Finite groups of Lie type

Finn Klein

March 4, 2025

Disclaimer. Part of these notes were taken from the notes of a talk on Tannakian reconstruction I had previously given at FAU Erlangen-Nürnberg.

1 Algebraic groups

1.1 What is an algebraic group?

Definition 1.1. 1. Let $\mathbf{C}$ be a category with finite products (note that this entails the existence of a terminal object $\top$ in $\mathbf{C}$). A **group object** in $\mathbf{C}$ is an object X of $\mathbf{C}$ together with morphisms $\mu : X \times X \to X, \eta : \top \to X, \iota : X \to X$, respectively called the multiplication, identity and inverse maps, such that the following diagrams commute:

$$\begin{tikzcd} X \times X \times X \arrow[r, "\mu \times 1_X"] \arrow[d, "1_X \times \mu"'] & X \times X \arrow[d, "\mu"] \\ X \times X \arrow[r, "\mu"] & X \end{tikzcd} \qquad \begin{tikzcd} X \arrow[r, "\langle 1_X, \eta \circ !_X \rangle"] \arrow[dr, "1_X"'] & X \times X \arrow[d, "\mu"] & X \arrow[l, "\langle \eta \circ !_X, 1_X \rangle"'] \arrow[dl, "1_X"] \\ & X & \end{tikzcd}$$

$$\begin{tikzcd} X \arrow[r, "\langle 1_X, \iota \rangle"] \arrow[dr, "\eta \circ !_X"'] & X \times X \arrow[d, "\mu"] & X \arrow[l, "\langle \iota, 1_X \rangle"'] \arrow[dl, "\eta \circ !_X"] \\ & X & \end{tikzcd}$$

(These diagrams respectively encode the associativity of the multiplication map, the identity element and the existence of inverses.)

2. Let (X, μ, η, ι) and $(X', \mu', \eta', \iota')$ be group objects in $\mathbf{C}$. A morphism $f : X \to X'$ is a morphism of group objects if the following diagrams commute:

$$\begin{tikzcd} X \times X \arrow[r, "\mu"] \arrow[d, "f \times f"'] & X \arrow[d, "f"] \\ X' \times X' \arrow[r, "\mu'"] & X' \end{tikzcd} \qquad \begin{tikzcd} \top \arrow[r, "\eta"] \arrow[dr, "\eta'"'] & X \arrow[d, "f"] \\ & X' \end{tikzcd} \qquad \begin{tikzcd} X \arrow[r, "\iota"] \arrow[d, "f"'] & X \arrow[d, "f"] \\ X' \arrow[r, "\iota'"] & X' \end{tikzcd}$$

This encodes that f commutes with multiplication and inversion and preserves the unit.

3. The group objects in $\mathbf{C}$ together with the morphisms of group objects form a category $\mathbf{Grp}(\mathbf{C})$.

Example 1.1. 1. A group object in $\mathbf{Set}$ is just an ordinary group. A morphism of group objects is just an ordinary homomorphism of groups. Hence, $\mathbf{Grp}(\mathbf{Set}) \cong \mathbf{Grp}$.

2. A group object in the category $\mathbf{Top}$ of topological spaces and continuous maps is a topological group. A morphism of group objects is a continuous group homomorphism. Hence, $\mathbf{Grp}(\mathbf{Top}) \cong \mathbf{TopGrp}$.

3. A group object in the category $\mathbf{SmoothMfd}$ of smooth manifolds and smooth maps is a Lie group. A morphism of group objects is a smooth homomorphism of groups. Hence, $\mathbf{Grp}(\mathbf{SmoothMfd}) \cong \mathbf{LieGrp}$.

In this context, it makes sense to define the groups of algebraic geometry to be group objects in the category of schemes. This is called a group scheme.

Definition 1.2. A group scheme over a field k is a group object in the category $\mathbf{Sch}_k$ of schemes over k and regular maps. A morphism of group schemes is a morphism of group objects in $\mathbf{Sch}_k$.

Group schemes deserve to be studied in their own right, however for this talk we are only interested in the simpler case where the group scheme X is affine, i.e. isomorphic to $\operatorname{Spec}(\mathcal{O}(X))$, and of finite type, i.e. $\mathcal{O}(X)$ is a finitely generated k-algebra.

Definition 1.3. An affine algebraic group over a field k is an affine group scheme of finite type over k. Affine algebraic groups form the full subcategory $\mathbf{AlgGrp}_k$ of $\mathbf{Grp}(\mathbf{Sch}_k)$. Since these notes only concern affine algebraic groups, we will drop the "affine" for the sake of brevity.

Remark (Schemes as functors)**.** Let X be an algebraic group over k. Let $A := \mathcal{O}(X)$ be the algebra of regular functions on X. As the contravariant functor $\mathcal{O}$ takes products to coproducts, the morphisms from Definition 1.1 translate into dualized morphisms for A: We obtain $\Delta : A \to A \otimes A$ (the **comultiplication**), $\epsilon : A \to k$ (the **counit**) and $S : A \to A$ (the **antipode**), respectively induced by μ, η and ι, such that diagrams dual to those in Definition 1.1 commute. These morphisms endow A with the structure of a Hopf algebra. This extends to a duality

$$\mathbf{AlgGrp}_k \simeq (\mathbf{CHopf}^{\mathrm{f}}_k)^{\mathrm{op}}$$

between the category of algebraic groups over k and the category of finitely generated commutative Hopf algebras over k.

The following is perhaps the most convenient and conceptual way to think about algebraic groups. Recall that the Yoneda embedding

$$\mathbf{AffSch}_k \xrightarrow{\;y\;} \operatorname{Fun}(\mathbf{AffSch}_k^{\mathrm{op}}, \mathbf{Set})$$

$$\begin{tikzcd} X \arrow[r, mapsto] \arrow[d, "f"] & \operatorname{Hom}(-, X) \arrow[d, "f\circ -"] \\ X' \arrow[r, mapsto] & \operatorname{Hom}(-, X') \end{tikzcd}$$

is fully faithful, thus $\mathbf{AffSch}_k$ is isomorphic to a full subcategory of $\mathrm{Fun}(\mathbf{AffSch}_k^{\mathrm{op}}, \mathbf{Set})$. We may thus replace an affine scheme X with the presheaf $h_X := \mathrm{Hom}(-, X)$. As products of affine schemes are again affine, we can consider an algebraic group as a group object in $\mathbf{AffSch}_k$. Since y is left exact, it preserves group objects, so h_X is a group object in $\mathrm{Fun}(\mathbf{AffSch}_k^{\mathrm{op}}, \mathbf{Set})$. This means we get commuting diagrams of the form[1]

$$\begin{tikzcd} h_X \times h_X \times h_X \arrow[r, "(\mu\circ -)\times 1_{h_X}"] \arrow[d, "1_{h_X}\times(\mu\circ -)"'] & h_X \times h_X \arrow[d, "\mu\circ -"] \\ h_X \times h_X \arrow[r, "\mu\circ -"] & h_X \end{tikzcd}$$

(etc.) as in Definition 1.1. The arrows in this diagram are natural transformations, and as we fix another affine scheme Z, one obtains group object diagrams (in **Set**!) of the form

$$\begin{tikzcd} \mathrm{Hom}(Z,X) \times \mathrm{Hom}(Z,X) \times \mathrm{Hom}(Z,X) \arrow[r] \arrow[d] & \mathrm{Hom}(Z,X) \times \mathrm{Hom}(Z,X) \arrow[d] \\ \mathrm{Hom}(Z,X) \times \mathrm{Hom}(Z,X) \arrow[r] & \mathrm{Hom}(Z,X) \end{tikzcd}$$

etc. This means that for every affine scheme Z we obtain an abstract group $h_X(Z)$ that is functorial with respect to scheme maps. This equivalently means that the functor h_X factors through the forgetful functor $U : \mathbf{Grp} \to \mathbf{Set}$, yielding a functor $\mathbf{AffSch}_k^{\mathrm{op}} \to \mathbf{Grp}$:

$$\begin{tikzcd} \mathbf{AffSch}_k^{\mathrm{op}} \arrow[r, dashed] \arrow[dr, "h_X"'] & \mathbf{Grp} \arrow[d, dashed, "U"] \\ & \mathbf{Set} \end{tikzcd}$$

We will abuse notation and still refer to the dotted arrow as h_X.

