STEINBERG'S THEOREM

SEAN COTNER

1. Introduction

Recall that for a field k, we say $\dim k \leq 1$ if every finite-dimensional division algebra over k is commutative. For some equivalent conditions, see [Ser02, Chap. II, Sec. 3.1, Prop. 5]. If k is perfect, it is equivalent that k has cohomological dimension at most 1, but in the imperfect case this is not quite the case. Two simple examples of fields k with $\dim k \leq 1$ are as follows:

- Finite fields: this is Wedderburn's little theorem.
- The maximal unramified extension K^{un} of a non-archimedean local field K: this follows from a result in local class field theory which states that every finite-dimensional division algebra over such a field splits after a finite unramified extension. This is the main case of interest in Bruhat-Tits theory.

We aim to prove the following theorem of Steinberg, proved in [Ste65]:

Theorem 1.1. *Let k be a field with $\dim k \leq 1$. If G is a connected reductive group over k, then $H^1(k, G) = 0$.*

For k a finite field, this is a consequence of Lang's theorem, a sharper result which states that $H^1(k, G) = 0$ for all connected algebraic groups G, not necessarily affine. In [Ser02, Chap. III, Sec. 2.3], Steinberg's theorem in the case that k is infinite is deduced in a self-contained way from the following general theorem:

Theorem 1.2. *Let k be a field. Let G be a quasi-split semisimple connected group over k and let C be a conjugacy class in $G(k_s)$ consisting of regular semisimple elements. If C is stable under the action of $\mathrm{Gal}(k_s/k)$, then it contains an element of $G(k)$.*

We will reproduce the deduction of Theorem 1.1 from Theorem 1.2 in the final section. The crux of the proof of Theorem 1.2 is the existence of a *variety of regular classes* V of G isomorphic to an affine space, and a natural map $G \to V$. We will find a section to this map in every case in which G does not contain any simple component of type A_{2m} and a complicated replacement for a section in the case of A_{2m}.

Because the only goal of this paper is to prove Theorem 1.1, we have avoided the notion of regular unipotent element which is analyzed extensively in [Ste65]. Although this is very natural in the theory and leads to many beautiful results, it is not ultimately necessary to the final result and thus has been excised.

This note was written in late 2020 and early 2021 in order to give an exposition of Steinberg's theorem. Since then, it has only been edited for formatting. All substantial ideas are due to Steinberg, and most are contained in [Ste65].

2. Background in reductive groups

In this section we gather several facts from the theory of reductive groups which we will use without further reference in what follows. Let G be a connected reductive group over a field k. If G is split and B is a Borel k-subgroup of G containing a split maximal torus T, then we let $W = N_G(T)/T$ denote the Weyl group of G, a finite constant k-group which we will frequently identify with its underlying abstract group of k-points. This is the Weyl group in the sense of

[Bou68, Chap. VI] for the root system $\Phi = \Phi(G,T)$ of T-weights on the Lie algebra $\mathfrak{g} = \mathrm{Lie}(G)$. Let $\Phi^+ = \Phi(B,T)$ and Δ denote the system of positive roots and the system of simple roots, respectively, corresponding to B. Let $\Phi^\vee$ denote the set of coroots, lying in the cocharacter lattice $X_*(T) = \mathrm{Hom}_k(\mathbf{G}_m, T)$; we say that G is **simply connected** if $\mathbf{Z}(\Phi^\vee)^* = X^*(T)$. Note that this implies that G is semisimple. In general, if G is not necessarily split, we say that G is simply connected if G_{k_s} is simply connected. By [Con22, Cor. M.1.2], every simply connected group is isomorphic to a product $\prod_i R_{k_i/k} G_i$ for finite separable extensions k_i/k and absolutely simple connected semisimple k_i-groups G_i. Here $R_{k_i/k} G_i$ denotes the Weil restriction, see [CGP15, Sec. A.5].

The case of simply connected semisimple connected groups G will be the most important case in what follows, and in the split case we will often tacitly assume that we are given a maximal k-torus T contained in a Borel k-subgroup B of G.

Recall the *Bruhat decomposition* (see [Bor69, Thm. 14.12]) which states

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

Moreover, if $U'_w = U \cap w U^- w^{-1}$, where U is the unipotent radical of B and U^- is the unipotent radical of the opposite Borel U^-, then $BwB \cong U'_w \times U \times T$ as k-schemes. 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). 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 $t u_a(x) t^{-1} = u_a(a(t)x)$ 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 (see [Con20, Lem. 24.3.3]).

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 connected.*

Proof. We may and do assume that k is algebraically closed. By [Con22, Thm. 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. 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 $x \in B(k)wB(k)$ for some $w \in W$, then $g = whw^{-1}$.*

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

$$wugu^{-1}w^{-1} = u'^{-1} g u' = u'^{-1}(gu'g^{-1})g.$$

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

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. Let $x \in Z_G(g)(k)$. Using the Bruhat decomposition and the fact that T centralizes g, we may assume $x = u'wu$ for some $w \in W$, $u' \in U'_w(k)$, and $u \in U(k)$. By the previous lemma, $wgw^{-1} = g$. Write $u = \prod_{a \in \Phi^+} u_a(x_a)$ and $u' = \prod_{a \in \Phi'_w} u_a(x'_a)$, so that

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

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

$$g(w^{-1}u'wu)g^{-1} = w^{-1}u'wu.$$

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, $w^{-1}u'wu$ is a product of elements of $U_a(k)$ for roots $a \in \Phi$ such that $a(g) = 1$. □

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 $n_a g n_a^{-1} = g$, 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.

Now suppose that G is simple and 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 rank 1 and indeed $Z_G(T_a) \cong \mathrm{GL}_2 \times D$ for a central torus D. Since T centralizes g, we may choose n_a to lie in the copy of GL_2. Letting $g = hd$ for $h \in \mathrm{GL}_2(k)$ and $d \in D(k)$, it follows that $n_a h n_a^{-1} = h$ and thus we are in the situation of the previous paragraph since $a|_D$ is trivial. □

Recall that, with notation as in the proof of the lemma, for any root $a \in \Phi$ the group $\mathscr{D}(Z_G(T_a)) \cong \mathrm{SL}_2$ is generated by the root groups U_a and U_{-a}. As these are both connected, 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 [Con22, Prop. 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 $X_*(T) = Q(\Phi^\vee)$, where $Q(\Phi^\vee)$ is the subgroup of $X_*(T)$ generated by the set of coroots $\Phi^\vee$. We are thus reduced finally to the following lemma, appearing as [Bou68, Chap. VI, Section 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 $w(x) - x \in Q(\Phi)$, 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, Chap. VI, no. 2.1]. By [Bou68, Chap. VI, no. 2.1, Prop. 1], W_a is the semidirect product of W and the group of translations of V corresponding to elements of $Q(\Phi)$, 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 underlying linear automorphism of V. By [Bou68, Chap. V, no. 3.2, Thm. 1] and [Bou68, Chap. VI, no. 2.1, Prop. 2], W_a is a Coxeter group and thus by [Bou68, Chap. V, no. 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, Lemma 3.9], which contains a very brief sketch of a proof attributed to Springer; the proof that we describe is an elaboration of the proof given there.

