REPRESENTATIONS OF REDUCTIVE GROUPS OVER FINITE LOCAL RINGS OF LENGTH TWO

ALEXANDER STASINSKI AND ANDREA VERA-GAJARDO

Abstract. Let $\mathbb{F}_q$ be a finite field of characteristic p, and let $W_2(\mathbb{F}_q)$ be the ring of Witt vectors of length two over $\mathbb{F}_q$. We prove that for any reductive group scheme $\mathbb{G}$ over $\mathbb{Z}$ such that p is very good for $\mathbb{G} \times \mathbb{F}_q$, the groups $\mathbb{G}(\mathbb{F}_q[t]/t^2)$ and $\mathbb{G}(W_2(\mathbb{F}_q))$ have the same number of irreducible representations of dimension d, for each d. Equivalently, there exists an isomorphism of group algebras $\mathbb{C}[\mathbb{G}(\mathbb{F}_q[t]/t^2)] \cong \mathbb{C}[\mathbb{G}(W_2(\mathbb{F}_q))]$.

1. Introduction

Let $\mathcal{O}$ be a discrete valuation ring with maximal ideal $\mathfrak{p}$ and residue field $\mathbb{F}_q$ with q elements and characteristic p. For an integer $r \geq 1$, we write $\mathcal{O}_r = \mathcal{O}/\mathfrak{p}^r$. Let $\mathcal{O}'$ be a second discrete valuation ring with the same residue field $\mathbb{F}_q$, and define $\mathcal{O}'_r$ analogously. For a finite group G, and an integer $d \geq 1$, let $\operatorname{Irr}_d(G)$ denote the set of isomorphism classes of irreducible complex representations of G of dimension d. It has been conjectured by Onn [19, Conjecture 3.1] (for $\lambda = r^n$, in the notation of [19]) that for all integers $r, n, d \geq 1$, we have

$$\# \operatorname{Irr}_d(\mathrm{GL}_n(\mathcal{O}_r)) = \# \operatorname{Irr}_d(\mathrm{GL}_n(\mathcal{O}'_r)),$$

or equivalently, that there exists an isomorphism of group algebras $\mathbb{C}[\mathrm{GL}_n(\mathcal{O}_r)] \cong \mathbb{C}[\mathrm{GL}_n(\mathcal{O}'_r)]$. This was proved for $r = 2$ by Singla [21]. The conjecture makes sense also when GL_n is replaced by any other group scheme $\mathbb{G}$ of finite type over $\mathbb{Z}$, although in general small primes have to be excluded. The analogous result was proved by Singla [22] for $r = 2$ when $\mathbb{G}$ is either SL_n with $p \nmid n$ or an adjoint form of a classical group of type B_n, C_n or D_n, provided that $p \neq 2$. Regarding the case SL_n when $p \mid n$, see Section 5.

In the present paper, we generalise Singla's results to arbitrary reductive group schemes for which p is a very good prime. More precisely, we prove that for all $d \geq 1$ and any reductive group scheme $\mathbb{G}$ over $\mathbb{Z}$ such that p is a very good prime for $\mathbb{G} \times \mathbb{F}_q := \mathbb{G} \times_{\operatorname{Spec} \mathbb{Z}} \operatorname{Spec} \mathbb{F}_q$, we have

$$\# \operatorname{Irr}_d(\mathbb{G}(\mathcal{O}_2)) = \# \operatorname{Irr}_d(\mathbb{G}(\mathcal{O}'_2)).$$

It is not hard to show that $\mathcal{O}_2$, and indeed any commutative local ring of length two with residue field $\mathbb{F}_q$, must be isomorphic to one of the rings $\mathbb{F}_q[t]/t^2$ or $W_2(\mathbb{F}_q)$ (see Lemma 2.1). From now on, let R be either of these two rings.

Our main result, which we will now explain, is more general than the above result in the sense that it covers a large class of representations when p is arbitrary and all representations when p is very good. As we explain in Section 4.1, every irreducible representation of $\mathbb{G}(R)$ determines a conjugacy orbit of one-dimensional characters ψ_β of the kernel of the canonical map $\rho : \mathbb{G}(R) \to \mathbb{G}(\mathbb{F}_q)$, and the characters ψ_β are parametrised by elements β in the $\mathbb{F}_q$-points of the dual Lie algebra $\operatorname{Lie}(\mathbb{G} \times \mathbb{F}_q)^*$.

For any such β, let $\mathrm{Irr}_d(\mathbb{G}(R) \mid \psi_\beta)$ denote the set of irreducible representations of $\mathbb{G}(R)$ lying above ψ_β and of dimension d.

Let k be an algebraic closure of $\mathbb{F}_q$. Let $G = (\mathbb{G} \times k)(k)$ (a reductive group), and let $\mathfrak{g}^*$ be the dual of its Lie algebra. We have a Frobenius endomorphism $F : G \to G$ corresponding to the $\mathbb{F}_q$-structure on G given by $\mathbb{G} \times \mathbb{F}_q$, and we define a compatible endomorphism F^* on $\mathfrak{g}^*$ such that $(\mathfrak{g}^*)^{F^*} = \mathrm{Lie}(\mathbb{G} \times \mathbb{F}_q)^*$ (see Section 2.2). The pth power map on k gives rise to a bijection $\sigma^* : (\mathfrak{g}^*)^{F^*} \to (\mathfrak{g}^*)^{F^*}$, which is related to Frobenius twists (see Sections 2.3 and 4.1). Our main result is then:

Theorem 1.1. *For any $\beta \in (\mathfrak{g}^*)^{F^*}$ such that p does not divide the order of the component group $C_G(\beta)/C_G(\beta)^\circ$, and any $d \in \mathbb{N}$, we have*

$$\# \mathrm{Irr}_d(\mathbb{G}(\mathbb{F}_q[t]/t^2) \mid \psi_{\sigma^*(\beta)})) = \# \mathrm{Irr}_d(\mathbb{G}(W_2(\mathbb{F}_q)) \mid \psi_\beta).$$

Moreover, if p is good, not a torsion prime for G and if there exists a G-equivariant bijection $\mathfrak{g} \xrightarrow{\sim} \mathfrak{g}^*$, then the above condition on p holds for all β, so that for any $d \in \mathbb{N}$, we have

$$\# \mathrm{Irr}_d(\mathbb{G}(\mathbb{F}_q[t]/t^2)) = \# \mathrm{Irr}_d(\mathbb{G}(W_2(\mathbb{F}_q))).$$

The conditions on p in the theorem hold for example when p is very good for G, or when $G = \mathrm{GL}_n$ (see Section 3.1). The proof builds on all the preceding results of the paper, and is concluded in Section 4.2.

Method of proof and overview of the paper. Our proof of Theorem 1.1 is based on geometric properties of the dual Lie algebra, together with results on centralisers in algebraic groups, and group schemes over local rings. We give an outline of the main steps of the proof, which may also serve as an overview of the contents of the paper. We define a connected algebraic group G_2 over k with a surjective homomorphism $\rho : G_2 \to G$ and a Frobenius map F such that $G_2^F = \mathbb{G}(R)$. For each $\beta \in (\mathfrak{g}^*)^{F^*}$, we want to show that $\# \mathrm{Irr}_d(\mathbb{G}(R) \mid \psi_\beta)$ depends only on structures over $\mathbb{F}_q$ (and not the choice of R with residue field $\mathbb{F}_q$). By elementary Clifford theory (see Lemma 4.2), this will follow if there exists an extension of the character ψ_β to its stabiliser

$$C_{G_2}(f)^F = C_{G_2^F}(f)$$

in G_2^F, where G_2^F acts on $(\mathfrak{g}^*)^{F^*}$ via its quotient G^F and the coadjoint action, and $f = \beta$ or $(\sigma^*)^{-1}(\beta)$ depending on whether $R = \mathbb{F}_q[t]/t^2$ or $W_2(\mathbb{F}_q)$. Most of the paper is devoted to proving the existence of an extension of ψ_β.

