Linear algebraic groups and their Lie algebras

Daniel Miller

Fall 2014

Contents

1 Introduction

The latest version of these notes can be found online at `http://www.math.cornell.edu/~dkmiller/bin/6490.pdf`. Comments and corrections are appreciated.

1.1 Disclaimer

These notes originated in the course MATH 6490: Linear algebraic groups and their Lie algebras, taught by David Zywina at Cornell University. However, the notes have been substantially modified since then, and are not an exact reflection of the content and style of the original lectures. In particular, the notes often switch from a somewhat elementary approach to a more sheaf-theoretic approach. Any errors are solely the fault of the author.

1.2 Notational conventions

We follow Bourbaki in writing $\mathbf{N}, \mathbf{Z}, \mathbf{Q} \ldots$ for the natural numbers, integers, rationals, ... The natural numbers are $\mathbf{N} = \{1, 2, \ldots\}$.

If A is a commutative ring, M is an A-module, and $a \in A$, we write M/a for $M/(aM)$. In particular, A/a is the quotient of A by the ideal generated by a. All abelian groups will be treated as $\mathbf{Z}$-modules. So A is an abelian group and $n \in \mathbf{Z}$, the quotient A/n means $A/n \cdot A$ even if A is written multiplicatively.

The notation $X_{/S}$ will mean "X is a scheme over S." If $S = \operatorname{Spec}(A)$, we will write $X_{/A}$ to mean that X is a scheme over $\operatorname{Spec}(A)$.

We write ${}^{\mathrm{t}}x$ for the transpose of a matrix x.

Examples are closed with a triangle $\triangleright$.

Content that can be skipped will be delimited by a star $\star$. Usually this material will be much more advanced.

1.3 Main references

The standard texts are [Bor91; Hum75; Spr09]. In these, the requisite algebraic geometry is done from scratch in an archaic language. A good reference for modern (scheme-theoretic) algebraic geometry is [Har77], and a (very abstract) modern reference for algebraic groups is the three volumes on group schemes [SGA 3_{I}; SGA 3_{II}; SGA 3_{III}] from the *Séminaire de Géométrie Algébrique*. A source lying somewhat in the middle is Jantzen's book [Jan03].

1.4 A bestiary of examples

Let k be an algebraically closed field whose characteristic is *not* 2. For example, k could be $\mathbf{C}$ or $\overline{\mathbf{F}_p(t)}$. For now, we define a *linear algebraic group* over k to be a subgroup $G \subset \mathrm{GL}_n(k)$ defined by polynomial equations.

Example 1.4.1 (General linear)**.** The archetypal example of an algebraic group is $\mathrm{GL}_n(k) = \{g \in \mathrm{M}_n(k) : g \text{ is invertible}\}$. As a subset of $\mathrm{GL}_n(k)$, this is defined by the empty set of polynomial equations. $\triangleright$

Example 1.4.2 (Special linear)**.** Let $\mathrm{SL}_n(k) = \{g \in \mathrm{GL}_n(k) : \det(g) = 1\}$. This is defined by the equation $\det(g) = 1$. $\triangleright$

Example 1.4.3 (Orthogonal)**.** Let $\mathrm{O}_n(k) = \{g \in \mathrm{GL}_n(k) : g\, {}^{\mathrm{t}}g = 1\}$. This is cut out by the equations

$$\sum_{j=1}^{n} g_{ij} g_{kj} = \delta_{ik}$$

for $1 \leqslant i, k \leqslant n$. $\triangleright$

Example 1.4.4 (Special orthogonal)**.** This is $\mathrm{SO}_n(k) = \mathrm{O}_n(k) \cap \mathrm{SL}_n(k)$. $\triangleright$

Example 1.4.5. This group doesn't have a special name, but for the moment we will write $U_n(k)$ for the group of strictly upper triangular matrices:

$$U_n(k) = \begin{pmatrix} 1 & \cdots & * \\ & \ddots & \vdots \\ & & 1 \end{pmatrix} \subset \mathrm{GL}_n(k).$$

Recall that a matrix $g \in \mathrm{GL}_n(k)$ is *unipotent* if $(g-1)^m = 0$ for some $m \geqslant 1$. All elements of $U_n(k)$ are unipotent. The group $U_n(k)$ is defined by the equations

$$\{g_{ij} = 0 \text{ for } j < i, g_{ii} = 1\}.$$

▷

Example 1.4.6 (Multiplicative)**.** We write $\mathbf{G}_{\mathrm{m}}(k) = k^\times$ for the multiplicative group of k with its obvious group structure. Note that $\mathbf{G}_{\mathrm{m}} = \mathrm{GL}(1)$. ▷

Example 1.4.7 (Additive)**.** Write $\mathbf{G}_{\mathrm{a}}(k) = k$, with its additive group structure. There is a natural isomorphism $\varphi : \mathbf{G}_{\mathrm{a}} \xrightarrow{\sim} U_2$ given by $\varphi(x) = \begin{pmatrix} 1 & x \\ & 1 \end{pmatrix}$. Since

$$\begin{pmatrix} 1 & x \\ & 1 \end{pmatrix} \begin{pmatrix} 1 & y \\ & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ & 1 \end{pmatrix},$$

this is a group homomorphism, and it is easy to see that φ is an isomorphism of the underlying varieties. ▷

Example 1.4.8. For any $n \geqslant 0$, $\mathbf{G}_{\mathrm{a}}^n(k) = k^n$ with the usual addition is a linear algebraic group. We could embed it into $\mathrm{GL}_{2n}(k)$ via 2×2 blocks and the isomorphism $\mathbf{G}_{\mathrm{a}} \xrightarrow{\sim} U_2$ in Example 1.4.7. ▷

Example 1.4.9 (Tori)**.** For any $n \geqslant 0$, we have a *torus* of rank n, namely

$$T(k) = \begin{pmatrix} * & & \\ & \ddots & \\ & & * \end{pmatrix} \subset \mathrm{GL}_n(k).$$

This is clearly isomorphic to $\mathbf{G}_{\mathrm{m}}^n(k)$. We call any linear algebraic group isomorphic to some $\mathbf{G}_{\mathrm{m}}^n$ a torus. ▷

This list almost exhausts the class of simple algebraic groups over an algebraically closed field. All of these groups make sense over an arbitrary field. But over non-algebraically closed fields (or even base rings that are not fields) thinking of algebraic groups in terms of their sets of points doesn't work very well.

1.5 Coordinate rings

The standard references [Bor91; Hum75; Spr09] all treat algebraic groups in terms of their sets of points in an algebraically closed field. This leads to convoluted arguments, and (sometimes) theorems that are actually wrong. It is better to use schemes. Since we will (almost) never use non-affine schemes, we can study algebraic groups via their coordinate rings.

