Math 249B. Applications of Borel's theorem on Borel subgroups

1. Motivation

In class we proved the important theorem of Borel that if G is a connected linear algebraic group over an *algebraically closed* field then $G(k)$ is covered by the groups $B(k)$ as B varies through the Borel subgroups of G. This is a vast generalization of the fact that every element of $\mathrm{GL}_n(k)$ can be upper-triangularized when k is algebraically closed.

The requirement for k to be algebraically closed cannot be dropped. To exhibit counterexamples over any $k \neq \overline{k}$, we use a fact to be proved later: if G is a split reductive group over a field k then all Borel k-subgroups are $G(k)$-conjugate, so all Borel subgroups of GL_n are $\mathrm{GL}_n(k)$-conjugate to the upper triangular Borel subgroup. Hence, if k is not algebraically closed and it admits a field extension K of degree $d > 1$, then for any $n \geq d$ the embedding of $K \times k^{n-d}$ into $\mathrm{Mat}_n(k)$ via a choice of k-basis puts $K^\times$ into $\mathrm{GL}_n(k)$ so that any $a \in K^\times \subset \mathrm{GL}_n(k)$ has characteristic polynomial $f_a(X)^{[K:k(a)]}(X-1)^{n-d}$ where $f_a \in k[X]$ is the minimal polynomial of a. This doesn't split over k if $a \notin k$, so such a cannot lie in a Borel k-subgroup of GL_n.

Despite the preceding example, Borel's theorem *does* have interesting applications to linear algebraic groups over general ground fields, as well as useful applications even over an algebraically closed field. In this handout we discuss such applications (Theorem 2.1, Proposition 3.1, Corollary 3.3, Proposition 3.7, §4, and Theorem 5.1); *none of these will be used in this course* but they're important in practice and hence worth knowing.

In several places we will refer to the largely self-contained Appendix B of (the 2nd edition of) "Pseudo-reductive Groups" for proofs of some important results of Tits on smooth connected unipotent groups in characteristic $p > 0$ (only needed over algebraically closed fields, where nonetheless the results we will require remain nontrivial though do not depend on anything in the theory of pseudo-reductive groups).

2. Semisimple and unipotent elements

The key application (upon which most others will depend) is this:

Theorem 2.1. *Let G be a connected linear algebraic group over an algebraically closed field k. If $g \in G(k)$ is semisimple then g lies in a torus $T \subset G$, and if $g \in G(k)$ is unipotent then g lies in a unipotent connected smooth subgroup $U \subset G$.*

In the semisimple case the subtlety is that although the Zariski closure $\overline{\langle g \rangle}$ has identity component that is a torus (since its elements are semisimple), it is not generally true that g lies in this identity component. For example, g could have finite order! Likewise, for unipotent g the case $\mathrm{char}(k) = p > 0$ is where the real work lies, since g then always has finite order (some p-power).

Proof. As a first (crucial) step, we apply Borel's covering theorem via Borel subgroups: there is a Borel subgroup $B \subset G$ containing g. The Jordan decomposition of g viewed in B must recover the one for g viewed in G (by functoriality of Jordan decomposition), so g is semisimple in B when it is so in G, and likewise for unipotence. Hence, we can replace G with B to reduce to the case that G is solvable (and connected).

Letting $U = \mathscr{R}_u(G)$, we have $G = T \ltimes U$ for any maximal torus T of G. The quotient map $G \to G/U = T$ onto a torus must kill all unipotent elements, so $U(k)$ is the set of unipotent elements of G. In particular, $g \in U(k)$ when g is unipotent, so U does the job in this case. (The fact that the unipotent elements form a subgroup is rather specific to the connected solvable case.

For example, it fails badly for SL_2: as is classically known, the upper and lower triangular unipotent elements of $\mathrm{SL}_2(k)$ generate the entire group.)

Now we turn to the harder case when g is semisimple. (Of course, the unipotent case was only "easy" because we have done the hard work to prove Borel's covering theorem!) We seek a conjugate of T that contains g. We will proceed by induction on $\dim U$, the case of dimension 0 being obvious (as then $G = T$). In general, suppose there is given a T-equivariant exact sequence

$$1 \to U' \to U \to U'' \to 1$$

with U' a nontrivial proper normal smooth connected subgroup of U, so U' and U'' both have strictly smaller dimension than U and we can apply the inductive hypothesis to the abstract semi-direct products $T \ltimes U'$ and $T \ltimes U''$.

Consider the semisimple image of g in $G'' = T \ltimes U''$. By dimension induction, this lies in some torus of G'', and hence in a maximal torus T'' of G''. Such a torus must be conjugate to T, so there exists $g'' \in G''(k)$ such that $T'' = g''Tg''^{-1}$. If $\gamma \in G(k)$ lifts G'', then by replacing T with $\gamma T \gamma^{-1} \subset G$ we may arrange that T'' is the image of T. Hence, the preimage of T'' in G is $T \ltimes U'$, so $g \in T \ltimes U'$. Now again we can apply dimension induction to conclude.

Thus, if there is such a nontrivial T-equivariant exact sequence then we win. For example, if U is not commutative then we can take $U' = \mathscr{D}(U)$ (which is a proper subgroup of U since U is solvable and $U \neq 1$). Hence, we can assume U is commutative. Likewise, if $\mathrm{char}(k) = p > 0$ but $pU \neq 0$ then we can take $U' = pU$ (which is a proper subgroup since the commutative U is killed by some p-power, due to the existence of a composition series with successive quotients $\mathbf{G}_a$). In this way we may arrange that U is also p-torsion when $\mathrm{char}(k) > 0$. (Note that we *cannot* instead work with the smooth nontrivial subgroup $U[p]_{\mathrm{red}}$ when $pU \neq 0$ because it might not be connected.) At this point, something wonderful happens (especially in positive characteristic): necessarily $U \simeq \mathbf{G}_a^n$!

Remark 2.2. The existence of such an isomorphism is nontrivial even in characteristic 0 (though is not surprising in that case), but in characteristic $p > 0$ it is especially remarkable, since in the absence of the p-torsion condition it fails: the k-group W_2 of "length-2 Witt vectors" (a nontrivial k-group structure on the affine plane, with identity $(0,0)$) is a commutative extension of $\mathbf{G}_a$ by $\mathbf{G}_a$ that is not killed by p. (Explicitly, the group law is

$$(x, y) + (x', y') = (x + x', y + y' + S_p(x, x'))$$

where S_p is the mod-p reduction of $((X + X')^p - X^p - X'^p)/p \in \mathbf{Z}[X, X']$.)

To construct the isomorphism $U \simeq \mathbf{G}_a^n$, we first treat characteristic 0:

Lemma 2.3. *If k is algebraically closed and* $\mathrm{char}(k) = 0$ *then any commutative connected unipotent k-group U' is a power of $\mathbf{G}_a$.*

This result holds over any field of characteristic 0 by Galois descent from $\overline{k}$, since $\mathrm{Aut}_{\overline{k}}(\mathbf{G}_a^n) = \mathrm{GL}_n(\overline{k})$ in characteristic 0 (shown in the paragraph following the proof below) and $\mathrm{H}^1(k, \mathrm{GL}_n) = 1$.

Proof. Recall (as was seen in the previous course) that since $k = \overline{k}$, there is a composition series of U' by smooth connected closed subgroups whose successive quotients are $\mathbf{G}_a$. Thus, to prove $U' \simeq \mathbf{G}_a^N$ we can use dimension induction to reduce to checking that any short exact sequence of *commutative* linear algebraic k-groups

$$1 \to \mathbf{G}_a^n \to U' \to \mathbf{G}_a \to 1$$

splits as a direct product. By using bi-additivity in the second variable for Ext^1 on the category of commutative linear algebraic k-groups (as in any abelian category), this reduces to the special case $n = 1$.

The exact sequence
$$1 \to \mathbf{G}_a \to U' \to \mathbf{G}_a \to 1$$
involves a smooth surjection on the right, so it admits étale-local sections. Hence, it identifies U' as a $\mathbf{G}_a$-torsor for the étale topology over the affine line, and as such corresponds to a class in $\mathrm{H}^1_{\text{ét}}(\mathbf{A}^1_k, \mathscr{O})$. But étale and Zariski cohomology agree for coefficients in a quasi-coherent sheaf, and more specifically the higher cohomology vanishes when the base scheme is affine. Hence, the map $U' \to \mathbf{G}_a$ admits a k-scheme section. By uniquely translating such a section via $\mathbf{G}_a(k)$ we can arrange that it respects the identity points.

