1991.

[20] B. Dwork, *On the rationality of the zeta function of an algebraic variety*, Amer. J. Math. **82** (1960), 631–648.

[21] E. B. Dynkin, *Semisimple subalgebras of semisimple Lie algebras*, Mat. Sbornik N.S. **30(72)** (1952), 349–462.

[22] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2004, (`http://www.gap-system.org`).

[23] S. M. Goodwin, *Prehomogeneous spaces for the coadjoint action of a parabolic group*, J. Algebra **279** (2004), no. 2, 558–565.

[24] ———, *Algorithmic testing for dense orbits of Borel subgroups*, J. Pure Appl. Algebra, To appear, 2004.

[25] ———, *On the conjugacy classes in maximal unipotent subgroups of simple algebraic groups*, Transform. Groups, To appear, 2004.

[26] ———, *Relative Springer isomorphisms*, Preprint, The University of Birmingham, 2004.

[27] S. M. Goodwin and G. Röhrle, *Prehomogeneous spaces for parabolic group actions in classical groups*, J. Algebra **276** (2004), no. 1, 383–398.

[28] ———, *Finite orbit modules for parabolic subgroups of exceptional groups*, Indag. Math. **15** (2004), no. 2, 189–207.

[29] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[30] G. Higman, *Enumerating p-groups. I. Inequalities*, Proc. London Math. Soc. (3) **10** (1960), 24–30.

[31] L. Hille, *Minimal infinite configurations for strictly filtered $k[t]/\langle t^n \rangle$-modules and parabolic group actions*, Representations of Algebras, vol. II, Proceedings of ICRA IX, Beijing, 2000.

[32] ______, *Aktionen Algebraischer Gruppen, geometrische Quotienten und Köcher*, Habilitationsschrift, 2002.

[33] L. Hille and G. Röhrle, *On parabolic subgroups of classical groups with a finite number of orbits on the unipotent radial*, C. R. Acad. Sci. Paris Sér. I Math. **325** (1997), no. 5, 465–470.

[34] ______, *A classification of parabolic subgroups of classical groups with a finite number of orbits on the unipotent radical*, Transform. Groups **4** (1999), no. 1, 35–52.

[35] ______, *Variation on a theme of Richardson*, Linear Algebra Appl **365** (2003), 239–246.

[36] D. F. Holt and N. Spaltenstein, *Nilpotent orbits of exceptional Lie algebras over algebraically closed fields of bad characteristic*, J. Austral. Math. Soc. Ser. A **38** (1985), no. 3, 330–350.

[37] J. E. Humphreys, *Introduction to Lie algebras and representation theory*, Graduate Texts in Mathematics, vol. 9, Springer-Verlag, New York, 1978.

[38] ______, *Conjugacy classes in semisimple algebraic groups*, Mathematical Surveys and Monographs, vol. 43, American Mathematical Society, Providence, RI, 1995.

[39] I. M. Isaacs and D. Karagueuzian, *Conjugacy in groups of upper triangular matrices*, J. Algebra **202** (1998), no. 2, 704–711.

[40] J. C. Jantzen, *Nilpotent orbits in representation theory*, Lie theory, Progr. Math., vol. 228, Birkhäuser Boston, Boston, MA, 2004, pp. 1–211.

[41] A. Joseph, *A preparation theorem for the prime spectrum of a semisimple Lie algebra*, J. Algebra **48** (1977), no. 2, 241–289.

[42] U. Jürgens and G. Röhrle, *MOP—algorithmic modality analysis for parabolic group actions*, Experiment. Math. **11** (2002), no. 1, 57–67.

[43] V. V. Kashin, *Orbits of an adjoint and co-adjoint action of Borel subgroups of a semisimple algebraic group*, Problems in group theory and homological algebra (Russian), Matematika, Yaroslav. Gos. Univ., Yaroslavl′, 1990, pp. 141–158.

[44] D. Kazhdan, *Proof of Springer's hypothesis*, Israel J. Math. **28** (1977), no. 4, 272–286.

[45] D. Kazhdan and G. Lusztig, *Representations of Coxeter groups and Hecke algebras*, Invent. Math. **53** (1979), no. 2, 165–184.

[46] A. G. Keeton, *Commuting varieties associated with symmetric pairs*, Ph.D thesis, University of California, San Diego, 1995.

[47] A. A. Kirillov, *Unitary representations of nilpotent Lie groups*, Uspehi Mat. Nauk **17** (1962), no. 4 (106), 57–110.

[48] B. Kostant, *The principal three-dimensional subgroup and the Betti numbers of a complex simple Lie group*, Amer. J. Math. **81** (1959), 973–1032.

[49] G. J. McNinch, *Abelian unipotent subgroups of reductive groups*, J. Pure Appl. Algebra **167** (2002), no. 2-3, 269–300.

[50] D. I. Panyushev, *ad-nilpotent ideals of a Borel subalgebra: generators and duality*, J. Algebra **274** (2004), no. 2, 822–846.

[51] K. Pommerening, *Über die unipotenten Klassen reduktiver Gruppen*, J. Algebra **49** (1977), no. 2, 525–536.