Example 1.5.1. Consider $G = \mathrm{GL}_n(k)$. For $g = (g_{ij}) \in \mathrm{M}_n(k)$, we have $g \in G$ if and only if $\det(g) \neq 0$. But this isn't an honest algebraic equation. We can remedy this by noting that $\det(g) \neq 0$ if and only if there exists $y \in k$ such that $\det(g) \cdot y = 1$. Thus we can define the *coordinate ring* $k[G]$ of G, as

$$k[G] = k[x_{ij}, y]/(\det(x_{ij})y - 1).$$

For k-algebras A, B, write $\hom_k(A, B)$ for the set of k-algebra homomorphisms $A \to B$. There is a natural identification

$$\hom_k(k[G], k) = \mathrm{GL}_n(k).$$

For $\varphi : k[G] \to k$, put $g_{ij} = \varphi(x_{ij})$ and $b = \varphi(y)$. Then φ is well-defined exactly if $\det(g) \cdot b = 1$. So φ is uniquely determined by the choice of an invertible matrix $g \in \mathrm{GL}_n(k)$. Since b is determined by g and g can be chosen arbitrarily in $\mathrm{GL}_n(k)$, this correspondence is a bijection. So in some sense, $k[G]$ recovers $\mathrm{GL}_n(k)$. ▷

Now let k be an arbitrary field. For concreteness, you could think of one of $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$, or $\mathbf{F}_p$. Put $A = k[x_{ij}, y]/(\det(x_{ij})y - 1)$, and define $\mathrm{GL}_n(R) = \hom_k(A, R)$ for any k-algebra R. We will think of "$\mathrm{GL}(n)_{/k}$" as $\operatorname{Spec}(A)$, which is a topological space with structure sheaf (essentially) A. The punchline is that the coordinate ring $k[G]$ of an algebraic group G determines everything we need to know about G.

Example 1.5.2. Let k be a field not of characteristic 2. For $d \in k^\times$, let $G_d \subset \mathbf{A}^2_{/k}$ be the subscheme cut out by $x^2 - dy^2 = 1$. In other words, $k[G_d] = k[x, y]/(x^2 - dy^2 - 1)$. The group operation is

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 x_2 + dy_1 y_2, x_1 y_2 + x_2 y_1).$$

We would like to realize G_d as a matrix group. Consider the map $\varphi_d : G_d \to \mathrm{GL}(2)_{/k}$ given by $(x, y) \mapsto \begin{pmatrix} x & dy \\ y & x \end{pmatrix}$. As an exercise, check that this is an isomorphism between G_d and the subgroup $\{g_{11} = g_{22}, x_{12} = dx_{21}\}$ of $\mathrm{GL}(2)_{/k}$.

If $k = \bar{k}$, then consider the composite of $G_d \hookrightarrow \mathrm{GL}(2)_{/k} \xrightarrow{\sim} \mathrm{GL}(2)_{/k}$, the second map being given by

$$g \mapsto \begin{pmatrix} & \sqrt{d} \\ 1 & \end{pmatrix} g \begin{pmatrix} & \sqrt{d} \\ 1 & \end{pmatrix}^{-1}.$$

It sends $(x, y) \in G_d$ to $\begin{pmatrix} a & b\sqrt{d} \\ b\sqrt{d} & a \end{pmatrix}$. This has the same image as $\varphi_1 : G_1 \to \mathrm{GL}(2)_{/k}$. So if $k = \bar{k}$, then $G_d \simeq G_1$. ▷

⋆ Write $A_d = k[x]/(x^2 - d)$. A more conceptual definition of G_d is that it is the restriction of scalars $G_d = \mathrm{R}_{A_d/k}\, \mathbf{G}_{\mathrm{m}}$. That is, for any k-algebra A, we have $G_d(A) = \mathbf{G}_{\mathrm{m}}(A \otimes_k A_d)$. ⋆

Example 1.5.3. Set $k = \mathbf{R}$. We claim that $G_1 \not\simeq G_{-1}$. We give a topological proof. The group $G_1(\mathbf{R}) \subset \mathbf{A}^2(\mathbf{R})$ is cut out by $x^2 - y^2 = 1$, hence non-compact. But $G_{-1}(\mathbf{R}) = \{x^2 + y^2 = 1\}$ is compact. Thus $G_1 \not\simeq G_{-1}$ over $\mathbf{R}$. But we have seen that $G_{-1} \simeq G_1$ "over $\mathbf{C}$." As an exercise, convince yourself that $G_1 \simeq \mathbf{G}_{\mathrm{m}}$. ▷

It turns out that "twists of $\mathbf{G}_{\mathrm{m}}$ over k up to isomorphism" are in bijective correspondence with $k^\times/2$, via the correspondence $d \mapsto G_d$.

$\star$ This is easy to see. The k-forms of $\mathbf{G}_{\mathrm{m}}$ is in natural bijection with $\mathrm{H}^1(k, \mathrm{Aut}\,\mathbf{G}_{\mathrm{m}}) = \mathrm{H}^1(k, \mathbf{Z}/2)$. Kummer theory tells us that $\mathrm{H}^1(k, \mathbf{Z}/2) = k^\times/2$. $\star$

1.6 Structure theory for linear algebraic groups

Let G be linear algebraic group over k. There is a filtration of normal subgroups

$$\begin{array}{l}
\begin{array}{lll} \phantom{\text{unipotent}} & G & \\ & \cup & \text{finite} \end{array}\\
\left.\begin{array}{lll} \text{connected} & G^\circ & \\ & \cup & \text{semisimple} \\ \text{solvable} & \mathcal{R}G & \\ & \cup & \text{torus} \\ \text{unipotent} & \mathcal{R}_{\mathrm{u}}G & \end{array}\right\}\text{reductive}\\
\begin{array}{lll} \phantom{\text{unipotent}} & \cup & \\ & 1 & \end{array}
\end{array}$$

Here, G° is the *identity component* (for the Zariski topology) of G. The quotient $\pi_0(G) = G/G^\circ$ is a finite group. We write $\mathcal{R}G$ for the *radical* of G, namely the maximal smooth connected solvable normal subgroup of G. Finally, $\mathcal{R}_{\mathrm{u}}G$ is the *unipotent radical* of G, namely the largest smooth connected unipotent subgroup of G. The quotient $G^\circ/\mathcal{R}G$ is semisimple, and the quotient $G^\circ/\mathcal{R}_{\mathrm{u}}G$ is reductive. In general, we say a connected algebraic group G is *semisimple* if $\mathcal{R}G = 1$, and *reductive* if $\mathcal{R}_{\mathrm{u}}G = 1$.

