

Linear Algebraic Groups I (Stanford, Winter 2010)

notes typed by Sam Lichtenstein, lectures and editing by Brian Conrad

February 8, 2020

Please send any errata (typos, math errors, etc.) to conrad@math.stanford.edu.

The sequel course “Linear Algebraic Groups II” treats the Borel-Tits structure theory of reductive groups over general fields (assuming knowledge of schemes, as in this course).

Contents

1	January 4	4
1.1	Some Definitions	4
1.2	Smoothness	5
1.3	Connectedness	5
1.4	Examples	6
2	January 6	7
2.1	Translations	7
2.2	Homomorphisms	7
2.3	Normal subgroups	8
2.4	Further discussion of examples	8
2.5	How far is a general smooth connected algebraic group from being either affine (i.e. linear algebraic) or projective (i.e. an abelian variety)?	9
3	January 8	10
3.1	How do linear algebraic groups arise in nature?	10
3.2	Zariski closures of subgroups	10
4	January 11 (Substitute lecture by A. Venkatesh)	12
4.1	Tori	12
4.2	Maximal split tori	12
4.3	Building up groups from tori	13
4.3.1	Construction of Φ	14
5	January 13	14
5.1	Mapping \mathbf{G}_a and \mathbf{G}_m into a reductive group	14
5.2	Classification of 1-dimensional connected linear algebraic groups	15
5.3	Examples of non-split 1-dimensional linear algebraic k-groups	15
5.4	Start of proof of the classification theorem	16
6	January 20 (Substitute lecture by A. Venkatesh)	16
6.1	End of proof of classification of 1-dimensional connected linear algebraic groups	16
6.2	Smoothness criteria	17

7	January 22	18
7.1	More on forms	18
7.2	A loose end concerning smoothness	19
7.3	How to apply Grothendieck's smoothness criterion	20
7.4	How to show algebraic k -groups are smooth	20
7.4.1	Smoothness of GL_n, SL_n in coordinates, via matrices	20
7.4.2	Smoothness of $GL(V), SL(V)$ without using coordinates (much)	21
8	January 25	21
8.1	How to Show Connectedness	21
8.2	Connectedness of SL_n	22
8.2.1	Method 1 - Flag varieties	22
8.2.2	Method 2 - Projective Space	22
8.3	Smoothness of Sp_{2n}	22
9	January 29	25
9.1	A little more about Sp_{2n}	25
9.2	Actions, Centralizers and Normalizers	26
9.3	Closed orbit lemma	26
9.4	Start of proof of closed orbit lemma (Theorem 9.3.5)	27
10	February 1	28
10.1	Conclusion of proof of closed orbit lemma (Theorem 9.3.5)	28
10.2	Criterion for a k -homomorphism of k -groups to be a closed immersion	29
11	February 3	29
11.1	Proof of Proposition 10.2.1	29
11.2	Embedding linear algebraic groups in GL_n	31
12	February 5	31
12.1	Actions of affine finite type k -groups on coordinate rings of affine k -schemes	31
12.1.1	Application to embedding a smooth linear algebraic group into GL_n	31
12.2	Proof of Theorem 12.1.1	32
13	February 8	33
13.1	Jordan decomposition	33
14	February 10	35
14.1	All subgroups of a smooth finite type k -group are stabilizers of a line	35
15	February 12	36
15.1	Unipotent groups	36
15.2	Proof of Theorem 15.1.8 on representations of unipotent groups	37
15.3	Remaining ingredients necessary for structure theory	38
16	February 17	38
16.1	Some motivation: a key calculation on $SL_2(k)$	38
16.2	Subgroups generated by connected varieties	39
16.3	Proof of Proposition 16.2.1	40
16.4	Improvements on Proposition 16.2.1	41
17	February 19	41
17.1	Conclusion of proof of Proposition 16.4.2	41
17.2	Solvable groups	42
17.3	Structure of smooth connected commutative affine k -groups	42
17.4	Coset spaces for closed subgroups (that is, quotients)	43

18 February 22	45
18.1 Existence of quotients (of smooth affine groups)	45
18.2 Lie algebras	46
18.2.1 Functoriality of $\text{Lie}(\cdot)$	47
19 February 24	47
19.1 Linear representations of split tori, over general rings	47
19.2 Proof of Theorem 19.1.2	49
20 February 26	50
20.1 k -split solvable groups	50
20.2 Borel Fixed Point Theorem	52
21 March 1	52
21.1 Remark on quotients	52
21.2 Lie-Kolchin Corollary 20.2.4	53
21.3 Structure theory of solvable groups	53
21.4 Unipotent radical	54
21.5 Reductive groups	55
22 March 3	56
22.1 Borel subgroups	56
23 March 5	58
23.1 Properties of parabolics	58
23.2 Conjugacy of maximal tori	59
24 March 8	60
24.1 Proof of Proposition 23.2.1	60
24.2 Cartan subgroups	61
24.3 $P_G(\lambda), U_G(\lambda), Z_G(\lambda)$ for a 1-parameter subgroup λ	61
25 March 10	62
25.1 Proof of Lemma 24.3.3 on P_G, U_G, Z_G	62
25.1.1 Proof that (i)+(ii) \Rightarrow (iii) [except unipotence of $U_G(\lambda)$]	62
25.1.2 Proof of (i)	62
25.1.3 Proof of (ii) and unipotence of $U_G(\lambda)$	63
26 March 12	64
26.1 Classification of split reductive groups of rank 1	64
A Properties of Orthogonal Groups	67
A.1 Basic definitions	67
A.2 Even rank	69
A.3 Odd rank	72
A.4 Center	75
A.5 Accidental isomorphisms	76
B Existence of Jordan decomposition	78
B.1 Variants in linear algebra over arbitrary fields	78
C Affine quotients	79
C.1 Introduction	79
C.2 Line stabilizers	80

D	Quotient formalism	80
D.1	Coset spaces and isomorphism theorems	81
D.2	Classifying some extension structures	84
D.3	Structure of split solvable groups	86
E	Grothendieck's theorem on tori	88
E.1	Introduction	88
E.2	Start of proof of Theorem E.1.1	89
E.3	The case of infinite k	91
E.4	Hypothesis (\star) for G implies the existence of a nontrivial k -torus	92
F	Covering by Borel subgroups	94
F.1	Main result	94
G	Conjugacy into a maximal torus	96
G.1	Main result	96
G.2	The proof	96
H	Dynamic approach to algebraic groups	97
H.1	Subgroups associated to a 1-parameter subgroup	97
H.2	Conjugacy for split tori	99

1 January 4

1.1 Some Definitions

Definition 1.1.1. A *group variety* over a field k is a smooth k -scheme G (possibly disconnected!) of finite type, equipped with k -morphisms $m : G \times G \rightarrow G, i : G \rightarrow G$, and a rational point $e \in G(k)$ satisfying the group axioms, in the sense that the following diagrams commute:

$$\begin{array}{ccccc}
 G \times G \times G & \xrightarrow{1_G \times m} & G \times G & & G & \xrightarrow{(1_G, i)} & G \times G \\
 m \times 1_G \downarrow & & m \downarrow & & \downarrow (i, 1_G) & \searrow & \downarrow m \\
 G \times G & \xrightarrow{m} & G & & G \times G & \xrightarrow{m} & G \\
 & & & & \downarrow e & & \\
 & & & & \text{Spec } k & &
 \end{array}$$

Remark 1.1.2. The rational point e can be regarded as a section of the structure map $G \rightarrow \text{Spec } k$. In the third diagram, the morphisms $e : G \rightarrow G$ are the “constant maps to the identity”, i.e. the compositions $G \rightarrow \text{Spec } k \xrightarrow{e} G$.

Remark 1.1.3. By HW1 Exercise 4(i), a connected group variety G over k is [geometrically connected and] geometrically irreducible. By some people's usage, this justifies the term “variety” in the name.

Definition 1.1.4. If we relax smoothness in Definition 1.1.1 to “finite type” but keep everything else, then G is called an *algebraic k -group scheme*. By HW1 Exercise 4(iii), over imperfect k reducedness does not imply geometric reducedness even for *connected* algebraic k -group schemes.

Definition 1.1.5. A group variety G over k is called *linear algebraic* if it is affine.

Remark 1.1.6. If G is an algebraic k -group scheme, then one can show that G is affine if and only if it is a k -subgroup scheme (cf. Definition 1.1.7) of GL_n for some n . (See Example 1.4.1 below for the definition of GL_n .) This is special to the case of fields in the sense that it is *not known* over more general rings (e.g., not even over the dual numbers over a field), though it is also true (and useful) over Dedekind domains by a variation on the argument used for fields.

Definition 1.1.7. Let G be a group variety over k , with corresponding multiplication map m_G , inversion map i_G , and identity section e_G . A k -subgroup $H \subset G$ is a closed subscheme such that there exist factorizations

$$\begin{array}{ccccc} \text{Spec } k & & H \times H & \xrightarrow{m_H} & H \\ \downarrow e_H & \searrow e_G & \downarrow & & \downarrow \\ H & \xrightarrow{\quad} & G \times G & \xrightarrow{m_G} & G \\ & & \downarrow & & \downarrow \\ & & G & \xrightarrow{i_G} & G \end{array}$$

By Yoneda's lemma, a k -group scheme is the same as a k -scheme G such that the Yoneda functor $h^G = \text{Hom}_{k\text{-Sch}}(-, G) : \text{Sch}/k \rightarrow \text{Sets}$ is equipped with a factorization through the forgetful functor $\text{Groups} \rightarrow \text{Sets}$. This is useful! Note that this is the same as the requirement that $G(R)$ is a group, functorially in R , for *all* k -algebras R , not just fields K/k . By the same reasoning, a closed subscheme $H \subset G$ is a k -subgroup if and only if $H(R) \subset G(R)$ is a [n abstract] subgroup for all k -algebras R .

Remark 1.1.8. Beware that over every imperfect k there exist connected non-reduced G with G_{red} *not* a k -subgroup (see [SGA3, VI_A, 1.3.2(2)]).

1.2 Smoothness

Let X be a k -scheme which is [locally] of finite type. Here is one definition of many for what it means for X to be smooth.

Definition 1.2.1. We say that X is *smooth* if and only if $X_{\bar{k}}^{-1}$ is regular, meaning that all of the local rings are regular local rings, which can be checked via the Jacobian criterion.

Remark 1.2.2. For the purpose of checking the Jacobian criterion, one may freely go up and down between algebraically closed fields containing k . For example, one might care about both $X_{\bar{\mathbf{Q}}}$ and $X_{\mathbf{C}}$ in the case $k = \mathbf{Q}$.

Remark 1.2.3. If k happens to be perfect, then smoothness is the same as regularity.

Let G be a k -group scheme [of finite type]. The group $G(\bar{k})$ acts on $G_{\bar{k}}$ by translation. Now G is smooth if and only if the local rings of $G_{\bar{k}}$ are regular, and over an algebraically closed field it is enough to check smoothness at the classical points $G_{\bar{k}}(\bar{k}) = G(\bar{k})$. But by commutative algebra plus the aforementioned “homogeneity”, it is thus enough to check that the completed local ring $\hat{\mathcal{O}}_{G_{\bar{k}}, e}$ is regular. On Homework 1, it is shown that it is equivalent to check that $\hat{\mathcal{O}}_{G_{\bar{k}}, e} \simeq \bar{k}[x_1, \dots, x_n]$ is a power series ring. In fact it is also shown there that it is equivalent to do this on the rational level; i.e. G is smooth if and only if $\hat{\mathcal{O}}_{G, e} \simeq k[x_1, \dots, x_n]$ is a power series ring over k ; and also that the latter has a functorial characterization due to Grothendieck. This is very useful for proving smoothness.

1.3 Connectedness

“Connectedness is a crutch”: it is essential to keep all the complexity of finite group theory from invading the theory of algebraic groups, since any finite group is a (disconnected) algebraic group. More specifically, a marvelous feature of the theory of smooth *connected* affine k -groups is that for a rather large class (the reductive ones) there is a rich classification and structure theory in terms of concrete combinatorial objects; nothing of the sort is available for a comparably broad class of finite groups, for example. (However, remarkably, the structure of most finite simple groups can be understood via the theory of connected reductive groups over finite fields.)

Let G^0 denote the connected component of the identity in a k -group scheme G of finite type.

Proposition 1.3.1. *The open and closed subscheme G^0 is a k -subgroup of G .*

Proof. To see that $G^0 \times G^0 \hookrightarrow G \times G \xrightarrow{m} G$ factors through G^0 , it suffices by topology to check that $G^0 \times G^0$ is connected. While it's not true *a priori* that a fiber product of connected schemes is connected, this *is* the case for a fiber product (over k) of *geometrically* connected k -schemes, and this is the situation we are in.

¹Here and throughout we use the convention that for an S -scheme X and a map $T \rightarrow S$, X_T denotes the base change $X \times_S T$.

In the finite type case (which is what we need) this is easily seen by extending scalars to \bar{k} and using linked chains of irreducible components to reduce to the more familiar fact that over an algebraically closed field a direct product of irreducible schemes of finite type is irreducible. For those interested in the hyper-generality without finite type hypotheses, see [EGA, IV₂, 4.5.8].

The case of inversion is handled similarly (in fact, it is much easier), and by construction the rational point e lies in G^0 . So we're done. \square

On Homework 1, it is shown that $[G(K) : G^0(K)] = [G(\bar{k}) : G^0(\bar{k})]$ for any algebraically closed field K/k .

Remark 1.3.2. The case of orthogonal groups, all of whose geometric connected components turn out to be defined over the ground field, is atypical. It is easy to write down examples of smooth affine k -group schemes whose non-identity connected components over k are not geometrically connected over k (and so there are more connected components over \bar{k} than there are over k). An example is the group scheme μ_5 of 5th roots of unity over $k = \mathbf{Q}$ (which has 5 geometric components, but only two connected components as a \mathbf{Q} -scheme).

This is an aspect of a more general phenomenon, whereby G might contain a lot more information than the group of rational points $G(k)$. Indeed, if k is finite then this is certainly the case (except when G is a finite constant k -group). Later, however, we'll see that *over infinite fields*, the set of rational points is often Zariski-dense in smooth connected affine groups (away from certain exceptional situations related to unipotent groups over imperfect fields), so for some proofs it will suffice to study the group of rational points!

1.4 Examples

Example 1.4.1. $GL_n = \{\det \neq 0\} \subset \text{Mat}_n = \mathbf{A}_k^{n \times n}$, is an open subset of an affine space, hence obviously smooth and connected.

Remark 1.4.2. For $k = \mathbf{R}$, the connectedness of GL_n as an algebraic group has nothing to do with the fact that in the classical topology $GL_n(\mathbf{R})$ is disconnected.

Remark 1.4.3. We'll develop a Lie algebra theory, so that for a k -group scheme [of finite type] G we get a Lie algebra $\text{Lie}(G)$, and it will be compatible with the analytic theory in the sense that when $k = \mathbf{R}$ we have $\text{Lie}(G) = \text{Lie}(G(\mathbf{R}))$ (and likewise when $k = \mathbf{C}$). This is actually very useful for studying disconnected Lie groups, when they happen to come from connected algebraic groups!

As a functor on k -algebras, GL_n is given by $GL_n(R) = \text{Aut}_R(R^n)$. It is, of course, an affine scheme: $GL_n = \text{Spec } k[x_{ij}][\frac{1}{\det}]$.

Example 1.4.4. A special case of Example 1.4.1 is GL_1 , which gets a special name, \mathbf{G}_m , the multiplicative group scheme.

Consider, by contrast, the circle group scheme, $\mathbf{S}^1 = \{x^2 + y^2 = 1\} \subset \mathbf{A}^2$ over an arbitrary field k . The group structure is given by $e = (1, 0)$, the composition law

$$(x, y)(x', y') = (xx' - yy', xy' + yx'),$$

and the inversion $(x, y)^{-1} = (x, -y)$. Note that when $k = \mathbf{R}$, the group $\mathbf{S}^1(\mathbf{R})$ is compact (in the classical topology), unlike $\mathbf{G}_m(\mathbf{R})$. Hence, $\mathbf{S}_\mathbf{R}^1 \not\cong \mathbf{G}_m$ as \mathbf{R} -groups. However, $\mathbf{S}_\mathbf{C}^1 \cong \mathbf{G}_m$ via the maps of group functors $(x, y) \mapsto x + iy$ [note that x and y lie in \mathbf{C} -algebras, not just in \mathbf{R} -algebras!] and in the other direction $t \mapsto (\frac{1}{2}(t + t^{-1}), \frac{1}{2i}(t - t^{-1}))$.

This example is so important that it gets a special generalization.

Definition 1.4.5. A k -torus is a group variety T over k such that $T_{\bar{k}} \cong \mathbf{G}_m^N$ for some $N \geq 0$. [So in particular, T must be commutative, connected, smooth, etc.]

Example 1.4.6. ["Example A"] Let $SL_n \subset GL_n$ be the closed k -subgroup scheme defined by $\det = 1$. There's an algebraic proof that SL_n is connected using that each variable x_{ij} occurs only once in the formula for the determinant; one can try to conclude (with some care) that $\det - 1$ is irreducible. But that's not a good proof. A more robust geometric approach is to use actions and fibrations: SL_n acts transitively on the connected \mathbf{P}^{n-1} with stabilizer that maps onto GL_{n-1} with kernel an affine space; this method will be discussed more generally (and the example of SL_n addressed more fully) in §8.2.

For smoothness, we can check the Jacobi criterion at the identity explicitly as follows. We have that $\det(1 + X) - 1 = \text{tr}(X) + (\text{higher order terms})$. The Jacobi criterion (for a hypersurface like $\text{SL}_n \subset \text{GL}_n$) says that SL_n is smooth, since the linear part $\text{tr}(X)$ of this expansion is nonzero.

Example 1.4.7. [“Example C”] Let V be a k -vector space of dimension $2n$, and $\langle \cdot, \cdot \rangle$ a symplectic [= nondegenerate alternating bilinear] form on V . For k -algebras R , define

$$G(R) = \{g \in \text{GL}(V)(R) \mid \langle gv, gw \rangle = \langle v, w \rangle \text{ for all } v, w \in V\} \subset \text{GL}(V)(R).$$

By Yoneda this defines a k -group scheme $\text{Sp}(\langle \cdot, \cdot \rangle)$, usually denoted Sp_{2n} since all pairs $(V, \langle \cdot, \cdot \rangle)$ with a given dimension $2n$ are isomorphic.

2 January 6

2.1 Translations

If G is a group variety over k then for any extension field k'/k the group $G(k')$ acts by translations on $G_{k'}$ – that is, *not* on G itself, only after extending scalars to k' . Concretely, this comes from defining for $g \in G(k') = G_{k'}(k')$ the left-translation-by- g map

$$\ell_g : G_{k'} \xrightarrow{x \mapsto (g, x)} G_{k'} \times G_{k'} \xrightarrow{m_{k'}} G_{k'}.$$

But of course there’s no reason this only works for extension *fields*. Rather, for any k -algebra R , we obtain an action of the group $G(R)$ on the R -scheme G_R in a similar fashion. There are a few entirely equivalent ways to think about this, as we now explain.

First, an R -point $g \in G(R)$ is the same as a k -map $\text{Spec } R \xrightarrow{g} G$, which is the same as an R -map $\tilde{g} : \text{Spec } R \rightarrow G_R$. Then ℓ_g is $G_R \xrightarrow{(\tilde{g}, 1_{G_R})} G_R \times G_R \xrightarrow{m_R} G_R$, where the \tilde{g} in the first factor means the “constant map” at \tilde{g} , i.e. the composition $G_R \rightarrow \text{Spec } R \xrightarrow{\tilde{g}} G_R$.

Equivalently, we can think of this as the R -map obtained by base-change from the k -map

$$G_R = \text{Spec } R \times_{\text{Spec } k} G \xrightarrow{(g, 1_G)} G \times G \xrightarrow{m} G.$$

Equivalently, and perhaps most elegantly, we can think about this functorially (via Yoneda) as the R -map corresponding to the map of functors on R -algebras defined by left-translation-by- g_B in the group $G(B)$ for any R -algebra B , where g_B is the base change of the R -point g to B . (Note that we are not requiring G to be affine, so we are implicitly using the elementary fact that to define a map of schemes it is enough to know the corresponding map between the functors they define on affine schemes. Often the restriction to evaluation on affines is just a notational or psychological convenience, but sometimes it is genuinely useful.)

2.2 Homomorphisms

Definition 2.2.1. A k -homomorphism $G' \rightarrow G$ of k -group schemes is a k -morphism such that the following diagrams commute:

$$\begin{array}{ccc} G' \times G' & \xrightarrow{m'} & G' \\ f \times f \downarrow & & \downarrow f \\ G \times G & \xrightarrow{m} & G \end{array} \quad \begin{array}{ccc} G' & \xrightarrow{\iota'} & G' \\ f \downarrow & & \downarrow f \\ G & \xrightarrow{\iota} & G \end{array} \quad \begin{array}{ccc} \text{Spec } k & \xrightarrow{e'} & G' \\ & \searrow e & \downarrow f \\ & & G \end{array}$$

Equivalently, by Yoneda’s lemma, it is a k -map such that for all k -algebras R , the corresponding map of sets $f_R : G'(R) \rightarrow G(R)$ is a group homomorphism.

Example 2.2.2. The determinant is a k -homomorphism $\det : \text{GL}_n \rightarrow \mathbf{G}_m$ for any n . This is easiest to see via the functorial characterization. The corresponding map of affine coordinate rings is $k[t, t^{-1}] \rightarrow k[x_{ij}][\frac{1}{\det}]$ given by $t \mapsto \det$.

Remark 2.2.3. For k -group *varieties* (i.e. smoothness is crucial, connectedness is not) a k -homomorphism $f : G' \rightarrow G$ is the same as a k -map such that the induced map on geometric points $G'(\bar{k}) \rightarrow G(\bar{k})$ is a group homomorphism. This is because to check that two maps of smooth varieties agree (or for that matter, that a map of smooth varieties factors through a smooth locally closed subvariety of the target) it is sufficient to check on geometric points.

2.3 Normal subgroups

Definition 2.3.1. A (closed) k -subgroup $H \subset G$ is called *normal* if the conjugation map $(h, g) \mapsto ghg^{-1} : H \times G \rightarrow G$ factors through the closed immersion $H \hookrightarrow G$:

$$\begin{array}{ccc} H \times G & \longrightarrow & G \\ & \searrow \exists & \uparrow \\ & & H \end{array}$$

Since $H \hookrightarrow G$ is a closed immersion, if this factorization exists it is automatically unique.

Equivalent reformulations of this definition include (1) that $H(R) \triangleleft G(R)$ for all k -algebras R ; and (2) in the smooth situation (cf. Remark 2.2.3 above), that $H(\bar{k}) \triangleleft G(\bar{k})$.

Example 2.3.2. $SL_n \triangleleft GL_n$.

2.4 Further discussion of examples

Example 2.4.1 (C_n). We return to the consideration of symplectic groups, Example “C”, or more properly C_n , from Example 1.4.7 above.

Let (V, B) be a symplectic space, so V is a finite-dimensional nonzero vector space over k , and $B : V \times V \rightarrow k$ is a nondegenerate alternating bilinear form. This forces $\dim V = 2n$ to be even, and with appropriately chosen coordinates the matrix of the bilinear form B is given in $n \times n$ blocks by $\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$. The **symplectic group** Sp_{2n} is defined (using coordinates) the functor of points $g \in Mat_{2n}$ such that

$$g^t \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} g = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

If we write such g in the block form $g = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ for $a, b, c, d \in Mat_n$ then it is the same to impose the conditions:

$$a^t c = c^t a, \quad b^t d = d^t b, \quad a^t d - c^t b = id_n.$$

Since the condition on $g \in GL_{2n} \subset Mat_{2n}$ is obviously Zariski-closed, and since the functorial description (as the subfunctor of GL_{2n} preserving B) makes it clear that Sp_{2n} is a subgroup, it is clear that $Sp_{2n} \subset GL_{2n}$ is a (closed) k -subgroup.

The natural questions about this group are not necessarily easy to answer. Is Sp_{2n} smooth? Yes, but the Jacobian criterion is difficult, or at least prohibitively laborious and inelegant, to verify directly. In §8.3 an elegant functorial method will be used to address it. Is Sp_{2n} connected? In §8.3 we will see that it is. The classical approach to this involved constructing explicit curves (families of symplectomorphisms) connecting an arbitrary group element to the identity, using the theory of so-called “transvections”.

Example 2.4.2 (B_n and D_n). Suppose that the characteristic of k is different from 2. (Fear not, we will revisit this with a better characteristic-free approach later. Characteristic 2 should never be ignored, as otherwise one cannot have a truly adequate version over rings.) Consider a *nondegenerate* quadratic space (V, q) over k . Here V is a nonzero finite-dimensional vector space over k , and q is a nondegenerate quadratic form on V , which means (because $\text{char}(k) \neq 2$) that the corresponding bilinear form B_q gives a perfect pairing $V \times V \rightarrow k$. When we later address a characteristic-free notion of non-degeneracy for quadratic spaces that works uniformly even over any ring (including $\mathbf{Z}/4\mathbf{Z}$ and \mathbf{Z} in which 2 may be a nonzero nilpotent or a non-unit that is not a zero-divisor), the smoothness of the projective quadric $(q = 0)$ will be the right perspective for defining non-degeneracy.

The **orthogonal group** of q is defined to be

$$O(q) = \{g \in GL(V) \mid q(gv) = q(v) \text{ for all } v \in V\}.$$

Functorially,

$$O(q)(R) = \{g \in \text{Aut}_R(V_R) : q(gv) = q(v) \text{ for all } v \in V_R\}.$$

It is easy to see, for example using coordinates, that preserving the quadratic form is a Zariski-closed condition on g . An equivalent condition (since 2 is a unit in the base ring k) is

$$O(q)(R) = \{g \in \text{Aut}_R(V_R) : B_q(gv, gw) = B_q(v, w) \text{ for all } v, w \in V_R\}.$$

Or equivalently

$$O(q) = \{g \in GL_n : g^t[B_q]g = [B_q]\},$$

where $[B_q]$ is your favorite matrix for the quadratic form B_q , after identifying V with k^n . The last description lets one write down a lot of explicit quadratic equations which cut out $O(q)$ from the affine space Mat_n . So, the moral is, $O(q) \subset GL_n$ is a closed k -subgroup scheme.

Is $O(q)$ smooth? Again, the answer is yes, and again checking the Jacobian criterion directly is probably not the way one wants to see this. Is $O(q)$ connected? As the case of $O_n = O(k^n, \sum x_i^2)$ over the reals indicates, the answer is No. What may be more surprising is that $O(q)$ always has exactly two connected components, for any q over any field k . (And in fact everything we have said works fine even in characteristic 2, provided one works to define the notion of nondegeneracy appropriately, which is not so obvious in this case.) We define the **special orthogonal group** to be $SO(q) = O(q)^0$. (This is the “wrong” definition in characteristic 2 when n is odd, as in such cases it turns out that $O(q) = SO(q) \times \mu_2$ as group schemes, with $SO(q) = O(q)_{\text{red}}$ a smooth closed subgroup. In particular, $O(q)$ is *connected* in such cases!)

Remark 2.4.3. This affords a good example of the phenomenon alluded to in Remark 1.4.3. Algebraically, $SO(q)$ is of course connected; but the Lie group $SO(q)(\mathbf{R})$ is disconnected whenever the quadratic form q has mixed signature $[\#\pi_0(SO(q)(\mathbf{R}))]$ in fact depends only on the signature of q , since the signature classifies quadratic forms uniquely over the reals]. Hence, Lie-algebra methods *can* be used to answer *algebraic* questions about $SO(q)$ which would have seemed to give information only about $SO(q)(\mathbf{R})^0$ in the classical Lie group setting.

Remark 2.4.4. The behavior of SO_n turns out to be qualitatively different depending on the parity of n , as we shall see. In the ABCDEFG classification, the examples SO_{2n+1} and SO_{2n} correspond to B_n and D_n respectively (with $n \geq 2$, say).

2.5 How far is a general smooth connected algebraic group from being either affine (i.e. linear algebraic) or projective (i.e. an abelian variety)?

Although we’ll never need it in this course, for cultural awareness we wish to mention two important theorems towards answering the question in the heading of this section.

Theorem 2.5.1 (Chevalley). *If k is perfect, then every connected k -group variety (N.B.: smooth!) fits into a unique short exact sequence (a notion to be defined later in the course)*

$$1 \rightarrow H \rightarrow G \rightarrow A \rightarrow 1$$

where H is linear algebraic and A is an abelian variety.

Define, for a smooth connected k -group G of finite type, the affinization to be $G^{\text{aff}} = \text{Spec } \mathcal{O}(G)$,

Theorem 2.5.2 (Anti-Chevalley). *For a smooth connected k -group G of finite type, $G^{\text{aff}} = \text{Spec } \mathcal{O}(G)$ is smooth (in particular, finite type!) and admits a unique k -group structure such that the natural map $G \rightarrow G^{\text{aff}}$ is a surjective homomorphism. Moreover, there is an exact sequence*

$$1 \rightarrow Z \rightarrow G \rightarrow G^{\text{aff}} \rightarrow 1$$

where Z is smooth, connected, and central in G . Moreover, if the characteristic of k is positive, then Z is semi-abelian: it fits into an exact sequence

$$1 \rightarrow T \rightarrow Z \rightarrow A \rightarrow 1$$

where T is a torus and A is an abelian variety.

The Anti-Chevalley theorem is quite amazing, and deserves to be more widely known (though its proof *uses* the Chevalley theorem over \bar{k} ; see [CGP, Theorem A.3.9] and references therein). It is actually more “useful” than the Chevalley theorem when $\text{char}(k) > 0$, even for perfect k , because the commutative (even central) term appears on the left, which is super-handy for studying degree-1 cohomology with coefficients in G (since degree-2 cohomology is most convenient with commutative coefficients).

3 January 8

Here’s an important example of a linear algebraic group: $\mathbf{G}_a = \mathbf{A}^1$, the additive group scheme, where “multiplication” is ordinary addition. It represents the forgetful functor from rings (or k -algebras, if we are working over a field) to abelian groups.

An important note is that $\mathbf{G}_a \not\cong \mathbf{G}_m$ as k -schemes, let alone k -groups. This is in contrast to the fact that in the classical topology, $(\mathbf{R}^\times)^0 \simeq \mathbf{R}$ as Lie groups, via logarithm and exponential; that isomorphism is actually more of a nuisance than useful in Lie theory.

It is an important fact that \mathbf{G}_a and \mathbf{G}_m are the only 1-dimensional connected (smooth) linear algebraic k -groups when k is algebraically closed; we’ll prove this later (building on Homework exercises).

3.1 How do linear algebraic groups arise in nature?

Here is a nice motivating example.

Example 3.1.1. Consider any abstract group Γ and a representation $\rho : \Gamma \rightarrow \text{GL}_n(k)$ in a finite dimensional vector space over a field. (This could be the monodromy representation for a fundamental group arising from a local system of finite-dimensional k -vector spaces, for instance. Or an ℓ -adic representation of a Galois group or of the étale fundamental group of a connected noetherian scheme.)

Inside the group variety GL_n there is a group of rational points $\text{GL}_n(k)$; inside *this* lies the image $\rho(\Gamma)$ of our representation. Let $\mathcal{G} \subset \text{GL}_n$ be the Zariski-closure of $\rho(\Gamma)$; it is some closed k -subscheme of GL_n . It turns out that \mathcal{G} is a smooth closed k -subgroup of GL_n , as we will discuss below.

3.2 Zariski closures of subgroups

To prove the claim at the end of Example 3.1.1, we will show something stronger:

Theorem 3.2.1. *Let G be any k -group variety and $\Sigma \subset G(k)$ any subgroup of the group of rational points. Then the Zariski closure $Z_\Sigma \subset G$ of Σ is a smooth closed k -subgroup, and for any field extension k'/k , in fact the closed subscheme $(Z_\Sigma)_{k'} \subset G_{k'}$ is the Zariski closure of $\Sigma \subset G(k') = G_{k'}(k') \subset G_{k'}$.*

Remark 3.2.2. Returning to Example 3.1.1, \mathcal{G} contains $\rho(\Gamma)$ as a Zariski-dense subset, so in fact \mathcal{G} is “controlled” by Γ . For example, this will imply that the irreducibility or complete reducibility of the representation ρ can be studied in the algebraic category by looking at the group variety \mathcal{G} . Note that \mathcal{G} might be highly disconnected, but at least the (geometric) component group will be finite. So representation theory questions over infinite fields can, in principle, be reduced to questions about connected algebraic groups and finite (étale) component groups, which might be more tractable.

Lemma 3.2.3. *If k is algebraically closed, then a reduced k -group scheme G (of finite type) is smooth.*

Proof. Over a perfect field, such as the algebraically closed field k , any reduced scheme of finite type is smooth on a dense open set. The proof of this standard fact from algebraic geometry rests upon finding a “separating transcendence basis” $\{t_i\}$ for the function field K of (each component of) the scheme, so that K is separable over $k(t_1, \dots, t_n)$; by the primitive element theorem, the smoothness situation is now amenable to study via the Jacobian criterion.

So let $U \subset G$ be a smooth, dense open subscheme. Choose a point $g \in G(k)$ and $u \in U(k)$ [there are plenty of points, because k is algebraically closed]. Look at the translation map $\ell_{gu^{-1}} : G \rightarrow G$, which is an isomorphism sending $u \mapsto g$. Hence $\widehat{\mathcal{O}}_u \simeq \widehat{\mathcal{O}}_g$; the left side is a power series ring, since U is smooth, so the right side is one too. This was one of our criteria for showing that G is smooth at g .

The point is that since $k = \bar{k}$, the $G(k)$ -translates of U cover G . Indeed, $\bigcup_{\gamma \in G(k)} \ell_\gamma(U)$ is open in G and by the above it contains all of $G(k)$. For any variety over an algebraically closed field, if an open set contains all the old-fashioned (rational) points $G(k)$, it must be the whole variety G . So we are done. \square

Proposition 3.2.4. *Let X be a k -scheme (locally) of finite type, and $\Sigma \subset X(k) \subset X$ any collection of rational points. Define $Z_{\Sigma, k}$ to be the Zariski closure of Σ in X . Then the following hold:*

- (i) *The scheme $Z_{\Sigma, k}$ is geometrically reduced over k .*
- (ii) *The formation of $Z_{\Sigma, k}$ is compatible with base change, in the sense that $(Z_{\Sigma, k})_{k'} = Z_{\Sigma, k'}$ inside $X_{k'}$, where on the right side we view $\Sigma \subset X(k) \subset X_{k'}(k')$.*
- (iii) *The formation of $Z_{\Sigma, k}$ is compatible with products, in the sense that for any other pair (X', Σ') over k , we have $Z_{\Sigma \times \Sigma', k} = Z_{\Sigma, k} \times Z_{\Sigma', k}$ as closed subschemes of $X \times X'$.*
- (iv) *The formation of $Z_{\Sigma, k}$ is functorial in the pair (X, Σ) , in the sense that if $f : X_1 \rightarrow X_2$ takes Σ_1 to Σ_2 , then it takes the subscheme $Z_{\Sigma_1} \subset X_1$ to $Z_{\Sigma_2} \subset X_2$.*

Proof of Theorem 3.2.1 from Proposition 3.2.4 (Sketch). Apply the proposition to $X = G$, our k -group variety, and $\Sigma \subset G(k)$ our subgroup of rational points. Compatibility with base change is part (ii) of the proposition. We use the functoriality of the closure construction [part (iv)] and compatibility with products [part (iii)], with respect to the multiplication, inversion, and identity maps to see that we actually have a subgroup scheme. To get smoothness, we use part (i) of the proposition, along with Lemma 3.2.3. \square

Proof of Proposition 3.2.4. The proof will be in a different order than the formulation of the result.

- (iv) Consider a map $f : X_1 \rightarrow X_2$ such that on k -points, f sends $\Sigma_1 \subset X_1(k)$ to $\Sigma_2 \subset X_2(k)$. We would like to show that $Z_{\Sigma_1} \hookrightarrow X_1 \rightarrow X_2$ factors through $Z_{\Sigma_2} \hookrightarrow X_2$. Form the fiber product $f^{-1}(Z_{\Sigma_2}) = X_1 \times_{X_2} Z_{\Sigma_2}$; it is a closed subscheme of X_1 , and by hypothesis it contains Σ_1 . Hence the scheme-theoretic closure Z_{Σ_1} must be contained in this preimage, which is equivalent to what we wanted.

- (i) and (ii) Note that the formation of Zariski-closures is Zariski-local, in the sense that it commutes with passage to open subsets. (This is just a fact from topology.) So we can assume without loss of generality that X is affine, equal to $\text{Spec } A$ for some k -algebra A , and thus the set of rational points Σ is a collection of maps $\{\sigma : A \rightarrow k\}$. Denote the kernel of σ by I_σ , which is a maximal – and in particular, a radical – ideal of A . The subscheme Z_Σ corresponds to the ideal $\bigcap_{\sigma \in \Sigma} I_\sigma$, the smallest ideal of A whose zero locus contains Σ . This is an intersection of radical ideals, so it is radical. Hence Z_Σ is reduced.

Geometric reducedness (i.e., assertion (i)) will follow immediately once we know compatibility with base change (i.e., assertion (ii)). For this, note that in $A_{k'} = A \otimes_k k'$, the ideal I'_σ of the point σ viewed as a point of $X_{k'} = \text{Spec } A_{k'}$ is simply $I_\sigma \otimes_k k'$. This is because $I'_\sigma = \ker(\sigma_{k'} : A_{k'} \rightarrow k') = I_\sigma \otimes_k k'$ (the latter equality because change of field is a flat base extension). So we are reduced to a problem in linear algebra: let V be a k -vector space (e.g., A) and $\{V_i\}$ a collection of k -subspaces of V (e.g. $\{I_\sigma : \sigma \in \Sigma\}$); then we want $(\bigcap_i V_i) \otimes_k k' = \bigcap_i (V_i \otimes_k k')$ inside $V \otimes_k k'$. To see why this equality holds, forget the multiplicative structure of k' and instead consider any k -vector space W in place of k' . We claim that $(\bigcap_i V_i) \otimes W = \bigcap_i (V_i \otimes W)$ inside $V \otimes W$. Any element of $V \otimes W$ lies in $V \otimes W'$ for some $W' \subset W$ finite-dimensional, and W' is a direct summand of W , so we are reduced to the easy case of finite-dimensional W .

- (iii) One inclusion of the desired equality $Z_{\Sigma \times \Sigma'} = Z_\Sigma \times Z_{\Sigma'}$ is easy. Since $\Sigma \times \Sigma'$ projects down to Σ (resp. Σ') in the first (resp. second) factor, which is contained in Z_Σ (resp. $Z_{\Sigma'}$), we automatically get an inclusion $\Sigma \times \Sigma' \subset Z_\Sigma \times Z_{\Sigma'}$. A product of closed subschemes is a closed subscheme of the product. Hence the Zariski closure $Z_{\Sigma \times \Sigma'}$ is certainly contained in $Z_\Sigma \times Z_{\Sigma'}$.

For the other direction, we first apply (i) and extend scalars, so we can assume k is algebraically closed, and $Z_\Sigma, Z_{\Sigma'}$ are reduced. Hence their product is reduced as well [since a product of reduced schemes of finite type over an algebraically closed field is reduced; e.g., this follows from consideration

of separating transcendence bases of function fields of irreducible components]. So it's enough to compare rational points. We want to prove $Z_\Sigma(k) \times Z_{\Sigma'}(k) \subset Z_{\Sigma \times \Sigma'}(k)$. This we do by a standard symmetry trick. First choose $\sigma \in \Sigma$. We claim that $\sigma \times Z_{\Sigma'}(k) \subset Z_{\Sigma \times \Sigma'}(k)$. Why does this hold? Well, $\sigma \times \Sigma' \subset \Sigma \times \Sigma' \subset Z_{\Sigma \times \Sigma'}$, and the closure of $\sigma \times \Sigma'$ in $\sigma \times X' \simeq X'$ is $\sigma \times Z_{\Sigma'}$. But $\sigma \times X'$ is closed in $X \times X'$. Hence the closure of $\sigma \times \Sigma'$ in $X \times X'$ is $\sigma \times Z_{\Sigma'}$, which is therefore contained in the closed subscheme $Z_{\Sigma \times \Sigma'}$, so the intermediate claim is proved. Now choose $z \in Z_{\Sigma'}(k)$. By analogous reasoning, we see that $Z_\Sigma(k) \times z \subset Z_{\Sigma \times \Sigma'}(k)$. The original claim follows. \square

4 January 11 (Substitute lecture by A. Venkatesh)

4.1 Tori

Definition 4.1.1. A k -split torus T is a k -group isomorphic (over k) to \mathbf{G}_m^r for some r .

Recall that a torus is a k -group such that $T_{\bar{k}}$ is \bar{k} -split. (Definition 1.4.5.)

Example 4.1.2. The special orthogonal group $\mathrm{SO}(x^2 + y^2) = \{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a^2 + b^2 = 1 \}$ is an \mathbf{R} -torus under the isomorphism $\mathrm{SO}(x^2 + y^2)_{\mathbf{C}} \rightarrow \mathbf{G}_m$ given by $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mapsto a + ib$. But it is not \mathbf{R} -split (cf. Example 1.4.4).

Definition 4.1.3. The *character group* $X(T)$ or $X^*(T)$ of a k -split torus T is $\mathrm{Hom}_k(T, \mathbf{G}_m)$. The *cocharacter group* $X_*(T)$ is $\mathrm{Hom}_k(\mathbf{G}_m, T)$.

(If T is not k -split then the “right” notions are not the group homomorphisms over k , but rather over \bar{k} , or as we shall see, over k_s .) Since (by Homework 1) $\mathrm{End}_k(\mathbf{G}_m) = \mathbf{Z}$ under the identification $(t \mapsto t^n) \leftrightarrow n$, we get several facts, assuming T is k -split:

1. The groups of characters and cocharacters $X^*(T)$ and $X_*(T)$ are both finite free \mathbf{Z} -modules, isomorphic to \mathbf{Z}^r if $T \simeq \mathbf{G}_m^r$.
2. We have a perfect pairing $X_*(T) \times X^*(T) \rightarrow \mathrm{Hom}_k(\mathbf{G}_m, \mathbf{G}_m) = \mathbf{Z}$ via composition. Explicitly, if $T = \mathbf{G}_m^r$ we identify $X^*(T)$ with \mathbf{Z}^r via $(n_1, \dots, n_r) \mapsto [(t_1, \dots, t_r) \mapsto \prod t_i^{n_i}]$, and $X_*(T)$ with \mathbf{Z}^r via $(m_1, \dots, m_r) \mapsto [t \mapsto (t^{m_1}, \dots, t^{m_r})]$. Under these identifications, the pairing is defined by

$$\langle (m_1, \dots, m_r), (n_1, \dots, n_r) \rangle = [t \mapsto t^{\sum m_i n_i}] \leftrightarrow \sum m_i n_i \in \mathbf{Z} \simeq \mathrm{End}_k(\mathbf{G}_m).$$

Remark 4.1.4. In the non-split case we have a functor $T \mapsto X^*(T_{k_s})$ from algebraic k -tori to finite free \mathbf{Z} -modules equipped with a discrete action by $\mathrm{Gal}(k_s/k)$ (where $\gamma \in \mathrm{Gal}(k_s/k)$ acts via scalar extension throughout by $\gamma : k_s \simeq k_s$). The theorem will be that this is an equivalence of categories.

Example 4.1.5. Returning to Example 4.1.2, i.e. $\mathrm{SO}(x^2 + y^2)$ over $k = \mathbf{R}$, the corresponding abelian group is just \mathbf{Z} with the unique nontrivial action of $\mathrm{Gal}(\mathbf{C}/\mathbf{R}) = \mathbf{Z}/(2)$.

Remark 4.1.6. Once the right definitions of character and cocharacter groups are given for a general k -torus T , it will be the case that all elements of these groups are defined (as homomorphisms to or from \mathbf{G}_m) over any extension of k that splits T .

4.2 Maximal split tori

The big theorem about maximal split tori is the following (for which we will later discuss the proof in some important special cases that we need in developing the basic theory).

Theorem 4.2.1. *If G is any smooth connected linear algebraic k -group, all maximal k -split tori $T \subset G$ are $G(k)$ -conjugate.*

Remark 4.2.2. (1) It might well be the case that any k -split torus $T \subset G$ is trivial; for example, this is true for $G = \mathrm{SO}(x^2 + y^2 + z^2)$ over \mathbf{R} .

- (2) The theorem is false if “maximal k -tori” were to replace “maximal k -split tori”. And note that it is trivial (by dimension reasons) that maximal k -split tori always exist; in contrast, there may be no k -split maximal k -tori (once again, $\mathrm{SO}(x^2 + y^2 + z^2)$ over \mathbf{R}).

Example 4.2.3. Over $k = \mathbf{R}$, both $\mathrm{SO}(x^2 + y^2)$ and the standard diagonal torus $\left\{ \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \right\}$ are maximal \mathbf{R} -tori inside SL_2 . But they’re not $\mathrm{SL}_2(\mathbf{R})$ -conjugate, or even \mathbf{R} -isomorphic.

Example 4.2.4. Let $G = \mathrm{GL}_n$ over a field k . Then any separable extension E/k of degree n gives rise to a “Weil restriction” maximal torus $R_{E/k} \mathbf{G}_m$ inside GL_n . (At the level of k -points, this consists of elements of E^\times acting on a k -basis for E by multiplication.)

Example 4.2.5. Let $G = \mathrm{SL}_n$. Let $T = \left\{ \begin{pmatrix} t_1 & & \\ & \ddots & \\ & & t_n \end{pmatrix} \mid \prod t_i = 1 \right\} \subset G$ be the standard torus. The claim is that T is maximal as a k -torus in G and that all maximal k -split tori in G are $G(k)$ -conjugate to T .

We will not prove the conjugacy assertion now, but it will follow from the fact that any commuting set of diagonalizable matrices can be simultaneously diagonalized, plus the fact that if $T' \subset \mathrm{SL}_n$ is a torus then $T'(k)$ consists of semisimple elements. But let’s at least now prove that this diagonal T is maximal in SL_n :

Proof of maximality. Note that it suffices to check this after extending scalars to an infinite field. Under this assumption, the claim follows from the fact that for any k -algebra R , we have

$$Z_{G(R)}(T_R) = T(R). \quad (\star)$$

Granting (\star) , in fact it follows that $T \subset G$ is a maximal commutative subgroup scheme, and hence *a fortiori* a maximal torus.

To see (\star) simply compute

$$\begin{pmatrix} t_1 & & \\ & \ddots & \\ & & t_n \end{pmatrix} [g_{ij}] \begin{pmatrix} t_1^{-1} & & \\ & \ddots & \\ & & t_n^{-1} \end{pmatrix} = [t_i t_j^{-1} g_{ij}].$$

By the infinitude of k , we thus see that if $g \in Z_{G(R)}(T_R)$ then $g_{ij} = 0$ for $i \neq j$. \square

Remark 4.2.6. There are plenty of other maximal commutative k -subgroups (not tori) non-conjugate to T . As an exercise, find a commutative $(n-1)$ -dimensional smooth connected unipotent subgroup of SL_n that is a maximal smooth commutative k -subgroup. Note that this is “as far as possible from being a torus” since it is unipotent. (The abstract notion of “unipotency” and its contrast with tori will be developed later in the course. For present purposes with this example, just think in terms of matrices.)

Example 4.2.7. Let $G = \mathrm{Sp}_{2n}$. Let U be an n -dimensional k -vector space, and U^* its dual. Denote the pairing $U \times U^* \rightarrow k$ by $[\cdot, \cdot]$. Define $W = U \oplus U^*$. It has a standard symplectic form ω defined by

$$\omega((x, x^*), (y, y^*)) = [x, y^*] - [y, x^*].$$

Thus we can realize G as $\mathrm{Aut}(W, \omega) = \mathrm{Sp}(W)$. There’s a map $\varphi : \mathrm{GL}(U) \rightarrow \mathrm{Sp}(W)$ given by $g \mapsto g \oplus (g^t)^{-1}$. This is easily seen to be a closed immersion. The claim about maximal tori in G is that for $T' \subset \mathrm{GL}(U)$ a maximal k -split torus, the image $\varphi(T') \subset \mathrm{Sp}(W)$ is maximal k -split, and any such is $G(k)$ -conjugate to $\varphi(T)$, where T is the standard maximal k -split torus in $\mathrm{GL}(U)$. In particular, the dimension of the maximal k -split tori in $G = \mathrm{Sp}_{2n}$ is n .

The proof of maximality is as before: show that $Z_{G(R)}(\varphi(T)_R) = \varphi(T)(R)$. The proof that all maximal k -split tori are $G(k)$ -conjugate to $\varphi(T)$ can in fact be reduced to the corresponding claim for $\mathrm{GL}(U)$. This is just an example, so we do not address rigorous details at the present time; we’ll come back to this more broadly in the sequel course as well.

4.3 Building up groups from tori

Given any connected *reductive*² k -group G , choose a maximal k -split torus T . One can construct the following data:

²This notion will be defined later.

- A finite subset of *roots* $\Phi \subset X^*(T)$,
- A finite subset of *coroots* $\Phi^\vee \subset X_*(T)$,
- A bijection $\alpha \mapsto \alpha^\vee$, mapping $\Phi \rightarrow \Phi^\vee$, and satisfying some combinatorial properties.

Theorem 4.3.1. *Over an algebraically closed field k , the torus T together with the above data will turn out to determine G up to isomorphism. This is a huge theorem; it will be the topic of the final section of the course.*

4.3.1 Construction of Φ

Fix a connected reductive G as above. Consider the set of all **unipotent 1-parameter subgroups** of G ; i.e., closed subgroups $u : \mathbf{G}_a \hookrightarrow G$ that are *normalized by* T . In view of the fact that the only automorphisms of \mathbf{G}_a over an algebraically closed field are unit scalings on the coordinate, it follows that there exists a k -homomorphism $\chi : T \rightarrow \mathbf{G}_m$ satisfying $t \cdot u(x) \cdot t^{-1} = u(\chi(t)x)$ at the level of functors. The set of these u turns out to be finite, and the set of χ 's which arise in this fashion are the roots Φ of T in G .

Example 4.3.2. Let $G = \mathrm{SL}_n$ and T the standard split torus. For $i \neq j$ there is a unipotent 1-parameter group u_{ij} given by $x \mapsto \begin{pmatrix} 1 & & * \\ & \ddots & \\ * & & 1 \end{pmatrix}$ where the off-diagonal entry in the ij -spot is x and the other off-diagonal entries are zero. For $t = \mathrm{diag}(t_1, \dots, t_n) \in T$, one computes $t \cdot u_{ij}(x) \cdot t^{-1} = u_{ij}(t_i t_j^{-1} x)$, so the roots of $T \subset G$ are of the form $\chi_{ij} : t \mapsto t_i t_j^{-1}$ for $1 \leq i \neq j \leq n$.

Example 4.3.3. Let $G = \mathrm{Sp}_{2n} = \mathrm{Sp}(W)$, let T be the standard diagonal split torus in $\mathrm{GL}(U)$, which we identify with its image in G via the map φ . The roots of $T \subset \mathrm{GL}(U) \hookrightarrow G$ are

$$\mathrm{diag}(t_1, \dots, t_n) \mapsto \begin{cases} t_i t_j^{-1} & i \neq j, 1 \leq i, j \leq n, \text{ or} \\ t_i t_j & \text{and } 1 \leq i, j \leq n \text{ (including } i = j). \end{cases}$$

Thus they are χ_{ij} for $i \neq j$ as above, plus new roots χ'_{ij} for all pairs (i, j) .

One can check that in both of these examples, multiplication into G from a direct product of T against the images of the roots in a suitable order is an isomorphism onto an open subset of the group G . This is the so-called “open cell”, and it exists in general (not just in the above examples). The structure of this open cell underlies why it is reasonable to believe that G can be reconstructed completely from T and the root system. We will make this more concrete at the beginning of the next lecture.

5 January 13

5.1 Mapping G_a and G_m into a reductive group

As a consequence of the theory of maximal tori, roots and coroots, there is an abundance of \mathbf{G}_a 's and \mathbf{G}_m 's sitting inside a so-called “split connected reductive” group such as SL_n or Sp_{2n} . To illustrate the principles involved, if we consider the standard upper and lower triangular unipotent 1-parameter subgroups in SL_2 then we get a map

$$\begin{aligned} \mathbf{G}_a \times \mathbf{G}_m \times \mathbf{G}_a &\rightarrow \mathrm{SL}_2 \\ (u, t, u') &\mapsto \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ u' & 1 \end{pmatrix} \end{aligned}$$

This is easily check to be an open immersion. More generally, we'll have an open immersion of the form

$$\left(\prod_i \mathbf{G}_a \right) \times \left(\prod_j \mathbf{G}_m \right) \times \left(\prod_k \mathbf{G}_a \right) \rightarrow G = \mathrm{SL}_n, \mathrm{Sp}_{2n}, \dots$$

The torus T in the middle is maximal in G ; the \mathbf{G}_a 's are normalized by T ; and the maps are determined by the corresponding “root data”.

5.2 Classification of 1-dimensional connected linear algebraic groups

Now we come back to a proper development of the subject, rather than a discussion of things to come much later. The goal for this lecture is to prove the following theorem. By convention, “linear algebraic k -group” will mean “smooth affine k -group”.

Theorem 5.2.1. *If k is algebraically closed, the only 1-dimensional connected linear algebraic k -groups are \mathbf{G}_m and \mathbf{G}_a .*

Corollary 5.2.2. *For any field k , if G is a 1-dimensional connected linear algebraic k -group, then the following hold.*

- (i) G is commutative.
- (ii) There exists a finite extension k'/k such that $G_{k'}$ is isomorphic to either \mathbf{G}_a or \mathbf{G}_m . The first case is known as the **additive** or **unipotent** case; the second is called the **multiplicative** case.

Remark 5.2.3. These two cases are in fact different. *Exercise:* Show that

$$\mathrm{Hom}_k(\mathbf{G}_a, \mathbf{G}_m) = \mathrm{Hom}_k(\mathbf{G}_m, \mathbf{G}_a) = 1$$

over a field k , although non-trivial homomorphisms can exist over an artin local ring k . (Such non-trivial homomorphisms cannot be isomorphisms, however.)

Proof of Corollary 5.2.2 from Theorem 5.2.1. (i) This is trivial, since by Homework 2, it suffices to prove that $G(\bar{k})$ is commutative.

(ii) Note that $\bar{k} = \varinjlim k'$, the direct limit of $k' \subset \bar{k}$ which are finite over k . Now in general, if X and Y are any finite type k -schemes (for example G and \mathbf{G}_a or \mathbf{G}_m), then a \bar{k} -map $f : X_{\bar{k}} \rightarrow Y_{\bar{k}}$ arises from a k' -map $f' : X_{k'} \rightarrow Y_{k'}$ for some k' in this direct system of intermediate fields. In the affine case this is more or less trivial: chase where the generators and relations in a finite presentation of $\Gamma(Y_{\bar{k}})$ go in $\Gamma(X_{\bar{k}})$, and observe that only finitely many elements of \bar{k} are involved in specifying the map f . So just take the subfield generated by these elements. Since the affine case is all we need here, and will be most important for us in this course, we won't prove the general case. But it's proved in [EGA, IV₃, §8] in vast generality, and note that the affine case does not tautologically imply the general case (i.e., some thought is required). \square

Refinements of Corollary 5.2.2(ii)

In the additive case, we can actually choose the finite extension k'/k to be purely inseparable. By the direct limit argument from the proof of Corollary 5.2.2, this is equivalent to the claim that over a perfect field k , a 1-dimensional connected linear algebraic k -group which is additive over \bar{k} , is actually k -isomorphic to \mathbf{G}_a (since the perfect closure of a field k is the direct limit of the purely inseparable finite extensions of k). In the multiplicative case, we likewise claim that we can choose the finite extension k'/k to be separable. Again by the direct limit argument, this is equivalent to the claim that if k is separably closed then a 1-dimensional connected linear algebraic k -group which is \mathbf{G}_m over \bar{k} is actually isomorphic to \mathbf{G}_m over k (recall that the separable closure of k is a direct limit of finite separable extensions).

The equivalent formulations of these facts – i.e., the claims over perfect and separably closed fields – will follow in the perfect/additive case from the proof of Theorem 5.2.1 and in the separably-closed/multiplicative case from Homework 2.

5.3 Examples of non-split 1-dimensional linear algebraic k -groups

Example 5.3.1 (Non-split multiplicative group). Let k be a field, and k'/k a quadratic Galois extension splitting an irreducible separable polynomial $f(t) = t^2 + at + b$. (If $\mathrm{char}(k) \neq 2$ we can assume $a = 0$, but why would one want to do that?) Consider the curve $G \subset \mathbf{A}_k^2$ defined by $x^2 + axy + by^2 = 1$. Secretly this is the norm-1 subgroup of the Weil restriction $R_{k'/k}\mathbf{G}_m$, which is “ k'^{\times} regarded as a k -group” (although that's a sloppy, imprecise way of defining the group). This has a natural k -group structure, defined in analogy to \mathbf{S}^1 over \mathbf{R} ; cf. Example 1.4.4.

