FINITE GROUPS OF LIE TYPE.

KEVIN MCGERTY

1. Affine Algebraic Groups

We will work over an algebraically closed field k, of arbitrary characteristic.

Definition 1.1. A *affine algebraic group* is a pointed affine k-variety (G, e) equipped with two morphisms

$$m\colon G \times G \to G; \qquad \iota\colon G \to G,$$

such that (G, m, ι, e) is an abstract group. A morphisms of affine algebraic groups is a morphism of varieties which is also a group homomorphism. (Thus we have a category of affine algebraic groups).

Example 1.2.
(1) Let $G = GL_n(\mathsf{k})$, the set of $n \times n$ invertible matrices over k. Then $GL_n(\mathsf{k})$ is naturally an affine algebraic group: indeed it is the complement of the hypersurface in k^{n^2} given by the determinant function, and so it is naturally an affine variety. It is easy to check that matrix multiplication and inversion are morphisms of varieties (using "Cramer's rule" for the inverse, for example).
(2) The special case of the previous example when $n = 1$ gives the multiplicative group, denoted $\mathbb{G}_m$.
(3) The group $T_n \subset GL_n(\mathsf{k})$ of upper triangular matrices is an affine algebraic group which is a subgroup of GL_n.
(4) The group U_n of upper triangular matrices with 1s on the diagonal, is a closed subvariety of GL_n which form an affine algebraic group (a subgroup of B).
(5) The subgroup of GL_n consisting of matrices in which each row and column contain exactly one nonzero entry is an affine algebraic group, known as the group of *monomial matrices*.

We begin with a few basic observations on algebraic groups.

Let $A = \mathcal{O}(G)$ be the ring of regular functions on G. For $x \in G$, we have two automorphisms λ_x, ρ_x of G given by left and right multiplication by x respectively. These yield pullback maps on A denoted λ_x^* and ρ_x^* respectively, which are related by $\lambda_x^* = \iota^* \rho_{x^{-1}}^* (\iota^*)^{-1}$. Note that, $x \mapsto \rho_x^*$ makes A into a G representation.

Lemma 1.3. *The representation of G on A is locally finite, that is for any finite set $F \subset A$, the span of $\{\rho_x^*(f) : x \in G, f \in F\}$ is finite dimensional.*

Proof. Clearly we may assume $F = \{f\}$. We simply describe the map ρ_x^* explicitly. The multiplication map m on A is a ring homomorphism $m^*\colon A \to A \otimes A$, and

Date: March, 2006.

x gives a homomorphism $\varepsilon_x \colon A \to \mathsf{k}$, such that ρ_x^* is given by the composition

$$A \xrightarrow{m^*} A \otimes A \xrightarrow{1 \otimes \varepsilon_x} A$$

Thus if we write $m(f) = \sum_{i=1}^{k} f_i \otimes g_i$, then we have

$$\rho_x^*(f)(y) = \sum_{i=1}^{k} f_i(y) g_i(x),$$

for all $y \in G$, and hence $\rho_x^*(f)$ lies in the span of $\{f_i : 1 \leq i \leq k\}$ for every $x \in G$. □

Proposition 1.4. *Let G be an affine algebraic group. Then there is an injective homomorphism $\phi \colon G \to GL(V)$ for some finite-dimensional vector space V.*

Proof. We first claim that if a subspace U of A is G-stable then $m^*(U) \subseteq U \otimes A$. To see this pick a basis of V and extend to a basis of A. Then we may write, for $f \in U$

$$m^*(f) = \sum_{j=1}^{m} v_j \otimes f_j + \sum_{k=1}^{n} w_k \otimes g_k$$

where v_i are elements of the basis of U, the w_k are elements of the basis of A not lying in V, and the $f_j, g_k \in A$. If the g_k are not all identically zero, we may pick $x \in G$ such that $g_k(x) \neq 0$ for some k. But then clearly $\rho_x(f) \notin U$, and we have a contradiction. (In fact, the condition $m^*(U) \subseteq U \otimes A$ is equivalent to U begin G-stable).

Now A is finitely generated, so we may find a finite dimensional k-subspace V of A which generates A as a k-algebra, which is also G-stable. Thus we have a map $\phi \colon G \to GL(V)$ given by the restriction of ρ. More explicitly, if $\{v_i : 1 \leq i \leq n\}$ is a basis of V, then we have $m^*(v_i) = \sum_{j=1}^{n} v_j \otimes f_{ij}$, so that ϕ is given by $x \mapsto (f_{ij}(x))$. To see that ϕ is an embedding we simply need to show that ϕ^* is surjective. But $\mathcal{O}(GL(V))$ is the algebra generated by the matrix coefficients, with the determinant function inverted. Since the f_{ij} are the pullbacks via ϕ of the matrix coefficients, and we have

$$v_i(x) = \sum_{j=1}^{n} v_j(e) f_{ij}(x)$$

the surjectivity follows from the fact that the v_i generate A. □

Remark 1.5. The previous proposition shows that any affine algebraic group is a closed subgroup of some $GL(V)$. This is why such groups are sometimes called "linear algebraic groups".

Definition 1.6. Let X be a variety and G an affine algebraic variety. An action of G on X is a morphism

$$\mu \colon G \times X \to X$$

such that $\mu(e, x) = x$ for all $x \in X$, and the obvious diagram involving $G \times G \times X$ commutes, *i.e.* we have $\mu(g, \mu(h, x)) = \mu(gh, x)$. (A variety equipped with an action of the group G is known as a G-variety).

A G-variety X is said to be *homogeneous* if the action of G is transitive. If $H < G$ is a closed subgroup of G, then we say that a pointed homogeneous G-variety (Y, y_0) is the *categorical quotient* of G by H if H stabilizes y_0, and for any pointed homogeneous G-space (X, x_0) such H stabilizes x_0 there is a unique G-equivariant morphism $\pi_X \colon Y \to X$ with $\pi_X(y_0) = x_0$. The categorical quotient is clearly unique up to unique isomorphism if it exists.

Arguments in a similar, but more elaborate, style to the previous proposition, establish that the categorical quotient, denoted G/H, exists and is a quasi-projective variety, which is again an affine algebraic group if H is normal. The crucial point in constructing a candidate for G/H is is to find a representation of G containing a line $L \subset \mathbb{P}(V)$ whose stabilizer is exactly H (there is also a subtlety related to the question of separability of morphisms).

Sketch of the construction: Let I be the ideal in A which vanishes on H. Then take a G-stable subspace U of A such that $U \cap I$ generates I as an ideal. Then U gives a representation of G for which the subgroup of G preserving the subspace $W = I \cap U$ is exactly H. Then taking the appropriate exterior power of U we get a representation V of G containing a line L such that $\{g \in G : g(L) = L\} = H$. Then G/H, the categorical quotient is the G-orbit of L in $\mathbb{P}(V)$.

1.1. **Jordan decomposition.** The Jordan normal form theorem for GL_n shows that each $g \in GL_n$ can be written as a product of commuting elements s and u, where s is a diagonalizable element and u is a unipotent element, that is, $(u-1)^N = 0$ for N large. Note that in fact one can write s as a polynomial in g without constant term (this is essentially the Chinese remainder theorem for polynomials). Such a decomposition always exists for elements of an affine algebraic group.

Definition 1.7. Let V be a k-vector space, and let $\alpha \colon V \to V$ be an automorphism. We say that α is *unipotent* if for each $v \in V$ we have $(\alpha - 1)^N(v) = 0$ for sufficiently large N, and that α is semisimple if V has a basis of eigenvectors for α. We say the action of α is *locally finite* if for each vector $v \in V$ the span of $\{\alpha^n(v) : n \in \mathbb{Z}\}$ is finite dimensional. Note any semisimple or unipotent α acts locally finitely.

