Algebraic Groups I. Grothendieck's theorem on tori (based on notes by S. Lichtenstein)

1. Introduction

In the early days of the theory of linear algebraic groups, the ground field was assumed to be algebraically closed (as in work of Chevalley). After experts acquired some experience, the needs of number theory and finite group theory ("finite simple groups of Lie type"!) led them to escape this hypothesis, and they were able to get the theory of connected reductive groups off the ground over a perfect field (using Galois-theoretic techniques to pull things down from the algebraically closed case). The needs of number theory over local and global function fields provided motivation to eliminate the perfectness assumption, but it was not at all clear how to do this. Then Grothendieck came along and in Theorem 1.1 of Exposé XIV of SGA3 he proved the decisive result which made it possible to make the theory of reductive groups work over an *arbitrary* field. The result was this:

Theorem 1.1 (Grothendieck)**.** *Let G be a smooth connected affine group over a field k. Then G contains a maximal k-torus T such that $T_{\overline{k}}$ is maximal in $G_{\overline{k}}$.*

Remark 1.2. The hardest case of the proof is when k is imperfect, and it was for this purpose that Grothendieck's scheme-theoretic ideas in SGA3 were essential, at first. (In Remark 1.5(d) of Exp. XIV, he gave an especially scheme-theoretic second proof for infinite k, invoking the "scheme of maximal tori" which he had constructed earlier and later proved to be rational over k in Theorem 6.1 of Exp. XIV, so he could invoke the elementary fact that rational varieties over infinite fields have rational points!) Borel found the SGA3 proof(s) to be "too technical" for such a concrete result over fields, and in his book he eliminates all the group schemes by using clever Lie-theoretic methods (which amount to working with certain infinitesimal group schemes in disguise, as we shall see). The proof we give is my scheme-theoretic interpretation of the argument in Borel's book [Borel, §18.2(i)]. It is very different from Grothendieck's proof.

In class we saw that Theorem 1.1 and torus-centralizer arguments (along with dimension induction) yield the following crucial improvement:

Corollary 1.3. *For any maximal k-torus $T \subset G$ and every field extension K/k, $T_K \subset G_K$ is maximal. In particular, taking $K = \overline{k}$, $\dim T$ is independent of the maximal k-torus T.*

The common dimension of the maximal k-tori is called the *reductive rank* of G because it coincides with the same invariant for the reductive quotient $G_{\overline{k}}/\mathscr{R}_u(G_{\overline{k}})$.

Remark 1.4. We have seen in class that if G is a smooth connected affine k-group such that $G_{\overline{k}}$ contains no nontrivial torus then $G_{\overline{k}}$ is unipotent (and so by definition G is unipotent). But Corollary 1.3 gives that $G_{\overline{k}}$ contains no nontrivial torus if and only if G contains no nontrivial k-torus, so we conclude that G is unipotent if and only if G contains no nontrivial k-torus (the implication "$\Leftarrow$" being trivial).

Beware that if $k \neq k_s$ then typically there are *many* $G(k)$-conjugacy classes of maximal k-tori, unlike the case of an algebraically closed field. For example, if $G = \mathrm{GL}_n$ then by HW5 Exercise 5(ii) the maximal k-tori in G are in bijective correspondence with maximal finite étale commutative k-subalgebras of $\mathrm{Mat}_n(k)$. In particular, two maximal k-tori are $G(k)$-conjugate if and only if the corresponding maximal finite étale commutative k-subalgebras of $\mathrm{Mat})_n(k)$ are $\mathrm{GL}_n(k)$-conjugate. Hence, if such k-subalgebras are not abstractly k-isomorphic then their corresponding maximal k-tori are not $G(k)$-conjugate. For example, non-isomorphic degree-n finite separable extension fields of k yield such algebras. Thus, when $k \neq k_s$ there are typically many $G(k)$-conjugacy classes of maximal k-tori in G.

We saw in class that $G_{\overline{k}}$ has no nontrivial tori if and only if $G_{\overline{k}}$ is unipotent, so it follows from Grothendieck's theorem that every smooth connected affine k-group is *either* unipotent or contains a nontrivial k-torus. If all k-tori in G are *central* then for a maximal k-torus T the quotient G/T is unipotent (as $(G/T)_{\overline{k}} = G_{\overline{k}}/T_{\overline{k}}$ contains no nontrivial torus). Hence, in such cases G is solvable. Thus, in the non-solvable case there are always k-tori S whose centralizer $Z_G(S)$ (which are always again smooth and connected, by HW8 Exercise 3 for smoothness and discussion in class for connectedness) has lower dimension than G. This enables us to "dig holes" in *non-solvable* smooth connected k-groups when trying to prove general theorems. Of course, the solvable case has its own bag of tricks (somewhat delicate over imperfect fields).

Definition 1.5. For a maximal k-torus T in a smooth connected affine k-group G, the associated *Cartan k-subgroup* $C \subset G$ is $C = Z_G(T)$, the scheme-theoretic centralizer.

By the torus-centralizer results from HW8 Exercise 3 and class discussion, Cartan k-subgroups are smooth and connected. Since T is central in its Cartan C, it follows that T is the *unique* maximal k-torus in C. (Indeed, if there were others then the k-subgroup they generate along with the central T would be a bigger k-torus.) We have $C_{\overline{k}} = Z_{G_{\overline{k}}}(T_{\overline{k}})$ since the formation of scheme-theoretic centralizers commutes with base change, and over $\overline{k}$ all maximal tori are conjugate. Hence, over $\overline{k}$ the Cartan subgroups are conjugate, so the dimension of a Cartan k-subgroup is both independent of the choice of Cartan k-subgroup and invariant under extension of the ground field. This number is called the *nilpotent rank* of G in SGA3, and the *rank* of G in Borel's book.