Finally, we apply the duality between affine schemes over k and k-algebras to obtain the following characterization of algebraic groups:

Theorem 1.2 (Characterization of algebraic groups)**.** An algebraic group is a representable functor $G : \mathbf{Alg}_k \to \mathbf{Grp}$ which is represented by a finitely generated k-algebra. This means that there exists a finitely generated k-algebra A such that there is a natural isomorphism $G \cong \mathrm{Hom}(A, -)$, i.e. for all k-algebras B one can choose isomorphisms $G(B) \cong \mathrm{Hom}(A, B)$ such that for all morphisms of k-algebras $f : B \to B'$ the following diagram in **Grp** commutes:

$$\begin{tikzcd} G(B) \arrow[r, "\sim"] \arrow[d, "G(f)"'] & \mathrm{Hom}(A,B) \arrow[d, "f\circ -"] \\ G(B') \arrow[r, "\sim"] & \mathrm{Hom}(A,B') \end{tikzcd}$$

Remark. In practice, this theorem means two things:

[1]from this point onwards, the arrow labeling will become a bit messy because we're identifying $h_X \times h_X$ with $h_{X\times X}$ by the universal property of the product, or alternatively by the left exactness of y.

- An algebraic group G is a family of (ordinary) groups, parametrized by k-algebras, such that every morphism of k-algebras gives a homomorphism of the associated groups. One can think of the group associated to the k-algebra B as the B-valued points of G. This will make sense once we look at an example like GL_n.

- There is a finitely generated (commutative Hopf) algebra A over k such that for every k-algebra B, every B-valued point of G (that is, every element of $G(B)$) corresponds to a unique morphism of k-algebras $f : A \to B$.

Example 1.3. 1. The **additive group** is the functor $\mathbb{G}_a : \mathbf{Alg}_k \to \mathbf{Grp}$ which assigns to a k-algebra R the additive group $(R, +)$ and to a k-algebra homomorphism f the underlying homomorphism of additive groups. Since elements of R are naturally in bijection with k-algebra homomorphisms from the polynomial algebra $k[X]$ to R, the functor $\mathbb{G}_a$ is represented by $k[X]$. Using the universal property of the tensor product of algebras, one verifies that the comultiplication on $k[X]$ is given by $\Delta(X) = 1 \otimes X + X \otimes 1$. The counit is the morphism defined by $X \mapsto 1$ and the antipode is given by multiplication of X with -1. Because $k[X] = \mathcal{O}(\mathbb{A}^1_k)$, the additive group is sometimes denoted by $\mathbb{A}^1_k$.

2. The **multiplicative group** is the functor $\mathbb{G}_m : \mathbf{Alg}_k \to \mathbf{Grp}$ which assigns to a k-algebra R the group $(R^\times, \cdot)$ of units of R and to a k-algebra homomorphism f the underlying homomorphism on groups of units. The invertible elements of R are naturally in bijection with k-algebra homomorphisms from $k[X, X^{-1}]$ to R, hence $\mathbb{G}_m$ is represented by $k[X, X^{-1}]$. The comultiplication on $k[X, X^{-1}]$ is given by $\Delta(X) = X \otimes X$, the counit by $X \mapsto 1$ and the antipode by $X \mapsto X^{-1}$.

3. Let V be a k-vector space. The algebraic group V_a assigns to a k-algebra R the group underlying the free R-module $V \otimes_k R$ and to a homomorphism of k-algebras the group homomorphism $1_V \otimes f$. By the Hom-$\otimes$-adjunction and the universal property of the symmetric algebra, we have natural isomorphisms $V \otimes R \cong \mathrm{Hom}_{\mathbf{Vect}_k}(V^\vee, R) \cong \mathrm{Hom}_{\mathbf{Alg}_k}(\mathrm{Sym}(V^\vee), R)$, hence V_a is represented by $\mathrm{Sym}(V^\vee)$. If W is another k-vector space and $f : V \to W$ is a k-linear map, one obtains a morphism $f_* : V_a \to W_a$ by $(f_*)_R = f \otimes 1_R$.

4. Let $n \in \mathbb{N}$. The **general linear group** GL_n assigns to a k-algebra R the group of invertible $(n \times n)$-matrices $\mathrm{GL}_n(R)$ and to a k-algebra homomorphism f the map from $\mathrm{GL}_n(R)$ to $\mathrm{GL}_n(S)$ that pushes forward coefficients[2]. Since $\mathrm{GL}_n(k) \subseteq \mathbb{A}^{n^2}$ is the non-vanishing locus of the determinant defined over k, basic algebraic geometry tells us that GL_n is affine and represented by the localization $k[X_{11}, X_{12}, \ldots, X_{nn}][\det^{-1}]$. The comultiplication is defined via

$$X_{ij} \mapsto \sum_{k=1}^{n} X_{ik} \otimes X_{kj}.$$

[2]Pushing forward coefficients preserves invertibility since f commutes with the determinant and takes units in R to units in S.

5. Let $n \in \mathbb{N}$. The **special linear group** SL_n is the closed subgroup $V(\det -1) \subseteq \mathrm{GL}_n$.

6. Let $n \in \mathbb{N}$ The **orthogonal group** O_n is the subgroup

$$\mathrm{O}_n = \{A \in \mathrm{GL}_n : A^T A = AA^T = \mathbb{1}\}.$$

(Here, $(-)^T$ denotes the transpose.) It is easy to see that the defining condition of O_n is given by the vanishing of polynomials in the entries of A and hence O_n is a closed subgroup of GL_n.

7. Let $n \in \mathbb{N}$. Let M be the antidiagonal $(2n \times 2n)$-matrix with antidiagonal entries $(1, -1, \ldots, 1, -1)$. The **symplectic group** Sp_{2n} is the subgroup

$$Sp_{2n} = \{A \in \mathrm{GL}_n : A^T M A = M\}.$$

Again, one readily checks that this is a closed condition.

Remark. Examples 6, 7 and 8 above are commonly referred to as the **classical groups**.

Definition 1.4. Let G be an algebraic subgroup over k. An algebraic subgroup H of G is a k-subscheme H of G such that the inclusion map $\iota : H \to G$ is a morphism of algebraic groups.

Lemma 1.4 (Products of algebraic groups)**.** Let G and G' be algebraic groups. Define $G \times G'$ to be the functor from k-algebras to groups that assigns to a k-algebra R the product group $G(R) \times G'(R)$ and to a k-algebra homomorphism f the group homomorphism $G(f) \times G'(f)$. Then, $G \times G'$ is an algebraic group: If G is represented by A and G' is represented by B, then $G \times G'$ is represented by $A \otimes_k B$.

Proof. By unpacking the definitions and applying the universal property of the tensor product of k-algebras, there are natural isomorphisms

$$\begin{aligned}(G \times G')(R) &= G(R) \times G'(R) \\ &= \mathrm{Hom}(A, R) \times \mathrm{Hom}(B, R) \\ &\cong \mathrm{Hom}(A \otimes_k B, R).\end{aligned}$$

Moreover, $A \otimes_k B$ is finitely generated. □

Remark (The role of $\mathcal{O}(G)$)**.** 1. If X is an affine scheme over k, then $\mathcal{O}(X)$ is the algebra of regular functions from X to the affine line $\mathbb{A}^1_k$:

$$\mathcal{O}(X) = \mathrm{Hom}_{\mathbf{Sch}_k}(X, \mathbb{A}^1_k).$$

By the fully-faithfulness of the Yoneda embedding, the schemes-as-functors interpretation of $\mathcal{O}(X)$ is the following:

$$\mathcal{O}(X) = \mathrm{Nat}(X, \mathbb{A}^1_k),$$

the set of natural transformations from the functor X to the functor $\mathbb{A}^1_k$.