First, we use the known fact (Lemma 4.3) that if ψ_β extends to a Sylow p-subgroup of its stabiliser, then it extends to the whole stabiliser. To show that ψ_β extends to a Sylow p-subgroup, we work in the connected reductive group G, as well as a connected algebraic group G_2 over k, which we define using the Greenberg functor, and which is isomorphic (as abstract group) to $\mathbb{G}(k[t]/t^2)$ or $\mathbb{G}(W_2(k))$. We let G^1 denote the kernel of ρ. Our key lemma (Lemma 3.3) says that there exists a closed subgroup H_β of $C_{G_2}(\beta)$ such that $H_\beta G^1$ is a maximal unipotent subgroup of $C_{G_2}(\beta)^\circ$, $H_\beta \cap G^1 = \exp(\mathrm{Lie}(U))$ and $\beta(\mathrm{Lie}(U)) = 0$. Here U is the unipotent radical of a Borel subgroup of G and exp is a certain isomorphism between $\mathrm{Lie}(G)$ and G^1. We show that if p satisfies the conditions of the second part of Theorem 1.1, then p does not divide the order of $C_G(\beta)/C_G(\beta)^\circ$, and hence $H_\beta^{F^n}(G^1)^{F^n}$ is a Sylow p-subgroup of $G_2^{F^n}$ for any power n such that H_β is stable under F^n (see Lemmas 3.4 and 4.4). The properties $H_\beta \cap G^1 = \exp(\mathrm{Lie}(U))$ and

$\beta(\mathrm{Lie}(U)) = 0$ imply that ψ_β is trivial on $(H_\beta \cap G^1)^{F^n}$. Thus, we can extend ψ_β to $H_\beta^{F^n}(G^1)^{F^n}$ by defining the extension to be trivial on $H_\beta^{F^n}$. This implies that ψ_β extends to its stabiliser $C_{G_2}(f)^{F^n}$ in $G_2^{F^n}$, and restricting this extension (which is one-dimensional) to $C_{G_2}(f)^F$, we finally obtain the sought-after extension.

In order to prove Lemma 3.3, we need a couple of geometric lemmas. First, we prove that the union of duals of Borel subalgebras cover the dual Lie algebra (see Lemma 3.1). This is an analogue of a theorem of Grothendieck that the union of Borel subalgebras cover the Lie algebra, but our proof is analogous to one by Borel and Springer. Next, we prove that any maximal connected unipotent subgroup of $C_G(\beta)$ is contained in a maximal unipotent subgroup of G on whose Lie algebra β is zero (see Lemma 3.2). This proof uses the preceding result on the union of dual Borel subalgebras as well as Borel's fixed-point theorem.

Acknowledgement. This work was carried out while the second author held a visiting position at Durham University, supported by Becas Chile. The second author was also supported by Conicyt through PAI/Concurso nacional inserción de capital humano avanzado en la Academia convocatoria 2017 cod. 79170117.

2. Group schemes over local rings and $\mathbb{F}_q$-structures

In this section, we will define the algebraic groups G_2 using reductive group schemes over R and the Greenberg functor. We will also define $\mathbb{F}_q$-rational structures given by Frobenius endomorphisms on G_2 as well as on the Lie algebra of G and its dual. A ring will mean a commutative ring with identity. We begin by characterising local rings of length two:

Lemma 2.1. *Let A be a local ring of length two with maximal ideal $\mathfrak{m}$ and perfect residue field F. Then A is isomorphic to either $F[t]/t^2$ or $W_2(F)$.*

Proof. The exact sequence

$$1 \longrightarrow \mathfrak{m} \longrightarrow A \longrightarrow F \longrightarrow 1$$

implies that the length of $\mathfrak{m}$ is 1 (since the length of F is 1). Thus A cannot have any other proper non-zero ideals than $\mathfrak{m}$, so $\mathfrak{m}$ is principal and $\mathfrak{m}^2 = 0$. Note that A is Artinian, hence complete.

If $\operatorname{char} A = \operatorname{char} F$, Cohen's structure theorem in equal characteristics [3, Theorem 9] implies that $A \cong F[[t]]/I$, for some ideal I. Since every non-zero ideal of $F[[t]]$ is of the form (t^i) and the length of A is two, we must have $I = (t^2)$.

If $\operatorname{char} A \neq \operatorname{char} F$, then $\operatorname{char} F = p$ for some prime p, and we have $p \in \mathfrak{m}$. Note that A is unramified in the sense that $p \notin \mathfrak{m}^2$. Cohen's structure theorem in mixed characteristics [3, Theorem 12] implies that A is a quotient of an unramified complete discrete valuation ring B of characteristic 0 and residue field F. By [20, II, Theorems 3 and 8], $B \cong W(F)$, the ring of Witt vectors over F (this is where the hypothesis that F is perfect is used). Since the length of A is two, it must be the quotient of $W(F)$ by the square of the maximal ideal, that is, $A \cong W_2(F)$. □

From now on, let A be a finite local ring of length two. Then A has finite residue field $\mathbb{F}_q$, for some power q of a prime p, and by the above lemma, A is either $\mathbb{F}_q[t]/t^2$ or $W_2(\mathbb{F}_q)$.

Let $k = \bar{\mathbb{F}}_q$ be an algebraic closure of $\mathbb{F}_q$. All the algebraic groups over k which we will consider will be reduced, and we will identify them with their k-points.

In particular, although centralisers are often non-reduced as group schemes, our notation $C_G(\beta)$ will always refer to the k-points of the reduced subgroup $C_G(\beta)_{\mathrm{red}}$. This makes our notation significantly lighter, especially in Section 3.

Let $\tilde{R} = k[t]/t^2$ if $R = \mathbb{F}_q[t]/t^2$ and $\tilde{R} = W_2(k)$ if $R = W_2(\mathbb{F}_q)$, so that in either case $\tilde{R}$ has residue field k. Let $\mathbb{G}$ be a reductive group scheme over R (we follow [7, XIX, 2.7] in requiring that reductive group schemes have geometrically connected fibres). For a scheme X over $\operatorname{Spec} A$, where A is a ring, and any ring homomorphism $A \to B$, we will (as in Section 1) write $X \times B$, or $X \times_A B$, for $X \times_{\operatorname{Spec} A} \operatorname{Spec} B$.

Define the groups

$$G_2 = \mathcal{F}_{\tilde{R}}(\mathbb{G} \times_R \tilde{R})(k) \qquad \text{and} \qquad G = (\mathbb{G} \times_R k)(k) = \mathbb{G}(k),$$

where $\mathcal{F}_{\tilde{R}}$ is the Greenberg functor with respect to $\tilde{R}$ (see [9]). Then G_2 and G are connected linear algebraic groups, and G_2 is canonically isomorphic to $\mathbb{G}(\tilde{R})$, as abstract groups.

Remark 2.2. The reason for the notation G_2 is that $\tilde{R} = \mathcal{O}/\mathfrak{p}^2$ for some complete discrete valuation ring $\mathcal{O}$ with maximal ideal $\mathfrak{p}$, and $\mathbb{G}$ lifts to a reductive group scheme $\widehat{\mathbb{G}}$ over $\mathcal{O}$, so G_2 sits in a tower of groups $G_r = \mathcal{F}_{\mathcal{O}/\mathfrak{p}^r}(\widehat{\mathbb{G}} \times_{\mathcal{O}} \mathcal{O}/\mathfrak{p}^r)(k)$, for $r \geq 2$. We will not need this.

Let $\rho : G_2 \to G$ be the surjective homomorphism induced by the canonical map $\tilde{R} \to k$, and let G^1 denote the kernel of ρ. By [9, Section 5, Proposition 2 and Corollary 5], ρ is induced on the k-points by a homomorphism

$$\mathcal{F}_{\tilde{R}}(\mathbb{G}) \longrightarrow \mathcal{F}_k(\mathbb{G} \times k) = \mathbb{G} \times k$$

of algebraic groups, so G^1 is closed in G_2. By Greenberg's structure theorem [10, Section 2], G^1 is abelian, connected and unipotent. We will freely use these properties of G^1 in the following.

2.1. **Frobenius endomorphisms.** Let φ be the unique ring automorphism of $\tilde{R}$ which induces the Frobenius automorphism φ_q on the residue field extension $k/\mathbb{F}_q$. In other words, φ is the map which raises coefficients of elements in $k[t]/t^2$ (or coordinates of vectors in $W_2(k)$) to the q-th power. Then the fixed points $\tilde{R}^{\varphi}$ of φ is the ring R.

We have an $\mathbb{F}_q$-rational structure

$$\mathcal{F}_R(\mathbb{G}) \times_{\mathbb{F}_q} k \cong \mathcal{F}_{\tilde{R}}(\mathbb{G} \times_R \tilde{R}),$$

giving rise to a Frobenius endomorphism

$$F : G_2 \longrightarrow G_2$$

such that

$$G_2^F = \mathcal{F}_R(\mathbb{G})(\mathbb{F}_q) \cong \mathbb{G}(R).$$

Under some embedding of $\mathbb{G} \times \tilde{R}$ in an affine space $\mathbb{A}^n_{\tilde{R}}$, the map F is the restriction of the endomorphism on $\mathcal{F}_{\tilde{R}}(\mathbb{A}^n_{\tilde{R}})(k) \cong \mathbb{A}^{2n}_{\tilde{R}}(\tilde{R})$ induced by φ.

