Math 249C. Lang's theorem and unirationality

1. Introduction

This handout aims to prove two theorems. The first theorem is very useful for solving problems with connected reductive groups over infinite fields, and the second is useful for bypassing the failure of the Zariski-density consequences of the first theorem when working over finite fields. The first theorem is this:

Theorem 1.1. *Let G be a smooth connected affine group over a field K. If K is perfect or G is reductive then G is unirational over K (i.e., admits a dominant K-morphism from a dense open subset of an affine space over K).*

The importance of this theorem is the consequence that over an *infinite* ground field, the set of rational points of a connected reductive group is always Zariski-dense. That is a very powerful tool for relating abstract group theory of the set of rational points to the structure of the algebraic group (e.g., checking normality of a closed K-subgroup scheme by using conjugation by K-rational points in settings which are sensitive to ground field extension, such as with maximal K-split tori or minimal parabolic K-subgroups).

Remark 1.2. In the absence of reductivity and perfectness, it is *not* true that the set $G(K)$ of rational points is necessarily Zariski-dense. The classic counterexample of a positive-dimensional G for which $G(K)$ is even *finite* is due to Rosenlicht: if $K = k(t)$ for a field k of characteristic $p > 0$ and $G \subset \mathbf{G}_{\mathrm{a}}^2$ is the subgroup defined by $y^q = x - tx^q$ for a p-power $q > 2$ then $G(K) = \{(0,0)\}$ if $p > 2$ whereas $G(K) = \{(0,0),(1/t,0)\}$ if $p = 2$. (Allowing $q = p = 2$ gives a smooth affine conic, hence infinitely many K-points.) Rather generally, if K is *any* imperfect field of characteristic $p > 0$ and $q > 2$ is a p-power then for any $a \in K - K^p$ the K-group $\{y^q = x - ax^q\}$ is not unirational over K (though its locus of K-points may be Zariski-dense, such as if $K = K_s$). See Examples 11.3.1 and 11.3.2 in "Pseudo-reductive groups" for more details.

Now we turn to the statement of the second theorem that we will prove, aimed at overcoming a basic difficulty when working with smooth affine groups over finite fields: the set rational points is finite and hence is often insufficient as a tool for investigating the structure of the algebraic group. The following theorem is a very effective technique to circumvent the absence of Zariski-density techniques with rational points in the study of *connected* linear algebraic groups over finite fields:

Theorem 1.3 (Lang)**.** *Let G be a connected group scheme of finite type over a finite field k, and let X be a non-empty finite type k-scheme equipped with a left G-action $G \times X \to X$ such that $G(\overline{k})$ acts transitively on $X(\overline{k})$. Then $X(k)$ is non-empty.*

Lang's theorem is stated and proved in §16 of Borel's "Linear algebraic groups" book in the affine setting, but the proof works without affineness and so we will proceed in that generality.

In practice, Lang's theorem is often applied to a special class of X, namely G-torsors. The torsor property is the condition that the action is "simply transitive". To be precise, if H is a group scheme of finite type over a field K and E is a finite type K-scheme equipped with a left H-action then E is an H-*torsor* (for the fppf topology) if the natural map

$$H \times E \to H \times H$$

defined by $(h, x) \mapsto (h, h.x)$ is an isomorphism. The techniques of descent theory imply that in such cases, E inherits many "nice" properties of H (smoothness, properness, geometric connectedness, etc.). In case H is smooth, such an E is necessarily smooth and so $E(K_s)$ is non-empty; we then say E is a torsor for the étale topology (over K).

Example 1.4. A typical source of H-torsors is fibers over K-points for the faithfully flat quotient map $G \to H\backslash G$ with a finite type K-group scheme G containing H as a closed K-subgroup scheme, especially when G is smooth (and H is often but not always smooth). Lang's theorem is the key tool to use for lifting rational points of $H\backslash G$ to rational points of G when working over a finite field, in the presence of connectedness of H. Such connectedness is an essential assumption, as we see by trying to lift k-rational points to k-rational points through the quotient map $\mathrm{GL}_1 \to \mathrm{GL}_1$ defined by $t \mapsto t^n$ for an integer $n > 1$ (using $H = \mu_n$).