2. If X is an affine scheme over k, then the corresponding functor from k-algebras to sets is represented by $\mathcal{O}(X)$.

Remark (Base change)**.** 1. Let X be an affine scheme over k, regarded as a functor from k-algebras to sets. If R is a k-algebra, then we can restrict the functor X to the subcategory $\mathbf{Alg}_R \subseteq \mathbf{Alg}_k$. This process is called **base change** and we introduce the notation X_R for the resulting functor. Scheme-theoretically, X_R is the fiber product $X \times_k \mathrm{Spec}(R) \in \mathbf{Sch}_R$. X_R is again affine and is represented by the R-algebra $\mathcal{O}(X) \otimes_k R$. This algebra is isomorphic to the algebra of regular functions from the R-scheme X_R to the affine line $\mathbb{A}^1_R := (\mathbb{A}^1_k)_R$ over R, and hence we can treat elements of $\mathcal{O}(X) \otimes_k R$ as if they were functions.

2. if G is an algebraic group over k, then the base change G_R is an algebraic group over the k-algebra R.[3] The R-Hopf algebra structure on $\mathcal{O}(G) \otimes_k R$ is given by tensoring the comultiplication, counit and antipode of $\mathcal{O}(G)$ with 1_R and identifying $R \cong R \otimes_R R$ where needed.

The following theorem is vital for everything that's to follow.

Theorem 1.5. Let G be an affine algebraic group. Then, there exists some $n \in \mathbb{N}$ such that G is isomorphic to a closed subgroup of GL_n.

Proof. A detailed proof can be found in [5], Theorem 4.9 A sketch of the proof is this: Using comodule methods, one can show that the regular representation of G on its coordinate ring $\mathcal{O}_G$ is faithful, so G embeds into $\mathrm{GL}_n(\mathcal{O}_G)$. □

Convention. Throughout the rest of this talk, fix a prime p and define $k := \overline{\mathbb{F}}_p$. Algebraic groups G will be taken to be affine and defined over k. We will freely identify G with its k-valued points $G(k)$.

1.2 Jordan decomposition is easy mod p

Recall the following classical result about algebraic groups.

Theorem 1.6. Let G be an algebraic group and let g be an element of G. There exist unique elements g_s, g_u, called the semisimple and nilpotent part of g, respectively, satisfying the following properties:

1. $[g_s, g_u] = e$

2. $g = g_s g_u$

3. For every rational representation (ρ, V) of G, $\rho(g_s)$ is semisimple (equivalently, diagonalisable) and $\rho(g_u)$ is unipotent.

[3] We haven't actually defined an algebraic group over an arbitrary ring R, but the definition is parallel to the case where R is a field.

Definition 1.7. Let G be an algebraic group. Define subgroups

$$G_u = \{g \in G : g = g_u\}$$

and

$$G_s = \{g \in G : g = g_s\},$$

the **unipotent** and **semisimple** subgroups of G, respectively.

In characteristic zero, a proof of this theorem requires quite a bit of heavy machinery. (One possible avenue to a proof is using the fact that the behavior of g_s and g_u is well-defined on representations and arguing via a version of Tannakian reconstruction that g_s and g_u must exist.) In characteristic p, however, the proof is much easier and is deferred to Exercise 2.

Lemma 1.5. Let $g \in G(k)$. By embedding G into some GL_n, it is clear that g has finite order. Let $m := \mathrm{ord}(g)$.

1. g is semisimple iff p does not divide m.

2. g is unipotent iff m is a power of p.

1.3 Connectedness

We will often examine whether an algebraic group G is connected. Many important theorems rely on connectedness, and many important distinguished subgroups of G are connected.

Definition 1.8 (Connectedness)**.** A topological space X is **connected** if it cannot be written as a union of two non-empty open subsets.

In fact, being connected has a desirable consequence for an algebraic group G:

Proposition 1.9. An algebraic group G over k is connected if and only if it is irreducible.

Proof. This is [3], Proposition 1.3.13c). □

2 Structure theory of reductive groups

2.1 Distinguished Subgroups

Definition 2.1 (Tori)**.** Let G be an algebraic group over a field k (not necessarily algebraically closed).

1. A **torus** in G is a subgroup of G that becomes isomorphic to a direct product of copies of the multiplicative group $\mathbb{G}_m$ when passing to some finite field extension K of k.

2. A **split torus** in G is a torus such that $K = k$ in the above definition.

Example 2.1. Let $p > 2$ and let $z \in \mathbb{F}_q$ not be a perfect square. Then, the polynomial $x^2 - z \in \mathbb{F}_q[x]$ is irreducible, and thus $\mathbb{F}_q[x]/(x^2 - z)$ is again a field. By basic field theory, one identifies this field as $\mathbb{F}_{q^2}$. As a $\mathbb{F}_q$-vector space, $\mathbb{F}_{q^2}$ has a basis given by $\{1, x\}$, and for any element $y = a + bx \in \mathbb{F}_{q^2}$, multiplication by y is an $\mathbb{F}_q$-linear map with representing matrix

$$\begin{pmatrix} a & bz \\ b & a \end{pmatrix}$$

. This gives an injective map from $\mathbb{F}_{q^2}$ into $\mathrm{GL}_2(\mathbb{F}_q)$. Let the image of this map be denoted by T_{nonsplit}. Over the algebraic closure k, the polynomial $x^2 - z$ splits, so T_{nonsplit} is a torus in G. One can also show that it is a maximal torus. But it is non-split, as it is not isomorphic to a direct product of copies of $\mathbb{G}_m$ over $\mathbb{F}_q$.

The following lemma will become important later.

Lemma 2.2. Let G be a connected algebraic group over k, and let $S \leq G$ be a torus. Then, $C_G(S)$ is connected.

Proof. This is [2], Theorem 1.3.3 (iii). □

Definition 2.3 (Unipotent radical)**.**

1. A subgroup H of G is unipotent if $g = g_u$ holds for all $g \in H$.
2. The unipotent radical $R_u(G)$ of G is the largest normal unipotent subgroup of G.

Remark. In positive characteristic, it is easy to see that such a group must exist if G is finite: Concretely, one easily checks the fact that the product of unipotent subgroups of G is again unipotent.

Lemma 2.2. $R_u(G)$ is closed and connected in G.

Definition 2.4. G is called **reductive** if $R_u(G) = 1$.

Definition 2.5 (Borel subgroups)**.** A **Borel subgroup** of G is a maximal closed connected solvable subgroup of G.

Solvable subgroups of algebraic groups admit an elegant description as groups of upper triangular matrices. Recall that G embeds as a closed subgroup into some GL_n.

Theorem 2.6 (Lie-Kolchin)**.** Let G be a connected solvable subgroup of GL_n. Then, G is conjugate to some subgroup of the group B_n of upper triangular matrices.

There is an elegant proof relying on the following theorem of Borel:

Theorem 2.7 (Borel's Fixed Point Theorem)**.** Let G act rationally on a complete nonempty variety X. Then, there is some element $x \in X$ which is fixed by G.

Proof. A proof can be found in [1], Proposition 15.2. □

Proof of Lie-Kolchin. We proceed by induction on n. If $n = 1$, then the statement is clear, as $\mathrm{GL}_1 = \mathrm{B}_1$. Now suppose that the theorem is known for GL_n. We claim that any nonzero representation V of G has a nonzero fixed vector. This can be easily seen by applying Borel's fixed point theorem to the projectivisation of V. It follows that G is conjugate in GL_{n+1} to a group of matrices of the form

$$\begin{pmatrix} * & v^T \\ 0 & A \end{pmatrix},$$

where $A \in \mathrm{GL}_n$. The span of $\{e_2, \ldots, e_{n+1}\}$ is G-stable and one obtains an induced n-dimensional representation of G. By induction, G already acts on this representation by upper triangular matrices. This, together with the block matrix presentation of G, concludes the proof. □

The Lie-Kolchin theorem has important implications for the structure theory of connected solvable algebraic groups.