To summarize, we have identified U' as a variety with $\mathbf{G}_a \times \mathbf{G}_a$ such that the identity is $(0,0)$ and the group law is $(x,y)(x',y') = (x + x' + f(y,y'), y + y')$ for a suitable symmetric polynomial $f \in k[Y, Y']$ satisfying $f(0, Y') = 0$, $f(Y, 0) = 0$, and a "2-cocycle" condition expressing the associativity. So far we have not used anything about the characteristic of k. It is a classical result of Lazard in characteristic 0 (see Proposition 8 of Chapter VII.7 in Serre's book "Algebraic groups and class fields" for the precise reference) that the only possibilities for $f(Y, Y')$ are $h(Y+Y') - h(Y) - h(Y')$ for $h \in k[X]$ with $h(0) = 0$ (i.e., "f is a 2-coboundary"). Thus, we can modify the initial section via $(x, y) \mapsto (x - h(y), y)$ to arrive at the desired description of the group law on U' (respecting the given filtration on it). ■

In view of Lemma 2.3, now assume $\mathrm{char}(k) = 0$. In such cases we have shown that $G = T \ltimes V$ where $V \simeq \mathbf{G}_a^n$ and T acts on V as a k-group. Is the T-action on V necessarily linear (relative to a fixed choice of k-group isomorphism with $\mathbf{G}_a^n$)? To address this, we first consider the endomorphism functor of the group scheme $\mathbf{G}_a^n$ on the category of k-algebras. Observe that the only additive polynomials in one variable over a k-algebra R (i.e., $f(X+Y) = f(X) + f(Y)$ in $R[X,Y]$) are cX for $c \in R$; this uses that $\mathrm{char}(k) = 0$ (check!). Thus, the endomorphism functor $\underline{\mathrm{End}}_k(\mathbf{G}_a)$ on the category of k-algebras is represented by $\mathbf{G}_a$. Passing to powers, $\underline{\mathrm{End}}_k(\mathbf{G}_a^n)$ is represented by Mat_n. Hence, the automorphism functor of the k-group $V \simeq \mathbf{G}_a^n$ is represented by GL_n. In particular, all k-group automorphisms of $\mathbf{G}_a^n$ are *linear* (i.e., commute with the evident $\mathbf{G}_m$-scaling action). This is *false* in positive characteristic (e.g., $(x,y) \mapsto (x, y + x^p)$ is an automorphism of the affine plane in characteristic $p > 0$), and so will make the treatment of such cases rather more serious.

It follows (in characteristic 0) that the T-action on V is a *linear representation* (relative to a fixed choice of k-group isomorphism $V \simeq \mathbf{G}_a^n$). In any characteristic we have:

Lemma 2.4. *If a torus T acts linearly on a finite-dimensional vector space V over an algebraically closed field k then for $G = T \ltimes V$ any semisimple $g \in G(k)$ lies in a conjugate of T.*

Proof. By complete reducibility, $V = \prod L_i$ for lines L_i on which T acts through characters χ_i (some of which may be the same as others). The T-equivariant exact sequence $0 \to L_1 \to V \to V/L_1 \to 0$ thereby reduces our problem to the case $V = \mathbf{G}_a$ on which T acts through some character χ. Hence, now $G = T \ltimes \mathbf{G}_a$.

The semisimple element g can be written as (t, x) for some $x \in k$ and $t \in T(k)$. Beware that t and x may not commute in G, so these do not generally give the Jordan decomposition of g (which is $g_{\mathrm{ss}} = g$ and $g_{\mathrm{u}} = 1$). We seek $x' \in k$ such that $(0, x')$ conjugates g into T (so g lies in $(0,x')^{-1}T(0,x')$). By direct computation, using the definition of the semi-direct product structure,
$$(0, x')g(0, -x') = (t, x + (\chi(t)^{-1} - 1)x').$$
Hence, we seek $x' \in k$ such that $x + (\chi(t)^{-1} - 1)x' = 0$. If $\chi(t) \neq 1$ then we use $x' = x/(\chi(t)^{-1} - 1)$. If $\chi(t) = 1$ then t is *central* in G, so the semisimplicity of g implies that $(0, x)$ is semisimple, so $x = 0$ and hence $g = t \in T(k)$. ■

Since Lemma 2.4 was characteristic-free, to complete the proof of Theorem 2.1 we just need the following replacement of Lemma 2.3 for positive characteristic.

Lemma 2.5. *If k is algebraically closed and $\mathrm{char}(k) = p > 0$ then any p-torsion commutative connected unipotent k-group U' is a power of $\mathbf{G}_a$.*

Proof. An elegant proof due to Tits is given in Lemma B.1.10 in "Pseudo-reductive Groups", ultimately resting on Lazard's result in characteristic p that replaces the result in characteristic 0 which was cited in the proof of Lemma 2.3. ■

It remains, with $\mathrm{char}(k) = p > 0$, to relate an abstract semi-direct product $T \ltimes V$ with $V \simeq \mathbf{G}_a^n$ to the special case when the T-action on V appears linear under some k-group isomorphism $V \simeq \mathbf{G}_a^n$ (so then we may apply Lemma 2.4 to conclude). Here again, the main difficulty was solved by Tits: he proved the remarkable result that $V = V^T \times V'$ where V' is a T-stable smooth connected k-subgroup admitting a k-group isomorphism $V' \simeq \mathbf{G}_a^{n'}$ under which the T-action on V' becomes linear! This is Theorem B.4.3 in "Pseudo-reductive Groups". Since V^T is smooth and connected (as for centralizers of torus actions on smooth connected subgroups in general), and also commutative and p-torsion, it is isomorphic to $\mathbf{G}_a^N$. Thus, we have identified V with a power of $\mathbf{G}_a$ in a way that linearizes the T-action. This completes the proof of Theorem 2.1. ■

3. Consequences of Theorem 2.1

Here is a remarkable refinement over general fields:

Proposition 3.1. *If G is a connected linear algebraic group over an arbitrary field k and $g \in G(k)$ is semisimple then g lies in a k-torus of G.*

Proof. Let M denote the Zariski closure of $g^{\mathbf{Z}}$. This is a smooth closed k-subgroup whose geometric points are semisimple, so M^0 is a torus and M/M^0 has order not divisible by $\mathrm{char}(k)$ (since M/M^0 is a finite étale group whose geometric points are semisimple). Note that $Z_G(M)$ is exactly the scheme-theoretic centralizer of g (i.e., it is $Z_G(g)$ by another name). We prefer to work with the "$Z_G(M)$" description, since M is a k-subgroup of G and so encodes more "structure" than the individual element g.

The idea is to pass to the group $Z_G(M)^0$ in place of G to reduce to the case that g is *central* in G. But there are two problems: is $Z_G(M)$ smooth, and is g in $Z_G(M)^0$? The first of these is a generalization of our earlier result on fixed-point schemes for torus actions, now allowing for the fact that M might not be connected:

Lemma 3.2. *Let M be a smooth commutative affine group over a field k such that $S := M^0$ is a torus and M/M^0 has order not divisible by $\mathrm{char}(k)$. For any action by M on a smooth k-scheme Y, the scheme-theoretic fixed locus Y^M is smooth.*

Proof. We may and do assume $k = \overline{k}$. In the case of a torus action this problem was solved in Exercise 3 of HW8 of the previous course; the only relevant property about tori (apart from their commutativity) was the complete reducibility of linear representations of tori over an algebraically closed field. Thus, it suffices to prove that linear representations of M over $k = \overline{k}$ are also completely reducible. We will split the exact sequence $1 \to S \to M \to \mu \to 1$ (with $\mu = M/M^0$ a finite constant group of order not divisible by $\mathrm{char}(k)$), from which the complete reducibility is clear.

All points in $M(k)$ are semisimple (as any unipotent element in $M(k)$ must be trivial, and then we can apply the Jordan decomposition in linear algebraic groups), and by hypothesis M is commutative. Thus, upon choosing a subgroup inclusion $M \hookrightarrow \mathrm{GL}_n$ we may simultaneously diagonalize all elements of $M(k)$. Hence, M is a k-subgroup of the diagonal torus D in GL_n. The subtorus S in D splits off as a direct factor (as for any inclusion between tori over an algebraically closed field), say $D = S \times S'$. Since $S \subset M \subset D$, we then have $M = S \times (M \bigcap S')$. This identifies $M \bigcap S'$ with $M/S = \mu$. ■

Now consider the smooth connected k-subgroup $Z_G(M)^0$. We claim that this contains g. To prove it, we apply Theorem 2.1 to $G_{\overline{k}}$ (!) to get a torus $T' \subset G_{\overline{k}}$ that contains g. Hence, $M_{\overline{k}} \subset T'$, so since T' is commutative we get $T' \subset Z_{G_{\overline{k}}}(M_{\overline{k}}) = Z_G(M)_{\overline{k}}$. But T' is connected, so $T' \subset Z_G(M)^0_{\overline{k}}$. Since $g \in T'(\overline{k})$, we conclude that $g \in Z_G(M)^0(\overline{k}) \bigcap Z_G(M)(k) = Z_G(M)^0(k)$ as desired. Hence, we may indeed replace G with $Z_G(M)^0$ so that now g is central in G.