Lemma 1.8. *If $g \colon V \to V$ is a locally finite automorphism then there are unique automorphisms g_s and g_u such that g_s is semisimple, g_u is unipotent, and $g = g_s g_u = g_u g_s$. Moreover any subspace of V stable under g is stable under g_s and g_u.*

Proof. This follows by reducing to the finite dimensional case. (Note that if W is finite dimensional, and $U \subseteq W$ is a subspace of W, the Jordan decomposition of $g_{|U}$ is the restriction of the Jordan decomposition of g on W). □

Note that Lemma 1.3 shows that for any $g \in G$, the automophism ρ_g^* is locally finite. Hence we will say that $g \in G$ is semisimple or unipotent if ρ_g^* is (or equivalently if λ_g^* is). For $g \in G$, if $g = g_s g_u = g_u g_s$ where g_s is semisimple and g_u is unipotent, then we say (g_s, g_u) is the *Jordan decomposition* of g. Note that if it exists, Lemma 1.8 shows that it is unique. For convenience of notation, from now on we will write $\rho \colon G \to \mathrm{Aut}(A)$ for the representation given by $g \mapsto \rho_g^*$.

Lemma 1.9. *Suppose that $G = GL(V)$, and $g \in G$. Then if $g = g_s g_u$ is the Jordan decomposition of g as an automorphism of V, then g_s is semisimple and g_u is unipotent. In particular, every element of G has a Jordan decomposition.*

Proof. Note that the naive Jordan decomposition is compatible with the operations of tensor product, direct sums and duals of vector spaces (this is an easy exercise). Thus (g_s, g_u) is the Jordan decomposition the action of g on $\mathrm{Sym}(V \otimes V^*)$. Since the

$\mathsf{k}[G]$ is just the localization of this algebra at the determinant function (an eigenvector for the action of g), it follows immediately that $\rho(g_s)$ and $\rho(g_u)$ are the Jordan decomposition of $\rho(g)$. □

Theorem 1.10. *There is a Jordan decomposition for any $g \in G$.*

Proof. Pick an embedding $\phi\colon G \to GL(V)$, and let $B = \mathcal{O}(GL(V))$ be the coordinate algebra of $GL(V)$. Let $I = \ker(\phi^*)$, where $\phi^*\colon B \to A$. Let $\rho\colon GL(V) \to B$ be the representation of $GL(B)$ on B. By definition, $g \in GL(V)$ lies in G if and only if $\varepsilon_g(I) = 0$. It is easy to see that $\varepsilon_g = \varepsilon_e \circ \rho(g)$, hence since $\varepsilon_e(I) = 0$, it follows that if $\rho(g)(I) \subseteq I$, then $g \in G$. But since $\rho(\phi(g))$ preserves I, it follows from the "moreover" part of Lemma 1.8 that $\rho(g_s)$ and $\rho(g_u)$ do also. Hence g_s and g_u lie in $\phi(G)$ as required. □

One can show that the Jordan decomposition is functorial in the sense that if $\phi\colon G \to H$ is a homomorphism of algebraic groups, then

$$\phi(g)_s = \phi(g_s); \qquad \phi(g_u) = \phi(g)_u.$$

Exercise 1.11. Show this.

2. Orbits and the topology of G

We now discuss briefly some of the geometry of G. Recall that if X is a topological space, then a subset Y is *locally closed* if it is open in its closure, or equivalently if it is the intersection of an open and a closed subset of X. A *constructible set* is a finite union of locally closed subsets. A theorem of Chevalley asserts that if $f\colon X \to Y$ is a morphism of varieties, then the image of f is a constructible subset of Y.

Lemma 2.1. *Let G be an affine algebraic group, then G has finitely many smooth connected components. The component containing e, denoted G^0, is a normal subgroup, so that the set of components has a group structure.*

Proof. If $g \in G$, then the map $\lambda_g\colon G \to G$ given by left-multiplication by g is an automorphism of G. Since there is an $x \in G$ which lies in exactly one component if G, the translations λ_g show that this is true for all $x \in G$. Thus the irreducible components of G are disjoint, and hence are the connected components. Let G^0 be the irreducible component of G containing e. Then G^0 is a subgroup, since $m\colon G^0 \times G^0 \to G$ has an irreducible image containing e which therefore lies in G^0, and similarly $\iota(G^0) \subset G^0$. In the same way, by considering the automorphisms $Ad_x\colon G \to G$, given by $g \mapsto xgx^{-1}$, we see that G^0 is in fact normal, and so the connected components of G are just the G^0-cosets.

Finally to see that the components of G are smooth, note that if U is an open dense smooth subvariety of G^0, then $G^0 = \bigcup_{g\in G^0} \lambda_g(U)$, and so G^0, and hence each components of G, is smooth. □

Lemma 2.2. *Let G act on a variety X, and suppose that $x \in X$. Then the orbit of x is a locally closed subset of X. Moreover, if $\phi\colon G \to H$ is a morphism of affine algebraic groups, then $\phi(G)$ is a closed subgroup of H.*

Proof. Let $\mathcal{O}$ be the orbit of $x \in X$. Then $\mathcal{O}$ is the image of G under the morphism given by $g \mapsto g(x)$, and hence it is a constructible subset of X. Thus there exists a subset $U \subset \mathcal{O}$ which is open in the closure $\bar{\mathcal{O}}$. But then $\mathcal{O} = \bigcup_{g\in G} g(U)$ is also open in $\bar{\mathcal{O}}$, and $\mathcal{O}$ is locally closed as required. It is easy to see that $\bar{\mathcal{O}}$ is preserved by the action of G, hence we see that X must contain a closed orbit (take an orbit of minimal dimension, for example).

For the last part, note that G acts on H via ϕ, and moreover the orbits are precisely the cosets of the image $\phi(G)$. It follows that they are all isomorphic. Since we have shown there is a closed orbit for any action, it follows that all the orbits are closed, and in particular, $\phi(G)$ is closed as required. □

Note that the final part of the previous lemma is very much not true if one is working with Lie groups.

Lemma 2.3. *Let G be a connected affine algebraic group.*

1. *Suppose that A is a dense constructible subset of G.Then $G = A.A$.*
2. *Let $\{A_1, A_2, \ldots, A_k\}$ be irreducible affine varieties, and $f_i\colon A_i \to G$ morphisms such that $e \in f_i(A_i)$ for each i ($1 \leq i \leq k$). Then the subgroup H generated by $\{f_i(A_i) : 1 \leq i \leq k\}$ is a closed connected subgroup of G.*

Proof. For the first part, note that if $g \in G$, then $g\iota(A)$ is also a dense constructible subset of A, and so $A \cap g\iota(A) \neq \emptyset$. Thus $G = A.A$.

For the second part, since $e \in f(A_i)$ for all i, we can replace the collection of morphisms $(f_i)_{1\leq i\leq k}$ by the single morphism $f\colon A_1 \times A_2 \times \ldots \times A_k \to G$ given by

$$f(a_1, a_2, \ldots, a_k) = f_1(a_1)f_2(a_2)\ldots f_k(a_k).$$

Thus we may assume that $k = 1$, and write $A = A_1 \times A_2 \times \ldots \times A_k$. Let B be the image of the map $A \times A \to G \times G \to G$ given by

$$(a_1, a_2) \mapsto (f(a_1), f(a_2)) \mapsto f(a_1)f(a_2)^{-1}.$$

Then B is an irreducible constructible subvariety of G containing e, and $B = B^{-1}$. Now H be the union $B \cup B^2 \cup \ldots$. But each B^n is irreducible and constructible, and $B^n \subset B^{n+1}$, thus for dimension reasons there is an $n \geq 1$ such that $\overline{B^n} = \overline{B^{n+1}} = \ldots$ and so $B^m \subset \overline{B^n}$ for all $m \geq n$. Thus we see that $H \subset \overline{B^n}$. But now $\bar{H}$ is a closed subgroup of H, and $B^n \subset \bar{H} \subset \overline{B^n}$, and that H is irreducible (thus connected) and B^n is a dense constructible subset of $\bar{H}$. Thus by the first part, we see that $\bar{H} = B^{2n}$, and so $\bar{H} = B^{2n} \subseteq H$, and $H = \bar{H}$ as required. □

Corollary 2.4. *Let G be a connected affine algebraic group, and let H_1, H_2 be closed subgroups with H_1 connected. Then (H_1, H_2), the subgroup generated by the commutators $[x, y] = xyx^{-1}y^{-1}$, $x \in H_1, y \in H_2$ is a closed connected subgroup.*

Proof. Let $C_1, C_2, \ldots, C_k$ be the components of H_2, and let $f_i\colon H_1 \times C_i \to G$ be given by $f(x, y) = [x, y]$. Then apply the previous lemma. □

3. TORI, SOLVABLE GROUPS AND UNIPOTENT GROUPS.

We define some basic classes of affine algebraic groups. The first of these is the class of abelian affine algebraic groups. A *torus* is an affine algebraic group which is isomorphic to a product of $\mathbb{G}_m$s. It is known that closed connected subgroups and quotients of tori are again tori. The following lemma shows that in the abelian case, the Jordan decomposition gives a decomposition of the group.