Similarly, the $\mathbb{F}_q$-rational structure

$$(\mathbb{G} \times_R \mathbb{F}_q) \times_{\mathbb{F}_q} k \cong \mathbb{G} \times_R \mathbb{F}_q$$

gives rise to a Frobenius endomorphism $F : G \to G$ (note that we use the same notation as for the map on G_2) such that

$$G^F = \mathbb{G}(\mathbb{F}_q)$$

and F is the restriction of the q-th power map under the embedding of $\mathbb{G} \times k$ in $\mathbb{A}^n_k$ corresponding to the embedding of $\mathbb{G} \times \tilde{R}$ in $\mathbb{A}^n_{\tilde{R}}$. Thus, with our notation, ρ is compatible with the Frobenius maps on G_2 and G in the sense that $\rho \circ F = F \circ \rho$, and it follows from this that the kernel G^1 is F-stable.

2.2. **The Lie algebra and its dual.** Consider the reductive group G over k and let $\mathfrak{g} = \mathrm{Lie}(G)$ be its Lie algebra. The $\mathbb{F}_q$-structure $G = (\mathbb{G} \times \mathbb{F}_q) \times k$ gives rise to the $\mathbb{F}_q$-structure

$$\mathfrak{g} = \mathrm{Lie}(\mathbb{G} \times \mathbb{F}_q) \otimes k$$

on $\mathfrak{g}$, and we denote the corresponding Frobenius endomorphism by $F : \mathfrak{g} \to \mathfrak{g}$. The adjoint action

$$\mathrm{Ad} : G \longrightarrow \mathrm{GL}(\mathfrak{g})$$

comes from the adjoint action of $\mathbb{G} \times \mathbb{F}_q$ on $\mathrm{Lie}(\mathbb{G} \times \mathbb{F}_q)$ by extension of scalars (see [6, II, §4, 1.4]), and thus it is compatible with the Frobenius maps in the sense that

$$F(\mathrm{Ad}(g)X) = \mathrm{Ad}(F(g))F(X), \tag{2.1}$$

for $g \in G$ and $X \in \mathfrak{g}$.

Let $\mathfrak{g}^* = \mathrm{Hom}_k(\mathfrak{g}, k)$ be the linear dual of $\mathfrak{g}$ and let

$$\langle \cdot\,, \cdot \rangle : \mathfrak{g}^* \times \mathfrak{g} \longrightarrow k$$

be the canonical pairing given by $\langle f, X \rangle = f(X)$. The k-vector space structure on $\mathfrak{g}^*$ gives rise to a structure of affine space on $\mathfrak{g}^*$, and we will consider $\mathfrak{g}^*$ as a variety with its Zariski topology. We have an endomorphism

$$F^* : \mathfrak{g}^* \longrightarrow \mathfrak{g}^*, \qquad f \longmapsto \varphi_q \circ f \circ F^{-1}.$$

This is compatible with the canonical pairing, in the sense that

$$\langle F^*(f), F(X) \rangle = (F^*(f))(F(X)) = \varphi_q \circ f \circ F^{-1}(F(X)) = \varphi_q \circ f(X) = \varphi_q(\langle f, X \rangle).$$

It follows from this that if $f \in (\mathfrak{g}^*)^{F^*}$ and $X \in \mathfrak{g}^F$, then $\varphi_q(\langle f, X \rangle) = \langle f, X \rangle$, that is, $\langle f, X \rangle \in \mathbb{F}_q$.

We will consider $\mathfrak{g}^*$ with the coadjoint action of G, given by $\mathrm{Ad}^*(g)f = f \circ \mathrm{Ad}^{-1}(g)$, for $g \in G$. The coadjoint action is compatible with F^*, in the sense that

$$F^*(\mathrm{Ad}^*(g)f) = \mathrm{Ad}^*(F(g))F^*(f). \tag{2.2}$$

Indeed, for $X \in \mathfrak{g}$, we have

$$F^*(\mathrm{Ad}^*(g)f)(X) = F^*(f \circ \mathrm{Ad}^{-1}(g))(X) = \varphi_q \circ f \circ \mathrm{Ad}^{-1}(g) \circ F^{-1}(X)$$

and on the other hand, by (2.1),

$$\begin{aligned}(\mathrm{Ad}^*(F(g))F^*(f))(X) &= F^*(f) \circ \mathrm{Ad}^{-1}(F(g))(X) = \varphi_q \circ f \circ F^{-1} \circ \mathrm{Ad}^{-1}(F(g))(X) \\ &= \varphi_q \circ f \circ F^{-1}F(\mathrm{Ad}^{-1}(g)(F^{-1}(X))) \\ &= \varphi_q \circ f \circ \mathrm{Ad}^{-1}(g) \circ F^{-1}(X).\end{aligned}$$

It follows from (2.2) that if $\beta \in (\mathfrak{g}^*)^{F^*}$, then the centraliser $C_G(\beta)$ is F-stable.

2.3. **Frobenius twists and the kernel G^1 .** In order to describe the kernel G^1 and the conjugation action of G_2 when $\tilde{R} = W_2(k)$, we need the notion of Frobenius twists of schemes and representations.

Let $\sigma : k \to k$ be the homomorphism $\lambda \mapsto \lambda^p$, and let k_σ be the k-algebra structure on k given by σ. For any k-vector space M, its *Frobenius twist* is the base change

$$M^{(p)} = M \otimes k_\sigma.$$

For $m \otimes 1 \in M^{(p)}$, $m \in M$, and any $\lambda \in k$, we thus have $\lambda(m \otimes 1) = m \otimes \lambda = \lambda^{1/p} m \otimes 1$. In particular, if $X = \operatorname{Spec} A$, where A is a k-algebra, we have the Frobenius twist

$$X^{(p)} = X \times k_p = \operatorname{Spec} A^{(p)},$$

and the map $A^{(p)} \to A$, $a \otimes \lambda \mapsto \lambda a^p$ gives rise to a morphism $F_X : X \to X^{(p)}$. Any representation $\alpha : G \to \mathrm{GL}(M)$ of G as an algebraic group, induces a representation $\alpha' : G^{(p)} \to \mathrm{GL}(M^{(p)})$, which, on the level of k-points has the effect

$$\alpha'(g')(m \otimes 1) = \alpha(g')m \otimes 1, \qquad \text{for } g' \in G^{(p)}(k), m \in M.$$

Composing α' with the map F_G, we get a representation $\alpha^{(p)}$ of G on $M^{(p)}$, which is the Frobenius twist of α. We have natural bijections

$$X^{(p)}(k) = \operatorname{Hom}_k(A \otimes k_\sigma, k) \cong \operatorname{Hom}_k(A, \operatorname{Hom}_k(k_\sigma, k)) \cong \operatorname{Hom}_k(A, k_\sigma) = X(k_\sigma),$$

where $X(k_\sigma)$ coincides with the points obtained by applying the map $\sigma : X(k) \to X(k)$ induced by σ. On k-points we thus have, for $g \in G(k)$,

$$\alpha^{(p)}(g) \cdot (m \otimes 1) = \alpha^{(p)}(\sigma(g))(m \otimes 1) = \alpha(\sigma(g))m \otimes 1. \tag{2.3}$$

If the module M is defined over $\mathbb{F}_p$, that is, if $M \cong M_0 \otimes_{\mathbb{F}_p} k$, for some $\mathbb{F}_p$-module M_0, then $M^{(p)} \cong (M_0 \otimes k) \otimes k_\sigma \cong M_0 \otimes k = M$ (note that σ is $\mathbb{F}_p$-linear). In this situation, $\alpha^{(p)}$ is isomorphic to the representation $\alpha^{(p)} : G \to \mathrm{GL}(M)$ given by $\alpha^{(p)}(g)m = \alpha(\sigma(g))m$.

In terms of notation, let

$$\begin{cases} \sigma^{(0)} = \mathrm{Id} & \text{if } \tilde{R} = k[t]/t^2, \\ \sigma^{(p)} = \sigma & \text{if } \tilde{R} = W_2(k). \end{cases}$$

Lemma 2.3. *There exists an isomorphism of k-modules* $\exp : \mathfrak{g} \to G^1$ *such that, for $g \in G$, $X \in \mathfrak{g}$, we have*

$$g \exp(X) g^{-1} = \exp(\operatorname{Ad}(\sigma^{(i)}(g))X), \qquad i \in \{0, p\}.$$

Moreover, $\exp \circ F = F \circ \exp$.