We have $G_{k'} \simeq G_m$. But G is not k -isomorphic to G_m even as mere k -schemes. One way to see this is that the unique regular compactification $\{x^2 + axy + by^2 = z^2\} \subset \mathbf{P}_k^2$ has only 1 point complementary to G and its residue field is k' , while the unique regular compactification \mathbf{P}_k^1 of G_m has two points complementary to G_m and they are both k -rational.

Example 5.3.2 (Non-split additive group). Let k be an imperfect field of characteristic $p > 0$ and choose $a \in k - k^p$. Let $G \subset \mathbf{A}^2$ be the curve defined by $y^p = x + ax^p$. This equation is easily seen to be additive, so G is a subgroup. For $k' = k(\alpha)$, where $\alpha^p = a$, the curve $G_{k'}$ is the same as $x = (y - \alpha x)^p$, on which the coordinate $y - \alpha x$ gives a k' -group isomorphism $G_{k'} \simeq G_a$. Over k itself, the compactification of G in \mathbf{P}^2 is $y^p = xz^{p-1} + ax^p$. This is actually regular, as we'll see in a moment. At infinity, $y^p = ax^p$ is the only point, with residue field k' . Since this is not k -rational, as long as we know it is regular then we know that $G \not\simeq G_a$ as k -schemes, since the unique point complementary to G_a in its regular compactification \mathbf{P}_k^1 is k -rational.

To see the asserted regularity, note that when $x = 1$ the equation $y^p = xz^{p-1} + ax^p$ becomes $y^p = a + z^{p-1}$. This actually defines a Dedekind ring (exercise), which proves regularity.

5.4 Start of proof of the classification theorem

Given a connected 1-dimensional linear algebraic k -group G (recall that $k = \bar{k}$), choose an open immersion $G \hookrightarrow X$ where X is a smooth projective curve over k . Then $X - G$ is a finite nonempty set of k -points.

Claim 5.4.1. $X \simeq \mathbf{P}_k^1$.

Proof. It suffices to prove that the genus g of X vanishes. The infinite set $G(k) - \{e\}$ acts on G via fixed-point-free automorphisms. Since the smooth compactification process is functorial, these all extend to automorphisms of X . But it is a general fact that any smooth projective (connected) curve C over an algebraically closed field with genus $g \geq 2$ has finite automorphism group, so $g \leq 1$.

[Here is one method to show that C has finite automorphism group: we'll show that the locally finite type automorphism scheme of C is both étale and finite type. The étaleness follows because the tangent space at the identity to the Aut-scheme is the space of global vector fields, which vanishes because the sheaf of vector fields (dual to $\Omega_{C/k}^1$) has degree $2 - 2g < 0$. To prove the finite type property, the formation of graphs of automorphisms defines a map from the automorphism scheme to the Hilbert scheme of $C \times C$, and one shows this is a locally closed immersion by the same argument that already occurs in the construction of Hom-schemes as subschemes of Hilbert schemes via consideration of graphs. Although the Hilbert scheme is just locally of finite type, the locus with a given Hilbert polynomial relative to a specified ample line bundle is contained in a finite type part. The graphs of automorphisms of C all have the same Hilbert polynomial on $C \times C$ relative to a fixed ample line bundle arising from one on C and hence these graphs lie in a finite-type part of the Hilbert scheme.]

Next observe that $G(k) \curvearrowright X$ preserving the finite set $X - G$. Hence some finite index subgroup of $G(k)$ must fix $X - G$ pointwise.

Suppose for contradiction that $g = 1$. Choose any point $O \in X - G$. Then (X, O) is an elliptic curve E . But then E has an infinite group of automorphisms, which contradicts the theory of elliptic curves [Sil, Thm. III.10.1]. \square

So we know $X = \mathbf{P}^1$. We have an infinite group Γ acting on \mathbf{P}^1 fixing a finite set of points $\mathbf{P}^1 - G$. If an automorphism of \mathbf{P}^1 fixes 3 points, it is trivial. Thus $\mathbf{P}^1 - G$ consists of either 1 or 2 points. Therefore we obtain, after a change of coordinates, an isomorphism of pointed curves $(G, e) \simeq (\mathbf{A}^1, 0)$ or $(G_m, 1)$.

Now we are almost done. It suffices to check that G_a and G_m each admit a unique group structure.

6 January 20 (Substitute lecture by A. Venkatesh)

6.1 End of proof of classification of 1-dimensional connected linear algebraic groups

To finish the proof of Theorem 5.2.1, we just need to show the following.

Theorem 6.1.1. *The only k -group structures on \mathbf{A}^1 and \mathbf{G}_m are the usual ones, up to a curve automorphism moving the identity point. In particular, for the usual identity point the group structure is uniquely determined.*

Proof. We can assume $k = \bar{k}$.

First let's do the case of \mathbf{A}^1 . Since $\text{Aut}(\mathbf{A}^1)$ acts transitively on $\mathbf{A}^1(k)$, we can assume that the identity is $0 \in \mathbf{A}^1(k)$. Say we have a group law on \mathbf{A}^1 . For $x \in \mathbf{A}^1(k)$, translation by x is a k -automorphism t_x of \mathbf{A}^1 . If $x \neq 0$, there are no fixed k -points (this is a fact about groups). Now we know what $\text{Aut}(\mathbf{A}^1)$ is: it consists of affine transformations $y \mapsto ay + b$. To be fixed-point free on k -points, it must be of the form $y \mapsto y + c$. Since it takes 0 to x , $c = x$. So the group is the usual \mathbf{G}_a .

The argument for \mathbf{G}_m is much the same. In this case, automorphisms of \mathbf{G}_m extend to automorphisms of \mathbf{P}^1 which either fix or swap zero and infinity. That is, they are of the form $y \mapsto y\alpha$ or $y \mapsto \alpha/y$. Since $k = \bar{k}$, $\sqrt{\alpha} \in k$, so $y \mapsto \alpha/y$ has fixed points. Hence t_x is $y \mapsto y\alpha$ for some α , and if we pin down the identity in the group law to be $1 \in \mathbf{G}_m(k)$ (as we may) then we must have $\alpha = x$. \square

So now we know that over a field k , while there can be many isomorphism classes of 1-dimensional smooth connected linear algebraic groups, they all become isomorphic to \mathbf{G}_m or \mathbf{G}_a over \bar{k} . We say that they are **forms** of \mathbf{G}_m or \mathbf{G}_a .

Example 6.1.2. If q is a non-degenerate quadratic form on a 2-dimensional vector space V over a field k (say with $\text{char}(k) \neq 2$ for now, since we haven't defined non-degeneracy more generally yet), then $\text{SO}(q)$ is a form of \mathbf{G}_m . (This is also valid in characteristic 2 for the right notion of "non-degenerate".)

Example 6.1.3. \mathbf{G}_a can actually have forms U over an imperfect field k which have no nontrivial k -points; i.e. $U(k) = \{0\}$. For an example, let $k = k_0(t)$ for k_0 a field of characteristic p . Let $q = p^r > 2$. Then $U \subset \mathbf{A}^2$ defined by $y^q = x - tx^p$ is such a form.

6.2 Smoothness criteria

Theorem 6.2.1. *Let k be a field. Let A be a complete local Noetherian k -algebra with maximal ideal \mathfrak{m}_A and residue field $A/\mathfrak{m}_A = k$. Then the following are equivalent:*

- (i) A is regular; i.e. $\dim_k \mathfrak{m}_A/\mathfrak{m}_A^2 = \dim A$.
- (ii) $A \simeq k[[x_1, \dots, x_d]]$ for some d .
- (iii) A satisfies Grothendieck's "infinitesimal criterion for smoothness": for an Artin local k -algebra R and an ideal $J \triangleleft R$ satisfying $J^2 = 0$, any k -homomorphism $A \rightarrow R/J$ lifts to a k -map $A \rightarrow R$.

Before giving the proof, let's see a non-example.

Example 6.2.2. Let $X = \text{Spec } k[x, y]/xy$ be the axes in \mathbf{A}^2 . Let $A = \widehat{\mathcal{O}_{X,0}}$ be the completed local ring at the origin. Let $R = k[\epsilon]/(\epsilon^3)$ and $R/J = k[\epsilon]/(\epsilon^2)$. Then $x \mapsto \epsilon, y \mapsto \epsilon : A \rightarrow R/J$ does not lift to a k -map $A \rightarrow R$.

Proof of Theorem 6.2.1. We'll prove the equivalences one by one.

(ii) \Rightarrow (i) This is easy. One just needs to check that $\dim k[[x_1, \dots, x_n]] = n$, which follows from the characterization of the dimension of a ring via its Hilbert polynomial; i.e. $\dim_k R/\mathfrak{m}^\ell$ is eventually polynomial of degree $\dim R$ in ℓ .

(i) \Rightarrow (ii) Pick generators $\bar{x}_1, \dots, \bar{x}_d$ for $\mathfrak{m}_A/\mathfrak{m}_A^2$ as a k -vector space. Lifting them gives a map $\varphi : R = k[[t_1, \dots, t_d]] \rightarrow A$ sending $t_i \mapsto x_i$. The claim is that φ is an isomorphism. For surjectivity, we argue by "successive approximation". Given $a \in A$ we can find $r \in R$ so that $\varphi(r) \in a + \mathfrak{m}_A^2$. Write $\varphi(r) = a + \sum m_i m'_i$ where $m_i, m'_i \in \mathfrak{m}_A$. Now we can find $r_i, r'_i \in \mathfrak{m}_R$ so that $\varphi(r_i) \in m_i + \mathfrak{m}_A^2$. Thus $\varphi(r - \sum r_i r'_i) \in a + \mathfrak{m}_A^3$. Continue in this manner. We can pass to the limit since R is complete. So there exists r with $\varphi(r) = a$.

For injectivity, suppose otherwise. Then there is a nontrivial power series relation over k among the x_i 's. That is, choose a nonzero $f \in \ker(\varphi)$. Then A is a quotient of $R/(f)$. But $\dim R/(f) = \dim R - 1 =$

$d - 1 < \dim A$, which is a contradiction.

(ii) \Rightarrow (iii) If $A = k[x_1, \dots, x_n]$ then (iii) is easy to verify. This is because $\text{Hom}_{\text{Alg}/k}(A, R)$ for an Artin local k -algebra R is just a product of n copies of \mathfrak{m}_R , one for each generator of A . The lifting property thus holds trivially, since \mathfrak{m}_R surjects onto \mathfrak{m}_R/J . So given $A \rightarrow R/J$, wherever you're sending the generators of A in \mathfrak{m}_R/J , lift those elements arbitrarily to \mathfrak{m}_R to get the desired map $A \rightarrow R$.

(iii) \Rightarrow (ii) Choose a k -basis $\bar{x}_1, \dots, \bar{x}_d$ for $\mathfrak{m}_A/\mathfrak{m}_A^2$. Lift \bar{x}_i to $x_i \in \mathfrak{m}_A$. We get a map $\varphi : R = k[t_1, \dots, t_d] \rightarrow A$ as before. By construction φ induces an isomorphism $\bar{\varphi} : R/\mathfrak{m}_R^2 \xrightarrow{\sim} A/\mathfrak{m}_A^2$. So we have a map $\theta^{(2)} : A \rightarrow A/\mathfrak{m}_A^2 \xrightarrow{\bar{\varphi}^{-1}} R/\mathfrak{m}_R^2$. Apply the lifting property for $J = \mathfrak{m}_R^2/\mathfrak{m}_R^3 \triangleleft R/\mathfrak{m}_R^3$. So we can lift $\theta^{(2)}$ to $\theta^{(3)} : A \rightarrow R/\mathfrak{m}_R^3$. We can then continue in this manner getting $\theta^{(i)} : A \rightarrow R/\mathfrak{m}_R^i$ for all i . By completeness of R , there is thus a map $\theta : A \rightarrow R$. The claim is that θ is an isomorphism.

For surjectivity, argue by successive approximation as in (i) \Rightarrow (ii). This works because θ induces the isomorphism $\theta_2 = \bar{\varphi}^{-1} : A/\mathfrak{m}_A^2 \xrightarrow{\sim} R/\mathfrak{m}_R^2$, which lets the inductive proof get started.

For injectivity, one could argue by dimension as in (i) \Rightarrow (ii), but here is a rephrasing of the same idea. It suffices to show that each $\theta_i : A/\mathfrak{m}_A^i \rightarrow R/\mathfrak{m}_R^i$ is injective, since $\ker \theta$ must “show up” at some finite level if it is nonzero (Krull intersection theorem). We know θ_i is surjective for each i , since θ is. Now count k -dimensions. Observe that $\mathfrak{m}_A^{i-1}/\mathfrak{m}_A^i$ is spanned by monomials of degree $n - 1$ in x_1, \dots, x_d . They go to t_1, \dots, t_d , which are linearly independent in $\mathfrak{m}_R^{i-1}/\mathfrak{m}_R^i$. Hence $\dim_k \mathfrak{m}_A^{i-1}/\mathfrak{m}_A^i \leq \dim_k \mathfrak{m}_R^{i-1}/\mathfrak{m}_R^i$ for each i . Thus $\dim_k A/\mathfrak{m}_A^i \leq \dim_k R/\mathfrak{m}_R^i$ for each i , since we have the corresponding inequality on the dimensions of the subquotients of the obvious filtrations. So by linear algebra, the surjectivity of θ_i implies that equality holds, and that θ_i is an isomorphism, and in particular is injective.

□

Remark 6.2.3. We did not use the full strength of the infinitesimal lifting hypothesis. It is enough to assume that hypothesis holds when R is a finite local k -algebra, since that's all we used. We can also assume $J = (\epsilon)$ for some $\epsilon \in R$ satisfying $\epsilon \mathfrak{m}_R = 0$, since we can factor the general case $R \rightarrow R/J$ into a composition of maps of the form $R \rightarrow R/\epsilon \rightarrow R/(\epsilon, \epsilon') \rightarrow \dots \rightarrow R/J$.

Example 6.2.4. As an example of the usefulness of the infinitesimal criterion, we will rederive the Jacobian criterion for an affine hypersurface. Choose a nonzero $f \in k[x_1, \dots, x_n]$ and suppose $f(0, \dots, 0) = 0$. Note that $X = V(f)$ is smooth at 0 if and only if $\widehat{\mathcal{O}}_{X,0}$ is regular.

Claim. A sufficient condition for such regularity to hold is that $(\partial x_1 f, \dots, \partial x_n f)(0) \neq \vec{0}$.

We will show this by verifying the infinitesimal criterion. A map $\widehat{\mathcal{O}}_{X,0} \rightarrow R/J$, or the corresponding map $\varphi : A = k[x_1, \dots, x_n]/(f) \rightarrow R/J$, is specified by choosing $t_i = \varphi(x_i) \in \mathfrak{m}_R + J$ satisfying $f(t_1, \dots, t_n) = 0 \pmod{J}$. The claim is that we can lift this to a map $\tilde{\varphi} : A \rightarrow R$ under the Jacobian non-vanishing hypothesis. In other words, we need to find $\tilde{t}_i \in R$ lifting the $t_i \in R/J$ and satisfying $f(\tilde{t}_1, \dots, \tilde{t}_n) = 0$. First choose arbitrary lifts \tilde{t}'_i of t_i . So $f(\tilde{t}'_1, \dots, \tilde{t}'_n) \in J$. Set $\tilde{t}_i = \tilde{t}'_i + j_i$. We're trying to solve $f(\tilde{t}_1, \dots, \tilde{t}_n) = 0$ for j_i . The point is that by Taylor expanding, $f(\tilde{t}_1, \dots, \tilde{t}_n) = f(\tilde{t}'_1, \dots, \tilde{t}'_n) + \sum \partial_{x_i} f(0) j_i + O(J^2)$. The quadratic term vanishes since $J^2 = 0$. So we just need show that the map $J^n \rightarrow J$ defined by $\vec{j} \mapsto \sum \partial_{x_i} f(0) j_i$ is surjective, since then we can take \vec{j} to be something mapping to $-f(\tilde{t}'_1, \dots, \tilde{t}'_n) \in J$. But in fact it is surjective since $\partial_{x_i} f(0) \neq 0$ for some i .

7 January 22

7.1 More on forms

Definition 7.1.1. Let k be a field and X a finite type k -scheme. A k -form of X is a k -scheme X' of finite type such that $X'_k \simeq X_{\bar{k}}$. Equivalently (but not tautologically so), the condition is $X'_k \simeq X_k$ for some algebraically closed extension field K/k (so we can consider \mathbf{C}/\mathbf{Q} for example). Equivalently (but not tautologically so), the condition is that $X'_k \simeq X_k$ for some finite extension K/k .

This definition has an evident analogue for k -schemes with extra structure, like k -groups.

We saw already that every 1-dimensional connected linear algebraic k -group G is a form of \mathbf{G}_a or \mathbf{G}_m . In fact, we also saw refinements of this. On Homework 2 it is shown that if G is additive then in fact it splits (becomes isomorphic to \mathbf{G}_a) over a finite, purely inseparable extension k'/k . In the multiplicative case we saw that G splits over a finite separable extension.

The additive case is ill-behaved in the sense that there can be forms of \mathbf{G}_a with only a single rational point. The multiplicative case turns out to be much better. We'll see later that when k is infinite then when G is multiplicative, $G(k)$ is Zariski-dense. Really we'll show something stronger (over an arbitrary, even finite, field): if T is a torus then T is **unirational**. (Recall that a variety X over a field k is unirational if it admits a dominant rational k -map from an open subscheme of an affine space over k . This is equivalent to there being a k -embedding of the function field $k(X)$ into a rational function field $k(t_1, \dots, t_n)$.)

7.2 A loose end concerning smoothness

One thing not quite addressed by Theorem 6.2.1 is the sensitivity of the notion of smoothness to ground field extension. Here is a lemma to clear this up.

Lemma 7.2.1. *Let A be a local Noetherian k -algebra with residue field k . Let k'/k be a field extension. Let $\mathfrak{m}' = \ker(A \otimes_k k' \rightarrow k')$. Assume $A' = (A_{k'})_{\mathfrak{m}'}$ is Noetherian. Then A is regular if and only if A' is regular.*

Example 7.2.2. A ring which does *not* satisfy the hypotheses of Lemma 7.2.1 is $A = \mathbf{Q}[[x]]$ and $k' = \mathbf{C}$; i.e., $\mathbf{Q}[[x]] \otimes_{\mathbf{Q}} \mathbf{C}$ has non-noetherian local ring at the “origin”. This localization injects into $\mathbf{C}[[x]]$, but it is far from the whole thing. You only get power series whose coefficients all live in a finite dimensional \mathbf{Q} -subspace of \mathbf{C} .

Example 7.2.3. A ring which does satisfy the hypotheses of lemma 7.2.1 is $A = \mathcal{O}_{X,x} = B_{\mathfrak{m}}$ where $x \in X(k)$ is a rational point of a finite type k -scheme X , and x sits inside an open affine $\text{Spec } B \subset X$. **Exercise.** Show that $A' = (A_{k'})_{\mathfrak{m}'} = \mathcal{O}_{X_{k'},x'}$ where $x' = x \in X(k) \hookrightarrow X_{k'}(k')$.

An example of this situation is $A = \mathcal{O}_{G,e}$ and $A' = \mathcal{O}_{G_{k'},e'}$ for an algebraic k -group G .

Proof of Lemma 7.2.1. $A \rightarrow A'$ is a local map of local Noetherian rings, and it is flat since $A \rightarrow A_{k'}$ is, as it is a localization. So by the dimension formula (e.g. [CRT, §15]) we have $\dim A' = \dim A + \dim(A'/\mathfrak{m}A')$. But $\mathfrak{m}A' = \mathfrak{m}'$ so $\dim(A'/\mathfrak{m}A') = \dim(k') = 0$. Check that $k' \otimes_k \mathfrak{m}/\mathfrak{m}^2 \xrightarrow{\sim} \mathfrak{m}'/\mathfrak{m}'^2$ canonically. Hence by comparing the definitions of regularity, the lemma follows. \square

Corollary 7.2.4. *Let G be an algebraic k -group. Then the following are equivalent.*

- (i) G is smooth.
- (ii) $G_{\bar{k}}$ is regular.
- (iii) $\mathcal{O}_{G_{\bar{k}},e_{\bar{k}}}$ is regular.
- (iv) $\mathcal{O}_{G,e}$ is regular.
- (v) $\widehat{\mathcal{O}}_{G,e} = k[[x_1, \dots, x_n]]$.
- (vi) $\widehat{\mathcal{O}}_{G,e}$ satisfies the infinitesimal lifting criterion.

Proof. (i) is equivalent to (ii) by definition. (ii) is equivalent to (iii) by translating by $G_{\bar{k}}(\bar{k})$. (iii) is equivalent to (iv) by the lemma. (vi) is equivalent to (v) and (vi) by Theorem 6.2.1. \square

7.3 How to apply Grothendieck's smoothness criterion

Recall the infinitesimal lifting criterion for the smoothness of a complete local Noetherian k -algebra A with residue field k , from Theorem 6.2.1: it says that for all local Artin k -algebras (R, \mathfrak{m}) and all square zero ideals $J \triangleleft \mathfrak{m}$, and local k -map $f : A \rightarrow R/J$ can be lifted along $\pi : R \rightarrow R/J$ to a map $\tilde{f} : A \rightarrow R$ so that $f = \pi\tilde{f}$.

How should this criterion be interpreted? Loosely speaking, $A \simeq k[[x_1, \dots, x_n]]/(g_1, \dots, g_m)$ “for free”. The power series g_i can be evaluated at *nilpotent* elements of R , even though in general it does not make sense to evaluate a power series at an arbitrary element of a ring. So the map f above is nothing more than a solution to $\{g_i = 0\}$ in \mathfrak{m}/J , and \tilde{f} is a lift of it to a solution in \mathfrak{m} . Thus, the criterion is that A is a power series ring over k if and only if there are no obstruction to such lifting problems. Also bear in mind Remark 6.2.3, which says that the class of lifting problems we need to consider is actually quite narrow.

The following special case will be the most important one for us.

Example 7.3.1. Let X be a finite type k -scheme, $x \in X(k)$ a rational point, and $A = \hat{\mathcal{O}}_{X,x}$. Consider R as in the criterion. Since R is artinian, and in particular complete, by the universal property of completion, to give a local k -map $A \rightarrow R$ is the same as to give a local k -map $\mathcal{O}_{X,x} \rightarrow R$. By the universal property of the local ring $\mathcal{O}_{X,x}$, to give a local k -map $\mathcal{O}_{X,x} \rightarrow R$, or equivalently a map $\text{Spec } R \rightarrow \text{Spec } \mathcal{O}_{X,x}$, is the same as to give a map $\text{Spec } R \rightarrow X$ sending the closed point to x .

Thus we actually have a fairly “global” interpretation of the infinitesimal criterion in this situation, or at least one that can be viewed in terms of the functor of points of X : namely, we require that $X(R) \rightarrow X(R/J)$ surjects onto the points of $X(R/J)$ that lift $x \in X(k)$.

If $(X, x) = (G, e)$ for a k -group G , it follows that G is smooth if and only if $G(R) \rightarrow G(R/J)$ maps $\ker(G(R) \rightarrow G(k))$ surjectively onto $\ker(G(R/J) \rightarrow G(k))$.

7.4 How to show algebraic k -groups are smooth

Now we apply the method of Example 7.3.1 to show how one might prove that a k -group G is smooth and compute its tangent space, and hence (by smoothness) its dimension. It should be remarked that proving connectedness is an entirely separate issue!

The idea follows Example 7.3.1 closely. Take a k -finite Artin local ring R , and $J \triangleleft \mathfrak{m}$ a square zero ideal. Sometimes it will be computationally convenient to restrict to **small extensions** $R \twoheadrightarrow R/\epsilon$, i.e. we take $J = (\epsilon)$ with $\epsilon\mathfrak{m} = 0$. It might also be helpful to assume $R/\mathfrak{m} = k$. Then we will show that $G(R) \rightarrow G(R/J)$ is surjective, at least when we restrict to points lifting $e \in G(k)$. Next we compute $T_e(G)$, which as a set is $\mathfrak{g} = \ker(G(k[\epsilon]) \rightarrow G(k))$. However, that kernel will turn out to have a natural vector space structure, with addition coming from the group structure on G (whether or not G is commutative!) and a k -action from scaling ϵ . On Homework 4 it is shown that $T_e(G) = \mathfrak{g}$ as vector spaces, not just sets.

7.4.1 Smoothness of GL_n, SL_n in coordinates, via matrices

In fact $GL_n(R) \rightarrow GL_n(R/J)$ is surjective, which we can see as follows. Take $\overline{M} \in GL_n(R/J)$, and lift it entry-wise to $M \in Mat_n(R)$. Is M invertible? Yes, because $\det(M) \equiv \det(\overline{M}) \in (R/J)^\times \pmod{J}$. So $\det M = r + j$ and there exists r' so that $(r + j)r' = 1 + j'$ for $j' \in J$. Hence some multiple of $\det M$ is in $1 + \mathfrak{m} \subset R^\times$. So $\det M \in R^\times$.

Now $T_1(GL_n) = \ker(GL_n(k[\epsilon]) \rightarrow GL_n(k)) = \{1 + \epsilon M \mid M \in Mat_n(k)\} \simeq Mat_n(k)$ as an abelian group, since $(1 + \epsilon M)(1 + \epsilon M') = 1 + \epsilon(M + M') + O(\epsilon^2)$ and $\epsilon^2 = 0$; in fact the vector space structure is correct, as Homework 4 will address.

Also $SL_n(R) \rightarrow SL_n(R/J)$ is surjective; lift $\overline{M} \in SL_n(R/J)$ to $M \in GL_n(R)$. Suppose $\det M = a \in 1 + J \subset R^\times$. Adjust M to $\begin{pmatrix} a^{-1} & & \\ & 1 & \\ & & \ddots \\ & & & 1 \end{pmatrix} M$, which still lifts \overline{M} and has determinant 1.

Finally we compute $T_1(SL_n) = \{1 + \epsilon M \mid M \in Mat_n(k), \det(1 + \epsilon M) = 1\}$. Since $\det(1 + \epsilon M) = 1 + \epsilon \text{tr}(M)$, this shows that $\mathfrak{sl}_n = Mat_n(k)^{\text{tr}=0}$.

7.4.2 Smoothness of $GL(V), SL(V)$ without using coordinates (much)

This “functorial” method will lead to an intrinsic description of $\mathfrak{gl}(V), \mathfrak{sl}(V)$, which is useful because it is obviously functorial in V . When we have representations floating around, this functoriality will be a convenient way to avoid having to think too much.

For $GL(V)$, we ask whether $\text{Aut}_{\mathbf{R}}(V_{\mathbf{R}}) \rightarrow \text{Aut}_{\mathbf{R}/J}(V_{\mathbf{R}/J})$ is surjective. If $\bar{T} : V_{\mathbf{R}/J} \xrightarrow{\sim} V_{\mathbf{R}/J}$, observe that since these are free modules we can lift \bar{T} to an \mathbf{R} -endomorphism $T : V_{\mathbf{R}} \rightarrow V_{\mathbf{R}}$. It’s an automorphism because its determinant is a unit mod J , and so it is itself a unit.

For $SL(V)$ we do similarly, and exhibit an explicit element of $\text{Aut}_{\mathbf{R}}(V_{\mathbf{R}})$ with any determinant in $1 + J$ which is congruent to $1 \bmod J$. Just use the same matrix as in the previous example.

To do the tangent spaces, we compute $T_1(GL(V)) = \ker(\text{Aut}_{k[\epsilon]}(V_{k[\epsilon]}) \rightarrow \text{Aut}_k(V))$. Since

$$\text{Aut}_{k[\epsilon]}(V_{k[\epsilon]}) \subset \text{End}_{k[\epsilon]}(V_{k[\epsilon]}) = k[\epsilon] \otimes_{\mathbf{k}} \text{End}_{\mathbf{k}} V,$$

we have a natural ambient vector space. Observe that the kernel

$$\{1 + \epsilon T \mid T \in \text{End}_{\mathbf{k}}(V)\} = 1 + \epsilon k[\epsilon] \otimes_{\mathbf{k}} \text{End}_{\mathbf{k}}(V)$$

is naturally a k -affine linear subspace of $k[\epsilon] \otimes_{\mathbf{k}} \text{End}_{\mathbf{k}}(V)$, so by subtracting off 1 it gets a canonical vector space structure itself. Hence we can identify $\mathfrak{gl}(V) = \epsilon \text{End}_{\mathbf{k}}(V)$. Similarly, since $\det(1 + \epsilon T) = 1 + \epsilon \text{tr } T$ [which can be proved in a coordinate-free manner using exterior algebra, should one wish to do so] we obtain $T_1(SL(V))$ in similar fashion to be $\mathfrak{sl}(V) = \epsilon \text{End}_{\mathbf{k}}^0(V)$.

8 January 25

Our next goal will be to establish smoothness for other classical groups, the series C_n, B_n and D_n corresponding to symplectic groups $Sp(V, B)$ and orthogonal groups $O(q)$. Actually, we’ll do Sp and defer the orthogonal case to Appendix A (where we systematically incorporate characteristic 2). Before doing so, let us consider connectedness.

8.1 How to Show Connectedness

Example 8.1.1. $O(q)$ is actually always disconnected, scheme-theoretically. A prototypical example is $q = xy$ on $V = k^2$. Then $O(q) = \{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2 \mid (ax + by)(cx + dy) = xy \}$. These conditions are equivalent to $ac = bd = 0$ and $ad + bc = 1$. Over any local ring one can track units and show that $a = d = 0, bc = 1$ or $b = c = 0, ad = 1$. In generally these equations will define $O(q)$, Zariski-locally on $\text{Spec } R$ over any ring R . Thus $O(q) = SO(q) \sqcup SO(q) \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, i.e. $\{ \begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} \} \sqcup \{ \begin{pmatrix} 0 & b \\ b^{-1} & 0 \end{pmatrix} \}$.

The technique for proving a finite type k -group scheme G to be connected is the following.

1. Find a smooth, geometrically connected k -scheme X (usually not affine!) with a G -action $\alpha : G \times X \rightarrow X$.
2. Ensure the action is transitive on \bar{k} -points, i.e. $\alpha_{x_0} : G_{\bar{k}} \rightarrow X_{\bar{k}}$ should be surjective for $x_0 \in X(\bar{k})$.
3. Prove the stabilizer $\text{Stab}_{G_{\bar{k}}}(x_0)$ is connected.

Proposition 8.1.2. *Given 1-3 above, G is connected (and this holds if and only if $G_{\bar{k}}$ is connected).³*

Proof. Rename $k = \bar{k}$, and replace G with G_{red} so that it is smooth. Now G is regular and equidimensional of some dimension d (by translating a neighborhood of the origin!). The surjection $G \rightarrow X$ has equidimensional fibers all of the same dimension, since they are conjugates of $\text{Stab}_G(x_0)$. The base X is regular, hence irreducible of some pure dimension d' . Therefore all the fibers are of expected dimension $d - d'$. (This holds on a Zariski-open subset of X , by a classical fact; since all the fibers are conjugate - hence isomorphic - it holds everywhere.)

Now we invoke the Miracle Flatness Theorem [Mat, 23.1], which entails that $G \rightarrow X$ is flat, and hence open. By an easy topological argument, the existence of an open continuous surjection from a topological space Y onto a connected base with connected fibers entails that Y is connected. \square

³By Homework 1, Problem 3(i), a connected k -group G of finite type is automatically geometrically connected.

Remark 8.1.3. If G acts on X and $x \in X(k)$ then $\text{Stab}_G(x)$ is the scheme-theoretical fiber of α_x over x . Since it represents the stabilizer-subgroup functor of G , it follows that it is a subgroup scheme of G . But it might not be smooth! (In characteristic p , that is; everything is OK in characteristic 0, by a theorem of Cartier which says *all* k -group schemes locally of finite type are smooth when $\text{char}(k) = 0$.)

8.2 Connectedness of SL_n

Fix an n -dimensional vector space V and let $G = \text{SL}(V) \simeq \text{SL}_n$.

8.2.1 Method 1 - Flag varieties

For V a k -vector space of dimension $n > 0$, let X be the functor on k -algebras given by

$$R \mapsto X(R) = \{0 = F_0 \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots \subsetneq F_n = V_R \mid \\ F_i = \text{locally free } R\text{-submodule of } V_R \text{ of finite rank, } F_i/F_{i-1} = \text{locally free of rank } 1\}.$$

The following is standard (so we omit the proof):

Proposition 8.2.1. *X is representable by a smooth geometrically connected projective variety, covered by open sets isomorphic to affine spaces having non-empty overlaps.* \square

Let $\text{GL}(V)$ act on X in the obvious way. We can restrict this to an action $\alpha : \text{SL}(V) \times X \rightarrow X$.

Claim 8.2.2 (Exercise). *The map α is transitive on \bar{k} -points.* \square

Compute the stabilizer Stab in $\text{SL}(k^n)$ of the standard flag in k^n explicitly: we find as schemes

$$\text{Stab} = \left\{ \begin{pmatrix} a_1 & * & * & * & \cdots & * \\ 0 & a_2 & * & * & \cdots & * \\ 0 & 0 & a_3 & * & \cdots & * \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & a_{n-1} & * \\ 0 & 0 & \cdots & 0 & 0 & a_n \end{pmatrix} : \prod a_i = 1 \right\}$$

This is visibly isomorphic to $\mathbf{G}_m^{n-1} \times \mathbf{A}^{\binom{n}{2}}$ as a variety, and is thus irreducible and geometrically connected by inspection. So the method of the previous section will go through.

8.2.2 Method 2 - Projective Space

More naively, if you cannot guess what the right homogeneous space is, one can try to use a more obvious action of the linear group one is trying to prove connected, namely the action on \mathbf{P}^{n-1} if $G \subset \text{GL}_n$.

So give the geometrically connected, etc., variety \mathbf{P}^{n-1} the standard (transitive) action of SL_n . The stabilizer in this case is

$$\text{Stab}_{\text{SL}_n}([1 : 0 : \cdots : 0]) = \left\{ \begin{pmatrix} a & * & \cdots & * \\ 0 & x & \cdots & x \\ \vdots & \vdots & [g] & \vdots \\ 0 & x & \cdots & x \end{pmatrix} \mid a = \det g^{-1} \right\}.$$

Here the top row is arbitrary after the first entry; the x 's denote that the bottom right $(n-1) \times (n-1)$ block is given by $g \in \text{GL}_{n-1}$. Hence $\text{Stab}_{\text{SL}_n}([1 : 0 : \cdots : 0]) = \text{GL}_{n-1} \times \mathbf{A}^{n-1}$ as a variety. Again we get lucky and can see that it is connected, so we're done.

8.3 Smoothness of Sp_{2n}

Let $G = \text{Sp}_{2n} \simeq \text{Sp}(V, B)$ where V is an $2n$ -dimensional vector space over k and $B : V \times V \rightarrow k$ is a symplectic form. We will prove that G is smooth via the infinitesimal criterion. We will also use Remark 6.2.3 to reduce our work to the case where R is a local finite k -algebra with residue field k , $0 \neq \epsilon \in \mathfrak{m}_R$ satisfies $\epsilon \mathfrak{m}_R = 0$, and $J = \epsilon R$; we must prove $G(R) \twoheadrightarrow G(R/J)$.

Choose $\bar{T} \in \text{Aut}_{R/J}(V_{R/J})$ preserving $B_{R/J}$. We want to lift it to an element of $\text{Aut}_R(V_R)$ preserving V_R . In other words, \bar{T} satisfies $B_{R/J}(\bar{T}v, \bar{T}v') = B_{R/J}(v, v')$ for all $v, v' \in V_{R/J}$. But note that by R/J -bilinearity, this condition is completely determined by the fact that it holds for all $v, v' \in V \subset V_{R/J}$. In other words, the right side of the equation is “constant” in $k \subset R/J$.

Start by choosing any R -linear automorphism T of V_R lifting \bar{T} . We want to know whether $B_R(Tv, Tv') = B_R(v, v') \in R$, for all $v, v' \in V \subset V_R$. Probably this is not the case. But since T lifts \bar{T} , we know, at least, that $B_R(Tv, Tv') = B_R(v, v') \bmod J$. We shall contemplate the automorphisms $T + S$ for $S \in \text{Hom}_R(V_R, V_{\frac{R}{k}} \otimes_k J)$. These are precisely the lifts of \bar{T} . A choice of $S \in \text{Hom}_R(V_R, V_{\frac{R}{k}} \otimes_k J)$ is equivalent to a choice of $\epsilon S_0 \in \text{Hom}_k(V, V_{\frac{R}{k}} \otimes_k J)$ where $S_0 \in \text{End}_k(V)$. Any $S_1 \in \text{Hom}_k(V, V_{\frac{R}{k}} \otimes_k J)$ is automatically of the form ϵS_0 since $J = \epsilon R$ is a k -line (because $\epsilon m_R = 0$); we’re really using the fact that small extensions are small to make our life easier.

Now we calculate

$$B_R((T + \epsilon S_0)v, (T + \epsilon S_0)v') = B_R(Tv, Tv') + \epsilon(B_R(Tv, S_0v') + B_R(S_0v, Tv')).$$

Since $\epsilon m_R = 0$, the coefficient of ϵ , namely $B_R(Tv, S_0v') + B_R(S_0v, Tv')$, only matters mod m_R . Let $T_0 = \bar{T} \bmod m_R$. The ϵ -coefficient is $B(T_0v, S_0v') + B(S_0v, T_0v') \in k$. Thus the condition on S_0 for $T + \epsilon S_0$ to be our desired lift is that

$$\epsilon(B(T_0v, S_0v') + B(S_0v, T_0v')) = B(v, v') - B(Tv, Tv') =: \epsilon h(v, v') \in J = \epsilon R.$$

Here $h : V \times V \rightarrow k$ is defined uniquely by the condition that $B(v, v') - B(Tv, Tv') = \epsilon h(v, v')$. By inspection it is alternating and bilinear.

So we have reduced ourselves to a problem in linear algebra: is the map

$$\text{End}(V) \rightarrow (\wedge^2 V)^*$$

defined by $S_0 \mapsto [(v, v') \mapsto B(T_0v, S_0v') + B(S_0v, T_0v')]$ surjective, so that it must hit h ?

If $\dim_k V = 2n$ then $\dim_k \text{End}(V) = 4n^2$ and $\dim_k (\wedge^2 V)^* = \binom{2n}{2} = \frac{2n(2n-1)}{2} = n(2n-1)$. So we want the dimension of the kernel of the map above to be $n(2n+1)$.

What is the kernel? It is

$$\{S_0 \in \text{End}(V) \mid B(T_0v, S_0v') = -B(S_0v, T_0v') = B(T_0v', S_0v) \text{ for all } v, v' \in V\}.$$

In other words, it is

$$\{S_0 \in \text{End}(V) \mid [(v, v') \mapsto B(T_0v, S_0v')] \in (\text{Sym}^2 V)^*\}.$$

Since $T_0 \in \text{Sp}(V, B)$ is invertible, we can set $S_1 = T_0^{-1}S_0$; then the space above is the same as

$$\{S_1 \in \text{End}(V) \mid B((\cdot), S_1(\cdot)) \in (\text{Sym}^2 V)^*\}.$$

But $S_1 \mapsto B((\cdot), S_1(\cdot))$ gives an identification of $\text{End}(V)$ with $V^* \otimes V^* = (V \otimes V)^*$, since B is non-degenerate. Hence the space above is precisely $(\text{Sym}^2 V)^* \subset V^* \otimes V^*$ which has the correct dimension. QED

Finally, we can compute the Lie algebra \mathfrak{sp}_{2n} and determine $\dim \text{Sp}_{2n}$. As usual, we regard $T_1(\text{Sp}(V, B)) \subset T_1(\text{GL}(V)) = \mathfrak{gl}(V) = \text{End}(V)$. Then

$$\mathfrak{sp}_{2n} = \{1 + \epsilon T \in \text{Aut}_{k[\epsilon]}(V_{k[\epsilon]}) \mid T \in \text{End}(V), B((1 + \epsilon T)v, (1 + \epsilon T)v') = B(v, v') \text{ for all } v, v' \in V \subset V_{k[\epsilon]}\}.$$

We compute that the condition on T is that $B(Tv, v') + B(v, Tv') = 0$; i.e. $B(T(\cdot), (\cdot)) \in (\text{Sym}^2 V)^*$, since B is alternating. Hence $\mathfrak{sp}_{2n} = \mathfrak{sp}(B, V) = (\text{Sym}^2 V)^*$ identified as a subspace of $\text{End}(V)$ via B . Thus its dimension is

$$\dim \text{Sp}_{2n} = \frac{(2n)(2n+1)}{2} = n(2n+1).$$

Explicitly, \mathfrak{sp}_{2n} consists of $2n \times 2n$ block matrices $\begin{pmatrix} a & b \\ c & -a^t \end{pmatrix}$ such that $b = b^t, c = c^t$.

January 27

Sp_{2n} is connected

The goal for today is to prove the following result.

Theorem 8.3.1. *Let V be a vector space of dimension $2n \geq 0$ equipped with a nondegenerate alternating bilinear form B . Then the symplectic group $\mathrm{Sp}(V, B)$ is connected.*

The proof is by induction following the general strategy outlined earlier; the inductive step comes down to an exercise in (fairly delicate) linear algebra. If anything, it is an indication that **connectedness results for algebraic groups should be treated with respect!**

Proof. We induct on n . The case $n = 0$ is OK (alternatively, $n = 1$ is SL_2 , which we know is connected). Let $G = \mathrm{Sp}(V, B)$ act on \mathbf{P}^{2n-1} in the obvious way. After renaming \bar{k} as k , what we need to check is that (i) the action is transitive, and (ii) one stabilizer is connected.

For transitivity, choose two lines $ke, ke' \subset V$. We seek a symplectic automorphism g such that $g(ke) = ke'$. There are two cases.

Case 1: $B(e, e') \neq 0$. After rescaling e' we can take $B(e, e') = 1$. So $H = ke \oplus ke'$ is a **hyperbolic plane**; i.e. the restriction $B|_H$ is nondegenerate, or equivalently $B = H \oplus H^\perp$. So we can just take g to be the automorphism of V given by $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ on H and the identity on H^\perp . This swaps the lines and is easily seen to be symplectic.

Case 2: $B(e, e') = 0$. Since e and e' are (without loss of generality) linearly independent and B is nondegenerate, there exists a pair of hyperbolic planes H, H' containing e and e' respectively, which are orthogonal to one another; i.e. $V = W \oplus H \oplus H'$. Take g to be the automorphism of V which swaps H and H' , taking e and e' to one another, and fixes W . Thus transitivity is established.

For the connectedness of the stabilizer, fix a line $L \subset V$. We want $G_L = \mathrm{Stab}_G(L)$ to be connected. Since B is alternating, we have $L \subset L^\perp$, and L^\perp is a hyperplane in V . Let $\bar{V} = L^\perp/L$, which is a vector space of dimension $2(n-1)$. The form $B|_{L^\perp}$ descends (check!) to an alternating (check!) nondegenerate (check!) form on \bar{V} . Hence we get a k -group homomorphism $\xi: G_L \rightarrow \mathrm{Sp}(\bar{V}, \bar{B})$ sending $g \mapsto \bar{g} = g|_{L^\perp} \bmod L$.

Remark 8.3.2. If $\dim V = 2$ then $G_L = \left\{ \begin{pmatrix} a & * \\ 0 & a^{-1} \end{pmatrix} \right\} \simeq \mathbf{G}_m \times \mathbf{A}^1$ is connected.

By induction $\mathrm{Sp}(\bar{V}, \bar{B})$ is connected. If we knew that ξ were surjective with connected kernel then connectedness of G_L follows, completing the proof. Thus it remains only to show the following.

Claim 8.3.3. *ξ is surjective with connected kernel.*

For surjectivity, choose $L = ke \subset V$, and e' such that $B(e, e') = 1$ (by nondegeneracy) so that $H = ke \oplus ke'$ is hyperbolic and $V = H \oplus H^\perp$. Since $L^\perp (\supset H^\perp)$ surjects onto \bar{V} with kernel $L \subset H$, we get an injection $H^\perp \rightarrow \bar{V}$, which by dimension considerations is a symplectic isomorphism. So take any $\bar{g} \in \mathrm{Sp}(\bar{V}, \bar{B})$ and view it in $\mathrm{Sp}(H^\perp, B|_{H^\perp})$; extend it by the identity on H to get $g \in G_L$ which induces \bar{g} , i.e. such that $\xi(g) = \bar{g}$.

To describe the kernel $\ker \xi$, and in particular show it is connected, we will view its elements as $g = 1 + T$ for $T \in \mathrm{End}(V)$ and figure out the conditions on T which encode the defining properties (i) g is an automorphism, (ii) g fixes L , (iii) $g \in \ker \xi$, and (iv) g preserves B . Seeing that the result is connected appears, *a priori*, nontrivial, since while (i)–(iii) are Zariski-open or linear conditions, (iv) is a quadratic condition. But in fact, it will work out quite nicely. As motivation, consider a special case.

Example 8.3.4. Let $G = \mathrm{Sp}(k^2, B) = \mathrm{SL}_2$ and let $L = ke = L^\perp$. Then G_L is the Borel subgroup, which is of the form $\{1 + \begin{pmatrix} \lambda & b \\ 0 & -\lambda \end{pmatrix} \mid \lambda \neq -1\}$, which is quite tractable.

If we decompose $V = L^\perp \oplus ke'$, then $T: V \rightarrow V$ must satisfy some conditions: We have $S_0 = T|_L: L \rightarrow L$ is a scalar λ different from -1 (since g is an automorphism preserving L). We have $S = T|_{L^\perp}: L^\perp \rightarrow L^\perp$ since g preserves L^\perp (due to leaving B invariant) and induces the identity on \bar{V} , with $S|_L = S_0$ being multiplication by $\lambda \neq -1$ on the line L . Also, since g is an automorphism, so $g(e') \notin L^\perp$, necessarily $T(e') = ce' + \ell^\perp$ with $c \neq -1$.

We have shown that $g = 1 + T$ with $T = S \oplus T_0 : L^\perp \oplus ke' \rightarrow V$ for $S : L^\perp \rightarrow L$ restricting to multiplication by a scalar $\lambda \neq -1$ on L and $T_0 : ke' \rightarrow V$ carrying e' to $ce' + \ell^\perp$ for some scalar $c \neq -1$. Any such g is automatically an automorphism of V preserving L^\perp and L and inducing the identity on $\bar{V} = L^\perp/L$. What is the condition that such a g preserves B ?

Using the condition that $B(e, e') \neq 0$, the condition $B(ge, ge') = B(e, e')$ says exactly that $\lambda c + \lambda + c = 0$, or equivalently $(1 + \lambda)(1 + c) = 1$. So necessarily $c = -\lambda/(1 + \lambda)$ (an expression that cannot ever equal -1); cf. the example above. Assuming $c = -\lambda/(1 + \lambda)$ (with $\lambda \neq -1$), one can check that $\varphi_S : L^\perp \rightarrow k$ defined by $v \mapsto B(-cv - (1 + c)Sv, e)$ kills $L = ke$, and hence induces $\bar{\varphi}_S : \bar{V} \rightarrow k$. But we have the nondegenerate form \bar{B} on \bar{V} , so all functionals $\bar{\psi} \in \bar{V}^*$ have the form $\bar{B}(\bar{v}, \bar{x})$ for a unique $\bar{x} \in \bar{V}$. Hence, $\bar{\varphi}_S(\bar{v}) = \bar{B}(\bar{v}, \bar{x}_S)$ for a unique $\bar{x}_S \in \bar{V}$. Note that \bar{x}_S is determined by S since $c = -\lambda/(1 + \lambda)$ is determined by S (as $S(e) = \lambda e$).

It then follows (check!) that for the automorphism $g = 1 + (S \oplus T_0)$ [where T_0 is determined by ℓ^\perp since $c = -\lambda/(1 + \lambda)$], the condition that g preserves B is encoded by the condition that ℓ^\perp is a representative of $\bar{x}_S \in L^\perp/L$. Although the preceding description of $\ker \xi$ was written in terms of k -valued points, it works as written with k replaced by any k -algebra (provided we replace “ $\lambda \neq -1$ ” with “ $\lambda + 1$ is a unit”, and likewise for c , as we may do), so it defines a morphism $f : \ker \xi \rightarrow \text{Hom}(L^\perp, L)$ by $g \mapsto S$ that is surjective onto $\mathcal{U} := \{S \in \text{Hom}(L^\perp, L) \mid S|_L \text{ acts on } L \text{ through } -1 + \mathbf{G}_m\}$.

The fiber of f over a specific S consists of the L -coset of choices $\ell^\perp \in L^\perp$ representing $\bar{x}_S \in L^\perp/L$. More precisely, working with functors of points valued in k -algebras, we see that f is an L -torsor over \mathcal{U} for the Zariski topology, so in particular it is flat. Hence, connectedness of \mathcal{U} and of the geometric fibers implies connectedness of $\ker \xi$, which completes the proof. \square

9 January 29

9.1 A little more about Sp_{2n}

We proved $G = \text{Sp}(V, B)$ is connected. Here is a useful “matrix description” of the group, using our proof. Recall that we endowed $\mathbf{P}(V)$ with the natural action of $G \subset \text{GL}(V)$, chose a line $L \subset V$ spanned by $e \in V$, and took a complementary line $ke' \subset V$ so that $H = ke \oplus ke'$ is a hyperbolic plane; i.e. $B(e, e') = 1$. Then $L \subset L^\perp$, $V = L^\perp \oplus ke' = H \oplus H^\perp \simeq H \oplus L^\perp/L \simeq H \oplus \bar{V}$. The stabilizer G_L had the following structure, where the first two basis vectors are e, e' and the remainder parametrize $\bar{V} = H^\perp = L^\perp/L$:

$$\left\{ \begin{pmatrix} \alpha & * & [& S \in \text{Hom}(L^\perp/L, L) &] \\ 0 & \alpha^{-1} & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \square & [& [& [\cdots] &] &] \\ \vdots & \vdots & [& [& \vdots &] &] \\ \vdots & \bar{x}_S \in \bar{V} & [& [& [\bar{g} \in \text{Sp}(\bar{V}, \bar{B})] &] &] \\ \vdots & \vdots & [& [& \vdots &] &] \\ 0 & \square & [& [& [\cdots] &] &] \end{pmatrix} : \alpha = 1 + \lambda, \lambda \neq -1 \right\}$$

This description makes connectedness obvious, since visibly $G_L = (\mathbf{A}^1 - \{-1\}) \times \mathbf{A}^1 \times \mathbf{A}^{2n-2} \times \text{Sp}_{2n-2}$ and $\text{Sp}_2 = \text{SL}_2$.

Corollary 9.1.1 (of connectedness, or the matrix description). $\text{Sp}(V, B) \subset \text{SL}(V)$.

Proof. Recall that we know $\text{Sp}(V, B)$ is smooth and connected. For any geometric point $T \in \text{Sp}(V, B)$ we have $(\det T)^2 = 1$ from the equation which says T is symplectic. Hence $\det : \text{Sp}(V, B) \rightarrow \mathbf{G}_m$ factors through the finite group scheme $\mu_2 \subset \mathbf{G}_m$ on geometric points (even in characteristic 2). Thus, since $\text{Sp}(V, B)$ is smooth and connected, it follows that \det is trivial on $\text{Sp}(V, B)$.

Alternately, use the matrix description and argue by induction, row expanding along the second row. This says that $G_L \subset \text{SL}(V)$. Now you need to do a bit of work to check that this implies all of G has determinant 1, but it shouldn't be so bad. \square

9.2 Actions, Centralizers and Normalizers

Now we want to study actions of k -groups on k -schemes.

Definition 9.2.1. An *action* $\alpha : G \times X \rightarrow X$ is a map defined on the product of a finite type k -group G and a finite type k -scheme X , such that the induced map on S -points endows $X(S)$ with an action of $G(S)$ functorially in S [or even just in R as S ranges through $\text{Spec } R$ for k -algebras R]. Of course this is equivalent to another definition with diagrams expressing that the identity acts trivially and the action is “associative” in the usual sense.

The key example is when $X = G$ and α is multiplication (left translation). This will be crucial in proving that a linear algebraic k -group actually occurs as a closed subgroup scheme of some GL_n !⁴

Let $\alpha : G \times X \rightarrow X$ be a left action, and $W, W' \subset X$ closed subschemes, for example smooth.

Example 9.2.2. Take $X = G$ and α to be the conjugation action. Given $W = H \subset G = X$ a closed k -subgroup, asking whether H is normal amounts to asking whether it is preserved by the action.

This example motivates the following definition.

Definition 9.2.3. The *functorial centralizer* is

$$\underline{Z}_G(W) : R \mapsto \{g \in G(R) : g : X_R \rightarrow X_R \text{ is the identity on } W_R\}.$$

The *functorial transporter* is $\underline{\text{Tran}}_G(W, W') : R \mapsto \{g \in G(R) : g(W_R) \subset W'_R\}$. The *functorial normalizer* is $\underline{N}_G(W) = \underline{\text{Tran}}_G(W, W)$.

Proposition 9.2.4 (Homework 3). *If $W \subset X$ is geometrically reduced, then $\underline{Z}_G(W)$ and $\underline{N}_G(W)$ are representable by closed k -subgroup schemes $Z_G(W), N_G(W)$ of G .* \square

(The idea of the proof is to deduce the general case from the case $k = k_s$ by Galois descent. In the separably closed case, since W is geometrically reduced, W has a dense set of rational points, which allows one to prove representability quite easily.)

Example 9.2.5. Let $X = G$ be a smooth k -group of finite type, and α the conjugation action. Then $Z_G = Z_G(G)$ is the **scheme theoretic center** of G ; its R -points are

$$Z_G(R) = \{g \in G(R) \mid g \text{ conjugates trivially on } G_R\} = \{g \in G(R) \mid g \in Z(G(A)) \text{ for all } A \in \text{Alg}/R\}.$$

Example 9.2.6 (Homework 3). $Z_{\text{GL}_n} \simeq \text{GL}_1$ is the diagonal copy of \mathbf{G}_m . $Z_{\text{SL}_n} \simeq \mu_n \subset \text{GL}_1$ is the diagonal copy of the scheme of n th roots of unity. $Z_{\text{GL}_n}(T) = T$ where T is the diagonal torus. In particular $Z_{\text{GL}_n}(T)$ is smooth by inspection, which will turn out to be an instance of a more general phenomenon.

Example 9.2.7. When $k = \bar{k}$ is algebraically closed, we have $Z_G(W)(\bar{k}) = \{g \in G(\bar{k}) \mid g \text{ centralizes } W_{\bar{k}} \subset X_{\bar{k}}\}$. But since $W_{\bar{k}}$ is reduced and \bar{k} is algebraically closed, *in this case* the condition is the same as centralizing $W(\bar{k}) \subset X(\bar{k})$!

9.3 Closed orbit lemma

Example 9.3.1. Let $G = \mathbf{G}_m$ act on $X = \mathbf{A}^2$ by $t(x, y) = (tx, t^2y)$. We ask what the **G -orbits** of $X(k)$ are; i.e. what are the set-theoretic images of the orbit maps $G \rightarrow X : g \mapsto gx$ for $x \in X(k)$? It is not difficult to check that they consist of the x -axis minus the origin, the y -axis minus the origin, the parabolas $y = \lambda x^2$ for various $\lambda \neq 0$ (each minus the origin), and finally the origin itself. The observations one should make are that

1. All orbits are locally closed, smooth subschemes of X .

⁴Briefly, the idea is to have G act on itself by multiplication, endowing it with an action on its own coordinate ring, an infinite dimensional vector space, but with a certain exhaustive filtration by finite-dimensional G -stable subspaces. A sufficiently large one of these subspaces will contain all the generators of the algebra, and G will act faithfully on that subspace, producing the desired closed immersion that is a homomorphism too.

⁵It should be emphasized that the condition that $g \in G(R)$ be in $\underline{Z}_G(W)(R)$ is **much** stronger than that g act trivially on $W(R) \subset X(R)$!

2. The only closed orbit is $(0,0)$, and it is of minimal dimension among the orbits.

These properties turn out to generalize.

Remark 9.3.2. It must be emphasized that the rational points $\alpha_x(G)(k)$ of the set theoretic image of the action map $\alpha_x : G \rightarrow X : g \mapsto gx$ for $x \in X(k)$, may be much bigger than the set theoretic image $\alpha_x(G(k))$ of the rational points of G ! For example, $GL_1 \rightarrow GL_1$ given by squaring is surjective as a map of schemes, so its set theoretic image has lots of rational points. But for most fields, it is not close to being surjective on k -points!

Why do we care about the orbits of k -group actions? One reason is the following.

Example 9.3.3. Let $f : G \rightarrow G'$ be a k -homomorphism of smooth k -groups of finite type. Let $G \curvearrowright X = G'$ by left translation through the homomorphism f . The orbit of the identity $e' \in G'(k)$ is precisely the (set theoretic) image of f , as a subset of G' . In this case, at least over $k = \bar{k}$, all the orbits have the same dimension, since they are translates of one another. So if we knew that orbits of minimal dimension are closed (as we will see shortly) then it follows that the set theoretic image of f is a closed subset of G' , so it is the underlying space of the schematic image. But the schematic image is geometrically reduced, since G is smooth, and visibly a subgroup at the level of geometric points, so we conclude that the image of f is a smooth closed k -subgroup of G' (since any geometrically reduced k -group of finite type is smooth). See Corollary 9.3.6.