Theorem 2.3. Let G be a connected solvable algebraic group. Then, the following holds:

1. G_u is a normal connected subgroup of G.
2. Let T be any maximal torus in G. Then, $G \cong G_u \rtimes T$.
3. For any torus S in G, one has the equality $N_G(S) = C_G(S)$.

Here are some important statements about Borel subgroups of G.

Theorem 2.8. Let G be a connected algebraic group. Then, the following holds:

1. Any two Borel subgroups in G are conjugate.
2. Every element of G is contained in some Borel.
3. If B is any Borel in G, then $N_G(B) = B$.
4. Every maximal torus of G is contained in some Borel.

Proof. This is [2], Theorem 1.3.3. □

Corollary 2.9. Any two maximal tori in G are conjugate.

Proof. See [3], Corollary 3.5.7. □

Definition 2.10. Let G be an algebraic group.

1. The **radical** $R(G)$ of G is the product of all connected solvable normal subgroups in G.
2. G is called **semisimple** if $R(G) = 1$.

Proposition 2.11. $R(G)$ is a connected solvable normal subgroup of G.

2.2 Root data

Throughout this section, fix a connected reductive group G and a maximal torus T in G. Note that T will be automatically split since our field of definition is algebraically closed.

T acts on G by conjugation, and this induces an action of $\mathfrak{t} := \mathrm{Lie}(T)$ on $\mathfrak{g} = \mathrm{Lie}(G)$. Since T is a torus, it acts diagonalisably, and the weights of this action are called the **roots** of (G, T) and denoted by R. It is a well-known fact that $R = -R$. The roots are intrinsically characterised in terms of the group as follows.

Theorem 2.12. Let G be connected reductive. The minimal unipotent T-stable subgroups of G are all isomorphic to $\mathbb{G}_a$. A character $\alpha \in X^*(T)$ is a root of (G, T) if and only if there is some minimal unipotent T-stable one-parameter subgroup $u : \mathbb{G}_a \to T$ such that for all $t \in T$ one has

$$tu(x)t^{-1} = u(\alpha(t)x).$$

Proof. This is [2], Theorem 2.3.1 (i). □

We have notions of positive and simple roots:

Definition 2.13. Let G be connected reductive, let T be a maximal torus in G and let Φ be the set of roots.

1. A subset $\Phi_+ \subseteq \Phi$ is called a **set of positive roots** if it satisfies the following two properties:
   (a) $\Phi = \Phi^+ \amalg -\Phi^+$.
   (b) If $\alpha, \beta \in \Phi^+$ and $\alpha + \beta \in \Phi$, then $\alpha + \beta \in \Phi+$.
2. Fix a set of positive roots Φ^+. A subset Δ is called a **set of simple roots** for Φ^+ if every element of Φ^+ can be uniquely written as a $\mathbb{Z}_+$-linear combination of elements of Δ.

For any choice of root $\alpha \in R$, let $u_\alpha : \mathbb{G}_a \to G$ be the corresponding T-stable one-parameter subgroup. There is a homomorphism of algebraic groups $f_\alpha : \mathrm{SL}_2 \to G$ which satisfies

$$f_\alpha\left(\begin{pmatrix} 1 & \xi \\ 0 & 1 \end{pmatrix}\right) = u_\alpha(\xi)$$

and

$$f_\alpha\left(\begin{pmatrix} 1 & 0 \\ \xi & 1 \end{pmatrix}\right) = u_{-\alpha}(\xi)$$

for all $\xi \in k$. One can then define the coroot $\alpha^\vee$ as the cocharacter of T satisfying

$$\alpha^\vee(\xi) = f_\alpha\left(\begin{pmatrix} \xi & 0 \\ 0 & \xi^{-1} \end{pmatrix}\right)$$

for all $\xi \in k^\times$. Let G_α denote the image of f_α.

Definition 2.14. The **Weyl group** $W(G, T)$ of (G, T) is the quotient $N_G(T)/T$.

The Weyl group acts in obvious ways on the (co)characters of T.

Lemma 2.4. $W(G,T)$ is generated by $W(G_\alpha, T)$, where α ranges over the roots of (G,T).

Here are two tools that are helpful in performing calculations with reductive groups.

Theorem 2.15. Let G be a connected reductive group over k and let T be a maximal torus in G.

1. Let H be a closed connected subgroup of G which is normalised by T. Then, H is generated by $H^\circ \cap T$ and all root subgroups U_α which are contained in H.

2. There is a bijection between Borel subgroups and subsets of positive roots $\Phi^+ \subseteq \Phi$, given as follows: If B corresponds to Φ^+, then the unipotent radical $R_u(B)$ is equal to $\prod_{\alpha\in\Phi^+} U_\alpha$.

Proof. This is [2], Theorem 2.3.1, (iv) and (vi). □

3 BN-pairs and more distinguished subgroups

3.1 BN-pairs

We will see that reductive groups give rise to so-called BN-pairs.

Definition 3.1. Let G be a group. A BN-pair is a tuple (B,N) of subgroups of G subject to the following axioms.

(BN1) G is generated by B and N.

(BN2) $H := B \cap N$ is normal in N, the quotient $W := N/H$ is finite and generated by some set of involutions $S \subseteq W$.

(BN3) Let $s \in S$ and choose a lifting $n_s \in \pi^{-1}(s)$, where π denotes the canonical projection from N onto the quotient. Then, $n_s B n_s^{-1} \neq B$.

(BN4) Let $s \in S, n \in N$. Then, $n_s B n \subseteq B n_s n B \cup BnB$.

(B,N) is a **split** BN-pair if $B = U \rtimes H$.

Proposition 3.2. Let G be a reductive algebraic group. Fix a maximal torus T inside G and a Borel B containing T. Define $N := N_G(T)$. Then, (B,N) is a BN-pair.

Proof.

(BN1) Every element $g \in G$ is contained in some Borel, and N acts transitively on the set of Borel subgroups by conjugation. Hence, G is generated by B and N.

(BN2) By Lemma 2.4, W is generated by $W(G_\alpha, T)$, where α runs through the roots. But $W(G_\alpha, T)$ is generated by the simple reflection s_α through the coroot hyperplane associated to α, which is an involution.

(BN3) Let s be a simple reflection of W and let n_s be a lift of s. By the first part of 2.15, W operates freely on the set of subsets of positive roots. If B is the Borel associated to a set Φ_+ of simple roots, then $n_s B n_s^{-1}$ is the Borel associated to the set Φ'_+ of simple roots obtained from Φ_+ by replacing α with $-\alpha$. It follows that $B \neq n_s B n_s^{-1}$.

(BN4) This can be found in [4], 28.3.

□

Definition 3.3 (Coxeter system)**.** A **Coxeter system** is a tuple (W, S) where W is a group and S is a subset of W called the set of simple reflections, such that W has a presentation of the form

$$W = \langle s \in S \mid (s_i s_j)^{m_{ij}} = 1 \rangle$$

for integers $m_{ij} \in \mathbb{Z}_{\geq 2} \cup \{\infty\}$ subject to the relations $m_{ij} = m_{ji}$ and $m_{ii} = 1$. W is called a Coxeter group.

Remark. The same Coxeter group can be associated to different Coxeter systems. (See Exercise 3)

Definition 3.4 (Length of a Coxeter group element)**.** Let (W, S) be a Coxeter system and let $w \in W$.

1. A **reduced expression** for W is a word in S

$$s_{i_1} s_{i_2} \cdots s_{i_k}$$

   such that w is equal to the product of the s_{i_ℓ} and the word cannot be made shorter by applying the defining relations of W.

2. The **length** $\ell(w)$ of w is the length of a reduced expression for w. (One can show that this number is independent of the reduced expression chosen.)

Lemma 3.5. If G has a BN-pair (B, N) and (W, S) are as in the axiom (BN2), then (W, S) is a Coxeter system.

Proof. See [2], Theorem 3.1.3. □

Lemma 3.6. If G is a reductive group, $T \leq G$ a maximal torus, $B \leq G$ a Borel, and (W, S) is the Coxeter system associated to the root system of G, then for any $w \in W$, the length of w is equal to the cardinality of $w\Phi^+ \cap \Phi^-$.