Lemma 3.1. *Let G be an connected abelian linear algebraic group. Then if G_s and G_u denote the set of semisimple (respectively unipotent) elements of G, we have $G = G_s \times G_u$, a product of linear algebraic group. Moreover G_s is a torus.*

Proof. Since G is abelian, it is easy to see that G_s and G_u are subgroups. The map $G_s \times G_u \to G$ is a bijective morphism of varieties, so one just needs to show that its inverse is a morphism of varieties also. To do this, embed G in some $GL_n(\mathsf{k})$. Since an abelian group is solvable, we may assume the image lies in T_n the group of upper triangular matrices. Then one sees that $G_s = G \cap D_n$, where D_n is the diagonal torus, and $G_u = G \cap U_n$. It is then easy to see that the map $G \to G_s$ is a morphism, and so since $g_u = gg_s^{-1}$, the map $G \to G_u$ is also. The moreover part follows from the fact that a closed connected subgroup of a torus is a torus. □

It can be shown that the only one dimensional abelian linear algebraic groups are $\mathbb{G}_m$, the multiplicative group, and $\mathbb{G}_a$, the additive group. Note that it is easy to see that a connected affine algebraic group which consists only of semisimple elements must be a torus.

Lemma 3.2. *Any action of a connected algebraic group on a torus is trivial.*

Proof. This follows from the fact that the elements of finite order are dense in a torus, and that there are only finitely many of any given order. □

Definition 3.3. Given any affine algebraic group G, we may consider the derived subgroups $D^i(G)$, where $D^{i+1}(G) = D(D^i(G))$, and $D(G) = [G, G]$ the (normal) subgroup generated by commutators (note that these subgroups are automatically affine algebraic groups). A group is said to be *solvable* if $D^i(G) = \{e\}$ for some i.

The first result on connected solvable groups is the theorem of Lie-Kolchin, which shows that the irreducible representations of such a group are all one-dimensional.

Proposition 3.4. *(Lie-Kolchin theorem) Let G be a connected solvable group, and let $\rho\colon G \to GL(V)$ be a representation of G. Then there is a line $L \subset V$ preserved by G, i.e. V contains a one-dimensional subrepresentation.*

Proof. We use induction on $\dim(G)$. Clearly we may assume that V is an irreducible G-representation. Since G is connected, and $D(G)$ is a connected subgroup, and G is solvable, so that $G \neq D(G)$, the derived group $D(G)$ must have smaller dimension. Hence there is a line L in V which is stabilized by $D(G)$. Let V' be the sum of all such lines. Note that if L is such a line, then since $D(G)$ is a normal subgroup, $g(L)$ is another such line for all $g \in G$. It follows that V' is preserved by G, and hence by the irreducibility of V, we have $V = V'$. Thus the action of $D(G)$ on V is diagonalizable – that is, we may find a decomposition of V into a direct sum of lines $L_1 \oplus L_2 \ldots \oplus L_n$, where $D(G)$ preserves each of the lines L_i $(1 \leq i \leq n)$.

Now fix $g_1 \in D(G)$ and let $g \in G$. Then $\rho(gg_1g^{-1}) = \rho(g)\rho(g_1)\rho(g)^{-1} \in \rho(D(G))$, and moreover the eigenvalues of $\rho(gg_1g^{-1})$ are the same as those of $\rho(g_1)$, so that, since $\rho(g_1)$ is diagonalizable, the map $g \mapsto \rho(gg_1g^{-1})$ is a morphism of varieties from G to a finite set. Since G is connected, this map must be constant, and hence equal to $\rho(g_1)$. Thus we find that $\rho(g)\rho(g_1) = \rho(g_1)\rho(g)$, for all $g \in G$ and $g_1 \in D(G)$.

Let $\chi\colon D(G) \to \mathsf{k}^\times$ be the representation of $D(G)$ afforded by L_1. Then since $\rho(g)$ commutes with $\rho(D(G))$ it follows that $g(L_1)$ also affords χ. Since V is irreducible it is the span of the lines $g(L)$, and so as a $D(G)$ representation it is isomorphic to a direct sum of n copies of χ. Since each $g_1 \in D(G)$ is a product of commutator in the elements $\{\rho(g) : g \in G\}$, we see that $\det(\rho(g_1)) = 1$, and so $\chi(g_1)^n = 1$ for all $g_1 \in D(G)$. But then $\chi\colon G \to \mathsf{k}^\times$ is a morphism to a finite set, so that since $D(G)$ is connected, it must be constant. Thus $D(G)$ acts trivially on V.

Finally, it follows that the image of $\rho(G)$ is abelian, and hence V must be one-dimensional and we are done. □

Definition 3.5. A *unipotent group* is an affine algebraic group each of whose elements is unipotent.

It can be shown that a unipotent group is solvable, indeed nilpotent. In fact we have:

Proposition 3.6. *Let U be a unipotent group, and suppose that $\sigma\colon U \to GL(V)$ is a representation of U. Then there is a basis of V with respect to which the matrices of the elements of $\sigma(U)$ are all upper triangular.*

Proof. Clearly it is enough to show that there is a line L in V which is preserved by U, as then we may use induction on the dimension of V. To see that there is a fixed line, we may assume that V is irreducible as a U-representation. Let $A \subset \text{End}(V)$ be the span of the elements $\{\sigma(g) : g \in U\}$. Since V is an irreducible U-representation, it is a simple A-module. But since A is a finite dimensional algebra, by Burnside's theorem, it follows that $A = \text{End}(V)$. Hence we may find elements $\{g_i : 1 \leq i \leq n^2\}$ (where $n = \dim(V)$), such that $\{\sigma(g_i) : 1 \leq i \leq n^2\}$ is a basis for $\text{End}(V)$.

Now consider the function $\chi\colon U \to \mathsf{k}^{n^2}$ given by $\chi = (\chi_i)_{1 \leq i \leq n^2}$ where

$$\chi_i(g) = \text{tr}(\sigma(gg_i)) \qquad (1 \leq i \leq n^2).$$

Then if $\chi(g) = \chi(g')$ we have $\text{tr}((\sigma(g) - \sigma(g'))(\sigma(g_i)) = 0$ for all i, and since the g_i span $\text{End}(V)$ it follows that $\sigma(g) = \sigma(g')$ (since $\text{tr}(ST) = 0$ for all $T \in \text{End}(V)$ if and only if $S = 0$). Thus χ is injective. But by assumption, gg_i is unipotent for all g, and hence $\chi(g) = (n, n, \dots, n)$ for all $g \in U$. It follows that $\sigma(U) = \{\text{Id}\}$, and we are done. □

Next we state the main structure theorem for solvable groups.