Remark 9.3.4. By the previous example, the image of a k -homomorphism of k -groups is a smooth closed k -subgroup. But there is much danger in conflating the k -points of the image with the image of the k -points – these are usually very different! For example, the projection $\pi : SL_n \rightarrow PGL_n$ is a degree n finite flat cover; in particular it is surjective. In some sense PGL_n deserves the name “ SL_n/μ_n ” because any μ_n -invariant map $SL_n \rightarrow X$ uniquely factors through π (proof later). But PGL_n is actually more like the sheafification of this quotient. However, traditionally this quotient is called PSL_n , which is “bad” notation because whereas the naive notion $PGL_n(k) := GL_n(k)/k^\times$ gives the points of the expected group scheme, $SL_n(k)/\mu_n(k)$ is usually not the k -points of anything interesting since as functor of the field k it tends to not even satisfy Galois descent. (The distinction is that Hilbert 90 holds for G_m but not for μ_n .)

Theorem 9.3.5 (Closed orbit lemma). *Let G be a smooth k -group of finite type⁶ and let $\alpha : G \curvearrowright X$ be an action of G on a finite type k -scheme X . Let $x \in X(k)$ be a rational point, and $\alpha_x : G \rightarrow X : g \mapsto gx$ the orbit map. Then the set theoretic image of α_x is locally closed, and with the reduced induced scheme structure it is smooth. Moreover if $k = \bar{k}$ then the orbits of minimal dimension are closed.*

Before we prove this, we record:

Corollary 9.3.6. *Let $f : G \rightarrow G'$ be a k -homomorphism of k -groups of finite type, and suppose G is smooth. Then $f(G)$ is closed and smooth.*

Proof of corollary. By the closed orbit lemma, $f(G) \subset \overline{f(G)}$ is an inclusion of an open subset into a closed subscheme [this is a defining property of locally closed subschemes]. Since schematic image for a finite type map commutes with flat base change, the formation of both sides commutes with scalar extension of k (and equality can be tested after such an extension). So we can assume without loss of generality that $k = \bar{k}$, and thus the last part of the closed orbit lemma gives the result. \square

9.4 Start of proof of closed orbit lemma (Theorem 9.3.5)

The first step is to reduce to the case where k is separably closed. Because G is smooth, so reduced, the formation of $\alpha_x(G)$ with the reduced induced scheme structure (i.e. the formation of the “schematic” or “scheme theoretic” image) is the same as the formation of the kernel of the map of sheaves $\mathcal{O}_X \rightarrow (\alpha_x)_* \mathcal{O}_G$. Since pushforward of quasicoherent sheaves commutes with flat base change, it commutes with extension of scalars. So the formation of the closure of the orbit of $x \in X(k)$ commutes with scalar extension.

The statement that the orbit $\alpha_x(G)$ itself is locally closed in G' is the same as the statement that the subset $\alpha_x(G) \subset \alpha_x(G)$ is an open subset. The formation of the set theoretic image always commutes with scalar extension, in the appropriate sense that the set theoretic image $\alpha_x(G_{k'})$ is the preimage in $G_{k'}$ of $\alpha_x(G) \subset G'$. Thus by Galois descent, it is enough to work over $k = k_s$.

⁶Not necessarily connected!

10 February 1

10.1 Conclusion of proof of closed orbit lemma (Theorem 9.3.5)

Above we reduced the proof to the case $k = k_s$. By Homework 2, problem 5(iii), we thus have $G(k)$ dense in G . By Theorem 3.2.1 this means that $G(k)$ is dense in G_K for all field extensions K/k .

The next step is to reduce to the case when the orbit map $\alpha_x : G \rightarrow X$ is dominant, so that $X = \overline{\alpha_x(G)}$ with the reduced structure.

Let $Y = \overline{\alpha_x(G)}$ with its reduced structure, i.e. the scheme theoretic image of α_x . Since $G(k) \subset G$ is dense, $Y = \overline{\alpha_x(G(k))}$. Moreover Y is geometrically reduced by Proposition 3.2.4. Finally, since $\alpha_x(G(k))$ is stable under translation by $G(k)$, so is Y ; i.e. the group action $G(k) \curvearrowright X$ restricts to a group action $G(k) \curvearrowright Y$. To reduce to the case $X = Y$ we need to show that the action $\alpha : G \times X \rightarrow X$ also restricts to an action $G \times Y \rightarrow Y$, which is a much stronger statement:

$$\begin{array}{ccc} G \times Y & \xrightarrow{\exists?} & Y \\ \downarrow & \searrow \varphi & \downarrow \\ G \times X & \xrightarrow{\alpha} & X \end{array}$$

The existence of such a dotted map can be checked by showing that $\varphi^\sharp : \mathcal{O}_X \rightarrow \varphi_* \mathcal{O}_{G \times Y}$ kills the quasicoherent ideal sheaf $\mathcal{I}_Y \subset \mathcal{O}_X$. To check this factorization we can extend scalars to \bar{k} . Since $Y_{\bar{k}}$ is reduced, as is $G_{\bar{k}} \times Y_{\bar{k}}$, it's enough to check on \bar{k} -points. The upshot is that it's enough to check that $G(\bar{k})$ acting on $Y(\bar{k}) \subset X(\bar{k})$ stays inside $Y(\bar{k})$; i.e., for all $y \in Y(\bar{k})$ we want $G(\bar{k})y \subset Y(\bar{k})$. In other words, for all $y \in Y(\bar{k})$ we want $\alpha_y : G_{\bar{k}} \rightarrow X_{\bar{k}}$ to land in the closed, reduced subscheme $Y_{\bar{k}}$. By topology, it's enough to check that $G(k) \subset G_{\bar{k}}$ (which is a dense subset) lands in $Y_{\bar{k}}$. Since $Y \subset X$ is $G(k)$ -stable, so is $Y_{\bar{k}} \subset X_{\bar{k}}$. So we have completed the reduction.

Now we can assume X is geometrically reduced, and $\alpha_x : G \rightarrow X$ is dominant (in fact, $G(k)x \subset X(k)$ is dense). We need to prove $\alpha_x(G)$ is open and smooth to conclude the first statement of the closed orbit lemma. Actually, this will give the second statement as well. Because if α_x is not surjective, then its closed G -stable (!) complement has smaller dimension. If $k = \bar{k}$ we can choose a rational point in the complement and look at its orbit, which will thus have smaller dimension (since the complement of a dense open subset of a finite type k -scheme always has strictly smaller dimension). Thus the only way the orbit of x could have been of minimal dimension is if it is closed (since the above reduction steps replaced the original X with a certain *closed* subset).

To prove that the subset $\alpha_x(G) \subset X$ is open, first observe that since $k = k_s$, $\pi : X_{\bar{k}} \rightarrow X$ is a homeomorphism, and $\pi^{-1}\alpha_x(G) = (\alpha_x)_{\bar{k}}(G_{\bar{k}}) \subset X_{\bar{k}}$ (exercise). So it's enough to work over \bar{k} .

Chevalley's constructibility theorem says that $\alpha_x(G)$ is constructible in X . We've rigged it to be dense. A dense constructible set contains a dense open set of the ambient space. (Obvious if you think about constructible sets as finite unions of locally closed subsets.) Now over $k = \bar{k}$, to show a constructible set $\Sigma \subset X$ is open, it's enough to show that $\Sigma(k) \subset X(k)$ is open in the Zariski topology. Since $k = \bar{k}$, $\alpha_x(G)(k) = \alpha_x(G(k)) = G(k)x \subset X(k)$. Since $\alpha_x(G)(k)$ contains $U(k)$ for a dense open $U \subset X$, and since $G(k)x$ is homogeneous, we conclude that $\alpha_x(G)(k) = \bigcup_{g \in G(k)} gU(k)$, and this is visibly open in $X(k)$.

It remains only to prove that the open subset $\alpha_x(G) \subset X$ is smooth with the open subscheme structure. Since $\alpha_x(G) = \overline{\alpha_x(G(k))}$ is geometrically reduced, it is smooth on a dense open. Consider $\alpha_x : G \rightarrow \alpha_x(G)$. If we base change to \bar{k} we obtain $(\alpha_x)_{\bar{k}} : G_{\bar{k}} \rightarrow (\alpha_x(G))_{\bar{k}}$, where the target is the image of the orbit map for x on $X_{\bar{k}}$. Hence without loss of generality we can assume $k = \bar{k}$. Now $G(k) \rightarrow \alpha_x(G)(k)$ is a surjection, i.e. $\alpha_x(G)(k) = G(k)x$, so $G(k)$ acts transitively on $\alpha_x(G)(k)$, so if there exists one smooth k -point then all k -points are smooth. (Alternately, the $G(k)$ -orbits of a smooth dense open cover the space.) This completes the proof of the closed orbit lemma.

Example 10.1.1. Let G be a smooth k -group of finite type, and suppose we have a representation, i.e. a k -homomorphism $G \rightarrow GL(V)$ for a finite dimensional k -vector space V . Then the image is a smooth closed k -subgroup of $GL(V)$.

10.2 Criterion for a k -homomorphism of k -groups to be a closed immersion

Proposition 10.2.1. *Let $f : G \rightarrow G'$ be a homomorphism of finite type k -groups. Suppose G is smooth. Then $T_e \ker f = \ker(T_e f)$ and the following are equivalent:*

- (i) $\ker f = 1$ (trivial as a scheme, not just rationally!).
- (ii) f is injective on geometric points and $T_e(f)$ is injective.
- (iii) f is a closed immersion.

We will prove this next time. Note that there are no smoothness hypotheses on $\ker f$.

11 February 3

11.1 Proof of Proposition 10.2.1

Remark 11.1.1. In practice, condition (iii) of Proposition 10.2.1 is the desired conclusion; often (ii) is easiest to check. However, to prove that a smooth linear algebraic k -group is a closed k -subgroup of some GL_n , we will actually verify (i).

First we will prove the claim about the tangent space of the kernel. Let $H = \ker f$. Then we have a commutative diagram

$$\begin{array}{ccccccc}
 & & 1 & & 1 & & 1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & T_e(\ker f) & \longrightarrow & T_e G & \xrightarrow{T_e(f)} & T_e G' \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & H(k[\epsilon]) & \longrightarrow & G(k[\epsilon]) & \longrightarrow & G'(k[\epsilon]) \\
 & & \downarrow & & \downarrow & & \downarrow \\
 1 & \longrightarrow & H(k) & \longrightarrow & G(k) & \longrightarrow & G'(k)
 \end{array}$$

The columns and the bottom two rows are exact. By a diagram chase, the top row is exact. By Homework 4, the group structures on the top rows are really the (additive structures of) the vector space structures of the tangent space. So we are done.

(iii) \Rightarrow (ii) is clear.

(ii) \Rightarrow (i): As above set $H = \ker f$. By hypothesis $H(\bar{k}) = 1$, so H is artin local; say $H = \text{Spec } A$ for an artin local ring (A, \mathfrak{m}) with residue field k . (The closed point is rational because we know H contains the identity!) In particular, the maximal ideal \mathfrak{m} is nilpotent. By the injectivity of $T_e f$, we have $(\mathfrak{m}/\mathfrak{m}^2)^* = T_e(H) = \ker(T_e f) = 0$ by the above. So $\mathfrak{m} = \mathfrak{m}^2$ and hence (by nilpotence) $\mathfrak{m} = 0$, so $H = \text{Spec } k$ is just the identity with no fuzz.

(i) \Rightarrow (iii): This is the interesting part. We have a diagram

$$\begin{array}{ccc}
 G & \xrightarrow{f} & G' \\
 & \searrow & \uparrow \text{cl.imm} \\
 & & f(G)
 \end{array}$$

The image $f(G)$ [set theoretic!] is a closed k -subgroup of G' (smooth, with the reduced structure) by the Closed Orbit Lemma 9.3.5, or more precisely by Corollary 9.3.6. The map $G \twoheadrightarrow f(G)$ has trivial kernel, because functorially we know its kernel is contained in $\ker f$, which is trivial by hypothesis. Hence it is enough to show that $G \twoheadrightarrow f(G)$ is an isomorphism.

So we have a new setup; the proof of the following claim will complete the proof of Proposition 10.2.1.

Lemma 11.1.2. *Let $f : G \rightarrow G'$ be a surjective k -homomorphism of smooth, finite type k -groups, with $\ker f = 1$. Then f is an isomorphism.*

Proof. We can assume without loss of generality (Homework 2) that $k = \bar{k}$.

Both G and G' are equidimensional because they are groups, so homogeneous. Say G has pure dimension d , and G' has pure dimension d' . Consider the map $G^0 \rightarrow G'^0$. Since G has finitely many connected (= irreducible!) components, it's automatic that $G^0 \rightarrow G'^0$ is surjective; this follows from the closedness of the image and dimension considerations, since if G^0 didn't fill up G'^0 its image would have strictly smaller dimension than d' , and hence the finitely many translates of the image, i.e. the entirety of $f(G)$, could not fill up G'^0 , a contradiction since f is surjective.

All the fibers of $G^0 \rightarrow G'^0$ over k -points are one-point sets, because they are conjugates of $\ker f = 1$. Because fiber dimension behaves correctly over a dense open subset of the base, and because $k = \bar{k}$ we can find a rational point in such a dense open, it follows that $d = d'$.

Because k is algebraically closed, the finiteness of the k -fibers thus entails the finiteness of all fibers; if $x \mapsto y$ we therefore have $[k(x) : k(y)] < \infty$, and hence $\text{trdeg}_k k(x) = \text{trdeg}_k k(y)$ over k . Consequently the generic points of G surject onto the generic points of G' , and this restricted set-map gives us the full fibers of f over the generic points.

Claim 11.1.3. *There exists a dense open $U' \subset G'$ such that $f^{-1}U' \rightarrow U'$ is finite flat.*

Proof of claim. We use the method of “spreading out” from generic points. Pass to the local ring $\mathcal{O}_{G', \eta'} = k(\eta')$ for a generic point $\eta' \in G'$. Then $\emptyset \neq \coprod_{\eta \in f^{-1}(\eta')} \text{Spec } k(\eta) = f^{-1}(\eta') \rightarrow \{\eta'\}$ is finite, because it is quasifinite and quasifiniteness implies finiteness over a field (i.e., the fiber $f^{-1}\eta'$ is a localization of \mathcal{O}_G , so it is just the reduced product of the function fields of the generic points of G over η' .) Finite implies finite flat, over a field. By general nonsense, viewing $\mathcal{O}_{G', \eta'} = \varinjlim_{\text{affine } U' \ni \eta'} \mathcal{O}_{G'}(U')$, the property of finite flatness thus spreads out to an actual open set containing η' . Doing this for all the generic points η' of G' gives the claim. (Actually all we'll need is any nonempty open set, but we might as well get a dense one.) \square

Returning to the proof of the lemma, we will now use the group structure to translate the finite flatness of f to the whole of G' .

Since $k = \bar{k}$ we can cover G' by $G'(k)$ -translates over U' . Moreover, again because $k = \bar{k}$, $G'(k) = f(G(k))$ since a surjective map of varieties over an algebraically closed field is surjective on closed points. The property of being finite flat of a given rank is local on the base, and passes through pullback along an automorphism of the base. So these translations by points of $f(G(k))$ give that $f : G \rightarrow G'$ is actually finite flat of constant rank r . Since we know $f^{-1}(e') = \ker f = \text{Spec } k$ by hypothesis (i), in fact the rank $r = 1$. In other words, $f_*\mathcal{O}_G$ is an invertible sheaf on G' .

Since finite morphisms are affine, we are now reduced to the following algebra problem:

Claim 11.1.4. *If $A \rightarrow B$ is a ring map making B an invertible A -module, then it is an isomorphism.*

Proof. This can be checked on stalks on $\text{Spec } A$. At a prime $\mathfrak{p} \in \text{Spec } A$ the map $A_{\mathfrak{p}} \rightarrow B_{\mathfrak{p}}$ makes $B_{\mathfrak{p}}$ a free $A_{\mathfrak{p}}$ -module of rank 1. On the other hand, it is a local ring homomorphism, and in particular $1 \mapsto 1$. Since $B_{\mathfrak{p}} \neq 0$ (it is of rank 1) we must have $1 \neq 0$. Therefore the image of 1 generates the 1-dimensional $A_{\mathfrak{p}}/\mathfrak{p}A_{\mathfrak{p}}$ -vector space $B_{\mathfrak{p}}/\mathfrak{p}B_{\mathfrak{p}}$. Thus by Nakayama $A_{\mathfrak{p}} \rightarrow B_{\mathfrak{p}}$ is surjective, and in fact $B_{\mathfrak{p}}$ is generated over $A_{\mathfrak{p}}$ by 1. Since $B_{\mathfrak{p}}$ is free, this means the map is injective as well. \square

The previous claim completes the proof of the lemma. \square

This finishes the proof of Proposition 10.2.1.

Remark 11.1.5. (i) \Leftrightarrow (iii) is actually true *sans* smoothness hypotheses; see [SGA3, VI_B, 1.4.2]. In the following when we parenthesize a hypothesis (smooth) we mean that the result is true without that hypothesis, but for our purposes we only need the smooth case, and that it rests upon Proposition 10.2.1 (which we only proved in the smooth case, but is true more generally).

11.2 Embedding linear algebraic groups in GL_n

Does a (smooth) affine k -group G of finite type admit a closed immersion into GL_n as a k -subgroup for some n ? The answer is yes. The method will be to study “ G acting on the coordinate ring $k[G]$ ”.

We have the following.

Corollary 11.2.1 (of Proposition 10.2.1). *Let G be a (smooth) k -group of finite type. Then the data of closed immersion $\rho : G \hookrightarrow GL(V)$ which is a k -homomorphism is equivalent to the data of a faithful⁷ R -linear action of $G(R)$ on V_R , functorial in R .* \square

We will find the desired representation (V, ρ) inside $k[G]$.

Remark 11.2.2. “ $GL(W)$ ” doesn’t really make sense if $\dim W = \infty$.

To get around the infinite dimension issue, we make the following definition.

Definition 11.2.3. A functorial linear representation of a k -group G on a (possibly infinite dimensional) k -vector space V is an R -linear action of $G(R)$ on V_R , which is functorial in the k -algebra R . That is, it is a map of group functors $\underline{G} \rightarrow \underline{\text{Aut}}(V)$. We say a subspace $W \subset V$ of a functorial linear representation V of G , is G -stable if the action of $G(R)$ on V_R restricts to a functorial action of $G(R)$ on W_R for all R .

Example 11.2.4. If X is affine and $G \times X \rightarrow X$ is a left action, we have a group action of $G(R) \curvearrowright X_R$ for all R , and hence a *right* action $G(R) \curvearrowright \mathcal{O}(X_R) = \mathcal{O}(X) \otimes_k R$. We turn this into a functorial linear representation (i.e. a left action) by setting $g.f = f \circ (\text{act}_{g^{-1}})$.

Example 11.2.5. Let $X = G$ be affine in the previous example, with the action of left multiplication λ . Then $g.f = f \circ \lambda_{g^{-1}}$ for $g \in G(R)$, $f \in R[G]$.

12 February 5

12.1 Actions of affine finite type k -groups on coordinate rings of affine k -schemes

Consider the following setup. Let G be an affine k -group of finite type, and $\alpha : G \times X \rightarrow X$ a left action on an affine k -scheme X .

This implies that $V = k[X]$ is a functorial linear representation of G in the sense of Definition 11.2.3; explicitly, $g \in G(R)$ acts on $f \in R[X] = R \otimes_k \mathcal{O}_X(X)$ by $(g.f)(x) = f(g^{-1}x) = f(\alpha(g^{-1}, x))$ for x any point of $X_R(A)$ and A any R -algebra.

Theorem 12.1.1. *The G -stable finite dimensional k -subspaces $W \subset V = k[X]$ form a directed system under inclusion and exhaust V .*

Remark 12.1.2. As usual, it’s worth emphasizing that the G -stability of $W \subset V$ is much stronger than saying that W is $G(k)$ -stable. It says rather that W_R is $G(R)$ -stable in V_R for all k -algebras R .

12.1.1 Application to embedding a smooth linear algebraic group into GL_n

Take $X = G$ and α left multiplication, so that $f \in R[G]$, $g \in G(R)$, we have $(g.f)(g') = f(g^{-1}g')$ for $g' \in G(R')$, R' an R -algebra.

Choose a finite set of k -algebra generators for $k[G]$. By Theorem 12.1.1 there exists a G -stable finite dimensional subspace $W \subset k[G]$ containing all those generators. Consider the resulting k -homomorphism $\rho : G \rightarrow GL(W)$ arising from the action of $G(R)$ on W_R functorially in the k -algebra R .

Claim 12.1.3. *$\ker \rho = 1$, i.e. ρ is injective on R -points for all R .*

⁷Meaning $(\ker \rho)(R) = 1$ for all k -algebras R .

Proof. We want to prove that $G(R)$ acts on W_R faithfully, i.e. if $g \in G(R)$ acts trivially on W_R then $g = 1$. Observe that $g \curvearrowright R[G] = V_R$ as an R -algebra automorphism. But W_R contains a set of R -algebra generators, so $g \curvearrowright R[G]$ trivially. In other words, $f(g') = f(g^{-1}g')$ for all $f \in R[G], g' \in G(R'), R' \in \text{Alg}/R$. Take $g' = 1, R' = R$; this gives $f(g^{-1}) = f(1)$ for all $f \in R[G]$. But this means that g^{-1} corresponds to the map of rings $(g^{-1})^* : R[G] \rightarrow R$ given by $f \mapsto f(g^{-1}) = f(1)$; thus g^{-1} coincides with e as maps $\text{Spec } R \rightarrow G_R$, since they coincide on coordinate rings.⁸ Therefore $g^{-1} = e$ so $g = e$. \square

The previous claim immediately yields the following, via Proposition 10.2.1.

Corollary 12.1.4. *If G is a (smooth)⁹ finite type affine k -group, then there exists a k -homomorphism $\rho : G \hookrightarrow \text{GL}(W)$ that is a closed immersion, with W some finite-dimensional k -vector space.* \square

12.2 Proof of Theorem 12.1.1

Observe that if $W_1, \dots, W_n \subset k[X] = V$ are G -stable subspaces, so is their sum $\sum W_i \subset V$. So it's enough to pick any $w \in V$ and show that there exists a finite dimensional G -stable subspace $W \subset V$ such that $w \in W$.

The action $\alpha : G \times X \rightarrow X$ corresponds to a map $\alpha^* : k[X] \rightarrow k[G] \otimes_k k[X]$. Let $\alpha^*(w) = \sum f_i \otimes h_i$; we can arrange so that the set $\{f_i\} \subset k[G]$ is k -linearly independent. Concretely, if R is a k -algebra, R' is an R -algebra, $g \in G(R), x \in X(R')$, then we have

$$(g.w)(x) = w(g^{-1}.x) = w(\alpha(g^{-1}, x)) = (\alpha^*w)(g^{-1}, x) = \sum f_i(g^{-1})h_i(x);$$

by Yoneda's lemma, this implies that $g.w = \sum f_i(g^{-1})h_i \in R[X]$ since they have the same values at all R -algebra valued points x .

By the previous calculation, for example, we have $w = 1.w = \sum f_i(1)h_i \in \text{Span}\{h_i\}$.

Claim 12.2.1. $W := \text{Span}\{h_i\} \subset V$ is G -stable.

Consider the following diagram.

$$\begin{array}{ccc} k[X] & \xrightarrow{\alpha^*} & k[G] \otimes_k k[X] \\ \uparrow & & \uparrow \\ W & \xrightarrow[\exists?]{-} & k[G] \otimes_k W \end{array}$$

Suppose the dotted map exists. Then for all $w' \in W$ and $g \in G(R)$, $g.w' = \sum (R\text{-coeff.s}) \cdot w_i$ for $w_i \in W$; so $G(R) \cdot W_R \subset W_R$, which proves G -stability as claimed.¹⁰

To prove the existence of such a map, we will use the associativity of the left action α :

$$\begin{array}{ccc} G \times G \times X & \xrightarrow{1 \times \alpha} & G \times X \\ m \times 1 \downarrow & & \downarrow \alpha \\ G \times X & \xrightarrow{\alpha} & X \end{array} \tag{†}$$

We need to compute $\alpha^*(h_i) \in k[G] \otimes_k k[X]$; we hope $\alpha^*(h_i) = \sum_j \varphi_{ij} \otimes h_j$. We will instead work inside

⁸This is where we use that G is affine, crucially!

⁹cf. Remark 11.1.5

¹⁰The G -stability of W also *implies* the existence of a dotted map, but we won't need this.

$k[G] \otimes_k k[G] \otimes_k k[X]$. We compute:

$$\begin{aligned}
\sum f_i \otimes \alpha^* h_i &= (\mathbf{1} \otimes \alpha^*) \left(\sum f_i \otimes h_i \right) \\
&= (\mathbf{1} \otimes \alpha^*)(\alpha^* w) \\
&\stackrel{(\dagger)}{=} (m^* \otimes \mathbf{1})(\alpha^* w) \\
&= (m^* \otimes \mathbf{1}) \left(\sum f_i \otimes h_i \right) \\
&= \sum (m^* f_i) \otimes h_i.
\end{aligned}$$

Now $k[G]$ has a k -basis $\{f_j\} \sqcup \{b\}_{b \in B}$, since we chose the $\{f_j\}$ to be linearly independent. Expand $m^* f_i$ with respect to this basis in the first factor:

$$m^*(f_i) = \sum_j f_j \otimes \varphi_{ij} + \sum_{b \in B} b \otimes \varphi_{ib}.$$

Then the computation above gives

$$\sum_i f_i \otimes \alpha^* h_i = \sum_j f_j \otimes \left(\sum_i \varphi_{ij} \otimes h_i \right) + \sum_b b \otimes \left(\sum_i \varphi_{ib} \otimes h_i \right).$$

But $\{f_i\} \sqcup \{b\}$ is a basis. Hence comparing both sides of the equation above says that $\sum_b b \otimes (\sum_i \varphi_{ib} \otimes h_i) = 0$ and $\alpha^* h_i = \sum_j \varphi_{ij} \otimes h_j$ for each i , as desired. This completes the proof of the claim above, and hence of Theorem 12.1.1. \square

13 February 8

13.1 Jordan decomposition

For $g \in GL_n(\bar{k})$ we have a **multiplicative Jordan decomposition**:

$$g \stackrel{!}{=} g_{ss} g_u \stackrel{*}{=} g_u g_{ss}$$

where g_{ss} is semisimple as an operator on \bar{k}^n (which is the same as diagonalizable, since we are over an algebraically closed field) and g_u is unipotent (meaning that $g_u - 1 \in \text{Mat}_n(\bar{k})$ is nilpotent).

Remark 13.1.1. If k is perfect then $T \in \text{End}_k(V)$ [for a finite dimensional k -vector space V] is semisimple if and only if $T_{\bar{k}} \curvearrowright V_{\bar{k}}$ is semisimple.

Remark 13.1.2. We used the identification $GL_n = \text{Mat}_n^\times$ to define unipotence.

We would like to generalize the Jordan decomposition to any smooth affine k -group, functorially in G .

Remark 13.1.3. Due to the uniqueness of Jordan decomposition over $k = \bar{k}$, by Galois descent we obtain a multiplicative Jordan decomposition in $GL_n(k)$ for any *perfect* field k ; this is also invariant under further extension of the ground field. However a good theory of Jordan decomposition for imperfect fields is basically hopeless, since while one can (in fact) prove that such a decomposition exists and is unique, a semisimple operator on a vector space over an imperfect field may no longer be semisimple after making an inseparable field extension; see Appendix B for more on this. Thus in the imperfect case, the Jordan decomposition is not compatible with scalar extension and hence works poorly.

The idea for how to obtain our generalization is to make use of a closed embedding $i : G \hookrightarrow GL_n$, which we know exists by our previous results. Take $g \in G(\bar{k})$, which gives $i(g) \in GL_n(\bar{k})$, and hence $i(g)_{ss}, i(g)_u \in GL_n(\bar{k})$ which are semisimple and unipotent, respectively.

There are two problems:

- (i) We must show $i(g)_{ss} = i(g_{ss}), i(g)_u = i(g_u)$ for some $g_{ss}, g_u \in G(\bar{k})$, independent of the choice of embedding i .

- (ii) We must establish the functoriality of this construction, and hopefully find an internal characterization which does not reference the GL_n at all.

To avoid the issues of imperfect fields, assume throughout the following that $k = \bar{k}$. (At the end we will make definitions over k by passage to \bar{k} .) For $g \in G(k)$, $g \curvearrowright G$ by *right* translation ρ_g ; this gives rise to the **right regular representation** $\rho_g : k[G] \xrightarrow{\sim} k[G]$ which sends a function f to $\rho_g f$ where $(\rho_g f)(x) = f(xg) = f \circ \rho_g(x)$ for $x \in G(R)$ for any k -algebra R ; this is a left action, as one can easily compute.

Now $k[G] = \varinjlim W$ where the filtered direct limit is over finite-dimensional $G(k)$ -stable subspaces W . The action ρ_g restricts to an action $\rho_g|_W \in GL(W)(k)$ on each piece W . Thus we obtain a multiplicative Jordan decomposition

$$\rho_g|_W = (\rho_g)_{ss,W} \cdot (\rho_g)_{u,W}$$

into commuting semisimple (resp. unipotent) operators on W . To work with this as W varies, we now briefly digress for some elementary generalities.

Let T_{ss}, T_u be a semisimple and a unipotent operator, respectively, on a vector space V . If V' (resp. V'') is a T -invariant subspace (resp. quotient with an induced T -action), then the restriction of the T -action (resp. induced T -action) on V' (resp. V'') is also semisimple or unipotent for $T = T_{ss}$ or $T = T_u$. In a pithy catchphrase, semisimplicity and unipotence are well-behaved with respect to subquotients. Obviously if two operators on V commute then the restricted (resp. induced) operators on V' (resp. V'') also commute.

Since Jordan decomposition is unique, we conclude that $(\rho_g)_{ss,W'} = (\rho_g)_{ss,W}|_{W'}$ and $(\rho_g)_{u,W'} = (\rho_g)_{u,W}|_{W'}$ for any pair of finite-dimensional $G(k)$ -stable subspaces $W' \subset W \subset k[G]$. In other words, the construction of $(\rho_g)_{ss,W}$ and $(\rho_g)_{u,W}$ is *compatible with change in W* .

By this compatibility, we can pass to the direct limit and conclude that ρ_g itself factors as a product $\rho_g = (\rho_g)_{ss}(\rho_g)_u$ of commuting operators on $k[G]$ with semisimple (resp. unipotent) restriction to any finite dimensional $G(k)$ -stable subspace W .

We now make a temporary definition.

Definition 13.1.4. Say that g is *right semisimple* (resp. *right unipotent*) if $\rho_g = (\rho_g)_{ss}$ (resp. $\rho_g = (\rho_g)_u$).

Remark 13.1.5. Observe that g is right semisimple (resp. right unipotent) if and only if $\rho_g|_W = (\rho_g)_{ss,W}$ (resp. $\rho_g|_W = (\rho_g)_{u,W}$) for a single finite dimensional $G(k)$ -stable subspace $W \subset k[G]$ containing algebra generators for $k[G]$ over k . To see this, recall that semisimplicity (resp. unipotence) is inherited by tensor products, direct sums, and quotients thereof for the spaces in question, and we have a surjection $\mu : \text{Sym}^* W \twoheadrightarrow k[G]$ given by multiplication, when W is as just specified. Since ρ_g acts by k -algebra automorphisms on $k[G]$, so μ is ρ_g -equivariant, semisimplicity (resp. unipotence) of $\rho_g|_W$ passes to its action on $W^{\oplus r}$, hence to the tensor algebra, hence to its quotient the symmetric algebra, hence to its quotient $k[G]$.

Proposition 13.1.6. *Let $G = GL_n$. Then $g \in GL_n(\bar{k})$ is semisimple (resp. unipotent) if and only if g is right semisimple (resp. right unipotent).*

Sketch. We have $k[G] = k[\text{End}(V)][\frac{1}{\det}] = \sum_{n \in \mathbb{Z}} k[\text{End } V] \cdot \det^n$ as a “ g -module”; that is, $GL(V) \subset \underline{\text{End}}(V)$ is an open subfunctor and the action of ρ_g is the restriction of the action – also denoted ρ_g – of g on $\underline{\text{End}}(V)$ by the same formula (multiplication of matrices on the right). Inside $k[G]$, \det^n is a ρ_g -eigenvector with eigenvalue $\det(g)^n \in k^\times$. One can show that g is right-semisimple (resp. right-unipotent) if and only if ρ_g acting on $k[\text{End}(V)]$ is semisimple (resp. unipotent) on finite-dimensional $G(k)$ -stable subspaces of $k[\text{End}(V)]$. The crucial idea here is the eigenvector property of the \det^n ’s. See [Bor, Ch. I, §4.3] for details.

Now $\text{End}(V) = V \otimes_k V^*$. Thus $k[\text{End}(V)] = \text{Sym}^*(V \otimes V^*)$. We wish to describe the right regular action ρ_g of g on $\text{End}(V) \xleftarrow{k} V \otimes V^*$. First, some generalities. If W is a finite dimensional k -vector space and $\mathbf{A}(W)$ is the associated affine space $R \mapsto W_R$, then $\mathbf{A} = \text{Spec } \text{Sym } W^*$; note the duality, which is essential for the variance to be correct. If $W = \text{End}(V)$ the coordinate ring $\mathbf{A}(W)$ is thus $k[\text{End}(V)^*]$; the right-translation action by $GL(V)$ is given by $(g^* \cdot \varphi)(T) = \varphi(Tg)$ for $g \in GL(V)(k)$, $\varphi \in \text{End}(V)^*$. If we identify $\text{End}(V)^*$ with $V \otimes V^*$ via $v \otimes \ell \mapsto \varphi_{v \otimes \ell}(T) = [T \mapsto \ell(Tv)]$ then this action is $g^* \varphi_{v \otimes \ell}(T) = \varphi_{v \otimes \ell}(Tg) = \ell(Tgv) = \varphi_{gv \otimes \ell}(T)$; i.e. $g^* \varphi_{v \otimes \ell} = \varphi_{gv \otimes \ell}$. Hence the compatible $GL(V)$ -action on $V \otimes V^*$ is $g \otimes \mathbf{1}$ (which is a left action, as it should be).

Consequently ρ_g is semisimple (resp. unipotent) on $k[\text{End}(V)]$, if and only if it is such on $\text{End}(V)$ if and only if $g \otimes \mathbf{1}$ is such on $V \otimes V^*$, if and only if g is such on V . \square

The previous proposition is by way of motivation for the main theorem of today.

Theorem 13.1.7. *Let G be a smooth affine k -group, $k = \bar{k}$, $g \in G(k)$, $j : G \hookrightarrow GL_n$ a closed immersion which is a k -homomorphism. Consider ρ_g acting on $k[G]$ and the Jordan decomposition $j(g) = j(g)_{ss}j(g)_u \in GL_n(k)$. Then $j(g)_{ss} = j(g_{ss})$ and $j(g)_u = j(g_u)$ for some $g_{ss}, g_u \in G(k)$. Moreover, $\rho_{g_{ss}} = (\rho_g)_{ss}$ and $\rho_{g_u} = (\rho_g)_u$ as operators on $k[G]$, g_{ss} and g_u are independent of j , and the formation of g_{ss} and g_u is functorial in G .*

In particular, $g = g_{ss}$ (resp. $g = g_u$) if and only g is right semisimple (resp. right unipotent).

Proof. In Appendix B it is proved (conditional on Theorem 14.1.1 to be discussed next time) that g_{ss} and g_u exist in $G(k)$ giving rise to $j(g)_{ss}$ and $j(g)_u$ respectively. Note that the actions of $\rho_{j(g)}$ and ρ_g on $k[GL_n]$ and $k[G]$ respectively are compatible with the surjection j^* , so $\rho_{j(g)}$ determines ρ_g . Since the formation of Jordan decomposition is compatible with passage to quotients, and the operators $\rho_{j(g)_{ss}}$ and $\rho_{j(g)_u}$ are the “Jordan components” of $\rho_{j(g)}$ (due to the unique characterization of Jordan decomposition in terms of commuting semisimple and unipotent operators), we conclude that $\rho_{g_{ss}}$ and ρ_{g_u} are the respective semisimple and unipotent Jordan components of ρ_g on $k[G]$. This gives an intrinsic characterization of $\rho_{g_{ss}}$ and ρ_{g_u} in terms of $g \in G(k)$ without reference to j , so we conclude that $\rho_{g_{ss}}$ and ρ_{g_u} are independent of j , so likewise for g_{ss} and g_u (indeed, ρ_h determines h , since as an endomorphism of the variety G it carries e to h).

It remains to consider the issues of functoriality. That is, if $f : G \rightarrow G'$ is a k -homomorphism between smooth affine k -groups and $g \in G(k)$ then we claim that $f(g)_{ss} = f(g_{ss})$ and $f(g)_u = f(g_u)$. By factoring f into a surjection onto a smooth closed subgroup, it suffices to separately treat the cases when f is surjective and when f is a closed immersion. The closed immersion case is immediate from the “independence of j ” established above. If instead f is surjective then $k[G'] \hookrightarrow k[G]$ via f^* , and this maps $k[G']$ to a $G(k)$ -stable subspace via the right regular action. More specifically, ρ_g on $k[G]$ restricts to $\rho_{f(g)}$ on the subspace $k[G']$. Since Jordan decomposition passes to subspaces, it follows that the semisimple and unipotent parts of $\rho_{f(g)}$ are respectively obtained by restriction to $k[G']$ of the semisimple and unipotent parts of ρ_g . In other words, $\rho_{f(g)_{ss}} = \rho_{g_{ss}}|_{k[G']} = \rho_{f(g_{ss})}$ and similarly for the unipotent parts. It follows that $f(g_{ss}) = f(g)_{ss}$ and $f(g_u) = f(g)_u$. \square

14 February 10

14.1 All subgroups of a smooth finite type k -group are stabilizers of a line

To tie up a loose end in the proof of Theorem 13.1.7, and more specifically to fill in a key step used in Appendix B, we need the following result, somewhat remarkable for its extraordinary generality and usefulness.

Theorem 14.1.1. *Let $j : G \hookrightarrow G'$ be a closed k -subgroup scheme of a (smooth) affine k -group G' of finite type. Then there exists a k -linear representation $\pi : G' \rightarrow GL(V)$ and a line $L \subset V$ such that $G = N_{G'}(L)$.*

Proof. Let $I = \ker(j^* : k[G'] \rightarrow k[G])$. The group G acts on G' by right translation, through j . The induced action on $k[G']$ is compatible (equivariant) with the right translation action on $k[G]$. Hence I is a G -stable subspace of $k[G']$. Now $k[G'] = \varinjlim V$ is the rising union of finite dimensional G' -stable (hence G -stable) subspaces V . Since $k[G']$ is Noetherian, I is finitely generated, so we can choose V once and for all to be a finite dimensional G -stable subspace of $k[G']$ which contains ideal generators for I . Let $W = I \cap V$.

We will show that $G = \text{Stab}_{G'}(W)$ for the induced action of G' on V .

Note that without loss of generality we can assume $I \neq 0$, hence $W \neq 0$, since if $I = 0$ then $G = G'$ and we can take any stupid representation of G' to fulfill the conditions of the theorem.

Consider $\pi : G' \rightarrow GL(V)$.

Claim 14.1.2. $G = N_{G'}(W)$, i.e. for all k -algebras R , $g' \in G'(R)$ lies in $G(R)$ if and only if $g'(W_R) \subset W_R$.

Suppose $g'(W_R) \subset W_R$. Since W generates I and $\rho_{g'}$ acts on $k[G'_R]$ by an R -algebra automorphism, we have $\rho_{g'}(I_R) \subset I_R$. Hence $\rho_{g'}$ acting in G'_R preserves the closed subscheme G_R . Applying this to $e' = j(e)$, we see that $\rho_{g'}(j(e)) = g' \in j(G(R)) \subset G'(R)$.

Conversely if $g' \in G(R)$ then the action of $\rho_{g'}$ by right translation on G'_R preserves $G_R \subset G'_R$. Hence the action of $\rho_{g'}$ on $k[G'_R]$ preserves I_R . Since V_R is G' -stable, $\rho_{g'}$ also preserves V_R . Hence it preserves the intersection $V_R \cap I_R$. Since $k \rightarrow R$ is flat, $V_R \cap I_R = (V \cap I)_R = W_R$. Hence g' preserves W_R .

Thus the claim holds.

To deduce the theorem from the claim, we need only improve V to be a line. Set $d = \dim W > 0$. Take $\wedge^d \pi : G' \rightarrow GL(\wedge^d V)$. Then (exercise) $N_{G'}^\pi(W) = N_{G'}^{\wedge^d \pi}(\wedge^d W)$. But $L = \wedge^d W$ is a line, so we are done. \square

Remark 14.1.3. Use the direct sum of $\wedge^d \pi$ and any faithful G' -representation to ensure that G is the stabilizer of a line in a *faithful* G' -representation.

15 February 12

15.1 Unipotent groups

Definition 15.1.1. A smooth affine k -group U is *unipotent* if for all $g \in U(\bar{k})$, $g = g_u$ (where g_u is the unipotent factor in the Jordan decomposition).

Remark 15.1.2. It is possible to define unipotence for possibly non-smooth group schemes over a field k ; see [SGA3, XVII, 1.3, 3.5(i)-(v)].

Example 15.1.3. The ur-unipotent group is

$$U_n = \left\{ \begin{pmatrix} 1 & * & * \\ & 1 & * \\ 0 & \ddots & 1 \\ 0 & 0 & 1 \end{pmatrix} \right\} \subset GL_n.$$

A special case is U_2 , which is easily seen to be isomorphic to G_a .

Example 15.1.4. If U is unipotent, then any smooth closed k -subgroup $U' \subset U$ and any smooth image (quotient) $U \twoheadrightarrow U''$ are unipotent.

This is trivial in the subgroup case, since $U'(\bar{k}) \subset U(\bar{k})$. For quotients, use the functoriality of Jordan decomposition. Thus we see that if $u \in U(\bar{k})$ maps to $u'' \in U''(\bar{k})$, then $u'' = u_u'' u_{ss}''$ where u_u'' and u_{ss}'' are the images of the unipotent and semisimple factors of u . But $u_{ss} = 1$, so $u_{ss}'' = 1$, so $u'' = u_u''$.

Example 15.1.5. If $\text{char}(k) = p > 0$ then the constant subgroup $\mathbf{Z}/p\mathbf{Z} \subset G_a$ given as $\text{Spec } k[t]/(t^p - t)$ is unipotent.

Example 15.1.6. A non-example is any k -torus T of positive dimension. For given any nontrivial $t \in T(\bar{k})$, since $T_{\bar{k}}$ is isomorphic to the standard diagonal torus in $GL_{\dim T}$ and we can compute the Jordan decomposition of $t \in T(\bar{k}) = T_{\bar{k}}(\bar{k})$ with respect to that representation, so we see that $t_u = 1$. Thus in fact tori are *maximally* non-unipotent in some vague sense.

Remark 15.1.7. Later we'll see that for all smooth connected affine k -groups G such that $g = g_{ss}$ for all $g \in G(\bar{k})$, G is in fact a torus. See Homework 5 for the case where G is a priori assumed commutative.

Theorem 15.1.8. *Let U be unipotent. Then for any k -linear representation $\rho : U \rightarrow GL_n$, some $GL_n(k)$ -conjugate ρ' of ρ satisfies $\rho'(U) \subset U_n \subset GL_n$.*

We will prove this next time. Now we deduce some consequences.

Corollary 15.1.9. *If U is unipotent over k and K/k is any algebraically closed extension field, then $g = g_u$ for all $g \in U(K)$.* \square

(This can of course also be seen more directly, by considering the characteristic polynomial of g .)

Corollary 15.1.10. *Suppose U is a finite unipotent group (hence smooth). If $\text{char}(k) = 0$ then U is trivial, while if $\text{char}(k) = p > 0$ then $U(\bar{k})$ is a p -group.*

Proof. Without loss of generality $k = \bar{k}$. By the theorem, $U(k)$ is a subset of $U_n(k)$. Now $U_n(k)$ has a composition series by subgroups which have zeroes on several superdiagonal rows, followed by arbitrary entries in a top-right corner triangle. The Jordan-Holder factors are diagonal lines which are easily seen to be isomorphic to products of the additive group k .¹¹ These Jordan-Holder factors are thus torsion-free in

¹¹Once we do quotients, U itself will have a composition series with Jordan-Holder factors being powers of G_a .

characteristic zero; hence the image of $U(k)$ in each is finite and torsion-free, so trivial. In characteristic p , the Jordan-Holder factors are exponent p . Hence $U(k)$ has a composition series with abelian p -group subquotients, so it is a p -group. \square

Corollary 15.1.11. *If U is unipotent and $\text{char}(k) = 0$ then U is connected. If $\text{char}(k) = p > 0$, the component group $U(\bar{k})/U^0(\bar{k})$ is a p -group.*

Proof. Without loss of generality $k = \bar{k}$. Let $\Gamma = U(k)/U^0(k)$, regarded as a finite constant k -group. Then $U \simeq \coprod_{\gamma \in \Gamma} \tilde{\gamma}U^0$ as a scheme, where $\tilde{\gamma} \in U$ as any k -point of the γ -component of U . Thus U has an evident k -map, and in fact a k -homomorphism $U \twoheadrightarrow \Gamma$, given by sending $\tilde{\gamma}U^0$ to γ . This is a morphism of schemes, and even a homomorphism of group-schemes, because it is induced by translation from the constant map $U^0 \rightarrow \Gamma^0 = \{e_\Gamma\}$. Hence Γ is unipotent by Example 15.1.4. So we can apply Corollary 15.1.10 to deduce the result. \square

The main reason why unipotent groups are important is because they and their representations are easy to analyze, due to the filtration with additive subquotients. Moreover, an analysis of unipotent groups is complementary to an analysis of tori (which we will see also behave extremely well), because of the following miraculous result.

Theorem 15.1.12 (Big Miracle). *Let G be a smooth connected affine k -group, for an arbitrary field k . If G is not unipotent, then G contains a nontrivial k -torus as a closed k -subgroup.*

This will be proved much later over \bar{k} (Corollary 22.1.4), and lies quite deep over general fields: see Remark E.1.4 for the descent from \bar{k} .

15.2 Proof of Theorem 15.1.8 on representations of unipotent groups

Write $\rho : U \rightarrow GL(V)$ for the given representation. If $V = 0$, the claim is trivial; so we can assume $V \neq 0$. We seek a nonzero k -subspace $W \subset V$ such that W is U -fixed. Then we can conjugate ρ so that the image of U looks like

$$\begin{pmatrix} 1 & ?_1 \\ 0 & ?_2 \end{pmatrix}$$

by taking the first several basis vectors to be a basis for W . We don't care about $?_1$. But now we can look at the induced U -action on V/W – i.e. at $?_2$ – and induct on dimension. Note that we set up Theorem 15.1.8 for all representations, not just faithful ones. This is good, because probably we lose faithfulness when passing to V/W .

By Homework #5, problem 2, for any linear representation of a smooth finite type k -group G on a vector space V , the functorially G -fixed vectors $\underline{V}^G \subset \underline{V} = \mathbf{A}(V)$ [the affine space corresponding to V , equipped with its natural G -action through ρ] constitute the points of a scheme of the form $\underline{W} = \mathbf{A}(W)$ for a unique linear subspace $W \subset V$, which we denote by V^G . So we just need to prove that $V^G \neq 0$ if G is unipotent and V is nonzero.

From the construction of V^G in Homework 5, or from the universal property of \underline{V}^G , we see that $(V^G)_K = V_K^{G_K}$ for any K/k field extension. Thus we can assume without loss of generality that $k = \bar{k}$. Now when $k = \bar{k}$, by a schematic density argument or by the construction in Homework 5, it is easy to see that $V^G = V^{G(k)}$.

So we are reduced to showing that $V^{G(k)} \neq 0$. Now since $V \neq 0$, it contains a nonzero irreducible $G(k)$ -subrepresentation. Rename that as V . Hence we can assume without loss of generality that V is irreducible for $G(k)$.

We will now show that, in fact, $V = k$ with the trivial G -action, when G is unipotent. The key fact we need is the following.

Theorem 15.2.1 (Wedderburn). *If $k = \bar{k}$ and $\Gamma \subset GL(V)$ is such that V is an irreducible Γ -representation, then $\text{End}_k(V)$ is generated as a k -algebra by Γ .* \square

Since Γ is a group, in fact this means that $\text{End}_k(V)$ is spanned by Γ .

To apply the theorem, we take $\Gamma = \rho(G(k))$. Choose $g \in G(k)$. Note that by functoriality of Jordan decomposition, $\rho(g)$ is unipotent. [E.g. we can enlarge V to a faithful G -representation and take the Jordan

decomposition there, where g is unipotent by assumption; hence g acts unipotently on the subrepresentation V .] So write $\rho(g) = \mathbf{1} + x$ for some $x \in \text{End}_k(V)$, which in fact is nilpotent. Then for all $g' \in G(k)$ we have

$$\text{tr}(x\rho(g')) = \text{tr}((\rho(g) - \mathbf{1})\rho(g')) = \text{tr}(\rho(gg')) - \text{tr}(\rho(g)) = \dim V - \dim V = 0$$

since both $\rho(gg')$, $\rho(g)$ are unipotent on V . Since $\Gamma = \rho(G(k))$ spans $\text{End}_k(V)$, it follows that $\text{tr}(xy) = 0$ for all $y \in \text{End}_k(V)$. But the trace pairing on $\text{End}_k(V)$ is non-degenerate, so $x = 0$. Hence ρ is trivial, so by irreducibility $V = k$, and the theorem follows. \square

15.3 Remaining ingredients necessary for structure theory

1. Commutator and derived subgroups “as algebraic groups” (in the smooth case). Note that these algebraic groups will not represent the “expected” thing at the level of all field-valued points, but they will be what one expects on geometric points.
2. Lie algebras.
3. Complete reducibility theorem for linear representations of split tori \mathbf{G}_m^r . (This is the analogue of Maschke’s theorem for compact Lie groups, which implies complete reducibility for representations of “tori” $\mathbf{T}^r = (\mathbf{S}^1)^r$ in Lie theory.)
4. Coset spaces G/H for not-necessarily-smooth, not-necessarily-normal, not-necessarily connected closed subgroups $H \subset G$. This will use the closed orbit lemma, and it will allow us to show that, in a suitable sense, we have

$$\text{PGL}_n = \text{GL}_n / \mathbf{G}_m = \text{SL}_n / \mu_n, \text{GL}_2 / B = \mathbf{P}^1, \dots$$

16 February 17

16.1 Some motivation: a key calculation on $\text{SL}_2(k)$

Proposition 16.1.1. *If k is a field other than \mathbf{F}_2 or \mathbf{F}_3 (which have the undesirable property that $(\mathbf{F}_2^\times)^2 = 1, (\mathbf{F}_3^\times)^2 = 1$) then $\text{SL}_2(k)$ is its own commutator subgroup.*

To prove this, we need the following fact.

Lemma 16.1.2. *[L, Ch. XIII, Lemma 8.1] For any field k , $\text{SL}_2(k)$ is generated by the upper and lower triangle unipotent subgroups*

$$\mathbf{U}^+(k) = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \stackrel{\text{def}}{=} x^+(a) : a \in k \right\}, \quad \mathbf{U}^-(k) = \left\{ \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \stackrel{\text{def}}{=} x^-(a) : a \in k \right\}. \quad \square$$

Note that $x^\pm : \mathbf{G}_a \xrightarrow{\sim} \mathbf{U}^\pm$ is an isomorphism of algebraic groups.

Proof of Proposition 16.1.1. Let $D = \left\{ \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \stackrel{\text{def}}{=} \lambda(t) \right\}$ be the diagonal torus in SL_2 . (So $\lambda : \mathbf{G}_m \rightarrow D$ is an isomorphism.)

The first claim is that D normalizes \mathbf{U}^\pm , i.e. $D \subset N_{\text{SL}_2}(\mathbf{U}^\pm)$ as algebraic groups. This follows from the computation (valid over any k -algebra R)

$$\lambda(t)x^\pm(a)\lambda(t)^{-1} = x^\pm(t^{\pm 2}a).$$

This implies that

$$[\lambda(t), x^\pm(a)] = x^\pm((t^{\pm 2} - 1)a).$$

So as long as there exists $t \in k^\times$ such that $t^{\pm 2} - 1 \in k^\times$, i.e. $t \neq \pm 1$, any $x^\pm(a') \in \mathbf{U}^\pm(k)$ is a commutator. So $\mathbf{U}^\pm(k) \subset [\text{SL}_2(k), \text{SL}_2(k)]$, which, in light of the lemma, proves the proposition. \square

Proposition 16.1.1 suggests that as a k -group, SL_2 should be **perfect**, i.e. equal to its own derived subgroup in some suitable sense yet to be defined. In particular $\text{SL}_2(K) = [\text{SL}_2(K), \text{SL}_2(K)]$ for any $K = \bar{k}$. The same should hold for any quotient, such as $\text{SL}_2 \twoheadrightarrow \text{PGL}_2$.

Remark 16.1.3. Over interesting large fields k which are not algebraically closed, $\mathrm{PGL}_2(k)$ is not equal to its own commutator subgroup, because it has nontrivial commutative quotients. For example, $\mathrm{PGL}_2(k) \twoheadrightarrow k^\times/(k^\times)^2$ via the determinant. Usually the target is nontrivial.

The principle is that we expect Zariski closed conditions to capture group-theoretic constructions [e.g. commutator subgroups] for K -points when $K = \bar{k}$, but not necessarily for k -rational points when $k \neq \bar{k}$.

The difficulty in establishing that this indeed is the case is “bounding the lengths of words”. Roughly, if one knows that all the commutators can be realized as products of bounded length, then one has a hope of defining the commutator subgroup of two subgroups of G as an closed subgroup of G . This is certainly false in general; see Remark 16.2.3 below. To overcome the difficulty, we must lean upon connectedness hypotheses.

16.2 Subgroups generated by connected varieties

The key proposition for dealing with derived subgroups is the following.

Proposition 16.2.1. *Let G be a smooth k -group of finite type and $\{f_i : X_i \rightarrow G\}$ a collection of k -maps from geometrically integral finite type k -schemes X_i , such that $e \in f_i(X_i)$ for all i . Then*

- (i) *There exists a unique smooth closed k -subgroup $H \subset G$ such that for all algebraically closed extension fields K of k , the K -points*

$$H(K) = \langle f_i(X_i(K)) \rangle_i$$

are the subgroup of G generated by the images of the K -points of the X_i . Moreover, H is connected.

- (ii) *There exists a finite sequence X_{i_1}, \dots, X_{i_n} (indices not necessarily distinct) and signs $e_1, \dots, e_n \in \{\pm 1\}$ such that*

$$X_{i_1} \times \cdots \times X_{i_n} \rightarrow H$$

defined by

$$(x_1, \dots, x_n) \mapsto f_{i_1}(x_1)^{e_1} \cdots f_{i_n}(x_n)^{e_n}$$

is surjective.

An important example of the setup above is the single map $G \times G \rightarrow G$ given by taking commutators. See Example 16.2.4 below. Here are some others.

Example 16.2.2. Let $H, H' \subset G$ be smooth connected closed k -subgroups of a smooth k -group G of finite type. Using the inclusions $H \hookrightarrow G, H' \hookrightarrow G$, Proposition 16.2.1 we obtain a smooth, connected closed k -subgroup $H \cdot H' \subset G$ which deserves to be called “the subgroup generated by H and H' ”; it has the correct geometric points: for algebraically closed K/k we have $(H \cdot H')(K) = H(K) \cdot H'(K) \subset G(K)$.

Remark 16.2.3. In Example 16.2.2, H and H' must be connected. Otherwise the conclusion is false. Take $G = \mathrm{SL}_2/\mathbf{Q}$ and $H, H' \subset \mathrm{SL}_2(\mathbf{Z}) \subset \mathrm{SL}_2/\mathbf{Q}$ finite (disconnected) subgroups of orders 3 and 4 which generate $\mathrm{SL}_2(\mathbf{Z})$. Thus the subgroup of $\mathrm{SL}_2/\mathbf{Q}(\mathbf{C})$ generated by H and H' is $\mathrm{SL}_2(\mathbf{Z})$ which is not algebraic. (It is an infinite disjoint union of points.)