The existence of a BN-pair on G implies an incredibly powerful structural result: The Bruhat decomposition.

Theorem 3.7 (Bruhat decomposition)**.** Let G be a group with a BN-pair (B, N). Then, G admits a decomposition

$$G = \coprod_{w \in W} B\dot{w}B,$$

where $\dot{w}$ is any lift of w in N.

Corollary 3.8. If G is a reductive group and the BN-pair on G is one of the natural ones, then one can sharpen the Bruhat decomposition slightly:

$$G = \coprod_{w \in W} B\dot{w}U_w,$$

where $U_w = (\dot{w}_0\dot{w})^{-1}U(\dot{w}_0\dot{w}) \cap U$.

Proof. We defer the proof to Exercise 4. □

3.2 Parabolic subgroups

Definition 3.9. Let (W, S) be a Coxeter system. A **standard parabolic subgroup** is a subgroup of W generated by some subset $I \subseteq S$.

Lemma 3.10. If W_I is a standard parabolic subgroup of W associated to $I \subseteq S$, then (W_I, I) is again a Coxeter system. For any $w \in W$, there is a unique coset representative wW_I in W/W_I (or $W_I\backslash W$) of minimal length. Moreover, for any $I, J \subseteq S$, there is a unique double coset representative W_IwW_J in $W_I\backslash W/W_J$ of minimal length.

Proof. This is [2], Lemmata 3.2.1. and 3.2.2 □

To any standard parabolic subgroup of a Weyl group acting on a root system we can associate a subset of roots.

Definition 3.11. Let (W, S) be a Coxeter system acting on a root system Φ. If $I \subseteq S$ is a subset, define $\Delta_I := \{\alpha \text{ simple root}, s_\alpha \in I\}$. Then, Φ_I is defined as $\mathbb{Q}\Delta_I \cap \Phi$.

Definition 3.12 (Parabolic subgroups of W)**.** Let (W, S) be a Coxeter system. A **parabolic subgroup** of W is a subgroup that is conjugated to some standard parabolic subgroup of W.

Definition 3.13 (Parabolic subgroups associated to a BN-pair)**.** Let G be a group with a BN-pair (B, N). A **parabolic subgroup** of G is a subgroup containing B.

We have given the same name to two different structures. Since nomenclature in mathematics is never confusing and always optimal, the following proposition should come as no surprise.

Proposition 3.14. Let G be a group with a BN-pair (B, N). The parabolic subgroups of G containing B are of the form BW_IB for some subset $I \subseteq S$. Moreover, one has the relative Bruhat decomposition with respect to any choice of two standard parabolic subgroups W_I, W_J of W:

$$G = \coprod_{\substack{w \in W_I \backslash W / W_J \\ \text{minimal}}} P_I \dot{w} P_J.$$

Proof. See [2], Proposition 3.2.3. □

3.3 Levi subgroups

Let G be a group with a BN-pair (B, N). Recall that B admits a semidirect product decomposition $B = U \rtimes T$ and that moreover $U = R_u(B)$. The following theorem generalises this decomposition to standard parabolics.

Theorem 3.15. Any standard parabolic $P_I \leq G$ admits a semidirect product decomposition

$$R_u(P_I) \rtimes L_I.$$

Moreover, $R_u(P_I)$ is the subgroup of U generated by the root subgroups U_α for $\alpha \in \Phi^+ \setminus \Phi_I$ and L_I is reductive.

Equivalently, a Levi subgroup of G can be defined as the centraliser of a subtorus $T' \subseteq T$:

Theorem 3.16. In the above setting, let T' be the subtorus of T defined as

$$T' = \bigcap_{\alpha \in \Phi_I} \ker \alpha.$$

Then, $L_I = C_G(T')$.

Proof. This is Proposition 3.4.6 in [2]. □

3.4 Descent for BN-pairs

Definition 3.17 (split BN-pairs)**.** Let G be a group. A BN-pair (B, N) of G is **split** if there exists a normal subgroup $U \leq B$ following conditions are satisfied.

1. $B = UH$ and $U \cap H = 1$. (This implies $B = U \rtimes H$.)

2. For all $n \in N$, one has $n^{-1}Bn \cap B \subseteq U$.

Let G be a reductive algebraic group with a split BN-pair (B, N) and let $\phi : G \to G$ be an automorphism. Consider $G^\phi := \{g \in G : \phi(g) = g\}$, the subgroup of G containing the ϕ-fixed points. Suppose that ϕ interacts nicely with (B, N) in that the following conditions are satisfied:

1. $\phi(B) = B.$, $\phi(N) = N$, and $\phi(U) = U$

2. If ϕ stabilises a coset $Hn \in H\backslash N$, then Hn contains a ϕ-fixed point.

One can then show that ϕ preserves the direct product decomposition $B = U \rtimes H$. Moreover, the second property implies that $W^\phi := N^\phi / H^\phi$ injects into W and its image is the subgroup of elements of w fixed by the induced map $\bar{\phi} : W \to W$. We can concretely identify W^ϕ as follows: ϕ induces an action on the simple reflections S, and every orbit $J \in S/\phi$ has a unique representative w_J of maximal length. Then, W^ϕ is exactly the subgroup of W generated by the w_J. (See [3], Subsection 1.7.)

Proposition 3.18. In the above setting, G^ϕ is generated by B^ϕ and N^ϕ and one has a Bruhat decomposition

$$G^\phi = \coprod_{w \in W^\phi} U^\phi H^\phi \dot{w} U^\phi_w,$$

where $U^\phi_w = (\dot{w}_0 \dot{w})^{-1} U^\phi (\dot{w}_0 \dot{w}) \cap U^\phi$.

Proposition 3.19. If U_{w_J} has a ϕ-fixed point for all $J \in S/\phi$, then (B^ϕ, N^ϕ) is a split BN-pair for G^ϕ.

Proof. This is Proposition 1.7.2 in [3]. □

4 Examples

4.1 GL_n

Let $G = \mathrm{GL}_n$. Recall that the functor of points is given as $G(R) = \{A \in M_n(R) : \det(A) \neq 0\}$. We describe the k-points of G. A split maximal torus of G is given by the diagonal matrices:

$$T = \{\mathrm{diag}(t_1, \dots, t_n) : t_i \in k\}.$$

The character lattice $X^*(T)$ is generated by the maps

$$\begin{aligned} \varepsilon_i : T &\longrightarrow \mathbb{G}_m \\ \mathrm{diag}(t_1, \dots, t_n) &\mapsto t_i \end{aligned}$$

and the cocharacter lattice $X_*(T)$ is generated by the maps

$$\begin{aligned} \eta_i : \mathbb{G}_m &\to T \\ t &\mapsto diag(1, \dots, t, \dots, 1), \end{aligned}$$

where t is the i-th diagonal entry.

The roots of T are given by $\alpha_{ij} = \varepsilon_i - \varepsilon_j$ for $i \neq j$. The root subgroup $U_{ij} := U_{\alpha_{ij}}$ is given by those $(n \times n)$-matrices which have nonzero entries only in the (i, j)-position.

Recall that the Weyl group W of G is given by $N_G(T)/T$. It is an exercise to show that $N_G(T)$ is the set of generalised permutation matrices. A system of representatives for W can then be given by the strict permutation matrices (i.e.

generalised permutation matrices with all entries equal to 0 or 1) and it follows that $W = S_n$.

Let us choose the Borel subgroup $B := \{A \in \mathrm{GL}_n : A \text{ upper-triangular}\}$. It corresponds to the choice of positive roots $\varepsilon_i - \varepsilon_j$ where $i < j$. The simple roots are given by $\alpha_1 = \varepsilon_1 - \varepsilon_2, \ldots, \alpha_{n-1} := \varepsilon_{n-1} - \varepsilon_n$, with corresponding simple reflection representatives $\dot{s}_i = E_{i,i+1} + E_{i+1,i}$.

