MOD p REPRESENTATIONS OF FINITE GROUPS OF LIE TYPE

SEAN COTNER

1. Introduction

In this note we aim to prove that if G is a connected reductive group over a finite field k of characteristic p and G is simply connected, then the irreducible $\overline{k}$-representations of $G(k)$ are precisely the restrictions to $G(k)$ of the representations of the algebraic group $G_{\overline{k}}$, all describable by "highest weight". Recall the theorem of Brauer [Ser77, 18.2, Thm. 42] stating that the number of irreducible $\overline{k}$-representations of $G(k)$ is equal to the number of conjugacy classes of "p-regular" elements of $G(k)$; these are precisely the semisimple elements of $G(k)$ in the sense of algebraic groups. The first step, therefore, is to determine the number of conjugacy classes of semisimple elements in $G(k)$, which we obtain in section 1 as q^ℓ, where $\ell = \mathrm{rk}(G)$. Next, we will describe a collection of q^ℓ representations of $G(k)$ coming from irreducible algebraic representations of $G_{\overline{k}}$ and prove that they remain irreducible and distinct upon restriction to $G(k)$. The proof of irreducibility involves some tricky calculations to make a connection with the irreducibility of representations of Frobenius kernels proved in [Jan03] (itself very nontrivial); the basic difficulty is to show that the space of fixed points for the action of $U(k)$ on a simple representation of G is 1-dimensional, where U is the unipotent radical of a Borel subgroup of G. Once this is done, we prove distinctness by reducing to the relative rank 1 case, where distinctness can be detected by the k-points of the normalizer of a maximal torus lying in a Borel subgroup.

Roughly speaking, the first section is an exposition of the proof of Lemma 3.9 in Steinberg's paper [Ste63]. At several important points, our exposition is significantly more detailed than Steinberg's. The arguments in the second section are inspired by [Hum06, Chap. 2] (itself following [Jan87, App. 1]), and they rely heavily on the results in [Jan03]. We ignore the Suzuki and Ree groups, though it seems that these can be treated similarly.

2. Semisimple conjugacy classes

Theorem 2.1. Let G be a connected reductive algebraic group over a field k such that $\mathscr{D}(G)$ is simply connected and let $g \in G(k)$ be a semisimple element. Then the centralizer $Z_G(g)$ of g in G is a connected reductive group.

Proof. We may and do assume that k is algebraically closed. By [Con20, D.2.1], there is a maximal torus T of G containing the element g. Let B be a Borel subgroup of G containing T, and let $W = N_G(T)/T$ denote the Weyl group of G, a finite constant k-group. We will regularly identify W with its group of k-points. Recall the Bruhat decomposition of G, given by

$$G(k) = \coprod_{w \in W} B(k) n_w B(k),$$

where $(n_w)_{w \in W}$ is a system of representatives for the Weyl group W. Moreover, if $U'_w = U \cap n_w U^- n_w^{-1}$, where U is the unipotent radical of B and U^- is the unipotent radical of the opposite Borel, then $U'_w \times U \times T \cong B n_w B$ as k-schemes, via the natural map $(u', u, t) \mapsto u' n_w u t$. If $\Phi^+ = \Phi(B, T)$ is the system of positive roots corresponding to B, then there is an isomorphism of k-schemes $\prod_{a \in \Phi^+} U_a \to U$ given by multiplication (in any fixed order), where U_a is the root

Date: January 16, 2021.

group corresponding to the root a. If $\Phi'_w = \{a \in \Phi^+ : w^{-1}(a) \in -\Phi^+\}$, then there is also an isomorphism of k-schemes $\prod_{a\in\Phi'_w} U_a \to U'_w$ given by multiplication in any fixed order. For any $a \in \Phi$, let $u_a : \mathbf{G}_a \to U_a$ be an isomorphism such that $tu_a(x)t^{-1} = u_a(a(t)x)$ for all $t \in T$ and $x \in \mathbf{G}_a$. Finally, recall that the multiplication map $U^- \times U \times T \to G$ is an open immersion. The proofs of the following two results will not rely on the simple connectedness of G.

Lemma 2.2. If g, h are elements of $T(k)$ and $g = xhx^{-1}$ where $x \in B(k)n_wB(k)$ for some $w \in W$, then $g = n_whn_w^{-1}$.

Proof. Since T is commutative, we may assume $x = u'n_wu$ for some $w \in W$, $u' \in U'_w(k)$, and $u \in U(k)$. Then we have

$$n_wugu^{-1}n_w^{-1} = u'^{-1}gu' = u'^{-1}(gu'g^{-1})g.$$

so because $n_wugu^{-1}n_w^{-1} = n_w(u(gu^{-1}g^{-1}))n_w^{-1}(n_wgn_w^{-1})$ and T normalizes U and U'_w, it follows that $g = n_wgn_w^{-1}$. □

Lemma 2.3. The centralizer $Z_G(g)$ is generated by T, those root groups U_α with $\alpha(g) = 1$, and those elements $n \in N_G(T)$ such that $ngn^{-1} = g$.

Proof. Recall that $Z_G(g) = Z_G(\overline{\langle g\rangle})$ is smooth because it is the centralizer of a smooth group scheme of multiplicative type. Thus it suffices to prove this lemma on the level of k-points. Let $x \in Z_G(g)(k)$. Using the Bruhat decomposition and the fact that T centralizes g, we may assume $x = u'n_wu$ for some $w \in W$, $u' \in U'_w(k)$, and $u \in U(k)$. By the previous lemma, $n_wgn_w^{-1} = g$. Write $u = \prod_{a\in\Phi^+} u_a(x_a)$ and $u' = \prod_{a\in\Phi'_w} u_a(x'_a)$, so that

$$n_w^{-1}u'n_w = \prod_{a\in-\Phi^+\cap w^{-1}(\Phi^+)} u_a(x'_{wa}).$$

Because w lies in $Z_G(g)(k)$, we have $n_w^{-1}u'n_wu \in Z_G(g)(k)$ and thus

$$g(n_w^{-1}u'n_wu)g^{-1} = n_w^{-1}u'n_wu.$$

Using the T-equivariance of u_a, we see that

$$\prod_{a\in w^{-1}(\Phi'_w)} u_a(a(g)x'_{wa}) \prod_{b\in\Phi^+} u_b(b(g)x_b) = \prod_{a\in w^{-1}(\Phi'_w)} u_a(x'_{wa}) \prod_{b\in\Phi^+} u_b(x_b)$$

and thus $a(g) = 1$ for all $a \in -\Phi^+ \cap w^{-1}(\Phi^+)$ such that $x'_{wa} \neq 0$, and similarly $b(g) = 1$ for all $b \in \Phi^+$ such that $x_b \neq 0$. In other words, $n_w^{-1}u'n_wu$ is a product of elements of $U_a(k)$ for roots $a \in \Phi$ such that $a(g) = 1$. □

The above lemma quickly implies that $Z_G(g)$ is reductive: if $\mathscr{U}$ is the unipotent radical of G, then $\mathscr{U}$ is normalized by $N_G(T)$, so it is a product of root groups U_α for $\alpha \in \Phi$, and the collection of such α is closed under negation. Since $\langle U_\alpha, U_{-\alpha}\rangle \cong \mathrm{SL}_2$ for all $\alpha \in \Phi$, we see that if $\mathscr{U} \neq 0$ then $\mathrm{SL}_2 \subset \mathscr{U}$, a contradiction. Next we deal with connectedness, for which we need the following lemma.