We now briefly describe the representation theory of split connected semisimple groups G. Let B^- denote the opposite Borel of B (see [CGP15, Prop. 3.3.5]). We say that $\lambda \in X^*(T)$ is a **dominant root** if $\langle \lambda, \alpha^\vee \rangle \geq 0$ for all $\alpha \in \Delta$. The set of all dominant roots will be denoted $X^*(T)_+$. For every $\lambda \in X^*(T)_+$ 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, Part II, Prop. 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 U^- denotes the unipotent radical of B^- and $w_0 \in W$ is the long Weyl element, then also $H^0(\lambda)^{U^-}$ is the $w_0\lambda$-eigenspace in $H^0(\lambda)$, and the dimension of this subspace is 1.

For each $\alpha \in \Phi^+$, choose an isomorphism $u_\alpha : \mathbf{G}_a \to U_\alpha$, where U_α is the unique smooth connected unipotent k-subgroup of G on whose Lie algebra T acts via the character α. Moreover, choose $n_\alpha \in G_\alpha = \mathscr{D}(Z_G((\ker \alpha)^0_{\mathrm{red}}))$ normalizing T and representing the reflection corresponding to α in the Weyl group of (G, T). It follows from the Bruhat decomposition that the n_α and U_α for $\alpha \in \Phi^+$ generate G as an algebraic k-group.

Lemma 2.7. *Let $V = L(\lambda)$ be a simple G-module, so that $V = \bigoplus_{\omega \in X^*(T)} V_\omega$ as T-modules, where V_ω is the ω-eigenspace for T. The k-vector space V admits a basis relative to which each n_α acts integrally and each $u_\alpha(c_\alpha)$ acts as a polynomial in c_α with integral coefficients.*

Proof. By the Existence Theorem [Con14, Thm. 6.1.16(2)], there is some split semisimple group $\mathscr{G}$ over $\mathbf{Z}$ such that $G = \mathscr{G} \otimes_{\mathbf{Z}} k$. The k-representation $H^0(\lambda)$ of G is the base change of a $\mathbf{Z}$-representation W_λ of $\mathscr{G}$ (see [Jan03, Part II, Chap. 8]). The root groups U_α, isomorphisms u_α, and Weyl elements can be defined over $\mathbf{Z}$ by [Con14, Prop. 5.1.6], so this is immediate. □

The condition that the split connected semisimple k-group G be simply connected is equivalent to the condition that the coroot lattice $\mathbf{Z}\Phi^\vee$ be equal to the cocharacter lattice $X_*(T)$, with basis given by $\Delta^\vee$. In this case the dual $(\mathbf{Z}\Phi^\vee)^*$ is equal to $X^*(T)$ and we say that $\omega \in X^*(T)$ is a **fundamental weight** for T precisely when $\omega \in (\Delta^\vee)^*$; the fundamental weights evidently form a $\mathbf{Z}$-basis for $X^*(T)$, and whenever we deal with simply connected groups below we will choose an enumeration $\omega_1, \dots, \omega_r$ of these fundamental weights. We will also let $\chi_i : G \to \mathbf{A}^1_k$ denote the character obtained as the trace of the representation of G with highest weight ω_i, called the ith fundamental representation; we will call this χ_i a **fundamental character** for G.

Example 2.8. Let $G = \mathrm{SL}_{n+1}$, let T be the diagonal torus in G, and let B be the Borel subgroup consisting of the upper-triangular matrices in G. The fundamental weights of T may be computed to be given by

$$\omega_i(\mathrm{diag}(t_1, \dots, t_{n+1}) = t_1 \cdots t_i$$

for $1 \leq i \leq n$. The corresponding fundamental representations of G are then given by the wedge powers $\bigwedge^k V$ of the standard representation V of G; this will be important for us when dealing with the A_{2m} case alluded to in the introduction.

3. Class functions

Let G be a group scheme over a field k which acts on a k-scheme X. A G-**invariant function** on X is an element of $k[X]$ constant on orbits, i.e., it is a k-morphism $f : X \to \mathbf{A}^1_k$ such that the diagram

$$\begin{tikzcd} G \times X \arrow[r, "\alpha"] \arrow[d, "\mathrm{pr}_2"] & X \arrow[d, "f"] \\ X \arrow[r, "f"] & \mathbf{A}^1_k \end{tikzcd}$$

commutes, where $\alpha : G \times X \to X$ is the action map. If G is smooth over k, then it sufficient for this commutativity to hold on the level of $\overline{k}$-points, where $\overline{k}$ is an algebraic closure of k. We will denote the ring of G-invariant functions on X by $k[X]^G$. If $X = G$ and α is the conjugation action $\alpha(g, g') = gg'g^{-1}$, we will call a G-invariant function a **class function** and denote the ring of class functions by $C[G]$.

For the rest of this section, let G be a split semisimple connected group over a field k, and let T be a split maximal k-torus of G. Let $W = N_G(T)/T$ denote the Weyl group of (G, T), a finite constant k-group scheme acting on T. We will often identify W with the group $W(k)$.

Lemma 3.1. *The ring $k[T]^W$ is freely generated as a k-vector space by the irreducible characters of G restricted to T. If G is simply connected, then $k[T]^W$ is a polynomial algebra over k generated by the fundamental characters of G restricted to T.*

Proof. For a dominant root $\lambda \in X^*(T)_+$, let $\operatorname{sym}\lambda$ denote the sum of all distinct conjugates of λ under W. We will write $\lambda_1 < \lambda_2$ if $\lambda_1^{-1}\lambda_2$ is a sum of positive roots.

Since $T \cong \mathbf{G}_m^r$ for $r = \mathrm{rk}(G)$, we have $k[T] = k[X^*(T)]$. Recall that every element of $X^*(T)$ is W-conjugate to a unique element of $X^*(T)_+$ [Bou68, no. 1.5, Thm. 2], so the functions $\operatorname{sym}\delta$, $\delta \in D$, freely generate $k[T]^W$ as a k-vector space. By [Jan03, Part II, Cor. 2.7], there is a one-to-one correspondence between the elements of $X^*(T)_+$ and the irreducible representations of G; if $\delta \in D$, say that χ_δ is the corresponding irreducible character of G. The restriction of any character of G to T is evidently W-invariant, and indeed (see [Jan03, Part II, Prop. 2.2]) given $\delta \in D$ there are elements $c(\delta') \in k$ for all $\delta' \in D$, $\delta' < \delta$, such that $\chi_\delta|_T = \operatorname{sym}\delta + \sum_{\delta'<\delta} c(\delta') \operatorname{sym}\delta'$. This shows that the first claim holds.

