Reductive groups over finite fields

Reductive groups

All algebraic groups are automatically assumed to be affine (and thus linear) and varieties over an algebraically closed field. They are reduced, separated, of finite type, but not necessarily connected. Every such group is isomorphic to a closed subgroup of GL_n. G will always be an arbitrary algebraic group.

(Examples of this include GL_n, SL_n, SO_n, $\mathbb{G}_a$ defined by the algebra $k[t]$, $\mathbb{G}_m$ defined by the algebra $k[t, t^{-1}]$, U_n, B_n)

First, let's define what our main object of interest actually is, more precisely: what do we mean when we say an algebraic group is reductive?

Definition An element of G is called *unipotent* if its image in some embedding of G as a closed subgroup of GL_n is unipotent *(meaning that $(A - I)^m = 0$ for the identity matrix I and any matrix A)*. This property does not depend on the embedding. Let G_u denote the set of unipotent elements of an algebraic group G.

Definition A *unipotent* algebraic group is a group containing only unipotent elements.

Proposition (Intuition) *As an algebraic variety, a connected unipotent group is isomorphic to an affine space; in characteristic 0 a unipotent group is necessarily connected.*

Lemma G contains a unique maximal normal connected unipotent subgroup called the *unipotent radical* of G and denoted by $R_u(G)$.

Definition G is called *reductive* if $R_u(G)$ is trivial.

Remark (Intuition) *In characteristic 0, this is equivalent to the condition that any rational representation of G is completely reducible. This is not the case in positive characteristic.*

(A linear representation of an algebraic group is said to be rational if, viewed as a map from the group to GL_n, it is a morphism of algebraic varieties)

Examples $\mathbb{T}_r := \mathbb{G}_m^r$ *(where $r \geq 1$; called tori), GL_n, SL_n, SO_n, and their products.*

Definition Maximal connected solvable subgroups of an algebraic group are called *Borel subgroups*.

Example *The subgroup $B_n \subseteq \mathrm{GL}_n$, the group of all upper-triangular matrices, is Borel.*

Theorem Let G be a connected algebraic group; then:

1. All Borel subgroups of G are conjugate.
2. Every element of G is in some Borel subgroup.
3. A Borel subgroup is equal to its normalizer in G.
4. Every maximal torus of G is in some Borel subgroup.

Proposition If B is a Borel subgroup, then G/B is a projective variety.

Classification

Starting now, we will assume that G is a connected reductive group over k, and that $T \subseteq G$ is a maximal torus.

Definition A *root system* in a real vector space V is a subset Φ with the following properties

1. Φ is finite, generates V, and $0 \notin \Phi$.
2. For any $\alpha \in \Phi$, there exists an $\check{\alpha}$ in the vector space dual to V such that $\langle \alpha, \check{\alpha} \rangle = 2$ and such that Φ is stable under the reflection $s_\alpha : V \to V$ defined by $x \mapsto x - \langle x, \check{\alpha} \rangle \alpha$.
3. $\check{\alpha}(\Phi) \subseteq \mathbb{Z}$ for any $\alpha \in \Phi$.

The $\check{\alpha}$ form a root system $\check{\Phi}$ in the dual of V. They are called coroots.

Definition A root system is said to be *reduced* if for any $\alpha \in \Phi$ we have $\Phi \cap \langle \alpha \rangle = \{\alpha, -\alpha\}$.

(Any line in V containing a root contains exactly two (opposed) roots)

Definition A *rational character* of G is a morphism of algebraic groups $G \to \mathbb{G}_m$. The character group $X(G)$ of an algebraic group G is the group of rational characters of G.

Definition A subgroup $U' \subseteq G$ is called a root subgroup (w.r.t. T) if

- $U' \cong \mathbb{G}_a$;
- There is an α (called a *root*) in the character lattice $X(T)$ such that $tut^{-1} = \alpha(t)u$ (viewing u as an element of $\mathbb{G}_a$) for all $t \in T, u \in U'$.

Example Consider $G = \mathrm{GL}_n(k)$. Let $U_{ij} = \{\, I + tI_{ij} \mid t \in k \,\}$, where we write I_{ij} for the matrix unit in position (i, j). Then U_{ij} is a root subgroup and the corresponding root α is $\epsilon_i - \epsilon_j$, where ϵ_k maps $\mathrm{diag}(t_1, \ldots, t_n) \in T$ to $t_k \in \mathbb{G}_m$.

Theorem The following claims are true.