Lemma 2.4. Suppose that $a \in \Phi$ is a root and $n_a \in N_G(T)$ restricts to the reflection $r_a \in W$. If $n_agn_a^{-1} = g$, then $a(g) = 1$.

Proof. First, suppose that $G = \mathrm{GL}_2$ and that T is the diagonal torus in G, so that there is a unique nontrivial element of W, represented by the matrix $n = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. There are precisely two roots of (G, T), one of which is given by $a(\mathrm{diag}(s, t)) = st^{-1}$, and the other of which is a^{-1}. Note $n\,\mathrm{diag}(s, t)n^{-1} = \mathrm{diag}(t, s)$, so n centralizes $\mathrm{diag}(s, t)$ precisely when $s = t$. As $a(\mathrm{diag}(t, t)) = 1$, we see that the result is true for GL_2, hence also for SL_2. By [Con14, 5.1.8], every connected reductive group of semisimple rank 1 is either of the form $\mathrm{GL}_2 \times D$, $\mathrm{SL}_2 \times D$, or $\mathrm{PGL}_2 \times D$ for a (central) torus

D. Of these, only the former two have simply connected derived group, and so we have established the result in the case of semisimple rank 1.

Now suppose that G has semisimple rank > 1 and let $T_a = \ker(a)^0_{\mathrm{red}}$, so that $Z_G(T_a)$ is a connected reductive group of semisimple rank 1 and there is a central isogeny $T_a \times \mathscr{D}(Z_G(T_a)) \to Z_G(T_a)$. Since T centralizes g, we may choose n_a to lie in $\mathscr{D}(Z_G(T_a))$. Letting $g = hd$ for $h \in \mathscr{D}(Z_G(T_a))(k)$ and $d \in T_a(k)$, it follows that $n_a h n_a^{-1} = h$ and thus we are in the situation of the previous paragraph since $a|_{T_a}$ is trivial. □

Recall that, with notation as in the proof of the lemma, for any root $a \in \Phi$ the group $\mathscr{D}(Z_G(T_a))$ is generated by the root groups U_a and U_{-a}, and one can choose some representative n_a of r_a lying in $\mathscr{D}(Z_G(T_a))$. We are reduced to showing the following: if $w \in W$ is any element fixing g, then w is the product of reflections r_a for $a \in \Phi$ such that each r_a also fixes g. In other words, we wish to show that the stabilizer of g in W is generated by reflections. We will reduce this to a statement purely about root systems.

Let $M = \overline{\langle g \rangle}$ be the closed k-subgroup of G generated by g, so that M is a multiplicative type group and $Z_G(g) = Z_G(M)$. We have $M = M^0 \times D$, where M^0 is a torus and D is a finite constant group. Write $g = st$ for $s \in M^0(k)$ and $t \in D(k)$, so that $Z_G(g) = Z_{Z_G(M^0)}(t)$. By [Con20, 1.4.3] (essentially a consequence of the existence of the open cell), $Z_G(M^0)$ is connected, so to prove the result it suffices to consider semisimple elements g *of finite order*, say d. Note that the characteristic of k does not divide d since g is semisimple.

Recall that there is a natural isomorphism $X_*(T) \otimes k^* \to T(k)$, where $X_*(T)$ is the cocharacter group of T, given by $v^* \otimes a \mapsto v^*(a)$. The group of dth roots of unity in k^* is isomorphic to $\mathbf{Z}/d$, so we may identify g with an element of $X_*(T) \otimes \mathbf{Z}/d$, say $v^* \otimes 1$ for $v^* \in X_*(T)$. The stabilizer of g in W is then identified with the group

$$\begin{aligned} W(g) &= \{w \in W : w(v^*) - v^* \in dX_*(T)\} \\ &= \{w \in W : w(v^*/d) - v^*/d \in X_*(T)\}, \end{aligned}$$

where we consider v^*/d as an element of $X_*(T) \otimes \mathbf{R}$. Since G is simply connected, we have $X_*(T) = \mathbf{Z}\Phi^\vee$, where $\Phi^\vee$ is the set of coroots. We are thus reduced finally to the following lemma, appearing as [Bou68, VI, §2, Exerc. 1]. □

Lemma 2.5. Let Φ be a reduced root system in a finite-dimensional real vector space V. Let $v \in V$ and let $W(v)$ be the subgroup of $W(\Phi)$ consisting of those elements $w \in W$ such that $w(x) - x \in \mathbf{Z}\Phi$, where W is the Weyl group of Φ. Then $W(v)$ is generated by reflections.

Proof. Let W_a denote the affine Weyl group of the dual root system $\Phi^\vee$, defined in [Bou68, VI, 2.1]. By [Bou68, VI, 2.1, Prop. 1], W_a is the semidirect product of W and the group of translations of V corresponding to elements of $\mathbf{Z}\Phi$, so if $W_a(v)$ is the stabilizer of v in W_a then $W_a(v) \cong W(v)$ via the homomorphism sending an element of $W_a(v)$ to the induced linear automorphism of V. By [Bou68, V, 3.2, Thm. 1] and [Bou68, VI, 2.1, Prop. 2], W_a is a Coxeter group and thus by [Bou68, V, 3.3, Prop. 2], $W_a(v)$ is generated by reflections. This completes the proof of the lemma and hence also the proof of the theorem. □

Remark 2.6. Theorem 2.1 originally appeared in [Ste63, 3.9], which contains a very brief sketch of a proof attributed to Springer; the proof that we describe is essentially an elaboration of the proof given there.

From now on, let k be a finite field of $q = p^r$ elements and let G be a connected linear algebraic group over k. Let $F = F_{G/k,q} : G \to G$ denote the "absolute q-Frobenius" for G over k, given on the coordinate ring $k[G]$ by $x \mapsto x^q$. If $g \in G$, we will usually use the notation $g^{[q]} = F(g)$. Let $L : G \to G$ be the Lang map defined functorially by $L(g) = g^{-1}g^{[q]}$. A fundamental result of

Lang states that L is *surjective*; this can be used to prove that G contains a Borel subgroup and a (geometrically) maximal torus over k. We are ready now to prove the main result of this section.

Theorem 2.7. Let G be a connected semisimple group over k, and assume that G is simply connected. If ℓ is the rank of G, then the number of conjugacy classes of semisimple elements in $G(k)$ is q^ℓ.

Proof. First we need the following two group-theoretic lemmas, in whose statements we will preserve the notation in the theorem statement.

Lemma 2.8. Two semisimple elements of $G(k)$ are conjugate in $G(\overline{k})$ if and only if they are conjugate in $G(k)$.