We examine some parabolics of GL_4 in detail. Let $I := \{s_1\} \subseteq S_4 = W$. Then, $P_I = BW_IB = B \cup Bs_1B$. Note that

$$\begin{aligned}
Bs_1B &= U_1 s_1 B \\
&= U_1 \begin{pmatrix} * & * & * & * \\ * & 0 & * & * \\ 0 & 0 & * & * \\ 0 & 0 & 0 & * \end{pmatrix} \\
&= \begin{pmatrix} 1 & * & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} \begin{pmatrix} * & * & * & * \\ * & 0 & * & * \\ 0 & 0 & * & * \\ 0 & 0 & 0 & * \end{pmatrix} \\
&\subseteq \begin{pmatrix} * & * & * & * \\ * & * & * & * \\ & & * & * \\ & & & * \end{pmatrix}
\end{aligned}$$

and from this (and the Gauss-Jordan algorithm) it is not hard to see that P_I is indeed the subgroup of block matrices of the form

$$\begin{pmatrix} * & * & * & * \\ * & * & * & * \\ & & * & * \\ & & & * \end{pmatrix}.$$

Similarly, $B\langle s_1, s_2\rangle_W B$ is the subgroup of block matrices of the form

$$\begin{pmatrix} * & * & * & * \\ * & * & * & * \\ * & * & * & * \\ & & & * \end{pmatrix}.$$

By Theorem 3.16, L_I is the centraliser of the subtorus

$$T' = \bigcap_{\alpha \in \Phi_I} \ker \alpha.$$

of T. It is easy to check that this centraliser is normalised by T, and it is connected by Lemma 2.2. By theorem 2.15, it is generated by $C_G(T') \cap T$ and the root subgroups U_α it contains. Now, $[T, T'] = 1$ implies that $T \subseteq C_G(T')$ and hence $C_G(T') \cap T = T$, and one easily checks that the only root subgroups contained in $C_G(T')$ are those U_α for $\alpha \in \Phi_I$. It follows that

$$L_{\{s_i\}} = \left\{ \begin{pmatrix} * & * & & \\ * & * & & \\ & & * & \\ & & & * \end{pmatrix} \right\} \cong GL_2 \times \mathbb{G}_m^2.$$

Similarly, one has

$$L_{\{s_1,s_2\}} \cong GL_3 \times \mathbb{G}_m.$$

More generally, a subset I of simple reflections of S_n generates a subgroup isomorphic to $S_{k_1} \times \ldots \times S_{k_\ell}$, where the k_i define a partition of n. One then has $L_I \cong GL_{k_1} \times \ldots \times GL_{k_\ell}$.

4.2 Sp_4

Definition 4.1. Let M be the antidiagonal matrix with entries $(1,-1,1,-1)$. The algebraic group $Sp_4(k)$ is defined as the isometry group of the bilinear form defined by M:

$$Sp_4(k) = \left\{ A \in GL_4(k) : A^T M A = M \right\}.$$

There are two worthwhile ways to determine the structure of Sp_4: One by hand, using the above definition. The other way is to recognise Sp_4 as the set of fixed points of GL_4 under the automorphism

$$\begin{aligned} \phi : GL_4 &\to GL_4 \\ A &\mapsto M^{-1} A^T M \end{aligned}$$

and to use descent theory for BN-pairs.

We will first do it the pedestrian way, accepting the fact that $T_{GL_4} \cap Sp_4$ is a maximal torus T for Sp_4. The torus T can be easily determined to be the subgroup of diagonal matrices of the form

$$\begin{pmatrix} t_1 & & & \\ & t_2 & & \\ & & t_2^{-1} & \\ & & & t_1^{-1} \end{pmatrix},$$

where t_1 and t_2 are elements in $k^\times$.

The injection $i : T \hookrightarrow T_{GL_4}$ induces a surjection on characters: $i^* : X^*(T_{\mathrm{GL}_n}) \twoheadrightarrow X^*(T)$. One readily checks that $i^*(\varepsilon_1) = -i^*(\varepsilon_4)$ and $i^*(\varepsilon_2) = -i^*(\varepsilon_3)$, whence $X^*(T)$ is generated by ε_1 and ε_2. Dually, $X_*(T)$ is the sublattice of $X_*(GL_4)$ generated by the one-parameter subgroups

$$\begin{aligned} \lambda_1 : \mathbb{G}_m &\to T \\ t &\mapsto \begin{pmatrix} t & & & \\ & 1 & & \\ & & 1 & \\ & & & t^{-1} \end{pmatrix} \end{aligned} \qquad \text{and} \qquad \begin{aligned} \lambda_2 : \mathbb{G}_m &\to T \\ t &\mapsto \begin{pmatrix} 1 & & & \\ & t & & \\ & & t^{-1} & \\ & & & 1 \end{pmatrix}. \end{aligned}$$

We determine the roots of Sp_4 by means of the Lie algebra. Differentiating the condition $A^T M A = M$ at $A = \mathbb{1}$ yields

$$\mathfrak{sp}_4 = \left\{X \in \mathfrak{gl}_4 : MX + X^T M = 0\right\} = \left\{ \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & -a_{13} \\ a_{31} & a_{32} & -a_{22} & -a_{12} \\ a_{41} & -a_{31} & -a_{21} & -a_{11} \end{pmatrix} \right\}$$

Consider now the conjugation by a torus element $t = \mathrm{diag}(t_1, t_2, t_2^{-1}, t_1^{-1}$. One computes

$$t \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & -a_{13} \\ a_{31} & a_{32} & -a_{22} & -a_{12} \\ a_{41} & -a_{31} & -a_{21} & -a_{11} \end{pmatrix} t^{-1} = \begin{pmatrix} a_{11} & t_1 t_2^{-1} a_{12} & t_1 t_2 a_{13} & t_1^2 a_{14} \\ t_1^{-1} t_2 a_{21} & a_{22} & t_2^2 a_{23} & -t_1 t_2 a_{13} \\ t_1^{-1} t_2^{-1} a_{31} & t_2^{-2} a_{32} & -a_{22} & -t_1 t_2^{-1} a_{12} \\ t_1^{-2} a_{41} & -t_1^{-1} t_2^{-1} a_{31} & -t_1^{-1} t_2 a_{21} & -a_{11} \end{pmatrix}$$

and thus the roots of Sp_4 are given by $\{\pm 2\varepsilon_1, \pm(\varepsilon_1 + \varepsilon_2), \pm(\varepsilon_1 - \varepsilon_2), \pm 2\varepsilon_2\}$.

The unipotent root subgroups are given as follows.

$$\begin{aligned} U_{2\varepsilon_1} &= \{\mathbb{1} + \lambda E_{14} \mid \lambda \in k\}. \\ U_{\varepsilon_1 - \varepsilon_2} &= \{\mathbb{1} + \lambda(E_{12} - E_{34}) \mid \lambda \in k\}. \\ U_{\varepsilon_1 + \varepsilon_2} &= \{\mathbb{1} + \lambda(E_{13} - E_{24}) \mid \lambda \in k\}. \\ U_{2\varepsilon_2} &= \{\mathbb{1} + \lambda E_{23} \mid \lambda \in k\}. \end{aligned}$$

The root subgroups $U_{-\alpha}$ are obtained from U_α by transposition.

One can again show that $N_G(T)$ is given by the monomial matrices in G (Exercise.) Note that the monomial matrices centralising M must have entries equal to ± 1. From this it is an exercise to work out the representatives of $N_G(T)/T$. Concretely, they are given as follows:

$$\begin{pmatrix} & & & 1 \\ & 1 & & \\ & & 1 & \\ -1 & & & \end{pmatrix}, \begin{pmatrix} 1 & & & \\ & & 1 & \\ & -1 & & \\ & & & 1 \end{pmatrix}, \begin{pmatrix} & 1 & & \\ 1 & & & \\ & & & -1 \\ & & -1 & \end{pmatrix}, \begin{pmatrix} & & 1 & \\ & & & 1 \\ 1 & & & \\ & 1 & & \end{pmatrix},$$

$$\begin{pmatrix} 1 & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix}, \begin{pmatrix} & & 1 & \\ 1 & & & \\ & & & -1 \\ & 1 & & \end{pmatrix}, \begin{pmatrix} & & & 1 \\ & & -1 & \\ & 1 & & \\ -1 & & & \end{pmatrix}, \begin{pmatrix} & 1 & & \\ & & & 1 \\ 1 & & & \\ & & -1 & \end{pmatrix}.$$

By looking at generators and relations of W, it is easy to see that $W \cong D_8$.