We've seen examples of tori and unipotent groups, and everybody knows plenty of finite groups. Here is a more direct definition of semisimple groups that allows us to give some basic examples.

Example 1.6.1 (Semisimple)**.** Let $k = \mathbf{C}$, and let G be a connected linear algebraic group over k. We say that G is *simple* if it is non-commutative, and has no proper nontrivial closed normal subgroups. We say G is *almost simple* if the only such subgroups are finite.

For example, $\mathrm{SL}(2)$ is almost simple, because its only nontrivial closed normal subgroup is $\{\pm 1\}$.

A group G is *semisimple* if we have an isogeny $G_1 \times \cdots \times G_r \to G$ with the G_i almost simple. Here an *isogeny* is a surjection with finite kernel. $\triangleright$

Over $\mathbf{C}$, the almost simple groups (up to isogeny) are:

label	group	dimension
A_n $(n \geqslant 1)$	$\mathrm{SL}(n+1)$	$n^2 - 1$
B_n $(n \geqslant 2)$	$\mathrm{SO}(2n+1)$	$n(2n+1)$
C_n $(n \geqslant 3)$	$\mathrm{Sp}(2n)$	$n(2n+1)$
D_n $(n \geqslant 4)$	$\mathrm{SO}(2n)$	$n(2n-1)$

We make requirements on the index in these families to prevent degenerate cases (e.g. $\mathrm{B}_1 = 1$) or matching (e.g. $\mathrm{A}_2 = \mathrm{C}_2$). There are five *exceptional groups*

label	dimension
E_6	78
E_7	133
E_8	248
F_4	52
G_2	14

Later on, we'll be able to understand why this list is complete.

2 Lie algebras

A Lie algebra is a linear object whose representation theory is (in principle) manageable. To any linear algebraic group G we will associate a Lie algebra $\mathfrak{g} = \mathrm{Lie}(G)$, and study the representation theory of G via that of $\mathfrak{g}$.

2.1 Definition and first properties

Fix a field k. Eventually we'll avoid characteristic 2, and some theorems will only be valid in characteristic zero.

Definition 2.1.1. *A* Lie algebra *over k is a k-vector space $\mathfrak{g}$ equipped with a map $[\cdot,\cdot] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$ such that the following hold:*

- $[\cdot,\cdot]$ *is bilinear (it factors through $\mathfrak{g} \otimes \mathfrak{g}$).*
- $[x, x] = 0$ *for all $x \in \mathfrak{g}$ ($[\cdot,\cdot]$ factors through $\bigwedge^2 \mathfrak{g}$).*
- *The Jacobi identity $[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$ holds for all $x, y, z \in \mathfrak{g}$.*

We could have defined a Lie algebra over k as being a k-vector space $\mathfrak{g}$ together with $[\cdot,\cdot] : \bigwedge^2 \mathfrak{g} \to \mathfrak{g}$ satisfying the Jacobi identity. We call $[\cdot,\cdot]$ the *Lie bracket.*

The Lie bracket satisfies a number of basic properties. For example, $[x, y] = -[y, x]$ because

$$\begin{aligned} 0 &= [x + y, x + y] && \text{(alternating)} \\ &= [x, x] + [x, y] + [y, x] + [y, y] && \text{(bilinear)} \\ &= [x, y] + [y, x]. && \text{(alternating)} \end{aligned}$$

Later on, we'll use an alternate form of the Jacobi identity:

$$[x, [y, z]] - [y, [x, z]] = [[x, y], z]. \tag{$*$}$$

2.2 The main examples

Example 2.2.1. Let V be any k-vector space. Then the zero map $\bigwedge^2 V \to V$ trivially satisfies the Jacobi identity. We call any Lie algebra whose bracket is identically zero *commutative* (or *abelian*). ▷

Example 2.2.2 (General linear)**.** Again, let V be a k-vector space. The Lie algebra $\mathfrak{gl}(V) = \mathrm{End}_k(V)$ as a k-vector space, with bracket $[X, Y] = X \circ Y - Y \circ X$. It is a good exercise (which everyone should do at least once in their life) to check that this actually is Lie algebra. When $V = k^n$, we write $\mathfrak{gl}_n(k)$ instead of $\mathfrak{gl}(k^n)$. ▷

Often, we will just write $\mathfrak{gl}_n$ instead of $\mathfrak{gl}_n(k)$. We will also do this for the other "named" Lie algebras.

Example 2.2.3 (Special linear)**.** Put $\mathfrak{sl}_n(k) = \{X \in \mathfrak{gl}_n(k) : \mathrm{tr}\, x = 0\}$. Since $\mathrm{tr}[x, y] = 0$, this is a Lie subalgebra of $\mathfrak{gl}_n$. In fact, $[\mathfrak{gl}_n, \mathfrak{gl}_n] \subset \mathfrak{sl}_n$. ▷

Example 2.2.4 (Special orthogonal)**.** Put $\mathfrak{so}_n(k) = \{x \in \mathfrak{gl}_n(k) : {}^{\mathrm{t}}x = -x\}$. This is a Lie subalgebra of $\mathfrak{gl}_n(k)$ because if $x, y \in \mathfrak{so}_n(k)$, then

$$\begin{aligned} {}^{\mathrm{t}}[x, y] &= {}^{\mathrm{t}}y\, {}^{\mathrm{t}}x - {}^{\mathrm{t}}x\, {}^{\mathrm{t}}y \\ &= (-y)(-x) - (-x)(-y) \\ &= -[x, y]. \end{aligned}$$

▷

Example 2.2.5 (Symplectic)**.** Let $J_n = \begin{pmatrix} & -1_n \\ 1_n & \end{pmatrix} \in \mathfrak{gl}_{2n}(k)$. Put

$$\mathfrak{sp}_{2n}(k) = \{x \in \mathfrak{gl}_{2n}(k) : Jx + {}^{\mathrm{t}}xJ = 0\}.$$

As an exercise, check that this is a Lie subalgebra of $\mathfrak{gl}_{2n}$. ▷

As an exercise, show that $\mathbf{R}^3$ with the bracket $[u, v] = u \times v$ (cross product) is a Lie algebra over $\mathbf{R}$.

Theorem 2.2.6 (Ado)**.** *Any finite dimensional Lie algebra over k is isomorphic to a Lie subalgebra of some $\mathfrak{gl}_n(k)$.*

Proof. In characteristic zero, this is in [Lie_{1-3}, I §7.3]. The positive-characteristic case is dealt with in [Jac79, VI §3]. □

Another good exercise is to realize $\mathbf{R}^3$ with bracket $[u, v] = u \times v$ as a subalgebra of some $\mathfrak{gl}_n(\mathbf{R})$.