Proof. Let $x, y \in G(k)$ be semisimple and suppose that $x = zyz^{-1}$ for some $z \in G(\overline{k})$. Then $x = z^{[q]}y(z^{[q]})^{-1}$ and so $z(z^{[q]})^{-1}xz^{[q]}z^{-1}$, i.e., $z^{[q]}z^{-1} \in Z_G(x)(\overline{k})$. By Theorem 2.1, $Z_G(x)$ is connected and thus by surjectivity of the Lang map for *connected* linear algebraic groups, there exists some $w \in Z_G(x)(\overline{k})$ such that $w^{[q]}w^{-1} = z^{[q]}z^{-1}$. Then $w^{-1}z \in G(k)$ and $w^{-1}zyz^{-1}w = w^{-1}xw = x$, so we are done. □

Lemma 2.9. An element of $G(\overline{k})$ is conjugate to an element of $G(k)$ if and only if it is conjugate to its image under F.

Proof. Let $g \in G(\overline{k})$. If g is conjugate to an element of $G(k)$ then certainly g is conjugate to its image under F, so suppose conversely that $g = xg^{[q]}x^{-1}$ for some $x \in G(\overline{k})$. By Lang's theorem, there is some $y \in G(\overline{k})$ such that $y^{-1}y^{[q]} = x$, so that $g = y^{-1}y^{[q]}g^{[q]}(y^{[q]})^{-1}y$, so that ygy^{-1} is invariant under F, i.e., $ygy^{-1} \in G(k)$. □

Now fix a maximal k-torus T of G, and we let $W = W(G,T)$ denote the Weyl group of T, a finite etale k-group scheme. We note that W is usually not constant, but the set $W(\overline{k})$ of $\overline{k}$-points is isomorphic to the usual Weyl group of the pair $(G_{\overline{k}}, T_{\overline{k}})$. By [Con20, D.2.1] and the conjugacy of maximal tori over an algebraically closed field, an element of $G(\overline{k})$ is semisimple if and only if it is conjugate to an element of $T(\overline{k})$. Moreover, by Lemma 2.2 two elements of $T(\overline{k})$ are $G(\overline{k})$-conjugate if and only if they are $W(\overline{k})$-conjugate. So if $[G(k)]_{\mathrm{ss}}$ denotes the collection of conjugacy classes of semisimple elements of $G(k)$ and $(T(\overline{k})/W(\overline{k}))^F$ denotes the collection of $W(\overline{k})$-conjugacy classes in $T(\overline{k})$ which are stable under F, then there is a well-defined function $\varphi : [G(k)]_{\mathrm{ss}} \to (T(\overline{k})/W(\overline{k}))^F$ given by sending the $G(k)$-conjugacy class of the semisimple element $g \in G(k)$ to the intersection of the $G(\overline{k})$-conjugacy class of g with $T(\overline{k})$. Injectivity of φ follows from Lemma 2.8 and surjectivity follows from Lemma 2.9. Thus we are reduced to counting the number of points in $(T(\overline{k})/W(\overline{k}))^F$.

Let $T/\!/W$ denote the k-scheme $\operatorname{Spec} k[T]^W$, so that $(T/\!/W)(\overline{k}) = T(\overline{k})/W(\overline{k})$ and the natural action of F on $\overline{k}[T]^W$ is compatible with the natural action of F on $T(\overline{k})/W(\overline{k})$. Thus to prove the theorem, we are reduced to proving the following general proposition. □

Proposition 2.10. For any field k, suppose that G is a quasi-split connected semisimple k-group of rank ℓ which is simply connected. Let B be a Borel k-subgroup of G and let T be a maximal k-torus of G contained in B. The k-scheme $T/\!/W$ is isomorphic to the affine space $\mathbf{A}^\ell_k$.

Proof. We will first show that $k_s[T_{k_s}]^{W(k_s)}$ is a polynomial ring. Since G is simply connected, the coordinate ring $k_s[T_{k_s}]$ is equal to $k_s[\{\omega_a, \omega_a^{-1}\}_{a\in\Delta}]$, where Δ is a system of simple roots in Φ corresponding to a Borel k-subgroup of G containing T and $\{\omega_a\}$ is the basis of $X^*(T_{k_s})$ dual to the basis $\{a^\vee\}$ of $X_*(T_{k_s})$. Let γ_a be the sum of the distinct images of ω_a under $W(k_s)$; we will show that $k_s[T_{k_s}]^{W(k_s)} = k_s[\{\gamma_a\}_{a\in\Delta}]$.

We partially order the monomials $\prod_{a\in\Delta}\omega_a^{n_a}$ in $k_s[T_{k_s}]$ by declaring that all positive roots are positive and extending multiplicatively. Let β be a nonzero $W(k_s)$-invariant polynomial in $k_s[T_{k_s}]$ and let $c\prod_{a\in\Delta}\omega_a^{n_a}$ be one of the highest terms of β. By [Bou68, VI, 1.10], if C is the chamber

corresponding to Φ^+ then $\overline{C}$ is the collection of products of the ω_a with exponents ≥ 0. Since $W(k_s)$ acts simply transitively on the set of chambers of $X^*(T_{k_s})$ it follows from maximality that $n_a \geq 0$ for all $a \in \Delta$. Next we show that for all sequences $(w_a)_{a\in\Delta}$ of elements of $W(k_s)$ we have $c\prod_{a\in\Delta} w_a(\omega_a)^{n_a} \leq c\prod_{a\in\Delta}\omega_a^{n_a}$. This is contained in the following lemma, valid for all root systems.

Lemma 2.11. If $a \in \Delta$ and $w \in W$, then $w(\omega_a) = \omega_a \prod_{b\in\Delta} b^{m_b}$ for $m_b \leq 0$.

Proof. First let $b \in \Delta$ be an arbitrary simple root. By [Bou68, VI, 1.10, eq. (15)], we have $s_b(\omega_a) = \omega_a b^{-\delta_{ab}}$, where δ_{ab} is the Kronecker delta. In general, let $w = s_{b_1}\cdots s_{b_n}$ be a reduced decomposition of w, where $b_i \in \Delta$ for all i. Inductively, we see

$$s_{b_1}\cdots s_{b_n}(\omega_a) = \omega_a \prod_{i=0}^{n-1} s_{b_1}\cdots s_{b_i}(b_{i+1}^{-\delta_{ab_{i+1}}})$$

so it suffices to show that $s_{b_1}\cdots s_{b_i}(b_{i+1})$ is a positive root for all i, and this is [Bou68, VI, 1.6, Cor. 2 à Prop. 17]. □

We return to the proof of the proposition. Now that we have seen that $c\prod_{a\in\Delta} w_a(\omega_a)^{n_a} \leq c\prod_{a\in\Delta}\omega_a^{n_a}$ for all sequences (w_a) of elements of W, it follows that

$$c\prod_{a\in\Delta}\gamma_a^{n_a} = c\prod_{a\in\Delta}\omega_a^{n_a} + \chi$$

where $\chi \in X^*(T_{k_s})$ is a sum of monomials strictly less than $c\prod_{a\in\Delta}\omega_a^{n_a}$ in the above ordering. Thus $\beta - c\prod_{a\in\Delta}\gamma_a^{n_a}$ is a sum of monomials such that each maximal term is either a maximal term of β or is strictly less than $c\prod_{a\in\Delta}\omega_a^{n_a}$, and this latter term does not appear. Thus by induction we see that $k_s[T_{k_s}]^{W(k_s)}$ is a polynomial ring in the γ_a.