Proof. When $\tilde{R} = k[t]/t^2$, the first statement follows from definition of $\mathfrak{g}$ as G^1, together with the corresponding definition of Ad (see, [6, II, §4, 1.2, 1.3 and 4.1]). Assume now that $\tilde{R} = W_2(k)$. By [5, A.6.2, A.6.3], there exists an isomorphism $\exp^{(p)} : G^1 \xrightarrow{\sim} \mathfrak{g}^{(p)}$ (equal to θ_1^{-1} in loc. cit.). The map $i(g) : \mathbb{G} \to \mathbb{G}$, $g \in \mathbb{G}(\tilde{R})$ defined by $h \mapsto ghg^{-1}$ is a homomorphism of $\tilde{R}$-groups, so by [5, A.6.2, A.6.3] applied to $\bar{x} = 1$, it induces the map $d(i(g))^{(p)} = \operatorname{Ad}(g)^{(p)}$ on $\mathfrak{g}^{(p)}$. Thus, we have $g \exp^{(p)}(X) g^{-1} = \exp(\operatorname{Ad}^{(p)}(g)X)$, for $X \in \mathfrak{g}^{(p)}$. Since $\mathbb{G} \times \mathbb{F}_p$ provides an $\mathbb{F}_p$-structure on G, we have an induced $\mathbb{F}_p$-structure on $\mathfrak{g}$, so by the above discussion of Frobenius twists, we have an isomorphism $\mathfrak{g}^{(p)} \cong \mathfrak{g}$, which composed with $\exp^{(p)}$ gives the isomorphism exp satisfying the asserted relation.

Finally, the relation $\exp\circ F = F\circ\exp$ follows in either case by the description of F on the points of G_2 and $\mathfrak{g}$, respectively. □

3. Lemmas on algebraic groups and Lie algebra duals

As before, G will denote a connected reductive group over $k=\overline{\mathbb{F}}_q$. Note however, that Lemmas 3.1 and 3.2 hold for G over an arbitrary algebraically closed field (including characteristic 0).

Let Φ be the set of roots with respect to a fixed maximal torus T of G. Let B be a Borel subgroup of G containing T, determining a set of positive roots Φ^+. Following Kac and Weisfeiler [15] (who attribute this to Springer; see [23, Section 2]), we define

$$\mathfrak{b}^* = \{f\in\mathfrak{g}^* \mid f(\mathrm{Lie}(U))=0\},$$

where U is the unipotent radical of B. Since $\mathfrak{b}^*$ is a linear subspace of $\mathfrak{g}^*$, it is closed.

By a well known result of Borel, G is the union of its Borel subgroups, and an analogous theorem of Grothendieck says that $\mathfrak{g}$ is the union of its Borel subalgebras (i.e., Lie algebras of Borel subgroups); see [2, 14.25] or [7, XIV 4.11]. In [15, Lemma 3.3] the analogous statement for the dual $\mathfrak{g}^*$ is claimed under the hypotheses that $p\neq 2$ and $G\neq \mathrm{SO}(2n+1)$. Since the argument in [15] is short on details and omits non-trivial steps (such as the existence of regular semisimple elements in $\mathfrak{g}^*$ when $p\neq 2$), we give a complete proof for any p and a reductive group G. Note that while Borel's and Grothendieck's theorems hold for any connected linear algebraic group, the dual Lie algebra version does not. For example, for a unipotent group, $\mathfrak{b}^*$ defined as above, would just be 0.

For each $\alpha\in\Phi$, let

$$x_\alpha : k \longrightarrow U_\alpha \subset G$$

be the corresponding isomorphism such that $tx_\alpha(u)t^{-1}=x_\alpha(\alpha(t)u)$ for all $t\in T$, $u\in k$.

Let $X_\alpha : k\to\mathfrak{g}$ denote the differential of x_α, so that $\mathrm{Ad}(t)X_\alpha(u)=X_\alpha(\alpha(t)u)$ for all $t\in T$, $u\in k$. We write

$$e_\alpha := x_\alpha(1), \qquad E_\alpha := X_\alpha(1).$$

Furthermore, we define $E_\alpha^*\in\mathfrak{g}^*$ via

$$\begin{cases} \langle E_\alpha^*, E_{-\alpha}\rangle = 1, & \\ \langle E_\alpha^*, E_\beta\rangle = 0 & \text{if } \beta\neq -\alpha,\\ \langle E_\alpha^*, \mathrm{Lie}(T)\rangle = 0. & \end{cases}$$

It is well known that the Weyl group W of G with respect to T acts on the elements E_α by $w(E_\alpha):=\mathrm{Ad}(\dot w)E_\alpha = E_{w(\alpha)}$, where $\dot w\in N_G(T)$ is a representative of $w\in W$. It also acts on the elements E_α^* by $w(E_\alpha^*):=\mathrm{Ad}^*(\dot w)E_\alpha^*$. We thus have

$$w(E_\alpha^*)(E_\beta) = E_\alpha^*(\mathrm{Ad}(\dot w)^{-1}E_\beta) = E_\alpha^*(E_{w^{-1}(\beta)}) = \begin{cases} 1 & \text{if } -\alpha = w^{-1}(\beta),\\ 0 & \text{otherwise,}\end{cases}$$

and moreover $w(E_\alpha^*)(\mathrm{Lie}(T))=0$ because w preserves $\mathrm{Lie}(T)$. Therefore, since $-\alpha=w^{-1}(\beta)$ is equivalent to $\beta=-w(\alpha)$, we have

$$w(E_\alpha^*) = E_{w(\alpha)}^*.$$

The proof of the following result follows the same lines as [2, 14.23-14.24]. We give the proof here for the sake of completeness.

Lemma 3.1. *The conjugates of* $\mathfrak{b}^*$ *cover* $\mathfrak{g}^*$*, that is,* $\mathfrak{g}^* = \bigcup_{g\in G} \mathrm{Ad}^*(g)\mathfrak{b}^*$.

Proof. First, we prove that there exists an $n \in \mathfrak{b}^*$ such that

$$\{g \in G \mid \mathrm{Ad}^*(g)n \in \mathfrak{b}^*\} = B. \tag{3.1}$$

Let $\Delta \subset \Phi^+$ be a set of simple roots and define

$$n = \sum_{\alpha\in\Delta} E^*_\alpha.$$

Let $g \in \{g \in G \mid \mathrm{Ad}^*(g)n \in \mathfrak{b}^*\}$. By the Bruhat decomposition of G, we may write $g = b'\dot{w}b$, for $b, b' \in B$, $\dot{w} \in N_G(T)$. Since B normalises $\mathfrak{b}^*$, we may assume $b' = 1$. The formula

$$\mathrm{Ad}^*(x_\alpha(u))E^*_\beta = E^*_\beta + \sum_{i\geq 1} c_i u^i E^*_{\beta+i\alpha}, \qquad \text{for all } u \in k,\ \alpha, \beta \in \Phi,\ \beta \neq -\alpha,$$

where $c_i \in k$ (see the third equation in [23, 2.2, (1)]; note the two missing dashes) implies that

$$\mathrm{Ad}^*(b)n - n \in \langle E^*_\alpha \mid \alpha \in \Phi^+,\ \alpha \notin \Delta\rangle.$$

Note that the condition $\alpha \notin \Delta$ above is due to the fact that if $\beta \in \Delta$ and $\alpha \in \Phi^+$, then $\beta + i\alpha \notin \Delta$, for any $i \geq 1$ (since Δ is linearly independent). Thus

$$\mathrm{Ad}^*(g)n = \mathrm{Ad}^*(\dot{w})\Big(n + \sum_{\alpha\in\Phi^+\setminus\Delta} c_\alpha E^*_\alpha\Big),$$

for some $c_\alpha \in k$.

Since w permutes the E^*_α according to $w(E^*_\alpha) = E^*_{w(\alpha)}$, we conclude that

$$\mathrm{Ad}^*(g)n = \sum_{\alpha\in\Delta} E^*_{w(\alpha)} + \sum_{\alpha\in\Phi^+\setminus\Delta} c_\alpha E^*_{w(\alpha)}.$$

Since the sets $\{w(\alpha) \mid \alpha \in \Delta\}$ and $\{w(\alpha) \mid \alpha \in \Phi^+ \setminus \Delta\}$ are disjoint and the E^*_α are linearly independent, the condition $\mathrm{Ad}^*(g) \in \mathfrak{b}^*$ implies that $w(\Delta) \subseteq \Phi^+$. As is well known, this implies that $w = 1$; hence $g \in B$.