For example, if G is reductive then it turns out (as is shown in the handout "Unipotent radicals and reductivity") that $C = T$. That is, in a connected reductive group the Cartan subgroups are precisely the maximal tori.

Remark 1.6. It is a very difficult theorem that in any smooth connected affine group G over any field k, all maximal *k-split* tori are $G(k)$-conjugate. This is 20.9(ii) in Borel's textbook for reductive G, which we will treat in the sequel course. The general case was announced without proof by Borel and Tits, and is proved as Theorem C.2.3 in the book " Pseudo-reductive groups". The dimension of a maximal *split* k-torus is thus also an invariant, sometimes called the *k-rank* of G (and mainly of interest in the reductive case).

As a final comment before we embark on the proof of Theorem 1.1, note that since tori split over a finite separable extension, we have the following important consequence of Theorem 1.1.

Corollary 1.7. *For a smooth connected affine group G over a field k, there exists a finite Galois extension k'/k such that $G_{k'}$ has a split maximal k'-torus.*

2. Start of proof of theorem 1.1

We will primary focus on the case in which k is *infinite*, which ensures that $k^n \subset \mathbf{A}^n_k$ is Zariski-dense, and thus in particular $\mathfrak{g} = \mathrm{Lie}(G)$ is Zariski-dense in $\mathfrak{g}_{\overline{k}}$. The case of finite k requires a completely different argument, using "Lang's theorem", and is explained in Proposition 16.6 of Borel's book. (In general, §16 of Borel's book explains the elegant technique due to Lang which is often useful to overcome difficulties with lack of Zariski-density over finite fields. In SGA3 the case of finite k is likewise handled by using Lang's trick.)

We first treat the "easy" case in which $G_{\overline{k}}$ has a *central* maximal torus S. (This case will work over all k, even finite fields.) Since all maximal tori are $G(\overline{k})$ conjugate, a unique one is automatically normal in $G_{\overline{k}}$. By HW 6, Exercise 3(ii), a normal torus in a smooth connected $\overline{k}$-group is automatically central. (This is basically because the automorphism scheme of a split torus of rank n is the constant group $\mathrm{GL}_n(\mathbf{Z})$ that is étale, so the conjugation action of $G_{\overline{k}}$ on a normal torus is classified by a homomorphism to the étale automorphism scheme, which in turn must be trivial when G is connected. Note the similarity with how one proves the commutativity of the fundamental group of a connected Lie group.)

Thus, we are in the situation where there exists a *unique* maximal $\overline{k}$-torus $S \subset G_{\overline{k}}$. Our problem is to produce one defined over k. This is rather elementary over perfect fields via Galois descent, but here is a uniform method using group schemes that applies over all fields; this technique will be useful later on as well.

Let $Z = Z_G^0$, the identity component of the scheme-theoretic center of G. Since the formation of the center (and identity component) commutes with base change, we have $S \subset (Z_{\overline{k}})_{\mathrm{red}}$ as a maximal torus in the smooth commutative $\overline{k}$-group $(Z_{\overline{k}})_{\mathrm{red}}$. By the structure of smooth connected commutative $\overline{k}$-groups, it follows that $(Z_{\overline{k}})_{\mathrm{red}} = S \times U$ for a smooth connected unipotent $\overline{k}$-group U. For any n not divisible by $\mathrm{char}(k)$, consider the torsion subgroup $Z[n]$. This is a commutative, affine algebraic k-group, and since the derivative of $[n] : Z \to Z$ is $n : \mathrm{Lie}(Z) \to \mathrm{Lie}(Z)$, it follows that $\mathrm{Lie}(Z[n])$ is killed by $n \in k^\times$. Thus $\mathrm{Lie}(Z[n]) = 0$, so $Z[n]$ is finite étale over k.

This implies that

$$Z[n]_{\overline{k}} = Z_{\overline{k}}[n] \supset (Z_{\overline{k}})_{\mathrm{red}}[n] \supset Z_{\overline{k}}[n] = Z[n]_{\overline{k}},$$

so $Z[n]_{\overline{k}} = (Z_{\overline{k}})_{\mathrm{red}}[n]$. Since U is unipotent, $U[n] = 0$. Hence, $Z[n]_{\overline{k}} = S[n]$.

Set $H = (\overline{\bigcup_n Z[n]})^0 \subset G$, where the union is taken over n not divisible by $\mathrm{char}(k)$. This is a smooth connected closed k-subgroup of G.

Lemma 2.1. *The k-group H is a torus descending S.*

Proof. By Galois descent, the formation of H commutes with scalar extension to k_s, so we can assume $k = k_s$. Hence, the finite étale groups $Z[n]$ are constant, so H is the identity component of the Zariski closure of a set of k-points. It follows that the formation of H commutes with any further extension of the ground field, so

$$H_{\overline{k}} = (\overline{\bigcup_n Z_{\overline{k}}[n]})^0 = (\overline{\bigcup_n S[n]})^0 = S$$

where the final equality uses that in any k-torus, the collection of n-torsion subgroups for n not divisible by $\mathrm{char}(k)$ is dense (as we see by working over $\overline{k}$ and checking for GL_1 by hand). ∎

Now we turn to the hard case, when $G_{\overline{k}}$ does not have a central maximal torus. In particular, there must exist a non-central $S = \mathrm{GL}_1 \hookrightarrow G_{\overline{k}}$. We are going to handle these cases using induction on $\dim G$. (Note that the general case $\dim G = 1$ is trivial.)