Example 16.2.4. Assume G is smooth, and for now assume G is connected (but see Example 16.4.4 below). Then taking

$$[\cdot, \cdot] : G \times G \rightarrow G$$

in Proposition 16.2.1 yields a smooth connected closed k -subgroup $\mathcal{D}G \subset G$, such that for $K = \bar{k}$ over k we have

$$(\mathcal{D}G)(K) = [G(K), G(K)].$$

Example 16.2.5. Let $G = \mathrm{GL}_n$. We have

$$\mathrm{SL}_n = \ker(\mathrm{GL}_n \xrightarrow{\det} \mathbf{G}_m).$$

Now $\mathcal{D}\mathrm{GL}_n$ must map trivially to \mathbf{G}_m under \det , because everything is smooth, so we can compute on geometric points, and we know that commutators die when mapped to an abelian group. So $\mathcal{D}\mathrm{GL}_n$ factors through $\mathrm{SL}_n \hookrightarrow \mathrm{GL}_n$.

Later we will see that $\mathrm{SL}_n = \mathcal{D}\mathrm{GL}_n = \mathcal{D}\mathrm{SL}_n$; we'll deduce the outer equality from the case $n = 2$.

Caution: this does not mean that $\mathrm{SL}_n(k) = [\mathrm{SL}_n(k), \mathrm{SL}_n(k)]$ on the level of rational points. The latter is actually true, however, when k is not too small. The proof requires some structure theory for split reductive groups (in terms of which SL_2 plays a central role, akin to the special role of \mathfrak{sl}_2 in the theory of complex semisimple Lie algebras).

Example 16.2.6. Let $G \twoheadrightarrow G'$ be a surjective homomorphism of smooth k -groups. Then we get an induced map $\mathcal{D}G \rightarrow \mathcal{D}G'$ and this is surjective because it can be checked on the level of geometric points. Consequently PGL_n is perfect as an algebraic group; i.e., $\mathrm{PGL}_n = \mathcal{D}(\mathrm{PGL}_n)$, because of the surjection $\mathrm{SL}_n \twoheadrightarrow \mathrm{PGL}_n$.

16.3 Proof of Proposition 16.2.1

First note that uniqueness in (i) is guaranteed, because H is determined by its geometric points.

Next observe that without loss of generality we can add maps $g_i : X_i \rightarrow G$ to our collection, where $g_i(x) = f_i(x)^{-1}$. Now we don't need to mention inverses, and can restrict our attention to taking products of the $f_i(X_i)$'s.

Now for $I = (i_1, \dots, i_n)$ an n -tuple of indices, define

$$m_I : X_I \stackrel{\mathrm{def}}{=} X_{i_1} \times \cdots \times X_{i_n} \xrightarrow{\prod f_{i_j}} G \times \cdots \times G \rightarrow G.$$

The set theoretic image $W_I = m_I(X_I)$ is constructible by Chevalley's theorem. By hypothesis, W_I contains the identity e . Therefore W_I contains a dense open U in W_I , the schematic image of m_I (= the Zariski closure of W_I), which is a geometrically integral closed subscheme of G passing through e . [Note that W_I is geometrically integral because $X_I \rightarrow W_I$ is dominant, so locally $\mathcal{O}_{W_I} \subset \mathcal{O}_{X_I}$, and the sections of $(\mathcal{O}_{X_I})_{\bar{k}}$ are domains (as X_I is geometrically integral) so the same is true for $(\mathcal{O}_{W_I})_{\bar{k}}$.]

Next choose I such that $\dim \overline{W}_I$ is maximal. We will show that $H \stackrel{\mathrm{def}}{=} \overline{W}_I$ satisfies the conclusions of the proposition.

Claim 16.3.1. *The map $\overline{W}_J \times \overline{W}_{J'} \rightarrow \overline{W}_{J \sqcup J'}$ given by multiplication is dominant, where $J \sqcup J'$ denotes concatenation of multisets.*

The proof is similar to that of Proposition 3.2.4(iii), and we omit it.

Now for any J we have on K -points ($K = \bar{K}$) that $\overline{W}_J(K), \overline{W}_I(K) \subset \overline{W}_J(K) \cdot \overline{W}_I(K) \subset \overline{W}_{I \sqcup J}(K)$. But $\overline{W}_I(K) = \overline{W}_{I \sqcup J}(K)$ by the maximality of I ; both are irreducible and closed and they have the same dimension, so since one is contained in the other they coincide.

The upshot is that \overline{W}_I is stable under left (and by analogous reasoning, right) multiplication by any \overline{W}_J , on K -points. But we get more: since $\overline{W}_I = \overline{W}_{I \sqcup J}$, we have $\overline{W}_J \subset \overline{W}_I$ for all J . Thus \overline{W}_I is stable under left and right multiplication against itself. Moreover $\overline{W}_I = \overline{W}_I^{-1} = \overline{W}_{I^{\mathrm{opp}, -1}} \subset \overline{W}_I$ where $I^{\mathrm{opp}, -1}$ denotes the set of indices corresponding to taking the inverse maps g_i of the f_i for $i \in I$, in the opposite order. Thus H is stable under multiplication and inversion, and by construction it is smooth and connected. Therefore H is a smooth connected closed k -subgroup of G , and moreover it contains $f_j(X_j)$ for all j by construction.

Now we have $U \subset W_I \subset H$ and $U \hookrightarrow H$ is open and dense. On K -points, $W_I(K)$ comes from $X_i(K)$'s for $i \in I$ multiplied in order. Therefore to show the last bit of (i) as well as (ii), it's enough to show that $U \times U^{-1} \rightarrow H$ is surjective, or equivalently, surjective on K -points.

We can extend scalars to K , rename K as k . Then we are reduced to showing the following lemma.

Lemma 16.3.2. *Let $k = \bar{k}$ and let H be a smooth k -group of finite type. Let $U \subset H$ be a dense open.¹² Then $U(k)U(k)^{-1} = H(k)$.*

Proof. Choose $h \in H(k)$. We just need to show that $h \cdot U(k) \cap U(k)$ is nonempty. But $h \cdot U(k) = (hU)(k)$ where hU is the translation of U by h . But hU and U are dense opens in H , so their intersection is nonempty, so since $k = \bar{k}$ it contains a rational point. \square

¹²In practice this density will be automatic if H is connected and U is nonempty.

16.4 Improvements on Proposition 16.2.1

Corollary 16.4.1. *Let H, H' be smooth closed subgroups of a smooth finite type k -group G . Suppose H (but not necessarily H') is connected. Then there exists a unique smooth closed connected subgroup $[H, H'] \subset G$ which on geometric points is the commutator subgroup of $[H(K), H'(K)]$.*

Proof. Uniqueness follows from existence because H is determined by its geometric points. By uniqueness and Galois descent, we can therefore assume without loss of generality that $k = k_s$.

Write $H' = \coprod H'_i$ as a finite disjoint union of connected components, which because $k = k_s$ are geometrically connected. Consequently the $(H'_i)_{\bar{k}}$ are the connected components of $H'_{\bar{k}}$. Hence they are translates of the irreducible variety $(H'_{\bar{k}})^0$, and are thus themselves irreducible. Since the H'_i are smooth, it follows that the H'_i are geometrically integral over k , and hence the rational points $H'_i(k) \neq \emptyset$. So there exist $h'_i \in H'_i(k)$ such that $H'_i = (H')^0 h'_i$. Thus “the disconnectedness of H' is completely explained by a finite set of rational points”. In particular

$$H' = \coprod_{h'_i \in H'(k) \text{ (finite)}} (H')^0 h'_i.$$

Form the maps

$$f_i : H \times (H')^0 \rightarrow G$$

by $f_i(h, h') = [h, h' h'_i]$. Applying Proposition 16.2.1 to these maps yields the corollary. \square

Proposition 16.4.2. *If $H, H' \subset G$ are smooth closed k -subgroups a smooth finite type k -group G and $H \subset N_G H'$ then there exists a unique smooth closed commutator k -subgroup $[H, H'] \subset G$ with the expected geometric points.*

Remark 16.4.3. In Proposition 16.4.2, $[H, H']$ is generally not connected if neither H nor H' is.

Example 16.4.4. Take $H = H' = G$ in Proposition 16.4.2. We obtain $\mathcal{D}G$ even when G is disconnected. Consequently (by noetherianity) any smooth G of finite type has a finite derived series.

Start of proof of Proposition 16.4.2. By Galois descent (as in Corollary 16.4.1) we can assume without loss of generality that $k = k_s$.

Since $H \subset N_G H'$, there is a k -homomorphism $H \ltimes H' \rightarrow G$. By Corollary 9.3.6, the image is a smooth closed k -subgroup of G . Since smooth closed subgroups of $H \ltimes H'$ thus map to smooth closed subgroups of G , it is enough to treat the case $G = H \ltimes H'$. In particular we can assume $H' \triangleleft G$.

Exercise: If $H' \triangleleft G$ then $(H')^0 \triangleleft G$.

By Corollary 16.4.1, we have smooth connected closed k -subgroups

$$[H, (H')^0], [H^0, H'] \subset G.$$

Let $L = [H, (H')^0] \cdot [H^0, H'] \subset G$ be the smooth closed k -subgroup they generate, using Proposition 16.2.1 in the guise of Example 16.2.2.

Now consider gLg^{-1} for $g \in G(k)$, and form the smooth connected closed subgroup

$$N = \langle gLg^{-1} \rangle_{g \in G(k)} \subset G$$

generated by all of them, again using Proposition 16.2.1. Since $G = H \ltimes H'$, $N \subset \mathcal{D}G$. Since $G(k) \subset G$ is Zariski-dense (as $k = k_s$) $N \triangleleft G$.

Now we are almost done; we'll finish the proof next time. \square

17 February 19

17.1 Conclusion of proof of Proposition 16.4.2

Last time we reduced to the case $H, H' \subset H \ltimes H' = G$ all smooth k -groups of finite type over $k = k_s$, and we constructed a smooth connected normal closed k -subgroup $N \triangleleft G$ such that

$$[H, H'^0] \cdot [H^0, H'] \subset N, \quad N(K) \subset [H(K), H'(K)] \text{ for all } K = \bar{K}/k.$$

Since $k = k_s$ we can choose representatives $h_i \in H(k)$ and $h'_j \in H'(k)$ for the component groups, so that

$$H = \coprod_{\text{finite}} H^0 h_i, \quad H' = \coprod_{\text{finite}} H'^0 h'_j.$$

Since in the quotient group $G(\bar{k})/N(\bar{k})$ the component $H^0(\bar{k})$ centralizes $H'(\bar{k})$ and $H'^0(\bar{k})$ centralizes $H(\bar{k})$ [this is because $[H, H'^0] \cdot [H^0, H'] \subset N$] we compute that

$$[h_i h, h'_j h'] \equiv [h_i, h'_j] \pmod{N(\bar{k})}$$

on geometric points for $h \in H^0(\bar{k})$ and $h' \in H'^0(\bar{k})$. Hence, for varying $g \in H(\bar{k})$ and $g' \in H'(\bar{k})$, there are only finitely many possibilities for the image of the commutator $[g, g']$ in $G(\bar{k})/N(\bar{k})$. This finiteness, together with the fact that H normalizes H' , implies that the commutator subgroup $[H(\bar{k}), H'(\bar{k})] \subset G(\bar{k})$ has *finite* image in $G(\bar{k})/N(\bar{k})$ due to a purely group-theoretic result called the “Lemma of Baer” that is proved in [Bor, end of §I.2]. This latter finiteness completes the proof. \square

17.2 Solvable groups

Taking $H = H' = G$ in Proposition 16.4.2, we obtain for *any* smooth finite type k -group (possibly disconnected!) G a derived subgroup $\mathcal{D}G$ and hence a derived series

$$G \supset \mathcal{D}G \supset \mathcal{D}^2 G := \mathcal{D}(\mathcal{D}G) \supset \cdots.$$

By Noetherian-ness, the series eventually stabilizes

Lemma 17.2.1. *Let K/k be any algebraically closed extension field. Then $G(K)$ is a solvable group if and only if $\mathcal{D}^n G = 1$ for all $n \gg 0$.*

Remark 17.2.2. Note that the solvability of $G(K)$ is thus independent of K .

Proof. We have $\mathcal{D}^n G = \mathcal{D}^{n+1} G$ for $n \gg 0$. So $(\mathcal{D}^n G)(K) = \mathcal{D}^n(G(K)) \stackrel{?}{=} 1$ if and only if $\mathcal{D}^n G = 1$ because $K = \bar{K}$. In other words, the triviality of $\mathcal{D}^n G$ for large n can be checked on geometric points. \square

The last lemma motivates the definition of a solvable group.

Definition 17.2.3. We say that a smooth k -group G is *solvable* if $\mathcal{D}^n G = 1$ for $n \gg 0$.

Example 17.2.4. If G is commutative then $\mathcal{D}G$ is trivial, so G is solvable.

Example 17.2.5. Given maps $G' \hookrightarrow G \twoheadrightarrow G''$, if G is solvable then so are G' and G'' . This follows from the analogous fact from group theory, since it can be checked on geometric points. If moreover $G'(\bar{k}) = \ker(G \twoheadrightarrow G'')(\bar{k})$ then G', G'' solvable implies G is solvable, by similar reasoning. In particular G is solvable if and only if G^0 is solvable and $G(\bar{k})/G^0(\bar{k})$ is solvable in the usual group theoretic sense.

Example 17.2.6. If G is unipotent, then G is solvable. This is because by Theorem 15.1.8 we can find an embedding $G \hookrightarrow U_n$. And U_n is solvable because this can be checked on geometric points, and $U_n(\bar{k})$ has an obvious composition series with successive quotients isomorphic to products of additive groups, hence abelian.

Example 17.2.7. If G has a composition series in the sense of algebraic groups, i.e. a chain $1 = G_n \triangleleft G_{n-1} \triangleleft \cdots \triangleleft G_1 \triangleleft G_0 = G$ all smooth closed k -subgroups, and $\mathcal{D}G_i \subset G_{i+1}$ for all i , then G is solvable. Just check on geometric points!

17.3 Structure of smooth connected commutative affine k -groups

Theorem 17.3.1. *Let k be a perfect field and G a smooth connected commutative affine k -group. Then there exists a decomposition $G = M \times U$ where M, U are smooth closed k -subgroups of G , such that U is unipotent and $M(K)$ consists of semisimple elements of $G(K)$ for any algebraically closed extension field K/k . Moreover this decomposition is functorial in G , M^0 is a torus, and the component group $M(\bar{k})/M^0(\bar{k})$ has order not divisible by the characteristic of k .*

Remark 17.3.2. This is false for imperfect k , as the example of the Weil restriction of scalars $R_{k'/k}(\mathbf{G}_m)$ for an inseparable field extension k'/k shows.

Proof. Uniqueness is immediate because the geometric points of M and U must be given by the Jordan decomposition as the semisimple and unipotent elements of $G(\bar{k})$, respectively, and these determine the groups M and U uniquely.

Thus by Galois descent we may assume without loss of generality that $k = k_s$, and hence since k is perfect that $k = \bar{k}$.

Since G is commutative, gg' is semisimple (resp. unipotent) if $g, g' \in G(k)$ are both semisimple (resp. unipotent). Upon passing to a faithful representation of G , this is because commuting diagonalizable matrices are simultaneously diagonalizable, so their product is diagonalizable; likewise commuting nilpotent matrices have nilpotent product, which implies the claim for unipotent matrices.

Thus we have abstract *subgroups* $G(k)_{ss}$ and $G(k)_u$ of $G(k)$ consisting of exactly the semisimple (resp. unipotent) elements. Define U to be the Zariski closure of $G(k)_u$, which is a smooth closed k -subgroup by previous results.

Lemma 17.3.3. *U is unipotent, which is equivalent to $U(k) = G(k)_u$.*

To prove the lemma, choose a faithful representation $G \hookrightarrow GL(V)$ and consider the condition that the characteristic polynomial of $g \in G(k)$ is $(T - 1)^{\dim V}$. This is manifestly Zariski closed on $GL(V)$, and hence on G . So $G(k)_u$ is a Zariski closed locus in $G(k)$, which implies $U(k) = G(k)_u$ as desired.

Next define M to be the Zariski closure of $G(k)_{ss}$. The analogous lemma is

Lemma 17.3.4. *There exists a faithful representation $G \hookrightarrow GL(V)$ such that M maps to a torus.*

In particular, by Homework 5, this implies that all elements of $M(k)$ are semisimple in G , so $M(k) = G(k)_{ss}$.

To prove this lemma, take any faithful representation at all. Then the subgroup $G(k)_{ss} \subset GL(V)$ is a commutative group of diagonalizable matrices (albeit an infinite one) and is thus simultaneously diagonalizable over $GL(V)(k)$. So $G(k)_{ss} \subset T(k)$ for a $GL(V)(k)$ -conjugate T of the standard diagonal torus in $GL_{\dim V}$. Since $T \subset GL(V)$ is closed, the Zariski closure M can be computed inside $GL(V)$ to be contained in T .

By the preceding lemma and Homework 5, we conclude that M^0 is a torus and the component group has order prime to the characteristic.

Finally consider the k -homomorphism $M \times U \rightarrow G$ given by multiplication. This is a homomorphism precisely because G is commutative.

Claim 17.3.5. *This is an isomorphism.*

The map is surjective because this can be checked on geometric points, where one can appeal to Jordan decomposition.

To prove injectivity, notes that the kernel is precisely $M \cap U$. This has no nontrivial geometric points by Jordan decomposition. Hence $M \cap U \subset M^0 \cap U$, so it's enough to prove the latter is trivial (as a scheme!). But that is the intersection of a torus and a unipotent group. Take any faithful representation of G ; this can be conjugated so that U lands in U_n by Theorem 15.1.8. So $M^0 \cap U$ is a subgroup of $T \cap U_n$ for a torus $T \subset GL_n$. But by Homework 5, $T \cap U_n$ is trivial (as a scheme). \square

17.4 Coset spaces for closed subgroups (that is, quotients)

Definition 17.4.1. Let G be a finite type k -group and $H \subset G$ a closed k -subgroup. A *quotient* G/H is a map $\pi : G \rightarrow X$ for a finite type k -scheme X , which is flat, surjective, and invariant under the right translation action of H on G , such that the map

$$G \times H \rightarrow G \times_X G$$

given by

$$(g, h) \mapsto (g, gh)$$

is an isomorphism.

Remark 17.4.2. The last condition is equivalent to the condition that on \mathbf{R} -points, the fibers of $G(\mathbf{R}) \rightarrow X(\mathbf{R})$ are precisely the $H(\mathbf{R})$ -orbits of the right translation action on $G(\mathbf{R})$.

Remark 17.4.3. If $\pi : G \rightarrow X$ is a quotient G/H then $\pi_{k'} : G_{k'} \rightarrow X_{k'}$ is easily seen to be a quotient $G_{k'}/H_{k'}$. Moreover that π is a quotient G/H can be *checked* after scalar extension.

Remark 17.4.4. By passing to $\mathrm{pr}_1^{-1}(e)$ in the isomorphism $G \times H \simeq G \times_X G$, one can easily check that $\pi^{-1}(\pi(e)) = H$.

Example 17.4.5. A surjective k -homomorphism $\pi : G \rightarrow G'$ of smooth finite type k -groups is a quotient $G/\ker \pi$. To prove this, note that π is surjective by assumption, flat by the Miracle Flatness Theorem [Mat, 23.1] and that $G \times \ker \pi \simeq G \times_{G'} G$ via the specified map can be checked group-theoretically on \mathbf{R} -points for any k -algebra \mathbf{R} .

The definition of quotients leaves open three crucial questions, which we will address in the sequel.

1. Under what circumstances does G/H exist?
2. If $H \triangleleft G$ is normal, does G/H necessarily have a unique k -group structure making the projection $G \rightarrow G/H$ a k -homomorphism?
3. Does the projection $\pi : G \rightarrow G/H$ (for any closed subgroup H) satisfy the right universal mapping property, i.e. is it initial among right- H -invariant maps to k -schemes?

We address question 3 in the next lemma, and question 2 in the following corollary.

Lemma 17.4.6. *If $\pi : G \rightarrow G/H$ is a quotient then it is initial among right- H -invariant k -maps $f : G \rightarrow Y$ to k -schemes Y .*

(An immediate consequence is that if the quotient exists, it is unique up to unique isomorphism.)

Proof. Consider the diagram

$$\begin{array}{ccccc}
 G \times H & \xrightarrow[\mathrm{pr}_1]{\mathrm{mult}} & G & \xrightarrow{f} & Y \\
 \downarrow (g,h) \mapsto (g,gh) \sim & & \parallel & & \parallel \\
 G \times_{G/H} G & \xrightarrow[\mathrm{pr}_1]{\mathrm{pr}_2} & G & \xrightarrow{f} & Y \\
 & & \downarrow \pi & \nearrow \exists?! & \\
 & & G/H & &
 \end{array}$$

In both rows, both compositions agree. But by using the isomorphism in the first column from the definition of a quotient, the second row has lost all mention of group theory. Since π is flat and surjective and finite type (hence quasicompact) the existence of the dotted map is thus reduced to the following, which is essentially the content of faithfully flat descent.

Theorem 17.4.7 (Grothendieck). *Let $S' \xrightarrow{\pi} S$ be a flat surjective quasicompact map. Given a diagram with both compositions in the top row agreeing,*

$$\begin{array}{ccccc}
 S' \times_{S'} S' & \xrightarrow[\mathrm{pr}_2]{\mathrm{pr}_1} & S' & \xrightarrow{f} & Y \\
 \downarrow \pi & & \downarrow & \nearrow \exists! & \\
 S & & S & &
 \end{array}$$

there exists a unique dotted map making the diagram commute.

For the proof, see [BLR, §6.1]. □

Example 17.4.8. The proof of faithfully flat descent essentially reduces to the affine case, where one must actually do something. The setup is that $A \rightarrow A'$ is a faithfully flat algebra and we have a diagram

$$\begin{array}{ccccc} B & \longrightarrow & A' & \xrightarrow{j_1} & A' \otimes_A A' \\ & \searrow & \uparrow & \xrightarrow{j_2} & \\ & & A & & \end{array}$$

such that both composition in the row agree. Then there exists a unique dotted map making the diagram commute. The real content of this is that $A \hookrightarrow A' \rightrightarrows A' \otimes_A A'$ is exact, which one must prove.

Example 17.4.9. The toy example is the case of S quasicompact and separated, $S' = \coprod \mathcal{U}_i'$ a disjoint union of \mathcal{U}_i' 's giving a finite open affine cover of S . Then $S' \times_S S' = \coprod \mathcal{U}_i' \cap \mathcal{U}_j'$, and the content of faithfully flat descent in this case is that morphisms glue.

Now we address question 2 above.

Corollary 17.4.10. *If $H \triangleleft G$ is normal and the quotient G/H exists, then there exists a unique k -group structure on G/H such that $\pi: G \rightarrow G/H$ is a k -homomorphism.*

Proof. One can check that $\pi \times \pi: G \times G \rightarrow G/H \times G/H$ is a quotient map for $(G \times G)/(H \times H)$; this follows easily from the definition. Therefore it has the universal property of the preceding lemma. But consider the diagram

$$\begin{array}{ccc} G \times G & \xrightarrow{\pi \times \pi} & G/H \times G/H \\ \downarrow \times & & \downarrow \exists?! \\ G & \xrightarrow{\pi} & G/H \end{array}$$

The induced map, if it exists, is unique and must be the unique multiplication law giving the group structure on G/H compatible with π .

To see that the dotted map exists, we just need to check $\pi \circ (\times): G \times G \rightarrow G/H$ is right $H \times H$ -invariant, which can be checked functorially on R -points. Here this says that $\pi(ghg'h') = \pi(gg')$. This follows from the usual group theoretic computation that $ghg'h' = gg'g'^{-1}hg'h \in gg'H(R)$ because $H(R) \triangleleft G(R)$ is normal. \square

Example 17.4.11. $SL_n/\mu_n \simeq PGL_n$, so given a μ_n -invariant map $SL_n \rightarrow Y$, there exists a unique induced map $PGL_n \rightarrow Y$ making the triangle commute. Thus for all intents and purposes, PGL_n is the quotient of SL_n by μ_n , although this is manifestly false on the level of rational points.

18 February 22

18.1 Existence of quotients (of smooth affine groups)

Theorem 18.1.1. *If G is a smooth affine k -group and $H \subset G$ is a closed k -subgroup, then G/H exists as a smooth quasiprojective k -scheme, and $(G/H)(K) = G(K)/H(K)$ when K/k is algebraically closed.*

Example 18.1.2. If $G = GL_n$ and H is the subgroup $\left\{ \begin{pmatrix} * & * & * & * & * \\ 0 & * & * & * & * \\ \vdots & & & & \\ * & * & * & * & * \\ 0 & * & * & * & * \end{pmatrix} \right\}$ (where anything can go in the \star 's), then $G/H \simeq \mathbf{P}^n$. The method of proof will in fact show that if $G \curvearrowright X$, a finite type k -scheme, and $H = \text{Stab}_G(x)$ for a rational point $x \in X(k)$, then G/H sits as a locally closed subscheme of X as the orbit of x , with the reduced structure.

Proof. Using that G is smooth and affine and H is closed, by Theorem 14.1.1 there is a representation $\rho: G \rightarrow GL(V)$ such that $H = N_G(L)$ for a line $L \subset V$. Consider the projective representation $G \curvearrowright \mathbf{P}(V)$,

and let $x_0 \in \mathbf{P}(V)$ be the point corresponding to $L \subset V$. Then $H = Z_G(x_0)$ is the scheme theoretic centralizer of x_0 for this action. Let $X \subset \mathbf{P}(V)$ be the locally-closed G -orbit of x_0 , with the reduced structure, so that X is smooth. (We are here invoking the closed orbit lemma 9.3.5.)

Now look at $\pi : G \rightarrow X$, sending $g \mapsto gx_0$ (the orbit map). This certainly induces an isomorphism $G(K)/H(K) = X(K)$ on geometric points, because on geometric points $X(K)$ is the $G(K)$ -orbit of x_0 . In particular π is geometrically surjective, so surjective. Moreover G and X are smooth varieties of pure dimension. Since the fibers $\pi^{-1}(x)$ are (geometrically, hence scheme-theoretically) translates of the equidimensional variety H , they are all equidimensional of dimension $\dim H$. Since generically the fiber dimension plus $\dim X$ is equal to $\dim G$, this equation must therefore hold everywhere. So by the Miracle Flatness theorem [Mat, 23.1] π is flat. Finally, by definition π is right H -invariant. So we just need to show $G \times H \rightarrow G \times_X G$ sending $(g, h) \mapsto (g, gh)$ is an isomorphism. But on R -points we have

$$\begin{aligned} G \times_X G(R) &= G \times_{\mathbf{P}(V)} G(R) = \{(g, g') \in G(R)^2 : gx_0 = g'x_0 \in \mathbf{P}(V)(R)\} \\ &= \{(g, g') : g^{-1}g' \in Z_G(x_0)(R) = H(R)\} = \{(g, g') : g' = gh, \text{ for a unique } h \in H(R)\} = (G \times H)(R). \end{aligned}$$

□

Remark 18.1.3. The existence of quotients in more general settings (over a field) is discussed in [SGA3, VI_A]; for even more general settings one must use the theory of algebraic spaces.

Example 18.1.4. The important example of the above theorem is when $H \triangleleft G$ is normal. In this case G/H is actually affine. For a proof, see Appendix C. The idea is to go back to the construction and rig the representation V so that H acts on all of V by the same character $\chi \in \text{Hom}(H, \mathbf{G}_m) = \text{Hom}(H, \text{GL}(L))$ it acts by on L . Then one finds that $G/H \hookrightarrow \text{PGL}(V)$ is a closed (by the closed orbit lemma) subscheme of $\text{PGL}(V)$, and is thus affine.

Remark 18.1.5. See Homework 7 for a discussion of exact sequences of k -groups, as well as more examples.

18.2 Lie algebras

Let G be a locally finite type k -group, but *not* necessarily a smooth one. Let $\mathfrak{g} = T_e G$. For $v \in \mathfrak{g} \subset G(k[\epsilon])$, consider right multiplication over $k[\epsilon]$ as a map

$$\begin{aligned} G_{k[\epsilon]} &\xrightarrow{\sim} G_{k[\epsilon]} \\ g &\mapsto gv. \end{aligned}$$

This is the identity on the special fiber, since v is a tangent vector at the identity. In particular, on the underlying topological space $|G_{k[\epsilon]}| = |G|$ this map is the identity. On structure sheaves, regarded as sheaves on $|G|$, the map is an isomorphism

$$\mathcal{O}_{G_{k[\epsilon]}} = \mathcal{O}_G \oplus \mathcal{O}_G \epsilon \simeq \mathcal{O}_G \oplus \mathcal{O}_G \epsilon.$$

More particularly, it is a $k[\epsilon]$ -algebra automorphism deforming the identity on \mathcal{O}_G . By an easy computation, it is uniquely of the form

$$f_1 + f_2 \epsilon \mapsto f_1 + f_2 \epsilon + D_v(f_1) \epsilon$$

for $D_v \in \text{Der}_k(\mathcal{O}_G, \mathcal{O}_G)$.

Remark 18.2.1. The data of D_v is equivalent to that of a map $\Omega_{G/k}^1 \rightarrow \mathcal{O}_G$, and hence in the smooth case (by duality) to a global vector field $\mathcal{O}_G \rightarrow T_{G/k}$. It is easy to see that this vector field is left- G -invariant, relating \mathfrak{g} to the interpretation of Lie algebras in terms of left invariant vector fields on Lie groups in the classical, analytic setting.

As in the remark, D_v (as a derivation) is left-invariant, in the sense that

$$D_v(f \circ \ell_g) = D_v f \circ \ell_g \text{ for all } g \in G(R), f \in \mathcal{O}_{G_R},$$

as is easy to check by hand.

Lemma 18.2.2. *The map we just produced*

$$\mathfrak{g} \rightarrow \{\text{left-invariant } \mathbf{k}\text{-algebra derivations } D : \mathcal{O}_G \rightarrow \mathcal{O}_G\}$$

is a \mathbf{k} -linear isomorphism of vector spaces.

Proof. See [CGP, A.7.1, A.7.2]. □

Remark 18.2.3. It is this lemma which underlies Cartier's theorem on the smoothness of algebraic groups in characteristic zero.

Definition 18.2.4. Let $\text{Lie}(G) = (\mathfrak{g}, [\cdot, \cdot]_G)$ where $[\cdot, \cdot]_G$ is the commutator of (left-invariant) \mathbf{k} -derivations $\mathcal{O}_G \rightarrow \mathcal{O}_G$, pulled back to a Lie bracket on \mathfrak{g} along the isomorphism of the previous lemma.

(Note that one must check that the commutator of left-invariant derivations is a left-invariant derivation, but this is trivial.)

Example 18.2.5. If $G = \text{GL}(V)$ then $\mathfrak{g} = \mathfrak{gl}(V) = \text{End}(V)$ and $[\cdot, \cdot]_{\text{GL}(V)}$ is the commutator on $\text{End}(V)$; cf. Homework 7.

18.2.1 Functoriality of $\text{Lie}(\cdot)$

Proposition 18.2.6. *The derivative*

$$\text{ad}_G = T_e(\text{Ad}_G) : \mathfrak{g} \rightarrow \mathfrak{gl}(\mathfrak{g}) = \text{End}(\mathfrak{g})$$

of the adjoint representation

$$\begin{aligned} \text{Ad}_G : G &\rightarrow \text{GL}(\mathfrak{g}) \\ \mathfrak{g} \mapsto T_e(\mathbf{c}_g), \quad \mathbf{c}_g : x &\mapsto gxg^{-1} \end{aligned}$$

satisfies

$$\text{ad}_G(X) = [X, \cdot]_G.$$

Proof. See [CGP, A.7.5]. Note that Ad_G is well-defined because $\mathfrak{g}_R = T_{e_R}(G_R)$, so $\mathfrak{g} \mapsto T_e(\mathbf{c}_g)$ really gives a functorial representation of G on \mathfrak{g} . □

Now given $f : G' \rightarrow G$ we have the identity

$$f \circ \text{Ad}_{G'} = \text{Ad}_G \circ f$$

because f is a homomorphism and so commutes with conjugation. Differentiating this identity we obtain

$$T_e f \circ \text{ad}_{G'} = \text{ad}_G \circ T_e f.$$

In light of the proposition, this establishes that the Lie bracket, and hence the Lie functor, is functorial in G .

19 February 24

19.1 Linear representations of split tori, over general rings

Let \mathbf{k} be any commutative ring, not equal to the zero ring. Let $T \simeq \mathbf{G}_m^r$ be a split torus over \mathbf{k} . Set $\Lambda = \mathbf{Z}^r$. We have an injection

$$\Lambda \hookrightarrow \text{Hom}_{\mathbf{k}\text{-gp}}(T, \mathbf{G}_m) =: X(T) \quad (\star)$$

given by $\lambda = \vec{n} \mapsto [\lambda : (t_1, \dots, t_r) \mapsto \prod t_i^{n_i}]$.

Remark 19.1.1. On Homework 1, it was shown that $\text{End}_{\mathbf{k}}(\mathbf{G}_m) = \mathbf{Z}$ if $\text{Spec } \mathbf{k}$ is connected; so under this hypothesis (\star) is an isomorphism.

The main theorem about linear representations of split tori is the following.

Theorem 19.1.2. Let V be a k -module, equipped with a functorial k -linear representation of T , i.e. a map $T(R) \rightarrow \text{End}_R(V_R)$ natural in R . Then V has a unique decomposition $V = \bigoplus_{\lambda \in \Lambda} V_\lambda$ where the λ **weight space** V_λ is T -stable and has action via the character λ ; in other words, for all $v \in V_R$ we have

$$v \stackrel{!}{=} \sum_{\text{finite}} v_\lambda \text{ for some } v_\lambda \in (V_\lambda)_R$$

and for all $t \in T(R)$ we have

$$t.v = \sum \lambda(t)v_\lambda \in V_R,$$

where $\lambda(t) \in R^\times$ is given as above via (\star) .

Remark 19.1.3. If k is local (e.g. a field or a dvr) or a PID [all we need is that projective finite modules are free] then if V is finite free in Theorem 19.1.2, so are all the weight spaces V_λ (and all but finitely many vanish, of course).

Theorem 19.1.2 will be proved next time and is part of a theme: to give a linear representation of a split torus T on V is to give a k -linear Λ -grading on V . That this works over rings is a fundamental discovery by Grothendieck.

Example 19.1.4. If k is a field then V is a *semisimple* T -representation, in the sense that any T -stable subspace W admits a T -stable direct complement W' .

To prove this, use the theorem to fix decompositions $V = \bigoplus V_\lambda, W = \bigoplus W_\lambda$.

Claim 19.1.5. $W_\lambda = W \cap V_\lambda$.

Granting the claim, we can take $W' = \bigoplus W'_\lambda$ where W'_λ is any complement of W_λ in V_λ ; since T acts by scalars on V_λ , any such complement is T -stable, so we win.

To prove the claim, observe that by the uniqueness of the weight space decomposition in Theorem 19.1.2, its formation commutes with scalar extension. The formation of intersection also commutes with scalar extension. So we may assume without loss of generality that $k = \bar{k}$. Now $V_\lambda = \{v \in V : t.v = \lambda(t)v \text{ for all } t \in T(k)\}$ because $T(k) \subset T$ is dense. As W_λ has a similar description, the claim follows.

Example 19.1.6. Let T be the diagonal torus in GL_r . Then $X(T) = \bigoplus \mathbb{Z}_{\lambda_i}$ where $\lambda_i : T \xrightarrow{\text{pr}_i} \mathbb{G}_m$ is the projection onto the i th diagonal entry. Consider $T \subset \text{GL}_r \xrightarrow{\text{Ad}} \text{GL}(\mathfrak{gl}_r) = \text{Aut}(\text{Mat}_r(k))$. [Recall that the adjoint representation is given by $\text{Ad}(g)(X) = gXg^{-1}$ because $g(1 + \epsilon X)g^{-1} = 1 + \epsilon gXg^{-1}$, where we identify vectors in the Lie algebra with deformations of the identity in $\text{GL}_r(k[\epsilon])$.]

We would like to describe explicitly the weight space decomposition of \mathfrak{gl}_n into T -stable lines. One obvious T -stable piece is the diagonal

$$\text{Lie}(T) = \mathfrak{t} = \left\{ \begin{pmatrix} * & & \\ & \ddots & \\ & & * \end{pmatrix} \right\} \subset \mathfrak{gl}_r.$$

Since T conjugates the diagonal trivially, this has trivial T -action, so \mathfrak{t} is an r -dimensional part of the $\lambda = 0$ weight space. As we will see in a moment, it is the whole 0 -weight space.

In general, the other weight spaces are spanned by the elementary matrices $e_{ij} \in \mathfrak{gl}_n$. Let

$$t = \text{diag}(t_1, \dots, t_r) \in T(R).$$

Then we easily compute

$$\text{Ad}(t)(e_{ij}) = te_{ij}t^{-1} = \frac{t_i}{t_j}e_{ij} = \frac{\lambda_i(t)}{\lambda_j(t)}e_{ij} = (\lambda_i - \lambda_j)(t)e_{ij}$$

where the switch between additive and multiplicative notation when thinking about characters is something that just takes getting used to.

So all non-diagonal elementary matrices span nonzero weight spaces, which are pairwise disjoint, and e_{ij} spans the $\lambda_i - \lambda_j$ weight space. All weight spaces with $\lambda \notin \{0\} \cup \{\lambda_i - \lambda_j : i \neq j\}$ vanish. In sum, the nonzero weight spaces of $\text{Ad} = \mathfrak{gl}_r$ are

$$\text{Ad}_0 = \mathfrak{t}, \text{ of dimension } r$$

$\text{Ad}_{\lambda_i - \lambda_j} = \text{Span}(\mathbf{e}_{ij})$, of dimension 1, for $i > j$

$\text{Ad}_{-(\lambda_i - \lambda_j)} = \text{Span}(\mathbf{e}_{ji})$, of dimension 1, for $i > j$.

Observe that all the characters λ corresponding to nonzero weight spaces factor through the **adjoint torus** $\mathbf{T}/\mathbf{Z}_{\text{GL}_r} \subset \text{PGL}_r$, so are in $X(\mathbf{T}/\mathbf{Z}_{\text{GL}_r}) \subset X(\mathbf{T})$; this is unsurprising since conjugation by the center always acts trivially. The adjoint torus has dimension $r - 1$ and corresponds to the hyperplane $\Lambda_0 = \{\vec{n} \in \Lambda : \sum n_i = 0\} \subset \Lambda$.

Caution: it is *not* always the case that the eigencharacters of a maximal split subtorus \mathbf{T} of a linear algebraic group \mathbf{G} span the character group of the adjoint torus; however, in this example they do. (E.g. for $r = 3$ one can draw these characters inside Λ_0 and see the A_2 root system, which spans Λ_0 .)

19.2 Proof of Theorem 19.1.2

The proof will use Yoneda's lemma rather heavily, so watch out.

Work, for the moment, in the generality of any affine k -group \mathbf{G} ; later we will specialize to $\mathbf{G} = \mathbf{T}$. A functorial linear representation of \mathbf{G} on a k -module V is the data of maps $\rho(\mathbf{g}) \in \text{End}_R(V_R)$ for all $\mathbf{g} \in \mathbf{G}(R)$, which satisfy certain multiplicativity and identity axioms, and in particular these force all the $\rho(\mathbf{g})$ to be automorphisms; moreover functoriality in R is obviously required. Now $\rho(\mathbf{g}) \in \text{Hom}_R(V_R, V_R)$ corresponds uniquely to $[g] \in \text{Hom}_k(V, V_R)$.

By Yoneda's lemma, all of the above data is equivalent to the data of $\rho(\mathbf{g}_0) \in \text{End}_{k[\mathbf{G}]}(V_{k[\mathbf{G}]})$ coming from $\mathbf{g}_0 = \mathbf{1}_{k[\mathbf{G}]} : k[\mathbf{G}] \rightarrow k[\mathbf{G}]$ viewed as a point of $\mathbf{G}(k[\mathbf{G}])$, satisfying certain properties corresponding to the multiplicativity and identity axioms. This again is equivalent to the data of $\alpha_\rho = [g_0] : V \rightarrow V \otimes_k k[\mathbf{G}]$, a k -linear map satisfying certain properties, which we will make specific in the case $\mathbf{G} = \mathbf{T}$ in a moment.

Take $\mathbf{G} = \mathbf{T} = \mathbf{G}_m^r$. Then $k[\mathbf{G}] = k[X_1^{\pm 1}, \dots, X_r^{\pm 1}] = k[\Lambda] = \bigoplus_{\lambda \in \Lambda} k\mathbf{e}_\lambda$ is a free k -algebra with basis $\{\mathbf{e}_\lambda : \lambda \in \Lambda\}$ where $\mathbf{e}_{\vec{n}} = \prod X_i^{n_i}$ when viewed as an element of the Laurent polynomial ring. Thus the map α_ρ coming from our given k -linear representation ρ of \mathbf{T} on V is a map

$$\alpha_\rho : V \rightarrow V \otimes_k k[\Lambda]$$

$$v \mapsto \sum_{\text{finite}} f_\lambda(v) \otimes \mathbf{e}_\lambda$$

and its properties are encoded by properties of the coefficient functions $f_\lambda : V \rightarrow V$.

First of all, since α_ρ is k -linear, so are all the f_λ 's.

Next, unwinding the proof of Yoneda's lemma, we see that for all $\mathbf{t} \in \mathbf{T}(R)$ and $v \in V_R$ we have

$$\mathbf{t}.v = \sum \lambda(\mathbf{t})f_\lambda(v) \in V_R \tag{\dagger}$$

(ramping up f_λ to a map $V_R \rightarrow V_R$).

The condition that ρ is multiplicative says that for all k -algebras R , and for all $\mathbf{t}, \mathbf{t}' \in \mathbf{T}(R)$, $v \in V_R$, we have

$$\sum_{\lambda \in \Lambda} \lambda(\mathbf{t}\mathbf{t}')f_\lambda(v) = \sum_{\lambda, \mu \in \Lambda} \lambda(\mathbf{t})\mu(\mathbf{t}')(f_\lambda \circ f_\mu)(v).$$

If we take $(\mathbf{t}, \mathbf{t}')$ to be the universal pair of R -points of \mathbf{T} , namely a point $(\mathbf{t}, \mathbf{t}') \in \mathbf{T}(k[\mathbf{T} \times \mathbf{T}])$, the previous equation yields

$$f_\lambda \circ f_\mu = \begin{cases} 0, & \lambda \neq \mu, \\ f_\lambda, & \lambda = \mu. \end{cases}$$

For details on this, see [CGP, A.8.8]. In other words, $f_\lambda : V \rightarrow V$ is a projection onto a subspace V_λ , and the V_λ 's are pairwise disjoint.

By the above, we see that \mathbf{T} acts by λ on V_λ .

So it remains only to show that $\sum V_\lambda = V$. Using the identity axiom for ρ , and taking $\mathbf{t} = 1$ in (\dagger) , we find that for all $v \in V$,

$$v = \sum f_\lambda(v)$$

which says $v \in \sum V_\lambda$.

Combining the above, $V = \bigoplus V_\lambda$ is a direct sum of λ -eigenspaces, with projections given by f_λ . \square

An important corollary (which is not obviously, but is in fact, related to Theorem 19.1.2) is the following.

Corollary 19.2.1 (Homework 8). *If k is a field, Y is a smooth separated k -scheme of finite type, and a (not necessarily split!) k -torus T acts on Y , then the closed subscheme $Y^T \subset Y$ given by functorial fixed-points of the T -action on Y is smooth.* \square

Example 19.2.2. If T is a subtorus of a smooth k -group G of finite type upon which T acts upon by conjugation, then $Z_G(T) = G^T$ is smooth.

20 February 26

20.1 k -split solvable groups

Recall from Homework 5 that the category of k -tori is anti-equivalent to the category of finite free abelian groups equipped with a continuous discrete action by $\Gamma = \text{Gal}(k_s/k)$. Given an exact sequence of algebraic groups

$$1 \rightarrow T' \rightarrow T \rightarrow T'' \rightarrow 1$$

if T' and T are tori then so is T'' because it is smooth connected affine and its geometric points are semisimple. By Homework 7 we get an exact sequence of Γ -lattices

$$0 \leftarrow X(T') \leftarrow X(T) \leftarrow X(T'') \leftarrow 0.$$

If T' and T'' are k -split then $X(T'')$ and $X(T')$ have trivial Γ -action, which forces $X(T)$ to have trivial Γ -action, so T is also split. This fact that splitting is respected by extensions is particular to groups of “multiplicative type”. In particular, it has no analogue for unipotent groups.

The splitting behavior of multiplicative and unipotent groups also contrasts in the type of field extensions over which these groups split: as we know, tori split over *separable* field extensions, but as the next lemma shows, to guarantee that a unipotent group splits we should go to the *perfect* closure (rather than the separable closure).

Lemma 20.1.1. *Let $U \neq 1$ be a smooth connected unipotent group over a perfect field k . Then U has a composition series*

$$1 = U_m \triangleleft U_{m-1} \triangleleft U_{m-2} \triangleleft \cdots \triangleleft U_1 \triangleleft U_0 = U$$

such that the successive quotients U_i/U_{i+1} are all k -isomorphic to \mathbf{G}_a .

Proof. Choose a faithful representation $U \hookrightarrow U'$ into a standard upper triangle unipotent group U' . We can see by hand that U' has such a composition series, say $\{U'_i\}_{i=0}^N$. (First decompose into the successive subgroups, all normal in U' , with 0's on the first several superdiagonals. Each subquotient is abelian, isomorphic to a power of \mathbf{G}_a . Now just refine these to obtain the desired composition series.) Define $U_i = (U'_i \cap U)_{\text{red}}^0$. This is connected by fiat, geometrically reduced because k is perfect, and thus is a smooth k -subgroup of U .

It is easy to check that $U_{i+1} \triangleleft U_i$, as normality can be checked on geometric points. Now the subquotient U_i/U_{i+1} is smooth and connected because U_i is such, and has dimension ≤ 1 because $U'_i/U'_{i+1} \simeq \mathbf{G}_a$ does, and it is unipotent because U is. So if U_i/U_{i+1} is nontrivial, it must be geometrically \mathbf{G}_a , and hence isomorphic over k to \mathbf{G}_a because k is perfect (see Homework 2). \square

Example 20.1.2. The lemma is false if k is not perfect. Take k'/k to be a degree p purely inseparable extension of an imperfect field k of characteristic p . Then $R_{k'/k}(\mathbf{G}_m)$ is a smooth p -dimensional k -group with a natural subgroup \mathbf{G}_m ; the quotient $R_{k'/k}(\mathbf{G}_m)/\mathbf{G}_m$ is a $(p-1)$ -dimensional smooth p -torsion group. On Homework 9 it is shown that it is actually unipotent, and contains no k -subgroup isomorphic to \mathbf{G}_a !

Definition 20.1.3. A **k -split solvable group** is a solvable smooth connected¹³ affine k -group G with a composition series $\{G_i\}$ by k -subgroups so that $G_i/G_{i+1} \simeq \mathbf{G}_a$ or \mathbf{G}_m (over k) for all i .

¹³Some authors leave out connectedness, and so must change the definition!

Example 20.1.4. A k -torus T is k -split in the usual sense if and only if it is so in the sense of Definition 20.1.3. (Use character theory, as remarked at the start of this section.)

Example 20.1.5. If $k = \bar{k}$ then any solvable smooth connected k -group is k -split.

Proof. Using the derived series $\{\mathcal{D}^i G\}$ we can treat each commutative subquotient $\mathcal{D}^i G / \mathcal{D}^{i+1} G$ separately. So without loss of generality G is commutative. Thus, by Theorem 17.3.1, $G \simeq T \times U$ for a torus T and a unipotent group U . So we can treat tori and unipotent groups separately, and this will suffice. Now since $k = \bar{k}$, we have both $k = k_s$ and $k = k_p$. The first guarantees that tori split, and the second (by Lemma 20.1.1) guarantees that unipotent groups split. \square

Example 20.1.6. (i) If $G \twoheadrightarrow G''$ is a surjective k -homomorphism of smooth connected affine k -groups and G is k -split solvable, then so is G'' .

(ii) If $G' \hookrightarrow G$ is an injective k -homomorphism of smooth connected affine k -groups, k is perfect, and G is k -split solvable, then so is G' .

Proof. (ii) Since k is perfect, the property of being \mathbf{G}_a can be checked over \bar{k} . Thus, by using the $(G_i \cap G')_{\text{red}}$ -trick we just have to observe that if $H \twoheadrightarrow \mathbf{G}_m$ is a k -isogeny and H is smooth and connected then $H \simeq \mathbf{G}_m$ over k . To prove this final k -isomorphism claim, first note that $\dim H = 1$ so $H_{\bar{k}} \simeq \mathbf{G}_a$ or \mathbf{G}_m . But \mathbf{G}_a is impossible since there are no nontrivial homomorphisms $\mathbf{G}_a \rightarrow \mathbf{G}_m$. So H is a 1-dimensional torus, and $X(H)$ is isogenous to the trivial Galois lattice \mathbf{Z} , and is thus itself trivial. So $H \simeq \mathbf{G}_m$.

(i) Take the image of a splitting solvability series for G ; we'd like to show it is a splitting solvability series for G'' . This reduces to showing that if \mathbf{G}_a or \mathbf{G}_m maps isogenously onto H then H is accordingly isomorphic to \mathbf{G}_a or \mathbf{G}_m over k . By much the same method as in (ii), the \mathbf{G}_m case is fine. For the \mathbf{G}_a case, consider the diagram

$$\begin{array}{ccc} \mathbf{G}_a & \xrightarrow{f} & H \\ \downarrow & & \downarrow \\ \mathbf{P}_k^1 & \xrightarrow{\exists \bar{f}} & \bar{H} \end{array}$$

where \bar{H} is the regular compactification of the curve H . The map \bar{f} is finite, and a finite extension of Dedekind domains is flat, so \bar{f} is flat. But is \bar{H} actually smooth? That is, does it remain Dedekind after a ground field extension to \bar{k} ? For this we will apply the following Claim after scalar extension to \bar{k} :

Claim 20.1.7. If $A \hookrightarrow B$ is a finite flat inclusion into a Dedekind domain, then A is Dedekind as well.

Proof of claim. A is clearly a domain. Its nonzero primes are maximal since this is true for B , and B is A -finite. Thus $\dim A = 1$, so it remains to prove regularity. Since we are in dimension 1, this is equivalent to the invertibility of nonzero ideals as A -modules. Since A is integral, that is equivalent to the flatness of all ideals. Since $A \rightarrow B$ is finite flat injective, it is faithfully flat. Hence I is A -flat if and only if I_B is B -flat. But $I_B \rightarrow IB$ is an isomorphism since B is A -flat. Hence it's enough to show $IB \triangleleft B$ is B -flat. But B is Dedekind, so we win. \square

Remark 20.1.8. There is a vast generalization: a Noetherian commutative ring with a regular faithfully flat extension is regular. This is shown in [Mat, 23.7(i)] using Serre's homological criterion of regularity.

Let us return to the proof of (i) in the example. Now \mathbf{P}_k^1 is geometrically regular, and the “finite flatness” of the surjective \bar{f} is preserved by any ground field extension, so by the Claim we see that \bar{H} is geometrically regular, i.e. smooth. Thus \bar{H} is a smooth projective curve, and by Riemann-Hurwitz considerations it must have genus zero (even though \bar{f} may be highly inseparable, etc.). Moreover $\bar{f}(\infty)$ is a k -rational point of \bar{H} , so in particular $\bar{H}(k) \neq \emptyset$. So $\bar{H} \simeq \mathbf{P}_k^1$ and thus $H = \bar{H} - \bar{f}(\infty) \simeq \mathbf{A}_k^1$ as a curve. By our classification of 1-dimensional smooth connected k -groups, we know this implies $H = \mathbf{G}_a$ as k -groups. \square

20.2 Borel Fixed Point Theorem

Theorem 20.2.1. *Let X be a proper k -scheme, $X(k) \neq \emptyset$, and suppose X is equipped with an action of a k -split solvable group G . Then $X(k)$ contains a G -fixed point (i.e. the corresponding orbit map $G \rightarrow X$ is the constant map).*

Proof. We induct on $d = \dim G$. The case $d = 0$ is fine, so we'll skip that. If $d = 1$ then $G = \mathbf{G}_a$ or \mathbf{G}_m . Equipping G with the left-translation action, if we fix a rational point $x_0 \in X(k)$, the orbit map $g \mapsto gx_0 : G \rightarrow X$ is G -equivariant. Now $G \hookrightarrow \overline{G} \simeq \mathbf{P}_k^1$ sits inside its regular compactification \mathbf{P}_k^1 , and by inspect the left translation action on G extends to \mathbf{P}_k^1 fixing any added points. Thus by the valuative criterion of properness, the orbit map $G \rightarrow X$ extends to a G -equivariant map $\mathbf{P}_k^1 \rightarrow X$. (To prove G -equivariance, observe that it holds on a dense open and X is proper, so separated, so this is enough.) In particular the image of ∞ (which is G -fixed in \mathbf{P}_k^1 for both $G = \mathbf{G}_a$ and $G = \mathbf{G}_m$) is a G -fixed rational point of X .

Next suppose $d > 1$. Then there exists a codimension 1 k -split solvable normal subgroup $G' \triangleleft G$. By induction there exists $x' \in X(k)$ which is G' -fixed. The corresponding orbit map $G \rightarrow X$ induces (by the universal property of quotients) a map $G/G' \rightarrow X$ which is equivariant for the obvious G -action on G/G' . But this quotient is again \mathbf{G}_a or \mathbf{G}_m , so repeating the argument from the case $d = 1$ we get a G/G' -equivariant, and hence G -equivariant, map $\mathbf{P}_k^1 \rightarrow X$. The image of ∞ gives us the point we want. \square

Corollary 20.2.2 (Lie-Kolchin theorem). *If G is k -split solvable, then any representation $\rho : G \rightarrow \mathrm{GL}(V)$ can be conjugated over k into the upper triangular subgroup of $\mathrm{GL}(V)$.*

Proof. Let X be the smooth projective variety of full flags in V . It has a natural G -action via ρ . A rational G -fixed point is precisely a flag in V which is preserved by G acting on V via ρ . So taking a basis for V adapted to this flag proves the corollary. \square

Corollary 20.2.3. *If G is k -split solvable then $G = T \ltimes U$ for a k -split torus T and a k -split unipotent group U , although this expression is not unique.*

Proof. We will discuss this next time. (The proof uses Corollary 20.2.2.) \square

Corollary 20.2.4. *If G is a smooth connected solvable affine group then $\mathcal{D}G$ is unipotent.*

We will prove this final corollary next time.

21 March 1

21.1 Remark on quotients

See Appendix D to resolve the following outstanding issue concerning quotients. To really work effectively with quotients, and in particular to make induction arguments go through, e.g. for proving facts about solvable groups, it is essential to know that quotients respect certain basic properties. We also would really like some basic facts like the “second isomorphism theorem” $H'/H'' \xrightarrow{\sim} \overline{H'}/\overline{H''}$ where $\overline{}$ denotes the reduction of a subgroup $H \subset K \subset G$ to G/H for $H \triangleleft G$, say.

What is shown in Appendix D is that

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/H \\ \uparrow & & \uparrow \\ Z = \pi^{-1}\overline{Z} & \xrightarrow{\pi|_Z} & \overline{Z} \end{array}$$

sets up a bijection

$$\begin{array}{ccc}
\{\text{H-stable closed subschemes } Z \subset G\} & \xlongequal{\quad} & \{\text{closed subschemes } \bar{Z} \subset G/H\} \\
\uparrow & & \uparrow \\
\{\text{closed subgroups } H \subset H' \subset G\} & \xlongequal{\quad} & \{\text{closed subgroups } \bar{H}' \subset G/H\} \\
\uparrow & & \uparrow \\
\{\text{normal ones}\} & \xlongequal{\quad} & \{\text{normal ones}\}
\end{array}$$

etc. and everything behaves well with respect to smoothness.

21.2 Lie-Kolchin Corollary 20.2.4

To recapitulate the proof of Corollary 20.2.4, we wish to prove that if G is a solvable smooth connected affine k -group then $\mathcal{D}G$ is unipotent. Without loss of generality we can take $k = \bar{k}$, since unipotency can be detected on geometric points and the formation of derived subgroups is compatible with scalar extension. So G is k -split solvable, so the Lie-Kolchin Theorem 20.2.2 applies. That theorem says we can embed $G \hookrightarrow B_n$, the standard upper triangular subgroup of GL_n , for some n . So we obtain $\mathcal{D}G \hookrightarrow \mathcal{D}(B_n)$. Now $B_n = T \ltimes U$ is the semidirect product of the unipotent upper triangular subgroup $U = U_n \triangleleft B_n$ and the diagonal torus T . In particular $\mathcal{D}(B_n) \subset U_n$, since T is commutative so the commutators of the T -part die in $\mathcal{D}(B_n)$. But U_n is unipotent, and a subgroup of a unipotent is unipotent (e.g. by functoriality of Jordan decomposition), so the claim follows.

Remark 21.2.1. If G is k -split solvable then one can actually show $\mathcal{D}G$ is k -split solvable. See [Springer, Thm. 14.3.8(i)]. The idea is to prove a more robust (easier to check) criterion for k -split solvability than the definition, along the lines of being dominated as a variety by a product of \mathbf{G}_a 's and \mathbf{G}_m 's, which is amenable to proving this particular claim.