Next, consider the morphisms

$$G \times \mathfrak{g}^* \xrightarrow{\varphi_1} G \times \mathfrak{g}^* \xrightarrow{\varphi_2} G/B \times \mathfrak{g}^*,$$

where $\varphi_1(g, f) = (g, \mathrm{Ad}^*(g)f)$ and $\varphi_2(g, f) = (gB, f)$, for any $f \in \mathfrak{g}^*$. Let

$$M = \varphi_2\varphi_1(G \times \mathfrak{b}^*) = \{(gB, f) \mid g \in G,\ \mathrm{Ad}^*(g)^{-1}f \in \mathfrak{b}^*\}.$$

The fibre over gB of the surjective projection $\mathrm{pr}_1 : M \to G/B$ is isomorphic to $\mathrm{Ad}^*(g)\mathfrak{b}^*$, so the dimension of each fibre is $\dim \mathfrak{b}^* = \dim B$. Hence $\dim M = \dim G/B + \dim B = \dim G$. On the other hand, the fibre $\mathrm{pr}_2^{-1}(l)$ of the second projection $\mathrm{pr}_2 : M \to \mathfrak{g}^*$ over any $l \in \mathfrak{g}^*$ is isomorphic to

$$\{gB \mid \mathrm{Ad}^*(g)^{-1}l \in \mathfrak{b}^*\} = \{g \mid \mathrm{Ad}^*(g)^{-1}l \in \mathfrak{b}^*\}/B.$$

It follows from (3.1) that $\mathrm{pr}_2^{-1}(n) = \{1\}$, so in particular, there exist finite non-empty fibres of pr_2 in M. Therefore, since M is irreducible (being the image of the irreducible set $G \times \mathfrak{b}^*$), the fibres of $\mathrm{pr}_2 : M \to \mathfrak{b}^*$ are finite over some dense open set in $\overline{\mathrm{pr}_2(M)}$. Since $\dim M = \dim G = \dim \mathfrak{g}^*$ and $\mathfrak{g}^*$ is connected, it follows that

$\mathrm{pr}_2 : M \to \mathfrak{g}^*$ is dominant. Thus $\mathrm{pr}_2(M) = \bigcup_{g\in G} \mathrm{Ad}^*(g)\mathfrak{b}^*$ contains a dense subset of $\mathfrak{g}^*$.

We show that M is closed in $G/B\times\mathfrak{g}^*$. If $\mathrm{Ad}^*(g)^{-1}f \in \mathfrak{b}^*$, then $\mathrm{Ad}^*(gb)^{-1}f \in \mathfrak{b}^*$, for all $b \in B$, so $\varphi_2^{-1}(M) = \varphi_1(G \times \mathfrak{b}^*)$. Thus, since φ_1 is an isomorphism of varieties, $\varphi_2^{-1}(M)$ is closed. Since $\varphi_2 : G \times \mathfrak{g}^* \to (G \times \mathfrak{g}^*)/(B \times \{0\})$ is a quotient morphism (hence open), the set

$$\varphi_2(G \times \mathfrak{g}^* \setminus \varphi_2^{-1}(M)) = (G/B \times \mathfrak{g}^*) \setminus M$$

is open, so M is closed.

Finally, since G/B is a complete variety, the image of M under the projection $\mathrm{pr}_2 : G/B\times\mathfrak{g}^* \to \mathfrak{g}^*$ is closed. But $\mathrm{pr}_2(M) = \bigcup_{g\in G} \mathrm{Ad}^*(g)\mathfrak{b}^*$, which we have shown is dense in $\mathfrak{g}^*$. Thus $\bigcup_{g\in G} \mathrm{Ad}^*(g)\mathfrak{b}^*$ is closed and dense, so $\mathfrak{g}^* = \bigcup_{g\in G} \mathrm{Ad}^*(g)\mathfrak{b}^*$. □

In the following lemma, the proof follows the lines of the first part of the proof of ii) on p. 143 of [15], but in addition, we also provide a proof of the fact that X is closed in G/B.

Lemma 3.2. *Let $\beta \in \mathfrak{g}^*$, B_β be a Borel subgroup of $C_G(\beta)$ and U_β be the unipotent radical of B_β. Then there exists a Borel subgroup of G with unipotent radical V such that*

$$U_\beta \subseteq V \qquad \textit{and} \qquad \beta(\mathrm{Lie}(V)) = 0.$$

Proof. Let B be a fixed Borel subgroup of G with unipotent radical U, and define the set

$$X = \{gB \in G/B \mid \beta(\mathrm{Ad}(g)\,\mathrm{Lie}(U)) = 0\}.$$

We then have $X = \{gB \in G/B \mid \mathrm{Ad}^*(g)^{-1}\beta \in \mathfrak{b}^*\}$, and we note that X is non-empty thanks to Lemma 3.1 (this will be crucial for the application of Borel's fixed-point theorem below).

We show that X is closed in G/B. Let $M = \{(gB, f) \mid g \in G,\ \mathrm{Ad}^*(g)^{-1}f \in \mathfrak{b}^*\}$ and $\mathrm{pr}_2 : M \to \mathfrak{g}^*$ be as in the proof of Lemma 3.1. We have

$$\mathrm{pr}_2^{-1}(\beta) = \{(gB, \beta) \in G/B \times \{\beta\} \mid \mathrm{Ad}^*(g)^{-1}\beta \in \mathfrak{b}^*\},$$

so $\mathrm{pr}_2^{-1}(\beta)$ is closed in M since β is a closed point. Moreover, we have proved that M is closed in $G/B \times \mathfrak{g}^*$, so $\mathrm{pr}_2^{-1}(\beta)$ is closed in $G/B \times \mathfrak{g}^*$. To conclude that X is closed in G/B, it remains to note that the map $\lambda : G/B \to G/B \times \mathfrak{g}^*$ given by $\lambda(gB) = (gB, \beta)$ is a morphism of varieties, and that

$$\lambda^{-1}(\mathrm{pr}_2^{-1}(\beta)) = \{gB \mid \mathrm{Ad}^*(g)^{-1}\beta \in \mathfrak{b}^*\} = X.$$

Now, since X is closed in the complete variety G/B, it is itself complete. Any subgroup of $C_G(\beta)$ acts on X, because for $gB \in X$ and $h \in C_G(\beta)$ we have

$$\beta(\mathrm{Ad}(hg)\,\mathrm{Lie}(U)) = (\mathrm{Ad}^*(h^{-1})\beta)(\mathrm{Ad}(g)\,\mathrm{Lie}(U)) = \beta(\mathrm{Ad}(g)\,\mathrm{Lie}(U)) = 0,$$

so $hgB \in X$. Thus B_β acts on X and since it is a connected solvable group, Borel's fixed-point theorem implies that there exists a $gB \in X$ such that $hgB = gB$, for all $h \in B_\beta$; thus $B_\beta \subseteq gBg^{-1}$. Setting $V = gUg^{-1}$ we then have $U_\beta \subseteq V$, and

$$\beta(\mathrm{Lie}(V)) = \beta(\mathrm{Ad}(g)\,\mathrm{Lie}(U)) = 0.$$

□

We recall that maximal unipotent subgroups of a connected linear algebraic group over k coincide with unipotent radicals of Borel subgroups (see [12, 30.4], where one immediately reduces to reductive groups by taking unipotent radicals). For an algebraic group H, we let H° denote the connected component of the identity.

Lemma 3.3. *For any $\beta \in \mathfrak{g}^*$ there exists a closed subgroup H_β of $C_{G_2}(\beta)^\circ$ and a maximal unipotent subgroup U of G such that:*

(i) $H_\beta G^1$ *is a maximal unipotent subgroup of* $C_{G_2}(\beta)^\circ$,
(ii) $H_\beta \cap G^1 = \exp(\mathrm{Lie}(U))$,
(iii) $\beta(\mathrm{Lie}(U)) = 0$.

Proof. Let U_β be a maximal unipotent subgroup of $C_G(\beta)^\circ$. Then U_β is the unipotent radical of a Borel subgroup of $C_G(\beta)^\circ$ (so, in particular, U_β is connected). By Lemma 3.2 there exists a Borel subgroup B of G with unipotent radical U containing U_β, and such that $\beta(\mathrm{Lie}(U)) = 0$. Given this U, it will therefore be enough to prove the existence of an H_β such that (i) and (ii) hold.

By [7, XXVI, 3.5] (see also [7, XXVI,7.15]), there exists a Borel subgroup scheme $\mathbb{B}$ of $\mathbb{G}$ over $\mathcal{O}_2^{\mathrm{ur}}$ such that $\mathbb{B} \times k = B$. Let $\mathbb{U}$ be the unipotent radical of $\mathbb{B}$ (see [7, XXII, 5.11.4 (ii)] as well as [4, 5.2.5]), so that $\mathbb{U} \times k = U$. Let $U_2 = \mathcal{F}(\mathbb{U})$ be the Greenberg transform, and define

$$H_\beta = U_2 \cap C_{G_2}(\beta)^\circ.$$

Let $u \in U \cap C_G(\beta)^\circ$. Since $\mathbb{U}$ is smooth, there exists an element $\hat{u} \in U_2$ such that $\rho(\hat{u}) = u$, and since $C_{G_2}(\beta)^\circ = \rho^{-1}(C_G(\beta)^\circ)$, we must have $\hat{u} \in C_{G_2}(\beta)^\circ$, so that $\hat{u} \in H_\beta$. Thus

$$\rho(H_\beta) = \rho(U_2 \cap C_{G_2}(\beta)^\circ) = U \cap C_G(\beta)^\circ = U_\beta.$$

Since G^1 is unipotent, normal in G and $\rho(H_\beta G^1) = U_\beta$, it follows that $H_\beta G^1$ is a maximal unipotent subgroup of $C_{G_2}(\beta)^\circ$, proving (i).