Lemma 2.2. *It suffices to prove that G contains a nontrivial k-torus.*

Proof. Suppose there exists a nontrivial k-torus $M \subset G$. Consider $Z_G(M)$, which is a smooth connected k-subgroup of G. The maximal tori of $Z_G(M)_{\overline{k}} = Z_{G_{\overline{k}}}(M_{\overline{k}})$ must have the same dimension as those of $G_{\overline{k}}$, as can be seen by considering one containing $M_{\overline{k}}$. So if we can find a k-torus in $Z_G(M)$ that remains maximal as such after extension of the ground field to $\overline{k}$ then the $\overline{k}$-fiber of such a torus must also be maximal in $G_{\overline{k}}$ for dimension reasons. Thus it suffices to prove the theorem with G replaced by $Z_G(M)$.

Now consider $Z_G(M)/M$. Since M was assumed nontrivial, this has strictly smaller dimension (even if $Z_G(M) = G$, which might have happened). Hence, by dimension induction, there exists a k-torus $\overline{T} \subset Z_G(M)/M$ which is geometrically maximal. Let T be the scheme-theoretic preimage of $\overline{T}$ in $Z_G(M)$. Since M is smooth and connected, the quotient map $Z_G(M) \to Z_G(M)/M$ is smooth, so T is a smooth connected closed k-subgroup of G. It sits in a short exact sequence of k-groups

$$1 \to M \to T \to \overline{T} \to 1.$$

Since M and $\overline{T}$ are tori and T is smooth and connected, by the structure theory for solvable groups it follows that T is a torus.

Now we claim T is geometrically maximal in $Z_G(M)$. To prove this, first note that any maximal torus T' in $Z_G(M)_{\overline{k}}$ must contain the central $M_{\overline{k}}$ (since otherwise the subgroup $T'M_{\overline{k}}$ would be a bigger torus). Thus, maximality of T' in $Z_G(M)_{\overline{k}}$ is in fact equivalent to the maximality of the quotient $T'/M_{\overline{k}}$ in $(Z_G(M)/M)_{\overline{k}}$. In particular, $T_{\overline{k}}$ is maximal in $Z_G(M)_{\overline{k}}$, and thus in $G_{\overline{k}}$ as we already remarked. ■

So much for motivation: now we need to find such an M. The basic idea for infinite k is to use $\mathrm{Lie}(S) = \mathfrak{gl}_1 \subset \mathfrak{g}_{\overline{k}}$, a non-central Lie subalgebra, plus the Zariski-density of $\mathfrak{g}$ in $\mathfrak{g}_{\overline{k}}$ (infinite k!), to create a suitable nonzero $X \in \mathfrak{g}$ that is "semisimple" and such that $Z_G(X)^0 \subset G$ is a lower-dimensional smooth subgroup in which the maximal $\overline{k}$-tori are maximal in $G_{\overline{k}}$, so a geometrically maximal $\overline{k}$-torus in $Z_G(X)^0$ will do this job. (Below we will define what we mean by "semisimple" for elements of $\mathfrak{g}_{\overline{k}}$. This is a Lie-theoretic version of Jordan decomposition for linear algebraic groups.) The motivation is that whereas it is hard to construct tori over k, it is much easier to use Zariski-density arguments in $\mathfrak{g}_{\overline{k}}$ to create semisimple elements in $\mathfrak{g}$. Those will serve as a substitute for tori to carry out a centralizer trick and apply dimension induction.

There will be some extra complications in positive characteristic, and the case of finite fields needs a separate argument (as noted above).

3. The case of infinite k

Now we assume k is infinite, but otherwise arbitrary. To flesh out the preceding basic idea, consider the following hypothesis:

$(\star)$ there exists a non-central semisimple element $X \in \mathfrak{g}$.

To make sense of this, we now have to define what we mean by "non-central, semisimple" in $\mathfrak{g}$. The definition of "semisimple" will involve G. This is not surprising, since the trivial 1-dimensional Lie algebra k arises for both $\mathbf{G}_a$ and $\mathbf{G}_m$, and in the first case we want to declare all elements of the Lie algebra to be nilpotent (since unipotent subgroups of GL_N have all elements in their Lie algebra nilpotent inside $\mathfrak{gl}_N$, by the Lie-Kolchin theorem) and in the latter case we want to declare all elements of the Lie algebra to be semisimple! (Observe that the same issue is relevant in the study of ordinary connected Lie groups over $\mathbf{R}$ and $\mathbf{C}$: the case of commutative or solvable Lie groups is a source of confusion because the exponential map relates additive and multiplicative groups, and it is very far from an isomorphism in the complex-analytic case.)

We now briefly digress for an interlude on Lie algebras of smooth linear algebraic groups over general fields k. The *center* of a Lie algebra $\mathfrak{g}$ is the kernel of the adjoint action

$$\mathrm{ad} : \mathfrak{g} \to \mathrm{End}(\mathfrak{g}), X \mapsto [X, -].$$

In Borel's book (see §4.1–§4.4), a general "Jordan decomposition" is constructed as follows in $\mathfrak{g}_{\overline{k}}$. Choose a closed k-subgroup inclusion $G \hookrightarrow \mathrm{GL}_N$, and consider the resulting inclusion of Lie algebras $\mathfrak{g} \hookrightarrow \mathfrak{gl}_N$ over k. For any $X \in \mathfrak{g}_{\overline{k}}$ we have an additive Jordan decomposition $X = X_s + X_n$ in $\mathfrak{gl}_N(\overline{k}) = \mathrm{Mat}_N(\overline{k})$. In particular, $[X_s, X_n] = 0$. Borel proves that $X_s, X_n \in \mathfrak{g}_{\overline{k}}$ and that that are independent of the initial choice of $G \hookrightarrow \mathrm{GL}_N$; the arguments are similar to what we did long ago to make the Jordan decomposition in $G(\overline{k})$. Borel also shows that this decomposition is functorial, so in particular $\mathrm{ad}(X_s) = \mathrm{ad}(X)_s$ and $\mathrm{ad}(X_n) = \mathrm{ad}(X)_n$.