If G is simply connected, then by the above every element of $X^*(T)_+$ is uniquely a $\mathbf{Z}_{\geq 0}$-linear combination of the fundamental weights ω_i. If $\delta = \sum_i n_i\omega_i$, then we have $\chi_\delta = \prod_i \chi_i^{n_i} + \sum_{\delta'<\delta} c(\delta')\chi_{\delta'}$ by [Jan03, Part II, Prop. 2.2], so by induction we see that that $\chi_i|_T$ generate $k[T]^W$ as a k-algebra. Moreover, the existence of the order above shows that the map $k[\{X_i\}] \to k[T]^W$ given by $X_i \mapsto \chi_i|_T$ is injective, so the second statement also holds. $\square$

Theorem 3.2. *The ring $C[G]$ is freely generated as a k-vector space by the irreducible characters of G. If G is simply connected, then $C[G]$ is a polynomial algebra over k generated by the fundamental characters of G.*

Proof. First, we claim that two elements of $T(\overline{k})$ are $G(\overline{k})$-conjugate if and only if they are W-conjugate. To see this, let $t, t' \in T(\overline{k})$ and suppose that $gtg^{-1} = t'$ for some $g \in G(\overline{k})$. Let B be a Borel k-subgroup of G containing T, and let U be the unipotent radical of B; let U^- be the unipotent radical of the opposite Borel of B. By the Bruhat decomposition, there are some $w \in W$, $u \in U(\overline{k})$, $\widetilde{t} \in T(\overline{k})$ $u' \in U(\overline{k}) \cap w^{-1}U^-(\overline{k})w$ such that $g = u'wu\widetilde{t}$. Since T is commutative, we may assume that $\widetilde{t} = 1$, so that we obtain

$$wutu^{-1}w^{-1} = u'^{-1}t'u'.$$

Note that $wutu^{-1}w^{-1} = w(u(tu^{-1}t^{-1}))w^{-1}wtw^{-1}$ and $u(tu^{-1}t^{-1}) \in U(\overline{k})$, so $w(u(tu^{-1}t^{-1}))w^{-1}$ lies in the image of $U^-(\overline{k}) \times U(\overline{k})$ in $G(k)$ under multiplication. Similarly $u'^{-1}t'u' = u'^{-1}(t'u't'^{-1})t'$ and $u'^{-1}(t'u't'^{-1}) \in U^-(\overline{k})$. The multiplication morphism $U^- \times U \times T \to G$ is an open immersion, so it follows that $wtw^{-1} = t'$, and the claim is proved. From this it follows that there is a restriction map $\beta : C[G] \to k[T]^W$.

Suppose that $f \in C[G]$ is a class function such that $\beta(f) = 0$. Since every semisimple element of $G(\overline{k})$ is conjugate to an element of $T(\overline{k})$ [Con22, Thm. D.2.1], it follows that f vanishes on the set of semisimple elements of $G(\overline{k})$. These are the $\overline{k}$-points of a dense open subset of G, so it follows that $f = 0$, i.e., β is injective. By Lemma 3.1, β is clearly surjective, so it is an isomorphism and another application of Lemma 3.1 proves the Theorem. □

Corollary 3.3. *If $x \in G(\overline{k})$ and $x = x_s x_u$ is its Jordan decomposition, then $f(x) = f(x_s)$ for every class function $f \in C[G]$.*

Proof. This is true for every character f of G: using the functoriality of the Jordan decomposition [Con20, Thm. 13.1.7], this simply comes down to the fact that $\mathrm{tr}(yz) = \mathrm{tr}(y)$ if $y, z \in \mathrm{GL}_n(\overline{k})$ commute with y semisimple and z unipotent. □

Corollary 3.4. *Let $x, y \in G(k)$ be two semisimple elements of G. The following are equivalent:*

(1) x and y are conjugate.
(2) $f(x) = f(y)$ for all $f \in C[G]$.
(3) $\chi(x) = \chi(y)$ for all characters χ of G.
(4) $\rho(x)$ and $\rho(y)$ are conjugate for every representation ρ of G.

If G is simply connected, then 3) and 4) need only hold for the fundamental characters and representations of G.

Proof. Clearly 1 implies 4 implies 3 implies 2 by Theorem 3.2. To show that 2 implies 1, first note that we may conjugate x and y to assume that they lie in T. Since W is a finite group of automorphisms of T, the $\overline{k}$-points of the scheme $T/W = \operatorname{Spec} k[T]^W$ are the same as the W-orbits in $T(\overline{k})$ (since T/W is by definition the ringed space quotient), and it follows that $k[T]^W$ separates W-orbits in $T(\overline{k})$, and thus 2 implies 1. □

We come now to a very important construction. Assume that G is simply connected, and define a morphism $p : G \to \mathbf{A}^r_k$ functorially via $p(x) = (\chi_1(x), \ldots, \chi_r(x))$. We will retain this notation in all that follows. We say that a semisimple element $x \in G(k)$ is **regular** if the scheme-theoretic centralizer $Z_G(x)$ is a torus.

Corollary 3.5. *If $c \in \overline{k}^r$, then $p^{-1}(c)$ is closed in $G_{\overline{k}}$; it is a union of conjugacy classes of $G(\overline{k})$, and it contains a unique semisimple class, which is closed. If $p^{-1}(c)$ contains a regular semisimple element, then it is irreducible.*

Proof. The only point not following immediately from the definitions and the preceding two corollaries is the final one. Suppose that $p(x) = c$ for some regular semisimple element $x \in G(\overline{k})$. By Corollary 3.3, every element in $p^{-1}(c)$ has semisimple part a conjugate of x, so because $Z_G(x)$ is a torus (by Theorem 2.1) we see that $p^{-1}(c)$ is the conjugacy class of x; in particular, it is irreducible since it is the set-theoretic image of the morphism $G \to G$, $g \mapsto gxg^{-1}$. □

Remark 3.6. In [Ste65, Thm. 6.11], it is proved, among other things, that in fact *every* fiber of the map p is irreducible, using the existence of regular unipotent elements. Since we are trying to avoid using this result, we can only prove the weaker statement above.

4. The Steinberg section

For this section, unless mention is made to the contrary we will assume that G is a simply connected split semisimple connected group of rank r over a field k and that T is a split maximal k-torus contained in a Borel k-subgroup B of G. Let $\{\alpha_i : 1 \le i \le r\}$ be a system of simple roots and for each i let $U_i = U_{\alpha_i}$ be the root group corresponding to the simple root and let $n_i \in N_G(T)(k)$ be an element reducing to the reflection w_i corresponding to α_i in the Weyl group. For each i let $u_i : \mathbf{G}_a \to U_i$ be an isomorphism of k-groups. Let $N = \prod_{i=1}^r (U_i n_i)$.