21.3 Structure theory of solvable groups

What is the general structure of a solvable smooth connected linear algebraic k -group? In general this is very mysterious. But if G is k -split then we will see shortly that $G = T \ltimes U$ is a semidirect product of a k -split torus T and a k -split unipotent group U .

Warning! T is far from unique – e.g. one can conjugate it by any rational point of U . On the other hand we will see that U is intrinsic to G ; it is the so-called *unipotent radical*.

Here is the idea: By Corollary 20.2.4, if G is k -split solvable then $\mathcal{D}G$ is unipotent. Consider the projection

$$\pi: G \twoheadrightarrow G/\mathcal{D}G.$$

The quotient $G/\mathcal{D}G$ is k -split commutative (since the image of a split solvable group is split solvable; see Example 20.1.6(i)). By Theorem 17.3.1, it follows that $G/\mathcal{D}G = T_0 \times U_0$ is the product of a split torus T_0 and a split unipotent group U_0 . Set $U = \pi^{-1}U_0$; this is unipotent and is the natural candidate for the decomposition $G = T \ltimes U$.

The problem is how to lift T_0 to a torus $T \subset G$. For example, given a short exact sequence

$$1 \rightarrow \mathbf{G}_a \rightarrow G \rightarrow \mathbf{G}_m \rightarrow 0$$

is it automatic that $G = \mathbf{G}_m \ltimes \mathbf{G}_a$ using some action $tx = t^n x$ ($t \in \mathbf{Z}$) of \mathbf{G}_m on \mathbf{G}_a ? It's not entirely clear how we find the \mathbf{G}_m inside G .

We now state the general result (already mentioned last time):

Proposition 21.3.1. *Let G be a k -split solvable group. Then $G = T \ltimes U$ for a k -split torus T and a k -split unipotent group U (which is necessarily $\mathcal{R}_{u,k}(G)$; see the next section).*

We emphasize again that U is intrinsic, but T is *not*.

Proof. The commutative case is already done by Theorem 17.3.1. In the general case, a delicate induction on $\dim G$ is required, using a splitting composition series (i.e. one with consecutive subquotients equal to \mathbf{G}_a or \mathbf{G}_m).

There are two problems to deal with. (1) The terms in the composition series need not be normal in the whole group. (2) Smooth connected subgroups of k -split solvable groups are solvable, but need not be k -split.

The crucial input for the induction is Tits' structure theory for (smooth connected) unipotent groups, which is described in [CGP, App. B].

The issue comes down to two crucial cases:

$$1 \rightarrow \mathbf{G}_a \rightarrow G \rightarrow \mathbf{G}_m \rightarrow 1,$$

$$1 \rightarrow \mathbf{G}_m \rightarrow G \rightarrow \mathbf{G}_a \rightarrow 1.$$

In the first case we must lift \mathbf{G}_m back up to G ; in the second we not only need to lift \mathbf{G}_a , but to do so essentially uniquely, and after the fact we should find that $G = \mathbf{G}_a \times \mathbf{G}_m$ is commutative.

All of this is worked out in detail in §2–§3 of Appendix D, where the method is to view G in the exact sequences above as a torsor for the subgroup, in the étale topology. Borel's method in [Bor] is to work with the Lie algebras. \square

21.4 Unipotent radical

In the following lemma, we will find an intrinsic unipotent normal subgroup in a smooth affine k -group G , which is thus a **characteristic subgroup** of G , in the classical group theoretic sense of being uniquely determined by G and thus invariant under all automorphisms of G , which is a very useful property.

Lemma 21.4.1. *Let G be a smooth affine k -group. There exists a (necessarily unique)*

$$\text{unipotent normal smooth connected } k\text{-subgroup of } G \tag{*}$$

(denoted $\mathcal{R}_{u,k}(G)$) containing all subgroups of G satisfying (*).

Proof. The problem is to show that any two subgroups of G satisfying (*) are both contained in a third. This shows that there is a unique subgroup of G which is maximal for the conditions (*). (The assertion here is the uniqueness of the maximal one, since existence follows from connectedness and dimension considerations.)

So let $U, U' \subset G$ satisfy (*). Then since $U' \triangleleft G$, the semidirect product $U \ltimes U'$ makes sense. It is unipotent since it sits in a short exact sequence of unipotent groups, and Jordan decomposition is functorial. There is a natural map

$$U \ltimes U' \rightarrow G$$

and the image is precisely the subgroup $U \cdot U' \subset G$ generated by U and U' . This is smooth and connected by the general theory of the subgroups generated by smooth connected subvarieties. It is the image of the unipotent group $U \ltimes U'$, and hence unipotent. Finally, it is normal because U and U' are. (This is just a fact from group theory, done on geometric points: two normal subgroups of a big group generate a normal subgroup of the big group.) Thus $U \cdot U'$ satisfies (*). \square

Definition 21.4.2. The subgroup $\mathcal{R}_{u,k}(G) \triangleleft G$ of Lemma 21.4.1 is called the k -unipotent radical of G .

Here are some basic properties of the unipotent radical.

Proposition 21.4.3. (i) $\mathcal{R}_{u,k}(G)_K \subset \mathcal{R}_{u,K}(G_K)$ for all field extensions K/k , and if $K = k_s$ then equality holds.

(ii) $\mathcal{R}_{u,k}(G^0) = \mathcal{R}_{u,k}(G)$.

Proof. (i) is elementary; just use Galois descent.

(ii) $\mathcal{R}_{u,k}(G)$ is unipotent, smooth, connected and normal in G . It is thus contained in G^0 and therefore normal in G^0 . So certainly $\mathcal{R}_{u,k}(G^0) \supset \mathcal{R}_{u,k}(G)$. For the reverse inclusion it is enough to show that $\mathcal{R}_{u,k}(G^0) \triangleleft G$. By (i) we can assume without loss of generality that $k = k_s$. Then $G(k) \subset G$ is dense. It is therefore enough to show that conjugation by $G(k)$ preserves $\mathcal{R}_{u,k}(G^0)$. And this is true because such conjugations are honest k -group automorphisms of G^0 , which must preserve the characteristic subgroup $\mathcal{R}_{u,k}(G^0)$. \square

Remark 21.4.4. One might ask why we allow disconnected G in the definition of the unipotent radical, since by Proposition 21.4.3(ii) the component group of G is not detected by $\mathcal{R}_{u,k}(G)$. An example is the centralizer of $g = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in G(k) = \mathrm{PGL}_2(k)$. We have $Z_{\mathrm{PGL}_2}(g) = D \sqcup D \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ where $D \subset \mathrm{PGL}_2$ is the diagonal torus. This is an interesting (from a group theoretic perspective) yet disconnected group, whose structure we might wish to analyze to study PGL_2 .

Example 21.4.5 (Homework 9). If $G \in \{\mathrm{SL}_n, \mathrm{GL}_n, \mathrm{PGL}_n, \mathrm{Sp}_{2n}, \mathrm{SO}_n\}$ over any field k then $\mathcal{R}_{u,k}(G) = 1$.

Remark 21.4.6. One must be careful: in [CGP, Ex. 1.1.3] there is given an example over *any* imperfect field of a smooth affine k -group G such that $\mathcal{R}_{u,k}(G) = 1$ but $\mathcal{R}_{u,\bar{k}}(G_{\bar{k}}) \neq 1$!

Proposition 21.4.7. *If K/k is a separable (not necessarily even finitely generated!) extension of fields then $\mathcal{R}_{u,k}(G)_K = \mathcal{R}_{u,K}(G_K)$.*

Proof. Without loss of generality we can take $k = k_s, K = K_s$. From here one must use a “specialization” argument; see [CGP, Prop. 1.1.9(1)]. The idea: if the unipotent radical is bigger after going up to K , then it must become bigger over some finitely generated subextension field K_0/k . Now K_0 is the function field of a smooth k -variety X , and specialization at separable algebraic points is available (after “spreading out” over a dense open subscheme of X). \square

21.5 Reductive groups

We often write \mathcal{R}_u rather than $\mathcal{R}_{u,k}$ when k is algebraically closed.

Definition 21.5.1. Let G be a smooth affine k -group. We say G is *pseudo-reductive* over k if G is connected and the k -unipotent radical is trivial: $\mathcal{R}_{u,k}(G) = 1$. We say G is *reductive* if G is (not necessarily connected but) the geometric unipotent radical is trivial: $\mathcal{R}_u(G_{\bar{k}}) = 1$.

(Allowing G to be disconnected in the definition of reductive groups over fields is a matter of convention. In contrast, for a good relative theory over rings as in [SGA3] or [C] one must stick to the connected case.)

Remark 21.5.2. If $\mathrm{char}(k) = 0$ it turns out that reductivity (without the connectedness condition) is equivalent to complete reducibility for all finite-dimensional representations; that is the reason for the terminology!

Lemma 21.5.3. *Let G be a smooth affine k -group and $N \triangleleft G$ a smooth normal closed k -subgroup. Then $\mathcal{R}_u(N_{\bar{k}}) = (N_{\bar{k}} \cap \mathcal{R}_{u,\bar{k}}(G_{\bar{k}}))_{\mathrm{red}}^0$.*

Corollary 21.5.4. *Reductivity passes to smooth normal subgroups.* \square

Proof of Lemma 21.5.3. Without loss of generality $k = \bar{k}$. Now $(N \cap \mathcal{R}_{u,k}(G))_{\mathrm{red}}^0$ is unipotent since it is contained in the unipotent radical. It is connected since we passed to the connected component. It is smooth since we passed to the underlying reduced. Since $k = \bar{k}$ it is actually a group (geometrically connected, geometrically reduced). It is normal in G since the intersection of normal subgroups is normal and passing to $(\cdot)_{\mathrm{red}}^0$ preserves normality. Finally it is contained in N , as is clear. So the inclusion $\mathcal{R}_u(N) \supset (N \cap \mathcal{R}_u(G))_{\mathrm{red}}^0$ is obvious.

For the reverse inclusion, it suffices to show that $\mathcal{R}_u(N) \triangleleft N$ is normal in G , not just in N . This is true because $N \triangleleft G$ is normal and $\mathcal{R}_u(N)$ is a characteristic subgroup of N , so conjugating by rational points (which are dense in G) must preserve it. \square

Lemma 21.5.5. *Let*

$$1 \rightarrow G' \rightarrow G \rightarrow G'' \rightarrow 1$$

be a short exact sequence of smooth affine k -groups. If G', G'' are reductive then so is G .

Proof. Exercise. The basic idea is that $G \twoheadrightarrow G''$ takes $\mathcal{R}_u(G_{\bar{k}})$ to $\mathcal{R}_u(G''_{\bar{k}})$ because surjections take normal subgroups to normal subgroups and the image of a unipotent thing is unipotent. Thus since G'' is reductive, $\mathcal{R}_u(G_{\bar{k}}) \subset G'_{\bar{k}}$. But it is normal in $G_{\bar{k}}$, hence normal in $G'_{\bar{k}}$, and it is smooth connected unipotent, so it is contained in $\mathcal{R}_u(G'_{\bar{k}}) = 1$ by reductivity of G' . \square

Example 21.5.6. Take

$$P = \begin{pmatrix} GL_2 & \star \\ 0 & GL_3 \end{pmatrix} \subset GL_5.$$

Then

$$\mathcal{R}_{u,k}(P) = \begin{pmatrix} 1_2 & \star \\ 0 & 1_3 \end{pmatrix} = \ker(P \twoheadrightarrow GL_2 \times GL_3).$$

Example 21.5.7. A non-example: note that $U \hookrightarrow GL_n$ for any unipotent group U . Obviously $\mathcal{R}_{u,k}(U) = U$ but GL_n is reductive. The point is that $\mathcal{R}_{u,k}$ is only functorial for normal inclusions and arbitrary surjections, but not more general k -homomorphisms.

Example 21.5.8. Let G be smooth connected and affine. Then $G/\mathcal{R}_{u,k}(G)$ is pseudo-reductive (over k), and if k is perfect then $G/\mathcal{R}_{u,k}(G)$ is reductive.

22 March 3

22.1 Borel subgroups

Theorem 22.1.1. *Let G be a smooth connected affine group over $k = \bar{k}$.*

(i) *Let R (for “radical”) denote a*

solvable smooth connected k -subgroup (†)

*of G . (Such will be called a (†)-subgroup of G in the sequel.) Then R is maximal among (†)-subgroups of G , if and only if G/R is proper. If this is the case we call R a **Borel subgroup** of G .*

(ii) *All Borel subgroups of G are $G(k)$ -conjugate.*

Remark 22.1.2. By Theorem 18.1.1, G/R is automatically quasi-projective for any closed k -subgroup $R \subset G$. So G/R is proper if and only if it is projective.

Proof. First assume the following.

Lemma 22.1.3. *If R is a (†)-subgroup of dimension maximal among the dimensions of all (†)-subgroups, then G/R is proper.*

Note that the hypothesis of the lemma is stronger than the condition that R is maximal among (†)-subgroups; this is because a priori (before proving (ii) of the theorem) we do not know that all maximal (†)-subgroups are of the same dimension.

Granting the lemma, let us deduce the theorem. Consider any (†)-subgroup $R' \subset G$. Then R' is k -split solvable since $k = \bar{k}$ and $R' \curvearrowright G/R$, which is proper by Lemma 22.1.3. So by the Borel fixed point Theorem 20.2.1, R' fixes a coset in $(G/R)(k)$. By Theorem 18.1.1, this coset is of the form gR for some $g \in G(k)$, since $k = \bar{k}$. That R' fixes gR says precisely that $R' \subset gRg^{-1}$. Now gRg^{-1} is the conjugate of a (maximal) (†)-subgroup. So if R' is a *maximal* (†)-subgroup, it must equal gRg^{-1} , and thus both have the same dimension as R and be conjugate to R by $G(k)$. Conversely if G/R' is proper then by the same reasoning (reversing the roles of R and R') we find $R \subset gR'g^{-1}$ and so by maximality of R , $R = gR'g^{-1}$. Thus $\dim R' = \dim R$ is maximal among (†)-subgroups, so in particular R' is a maximal (†)-subgroup.

It remains to do the hardest, but coolest, part: prove Lemma 22.1.3. So fix a (†)-subgroup R of maximal dimension. We need to show G/R is proper. Choose a faithful representation $\rho : G \hookrightarrow GL(V)$ such that $R = N_G(L)$ for a line $L \subset v$ under the resulting action $G \curvearrowright V$. Look at the action of R on the flag variety $\text{Flags}_{\text{full}}(V/L)$, which is proper. Since R is k -split solvable, the Borel fixed point Theorem 20.2.1 entails that R fixes a flag in V/L . We can lift this to a maximal flag \mathcal{F} in V starting with L . Let $X = \text{Flags}_{\text{full}}(V)$ and $x \in X(k)$ the point corresponding to \mathcal{F} . Observe that $R \subset \text{Stab}_G^p(x) \subset N_G(L) = R$, where the first inclusion is because R preserves the flag \mathcal{F} and the second is because any g which preserves the flag preserves the first subspace L in it. Hence $R = \text{Stab}_G(x)$.

From our construction of quotients (Theorem 18.1.1) this implies that the orbit map $G \twoheadrightarrow Gx \subset X$ is precisely the quotient G/R . Since X is proper, it is therefore enough to show that $Gx \subset X$ is closed. By the closed orbit lemma 9.3.5, it therefore suffices to show that Gx is an orbit of minimal dimension.

Take $x' = \mathcal{F}' \in X$. Then $Gx' = G/\text{Stab}_G(x')$. Set $R' = \text{Stab}_G(x')_{\text{red}}^0$, which is smooth and connected.

In fact, R' is solvable, because with respect to a basis for V adapted to the flag \mathcal{F}' , R' is a subgroup via ρ of the upper triangular subgroup of $\text{GL}(V)$, which is solvable because it has an obvious composition series, and a subgroup of a solvable group is solvable, as we've seen earlier.

Thus R' is a (\dagger) -subgroup of G . In particular, $\dim R' \leq \dim R$. So $\dim G/R' \geq \dim G/R$.

But $G/R' = G/\text{Stab}_G(x')_{\text{red}}^0 \twoheadrightarrow G/\text{Stab}_G(x')$ has finite fibers: passing to the underlying reduced does not affect the topology and the component group of the finite type k -group $\text{Stab}_G(x')$ is finite. Thus $\dim Gx' = \dim G/\text{Stab}_G(x') = \dim G/R' \geq \dim G/R = \dim Gx$. So Gx' is an orbit of minimal dimension, so we are done. \square

Corollary 22.1.4. *Let $k = \bar{k}$ and G a smooth connected affine k -group. If G is not unipotent, then there exists a nontrivial torus $G_m \subset G$.*

Proof. Let $B \subset G$ be a Borel subgroup, which exists by Theorem 22.1.1. By the structure of split solvable groups (Proposition 21.3.1) we have $B = T \ltimes U$. (Note that B is split solvable because $k = \bar{k}$!) If $T \neq 1$ then the split torus $T \subset B \subset G$ gives such what we want. So we just need to rule out the case $B = U$ when B is unipotent. Assume for contradiction that B is unipotent. Since G is not unipotent, $B \neq G$. So G/B is proper and of *positive* dimension (since G is *connected*). Choose a representation $\rho : G \rightarrow \text{GL}(V)$ such that $B = N_G(L)$ normalizes a line $L \subset V$. So we have a map $B \rightarrow \underline{\text{Aut}}(L) \simeq G_m$. But B is unipotent, so there are no nontrivial such maps. Therefore in fact $B = Z_G(L)$ *centralizes* L . Since L is a line, this is the same as $B = Z_G(v)$ for any nonzero $v \in L$. If we look at the induced orbit map $G/B \simeq Gv \subset V$, we see that it is an isomorphism from a proper variety to a quasi-affine variety. (Since $Gv \subset V$ is locally closed.) Since G/B has positive dimension, this is a contradiction. \square

Corollary 22.1.5. *If $g \in G(\bar{k})$ are semisimple then G is a torus.*

Proof. To check whether G is a torus we can extend scalars, so without loss of generality $k = \bar{k}$. Choose a Borel subgroup $B = T \ltimes U \subset G$. Since $B(k)$ consists only of semisimple points, U must be trivial. Hence $B = T$ is commutative.

If we can show $B \subset Z_G$ (i.e., B is central in G) then in particular $B \triangleleft G$ is normal, so G/B is both affine and proper by Theorem 22.1.1 and Appendix C. Hence G/B would be finite and connected, so trivial, so $G = B$ is a torus.

To show B is central it suffices to show that conjugation by G on any element of $B(k)$ is trivial, since $k = \bar{k}$ (so $B(k) \subset B$ is dense). So pick $b \in B(k)$, and consider $G \rightarrow G$ given by $g \mapsto gbg^{-1}$. Since B is commutative, this induces a map $G/B \rightarrow G$. But this is a map from a proper connected variety to an affine one, hence constant, hence the trivial map. So the conjugation $G \rightarrow G$ on b is trivial as desired. \square

Remark 22.1.6. One consequence of Corollary 22.1.5 is that if

$$1 \rightarrow T \rightarrow G \rightarrow T' \rightarrow 1$$

is an exact sequence of smooth connected affine k -groups with tori T and T' then G is a torus, since the geometric points of G are forced to be semisimple. But this is definitely overkill. Instead, clearly G is solvable, so by extending scalars to \bar{k} and using the structure theory for split solvable groups, we have $G = T'' \ltimes U$. Now it is clear that $U = 1$ since G has semisimple geometric points.

Remark 22.1.7. The proof of Corollary 22.1.5 shows that if G is not solvable then $B \not\triangleleft G$ and B is not commutative. This in fact forces $\dim G \geq 3$: if $\dim G = 1$ then $G = G_a$ or G_m , which are both commutative; if $\dim G = 2$ then since B is solvable and G is not, $\dim B \leq 1$, and there are no noncommutative such groups.

Definition 22.1.8. A *Borel k -subgroup* $B \subset G$ is a solvable smooth connected k -subgroup (i.e. a (\dagger) -subgroup) such that $B_{\bar{k}} \subset G_{\bar{k}}$ is a Borel subgroup in the earlier sense.

This is equivalent to the properness of $G_{\bar{k}}/B_{\bar{k}} = (G/B)_{\bar{k}}$, which by faithfully flat descent is equivalent to the properness of G/B .

Definition 22.1.9. A *parabolic k -subgroup* of G is a smooth k -subgroup $P \subset G$ such that G/P is proper.

Thus a Borel k -subgroup is precisely a solvable connected parabolic k -subgroup. Many examples of parabolic subgroups can be found on Homework 9.

Unfortunately, nontrivial parabolics need not exist over general fields. Fortunately we have another way of digging holes into linear algebraic groups: according to the following amazing theorem of Grothendieck, we can *always* find maximal tori.

Theorem 22.1.10 (Grothendieck). *If G is any smooth affine k -group, there exists a k -torus $T \subset G$ such that $T_{\bar{k}} \subset G_{\bar{k}}$ is a maximal torus.*

Proof. This is a huge deal, very non-trivial. We give a proof in Appendix E based on arguments with finite group schemes (inspired by the proof in [Bor, 18.2(i)] that uses \mathfrak{p} -Lie-algebra techniques). It is recommended to skip this proof and to read it after the course is over. \square

23 March 5

23.1 Properties of parabolics

Let G be a smooth connected affine k -group.

Remark 23.1.1. We saw last time that the parabolicity of a subgroup $P \subset G$ is insensitive to field extension, because properness of the quotient G/P is so insensitive.

Remark 23.1.2. We left connectedness out of the definition of a parabolic k -subgroup, because (it will turn out) we get this for free!

Proposition 23.1.3. *Let $P \subset G$ be a smooth connected closed k -subgroup. Then P is parabolic if and only if $P_{\bar{k}}$ contains a Borel subgroup of $G_{\bar{k}}$.*

Proof. If $P_{\bar{k}}$ contains a Borel B then $G_{\bar{k}}/B$ is proper, and it surjects onto $G_{\bar{k}}/P_{\bar{k}}$, which is separated and finite type (being quasiprojective). Under these conditions, the image of a proper thing is proper, so $P_{\bar{k}}$ and hence P is parabolic.

Conversely suppose P is parabolic. Without loss of generality we can assume $k = \bar{k}$. Thus we can find a Borel $B \subset G$. The split solvable group B acts on the proper quotients G/P , so by the Borel fixed point Theorem 20.2.1 there exists $g \in G(k)$ with $BgP \subset gP$, which says precisely that $g^{-1}Bg \subset P$, so P contains a Borel. \square

The next thing to consider is connectedness of parabolics.

Example 23.1.4. Connectedness results should be appreciated, as we have stressed before. Suppose $H \subset H' \subset G$ is a containment of closed k -subgroups and H is smooth. Then in fact H' is smooth and $H^0 = H'^0$, if and only if $\dim H = \dim H'$, if and only if $\mathfrak{h} \subset \mathfrak{h}'$ is an equality inside \mathfrak{g} . So to prove $H = H'$ (assuming H is smooth) from the Lie algebraic fact $\mathfrak{h} = \mathfrak{h}'$, we need to know H' is connected!

Theorem 23.1.5 (Chevalley). *Let $P \subset G$ be a parabolic k -subgroup of a smooth connected affine k -group G . Then P is connected, and $P = N_G(P)$ on geometric points.*

Proof. We sketch the idea, and will address it in full detail without circularity at the start of the next course (so it is taken on faith for this course, or see [Bor, Thm. 11.16] if you are impatient).

The first observation is that the connectedness of P is very closely related to $P = N_G(P)$: it's easy to see that P^0 is automatically parabolic, and $P^0 \triangleleft P$, so $P \subset N_G(P^0)$; if we knew $N_G(P^0) = P^0$ this gives $P = P^0$ connected.

The ingredients for the proof are the following.

- I. Conjugacy of Borels in $G_{\bar{k}}$, which we have already shown.
- II. The image of a Borel under a quotient map is a Borel. This will be shown in Theorem 23.2.2 below.
- III. The centralizer of a torus is connected. This will be proved next week.
- IV. If $\dim G \leq 2$ then G is solvable. This was shown in Remark 22.1.7. \square

Remark 23.1.6. Granting Chevalley's theorem, $N_G(P)$ is connected because P is connected and $P = N_G(P)$ on geometric points. So by Example 23.1.4 one can prove the scheme theoretic equality $P = N_G(P)$ using the Lie algebras. This is a bit tricky, and will never be needed. (Sketch: Pass to \bar{k} , reduce to the case when G is reductive, and use the structure theory of reductive groups.)

Example 23.1.7. Obviously, by Proposition 23.1.3, a solvable smooth connected affine k -group G contains no proper (i.e. $\neq G$) parabolic subgroups. One thing to watch out for is that this can happen for non-solvable G as well, even connected reductive G .

The phenomenon at the end of the preceding example is best illustrated and understood via the following remarkable and very important result that we mention just for general awareness but will not use in this course and will prove in the next course (it lies way beyond our present scope):

Proposition 23.1.8. *If $G = \mathcal{D}G$ is reductive and perfect, then G is k -isotropic (i.e., contains G_m as a k -subgroup) if and only if G contains a proper parabolic k -subgroup.*

For instance, if D is a finite-dimensional central division k -algebra with $\dim D > 1$, then the group norm-1 units $SL(D)$ is such an example. Likewise, if (V, q) is a non-degenerate quadratic space of dimension at least 3 that is anisotropic (meaning q has no nontrivial zeroes in V) then $SO(q)$ is also such an example.

Here is another result that we mention now for general awareness only:

Proposition 23.1.9. *Let G be a connected reductive group. If k is a local field (allowing \mathbf{R}) then G is k -anisotropic if and only if $G(k)$ is compact in the analytic topology. If k is a global field then G is k -anisotropic if and only if $G(\mathbf{A}_k)/G(k)$ is compact in its analytic topology. \square*

(Again, proving this is beyond our scope; the case of local fields will be revisited in the next course. This result underlies the role of parabolic induction in representation theory because it says that the only connected reductive groups whose structure we can't get a handle on using a non-central k -torus are those whose arithmetically interesting associated spaces for representation-theoretic purposes are compact and thus amenable to study in other ways.)

23.2 Conjugacy of maximal tori

The proof of Grothendieck's Theorem 22.1.10 on the existence of geometrically maximal tori rests upon the conjugacy of maximal tori over an algebraically closed field (Theorem 23.2.2 below) plus the following fact, which is also used to prove Theorem 23.2.2.

Proposition 23.2.1. *If $k = \bar{k}$ and G is a solvable smooth connected affine k -group, then all maximal tori in G are conjugate, and the image of a maximal torus under a surjection $G \twoheadrightarrow G'$ is again a maximal torus.*

We will prove this later. First let us deduce the following.

Theorem 23.2.2. *Let $k = \bar{k}$ and G any smooth connected affine k -group. Then*

- (i) *All maximal tori in G are $G(k)$ -conjugate.*
- (ii) *If $f : G \twoheadrightarrow \bar{G}$ is a quotient map then the image of a Borel of G is a Borel of \bar{G} , and the image of a maximal torus of G is a maximal torus of \bar{G} .*

Proof. (i) Every torus lies in a Borel, since a torus is in particular solvable smooth and connected, and a Borel is a maximal such. All Borels are conjugate, by Theorem 22.1.1. So we are reduced to the case of showing that two maximal tori of G both contained in a single Borel B are conjugate. But in particular they are maximal tori of B . If they are $B(k)$ -conjugate then they are $G(k)$ -conjugate. So we are reduced to proving (i) for the case when G is solvable. But this follows from Proposition 23.2.1.

(ii) We have a surjection $G/B \twoheadrightarrow \bar{G}/f(B)$. Since G/B is proper, so is $\bar{G}/f(B)$. So $f(B)$ is parabolic. But it is also solvable, since the image of a solvable thing is solvable. It is also smooth and connected (smoothness by earlier results). So $f(B)$ is radical (what we called a (\dagger) -subgroup before) and parabolic, which is equivalent to being a Borel by Theorem 22.1.1.

Now let T be a maximal torus of G . Choose a Borel B of G containing T . Then $f(T)$ is a maximal torus of $f(B)$, by Proposition 23.2.1. And by the above, $f(B)$ is a Borel of \bar{G} . So it is enough to show

that a maximal torus $\bar{T} = f(T)$ of a Borel \bar{B} of \bar{G} is also a maximal torus of \bar{G} . But by (i), any maximal torus \bar{S} of \bar{G} can be conjugated into \bar{B} . It is then maximal in \bar{B} . So by (i) applied to \bar{B} we have $\dim \bar{S} = \dim(\text{some conjugate of } \bar{S}) = \dim \bar{T}$, since maximal tori of \bar{B} must have the same dimension. Hence \bar{T} is of the maximal dimension $\dim \bar{S}$ of tori contained in \bar{G} , so it must be maximal in \bar{G} . \square

24 March 8

24.1 Proof of Proposition 23.2.1

First we assume the conjugacy of maximal tori and deduce that the image of a maximal torus under a quotient map is another maximal torus.

By the conjugacy of maximal tori, all maximal tori in G have the same dimension, say d_G .

Write $G = T \ltimes U$ where $U = \mathcal{R}_u(G)$. We claim that T is maximal. To see this, note that if $T \subset T'$ is another torus, then by group theory (on the functor of points) we have $T' = T \ltimes (T' \cap U)$. But the intersection $T' \cap U$ of a torus and a unipotent is trivial. So $T' = T$ is maximal.

Now write $f : G \rightarrow \bar{G}$ and $\bar{G} = \bar{T} \ltimes \bar{U}$ where \bar{T} is a maximal torus, and $\bar{U} = \mathcal{R}_u(\bar{G})$ is unipotent. (We can do this since \bar{G} is the image of the solvable group G , so solvable.) Now \mathcal{R}_u is functorial with respect to surjections (because the surjective image of a normal subgroup is normal, which fails for not-necessarily-surjective maps in general). Thus $f(U) \subset \bar{U}$. And since $U \triangleleft G$, we have $f(U) \triangleleft \bar{G}$. So we get a map $T = G/U \xrightarrow{f} \bar{G}/f(U) = \bar{T} \ltimes (\bar{U}/f(U))$. Since the image of a torus is a torus, we conclude that $\bar{T} \ltimes (\bar{U}/f(U))$ is a torus. Since \bar{U} is unipotent, so is its quotient $\bar{U}/f(U)$, whence $\bar{U}/f(U) = 1$, so $\bar{U} = f(U)$.

So great, we've seen that $f(\mathcal{R}_u(G)) = \mathcal{R}_u(\bar{G})$. Now we have $\bar{G} = f(G) = f(T) \cdot \bar{U}$ is generated by a torus $f(T)$ and a unipotent group \bar{U} , which must intersect trivially. Hence $\dim \bar{G} = \dim f(T) + \dim \bar{U}$. So $\dim f(T) = \dim \bar{G} - \dim \bar{U} = \dim \bar{T} = d_{\bar{G}}$. Thus for dimension reasons the torus $f(T)$ must be maximal.

Now we show the conjugacy of maximal tori. Write $G = T \ltimes U$ for a maximal torus T and $U = \mathcal{R}_u(G)$. Let T' be any maximal torus. We want to show that T' is $G(k)$ -conjugate to T .

The easy case is when $T \subset Z_G$. For now $T \triangleleft G$ so $G = T \ltimes U$. Thus the image of T' in G/T (which is unipotent) must be trivial, so $T' \subset T$. Thus by maximality $T' = T$.

If T is not central, but $T' \subset Z_G$ then $T \times T' \rightarrow G$ is a homomorphism, so $T \cdot T' \subset G$ is a torus (being the image of the torus $T \times T'$) and contains T' ; so by maximality $T' = T \cdot T'$ whence $T \subset T'$ whence $T = T'$ by maximality of T .

Thus we can reduce to the case $G' = (Z_G T')^0 \subsetneq G$. Therefore $\dim G' < \dim G$, so $\mathfrak{g} \supsetneq \mathfrak{g}' = \text{Lie}(Z_G T') = \mathfrak{g}^{T'}$, the $\text{Ad}(T')$ -invariants of \mathfrak{g} , by Homework 7, #4.

Consider the set of **roots** $\Phi(G, T') = \{\alpha \in X(T') : \alpha \neq 1, \mathfrak{g}_\alpha \neq 0\}$ where \mathfrak{g}_α denotes the α -weight space. This is some finite set $\{\alpha_1, \dots, \alpha_n\}$. Then $T' - \bigcup \ker \alpha_i \subset T'$ is open, so since $k = \bar{k}$ there is a rational point $s \in (T' - \bigcup \ker \alpha_i)(k)$. This satisfies $\alpha(s) \neq 1$ for all $\alpha \in \Phi(G, T')$. Such an element s is called **regular**. Now we certainly have an inclusion $G' = Z_G(T')^0 \subset Z_G(s)^0$. But by construction $\mathfrak{g}' \subset \text{Lie}(Z_G(s)^0) = \text{Lie}(Z_G(s)) = \mathfrak{g}^{\text{Ad}(s)}$ is an equality. So by Example 23.1.4 we conclude that $Z_G(s)$ is forced to be smooth and $G' = Z_G(s)^0$.

Claim 24.1.1. *Every semisimple element $\gamma \in G(k)$ has a $G(k)$ -conjugate contained in $T(k)$.*

Sketch of proof. Use a composition series to induct on $\dim G$, ultimately reducing to the case where $G = \mathbf{G}_m \ltimes \mathbf{G}_a$ (with the standard action of \mathbf{G}_m on \mathbf{G}_a) is the “ $\alpha x + b$ group” $\{(\begin{smallmatrix} t & x \\ 0 & 1 \end{smallmatrix})\}$. Here one can compute by hand. For details of this argument, see Appendix G. \square

By the claim, choose $g \in G(k)$ such that $gsg^{-1} \in T(k)$, so $s \in g^{-1}Tg$. This is a commutative group so $g^{-1}Tg \subset Z_G(s)^0 = G'$. Hence $g^{-1}Tg$ centralizes the maximal torus T' . As we saw, this forces $g^{-1}Tg \subset T'$. Hence $\dim T \leq \dim T'$. On the other hand $\dim T' \leq \dim G/U = \dim T$ since $T' \cap U = 1$. Therefore for dimension reasons $T' = g^{-1}Tg$. \square

Corollary 24.1.2. *If G is smooth connected and affine, $T \subset G$ is a maximal k -torus, and K/k is any field extension, then $T_K \subset G_K$ is a maximal K -torus.*

Corollary 24.1.3. *All maximal k -tori in a smooth connected affine group G have the same dimension.* \square

Proof of Corollary 24.1.2. Let $H = Z_G(T)^0$. The formation of H commutes with scalar extension: $H_K = Z_{G_K}(T_K)^0$. So if T_K were not maximal in G_K , it would not be maximal in H_K . (Since tori are commutative, a bigger torus in G_K would have to centralize T_K .) So renaming H as G we can assume without loss of generality that $T \subset Z_G$. Then we can pass to the quotient G/T to reduce to the case $T = 1$, i.e. assume G has no nontrivial tori and show the same for G_K . (For a nontrivial torus in T' lifts to a subgroup of G which sits in a short exact sequence between T and T' , and is thus itself a torus strictly bigger than T .)

Now by Grothendieck's Theorem 22.1.10, $G_{\bar{k}}$ has no nontrivial tori, since if it had one it would descend to a nontrivial torus of G . Hence $G_{\bar{k}}$ is unipotent, by Corollary 22.1.4. So G is unipotent, hence so is G_K , hence G_K contains no nontrivial torus. \square

24.2 Cartan subgroups

Definition 24.2.1. A *Cartan subgroup* of a smooth connected affine k -group G is one of the form $Z_G(T)$ for a maximal k -torus $T \subset G$.

Remark 24.2.2. By Exercise 4(i) HW8, Cartan subgroups are smooth. We'll soon prove they are connected, so they are solvable: $Z_G(T)/T$ is connected with no nontrivial tori, so it is unipotent (Corollary 22.1.4).

Remark 24.2.3. Since $T \subset Z_G(T)$ is central, we have $Z_G(T)_{\bar{k}} = T_{\bar{k}} \times U$ for some unipotent U by the structure theory for connected solvable affine \bar{k} -groups.

Remark 24.2.4. For reductive groups G , it will turn out that $Z_G(T) = T$.

The connectedness of Cartan subgroups is a special case of:

Theorem 24.2.5. *Let G be a smooth connected affine k -group, $S \subset G$ a k -torus. Then $Z_G(S)$ is connected.*

Proof. To show connectedness we can assume without loss of generality that $k = \bar{k}$. Since G is connected, we can also assume $S \neq 1$ so $S \simeq \mathbf{G}_m^r$ for some r . Take any decomposition $S = S' \times S''$ into smaller tori. Then $S'' \subset Z_G(S')$ because S is commutative. Hence $Z_G(S) = Z_{Z_G(S')}(S'')$. Thus by induction on $\dim S$ we easily reduce to the case where $S = \mathbf{G}_m$. Then $S \hookrightarrow G$ is given by a cocharacter $\lambda : \mathbf{G}_m \hookrightarrow G$, which happens to be injective, but we don't care. So Lemma 24.3.3 below completes the proof. \square

24.3 $P_G(\lambda), U_G(\lambda), Z_G(\lambda)$ for a 1-parameter subgroup λ

Now consider any **1-parameter subgroup** $\lambda : \mathbf{G}_m \rightarrow G$ for a smooth affine group G . Define an action of $\mathbf{G}_m \curvearrowright G$ by $t.g = \lambda(t)g\lambda(t)^{-1}$.

Example 24.3.1. If $G = \mathrm{GL}_2$, $\lambda(t) = \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$ then $t. \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & t^2 b \\ t^{-2} c & d \end{pmatrix}$.

For any $R \in \mathrm{Alg}/k$, $g \in G(R)$ say that **the limit** $\lim_{t \rightarrow 0} t.g$ **exists** if the orbit map $\mathbf{G}_{m/R} \rightarrow G_R$ extends to a map $\mathbf{A}_R^1 \rightarrow G_R$, and define **the limit** $\lim_{t \rightarrow 0} t.g$ to be the image “ $0.g$ ” of $0 \in \mathbf{A}_R^1(R)$ in $G(R)$.

Definition 24.3.2. Let G be a smooth affine k -group and $\lambda : \mathbf{G}_m \rightarrow G$ a 1-parameter subgroup. For a k -algebra R , define the functor $P_G(\lambda)$ by

$$P_G(\lambda)(R) = \{g \in G(R) : \lim_{t \rightarrow 0} t.g \text{ exists}\}.$$

Define the subfunctor $U_G(\lambda)$ by

$$U_G(\lambda)(R) = \{g \in P_G(\lambda)(R) : \lim_{t \rightarrow 0} t.g = 1\}.$$

Define the centralizer $Z_G(\lambda)$ by

$$Z_G(\lambda)(R) = \{g \in G(R) : \mathbf{G}_{m/R} \text{ acts trivially on } g\}.$$

Lemma 24.3.3. *(0) $P_G(\lambda), U_G(\lambda), Z_G(\lambda)$ are subgroup functors of G .*

(i) The functors $P_G(\lambda), U_G(\lambda), Z_G(\lambda)$ are representable by closed k -subgroups, and $P_G(\lambda) = Z_G(\lambda) \ltimes U_G(\lambda)$.

(ii) Multiplication $U_G(\lambda^{-1}) \times P_G(\lambda) \rightarrow G$ is an open immersion.

(iii) $P_G(\lambda), U_G(\lambda), Z_G(\lambda)$ are smooth; they are connected if G is connected; and $U_G(\lambda)$ is unipotent.

We'll discuss the proof next time.

Example 24.3.4. $\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix} \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} t & ty \\ tx & t' + txy \end{pmatrix}.$

Example 24.3.5. If $G = GL_3$ and $\lambda(t) = \begin{pmatrix} t^3 & & \\ & t^3 & \\ & & t \end{pmatrix}$ one computes

$$Z_G(\lambda) = \left\{ \begin{pmatrix} * & * & * \\ * & * & * \\ * & * & * \end{pmatrix} \right\}.$$

Using $3 > 1$ one sees

$$P_G(\lambda) = \left\{ \begin{pmatrix} * & * & * \\ * & * & * \\ * & * & * \end{pmatrix} \right\}$$

and

$$U_G(\lambda) = \left\{ \begin{pmatrix} 1 & * & * \\ & 1 & * \\ & & 1 \end{pmatrix} \right\}, U_G(\lambda^{-1}) = \left\{ \begin{pmatrix} 1 & & \\ & 1 & \\ * & * & 1 \end{pmatrix} \right\}.$$

We will use these “dynamic” constructions in our proof in the final lecture that SL_2 and PGL_2 are the only non-solvable (equivalently: non-torus) split connected reductive groups of rank 1 over any field. The real significance of these constructions and their properties will only become apparent in the sequel course on the general structure theory of connected reductive groups, where their use will be pervasive and their importance impossible to overestimate.

25 March 10

25.1 Proof of Lemma 24.3.3 on P_G, U_G, Z_G

We leave (0) as an exercise; use that \mathbf{A}^1 is a ring functor which lets us multiply the limits, if they exist.

25.1.1 Proof that (i)+(ii) \Rightarrow (iii) [except unipotence of $U_G(\lambda)$]

This is pretty easy. Since $U_G(\lambda^{-1}) \times P_G(\lambda)$ is an open subscheme of the smooth scheme G , we see that U_G and P_G are always smooth. Since $P_G = Z_G \times U_G$ we see that Z_G is also smooth. Connectedness is similar.

25.1.2 Proof of (i)

We begin by making some functorial observations.

First, $Z_G(\lambda) = P_G(\lambda) \cap P_G(\lambda^{-1})$.

Proof. The containment $Z_G(\lambda) \subset P_G(\lambda) \cap P_G(\lambda^{-1})$ is clear, because for an element which centralizes λ (and hence λ^{-1}), the orbit maps for both λ and λ^{-1} are constant; hence they certainly extend to \mathbf{A}^1 .

Conversely, if $\mathbf{G}_m \rightarrow G_R$ given by $t \mapsto t.g$ for $g \in P_G(\lambda) \cap P_G(\lambda^{-1})$, the induced map $\mathcal{O}(G_R) \rightarrow R[t, t^{-1}]$ factors through both $R[t]$ and $R[t^{-1}]$. Hence it lands in their intersection R , which implies $t.g = g$ for all t since $1.g = g$. \square

Thus we see that if P_G is representable for all λ , the same is true for Z_G , since we can take scheme theoretic intersections.

Next observe that the map $P_G(\lambda) \rightarrow G$ given by $g \mapsto \lim_{t \rightarrow 0} t.g$ is a homomorphism of group functors. (Exercise!) By definition its kernel is $U_G(\lambda)$. Thus if $P_G(\lambda)$ is representable, so is $U_G(\lambda)$.

Next note that the above map $P_G(\lambda) \rightarrow G$ automatically factors through $Z_G(\lambda)$. This is because for $g \in P_G(\lambda)(R)$ the orbit map $\mathbf{G}_m \rightarrow G_R$ extends to a map $\mathbf{A}_R^1 \rightarrow G_R$ which is equivariant for the standard action of \mathbf{G}_m on \mathbf{A}^1 (check!), and the origin is fixed by this action. Moreover $P_G(\lambda) \rightarrow Z_G(\lambda)$ is a section of the inclusion $Z_G(\lambda) \hookrightarrow P_G(\lambda)$

Combining the last two observations, we see that $P_G(\lambda) = Z_G(\lambda) \ltimes U_G(\lambda)$ as group functors. Hence (i) reduces to showing the representability of $P_G(\lambda)$. Now we have $\mathbf{G}_m \curvearrowright G$, which gives a functorial linear representation of \mathbf{G}_m on $k[G]$, and hence a weight space decomposition

$$k[G] = \bigoplus_{n \in \mathbf{Z} = X(\mathbf{G}_m)} k[G]_n$$

where $t^*(f) = t^n f$ for $f \in k[G]_n$. One can check that $P_G(\lambda)$ is the zero scheme of the ideal $\langle k[G]_n \rangle_{n < 0}$. For details, see [CGP, Lemma 2.1.4].

25.1.3 Proof of (ii) and unipotence of $U_G(\lambda)$

First consider an injective homomorphism (hence closed immersion) $j : G \hookrightarrow G'$; set $\lambda' = j \circ \lambda$ to be the induced 1-parameter subgroup. Check that $G \cap P_{G'}(\lambda') = P_G(\lambda)$, $G \cap U_{G'}(\lambda') = U_G(\lambda)$, $G \cap Z_{G'}(\lambda') = Z_G(\lambda)$.

Consequently multiplication $U_G(\lambda^{-1}) \times P_G(\lambda) \rightarrow G$ is monic, if and only if $U_G(\lambda^{-1}) \cap P_G(\lambda) = 1$, if and only if $U_{G'}(\lambda'^{-1}) \times P_{G'}(\lambda') \rightarrow G'$ is monic, and $U_G(\lambda)$ is unipotent if $U_{G'}(\lambda')$ is unipotent *granting smoothness* of $U_G(\lambda)$.

Appendix H shows that $G \cap (U_{G'}(\lambda'^{-1}) \times P_{G'}(\lambda')) = U_G(\lambda^{-1}) \times P_G(\lambda)$, assuming $U_{G'}(\lambda'^{-1}) \times P_{G'}(\lambda') \rightarrow G'$ is monic. Therefore if we can show that $U_{G'}(\lambda'^{-1}) \times P_{G'}(\lambda') \rightarrow G'$ is an open immersion, so is $U_G(\lambda^{-1}) \times P_G(\lambda) \rightarrow G$, hence $U_G(\lambda)$ is always smooth, so if we can show that $U_{G'}(\lambda')$ is always unipotent, the same is true for $U_G(\lambda)$.

Putting all this together, we have reduced to proving the claim in a bigger group. Obviously we take $G' = GL(V)$. Now λ' gives a \mathbf{G}_m action on V , so we have a weight space decomposition $V = \bigoplus V_{e_i}$ for $e_1 > \dots > e_n$ say, where $t.v = t^{e_i}v$ for $v \in V_{e_i}$.

Now introduce a partial flag

$$\mathcal{F} = [V_{e_1} \subset V_{e_1} \oplus V_{e_2} \subset \dots \subset V].$$

On Homework 10 it is shown that $P_{GL(V)}(\lambda') = \{g : \text{preserves the flag}\}$ which is a block upper triangle subgroup of $GL(V)$, and hence smooth by inspection. Similarly $U_{GL(V)}(\lambda') = \{g \in P_{GL(V)}(\lambda') : \text{gr}_{\mathcal{F}}^{\bullet}(g) = 1\}$ is the standard unipotent subgroup of the block upper triangle subgroup $P_{GL(V)}(\lambda')$, which by inspection is unipotent and smooth, and similarly $U_{GL(V)}(\lambda'^{-1})$ is the corresponding standard unipotent subgroup of the complementary block lower triangle subgroup. Hence $P_{GL(V)}(\lambda') \cap U_{GL(V)}(\lambda'^{-1}) = 1$. This gives monicity. On Homework 10 it is shown that this implies the map is an open immersion as well. \square

Next we record another nice fact about P_G, U_G, Z_G .

Proposition 25.1.1. *Consider a diagram*

$$\mathbf{G}_m \xrightarrow{\lambda} G \xrightarrow{f} \overline{G}$$

and assume G is connected, and set $\overline{\lambda} = f\lambda$. Then $P_G(\lambda)$ maps onto $P_{\overline{G}}(\overline{\lambda})$ and similarly for U and Z .

Proof. We certainly have a commutative diagram

$$\begin{array}{ccc} U_G(\lambda^{-1}) \times P_G(\lambda) & \xrightarrow{\text{open}} & G \\ \downarrow & & \downarrow f \\ U_{\overline{G}}(\overline{\lambda}^{-1}) \times P_{\overline{G}}(\overline{\lambda}) & \xrightarrow{\text{open}} & \overline{G} \end{array}$$

The problem is to show that the two left maps are surjective. But if either is not, then its image has strictly smaller dimension than the dimension of the guy upstairs. Hence the image of the total map on the left side and then across on the bottom cannot be dense, giving a contradiction (to the openness of the bottom map) since \overline{G} is irreducible.

Since $P = Z \ltimes U$ we get the analogous result for Z too. \square

26 March 12

26.1 Classification of split reductive groups of rank 1

Definition 26.1.1. A connected reductive k -group G is called k -split if it has a split maximal k -torus.

Example 26.1.2. $SL_n, Sp_{2n}, GL_n, SO_n, PGL_n$.

Theorem 26.1.3. *Any split connected reductive group is quasi-split, i.e. has a Borel k -subgroup.*

This is a hard theorem, and relies on getting some classification results off the ground, so we cannot invoke it yet. (It will be proved in the next course.)

Definition 26.1.4. The k -rank of a connected reductive group G is the dimension of its maximal k -split tori. The rank is the \bar{k} -rank.

For example, “ k -rank zero” means k -anisotropic. The following theorem over general fields will be proved in the next course (whereas we have already established the crucial case of algebraically closed ground fields):

Theorem 26.1.5. *All the maximal k -split tori in a connected reductive group are $G(k)$ -conjugate (so the k -rank is well-defined!).*

We already know the rank is well-defined. But the above theorem must be proved before we know the same for the k -rank!

The following theorem, which we will prove via dynamic methods as the punchline to this course (taking for granted Chevalley’s theorem on parabolic subgroups that we will prove without circularity near the start of the next course), is literally the key to getting the classification theory for connected reductive groups off the ground:

Theorem 26.1.6. *Let G be a connected reductive k -group which is not solvable (i.e. is not a torus). Assume G is k -split of rank 1, with split maximal k -torus T . Then $G \simeq SL_2$ or PGL_2 .*

Proof. We cannot use the (not proved!) theorem that split implies quasi-split, so a priori it is not obvious that G has a Borel k -subgroup. Of course this is no problem over \bar{k} . So the plan is to do the proof “in two passes”: first show that the result over \bar{k} implies the existence of a Borel k -subgroup, and then prove the result assuming the existence of such a subgroup (an assumption that we know holds over \bar{k} !).

So assume the theorem holds over \bar{k} . Let $\lambda : \mathbf{G}_m \simeq T \subset G$. Then we have $Z_G(\lambda) = Z_G(T) = T$, since the last equality can be checked over \bar{k} and we know it holds for the maximal torus in SL_2, PGL_2 . Likewise we know $U_G(\lambda^{\pm 1})$ are both 1-dimensional, since geometrically they must be the two \mathbf{G}_a ’s inside SL_2 or PGL_2 . So consider the open subscheme $U(\lambda^{-1}) \times Z(\lambda) \times U(\lambda) \hookrightarrow G$. We have $Z(\lambda) \times U = T \times (\text{unipotent}) = \text{solvable}$, and $\dim U(\lambda^{-1}) = 1$. So for dimension reasons, since G is not solvable, $Z(\lambda) \times U$ is a Borel: there is simply no extra room to make a bigger solvable connected subgroup. Consequently, assuming the theorem holds over \bar{k} , there exists a Borel k -subgroup.

So now we can prove the theorem assuming the existence of a Borel k -subgroup B . The idea is as follows. First we will construct a map $G \rightarrow PGL_2 = \underline{\text{Aut}}_{\mathbf{P}^1/k}$ using B . Then we will show the map is a central isogeny, and finally that its kernel must be μ_e for $e|2$. (If $e = 1$ this gives $G = PGL_2$ and if $e = 2$ this will give $G = SL_2$.)

First consider the torus action $T \subset G \curvearrowright G/B$. This quotient is proper because B is parabolic, and T is (split) solvable. A refinement of the Borel fixed point theorem [Bor, §13.5]) shows that there exist $\geq 1 + \dim(G/B) \geq 2$ [since $G \neq B$ as G is not solvable] fixed \bar{k} -points for the actions $T_{\bar{k}} \curvearrowright (G/B)_{\bar{k}}$. Any such $gB_{\bar{k}}$ for $g \in G(\bar{k})$ gives $T_{\bar{k}}gB_{\bar{k}} \subset gB_{\bar{k}}$ and hence $T_{\bar{k}} \subset gB_{\bar{k}}g^{-1}$, i.e. this conjugate of $B_{\bar{k}}$ is a Borel of $G_{\bar{k}}$ containing $T_{\bar{k}}$. Any such Borel is conjugate to $B_{\bar{k}}$, and the corresponding conjugator g is determined modulo $N_{G_{\bar{k}}}(B_{\bar{k}}) = B_{\bar{k}}$ [using Chevalley’s theorem on parabolic subgroups!]. Thus in fact $T_{\bar{k}}$ -fixed \bar{k} -points of $(G/B)_{\bar{k}}$ are in bijection with the set of Borels of $G_{\bar{k}}$ containing $T_{\bar{k}}$. By Homework 9, #6, the latter is in bijection with the Weyl group $W = (N_G(T)/Z_G(T))(\bar{k})$. So $2 \leq 1 + \dim(G/B) \leq \#\{T_{\bar{k}}\text{-fixed } \bar{k}\text{-points of } (G/B)_{\bar{k}}\} = \#W$. But W injects into $\text{Aut}_{\bar{k}}(T_{\bar{k}}) = \text{Aut}(\mathbf{G}_m) = \pm 1$. So $\#W \leq 2$. Hence we have (by squeezing) $\dim(G/B) = 1$.

So G/B is a smooth projective geometrically connected curve over k with a rational point (the coset of the identity). We claim it is \mathbf{P}^1 . It suffices to show its genus is zero, which can be checked over \bar{k} . But there are only two fixed points, geometrically, and plenty of rational points. If we consider the orbit map

$\mathbf{G}_m = T_{\bar{k}} \rightarrow (G/B)_{\bar{k}}$ for any *non*-fixed point, the map is dominant. Hence $(G/B)_{\bar{k}}$ is a rational curve, and so has genus zero.

So we have shown $G/B \simeq \mathbf{P}_k^1$ over k . Great! Thus the action $G \curvearrowright G/B$ defines a k -homomorphism $\varphi : G \rightarrow \underline{\text{Aut}}_{\mathbf{P}^1/k} = \text{PGL}_2$. Of course the last equality requires serious stuff (the theorem on formal functions,...). Instead we can get the map $G \rightarrow \text{PGL}_2$ in a more elementary fashion, since G is a variety: we can spread out from the generic fiber G_η using that $k(\eta)$ is a field and we know the automorphisms of $\mathbf{P}_{k(\eta)}^1$ are $\text{PGL}_2(k(\eta))$; this gives us a map from a dense open of G to PGL_2 , and using that $\varphi : G \rightarrow \underline{\text{Aut}}_{\mathbf{P}^1/k}$ is a homomorphism we can translate it around to all of G . More precisely, we appeal to the general fact that a rational map between smooth connected k -group varieties that is multiplicative in the evident “rational maps” sense extends uniquely to a k -homomorphism. To prove it we may pass up to k_s and then use translation by rational points to extend the domain of definition, since the k -point translates of any dense open *do* cover the group: exercise!

The next claim is that $\varphi : G \rightarrow \text{PGL}_2$ is surjective. We have $g \in \ker \varphi \Rightarrow g$ acts trivially on $G/B \Rightarrow gB \subset B \Rightarrow g \in B$, totally functorially. This gives $\ker \varphi \subset B$. Consequently $(\ker \varphi_{\bar{k}})_{\text{red}}^0$ is solvable. Now we have a map $G_{\bar{k}}/(\ker \varphi_{\bar{k}})_{\text{red}}^0 \rightarrow \text{PGL}_2$ with finite kernel. If this map is not surjective, then the image (being closed) has dimension $\leq \dim \text{PGL}_2 - 1 = 3 - 1 = 2$ and is thus solvable. But this gives a short exact sequence

$$1 \rightarrow (\ker \varphi_{\bar{k}})_{\text{red}}^0 \rightarrow G_{\bar{k}} \rightarrow (\text{something}) \rightarrow 1$$

and the outer terms are both solvable. So $G_{\bar{k}}$ is solvable too, a contradiction. Thus φ must be surjective.

Let $N = (\ker \varphi_{\bar{k}})_{\text{red}}^0$. This is smooth and connected, and normal in the reductive group $G_{\bar{k}}$. On Homework 10 it is shown that this implies N is reductive as well. But we already saw N is solvable. Hence N is a torus.

On Homework 6 #3(ii) it was shown that a normal torus in a connected group is central. Therefore N is a central torus. If N is nontrivial, then it is one dimensional (this being the dimension of maximal split tori in the rank 1 group $G_{\bar{k}}$) and hence equal to $T_{\bar{k}}$. [By centrality $N \cdot T_{\bar{k}}$ is a torus, so contains $T_{\bar{k}}$, so is equal to $T_{\bar{k}}$.] Therefore $T_{\bar{k}}$ is central in $G_{\bar{k}}$. So the quotient $G_{\bar{k}}/T_{\bar{k}}$ is a group with no nontrivial maximal torus, and hence is unipotent, hence solvable. The same short exact sequence trick gives a contradiction since G is not solvable. Thus N must be trivial, so $\ker \varphi$ is finite, so $\dim G = 3$ and φ is an isogeny.