Definition 3.1. An element $X \in \mathfrak{g}$ is *semisimple* (resp. *nilpotent*) when $X = X_s$ (resp.$X = X_n$).

Remark 3.2. Note that we are *not* claiming that $\mathrm{ad}(X)$ alone detects the semisimplicity or nilpotence, nor that the definition is being made intrinsically to $\mathfrak{g}$. The definitions of semisimplicity and nilpotence rest upon k-group inclusions $G \hookrightarrow \mathrm{GL}_N$ (and more specifically, involve the k-group G). Moreover, by definition, these concepts are preserved under passage to $\mathfrak{g}_{\overline{k}}$ (and as with algebraic groups, the Jordan components of $X \in \mathfrak{g}$ are generally only rational over the perfect closure of k).

If $p = \mathrm{char}(k) > 0$, then upon choosing a faithful representaiton $G \hookrightarrow \mathrm{GL}_N$, the resulting inclusion $\mathfrak{g} \hookrightarrow \mathfrak{gl}_N$ makes the p-power map on $\mathfrak{gl}_N$ induces the structure of a *p-Lie algebra* on $\mathfrak{g}$. This is a certain kind of a Frobenius semi-linear map $X \mapsto X^{[p]} : \mathfrak{g} \to \mathfrak{g}$ that is functorial in G (independent of the chosen faithful linear representation) and has the intrinsic description of being the map $D \mapsto D^p$ from the space of left-invariant derivations to itself. One can compute using $\mathfrak{gl}_N$ that $\mathrm{ad}(X^{[p]}) = \mathrm{ad}(X)^{[p]}$ (as is one of the axioms for p-Lie algebras). For further details on p-Lie algebras, see §3.1 in Borel's book and Appendix A.7 (especially Lemma A.7.13) in "Pseudo-reductive groups".

Remark 3.3. In characteristic $p > 0$, if $X \in \mathfrak{g}$ is nilpotent, then $X^{[p^r]} = 0$ for $r \gg 0$. This is very important below, and follows from a computation in the special case of $\mathfrak{gl}_N$.

Returning to our original problem over infinite k, let us verify hypothesis ($\star$) in characteristic zero. The non-central $S = \mathrm{GL}_1 \hookrightarrow G_{\overline{k}}$ gives an action of S on $\mathfrak{g}_{\overline{k}}$ (via the adjoint action of $G_{\overline{k}}$ on $\mathfrak{g}_{\overline{k}}$), and this decomposes as a direct sum of weight spaces

$$\mathfrak{g}_{\overline{k}} = \bigoplus \mathfrak{g}_{\chi_i}.$$

The S-action is described by the weights n_i, where $\chi_i(t) = t^{n_i}$.

Lemma 3.4. *There is at least one nontrivial weight.*

Proof. The centralizer $Z_G(S)$ is a smooth (connected) subgroup of $G_{\overline{k}}$, and by functorial consideration with the dual numbers we see that $\mathrm{Lie}(Z_{G_{\overline{k}}}(S)) = \mathfrak{g}_{\overline{k}}^S$ is the subspace of S-invariants in $\mathfrak{g}_{\overline{k}}$. Thus, if S acts trivially then $Z_{G_{\overline{k}}}(S)$ has Lie algebra with full dimension, forcing $Z_{G_{\overline{k}}}(S) = G_{\overline{k}}$ by smoothness, connectedness, and dimension reasons. This says that S is central in $G_{\overline{k}}$, which is contrary to our hypotheses on S. ■

If we choose a $\overline{k}$-basis Y for $\mathrm{Lie}(S)$ then $Y \in \mathfrak{g}_{\overline{k}}$ is semisimple since any $G_{\overline{k}} \hookrightarrow \mathrm{GL}_N$ carries S into a torus and hence $\mathrm{Lie}(S)$ into a semisimple subalgebra of $\mathfrak{gl}_N$. By Lemma 3.4, some weight is nonzero. Thus, in characteristic zero (or more generally if $\mathrm{char}(k) \nmid n_i$ for some i) we know moreover that $\mathrm{ad}(Y)$ is nonzero. Hence, Y is semisimple and in characteristic 0 is *non-central.*

We have not yet verified ($\star$), since $Y \in \mathfrak{g}_{\overline{k}}$, and we seek a non-central semisimple element of $\mathfrak{g}$. To fix this, consider the characteristic polynomial $f(X,t)$ of $\mathrm{ad}(X)$ for generic $X \in \mathfrak{g}$, as a polynomial in $k[\mathfrak{g}^*][t]$. Viewed in $\overline{k}[\mathfrak{g}^*][t] = \overline{k}[\mathfrak{g}^*_{\overline{k}}][t]$, the existence of the noncentral, semisimple element as established above shows that $f(X,t) \neq t^{\dim \mathfrak{g}}$. In other words, there are lower-order (in t) coefficients in $k[\mathfrak{g}^*]$ which are nonzero as functions on $\mathfrak{g}_{\overline{k}}$. Since $\mathfrak{g} \subset \mathfrak{g}_{\overline{k}}$ is Zariski-dense (as k is infinite) it follows that there exists $X \in \mathfrak{g}$ such that $f(X,t) \in k[t]$ is not equal to $t^{\dim \mathfrak{g}}$. In particular, $\mathrm{ad}(X)$ is not nilpotent, so $\mathrm{ad}(X)_s$ is nonzero. Since $\mathrm{ad}(X_s) = \mathrm{ad}(X)_s \neq 0$, X_s is noncentral and semisimple in $\mathfrak{g}_{\overline{k}}$. When k is perfect, such as a field of characteristic 0, the Jordan decomposition is rational over the ground field, so then X_s satisfies the requirements in ($\star$).