Theorem 3.7. *Let G be a connected solvable algebraic group. Then*

1. *The set G_u of unipotent elements in G is a closed connected normal subgroup.*
2. *The maximal tori of G are all conjugate, and for any such torus T, the group G is the semidirect product of T with G_u.*
3. *Every semisimple element of G lies in a maximal torus.*
4. *The centralizer of a subgroup $H < G$ all of whose element are semisimple is connected.*

Proof. (*sketch*): Embed G into $GL(V)$ for some V. By the Lie-Kolchin theorem, we can find a basis $\{v_i\}_{1 \leq i \leq n}$ of V such that the image of G lies in group of upper triangular matrices U_n (with respect to this basis). Then the unipotent elements will be exactly $G \cap U_n$. This gives an exact sequence

$$1 \to G_u \to G \to D \to 1,$$

where D is the image of G in T_n/U_n, a torus. The difficulty in the proof of the second part is to show this sequence splits: one shows it first for the abelian and nilpotent cases (where there is just one maximal torus), and then by induction on dimension in the general case. The third statement is proved in the course of proving the second. For the last statement, use induction on $\dim(G)$. If H is cental the result is immediate, since G is connected. Otherwise picking an $s \in H \backslash Z(G)$ so that we have $\dim(C_G(s)) < \dim(G)$. Since H consists of semisimple elements, and G/G_u is abelian, H must be abelian, so that $H < C_G(s)$. If we know that $C_G(s)$ is connected then we are done by induction. Since s lies in a maximal torus, it follows that $C_G(s)$ is the semidirect product of T with $C_{G_u}(s)$. One the shows that $C_{G_u}(s)$ is connected directly, using the fact that $C_{G_u}(s)$ is unipotent. (In characteristic zero, any unipotent group is connected, so this is obvious). □

4. BOREL SUBGROUPS

The primary strategy for the study of the structure of a general affine algebraic group is to reduce to the theory of connected solvable groups. In this respect the following theorem, due to Borel, is crucial.

Theorem 4.1. *(Borel) Let G be a connected solvable affine algebraic group acting on a nonempty projective variety X. Then G has a fixed point.*

We will not prove this, but rather a weaker result which is as good for almost all purposes.

Proposition 4.2. *(Sweedler): Let G be a connected solvable group, and let V be a G-representations. Suppose that X is a nonempty closed subvariety of $\mathbb{P}(V)$ which is G-stable. Then X contains a fixed point of G.*

Proof. We use induction on $\dim(X)$. Clearly we may assume that X is irreducible. Let I be the homogeneous ideal corresponding to X in Sym(V^*). Then $I \cap V^* \neq V^*$, since X is nonempty, and so $W = V^*/(I \cap V^*)$ is a nonzero vector space. Moreover, G acts on W since it preserves I and V^* (the action on V^* is the contragredient one). By the Lie-Kolchin theorem, there is a fixed line for the G-action in W. Let v be a nonzero element of this line, and let f be a representative of v in V^*. We claim that $X' = \{x \in X : f(x) = 0\}$ is a proper subvariety of X which is preserved by G. Indeed it is clear by the choice of f that $f \notin I$, hence $X' \neq X$. Now by construction, there is a homomoprhism $\chi \colon G \to \mathsf{k}^\times$ such that $g(f) = \chi(g)f + f'$ where $f' \in I \cap V^*$. Thus if $x \in X'$ we have $f(g.x) = \chi(g^{-1})f(x) + f'(x) = 0$, so that X' is G-stable.

Since X is irreducible, we see that $\dim(X') < \dim(X)$, and so by induction, G has a fixed point on X' as required. □

Remark 4.3. If $\phi \colon X \to Y$ is a bijective morphism of varieties, and X is affine, Y is projective (and, say, normal), is it necessarily the case that X and Y are isomorphic? (They must be if the varieties are homogeneous spaces for some algebraic group, and the map is equivariant).

Definition 4.4. If G be an affine algebraic group, a *Borel subgroup* of G is a maximal closed connected solvable subgroup.

Proposition 4.5. *Let B be a Borel subgroup of G. Then we have*

(1) *The variety G/B is projective.*
(2) *All Borel subgroups are conjugate.*

Proof. Let B_0 be a Borel subgroup of maximal dimension. Then, as in Remark 1.5 we may find a representation (V, σ) of G such that there is a line $V_1 \subset V$ with

$$B_0 = \{g \in G : \sigma(g)(V_1) \subset V_1\}.$$

Considering V/V_1 as a B_0-representation, and applying the Lie-Kolchin theorem, we may find a line preserved by B_0. Continuing in this way we can obtain a *flag* in V: a sequence of nested subspaces

$$\mathfrak{f} = (O \subset V_1 \subset V_2 \subset \ldots \subset V_n = V),$$

where $\dim(V_i) = i$, and stabilizer of $\mathfrak{f}$ in G is exactly B_0. Now the set of all flags in V is a projective variety, and

The stablizer of any flag is clearly a solvable subgroup, since it is filtered by the kernel of σ, and the image of the stabilizer in $GL(V)$, and each of these groups is solvable (the former because it is a subgroup of B_0 and the latter because the group of upper triangular matrices is). It follows from the maximality of the dimension of B_0 that the orbit of B_0 is of minimal dimension, and hence closed in the variety of all flags. Since this last variety is projective, it follows that G/B_0 is projective.

Next let B be any other Borel subgroup, and consider the action of B on G/B_0. Using the Borel fixed point theorem, there is an $x \in B$ such that $BxB_0 = xB_0$. Hence $B \subset xB_0x^{-1}$. By maximality of B, we must have $B = xB_0x^{-1}$ as required. Moreover it is thus clear that G/B is projective for any Borel subgroup. □

Definition 4.6. A *parabolic subgroup* of an affine algebraic group G is a subgroup P which contains a Borel subgroup. By the Borel fixed point theorem, this is equivalent to the requirement that G/P is a projective variety.

Remark 4.7. Clearly every connected solvable subgroup S of G is contained in a Borel subgroup. Is the same thing true if we remove the condition that S is connected?

Example 4.8. Consider the case $G = GL(V)$. Then we claim that the Borel subgroups are the stabilizers of complete flags in V – that is, they are the subgroups conjugate to the subgroup of upper triangular matrices. This can be checked in a similar fashion to the proof of the previous proposition – the one essential calculation is to check that the group of upper triangular matrices is solvable.

This result immediately implies the following:

Corollary 4.9. *Let G be an affine algebraic group. Then*

1. *The maximal tori in G are all conjugate.*
2. *G acts transitively on the set of pairs (T, B) where T is a maximal torus in B, a Borel subgroup.*
3. *The maximal unipotent subgroups of G are all conjugate.*

Proof. Both tori and unipotent groups are solvable, so the corollary follows from the conjugacy of Borel subgroups and the structure theorem for solvable groups Theorem 3.7. □

Finally we record some results whose proof we only sketch. A *Cartan* subgroup C of an affine algebraic group G is a subgroup of the form $Z_G(T)^0$, where T is a maximal torus of G. It follows from Corollary 4.9 that T is the unique maximal torus of C. It can be shown that this implies C is a nilpotent group, and so C lies in a Borel subgroup.

Exercise 4.10. Let G be a linear algebraic group, and S a torus in G. Then for a generic $s \in S$, we have $C_G(S) = C_G(s)$.

For the next theorem we also need the fact that for a maximal torus T, it may also be shown that for generic $t \in T$ we have $C_G(t) = C_G(T)$.

Theorem 4.11. *Let G be a connected linear algebraic group. Then we have:*

(1) *Let T be a maximal torus, and C the associated Cartan subgroup, then the set $\bigcup_{g \in G} gCg^{-1}$ contains an open dense subset of G.*
(2) *Every element of G lies in a Borel subgroup, i.e. if B is any Borel subgroup, then $G = \bigcup_{g \in G} gBg^{-1}$.*
(3) *Every semisimple element lies in a maximal torus, i.e. we have $G_s = \bigcup_{g \in G} gTg^{-1}$.*
(4) *It $S \subset G$ is a torus, then $C_G(S)$ is connected.*
(5) $N_G(B) = B$.