2. Proof of Theorem 1.3

Since X is non-empty, we may and do choose $x_0 \in X(\overline{k})$. We seek a k-point in X, and over $\overline{k}$ such a point must have the form $g_0(x_0)$ for some $g_0 \in G(\overline{k})$. For any k-scheme Z, denote the q-Frobenius morphism $F_{Z/k,q} : Z \to Z$ over k by the notation $z \mapsto z^{[q]}$ functorially on points. (Note that $F_{Z/k,q}$ is functorial in Z over k.) The k-rationality of a point $g_0(x_0) \in X(\overline{k})$ amounts to the "Galois-invariance" property $g_0(x_0)^{[q]} = g_0(x_0)$.

The G-action on X is defined over k, so

$$g_0(x_0)^{[q]} = (g_0)^{[q]}(x_0^{[q]}).$$

Hence, we can recast our problem is that of finding $g_0 \in G(\overline{k})$ such that

$$(g_0^{-1} \cdot (g_0)^{[q]})(x_0^{[q]}) = x_0.$$

Since the $G(\overline{k})$-action on $X(\overline{k})$ is transitive by hypothesis, $x_0^{[q]} = g'(x_0)$ for some $g' \in G(\overline{k})$. Thus, it suffices to show that for any $g' \in G(\overline{k})$, g'^{-1} has the form $g_0^{-1} \cdot (g_0)^{[q]}$ for some $g_0 \in G(\overline{k})$, or equivalently $g' = (g_0^{-1})^{[q]} \cdot g_0$. In other words, we are reduced to proving that the k-scheme morphism $L : G \to G$ defined by

$$L(g) = g^{[q]} \cdot g^{-1}$$

is surjective on $\overline{k}$-points (or equivalently, is a surjective map of k-schemes, as G is finite type over k). In the special case $G = \mathbf{G}_{\mathrm{a}}$ this is the Artin-Schreier map $t \mapsto t^q - t$, so the map L is a generalization of the Artin-Schreier homomorphism; it is called the *Lang map* (and is generally not a homomorphism when G is non-commutative). Our problem is now entirely about G and has nothing anymore to do with X.

Since k is perfect, G_{red} is a closed k-subgroup scheme of G whose formation commutes with any extension of the ground field, and it has the same $\overline{k}$-points as G. Thus, by functoriality of the q-Frobenius morphism with respect to the inclusion of G_{red} into G we may replace G with G_{red} so that G is reduced and hence smooth (as for any reduced group scheme of finite type over a perfect field). Now we may use tangent space considerations to investigate the local structure of k-morphisms from G to itself.

Consider the action of G on itself via $g.x = g^{[q]}xg^{-1}$. Clearly $L(G)$ is the orbit of the identity point. To show that this is the only orbit (and so L is surjective), by the connectedness of G and the disjointeness of distinct orbits it is enough to prove that *every* G-orbit on $G_{\overline{k}}$ is open. To do this, it is enough to show that the orbit map $g \mapsto g^{[q]}g_0g^{-1}$ through every $g_0 \in G(\overline{k})$ is an open map. We will show that all of these orbit maps $G \to G$ are étale. By smoothness of G, it is equivalent to check that such orbit maps are isomorphisms on tangent spaces at all points of the source. The homogeneity of orbit maps reduces this assertion to the isomorphism property at a single point of $G(\overline{k})$, such as the identity point.

More specifically, the map $g \mapsto g^{[q]}g_0g^{-1}$ carries e to g_0 and we claim that the induced map $\mathrm{T}_e(G) \to \mathrm{T}_{g_0}(G)$ is an isomorphism. It is harmless to post-compose with right translation by g_0^{-1}, so we are analyzing the map $f_{g_0} : g \mapsto L(g)\cdot(gg_0g^{-1}g_0^{-1})$. Recall the following differential identities: the group law $m : G\times G \to G$ induces addition $\mathrm{T}_e(G)\oplus\mathrm{T}_e(G) \to \mathrm{T}_e(G)$, inversion induces negation on $\mathrm{T}_e(G)$, and $F_{G/k,q}$ induces the zero map on $\mathrm{T}_e(G)$. Thus, $\mathrm{d}L(e)$ is negation and so

$$\mathrm{d}f_{g_0}(e) = \mathrm{d}L(e) + \mathrm{id} - \mathrm{Ad}_G(g_0) = -\mathrm{Ad}_G(g_0).$$