Next, since $C_{G_2}(\beta)^\circ$ contains G^1, we have

$$H_\beta \cap G^1 = U_2 \cap G^1 = \mathrm{Ker}(\rho : \mathbb{U}(\mathcal{O}_2^{\mathrm{ur}}) \to \mathbb{U}(k)) = \exp(\mathrm{Lie}(U)),$$

proving (ii). Finally, as we have already noted, $\beta(\mathrm{Lie}(U)) = 0$ holds by our choice of U, so (iii) holds. □

3.1. **Very good primes and component groups of centralisers .** We recall the notions of good and very good primes. If H is a connected almost simple group over k, the prime $p = \mathrm{char}\, k$ is *good* for H if any of the following conditions hold:

- H is of type A_n,
- H is of type B_n, C_n or D_n and $p \neq 2$,
- H is of type G_2, F_4, E_6 or E_7 and $p > 3$,
- H is of type E_8 and $p > 5$,

(see, for example, [24, I, 4] or [16, Definition 2.5.2]). If, moreover, p does not divide $n+1$ whenever H is of type A_n, then p is said to be *very good* for H (see, for example, [16, Definition 2.5.5]). There is also a notion of torsion prime for H due to Steinberg [26] (cf. [16, Definition 2.5.4]). If p is very good for H, then it is not a torsion prime for H (see [16, Remark 2.5.6]). Now let G' be the derived group of the reductive group G. Then G' is semisimple and p is said to be good/very good/torsion for G if p is good/very good/torsion for each of the simple components of G'.

If there exists a G-equivariant bijection $\mathfrak{g}\xrightarrow{\sim}\mathfrak{g}^*$, then each centraliser of an element in $\mathfrak{g}^*$ equals a centraliser of an element in $\mathfrak{g}$. Such a bijection exists when there exists a non-degenerate G-invariant bilinear form on $\mathfrak{g}$, and this is always the case when p is very good for G (see [16, Proposition 2.5.12]).

For $\beta \in \mathfrak{g}^*$, let $A(\beta)$ denote the component group $C_G(\beta)/C_G(\beta)^\circ$. Note that since G^1 is connected and normal in G, we have

$$C_{G_2}(\beta)/C_{G_2}(\beta)^\circ \cong C_G(\beta)/C_G(\beta)^\circ = A(\beta). \tag{3.2}$$

Lemma 3.4. *Assume that p is good and not a torsion prime for G, and that there exists a G-equivariant bijection $\mathfrak{g} \xrightarrow{\sim} \mathfrak{g}^*$ (e.g., these conditions hold when p is very good for G, or when $G = \mathrm{GL}_n$). Then, for any $\beta \in \mathfrak{g}^*$, p does not divide $|A(\beta)|$.*

Proof. Using the G-equivariant bijection $\mathfrak{g}^* \xrightarrow{\sim} \mathfrak{g}$, we may replace β by an element $X \in \mathfrak{g}$. We reduce to centralisers of nilpotent elements in the standard way: Let $X = X_s + X_n$ be the Jordan decomposition of X, where X_s is semisimple and X_n is nilpotent. Uniqueness of Jordan decomposition implies that $C_G(X) = C_{C_G(X_s)}(X_n)$. Since p is not torsion for G, [26, Theorem 3.14] implies that $C_G(X_s)$ is connected. Moreover, by [16, Proposition 2.6.4], it is reductive. By [17, Proposition 16], p is good (but not necessarily very good) for $C_G(X_s)$, and $X_s \in C_{\mathfrak{g}}(X_s) = \mathrm{Lie}(C_G(X_s))$ (since $C_G(X_s)$ is smooth; see [13, Proposition 1.10]) so we are reduced to proving the lemma in the case when p is good for G and β is replaced by a nilpotent element in $\mathfrak{g}$.

Assume that p is good for G and let $X \in \mathfrak{g}$ be nilpotent. By [17, Proposition 5], there exists a G-equivariant bijection between the nilpotent variety in $\mathfrak{g}$ and the unipotent variety in G. Thus $C_G(X) = C_G(u)$, for some unipotent element $u \in G$. By [24, III, 3.15] (see [17, Proposition 12, Corollary 13] for the extension to reductive groups), every element in the component group $A(u)$ of $C_G(u)$ is represented by a semisimple element in $C_G(u)$. By Jordan decomposition, the image of a semisimple element under a homomorphism of affine algebraic groups is semisimple, and semisimple elements in a finite group like $A(u)$ are exactly the p'-elements, that is, elements not divisible by p. Thus the group $A(u)$ has no element of order p. The lemma follows. □

Remark 3.5. (a) We do not know whether the converse of Lemma 3.4 holds. The hypotheses on p in the lemma imply that p is a pretty good prime for G (see [11]). Indeed, assume for simplicity that G is simple with root system Φ and dual root system $\Phi^\vee$ (with respect to some maximal torus). Then p is good for G if $\mathbb{Z}\Phi/\mathbb{Z}\Phi'$ has no p-torsion, for any closed subsystem Φ' (see [24, I, 4]). Moreover, p is not a torsion prime for G if $\mathbb{Z}\Phi^\vee/\mathbb{Z}\Phi'^\vee$ has no p-torsion, for any Φ', and if p does not divide the order of the fundamental group $\pi_1(G)$ (see [16, Definition 2.5.4]). By [11, proof of Lemma 2.12 (a)], the assumption that p is good and $\mathbb{Z}\Phi^\vee/\mathbb{Z}\Phi'^\vee$ has no p-torsion for any Φ' is equivalent to p being pretty good for G. Thus, the hypotheses in Lemma 3.4 are equivalent to p being pretty good, not dividing the order of $\pi_1(G)$ and such that there exists a G-equivariant bijection $\mathfrak{g} \xrightarrow{\sim} \mathfrak{g}^*$.

(b) In general, many elements $\beta \in \mathfrak{g}^*$ satisfy the conclusion of Lemma 3.4, even when some of the hypotheses of the lemma fail. For example, take any G-invariant bilinear (but not necessarily non-degenerate) form $\langle\,\cdot\,,\,\cdot\,\rangle$ on $\mathfrak{g}$. Then $X \mapsto \langle X,\,\cdot\,\rangle$ defines a G-equivariant map $\mathfrak{g} \to \mathfrak{g}^*$, and every element in $\mathfrak{g}^*$ in the image of this map will satisfy the conclusion of the lemma whenever p is a good and non-torsion for G. For example, when $G = \mathrm{SL}_n$ and $\langle\,\cdot\,,\,\cdot\,\rangle$ is the trace form, this applies for any p (in particular, when $p \mid n$).

On the other hand, when $G = \mathrm{SL}_n$ and $p \mid n$, the conclusion of Lemma 3.4 does not hold in general, even though p is good and non-torsion for G. For example, when $p = n = 2$, $\mathfrak{g}^*$ may be identified with $\mathrm{M}_2(k)/Z$, where $\mathrm{M}_2(k)$ is the 2×2 matrices and Z is the subalgebra of scalar matrices. It is easy to see that when $\beta = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, the component group of $C_G(\beta + Z)$ has order 2.

4. Representations

4.1. **Clifford theory set up.** For a finite group Γ, we will write $\mathrm{Irr}(\Gamma)$ for the set of irreducible complex representations of Γ (up to isomorphism). If $\Gamma' \subseteq \Gamma$ is a subgroup and ρ is a representation of Γ', we will write $\mathrm{Irr}(\Gamma \mid \rho)$ for the subset of $\mathrm{Irr}(\Gamma)$ consisting of representations which have ρ as an irreducible constituent when restricted to Γ. Recall the notation introduced in Section 2.

Fix a non-trivial irreducible character $\psi : \mathbb{F}_q \to \mathbb{C}^\times$. For $\beta \in (\mathfrak{g}^*)^{F^*}$, define the character $\psi_\beta \in \mathrm{Irr}((G^1)^F)$ by

$$\psi_\beta(\exp(X)) = \psi(\langle \beta, X\rangle), \qquad \text{for } X \in \mathfrak{g}^F$$

Note that here $\langle \beta, X\rangle \in \mathbb{F}_q$ and also, $\exp(\mathfrak{g}^F) = (G^1)^F$ by Lemma 2.3. Recall the notation $\sigma^{(i)}$ from Section 2.3.

Lemma 4.1. *The function $\beta \mapsto \psi_\beta$ defines an isomorphism of abelian groups $(\mathfrak{g}^*)^{F^*} \to \mathrm{Irr}((G^1)^F)$ and for any $g \in G_2^F$, we have*

$$\mathrm{Ad}^*(\sigma^{(i)}(g))\beta \longmapsto \psi_\beta^g, \qquad \textit{for } i \in \{0, p\},$$

where G_2^F acts on $(\mathfrak{g}^*)^{F^*}$ via its quotient G^F, that is, $\mathrm{Ad}^*(g)\beta = \mathrm{Ad}^*(\bar{g})\beta$, where $\bar{g} = \rho(g)$.