2.3 Homomorphisms and the adjoint representation

Definition 2.3.1. *A* homomorphism *of Lie algebras $\varphi : \mathfrak{g} \to \mathfrak{h}$ is a k-linear map such that $\varphi([x, y]) = [\varphi x, \varphi y]$.*

If $\varphi : \mathfrak{g} \to \mathfrak{h}$ is a homomorphism of Lie algebras, then $\mathfrak{a} = \ker(\varphi)$ is a Lie subalgebra of $\mathfrak{g}$. This is easy:

$$\begin{aligned}\varphi[x,y] &= [\varphi(x), \varphi(y)] \\ &= [0,0] \\ &= 0.\end{aligned}$$

Definition 2.3.2. *A Lie subalgebra* $\mathfrak{a}$ *of* $\mathfrak{g}$ *is an* ideal *if* $[\mathfrak{a}, \mathfrak{g}] \subset \mathfrak{a}$, *i.e.* $[a, x] \in \mathfrak{a}$ *for all* $a \in \mathfrak{a}$, $x \in \mathfrak{g}$.

Equivalently, $\mathfrak{a} \subset \mathfrak{g}$ is an ideal if $[\mathfrak{g}, \mathfrak{a}] \subset \mathfrak{a}$. If $\mathfrak{a} \subset \mathfrak{g}$ is an ideal, we define the *quotient algebra* $\mathfrak{g}/\mathfrak{a}$ to be $\mathfrak{g}/\mathfrak{a}$ as a vector space, with bracket induced by that of $\mathfrak{g}$. So

$$[x + \mathfrak{a}, y + \mathfrak{a}] = [x, y] + \mathfrak{a}.$$

Let's check that this makes sense. If $a_1, a_2 \in \mathfrak{a}$, then

$$\begin{aligned}[x + a_1, x + a_2] &= [x, y] + [x, a_2] + [a_1, y] + [a_1, a_2] \\ &\equiv [x, y] \pmod{\mathfrak{a}}.\end{aligned}$$

If $\varphi : \mathfrak{g} \to \mathfrak{h}$ is a Lie homomorphism, then we get an induced isomorphism $\mathfrak{g}/\ker(\varphi) \xrightarrow{\sim} \operatorname{im}(\varphi) \subset \mathfrak{h}$.

Example 2.3.3. Give k the trivial Lie bracket. Then $\operatorname{tr} : \mathfrak{gl}_n(k) \to k$ is a a homomorphism. Indeed,

$$\operatorname{tr}[x, y] = \operatorname{tr}(xy) - \operatorname{tr}(yx) = 0.$$

We could have defined $\mathfrak{sl}_n(k) = \ker(\operatorname{tr})$; this is an ideal in $\mathfrak{gl}_n$, and $\mathfrak{gl}_n(k)/\mathfrak{sl}_n(k) \xrightarrow{\sim} k$. ▷

Definition 2.3.4. *Let* $\mathfrak{g}$ *be a Lie algebra over* k. *The* adjoint representation *of* $\mathfrak{g}$ *is the map* $\operatorname{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$ *defined by* $\operatorname{ad}(x)(y) = [x, y]$ *for* $x, y \in \mathfrak{g}$.

It is easy to check that $\operatorname{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$ is k-linear, that is $\operatorname{ad}(cx) = c \operatorname{ad}(x)$ and $\operatorname{ad}(x+y) = \operatorname{ad}(x) + \operatorname{ad}(y)$. It is bit less obvious how the adjoint action behaves with respect to the Lie bracket. We compute

$$\begin{aligned}\operatorname{ad}([x, y])(z) &= [[x, y], z] \\ &=_{(*)} [x, [y, z]] - [y, [x, z]] \\ &= (\operatorname{ad}(x) \operatorname{ad}(y))(z) - (\operatorname{ad}(y) \operatorname{ad}(x))(z).\end{aligned}$$

Thus $\operatorname{ad}[x, y] = [\operatorname{ad}(x), \operatorname{ad}(y)]$ and we have shown that $\operatorname{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g})$ is a homomorphism of Lie algebras. If $n = \dim_k(\mathfrak{g}) < \infty$, then $\operatorname{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g}) \simeq \mathfrak{gl}_n(k)$ is an interesting finite-dimensional representation of $\mathfrak{g}$. If $\dim(\mathfrak{g}) > 1$, it cannot be surjective, and there are easy ways for it to fail to be injective.

Definition 2.3.5. *Let* $\mathfrak{g}$ *be a Lie algebra over* k. *The* center *of* $\mathfrak{g}$ *is*

$$\mathrm{Z}(\mathfrak{g}) = \{x \in \mathfrak{g} : [x, y] = 0 \text{ for all } y \in \mathfrak{g}\}.$$

Note that $\mathrm{Z}(\mathfrak{g}) = \ker(\mathrm{ad})$. There is a natural injection $\mathfrak{g}/\mathrm{Z}(\mathfrak{g}) \hookrightarrow \mathfrak{gl}(\mathfrak{g})$.

Definition 2.3.6. *A Lie algebra* $\mathfrak{g}$ *is* simple *if it is non-commutative, and has no ideals except* 0 *and* $\mathfrak{g}$.

Just as with simple algebraic groups, there is a classification theorem for simple Lie algebras. Even better, since Lie algebras are more "rigid" than algebraic groups, we don't have to worry about isogeny.

Theorem 2.3.7. *Let k be an algebraically closed field of characteristic zero. Up to isomorphism, every Lie algebra is a member of the following list:*

A_n $(n \geqslant 1)$	$\mathfrak{sl}_{n+1}$
B_n $(n \geqslant 2)$	$\mathfrak{so}_{2n+1}$
C_n $(n \geqslant 3)$	$\mathfrak{sp}_{2n}$
D_n $(n \geqslant 4)$	$\mathfrak{so}_{2n}$
exceptional	$\mathfrak{e}_6$, $\mathfrak{e}_7$, $\mathfrak{e}_8$, $\mathfrak{f}_4$, $\mathfrak{g}_2$

The classification theorem for algebraic groups is proved via the classification theorem for Lie algebras, which ends up being a matter of combinatorics.

2.4 Tangent spaces

For the sake of clarity, we give a scheme-theoretic definition of algebraic groups:

Definition 2.4.1. *Let S be a scheme. An* algebraic group *over S is an affine group scheme of finite type over S.*

For the moment, we will say that an algebraic group G over S is *linear* if G is a subgroup scheme of $\mathrm{GL}(\mathscr{L})$ for some locally free sheaf $\mathscr{L}$ on S.