Hence, $\mathrm{d}f_{g_0}(e)$ is an isomorphism, so f_{g_0} is étale. This proves that every G-orbit is open, so we are done. In particular, the Lang map L is an étale surjection. In fact, we can do a bit better:

Proposition 2.1. *The fibers of L are right $G(k)$-cosets inside G. In particular, L has* constant *fiber rank (namely, the size of $G(k)$) over its open image $f(G)$.*

By using Zariski's Main Theorem, one can show that a quasi-compact separated étale map with constant fiber rank is necessarily *finite*, so $L : G \to G$ is not merely surjective étale but even finite. In fact, $L : g \mapsto g^{[q]}g^{-1}$ is visibly invariant under the right $G(k)$-action on G, so L actually exhibits G as a right $G(k)$-torsor over itself. For commutative G, the map L is usually called the *Lang isogeny.*

Proof. It suffices to check that L is étale on $G_{\overline{k}}$ at any $\overline{k}$-point g_0, with each fiber $L^{-1}(L(g_0))$ a right $G(k)$-coset inside $G(\overline{k})$. For the étale property of L at g_0, it is equivalent to prove the étale property of $g \mapsto L(g_0g)$ at the identity. But

$$L(g_0g) = g_0^{[q]}(g^{[q]}g^{-1})g_0^{-1} = g_0^{[q]} \cdot L(g) \cdot g_0^{-1}.$$

Since L is étale at the identity, and post-composing with left translation by $g_0^{[q]}$ and right translation by g_0^{-1} amounts to applying automorphisms on the target, the desired étaleness is established.

Analyzing the fibers amounts to an elementary computation: for $g, g_0 \in G(\overline{k})$, the equality $L(g) = L(g_0)$ says exactly that $g_0^{-1}g$ is fixed by $F_{G/k,q}$ on $G(\overline{k})$. But the set of such fixed points is exactly $G(k)$, so $L(g) = L(g_0)$ if and only if $g_0^{-1}g \in G(k)$, which is to say $g \in g_0G(k)$. ■

Lang's theorem has some very useful consequences:

Corollary 2.2. *Let G be a smooth connected affine group over a finite field k. There exists a k-torus $T \subset G$ that is maximal over $\overline{k}$ and there exists a Borel k-subgroup $B \subset G$.*

The proof of Grothendieck's theorem on the existence of (geometrically!) maximal tori over the ground field is carried out almost entirely over infinite fields via Zariski-density considerations with "rational points" in Lie algebras over the ground field. The case of finite fields is punted to Lang's theorem via exactly the torus part of the corollary that we are now going to prove.

Proof. The "right" proof is to construct moduli schemes $\mathrm{Tor}_{G/k}$ and $\mathrm{Bor}_{G/k}$ whose sets of rational points over any extension field k'/k are respectively naturally identified with the set of geometrically maximal k'-tori and the set of Borel k'-subgroups, and to apply Lang's theorem with X taken to be either of these moduli schemes (equipped with the natural *transitive* G-action via conjugation). To be precise, over an arbitrary field k there exist closed subschemes

$$\mathscr{T} \subset G \times \mathrm{Tor}_{G/k}, \;\; \mathscr{B} \subset G \times \mathrm{Bor}_{G/k}$$

that respectively represent functors of maximal tori and Borel subgroups in a relative setting, or in a weaker (but sufficient) sense recover exactly the geometrically maximal k'-tori and the Borel k'-subgroups as we vary through all k'-point fibers of $\mathscr{T} \to \mathrm{Tor}_{G/k}$ and $\mathscr{B} \to \mathrm{Bor}_{G/k}$ inside $G_{k'}$ with any extension field k'/k. For our limited purposes, rather than construct such moduli schemes (which is a game of Galois descent for perfect ground fields, and very delicate over imperfect fields), we will instead adapt the *method* of proof of Lang's theorem rather than apply the *statement* of the theorem.