Recall the earlier big theorem of Grothendieck: maximal k-tori in G remain maximal after any ground field extension. Letting $T \subset G$ be a maximal k-torus, we claim that the central semisimple $g \in G(k)$ lies in $T(k)$. To prove this, it is harmless to replace k with $\overline{k}$ (since $T_{\overline{k}}$ is maximal in $G_{\overline{k}}$!). Thus, now we may and do assume k is algebraically closed at the cost of having *specified* a maximal torus T which we must prove contains the central semisimple g. But by another application of Theorem 2.1 we know that there is *some* torus of G containing the semisimple g, and hence a maximal torus $T' \subset G$ that does the job. Since $k = \overline{k}$, T' is conjugate to T. However, conjugacy has no effect on the central g, so $g \in T$ since $g \in T'$. ■

As a corollary, we obtain a description of semisimple conjugacy classes over k_s. This is rather important in representation theory:

Corollary 3.3. *Let G be a connected linear algebraic group over a field k, and let $T \subset G$ be a maximal k-torus. Let $W = N_G(T)/Z_G(T)$ be the associated finite étale Weyl group over k. The natural map of sets*

$$T(k_s)/W(k_s) \to \{\text{semisimple } g \in G(k_s)\}/G(k_s)\text{-conjugacy}$$

is bijective.

For example, if $G = \mathrm{GL}_n$ and T is the diagonal torus then this recovers the well-known fact that a matrix $m \in \mathrm{GL}_n(k)$ that is semisimple in the sense of linear algebraic groups (i.e., *geometrically* semisimple, or equivalently is semisimple with separable eigenvalues) is determined up to k_s-rational conjugacy by its characteristic polynomial. This is weaker than rational canonical form, but it applies to arbitrary linear algebraic groups.

Proof. Since T_{k_s} is a maximal torus in G_{k_s}, we may replace k with k_s so that k is separably closed. In this case we need to show that every semisimple element of $G(k)$ is conjugate to an element of $T(k)$ ("surjectivity") that in turn is unique up to precisely the action of $W(k)$ on $T(k)$ ("injectivity"). The surjectivity step is where Proposition 3.1 will be used.

Now that k is separably closed, since $Z_G(T)$ is smooth we have

$$W(k) = (N_G(T)/Z_G(T))(k) = N_G(T)(k)/Z_G(T)(k) = N_{G(k)}(T)/Z_{G(k)}(T),$$

so clearly elements of $T(k)$ in the same $W(k)$-orbit are conjugate in $G(k)$. Hence, the map in question is well-defined.

We first prove injectivity: if $t, t' \in T(k)$ are conjugate in $G(k)$ then that they are $N_{G(k)}(T)$-conjugate and so lie in the same $W(k)$-orbit. Choose $g \in G(k)$ such that $gt'g^{-1} = t$. Hence, gTg^{-1} and T are two maximal k-tori that contain t, so each lies in $Z_G(t)^0$. By Lemma 3.2 (applied with M equal to the Zariski closure of $t^{\mathbf{Z}}$), the group $Z_G(t)$ is smooth, so $H := Z_G(t)^0$ is a connected linear algebraic group over k in which gTg^{-1} and T are maximal k-tori.

We claim that these tori are $H(k)$-conjugate, which is to say that there exists $h \in H(k) = Z_G(t)^0(k) \subset Z_{G(k)}(t)$ such that $gTg^{-1} = hTh^{-1}$. Granting that, $h^{-1}g \in N_G(T)(k) = N_{G(k)}(T)$ and

$$h^{-1}gt'(h^{-1}g)^{-1} = h^{-1}(gt'g^{-1})h = h^{-1}th = t,$$

so t' is $N_{G(k)}(T)$-conjugate to t as desired. The proof of injectivity has now been reduced to the following result applied to $Z_G(t)^0$:

Lemma 3.4. *Let H be a connected linear algebraic group over a separably closed field k. Then all maximal k-tori in H are $H(k)$-conjugate.*

Proof. Let $T, T' \subset H$ be maximal k-tori, and let $Z \subset H$ be the closed subscheme representing the functor $\underline{\mathrm{Tran}}_G(T, T')$ of points of H that conjugate T into T' (see Exercise 3 in HW3 of the previous course). Our problem is to prove that $Z(k)$ is non-empty. We claim that Z is *smooth and non-empty* over k. Since $k = k_s$, that will suffice to ensure the existence of a k-point (as then Z is étale onto a non-empty open locus in an affine space, so a fiber over a k-point of that open provides a k-point of Z).

The key is that to prove the k-scheme Z is smooth and non-empty, we may extend the ground field to $\overline{k}$! That is, for this purpose we can assume k is algebraically closed. Hence, T' is conjugate to T (i.e., Z is non-empty), and a choice of such conjugator makes Z conjugate to $\mathrm{Tran}_G(T, T) = N_G(T)$. But we know that the normalizer scheme of a torus in a linear algebraic group is always smooth, so we are done. ∎

Continuing with the proof of Corollary 3.3, we have to show that if $g \in G(k)$ is a semisimple element then it is conjugate to an element of $T(k)$. By Proposition 3.1, there is some k-torus of G that contains g, and hence a maximal k-torus T' of G that contains g. By Lemma 3.4, $T = \gamma T' \gamma^{-1}$ for some $\gamma \in G(k)$, so $\gamma g \gamma^{-1} \in T(k)$. That is, g has a $G(k)$-conjugate lying in $T(k)$. ∎

Example 3.5. In view of Proposition 3.1, it is natural to wonder if Theorem 2.1 in the unipotent case has an analogue over a general ground field. That is, if G is a connected linear algebraic group over a general field k and $u \in G(k)$ is a unipotent element, does u lie in a unipotent smooth connected k-subgroup of G? This question is only interesting in characteristic $p > 0$, since in general the Zariski closure of $u^{\mathbf{Z}}$ is a unipotent linear algebraic group and all unipotent linear algebraic groups are connected in characteristic 0. Thus, now assume $\mathrm{char}(k) = p > 0$. We now explain several senses in which this question has both negative and affirmative answers.

First of all, over any imperfect field there are counterexamples (of a rather special type), as follows. In Example 1.6.3 of "Pseudo-reductive Groups", there is given an example over any imperfect k of a *commutative* connected linear algebraic group G such that $G(k)$ has non-trivial p-torsion and G is pseudo-reductive (i.e., $\mathscr{R}_{u,k}(G) = 1$). If $U \subset G$ is a unipotent smooth connected k-subgroup then by normality (due to the commutativity of G) we have $U \subset \mathscr{R}_{u,k}(G) = 1$, so nontrivial elements in $G(k)[p]$ provide a counterexample to a k-rational version of the unipotent case of Theorem 2.1.

But it is natural to seek "better" counterexamples: either over a perfect field, or with G a connected semisimple group. In a practical sense, the most interesting case is not just to find a unipotent smooth connected k-subgroup that contains u, but to find a 1-parameter k-subgroup $\lambda : \mathbf{G}_m \to G$ such that $u \in U_G(\lambda)$ (i.e., λ "contracts" u to 1 under conjugation as $t \to 0$). Indeed, when G is reductive then we will see later that such $U_G(\lambda)$'s are exactly the unipotent radicals of parabolic k-subgroups, whose structure can be understood via root systems. In other words, rather than finding some random unipotent smooth connected k-subgroup $U \subset G$ containing u, it is more interesting to find one of the form $U = U_G(\lambda)$ for some λ.

Tits called u *good* when it lies in such a $U_G(\lambda)$, and "bad" otherwise. It is easy to give examples of bad unipotent elements in semisimple groups over local function fields: for example, if D is a central division algebra of dimension p^2 over a local function field k of characteristic p then $k' = k^{1/p}$ is a degree-p extension (as $k = \mathbf{F}_q((t))$) and so embeds into D over k. Thus, for the k-form $G = \underline{D}^\times/\mathbf{G}_m$ of PGL_p, $k'^\times/k^\times$ is an infinite p-torsion subgroup of $G(k)$ yet G is k-anisotropic (either because $G(k)$ is compact, or by observing that $\underline{D}^\times/\mathbf{G}_m$ is F-anisotropic for *any* central division algebra D over *any* field F: a nontrivial split torus in such a quotient would have preimage in $\underline{D}^\times$ that is a split torus of dimension at least 2, contradicting that étale F-subalgebras of D cannot contain nontrivial idempotents, since D is a division algebra). In other words, we get lots of "bad" unipotent elements in such examples. These are *not* counterexamples to the original question, however, since $\mathrm{R}_{k'/k}(\mathbf{G}_m)/\mathbf{G}_m$ is a unipotent connected linear algebraic subgroup of G that contains such elements.

Notice that in these examples of "bad" unipotent elements, the semisimple group G is not "simply connected" (the group $\mathrm{SL}_1(D)$ of units of reduced norm 1 in D is a form of SL_p and is a nontrivial central cover of G). Tits conjectured that if $[k : k^p] \leq p$ and G is *simply connected* semisimple then all unipotent elements are good (and in particular lie in a unipotent connected smooth k-subgroup). The degree restriction arises because Tits made bad unipotent elements over fields with $[k : k^p] \geq p^2$. Tits' conjecture was proved by Gille in 2002 using Bruhat–Tits theory.