Fix a field k, and let $G \subset \mathrm{GL}(n)_{/k}$ be a linear algebraic group cut out by polynomials $f_1, \dots, f_r$. For any k-algebra R, we define

$$G(R) = \{g \in \mathrm{GL}_n(R) : f_1(g) = \cdots = f_r(g) = 0\}.$$

This is a functor $\mathsf{Alg}_k \to \mathsf{Set}$. Since G is a subgroup scheme of $\mathrm{GL}(n)_{/k}$, the set $G(R)$ inherits the group structure from $\mathrm{GL}_n(R)$. So we will think of G as a functor $G : \mathsf{Alg}_k \to \mathsf{Grp}$. By the Yoneda Lemma, the variety G is determined by its functor of points $G : \mathsf{Alg}_k \to \mathsf{Set}$.

We are especially interested in the k-algebra of *dual numbers*, $k[\varepsilon] = k[x]/x^2$. Informally, ε should be thought of as a "infinitesimal quantity" in the style of Newton and Leibniz. The scheme $\mathrm{Spec}(k[\varepsilon])$ should be thought of as a "point together with a direction."

$\star$ For the moment, let k be an arbitrary base ring, $X_{/k}$ a scheme. We define the *n-Jet space* of X to be the scheme $\mathrm{J}_n X$ whose functor of points is $(\mathrm{J}_n X)(A) = X(A[t]/t^{n+1})$. By [Voj07], this functor is representable, so $\mathrm{J}_n X$ is actually a scheme. The first jet space $\mathrm{J}_1 X$ is called the *tangent space* of X, and denoted $\mathrm{T}X$. The maps $A[t]/t^{n+1} \twoheadrightarrow A[t]/t^n$ induce projections $\mathrm{J}_{n+1}X \to \mathrm{J}_n X$. In particular, the tangent space of X comes with a canonical projection $\pi : \mathrm{T}X \to X$. $\star$

Consider $G(k[\varepsilon])$. As a set, this consists of invertible $n \times n$ matrices with entries in $k[\varepsilon]$ on which the f_i vanish. The map $\varepsilon \mapsto 0$ from $k[\varepsilon] \to k$ induces a group homomorphism $\pi : G(k[\varepsilon]) \to G(k)$. We will consider this map as the "tangent space" of $G(k)$. For each $g \in G(k)$, the fiber $\pi^{-1}(g)$ is the "tangent space of G at g."

Note that

$$\pi^{-1}(g) = \{g + \varepsilon v : v \in \mathrm{M}_n(k) : f_i(g + \varepsilon v) = 0 \text{ for all } i\}.$$

For each s, the polynomial f_s has a Taylor series expansion

$$f_s(x_{ij}) = f_s(g) + \sum_{i,j} \frac{\partial f_s}{\partial x_{i,j}}(g)(x_{i,j} - g_{i,j}).$$

Since $f_s(g) = 0$, we get $f_s(g + \varepsilon v) = \varepsilon \sum_{i,j} \frac{\partial f_s}{\partial x_{i,j}}(g) v_{i,j}$. It follows that

$$\pi^{-1}(g) = \left\{ g + \varepsilon v : v \in \mathrm{M}_n(k) : \sum_{i,j} \frac{\partial f_s}{\partial x_{ij}}(g) v_{ij} = 0 \text{ for all } 1 \leqslant s \leqslant r \right\}.$$

We will be especially interested in $\mathfrak{g} = \pi^{-1}(1)$. We will turn this into a Lie algebra using the group structure on G.

$\star$ From the scheme-theoretic perspective, the identity element $1 \in G(k)$ comes from a section $e : \operatorname{Spec}(k) \to G$ of the structure $G \to \operatorname{Spec}(k)$. The *scheme-theoretic Lie algebra* of G is the fiber product

$$\mathfrak{g} = e^* 1 = \mathrm{T}(G) \times_G \operatorname{Spec}(k).$$

By definition, $\mathfrak{g}(A) = \ker\left(G(A[\varepsilon]) \to G(A)\right)$ for any k-algebra A. Just as with algebraic groups, we will write $\mathfrak{g}_{/k}$ for $\mathfrak{g}$ thought of as a group scheme over k, and just $\mathfrak{g}$ for $\mathfrak{g}(k)$. $\star$

2.5 Functors of points

Recall that schemes can be thought of as functors $\mathsf{Alg}_k \to \mathsf{Set}$. For example, affine n-space is the functor $\mathbf{A}^n(A) = A^n$. In fact, this is an algebraic group, the operation coming from addition on A. Moreover, $\mathbf{A}^n$ is *representable* in the sense that

$$\mathbf{A}^n(A) = \hom_k(k[x_1, \dots, x_n], A),$$

via $(a_1, \dots, a_n) \mapsto (x_i \mapsto a_i)$. Similarly, $\mathrm{SL}(n)_{/k}$ sends a k-algebra A to $\mathrm{SL}_n(A)$. It is represented by the ring $k[x_{ij}]/(\det(x) - 1)$. In general, we take some polynomials $f_1, \dots, f_r \in k[x_1, \dots, x_n]$, and consider the subscheme $X = V(f_1, \dots, f_r) \subset \mathbf{A}^n$ which represents the functor

$$X(A) = \{a \in A^n : f_1(a) = \cdots = f_r(a) = 0\}.$$

This has coordinate ring $k[x_1,\dots,x_n]/(f_1,\dots,f_r)$. Note that *any* finitely generated k-algebras is of this form. In other words, all affine schemes of finite type over k are subschemes of some affine space.

Clasically, one gives $X(\bar{k})$ the *Zariski topology.* If $f \in k[X] = \mathbf{A}^1(X)$, we get (by definition) a function $f : X(\bar{k}) \to \bar{k}$. We define open subsets of $X(\bar{k})$ to be those of the form $\{x \in X(\bar{k}) : f(x) \neq 0\}$. More scheme-theoretically, we say that an *open subscheme* of X is the complement of any $V(f)$ for $f \in k[X]$.

$\star$ We can think of the Zariski topology as giving a Grothendieck topology on the category of affine schemes over k. It is subcanonical, i.e. all representable functors are sheaves. So if we formally put $\mathsf{Aff}_k = (\mathsf{Alg}_k)^\circ$, then the category of schemes over k embeds into $\mathrm{Sh}_{\mathrm{zar}}(\mathsf{Aff}_k)$. When working with algebraic groups, often it is better with the étale or fppf topologies. In particular, we will think of quotients as living in $\mathrm{Sh}_{\mathrm{fppf}}(\mathsf{Aff}_k)$. $\star$

Definition 2.5.1. *Let k be a feld. A* variety *over k is a reduced separated scheme of finite type over k.*

In particular, an affine variety is determined by a reduced k-algebra. We can directly associate a "geometric object" to a k-algebra A, namely its *spectrum* $\mathrm{Spec}(A) = \{\mathfrak{p} \subset A \text{ prime ideal}\}$. Finally, we note that if $X = \mathrm{Spec}(A)$ is of finite type over k and if $k = \bar{k}$, then $X(k) = \hom_k(A, k)$ is the set of maximal ideas in A.