Now we must descend this result to k. Let $\Gamma = \mathrm{Gal}(k_s/k)$ be the absolute Galois group of k, so because T is a k-torus, Γ acts on the root system Φ. Moreover, because B is a Borel k-subgroup of G, Γ preserves the system of positive roots Φ^+ and hence also the system of simple roots $\Delta \subset \Phi^+$. It follows that Γ preserves the set $\{\omega_a\}_{a\in\Delta}$, hence also the set $\{\gamma_a\}_{a\in\Delta}$. By the description of $T//W$ above we have

$$(T//W)_{k_s} = \prod_{\text{orbits } \Omega\subset\Delta} \mathrm{Spec}\, k_s[\{\gamma_a\}_{a\in\Omega}]$$

where Γ acts semilinearly on $\mathrm{Spec}\, k_s[\{\gamma_a\}_{a\in\Omega}] = \prod_{a\in\Omega}\mathbf{A}^1_{k_s}$ via permuting the factors of this product according to the action of Γ on Ω. If k_Ω is the stabilizer of a fixed $a \in \Omega$, then this is precisely the Galois descent datum for the *Weil restriction* $R_{k_\Omega/k}\mathbf{A}^1_{k_\Omega}$ (see [CGP15, App. A.5]), and this is well-known to be isomorphic to $\mathbf{A}^{[k_\Omega:k]}_k$. It follows that

$$T//W \cong \prod_{\text{orbits } \Omega\subset\Delta} \mathbf{A}^{[k_\Omega:k]}_k \cong \mathbf{A}^\ell_k,$$

and we are done with the proof of the proposition and thence the proof of the theorem. □

Remark 2.12. The point count implied by Proposition 2.10 could also be proved as follows: first, establish Proposition 2.10 in the easier split case, then use the general result (an application of the Grothendieck-Lefschetz trace formula and the computation of the etale cohomology of affine space) that any form of affine n-space over $\mathbf{F}_q$ has q^n points. (It seems to be an open question whether there are nontrivial forms of affine n-space over finite fields, at least when $n \geq 3$.)

3. Representations of finite groups

In this section, G will denote a connected semisimple group over a field k. Soon we will assume that k is a finite field. We first recall various facts and constructions from [Jan03] concerning representations of G in the split case (e.g., when $k = k_s$), see [Jan03, II, Secs. 2-...]. To facilitate these references, we will use the *opposite* convention on ordering roots as in Section 1.

So suppose for the time being that G is split, and let T be a split maximal torus of G contained in a Borel k-subgroup B of G. Let $\Phi = \Phi(G,T)$ denote the root system corresponding to T and let Φ^+ and Δ denote the system of positive roots and the system of simple roots, respectively, corresponding to the *opposite Borel* of B, which we denote by B^+. We say that $\lambda \in X^*(T)$ is a **dominant root** if $\langle \lambda, \alpha^\vee \rangle \geq 0$ for all $\alpha \in \Delta$. For every dominant root λ there is a line bundle $\mathscr{L}(\lambda) = \mathscr{L}_G(\lambda)$ on G/B such that $H^0(\lambda) := H^0(G/B, \mathscr{L}(\lambda))$ is the induced representation $\mathrm{ind}_B^G(\lambda)$. There is a unique simple G-subrepresentation $L(\lambda) = L_G(\lambda) \subset H^0(\lambda)$. All simple G-representations are obtained this way, and for two dominant roots λ and μ we have $L(\lambda) \cong L(\mu)$ if and only if $\lambda = \mu$. By [Jan03, II, 2.2], if U^+ denotes the unipotent radical of B^+ then $H^0(\lambda)^{U^+}$ is equal to the λ-eigenspace for the action of T on $H^0(\lambda)$, and the dimension of this subspace is 1.

If $\pi : G \to G/B$ is the projection map and $W \subset G/B$ is an open set, then we have the concrete description

$$\mathscr{L}(\lambda)(W) = \{f \in \mathrm{Hom}\left(\pi^{-1}(W), \mathbf{A}_k^1\right) : f(gb) = \lambda(b)^{-1} f(g) \text{ as morphisms } G \times B \to \mathbf{A}_k^1\}$$

where we have extended λ from T to B by defining $\lambda(u) = 1$ for all $u \in U$, the unipotent radical of B. The action of G on $H^0(\lambda)$ is given explicitly by

$$(g \cdot f)(h) = f(g^{-1}h).$$

Note that there is a natural homomorphism $H^0(\lambda) \to k[U^+]$ given by restriction of functions, equivariant for the left translation action of U^+ on functions; this map is injective because the multiplication map $U \times T \times U^+ \to G$ is an open immersion. There is an action of T on $k[U^+]$ given by conjugation: if $t \in T$ and $f \in k[U^+]$, then we define

$$(t \cdot f)(u) = f(t^{-1}ut).$$

With respect to this action, the inclusion $H^0(\lambda) \to k[U^+]$ is not equivariant; the action on $k[U^+]$ restricts to an action on $H^0(\lambda)$ which is the natural one shifted down by λ. In particular, $H^0(\lambda) \cap k[U^+]^{U^+} = k$.

Lemma 3.1. If G is split, then the T-weights on $k[U^+]$ are precisely the nonnegative $\mathbf{Z}$-linear combinations of negative roots.

Proof. Let $a \in \Phi^+$ and let $u_a : \mathbf{G}_a \to U_a$ be a T-equivariant isomorphism, where the action of T on $\mathbf{G}_a$ is given by $t \cdot x = a(t)x$. Then we see that

$$k[U_a] \cong \bigoplus_{n=0}^{\infty} k \cdot f_{na}$$

where $f_{na}(u_a(x)) = x^n$. Note that

$$\begin{aligned}(t \cdot f_{na})(u_a(x)) = f_{na}(t^{-1}u_a(x)t) &= f_{na}(u_a(a(t)^{-1}x)) \\ &= a(t)^{-n}x^n \\ &= a(t)^{-n} f_{na}(u_a(x)),\end{aligned}$$

so that $k \cdot f_{na}$ is a T-eigenspace for $k[U_a]$ of eigenvalue $-na$. Recall that the multiplication map $\prod_{a \in \Phi^+} U_a \to U^+$ (in any order) is an isomorphism of k-schemes. We have then

$$k[U^+] = \bigotimes_{a \in \Phi^+} k[U_a],$$

so the calculation above yields the lemma. □

Now suppose that k is a finite field of order $q = p^r$; we will no longer assume G to be split. As in the previous section, let $F = F_{G/k,q} : G \to G$ denote the Frobenius endomorphism of G. This is a homomorphism of k-groups, and we will denote its kernel by G_r: this is a finite connected group scheme over k. Similarly we will write T_r, B_r, etc. for the corresponding kernels of F restricted to T, B, etc. Recall also the Lang map $L : G \to G$ defined by $L(g) = g^{-1}g^{[q]}$.

Lemma 3.2. The algebra of invariants $k[U^+]^{U_r^+}$ is the image of $F^* : k[U^+] \to k[U^+]$. Moreover, $k[U^+]^{U^+(k)}$ is the image of $L^* : k[U^+] \to k[U^+]$. If $f \in k[U^+]$ has T-weight μ then $f \circ F$ has T-weight $q\mu$.