1. A root $\alpha \in \Delta$ determines a root subgroup uniquely, let us write U_α for this subgroup.

2. U_α and $U_{-\alpha}$ generate a subgroup of G isomorphic to SL_2 or PGL_2.
3. The set of all roots Δ is a reduced root system, independent of k, $\Delta^\vee$ is a dual root system.

Definition A root datum RD is a quadruple $(\Lambda, \Lambda^\vee, \Delta, \Delta^\vee)$, where

- $\Lambda, \Lambda^\vee$ are mutually dual lattices *(mutually dual meaning there exists a perfect pairing, i.e. a $\mathbb{Z}$-bilinear map $(\cdot, \cdot)$ such that $v \mapsto (v, \cdot)$ is an isomorphism between λ and $\lambda^{\vee *}$, $\Lambda \times \Lambda^\vee \to \mathbb{Z}$)*,
- $\Delta \subseteq \Lambda$, $\Delta^\vee \subseteq \Lambda^\vee$ are dual reduced root systems

Definition A *one-parameter subgroup* of G is a morphism of algebraic groups $\mathbb{G}_m \to G$. The abelian group of one-parameter subgroups of a torus T is denoted by $Y(T)$.

Lemma There is a perfect pairing between $X(T)$ and $Y(T)$.

Example Let G be a connected reductive group and $T \subseteq G$ be a maximal torus. Then $(X(T), Y(T), \Delta, \Delta^\vee)$ is a root datum.

Definition Let $\mathrm{RD}_1 = (\Lambda_1, \Lambda_1^\vee, \Delta_1, \Delta_1^\vee), \mathrm{RD}_2 = (\Lambda_2, \Lambda_2^\vee, \Delta_2, \Delta_2^\vee)$ be two root data. By a homomorphism $\mathrm{RD}_1 \to \mathrm{RD}_2$ we mean a lattice homomorphism $\varphi : \Lambda_2 \to \Lambda_1$ such that $\varphi : \Delta_2 \xrightarrow{\sim} \Delta_1$ and $\varphi^*(\varphi(\alpha)^\vee) = \alpha^\vee$ for all $\alpha \in \Delta_2$.

Theorem The following claims hold:

1. Isomorphism classes of reductive algebraic groups are in bijection with isomorphism classes of root data via the construction of the example two up.
2. Let $\mathrm{RD}_1, \mathrm{RD}_2$ be two root data and G_1, G_2 be the corresponding connected reductive groups. Then any homomorphism $\mathrm{RD}_1 \to \mathrm{RD}_2$ gives a rise to a homomorphism $G_1 \to G_2$ and vice-versa.

Weyl group

Theorem All maximal tori are conjugate.

Definition The Weyl group $W = W(G)$ is, by definition, $N_G(T)/T$.

Note that since all maximal tori are conjugate, W is independent of the choice of T

Remark The Weyl group W of G is generated by the reflections s_α for $\alpha \in \Delta$.

Remark Given a $\sigma \in W$, represented by $n \in N_G(T)$, conjugation by n is a morphism $T \to T$ depending only on $\sigma \in W$. Given a character $\alpha : T \to \mathbb{G}_m$, let $\sigma\alpha$ be the character obtained by composing with this conjugation: $(\sigma\alpha)(t) = \alpha(n^{-1}tn)$. This defined an action of W on $X(T)$, which is easily seen to permute Δ *(restriction to Δ is well-defined; sends root to root)*. Similarly, W acts on $Y(T)$ by $(\sigma\lambda)(x) = n\lambda(x)n^{-1}$.

Note the direction of conjugation, which ensures that $\langle \sigma\alpha, \sigma\lambda \rangle = \langle \alpha, \lambda \rangle$ for $\sigma \in W$, $\alpha \in X(T)$, $\lambda \in Y(T)$.

Example *In the case of $G = \mathrm{GL}_n$, $W \cong S_n$.*

Flag variety, Bruhat decomposition

We fix a Borel subgroup $B \subseteq G$ and consider the *flag variety* $\mathcal{B} := G/B$. This is a smooth projective variety of dimension $|\Delta_+|$. It can be identified with the variety of Borel subgroups of G via the map $gB \mapsto gBg^{-1}$.

Example *In the case $G = \mathrm{GL}_n$ we get the variety Fl of full flags in k^n.*

(Full flags being $\Set{k^n = V_n \supset V{n-1} \supset \ldots \supset V{0} = \Set{0}}$)

For each $w \in W$, fix a lift $\dot{w} \in N_G(T)$. Consider the locally closed subvariety $BwB := B\dot{w}B \subseteq G$. Note that $BwB = UwB$, where we write U for $R_u(B)$. Set $Y_w := BwB/B \subseteq \mathcal{B}$.