The intervention of imperfect fields in the preceding examples is essential:

Theorem 3.6 (Borel–Tits)**.** *If k is perfect of characteristic $p > 0$ and G is any connected linear algebraic k-group then any unipotent $u \in G(k)$ lies in a unipotent smooth connected k-subgroup $U \subset G$.*

The proof requires the full strength of the structure theory of reductive groups via root systems. This result is not used anywhere in the course.

Proof. By Borel's covering theorem, we know that there is such a U over $\overline{k}$. The idea, which is rather marvelous, is to show that there is a *canonical* such U over $\overline{k}$, meaning one whose formation is functorial with respect to isomorphisms in the pair $(G_{\overline{k}}, u)$. If such a canonical choice can be made then it must be Galois-invariant and hence descend (since $\overline{k}/k$ is Galois, as k is perfect). So our problem becomes a finer one over $\overline{k}$: over an algebraically closed ground field prove the refinement of Borel's theorem that there is a *canonical* parabolic subgroup $P \subseteq G$ such that $u \in \mathscr{R}_u(P)$ (where by "canonical" we mean that P is functorial with respect to isomorphisms in the pair (G, u)).

More generally, consider an algebraically closed field k of *any* characteristic and a unipotent smooth closed subgroup $U \subseteq G$ such that U is "embeddable" in the sense that it lies inside some unipotent smooth connected subgroup of G, or equivalently inside the unipotent radical of a Borel subgroup. (For example, by Borel's theorem we could take U to be the finite cyclic subgroup generated by a unipotent element when $\mathrm{char}(k) > 0$.) In this generality, we claim that there is a *canonical* parabolic subgroup P (i.e., one that is functorial with respect to isomorphisms in the pair (G, U)) such that $U \subseteq \mathscr{R}_u(P)$.

[This general claim, once proved, has a rather striking consequence: every unipotent smooth closed subgroups of G is embeddable, and so consequently lies in the unipotent radical of a canonical parabolic subgroup (and so by Galois descent the same is true over any perfect field)! This is remarkable even for connected unipotent groups, and in particular even in characteristic 0. We prove this consequence by induction on $\dim G$. The case $\dim G = 0$ is trivial, and in general if G is not reductive then we can replace G with $G/\mathscr{R}_u(G)$ to apply dimension induction. Thus, we can assume G is reductive. We can also assume $U \neq 1$, so by nilpotence of unipotent groups there exists a nontrivial central $u \in U(k)$. By Borel's theorem, the Zariski closure of the subgroup generated by u is embeddable! Thus, by the claim we are assuming concerning canonical parabolics associated to embeddable unipotent smooth connected subgroups, there is a parabolic subgroup $P \subseteq G$ such that $u \in \mathscr{R}_u(P)$ and P is functorial in (G, u). Hence, P is normalized by U, so $U \subseteq P$ since parabolics are their own normalizers. But $P \neq G$ since $\mathscr{R}_u(P)$ contains $u \neq 1$ whereas we have arranged for G to be reductive, so by dimension induction we get a unipotent smooth connected subgroup of P containing U. Thus, U is indeed embeddable.]

Finally, we turn to the real issue, which is constructing a canonical parabolic subgroup whose unipotent radical contains a given embeddable unipotent U. The basic idea of Borel and Tits is to build it by an iterative process. Consider the normalizer $N(U)$, and define $L(U) = U \cdot \mathscr{R}_u(N(U))$. Obviously $U \subseteq L(U)$, and $L(U)$ is visibly unipotent (being generated by two unipotent subgroups, one of which normalizes the other). It is clear that $L(U)$ is functorial with respect to isomorphisms in the pair (G, U). Moreover, $L(U)$ inherits the embeddability property of U: if U lies in the unipotent radical of a Borel subgroup then so does $L(U)$. To see this, the problem is to find a Borel subgroup B containing U that also contains $\mathscr{R}_u(N(U))$. But note that $\mathscr{R}_u(N(U))$ is a connected solvable group, and (for an initial choice of Borel subgroup B_0 of G) in the "variety of Borel subgroups" G/B_0 the locus of Borels that contain U is a *non-empty closed* set. (It is closed because $U \subseteq gB_0g^{-1}$ if and only if $gug^{-1} \in B_0$ for all $u \in U(k)$, a collection of Zariski-closed conditions on g by using the maps $f_u : G \to G$ defined by $g \mapsto gug^{-1}$ for $u \in U(k)$.) Thus, the locus of Borels containing U is proper, so by the Borel fixed point theorem there exists a point on it that is fixed by $\mathscr{R}_u(N(U))$, providing a Borel that contains $L(U)$.

It is now legitimate to replace U with $L(U)$. Continuing in this way, eventually we reach the situation that the dimension stabilizes. That is, $\dim L(U) = \dim U$, or equivalently $U^0 = L(U)^0$ (as $U \subseteq L(U)$ in general). In such a situation, the remarkable fact is that U is connected and $U = \mathscr{R}_u(N(U))$ with $N(U)$ actually parabolic (so this is the "canonical" parabolic that we sought, relative to the long-lost original U with which the entire argument began). The proofs of these properties require a masterful command of the structure theorem of reductive groups via root systems, so we cannot get into the matter here. For an exposition of the argument of Borel and Tits, see the last six paragraphs of the accepted answer to Question 104201 on Math Overflow. ■

One may wonder if there is an analogous affirmative result over k with $[k : k^p] = p$ provided that either G is reductive or that $G = \mathscr{D}(G)$ (to avoid the commutative counterexamples mentioned above over any imperfect field). I don't know the answer.

We end this section with an application of Theorem 2.1 and the *method* of its proof (as well as of Borel's covering theorem):

Proposition 3.7. *For a connected linear algebraic group G over $k = \overline{k}$ and $g \in G(k)$ with Jordan decomposition su, $g \in Z_G(s)^0$.*

A special case of this result is semisimple g (i.e., $g = s$), for which it says $g \in Z_G(g)^0$: this is immediate from the fact that g lies in a torus (which is commutative and connected), thanks to Theorem 2.1.

Proof. By Borel's covering theorem, there is a Borel subgroup $B \subset G$ such that $g \in B(k)$. The Jordan decomposition of g in B must recover the one in G, so $s, u \in B$. Hence, $g \in Z_B(s) \subset Z_G(s)$, so it suffices to prove the stronger result that $Z_B(s)$ is *connected*. In other words, upon renaming B as G, we may assume that G is *solvable* (and connected) and that $g = s$ is semisimple at the cost of proving something much stronger: in such cases, $Z_G(s)$ is connected. By Theorem 2.1, there exists a maximal torus $T \subset G$ containing s, so $G = T \ltimes U$ with $U = \mathscr{R}_u(G)$. Thus, $Z_G(s) = T \ltimes Z_U(s)$, where $Z_U(s)$ is the scheme-theoretic centralizer of the s-action on U (so it inherits smoothness from $Z_G(s)$, which is provided by Lemma 3.2).

To get some insight into this result (whose proof in 10.6(3) of Borel's book is not too illuminating), consider the special case $G = T \ltimes V$ for a linear representation of T on a vector space V of finite dimension. Via the weight space decomposition for V relative to the linear T-action, we obtain an eigenspace decomposition $V = \prod V_\lambda$ relative to the action of $s \in T(k)$. Hence, $Z_G(s) = T \ltimes V_1$, which is connected by inspection (perhaps $V_1 = 0$). The idea is to reduce the general case to this case, following the method of proof of Theorem 2.1.

We proceed by induction on $\dim U$. The key point is that if

$$1 \to U' \to U \to U'' \to 1$$

is a T-equivariant exact sequence with U' connected, smooth, nontrivial, and $\neq U$ (so U' and U'' both have strictly smaller dimension than U), then by induction the s-centralizers $Z_{U'}(s)$ and $Z_{U''}(s)$ are connected. We get a left-exact sequence of linear algebraic groups

$$1 \to Z_{U'}(s) \to Z_U(s) \to Z_{U''}(s)$$

for which the outer terms are connected, so to deduce connectedness for the middle it suffices to prove surjectivity on the right. Since $Z_{U''}(s)$ is *connected*, it suffices to show that the map on the right is surjective on Lie algebras (as it is then smooth, so its closed image is open and therefore full). But by the *functorial* definition of scheme-theoretic centralizers (!), the left exact sequence of Lie algebras is the sequence

$$0 \to \mathrm{Lie}(U')^{s=1} \to \mathrm{Lie}(U)^{s=1} \to \mathrm{Lie}(U'')^{s=1}$$

induced by the short exact sequence

$$0 \to \mathrm{Lie}(U') \to \mathrm{Lie}(U) \to \mathrm{Lie}(U'') \to 0.$$

But this latter sequence is equivariant for the *semisimple* action by s (induced by the compatible actions of T), and by semisimplicity it follows that the induced map between λ-eigenspaces for s is short exact for any $\lambda \in k$. Taking $\lambda = 1$ gives what to need.