Proof. Note that the morphisms $F : U^+ \to U^+$ and $L : U^+ \to U^+$ are both *fppf* (in fact L is étale). Since F is a homomorphism, a morphism $\varphi : U^+ \to X$ to a k-scheme X factors through F precisely when φ is invariant under left multiplication by U_r^+. This gives the first statement. Moreover, it is easy to see that a morphism $\psi : U^+ \to X$ factors through L precisely when ψ is invariant under left multiplication by $U^+(k) = (U^+)^L$, so we also obtain the second statement.

Now let $f \in k[U^+]$ have T-weight μ. With notation as in the proof of Lemma 3.1, we may assume $f = \bigotimes_{a\in\Phi^+} f_{n_a a}$ where $\mu = -\sum_{a\in\Phi^+} n_a a$. We have

$$\begin{aligned} t \cdot (f \circ F)\left(\prod_{a\in\Phi^+} u_a(x_a)\right) &= f\left(\prod_{a\in\Phi^+} u_a(a(t)^{-1}x_a)^{[q]}\right) \\ &= \prod_{a\in\Phi^+} a(t)^{-n_a q} x_a^{n_a q} \\ &= (q\mu)(t)(f \circ F)\left(\prod_{a\in\Phi^+} u_a(x_a)\right). \end{aligned}$$

This shows that $f \circ F$ has T-weight $q\mu$, as desired. □

Proposition 3.3. If $f \in k[U^+]$ has T-weight μ then $f \circ L$ is the sum of $f \circ F$ and various weight vectors of strictly higher weight.

Here by strictly higher weight we refer to an inequality between the coefficients in a representation of the weight as a $\mathbf{Z}$-linear combination of simple roots. We postpone the proof of Proposition 3.3 until after the proof of Theorem 3.6. It is an elementary inductive argument using the commutation relations for root groups of G, but it is long and giving it here would distract from the main development. Nonetheless, this is a key calculation, and it is the most serious point not explained in [Jan87, App. 1] or [Hum06, Chap. 2].

We let

$$X_r(T) = \{\lambda \in X^*(T_{k_s}) : 0 \le \langle \lambda, \alpha^\vee \rangle < p^r \text{ for all } \alpha \in \Delta\},$$

so that $X_r(T)$ consists of those dominant weights all of whose coefficients with respect to the fundamental weights of G are less than p^r. We will need a nontrivial result from [Jan03] concerning representations of Frobenius kernels of reductive groups: by [Jan03, II, 3.10, 3.15], we have $L(\lambda)^{U_r^+} = L(\lambda)^{U^+}$, which as above is the 1-dimensional λ-eigenspace for the action of T.

We need one more fact from [Jan03] before we can prove our main theorem. In [Jan03, II, 1.16], it is proved as a simple consequence of the Isomorphism Theorem (see [Con14, 6.1.17]) that there is an antiautomorphism τ of G with $\tau^2 = \mathrm{id}_G$, $\tau|_T = \mathrm{id}_T$, and $\tau(U_\alpha) = U_{-\alpha}$ for all $\alpha \in \Phi$. In [Jan03, II, 8.17] it is shown that for each dominant weight λ there is a nondegenerate bilinear form θ on $L(\lambda)$ satisfying $\theta(g \cdot v, v') = \theta(v, \tau(g) \cdot v')$ for all g, v, and v'. This bilinear form is symmetric and unique up to scaling. Since $\tau|_T = \mathrm{id}_T$, it follows from the condition on θ that two distinct

weight spaces for the action of T on $L(\lambda)$ are θ-orthogonal. In particular, because $\dim L(\lambda)_\lambda = 1$, nondegeneracy implies $\theta(v^+, v^+) \neq 0$.

Concretely, θ comes about as follows: given a G-module M there is an associated G-module ${}^\tau M$ with underlying k-vector space M^* and G-action given by $g \cdot \varphi = \varphi \circ \tau(g)$. If $M = L(\lambda)$, then because simple modules are determined by their highest weight, a weight calculation shows that there is some *isomorphism* $\varphi : L(\lambda) \to {}^\tau L(\lambda)$. We can define the bilinear form θ via

$$\theta(v, v') := \varphi(v)(v').$$

The properties of θ listed above are simple consequences of this definition.

In the following two results, we assume that G is *simply connected*.

Theorem 3.4. If $\lambda \in X_r(T)$, then $L(\lambda)$ is irreducible as a $G(k)$-representation.

Proof. We first show that we may reduce to proving

$$L(\lambda)^{U^+(k)} = L(\lambda)_\lambda. \tag{1}$$

Indeed, let $v^+ \in L(\lambda)_\lambda$. Since $U^+(k)$ is a p-group, it has a nonzero fixed vector in any $U^+(k)$-submodule of $L(\lambda)$. Thus every simple $G(k)$-submodule of $L(\lambda)$ contains v^+. With θ as above, the θ-orthogonal complement to $\overline{k}(G(k)v^+)$ is a $G(k)$-submodule of $L(\lambda)$ which does not contain v^+, so it must be trivial, whence $\overline{k}(G(k)v^+) = L(\lambda)$ and $L(\lambda)$ is a simple $G(\overline{k})$-module.

Thus everything hinges on proving (1). As already mentioned, we know that $L(\lambda)^{U_r^+} = L(\lambda)_\lambda$, so it suffices to show that if V is a finite-dimensional $B^+_{\overline{k}}$-submodule of $\overline{k}[U^+]$ then

$$V \cap \overline{k}[U^+]^{U_r^+} = \overline{k} \text{ implies } V \cap \overline{k}[U^+]^{U^+(k)} = \overline{k}.$$

So let V be such a module. By Lemma 3.2, every element of $\overline{k}[U^+]^{U^+(k)}$ is of the form $f \circ L$ for some $f \in \overline{k}[U^+]$. So choose $f \in \overline{k}[U^+]$ such that $f \circ L \in V$. Write $f = \sum_\mu f_\mu$ and $f \circ L = \sum_\mu g_\mu$ as sums of $T_{\overline{k}}$-weight vectors. As $f \circ L$ lies in the T-module V, it follows from complete reducibility of T-representations that $g_\mu \in V$ for all μ. Let ν be minimal such that $f_\nu \neq 0$. By Lemma 3.2 and Proposition 3.3, we have $f_\nu \circ F = g_{q\nu}$, so $f_\nu \circ F \in V \cap \overline{k}[U^+]^{U_r^+} = \overline{k}$. So $q\nu = 0$ and thus $\nu = 0$. It follows from Lemma 3.1 and the assumed minimality of ν that $f \circ L = g_0$. □

Theorem 3.5. If $\lambda, \mu \in X_r(T)$ are distinct, then $L(\lambda)$ and $L(\mu)$ are not isomorphic as $G(k)$-modules.