4. Hypothesis ($\star$) for G implies the existence of a nontrivial k-torus

Now we assume there exists $X \in \mathfrak{g}$ that is noncentral and semisimple. We will show (for infinite k) that there exists a smooth k-subgroup $G' \subset G$ *which is a proper subgroup* (and hence $\dim G' < \dim G$) such that $\mathfrak{g}' = \mathrm{Lie}(G')$ contains a nonzero semisimple element of $\mathfrak{g}$. This implies that $G'_{\overline{k}}$ is not unipotent (for if it were, its Lie algebra would be nilpotent). By dimension induction, G' contains a geometrically maximal k-torus. Since $G'_{\overline{k}}$ is not unipotent, this means G' (and hence G!) contains a *nontrivial* k-torus, which is all we need to prove (Lemma 2.2).

In characteristic zero, it's very easy to finish the proof, as follows. Consider the scheme theoretic centralizer $Z_G(X)$ of X (for the action $\mathrm{Ad} : G \to \mathrm{GL}(\mathfrak{g})$). By Cartier's theorem, Z is smooth. We must have $Z_G(X) \neq G$ (in any characteristic) for the following reason. If $Z_G(X) = G$ then X is fixed by $\mathrm{Ad}(G)$, so by differentiating we get $\mathrm{ad}(X) = 0$ on $\mathfrak{g}$. But X was non-central, so this is a contradiction. Thus $Z_G(X)$ is a smooth subgroup of G distinct from G, and its Lie algebra contains the nonzero semisimple X. This does the job as required above, so we are done in characteristic 0.

Remark 4.1. Borel's book shows in §9.1 that $Z_G(X)$ is smooth in any characteristic, but the problem is that hypothesis ($\star$) may not hold in positive characteristic. We will avoid this approach because we have not developed any general theory for semisimple elements of $\mathfrak{g}$. The reader who is happy with Borel's proof of the smoothness of $Z_G(X)$ should skip ahead to §5.

For the remainder of the proof, we will assume $\mathrm{char}(k) = p > 0$. Now we will make essential use of p-Lie algebras, and especially an interesting construction from SGA3, Exposé $\mathrm{VII_A}$, 7.2, 7.4 (also formulated in "Pseudo-reductive groups", Proposition A.7.14): p-Lie subalgebras $\mathfrak{h} \subset \mathfrak{g}$ are in functorial bijection with infinitesimal k-subgroup schemes $H \subset G$ of height 1 (meaning $a^p = 0$ for all $a \in \mathfrak{m}_H$) via $H \mapsto \mathrm{Lie}(H)$, and moreover $\mathfrak{h}$ is commutative if and only if H is. (The idea behind the proof of this is to emulate the classical Lie-theoretic version, by defining H to be "$\exp(\mathfrak{h})$" and using the p-Lie subalgebra property to prove that this makes sense, i.e. the power series stops before division by zero becomes an issue.) The more precise statement proved in SGA3 is this:

Theorem 4.2 (SGA3, Exposé $\mathrm{VII_A}$, 7.2, 7.4)**.** *Let B be a commutative $\mathbf{F}_p$-algebra. The functor $H \rightsquigarrow \mathrm{Lie}_p(H)$ is an equivalence between the category of finite locally free B-group schemes whose augmentation ideal is killed by the p-power map and the category of finite locally free p-Lie algebras over B.*

In particular, if k is a field of characteristic $p > 0$ and G is a k-group scheme of finite type, then the p-Lie algebra functor defines a bijection

$$\mathrm{Hom}_k(H, G) = \mathrm{Hom}_k(H, \ker F_{G/k}) \simeq \mathrm{Hom}(\mathrm{Lie}_p(H), \mathrm{Lie}_p(\ker F_{G/k})) = \mathrm{Hom}(\mathrm{Lie}_p(H), \mathrm{Lie}_p(G)).$$

In this result, $F_{G/k} : G \to G^{(p)}$ denotes the relative Frobenius morphism, discussed in §A.3 (especially up through A.3.4) in "Pseudo-reductive groups". (For GL_n it is the p-power map on matrix entries, and in general it is functorial in G.) Also, note that by (an easy instance of) Nakayama's Lemma, a map $H \to G$ is a closed immersion if and only if the p-Lie algebra map is injective. This will be used implicitly without comment. Finally, we note that in §A.7 of "Pseudo-reductive groups", the basic aspects of Lie algebras and p-Lie algebras of general group schemes over rings are developed from scratch.

Remark 4.3. In the special case of commutative k-groups whose augmentation ideal is killed by the p-power map, the equivalence with finite-dimensional commutative p-Lie algebras over k is nicely explained in the unique Theorem in §14 in Mumford's "Abelian Varieties", via a method which works over any field (even though he always assumes his ground field is algebraically closed). But beware that the commutative case is really not enough, since we need the final bijection among

Hom's in the preceding theorem, and that rests on using the k-group scheme $\ker F_{G/k}$ which is generally very non-commutative.

Let $\mathfrak{h} = \mathrm{Span}_k(X^{[p^i]})$. This is manifestly closed under the map $v \mapsto v^{[p]}$. Moreover (as can be seen by using an embedding $\mathfrak{g} \hookrightarrow \mathfrak{gl}_n$ arising from a k-group inclusion of G into GL_n), the $X^{[p^i]}$ all commute with one another. Thus $\mathfrak{h}$ is a commutative p-Lie subalgebra of $\mathfrak{g}$. A linear combination of commuting semisimple operators is semisimple. Moreover the pth power of a nonzero semisimple operator is nonzero. So $v \mapsto v^{[p]}$ has no kernel on $\mathfrak{h}$. It is a general fact in Frobenius-semilinear algebra (see §1 in Exposé XXII of SGA7 for a nice discussion, especially (1.0.9) and Proposition 1.1 there, or alternatively the Corollary at the end of §14 of Mumford's book "Abelian Varieties" over algebraically closed fields, which is enough for our needs) that if V is a finite-dimensional vector space over a perfect field F of characteristic p and if $\phi : V \to V$ is a Frobenius-semilinear endomorphism then there is a unique decomposition $V = V_{\mathrm{ss}} \oplus V_{\mathrm{n}}$ such that ϕ is nilpotent on V_{n} and $(V_{\mathrm{ss}})_{\overline{F}}$ admits a basis of "ϕ-fixed vectors" ($\phi(v) = v$).