We give the argument for geometrically maximal tori, and the case of Borel subgroups goes in exactly the same way. Pick a maximal torus $T' \subset G_{\overline{k}}$, so we seek $g \in G(\overline{k})$ such that $gT'g^{-1}$ is $\mathrm{Gal}(\overline{k}/k)$-invariant. In other words, if k has size q then we want that $F_{G/k,q}(gT'g^{-1}) = gT'g^{-1}$. This says that $(g^{[q]})^{-1}gT'g^{-1}g^{[q]} = T'^{[q]}$. Since $T'^{[q]}$ and T' are maximal tori in $G_{\overline{k}}$, by the conjugacy of maximal tori over $\overline{k}$ there exists $g' \in G(\overline{k})$ such that $g'T'g'^{-1} = T'^{[q]}$. Hence, it suffices to find $g \in G(\overline{k})$ such that $(g^{[q]})^{-1}g = g'$. This says that the Lang map $L : G \to G$ carries g^{-1} onto g'. Since the Lang map is surjective, we are done. ■

3. Proof of Theorem 1.1

First we show that the general case over perfect fields reduces to the reductive case. Over perfect K the unipotent radical $\mathscr{R}_u(G_{\overline{K}})$ descends to a normal unipotent smooth connected K-subgroup $U \subset G$ due to Galois descent, and G/U is reductive. Since K is perfect, we know that U is K-split; i.e., has a composition series

$$\{1 = U_0 \subset U_1 \subset \cdots \subset U_n = U\}$$

over K whose successive quotients U_i/U_{i-1} are K-isomorphic to $\mathbf{G}_{\mathrm{a}}$. Thus, a U-torsor over *any* field extension of K (such as the function field $K(G/U)$) vanishes by successive applications of additive Hilbert 90, so the U-torsor $q : G \to G/U$ admits a rational point on its generic fiber. This $K(G/U)$-point "spreads out" to a section s of q over a dense open Ω in G/U, so there is an open immersion $U \times \Omega \to G$ defined by $(u, \omega) \mapsto u \cdot s(\omega)$. Thus, if G/U (and hence Ω) is unirational over K then the unirationality of G reduces to that of U. But the same torsor method applied to a composition series of U via induction on $\dim(U)$ shows that U has a dense open subset that is open in an affine space. (Stronger cohomological methods show that U itself is K-isomorphic to an affine space, but we do not need that here.)

Now it remains to treat the reductive case over any field, though we will treat characteristic zero by a separate argument from positive characteristic (and finite fields will also be treated by a special argument). The idea of the proof in the reductive case is to show that G is "generated by K-tori", which is to say that there is a finite set of K-tori in G that generate G as a K-group, or equivalently a finite set of K-tori $T_1, \dots, T_r \subset G$ such that the multiplication map of K-schemes

$$T_1 \times \cdots \times T_r \to G$$

is dominant. The reason that such dominance suffices is to due:

Lemma 3.1. *Every torus T over a field K is unirational over K.*

Proof. Let $\Gamma = \mathrm{Gal}(K_s/K)$, so the category of K-tori is anti-equivalent to the category of Γ-lattices (i.e., finite free $\mathbf{Z}$-modules equipped with a discrete continuous left Γ-action); the Γ-lattice associated to T is the character group $\mathrm{X}(T_{K_s})$.

Let K'/K be a finite Galois subextension of K_s that splits T, so $\mathrm{X}(T_{K_s})$ is a $\mathrm{Gal}(K'/K)$-lattice. The category of $\mathrm{Gal}(K'/K)$-representations on finite-dimensional $\mathbf{Q}$-vector spaces is semisimple, and more specifically $\mathrm{X}(T_{K_s})_{\mathbf{Q}}$ is a subrepresentation of a finite direct sum of copies of the regular representation $\mathbf{Q}[\mathrm{Gal}(K'/K)]$. Scaling by a sufficiently divisible nonzero integer, we thereby identify $\mathrm{X}(T_{K_s})$ as a subrepresentation of a finite direct sum of copies of $\mathbf{Z}[\mathrm{Gal}(K'/K)]$ equipped with its natural Γ-action.