Proof. Consider the set $Z_C = \{(xC, g) : g = xyx^{-1} \text{ for some } y \in C\}$. Then we have obvious maps $p_1 \colon Z_C \to G/H$ and $p_2 \colon Z_C \to G$. Clearly p_2 is surjective, and its fibers are the conjugates of H. In particular, Z is connected of dimension $\dim(G/C) + \dim(C) = \dim(G)$. Since $X = p_2(Z_C)$, it is a constructible subset of G, so to prove it is dense in G, we just need to show that it has dimension $\dim(G)$. But this follows if we can show some fiber of p_2 is finite, since then $\dim(p_2(Z_C)) = \dim(Z) = \dim(G)$. Picking $t \in T < G$ as in the previous exercise gives us exactly such a fiber: indeed the fiber $p_2^{-1}(t)$ is the set xC such that $t \in xCx^{-1}$, that is such that $x^{-1}tx \in C$. But then $x^{-1}tx \in C_s = T$, and so $T < C_G(x^{-1}tx)^0 = x^{-1}C_G(t)^0x = x^{-1}Cx$. But then T is the unique maximal torus of $x^{-1}Cx$, so that $x^{-1}Tx = T$, that is, $x \in N_G(T)$. But by the rigidity of tori $C = N_G(T)^0$, so that there are only finitely many choices for xC as required.

For the second part, let $Z_B = \{(gB, x) \in G/B \times G : x \in gBg^{-1}\}$, a closed subvariety of $G/B \times G$. Then notice that the set $\bigcup_{g \in G} gBg^{-1}$ is the image of Z_B under the second projection $p_2 \colon G/B \times G \to G$. Since G/B is a projective variety, it follows that the image of Z_B is closed. Now since we may assume that B contains C it follows that $p_2(Z)$ must be all of G.

The third part follows from the corresponding result for solvable groups and the second part. To see that $C_G(S)$ is connected, suppose that $x \in N_G(S)$. We claim that there is a Borel subgroup B containing S and x. This proves the result, since then $x \in C_B(S)$ which is connected by the corresponding result for solvable groups. To see that such a Borel exists, pick a Borel B_0 containing x. Then S acts on the projective variety G/B_0, and moreover since it commutes with x, it acts on the closed subvariety of x-fixed points in G/B_0. Since S is solvable, it has a fixed point on this subvariety, and this corresponds to a Borel containing both S and x.

To see that $B = N_G(B)^0$, note that by the conjugacy of Borel subgroups, B is the unique Borel subgroup of $N_G(B)$. By the second part it follows that $B = N_G(B)^0$. To see that $N_G(B)$ is connected one uses induction on the dimension of G, and the fourth part, to find a group of smaller dimension. □

Remark 4.12. We give a proof of the first property for $GL(V)$: In this case, $T = C_G(T)$, for any maximal torus, and since an endomorphism $\alpha \colon V \to V$ lies in a maximal torus if and only if it is diagonalizable, we must only show that the set of diagonalizable elements is contains an open dense subset of $GL(V)$. But α is diagonalizable with distinct eigenvalues if its characteristic polynomial χ has no repeated roots, that is, if χ and its derivative $d\chi$ are relatively prime. Since this can be expressed as the nonvanishing of the resultant of χ and $d\chi$, it follows that the set of diagonalizable elements contains a principal open subset of End(V), and so we see that the semisimple elements of $GL(V)$ are dense in $GL(V)$.

It is also worth noting that the conjugates of a Cartan subgroup is not necessarily open – in the case of SL_2, it is easy to see that a Cartan subgroup is just a maximal torus, and then the union of its conjugates is the set of semisimple elements. These are the union of the (open) locus of semisimple elements with distinct eigenvalues, and the two points $\{\pm I\}$.

Remark 4.13. This theorem shows that there is a *canonical* torus attached to a connected algebraic group: indeed we know from the structure theorem for solvable algebraic groups that if B is a Borel subgroup, then $B/[B,B]$ is a torus. Moreover, if B' is another Borel subgroup, then picking any $g \in G$ with $B' = gBg^{-1}$ we get a canonical isomorphism $B/[B,B] \to B'/[B',B']$.

5. TORI AND REDUCTIVE GROUPS

If G is an affine algebraic group, then we let $R(G)$, the *radical* of G to be the maximal closed connected solvable normal subgroup, and similarly $R_u(G)$, the *unipotent radical* of G to be the maximal closed connected unipotent normal subgroup (so that $R_u(G) \subseteq R(G)$). (Here one shows that there is a *unique* maximal such subgroup). A connected algebraic group is said to be *semisimple* if $R(G) = \{e\}$, and *reductive* if $R_u(G) = \{e\}$. Note that since $R(G)$ is solvable, $R(G) = S \ltimes R(G)_u$, where S is a maximal torus of $R(G)$, and $R(G)_u$ is the subgroup of $R(G)$ consisting of the unipotent elements. Thus clearly $R(G)_u$ is a closed connected unipotent normal subgroup of G and so $R(G)_u \subset R_u(G)$. On the other hand, $R_u(G)$ must lie in $R(G)$, so that $R_u(G) \subset R(G)_u$ (since it consists of unipotent elements), and so in fact $R_u(G) = R(G)_u$. Thus for a reductive group G, the radical consists entirely of semisimple elements, and so is a torus.

Lemma 5.1. *If G is a reductive group, the $R(G)$ is $Z(G)^0$, the identity component of the center of G. Moreover the derived group $D(G)$ of G has finite intersection with $R(G)$.*

Proof. Since $R(G)_u$ is trivial, it follows that $R(G)$ is a torus. We have $N_G(S)^0 = C_G(S)$ for any torus S, thus $R(G)$, being connected, must lie in $Z(G)^0$. On the other hand $Z(G)^0$ is closed connected and normal, so certainly it lies in $R(G)$.

To see that the derived group of G is semisimple, embed G in some $GL(V)$, and write V as a direct sum of its isotypic components as a $Z(G)$-representation. Then $Z(G) \cap D(G)$ lies in the center of the corresponding product of special linear groups, and hence is finite. Now $R(D(G))$ lies in $R(G)$ (since we have shown $R(D(G))$ is a characteristic subgroup of $D(G)$), and so it lies in $Z(G) \cap D(G)$. Since it is connected it must be trivial, and $D(G)$ is semisimple as required. □

Matrix groups like GL_n, $\mathrm{Sp}(2n)$ and $\mathrm{O}(n)$ are all examples of reductive groups. Even if one is primarily interested in simple affine algebraic groups, in order to understand their structure one is inevitably led to reductive groups.

Basic properties of reductive groups are the following:

Proposition 5.2. *Suppose that G is a algebraic group. Then we have*

(1) *$R_u(G)$ is the unipotent radical of the intersection of the all Borel subgroups containing a given maximal torus.*

(2) *The centralizer of a torus in a connected reductive group is connected and reductive.*
(3) *In a connected reductive algebraic group, every maximal torus is equal to its centralizer (and so Cartan subgroups are just maximal tori).*

Definition 5.3. A *character* of a torus T is a homomorphism $\chi\colon T \to \mathbb{G}_m$. The set of all characters of T is denoted $X(T)$. It is clearly an abelian group under multiplication. A *cocharacter* of T is a homomorphism $\nu\colon \mathbb{G}_m \to G$. The set of cocharacters of T is denoted $Y(T)$. It is also an Abelian group under multiplication.

A *one-parameter subgroup* of G is a homomorphism from a one-dimensional affine algebraic group to G. Thus cocharacters are examples of one-parameter subgroups.

Since $X(\mathbb{G}_m) = \mathbb{Z}$, (the only characters are given by $z \mapsto z^n$ for some n), we see that in general $X(T)$ is isomorphic to $\mathbb{Z}^d$, where T is isomorphic to a product of d copies of $\mathbb{G}_m$. Similarly, $Y(T)$ is isomorphic to $\mathbb{Z}^d$, with $(n_1, n_2, \ldots, n_d)$ corresponding to the map $\mathbb{G}_m \to \mathbb{G}_m^d$ given by $z \mapsto (z^{n_1}, \ldots, z^{n_d})$. There is a natural pairing

$$Y(T) \times X(T) \to \mathbb{Z}; \qquad \langle \nu, \chi \rangle = \chi \circ \nu \in \mathrm{Hom}(\mathbb{G}_m, \mathbb{G}_m) \cong \mathbb{Z}.$$

(the last isomorphism has already been used; note that it is canonical).