To summarize, we can carry out the induction on $\dim U$ if U contains a T-stable nontrivial connected proper smooth closed subgroup. For example, if U is not commutative we can take $U' = \mathscr{D}(U)$, so we can assume U is commutative. If $\mathrm{char}(k) = p > 0$ and U is not p-torsion then we can take $U' = pU$. Hence, exactly as in the proof of Theorem 2.1, we may arrange that $U \simeq \mathbf{G}_a^n$ for some $n \geq 0$, and moreover this isomorphism can be chosen (even in positive characteristic!) to ensure that the T-action on U is *linear*. In other words, we have reduced to exactly the special case treated at the start. ■

4. Regular elements

For a general connected linear algebraic group G over an algebraically closed field k and torus $T \subset G$, if $g \in T(k)$ then the centralizer $Z_G(g)$ coincides with $Z_G(M)$ for the Zariski closure $M \subset T$ of $g^{\mathbf{Z}}$, so its is smooth with Lie algebra $\mathfrak{g}^M = \mathfrak{g}^{g=1}$. Hence, $\dim Z_G(g)$ is at least the common dimension $\dim Z_G(T)$ of the Cartan subgroups of G, with equality if and only if $a(g) \neq 1$ for all $a \in \Phi(G,T)$. We called the semisimple element g *regular* when equality holds, and via Lie algebra considerations we easily see that in such cases $Z_G(g)^0 = Z_G(T)$ and T is the unique torus containing g and $Z_G(T)$ is the unique Cartan subgroup containing g. (For example, if $G = \mathrm{GL}_n$, we saw that regularity amounts to having pairwise distinct eigenvalues.) Now we will use Theorem 2.1 to improve our viewpoint on regularity, making it intrinsic to any semisimple element of G without reference to T and also extending the notion to the non-semisimple case.

Let $g \in G(k)$ be a semisimple element. By Theorem 2.1, there exists a maximal torus $T \subset G$ containing g, so $Z_G(g)$ is smooth (Lemma 3.2) and contains $Z_G(T)$, with

$$\mathrm{Lie}(Z_G(g)) = \mathfrak{g}^{g=1} \supset \mathfrak{g}^T.$$

Hence, the minimal possible dimension for $Z_G(g)$ is the *rank* $r(G)$ (the common dimension of the Cartan subgroups), and this is attained precisely when g is regular in T. But in such cases we know that T is the *only* maximal torus of G containing g, so we arrive at an intrinsic notion:

Definition 4.1. Let G be a connected linear algebraic group over $k = \overline{k}$. A semisimple element $g \in G(k)$ is *regular* if $\dim Z_G(g) = r(G)$.

The preceding shows that such g lie in a unique maximal torus and are regular in that torus in the sense defined earlier. Hence, this definition recovers the earlier notion without mentioning an a-priori choice of ambient maximal torus. We emphasize that the semisimple case of Theorem 2.1 has been used in an essential way here.

Here is a mild extension of this concept: for a general $g \in G(k)$, with Jordan decomposition $g = su$, the algebraic homomorphism $\mathrm{Ad}_G : G \to \mathrm{GL}(\mathfrak{g})$ identifies $\mathrm{Ad}_G(s)$ and $\mathrm{Ad}_G(u)$ as the semisimple and unipotent parts of $\mathrm{Ad}_G(g)$. Hence, $\mathrm{Ad}_G(g)$ has the same characteristic polynomial as $\mathrm{Ad}_G(s)$, so the multiplicity of 1 as an eigenvalue of this polynomial is at least $r(G)$. (This multiplicity is the dimension of the generalized 1-eigenspace for $\mathrm{Ad}_G(g)$, not generally the dimension of the 1-eigenspace; e.g., consider the case $g = u$!) This minimal multiplicity is attained precisely when s is regular.

Consider the characteristic polynomial of the adjoint action of G on $\mathfrak{g}$. This is a monic polynomial $f_G \in k[G][X]$, and $(X-1)^{r(G)}$ divides $f_G(g, X)$ for all $g \in G(k)$. An elementary induction argument shows that if $V = \mathrm{Spec}\, A$ is an integral affine k-variety and $f \in A[X]$ is a monic polynomial such that $f(v, X)$ is divisible by a fixed polynomial $h \in k[X]$ for all $v \in V(k)$, then $h|f$ in $A[X]$. Hence,

$$f_G(X) = (X-1)^{r(G)}(X^m + c_{m-1}X^{m-1} + \cdots + c_0)$$

for some $c_j \in k[G]$, and $\sigma := 1 + c_{m-1} + \cdots + c_0 \in k[G]$ is nonzero because for regular semisimple $g \in G(k)$ (which *do* always exist) we know that $X - 1$ appears as a factor of $f_G(g, X)$ with multiplicity exactly $r(G)$. It follows that $\mathrm{Ad}_G(g)$ has "minimal" multiplicity $r(G)$ for 1 as a root of its characteristic polynomial if and only if $\sigma(g) \neq 0$. To summarize:

Proposition 4.2. *For $g \in G(k)$, the following are equivalent:*

(1) *the characteristic polynomial of* $\mathrm{Ad}_G(g)$ *has minimal multiplicity* $r(G)$ *for* 1 *as a root,*
(2) *the semisimple part of g is regular,*
(3) $\sigma(g) \neq 0$.

We say that $g \in G(k)$ is *regular* when it satisfies the above equivalent conditions. For semisimple g it recovers the earlier notion, and in view of part (3) it is is a Zariski-dense open condition (non-empty because of the existence of regular semisimple elements!). A boring example is unipotent G, for which all elements are regular (so this case is not interesting). But there are interesting cases in which the set of regular semisimple elements is Zariski-dense in $G(k)$ or even exhausts the entire open regular locus. Here is a basic example:

Example 4.3. If $g \in \mathrm{GL}_n(k)$ is regular, then it must be semisimple. Indeed, the Jordan decomposition is $g = su$ with regular semisimple s, so s has distinct eigenvalues. Hence, upon diagonalizing s we see that the centralizer of s is a torus, yet u lies in this centralizer, so $u = 1$ due to the unipotence of u.

The following result of Steinberg rests on the full force of the classification and structure theory of connected semisimple groups, as well as a deep connectedness theorem (also due to Steinberg) that we will state but not prove (and these results of Steinberg will not be used in this course, but they are rather important).

Theorem 4.4 (Steinberg)**.** *If G is connected reductive over a field k then all regular elements g of $G(\overline{k})$ are semisimple, and $Z_G(g)/Z_G(g)^0$ is commutative with order not divisible by* $\mathrm{char}(k)$*. In particular, the regular locus is Zariski open.*

Note that by dimension considerations, the centralizer of a regular semisimple element has identity component equal to a Cartan subgroup, and hence to a maximal torus in the reductive case. Thus, in the setting of the theorem, $Z_G(g)^0$ is a torus.

Proof. We may assume $k = \overline{k}$. Let $g \in G(k)$ be a regular element. To prove it is semisimple it is harmless to multiply g against a *central* semisimple element (check!), and since $G = Z \cdot \mathscr{D}(G)$ where Z is the maximal central torus, we may replace G with $\mathscr{D}(G)$, so G is now semisimple.

The Existence, Isomorphism, and Isogeny Theorems for semisimple groups over an algebraically closed field provide the existence of a central isogeny $f : G' \to G$ where G' is a connected semisimple group that is *simply connected* in the sense that it admits no nontrivial central isogenous cover by another connected semisimple group. (Example: if $G = \mathrm{PGL}_n$ then $G' = \mathrm{SL}_n$, if $G = \mathrm{SO}_n$ then $G' = \mathrm{Spin}_n$, and Sp_{2g} is simply connected.)

There are several equivalent formulations of the "simply connected" property, especially in terms of the root system for G' (to be discussed later). Also, if $k = \mathbf{C}$ then this coincides with simply connectedness in the sense of topology (but this is not at all obvious: it is proved in C.4.1 in my SGA3 summer school notes, resting on a lot of input from the analytic theory). For our purposes, what matters is the important theorem of Steinberg (see 8.1 in his book "Endomorphisms of Linear Algebraic Groups") that centralizers of semisimple elements in *simply connected* semisimple groups are always *connected*. (Example: in class we saw a disconnected centralizer for an anti-diagonal element in PGL_2 away from characteristic 2; the analogous centralizer in SL_2 is connected.) It is this property that will be used in what follows. The proof of Steinberg's theorem uses the full force of the "root system" structure theory of connected semisimple groups.