The Γ-lattice $\mathbf{Z}[\mathrm{Gal}(K'/K)]$ corresponds to the Weil restriction torus $\mathrm{R}_{K'/K}(\mathrm{GL}_1)$ (check!), so an inclusion

$$\mathrm{X}(T_{K_s}) \hookrightarrow \mathbf{Z}[\mathrm{Gal}(K'/K)]^{\oplus r}$$

corresponds to a surjective map of K-tori $\mathrm{R}_{K'/K}(\mathrm{GL}_1)^r \to T$. The unirationality of tori over K is thereby reduced to the special case of tori of the form $\mathrm{R}_{K'/K}(\mathrm{GL}_1)$ for finite separable extensions K'/K. By thinking functorially, we see that $\mathrm{R}_{K'/K}(\mathrm{GL}_1)$ is the open non-vanishing locus of the norm morphism $\mathrm{N}_{K'/K} : \mathrm{R}_{K'/K}(\mathbf{A}^1_{K'}) \to \mathbf{A}^1_K$). ■

Beware that we *cannot* expect to establish dominance of a map $T_1 \times \cdots \times T_r \to G$ by proving surjectivity on tangent spaces at $(e, \dots, e)$ (which would ensure smoothness, and hence openness, at $(e, \dots, e)$), since such surjectivity can fail: for $G = \mathrm{SL}_2$ in characteristic 2 the diagonal maximal torus D has Lie equal equal to $\mathrm{Lie}(D[2])$ where $D[2] = \mu_2$ is the *center* of G, so conjugation on D has no effect on this Lie algebra! That is, all maximal tori in SL_2 have the *same* Lie algebra. Observe that this problem does not arise for PGL_2.

As in the proof of Grothendieck's theorem on (geometrically) maximal tori, we will use Zariski-density arguments with rational points of Lie algebras, so the case of finite ground fields has to be treated separately. Thus, we first dispose of the case of finite fields:

Lemma 3.2. *Any connected reductive group G over a finite field k is unirational over k.*

Proof. We abandon the attempt to show that G is generated by maximal k-tori, and instead proceed in another way. (In fact G *is* generated by its maximal k-tori, but Gabber's proof of this fact over finite fields is rather delicate and so we omit it.) By Corollary 2.2, there exists a Borel k-subgroup $B \subset G$. Choose a maximal k-torus $T \subset B$. Over $\overline{k}$ there is a unique

Borel subgroup of $G_{\overline{k}}$ containing $T_{\overline{k}}$ that is "opposite" to $B_{\overline{k}}$ (i.e., its intersection with $B_{\overline{k}}$ is precisely $T_{\overline{k}}$, or equivalently its Lie algebra supports precisely the set of roots $-\Phi(B_{\overline{k}}, T_{\overline{k}})$ inside $\Phi(G_{\overline{k}}, T_{\overline{k}})$). The uniqueness over $\overline{k}$ implies via Galois descent that this opposite Borel subgroup descends to a Borel k-subgroup $B' \subset G$ containing T with $B' \cap B = T$.

By another application of Galois descent for the perfect field k, the k-unipotent radicals $U := \mathscr{R}_{u,k}(B)$ and $U' := \mathscr{R}_{u,k}(B')$ descend the unipotent radicals of $B_{\overline{k}}$ and $B'_{\overline{k}}$ respectively. Thus, the "open cell" structure for $(G_{\overline{k}}, T_{\overline{k}}, B_{\overline{k}})$ implies that the multiplication map

$$U' \times T \times U \to G$$

is an open immersion, so it suffices to show that each of T, U, and U' are unirational over k. The case of T is handled by Lemma 3.1, so it suffices to show that any unipotent smooth connected affine k-group U is unirational over k. This unirationality has been explained at the start of this section for *split* unipotent smooth connected groups over any field, and the split condition is automatic when the ground field is perfect (such as a finite field). ■

Now we may and do assume that K is infinite. We give two proofs, depending on the characteristic of K. The arguments are similar, but technically not quite the same.

Case 1: characteristic 0. First we assume K has characteristic 0, and shall proceed by induction on $\dim(G)$ without a reductivity hypothesis. As we have already noted, we may assume both that G is reductive (so the characteristic 0 hypothesis has not been of much use yet) and that all lower-dimensional smooth connected K-subgroups are generated by K-tori. Consider the central isogeny $\pi : G \to G^{\mathrm{ad}} := G/Z_G$ with G^{ad} having *trivial* center. As for any central quotient map between connected reductive groups, the formation of images and preimages defines a bijective correspondence between the sets of maximal K-tori of G (all of which contain Z_G) and of G^{ad}. Hence, if we can find maximal K-tori $T'_1, \dots, T'_r$ of G^{ad} that generate G^{ad} then G is generated by their maximal K-torus preimages $T_i = \pi^{-1}(T'_i)$. Consequently, it is harmless to assume that G is semisimple of adjoint type, and nontrivial.