Next we want to show that φ is a central isogeny. Inside G we have T , a one dimensional split maximal torus. Hence $\varphi(T)$ is a split maximal torus in PGL_2 . In Appendix H, it is shown that all split maximal tori in PGL_2 are rationally conjugate. So composing φ with an appropriate $\text{PGL}_2(k)$ -conjugation, which amounts to changing the isomorphism $G/B \simeq \mathbf{P}_k^1$, we can assume without loss of generality that $\varphi : G \twoheadrightarrow \text{PGL}_2$ maps T surjectively onto the diagonal split torus in PGL_2 .

In PGL_2 the maximal torus is its own centralizer. Since φ is finite, for dimension reasons we see that $Z_G(T) = T$ as well. Choose an isomorphism $\lambda : \mathbf{G}_m \simeq T$. This gives $\varphi\lambda : \mathbf{G}_m \rightarrow (\text{diag.torus}) \simeq \mathbf{G}_m$, which must be given by a map $t \mapsto t^e$ for some $e \neq 0$ (by surjectivity). Replacing λ by λ^{-1} if necessary, we can assume $e \geq 1$. Now $G \supset U(\lambda^{-1}) \times Z(\lambda) \times U(\lambda)$, and since φ is surjective, $U(\lambda^{\pm 1})$ maps surjectively via φ onto $U_{\text{PGL}_2}(\varphi\lambda^{\pm 1}) = U^\pm \simeq \mathbf{G}_a$, where U^\pm are the standard upper and lower triangular unipotent subgroups of PGL_2 . (That $U_{\text{PGL}_2}(\varphi\lambda^{\pm 1}) = U^\pm$ can be seen by direct calculation.) Consequently $\dim U(\lambda^{\pm 1}) = 1$, as $U(\lambda^{\pm 1})$ is smooth unipotent and connected.

The action of $T \curvearrowright U_G(\lambda^{\pm 1})$ lies over the action of the diagonal \mathbf{G}_m in PGL_2 on U^\pm (by conjugation). Said action is nontrivial, so since φ is surjective, T acts nontrivially on $U_G(\lambda^{\pm 1})$. By Homework 9, #1 (structure of unipotent groups a la Tits in [CGP, App. B]), this forces $U_G(\lambda^{\pm 1}) \simeq \mathbf{G}_a$ as k -groups. Since $\dim G = 3$, $B^\pm := T \ltimes U_G(\lambda^{\pm 1})$ are Borels, for dimension reasons; their intersection is T . Geometrically, it is easy to see, $(\ker \varphi)(\bar{k})$ is contained in the intersection of all Borels. Hence in particular $\ker \varphi \subset B^+ \cap B^- = T = \mathbf{G}_m$. Since φ maps $T \rightarrow \text{diag}$ by $t \mapsto t^e$, we can compute directly that $\ker \varphi = \mu_e \triangleleft G$. Thus we get an action of the connected group G on μ_e , hence a morphism $G \rightarrow \underline{\text{Aut}}(\mu) \simeq (\mathbf{Z}/e\mathbf{Z})^\times$ (which is discrete), the last isomorphism being by Homework 10. Thus G acts trivially on μ_e , so $\ker \varphi = \mu_e$ is central, and thus φ is a central isogeny.

It remains to show $e|2$ and to verify this forces $G \simeq \text{SL}_2$ or PGL_2 . Go back and choose $n \in N_G(T)(\bar{k})$ representing the unique nontrivial element of the Weyl groups (which we saw has order 2). Conjugation by n must be the unique nontrivial automorphism of $T = \mathbf{G}_m$, and hence be inversion. Since μ_e is central it is fixed pointwise by this automorphism. So inversion acts trivially on μ_e . This indeed forces $e|2$.

If $e = 1$ obviously φ is an isomorphism $G \simeq \text{PGL}_2$.

If $e = 2$, observe that since $\ker \varphi \subset T$ and φ maps $U_G(\lambda^{\pm 1})$ isomorphically onto U^{\pm} , we obtain a diagram

$$\begin{array}{ccc}
 \mathbf{G}_a \times \mathbf{G}_m \times \mathbf{G}_a & \xrightarrow{\text{open}} & \mathbf{G} \\
 \parallel & & \downarrow \text{dashed} \\
 \mathbf{G}_a \times \mathbf{G}_m \times \mathbf{G}_a & \xrightarrow[\text{open}]{} & \mathbf{SL}_2
 \end{array}
 \quad
 \begin{array}{c}
 \searrow \varphi = \text{homom.} \\
 \text{PGL}_2 \\
 \nearrow \text{can.}
 \end{array}$$

There are actions of \mathbf{G}_m on both copies of \mathbf{G}_a on both the top and the bottom (the identification of \mathbf{G}_a 's expressing exactly that $U_G(\lambda^{\pm 1}) \rightarrow U^{\pm}$ are isomorphisms). By design the actions are compatible with the identification given by the vertical $=$, so this diagram commutes. The vertical $=$ induces the indicated rational map $\mathbf{G} \rightarrow \mathbf{SL}_2$. The finiteness of the kernels of the diagonal maps forces $\mathbf{G} \dashrightarrow \mathbf{SL}_2$ to be a homomorphism. By translation, any rational homomorphism is an actual morphism. (This is shown on Homework 10 by Galois descent from the case $k = k_s$.) The theorem follows. \square

Why do we care about the theorem? Inside any reductive group \mathbf{G} suppose we have a k -split maximal torus T . The torus acts on the Lie algebra \mathfrak{g} giving a weight space decomposition $\mathfrak{g} = \bigoplus \mathfrak{g}_{\alpha}$. Let $T_{\alpha} = (\ker \alpha)_{\text{red}}^0$ for $\alpha \neq 0$ that arise. Then it turns out that $\mathcal{DZ}_{\mathbf{G}}(T_{\alpha})$ is a k -split non-solvable reductive group of rank 1, and thus is \mathbf{SL}_2 or \mathbf{PGL}_2 by the theorem. So these groups show up all over the place, and are what will allow us to classify reductive groups! The first step towards this is to use this rank-1 classification to build the root datum associated to a split connected reductive group over a general field as part of the structure theory of connected reductive groups in the sequel course.

A Properties of Orthogonal Groups

[This appendix is a lightly edited extraction from [C, App. C]; we are grateful to the SMF for permission to include it here.]

A.1 Basic definitions

Let V be a vector bundle of constant rank $n \geq 1$ over a scheme S , and let $q : V \rightarrow \mathcal{L}$ be a quadratic form valued in a line bundle \mathcal{L} , so we get a symmetric bilinear form $B_q : V \times V \rightarrow \mathcal{L}$ defined by

$$B_q(x, y) = q(x + y) - q(x) - q(y).$$

Assume q is fiberwise non-zero over S , so $(q = 0) \subset \mathbf{P}(V^*)$ is an S -flat hypersurface with fibers of dimension $n - 2$ (understood to be empty when $n = 1$). By HW2, Exercise 4 (and trivial considerations when $n = 1$), this is smooth precisely when for each $s \in S$ one of the following holds: (i) B_{q_s} is non-degenerate and either $\text{char}(k(s)) \neq 2$ or $\text{char}(k(s)) = 2$ with n even, (ii) the defect δ_{q_s} is 1 and $\text{char}(k(s)) = 2$ with n odd and $q_s|_{V_s^\perp} \neq 0$. (Likewise, $\delta_{q_s} \equiv \dim V_s$ when $\text{char}(k(s)) = 2$.) In such cases we say (V, q) is *non-degenerate*; (ii) is the “defect-1” case at s . (In [SGA7, XII, §1], such (V, q) are called *ordinary*.)

Clearly the functor

$$S' \rightsquigarrow \{g \in \text{GL}(V_{S'}) \mid q_{S'}(gx) = q_{S'}(x) \text{ for all } x \in V_{S'}\}$$

on S -schemes is represented by a finitely presented closed S -subgroup $O(q)$ of $\text{GL}(V)$, even without the non-degeneracy condition on q . We call it the *orthogonal group* of (V, q) . Define the *naive special orthogonal group* to be

$$SO'(q) := \ker(\det : O(q) \rightarrow \mathbf{G}_m).$$

We say “naive” because this is the wrong notion in the non-degenerate case when n is even and 2 is not a unit on S . The *special orthogonal group* $SO(q)$ will be defined shortly in a characteristic-free way, using input from the theory of Clifford algebras when n is even. (The distinction between even and odd n when defining $SO(q)$ is natural, because it will turn out that $O(q)/SO(q)$ is equal to μ_2 for odd n but $(\mathbf{Z}/2\mathbf{Z})_S$ for even n . In the uninteresting case $n = 1$ we have $O(q) = \mu_2$ and $SO(q) = 1$.)

Definition A.1.1. Let $S = \text{Spec } \mathbf{Z}$. The *National Bureau of Standards* (or *standard split*) quadratic form q_n on $V = \mathbf{Z}^n$ is as follows, depending on the parity of $n \geq 1$:

$$q_{2m} = \sum_{i=1}^m x_{2i-1}x_{2i}, \quad q_{2m+1} = x_0^2 + \sum_{i=1}^m x_{2i-1}x_{2i}$$

(so $q_1 = x_0^2$). We define $O_n = O(q_n)$ and $SO'_n = SO'(q_n)$.

It is elementary to check that (\mathbf{Z}^n, q_n) is non-degenerate.

Remark A.1.2. In the study of quadratic forms q over a domain A , such as the ring of integers in a number field or a discrete valuation ring, the phrase “non-degenerate” is often used to mean “non-degenerate over the fraction field”. Indeed, non-degeneracy over A in the sense defined above is rather restrictive. In addition to the National Bureau of Standards form q_n , other non-degenerate examples over \mathbf{Z} (in our restrictive sense) are the quadratic spaces arising from even unimodular lattices, such as the E_8 and Leech lattices.

Lemma A.1.3. *If (V, q) is a non-degenerate quadratic space of rank $n \geq 1$ over a scheme S then it is isomorphic to (\mathcal{O}_S^n, q_n) fppf-locally on S . If n is even or 2 is a unit on S then it suffices to use the étale topology rather than the fppf topology.*

Proof. In [SGA7, XII, Prop. 1.2] the smoothness of $(q = 0)$ is used to prove the following variant by a simple induction argument: q is an étale form of q_n when n is even and is an étale form of $ux_0^2 + q_{2m}$ when $n = 2m + 1$ is odd, with u a unit on the base. Once the induction is finished, we are done when n is even and we need to extract a square root of u when n is odd. This accounts for the necessity of working fppf-locally for odd n when 2 is not a unit on the base. \square

Lemma A.1.3 is very useful for reducing problems with general non-degenerate quadratic spaces to the case of q_n over \mathbf{Z} . This will be illustrated numerous times in what follows, and now we illustrate it with Clifford algebras in the relative setting. Consider a non-degenerate (V, q) with rank $n \geq 1$. The *Clifford algebra* $C(V, q)$ is the quotient of the tensor algebra of V by the relation $x^{\otimes 2} = q(x)$ for local sections x of V . This inherits a natural $\mathbf{Z}/2\mathbf{Z}$ -grading from the \mathbf{Z} -grading on the tensor algebra, and by considering expansions relative to a local basis of V we see that $C(V, q)$ is a finitely generated \mathcal{O}_S -module. The Clifford algebra is a classical object of study over fields, and we need some properties of it over a general base ring (or scheme) when n is even:

Lemma A.1.4. *Assume n is even. The \mathcal{O}_S -algebra $C(V, q)$ and its degree-0 part $C^+(V, q)$ are vector bundles over S of finite rank. Their quasi-coherent centers are respectively equal to \mathcal{O}_S and a rank-2 finite étale \mathcal{O}_S -algebra Z_q .*

Proof. We may work fppf-locally on S , so by Lemma A.1.3 we may assume that V admits a basis identifying q with q_n . Since n is even, there are complementary isotropic free subbundles $W, W' \subset V$ (in perfect duality via B_q). This leads to concrete descriptions of $C(V, q)$ and $C^+(V, q)$ in [SGA7, XII, 1.4]: $C(V, q)$ is naturally isomorphic as a $\mathbf{Z}/2\mathbf{Z}$ -graded algebra to the endomorphism algebra of the exterior algebra $A = \wedge^\bullet(W)$, where $w \in W$ acts via $w \wedge (\cdot)$ and $w' \in W'$ acts via the contraction operator

$$w_1 \wedge \cdots \wedge w_m \mapsto \sum_{i=1}^m (-1)^{i-1} B_q(w_i, w') w_1 \wedge \cdots \widehat{w_i} \cdots \wedge w_m.$$

(It is natural to consider the exterior algebra of W , since $q|_W = 0$ and the Clifford algebra associated to the vanishing quadratic form is the exterior algebra.) The $\mathbf{Z}/2\mathbf{Z}$ -grading of the endomorphism algebra of A is defined in terms of the decomposition $A = A_+ \oplus A_-$, where A_+ is the “even part” and A_- is the “odd part”: an endomorphism of A is *even* when it respects this decomposition and *odd* when it carries A_- into A_+ and vice-versa. We thereby see that $C^+(V, q)$ is the direct product of the endomorphism algebras of A_+ and A_- . Since the center of a matrix algebra over any ring consists of the scalars, we are done. \square

The action of $O(q)$ on $C(V, q)$ preserves the grading and hence induces an action on $C^+(V, q)$, so we obtain an action of $O(q)$ on the finite étale center Z_q of $C^+(V, q)$. The automorphism scheme $\underline{\text{Aut}}_{Z_q/\mathcal{O}_S}$ is uniquely isomorphic to $(\mathbf{Z}/2\mathbf{Z})_S$ since Z_q is finite étale of rank 2 over \mathcal{O}_S . Thus, for even n we get a homomorphism

$$D_q : O(q) \rightarrow (\mathbf{Z}/2\mathbf{Z})_S$$

that is compatible with isomorphisms in (V, q) , and its formation commutes with any base change on S . This is called the *Dickson morphism* because D_{q_n} underlies the definition of the *Dickson invariant* (see Remark A.2.6).

Proposition A.1.5. *Assume n is even. The map D_q is surjective.*

Flatness properties for D_q require more work; see Proposition A.2.3

Proof. We may pass to geometric fibers over S , where the assertion is that the center Z_q of $C^+(V, q)$ is not centralized by the action of $O(q)$ on $C(V, q)$. This is a classical fact from the theory of Clifford algebras, and we now recall the proof.

Let (V, q) be an even-dimensional nonzero quadratic space (V, q) over a field k . Naturally V is a subspace of $C(V, q)$ and the conjugation action on V by the Clifford k -group

$$\text{Cliff}(V, q) := \{u \in C(V, q)^\times \mid uVu^{-1} = V\}$$

defines a homomorphism from $\text{Cliff}(V, q)$ onto $O(q)$ [Bou, IX, §9.5, Thm. 4(a)]. Thus, the nontriviality of D_q amounts to the assertion that the rank-2 center Z_q of $C^+(V, q)$ is not centralized by the units in $\text{Cliff}(V, q)$. Viewing V as an affine space, the Zariski-open non-vanishing locus of q on V is Zariski-dense in V and lies in $\text{Cliff}(V, q)$ (such $v \in V - \{0\}$ act on V via orthogonal reflection $x \mapsto -x + (B_q(x, v)/q(v))v$ through v [Bou, IX, §9.5, Thm. 4(b)]), so this part of V generates $C(V, q)$ as an algebra. Hence, if Z_q were centralized by the group $\text{Cliff}(V, q)$ then it would be central in the algebra $C(V, q)$, an absurdity since $C(V, q)$ has scalar center. \square

We can finally define special orthogonal groups, depending on the parity of n .

Definition A.1.6. Let (V, q) be a non-degenerate quadratic space of rank $n \geq 1$ over a scheme S . The *special orthogonal group* $SO(q)$ is $SO'(q) = \ker(\det|_{O(q)})$ when n is odd and $\ker D_q$ when n is even. For any $n \geq 1$, $SO_n := SO(q_n)$.

By definition, $SO(q)$ is a closed subgroup of $O(q)$, and it is also an open subscheme of $O(q)$ when n is even. (In contrast, SO_{2m+1} is not an open subscheme of O_{2m+1} over \mathbf{Z} because we will prove that $O(q) = SO(q) \times \mu_2$ for odd n via the central $\mu_2 \subset GL(V)$, and over $\text{Spec } \mathbf{Z}$ the identity section of μ_2 is not an open immersion.)

The group $SO'(q)$ is not of any real interest when n is even and 2 is not a unit on the base (and we will show that it coincides with $SO(q)$ in all other cases). The only reason we are considering $SO'(q)$ in general is because it is the first thing that comes to mind when trying to generalize the theory over $\mathbf{Z}[1/2]$ to work over \mathbf{Z} . We will see that SO'_{2m} is not $\mathbf{Z}_{(2)}$ -flat. (Example: Consider $m = 1$ and $S = \text{Spec } \mathbf{Z}_{(2)}$. We have $O_2 = \mathbf{G}_m \times (\mathbf{Z}/2\mathbf{Z})$ and $SO_2 = \mathbf{G}_m$, whereas SO'_2 is the reduced closed subscheme of O_2 obtained by removing the open non-identity component in the generic fiber.)

From now on, we only consider non-degenerate (V, q) . To orient ourselves, it is useful to record the main properties we shall prove for the “good” groups associated to such (V, q) :

Theorem A.1.7. *The group $SO(q)$ is smooth of relative dimension $n(n-1)/2$ with connected fibers. Its functorial center is trivial for odd n and equals the central $\mu_2 \subset O(q)$ for even n .*

1. Assume n is even. The Dickson morphism D_q is a smooth surjection identifying $(\mathbf{Z}/2\mathbf{Z})_S$ with $O(q)/SO(q)$. In particular, $O(q)$ is smooth with $\#\pi_0(O(q)_s) = 2$ for all $s \in S$.
2. Assume n is odd. Multiplication against the central $\mu_2 \subset O(q)$ defines an isomorphism $\mu_2 \times SO(q) \simeq O(q)$. In particular, $O(q)$ is smooth over $S[1/2]$ and flat over S , and $O(q)/SO(q) = \mu_2$ (so $O(q)_s$ is connected if $\text{char}(k(s)) = 2$).

We will also determine the functorial centers of these groups when $n \geq 3$: $O(q)$ has functorial center represented by the central μ_2 , whereas the centers of $SO(q)$ and $SO'(q)$ coincide and equal μ_2 (resp. 1) when n is even (resp. odd). Since the case of odd rank requires special care in residue characteristic 2, we shall first analyze even rank, where we can use characteristic-free arguments.

A.2 Even rank

We will prove the smoothness of the closed subscheme $O(q) \subset GL(V)$ when n is even by comparing its fibral dimension to the number of local equations that cut it out inside the smooth scheme $GL(V)$. (A proof can be given by using the infinitesimal criterion, but equation-counting is simpler in this case.)

One subtlety is that since we do not yet know S -flatness for $O(q)$ (which will be obtained from smoothness results for $SO(q)$), we do not know that there is a plentiful supply of sections after fppf-local base change on S . In particular, it is not evident whether smoothness near the identity section is sufficient to deduce smoothness of the entire group (as that intuition over a field is based on the ability to do translations after a ground field extension, which is always faithfully flat).

As a concrete counterexample, consider the reduced closed complement G of the open non-identity point in the generic fiber of the constant group $(\mathbf{Z}/2\mathbf{Z})_R$ over a discrete valuation ring R . This R -group is a disjoint union of the identity section and an additional rational point in the special fiber, so it is affine and also R -smooth near the identity section with constant fibers but is not R -flat. To circumvent this problem, we will use a “global” criterion in terms of equation-counting:

Lemma A.2.1. *Let R be a ring and G a smooth affine R -group. Let $G' \hookrightarrow G$ be a closed subgroup scheme whose defining ideal admits c global generators f_1, \dots, f_c and whose fibers G'_s satisfy $\dim \text{Tan}_{e(s)}(G'_s) = \dim \text{Tan}_{e(s)}(G_s) - c$. Then G' is R -smooth.*

The special case $G = GL(V)$ is [DG, II, §5, 2.7].

Proof. Each fiber G'_s has codimension at most c in G_s , so

$$\dim G'_s \geq \dim G_s - c = \dim \text{Tan}_{e(s)}(G_s) - c = \dim \text{Tan}_{e(s)}(G'_s).$$

Thus, the $k(s)$ -group G'_s is smooth for all $s \in S$ (due to the homogeneity of the geometric fiber G'_s). Since an open subset of G' that contains all closed points of all fibers must be the entire space, by openness of the smooth locus it suffices to prove that G' is smooth at each point g' that is closed in its fiber G'_s . The $k(s)$ -smoothness of G'_s at the closed point g' implies that the local ring $O_{G'_s, g'} = O_{G_s, g'} / ((f_1)_s, \dots, (f_c)_s)$ is regular with dimension $\dim G'_s = \dim G_s - c = \dim O_{G_s, g'} - c$. In other words, in the regular local ring $O_{G_s, g'}$ the sequence $\{(f_j)_s\}$ in the maximal ideal is part of a regular system of parameters. Since G_s and G'_s are $k(s)$ -smooth, by computing at a point over g' on geometric fibers over s we see that the elements

$$d(f_j)(g') \in \Omega_{G'/S, g'}^1 / \mathfrak{m}_{g'} = \Omega_{G'_s/k(s), g'}^1 \otimes_{O_{G'_s, g'}} k(g')$$

are $k(g')$ -linearly independent. Hence, by the Jacobian criterion for smoothness of a closed subscheme of a smooth scheme [BLR, 2.2/7], G' is \mathbb{R} -smooth. \square

Lemma A.2.2. *Inside $\text{End}(V) = \text{Tan}_e(\text{GL}(V))$, we have*

$$\text{Tan}_e(O(q)) = \{T \in \text{End}(V) \mid B_q(v, Tw) \text{ is alternating}\}.$$

This lemma makes no hypothesis on the parity of n .

Proof. We may assume $S = \text{Spec } k$ for a ring k . In terms of dual numbers, $\text{Tan}_e(O(q))$ is the space of linear endomorphisms T of V such that $1 + \epsilon T$ preserves $q_{k[\epsilon]}$ on $V_{k[\epsilon]}$. For any $x \in V_{k[\epsilon]}$ with reduction $x_0 \in V$, clearly $\epsilon T(x) = \epsilon T(x_0)$, so

$$q_{k[\epsilon]}(x + \epsilon T(x_0)) = q_{k[\epsilon]}(x) + \epsilon B_q(x_0, T(x_0))$$

since $\epsilon^2 = 0$. Thus, the necessary and sufficient condition on T is that the bilinear form $B_q(v, Tw)$ vanishes on the diagonal, which is to say that it is alternating. \square

Proposition A.2.3. *If n is even then $O(q)$ is smooth of relative dimension $n(n-1)/2$. In particular, the open and closed subgroup $SO(q)$ is smooth and the surjective Dickson morphism $D_q : O(q) \rightarrow (\mathbb{Z}/2\mathbb{Z})_S$ is smooth, identifying $(\mathbb{Z}/2\mathbb{Z})_S$ with $O(q)/SO(q)$.*

Proof. Once smoothness of $O(q)$ is proved, the Dickson morphism must be smooth since it is visibly smooth over fibers over S . The other assertions are then clear as well. The smoothness of $O(q)$ is fppf-local on the base, so by Lemma A.1.3 it suffices to treat $q = q_n$ over \mathbb{Z} (or over any affine base). By a permutation of the variables, we may equivalently assume $q = \sum_{i=0}^m x_i x_{i+m}$ where $2m = n$. To prove the smoothness for this q , we will use the criterion in Lemma A.2.1.

We express $n \times n$ matrices in the block form $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$ where A, B, C, D are $m \times m$ matrices, and we likewise express (x_1, \dots, x_n) as a pair (x, y) where x and y are ordered m -tuples. Thus, our quadratic form is $q(x, y) = \bar{y}^t \bar{x}$ where \bar{y} and \bar{x} are “column vectors” (i.e., $m \times 1$ matrices). For any $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ we have $M(x, y) = (Ax + By, Cx + Dy)$, so

$$q(M(x, y)) = \bar{x}^t C^t A \bar{x} + \bar{y}^t D^t B \bar{y} + \bar{y}^t (D^t A + B^t C) \bar{x}.$$

Hence, $M \in O(q)$ if and only if $D^t A + B^t C = 1_m$ and the matrices $C^t A$ and $D^t B$ are alternating (in the sense that the associated bilinear forms in m variables that they define are alternating; i.e., vanish on pairs (x, x)).

The alternating condition on an $m \times m$ matrix amounts to $m + m(m-1)/2 = m(m+1)/2$ equations in the matrix entries, so the alternating conditions on $C^t A$ and $D^t B$ amount to $m(m+1)$ equations in the matrix entries of A, B, C, D . The condition $D^t A + B^t C = 1_m$ amounts to m^2 such equations, so the closed subscheme $O(q) \subset \text{GL}_n$ is defined by an ideal generated by $m^2 + m(m+1) = m(2m+1)$ elements. Thus, by Lemma A.2.1, to prove $O(q)$ is smooth we just need to check that over an algebraically closed field k , $\text{Tan}_e(O(q))$ has codimension $m(2m+1)$ in $\mathfrak{gl}_{2m}(k)$. By Lemma A.2.2, an element $M \in \mathfrak{gl}_{2m}(k)$ lies in $\text{Tan}_e(O(q))$ if and only if the matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} M = \begin{pmatrix} C & B \\ A & D \end{pmatrix}$ is alternating. This says that B and C are alternating and $D = -A^t$, which again amounts to $m(2m+1)$ (linear) equations on $\mathfrak{gl}_{2m}(k)$. We also conclude that the relative dimension of $O(q)$ is $(2m)^2 - m(2m+1) = 2m^2 - m = n(n-1)/2$. \square

Corollary A.2.4. *If n is even then $SO(q) \rightarrow S$ has connected fibers.*

Proof. We proceed by 2-step induction on n , and we can assume $S = \text{Spec } k$ for an algebraically closed field k . Without loss of generality, $q = q_n$. In view of the surjectivity of the Dickson morphism, it is equivalent to show that $O(q)$ has exactly two connected components. Since $q_2 = xy$, clearly $O_2 = \mathbf{G}_m \amalg \mathbf{G}_m \iota$ for $\iota = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Now assume $n \geq 4$ and that the result is known for $n - 2$.

Since q is not a square (as $n > 1$), it is straightforward to check that the smooth affine hypersurface $H = \{q = 1\}$ is irreducible. The points in $H(k)$ correspond to embeddings of quadratic spaces $(k, x^2) \hookrightarrow (V, q)$. By Witt's extension theorem [Chev, I.4.1], if (W, Q) is a finite-dimensional quadratic space over a field K and B_Q is non-degenerate (so $\dim W$ is even when $\text{char}(K) = 2$) then $O(Q)(K)$ acts transitively on the set of embeddings of a fixed (possibly degenerate) quadratic space into (W, Q) . Hence, $O(q)(k)$ acts transitively on $H(k)$, so the orbit map $O(q) \rightarrow H$ through e_2 is surjective with stabilizer $G' := \text{Stab}_{e_2}(O(q))$ that preserves the orthogonal complement $V' := e_2^\perp = \sum_{i \geq 2} ke_i$. Since H is connected, it follows that $O(q)^0$ acts transitively on H too, so $\#\pi_0(O(q)) \leq \#\pi_0(G')$. Hence, it suffices to show that G' has 2 connected components.

The action map $G' \rightarrow \text{GL}(V')$ has kernel consisting of automorphisms of V that fix $\{e_2, \dots, e_n\}$ and preserve q . Such automorphisms must preserve the orthogonal complement $ke_1 + ke_2$ of the span of $\{e_3, \dots, e_n\}$, so it is an elementary calculation that the scheme-theoretic kernel of $G' \rightarrow \text{GL}(V')$ is trivial. Let $W = (ke_1 + ke_2)^\perp = \sum_{i \geq 3} ke_i$. For any $w \in W$ we have $q(ce_2 + w) = c^2q(e_2) + B_q(ce_2, w) + q(w) = q(w)$, so relative to the ordered basis $\{e_2, \dots, e_n\}$ of V' the map $G' \rightarrow \text{GL}(V')$ is an isomorphism onto the subgroup of $(n-1) \times (n-1)$ matrices whose left column is $(1, 0, \dots, 0)$, top row has arbitrary entries beyond the initial 1, and lower right $(n-2) \times (n-2)$ block is $O(q|_W)$. In other words, G' is an extension of $O(q|_W)$ by \mathbf{G}_a^{n-2} . By induction we know that $O(q|_W)$ has exactly two connected components, so the same holds for G' . \square

Corollary A.2.5. *For even n , the determinant map $\det : O(q) \rightarrow \mathbf{G}_m$ factors through μ_2 and kills $SO(q)$. The resulting inclusion $SO(q) \subset SO'(q)$ is an equality over $S[1/2]$, and $SO'(q) \hookrightarrow O(q)$ is an equality on fibers at points in characteristic 2.*

Proof. Any point of $O(q)$ preserves the symmetric bilinear form B_q , and B_q is a perfect pairing (as we may check on fibers, since n is even). Thus, the classical matrix calculation carries over to the relative setting to show that any automorphism of V preserving B_q must have determinant valued in μ_2 .

To prove that $SO(q)$ is killed by the determinant, by working fppf-locally on S and using Lemma A.1.3 we may pass to the case $q = q_n$ over \mathbf{Z} . The flatness of $SO(q)$ then reduces the problem to the generic fiber over \mathbf{Q} , so we are over a field not of characteristic 2. Hence, μ_2 is étale, so the *connected* $SO(q)$ has no nontrivial homomorphism to μ_2 .

The determinant is fiberwise nontrivial on O_n over $\mathbf{Z}[1/2]$ since the automorphism of \mathbf{Z}^n that swaps e_1 and e_2 has determinant -1 and preserves q_n . Hence, at points away from characteristic 2 the determinant map factors through a nontrivial homomorphism $O(q_s)/SO(q_s) \rightarrow \mu_2$. Since $O(q_s)/SO(q_s) = \mathbf{Z}/2\mathbf{Z}$, it follows that $SO(q_s) = SO'(q_s)$ for such s . In other words, over $S[1/2]$ the closed subscheme $SO'(q)$ in $O(q)$ is topologically supported in the open and closed subscheme $SO(q)$, and that forces the inclusion $SO(q) \subset SO'(q)$ to be an equality over $S[1/2]$. At points s of characteristic 2, the smooth group $O(q_s)$ must be killed by the determinant map into the infinitesimal μ_2 , so $SO'(q_s) = O(q_s)$ for such s . \square

Remark A.2.6. For even n , consider the element $g \in O_n(\mathbf{Z})$ that swaps x_1 and x_2 while leaving all other x_i 's invariant. The section $D_q(g)$ of the constant \mathbf{Z} -group $\mathbf{Z}/2\mathbf{Z}$ is equal to 1 mod 2 since it suffices to check this on a single geometric fiber, and at any fiber away from characteristic 2 it is clear (as SO_n coincides with SO'_n over $\mathbf{Z}[1/2]$). Thus, the Dickson morphism $D_q : O(q) \rightarrow (\mathbf{Z}/2\mathbf{Z})_S$ splits as a semidirect product when $q = q_n$.

The induced map $H^1(S_{\text{ét}}, O_n) \rightarrow H^1(S_{\text{ét}}, \mathbf{Z}/2\mathbf{Z})$ assigns to every non-degenerate (V, q) of rank n over S (taken up to isomorphism) a degree-2 finite étale cover of S . This is the *Dickson invariant* of (V, q) . If S is a $\mathbf{Z}[1/2]$ -scheme (so $(\mathbf{Z}/2\mathbf{Z})_S = \mu_2$) then it recovers the *discriminant* viewed in $\mathbf{G}_m(S)/\mathbf{G}_m(S)^2$. If S is an \mathbf{F}_2 -scheme then it recovers the *pseudo-discriminant*, also called the *Arf invariant* when $S = \text{Spec } k$ for a field k/\mathbf{F}_2 . The existence of the section to D_{q_n} implies that every degree-2 finite étale S -scheme arises as the Dickson invariant of some rank- n non-degenerate quadratic space over S .

Corollary A.2.7. *For even n , the \mathbf{Z} -group SO'_n is reduced and the open and closed subscheme $SO_n \hookrightarrow SO'_n$ has complement equal to the non-identity component of $(O_n)_{\mathbf{F}_2}$. In particular, SO'_n is not \mathbf{Z} -flat when n is even.*

Proof. Corollary A.2.5 gives the result over $\mathbf{Z}[1/2]$, as well as the topological description of the \mathbf{F}_2 -fiber. It remains to show that SO'_n is reduced. It is harmless to pass to the quotient by the *smooth* normal subgroup SO_n , so under the identification of $\mathrm{O}_n/\mathrm{SO}_n$ with the constant group $\mathbf{Z}/2\mathbf{Z}$ via the Dickson morphism we see that $G = \mathrm{SO}'_n/\mathrm{SO}_n$ is identified with the kernel of a homomorphism of \mathbf{Z} -groups $f : \mathbf{Z}/2\mathbf{Z} \rightarrow \mu_2$. The map f is nontrivial since $\mathrm{SO}'_n \neq \mathrm{SO}_n$, and there is only one nontrivial homomorphism from $\mathbf{Z}/2\mathbf{Z} = \mathrm{Spec} \mathbf{Z}[t]/(t^2 - t)$ to $\mu_2 = \mathrm{Spec} \mathbf{Z}[\zeta]/(\zeta^2 - 1)$ over \mathbf{Z} (as we see by using flatness to pass to the \mathbf{Q} -fiber). This map corresponds to $1 \mapsto -1$, or equivalently $\zeta - 1 \mapsto -2t$ on coordinate rings, so the kernel G is equal to $\mathrm{Spec} \mathbf{Z}[t]/(-2t, t^2 - t)$. This is precisely the disjoint union of the identity section and a single \mathbf{F}_2 -point in the \mathbf{F}_2 -fiber. \square

A.3 Odd rank

In contrast with the case of even n , our proof of the smoothness of $\mathrm{SO}(q)$ for odd n has to be different because $\mathrm{O}(q)$ is not smooth over \mathbf{Z} . This is already seen in the trivial case $n = 1$, and in general we will show that $\mathrm{O}(q) = \mu_2 \times \mathrm{SO}(q)$, so smoothness always fails in characteristic 2. The infinitesimal criterion is ill-suited to this situation, because over a base ring such as $\mathbf{Z}/4\mathbf{Z}$ or $\mathbf{Z}_{(2)}$ in which 2 is neither a unit nor 0 we encounter the problem that the “defect space” V^\perp is generally not a subbundle of V . That complicates efforts to verify the infinitesimal criterion when “deforming away from defect-1”.

By Lemma A.1.3, to prove smoothness of $\mathrm{SO}(q)$ for odd n in general, it suffices to treat the case $q = q_n$ over \mathbf{Z} . Our replacement for Lemma A.2.1 is a criterion over a Dedekind base that upgrades fibral smoothness to relative smoothness in the presence of a *global* hypothesis of fibral connectedness. First we need to record the useful *fibral isomorphism criterion*:

Lemma A.3.1. *Let $h : Y \rightarrow Y'$ be a map between finite type schemes over a noetherian scheme S , and assume that Y is S -flat. If h_s is an isomorphism for all $s \in S$ then h is an isomorphism.*

Proof. This is part of [EGA, IV₄, 17.9.5], but here is a sketch of an alternative proof. By using that $\Delta_h : Y \rightarrow Y \times_{Y'} Y$ satisfies the given hypotheses and is separated, we can reduce to the case when h is separated, and then that Y and Y' are S -separated. For artin local $S = \mathrm{Spec} A$ it is easy to show that h is a closed immersion, and then S -flatness of Y implies that the ideal defining Y in Y' vanishes modulo \mathfrak{m}_A , so $Y = Y'$. This settles the result over an artin local base, so in general h is an isomorphism between infinitesimal fibers over S . Hence, h is *flat* (by the so-called “local flatness criterion”).

Now we can use a remarkable finiteness criterion of Deligne and Rapoport [DR, II, 1.19]: a quasi-finite separated flat map $f : X \rightarrow T$ between noetherian schemes is finite if its fibral rank is Zariski-locally constant on the base (the converse being obvious). Granting this criterion, it follows that h is finite (as its fibral rank is always 1), and being finite flat of degree 1 it must be an isomorphism (check!).

It remains to prove the Deligne–Rapoport finiteness criterion, for which we may assume the fibral rank is constant. Since a proper quasi-finite map is finite, it suffices to prove that f is proper. By the valuative criterion for properness, this reduces the problem to the case when $T = \mathrm{Spec} R$ for a discrete valuation ring R . By Zariski’s Main Theorem, the quasi-finite separated X over T admits an open immersion $j : X \hookrightarrow \bar{X}$ into a finite T -scheme \bar{X} . We can replace \bar{X} with the schematic closure of X , so \bar{X} has structure sheaf that is torsion-free over R . Hence, \bar{X} is R -flat, so as a finite flat R -scheme it has constant fiber rank. But its open subscheme X also has constant fiber rank and both X and \bar{X} have the same generic fiber. Thus, their constant fiber ranks coincide, and the equality of closed fiber ranks then forces $X = \bar{X}$, so we are done. \square

Now we can prove the desired smoothness criterion:

Proposition A.3.2. *Let S be a Dedekind scheme, and G an S -group of finite type such that all fibers G_s are smooth of the same dimension. Then G contains a unique smooth open subgroup G^0 whose s -fiber is $(G_s)^0$ for all $s \in S$. In particular, G is smooth if its fibers are connected.*

Proof. We may assume S is connected, say with generic point η . The smooth open subgroup $G_\eta^0 \subset G_\eta$ then “spreads out” over a dense open $U \subset S$ to a smooth open subgroup of G_U with connected fibers. This solves the problem over U , and to handle the remaining finitely many closed points in $S - U$ we may assume that $S = \mathrm{Spec} R$ for a discrete valuation ring R , say with fraction field K . We may and do remove the closed union of the non-identity components of the special fiber, so G has connected special fiber.

Let \mathcal{G} denote the schematic closure in G of the generic fiber G_K , so $\mathcal{G}_K = G_K$. The R -flat $\mathcal{G} \times \mathcal{G}$ is the schematic closure of its generic fiber $G_K \times G_K$, so it follows that the R -flat \mathcal{G} is an R -subgroup of G . This is a flat closed subscheme of G with constant fiber dimension (by flatness), so the closed immersion $\mathcal{G}_0 \hookrightarrow G_0$ between special fibers must be an isomorphism, as G_0 is smooth and connected and $\dim \mathcal{G}_0 = \dim \mathcal{G}_K = \dim G_K = \dim G_0$. Thus, \mathcal{G}_0 is smooth (as is $\mathcal{G}_K = G_K$), so \mathcal{G} is smooth.

The closed immersion $\mathcal{G} \hookrightarrow G$ is an isomorphism on fibers, so by flatness of \mathcal{G} it is an isomorphism, due to Lemma A.3.1 above. \square

Remark A.3.3. The final assertion in Proposition A.3.2 is valid more generally: if $G \rightarrow S$ is a finite type group over any reduced noetherian scheme S and if the fibers G_s are smooth and connected of the same dimension then G is smooth. Indeed, the problem is to verify flatness, and by the “valuative criterion for flatness” over a reduced noetherian base [EGA, IV₃, 11.8.1] it suffices to check this after base change to discrete valuation rings, to which Proposition A.3.2 applies. See [SGA3, VI_B, 4.4] for a further generalization.

The role of identity components in Proposition A.3.2 cannot be dropped. For a quasi-finite example, consider the constant group $(\mathbf{Z}/d\mathbf{Z})_R$ over a discrete valuation ring R with $d > 1$. This contains a reduced closed subgroup $G^{(d)}$ given by the reduced closed complement of the open non-identity points in the generic fiber. The R -group $G^{(d)}$ has étale fibers but is not flat over R (the non-identity points of the special fiber are open). A more interesting example is SO'_{2m} over $\mathbf{Z}_{(2)}$ (which is the pushout of $G^{(2)}$ along the identity section $\text{Spec } \mathbf{Z}_{(2)} \hookrightarrow SO_{2m}$; see the proof of Corollary A.2.7).

To apply Proposition A.3.2 to $SO(q)$ when n is odd, we need to verify three things in the theory over an algebraically closed field: connectedness, smoothness, and dimension depending only on n . We first address the connectedness and dimension aspects by a fibration argument in the spirit of the proof of connectedness for SO_{2m} :

Proposition A.3.4. *Let (V, q) be a non-degenerate quadratic space over a field k , with $n = \dim V$ odd. The group $SO(q)$ is connected with dimension $n(n-1)/2$ and multiplication against the central μ_2 defines an isomorphism $\mu_2 \times SO(q) \simeq O(q)$*

Proof. We may assume k is algebraically closed and $q = q_n$. The case $n = 1$ is trivial, so we assume $n \geq 3$. We treat characteristic 2 separately from other characteristics, due to the appearance of the defect space $V^\perp = ke_0$ in characteristic 2.

First assume $\text{char}(k) \neq 2$, so the symmetric bilinear form B_q is non-degenerate. Points of $O(q)$ preserve B_q and hence must have determinant valued in μ_2 (by a classical calculation with matrices). Since n is odd, the restriction of $\det : O(q) \rightarrow \mu_2$ to the central μ_2 is the identity map on μ_2 . Thus, $\mu_2 \times SO(q) = O(q)$. Hence, $O(q)$ has at least 2 connected components, and exactly 2 such components if and only if $SO(q)$ is connected. Since $n > 1$, the hypersurface $H = \{q = 1\}$ is irreducible, and exactly as in the proof of Corollary A.2.4 we may apply Witt’s extension theorem (valid for odd n since $\text{char}(k) \neq 2$) to deduce that the action of $O(q)$ on H is transitive. The orthogonal complement V' of e_0 is spanned by $\{e_1, \dots, e_{2m}\}$ since $\text{char}(k) \neq 2$, and it is preserved by $\text{Stab}_{e_0}(O(q))$. It is straightforward to check that the action of this stabilizer on V' defines an isomorphism onto $O(q|_{V'}) \simeq O_{2m}$. We already know that O_{2m} has 2 connected components and dimension $2m(2m-1)/2 = m(2m-1)$, whereas H is irreducible of dimension $n-1 = 2m$, so it follows that $O(q)$ has dimension $2m + m(2m-1) = n(n-1)/2$ and at most 2 connected components (hence exactly 2 such components). This settles the case $\text{char}(k) \neq 2$.

Now assume $\text{char}(k) = 2$. The non-vanishing defect space obstructs induction using the action on H , so instead we will use an entirely different procedure that is specific to characteristic 2. When $\text{char}(k) \neq 2$ we passed to the hyperplane ke_0^\perp spanned by e_1, \dots, e_{2m} on which B_q restricted to a non-degenerate symmetric bilinear form. In characteristic 2, we will use the $(n-1)$ -dimensional quotient $V' := V/V^\perp = V/ke_0$ rather than a hyperplane. More specifically, because V^\perp is the defect space, B_q factors through a non-degenerate symmetric bilinear form B'_q on V' . This has an extra property: it is *alternating*, since $\text{char}(k) = 2$. Any point of $O(q)$ preserves the defect space, and the induced automorphism of V' preserves \bar{B}_q . This defines a homomorphism

$$h : O_{2m+1} = O(q) \rightarrow \text{Sp}(V', B'_q) \simeq \text{Sp}_{2m}$$

from our orthogonal group to a symplectic group.

The kernel is seen by direct calculation to be $\alpha_2^{n-1} \rtimes \mu_2$ (along the top row of matrices, with μ_2 in the upper left), where μ_2 acts on the Frobenius kernel $\alpha_2 \subset \mathbf{G}_a$ by the usual scaling action. Indeed, rather

explicitly, since a point T of $O(q)$ must restrict to an automorphism of the quadratic space $V^\perp = (ke_0, x_0^2)$, it has the block form

$$T = \begin{pmatrix} \zeta & \alpha & \alpha' \\ 0 & A & B \\ 0 & C & D \end{pmatrix}$$

for $m \times m$ matrices A, B, C, D , a point ζ of μ_2 , and ordered m -tuples α and α' . Writing a typical ordered $(2m+1)$ -tuple as (x_0, x, x') for ordered m -tuples x and x' , we see that

$$q(T(x_0, x, x')) = x_0^2 + \langle \alpha, x \rangle^2 + \langle \alpha', x' \rangle^2 + B'_q(Ax + By, Cx + Dy),$$

where $\langle \cdot, \cdot \rangle$ is the standard bilinear form $(w, z) \mapsto \sum w_j z_j$. Setting this equal to $q(x_0, x, x')$ then imposes equations on $\alpha, \alpha', A, B, C, D$ that define the closed subscheme $O(q) \subset GL_n$. This not only implies the description of $\ker h$, but also shows that h is surjective.

The smoothness of symplectic group schemes is easily proved by the infinitesimal criterion, and the dimension is likewise easily determined by direct computation of the tangent space. This gives that Sp_{2m} has dimension $m(2m+1) = n(n-1)/2$. Finally, the connectedness of symplectic groups is easily proved by an inductive fibration argument (using lower-dimensional symplectic spaces). Since h is surjective with infinitesimal kernel, we conclude that $O(q)$ is connected of dimension $n(n-1)/2$.

Since $Sp_{2m} \subset SL_{2m}$ as k -groups, the above functorial description of points T of O_{2m+1} shows that $\det T = \zeta \in \mu_2$. Thus, $\det : O(q) \rightarrow \mathbf{G}_m$ factors through μ_2 , and once again the oddness of n implies that the central μ_2 in $O(q)$ thereby splits off as a direct factor. Hence, $\mu_2 \times SO(q) = O(q)$. This implies that $SO(q)$ is connected of dimension $n(n-1)/2$ since μ_2 is infinitesimal in characteristic 2. \square

Now we can pass to the relative case and establish smoothness too:

Proposition A.3.5. *If n is odd then $SO(q) \rightarrow S$ is smooth with connected fibers of dimension $n(n-1)/2$, and the multiplication map $\mu_2 \times SO(q) \rightarrow O(q)$ against the central μ_2 is an isomorphism.*

Proof. By Lemma A.1.3, we may assume $q = q_n$ over $S = \text{Spec } \mathbf{Z}$. The case $n = 1$ is trivial, so we assume $n = 2m+1$ with $m \geq 1$. Since the fibers are connected of the same dimension $(n(n-1)/2)$, by Proposition A.3.4, to prove smoothness we may apply Proposition A.3.2 to reduce to proving fibral smoothness. In other words, we wish to show that over a field k , the tangent space $\text{Tan}_e(SO(q))$ has dimension $n(n-1)/2$. To do this we will treat characteristic 2 separately from other characteristics.

First assume $\text{char}(k) \neq 2$, so the equality $\mu_2 \times SO(q) = O(q)$ implies $\text{Tan}_e(SO(q)) = \text{Tan}_e(O(q))$. This latter tangent space is identified in Lemma A.2.2: it is the space of linear endomorphisms T of V such that $B_q(v, Tw)$ is alternating. But B_q is non-degenerate since $\text{char}(k) \neq 2$, so $T \mapsto B_q(\cdot, T(\cdot))$ identifies $\text{Tan}_e(O(q))$ with the space $\text{Alt}^2(V)$ of alternating bilinear forms on V . This is the dual of $\wedge^2(V)$, so it has dimension $n(n-1)/2$, as desired.

Now assume $\text{char}(k) = 2$. Let $V' = V/V^\perp$, and let B'_q the induced non-degenerate alternating form on V' . Since $\mu_2 \times SO(q) = O(q)$ and $\text{Tan}_e(\mu_2)$ is 1-dimensional, it is equivalent to show that $\text{Tan}_e(O(q))$ has dimension $1 + n(n-1)/2$. We will construct a short exact sequence

$$0 \rightarrow \text{Hom}(V, V^\perp) \rightarrow \text{Tan}_e(O(q)) \rightarrow \text{Alt}^2(V/V^\perp) \rightarrow 0,$$

from which we will get the desired dimension count

$$n + (n-1)(n-2)/2 = m(2m-1) + (2m+1) = 2m^2 + m + 1 = m(2m+1) + 1 = 1 + n(n-1)/2.$$

To construct the exact sequence, we will compute using dual numbers as in the proof of Lemma A.2.2. Using notation as in that calculation, since the alternating property for $B_q(v, Tw)$ implies skew-symmetry and hence symmetry (as $\text{char}(k) = 2$), T must preserve the defect line V^\perp (as $B_q(v, Tw) = 0$ for $v \in V^\perp$ and any w , and $B_q(v, Tw)$ is symmetric for general $v, w \in V$). Thus, $\text{Tan}_e(O(q))$ consists of those T which preserve V^\perp and whose induced endomorphism T' of $V' = V/V^\perp$ makes $B'_q(v', T'w')$ alternating. By non-degeneracy of B'_q , every bilinear form on V' is $B'_q(v', Lw')$ for a unique endomorphism L of V' , so the vector space $\text{Tan}_e(O(q))$ fits into the asserted exact sequence since $\text{Hom}(V, V^\perp)$ is precisely the ambiguity in T when T' is given.

Smoothness has now been proved in the general relative setting, and it remains to prove that the natural homomorphism $f : \mu_2 \times \mathrm{SO}(q) \rightarrow \mathrm{O}(q)$ is an isomorphism. The map f_s between fibers over any $s \in S$ is an isomorphism (Proposition A.3.4), and the source of f is S -flat (as $\mathrm{SO}(q)$ is even S -smooth). Thus, f is an isomorphism due to the fibral isomorphism criterion in Lemma A.3.1. \square

Corollary A.3.6. *Assume n is odd. The map $\det : \mathrm{O}(q) \rightarrow \mathbf{G}_m$ factors through μ_2 , and its kernel is $\mathrm{SO}(q)$. In particular, \det identifies $\mathrm{O}(q)/\mathrm{SO}(q)$ with μ_2 .*

Proof. Since $\mathrm{O}(q) = \mu_2 \times \mathrm{SO}(q)$ via multiplication and the determinant on the central μ_2 is the inclusion $\mu_2 \hookrightarrow \mathbf{G}_m$ (as n is odd), we are done. \square

Remark A.3.7. In the proof of Proposition A.3.4, over any field k of characteristic 2 we constructed a surjective homomorphism $\mathrm{O}(q) \rightarrow \mathrm{Sp}(V', B'_q)$ with infinitesimal geometric kernel $\mu_2 \rtimes \alpha_2^{n-1}$ when n is odd. This kernel meets the kernel $\mathrm{SO}(q)$ of the determinant map on $\mathrm{O}(q)$ in α_2^{n-1} , so by smoothness of $\mathrm{SO}(q)$ we obtain a purely inseparable isogeny $\mathrm{SO}(q) \rightarrow \mathrm{Sp}(V', B'_q)$ with kernel that is a form of α_2^{n-1} . This “unipotent isogeny” is a source of many weird phenomena related to algebraic groups in characteristic 2 (e.g., see [CP, A.3]).

For the benefit of those who have some prior awareness of the theory of root systems (perhaps in the context of connected compact Lie groups or semisimple Lie algebras over \mathbf{C}), here is the broader significance of the preceding strange isogenies. In the setting of connected semisimple algebraic groups over arbitrary fields to be taken up in the sequel course, special orthogonal groups in $2m+1$ variables are type B_m and symplectic groups in $2m$ variables are type C_m (as in Lie theory over \mathbf{C}). These types are distinct for $m \geq 3$ (for $m = 1$ and $m = 2$ the types coincide; see Example A.5.2 and Example A.5.5 respectively), and the deeper structure theory of semisimple groups via root systems shows that in characteristics distinct from 2 and 3 there are no isogenies between (absolutely simple) connected semisimple groups of different types. However, in characteristic 2 we have just seen that isogenies exist between the distinct types B_m and C_m for all $m \geq 3$. See [SGA3, XXI, 7.5] for further details.

A.4 Center

The remaining structural property of the groups $\mathrm{SO}(q)$ and $\mathrm{O}(q)$ (and $\mathrm{SO}'(q)$) that we wish to determine is the functorial center. Since $\mathrm{O}(q)$ is commutative when $n \leq 2$, we will assume $n \geq 3$. For odd n , the central μ_2 in $\mathrm{O}(q)$ has trivial intersection with $\mathrm{SO}'(q)$, and hence with $\mathrm{SO}(q)$, so there is no obvious nontrivial point in the center. If n is even then the central μ_2 is contained in $\mathrm{SO}'(q)$, and we claim that it also lies in $\mathrm{SO}(q)$. In other words, for even n we claim that the Dickson morphism $D_q : \mathrm{O}(q) \rightarrow (\mathbf{Z}/2\mathbf{Z})_S$ kills the central μ_2 . It suffices to treat the case of $q = q_n$ over \mathbf{Z} , in which case we just need to show that the *only* homomorphism of \mathbf{Z} -groups $\mu_2 \rightarrow \mathbf{Z}/2\mathbf{Z}$ is the trivial one. By flatness, to prove such triviality it suffices to check after localization to $\mathbf{Z}_{(2)}$. But over the local base $\mathrm{Spec} \mathbf{Z}_{(2)}$ the scheme μ_2 is connected and thus it must be killed by a homomorphism into a constant group.

Proposition A.4.1. *Assume $n \geq 3$. The functorial centers of $\mathrm{SO}(q)$ and $\mathrm{SO}'(q)$ coincide. This common center is represented by μ_2 in the central $\mathbf{G}_m \subset \mathrm{GL}(V)$ when n is even, and it is trivial when n is odd.*

Proof. By Lemma A.1.3, it suffices to treat the Bureau of Standards form q_n and $S = \mathrm{Spec} k$ for a ring k . We will use a method similar to the treatment of $Z_{\mathrm{Sp}_{2n}}$ in HW4 Exercise 1: we will exhibit a specific torus T that we show to be its own centralizer in $G := \mathrm{SO}'(q)$ (so T its own centralizer in $\mathrm{SO}(q)$) and then we will look for the center inside this T . To write down an explicit such T , we will use the standard form of q .

First suppose $n = 2m$, so relative to a suitable ordered basis $\{e_1, e'_1, \dots, e_m, e'_m\}$ we have $q = \sum_{i=1}^m x_i x'_i$. In this case we identify GL_1^m with a k -subgroup T of $\mathrm{SO}'(q)$ via

$$j : (t_1, \dots, t_m) \rightarrow (t_1, 1/t_1, \dots, t_m, 1/t_m).$$

To prove that $Z_G(T) = T$, we consider the closed subgroup $T_j \simeq \mathbf{G}_m$ given by the j th factor of GL_1^m (so $T = \prod T_j$). It is easy to compute that the centralizer of T_j in $\mathrm{GL}(V) = \mathrm{GL}_{2m}$ is a direct product $D_j \times \mathrm{GL}_{2m-2}$ according to the decomposition

$$V = (ke_j \oplus ke'_j) \bigoplus_{i \neq j} (ke_i \oplus ke'_i),$$

where $D_j \subset GL_2$ is the diagonal torus. Thinking functorially, the centralizer of T in $GL(V)$ is the (scheme-theoretic) intersection of the centralizers of the T_j 's, so this is the diagonal torus D in $GL(V)$. But the explicit form of q shows that $D \cap SO'(q) = T$.

Now suppose $n = 2m + 1$ with $m \geq 1$. Pick a basis $\{e_0, e_1, e'_1, \dots, e_m, e'_m\}$ relative to which

$$q = x_0^2 + \sum_{i=1}^m x_i x'_i.$$

If we define T in the same way (using the span of $e_1, e'_1, \dots, e_m, e'_m$) then the same analysis gives the same result: T is its own scheme-theoretic centralizer in $SO'(q)$. The point is that there is no difficulty created by e_0 because we are requiring the determinant to be 1. (If we try the same argument with $O(q)$ then the centralizer of T would be $\mu_2 \times T$.)

With $Z_{SO'(q)}(T) = T$ proved in general, we are now in position to identify the center of $SO'(q)$ when $n \geq 3$. First we assume $n \geq 4$ (i.e., $m \geq 2$). In terms of the ordered bases as above, consider the automorphisms obtained by swapping the ordered pairs (e_i, e'_i) and (e'_i, e_i) for $1 < i \leq m$. (Such i exist precisely because $m \geq 2$.) These automorphisms lie in $SO'(q)$ since the determinant is $(-1) \cdot (-1) = 1$, and a point of $T = \prod S_j$ centralizes it if and only if the components along S_1 and S_i agree. Letting i vary, we conclude that the center is contained in the “scalar” subgroup $GL_1 \hookrightarrow T$ given by $t_1 = \dots = t_m$. This obviously holds when $m = 1$ (i.e., $n = 3$) as well.

Letting t denote the common value of the t_j , to constrain it further we consider more points of $SO'(q)$ against which it should be central. First assume $m \geq 2$. Consider the automorphism f of V which acts on the plane $ke_i \oplus ke'_i$ by the matrix $w = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ (and leaves all other basis vectors invariant) for exactly *two* values $i_0, i_1 \in \{1, \dots, m\}$, so $\det f = 1$. Clearly f preserves q , so f lies in $SO'(q)(k)$. But f -conjugation of t viewed in $SO'(q)$ (or $GL(V)$) carries t_i to $1/t_i$ for $i \in \{i_0, i_1\}$. Thus, the centralizing property forces $t \in \mu_2$. This is the central μ_2 in $GL(V)$, so $Z_{SO'(q)} = \mu_2$ when $n \geq 4$ is even. If n is odd then the central μ_2 in $GL(V)$ has trivial intersection with $SO'(q) = SO(q)$, so $Z_{SO'(q)} = 1$ for odd $n \geq 5$.