Proof. The function $\beta \mapsto \psi_\beta$ is an additive injective homomorphism because of the linearity (in the first variable) and non-degeneracy of the form $\langle\,\cdot\,,\,\cdot\,\rangle$, respectively. Moreover, by Lemma 2.3, $\exp(\mathrm{Ad}(\sigma^{(i)}(\bar{g}))X) = g\exp(X)g^{-1}$, so for any $X \in \mathfrak{g}$, we have

$$\begin{aligned}\psi_{\mathrm{Ad}^*(\sigma^{(i)}(g))\beta}(\exp(X)) &= \psi(\langle \mathrm{Ad}^*(\sigma^{(i)}(g))\beta, X\rangle) = \psi(\langle \beta, \mathrm{Ad}^*(\sigma^{(i)}(\bar{g}^{-1}))X\rangle) \\ &= \psi_\beta(\exp(\mathrm{Ad}^*(\sigma^{(i)}(\bar{g}^{-1}))X)) = \psi_\beta(g^{-1}\exp(X)g) \\ &=: \psi_\beta^g(\exp(X)).\end{aligned}$$

□

Just like F, the map σ induces an endomorphism σ^* on $\mathfrak{g}^*$, and it follows immediately from the preceding lemma, together with the formula $\sigma^*(\mathrm{Ad}^*(\bar{g})\beta) = \mathrm{Ad}^*(\sigma(\bar{g}))\sigma^*(\beta)$, that the stabiliser of ψ_β in G_2^F is

$$\{g \in G_2^F \mid \mathrm{Ad}^*(\sigma^{(i)}(\bar{g}))\beta = \beta\} = \begin{cases} C_{G_2}(\beta)^F & \text{if } \tilde{R} = k[t]/t^2, \\ C_{G_2}((\sigma^*)^{-1}(\beta))^F & \text{if } \tilde{R} = W_2(k). \end{cases} \tag{4.1}$$

Here, as elsewhere, we take centralisers with respect to the coadjoint action (not its Frobenius twist). Recall from Section 2.2 that $\beta \in (\mathfrak{g}^*)^{F^*}$ implies that $C_{G_2}(\beta)$ and $C_G(\beta)$ are F-stable. The map σ^* is bijective and commutes with F^*, so it restricts to a bijection $\sigma^* : (\mathfrak{g}^*)^{F^*} \to (\mathfrak{g}^*)^F$.

The following is an immediate consequence of well known results in Clifford theory [14, 6.11, 6.17]:

Lemma 4.2. *Let $\beta \in (\mathfrak{g}^*)^{F^*}$ and assume that ψ_β has an extension $\tilde{\psi}_\beta \in \operatorname{Irr}(C_{G_2}(\beta)^F)$. Then there is a bijection*

$$\operatorname{Irr}(C_{G_2}(\beta)^F/(G^1)^F) \longrightarrow \operatorname{Irr}(G_2^F \mid \psi_\beta)$$
$$\theta \longmapsto \pi(\theta) := \operatorname{Ind}_{C_{G_2}(\beta)^F}^{G_2^F}(\theta\tilde{\psi}_\beta).$$

Thus

$$\#\operatorname{Irr}(G_2^F \mid \psi_\beta) = |C_{G_2}(\beta)^F/(G^1)^F| = |C_G(\beta)^F|$$

and

$$\dim\pi(\theta) = [G_2^F : C_{G_2}(\beta)^F]\cdot\dim\theta = [G^F : C_G(\beta)^F]\cdot\dim\theta.$$

In the following, we will prove that an extension of ψ_β to its stabiliser exists for any $\beta \in (\mathfrak{g}^*)^{F^*}$, under suitable hypotheses.

4.2. **Proof of the main theorem.** We will use the following lemma (see [25, Lemma 4.8]):

Lemma 4.3. *Let M be a finite group, N a normal p-subgroup, and P a Sylow p-subgroup of M. Suppose that $\chi \in \operatorname{Irr}(N)$ is stabilised by M and that χ has an extension to P. Then χ has an extension to M.*

The Sylow p-subgroup we will apply the above lemma to is given by the following result.

Lemma 4.4. *Let β and H_β be as in Lemma 3.3. Let $m \geq 1$ be an integer such that H_β is F^m-stable. Then $(H_\beta G^1)^{F^m}$ is a Sylow p-subgroup of $(C_{G_2}(\beta)^\circ)^{F^m}$. Moreover, if p does not divide $|A(\beta)|$, then $(H_\beta G^1)^{F^m}$ is a Sylow p-subgroup of $C_{G_2}(\beta)^{F^m}$.*

Proof. The first statement follows from Lemma 3.3 (i) together with [8, Proposition 3.19 (i)]. For the second statement, note that

$$[C_{G_2}(\beta)^{F^m} : (H_\beta G^1)^{F^m}] = [C_{G_2}(\beta)^{F^m} : (C_{G_2}(\beta)^\circ)^{F^m}]\cdot[(C_{G_2}(\beta)^\circ)^{F^m} : (H_\beta G^1)^{F^m}]$$

and $C_{G_2}(\beta)^{F^m}/(C_{G_2}(\beta)^\circ)^{F^m} \cong (C_{G_2}(\beta)/C_{G_2}(\beta)^\circ)^{F^m} = A(\beta)^{F^m}$ (see [8, Corollary 3.13] and (3.2)), so if $p \nmid |A(\beta)|$, then $p \nmid [C_{G_2}(\beta)^{F^m} : (C_{G_2}(\beta)^\circ)^{F^m}]$, hence $p \nmid [C_{G_2}(\beta)^{F^m} : (H_\beta G^1)^{F^m}]$. □

The purpose of the geometric lemmas in Section 3 is to prove the following result, from which our main theorem immediately follows.

Proposition 4.5. *Let $\beta \in (\mathfrak{g}^*)^{F^*}$ and assume that p does not divide $|A(\beta)|$. Then the character ψ_β has an extension $\tilde{\psi}_\beta$ to $C_{G_2}(\beta)^F$.*

Proof. Let H_β and U be as in Lemma 3.3. Then H_β (like any algebraic group over k) is defined over some finite extension of $\mathbb{F}_q$, or equivalently, it is stable under some power F^m, $m \geq 1$ of the Frobenius F. Since G^1 is F-stable, the group $H_\beta G^1$ is F^m-stable. By Lemma 3.3 (i), the group $H_\beta G^1$ is maximal unipotent in $C_{G_2}(\beta)^\circ$. Thus, given our hypothesis on p, Lemma 4.4 implies that $(H_\beta G^1)^{F^m}$ is a Sylow p-subgroup of $C_{G_2}(\beta)^{F^m}$.

Next, we show that ψ_β extends to $(H_\beta G^1)^{F^m}$. We claim that

$$(H_\beta G^1)^{F^m} = H_\beta^{F^m}(G^1)^{F^m}.$$

Indeed, the map $\rho : G_2 \to G$ is compatible with any power F^m on G_2 and G, respectively, so ρ maps $(H_\beta G^1)^{F^m}$ surjectively onto $U_\beta^{F^m}$, where U_β is the maximal connected unipotent subgroup of $C_{G_1}(\beta)^\circ$. Since $G^1 \cap (H_\beta G^1)^{F^m} = (G^1)^{F^m}$, the kernel is $(G^1)^{F^m}$. Similarly, ρ maps $H_\beta^{F^m}(G^1)^{F^m}$ surjectively onto $U_\beta^{F^m}$, with kernel $(G^1)^{F^m}$. Thus, the finite groups $H_\beta^{F^m}(G^1)^{F^m}$ and $(H_\beta G^1)^{F^m}$ have the same order, so the natural inclusion of the former into the latter is an isomorphism.