2.6 Affine group schemes and Hopf algebras

An affine group $G_{/k}$ will give us a functor $G : \mathsf{Alg}_k \to \mathsf{Grp}$. As such, it should have morphisms

$$\begin{aligned} m : G \times G &\to G && \text{“multiplication”} \\ e : 1 = \mathrm{Spec}(k) &\to G && \text{“identity”} \\ i : G &\to G && \text{“inverse”} \end{aligned}$$

These correspond to ring homomorphisms

$$\begin{aligned} \Delta &: A \to A \otimes_k A && \text{“comultiplication”} \\ \varepsilon &: A \to k && \text{“counit”} \\ \sigma &: A \to A && \text{“coinverse”} \end{aligned}$$

Obviously the maps on groups satisfy some axioms like associativity etc. These can be phrased by the commutativity of diagrams like

$$\begin{tikzcd} G \times G \times G \arrow[r, "\mathrm{id}\times m"] \arrow[d, "m\times \mathrm{id}"] & G \times G \arrow[d, "m"] \\ G \times G \arrow[r, "m"] & G. \end{tikzcd}$$

Most sources do not give all these diagrams explicitly. One that does is the book [Wat79].

It is a good exercise to show that we have the following maps for the additive and multiplicative groups:

group	ring	comultiplication	coident.	coinverse
$\mathbf{G}_{\mathrm{a}}$	$k[x]$	$x \mapsto x \otimes 1 + 1 \otimes x$	$x \mapsto 0$	$x \mapsto -x$
$\mathbf{G}_{\mathrm{m}}$	$k[x^{\pm 1}]$	$x \mapsto x \otimes x$	$x \mapsto 1$	$x \mapsto x^{-1}$

The analogue of associativity for coordinate rings and comultiplication is the commutativity of the following diagram:

$$\begin{tikzcd} A \arrow[r, "\Delta"] \arrow[d, "\Delta"] & A \otimes_k A \arrow[d, "\mathrm{id}\otimes\Delta"] \\ A \otimes_k A \arrow[r, "\Delta\otimes\mathrm{id}"] & A \otimes_k A \otimes_k A. \end{tikzcd}$$

The tuple $(A, \Delta, \varepsilon, \sigma)$ is called a *Hopf algebra*. In principle, all theorems about algebraic groups can be rephrased as theorems about Hopf algebras, but this is not very illuminating. The one advantage is that it is possible to speak of Hopf algebras for which the ring A is *not* commutative. These show up in algebraic number theory, combinatorics, and physics.

Theorem 2.6.1. *If G is an affine group scheme of finite type over k, then it is a linear algebraic group over k.*

Proof. This is [SGA 3_{I}, VI_{B} 11.11]. Essentially, one looks at the action of G on the (possibly infinite-dimensional) vector space $k[G]$. A general theorem yields a faithful finite-dimensional representation V, and we get G as a subgroup-scheme of $\mathrm{GL}(V)$. □

⋆ If S is a dedekind scheme (noetherian, one-dimensional, regular) and $G_{/S}$ is a affine flat separated group scheme of finite type over S, then the obvious generalization of Theorem 2.6.1 holds for G; it is a closed subgroup of $\mathrm{GL}(\mathscr{L})$ for $\mathscr{L}$ a locally free sheaf on S [SGA 3_{I}, VI_{B} 13.5]. Interestingly, this fails for more general base schemes. ⋆

2.7 Examples of group schemes

So all affine group varieties over k embed into $\mathrm{GL}(n)_{/k}$ *as an algebraic group*. We can think of an algebraic group in several ways:

1. As a group-valued functor on Alg_k.
2. As a commutative Hopf algebra over k.
3. As a subgroup of $\mathrm{GL}_n(k)$ cut out by poynomials.

Example 2.7.1. The group of *n-th roots of unity* is $\boldsymbol{\mu}_n$. Its coordinate ring is $k[x]/(x^n - 1)$. So

$$\boldsymbol{\mu}_n(A) = \{a \in A : a^n = 1\},$$

with the group operation coming from multiplication in A. Note that $\boldsymbol{\mu}_n \subset \mathbf{G}_{\mathrm{m}}$. If the base field k has characteristic $p \nmid n$, then $\boldsymbol{\mu}_n(\bar{k})$ is a cyclic group of order n. However, if $n = p$, then $x^p - 1 = (x-1)^p$. So the coordinate ring $k[x]/((x-1)^p)$ is non-reduced. This is our first example of a group scheme that is *not* a group variety. One realization of this is that $\boldsymbol{\mu}_p(\overline{\mathbf{F}_p}) = 1$. These problems can only occur in characteristic $p > 0$. If G is a group scheme over a characteristic zero field, then G is automatically reduced.

Let $\phi : \mathbf{G}_{\mathrm{m}} \to \mathbf{G}_{\mathrm{m}}$ be the homomorphism $x \mapsto x^p$. Note that $\ker(\phi) = \boldsymbol{\mu}_p$. On $\overline{\mathbf{F}}_p$-points, this map is an isomorphism, but ϕ is *not* an isomorphism of algebraic groups. ▷

Let $G_{/k}$ be a linear algebraic group. Recall that we defined the *Lie algebra* $\mathfrak{g} = \mathrm{Lie}(G)$ of G to be the functor on k-algebras given by

$$\mathfrak{g}(A) = \ker\left(G(A[\varepsilon]/\varepsilon^2) \to G(A)\right).$$

In subsection 2.4, we saw that if $G \subset \mathrm{GL}(n)_{/k}$ is cut out by $f_1, \ldots, f_r$, then the k-valued points could be computed as

$$\mathfrak{g} = \left\{ X \in \mathrm{M}_n(k) : \sum_{i,j} \frac{\partial f_\alpha}{\partial x_{ij}}(1_n) \cdot X_{ij} = 0 \right\}.$$

Example 2.7.2 (Special linear)**.** Consider $\mathrm{SL}(n)_{/k} \subset \mathrm{GL}(n)_{/k}$, cut out by $\det = 1$. Its Lie algebra $\mathfrak{sl}_n = \mathrm{Lie}(\mathfrak{sl}_n)$ is

$$\mathfrak{sl}_n = \{1 + x\varepsilon : x \in \mathrm{M}_n(k) \text{ and } \det(1 + x\varepsilon) = 1\}.$$