Theorem The following claims hold:

1. $G = \coprod_{w \in W} BwB$, hence $\mathcal{B} = \coprod_{w \in W} Y_w$
2. Y_w is an affine space of dimension $\ell(w)$.

Lang's theorem, quasi-split reductive groups

In the following k/k_0 will always be a field extension.

Definition A k_0-structure on a k-vector space V is a k_0-subspace V_0 such that $V = V_0 \otimes_{k_0} k$.
A k_0-structure on a finite type k-algebra A is a finite type k_0-algebra A_0 such that $A = A_0 \otimes_{k_0} k$.
A k_0-structure on an affine or projective k-variety V is the k_0 variety defined by A_0 where the algebra A of V has a k_0 structure A_0.
In general a k_0-structure on a variety is essentially given by a finite open affine covering where each open affine has a k_0-structure.

Definition An algebraic variety V over k is said to be defined over k_0, if it has a k_0-structure V_0. In this case we write $V = V_0 \otimes_{k_0} k$. One can also call V rational over k_0.

Definition* Let V be an $\bar{\mathbb{F}}_q$-variety with an $\mathbb{F}_q$-structure V_0. The associated *geometric Frobenius endomorphism* $F : V \to V$ is $F_0 \otimes_{\mathbb{F}_q} 1$ where F_0 is the endomorphism of V_0 which raises the functions on V_0 to the qth power. The endomorphism Φ of V induced by $(\lambda \mapsto \lambda^q) \in \mathrm{Gal}(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ is called the arithmetic Frobenius endomorphism.

Remark *The geometric Frobenius is a morphism of $\bar{\mathbb{F}}_q$-varieties, while the arithmetic Frobenius is only a morphism of $\mathbb{F}_q$-schemes.*

Given a variety V_0 over a finite field, we can base-change to $\bar{\mathbb{F}}_p$ (let V denote this base-changed variety); this however loses some information about V_0, as you cannot reconstruct V_0 solely from V (there exist non-isomorphic varieties over $\mathbb{F}_p$ whose base-change to $\bar{\mathbb{F}}_p$ is isomorphic). V_0 however has a frobenius $F : V_0 \to V_0$ defined through the pth power on the coordinate ring, which in turn induces a geometric frobenius F on V (since V has a $\mathbb{F}_q$ structure). you can now reconstruct V_0 through the pair (V, F) (in fact there exists a category equivalence between the two), e.g. $V_0(\mathbb{F}_p) = V^F$ *(this is pretty much just like keeping track of the Galois action)*.

Remark An example of the above is $V = \mathrm{GL}_n(\bar{\mathbb{F}}_q)$, $V_0 = U_n(\mathbb{F}_q)$, $F : A \mapsto \left({}^tA^{[q]}\right)^{-1}$, F is called the *twisted Frobenius* in this example.

Definition *Let G be a connected algebraic group over $\bar{\mathbb{F}}_p$ and F be a Frobenius endomorphism. An F-stable maximal torus of the algebraic group G which is contained in an F-stable Borel subgroup of G is called a quasi-split torus.*

Definition A reductive group G over k is called *quasi-split* if it contains a Borel subgroup over k.

Remark *The above notions of quasi-split are independent of each other.*

Theorem (Lang-Steinberg) Let G be a connected affine algebraic group over $\bar{\mathbb{F}}_p$, and F be a Frobenius endomorphism. Then the *Lang map* $\mathcal{L} : g \mapsto g^{-1}F(g)$ is a surjective étale endomorphism of G.

Corollary If G is a connected reductive group over a finite field $\mathbb{F}_q$, then G is quasi-split.
Proof Let B be a Borel subgroup of $G_{\bar{\mathbb{F}}_p}$, and let B^F be the Borel subgroup obtained by applying F. Then $aB^Fa^{-1} = B$ for some a in $G(\bar{\mathbb{F}}_p)$. By the Lang-Steinberg theorem, $a = g^{-1}F(g)$ for some g in $G(\bar{\mathbb{F}}_p)$. Now, we consider the Borel subgroup $H = gBg^{-1}$. We can check that H is defined over $\mathbb{F}_q$ by the following computation:

$$H^F = F(g)B^FF(g)^{-1} = gaB^Fa^{-1}g^{-1} = H.$$