Proof. First, assume that the theorem holds whenever G has relative rank 1; this is the case that we will reduce to. For general G, let $a \in {}_k\Delta$, where ${}_k\Delta$ is the basis for the relative root system ${}_k\Phi = {}_k\Phi(G, S)$ corresponding to B and the maximal split subtorus $S \subset T$. Let $G_a = Z_G(\ker a)$; this is a Levi factor in the parabolic subgroup P_a^+ containing B^+ and corresponding to a as in [Con20, paragraph following Cor. 11.4.8]. Let V_a^+ be the unipotent radical of P_a^+, so by (1) we have

$$(L_{G_{\overline{k}}}(\lambda)^{V_a^+(k)})^{U_a(k)} = L_{G_{\overline{k}}}(\lambda)^{U^+(k)} = L_{G_{\overline{k}}}(\lambda)_\lambda,$$

where again $L_{G_{\overline{k}}}(\lambda)_\lambda$ is 1-dimensional. Since $U^+(k)$, being a finite p-group, has a fixed point in every $\overline{k}$-representation, it follows that $L_{G_{\overline{k}}}(\lambda)^{V_a^+(k)}$ contains a unique simple $G_{a,\overline{k}}$-submodule, necessarily isomorphic to $L_{G_{a,\overline{k}}}(\lambda)$. Now suppose that there is a $G(k)$-module isomorphism $\varphi : L_{G_{\overline{k}}}(\lambda) \to L_{G_{\overline{k}}}(\mu)$. Taking $V_a^+(k)$-invariants we see that there is a $G_a(k)$-module isomorphism $\varphi_a : L_{G_{a,\overline{k}}}(\lambda) \to L_{G_{a,\overline{k}}}(\mu)$. By [Jan03, II, 2.10(2)] it follows that

$$L_{\mathscr{D}(G_a)_{\overline{k}}}(\lambda|_{T_a}) \cong L_{\mathscr{D}(G_a)_{\overline{k}}}(\mu|_{T_a}),$$

where T_a is the maximal torus of $\mathscr{D}(G_a)_{\overline{k}}$ contained in $T_{\overline{k}}$. If $\lambda \neq \mu$ then there is some $\alpha \in {}_k\Delta$ such that $\lambda|_{\alpha^\vee(\mathbf{G}_m)} \neq \mu|_{\alpha^\vee(\mathbf{G}_m)}$; by [Con20, 12.1.1], the restriction a of α to a character of $S_{\overline{k}}$ is

nontrivial, so that $\lambda|_{T_a} \neq \mu|_{T_a}$. Thus the assumed result in the relative rank 1 case applied to this root a reveals a contradiction, showing that in fact $\lambda = \mu$. So we are reduced to the case in which G has relative rank 1 over k. There are precisely two simply connected semisimple groups over k of relative rank 1, namely SL_2 and SU_3, and we deal separately with these two cases.

Suppose $G = \mathrm{SL}_2$, so if T is the diagonal torus and B is the lower triangular Borel then the unique fundamental weight of SL_2 is $\omega(\mathrm{diag}(t, t^{-1})) = t$, and the elements of $X_r(T)$ are precisely the characters $n\omega$ for $0 \leq n \leq q-1$. Let $\lambda = n\omega$ and $\mu = m\omega$, where $n < m$. If $(n, m) \neq (0, q-1)$, then $\lambda|_{T(k)} \neq \mu|_{T(k)}$, so that the actions of $T(k)$ on $L(\lambda)^{U^+(k)} = L(\lambda)_\lambda$ and $L(\mu)^{U^+(k)} = L(\mu)_\mu$ are not the same and thus $L(\lambda) \ncong L(\mu)$. Now suppose $(n, m) = (0, q-1)$. In this case $\lambda|_{T(k)} = \mu|_{T(k)}$, so these representations are not distinguished by the action of $T(k)$ on the highest weight vectors. However, they are distinguished by the action of $N_G(T)(k)$; to see this, let $g \in N_G(T)(k) \setminus T(k)$. If $t \in \overline{k}^*$ and $v^+ \in L(\mu)^{U^+}$ then we have

$$\begin{aligned} \mathrm{diag}(t, t^{-1}) \cdot (gv^+) &= g(g^{-1}\,\mathrm{diag}(t, t^{-1})g) \cdot v^+ \\ &= g(\mathrm{diag}(t^{-1}, t) \cdot v^+) \\ &= \mu^{-1}(\mathrm{diag}(t, t^{-1}))(gv^+). \end{aligned}$$

Since $\mu \neq \mu^{-1}$ as characters of $T_{\overline{k}}$, it follows that $gv^+ \neq v^+$. Since $L(\lambda)$ is the trivial $G(k)$-module, it follows that $L(\lambda) \ncong L(\mu)$ in all cases.

Finally suppose $G = \mathrm{SU}_3$, so that $G_{\overline{k}} \cong \mathrm{SL}_3$. The group G admits a Borel subgroup B containing a maximal torus T isomorphic to $\mathrm{R}_{k'/k}(\mathbf{G}_m)$ where k'/k is the unique quadratic extension of k such that the isomorphism $G_{\overline{k}} \cong \mathrm{SL}_3$ sends $B_{\overline{k}}$ to the lower triangular Borel subgroup of SL_3 and $T_{\overline{k}}$ to the diagonal torus. Under this isomorphism, $T(k)$ is identified with the collection of those diagonal matrices $\mathrm{diag}(x, x/x^q, (x^q)^{-1})$ with $x \in k'$. With respect to the choice of (B, T), $G_{\overline{k}}$ has precisely two fundamental characters, given by $\omega_1(\mathrm{diag}(r, s, t)) = r$ and $\omega_2(\mathrm{diag}(r, s, t)) = t^{-1}$. Now suppose $\lambda = m\omega_1 + n\omega_2$, so that

$$\lambda(\mathrm{diag}(x, x/x^q, (x^q)^{-1})) = x^{m+nq}.$$

If $\mu = m'\omega_1 + n'\omega_2$ and $(m, n) \leq (m', n')$ in the lexicographic ordering, then this calculation shows $\lambda|_{T(k)} \neq \mu|_{T(k)}$ unless $(m, n) = (0, 0)$ and $(m', n') = (q-1, q-1)$. In this latter case, let $g \in N_G(T)(k)$ be a representative for the nontrivial Weyl element of $W(G, T)(k)$. If $t \in T(\overline{k})$ and $v^+ \in L(\mu)^{U^+}$ then we have

$$\begin{aligned} t \cdot (gv^+) &= g(g^{-1}tg) \cdot v^+ \\ &= \mu(g^{-1}tg)(gv^+). \end{aligned}$$

As $\mu(g^{-1}tg) \neq \mu(t)$ identically as functions of $t \in T(\overline{k})$, it follows that $gv^+ \neq v^+$. Since $L(\lambda)$ is the trivial $G(k)$-module, this completes the proof. □

Theorem 3.6. Let G be a connected semisimple group of rank ℓ defined over a finite field k of $q = p^r$ elements, and suppose that G is simply connected. If T is a maximal k-torus contained in a Borel k-subgroup B, then the $L(\lambda)$, as λ ranges over the elements of $X_r(T)$, form the set of simple $\overline{k}$-representations of $G(k)$.