Lemma 5.4. *The map $\eta \otimes a \mapsto \eta(a)$ from $Y(T) \otimes_{\mathbb{Z}} \mathsf{k}^\times \to T$ is an isomorphism of algebraic groups.*

Proof. Picking dual bases of $X(T)$ and $Y(T)$, say $(v_i)_{1 \leq i \leq n}$ and $(w_i)_{1 \leq i \leq n}$ we can define a map $T \to Y(T) \otimes \mathsf{k}$ by $t \mapsto \sum_{i=1}^n w_i \otimes v_i(t)$. This is an inverse to the map defined in the statement of the lemma, as one can check using the fact that $\mathsf{k}[T]$ is the group algebra of $X(T)$, so that $\bigcap_{\chi \in X(T)} \ker(\chi) = \{1\}$. $\square$

We have a sort of Galois theory for tori: Suppose that $S \subset T$ is a subtorus of T. Then we set $S^\perp = \{\chi \in X(T) : \chi(s) = 1, \forall s \in S\}$. In positive characteristic we have. Similiarly, given a subgroup $A \subset X(T)$ we can define $A^\perp = \{t \in T : \chi(t) = 1, \forall \chi \in A\}$. Then if $\mathrm{char}(\mathsf{k}) = p > 0$, we have

$$A^{\perp\perp}/A = p\text{-torsion subgroup of } X(T)/A.$$

(the p-torsion arises because $x \mapsto x^{p^n}$ is an automorphism of k). The classification of tori is easy: up to isomorphism, tori as classified by the rank of the abelian group $X(T)$. In fact, one can show that X yields a functor which gives an equivalence of categories between the category of k-tori and the category of p-torsion-free finitely generated $\mathbb{Z}$-modules. The idea of the next section is to show that reductive groups can be classified by slightly more elaborate combinatorial data.

6. Classification of reductive algebraic groups

Reductive algebraic groups were completely classified by Chevalley. Remarkably the answer turns out not to depend on the characteristic of the base field. To describe the classification, we need the notion of a *root system*, and in fact a slightly more elaborate notion: that of a root datum. We prove very few of the results that we state in this section.

Definition 6.1. A *root system* is the data of a finite dimensional real vector space V, and a finite subset Φ of nonzero vectors such that

(1) $\mathrm{span}\langle\Phi\rangle = V$.
(2) For each $\alpha \in \Phi$ there is an $\check{\alpha} \in V^*$ such that $\langle \alpha, \check{\alpha}\rangle = 2$, and such that Φ is stable under the reflection $s_\alpha \colon V \to V$ given by $v \mapsto v - \langle v, \check{\alpha}\rangle\alpha$.

Clearly the set $\{\check{\alpha} \in V^*\}$ form another root system, the are called the *coroots*. If we equip V with a scalar product, then we may identify V and V^*, and in this case $\check{\alpha}$ becomes identified with $2\alpha/(\alpha,\alpha)$. Note that the second axiom implies that $-\alpha \in \Phi$ if $\alpha \in \Phi$. Moreover, since Φ is finite and spans V, the subgroup of $\mathrm{GL}(V)$ generated by the s_α is finite. This group, W, is called the *Weyl group* of the root system. There is a natural notion of an irreducible root system. A root system is said to be *reduced* if $2\alpha \notin \Phi$ whenever $\alpha \in \Phi$.

Given a root system (V, Φ), and a functional $L \colon V \to \mathbb{R}$, we say L is nondegenerate if L does not vanish on any root. Then we say a root is positive if $L(\alpha) > 0$ and negative if $L(\alpha) < 0$. A positive root is simple if it cannot be expressed as the sum of other positive root. We have the following result:

Lemma 6.2. *The simple roots form a basis of V, and every root can be written as a linear combination of simple roots where all the nonzero coefficients have the same sign.*

It can be shown that the sets of simple roots are all conjugate under the action of the Weyl group W. Any choice of simple roots gives a presentation of the Weyl group:

Lemma 6.3. *If Π is a set of simple roots then we have*

$$W = \langle s_\alpha : \alpha \in \Pi | \quad s_\alpha^2 = (s_\alpha s_\beta)^{m(\alpha,\beta)} = 1\rangle$$

where $m_{\alpha,\beta}$ is the order of the product $s_\alpha s_\beta$.

Thus if $S = \{s_\alpha\}_{\alpha \in Pi}$ then (W, S) is a *Coxeter system*. Thus there is a *length function* $l \colon W \to \mathbb{N}$, where $l(w)$ is the length of the shortest expression for w in terms of the generating set $\{s_\alpha\}_{\alpha\in\Pi}$. An expression for w in the s_α of length $l(w)$ is called a *reduced expression*. Basic properties of the length function are as follows:

Lemma 6.4. (1) *$l(w)$ is the number of positive roots which are sent to negative roots by w.*
(2) *(exchange condition): If $w = s_1 s_2 \dots s_{l(w)}$ is a reduced expression for w, and $l(s_\alpha w) < l(w)$, then for some i between 1 and $l(w)$ we have*

$$s_\alpha w = s_1 s_2 \dots s_{i-1} s_{i+1} \dots s_{l(w)}.$$

Note that since $s_\alpha^2 = 1$, the second part of the lemma shows that

$$w = s_\alpha s_1 s_2 \dots s_{i-1} s_i \dots s_{l(w)},$$

that is, we can exchange s_α for some s_i to obtain a new reduced expression for w (hence the name "exchange condition").

The explicit classification of root systems which lie in some lattice in V is well known – one gets four infinite families A_n, B_n, C_n, D_n, and five "exceptional cases" G_2, F_4, E_6, E_7, E_8. In these cases the roots are all *integral* combinations of simple roots (*i.e.* the simple roots are a basis for the lattice generated by the roots).

To understand the structure of reductive algebraic groups, we use one-parameter subgroups.

Theorem 6.5. *Fix a maximal torus in G, a connected reductive algebraic group.*

(1) *The minimal nontrivial closed unipotent subgroups U of G normalized by T are isomorphic to $\mathbb{G}_a$, thus the conjugation action of G on U define a character α of T.*
(2) *The characters so obtained form a root system in the subspace $X(T) \otimes_{\mathbb{Z}} \mathbb{R}$ which they span. The Weyl group $N_G(T)/C_G(T) = N_G(T)/T$ acts in $X(T) \otimes_{\mathbb{Z}} \mathbb{R}$ in the obvious way, and this gives an isomorphism between W and the Weyl group of this root system.*
(3) *G is generated by T and the subgroups U_α ($\alpha \in \Phi$), where U_α is the unipotent subgroup corresponding to $\alpha \in \Phi$.*
(4) *If $\alpha \neq -\beta$ are roots, then the subgroup generated by U_α and U_β lies in the product $\prod_\gamma U_\gamma$ where γ runs over the roots of the form $a\alpha + b\beta$, where a and b are positive integers.*
(5) *The Borel subgroups containing T are in bijection with the sets of simple roots in Φ, the correspondence is given by $B = T \ltimes \prod_{\alpha \in \Phi^+} U_\alpha$.*

Proof. (*just kidding*): To prove this theorem requires a reasonable amount of effort. An important notion is that of a *singular* torus: these are tori in T of codimension 1 whose centralizer is larger than T itself. These centralizers are reductive groups whose derived subgroup is of rank 1 (*i.e.* a maximal torus has rank 1). One then makes a study of such groups explicitly (they are all related to SL_2). The U_α are the maximal connected unipotent subgroups of these centralizers. □

In fact one can show that any closed unipotent subgroup of a connected reductive group G which is normalized by a maximal torus T is isomorphic (as a variety) to the product of the U_α it contains. The theorem shows that the root system given by Φ controls much of the structure of G. Moreover, if $\phi\colon \mathrm{SL}_2 \to G$ is the homomorphism corresponding to a root $\alpha \in \Phi$, then the image of $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ in W is the reflection s_α corresponding to α in $X(T) \otimes_{\mathbb{Z}} \mathbb{R}$. A consequence of this is that $s_\alpha U_\beta s_\alpha = U_{s_\alpha(\beta)}$.