It follows that $G_{\overline{K}}$ contains (i) a non-central GL_1 and (ii) *no* nontrivial central subgroup scheme over $\overline{K}$. It was precisely under such geometric hypotheses on a general smooth connected affine group over an infinite field K that we showed (via Zariski-density considerations in the Lie algebra over K, and a lot of extra work in positive characteristic) in the proof of Grothendieck's theorem on the existence of geometrically maximal K-tori that $\mathfrak{g}$ contains a semisimple element X that is non-central (i.e., $\mathrm{ad}_{\mathfrak{g}}(X) \neq 0$). The non-central non-nilpotent locus in $\mathfrak{g}$ is Zariski-open and non-empty, hence Zariski-dense (as K is infinite), so for any proper K-subspace $V \subset \mathfrak{g}$ there exists a non-central non-nilpotent $X \in \mathfrak{g} - V$. So far this is characteristic-free (and the non-nilpotence of X will not be used in characteristic 0).

Since $\mathrm{char}(K) = 0$, the K-subgroup $Z_G(X)^0$ is smooth and connected with Lie algebra equal to the *proper* subspace $\mathfrak{z}_{\mathfrak{g}}(X) \subset \mathfrak{g}$ which contains X and so is not contained in V. In other words, we have found a lower-dimensional smooth connected K-subgroup $H \subset G$ whose Lie algebra does not contain a specified proper K-subspace of $\mathfrak{g}$. Applying this procedure several times, we arrive at a finite set of smooth connected proper K-subgroups $H_1, \dots, H_n \subset G$ whose K-group structure is unclear but whose Lie algebras span G. Hence, the multiplication map

$$H_1 \times \cdots \times H_n \to G$$

is surjective on tangent spaces at the identity points, so it is smooth there. Thus, this map is dominant, so the unirationality of the lower-dimensional H_i's over K implies the unirationality of G over K. This settles the argument in characteristic 0.

Case 2: positive characteristic. Now assume $\mathrm{char}(K) = p > 0$, with G reductive if K is not perfect. We will again use the Lie algebra to dig out suitable lower-dimensional smooth connected K-subgroups of G for applying dimension induction. Exactly as above, we may always arrange (without an initial reductivity hypothesis for perfect K) that G is semisimple of adjoint type and that the problem is solved in all lower-dimensional case (with a reductivity hypothesis if K is not perfect).

The infinitude of K once again ensures that for any proper K-subspace V of $\mathfrak{g}$ there exists a non-central non-nilpotent $X \in \mathfrak{g} - V$. The Jordan decomposition $X_{\mathrm{s}} + X_{\mathrm{n}}$ of X in $\mathfrak{g}_{\overline{K}}$ may not be K-rational, but for a sufficiently large p-power q the Jordan decomposition $X_{\mathrm{s}}^{[q]} + X_{\mathrm{n}}^{[q]}$ of $X^{[q]}$ is K-rational. Note that the semisimple X_{s} is nonzero (since X is *non-nilpotent*), so $X_{\mathrm{s}}^{[q]} \neq 0$ by semisimplicity. Taking q large enough ensures that $X_{\mathrm{n}}^{[q]} = 0$, so $X^{[q]}$ is nonzero and semisimple. Consideration of the inclusion $\mathfrak{g} \hookrightarrow \mathfrak{gl}_N(K)$ arising from a K-subgroup inclusion $G \hookrightarrow \mathrm{GL}_N$ shows that $[X, X_{\mathrm{s}}^{[q]}] = 0$, so X lies in the Lie-theoretic centralizer $\mathfrak{z}_{\mathfrak{g}}(X^{[q]})$.