Theorem 4.1. *The scheme N is closed and irreducible in G. The natural morphism $\varphi : \mathbf{A}_k^r \to N$, $\varphi((c_i)) = \prod_{i=1}^r u_i(c_i) n_i$, is an isomorphism of k-schemes.*

First, we need the following two lemmas.

Lemma 4.2. *Let $\beta_i = w_1 w_2 \cdots w_{i-1} \alpha_i$ for $1 \le i \le r$ and $w = w_1 \cdots w_r$.*
(1) The roots β_i are positive, distinct, and independent.
(2) The β_i form the set of positive roots which become negative under w^{-1}.
(3) The sum of any two of the β_i is never a root.

Proof. The first two statements are [Bou68, Chap. VI, Cor. 2 à Prop. 17]; the third follows from the second because the sum of two β_i is positive and becomes negative under w^{-1}. □

Lemma 4.3. *The product $\prod_{i=1}^r U_{\beta_i}$ in U is direct, and if U_w is this product and $n_w = n_1 n_2 \cdots n_r$, then $N = U_w n_w$.*

Proof. The first statement follows from the fact that the β_i are positive and independent, see [CGP15, Thm. 3.3.11]. Note that $U_{\beta_i} = n_1 \cdots n_{i-1} U_i n_{i-1}^{-1} \cdots n_1^{-1}$, so

$$\prod_{i=1}^r U_{\beta_i} = U_1 n_1 U_2 n_2 \cdots U_r n_{r-1}^{-1} \cdots n_1^{-1},$$

and this gives the final equality. □

Proof of theorem. By the previous lemma and the fact that each $u_i : \mathbf{G}_a \to U_i$ is an isomorphism, this theorem follows immediately. □

Now define $G_i = \mathscr{D}(Z_G(\ker(\alpha_i)^0_{\mathrm{red}}))$, so that G_i is isomorphic to SL_2. Throughout the rest of this note, we will assume that we have chosen $n_i \in G_i$ to have order 4.

Theorem 4.4. *If G is simply connected, then the restriction of p to N induces an isomorphism $N \to \mathbf{A}_k^r$.*

Since G is simply connected, $X^*(T)_+$ is the set $\{\sum_{j=1}^r m_j \omega_j : m_j \ge 0 \text{ for all } j\}$, where $\{\omega_j\}_{j=1}^r$ is the set of fundamental weights, i.e., the basis of $X^*(T)$ dual to the basis $\{\alpha_j^\vee\}_{j=1}^r$ of $X_*(T)$. If $\omega = \sum_{j=1}^r m_j \omega_j$ for some integers m_j, then we will write $m_j(\omega) := m_j$.

We now define $\omega_i \prec \omega_j$ precisely when $i \ne j$ and there exists a dominant weight ω such that $m_j(\omega) > 0$ and $\omega_i - \omega$ is a sum of positive roots.

Lemma 4.5. *The relation $\prec$ is a partial order on the set of fundamental weights.*

Proof. Suppose $\omega_k \prec \omega_j$ and $\omega_j \prec \omega_i$, so there exist $\omega, \omega' \in D$ such that $m_k(\omega) > 0$, $m_j(\omega') > 0$, and $\omega_j - \omega$, $\omega_i - \omega'$ are both sums of positive roots. Thus

$$(\omega_i - \omega') + (\omega_j - \omega) = \omega_i - (\omega + \omega' - \omega_j)$$

is a sum of positive roots, $\omega + \omega' - \omega_j \in D$ since $m_j(\omega') > 0$, and $m_k(\omega + \omega' - \omega_j) \ge m_k(\omega) > 0$. As elements of $X^*(T)_+$ are all positive, it follows also that $k \ne i$. □

Lemma 4.6. *Let $T_i = G_i \cap T$. There exists an isomorphism of schemes $\beta : T_i \to U_i - \{0\}$ such that $x = \beta(t)$ if and only if $(xtn_i)^3 = 1$.*

Proof. Since G is simply connected, $G_i \cong \mathrm{SL}_2$ in such a way that T_i is sent isomorphically to the diagonal torus and U_i is sent isomorphically to the upper triangular unipotent subgroup. Suppose that $t = \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$, $n_i = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, and $x = \begin{pmatrix} 1 & ba^{-1} \\ 0 & 1 \end{pmatrix}$ for some units a, b in a k-algebra A. Then we have

$$xtn_i = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & a^{-1} \\ -a & 0 \end{pmatrix}$$

and thus a simple calculation shows

$$(xtn_i)^3 = \begin{pmatrix} b^3 - 2b & a - ab^2 \\ a^{-1}b^2 - a^{-1} & -b \end{pmatrix}.$$

If this matrix is the identity, then evidently $b = -1$, and the converse is simple to see. Thus the morphisms β must be given on points by

$$\beta\left(\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}\right) = \begin{pmatrix} 1 & -a^{-1} \\ 0 & 1 \end{pmatrix}$$

where b is as above. $\square$

Proposition 4.7. *Suppose we have chosen $n_i \in G_i(k)$ of order 4 for all i. If β is as in Lemma 4.6, we normalize $u_i : \mathbf{G}_a \to U_i$ so that $u_i(-1) = \beta(1)$. Let $\psi_i : N \to \mathbf{A}^1_k$ be defined by $\psi_i(\prod_{j=1}^r u_j(c_j)n_j) = c_j$. Then there exist $f_i, g_i \in k[G]$ such that*

1. *f_i (resp. g_i) is a polynomial with integral coefficients in those ψ_j (resp. χ_j) with $\omega_j \prec \omega_i$.*
2. *On N we have $\chi_i = \psi_i + f_i$ and $\psi_i = \chi_i + g_i$.*

Proof of Theorem 4.4 using Proposition 4.7. Using the notation in Proposition 4.7 and regarding f_i and g_i as elements of $\mathbf{Z}[T_1, \ldots, T_r]$, we define maps $f, g : \mathbf{A}^r_k \to \mathbf{A}^r_k$ via

$$f(c_1, \ldots, c_r) = (c_1 + f_1(\mathbf{c}), \ldots, c_r + f_r(\mathbf{c}))$$

and

$$g(c_1, \ldots, c_r) = (c_1 + g_1(\mathbf{c}), \ldots, c_r + g_r(\mathbf{c})).$$

If $\psi = (\psi_1, \ldots, \psi_r)$ and $\chi = (\chi_1, \ldots, \chi_r)$ then by assumption we have

$$(f \circ \psi)(x) = (\psi_1(x) + f_1(\psi(x)), \ldots, \psi_r(x) + f_r(\psi(x))) = \chi(x)$$

and

$$(g \circ \chi)(x) = (\chi_1(x) + g_1(\chi(x)), \ldots, \chi_r(x) + g_r(\chi(x))) = \psi(x).$$

Since ψ is an isomorphism from N to $\mathbf{A}^r_k$, it follows that χ is also an isomorphism, proving Theorem 4.4. $\square$

Proof of Prop 4.7. We may and do assume $k = \overline{k}$. Fix $x \in N(k)$ and write $x = \prod_{j=1}^r y_j$ for $y_j = u_j(c_j)n_j$. For a fixed index i, let V_i be the vector space for the ith fundamental representation of G, i.e., the irreducible representation of G with character χ_i. For each character $\omega \in X^*(T)$, let V_ω be the ω-weight space of V_i for T, so that $V_i = \bigoplus_{\omega \in X^*(T)} V_\omega$ by complete reducibility of representations of split tori. We will calculate $\chi_i(x)$.