Given a root $\alpha \in \Phi$, there is a homomorphism $\phi\colon SL_2 \to G$ whose image is exactly the subgroup generated by U_α and $U_{-\alpha}$. It is unique up to composition with conjugation by a diagonal element of SL_2, so that $\alpha \in \Phi$ determines a unique homomorphism from $\mathbb{G}_m$ (thought of as the the diagonal matrices in SL_2) to T. Under the pairing $Y(T) \times X(T) \to \mathbb{Z}$ this homomorphism can be identified with the coroot $\check{\alpha}$. This set of cocharacters is denoted $\check{\Phi}$.

We have shown that if T is a maximal torus in G, T determines the datum $(X(T), Y(T), \Phi, \check{\Phi})$. Since all maximal tori in G are conjugate, it is straightforward to show that this datum is independent of the choice of T.

Theorem 6.6. *(Chevalley): Let G be a connected reductive algebraic group. The datum $(X(T), Y(T), \Phi, \check{\Phi})$ determines G up to isomorphism, and any possible root datum arises as the root datum of some reductive group G.*

Remark 6.7. The statement splits into two parts: an existence result and a isomorphism theorem (for any two groups with isomorphic data, one can construct an isomorphism between them). Both theorems are presented in [S], and a short proof of the isomorphism theorem can be found in [St99].

Exercise 6.8. Work all of this out explicitly for at least GL_n, or better $\mathrm{Sp}(V)$ the symplectic group.

7. BN PAIRS AND THE BRUHAT DECOMPOSITION

A surprising amount of the structure of a reductive group can be captured in the following purely algebraic definition.

Definition 7.1. A BN-pair in a group G is a datum (B, N, S) consisting of subgroups B and N, such that $B \cap N$ is normal in N, and a set of involutions S in the quotient group $W = N/B \cap N$. The datum satisfies the following properties:

1. The set $B \cup N$ generates G.
2. The set S generates W.
3. For any $s \in S$, and $w \in W$ we have $sBw \subset BwB \cup BswB$.
4. For any $s \in S$ we have $sBs \not\subset B$.

Note that the sets sBw *etc.* do not depend on the choice of a lift for the elements of W. The group W is called the Weyl group of the BN-pair. It follows from these properties that (W, S) is in fact a Coxeter system, and moreover the third property can be refined to

$$BsBwB = \begin{cases} BswB & \text{if } l(sw) = l(w) + 1, \\ BwB \cup BswB & \text{if } l(sw) = l(w) - 1 \end{cases} \tag{1}$$

For the cases which interest us, these consequences of the definition will be evident, so we do not prove them here.

Theorem 7.2. *Let G be a connected reductive group. Then if B is a Borel subgroup and T is a maximal torus in B, the pair of subgroups B and $N = N_G(T)$ is a BN-pair for G, where the set S is the set $\{s_\alpha : \alpha \in \Pi\} \subset W$, where Π is the set of simple roots given by the root subgroups of B.*

Proof. We must first show that $B \cap N = T$, as this will establish that W is a Coxeter system with generators S as claimed, and that $B \cap N$ is normal in N. To see this it is enough to show that $R_u(B) \cap N_G(T) = \{e\}$. But if $x \in B$ lies in this intersection, then clearly the commutator xtx^1t^{-1} lies in T, and also in $[B, B]$. But the intersection $T \cap [B, B] = \{e\}$, and so we find that in fact $x \in C_G(T)$. Since G is reductive, this implies that $x \in T$ as required.

To see that B and N generate G, note that by Theorem 6.5 we know that G is generated by T and the root subgroups. Let H be the subgroup generated by B and N. For a root $\alpha \in \Phi$, either $U_\alpha \subset B$, of $U_{-\alpha} \subset B$. The former case is immediate while in the latter we have $s_\alpha U_\alpha s_\alpha = U_{-\alpha}$. This last equation also shows the fourth property.

It remains to show the third property, note that we have $B = T(\prod_{\beta \in \Phi^+ - \{\alpha\}} U_\beta)U_\alpha$. Then since $l(s_\alpha) = 1$ and the length of an element is the number of positive roots sent to negative roots, it follows that

$$s_\alpha Bw = T.(\prod_{\beta \in \Phi^+ - \{\alpha\}} U_\beta).s_\alpha U_\alpha w \subset Bs_\alpha U_\alpha w$$

Hence it is enough to show that $s_\alpha U_\alpha w \subset BwB \cup Bs_\alpha wB$ for each $\alpha \in \Phi^+$. But now $w^{-1}U_\alpha w = U_{w^{-1}(\alpha)}$, so that $s_\alpha U_\alpha w = s_\alpha w U_{w^{-1}(\alpha)}$. Thus if $w^{-1}(\alpha) \in \Phi^+$, then clearly $s_\alpha U_\alpha w \subset Bs_\alpha wB$. It is easy to check by a calculation in SL_2 that

$$U_{-\alpha} = s_\alpha U_\alpha s_\alpha \subset Bs_\alpha U_\alpha \cup TU_\alpha,$$

thus if $w^{-1}(\alpha) \notin \Phi^+$, so that $w^{-1}(-\alpha) \in \Phi^+$, and we have

$$\begin{aligned} s_\alpha U_\alpha w = U_{-\alpha} s_\alpha w &\subset B s_\alpha U_\alpha s_\alpha w \cup T U_\alpha s_\alpha w \\ &= B w U_{-w(\alpha)} \cup T U_\alpha s_\alpha w. \end{aligned}$$

and we are done.

□

One of the most important consequences of the existence of a BN-pair is the *Bruhat decomposition*. We record the first version of this in the following proposition.

Proposition 7.3. *Let G be a group with a BN-pair. Then we have*

$$G = \bigsqcup_{w \in W} BwB.$$

Proof. Note first that, as above, although w lies in a subquotient of G, the double cosets BwB are unambiguous, that is, they do not depend on the choice of a lift for an element of W. Now since B and N generate G, clearly any element $g \in G$ can be written as a product in the form $b_1 n_1 b_2 n_2 \dots b_k n_k$ for some $b_i \in B, n_i \in N$. Clearly using property (3) of a BN-pair and induction, we may rewrite this expression in the form $b_1 n b_2$ where $n \in N$ and $b_1, b_2 \in B$. Thus we are reduced to showing that the double cosets are all distinct. This we show by induction. Suppose that we know $BwB \neq Bw'B$ for all w, with $l(w) < l(w')$ and $l(w) < n$ say (the case $l(w) = 0$ is clear, since no nontrivial element of W has a lift in B). Then if $l(w) = n$ and $BwB = Bw'B$, we may pick an $s \in S$ such that $l(sw) < l(w)$. It follows the third property of a BN-pair that

$$BswB \subset BsBwB = BsBw'B \subset Bw'B \cup Bsw'B.$$

Hence since $l(ws) < n$ we have either $sw = w'$ or $sw = sw'$. Since $l(sw) < n$ and $l(w') \geq n$, we must have $sw = sw'$ and so $w = w'$ aw required. □

Exercise 7.4. It is easy to deduce from this decomposition that any two Borel subgroups have a common maximal torus. Show this directly for GL_n.