Proof. By the theorem of Brauer we mentioned in the introduction [Ser77, 18.2, Thm. 42] and Theorem 2.7, there are precisely q^ℓ simple $\overline{k}$-representations of $G(k)$. As G is simply connected, $X_r(T)$ has q^ℓ elements, and the result follows immediately from Theorems 3.4 and 3.5. □

Proof of Proposition 3.3. We retain the notation from the proof of Lemma 3.1. Let $\Delta = \{a_1, \ldots, a_\ell\}$ and for each root $b \in \Phi^+$, say $b = \sum_{i=1}^\ell m_i a_i$, let $|b| = \sum_{i=1}^\ell m_i$. Enumerate the positive roots as $\Phi^+ = \{a_1, \ldots, a_N\}$ extending the above enumeration on Δ such that whenever $1 \leq i < j \leq N$ we have $|a_i| \leq |a_j|$. A monomial $cX_1^{m_1} \ldots X_N^{m_N}$ will be said to have **weight** $\sum_{i=1}^N m_i a_i$. A polynomial

$w(X_1, \ldots, X_N)$ with coefficients in k will be called a i-**low** if every term of w has weight strictly less than qa_i. (This is not standard terminology, but it will be extremely convenient in the following proof.) For ease of notation, we will frequently write $w(\mathbf{X})$ in place of $w(X_1, \ldots, X_N)$ and $w(\mathbf{x})$ in place of $w(x_1, \ldots, x_N)$ for $x_1, \ldots, x_N \in \overline{k}$. Given an element $t \in T(\overline{k})$ and an integer n we will write $\mathbf{a}(t)^n\mathbf{X}$ in place of the n-tuple $(a_1(t)^n X_1, \ldots, a_N(t)^n X_N)$ and similarly for $\mathbf{a}(t)^n\mathbf{x}$.

We will reduce to proving the following lemma:

Lemma 3.7. There exist i-low polynomials $w_i(\mathbf{X})$, $1 \leq i \leq N$, such that for all $x_1, \ldots, x_N$ in $\overline{k}$ we have the equality

$$L\left(\prod_{i=1}^{N} u_{a_i}(x_i)\right) = \prod_{i=1}^{N} u_{a_i}(x_i^q + w_i(\mathbf{x})).$$

Indeed, suppose that the lemma holds. We may assume that $f = \bigotimes_{i=1}^{N} f_{n_i a_i}$ for some nonnegative integers n_i such that $\mu = -\sum_{i=1}^{N} n_i a_i$. Then for all $t \in T(\overline{k})$ we have

$$\begin{aligned} t \cdot (f \circ L)\left(\prod_{i=1}^{N} u_{a_i}(x_i)\right) &= (f \circ L)\left(\prod_{i=1}^{N} u_{a_i}\left(a_i(t)^{-1}x_i\right)\right) \\ &= f\left(\prod_{i=1}^{N} u_{a_i}\left(a_i(t)^{-q}x_i^q + w_i\left(\mathbf{a}(t)^{-1}\mathbf{x}\right)\right)\right) \\ &= \prod_{i=1}^{N}\left(a_i(t)^{-q}x_i^q + w_i\left(\mathbf{a}(t)^{-1}\mathbf{x}\right)\right)^{n_i}. \end{aligned}$$

Since each w_i is i-low, if $1 \leq m \leq n_i$ then every term in $w_i(\mathbf{a}(t)^{-1}\mathbf{X})^m$ is of the form $c\lambda(t)\prod_{j=1}^{N} X_j^{d_j}$ where $\lambda = -\sum_{j=1}^{N} d_j a_j$ is strictly greater than $-qma_i$. Since weight is additive in products of monomials, if we break up the final product into monomials in $x_1, \ldots, x_N$ then the terms are precisely $\prod_{i=1}^{N}(a_i(t)^{-q}x_i^q)^{m_i}$ and $c\lambda(t)\prod_{i=1}^{N} x_i^{m_i}$ where $\lambda = -\sum_{i=1}^{N} m_i a_i$ is *strictly* greater than $q\mu$. Thus we have

$$(f \circ L)\left(\prod_{i=1}^{N} u_{a_i}(x_i)\right) = (f \circ F)\left(\prod_{i=1}^{N} u_{a_i}(x_i)\right) + \sum_{\vec{m}}\left(\bigotimes_{i=1}^{N} f_{m_i a_i}\right)\left(\prod_{i=1}^{N} u_{a_i}(x_i)\right)$$

where the sum is over N-tuples of integers $\vec{m}$ with $-\sum_{i=1}^{N} m_i a_i > q\mu$, as desired. So we are reduced to proving Lemma 3.7. □

Proof of Lemma 3.7. This will involve a nested induction argument. First, note

$$L\left(\prod_{i=1}^{N} u_{a_i}(x_i)\right) = \left(\prod_{i=1}^{N} u_{a_i}(-x_i)\right)\left(\prod_{i=1}^{N} u_{a_i}(x_i^q)\right). \tag{2}$$

By induction and (2), we may further reduce to the following claim: suppose that we are given i-low polynomials v_i, $1 \leq i \leq N$. Then there exist i-low polynomials w_i, $1 \leq i \leq N$, such that for all $1 \leq n \leq N$ and $x_1, \ldots, x_N \in \overline{k}$ we have the equality

$$u_{a_n}(-x_n)\left(\prod_{i=1}^{N} u_{a_i}(x_i^q + v_i(\mathbf{x}))\right) = \left(\prod_{i=1}^{N} u_{a_i}(x_i^q + w_i(\mathbf{x}))\right). \tag{3}$$

In fact, we will prove the following stronger claim which will facilitate an inductive argument: suppose that $r \leq n \leq N$ are positive integers and we are given i-low polynomials v_i, $r \leq i \leq N$,

and an n-low polynomial v. Then there exist i-low polynomials w_i, $r \leq i \leq N$, such that for all $x_1, \ldots, x_N \in \overline{k}$ we have the equality

$$u_{a_n}(v(\mathbf{x})) \left(\prod_{i=r}^{N} u_{a_i}(x_i^q + v_i(\mathbf{x})) \right) = \left(\prod_{i=r}^{N} u_{a_i}(x_i^q + w_i(\mathbf{x})) \right). \tag{4}$$

Indeed, (3) follows from this in the case that $r = 1$ and $v(\mathbf{X}) = -X_n$: note that this polynomial is n-low because $q > 1$. We will first use downward induction on r, then complete the proof by downward induction on n.

As a precursor, recall the commutation relations for root groups (see [Con14, 5.1.14]): given roots $a, b \in \Phi^+$ and an ordering on the set of roots of the form $da + eb$ for positive integers d and e (below, we will always take this to be the induced order on Φ^+ defined above), we have

$$u_a(x)u_b(y)u_a(-x)u_b(-y) = \prod_{d,e>0} u_{da+eb}\left(C_{d,e,a,b}x^d y^e\right),$$

for all $x, y \in \overline{k}$, where $C_{d,e,a,b} \in k$ and the product is taken over all *roots* $da + eb$ with $d, e > 0$ in the prescribed order. In particular, this implies

$$u_a(x)u_b(y) = \left(\prod_{d,e>0} u_{da+eb}\left(C_{d,e,a,b}x^d y^e\right) \right) u_b(y)u_a(x). \tag{5}$$

Roughly speaking, (5) will allow us to push the term $u_{a_n}(v(\mathbf{x}))$ to the right in (4). For convenience (and to shorten the long equations which follow) we will use the notation

$$h_{a,b}(x, y) = \prod_{d,e>0} u_{da+eb}\left(C_{d,e,a,b}x^d y^e\right).$$

First suppose $n = N$. Then a_N is the longest root in Φ (see [Bou68, VI, 1.8] for a discussion) and thus the commutation relations (5) show that $u_{a_N}(v(\mathbf{x}))$ lies in the center of U^+. In particular, we see that

$$u_{a_N}(v(\mathbf{x})) \left(\prod_{i=r}^{N} u_{a_i}(x_i^q + v_i(\mathbf{x})) \right) = \left(\prod_{i=r}^{N} u_{a_i}(x_i^q + v_i(\mathbf{x})) \right) \cdot u_{a_n}(x_N^q + v_N(\mathbf{x}) + v(\mathbf{x})),$$

so we may take $w_i = v_i$ for all $i < N$ and $w_N = v_N + v$.