The subgroup $B = B_{\mathrm{GL}_n} \cap Sp_4$ is a Borel subgroup of Sp_4. It corresponds to a choice $\Phi^+ = \{2\varepsilon_1, \varepsilon_1 + \varepsilon_2, \varepsilon_1 - \varepsilon_2, 2\varepsilon_2\}$ of positive roots. The simple roots are given by $\{2\varepsilon_2, \varepsilon_1 - \varepsilon_2\}$. One verifies that the simple reflections associated to $2\varepsilon_2$ and $\varepsilon_1 - \varepsilon_2$ are given by

$$\begin{pmatrix} 1 & & & \\ & & 1 & \\ & -1 & & \\ & & & 1 \end{pmatrix} \text{ and } \begin{pmatrix} & 1 & & \\ 1 & & & \\ & & & -1 \\ & & -1 & \end{pmatrix},$$

respectively. (The way one verifies this is to check that s_α sends α to $-\alpha$ and permutes the other positive roots. Recall that s acts on a root β by

$$(s.\beta)(t) = \beta(\dot{s}t\dot{s}^{-1}),$$

where $\dot{s}$ is a lift of s in $N_G(T)$.) There are two minimal parabolics containing B, one for each simple root:

$$P_{2\varepsilon_2} = \begin{pmatrix} * & * & * & * \\ & * & * & * \\ & {\color{red}*} & * & * \\ & & & * \end{pmatrix} \text{ and } P_{\varepsilon_1-\varepsilon_2} = \begin{pmatrix} * & * & * & * \\ {\color{red}*} & * & * & * \\ & & * & * \\ & & {\color{red}*} & * \end{pmatrix}.$$

Finally, to determine the Levi subgroups, we again use the fact that L_I is generated by T and the root subgroups U_α for $\alpha \in \Phi_I$. First, we look at the long root $2\varepsilon_2$. One has

$$L_I := \left\langle \begin{pmatrix} t_1 & & & \\ & t_2 & & \\ & & t_2^{-1} & \\ & & & t_1^{-1} \end{pmatrix}, \begin{pmatrix} 1 & & & \\ & 1 & t & \\ & & 1 & \\ & & & 1 \end{pmatrix}, \begin{pmatrix} 1 & & & \\ & 1 & & \\ & t & 1 & \\ & & & 1 \end{pmatrix} : t \in k \right\rangle.$$

Note that the root subgroups only "interact" with the subtorus with diagonal entries $(1, t_2, t_2^{-1}, 1)$. In fact, one can check that the map

$$\begin{aligned} L_I &\to SL_2 \times \mathbb{G}_m \\ \operatorname{diag}(t_1, t_2, t_2^{-1}, t_1^{-1}) &\mapsto (\operatorname{diag}(t_2, t_2^{-1}), t_1) \\ u_{2\varepsilon_2}(t) &\mapsto \left(\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}, 1 \right) \\ u_{-2\varepsilon_2}(t) &\mapsto \left(\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}, 1 \right) \end{aligned}$$

extends to an isomorphism of algebraic groups. In a similar fashion, one can show that $L_{\varepsilon_1-\varepsilon_2}$ is isomorphic to a copy of GL_2.

5 Frobenius maps

5.1 Motivation and definition

Let $k := \bar{\mathbb{F}}_p$ be the algebraically closed field of characteristic p. For every $m \in \mathbb{N}$ one has a subfield $\mathbb{F}_{p^m}$ of k with p^m elements. (Commonly, one uses the notation $q := p^m$.) Now, if X is an affine subvariety of k^n whose algebra of regular functions is of the form $\mathcal{O}_X \leq \mathbb{F}_q[x_1, \ldots, x_n]$, then X is stable under the q-Frobenius $F_q := (x_1, \ldots, x_n) \mapsto (x_1^q, \ldots, x_n^q)$, and the set of fixed points

$$X^{F_q} = \{x \in X : F_q(x) = x\} = X \cap \mathbb{F}_q$$

is a finite subvariety of X. Using the freshman's dream, the image of the induced pullback map

$$F_q^* : \mathcal{O}_X \to \mathcal{O}_X$$

is generated by elements x_i^q, where $x_i \in \mathcal{O}_X$ is the image of the generator X_i under the quotient map $k[X_1, \ldots, X_n] \twoheadrightarrow \mathcal{O}_X$. Conversely, this is the universal way in which finite type varieties over k behave under the Frobenius: If A is a finitely generated subalgebra of $k[x_1, \ldots, x_n]$, then the generators of A can be chosen to lie in some finite field extension F of $\mathbb{F}_p$, which must be one of the $F_{q'}$ for q' a prime power. Hence, some high enough power q^ℓ must satisfy $F_{q^\ell}^* A = A^{q^\ell}$. This observation naturally leads us to the following definition:

Definition 5.1 (Frobenius map)**.** Let $(X, \mathcal{O}_X)$ be an affine variety of finite type over k. A morphism $F : X \to X$ is called a **Frobenius map** if there exists some prime power $q = p^m$ such that the following conditions are satisfied:

1. $F^* \mathcal{O}_X = \mathcal{O}_X^q$
2. For all $f \in \mathcal{O}_X$, there exists some $\ell \in \mathbb{N}$ such that $(F^*)^\ell (f) = f^{q^\ell}$.

Under these conditions, we say that $(X, \mathcal{O}_X)$ is **defined over** $\mathbb{F}_q$ or **admits an** $\mathbb{F}_q$**-rational structure**.

It turns out that Frobenius maps on affine varieties admit a simple representation in terms of the standard Frobenius F_q on k^n:

Theorem 5.2. Let X be an affine variety defined over $\mathbb{F}_q$ with Frobenius $F : X \to X$. Then, there exists some closed embedding $\iota : X \to k^n$ such that the following square commutes:

$$\begin{array}{ccc} X & \xrightarrow{\iota} & k^n \\ \downarrow{\scriptstyle F} & & \downarrow{\scriptstyle F_q} \\ X & \xrightarrow{\iota} & k^n \end{array}$$

Moreover, $I(\iota(X))$ is generated by polynomials in $\mathbb{F}_q$, F is a bijection and X^F is finite.

Proof. This is Theorem 4.1.4 in [3]. □

We can obtain new Frobenius maps from old ones by restricting and by composing with finite order automorphisms:

Theorem 5.3. Let $(X, \mathcal{O}_X)$ be an affine variety defined over $\mathbb{F}_q$ and let F be the associated Frobenius. Let $Y \subseteq X$ be a closed F-stable subvariety. Then, $F|_Y$ is a Frobenius map for $(Y, \mathcal{O}_Y)$.

Proof. This is [3], Corollary 4.1.5. □

Theorem 5.4. Let $(X, \mathcal{O}_X)$ be an affine variety defined over $\mathbb{F}_q$ and let F be the associated Frobenius. Let $g : X \to X$ be a regular map which commutes with F and which satisfies $g^\ell = id_X$ for some $\ell \in \mathbb{N}$. Then, $F_g := F \circ g$ is again a Frobenius map for X.

Proof. This is [3], Exercise 4.7.4. $\square$

Definition 5.5 (Finite algebraic groups)**.** Let $(G, \mathcal{O}_G)$ be an affine algebraic group over k. We say that $(G, \mathcal{O}_G)$ is defined over $\mathbb{F}_q$ if $(G, \mathcal{O}_G)$ admits a $\mathbb{F}_q$-rational structure and the corresponding Frobenius commutes with the multiplication and inversion maps.