Now set $Z = Z_G(\mathfrak{h})$.

Lemma 4.4. *The k-subgroup scheme Z in G is smooth.*

Proof. Without loss of generality, we can take $k = \overline{k}$, as smoothness can be detected over $\overline{k}$ and the formation of scheme theoretic centralizers commutes with base change. Now using Theorem 4.2, set $H = \exp(\mathfrak{h}) \subset G$ to be the infinitesimal k-subgroup scheme whose Lie algebra is $\mathfrak{h} \subseteq \mathfrak{g}$.

As observed above, $\mathfrak{h}$ splits as a direct sum of $(\cdot)^{[p]}$-eigenlines,

$$\mathfrak{h} = \bigoplus kX_i, \qquad X_i^{[p]} = X_i.$$

Thus, H is a power of the order-p infinitesimal commutative k-subgroup corresponding to the p-Lie algebra kX with $X^{[p]} = X$. But there are only *two* 1-dimensional p-Lie algebras over k: the one with $X^{[p]} = 0$ and the one with $X^{[p]} = X$ for some k-basis X. (Indeed, if $X^{[p]} = cX$ for some $c \in k^\times$ then by replacing X with $Y = aX$ where $a^{p-1} = c$ we get $Y^{[p]} = Y$; semi-linear algebra can be even better than linear algebra!) Hence, there are exactly two commutative infinitesimal order-p groups over an algebraically closed field, so the non-isomorphic μ_p and α_p must be these two possibilities.

Which is which? To figure it out, consider the embeddings $\alpha_p \hookrightarrow \mathbf{G}_a$ and $\mu_p \hookrightarrow \mathbf{G}_m$ which induces isomorphisms on p-Lie algebras. Nonzero invariant derivations on $\mathbf{G}_a$ resp. $\mathbf{G}_m$ are given by ∂_t and $t\partial_t$. Taking p-th powers (which is the derivation-version of the $(\cdot)^{[p]}$-map), we have $\partial_t^p = 0$ and $(t\partial_t)^p = t\partial_t$. Thus, the condition $X^{[p]} = X$ forces us to be in the μ_p-case. That is, $H = \mu_p^N$ for some N.

By Lemma A.8.8 in "Pseudo-reductive groups" (taking $\Lambda = \mathbf{Z}/m\mathbf{Z}$ there), μ_m has completely reducible representation theory over any field, just like a torus. Applying this with μ_p over k, we can emulate the proof of smoothness of torus centralizers from the homework (or see [*loc. cit.*, Proposition A.8.10(2)]) to show via the infinitesimal criterion that $Z_G(H)$ is smooth. (Note that the scheme-theoretic centralizer $Z_G(H)$ makes sense since G is smooth, even though H is not.) To conclude the proof, it will suffice to show that the evident inclusion $Z_G(H) \subseteq Z_G(\mathfrak{h})$ as k-subgroup schemes of G is an equality.

Theorem 4.2 provides more: if R is any k-algebra, then the p-Lie functor defines a bijective correspondence between R-group maps $H_R \to G_R$ and p-Lie algebra maps $\mathfrak{h}_R \to \mathfrak{g}_R$. Hence, by Yoneda's lemma, $Z_G(H) = Z_G(\mathfrak{h})$ because to check this equality of k-subgroup schemes of G it suffices to compare R-points for arbitrary k-algebras R. ■

As in the characteristic zero case, since $\mathfrak{h}$ contains noncentral elements of $\mathfrak{g}$, it follows that $Z_G(\mathfrak{h}) \neq G$. And as we saw above, this guarantees the existence of a nontrivial k-torus in G, by dimension induction (applied to the identity component $Z_G(\mathfrak{h})^0$).

We have completed the proof of Theorem 1.1 in characteristic zero, since $(\star)$ always holds in characteristic 0, and more generally we have completed it over any k whatsoever (even finite k!) for G that satisfy $(\star)$ when the conclusion of Theorem 1.1 is known over k in all lower dimensions (as we may always assume, since we argue by induction on $\dim G$).

5. The case $\mathrm{char}(k) = p > 0$ and $(\star)$ fails

Now the idea is to find a central infinitesimal k-subgroup $M \subset G$ such that G/M satisfies $(\star)$. We will then lift the result from G/M back to G when such an M exists, and if no such M exists then we will use a different method to produce a nontrivial k-torus in G.