Lemma 4.8. *Let $\pi_\omega : V_i \to V_\omega$ be the projection coming from the weight space decomposition. Then $\pi_\omega x \pi_\omega = \prod_{j=1}^r (\pi_\omega y_j \pi_\omega)$ as operators on V_i and $\chi_i(x) = \sum_{\omega \in X^*(T)} \operatorname{tr} \pi_\omega x \pi_\omega$.*

Proof. Let $v \in V_\omega$. By [Jan03, Part II, 1.19(6)] and the fact that $n_i v \in V_{\omega - m_i(\omega)\alpha_i}$ we have

$$y_j v = n_j v + \sum_{n \geq 1} \psi_j(x)^n v_n$$

for some $v_n \in V_{\omega + (n - m_i(\omega))\alpha_i}$. We have then

$$\pi_\omega y_j v = n_j v$$

and similarly

$$\pi_\omega x v = \pi_\omega y_1 \cdots y_r v = n_1 \cdots n_r v = \prod_{j=1}^{r} (\pi_\omega y_j \pi_\omega) v,$$

so the first claim holds. For the second claim, note that $1 = \sum_\omega \pi_\omega$, so $x = \sum_\omega x\pi_\omega$ and thus

$$\chi_i(x) = \operatorname{tr} x = \sum_\omega \operatorname{tr} x\pi_\omega = \sum_\omega \operatorname{tr} x\pi_\omega^2 = \sum_\omega \operatorname{tr} \pi_\omega x \pi_\omega.$$

□

Lemma 4.9. *If $\omega = \omega_i$, then $\operatorname{tr} \pi_\omega x \pi_\omega = \psi_i(x)$. If $\omega \in X^*(T)_+$ and $\omega \neq \omega_i$, then $\operatorname{tr} \pi_\omega x \pi_\omega$ depends only on those $\psi_i(x)$ with $\omega_j \prec \omega_i$. If $\omega \notin X^*(T)_+$ then $\pi_\omega x \pi_\omega = 0$.*

Proof. Suppose first that $\omega = \omega_i$. Let v be a nonzero vector in V_ω, so $V_\omega = kv$. Let $v' = -n_i v$. Then $y_i = u_i(c_i) n_i$ stabilizes the k-subspace V' generated by v and v', and it maps these vectors onto $-v' + ac_i v$ and bv respectively, for some $a, b \in k$, independent of c_i. (This follows from the proof of Lemma 4.8.) Note that V' is stabilized by G_i since elements of the form $u_i(c_i)n_i$ generate $G_i(k)$, so that G_i acts faithfully on V' by semisimplicity. Since n_i has order 4 and U_i acts trivially on kv, we have $b = 1$. We have

$$\begin{aligned} y_i^3 v = y_i^2(-v' + ac_i v) &= y_i(-v + ac_i(-v' + ac_i v)) \\ &= -(-v' + ac_i v) + ac_i(-v + ac_i(-v' + ac_i v)) \\ &= (1 - a^2 c_i^2) v' + (a^3 c_i^3 - 2ac_i) v \end{aligned}$$

and also

$$\begin{aligned} y_i^3 v' = y_i^2(v) = y_i(-v' + ac_i v) &= -v + ac_i(-v' + ac_i v) \\ &= -ac_i v' + (a^2 c_i^2 - 1) v, \end{aligned}$$

so clearly $y_i^3 = 1$ on V' if and only if $a^2 c_i^2 - 1 = 0$ and $a^3 c_i^3 - 2ac_i = -ac_i = 1$. This in turn is equivalent to $ac_i = -1$. By our normalization of β (see Lemma 4.6) and the fact that $y_i^3 = 1$ if and only if $u_i(c_i) = \beta(1)$, this is the case if and only if $c_i = -1$, so this gives $a = 1$. So $\pi_\omega y_i \pi_\omega v = c_i v$. If $j \neq i$, then $w_j \omega = \omega$, so U_j and n_j fix kv, so G_j fixes kv, so it is the identity on kv since $\mathscr{D}(G_j) = G_j$. So by (2) we have

$$\pi_\omega x \pi_\omega v = \left(\prod_{j=1}^{r} \pi_\omega y_j \pi_\omega \right) v = c_i v = \psi_i(x) v,$$

whence the first claim.

Now suppose that $\omega \in X^*(T)_+$ and $\omega \neq \omega_i$. Since ω_i is the highest weight of V_i it follows from Lemma 4.8 that $\pi_\omega x \pi_\omega$ depends only on those $\psi_j(x)$ with $m_j(\omega) > 0$. Since ω, being a weight for V_i, has the property that $\omega_i - \omega$ is a sum of positive roots, we get the second claim by definition of the $\prec$ relation.

Finally, suppose $\omega \notin X^*(T)_+$. If j is such that $m_j(\omega) < 0$, then $\pi_\omega y_j \pi_\omega = 0$, so this follows from Lemma 4.8. □

By Lemma 2.7 the function χ_i is a polynomial in the ψ_j with integral coefficients. Now to prove the lemma, we just combine Lemmas 4.8 and 4.9 to get the f_i and then solve $\chi_i = \psi_i + f_i$ recursively for the ψ_i to obtain the assertions about the g_i. □

Corollary 4.10. *Let C be a conjugacy class in G such that $C(\bar{k})$ consists of regular semisimple elements, i.e., C is the set-theoretic image of the map $G \to G$, $g \mapsto gxg^{-1}$ for some regular semisimple element $x \in G(k)$. Then $C \cap N$ is scheme-theoretically a single k-point.*

Proof. By Corollary 3.5, $C = p^{-1}(p(C))_{\mathrm{red}}$ (in fact, no reduction is necessary, but we do not need this finer point), so that $C \cap N$ is indeed a single k-point by Theorem 4.4. $\square$

Example 4.11. If $G = \mathrm{SL}_{r+1}$, then the function f_i is 0.