Remark. We will often drop $\mathcal{O}_G$ from the notation. If G is defined over $\mathbb{F}_q$ with Frobenius F, then the Frobenius fixed points G^F are a finite group.

Example 5.6. Let $G = \mathrm{GL}_n$. An invertible $(n \times n)$-matrix A with values in k is F_q-stable if and only if each entry of A is a F_q-fixed point (equivalently, if and only if each entry of A is contained in $\mathbb{F}_q$. It follows that $\mathrm{GL}_n(k)^F = \mathrm{GL}_n(\mathbb{F}_q)$.

Example 5.7. Consider the subgroup $\mathrm{SL}_n \leq \mathrm{GL}_n$. One checks that $\mathrm{SL}_n(k)$ is F_q-stable and thus F_q is the Frobenius for an $\mathbb{F}_q$-rational structure on $\mathrm{SL}_n(k)$ by Theorem 5.3. This way, one obtains $\mathrm{SL}_n(\mathbb{F}_q)$. In the same way, one can also obtain the finite symplectic and orthogonal groups.

Example 5.8. Using Theorem 5.4, we can construct more complicated finite algebraic groups from GL_n. In Exercise 7, we will construct the unitary group $\mathrm{U}_n(\mathbb{F}_q)$, which is notably not a subgroup of $\mathrm{GL}_n(\mathbb{F}_q)$ cut out by a polynomial condition.

We have a representation theorem similar to Theorem 5.2 for finite algebraic groups, perpetuating the slogan that GL_n is all one needs to know.

Theorem 5.9. Let G be a finite algebraic group defined over $\mathbb{F}_q$ with Frobenius F. Then, there exists an $n \in \mathbb{N}$ and a closed embedding $\iota : G \to \mathrm{GL}_n$ of algebraic groups such that the following diagram commutes:

$$\begin{tikzcd} G \arrow[r, "\iota"] \arrow[d, "F"] & \mathrm{GL}_n \arrow[d, "F_q"] \\ G \arrow[r, "\iota"] & \mathrm{GL}_n \end{tikzcd}$$

We can slightly weaken the notion of Frobenius map for algebraic groups.

Definition 5.10 (Generalised Frobenius map)**.** Let G be an algebraic group over k. A morphism $F : G \to G$ is a **generalised Frobenius map** if some positive power of F is a Frobenius map for an $\mathbb{F}_q$-rational structure for G.

5.2 The Lang-Steinberg theorem

The Lang-Steinberg theorem is fundamental for the theory of finite groups of Lie type.

Theorem 5.11 (Lang-Steinberg)**.** Let G be a connected algebraic group over k, and let $F : G \to G$ be a generalised Frobenius map. Then, the map

$$\begin{aligned} L : G &\to G \\ g &\mapsto g^{-1}F(g) \end{aligned}$$

is a dominant and finite morphism (so, in particular, it is surjective).

Theorem 5.12. Let G be a connected algebraic group over k and let $F : G \to G$ be a generalised Frobenius map. Let (B, N) be a BN-pair for G. Then, F has properties 1 and 2 from subsection 3.4.

Proof. The proof is left as Exercise 8. □

We can now reap the rewards of Propositions 3.18 and 3.19.

Corollary 5.13. (B^F, N^F) is a BN-pair for G^F. Moreover, one has a Bruhat decomposition

$$G^F = \coprod_{w \in W^F} U^F T^F \dot{w} U_w^F.$$

The first statement uses the following lemma and a theorem of Rosenlicht about cardinalities of unipotent groups modulo q:

Lemma 5.14. Let G be a reductive algebraic group over k with a BN-pair. Then, U_w is connected. If $\dim U = \ell(w_0)$, then $\dim U_w = \ell(w)$ for all $w \in W$.

Proof. See Lemma 4.2.1 in [3]. □

Theorem 5.15 (Rosenlicht)**.** Let U be a unipotent connected algebraic group over k admitting a rational structure over $\mathbb{F}_q$ with Frobenius F. Then, $|U^F| = q^{\dim U}$.

Proof. This is Theorem 4.2.4 in [3]. □

5.3 Group actions with a twist

Let G be an algebraic group over k admitting a rational structure over some $\mathbb{F}_q$ with corresponding Frobenius F, let X be a nonempty set with a transitive G-action, and let $F' : X \to X$ be a "twist" map compatible with the action of G in the sense that

1. $F'(g.x) = F(g).F'(x)$ for all $g \in G$ and $x \in X$.
2. For all (equivalently, for some) $x_0 \in X$, the stabiliser $H := \mathrm{Stab}_G(x_0)$ is a closed subgroup of G.

From Exercise 9, we know that $X^{F'}$ is nonempty, so let's pick an element x_0 which is fixed by F'. Let $A(x_0) := H/H^\circ$, where H° is the connected component of H containing the identity. For $h \in H$, denote by $\bar{h}$ the image in the quotient. Choose another $x \in X^{F'}$. There exists a $g \in G$ such that $x = g.x_0$ by transitivity of the action. One then computes

$$g.x_0 = x = F'(x) = F'(g.x_0) = F(g).F'(x_0) = F(g).x_0,$$

and it follows that $g^{-1}F(g)$ is contained in H and induces an element $\overline{g^{-1}F(g)} \in A(x_0)$. This motivates the following definition.

Definition 5.16. Define a relation $\sim \subseteq X^{F'} \times A(x_0)$ by requiring $x \sim a$ if and only if there exists some $g \in G$ such that $x = g.x_0$ and $\overline{g^{-1}F(g)} = a$.

Lemma 5.17. Let $x, x' \in X^{F'}$ and let $a, a' \in A(x_0)$. If $x \sim a$, $x' \sim a'$ and x is contained in the G^F-orbit of x', then a and a' are conjugate in $A(x_0)$.

Proof. This is a simple computation. □

Corollary 5.18. The relation $\sim$ induces a map

$$f_\sim : X^{F'}/G^F \to A(x_0)\backslash\backslash A(x_0).$$

(Here $H\backslash\backslash H$ means the set of conjugation classes for any group H)

Theorem 5.19. If G is connected, then $f_\sim$ is a bijection.

Proof. See [3], Theorem 4.3.5. □

Example 5.20. Let us apply the preceding theorem to a relevant question about finite groups of Lie type: Determining the maximal tori of G^F. Recall that over k, all maximal tori of G are conjugate. Hence G operates transitively on the set $X = \{T \leq G : T \text{ maximal torus}\}$ by conjugation. Let F be the the Frobenius for a $\mathbb{F}_q$-rational structure on G. Then, F induces an automorphism F' on X given by $T \mapsto F(T)$, and an action on W. The set of fixed points $X^{F'}$ is given by those tori of G stable under F. Exercise 9 implies that $X^{F'} \neq \emptyset$, and thus G has at least one F-stable torus (i.e. at least one maximal torus defined over $\mathbb{F}_q$.

Fix a maximal torus T_0 of G. Then, $Stab_G(T_0) = N_G(T_0)$. The identity component of $N_G(T_0)$ is exactly T_0, and thus $A(T_0) = W$, the Weyl group of G. Theorem 5.19 then asserts that the G^F-conjugation orbits of maximal tori of G^F are in bijection with the conjugacy classes of the subgroup $W^F \subseteq W$.

References

[1] A. Borel. *Linear Algebraic Groups.* Graduate Texts in Mathematics. Springer New York, 1991.

[2] François Digne and Jean Michel. *Representations of Finite Groups of Lie Type.* London Mathematical Society Student Texts. Cambridge University Press, 2 edition, 2020.

[3] M. Geck. *An Introduction to Algebraic Geometry and Algebraic Groups.* Oxford Graduate Texts in Mathematics. Clarendon Press, 2013.

[4] J.E. Humphreys. *Linear Algebraic Groups.* Graduate Texts in Mathematics. Springer New York, 2012.

[5] J. S. Milne. *Algebraic Groups: The Theory of Group Schemes of Finite Type over a Field.* Cambridge Studies in Advanced Mathematics. Cambridge University Press, 2017.