[52] ———, *Über die unipotenten Klassen reduktiver Gruppen. II*, J. Algebra **65** (1980), no. 2, 373–398.

[53] V. Popov and G. Röhrle, *On the number of orbits of a parabolic subgroup on its unipotent radical*, Algebraic groups and Lie groups, Austral. Math. Soc. Lect. Ser., vol. 9, Cambridge Univ. Press, Cambridge, 1997, pp. 297–320.

[54] A. Premet, *Nilpotent orbits in good characteristic and the Kempf-Rousseau theory*, J. Algebra **260** (2003), no. 1, 338–366, Special issue celebrating the 80th birthday of Robert Steinberg.

[55] ———, *Nilpotent commuting varieties of reductive Lie algebras*, Invent. Math. **154** (2003), no. 3, 653–683.

[56] R. W. Richardson, *Conjugacy classes in Lie algebras and algebraic groups*, Ann. of Math. (2) **86** (1967), 1–15.

[57] ———, *Conjugacy classes in parabolic subgroups of semisimple algebraic groups*, Bull. London Math. Soc. **6** (1974), 21–24.

[58] R. W. Richardson, G. Röhrle, and R. Steinberg, *Parabolic subgroups with abelian unipotent radical*, Invent. Math. **110** (1992), no. 3, 649–671.

[59] G. R. Robinson, *Counting conjugacy classes of unitriangular groups associated to finite-dimensional algebras*, J. Group Theory **1** (1998), no. 3, 271–274.

[60] G. Röhrle, *On normal abelian subgroups in parabolic groups*, Ann. Inst. Fourier (Grenoble) **48** (1998), no. 5, 1455–1482.

[61] G. M. Seitz, *Unipotent elements, tilting modules, and saturation*, Invent. Math. **141** (2000), no. 3, 467–502.

[62] J.-P. Serre, *Springer isomorphisms*, Appendix to: G.J. McNinch, *Optimal* SL(2)-*homomorphisms*, arXiv: math.RT/0309385.

[63] T. A. Springer, *A note on centralizers in semi-simple groups*, Indag. Math. **28** (1966), 75–77.

[64] ———, *Some arithmetical results on semi-simple Lie algebras*, Inst. Hautes Études Sci. Publ. Math. (1966), no. 30, 115–141.

[65] ———, *The unipotent variety of a semi-simple group*, Algebraic Geometry (Internat. Colloq., Tata Inst. Fund. Res., Bombay, 1968), Oxford Univ. Press, London, 1969, pp. 373–391.

[66] ———, *Linear algebraic groups*, second ed., Progress in Mathematics, vol. 9, Birkhäuser Boston Inc., Boston, MA, 1998.

[67] T. A. Springer and R. Steinberg, *Conjugacy classes*, Seminar on Algebraic Groups and Related Finite Groups, Lecture Notes in Mathematics, Vol. 131, Springer, Berlin, 1970, pp. 167–266.

[68] R. Steinberg, *Regular elements of semisimple algebraic groups*, Inst. Hautes Études Sci. Publ. Math. (1965), no. 25, 49–80.

[69] ———, *Lectures on Chevalley groups*, Yale University, New Haven, Conn., 1968, Notes prepared by John Faulkner and Robert Wilson.

[70] ———, *Conjugacy classes in algebraic groups*, Springer-Verlag, Berlin, 1974, Notes by Vinay V. Deodhar, Lecture Notes in Mathematics, Vol. 366.

[71] J. Thompson, $k(\mathrm{U}_n(F_q))$, Preprint, `http://www.math.ufl.edu/fac/thompson.html`, 2004.

[72] A. Vera López and J. M. Arregi, *Classes de conjugaison dans les p-sous-groupes de Sylow de* $\mathrm{GL}(n,q)$, C. R. Acad. Sci. Paris Sér. I Math. **310** (1990), no. 3, 81–84.

[73] ———, *Conjugacy classes in Sylow p-subgroups of* $\mathrm{GL}(n,q)$*. II*, Proc. Roy. Soc. Edinburgh Sect. A **119** (1991), no. 3-4, 343–346.

[74] ———, *Conjugacy classes in Sylow p-subgroups of* $\mathrm{GL}(n,q)$, J. Algebra **152** (1992), no. 1, 1–19.

[75] ———, *Conjugacy classes in Sylow p-subgroups of* $\mathrm{GL}(n,q)$*. IV*, Glasgow Math. J. **36** (1994), no. 1, 91–96.

[76] ———, *Some algorithms for the calculation of conjugacy classes in the Sylow p-subgroups of* $\mathrm{GL}(n,q)$, J. Algebra **177** (1995), no. 3, 899–925.

[77] ———, *Polynomial properties in unitriangular matrices*, J. Algebra **244** (2001), no. 1, 343–351.

[78] ———, *Conjugacy classes in unitriangular matrices*, Linear Algebra Appl. **370** (2003), 85–124.

[79] A. Vera López, J. M. Arregi, and F. J. Vera López, *On the number of conjugacy classes of the Sylow p-subgroups of* $\mathrm{GL}(n,q)$, Bull. Austral. Math. Soc. **52** (1995), no. 3, 431–439.