Proof. Let $V_i = \bigoplus_{\omega \in X^*(T)} V_\omega$, so by Example 2.8 we have $V = \bigwedge^i k^{r+1}$. Note that V_ω is nonzero precisely when ω is defined by $\omega(\mathrm{diag}(t_1, \ldots, t_{r+1})) = t_{j_1} \cdots t_{j_i}$ for $1 \le j_1 < \cdots < j_i \le r+1$, and this is a dominant weight precisely when $\omega = \omega_i$. Thus the claim follows directly from Lemma 4.9. $\square$

In the last part of this section, we will deduce Theorem 1.2 for any simply connected quasi-split semisimple connected k-group with no simple component of type A_{2n}; the case of A_{2n} is rather different will be taken up in the next section. Let $\Gamma = \mathrm{Gal}(k_s/k)$.

Theorem 4.12. *Let G be a simply connected quasi-split semisimple connected k-group with no simple component of type A_{2n}, and let B be a Borel k-subgroup of G. Enumerate the simple absolute roots α_i corresponding to B so that roots in the same Γ-orbit are adjacent. Then the closed subscheme N_{k_s} of G_{k_s} is Γ-stable and thus descends to a closed subscheme N of G.*

Proof. Let T be a maximal k-torus contained in B. To show that N_{k_s} is $\mathrm{Gal}(k_s/k)$-stable, it suffices to show that the product of the $U_j n_j$ over any single orbit is Γ-stable. So we will assume that $\alpha_1, \ldots, \alpha_\ell$ forms a single Γ-orbit in Φ. Note that Γ permutes the closed subschemes $U_{i,k_s} n_i$ of G_i, and these subschemes *pairwise commute* because the only Dynkin diagram with an automorphism sending one root to a distinct adjacent root is the Dynkin diagram of type A_{2n}. Thus indeed $\prod_{i=1}^{\ell} U_{i,k_s} n_i$ is Γ-stable, as desired. $\square$

Proof of Theorem 1.2 away from type A_{2m}. Let G be as in the statement of Theorem 1.2 and suppose that G has no simple component of type A_{2m}. Let $\overline{C}$ be a Γ-stable conjugacy class in $G(k_s)$ consisting of regular semisimple elements, so that $\overline{C}$ is the set of k_s points of some closed subscheme C of G. By Corollary 4.10, the intersection $C_{k_s} \cap N_{k_s}$ is scheme-theoretically a single k_s-point, so indeed $C \cap N$ is a single k-point and $\overline{C}$ contains a k-point. $\square$

5. The case of A_{2m}

Throughout this section, until mention is made to the contrary, G is a simply connected split semisimple connected group over a field k, and moreover G is simple of type A_{2m} for some $m \ge 1$. Choosing a maximal k-torus T contained in a Borel k-subgroup B of G, we will order the simple roots $\alpha_1, \ldots, \alpha_{2m}$ as they are ordered in the Dynkin diagram. As we saw in the previous section, the failure of $N = \prod_{i=1}^{2m} U_i \alpha_i$ to descend to k came essentially from the existence of an automorphism of the Dynkin diagram exchanging the two non-orthogonal roots α_m and α_{m+1}. In this section we will construct two subschemes N_1, N_2 of G, very similar to N, with the property that $p|_{N_1}$ is a *closed immersion*, $p|_{N_2}$ is an *open immersion*, and the images of these cover $\mathbf{A}_k^{2m}$. It is not clear whether an honest section to p exists in the case of A_{2m}, and we will not need it; once we have constructed N_1 and N_2, Theorem 1.2 will follow in the case of A_{2m} immediately as in the previous section.

We proceed to the construction of N_1 and N_2. Let $\alpha = \alpha_m + \alpha_{m+1}$, let $G_\alpha = \mathscr{D}(Z_G((\ker \alpha)^0_{\mathrm{red}}))$, and let T_α be the maximal torus of G_α contained in T. Let n_α be an element of $N_G(T)(k)$ corresponding to the reflection relative to α in the Weyl group. Choose elements $x_m \in U_m(k) - \{0\}$ and $x_{m+1} \in U_{m+1}(k) - \{0\}$ and set

$$N_1 = U_\alpha n_\alpha \prod_{j \ne m, m+1} U_j n_j$$

and

$$N_2 = x_{m+1}x_m U_\alpha n_\alpha T_\alpha \prod_{j\neq m,m+1} U_j n_j.$$

Note that the set $\Delta' = \{\alpha_1, \dots, \alpha_{m-1}, \alpha, \alpha_{m+2}, \dots, \alpha_{2m}\}$ forms a system of simple roots for a k-subgroup G' of G, simple of type A_{2m-1}, and N_1 is equal to the scheme N corresponding to G'.

Theorem 5.1. *Let $x_1, \dots, x_{2m}$ denote the coordinate functions on $\mathbf{A}_k^{2m}$. The restriction $p|_{N_1}$ is a closed immersion with image defined by the vanishing of $\sum_{i=1}^{2m}(-1)^i x_i$; the restriction $p|_{N_2}$ is an open immersion whose image is the open subscheme of $\mathbf{A}_k^{2m}$ defined by the non-vanishing of $\sum_{i=1}^{2m}(-1)^i x_i$.*

The proof will proceed just as in the proof of Theorem 4.4. In particular, there will be a direct analogue of Proposition 4.7.

Lemma 5.2. *The natural maps $U_\alpha \times \prod_{j\neq m,m+1} \to N_1$ and $U_\alpha \times T_\alpha \times \prod_{j\neq m,m+1} U_j \to N_2$ are isomorphisms of k-schemes.*

Proof. This follows immediately from the corresponding statement for N applied to G' above. □

We will prove the following two Propositions:

Proposition 5.3. *For $i \neq m, m+1$, let $\psi_i : N_1 \to \mathbf{A}_k^1$ be the composition of the projection onto U_i and u_j^{-1}, and similarly for ψ_α. Set $\psi_0 = \psi_{2m+1} = 0$. Then on N_1 we have*

(1) $\chi_i = \psi_i + \psi_{i-1}$ if $1 \leq i \leq m-1$,
(2) $\chi_i = \psi_i + \psi_{i+1}$ if $m+2 \leq i \leq 2m$,
(3) $\chi_m = \psi_\alpha + \psi_{m-1}$,
(4) $\chi_{m+1} = \psi_\alpha + \psi_{m+2}$.