The expansion of determinant is $\det(1 + x\varepsilon) = 1 + \mathrm{tr}(x)\varepsilon + O(\varepsilon^2)$. Thus

$$\mathfrak{sl}_n = \{x \in \mathrm{M}_n : \mathrm{tr}(x) = 0\}.$$

As a functor on k-algebras, $\mathfrak{sl}_n(A) = \{x \in \mathrm{M}_n(A) : \mathrm{tr}\, x = 0\}$. ▷

Example 2.7.3 (Orthogonal)**.** Recall that $\mathrm{O}(n) \subset \mathrm{GL}(n)$ is cut out by $g\,{}^{\mathrm{t}}g = 1$. So

$$\begin{aligned}
\mathrm{Lie}(\mathrm{O}_n) &= \{1 + x\varepsilon : (1 + x\varepsilon)\,{}^{\mathrm{t}}(1 + x\varepsilon) = 1\} \\
&= \{1 + X\varepsilon : x + {}^{\mathrm{t}}X = 0\} \\
&\simeq \{X \in \mathrm{M}_n : {}^{\mathrm{t}}x = -x\} \\
&= \mathfrak{so}_n.
\end{aligned}$$

If the characteristic of the base field is not 2, then $\dim(\mathfrak{so}_n) = n(n-1)/2$. ▷

2.8 Lie algebra of an algebraic group

Fix a field k. Let $G_{/k}$ be a linear algebraic group. For any k-algebra A, write $A[\varepsilon] = k[t]/t^2$. Then $A \mapsto G(A[\varepsilon])$ is a new group functor, and we can define the *Lie algebra* of G to be

$$\mathrm{Lie}(G)(A) = \ker\left(G(A[\varepsilon]) \to G(A)\right).$$

A priori, this is a group functor. Often, we will write $\mathfrak{g} = \mathrm{Lie}(G)$ to mean $\mathrm{Lie}(G)(k)$. If $G \subset \mathrm{GL}(n)$ is cut out by $f_1, \dots, f_r$, then

$$\mathfrak{g} = \{1 + \varepsilon x : x \in \mathrm{M}_n(k) \text{ and } f_\alpha(1+\varepsilon x) = 0 \text{ for all } \alpha\}.$$

The group operation is addition on x, i.e. $(1+\varepsilon x)(1+\varepsilon y) = 1 + \varepsilon(x+y)$. Thus $\mathfrak{g}$ is a k-vector space.

$\star$ This section will contain many "high-level" interludes on the functorial definition of $\mathrm{Lie}(G)$. They are all strongly influenced by the exposition in [SGA 3_{I}, II §3–4]. Let $\mathscr{O} : \mathsf{Alg}_k \to \mathsf{Alg}_k$ be the functor $A \mapsto A$. Note that $\mathscr{O}$ is represented by $k[t]$. Thus $\mathbf{A}^1_{/k}$ has the structure not only of a group scheme, but of a k-ring scheme, or (k,k)-biring in the sense of [BW05]. We define an *$\mathscr{O}$-module* to be a functor $V : \mathsf{Alg}_k \to \mathsf{Set}$ such that for each A, the set $V(A)$ is given an $\mathscr{O}(A) = A$-module structure in a functorial way.

If $S : \mathsf{Alg}_k \to \mathsf{Set}$ is a functor, we will write Sch_S for the category of representable functors $X : \mathsf{Alg}_k \to \mathsf{Set}$ together with a morphism $X \to S$. A morphism $(X \to S) \to (Y \to S)$ in Sch_S is a morphism of functors $X \to Y$ making the following diagram commute:

$$\begin{tikzcd} X \arrow[r] \arrow[dr] & Y \arrow[d] \\ & S. \end{tikzcd}$$

There is an easy generalization of $\mathscr{O}$ to a ring object $\mathscr{O} \in \mathsf{Sch}_S$. It sends a scheme X to the ring $\mathrm{H}^0(X, \mathscr{O}_X)$ of regular functions on X.

For a scheme X, the first jet space $\mathrm{J}_1 X$ is naturally an $\mathscr{O}$-module in Sch_X. We could be fancy and say that for any ring A, $A[\varepsilon]$ is naturally an abelian group object in Alg_A/A, or we could define the $\mathscr{O}$-module structure on $\mathrm{J}_1 X \xrightarrow{\pi} X$ directly. For $\varphi : \mathrm{Spec}(A) \to X$, we need to give

$$(\mathrm{J}_1 X)_{/X}(A) = \{f \in (\mathrm{J}_1 X)(A) : \pi \circ f = \varphi\}$$

the structure of an A-module. Given $a \in A$, define $\sigma_a : A[\varepsilon] \to A[\varepsilon]$ by $\varepsilon \mapsto a\varepsilon$. This is a ring homomorphism, so it induces $\sigma_a : \mathrm{J}_1 X(A) \to \mathrm{J}_1 X(A)$. The restriction of this map to $(\mathrm{J}_1 X)_{/X}(A)$ is the desired action of A. See [SGA 3_{I}, II 3.4.1] for a more careful proof that this gives $(\mathrm{J}_1 X)_{/X}$ the structure of an $\mathscr{O}$-module in Sch_X.

The point of all this is that if M is an $\mathscr{O}$-module in Sch_Y and $f : X \to Y$ is a morphism of schemes, then $f^* M$, defined by

$$(f^*M)(\mathrm{Spec}(A) \xrightarrow{p} X) = M(\mathrm{Spec}(A) \xrightarrow{p} X \xrightarrow{f} Y)$$

is naturally an $\mathscr{O}$-module in Sch_X. So if G is an algebraic group, $\mathrm{J}_1 X$ is naturally an $\mathscr{O}$-module in Sch_G, and the morphism $e : 1 \to G$ gives $\mathfrak{g} = e^* \mathrm{J}_1 G$ the structure of an $\mathscr{O}$-module in Sch_k. $\star$

Example 2.8.1 (Symplectic)**.** Let $J = \begin{pmatrix} & -1_n \\ 1_n & \end{pmatrix}$. Recall that

$$\mathrm{Sp}_{2n}(A) = \left\{g \in \mathrm{GL}_{2n}(A) : {}^{\mathrm{t}}g J g = J\right\}.$$

Let's compute the Lie algebra of Sp_{2n}. For $X \in \mathrm{M}_{2n}(A)$, we have

$$\begin{aligned} {}^{\mathrm{t}}(1+\varepsilon x)J(1+\varepsilon x) &= (1+\varepsilon\, {}^{\mathrm{t}}x)J(1+\varepsilon x) \\ &= J + \varepsilon({}^{\mathrm{t}}xJ + Jx). \end{aligned}$$

So $\mathfrak{sp}_{2n}(A) \simeq \{x \in \mathrm{M}_{2n}(A) : {}^{\mathrm{t}}xJ + Jx = 0\}$. ▷

Algebraic groups can be highly non-abelian, and so far all we've done is give $\mathfrak{g} = \mathrm{Lie}(G)$ the structure of a vector space. We'd like to give $\mathfrak{g}$ the structure of a Lie algebra.