Let ψ_m be an extension of ψ to the additive group of the field of definition of H_β. The formula $\psi_{\beta,m}(\exp(x)) = \psi_m(\langle\beta, x\rangle)$, for $x \in \mathfrak{g}^{F^m}$ defines an extension $\psi_{\beta,m}$ of ψ_β to $(G^1)^{F^m}$. We now show that $\psi_{\beta,m}$ extends to a character of $H_\beta^{F^m}(G^1)^{F^m}$ which is trivial on $H_\beta^{F^m}$. Since $H_\beta^{F^m}$ is a subgroup of the stabiliser $C_{G_2}(\beta)^{F^m}$ of $\psi_{\beta,m}$, it is easy to see that such an extension exists if $\psi_{\beta,m}$ is trivial on $H_\beta^{F^m} \cap (G^1)^{F^m}$. Now,

$$H_\beta^{F^m} \cap (G^1)^{F^m} \subseteq (U_2 \cap G^1)^{F^m} = \exp(\operatorname{Lie} U)^{F^m}$$

(note that U_2 and U as in the proof of Lemma 3.3 are stable under F^m since H_β and $C_{G_2}(\beta)^\circ$ are), and hence

$$\psi_{\beta,m}(H_\beta^{F^m} \cap (G^1)^{F^m}) \subseteq \psi_m(\langle\beta, (\operatorname{Lie} U)^{F^m}\rangle) = \psi_m(\{0\}) = \{1\},$$

by Lemma 3.3 (iii). Thus $\psi_{\beta,m}$ extends to $H_\beta^{F^m}(G^1)^{F^m} = (H_\beta G^1)^{F^m}$, so by Lemma 4.3, $\psi_{\beta,m}$ extends to $C_{G_2}(\beta)^{F^m}$. Restricting this (one-dimensional) extension to $C_{G_2}(\beta)^F$, we obtain the desired extension of ψ_β. □

We can now deduce our main theorem. Given a $\beta \in (\mathfrak{g}^*)^{F^*}$, the first assertion of the theorem follows from Lemma 4.2 and Proposition 4.5, together with the stabiliser formulas (4.1). Note that β for $\mathbb{G}(W_2(\mathbb{F}_q))$ is paired up with $\sigma^*(\beta)$ for $\mathbb{G}(\mathbb{F}_q[t]/t^2)$. The second assertion of the theorem follows from the first, together with Lemma 3.4. This completes the proof of Theorem 1.1.

5. Further directions

It is natural to ask whether Theorem 1.1 remains true for all $\beta \in (\mathfrak{g}^*)^{F^*}$ when p is arbitrary. We have not been able to prove this, but neither do we know a counter-example. It was stated in [22, Theorem 1.1] that for $p \mid n$ and any integers $n, d \geq 1$, one has $\#\operatorname{Irr}_d(\mathrm{SL}_n(\mathcal{O}_2)) = \#\operatorname{Irr}_d(\mathrm{SL}_n(\mathcal{O}'_2))$, with $\mathcal{O}$ and $\mathcal{O}'$ as in Section 1. However, the argument given in [22] for the crucial Lemma 2.3 has a gap (as acknowledged by the author in private communication). Namely, it is not clear that $T(\psi_A) \cap \mathrm{SL}_n(\mathcal{O}_2) = (Z_{\mathrm{GL}_n(\mathcal{O}_2)}(s(A)) \cap \mathrm{SL}_n(\mathcal{O}_2))L(SL)$, in the notation of [22]. Theorem 1.1 therefore remains open for $\mathbb{G} = \mathrm{SL}_n$, $p \mid n$.

Question 5.1. *Let $\mathbb{G}$ be a reductive group scheme over $\mathbb{Z}$. Is it true that if p is sufficiently large and $r \geq 3$, then $\#\operatorname{Irr}_d(\mathbb{G}(\mathcal{O}_r)) = \#\operatorname{Irr}_d(\mathbb{G}(\mathcal{O}'_r))$, for any integer $d \geq 1$?*

Given Theorem 1.1 (i.e., the case $r = 2$), this question is equivalent to the question posed in [1, Section 8.4] (in the case where $\mathbb{G}$ is split, that is, a Chevalley group scheme).

A weaker question is whether the groups $\mathbb{G}(\mathcal{O}_r)$ and $\mathbb{G}(\mathcal{O}'_r)$ have the same number of conjugacy classes, for sufficiently large p. This was settled in the affirmative in [1], at least for Chevalley group schemes (although the bound on p is not explicit). For $r = 2$, no counter-examples are known, even for small primes. On the other hand, for $r = 3$ even this weaker question can fail for small primes, for it is an exercise to compute that $\mathrm{SL}_2(\mathbb{F}_2[t]/t^3)$ has 24 conjugacy classes, while $\mathrm{SL}_2(\mathbb{Z}/8)$ has 30 conjugacy classes (see [18]) (these numbers can also be verified by computer).

References

[1] M. N. Berman, J. Derakhshan, U. Onn, and P. Paajanen, *Uniform cell decomposition with applications to Chevalley groups*, J. Lond. Math. Soc. (2) **87** (2013), no. 2, 586–606.
[2] A. Borel, *Linear Algebraic Groups*, volume 126 of *Graduate Texts in Mathematics*, Springer-Verlag, second edition, 1991.
[3] I. S. Cohen, *On the structure and ideal theory of complete local rings*, Trans. Amer. Math. Soc. **59** (1946), 54–106.
[4] B. Conrad, *Reductive group schemes*, in *Autour des schémas en groupes. Vol. I*, volume 42/43 of *Panor. Synthèses*, pp. 93–444, Soc. Math. France, Paris, 2014.
[5] B. Conrad, O. Gabber, and G. Prasad, *Pseudo-reductive groups*, volume 26 of *New Mathematical Monographs*, Cambridge University Press, Cambridge, second edition, 2015.
[6] M. Demazure and P. Gabriel, *Introduction to Algebraic Geometry and Algebraic Groups*, volume 39 of *North-Holland Mathematics Studies*, North-Holland Publishing Co., Amsterdam, 1980.
[7] M. Demazure and A. Grothendieck (eds.), *Schémas en groupes (SGA 3)*, volume I–III of *LNM 151–153*, Springer-Verlag, Berlin, 1970.
[8] F. Digne and J. Michel, *Representations of Finite Groups of Lie Type*, Cambridge University Press, Cambridge, 1991.
[9] M. J. Greenberg, *Schemata over local rings*, Ann. of Math. (2) **73** (1961), 624–648.
[10] M. J. Greenberg, *Schemata over local rings II*, Ann. of Math. (2) **78** (1963), 256–266.
[11] S. Herpel, *On the smoothness of centralizers in reductive groups*, Trans. Amer. Math. Soc. **365** (2013), no. 7, 3753–3774.
[12] J. E. Humphreys, *Linear Algebraic Groups*, Springer-Verlag, New York, 1975.
[13] J. E. Humphreys, *Conjugacy classes in semisimple algebraic groups*, volume 43 of *Mathematical Surveys and Monographs*, American Mathematical Society, Providence, RI, 1995.
[14] I. M. Isaacs, *Character Theory of Finite Groups*, Pure and Applied Mathematics, No. 69, Academic Press, New York, 1976.
[15] V. Kac and B. Weisfeiler, *Coadjoint action of a semi-simple algebraic group and the center of the enveloping algebra in characteristic p*, Nederl. Akad. Wetensch. Proc. Ser. A **79**=Indag. Math. **38** (1976), no. 2, 136–151.
[16] E. Letellier, *Fourier transforms of invariant functions on finite reductive Lie algebras*, volume 1859 of *Lecture Notes in Mathematics*, Springer-Verlag, Berlin, 2005.
[17] G. J. McNinch and E. Sommers, *Component groups of unipotent centralizers in good characteristic*, J. Algebra **260** (2003), no. 1, 323–337.
[18] A. Nobs, *Die irreduziblen Darstellungen der Gruppen $SL_2(Z_p)$, insbesondere $SL_2(Z_2)$. I*, Comment. Math. Helv. **51** (1976), no. 4, 465–489.
[19] U. Onn, *Representations of automorphism groups of finite $\mathfrak{o}$-modules of rank two*, Adv. in Math. **219** (2008), no. 6, 2058–2085.
[20] J.-P. Serre, *Local Fields*, Springer-Verlag, New York, 1979.
[21] P. Singla, *On representations of general linear groups over principal ideal local rings of length two*, J. Algebra **324** (2010), no. 9, 2543–2563.
[22] P. Singla, *On representations of classical groups over principal ideal local rings of length two*, Comm. Algebra **40** (2012), no. 11, 4060–4067.
[23] T. A. Springer, *Trigonometric sums, Green functions of finite groups and representations of Weyl groups*, Invent. Math. **36** (1976), 173–207.
[24] T. A. Springer and R. Steinberg, *Conjugacy classes*, in *Seminar on Algebraic Groups and Related Finite Groups*, LNM, Vol. 131, pp. 167–266, Springer, Berlin, 1970.
[25] A. Stasinski and S. Stevens, *The regular representations of GL_N over finite local principal ideal rings*, Bull. London Math. Soc. **49** (2017), no. 6, 1066–1084.
[26] R. Steinberg, *Torsion in reductive groups*, Advances in Math. **15** (1975), 63–92.

Alexander Stasinski, Department of Mathematical Sciences, Durham University, Durham, DH1 3LE, UK
E-mail address: alexander.stasinski@durham.ac.uk

Andrea Vera-Gajardo, Instituto de Matemática, Universidad de Valparaiso, Gran Bretaña 1091, Playa Ancha, Valparaíso.
E-mail address: andreaveragajardo@gmail.com