Pick $g' \in G'$ over g, so its Jordan decomposition $s'u'$ lifts the one for g. By hypothesis s is regular, and we claim the same for s'. Let T' be a maximal torus containing s', so its image $T = f(T')$ is a maximal torus in G containing s. Since f is a central isogeny, $T' = f^{-1}(T)$ and $T = T'/(\ker f)$. By regularity, T is the unique maximal torus of G containing s, so likewise (since f is an isogeny) T' is the unique maximal torus of G' containing s'. But to prove that s' is regular, we need to relate $\Phi(G', T')$ to $\Phi(G, T)$ (since regularity is characterized in terms of roots). Hence, a key fact is the important:

Proposition 4.5. *For any central isogeny $f : G' \to G$ between connected reductive groups over $k = \overline{k}$ and any maximal torus $T' \subset G'$ and $T = T'/(\ker f) \subset G$, the finite-index lattice inclusion* $\mathrm{X}(T) \subset \mathrm{X}(T')$ *carries the subset $\Phi(G, T)$ bijectively onto $\Phi(G', T')$.*

(This may seem slightly surprising when f is an inseparable isogeny, as it is then not surjective between Lie algebras yet we defined roots in terms of the action on Lie algebras.)

Proof. The isogeny $T' \to T$ gives that $\mathrm{X}(T)_{\mathbf{Q}} \to \mathrm{X}(T')_{\mathbf{Q}}$ is an isomorphism, so we can choose a cocharacter $\lambda' \in \mathrm{X}_*(T')$ that is "generic" for (G', T') and for which the composition $\lambda = f \circ \lambda'$ is "generic" for (G, T). Hence, we have compatible open subsets

$$U_{G'}(-\lambda') \times T' \times U_{G'}(\lambda') \subset G', \quad U_G(-\lambda) \times T \times U_G(\lambda) \subset G$$

such that the torus and either flanking factor forms a semi-direct product subgroup of the ambient group (G' or G). But centrality of f implies $\ker f \subset Z_{G'}(T') = T'$, so

$$\ker(G' \to G) = \ker(T' \to T)$$

and hence the quotient maps $U_{G'}(\pm\lambda') \twoheadrightarrow U_G(\pm\lambda)$ are *isomorphisms*. Passing to the resulting isomorphisms between their Lie algebras, equivariant with respect to $T' \twoheadrightarrow T$, it follows that each T'-root line in $\mathfrak{g}'$ is carried onto a T-root line in $\mathfrak{g}$. This gives the desired bijection. ■

Returning to the proof of Theorem 4.4, we now show that s' is regular in G'. It suffices to show that the roots in $\Phi(G', T')$ are all nontrivial on s'. But by Proposition 4.5, these roots are the pullback of $\Phi(G, T)$ along the isogeny $f : T' \to T$, so it is the same to check that $s = f(s')$ is not killed by any roots of $\Phi(G, T)$. That in turn holds because s is regular. Since s' is regular, so g' is regular, we know that $Z_{G'}(s')^0$ is a Cartan subgroup of G' (for dimension reasons). But this contains T', which is itself a Cartan subgroup (as G' is reductive), so $Z_{G'}(s')^0 = T'$. Now comes the key point: by Steinberg's theorem, $Z_{G'}(s')$ is connected, so in fact $Z_{G'}(s') = T'$; in particular, $Z_{G'}(s')$ is *commutative*. This is really the crux.

The same reasoning as just used shows that $Z_G(s)^0 = T$. We will construct an injective homomorphism of $Z_G(s)/T$ into $(\ker f)(k)$. The finite group $(\ker f)(k)$ lies in T', so it is abelian with order not divisible by the characteristic of k, and so it would follow that $g \in Z_G(s)$ would have to be semisimple, completing the argument.

To define the desired homomorphism, we first note that the G'-action on itself by conjugation factors through an action by the central quotient $G = G'/(\ker f)$. Concretely, for any $h \in G(k)$ we pick a lift $h' \in G'(k)$ and note that the h'-conjugation action on G' is independent of the choice of lift since it is unaffected by scaling h' by a central element of G'. Any $h \in Z_G(s)$ must normalize $T = Z_G(s)^0$, so its action on G' normalizes $T' = f^{-1}(T)$. Points of $Z_G(s)^0 = T$ act trivially on T' under this action, so we get an action of $Z_G(s)/T$ on T'. Denote this by $h.t'$, so $h.s'$ is a lift of s. But s' is also such a lift, so $(h.s')/s' \in (\ker f)(k)$. The map $h \mapsto (h.s')/s'$ is a homomorphism from $Z_G(s)/T$ into $(\ker f)(k)$ because

$$h_1.(h_2.s') = h_1.((h_2.s')/s')s') = ((h_2.s')/s')(h_1.s')$$

due to the triviality of the G-action on the *central* elements of G' such as $(h_2.s')/s' \in (\ker f)(k)$. Dividing by s' inside the commutative T' then gives the homomorphism property. By construction, if h is killed by this homomorphism then $h.s' = s'$, so for a representative $\widetilde{h} \in Z_G(s)$ of h we see that any lift $\widetilde{h}' \in f^{-1}(\widetilde{h})$ lies in $Z_{G'}(s')$. But $Z_{G'}(s')$ is *connected*, so in such cases $\widetilde{h} = f(\widetilde{h}') \in Z_G(s)^0$, which says $h = 1$. ■

Remark 4.6. The definition of "regular" that we use above coincides with the definitions in Borel's textbook and in Bourbaki LIE VII (for Lie groups and Lie algebras). But for connected reductive G over a field there is another definition which is useful and agrees on semisimple geometric points but otherwise is quite different. Moreover, it leads to a rich theory, even for unipotent geometric points (which are never regular in a nontrivial connected reductive group under the above definition, as their semisimple part is 1, which is never regular in such a group). This alternative viewpoint on regularity is developed in Steinberg's paper "Regular elements of semisimple groups" that is reprinted as an Appendix in the back of Serre's book "Galois cohomology".

The key point is that for *any* connected linear algebraic group G over a field k, the dimension function $g \mapsto \dim Z_{G_{k(g)}}(g)$ is upper semi-continuous on the scheme G (i.e.,"jumps up along closed sets", which is to say $\{\dim Z_{G_{k(g)}}(g) \geq n\}$ is closed in G for all n). To prove this, consider $V \subset G \times G$ the (possibly reducible) closed set defined by the condition $g = g'g{g'}^{-1}$ on pairs $(g, g') \in G \times G$, so $\mathrm{pr}_1 : V \to G$ has g-fiber $Z_{G_{k(g)}}(g)$. We just need to check that this surjective map has fiber dimension that is upper semi-continuous

In general, for a map $h : X \to Y$ between finite type k-schemes the function $x \mapsto \dim_x X_{h(x)}$ is upper semi-continuous (Chevalley's theorem), and $y \mapsto \dim X_y$ is generally only a constructible function. But the fibers of $\mathrm{pr}_1 : V \to G$ are *groups*, so they are equidimensional and so the fiber dimension can be read off at any geometric point of a fiber. Hence, for the identity section $\sigma : g \mapsto (g, e)$ to pr_1, the composition of the continuous σ with the upper semi-continuous "local fiber dimension" function on V recovers the function $g \mapsto \dim Z_{G_{k(g)}}(g)$ and so establishes its upper semi-continuity.

It follows from the upper semi-continuity that there is a dense open subscheme $\mathscr{U} \subset G$ that is *precisely* the locus on which the centralizer dimension attains its minimal value. By the deep Theorem 4.4 applied to the connected reductive G over $k = \overline{k}$, there is a dense open locus of points $\Omega \subset G(k)$ that are regular semisimple. But $Z_G(g)$ is *smooth* for semisimple g, and its Lie algebra is the 1-eigenspace for $\mathrm{Ad}_G(g)$, which is $\mathrm{Lie}(T)$ for the unique maximal torus T containing g. Since $\dim Z_G(g) = r(G)$ for such g and $\mathscr{U}(k) \bigcap \Omega$ must be non-empty, we conclude that the condition $\dim Z_G(g) = r(G)$ defines a *dense open* subscheme of G. Beware that this open locus may contain unipotent geometric points! (Indeed, nothing we have done above tells us much about the structure of $Z_G(g)$ when g is not semisimple.)

In fact, by the results in 3.1–3.3 of Steinberg's paper, the following hold. Unipotent regular elements exist in $G(k)$ for any connected reductive G over $k = \overline{k}$ (in contrast with the notion of regularity as defined in Borel's book and in Bourbaki LIE VII, assuming $G \neq 1$), such elements exhaust a single $G(k)$-conjugacy class, and they are characterized by the condition of lying in only finitely many or even exactly one Borel subgroup B of G. Moreover, if B is a Borel subgroup and $u \in \mathscr{R}_u(B)$ then there is a characterization of when u is regular in terms of the "root group" decomposition of $\mathscr{R}_u(B)$ relative to a maximal torus of B. For $G = \mathrm{GL}_n$ or SL_n and the upper triangular Borel subgroup B^+, this amounts to the condition of having nonzero entries along the entire super-diagonal (often called *principal unipotent* elements).