Next, we give a direct proof that $Z_{SO_3} = 1$. The action of PGL_2 on \mathfrak{sl}_2 via conjugation defines an isomorphism $PGL_2 \simeq SO_3$; see the self-contained calculations in Example A.5.2. By HW3 Exercise 4(ii) the scheme-theoretic center of PGL_r is trivial for any $r \geq 2$ (and for PGL_2 it can be verified by direct calculation), so SO_3 has trivial center.

We have settled the case of odd $n \geq 3$, and for even $n \geq 4$ we have proved that $SO'(q)$ has center μ_2 that also lies in $SO(q)$. It remains to show, assuming $n \geq 4$ is even, that the functorial center of $SO(q)$ is no larger than this μ_2 . We may and do assume $q = q_n$. The torus T constructed above in SO'_n lies in the open and closed subgroup SO_n for topological reasons, and $Z_{SO_n}(T) = T$ since T has been shown to be its own centralizer in SO'_n . Thus, it suffices to show that the central μ_2 is the kernel of the adjoint action of T on $\text{Lie}(SO_n) = \text{Lie}(O_n)$. The determination of the weight space decomposition for T acting on $\text{Lie}(O_n)$ is classical, from which the kernel is easily seen to be the diagonal μ_2 . \square

Corollary A.4.2. *For $n \geq 3$, the functorial center of $O(q)$ is represented by the central μ_2 .*

Proof. If n is odd then the identification $O(q) = \mu_2 \times SO(q)$ yields the result since $SO(q)$ has trivial functorial center for such n . Now suppose that n is even. In this case the open and closed subgroup $SO(q)$ contains the central μ_2 is its functorial center. To prove that μ_2 is the functorial center of $O(q)$ we again pass to the case $q = q_n$. It suffices to check that the diagonal torus T in SO_n is its own centralizer in O_n .

Writing $n = 2m$, we may rearrange variables so that $q = \sum_{i=1}^m x_i x_{i+m}$. Now the diagonal torus T consists of block matrices $\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix}$, and its centralizer in GL_{2m} consists of block matrices $\begin{pmatrix} a & 0 \\ 0 & a' \end{pmatrix}$ with diagonal $a, a' \in GL_m$. Membership in the orthogonal group is the condition $aa' = 1$, so indeed T is its own centralizer in O_n . \square

A.5 Accidental isomorphisms

The study of (special) orthogonal groups provides many examples of *accidental isomorphisms* between low-dimensional members of distinct “infinite families” of algebraic groups. This is analogous to the isomorphisms between small members of distinct “infinite families” of finite groups (such as $\mathbf{Z}/3\mathbf{Z} \simeq PGL_2(\mathbf{F}_2)$, $S_4 \simeq PGL_2(\mathbf{F}_3)$, $S_5 \simeq PGL_2(\mathbf{F}_5)$, and so on). In fact, when such accidental isomorphisms among algebraic

groups are applied at the level of rational points of algebraic groups over *finite* fields one obtains many of the accidental isomorphisms among small finite groups.

Just as isomorphisms among small finite groups are due to the limited range of possibilities for finite groups of small size, the accidental isomorphisms between certain low-dimensional algebraic groups are due to a limitation in the possibilities for a “small” case of the root datum that governs the (geometric) isomorphism class of a connected semisimple group.

Example A.5.1. Suppose $n = 2$. In this case $O(q)$ is an étale form of

$$O_2 = T \coprod T \left(\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ for } T = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} \right\}.$$

Hence, $O(q)$ is smooth and $SO(q)$ is a rank-1 torus, whereas $SO'(q_s) = O(q_s)$ is disconnected when $\text{char}(k(s)) = 2$.

Example A.5.2. Suppose $n = 3$. In this case $SO(q)$ is an étale form of SO_3 . We claim that $SO_3 \simeq PGL_2$. To see this, consider the linear “conjugation” action of $PGL_2 = GL_2/\mathbf{G}_m$ on the rank-3 affine space \mathfrak{sl}_2 .

This action preserves the non-degenerate quadratic form Q on \mathfrak{sl}_2 given by the determinant. Explicitly, $Q\left(\begin{smallmatrix} x & y \\ z & -x \end{smallmatrix}\right) = -(x^2 + yz)$ is, up to sign, the Bureau of Standards quadratic form q_3 in 3 variables. Preservation of q_3 is the same as that of $-q_3$, so the sign does not affect the group. We get a homomorphism $PGL_2 \rightarrow O_3 = \mu_2 \times SO_3$ over \mathbf{Z} with trivial kernel. By computing on the Q -fibers, the map to the μ_2 -factor must be trivial. Thus, the map $PGL_2 \rightarrow O_3$ factors through SO_3 . Since PGL_2 is smooth and fiberwise connected of dimension 3, it follows that the monic map $PGL_2 \rightarrow SO_3$ is an isomorphism on fibers and hence is an isomorphism (Lemma A.3.1).

Example A.5.3. Suppose $n = 4$. In this case $SO(q)$ is not “absolutely simple”; i.e., on geometric fibers it contains nontrivial smooth connected proper normal subgroups. (This is the only $n \geq 3$ for which that happens, and in terms of root systems it corresponds to the equality $D_2 = A_1 \times A_1$.) In more concrete terms, we claim that

$$(SL_2 \times SL_2)/M \simeq SO_4$$

with $M = \mu_2$ diagonally embedded in the evident central manner.

To see where this comes from, apply a sign to the third standard coordinate to convert q_4 into $Q = x_1x_2 - x_3x_4$, which we recognize as the determinant of a 2×2 matrix. The group SL_2 acts on the rank-4 space of such matrices in two evident commuting ways, via $(g, g').x = gxg'^{-1}$, and these actions preserve the determinant by the very definition of SL_2 . This defines a homomorphism $SL_2 \times SL_2 \rightarrow SO'(Q) \simeq SO'_4$ whose kernel is easily seen to be M . This map visibly lands in SO_4 since SL_2 is fiberwise connected and $O_4/SO_4 = \mathbf{Z}/2\mathbf{Z}$. Hence, we obtained a monomorphism

$$(SL_2 \times SL_2)/M \rightarrow SO_4$$

that must be an isomorphism on fibers (as both sides have smooth connected fibers of the same dimension), and therefore an isomorphism.

Remark A.5.4. In the preceding example, we can also consider the action by the smooth connected affine group $GL_2 \times GL_2$ via $(g, g').x = gxg'^{-1}$. This preserves the determinant provided that $\det g = \det g'$, so if $H = GL_2 \times_{GL_1} GL_2$ (with fiber product via determinant) then we get a homomorphism $H \rightarrow SO_4$ whose kernel is the diagonal GL_1 .

Example A.5.5. Suppose $n = 5$. In this case SO_5 is the quotient of Sp_4 by its center μ_2 . (This corresponds to the accidental isomorphism of root systems $B_2 = C_2$.) To establish the isomorphism, consider a rank-4 symplectic space (V, ω_0) with $\omega_0 \in \wedge^2(V)^* = \wedge^2(V^*)$ the given symplectic form. The rank-6 vector bundle $\wedge^2(V)$ contains a rank-5 subbundle W of sections killed by ω_0 , and on $\wedge^2(V)$ there is a natural non-degenerate quadratic form q valued on $L = \det(V)$ defined by $q(\omega, \eta) = \omega \wedge \eta$. The action of $SL(V)$ clearly preserves q , the restriction $q|_W$ is non-degenerate (by direct calculation), and $Sp(\omega_0)$ preserves W (due to the definition of W). Thus, the $Sp(\omega_0)$ -action on W defines a homomorphism

$$Sp(\omega_0) \rightarrow O(q|_W)$$

that must factor through $\mathrm{SO}(\mathfrak{q}|_W)$ (as we can check by passing to the standard symplectic space (V, ω_0) of rank 4 over \mathbf{Z} and computing over \mathcal{Q}), and it kills the center μ_2 .

We claim that the resulting map $h : \mathrm{Sp}_4/\mu_2 \rightarrow \mathrm{SO}_5$ is an isomorphism. A computation shows that $\ker h$ has trivial intersection with the “diagonal” maximal torus, so $\ker h$ is quasi-finite and hence h is surjective for fibral dimension reasons. This forces h to be fiberwise flat, hence flat [EGA, IV₃, 11.3.10], so h has locally constant fiber rank that we claim is 1. By base change, it suffices to treat the standard symplectic space of rank 4 over \mathbf{Z} , for which we can compute the fiber rank over \mathcal{Q} . But in characteristic 0, isogenies between connected semisimple groups of adjoint type are necessarily isomorphisms.

Example A.5.6. Finally, suppose $n = 6$. In this case SO_6 is the quotient of SL_4 by the subgroup μ_2 in the central μ_4 . This corresponds to the accidental isomorphism of root systems $D_3 = A_3$, and to explain it we will again use the natural action of $\mathrm{SL}(V)$ on the rank-6 bundle $\wedge^2(V)$ equipped with the non-degenerate quadratic form $q(\omega, \eta) = \omega \wedge \eta$ valued in the line bundle $\det V$. The homomorphism $\mathrm{SL}(V) \rightarrow \mathrm{O}(q)$ defined in this way clearly kills the central μ_2 , and it factors through $\mathrm{SO}(q)$ (as $\mathrm{O}(q)/\mathrm{SO}(q) = \mathbf{Z}/2\mathbf{Z}$).

To prove that the resulting map $h : \mathrm{SL}(V)/\mu_2 \rightarrow \mathrm{SO}(q)$ is an isomorphism, by Lemma A.1.3 we may pass to \mathfrak{q}_6 over \mathbf{Z} . As in Example A.5.5, we reduce to the isomorphism problem over \mathcal{Q} . Isogenies between smooth connected groups in characteristic 0 are always central, and μ_4/μ_2 is not killed by h , so we are done.

B Existence of Jordan decomposition

In this appendix, we address the key issue in the proof of existence of Jordan decomposition: if k is algebraically closed and G is a smooth closed subgroup of some GL_n via $j : G \hookrightarrow \mathrm{GL}_n$ then for any $g \in G(k)$ we claim that $j(g)_{ss}$ and $j(g)_u$ lie in $G(k)$.

By Theorem 14.1.1, we may choose an auxiliary closed k -subgroup inclusion $i : G' = \mathrm{GL}_n \hookrightarrow \mathrm{GL}(V)$ such that $G = N_{G'}(L)$ for a line L in V . Thus, $i(j(g))$ preserves L , so the Jordan components $i(j(g))_{ss}$ and $i(j(g))_u$ preserve L since they are k -polynomials in $i(j(g))$ (computed in the k -algebra $\mathrm{End}(V)$). Hence, $i(j(g))_{ss}$ and $i(j(g))_u$ lie in $G(k)$ *provided* they lie in $G'(k)$! Thus, by replacing j with i we are reduced to the following more concrete problem: if $j : G = \mathrm{GL}_m \rightarrow G' = \mathrm{GL}_N$ is a k -subgroup inclusion then for any $g \in G(k)$ we have $j(g)_{ss} = j(g_{ss})$ and $j(g)_u = j(g_u)$; this assertion at least *makes sense* since the groups $\mathrm{GL}_m(k)$ and $\mathrm{GL}_N(k)$ have an a-priori theory of Jordan decomposition (for which we have already seen that the classical notions of semisimplicity and unipotence are equivalent to the corresponding properties for the associated right-translation operators on the coordinate ring).

Let $g' = j(g)$. This has a Jordan decomposition, say $g' = g'_{ss}g'_u$, and the right translation $\rho_{g'}$ on $k[G']$ is equivariant with respect to ρ_g on the *quotient* $k[G]$, so it preserves the kernel $I = \ker(k[G'] \twoheadrightarrow k[G])$. But on each finite-dimensional G' -stable subspace W of $k[G']$, the operators $\rho_{g'_{ss}} = \rho_{g',ss}$ and $\rho_{g'_u} = \rho_{g',u}$ are k -polynomials in $\rho_{g'|_W}$ and thus preserve $I \cap W$. The W 's exhaust $k[G']$ in the limit, so it follows that $\rho_{g'_{ss}}$ and $\rho_{g'_u}$ preserve I in $k[G']$, so they preserve the closed subscheme G in G' defined by I . That is, right translation on G' by g'_{ss} and g'_u preserve G , but these translations move 1 to g'_{ss} and g'_u respectively. Hence, $g'_{ss}, g'_u \in G(k)$! Moreover, the right-translation operators on $k[G]$ by these points are induced by the corresponding operators on $k[G']$ that *are* respectively semisimple and unipotent since by definition $g'_{ss}, g'_u \in G'(k) = \mathrm{GL}_N(k)$ are respectively semisimple and unipotent. In other words, as elements of $G(k) = \mathrm{GL}_m(k)$ the elements g'_{ss} and g'_u are respectively semisimple and unipotent. But they also commute, so they *are* the Jordan components of g . This proves that the Jordan components of g in $G(k) = \mathrm{GL}_m(k)$ are carried to those of $g' = j(g)$ in $G'(k) = \mathrm{GL}_N(k)$, so we are done.

B.1 Variants in linear algebra over arbitrary fields

Jordan canonical form, upon which the preceding discussion rests, takes place over algebraically closed fields. As a supplement, the following optional exercises develop a version of “Jordan decomposition” in additive and multiplicative forms for finite-dimensional vector spaces over any field, including what can go wrong over an imperfect field. (Briefly, the formation of the decomposition commutes with arbitrary field extension when the initial ground field is perfect, but not otherwise. This leads to some difficulties when working with linear algebraic groups over imperfect fields.) The additive case underlies Jordan decomposition in Lie algebras, and the multiplicative case underlies Jordan decomposition in linear algebraic groups.

Let V be a finite-dimensional nonzero vector space over a field F , with dimension $n > 0$. A linear self-map $T : V \rightarrow V$ is *semisimple* if every T -stable subspace of V admits a T -stable complementary subspace. (That is, if $T(W) \subseteq W$ then there exists a decomposition $V = W \oplus W'$ with $T(W') \subseteq W'$.) Keep in mind that such a complement is not unique in general (e.g., consider T to be a scalar multiplication with $\dim V > 1$). Let χ_T denote the characteristic polynomial of T , and m_T the minimal polynomial of T ,

1. (i) For each monic irreducible $\pi \in F[t]$, define $V(\pi)$ to be the subspace of $v \in V$ killed by a power of $\pi(T)$. Prove that $V(\pi) \neq 0$ if and only if $\pi | m_T$, and that $V = \bigoplus_{\pi | m_T} V(\pi)$. (In case F is algebraically closed, these are the *generalized eigenspaces* of T on V .)

(ii) Use rational canonical form to prove that T is semisimple if and only if m_T has no repeated irreducible factor over F . (Hint: apply (i) to T -stable subspaces of V to reduce to the case when m_T has one monic irreducible factor.) Deduce that a Jordan block of rank > 1 is never semisimple, that m_T is the “squarefree part” of χ_T when T is semisimple, and that if $W \subseteq V$ is a T -stable nonzero proper subspace then the induced endomorphisms $T_W : W \rightarrow W$ and $\bar{T} : V/W \rightarrow V/W$ are semisimple when T is semisimple.

(iii) Let $T' : V' \rightarrow V'$ be another linear self-map with V' nonzero and finite-dimensional over F . Prove that T and T' are semisimple if and only if the self-map $T \oplus T'$ of $V \oplus V'$ is semisimple.

(iii) Choose $T \in \text{Mat}_n(F)$, and let F'/F be an extension splitting m_T . Prove that T is semisimple as an F' -linear endomorphism of F'^n if and only if T is diagonalizable over F' , and also if and only if $m_T \in F[t]$ is separable; we then say T is *absolutely semisimple* over F . Deduce that semisimplicity is equivalent to absolutely semisimplicity over F if F is perfect, and give a counterexample over *every* imperfect field.

2. (i) Using rational canonical form and Cayley-Hamilton, prove the following are equivalent: $T^N = 0$ for some $N \geq 1$, $T^n = 0$, with respect to some ordered basis of V the matrix for T is upper triangular with 0's on the diagonal, $\chi_T = t^n$. We call such T *nilpotent*.

(ii) We say that T is *unipotent* if $T - 1$ is nilpotent. Formulate characterizations of unipotence analogous to the conditions in (i), and prove that a unipotent T is invertible.

(iii) Assume F is algebraically closed. Using Jordan canonical form and generalized eigenspaces, prove that there is a unique expression $T = T_{ss} + T_n$ where T_{ss} and T_n are a pair of *commuting* endomorphisms of V with T_{ss} semisimple and T_n nilpotent. (This is the *additive Jordan decomposition* of T .) Show by example with $\dim V = 2$ that uniqueness fails if we drop the “commuting” requirement, and show in general that $\chi_T = \chi_{T_{ss}}$ (so T is invertible if and only if T_{ss} is invertible).

(iv) Assume F is algebraically closed and T is invertible. Using the existence and uniqueness of additive Jordan decomposition, prove that there is a unique expression $T = T'_{ss} T'_u$ where T'_{ss} and T'_u are a pair of *commuting* endomorphisms of V with T'_{ss} semisimple and T'_u unipotent (so T'_{ss} is necessarily invertible too). This is the *multiplicative Jordan decomposition* of T .

(v) Use Galois theory with entries of matrices to prove (iii) and (iv) for any perfect F (using the result over an algebraic closure, or rather over a suitable finite Galois extension), and give counterexamples for any imperfect F .

C Affine quotients

C.1 Introduction

Let G be a smooth group of finite type over a field k , and H a normal k -subgroup scheme. We have seen that G/H exists as a smooth quasi-projective k -scheme, and that the normality of H provides a unique k -group structure on G/H compatible with the k -group structure on G . If the normality hypothesis is dropped, the coset space G/H is generally not affine even when G is affine. Indeed, G/H is the orbit under a suitable action of G on a projective space, and such orbits can sometimes even be the entire projective space (e.g., $G = \text{GL}(V)$ with its natural action on $\mathbf{P}(V)$).

In this appendix, we prove the important fact that when H is a normal k -subgroup scheme in a smooth affine G then G/H is actually affine. (Just as the existence of G/H is valid without smoothness hypotheses on G , the same holds for our affineness claim when H is normal in G . As with the existence of quotients in such extra generality, we refer the interested reader to SGA3 for such generalizations.)

To prove that G/H is affine, it is harmless to first make an extension of the ground field (since we know that the formation of G/H commutes with such extensions), so we may and do assume that k is algebraically closed. Also, the k -homomorphism $G^0 \rightarrow G/H$ between smooth k -groups has image with finite index, so it has image $(G/H)^0$. Thus, $(G/H)^0 = G^0/(G^0 \cap H)$. Since G/H is a disjoint union of finitely many copies of $(G/H)^0$, to prove that G/H is affine we may replace G with G^0 so that G is connected.

C.2 Line stabilizers

By Theorem 14.1.1 there exists a finite-dimensional representation V for G such that H is the scheme-theoretic stabilizer of a line L in V (i.e., $H = N_G(L)$). In particular, the H -action on L corresponds to a k -homomorphism $\chi : H \rightarrow \mathrm{GL}(L) = \mathbf{G}_m$. Consider the span W of the lines $g.L$ in V for $g \in G(k)$. Clearly W is G -stable in V , and since $gHg^{-1} \subseteq H$ inside of G for each $g \in G(k)$ we see that $g.L$ is also H -stable with action by the twisted character $\chi^g : H \rightarrow \mathbf{G}_m$ defined by $h \mapsto \chi(g^{-1}hg)$. Replacing V with W without loss of generality, we can assume that V is spanned by H -stable lines $L = L_1, \dots, L_n$. Thus, $V = \oplus V_i$ for H -stable subspaces V_i on which H acts through pairwise distinct characters $\chi_i : H \rightarrow \mathbf{G}_m$, with $\chi_1 = \chi$ and with each χ_i having the form $\chi_i = \chi^g$ for some $g \in G(k)$.

Lemma C.2.1. *Necessarily $V = V_1$, which is to say that H acts on V through χ .*

Proof. Since H is normal in G , the condition on $g \in G(R)$ that $\chi_R^g = \chi_R$ as R -homomorphisms $H_R \rightarrow (\mathbf{G}_m)_R$ makes sense for any k -algebra R and clearly cuts out a closed k -subgroup G' scheme in G . To prove that this coincides with G , it suffices to prove $G'(k)$ has finite index in $G(k)$, as then the closed k -subscheme G'_{red} has finitely many $G(k)$ -translates which cover G , so G' has underlying space that is also open in G , forcing $G' = G$ since G is smooth and *connected*.

The finite index property for $G'(k)$ in $G(k)$ will hold provided that $\chi^g \in \{\chi_i\}$ for each $g \in G(k)$. The normality of H in G implies that the H -action on $V = \oplus V_i$ is given by the pairwise distinct characters $\{\chi_i^g\}$. Hence, it suffices to prove that if $\psi : H \rightarrow \mathbf{G}_m$ is any k -homomorphism such that V contains a ψ -eigenline for H then $\psi \in \{\chi_i\}$. Such a line has a nonzero image under projection into some V_i , so the result is clear (as $V_i \neq 0$). \square

Recall that $H = N_G(L)$. For any k -algebra R , if $g \in G(R)$ acts on V_R through scaling by an element of R^\times then clearly $g \in N_{G(R)}(L_R) = H(R)$. Conversely, by the Lemma, if $g \in H(R)$ then g acts on V_R through R^\times -scaling. Hence, H is the scheme-theoretic kernel of the k -homomorphism $f : G \rightarrow \mathrm{PGL}(V)$. Letting $\overline{G} \subseteq \mathrm{PGL}(V)$ be the smooth closed image of f , the natural map $G \rightarrow \overline{G}$ is a surjective homomorphism between smooth k -groups of finite type and the kernel is H , so $G/H = \overline{G}$.

We conclude that G/H is closed in $\mathrm{PGL}(V)$. But $\mathrm{PGL}(V)$ is *affine*, so G/H is also affine.

D Quotient formalism

Let G be a group scheme of finite type over a field k , and H a closed k -subgroup scheme (possibly not normal). We have defined a good notion of quotient $\pi : G \rightarrow G/H$ in general, and proved existence when G is smooth and affine, with G/H smooth and quasi-projective in such cases. Moreover, if H is normal we have seen that G/H is naturally a k -group if it exists, and that G/H is also affine when G is smooth and affine.

But one can ask for more: can we carry over basic manipulations with quotients as in elementary group theory? The first part of this appendix addresses such questions in many cases (and the reader who is familiar with Grothendieck topologies can adapt the arguments to a more general setting, as is also treated in SGA3). In the second part of this appendix, we discuss the classification of all smooth affine k -groups G fitting into a short exact sequence

$$1 \rightarrow G' \rightarrow G \rightarrow G'' \rightarrow 1$$

with $G', G'' \in \{\mathbf{G}_a, \mathbf{G}_m\}$.

In the third part of this appendix, we apply these results to describe the structure of a k -split solvable group over *any* field k as a semidirect product of toric and unipotent parts. This description is not canonical (generally there are many choices for the torus subgroup), but it is a decisive tool in the proof of general results for solvable groups.

D.1 Coset spaces and isomorphism theorems

We begin by relating closed subschemes of G/H to certain closed subschemes of G . For this we do not need any smoothness or affineness assumption; we merely need to assume that the quotient $\pi : G \rightarrow G/H$ exists (under the definition given in class, so it is required to be separated and of finite type over k). Recall that existence has been proved when G is smooth and affine (and it is proved in general over fields in SGA3, as was noted in class).

Proposition D.1.1. *If Z is a closed subscheme of G/H then $\pi^{-1}(Z)$ is a closed subscheme of G which is stable under the right-translation action of H on G , and $Z \mapsto \pi^{-1}(Z)$ is a bijective correspondence between the set of closed subschemes of G/H and the set of closed subschemes of G stable under the right translation action of H .*

We have $Z_1 \subseteq Z_2$ if and only if $\pi^{-1}(Z_1) \subseteq \pi^{-1}(Z_2)$.

Proof. By computing with the functor of points, it is clear that $\pi^{-1}(Z)$ has the asserted properties. To prove that $Z = Z'$ when $\pi^{-1}(Z) = \pi^{-1}(Z')$, recall that π is faithfully flat map between noetherian schemes, so it suffices to prove in general that if $f : X \rightarrow Y$ is a faithfully flat quasi-compact map between scheme then a closed subscheme Z in Y is uniquely determined by $f^{-1}(Z)$. We can assume Y is affine, and then by replacing X with the disjoint union of the constituents of a finite open affine covering we can assume X is also affine. But if $A \rightarrow B$ is a faithfully flat map of rings and J is an ideal of A then $A \cap JB = J$, so we get the assertion.

Now let W be a closed subscheme of G which is invariant under the right action of H . We seek to prove that $W = \pi^{-1}(Z)$ for some (necessarily unique) closed subscheme $Z \subset G/H$. Under the action isomorphism

$$G \times H \simeq G \times_{G/H} G$$

defined by $(g, h) \mapsto (g, gh)$, $W \times H$ goes over to $W \times_{G/H} W$ due to the right-invariance hypothesis on W . But $W \times_{G/H} G$ goes over to a closed subscheme of $G \times H$ which must be contained in $W \times H$ (by computing with first projections), so the containment $W \times_{G/H} W \subseteq W \times_{G/H} G$ of closed subschemes of $G \times_{G/H} G$ is an equality. Applying the “flip” automorphism, it follows that likewise $W \times_{G/H} W = G \times_{G/H} W$. Hence, $W \times_{G/H} G = G \times_{G/H} W$. In other words, if $q_1, q_2 : G \times_{G/H} G \rightrightarrows G$ are the two projections then $q_1^{-1}(W) = q_2^{-1}(W)$. Since $\pi : G \rightarrow G/H$ is faithfully flat and quasi-compact, by descent theory for closed subschemes (which is descent theory for quasi-coherent sheaves, applied to ideal sheaves inside of the structure sheaf) it follows that $W = \pi^{-1}(Z)$ for a closed subscheme Z in G/H .

To prove that the bijective correspondence respects inclusions in both directions it suffices to prove that if $\pi^{-1}(Z_1) \subseteq \pi^{-1}(Z_2)$ then $Z_1 \subseteq Z_2$. Letting $Z = Z_1 \cap Z_2$, we have $\pi^{-1}(Z) = \pi^{-1}(Z_1) \cap \pi^{-1}(Z_2) = \pi^{-1}(Z_1)$, so $Z = Z_1$. Hence, $Z_1 \subseteq Z_2$, as required. \square

Continuing to assume that G/H exists (a hypothesis we have proved when G is smooth and affine), we get the following existence result for additional quotients by H :

Corollary D.1.2. *For any closed subscheme $Z \subseteq G$ stable under the right H -action, the quotient $Z \rightarrow Z/H$ exists and is the projection from Z onto the unique closed k -subscheme $\bar{Z} \subseteq G/H$ such that $\pi^{-1}(\bar{Z}) = Z$.*

Of course, the definition of a quotient map $Z \rightarrow Z/H$ is identical to the definition of the quotient map $G \rightarrow G/H$ as in class (which never used the k -group structure on G apart from the right H -action on G arising from it). In particular, by the argument used in class, if such a quotient exists it automatically satisfies the expected universal property for H -invariant maps from Z .

Proof. Since $Z = \pi^{-1}(\bar{Z})$, the map $\pi : Z \rightarrow \bar{Z}$ is faithfully flat and quasi-compact (even finite type). This map is also clearly invariant under the right H -action on Z . By thinking in terms of functors, we see that $Z \times_{G/H} Z = Z \times_{\bar{Z}} Z$. But the preceding proof shows that $Z \times_{G/H} Z = Z \times H$ via the right action map, so $Z \times H \simeq Z \times_{\bar{Z}} Z$ via the action map. Thus, $Z \rightarrow \bar{Z}$ satisfies the requirements to be a quotient by the H -action. \square

As a nice application, we can now construct some more quotients in the affine case without smoothness hypotheses:

Example D.1.3. Let H' be an affine k -group of finite type that is a closed k -subgroup of GL_n for some $n \geq 1$. Then for any closed k -subgroup $H \subseteq H'$, the quotient H'/H exists and is quasi-projective over k . Indeed, we apply the preceding corollary to $Z = H'$ and the smooth affine $G = GL_n$ upon picking a faithful linear representation. (In SGA3 it is proved that every affine group of finite type over a field admits a closed k -subgroup inclusion into some GL_n . For our purposes, what matters is that if we begin life with a smooth affine k -group and then pass to collections of closed k -subgroups, the coset schemes always exist and are quasi-projective over k .)

Here is a group scheme version of some basic isomorphism nonsense from group theory.

Proposition D.1.4. *Assume G is smooth and affine, and H is normal in G . Equip $\overline{G} := G/H$ with its natural k -group structure. Then $\overline{H}' \mapsto H' := \pi^{-1}(\overline{H}')$ is a bijective correspondence between closed k -subgroup schemes of G/H and closed k -subgroup schemes of G containing H . Moreover, $H' \triangleleft G$ if and only if $\overline{H}' \triangleleft \overline{G}$, and if $H' \subseteq H''$ is a containment between such k -subgroups of G then the natural map $H'' \rightarrow \overline{H}''/\overline{H}'$ is right H' -invariant and the induced map $H''/H' \rightarrow \overline{H}''/\overline{H}'$ is an isomorphism.*

Note that under the hypothesis on G , Example D.1.3 applies to prove that H''/H' exists for any such pair (H'', H') inside of G . The same goes for $\overline{H}''/\overline{H}'$, since \overline{G} is smooth and affine. This is the only reason for assuming G is smooth and affine (rather than merely a k -group of finite type). If we grant the existence results for quotients in the generality of SGA3 then the proof below works verbatim without these restrictions on G .

If one approaches these matters from the viewpoint of Grothendieck topologies, the following proof can be done much more easily: it is identical to the version of sheaves of groups on a topological space (if done without the crutch of stalks), which in turn is modeled on the version in ordinary group theory.

Proof. Since π is a k -homomorphism, the formation of (scheme-theoretic!) preimages under π carries closed subgroups to closed subgroups and preserves normality. To prove the converse direction, consider a closed subscheme $\overline{Z} \subseteq \overline{G}$ such that $Z := \pi^{-1}(\overline{Z})$ is a k -subgroup of G . We wish to prove that \overline{Z} is a k -subgroup of \overline{G} , and that it is also normal if Z is normal in G . We have to check three properties: containment of the identity, stability under inversion, and stability under the ambient group law morphism.

We have $1 \in \overline{Z}(k)$ since $\pi(1) = 1$ and $1 \in Z(k)$. Also, the inversion involution of the k -scheme \overline{G} is compatible via π with the inversion involution of the k -scheme G , so the fact that Z is carried isomorphically to itself under inversion on G forces the analogue for \overline{Z} due to the condition $\pi^{-1}(\overline{Z}) = Z$ uniquely determining \overline{Z} as a closed k -subscheme of G . Finally, to prove that $m : G \times G \rightarrow G$ carries $Z \times Z$ into Z , we reformulate it as the condition $Z \times Z \subseteq m^{-1}(Z)$. Since π is a homomorphism, it is easy to check that

$$m^{-1}(Z) = (\pi \times \pi)^{-1}(m^{-1}(\overline{Z})) \supseteq (\pi \times \pi)^{-1}(\overline{Z} \times \overline{Z}) = Z \times Z.$$

This completes the proof of the bijective correspondence between closed k -subgroups.

To check the normality claim, we first observe that for any k -algebra R ,

$$H'(R) = \{g \in G(R) \mid \pi(g) \in \overline{H}'(R)\}.$$

This is clearly normal in $G(R)$ when $\overline{H}'(R)$ is normal in $\overline{G}(R)$. Conversely, suppose H' is normal in G . We seek to prove that \overline{H}' is normal in \overline{G} . In other words, we want the conjugation map $\overline{c} : \overline{G} \times \overline{H}' \rightarrow \overline{G}$ defined by $(\overline{g}, \overline{h}') \mapsto (\overline{g}\overline{h}'\overline{g}^{-1})$ to factor through \overline{H}' . But as we saw in our construction of the k -group structure on $\overline{G} = G/H$ in the normal case, the natural map

$$G \times H' \rightarrow \overline{G} \times \overline{H}'$$

is a quotient by the right translation action of $H \times H$. Hence, in view of the general universal mapping property of quotients, it suffices to prove that the map

$$G \times H' \rightarrow \overline{G}$$

defined by $(g, h') \mapsto \pi(gh'g^{-1})$ factors through \overline{H}' . But this map factors as

$$G \times H' \rightarrow H' \hookrightarrow G \rightarrow \overline{G}$$

where the first map is $(g, h') \mapsto gh'g^{-1}$ due to the normality of H in G . Since the second and third steps in this diagram have composite equal to the quotient map $H' \rightarrow \bar{H}'$ followed by the inclusion of \bar{H}' into \bar{G} , we are done.

Finally, we prove that if $H' \subseteq H''$ is a containment between closed k -subgroups of G containing H , then $H'' \rightarrow \bar{H}''/\bar{H}'$ is right H' -invariant with the induced map $\theta : H''/H' \rightarrow \bar{H}''/\bar{H}'$ an isomorphism. Since $H'' \rightarrow \bar{H}''$ is a k -homomorphism which carries H' into \bar{H}' , the desired right H' -invariance is immediate since the quotient map $\bar{H}'' \rightarrow \bar{H}''/\bar{H}'$ is right \bar{H}' -invariant. To prove that the induced map θ is an isomorphism, it is equivalent to prove that the natural map $q : H'' \rightarrow \bar{H}''/\bar{H}'$ satisfies the requirements to be a quotient by H' .

We have just seen that q is right H' -invariant, and it is faithfully flat and quasi-compact since it is the composite of the maps $H'' \rightarrow H''/H' = \bar{H}''$ and $\bar{H}'' \rightarrow \bar{H}''/\bar{H}'$ which both have these properties. Thus, it remains to check that the natural map

$$H'' \times H' \rightarrow H'' \times_{\bar{H}''/\bar{H}'} H'' \quad (1)$$

defined by $(h'', h') \mapsto (h'', h''h')$ is an isomorphism. Consider the isomorphism

$$H'' \times_{\bar{H}''/\bar{H}'} H'' = H'' \times_{\bar{H}''} (\bar{H}'' \times_{\bar{H}''/\bar{H}'} \bar{H}'') \times_{\bar{H}''} H'' = H'' \times_{\bar{H}''} (\bar{H}'' \times \bar{H}') \times_{\bar{H}''} H'',$$

where the final term has the second projection map $\bar{H}'' \times \bar{H}' \rightarrow \bar{H}''$ equal to the multiplication map in the group law of \bar{G} . It follows that for any k -algebra R and $h_1'', h_2'' \in H''(R)$, their images in $(\bar{H}''/\bar{H}')(R)$ coincide if and only if the image points $\bar{h}_1'', \bar{h}_2'' \in \bar{H}''(R)$ are related by the right $\bar{H}'(R)$ -action. But that says precisely that the point $(h_1'')^{-1}h_2'' \in H''(R)$ lies in $\pi^{-1}(\bar{H}'(R)) = H'(R)$ (since $H' = \pi^{-1}(\bar{H}')$), so (1) is bijective on R -points for every R . Hence, (1) is an isomorphism. \square

Remark D.1.5. In Proposition D.1.4, it is natural to wonder about the relationship between smoothness properties for H' and \bar{H}' . Since $H' \rightarrow \bar{H}'$ is faithfully flat, if H' is smooth then so is \bar{H}' (as its coordinate ring on small affine opens is geometrically reduced, due to the same for H'). The converse direction is more subtle, and the best that can be said in general is that if H is also smooth then smoothness of \bar{H}' implies the same for H' . In other words, under the quotient map $\pi : G \rightarrow G/H$ with smooth G and H , we claim that the scheme-theoretic preimage H' in G of a smooth k -subgroup $\bar{H}' \subseteq G/H$ is again smooth. To prove this in an elementary manner (without needing the general theory of smooth morphisms), we may extend scalars to \bar{k} so that k is algebraically closed. For a smooth subgroup $\bar{H}' \subseteq G/H$, consider the smooth subgroup $\pi^{-1}(\bar{H}')_{\text{red}}$ in G whose image in G/H is clearly \bar{H}' . This subgroup of G contains $H_{\text{red}} = H$ since H is smooth, so it is H -stable. Hence, under the bijective correspondence it must go over to its image $\bar{H}'_{\text{red}} = \bar{H}'$ since $\pi^{-1}(\bar{H}')_{\text{red}}/H$ is certainly smooth. The bijectivity therefore forces $\pi^{-1}(\bar{H}') = \pi^{-1}(\bar{H}')_{\text{red}}$, so we get the claim.

The last general nonsense issue we wish to address is the “image” of the natural map $H \rightarrow G/H'$ for a smooth affine k -group G , a closed k -subgroup H' , and an auxiliary closed k -subgroup H (not assumed to have any containment relation with H' in either direction). Clearly $H \cap H'$ is a closed k -subgroup of H , normal when H' is normal in G , and the quotient $H/(H \cap H')$ exists since G is smooth and affine (so Example D.1.3 can be applied). We then get an induced map

$$j : H/(H \cap H') \rightarrow G/H',$$

and it is natural to wonder: *is this map a locally closed immersion?* In some nice cases things work out well:

Proposition D.1.6. *Assume H is smooth. If H' is normal in G then j is a closed immersion. If instead H' is smooth then j is a locally closed immersion.*

Proof. First assume H' is normal, so j is a homomorphism between smooth k -groups of finite type. Thus, to prove it is a closed immersion we just have to prove triviality of the kernel. By the construction of quotients, it suffices to show that $H \rightarrow G/H'$ has kernel $H \cap H'$. Since $G \rightarrow G/H'$ has kernel H' , we are done.

Now suppose H' is smooth. The same Galois descent technique (using that \bar{k}/k_s is purely inseparable) as in our proof of the closed orbit lemma can be used to prove that the constructible image X of $H \times H' \rightarrow G/H'$ is locally closed and is smooth with its reduced structure. (We get around the fact that $H \times H'$ has no relevant group structure here by using left translation by H and right translation by H' .)

We thereby obtain a surjective map $H \rightarrow X$ between smooth equidimensional k -schemes of finite type, and by computation on \bar{k} -points the geometric fibers are all equidimensional of the same dimension (translates of $H \cap H'$ after a ground field extension). Thus, by the Miracle Flatness Theorem, $H \rightarrow X$ is faithfully flat. This map is visibly $H \cap H'$ -invariant on the right, so it remains to check that the natural map

$$H \times (H \cap H') \rightarrow H \times_X H$$

is an isomorphism. Thinking in terms of functors, $H \times_X H = H \times_{G/H'} H$. Thus, the desired result is clear since $G \times_{G/H'} G = G \times H'$ via the natural map. \square

Example D.1.7. Since H is closed in G , it may seem surprising that j may fail to be a closed immersion (and just be locally closed). But the relevant topology inside of G is not H but rather the image of $H \times H'$ under multiplication. This could be non-closed. Such a possibility happens very often in the theory of reductive groups, especially with the so-called Bruhat decomposition.

We illustrate this in the most basic (yet very important) case: $G = \mathrm{SL}_2$, $H' = B$ the upper triangular k -subgroup, and $H = U^-$ the lower triangular unipotent k -subgroup. In this case G/H' is identified with \mathbf{P}_k^1 and $H \cap H' = 1$, with j becoming the standard open immersion $\mathbf{A}_k^1 \rightarrow \mathbf{P}_k^1$ complementary to 0 . This example “works” the same way with real and complex Lie groups, so it has nothing to do with the peculiarities of algebraic geometry.

D.2 Classifying some extension structures

In this section we wish to describe all smooth connected affine k -groups G for which there is a short exact sequence of smooth affine k -groups

$$1 \rightarrow G' \rightarrow G \rightarrow G'' \rightarrow 1$$

with $G', G'' \in \{\mathbf{G}_a, \mathbf{G}_m\}$. We say that G is an extension of G'' by G' .

The case $G' = G'' = \mathbf{G}_a$ is the most subtle of all (especially in nonzero characteristic), and is addressed in HW9 Exercise 2. Also, if $G' = G'' = \mathbf{G}_m$ then G must be a k -split torus of dimension 2, so there is nothing to do (as the character group explains everything in such cases). Thus, the focus of our attention is on the other two cases.

Proposition D.2.1. *For any short exact sequence $1 \rightarrow \mathbf{G}_m \rightarrow G \rightarrow \mathbf{G}_a \rightarrow 1$, necessarily G is commutative and the exact sequence is uniquely split over k .*

Proof. By HW6, Exercise 3, $G' = \mathbf{G}_m$ is central in G . By HW9 Exercise 4, the commutator map $G \times G \rightarrow G$ factors through a k -scheme map $G'' \times G'' \rightarrow G'$. A calculation with (geometric) points shows that this map $\mathbf{G}_a \times \mathbf{G}_a \rightarrow \mathbf{G}_m$ is bi-additive. But the only such map is the trivial one, since there are no nontrivial homomorphisms from \mathbf{G}_a to \mathbf{G}_m over \bar{k} . Thus, the commutator map is trivial, so G is commutative.

It follows that if the given exact sequence splits then the splitting is unique, as the set of splittings is a torsor under $\mathrm{Hom}_k(\mathbf{G}_a, \mathbf{G}_m) = 1$. In view of the uniqueness, to construct the splitting over k it suffices (by Galois descent) to work over k_s . Hence, we can assume $k = k_s$. Since G is solvable and not a torus, in the decomposition $G_{\bar{k}} = T \times U$ for a torus T and $U := \mathcal{R}_u(G_{\bar{k}})$ we must have $U \neq 1$ and T is the copy of \mathbf{G}_m from the given short exact sequence. Hence, the given exact sequence splits over \bar{k} , so it splits over some finite extension k'/k with $k = k_s$. This settles the case when k is perfect.

To handle possibly imperfect k , I do not know a way to copy the Galois descent argument by using faithfully flat descent because general nonsense does not ensure the uniqueness of a splitting over $k'' = k' \otimes_k k'$: there do exist nontrivial k'' -homomorphisms $\mathbf{G}_a \rightarrow \mathbf{G}_m$! (For example, $x \mapsto 1 + \epsilon x$ for nonzero $\epsilon \in k''$ with $\epsilon^2 = 0$.) Instead, the only method I know is to use faithfully flat descent theory in a different way, as follows. The exact sequence identifies G with a \mathbf{G}_m -torsor over \mathbf{G}_a for the fppf or étale topologies. The isomorphism class of this torsor is classified by an element in the Picard group of \mathbf{G}_a relative to the fppf or étale topologies. By descent theory for quasi-coherent sheaves, this is the same as the Picard group

relative to the Zariski topology, which is trivial since $k[x]$ is a PID. Hence, it follows that the quotient map $G \rightarrow \mathbf{G}_a$ admits a section σ over k as a map of k -schemes. Composing with a suitable $G(k)$ -translation then brings us to the case $\sigma(0) = 1$.

To summarize, we have an isomorphism of pointed k -schemes $G = \mathbf{G}_m \times \mathbf{G}_a$ with group law

$$(t, x)(t', x') = (tt'h(x, x'), x + x')$$

where $h(0, 0) = 1$. The only units on $\mathbf{G}_a \times \mathbf{G}_a$ are the elements of k^\times , so $h = 1$. This is the standard group law, as desired. \square

Now consider an extension G of $G'' = \mathbf{G}_m$ by $G' = \mathbf{G}_a$. By the method of solution of HW9 Exercise 4, since G' is commutative the conjugation action of G on itself uniquely factors through an action of $G/G' = G'' = \mathbf{G}_m$ on $G' = \mathbf{G}_a$. I claim this action must be $t.x = t^n x$ for a unique $n \in \mathbf{Z}$. To prove this, let $S = \mathbf{G}_m$ and $H = S \times \mathbf{G}_a$ viewed as an S -group. The map $H \rightarrow H$ defined by $(t, x) \mapsto (t, t.x)$ is an S -group automorphism of the additive affine line H over S . Since S is *reduced*, the only such automorphisms are given by scalar of the line parameter by a unit on the base, as may be checked by working at the generic points of S and then Zariski-locally on S . Hence, $t.x = c(t)x$ for a k -scheme map $c : S \rightarrow \mathbf{G}_m$. Clearly $c(1) = 1$, and the only units on S are k^\times -multiples of powers of t . Hence, $c(t) = t^n$ for some $n \in \mathbf{Z}$, as desired. Observe that $n = 0$ if and only if \mathbf{G}_a is central in G . It turns out that this is equivalent to the commutativity of G . More generally:

Proposition D.2.2. *There is a k -group isomorphism between G and the semidirect product $\mathbf{G}_a \rtimes \mathbf{G}_m$ defined by the action $t.x = t^n x$.*

Proof. We cannot trivially use Galois descent, for the reason that the semidirect product structure is not unique when $n \neq 0$. That is, even if there is a k -group section to the quotient map $G \rightarrow \mathbf{G}_m$, we can compose it with $G(k)$ -conjugations to get more such sections when G is not commutative. Thus, we need a different method (and in the end will use Galois descent, but in a manner which is less elementary than above).

It suffices to find a nontrivial k -torus T in G . Indeed, $T \cap \mathbf{G}_a = 1$ (by applying HW5 Exercise 1 after picking a faithful linear representation of G and using k -rational conjugation so that \mathbf{G}_a lands in the standard upper triangular unipotent k -subgroup), so the induced nontrivial map $T \rightarrow G/\mathbf{G}_a = \mathbf{G}_m$ is an isomorphism. That would yield the desired semidirect product structure.

To construct a nontrivial k -torus in G , we first treat the case when k is not algebraic over a finite field, and then we use that case to handle the case when k is algebraic over a finite field. Now assume k is not algebraic over a finite field, so k^\times contains an element c with infinite order. The fiber of $q : G \rightarrow \mathbf{G}_m$ over c is geometrically a translate of \mathbf{G}_a , so it is smooth and non-empty and hence has k_s -points. Thus, $q^{-1}(c)(k_s)$ is a torsor under translation by $\mathbf{G}_a(k_s) = k_s$, with torsor structure that is $\text{Gal}(k_s/k)$ -equivariant. Hence, the obstruction to $q^{-1}(c)$ having a k -point is a class in $H^1(\text{Gal}(k_s/k), k_s) = 0$. That is, there exists $g \in G(k)$ such that $q(g) = c$. If $\text{char}(k) = p > 0$ then the geometric Jordan decomposition of g may have a nontrivial unipotent part. Replacing g (and so c) with a suitable p -power in such cases then brings us to the case when g is geometrically semisimple. Likewise, if $\text{char}(k) = 0$ then the Jordan decomposition of g is defined over k (as k is perfect), and the unipotent part must have trivial image in \mathbf{G}_m . Hence, in such cases we can replace g with its semisimple part in $G(k)$. To summarize, under the assumption that k is not algebraic over a finite field, we have constructed $g \in G(k)$ that is geometrically semisimple and has image in $\mathbf{G}_m(k) = k^\times$ with infinite order.

By working with a faithful linear representation of $G_{\bar{k}}$, it follows that the closure of the cyclic subgroup generated by g in $G(k)$ has identity component that is a nontrivial k -torus. (Beware that g may not lie in the identity component of this k -group!) This settles the case when k is not algebraic over a finite field.

Suppose instead that k is algebraic over a finite field. Let $K = k(u)$ be a rational function field over K . We can apply the preceding arguments to G_K , so we get a K -subgroup $\mathbf{G}_m \hookrightarrow G_K$. This closed immersion over $K = k(u)$ “spreads out” to a closed subgroup scheme inclusion over $k[u][1/h]$ for some sufficiently divisible nonzero $h \in k[u]$. If k is infinite then we can specialize at a point $u_0 \in k$ for which $h(u_0) \neq 0$. If k is finite then such a u_0 can be found in a finite extension k'/k .

It remains to treat the case when k is finite, and we have a section $\sigma : \mathbf{G}_m \rightarrow G_{k'}$ for some finite Galois extension k'/k . We will use nothing special about finite fields. It is an elementary calculation that for

any field F , the F -group sections to $\mathbf{G}_a \rtimes \mathbf{G}_m \rightarrow \mathbf{G}_m$ (using the n th-power action to define the semidirect product) are precisely the maps $t \mapsto (h(t), t)$ where $h(tt') = h(t) + t^n h(t')$ (which forces $h(1) = 0$). The regular function h on \mathbf{G}_m is a Laurent polynomial over F (i.e., $h \in F[t, 1/t]$), and it is elementary to verify that the only Laurent polynomials over F which satisfy the required functional equation are $h(t) = ct^n - c$ for a *unique* $c \in F$. But this in turn is exactly the effect of applying conjugation by $(c, 1)$ to the canonical section! In other words, in our situation with G (whose k -structure is *not yet known*), any two sections to $G_{k'} \twoheadrightarrow \mathbf{G}_m$ are related via conjugation by a *unique* element of $\mathbf{G}_a(k') \subseteq G(k')$. Hence, the obstruction to the existence of a $\mathbf{G}_a(k')$ -conjugate of σ that admits a k -descent (i.e., the measure of failure of σ to have a $\mathbf{G}_a(k')$ -conjugate that is $\text{Gal}(k'/k)$ -equivariant) is an element in $H^1(\text{Gal}(k'/k), k') = 0$. It follows that after applying a suitable $\mathbf{G}_a(k')$ -conjugation to σ it is defined over k , and so we get the desired nontrivial k -torus in G . \square

D.3 Structure of split solvable groups

Let G be a k -split solvable group, with k any field. (Recall this requires G to be a smooth connected affine k -group, among other things.) We wish to describe the structure of G in the form of a semidirect product $U \rtimes T$ for a smooth connected unipotent k -group U and a k -torus T , with U and T each k -split. Note that if there is such a decomposition then $U = \mathcal{R}_{u,k}(G)$ and the description persists over any extension field, so $U_K = \mathcal{R}_{u,K}(G_K)$ for any extension field K/k . In particular, $U_{\bar{k}} = \mathcal{R}_{u,\bar{k}}(G_{\bar{k}})$. We then call U the *unipotent radical* of G .

Remark D.3.1. Beware that if k is not perfect, there always exist examples of smooth connected commutative affine k -groups G such that $\mathcal{R}_{u,\bar{k}}(G_{\bar{k}})$ is nontrivial and does *not* descend to a k -subgroup of G . Thus, the possibility of a semidirect product description $G = U \rtimes T$ over a general field k relies in an essential way on the k -split hypothesis.

Before we take up the general case, let's consider the low-dimensional cases. If $\dim G \leq 1$, then by the very definition of “ k -split solvable” we are done (G is either \mathbf{G}_a or \mathbf{G}_m). If $\dim G = 2$ then by the definition of being k -split solvable, G is of the sort considered in §D.2. In particular, if it is an extension of \mathbf{G}_a by \mathbf{G}_a then G is unipotent so we can take $U = G$ and $T = 1$. Likewise, if G is an extension of \mathbf{G}_m by \mathbf{G}_m then G is a k -split k -torus (as we noted early in §D.2), so we can take $T = G$ and $U = 1$. The other two possibilities are addressed in Proposition D.2.2 and Proposition D.2.1. The case $\dim G \geq 3$ will be deduced from these low-dimensional cases by using induction on $\dim G$ with the help of a composition series as in the definition of G being k -split solvable.

Here is the main result.

Theorem D.3.2. *Let G be a k -split solvable group over a field k . Then $G = U \rtimes T$ for a k -split smooth connected unipotent k -group U and a k -split k -torus T equipped with an action on U .*

In the proof, we freely make use of §D.1, and especially Remark D.1.5 when arguing “as if” we were using ordinary groups (especially not needing to worry about smoothness issues when forming certain preimages through quotient maps by smooth normal k -subgroups).

Proof. As we have seen in the preceding discussion, the cases $\dim G \leq 2$ are settled. We will first treat the commutative case, and then the general case (by using dimension induction and the commutative case applied to $G/\mathcal{D}(G)$ when G is non-commutative). Assuming G to be commutative, a k -split composition series for G provides a k -split smooth connected k -subgroup $G' \subset G$ of codimension 1 such that G/G' is either \mathbf{G}_a or \mathbf{G}_m . Thus, dimension induction implies $G' = T' \times U'$ for a k -split k -torus T' and a k -split smooth connected commutative unipotent k -group U' . If $G/G' = \mathbf{G}_m$ then G/U' is an extension of \mathbf{G}_m by $G'/U' = T'$, so G/U' is a k -split k -torus. If $G/G' = \mathbf{G}_a$ then G/T' is an extension of \mathbf{G}_a by $G'/T' = U'$, so G/T' is k -split unipotent.

Thus, G is either an extension of T by U or of U by T , where T is a k -split k -torus and U is a unipotent smooth connected commutative k -group that is also k -split. That is, either there is a short exact sequence

$$1 \rightarrow T \rightarrow G \rightarrow U \rightarrow 1$$

or

$$1 \rightarrow U \rightarrow G \rightarrow T \rightarrow 1,$$

so it suffices (for the case of commutative G) to prove that any such exact sequence with commutative G is split over k .

The category of smooth connected commutative k -groups is not abelian (think of isogenies which are not isomorphisms), but it is an additive category and has a notion of short exact sequence which enjoys familiar properties as in the axioms for an “exact category”. This permits us to endow the set $\text{Ext}_k(H, H')$ of commutative k -group extensions of one object by another with a natural commutative group structure making it an additive bifunctor, and when given a short exact sequence in either H or H' (with the other variable fixed) we get a natural 6-term exact sequence in Hom_k ’s and Ext_k ’s. Our task in the commutative case is to prove that $\text{Ext}_k(T, U)$ and $\text{Ext}_k(U, T)$ both vanish. By using composition series for T and U with each successive quotient k -isomorphic to \mathbf{G}_m and \mathbf{G}_a respectively, the 6-term exact sequence formalism (just in the Ext_k aspect) reduces us to the case $T = \mathbf{G}_m$ and $U = \mathbf{G}_a$. Now Proposition D.2.1 and Proposition D.2.2 give the required vanishing (since the commutative case in Proposition D.2.2 forces $n = 0$).

Moving a bit beyond the commutative case, we next treat a case with a slightly weaker hypothesis which turns out to still imply commutativity.

Lemma D.3.3. *Any extension H of \mathbf{G}_a by a k -split torus T is k -isomorphic to $\mathbf{G}_a \times T$.*

Proof. The same argument as at the start of the proof of Proposition D.2.1 (replacing \mathbf{G}_m there with T) implies that G is commutative. Thus, by the settled commutative case we have $G = S \times U$ for a k -split torus S and a k -split unipotent smooth connected k -group U . Clearly $T \subseteq S$ since $G \twoheadrightarrow G/S = U$ must kill T , and likewise $S \subseteq T$ since $G \twoheadrightarrow G/T = \mathbf{G}_a$ must kill S . Hence, $S = T$, so $U \simeq \mathbf{G}_a$. \square

Turning to the general case, we may assume $\dim G \geq 3$. We may also assume that G is neither unipotent nor a torus. Choose a k -split composition series for G over k , so we get a codimension-1 k -split solvable k -subgroup $G' \subset G$ with G/G' isomorphic to either \mathbf{G}_a or \mathbf{G}_m . By induction, $G' = U' \rtimes T'$ for a smooth connected unipotent k -subgroup U' and a k -torus T' , and U' and T' are each k -split. Observe that since G' is normal in G and necessarily $U'_k = \mathcal{R}_{u,k}(G'_k)$, it is automatic that U' is also *normal in G* ! Thus, G/U' makes sense and is an extension of either \mathbf{G}_a or \mathbf{G}_m by T' . In the latter case, G/U' is a k -split torus, so $U' = \mathcal{R}_{u,k}(G)$ and this is k -split. In the former case, G/U' is an extension of \mathbf{G}_a by T' , and in the latter case $G/U' = \mathbf{G}_a \times T'$ as in Lemma D.3.3. Thus, in this latter case the preimage U of \mathbf{G}_a in G is a k -split unipotent smooth connected k -group which is normal in G and has quotient G/U that is a k -split torus. In other words, in the general case G is an extension of a k -split torus T by a k -split unipotent smooth connected k -group U . In particular, we have shown that $\mathcal{R}_{u,k}(G)$ is k -split and $\mathcal{R}_{u,k}(G)_{\bar{k}} = \mathcal{R}_{u,\bar{k}}(G_{\bar{k}})$.

It suffices to find a k -torus S in G that maps isomorphically onto $G/U = T$. Since G is not unipotent and not a torus, we have $T \neq 1$ and $U \neq 1$. We claim that U admits a composition series $\{U_i\}$ consisting of k -split unipotent smooth connected k -subgroups which are *normal in G* and for which U_i/U_{i-1} is a vector group. Once this is proved, by induction on $\dim U$ we can then pass to the case when U is a vector group. To construct this composition series $\{U_i\}$ we treat characteristic 0 first. In this case we can take it to be the derived series, since a commutative unipotent smooth connected group in characteristic 0 is always a vector group (HW9, Exercise 2(ii)). If instead $\text{char}(k) = p > 0$, we will use Tits’ structure theory for unipotent smooth connected k -groups, as developed in [CGP, App. B]. By [CGP, Prop. B.3.2], since U is k -split it contains a central \mathbf{G}_a . In general, a p -torsion commutative smooth connected k -group is a vector group if and only if it is k -split. (This follows from [CGP, Lemma B.1.10, Cor. B.1.12], together with a dimension induction.) The maximal such k -subgroup U_1 in U is nontrivial, and its formation commutes with scalar extension to k_s , due to Galois descent and the fact that the property of being a vector group is insensitive to scalar extension to k_s [CGP, Cor. B.2.6]. Hence, $(U_1)_{k_s}$ is stable under all automorphisms of U_{k_s} , such as $G(k_s)$ -conjugations, so U_1 is normal in G . Passing to G/U_1 and the k -split U/U_1 then allows us to construct $\{U_i\}$ by dimension induction.