Lemma 5.1. *Regardless of whether* $(\star)$ *holds* (*but still assuming, as we have been, that* $G_{\overline{k}}$ *has a noncentral* GL_1)*, there exists a nonzero semisimple element* $X \in \mathfrak{g}$*.*

Proof. Arguing as at the end of §3, and *using the infinitude of the field* k (finally!), there exists $X_0 \in \mathfrak{g}$ such that $\mathrm{ad}(X_0)$ is not nilpotent. Consider the additive Jordan decomposition $X_0 = X_0^{\mathrm{ss}} + X_0^{\mathrm{n}}$ in $\mathfrak{g}_{\overline{k}}$ as a sum of commuting semisimple and nilpotent elements. For $r \gg 0$ we see that $X := X_0^{[p^r]} = (X_0^{\mathrm{ss}})^{[p^r]}$ is nonzero and semisimple, and also (as the p^rth power of X_0 also in $\mathfrak{g}$) lies in $\mathfrak{g}$. ■

Obviously if $(\star)$ fails for G then every semisimple element of $\mathfrak{g}$ is central. Assume this is the case. Set

$$\mathfrak{m} = \mathrm{Span}_k(\text{all semisimple } X \in \mathfrak{g}) \subset \mathfrak{g};$$

this is nonzero due to Lemma 5.1. Since all the semisimple elements are central, this is a commutative Lie subalgebra of $\mathfrak{g}$. Since the pth power of a semisimple element of $\mathrm{Mat}_N(\overline{k})$ is semisimple, $\mathfrak{m}$ is $(\cdot)^{[p]}$-stable. So $\mathfrak{m}$ is a p-Lie subalgebra, and hence we can exponentiate it to $M \subset G$. As a linear combination of commuting semisimple elements in $\mathrm{Mat}_N(\overline{k})$ is semisimple, $\mathfrak{m}$ consists only of semisimple elements; this implies that $(\cdot)^{[p]}$ has vanishing kernel on $\mathfrak{m}_{\overline{k}}$. Thus, as we saw earlier, it follows that $M_{\overline{k}} = \mu_p^N$ for some $N > 0$.

Lemma 5.2. *The* k*-subgroup scheme* M *in* G *is central.*

Proof. Let $V \subset \mathfrak{g}_{k_s}$ be the k_s-span of all semisimple central elements of $\mathfrak{g}_{k_s}$. Manifestly we have $\mathfrak{m}_{k_s} \subset V$. Let $\Gamma = \mathrm{Gal}(k_s/k)$. Since V is Γ-stable, by Galois descent we have $V = (V^\Gamma)_{k_s}$. Since $V^\Gamma \subset \mathfrak{m}$, obviously, this gives $V = \mathfrak{m}_{k_s}$. By inspection, it's clear that V is stable under the action of $G(k_s)$, which is Zariski-dense in G_{k_s}. So G_{k_s} preserves $V = \mathfrak{m}_{k_s} \subset \mathfrak{g}_{k_s}$ under the adjoint action. Hence, G preserves $\mathfrak{m}$, so $M = \exp(\mathfrak{m})$ is normal in G. (Here we are again using that the exponential procedure has good functorial meaning over k-algebras, as was noted earlier.)

We now need to use Cartier duality $H \rightsquigarrow \mathbf{D}(H)$ for finite locally free commutative group schemes. This is nicely explained in §14 of Mumford's book "Abelian Varieties" (he works over an algebraically closed field, but his method applies over any ring at all, say working Zariski-locally so that a finite locally free coordinate ring becomes a free module). This duality operation is contravariant and self-inverse, and μ_p is dual to $\mathbf{Z}/p\mathbf{Z}$, so

$$\underline{\mathrm{Aut}}(M_{\overline{k}}) \simeq \underline{\mathrm{Aut}}(\mathbf{D}(M_{\overline{k}}))^{\mathrm{opp}} = \underline{\mathrm{Aut}}((\mathbf{Z}/p\mathbf{Z})^N)^{\mathrm{opp}},$$

which is the constant group $\mathrm{GL}_N(\mathbf{Z}/p\mathbf{Z})^{\mathrm{opp}}$, so it is étale. Hence, the conjugation action map $G_{\overline{k}} \to \underline{\mathrm{Aut}}(M_{\overline{k}})$ from a connected group to an étale group must be trivial. Consequently $M_{\overline{k}}$ is central in $G_{\overline{k}}$, so M is too. (This is the same argument which proves that normal tori in connected group schemes are central.) ■

Now consider the central purely inseparable k-isogeny $\pi : G \to G' := G/M$. Note that G' is smooth and connected of the same dimension as G, and even contains a non-central torus $\pi_{\overline{k}}(S)$ over $\overline{k}$ (as π is bijective on $\overline{k}$-points). Does G' satisfy $(\star)$? If it does not, then we can run through the same procedure all over again to get a nontrivial central $M' \subset G'$ such $M'_{\overline{k}} \simeq \mu_p^{N'}$, and can then consider the composite purely inseparable k-isogeny

$$G \to G/M = G' \to G'/M'.$$

This is not so bad: it turns out that the kernel E of this composite map is *also* a central k-subgroup, and it satisfies $E_{\overline{k}} \simeq \prod \mu_{p^{n_i}}$ for various n_i. To prove this, it is convenient to introduce the following terminology:

Definition 5.3. An infinitesimal k-group M is *multiplicative* if $M_{\overline{k}} \simeq \prod \mu_{p^{n_i}}$ for some integers $n_i \geq 1$.

Under the Cartier duality operation on finite commutative k-group schemes (whose formation commutes with direct products and extension of the ground field), μ_{p^n} is Cartier dual to $\mathbf{Z}/p^n\mathbf{Z}$. Hence, over k we can say that the multiplicative infinitesimal k-groups are Cartier dual to the finite étale k-groups of p-power order. The multiplicative infinitesimal k-groups exhibit many properties of tori (and in fact they are precisely the infinitesimal k-subgroup schemes of k-tori, but we do not use this). What we need is:

Lemma 5.4. *The automorphism scheme of an infinitesimal multiplicative k-group is étale, and if*

$$1 \to M' \to E \to M \to 1$$

is a short exact sequence of finite k-group schemes with M and M' multiplicative infinitesimal k-groups then so is E; in particular, E is commutative.

For finite k-schemes X, the automorphism functor $R \rightsquigarrow \mathrm{Aut}_R(X_R)$ on k-algebras is easily seen to be representable by an affine finite type group schemes, since the coordinate ring is a finite-dimensional k-algebra (with algebra structure governed by "structure constants"). The same goes for the automorphism functor of a finite k-group scheme. So no deep theorems on automorphism functors are required here.