5. Lie algebra application

We end this discussion of applications of Borel's covering theorem with a Lie-theoretic version of Theorem 2.1 (which we will never use):

Theorem 5.1 (Grothendieck)**.** *Let G be a connected linear algebraic group over $k = \overline{k}$. For $X \in \mathfrak{g}$, if $X \in \mathfrak{g}_{\mathrm{ss}}$ then $X \in \mathrm{Lie}(T)$ for a torus $T \subset G$ and if $X \in \mathfrak{g}_{\mathrm{n}}$ then $X \in \mathrm{Lie}(U)$ for some unipotent smooth connected subgroup $U \subset G$.*

We will give the proof for semisimple X, but in the nilpotent case we will reach a step where the entire apparatus of root systems and the structure theory of connected semisimple groups has to be invoked, at which point we will punt to Borel's book for the additional details (to be read later, after we develop that structure theory).

Suppose first that X is semisimple. Imitating the centralizer technique for building tori containing semisimple elements of G, consider the scheme-theoretic centralizer $Z_G(X)$ of X under the action $\mathrm{Ad}_G : G \to \mathrm{GL}(\mathfrak{g})$. (This is just the scheme-theoretic preimage under Ad_G of the smooth stabilizer group of $\mathrm{GL}(\mathfrak{g})$ fixing the point X.) In characteristic 0 this preimage is smooth by Cartier's theorem, and we claim it is smooth even in characteristic $p > 0$ (by analogy with Lemma 3.2). Granting such smoothness, we can settle the case of semisimple X as follows.

We can replace G with $Z_G(X)^0$ so that $X \in \mathfrak{g}^G$ (centralized by the adjoint action). Hence, for a maximal torus $T \subset G$ we have $X \in \mathfrak{g}^T = \mathrm{Lie}(Z_G(T))$. We can therefore replace G with its Cartan subgroup $Z_G(T) = T \times U$. But then $X \in \mathrm{Lie}(T)$ because the unipotent quotient map $G \to G/T = U$ induces a Lie algebra map that must kill the semisimple X since the Jordan decomposition in Lie algebras of linear algebraic groups is *functorial in the group* (and $\mathrm{Lie}(U)$ consists entirely of nilpotent elements relative to its incarnation as the Lie algebra of U). Thus, the semisimple case is reduced to proving:

Lemma 5.2. *If* $\mathrm{char}(k) = p > 0$ *and* $X \in \mathfrak{g}_{\mathrm{ss}}$ *then* $Z_G(X)$ *is smooth.*

Proof. We will imitate the technique of studying the action of a semisimple element by putting it inside a torus, except that now tori will be replaced by powers of μ_p. Fix an inclusion $j : G \hookrightarrow \mathrm{GL}_n$, so X is carried to a semisimple element X' of $\mathfrak{gl}_n = \mathrm{Mat}_n$ over $k = \overline{k}$. Since X' can be diagonalized, clearly $X' \in \mathrm{Lie}(T')$ for a maximal torus $T' \subset \mathrm{GL}_n$. Thus, $X \in \mathfrak{g} \bigcap \mathrm{Lie}(T') = \mathrm{Lie}(G \bigcap T')$. Although $G \bigcap T'$ may not be smooth, this doesn't matter: the Frobenius kernel $\mu = \ker F_{(G \bigcap T')/k}$ makes sense and is a subgroup scheme of $\ker F_{T'/k} = T'[p] = \mu_p^r$ ($r = \dim T'$). By Cartier duality with powers of $\mathbf{Z}/p\mathbf{Z}$, we see that every subgroup scheme of μ_p^r is a power of μ_p, so this applies to the Frobenius kernel μ of $G \bigcap T'$.

To summarize, $\mu \simeq \mu_p^e$ (with $e \geq 0$) is a subgroup scheme of G such that $X \in \mathrm{Lie}(\mu)$ inside $\mathfrak{g}$. The smoothness of $Z_G(X)$ now can be studied via the infinitesimal method, exactly as in the earlier work which proved the smoothness of torus centralizers (in Exercise 3 of HW8 of the previous course). The problem comes down to proving that under any linear representation $\rho : G \to \mathrm{GL}(V)$, the induced representation $\mathrm{Lie}(\rho) : \mathfrak{g} \to \mathrm{End}(V)$ makes X act semisimply on V (i.e., can be diagonalized). For this purpose it suffices to show that the entire action of $\mathrm{Lie}(\mu)$ is completely reducible according to *characters* $\chi : \mu \to \mathbf{G}_m$ (as then the restrictions of the tangential characters $\mathrm{Lie}(\chi)$ to X gives an eigenspace decomposition for V under the action of X, as desired). Now the role of X has been eliminated: it suffices to show that any linear representation of μ_p^e on V is completely reducible according to characters $\chi_i : \mu_p^e \to \mathbf{G}_m$.

For any finite abelian group Λ (such as $\Lambda = (\mathbf{Z}/p\mathbf{Z})^e$), linear representations of the Cartier dual $\mathbf{D}(\Lambda)$ on V are canonically identified with Λ-gradings on V; this goes *exactly* as in our study of $\mathbf{G}_m^r$-actions and $\mathbf{Z}^r$-gradings in the February 24 lecture of the previous course. Thus, exactness properties for graded parts yield the complete reducibility via $\mathbf{G}_m$-valued characters of μ. ■

Now we turn to the case $X \in \mathfrak{g}_{\mathrm{n}}$. If G is solvable then $G = T \ltimes U$ and the resulting quotient map $q : G \to T$ with kernel U must kill X on Lie algebras (due to the nilpotence of X and the functoriality *in the groups* of the Jordan decomposition in Lie algebras). Hence, $X \in \ker(\mathrm{Lie}(q)) = \mathrm{Lie}(\ker q) = \mathrm{Lie}(U)$, thereby settling the case of solvable G. Since the solvable case has been solved in general, it suffices to show that $\mathfrak{g}$ is covered by Lie algebras of solvable smooth connected subgroups, such as Borel subgroups. In other words, we are reduced to proving a Lie-theoretic analogue of Borel's covering theorem by Borel subgroups:

Proposition 5.3. *Let G be a connected linear algebraic group over $k = \overline{k}$, and $B_0 \subset G$ a Borel subgroup. Then* $\mathfrak{g} = \bigcup_{g \in G(k)} \mathrm{Ad}_G(g)(\mathrm{Lie}(B_0))$.

Proof. Let $R = \mathscr{R}(G)$, so R lies in every conjugate of B_0. Hence, for the connected semisimple $G' = G/R$ it is equivalent to show that

$$\mathfrak{g}' = \bigcup_{g' \in G'(k)} \mathrm{Ad}_{G'}(g')(\mathrm{Lie}(B_0/R)).$$

That is, we can assume that G is semisimple.

Let's try to imitate Borel's proof of the analogous result for groups by considering the composite morphism of varieties

$$f : G \times \mathfrak{g} \simeq G \times \mathfrak{g} \to (G/B_0) \times \mathfrak{g},$$

where the first step is $(g, v) \mapsto (g, \mathrm{Ad}_G(g)(v))$ and the second step is $(g, v) \mapsto (g \bmod B_0, v)$. Since G/B_0 is complete, the same arguments (now using f) as in the proof of the analogous result for groups gives that $\bigcup_{g \in G(k)} \mathrm{Ad}_G(g)(\mathrm{Lie}(B_0))$ is *closed* in $\mathfrak{g}$ relative to the Zariski topology.

Likewise, to prove the density of this closed set it suffices to prove a finiteness result: for some smooth closed subgroup $H \subset B_0$ with finite index in its normalizer we just need to find some $v \in \mathfrak{g}$ such that the number of $\mathrm{Ad}_G(G(k))$-conjugates $H' \subset G$ satisfying $v \in \mathrm{Lie}(H')$ is *finite*. In the group case we took H to be a Cartan subgroup (so H' varied through the Cartan subgroups of G) and found that a "generic" element of its maximal torus (namely, a regular semisimple element) did the job, even lying in a unique Cartan subgroup. In the Lie algebra case we will have to take $H = B_0$ because of certain complications (soon to be explained) in positive characteristic; note that B_0 is even equal to its normalizer (Chevalley's theorem). To summarize, we seek $v \in \mathfrak{g}$ that lies in $\mathrm{Lie}(B)$ for only finitely many B.