Now we are in the case that U is a vector group. In particular, since U is commutative in G the natural G -action on U factors through an action of $G/U = T$ on U . We wish to describe this action in more concrete terms. If $\text{char}(k) = 0$, it follows from HW9 Exercise 2(ii) that the T -action on $U \simeq \mathbf{G}_a^N$ respects the linear structure. If $\text{char}(k) = p > 0$ then by [CGP, Thm. B.4.3] there is a decomposition $U = U' \times U''$ with U'' a vector group admitting a linear structure respected by the T -action and U' having trivial T -action. But U' is also a vector group since it is k -split (being a quotient of the k -split U), so we conclude as in characteristic 0 that there is an isomorphism $U \simeq \mathbf{G}_a^N$ making the T -action linear. Any linear representation of a split

torus is a direct sum of 1-dimensional representations, so to lift T through the quotient map $G \twoheadrightarrow G/U$ we can use a filtration by such lines to reduce to the case $U = \mathbf{G}_a$ (via induction on $\dim U$)!

Finally, we are in the case that G is an extension of a split torus T by \mathbf{G}_a , in which the T -action on \mathbf{G}_a is given by some $\chi \in X(T)$. Letting S be the k -subtorus $(\ker \chi)_{\text{red}}^0$, so S is k -split. The preimage H of S in G is a *central* extension of S by \mathbf{G}_a . The commutator pairing argument as in the beginning of the proof of Proposition D.2.1 can now be adapted to this setting to infer that H is *commutative*. Hence, $H \simeq S \times \mathbf{G}_a$. It follows that S as a k -torus in H is central in G . If $\chi = 1$ then $S = T$ and we are done. Otherwise we can pass to G/S to reduce to the case $T = \mathbf{G}_m$. Now G is in exactly the setup for Proposition D.2.2. \square

E Grothendieck's theorem on tori

E.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 in [SGA3, XIV, Thm. 1.1] Grothendieck 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 E.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 $T_{\bar{k}}$ is maximal in $G_{\bar{k}}$.*

Remark E.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 [SGA3, XIV, Rem. 1.5(d)], 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 [SGA3, XIV, Thm. 6.1], so he could invoke the elementary fact that rational varieties over infinite fields have rational points!) Borel felt that the proof via [SGA3] was too technical for such a concrete result over fields, so in [Bor, 18.2(i)] he eliminated 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 Borel's argument. It is very different from Grothendieck's proof.

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

Corollary E.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 $K = \bar{k}$, $\dim T$ 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 $G_{\bar{k}}/\mathcal{R}_u(G_{\bar{k}})$.

Remark E.1.4. By Corollary 22.1.4, if G is a smooth connected affine k -group such that $G_{\bar{k}}$ contains no nontrivial torus then $G_{\bar{k}}$ is unipotent (and so by definition G is unipotent). But Corollary E.1.3 gives that $G_{\bar{k}}$ 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 $G = \text{GL}_n$ then by HW5 Exercise 5(ii) the maximal k -tori in G are in bijective correspondence with maximal finite étale commutative k -subalgebras of $\text{Mat}_n(k)$. In particular, two maximal k -tori are $G(k)$ -conjugate if and only if the corresponding maximal finite étale commutative k -subalgebras of $\text{Mat}_n(k)$ are $\text{GL}_n(k)$ -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 $G_{\bar{k}}$ has no nontrivial tori if and only if $G_{\bar{k}}$ 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 $(G/T)_{\bar{k}} = G_{\bar{k}}/T_{\bar{k}}$ 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 E.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 $C_{\bar{k}} = Z_{G_{\bar{k}}}(T_{\bar{k}})$ since the formation of scheme-theoretic centralizers commutes with base change, and over \bar{k} all maximal tori are conjugate. Hence, over \bar{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 [Bor].

For example, if G is reductive then it turns out (as will be shown in a sequel course) that $C = T$. That is, in a connected reductive group the Cartan subgroups are precisely the maximal tori.

Remark E.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 [Bor, 20.9(ii)] 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 in [CGP, Thm. C.2.3]. 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 E.1.1, note that since tori split over a finite separable extension, we have the following important consequence of Theorem E.1.1.

Corollary E.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.*

E.2 Start of proof of Theorem E.1.1

We will primarily focus on the case in which k is *infinite*, which ensures that $k^n \subset \mathbf{A}_{\bar{k}}^n$ is Zariski-dense, and thus in particular $\mathfrak{g} = \text{Lie}(G)$ is Zariski-dense in $\mathfrak{g}_{\bar{k}}$. The case of finite k requires a completely different argument, using “Lang’s theorem”, and is explained in [Bor, Prop. 16.6] (and will be addressed in the sequel course). In general, [Bor, §16] 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 $G_{\bar{k}}$ has a *central* maximal torus S . (This case will work over all k , even finite fields.) Since all maximal tori are $G(\bar{k})$ conjugate, a unique one is automatically normal in $G_{\bar{k}}$. By HW 6, Exercise 3(ii), a normal torus in a smooth connected \bar{k} -group is automatically central. (This is basically because the automorphism scheme of a split torus of rank n is the constant group $\text{GL}_n(\mathbf{Z})$ that is étale, so the conjugation action of $G_{\bar{k}}$ 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 \bar{k} -torus $S \subset G_{\bar{k}}$. 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 $S \subset (Z_{\bar{k}})_{\text{red}}$ as a maximal torus in the smooth commutative \bar{k} -group $(Z_{\bar{k}})_{\text{red}}$. By the structure of smooth connected commutative \bar{k} -groups, it

follows that $(Z_{\bar{k}})_{\text{red}} = S \times U$ for a smooth connected unipotent \bar{k} -group U . For any n not divisible by $\text{char}(k)$, consider the torsion subgroup $Z[n]$. This is a commutative, affine algebraic k -group, and since the derivative of $[n] : Z \rightarrow Z$ is $n : \text{Lie}(Z) \rightarrow \text{Lie}(Z)$, it follows that $\text{Lie}(Z[n])$ is killed by $n \in k^\times$. Thus $\text{Lie}(Z[n]) = 0$, so $Z[n]$ is finite étale over k .

This implies that

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

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

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

Lemma E.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

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

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

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

Lemma E.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 $Z_G(M)_{\bar{k}} = Z_{G_{\bar{k}}}(M_{\bar{k}})$ must have the same dimension as those of $G_{\bar{k}}$, as can be seen by considering one containing $M_{\bar{k}}$. So if we can find a k -torus in $Z_G(M)$ that remains maximal as such after extension of the ground field to \bar{k} then the \bar{k} -fiber of such a torus must also be maximal in $G_{\bar{k}}$ 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 $\bar{T} \subset Z_G(M)/M$ which is geometrically maximal. Let T be the scheme-theoretic preimage of \bar{T} in $Z_G(M)$. Since M is smooth and connected, the quotient map $Z_G(M) \rightarrow Z_G(M)/M$ is smooth, so T is a smooth connected closed k -subgroup of G . It sits in a short exact sequence of k -groups

$$1 \rightarrow M \rightarrow T \rightarrow \bar{T} \rightarrow 1.$$

Since M and \bar{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 $Z_G(M)_{\bar{k}}$ must contain the central $M_{\bar{k}}$ (since otherwise the subgroup $T'M_{\bar{k}}$ would be a bigger torus). Thus, maximality of T' in $Z_G(M)_{\bar{k}}$ is in fact equivalent to the maximality of the quotient $T'/M_{\bar{k}}$ in $(Z_G(M)/M)_{\bar{k}}$. In particular, $T_{\bar{k}}$ is maximal in $Z_G(M)_{\bar{k}}$, and thus in $G_{\bar{k}}$ as we already remarked. \square

So much for motivation: now we need to find such an M . The basic idea for infinite k is to use $\text{Lie}(S) = \mathfrak{gl}_1 \subset \mathfrak{g}_{\bar{k}}$, a non-central Lie subalgebra, plus the Zariski-density of \mathfrak{g} in $\mathfrak{g}_{\bar{k}}$ (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 \bar{k} -tori are maximal in $G_{\bar{k}}$, so a geometrically maximal \bar{k} -torus in $Z_G(X)^0$ will do this job. (Below we will define what we mean by “semisimple” for elements of $\mathfrak{g}_{\bar{k}}$. 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 $\mathfrak{g}_{\bar{k}}$ 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).

E.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:

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

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

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

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

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

Remark E.3.2. Note that we are *not* claiming that $\text{ad}(X)$ 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 $G \hookrightarrow GL_N$ (and more specifically, involve the k -group G). Moreover, by definition, these concepts are preserved under passage to $\mathfrak{g}_{\bar{k}}$ (and as with algebraic groups, the Jordan components of $X \in \mathfrak{g}$ are generally only rational over the perfect closure of k).

If $p = \text{char}(k) > 0$, then upon choosing a faithful representation $G \hookrightarrow GL_N$, 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 $X \mapsto X^{[p]} : \mathfrak{g} \rightarrow \mathfrak{g}$ 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 $\text{ad}(X^{[p]}) = \text{ad}(X)^{[p]}$ (as is one of the axioms for *p-Lie algebras*). For further details on *p-Lie algebras*, see [Bor, §3.1] and [CGP, A.7] (especially [CGP, Lemma A.7.13]).

Remark E.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 $S = GL_1 \hookrightarrow G_{\bar{k}}$ gives an action of S on $\mathfrak{g}_{\bar{k}}$ (via the adjoint action of $G_{\bar{k}}$ on $\mathfrak{g}_{\bar{k}}$), and this decomposes as a direct sum of weight spaces

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

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

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

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

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

We have not yet verified (\star) , since $Y \in \mathfrak{g}_{\bar{k}}$, and we seek a non-central semisimple element of \mathfrak{g} . To fix this, consider the characteristic polynomial $f(X, t)$ of $\text{ad}(X)$ for generic $X \in \mathfrak{g}$, as a polynomial in $k[\mathfrak{g}^*][t]$. Viewed in $\bar{k}[\mathfrak{g}^*][t] = \bar{k}[\mathfrak{g}_{\bar{k}}^*][t]$, 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 $\mathfrak{g}_{\bar{k}}$. Since $\mathfrak{g} \subset \mathfrak{g}_{\bar{k}}$ 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, $\text{ad}(X)$ is not nilpotent, so $\text{ad}(X)_s$ is nonzero. Since $\text{ad}(X_s) = \text{ad}(X)_s \neq 0$, X_s is noncentral and semisimple in $\mathfrak{g}_{\bar{k}}$.

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) . If instead $\text{char}(k) = p > 0$ then consider the additive Jordan decomposition $X = X^{\text{ss}} + X^n$ in $\mathfrak{g}_{\bar{k}}$ as a sum of commuting semisimple and nilpotent elements. For $r \gg 0$ we see that $X^{[p^r]} = (X^{\text{ss}})^{[p^r]}$ is nonzero and semisimple, and also (as the p^r th power of X is in \mathfrak{g}) lies in \mathfrak{g} . It is noncentral since $\text{ad}(X^{[p^r]}) = \text{ad}(X)^{p^r}$ is nonzero (as $\text{ad}(X)$ is not nilpotent, by design). So hypothesis (\star) holds for G over any infinite field k .

E.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 $\mathfrak{g}' = \text{Lie}(G')$ contains a nonzero semisimple element of \mathfrak{g} . This implies that G'_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'_k is not unipotent, this means G' (and hence $G!$) contains a *nontrivial* k -torus, which is all we need to prove (Lemma E.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 $\text{Ad} : G \rightarrow \text{GL}(\mathfrak{g})$). 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 $\text{Ad}(G)$, so by differentiating we get $\text{ad}(X) = 0$ 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 E.4.1. In [Bor, §9.1] it is shown that $Z_G(X)$ is smooth in any characteristic. We avoid that approach because we have not developed any general theory for semisimple elements of \mathfrak{g} .

For the remainder of the proof, we will assume $\text{char}(k) = p > 0$. Now we will make essential use of p -Lie algebras, and especially an interesting construction from [SGA3, VII_A, 7.2, 7.4] (also formulated in [CGP, Prop. 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 $\mathfrak{a}^p = 0$ for all $\mathfrak{a} \in \mathfrak{m}_H$) via $H \mapsto \text{Lie}(H)$, 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 is [SGA3, VII_A, 7.2, 7.4]:

Theorem E.4.2. *Let B be a commutative \mathbf{F}_p -algebra. The functor $H \rightsquigarrow \text{Lie}_p(H)$ 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

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

In this result, $F_{G/k} : G \rightarrow G^{(p)}$ denotes the relative Frobenius morphism, discussed in [CGP, A.3] (especially up through [CGP, A.3.4]). (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 $H \rightarrow G$ 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 [CGP, A.7], the basic aspects of Lie algebras and \mathfrak{p} -Lie algebras of general group schemes over rings are developed from scratch.

Remark E.4.3. In the special case of commutative k -groups whose augmentation ideal is killed by the \mathfrak{p} -power map, the equivalence with finite-dimensional commutative \mathfrak{p} -Lie algebras over k is nicely explained in the unique Theorem in [Mum, §14], 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 $\mathfrak{h} = \text{Span}_k(X^{[p^i]})$. 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 \mathfrak{p} -Lie subalgebra of \mathfrak{g} . A linear combination of commuting semisimple operators is semisimple. Moreover the p th 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 [SGA7, XXII, §1] for a nice discussion, especially [SGA7, (1.0.9), Prop. 1.1], or alternatively the Corollary at the end of [Mum, §14] 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 $\varphi : V \rightarrow V$ is a Frobenius-semilinear endomorphism then there is a unique decomposition $V = V_{ss} \oplus V_n$ such that φ is nilpotent on V_n and $(V_{ss})_{\overline{F}}$ admits a basis of “ φ -fixed vectors” ($\varphi(v) = v$).

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

Lemma E.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 E.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,

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

Thus, H is a power of the order- p infinitesimal commutative k -subgroup corresponding to the \mathfrak{p} -Lie algebra kX with $X^{[p]} = X$. But there are only *two* 1-dimensional \mathfrak{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 $\alpha_p \hookrightarrow G_a$ and $\mu_p \hookrightarrow G_m$ which induces isomorphisms on \mathfrak{p} -Lie algebras. Nonzero invariant derivations on G_a resp. 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 [CGP, Lemma A.8.8] (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 [CGP, Prop. 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 E.4.2 provides more: if R is any k -algebra, then the \mathfrak{p} -Lie functor defines a bijective correspondence between R -group maps $H_R \rightarrow G_R$ and \mathfrak{p} -Lie algebra maps $\mathfrak{h}_R \rightarrow \mathfrak{g}_R$. 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 . \square

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 $Z_G(\mathfrak{h})^0$).

F Covering by Borel subgroups

F.1 Main result

Throughout this appendix, we work over a fixed *algebraically closed* ground field k (so all subgroups of k -groups are understood to be k -subgroups). Let G be a smooth connected affine k -group, and B a Borel subgroup. Our aim is to prove the following important result:

Theorem F.1.1. *The subgroups $gB(k)g^{-1}$ for $g \in G(k)$ cover $G(k)$. In particular, every element of $G(k)$ lies in a Borel subgroup.*

Before we take up the proof of this result, we record a very interesting consequence.

Proposition F.1.2. *Choose $g \in G(k)$. If g is semisimple then it is contained in a torus of G . If g is unipotent then it is contained in a unipotent smooth connected subgroup of G .*

There is real content to this, since g might not lie in the identity component of the Zariski closure of $\langle g \rangle$ (e.g., g may have finite order, as for all unipotent elements when $\text{char}(k) > 0$).

Proof. By Theorem F.1.1, g lies in a Borel subgroup. We can rename that Borel subgroup as G , so now G is solvable. Since $k = \bar{k}$, so G is k -split, we have $G = U \rtimes T$ for a smooth connected unipotent U and a torus T . The projection map $G \rightarrow T$ kills all unipotent elements of $G(k)$, so such elements lie in $U(k)$. That settles the case when g is unipotent.

Now suppose g is semisimple. We seek a torus in G containing g . The case $U = 1$ is trivial, so we may assume $U \neq 1$. Since U is normal in G , so is its proper subgroup $\mathcal{D}(U)$. Using induction on $\dim U$ and the general structure of solvable smooth connected k -groups, it suffices to solve the problem for $G/\mathcal{D}(U)$. Hence, we may and do assume that U is commutative. In particular, the conjugation action of G on U factors through an action of T on U . If $\text{char}(k) = p > 0$, we can similarly reduce to the case when U is p -torsion. Thus, exactly as in the argument following Lemma D.3.3 in Appendix D, the k -group U is a vector group and we can choose the linear structure (especially when $\text{char}(k) > 0$) so that the T -action on U is linear. This yields a T -equivariant composition series for U with 1-dimensional jumps. The members of such a composition series are normal in G , so by induction on $\dim U$ we are thereby reduced to the case $U = G_a$, and T acts on U through some $\chi \in X(T)$. This described the semidirect product structure $G = G_a \rtimes T$.

If $\chi = 1$ then G is commutative and $g \in T(k)$. Hence, we can assume $\chi \neq 1$, so $S = (\ker \chi)_{\text{red}}^0$ is a torus of codimension 1 in T and it is central in G . We can therefore pass to G/S to reduce to the case $G = G_a \rtimes G_m$ using an action $t.x = t^n x$ for some $n \in \mathbb{Z}$. Then $g = (x, t)$ with $t \neq 1$. If $t^n \neq 1$ then for $x' = x/(t^n - 1)$ we have $(x', 0)g(x', 0)^{-1} = (1, t) \in T(k)$. If $g = (x, t)$ with $t^n = 1$ then the unipotent $(x, 1)$ and semisimple $(0, t)$ commute, so they are the Jordan constituents of g . We assumed g is semisimple, so this forces $x = 0$ and $g \in T(k)$. \square

The rest of this appendix is devoted to the proof of Theorem F.1.1. The main ingredients are given in [Bor, 11.9, 11.10]. The first step is to prove a general lemma concerning the union of the $G(k)$ -conjugates of *any* smooth connected closed k -subgroup H in G . We then apply it to two special cases: $H = B$ a fixed Borel subgroup and $H = Z_G(T)^0$ the (smooth!) Cartan subgroup associated to a maximal torus T in B (which we know is then also maximal in G).

Lemma F.1.3. *The union Ω of the conjugates $gH(k)g^{-1}$ for $g \in G(k)$ contains a non-empty open subset of its closure $\overline{\Omega}$ in $G(k)$, and Ω is closed in $G(k)$ if H is a parabolic subgroup of G .*

If $N_{G(k)}(H)$ contains $H(k)$ with finite index and some $h \in H(k)$ lies in only finitely many $G(k)$ -conjugates of $H(k)$ then Ω is dense in $G(k)$.

Lest the hypotheses on H in the second part of the lemma look strange, before proving the lemma we mention an important case in which these hypotheses are satisfied: $H = Z_G(T)^0$ for a maximal torus $T \subset B$. Indeed, T is a central maximal torus in H , so $N_{G(k)}(H) = N_{G(k)}(T)$ and we already know that $N_{G(k)}(T)/Z_{G(k)}(T)$ is finite (HW 6, Exercise 4). Since $H(k)$ has finite index in $Z_G(T)(k) = Z_{G(k)}(T)$, the Cartan subgroup H satisfies the finite-index requirement. To exhibit elements of $H(k)$ lying in only finitely many $G(k)$ -conjugates of H , we first observe the structure of H : the quotient H/T contains no nontrivial

tori, so it is unipotent and hence H is solvable. But its maximal torus T is central, so $H = T \times U$ by the structure of solvable smooth connected groups over $k = \bar{k}$.

Let $\Phi(G, T) = \{\chi_i\}$ denote the finite set of *nontrivial* characters in $X(T)$ which arise in the adjoint representation of T on $\mathfrak{g} = \text{Lie}(G)$. The kernel of each χ_i is a codimension-1 subscheme in T , so we can choose $t \in T(k)$ such that $\chi_i(t) \neq 1$ for all i . I claim that the containment $Z_G(T)^0 \subset Z_G(t)^0$ of closed subgroup schemes is an *equality*. By the functorial meaning of both centralizers (and HW7, Exercise 4), the respective Lie algebras inside of \mathfrak{g} are \mathfrak{g}^T and $\mathfrak{g}^{\text{Ad}(t)=1} = \mathfrak{g}^T$, the final equality arising from the weight space decomposition for the T -action on \mathfrak{g} and the way in which we chose t . Hence, the tangent spaces coincide. But $Z_G(T)^0$ is *smooth* (HW8, Exercise 4), so dimension considerations then force $Z_G(t)^0$ to be smooth and so equal to its closed subscheme $Z_G(T)^0$.

For such a t , if $t \in gHg^{-1}$ then $g^{-1}tg \in T \times U$ is a semisimple element. Hence, $g^{-1}tg \in T(k)$, so $t \in gTg^{-1}$. It follows from the commutativity and connectedness of gTg^{-1} that $gTg^{-1} \subset Z_G(t)^0 = Z_G(T)^0$, so gTg^{-1} is contained in the central maximal torus T in $Z_G(T)^0$. By dimension reasons, this forces $gTg^{-1} = T$, so $g \in N_G(T)(k)$. But $H = Z_G(T)$, so gHg^{-1} only depends on g in the coset space $N_G(T)(k)/Z_G(T)^0(k)$ which is *finite*. Thus, such $t \in H(k)$ satisfy the desired finiteness condition on $G(k)$ -conjugates of H .

Proof. Consider the “shearing” automorphism of $G \times G$ defined by $(g, g') \mapsto (g, gg'g^{-1})$. This carries $G \times H$ over to another irreducible smooth closed subscheme $Y \subset G \times G$ characterized by

$$Y(k) = \{(g, g') \in G(k) \times G(k) \mid g^{-1}g'g \in H(k)\}.$$

This description shows that Y is stable under the right H -action on the first factor G , so Y is the underlying space of the preimage of its image $Y' \subset (G/H) \times G$. But $G \times G \rightarrow (G/H) \times G$ is faithfully flat, hence an open surjection, so it is a topological quotient map. Since Y is closed in $G \times G$, it follows that Y' is closed in $(G/H) \times G$. Being the image of Y , we also see that Y' is irreducible.

Consider the second projection $p_2 : Y' \rightarrow G$. Clearly $(p_2(Y'))(k) = p_2(Y'(k)) = \bigcup_{g \in G(k)} gH(k)g^{-1} = \Omega$. Since $p_2(Y')$ is constructible in G , its closure in G has as its k -points exactly the closure in $G(k)$ of $(p_2(Y'))(k) = \Omega$, and so Ω contains a subset which is dense open in the closure of Ω within $G(k)$. If H is a parabolic subgroup then $p_2 : Y' \rightarrow G$ is a closed map since $G/H \rightarrow \text{Spec}(k)$ is universally closed. Hence, in such cases Ω is closed in $G(k)$.

In general the first projection $Y' \rightarrow G/H$ is surjective, with all fibers irreducible of the same dimension (namely, $\dim H$), so by irreducibility of Y' and G we get $\dim Y' = \dim H + \dim(G/H) = \dim G$. Now suppose that $H(k)$ has finite index in $N_{G(k)}(H)$ and some $h \in H(k)$ lies in only finitely many $G(k)$ -conjugates of $H(k)$. In this case, consider the fiber of $p_2 : Y' \rightarrow G$ over h . The fiber on k -points consists of points (gH, h) such that $g^{-1}hg \in H(k)$, which is to say $h \in gH(k)g^{-1}$. By hypothesis on H , this latter condition restricts $gH(k)g^{-1}$ to only finitely many possibilities, and in general if $gH(k)g^{-1} = g'H(k)g'^{-1}$ then $g^{-1}g' \in N_{G(k)}(H)$. Letting $\{\xi_1, \dots, \xi_m\}$ be a finite set of representatives for $N_{G(k)}(H)/H(k)$, we have $g^{-1}g' \in \xi_i H(k)$ for some i , so $g' \in g\xi_i H(k)$ and hence $g'H = g\xi_i H$. Thus, $p_2^{-1}(h)$ in Y' has at most m distinct k -points, so $p_2^{-1}(h)$ is finite in Y' . Semicontinuity of fiber dimension then forces $p_2 : Y' \rightarrow G$ to be quasi-finite on a dense open in Y' , yet $\dim Y' = \dim G$ with Y' and G irreducible. Thus, $p_2 : Y' \rightarrow G$ is dominant. This says exactly that Ω is dense in $G(k)$. \square

We now apply Lemma F.1.3 twice. Taking $H = Z_G(T)^0$, for which we have seen that the hypotheses are satisfied, we conclude that the $G(k)$ -conjugates of $H(k)$ have union in $G(k)$ that is dense. In other words, the Cartan subgroups of G have union at the level of k -points that is dense in $G(k)$. Every Cartan subgroup is solvable, and so lies in a Borel subgroup, so the union of the Borel subgroups at the level of k -points is dense. However, this latter union is also closed in $G(k)$ since Borel subgroups are parabolic! It follows that $G(k)$ is the union of the subgroups $B(k)$ as B varies through all Borel subgroups of G . Since the Borel subgroups of G are $G(k)$ -conjugate, we are done.

G Conjugacy into a maximal torus

G.1 Main result

This appendix addresses an intermediate step in the general proof of conjugacy of maximal tori in a smooth connected affine group over an algebraically closed field. We wish to prove:

Proposition G.1.1. *Let G be a solvable smooth connected group over an algebraically closed field k , and choose a semidirect product expression $G = T \ltimes U$ with T a torus and U unipotent. Then every semisimple $s \in G(k)$ admits a $G(k)$ -conjugate contained in T .*

Recall from Appendix F (which only required $G(k)$ -conjugacy of Borels, and no solvability hypotheses) that every semisimple element must lie in *some* torus. The problem is to relate things to a *specific* torus, and we cannot appeal to conjugacy of maximal tori since the proof of that rests on the above proposition in the solvable case (applied to a Borel subgroup). So to prove the proposition, we need to give a direct argument making essential use of the solvability of G .

The idea of the proof is to induct on dimension with the help of a composition series, but we will use a composition series whose terms are *normal* in G and have as successive quotients not individual G_a 's and G_m 's but rather vector groups and tori of possibly big dimension. Ultimately the problem will be reduced to the 2-dimensional case with T and U each of dimension 1, in which case a direct calculation becomes possible with little difficulty.

G.2 The proof

As a first step, we reduce to the case when U is commutative. To do this, first note that if $\{U_i\}$ is any characteristic composition series of U (i.e., each U_i is smooth connected and stable under all k -automorphisms of U) then all U_i are normalized by $G(k)$ and hence are normal in G (as $k = \bar{k}$). Thus, we could then consider $T \ltimes (U_i/U_{i-1})$ separated, moving down the composition series and inducting on $\dim U$ (the case $\dim U = 0$ being trivial). Applying these considerations to the derived series $\{\mathcal{D}^i(U)\}$ thereby reduces us to the case when U is commutative. Going a step further, if $\text{char}(k) = p > 0$ then the commutative U is killed by p^N for some big N and each image $p^i U$ is a smooth connected k -subgroup of U (in contrast with the torsion subgroups $U[p^i]$). This is also a characteristic composition series of U , so we can get to the case when U is p -torsion.

By Exercise 2(ii) in HW9, if $\text{char}(k) = 0$ then $U \simeq G_a^n$ with T acting linearly. Thus, we get a weight space decomposition for the action of the k -split U and can take a flag adapted to T -eigenlines to get a T -stable flag in U . That permits us to reduce to the case $U = G_a$ with a linear T -action when $\text{char}(k) = 0$. Let us reach the same special case when $\text{char}(k) = p > 0$. In these cases, Exercise 2(i) in HW9 (which rests on the beautiful work of Tits on the structure of unipotent smooth connected groups, presented in [CGP, App. B], especially [CGP, Thm. B.4.3]) implies that $U \simeq U_0 \times V$ where U_0 has trivial T action (and mysterious structure!) and V is a vector group with a *linear* T -action for some choice of isomorphism $V \simeq G_a^n$. Thus, we can again reduce to the special case $U = G_a$ with a linear T -action (as the case of U with trivial T -action is obvious).

Now back in the case of any characteristic, the linear T -action on G_a is given by some k -homomorphism $\chi : T \rightarrow G_m$, and we can assume $\chi \neq 1$ (as otherwise $G = T \times U$ and we are clearly done). Thus, $T/(\ker \chi) \simeq G_m$ via χ . Note that $\ker \chi \subset Z_G$, so we can easily pass to $G/(\ker \chi)$ and replace T with $T/(\ker \chi)$ without loss of generality to get to the case $G = G_m \ltimes G_a$ with the *standard* action $t.x = tx$ of G_m on $G_a = \mathcal{R}_u(G)$. This is just the “ $ax + b$ group” via

$$(t, x) \mapsto \begin{pmatrix} t & x \\ 0 & 1 \end{pmatrix}.$$

The semisimple point $s = (t, x) \in G(k)$ must have $t \neq 1$ (i.e., $s \notin G_a(k)$), and then for $x' = x/(t - 1)$ it is easy to compute

$$(1, x')g(1, -x') = (t, 0) \in T(k).$$

H Dynamic approach to algebraic groups

[Parts of H.1 are extracted from [CGP, §2.1]; e.g., the proof of H.1.1 comes from the proof of [CGP, 2.1.8(3)].]

H.1 Subgroups associated to a 1-parameter subgroup

Let G be a smooth affine group over a field k , and $\lambda : \mathbf{G}_m \rightarrow G$ a k -homomorphism (possibly trivial, though that case is not interesting). One often calls λ a *1-parameter k -subgroup* of G , even when $\ker \lambda \neq 1$. Such a homomorphism defines a left action of \mathbf{G}_m on G via the functorial procedure $t.g = \lambda(t)g\lambda(t)^{-1}$ for $g \in G(R)$ and $t \in R^\times$ for any k -algebra R . In lecture we introduced the following associated subgroup functors of G : for any k -algebra R ,

$$P_G(\lambda)(R) = \{g \in G(R) \mid \lim_{t \rightarrow 0} t.g \text{ exists}\}, \quad U_G(\lambda)(R) = \{g \in G(R) \mid \lim_{t \rightarrow 0} t.g = 1\},$$

and

$$Z_G(\lambda)(R) = \{g \in G(R) \mid \lambda_R \text{ centralizes } g\}.$$

In the March 10 lecture it was proved that these are all represented by closed k -subgroup schemes of G , with $P_G(\lambda) = Z_G(\lambda) \ltimes U_G(\lambda)$.

By a direct calculation with graded modules over the dual numbers, it is shown in [CGP, Prop. 2.1.8(1)] that when using the \mathbf{Z} -grading $\oplus_{n \in \mathbf{Z}} \mathfrak{g}_n$ of $\mathfrak{g} = \text{Lie}(G)$ defined by the \mathbf{G}_m -action induced by conjugation through λ (i.e., \mathfrak{g}_n is the space of $v \in \mathfrak{g}$ such that $\text{Ad}_G(\lambda(t))(v) = t^n v$ for all $t \in \mathbf{G}_m$), we have

$$\text{Lie}(Z_G(\lambda)) = \mathfrak{g}_0, \quad \text{Lie}(U_G(\lambda)) = \mathfrak{g}^+ := \bigoplus_{n > 0} \mathfrak{g}_n.$$

For example, if $T \subset G$ is a split k -torus and λ is valued in T , then using the resulting T -weight space decomposition $\mathfrak{g} = \text{Lie}(Z_G(T)) \oplus (\oplus_{\alpha \in \Phi} \mathfrak{g}_\alpha)$ (with Φ the set of nontrivial T -weights on \mathfrak{g}) we see that for any $n \in \mathbf{Z} - \{0\}$,

$$\mathfrak{g}_n = \bigoplus_{\langle \alpha, \lambda \rangle = n} \mathfrak{g}_\alpha$$

since the adjoint action of $\lambda(t)$ on \mathfrak{g}_α is multiplication by $\alpha(\lambda(t)) = t^{\langle \alpha, \lambda \rangle}$. Hence,

$$\mathfrak{g}_0 = \text{Lie}(Z_G(T)) \oplus (\oplus_{\langle \alpha, \lambda \rangle = 0} \mathfrak{g}_\alpha), \quad \text{Lie}(U_G(\lambda)) = \mathfrak{g}_+ = \oplus_{\langle \alpha, \lambda \rangle > 0} \mathfrak{g}_\alpha.$$

We write λ^{-1} to denote the reciprocal homomorphism $t \mapsto \lambda(t)^{-1} = \lambda(1/t)$. In HW10 you are led through a proof that if $G = \text{GL}(V)$ then the multiplication map

$$\mu = \mu_{G, \lambda} : U_G(\lambda^{-1}) \times P_G(\lambda) \rightarrow G$$

is an open immersion, with $P_G(\lambda)$ a subgroup of “block upper-triangular matrices” and $U_G(\lambda)$ its unipotent radical (even over \bar{k}). We first wish to deduce the open immersion property for general G from this, which immediately implies that $U_G(\lambda)$, $P_G(\lambda)$, and $Z_G(\lambda)$ are all smooth (direct factors inherit smoothness) and that they are connected when G is connected. Likewise, it would follow that $U_G(\lambda)$ is unipotent in general since functoriality with respect to an inclusion $G \hookrightarrow \text{GL}_n$ would reduce this to the settled case of GL_n . Finally, by iterating the connectedness of $Z_G(\lambda)$ several times (using λ 's that generate a given torus in $G_{\bar{k}}$) it would follow that if G is connected then so is $Z_G(S)$ for any k -torus S in G .

In general, with a general pair (G, λ) , consider a k -subgroup inclusion $j : G \hookrightarrow G'$ into another smooth affine k -group (the case of interest being $G' = \text{GL}(V)$), and let $\lambda' = j \circ \lambda$. By the functorial definition,

$$P_G(\lambda) = G \cap P_{G'}(\lambda'), \quad U_G(\lambda^{\pm 1}) = G \cap U_{G'}(\lambda'^{\pm 1}), \quad Z_G(\lambda) = G \cap Z_{G'}(\lambda').$$

In particular, if $U_{G'}(\lambda'^{-1}) \cap P_{G'}(\lambda') = 1$ then $U_G(\lambda^{-1}) \cap P_G(\lambda) = 1$. In other words, if $\mu' = \mu_{G', \lambda'}$ is a monomorphism then so is μ . This monicity hypothesis on μ for $G' = \text{GL}(V)$ (and any 1-parameter k -subgroup λ' of $\text{GL}(V)$) is verified in HW10, so μ is monic in general. But is it an open immersion? If μ' is an open immersion (as is proved on HW10 for $G' = \text{GL}(V)$!) then the same holds for μ by means of the following non-obvious lemma:

Lemma H.1.1. *With notation as above, if μ' is monic then*

$$G \cap (U_{G'}(\lambda'^{-1}) \times P_{G'}(\lambda')) = U_G(\lambda^{-1}) \times P_G(\lambda)$$

as subfunctors of G .

Proof. Since $P_{G'}(\lambda') = U_{G'}(\lambda') \rtimes Z_{G'}(\lambda')$, by evaluating on points valued in k -algebras R we have to show that if

$$u'_- \in U_{G'}(\lambda'^{-1})(R), \quad u'_+ \in U_{G'}(\lambda')(R), \quad z' \in Z_{G'}(\lambda')(R)$$

and $u'_- u'_+ z' = g \in G(R)$ then that $u'_+, u'_-, z' \in G(R)$.

As usual, we can pick a finite-dimensional k -vector space V , a k -homomorphism $\rho : G' \rightarrow GL(V)$, and a line L in V such that G is the scheme-theoretic stabilizer of L in G' . Let $v \in L$ be a basis element, so $\rho(g)(v) = cv$ in $V_R = R \otimes_k V$ for a unique $c \in R^\times$. Since $g = u'_- u'_+ z'$, we get

$$\rho(u'_+ z')(v) = c \rho((u'_-)^{-1})(v) \quad (2)$$

in V_R .

For any point t of \mathbf{G}_m valued in an R -algebra R' , the point $\lambda'(t)$ of $G'(R')$ lies in $G(R')$ and so acts on v (through ρ) by some R'^\times -scaling. Hence, we can replace v with $\rho(\lambda'(t)^{-1})(v)$ on both sides of (2). Now act on both sides of (2) by $\rho(\lambda'(t))$, and then commute $\rho(\lambda'(t)^{-1})$ past $\rho(z')$ (as we may, since $z' \in Z_{G'}(\lambda')(R)$) to get the identity

$$\rho((t u'_+) z')(v) = c \rho(t \cdot (u'_-)^{-1})(v) \quad (3)$$

as points of the affine space \underline{V}_R over R covariantly associated to V_R .

Viewing the two sides of (3) as R -scheme maps $(\mathbf{G}_m)_R \rightarrow \underline{V}_R$, the left side extends to an R -map $\mathbf{P}_R^1 - \{\infty\} = \mathbf{A}_R^1 \rightarrow \underline{V}_R$ and the right side extends to an R -map $\mathbf{P}_R^1 - \{0\} \rightarrow \underline{V}_R$. By combining these, we arrive at an R -map $\mathbf{P}_R^1 \rightarrow \underline{V}_R$ from the projective line to an affine space over R . The only such map is a constant R -map to some $v_0 \in \underline{V}_R(R) = V_R$ (concretely, $R[t] \cap R[1/t] = R$ inside of $R[t, 1/t]$), so both sides of (3) are independent of t (and equal to v_0). Passing to the limit as $t \rightarrow 0$ on the left side and as $t \rightarrow \infty$ on the right side yields $\rho(z')(v) = v_0 = cv$. We have proved that z' carries v to an R^\times -multiple of itself. Thus, the point $z' \in G'(R)$ is an R -point of the functorial stabilizer of L inside of V . This stabilizer is exactly G , by the way we chose ρ , so z' is an R -point of $G \cap Z_{G'}(\lambda') = Z_G(\lambda)$.

Since $\rho(z')(v) = cv$, by cancellation of c on both sides of the identity (3) we get

$$\rho(t \cdot u'_+)(v) = \rho(t \cdot (u'_-)^{-1})(v)$$

with both sides independent of t and equal to $c^{-1}v_0 = v$. Taking $t = 1$, this says that u'_\pm lies in the stabilizer G of v , so u'_\pm is an R -point of $G \cap U_{G'}(\lambda'^{\pm 1}) = U_G(\lambda^{\pm 1})$, as required. \square

At the end of the March 10 lecture, we used the open immersion property for μ to prove the following crucial result:

Proposition H.1.2. *Let $f : G \twoheadrightarrow G'$ be a surjective k -homomorphism between smooth connected affine k -groups, and let $\lambda : \mathbf{G}_m \rightarrow G$ be a k -homomorphism. For $\lambda' = f \circ \lambda$, the natural maps $P_G(\lambda) \rightarrow P_{G'}(\lambda')$, $U_G(\lambda) \rightarrow U_{G'}(\lambda')$, and $Z_G(\lambda) \rightarrow Z_{G'}(\lambda')$ are surjective.*

We have shown that surjective homomorphisms between smooth connected affine k -groups carry maximal k -tori onto maximal k -tori and Borel k -subgroups onto Borel k -subgroups. Another related important compatibility is the good behavior of *torus centralizers* under surjective homomorphisms. This follows from the preceding proposition:

Corollary H.1.3. *Let $f : G \twoheadrightarrow G'$ be a surjective k -homomorphism between smooth connected affine k -groups. Let S be a k -torus in G , and $S' = f(S)$. Then $f(Z_G(S)) = Z_{G'}(S')$.*

This result is also [Bor, 11.14, Cor. 2]. You may find it instructive to compare the proofs.

Proof. We may assume $k = \bar{k}$. If S_1 and S_2 are k -subtori in S such that $S_1 \cdot S_2 = S$, which is to say that the k -homomorphism $S_1 \times S_2 \rightarrow S$ is surjective, it is an exercise (do it!) to check that $Z_G(S) = Z_{Z_G(S_1)}(S_2)$. (Note that since torus centralizers in smooth affine groups are smooth, this equality may be checked by computing with geometric points.) Hence, by induction on $\dim S$, we may and do assume $S \simeq \mathbf{G}_m$.

With $S \simeq \mathbf{G}_m$, the inclusion of S into G is given by a k -homomorphism $\lambda : \mathbf{G}_m \rightarrow G$ with image S . Likewise, $\lambda' = f \circ \lambda : \mathbf{G}_m \rightarrow G'$ has image S' . Hence, $Z_G(S) = Z_G(\lambda)$ and $Z_{G'}(S') = Z_{G'}(\lambda')$. Thus, the map $Z_G(S) \rightarrow Z_{G'}(S')$ that we wish to prove is surjective is identified with the natural map $Z_G(\lambda) \rightarrow Z_{G'}(\lambda')$. By Proposition H.1.2, this latter map is surjective! \square

H.2 Conjugacy for split tori

It is a deep fact that in smooth connected affine groups G over any field k , all maximal k -split k -tori S in G (not to be confused with k -split maximal k -tori, which may not exist!) are $G(k)$ -conjugate; we will not use this. Their common dimension is called the k -rank of G ; it could be considerably smaller than the common dimension of the maximal k -tori (which may be called the *geometric rank*, since it is the \bar{k} -rank of $G_{\bar{k}}$). The proof of this conjugacy result rests on the theory of reductive groups (and pseudo-reductive groups when k is imperfect). We will prove it in the sequel course for reductive groups; in the general case see [CGP, Thm. C.2.3] for a proof.

The special case of PGL_2 plays a role in getting the structure theory of reductive groups off the ground, so we now give an elementary direct proof in the special case of PGL_n and GL_n :

Proposition H.2.1. *Let V be a finite-dimensional vector space over a field, and $G = \mathrm{GL}(V)$ or $\mathrm{PGL}(V)$. The maximal k -split k -tori in G are $G(k)$ -conjugate to each other.*

Proof. Using the quotient map $\mathrm{GL}(V) \rightarrow \mathrm{PGL}(V)$ whose kernel is \mathbf{G}_m and which is surjective on k -points (!), it is easy to reduce to the case of $\mathrm{GL}(V)$ in place of $\mathrm{PGL}(V)$ (check!). By HW5, Exercise 5, such k -tori correspond precisely to commutative k -subalgebras $A \subseteq \mathrm{End}(V)$ of the form $A \simeq k^n$ with $n = \dim V$. Such a k -subalgebra amounts to a k^n -module structure on an n -dimensional vector space V , which is nothing more or less than a decomposition of V into a direct sum of lines. But any two such decompositions are clearly related via the action of $\mathrm{Aut}_k(V) = \mathrm{GL}(V)(k)$, so we are done. \square

Now we turn our attention to an “axiomatic” $G(k)$ -conjugacy result. The axioms turn out to hold for all connected reductive k -groups containing a split maximal k -torus, as one shows when developing the structure theory of connected reductive groups. The verification of the axioms lies deeper in the theory (see Remark H.2.4), but we note here that it rests on the dynamic method (which is why we mention the topic in this appendix, to illustrate how useful the dynamic viewpoint is).

Theorem H.2.2. *Let G be a smooth connected affine k -group such that for every maximal torus T in $G_{\bar{k}}$, $Z_{G_{\bar{k}}}(T) = T$ and the finite group $W_{G_{\bar{k}}}(T)$ acts transitively on the set of Borel subgroups of $G_{\bar{k}}$ containing T . Also assume that any Borel subgroup B of $G_{\bar{k}}$ satisfies $N_{G_{\bar{k}}}(\bar{k})(B) = B(\bar{k})$.*

Assume that G contains a k -split maximal k -torus, and that for all such k -tori T there is a Borel k -subgroup B containing T . All such pairs (T, B) are $G(k)$ -conjugate to each other.

The centralizer hypothesis on the maximal tori of $G_{\bar{k}}$ is invariant under conjugation, so by the $G(\bar{k})$ -conjugacy of all maximal tori of $G_{\bar{k}}$ it suffices to check this condition for one maximal torus of $G_{\bar{k}}$. The same holds for the normalizer hypothesis on Borel subgroups.

Remark H.2.3. In the homework we have seen many examples of G for which $Z_G(T) = T$ for some maximal k -torus T , such as GL_n , SL_n , Sp_{2n} , and SO_n with their “diagonal” (split) maximal k -tori. But don’t forget that there are plenty of interesting nontrivial k -anisotropic connected reductive groups, such as $\mathrm{SL}(D)$ for a finite-dimensional central division algebra $D \neq k$ and $\mathrm{SO}(q)$ for an anisotropic quadratic space (V, q) over k with $\dim V \geq 3$, and in such cases there is *no nontrivial k -split torus* at all, let alone one which is maximal as a k -torus (so in such cases the proposition concerns an empty collection of k -tori).

Remark H.2.4. It is a general fact that $Z_G(T) = T$ for *every* maximal torus T in any connected reductive group G , but this is not at all obvious from the definitions; it is proved as part of a general development of basic structure theory of connected reductive groups. Likewise, the general development verifies the

transitivity axiom on Weyl groups in Theorem H.2.2 for connected reductive groups, as well as the fact that any k -split maximal k -torus (if one exists!) in a connected reductive k -group lies in a Borel k -subgroup. Finally, the self-normalizing property of Borel subgroups is a fundamental result of Chevalley, valid for any smooth connected affine \bar{k} -group. It underlies the entire structure theory of connected reductive groups.

To begin the proof of Theorem H.2.2, let T and T' be k -split maximal k -tori in G , and choose Borel k -subgroups $B \supset T$ and $B' \supset T'$. We have $T = Z_G(T)$ and $T' = Z_G(T')$, since such equality among k -subgroups may be checked over \bar{k} (where it follows from the hypotheses). The proof goes in two steps: conjugacy over k_s , and then a Galois cohomology argument to get down to k . But we follow the usual “reduction step” style and argue in reverse, by first showing that the general case can be reduced to the separably closed case, and then handling the case $k = k_s$.

Let's first reduce to the case of maximal tori over separably closed k : we will prove that if T_{k_s} and T'_{k_s} are $G(k_s)$ -conjugate then they are $G(k)$ -conjugate by an element carrying B_{k_s} to B'_{k_s} . Pick $g \in G(k_s)$ such that $T'_{k_s} = gT_{k_s}g^{-1}$, so $gB_{k_s}g^{-1}$ and B'_{k_s} are Borel k_s -subgroups containing T'_{k_s} . We first seek to choose g so that also these Borel k_s -subgroups coincide.

By hypothesis, the group $W_{G_{\bar{k}}}(T'_{\bar{k}})$ acts transitively on the set of Borel \bar{k} -subgroups containing $T'_{\bar{k}}$. But $W_G(T')$ is a finite étale k -group, so its geometric points are defined over k_s . Thus,

$$N_G(T')(k_s)/T'(k_s) = W_G(T')(k_s) = W_G(T')(\bar{k}) = W_{G_{\bar{k}}}(T'_{\bar{k}}).$$

In other words, the group $N_G(T')(k_s) = N_{G(k_s)}(T'_{k_s})$ acts transitively on the set of Borel \bar{k} -subgroups of $G_{\bar{k}}$ containing $T'_{\bar{k}}$. Hence, replacing $g \in G(k_s)$ with its left-translate by some element of $N_G(T')(k_s)$ (which doesn't affect the condition that $gT_{k_s}g^{-1} = T'_{k_s}$!) brings us to the case that the Borel k_s -subgroups $gB_{k_s}g^{-1}$ and B'_{k_s} containing T'_{k_s} coincide over \bar{k} and hence coincide over k_s .

Now we can carry out a Galois cohomology argument to push down the $G(k_s)$ -conjugacy to $G(k)$ -conjugacy. For any $\gamma \in \text{Gal}(k_s/k)$ we apply γ to both sides of the equalities

$$T'_{k_s} = gT_{k_s}g^{-1}, \quad B'_{k_s} = gB_{k_s}g^{-1}.$$

This gives

$$T'_{k_s} = \gamma(g)T_{k_s}\gamma(g)^{-1}, \quad B'_{k_s} = \gamma(g)B_{k_s}\gamma(g)^{-1},$$

so $\gamma(g)^{-1}g$ normalizes T_{k_s} as well as B_{k_s} . By hypothesis $N_{G(\bar{k})}(B_{\bar{k}}) = B(\bar{k})$, so

$$\gamma(g)^{-1}g \in B(\bar{k}) \cap G(k_s) = B(k_s)$$

and likewise $\gamma(g)^{-1}g \in N_G(T)(k_s)$.

If we did not have available the Borel k -subgroups and only worked with the split maximal k -tori, we would only have $\gamma(g)^{-1}g \in N_G(T)(k_s)$ and then we would get hopelessly stuck due to possible obstructions in $H^1(k_s/k, W_G(T))$. Now the importance of using the Borel k -subgroups emerges: $B(k_s) \cap N_G(T)(k_s) = T(k_s)$! Indeed, since $T = Z_G(T)$ (by our hypotheses) we can express this as the statement that $N_B(T)(k_s) = Z_B(T)(k_s)$, and this in turn is a special case of:

Lemma H.2.5. *Let H be a connected solvable smooth affine group over a field k , and let T be a maximal k -torus in H . Then $N_H(T)(k) = Z_H(T)(k)$.*

Proof. Since $T_{\bar{k}}$ is a maximal torus in $H_{\bar{k}}$, and the problem of showing a k -point of H lies in the closed subset $Z_H(T)$ may be checked over \bar{k} , it is harmless to extend the ground field to \bar{k} so that k is algebraically closed. Hence, the structure theorem for connected solvable groups becomes available: $H = T \ltimes U$ for $U = \mathcal{R}_u(H)$. To show that any $h \in H(k)$ normalizing T actually centralizes T , we may assume $h = u \in U(k)$. Hence, for any $t \in T(k)$ we have

$$utu^{-1} = t(t^{-1}ut)u^{-1}.$$

But $(t^{-1}ut)u^{-1} \in U(k)$ since U is normal in $H = T \ltimes U$, so the condition that $utu^{-1} \in T(k)$ forces it to equal t . \square

Thus, we have obtained a function $c : \gamma \mapsto \gamma(g)^{-1}g$ from $\text{Gal}(k_s/k)$ to $T(k_s)$. This functor factors through the quotient $\text{Gal}(K/k)$ for a finite Galois extension K/k inside of k_s such that $g \in G(K)$. It is therefore easy to check that $c \in Z^1(k_s/k, T(k_s))$. Consider the cohomology class $[c] \in H^1(k_s/k, T)$. Since $T \simeq \mathbf{G}_m^r$, this cohomology group vanishes by Hilbert 90. Hence, $c = \gamma(t)t^{-1}$ for some $t \in T(k_s)$. Thus, if we replace g with gt (as we may!), we get to the case when $\gamma(g) = g$ for all γ , so $g \in G(k)$. That does the job. (This idea adapts to pull down the result from \bar{k} by using Hilbert 90 for the fppf topology, but we give a more hands-on procedure below to get down to k_s from \bar{k} .)

Now we can assume that $k = k_s$, and it remains to show:

Proposition H.2.6. *If T and T' are maximal tori in a smooth connected affine group G over a separably closed field k then T and T' are $G(k)$ -conjugate.*

This says that the general conjugacy result over algebraically closed fields actually holds over separably closed fields. I think it is due to Grothendieck. Regardless, the argument we give is a version of the method he used in SGA3 for smooth affine groups over any scheme (working locally for the étale topology). The idea is similar to the trick with Isom-schemes in HW4 Exercise 5.

Proof. Consider the functor I on k -algebras defined by

$$I(R) = \{g \in G(R) \mid T'_R = gT_R g^{-1}\}.$$

This is a subfunctor of G , and its restriction $I_{\bar{k}}$ to \bar{k} -algebras is represented by a *smooth* closed subscheme of \bar{k} : since $T'_R = g_0 T_{\bar{k}} g_0^{-1}$ for some $g_0 \in G(\bar{k})$ by the known “geometric” case over \bar{k} , we see that $I_{\bar{k}}(R)$ consists of points $g \in G(R)$ such that $g_0^{-1}g \in Z_{G(R)}(T_R)$. In other words, $I_{\bar{k}}$ is represented by $g_0 Z_G(T)_{\bar{k}}$. By HW8, Exercise 3, this is smooth and non-empty. Thus, if we can prove that I is represented by a closed k -subscheme of G then its \bar{k} -fiber represents $I_{\bar{k}}$ and hence is smooth (and non-empty)! But we know that a smooth non-empty scheme over a *separably closed* field always has a k -point, so it would follow that $I(k) \neq \emptyset$, so the desired $G(k)$ -conjugacy of T and T' would follow.

It remains to prove that I is represented by a closed k -subscheme of G . We will do this by approaching tori through their torsion-levels. For each $n \geq 1$ not divisible by $\text{char}(k)$, define a functor on k -algebras as follows:

$$I_n(R) = \{g \in G(R) \mid T'[n]_R = gT[n]_R g^{-1}\}.$$

Clearly I is a subfunctor of I_n . Since $T[n]$ and $T'[n]$ are finite étale, each is just a finite set of k -points in G (as $k = k_s$). Thus, it is rather elementary to check that I_n is represented by a closed subscheme of G (verify!). The infinite intersection $\cap_n I_n$ as subfunctors of G is likewise represented by a closed subscheme of G (form the infinite intersection of representing closed subschemes for the I_n ’s). Thus, we just have to check that the inclusion $I(R) \subseteq \cap_n I_n(R)$ is an equality for all k -algebras R .

Equivalently, picking a point g of $G(R)$ lying in $\cap_n I_n(R)$ and conjugating T_R by this point, we are reduced to proving that $gT_R g^{-1}$ and T'_R coincide if their n -torsion subgroups coincide for all $n \geq 1$ not divisible by $\text{char}(k)$. By the same “relative schematic density” argument used in your solution to HW3 Exercise 3(iii), since the union of the $T[n](k)$ is Zariski-dense in T (why?) and likewise for T' it follows that a closed subscheme of G_R which contains all $T[n]_R$ ’s (resp. all $T'[n]_R$ ’s) must contain T_R (resp. T'_R). The automorphism of g -conjugation on G_R then implies likewise that a closed subscheme of G_R which contains every $gT[n]_R g^{-1}$ must contain $gT_R g^{-1}$. We conclude that if $gT[n]_R g^{-1} = T'[n]_R$ for all $n \geq 1$ not divisible by $\text{char}(k)$ then the closed subschemes $gT_R g^{-1}, T'_R \subseteq G_R$ each contain the other and so coincide. \square

References

- [Bor] A. Borel, *Linear algebraic groups* (2nd ed.) Springer-Verlag, New York, 1991.
- [BLR] S. Bosch, W. Lütkebohmert, M. Raynaud, *Néron Models*, Springer-Verlag, 1990.
- [Bou] N. Bourbaki, *Algebra* (Ch. 9), Hermann, Paris, 1959.
- [CP] C-Y. Chang, M. Papanikolas, *Algebraic independence of periods and logarithms of Drinfeld modules*, Journal of the AMS **25** (2012), pp.123-150.

- [Chev] C. Chevalley, *The algebraic theory of spinors*, Springer–Verlag, 1997.
- [CGP] B. Conrad, O. Gabber, G. Prasad, *Pseudo-reductive groups* (2nd ed.), Cambridge Univ. Press, 2015.
- [C] B. Conrad, “Reductive Group Schemes” in *Autour des Schémas en Groupes* Vol. I, Panoramas et Synthèses Numero 42–43, Société Math. de France, 2014; http://smf4.emath.fr/Publications/PanoramasSyntheses/2014/42-43/html/smf_pano-synth_42-43.php
- [SGA7] P. Deligne, N. Katz, *Groupes de monodromie en géométrie algébrique* II, LNM 340, Springer–Verlag, New York, 1973.
- [DR] P. Deligne, M. Rapoport, *Les schémas de modules des courbes elliptiques* in *Modular Functions of One Variable II*, Springer LNM **349** (1973), 143–316.
- [DG] M. Demazure, P. Gabriel, *Groupes algébriques*, Masson, Paris, 1970.
- [SGA3] M. Demazure, A. Grothendieck, *Schémas en groupes* I, II, III, *Lecture Notes in Math* **151**, **152**, **153**, Springer-Verlag, New York (1970).
- [EGA] A. Grothendieck, *Eléments de Géométrie Algébrique*, Publ. Math. IHES **4**, **8**, **11**, **17**, **20**, **24**, **28**, **32**, 1960–7.
- [L] S. Lang, *Algebra* (3rd edition), GTM 211, Springer–Verlag, 2002.
- [Mat] H. Matsumura, *Commutative Ring Theory*, Cambridge Univ. Press, 1990.
- [Mum] D. Mumford, *Abelian Varieties*, Oxford University Press, 1970.
- [Sil] J. Silverman, *Arithmetic of Elliptic Curves* (2nd ed.), Springer-Verlag, New York, 2009.