As in the proof of Grothendieck's theorem on geometrically maximal tori, the $\overline{K}$-span of the pairwise commuting semisimple elements $X^{[qp^i]}$ $(i \geq 0)$ has a $\overline{K}$-basis consisting of nonzero semisimple elements X_i satisfying $X_i^{[p]} = X_i$. Such X_i are necessarily K-rational (since $X_i = X_i^{[p^a]}$ for all $a \geq 0$). Each $\mathfrak{z}_{\mathfrak{g}}(X_i)$ contains X and so is not contained in the initial choice of proper K-subspace V of $\mathfrak{g}$. Applying this construction several times, we can find a finite set of nonzero (semisimple) elements $Y_1, \ldots, Y_m \in \mathfrak{g}$ such that $Y_i^{[p]} = Y_i$ for all i and the Lie-centralizers $\mathfrak{z}_{\mathfrak{g}}(Y_i)$ span $\mathfrak{g}$.

We shall prove that $\mathfrak{z}_{\mathfrak{g}}(Y_i) = \mathrm{Lie}(H_i)$ for smooth connected *reductive* K-subgroups H_i of G with *non-trivial* scheme-theoretic center Z_{H_i}. Since $Z_G = 1$ by design (as G has been arranged to be semisimple of adjoint type), it would follow that $H_i \neq G$, so $\dim H_i < \dim G$ for all i and hence we could conclude by dimension induction. To find such H_i's, rather generally if $X \in \mathfrak{g}$ is a nonzero (semisimple) element satisfying $X^{[p]} = X$ then we claim that $\mathfrak{z}_{\mathfrak{g}}(X) = \mathrm{Lie}(H)$ for a connected reductive K-subgroup H with $Z_H \neq 1$.

In the proof of Grothendieck's theorem on geometrically maximal tori we saw that any such X spans the tangent line to a K-subgroup μ that is the image of a K-subgroup inclusion $\mu_p \hookrightarrow G$. The schematic centralizer $Z_G(\mu)$ is *smooth*, and hence of smaller dimension than G since the schematic center Z_G is trivial whereas $Z_G(\mu)$ has schematic center that contains $\mu \neq 1$. Moreover, clearly $X \in \mathrm{Lie}(Z_G(\mu)) = \mathrm{Lie}(Z_G(\mu)^0)$. We may therefore define $H = Z_G(\mu)^0$ provided that the evident inclusion

$$\mathrm{Lie}(Z_G(\mu)) \subset \mathfrak{z}_{\mathfrak{g}}(X)$$

is an equality and $Z_G(\mu)^0$ is smooth.

Let $\mathfrak{m} = \mathrm{Lie}(\mu) \subset \mathfrak{g}$ and define the K-subgroup $\mathrm{Fix}(\mathfrak{m}) \subset \mathrm{GL}(\mathfrak{g})$ to be the subgroup of linear automorphisms of $\mathfrak{g}$ that restrict to the identity on $\mathfrak{m}$. Thus, we have a Cartesian square of K-groups

$$\begin{tikzcd} Z_G(\mu) \arrow[r] \arrow[d] & \mathrm{Fix}(\mathfrak{m}) \arrow[d] \\ G \arrow[r, "\mathrm{Ad}_G"'] & \mathrm{GL}(\mathfrak{g}) \end{tikzcd}$$

because we can verify the Cartesian property on R-valued points for any k-algebra R: this follows from the fact that the natural map

$$\mathrm{Hom}_{R\text{-gp}}(\mu_R, G_R) \to \mathrm{Hom}_{p\text{-Lie}}(\mathrm{Lie}(\mu)_R, \mathfrak{g}_R)$$

is bijective. (Here we use in an essential way that $\mu \simeq \mu_p$.) Passing to the Cartesian square of Lie algebras, we conclude that $\mathrm{Lie}(Z_G(\mu)) = \mathfrak{z}_{\mathfrak{g}}(\mathfrak{m})$ since $\mathrm{d}(\mathrm{Ad}_G)(e) = \mathrm{ad}_{\mathfrak{g}}$.