Proposition 5.4. *For $i \neq m, m+1$, let $\psi_i : N_2 \to \mathbf{A}_k^1$ be the composition of the projection onto U_j and u_j^{-1}. Let $\psi_\alpha : N_2 \to \mathbf{A}_k^1$ be the composition of the projection onto U_α and u_α^{-1}. Assume that x_m, x_{m+1}, and u_α are normalized such that $u_\alpha^{-1}([x_{m+1}, x_m]) = 1$. Let φ_α be defined by the composition $N_2 \to T_\alpha \to \mathbf{G}_m$, where the second map is the character α_m, or equivalently α_{m+1}. Then on N_2 we have*

(1) $\chi_i = \psi_i + \psi_{i-1}$ if $1 \leq i \leq m-1$,
(2) $\chi_i = \psi_i + \psi_{i+1}$ if $m+2 \leq i \leq 2m$,
(3) $\chi_m = \varphi_\alpha\psi_\alpha + \psi_{m-1}$,
(4) $\chi_{m+1} = \varphi_\alpha + \varphi_\alpha\psi_\alpha + \psi_{n+2}$.

Proof of Theorem 5.1 from Propositions 5.3 and 5.4. First we deal with N_1. If $1 \leq i \leq m-1$ then

$$\psi_i = \sum_{j=1}^{i} (-1)^{j-i}\chi_i.$$

If $m+2 \leq i \leq 2m$, then

$$\psi_i = \sum_{j=i}^{2m} (-1)^{j-i}\chi_j.$$

These calculations and the results for χ_m, χ_{m+1} show that

$$\sum_{i=1}^{2m} (-1)^i \chi_i = 0.$$

Define a map $q : N_1 \to \mathbf{A}_k^{2m}$ by

$$q = (0, \psi_\alpha, \psi_1, \dots, \psi_{m-1}, \psi_{m+2}, \dots, \psi_{2m}),$$

and note that by Lemma 5.2 this map is a closed immersion onto the subscheme of $\mathbf{A}_k^{2m}$ defined by the vanishing of x_1. From the above calculations it thus follows that $p|_{N_1}$ is a closed immersion onto the subscheme defined by $\sum_{i=1}^{2m}(-1)^i x_i$, as desired.

Now we analyze the situation with N_2. The relations for ψ_i, $i \neq m, m+1$, are the same as for N_1. Moreover,

$$\varphi_\alpha = \chi_{m+1} - \chi_m + \psi_{m-1} - \psi_{m+2} = \pm \sum_{i=1}^{2m} (-1)^i \chi_i$$

and $\psi_\alpha = \varphi_\alpha^{-1}(\chi_m - \psi_{m-1})$. Define a map $r : N_2 \to \mathbf{A}_k^{2m}$ by

$$r = (\psi_\alpha, \varphi_\alpha, \psi_1, \dots, \psi_{m-1}, \psi_{m+2}, \dots, \psi_{2m})$$

and note that Lemma 5.2 shows that r is an open immersion onto the open subset of $\mathbf{A}_k^{2m}$ defined by the nonvanishing of the second coordinate. From the above calculations it therefore follows that $p|_{N_2}$ is an open immersion onto the open subset of $\mathbf{A}_k^{2m}$ defined by the nonvanishing of $\sum_{i=1}^{2m}(-1)^i x_i$, where x_i is the ith coordinate function. So we are done. $\square$

To prove Proposition 5.3, we require the following lemma.

Lemma 5.5. *Let ρ_i be the ith fundamental representation of G, and ρ'_i that of G', according to the ordering of Δ' given above. The restriction of ρ_i to G' is isomorphic to the direct sum of ρ'_i and ρ'_{i-1}, where ρ'_0 is the trivial representation.*

Proof. Identify $G = \mathrm{SL}(V)$ for some k-vector space V of dimension $2m+1$. If $V = V' \oplus V''$ for V', V'' of dimensions $2m$ and 1, respectively, then G' can be identified with the subgroup $\mathrm{SL}(V') \times \mathrm{SL}(V'')$. Then ρ_i is given by the natural representation of G on $\bigwedge^i V$, and similarly for G'. We have a canonical decomposition $\bigwedge^i V = \bigwedge^i V' \oplus (\bigwedge^{i-1} V' \otimes V'')$, so this gives the result. $\square$

Proof of Proposition 5.3. By the lemma, we have $\chi_i = \chi'_i + \chi'_{i-1}$, so Proposition 5.3 follows directly from Proposition 4.7 and Example 4.11. $\square$

For the proof of Proposition 5.4, we will again require a few lemmas.

Lemma 5.6. *Let $1 \leq i \leq m$. There exist precisely two weights ω such that $\langle \omega, \beta^\vee \rangle \geq 0$ for all $\beta \in \Delta'$, and $V_\omega \neq 0$. For both, $\dim V_\omega = 1$. One is the highest weight ω_i and the other, say ω'_i, pairs to 0 with all terms of $\Delta'^\vee$ except the $(i-1)$th.*

Proof. Indeed, a simple calculation following Example 2.8 shows that we must have $\omega'_i(\mathrm{diag}(t_1, \dots, t_{2m+1})) = t_1 \cdots t_{i-1} t_{i+1}$. $\square$

Let $x = y_\alpha \prod_{j \neq m, m+1} y_j = y_\alpha y$ be an element of N_2 with $y_\alpha \in x_{m+1} x_m U_\alpha n_\alpha T_\alpha$ and $y_j \in U_j n_j$.

Lemma 5.7. *For all $\omega \in X^*(T)$ we have*

$$\pi_\omega x \pi_\omega = \pi_\omega y_\alpha \pi_\omega \prod_{j \neq m, m+1} (\pi_\omega y_j \pi_\omega) = \pi_\omega y_\alpha \pi_\omega \cdot \pi_\omega y \pi_\omega.$$

Also,

$$\chi_i(x) = \pi_{\omega_i} x \pi_{\omega_i} + \pi_{\omega'_i} x \pi_{\omega'_i}.$$

Proof. The proof of this is entirely similar to the proof of Lemma 4.8 above. $\square$

Proof of Proposition 5.4. We begin by proving the identity 1. Since $1 \leq i \leq m-1$, both ω_i and ω'_i are orthogonal to α_m, α_{m+1}, and therefore α. So if $\omega = \omega_i$ or ω'_i and z lies in the rank 2 group generated by G_m and G_{m+1} then $\pi_\omega z \pi_\omega = 1$ on V_ω, so $\pi_\omega x \pi_\omega = \pi_\omega n_\alpha y \pi_\omega$ and so by Lemma 5.7 we have $\chi_i(x) = \chi_i(n_\alpha y)$. But now $n_\alpha y \in N_1$, so that this follows from Proposition 5.3.