Inspired by the group case, it is tempting to try taking v to be a "generic" element of $\mathrm{Lie}(T_0)$ for a maximal torus $T_0 \subset B_0$, with an eye towards showing that if $v \in \mathrm{Lie}(B)$ for a Borel subgroup B then $B = B_0$, or at least $T_0 \subset B$ (which would restrict B to only finitely many possibilities). In view of the settled semisimple case (applied to B), if $v \in \mathrm{Lie}(B)$ then $v \in \mathrm{Lie}(S)$ for some maximal torus $S \subset B$, so $\mathrm{Lie}(S) \subset \ker([v, \cdot])$. But $\mathrm{ad}_{\mathfrak{g}} : \mathfrak{g} \to \mathrm{End}(\mathfrak{g})$ is $\mathrm{Lie}(\mathrm{Ad}_G)$, so $[v, \cdot] = \mathrm{ad}_{\mathfrak{g}}(v)$ acts on $\mathfrak{g}_a$ via multiplication by $\mathrm{d}a_1(v) \in k$ (and acts as 0 on $\mathrm{Lie}(T_0)$), where $\mathrm{d}a_1 : \mathrm{Lie}(T_0) \to k$ is $\mathrm{Lie}(a)$ composed with the *canonical* identification $\mathrm{Lie}(\mathbf{G}_m) = k$ via the invariant vector field $t\partial_t$ on $\mathbf{G}_m$ (e.g., for $a : \mathbf{G}_m \to \mathbf{G}_m$ given by $c \mapsto c^n$, $\mathrm{d}a_1(xt\partial_t) = nx$ since $t\partial_t$ is dual to $\mathrm{d}t/t$ and $a^*(\mathrm{d}t/t) = n\mathrm{d}t/t$).

Hence, if we had $\mathrm{d}a_1(v) \neq 0$ for all $a \in \Phi(G, T_0)$ (as is automatic for generic $v \in \mathrm{Lie}(T_0)$ when $\mathrm{char}(k) = 0$) then consideration of the T_0-weight decomposition of $\mathfrak{g}$ would give $\ker([v, \cdot]) = \mathrm{Lie}(T_0)$, so $\mathrm{Lie}(S) \subset \mathrm{Lie}(T_0)$, forcing equality for dimension reasons. This would yield $\mathrm{Lie}(T_0) = \mathrm{Lie}(S) \subset \mathrm{Lie}(B)$, so If we also knew that a containment $\mathrm{Lie}(T') \subset \mathrm{Lie}(B')$ for a maximal torus $T' \subset G$ and Borel subgroup $B' \subset G$ forces $T' \subset B'$ (as is automatic when $\mathrm{char}(k) = 0$) then we would win: B would have to contain T_0 and hence be constrained to finitely many possibilities.

The preceding argument shows that whenever $\mathrm{d}a_1 \neq 0$ for all $a \in \Phi(G, T_0)$ (i.e., $\mathrm{char}(k) = 0$ or $\mathrm{char}(k) = p > 0$ and all roots lie outside $p\mathrm{X}(T_0)$) then any $v \in \mathrm{Lie}(T_0)$ that lies outside the resulting "root hyperplanes" $\ker \mathrm{d}a_1 \subset \mathrm{Lie}(T_0)$ ("regular semisimple" in a Lie algebra sense) does the job *provided* that a containment relation "$T_0 \subset B$" can be detected at the Lie algebra level inside $\mathfrak{g}$. But this latter feature fails quite dramatically:

Example 5.4. Suppose $\mathrm{char}(k) = 2$. The 1-dimensional diagonal torus T_0 of SL_2 then has the same Lie algebra as the central infinitesimal $\mu_2 \subset T_0$ for dimension reasons. Hence, *every* maximal torus of SL_2 has Lie algebra equal to the central $\mathrm{Lie}(\mu_2) \subset \mathfrak{sl}_2$ (as all such torus are $\mathrm{SL}_2(k)$-conjugate to the diagonal one, and such conjugation has no effect on the central μ_2). It follows that for *every* maximal torus $T \subset \mathrm{SL}_2$ we have $\mathrm{Lie}(T) = \mathrm{Lie}(Z_{\mathrm{SL}_2}) \subset \mathrm{Lie}(B_0)$ (with B_0 a fixed Borel subgroup), but most maximal tori do not lie in a fixed B_0.

In principle there could be similar problems with other groups in any positive characteristic, but:

Remark 5.5. It turns out that Example 5.4 is the *only* counterexample: for "simple" semisimple groups aside from SL_2 in characteristic 2, containment relations between maximal tori and Borel subgroups can always be checked at the Lie algebra level! However, the proof of this requires case-checking with the full classification – not just general "root system" structure theory – of connected semisimple groups, and so lies way beyond the level of what we are presently trying to prove.

The preliminary condition that $da_1(v) \neq 0$ for all a is its own can of worms, since for any symplectic group Sp_{2g} there are roots in $2\mathrm{X}(T)$ (for $g = 1$ this is a basic fact for SL_2) and hence $da_1 = 0$ in characteristic 2 for such roots.

Remark 5.6. Inspection of the classification of semisimple groups shows that symplectic groups in characteristic 2 are the only simple semisimple groups in any characteristic such that $da_1 = 0$ for some root a. I don't know how to show that this cannot happen in other positive characteristics with other simple semisimple groups without case-checking against the classification.

To summarize, the attempt to use a generic $v \in \mathrm{Lie}(T_0)$ runs into serious potential problems in positive characteristic (which we know are real problems in characteristic 2). There remains only one other natural idea: try to use a "generic" nilpotent $v \in \mathrm{Lie}(B_0)$. That is, if $U_0 = \mathscr{R}_u(B_0)$ then we consider $v \in \mathrm{Lie}(U_0)$ and wonder if a "generic" such v may lie in $\mathrm{Lie}(B)$ only for $B = B_0$. But what should "generic" mean for $v \in \mathrm{Lie}(U_0)$? Here is where the theory of root systems must be used, as we now briefly explain (and a more complete argument along these lines is given in 14.23 in Borel's textbook).

For motivation, let's consider GL_n and the unipotent radical U^+ of the upper triangular Borel B^+. What should be a "generic" unipotent element u of U^+? It turns out that the right notion of genericity is that u should be what is called a *principal unipotent element*: its entries on the super-diagonal (entries just above the diagonal) are all nonzero (see the end of Remark 4.6). For example, in GL_3 a principal unipotent element in U^+ is one of the form

$$u = \begin{pmatrix} 1 & a & * \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}$$

with $a, b \neq 0$. Likewise at the Lie algebra level, we say $v \in \mathrm{Lie}(U^+)$ is "principal nilpotent" if

$$v = \begin{pmatrix} 0 & a & * \\ 0 & 0 & b \\ 0 & 0 & 0 \end{pmatrix}$$

with $a, b \neq 0$. What is the intrinsic meaning of this condition?

Relative to the diagonal maximal torus T_0 with $\mathrm{X}(T_0) = \mathbf{Z}^3$, $\Phi(\mathrm{GL}_3, T_0)$ consists of the elements $\pm(e_i - e_j)$ with $i \neq j$ (where $t^{e_i} = t_i$), so the set of roots $\Phi(B^+, T_0)$ consists of $\{e_i - e_j\}_{i<j}$. This is an example of a "positive system of roots" $\Phi^+ \subset \Phi$: a set of roots on one side of a hyperplane in $\mathrm{X}(T)_{\mathbf{Q}}$ that avoids all roots (there are other equivalent definitions that are useful). The root group for $e_i - e_j$ in $\mathfrak{gl}_3 = \mathrm{Mat}_3$ is the "ij-entry", and in $\Phi(B^+, T)$ the roots $e_1 - e_2$ and $e_2 - e_3$ correspond to the two root spaces which appear in our definition of "principal nilpotent" element. But what is the significance of these two positive roots among the set $\Phi(B^+, T)$? These are the so-called "simple" positive roots: all positive roots are uniquely a sum among them with *non-negative* integer coefficients; e.g., $e_1 - e_3 = (e_1 - e_2) + (e_2 - e_3)$.

In general, any positive system of roots Φ^+ in a root system Φ admits a unique *base* $\Delta \subset \Phi^+$, which is a subset such that all elements of Φ^+ are uniquely a $\mathbf{Z}_{\geq 0}$-linear combination of Δ. These are called the *simple roots* relative to the choice of Φ^+; these matters will be discussed later in the course. Anyway, in general we will see that $B \mapsto \Phi(B, T_0)$ is a bijection between the set of Borel subgroups $B \supset T_0$ and the set of all positive systems of roots $\Phi^+ \subset \Phi$, and if $\Phi^+ = \Phi(B, T_0)$ then

$$\mathrm{Lie}(\mathscr{R}_u(B)) = \bigoplus_{a \in \Phi^+} \mathfrak{g}_a.$$

We say $v \in \mathrm{Lie}(\mathscr{R}_u(B))$ is *principal nilpotent* if its components in $\mathfrak{g}_a$ for a in the *base* $\Delta \subset \Phi^+$ are all nonzero. This turns out to be the right notion for our needs.

More specifically, if Δ_0 is the base of the positive system of roots $\Phi(B_0, T_0)$ in $\Phi(G, T_0)$ and if $X_a \in \mathfrak{g}_a$ is a nonzero element for each $a \in \Delta_0$ then

$$v = \sum_{a \in \Delta_0} X_a$$

turns out to be sufficiently "generic": B_0 is the unique Borel subgroup $B \subset G$ such that $v \in \mathrm{Lie}(B)$. This is proved (using input from the theory of root systems, Weyl groups, etc., as well as the Bruhat decomposition of $G(k)$ relative to (B_0, T_0)) in 14.23 in Borel's textbook.

■