The above Cartesian square of K-groups implies that the schematic centralizer $Z_G(X)$ of $X \in \mathfrak{g}$ for the adjoint action of G on $\mathfrak{g}$ coincides with $Z_G(\mu)$, and in 13.19 of Borel's "Linear algebraic groups" he shows rather generally that $Z_G(X)^0$ is reductive for any nonzero semisimple $X \in \mathfrak{g}$ (over a field of any characteristic). Since our approach to the theory of linear algebraic groups avoids the $Z_G(X)$-construction, we now give a direct proof of what we need (and a bit more):

Proposition 3.3. *Let G be a smooth connected affine group over a field K of characteristic $p > 0$, and let $\mu \subset G$ be a connected K-subgroup scheme of multiplicative type (e.g., μ_p).*

(1) *There exists a maximal K-torus of G containing μ; equivalently, the maximal tori of the smooth connected subgroup $Z_G(\mu)^0$ are maximal in G.*
(2) *If G is reductive then the identity component $Z_G(\mu)^0$ is reductive.*

Proof. Without loss of generality K is algebraically closed. To prove (1) it suffices to find *some* torus S of G containing μ, as then any maximal torus of G containing S also centralizes μ (since tori are commutative). We shall prove (1) using induction on $\dim(G)$. The centralizer $H = Z_G(\mu)$ is smooth and $\mu \subset H^0$ is a nontrivial subgroup of multiplicative type, so H^0 is not unipotent. Hence, a maximal torus T of H^0 is not trivial, so $Z_{H^0}(T)$ is a smooth connected group.

If $Z_{H^0}(T) \neq H^0$ then by dimension induction some torus of $Z_{H^0}(T)$ contains μ, so (1) would be proved. Thus, we just need to consider the possibility that $Z_{H^0}(T) = H^0$, which is to say that H^0 has a central maximal torus, so (by conjugacy) H^0 has T as its unique maximal torus. In this situation we claim that $\mu \subset T$. The quotient H^0/T is a smooth connected affine group containing no nontrivial tori, so it must be unipotent. Hence, the composite map $\mu \to H^0 \to H^0/T$ has to be trivial since μ is of multiplicative type, so

$$\mu \subset \ker(H^0 \to H^0/T) = T.$$

Turning to the proof of (2), by (1) we may choose a maximal torus T of G containing μ. Assuming that the unipotent radical U of $Z_G(\mu)^0$ is nontrivial, we seek a contradiction. Since U is stable under T-conjugation, $\mathrm{Lie}(U)$ is a T-stable subspace of $\mathfrak{g}$. This subspace supports only nontrivial T-weights since $\mathfrak{g}^T = T$ by the reductivity of G. Hence, the nonzero $\mathrm{Lie}(U)$ is a direct sum of some of the root spaces $\mathfrak{g}_a$ for $a \in \Phi(G,T)$. Choose such an a and let $T_a = (\ker a)^0_{\mathrm{red}}$ be the codimension-1 subtorus killed by a.

The centralizer $H := Z_G(T_a)$ is a connected reductive subgroup of G with semisimple rank 1, and it meets U nontrivially since $\mathrm{Lie}(U) \cap \mathrm{Lie}(H) = \mathrm{Lie}(U)^{T_a} \supset \mathfrak{g}_a$. But $U \cap H$ is the centralizer for the T_a-action on U, so it inherits smoothness and connectedness from U. We conclude that $Z_H(\mu) = H \cap Z_G(\mu)$ contains the nontrivial $U \cap H$ in its unipotent radical. Thus, to reach a contradiction we may replace G with H to reduce to the case of semisimple rank 1.

We may assume that the subgroup μ is non-central in G (or else there is nothing to do), so μ has nontrivial image μ' in $G/Z_G = \mathrm{PGL}_2$. The nontrivial unipotent radical of $Z_G(\mu)^0$ has nontrivial image U' in PGL_2. But $Z_G(\mu)^0$ contains a maximal torus of G, so its image T' in PGL_2 is a maximal torus that must normalize U'. By dimension considerations, $B' := T' \ltimes U'$ is a Borel subgroup of PGL_2, and this forces $Z_G(\mu)^0$ to map onto B' (as it cannot map onto the reductive PGL_2, due to the normality of U' in its image). Thus, B' is the centralizer of μ' in PGL_2.

Applying a conjugation to PGL_2 brings $T' = \mathrm{GL}_1$ to the diagonal torus D and brings U' to the upper unipotent subgroup U^+. By inspection, the action of $D = \mathrm{GL}_1$ on $U^+ = \mathbf{G}_{\mathrm{a}}$ inside PGL_2 is given by ordinary scaling (possibly composed with inversion, depending on which identification $D = \mathrm{GL}_1$ is chosen), so a nontrivial subgroup scheme of D cannot centralize U^+. This is a contradiction, since $\mu' \neq 1$. ■