We can actually refine the decomposition to obtain a unique expression for $g \in G$ in terms of the groups B and N. Let $w \in W$, and set

$$U_w = \prod_{\alpha \in \Phi^+ : w(\alpha) \notin \Phi^+} U_\alpha.$$

(This is a subgroup, as one can show using Theorem 6.5 (4)). Pick a set of representatives $\{\dot{w} : w \in W\} \subset N$ for the elements of W. Then we have the following:

Proposition 7.5. *Every element $g \in G$ can be written uniquely as $g = ut\dot{w}v$ where $u \in U$, $t \in T$ and $v \in U_w$.*

Proof. By the Bruhat decomposition, there is a unique $w \in W$ such that $g \in BwB$, thus we may write $g = u_1 n u_2$ for $u_1, u_2 \in U$ and $n \in N$ such that $n = t\dot{w}$. Since U is the product of its root subgroups, we may decompose $u_2 = u_3 v$ where $u_3 \in \prod_{\alpha \in \Phi^+ : w(\alpha) \in \Phi^+} U_\alpha$ and $v \in U_w$. Then we have $u_4 = t\dot{w}u_2\dot{w}^{-1}t^{-1} \in U$, so that setting $u = u_1 u_4 \in U$ we have $g = ut\dot{w}v$. It remains to show the decomposition is unique. To see this note that if $ut\dot{w}v = u't'\dot{w}'v'$, then clearly $w = w'$ and we have

$u^{-1}u't'\dot{w}v'v^{-1} \in N_G(T)$. We claim this happens only if $u^{-1}u' = v'v^{-1} = 1$. Indeed suppose we have $ut\dot{w}v \in N_G(T)$. Then we must have

$$ut\dot{w}v = t'\dot{w}$$

for some $t' \in T$, and so $t\dot{w}v\dot{w}^{-1}t^{-1} = u^{-1}t't^{-1} \in \dot{w}U_w\dot{w}^{-1} \cap B = \{1\}$, so that $v = 1$, and hence $u = 1$. □

Recall that a parabolic subgroup P of G is a closed subgroup containing a Borel subgroup. By the fixed point theorem, this is equivalent to insisting that G/P is a complete variety. Once we have the Bruhat decomposition, it is easy to see that the parabolic subgroups containing a given Borel subgroup are very rigid. Given a subset $I \subset S$ we define W_I to be the subgroup of W generated by the elements of I, and set $P = P_I = BW_IB$. It is easy to see from the axioms for a BN-pair that P_I is a subgroup of G.

Lemma 7.6. *Let G be a group with a BN-pair.*

1. *Let $w \in W$. The subgroup generated by B and BwB for any $w \in W$ is P_I, where I is the set of simple reflections in a reduced expression for w, moreover P_I is generated by B and wBw^{-1}.*
2. *If P is a parabolic subgroup, then there is a subset $J \subset S$ such that $P = P_J$*

Proof. Let H be the subgroup generated by B and wBw^{-1} (certainly this is a subgroup of the group generated by B and BwB, so if we show it contains BwB it will be equal to it). Then clearly H is a union of B-double cosets, so we may set $R = \{v \in W : BvB \subseteq H\}$. Let $w = s_1s_2\dots s_r$ be a reduced expression for w, and let $I = \{s_1, s_2, \dots, s_r\}$. We claim that $R = W_I$. Now we have $s_1w < w$, so using (1) that s_1Bw intersects BwB nontrivially, and hence s_1B has nonempty intesection with $B.wBw^{-1} \subset H$. It follows that Bs_1B lies in H, and also Bs_1wB lies in H. By induction we see that $Bs_iB \in H$ for all i, $1 \leq i \leq r$. On the other hand, again using (1) the double cosets Bs_iB generate the subgroup $\bigsqcup_{v\in W_I} BvB$, which contains both B and BwB, hence we must have $H = P_I$ as claimed.

Now let P be a parabolic subgroup, so that $P = \bigsqcup_{v\in R} BvB$ for some subset R of W. By the above it is clear that R contains any simple reflection occuring in a reduced expression of any $v \in R$, and this is enough to ensure that $R = W_I$ for some $I \subset S$. □

We have already seen that Borel subgroups are self-normalizing. In fact this follows easily from the Bruhat decomposition, and so is true of any group where B arises in a BN-pair. Indeed we show a little more:

Lemma 7.7. *Any parabolic subgroup is self-normalizing and no two parabolics containing the same Borel are conjugate (thus the conjugacy classes of parabolic subgroups of G are indexed by subsets of the simple roots).*

Proof. Indeed suppose that P_I and P_J are conjugate subgroups. Then there is a $g \in G$ with $gP_Ig^{-1} = P_J$. Now by the Bruhat decomposition, we know that $g \in BwB$ for some $w \in W$, and so $\dot{w}P_I\dot{w}^{-1} = P_J$ for $\dot{w}$ any representative of w in G. In particular P_J contains B and $\dot{w}B\dot{w}^{-1}$, and so contains BwB and in particular $\dot{w}$. But then $\dot{w}P_J\dot{w}^{-1} = P_J$, and $P_I = P_J$ is self-normalizing as required. □

Before moving on to discuss reductive groups over a finite field, I would like to mention some of the uses of the notion of a BN-pair: it was noticed quite early that reductive groups defined over a not necessarily algebraically closed field k, such as the special linear groups $\mathrm{SL}_n(k)$ often possess a "large" normal subgroup which is simple modulo its center. Tits introduced the notion of a BN-pair to provide a unified framework in which to study such questions. For groups which he called "isotropic", meaning that they have proper parabolic subgroups defined over k, he obtained a general answer in [T], using the theory of BN-pairs – he proves a general criterion for a group with a BN-pair to be simple and then showed that $G(k)$ has a BN-pair defined as follows: We will write k for a fixed algebraic closure of the field k, identifying G with its k-points, and writing $G(k)$ for the group of k-points of G.

Let T be a maximal *split* torus in G, and let $\tilde{T}$ be a maximal torus of G containing T. Thus we have Φ the roots of G with repect to $\tilde{T}$. Let Σ be the restriction of the roots Φ to T, and for each $\alpha \in \Sigma$ let $U_{(\alpha)}$ be the group generated by the $U_{\tilde{\alpha}}$ where $\tilde{\alpha} \in \Phi$ restricts to α (these subgroups turn out to be defined over k). Then making a choice of positive roots in Φ, let U^+ be the subgroup generated by all the $U_{(\alpha)}$ for $\alpha \in \Sigma^+$. Let $H = C_G(T)$ and $N = N_G(T)$. One then sets $B^+ = H.U^+$ where U^+ is the subgroup generated by the $U_{(\alpha)}$ for $\alpha \in \Sigma$ positive (the group B^+ turns out to be minimal among parabolic subgroups of G defined over k).

Theorem 7.8. [T] *The group $G(k)$ has a BN-pair given by $B^+(k)$ and $N(k)$.*

In the same paper, Tits gives a general simplicity criterion for the group $G(k)$, which for example Steinberg [St68] showed can be applied to the fixed points of an endomorphism of a simple algebraic group over $\overline{\mathbb{F}}_q$, yielding a unifed proof of the simplicity of the groups known as "finite groups of Lie type".

REFERENCES

[B] A. Borel, *Linear algebraic groups*. Second edition. Graduate Texts in Mathematics, 126. Springer-Verlag, New York, 1991. xii+288 pp. ISBN: 0-387-97370-2

[DM] F. Digne, J. Michel, *Representations of finite groups of Lie type*, London Mathematical Society Student Texts, 21. Cambridge University Press, Cambridge, 1991. iv+159 pp. ISBN: 0-521-40117-8; 0-521-40648-X

[H] J. Humphreys, *Linear algebraic groups*, Graduate Texts in Mathematics, No. 21. Springer-Verlag, New York-Heidelberg, 1975. xiv+247 pp.

[S] T. A. Springer, *Linear algebraic groups*, Second edition. Progress in Mathematics, 9. BirkhŁuser Boston, Inc., Boston, MA, 1998. xiv+334 pp. ISBN: 0-8176-4021-5

[St68] R. Steinberg, *Endomorphisms of algebraic groups*, Memoirs of the American Mathematical Society, No.**80** American Mathematical Society, Providence, R.I. (1968) 108 pp.

[St99] R. Steinberg, *The isomorphism and isogeny theorems for reductive algebraic groups*, J. Algebra **216** (1999), no. 1, 366–383. 20G15

[T] J. Tits, *Algebraic and abstract simple groups*. Ann. of Math. (2) **80** (1964) 313–329.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CHICAGO.