Proof. We may assume $k = \overline{k}$. Then a multiplicative k-group M is Cartier dual to the constant group associated to a finite abelian p-group C. Since Cartier duality works over any base scheme (and is contravariant), it follows that the automorphism functor of M is the "opposite group" to the automorphism functor of C. But for a finite constant group, the automorphism functor is the finite constant group associated to the ordinary automorphism group. This proves that M has étale automorphism functor.

Now consider the given short exact sequence. The infinitesimal nature of M and M' implies that $E(k) = 1$ too, so E is infinitesimal (hence connected). The normality of M' in E implies that the conjugation action of E on M' is classified by a k-group homomorphism from the connected E to the étale automorphism group scheme of M'. This classifying map must be trivial, so M' is *central* in E. Since $M = E/M'$ is commutative, Hence, the functorial commutator $E \times E \to E$ therefore factors through a k-scheme morphism

$$[\cdot, \cdot] : M \times M = (E/M') \times (E/M') \to M'$$

which is seen to be bi-additive by thinking about $M = E/M'$ in terms of *fppf* quotient sheaves. In other words, this bi-additive pairing corresponds (in two ways!) to a k-group homomorphism

$$M \to \underline{\mathrm{Hom}}(M, M'),$$

where the target is the affine finite type k-scheme classifying group scheme homomorphisms (over k-algebras). By the exact same Cartier duality argument used in the analysis of automorphism schemes of multiplicative infinitesimal k-groups, it follows that this Hom-scheme is *also* étale, so the map to it from M must be *trivial*. This shows that E has trivial commutator, so E is commutative.

With commutativity of E established, it makes sense to apply Cartier duality to our original short exact sequence. This duality operation is contravariant and preserves exact sequences (since it is order-preserving and carries right-exact sequences to left-exact sequences), so we get an exact sequence

$$1 \to \mathbf{D}(M) \to \mathbf{D}(E) \to \mathbf{D}(M') \to 1.$$

The outer terms are finite constant groups of p-power order, so the middle one must be too. Hence, E is also multiplicative, as desired. ■

Returning to our setup of interest, under a composite isogeny

$$G \to G/M = G' \to G'/M',$$

the kernel E fits into a short exact sequence

$$1 \to M \to E \to M' \to 1$$

of k-group schemes. Hence, E must be infinitesimal and multiplicative. But it is normal in G and has étale automorphism scheme, so by the usual argument with connectedness of G it follows that E must be *central* in G. In other words, this composite isogeny is again a quotient by a central multiplicative infinitesimal k-group.

Now we're in position to wrap things up in positive characteristic (when k is infinite, arguing by induction on $\dim G$). First, we handle the case when the above process keeps going on *forever*. This provides a *strictly increasing* sequence $M_1 \subset M_2 \subset \dots$ of central multiplicative infinitesimal k-subgroups of G. This is all happening inside of the k-subgroup scheme Z_G, so it forces Z_G to not be finite (as otherwise there would be an upper bound on the k-dimensions of the coordinate rings of the M_j's). Since $(Z_G)^0_{\overline{k}}/((Z_G)^0_{\overline{k}})_{\mathrm{red}}$ is a finite infinitesimal group scheme, for large enough j the map to this from $(M_j)_{\overline{k}}$ must have non-trivial kernel. In other words, the smooth connected commutative group $((Z_G)^0_{\overline{k}})_{\mathrm{red}}$ contains a non-trivial infinitesimal subgroup that is multiplicative. This group therefore cannot be unipotent (since we know from HW5 Exercise 1 that a smooth unipotent group cannot contain μ_p), so it must contain a non-trivial torus! We conclude by the same argument with $Z_G[n]$'s as before (using n not divisible by $\mathrm{char}(k) = p$) that Z_G contains a non-trivial k-torus, so we win.

There remains the more interesting case when the preceding process does eventually stop, so we wind up with a central quotient map

$$G \to G/M$$

by a multiplicative infinitesimal k-subgroup M such that G/M satisfies $(\star)$; beware that now $M_{\overline{k}}$ is merely a product of several $\mu_{p^{n_i}}$'s, not necessarily a power of μ_p. We therefore get a nontrivial k-torus T in G/M, so if $E \subset G$ denotes its scheme-theoretic preimage then there is a short exact sequence of k-group schemes

$$1 \to M \to E \to T \to 1$$

with M central in E. We will be done (for infinite k) if any such E contains a nontrivial k-torus. This is the content of the following lemma.

Lemma 5.5. *For any field k of characteristic $p > 0$ and short exact sequence of k-groups*

$$1 \to M \to E \to T \to 1$$

with a central multiplicative infinitesimal k-subgroup M in E and a nontrivial k-torus T, there is a nontrivial k-torus in E.

Proof. Certainly $E_{\overline{k}}$ is connected, since T and M are connected. The commutator map on E factors through a bi-additive pairing $T \times T \to M$ which is trivial since T is smooth and M is infinitesimal. Hence, E is commutative. The map $E_{\overline{k}} \to T_{\overline{k}}$ is bijective on $\overline{k}$-points, so $(E_{\overline{k}})_{\mathrm{red}}$ is a smooth connected commutative $\overline{k}$-group. It is therefore a direct product of a torus and a smooth connected unipotent group, and the unipotent part must be trivial (since $T_{\overline{k}}$ is a torus). Hence, $(E_{\overline{k}})_{\mathrm{red}}$ is a torus. Now we can play the usual game: since E is commutative, the identity component of the Zariski-closure of the k-subgroup schemes $E[n]$ for n not divisible by p is a k-torus in E which maps onto $(E_{\overline{k}})_{\mathrm{red}}$ and hence is nontrivial. ■