Next we prove the identity 3. If $\omega = \omega'_m$, then ω is orthogonal to α, so $\pi_\omega x \pi_\omega = \pi_\omega n_\alpha y \pi_\omega$ as in the previous paragraph. Applying Example 4.11 to the representation ρ'_{m-1} of G' as in Lemma 5.5, we have

$$\operatorname{tr} \pi_\omega x \pi_\omega = \psi_{m-1}(x).$$

Suppose now $\omega = \omega_m$. Write $y_\alpha = x_{m+1} x_m x_\alpha n_\alpha t_\alpha$ and normalize the choices of n_m, n_{m+1} so that they lie in G_m, G_{m+1}, and $n_\alpha = n_{m+1} n_m n_{m+1}^{-1}$, as we may by a simple calculation in SL_3. Write $y_\alpha = z_1 z_2 z_3 t_\alpha$ with $z_1 = x_{m+1} n_{m+1}$, and $z_2 = n_{m+1}^{-1} x_\alpha n_\alpha n_{m+1}$, and $z_3 = n_{m+1}^{-1} n_\alpha^{-1} x_m n_\alpha$ (note that x_α and x_m commute, so this equality really holds). Then $z_1, z_3 \in G_{m+1}$ and $z_2 \in G_m$, as is seen by a simple calculation in SL_3. Note that t_α acts on V_ω by the scalar $\alpha_m(t_\alpha) = \varphi_\alpha(x)$. Because ω is orthogonal to α_{m+1} the factor z_3 can be suppressed, and independence of α_m and α_{m+1} shows that also z_1 can be suppressed. So

$$\pi_\omega x \pi_\omega = \varphi_\alpha(x) \pi_\omega z_2 \pi_\omega = \varphi_\alpha(x) \psi_\alpha(x)$$

on V_ω by Lemma 4.9. So Lemma 5.7 and the above calculations show that indeed $\chi_m = \varphi_\alpha \psi_\alpha + \psi_{m-1}$.

Finally we prove the identities 2 and 4. Let $\Phi : G \to G$ be an automorphism fixing T and interchanging the roots α_i and α_{2m+1-i} for all $1 \le i \le m$, as exists by the Isomorphism Theorem [Con14, Thm. 6.1.16(2)]. Applying Φ to the identities 1 and 3, we obtain 2 from 1 and 4 from 3, noting that in the latter case we must take the product of x_m and x_{m+1} in the opposite order, so x_α in the previous paragraph must be replaced by $[x_{m+1}, x_m] x_\alpha$. By the assumption on this commutator in Proposition 5.4, we obtain the extra term φ_α. □

Proof of Theorem 1.2. We have already dealt in the previous section with the case that G has no simple components of type A_{2m}, so we are reduced to the case that G is a product of simple groups of (absolute) type A_{2m}. We show that the closed subschemes N_1 and N_2 of G_{k_s} descend to closed k-subschemes of G. For N_1, this follows from the fact for N applied to G', which is $\mathrm{Gal}(k_s/k)$-stable in G_{k_s}. For N_2, note that $U_{m+1} U_m U_\alpha / U_\alpha$ is isomorphic to $\mathbf{G}_a \times \mathbf{G}_a$, so the additive Hilbert 90 shows that there exist x_m, x_{m+1} in $U_m(k_s)$, $U_{m+1}(k_s)$ such that the class of $x_{m+1} x_m$ in $U_{m+1} U_m U_\alpha / U_\alpha$ is $\mathrm{Gal}(k_s/k)$-stable. Thus indeed N_2 is $\mathrm{Gal}(k_s/k)$-stable. We will abuse notation and write N_1, N_2 for the corresponding closed k-subschemes of G as well.

Let C be a conjugacy class in G whose set of k_s-points consists of regular semisimple elements and let $x \in k_s^{2m}$ be the common image of the elements of C under p. Let $i \in \{1, 2\}$ be such that $x \in p(N_i(k_s))$, so that by Propositions 5.3 and 5.4 the scheme-theoretic intersection $C \cap N_i$ consists of a single k-point. This concludes the proof of Theorem 1.2. □

6. Proof of Theorem 1.1

We will need the following theorem, really a corollary of Theorem 1.2.

Theorem 6.1. *Let G be a quasi-split connected semisimple group over a field k. For each element $x \in H^1(k, G)$, there exists a maximal torus T of G such that x belongs to the image of $H^1(k, T) \to H^1(k, G)$.*

We deduce Theorem 1.1 from Theorem 6.1. Assume that $\dim k \le 1$, so that $H^1(k, T) = 0$ for all k-tori T by [Ser02, Chap. III, pf. of Thm. 1]. So we have $H^1(k, G) = 0$ for all quasi-split connected semisimple k-groups G by Theorem 6.1. In general, if H is any connected semisimple k-group, then we have $H \cong {}_a G$ for some quasi-split connected semisimple k-group G and a a 1-cocycle in the adjoint group $\overline{G}$ of G, see [Con14, Sec. 7.2]. But now $H^1(k, \overline{G})$ is trivial, so that $H \cong G$, i.e., H is quasi-split. Thus the result follows finally from [Ser02, Chap. III, Thm. 1].

Proof of Theorem 6.1. By Lang's theorem, we may assume that k is an infinite field. Let $a = (a_s)$ be a 1-cocycle of $\mathrm{Gal}(k_s/k)$ valued in $G(k_s)$ representing x. As G acts on itself by conjugation, it also acts on its universal cover $\widetilde{G}$ by automorphisms. Let $z \in {}_a\widetilde{G}(k)$ be a regular semisimple element, as exists because k is infinite. Let C be the conjugacy class of z in ${}_a\widetilde{G}(k_s) = \widetilde{G}(k_s)$. By the description of the Galois action on ${}_a\widetilde{G}(k_s)$ given in [Ser02, Chap. I, Sec. 5.3], it is clear that C is Galois-stable inside $\widetilde{G}(k_s)$. By Theorem 1.2 there is some $z_0 \in C \cap \widetilde{G}(k)$. Let $\widetilde{T}$ be the unique maximal k-torus of $\widetilde{G}$ containing z_0, and let T be its image in G, a maximal torus of G. By Theorem 2.1, the centralizer of z_0 is $\widetilde{T}$, so that the k_s-points of $\widetilde{G}/\widetilde{T} = G/T$ can be identified with the conjugacy class C. By contruction, the twist of $\widetilde{G}/\widetilde{T}$ by a contains the rational point z, so that ${}_aG/T$ has a rational point. Thus [Ser02, Chap. I, Prop. 37] shows that the class of a belongs to the image of $H^1(k, T)$ in $H^1(k, G)$. □

References

[Bor69] A. Borel. *Linear algebraic groups.* W. A. Benjamin, Inc., New York-Amsterdam, 1969. Notes taken by Hyman Bass.

[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*, volume No. 1337 of *Actualités Scientifiques et Industrielles [Current Scientific and Industrial Topics].* 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 i, 2020.

[Con22] B. Conrad. Reductive groups over fields (algebraic groups ii), 2022.

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

[Ser02] J.-P. Serre. *Galois cohomology.* Springer Monographs in Mathematics. Springer-Verlag, Berlin, english edition, 2002. Translated from the French by Patrick Ion and revised by the author.

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

[Ste65] R. Steinberg. Regular elements of semisimple algebraic groups. *Inst. Hautes Études Sci. Publ. Math.*, (25):49–80, 1965.