Now we use downward induction on r. In the case $r = N$, the assumed inequalities imply that $n = N$, so the result follows from the previous paragraph. So suppose that $r < N$ and that the desired result holds for all $r' > r$. We will now prove (4) by downward induction on n, the case $n = N$ following once again from the previous paragraph. So suppose that $n < N$ and that the result in (4) holds for all $n' > n$. Using the commutation relation (5), we have

$$u_{a_n}(v(\mathbf{x})) \left(\prod_{i=r}^{N} u_{a_i}(x_i^q + v_i(\mathbf{x})) \right) = h_{n,r}(v(\mathbf{x}), x_r^q + v_r(\mathbf{x}))u_{a_r}(x_r^q + v_r(\mathbf{x})) \cdot u_{a_n}(v(\mathbf{x})) \left(\prod_{i=r+1}^{N} u_{a_i}(x_i^q + v_i(\mathbf{x})) \right)$$

Since the result holds for $r + 1$, there exist some i-low polynomials w_i' such that

$$u_{a_n}(v(\mathbf{x})) \left(\prod_{i=r+1}^{N} u_{a_i}(x_i^q + v_i(\mathbf{x})) \right) = \prod_{i=r+1}^{N} u_{a_i}(x_i^q + w_i'(\mathbf{x})).$$

From the definition of $h_{n,r}$ we have

$$h_{n,r}(v(\mathbf{x}), x_r^q + v_r(\mathbf{x})) = \prod_{d,e>0} u_{da_n+ea_r}(C_{d,e,a_n,a_r} v(\mathbf{x})^d (x_r^q + v_r(\mathbf{x}))^e).$$

Let d, e, and L be such that $a_L = da_n + ea_r$. The term of lowest weight in the polynomial $v(\mathbf{X})^d(X_r^q + v_r(\mathbf{X}))^e$ has weight strictly less than $qda_M + qea_r = a_L$, so

$$v'(\mathbf{X}) = C_{d,e,a_n,a_r} v(\mathbf{X})^d (X_r^q + v_r(\mathbf{X}))^e$$

is an L-low polynomial. Since $|a_n| < |a_L|$, the choice of ordering on Φ^+ guarantees $n < L$. A repeated application of our inductive hypothesis and the displayed equations in this paragraph thus show that (4) holds in general. □

4. The Steinberg Representation

Let G be a connected reductive group of rank ℓ over a finite field k of $q = p^r$ elements, and assume that G is simply connected. Let B be a Borel k-subgroup of G, let T be a maximal k-torus contained in B, and let U be the unipotent radical of B. Steinberg proved that there exists an irreducible $\overline{k}$-representation V of $G(k)$ of degree $q^{\dim U}$, and by Theorem 3.6 there must exist some $\lambda \in X_r(T)$ such that $V = L(\lambda)$. The Weyl character formula (valid in characteristic p by [Jan03, II, 5.10]) states

$$\dim H^0(\lambda) = \prod_{\alpha \in \Phi^+} \frac{(\rho + \lambda, \alpha)}{(\rho, \alpha)}$$

whenever $\lambda \in X(T)_+$, where as usual ρ is half the sum of the positive roots. Since $\lambda < \mu$ implies $(\lambda, \alpha) \leq (\mu, \alpha)$ for all $\alpha \in \Phi^+$ with strict inequality for at least one $\alpha \in \Phi^+$ it follows that $\dim H^0(\lambda) < \dim H^0(\mu)$ in this case. Moreover, note

$$\dim H^0((q-1)\rho) = \prod_{\alpha \in \Phi^+} \frac{(q\rho, \alpha)}{(\rho, \alpha)} = q^{|\Phi^+|} = q^{\dim U}.$$

Since $(q-1)\rho$ is the maximum element of $X_r(T)$, it follows purely from dimension considerations that $L((q-1)\rho) = H^0((q-1)\rho) = V$. In particular, V arises via reduction modulo p from an irreducible representation in characteristic 0, and it is self-dual. This is quite important in applications; it is used, for instance, in the proofs of Kempf's vanishing theorem and Haboush's theorem. The latter theorem is used crucially in the following characterization of reductivity, at least in characteristic p.

Theorem 4.1 (Borel–Richardson)**.** Let G be a connected reductive group over a field k. If $H \subset G$ is a smooth k-subgroup of G, then H is reductive if and only if G/H is affine.

References

[Bou68] N. Bourbaki. *Éléments de mathématique. Fasc. XXXIV. Groupes et algèbres de Lie. Chapitre IV: Groupes de Coxeter et systèmes de Tits. Chapitre V: Groupes engendrés par des réflexions. Chapitre VI: systèmes de racines.* Actualités Scientifiques et Industrielles [Current Scientific and Industrial Topics], No. 1337. Hermann, Paris, 1968.

[CGP15] B. Conrad, O. Gabber, and G. Prasad. *Pseudo-reductive groups*, volume 26 of *New Mathematical Monographs*. Cambridge University Press, Cambridge, second edition, 2015. doi:10.1017/CBO9781316092439.

[Con14] B. Conrad. Reductive group schemes. In *Autour des schémas en groupes. Vol. I*, volume 42/43 of *Panor. Synthèses*, pages 93–444. Soc. Math. France, Paris, 2014.

[Con20] B. Conrad. Algebraic groups II. https://www.ams.org/open-math-notes/omn-view-listing?listingId=110663, 2020.

[Hum06] J. E. Humphreys. *Modular representations of finite groups of Lie type*, volume 326 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2006.

[Jan87] J. C. Jantzen. Representations of Chevalley groups in their own characteristic. In *The Arcata Conference on Representations of Finite Groups (Arcata, Calif., 1986)*, volume 47 of *Proc. Sympos. Pure Math.*, pages 127–146. Amer. Math. Soc., Providence, RI, 1987. doi:10.1016/s0022-4049(99)00142-5.

[Jan03] J. C. Jantzen. *Representations of algebraic groups*, volume 107 of *Mathematical Surveys and Monographs*. American Mathematical Society, Providence, RI, second edition, 2003.

[Ser77] J.-P. Serre. *Linear representations of finite groups*. Graduate Texts in Mathematics, Vol. 42. Springer-Verlag, New York-Heidelberg, 1977. Translated from the second French edition by Leonard L. Scott.

[Ste63] R. Steinberg. Representations of algebraic groups. *Nagoya Math. J.*, 22:33–56, 1963. URL http://projecteuclid.org/euclid.nmj/1118801156.