Let $f : G \to H$ be a homomorphism of algebraic groups. Then $f : G(A) \to H(A)$ is a homomorphism for all k-algebras A. A morphism $f : G \to H$ corresponds by the Yoneda Lemma to a unique element $\varphi \in \hom_k(k[H], k[G])$. For all A, the induced map $G(A) \to H(A)$ is defined by $\psi \mapsto \psi \circ \varphi$ via the identifications $G(A) = \hom(k[G], A)$ and $H(A) = \hom(k[H], A)$.

Example 2.8.2. Recall that $\mathbf{G}_{\mathrm{m}}(A) = A^{\times} = \hom(k[x^{\pm 1}], A)$. All homomorphisms $f : \mathbf{G}_{\mathrm{m}} \to \mathbf{G}_{\mathrm{m}}$ come from $x \mapsto x^n$ for some $n \in \mathbf{Z}$. On functors of points, this is $a \mapsto a^n$ for $a \in A^{\times}$. ▷

As before, let $f : G \to H$ be a morphism of algebraic groups. Let $\mathfrak{g} = \mathrm{Lie}(G)$, $\mathfrak{h} = \mathrm{Lie}(G)$. There is an induced map $\mathrm{Lie}(f) : \mathfrak{g} \to \mathfrak{h}$. On functors of points, it is induced by the inclusions $\mathfrak{g} \subset \mathrm{J}_1 G$, $\mathfrak{h} \subset \mathrm{J}_1 H$ and the fact that $f : \mathrm{J}_1 G \to \mathrm{J}_1 H$ is a group homomorphism. That is, for each k-algebra A, $f_* : \mathfrak{g}(A) \to \mathfrak{h}(A)$ is induced by the commutative diagram

$$\begin{tikzcd} G(A[\varepsilon]) \arrow[r, "f"] & H(A[\varepsilon]) \\ \mathfrak{g}(A) \arrow[u, hook] \arrow[r, "f_*"] & \mathfrak{h}(A). \arrow[u, hook] \end{tikzcd}$$

In particular, a representation $\rho : G \to \mathrm{GL}(n)$ induces a map on Lie algebras $\mathfrak{g} \to \mathfrak{gl}_n$.

⋆ The natural way of stating the above is that Lie is a functor from group schemes over k to $\mathscr{O}$-modules in Sch_k. What's more, if G is a group scheme and $\mathfrak{g} = \mathrm{Lie}(G)$, then by [SGA 3_{I}, II 3.3], there is a natural isomorphism of A-modules $\mathfrak{g}(k) \otimes_k A \xrightarrow{\sim} \mathfrak{g}(A)$. So the functor $\mathfrak{g}$ is actually determined by the vector space $\mathfrak{g}(k)$. This justifies our passing between $\mathfrak{g}$ and $\mathfrak{g}(k)$. ⋆

Let's construct the Lie bracket on the Lie algebra of an algebraic group. Recall that for a Lie algebra $\mathfrak{g}$, we defined a map $\mathrm{ad} : \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g}) = \mathrm{End}_k(\mathfrak{g})$ by $\mathrm{ad}(x)(y) = [x, y]$. The bracket on $\mathfrak{g}$ is clearly determined by the adjoint map.

For $\mathfrak{g} = \mathrm{Lie}(G)$, we'll define the adjoint map directly, then use this to give $\mathfrak{g}$ the structure of a Lie algebra. For any $g \in G(A)$, we have an action $\mathrm{ad}(g) : G_A \to G_A$ given by $x \mapsto gxg^{-1}$ for any $B \in \mathsf{Alg}_A$. So we have a homomorphism of group functors $\mathrm{ad} : G \to \mathrm{Aut}(G)$. In particular, $G(k)$ acts on G by k-automorphisms.

⋆ The general philosophy, due to Grothendieck and worked out carefully in SGA, is that "everything is a functor." That is, we think of every object as living in the category of functors $\mathsf{Alg}_k \to \mathsf{Set}$. For example, if X and Y are schemes over k, then $\hom(X,Y)$ is the functor whose

$$\hom(X,Y)(A) = \hom_{\mathsf{Sch}_A}(X_A, Y_A).$$

We recover the usual hom-set as $\hom(X,Y)(k)$. Similarly, we define $\mathrm{Aut}(G)(A) = \mathrm{Aut}_{\mathsf{Grp}_A}(G_A)$. These functors are not usually representable, but they are sheaves for all the reasonable Grothendieck topologies on Sch_k. See [SGA 3_{I}, I §1–3, II §1] for a careful exposition along these lines. ⋆

By functoriality, there is a natural homomorphism $\mathrm{Aut}(G) \to \mathrm{Aut}(\mathfrak{g})$. Composing this with the map $\mathrm{ad} : G \to \mathrm{Aut}(G)$ gives a map $\mathrm{ad} : G \to \mathrm{Aut}(\mathfrak{g})$. Explicitly, the map $\mathrm{ad} : G(A) \to \mathrm{Aut}(\mathfrak{g})(A) = \mathrm{Aut}(\mathfrak{g}_A)$ sends g to the automorphism $x \mapsto gxg^{-1}$ for any $x \in G(B[\varepsilon])$, $B \in \mathsf{Alg}_A$. It is easy to see that this action respects $\mathscr{O}$-module structure on $\mathfrak{g}$, so we in fact have a representation $\mathrm{ad} : G \to \mathrm{GL}(\mathfrak{g})$. Since $\mathfrak{g}(A) = \mathfrak{g}(k) \otimes_k A$, we can think of $\mathfrak{g}$ as an honest k-vector space and define $\mathrm{GL}(\mathfrak{g})$ as the functor $A \mapsto \mathrm{Aut}_A(\mathfrak{g} \otimes_k A)$. In either case, we have a morphism $\mathrm{ad} : G \to \mathrm{GL}(\mathfrak{g})$ of linear algebraic groups.

Apply $\mathrm{Lie}(-)$ to the adjoint representation $\mathrm{ad} : G \to \mathrm{GL}(\mathfrak{g})$. We get a map $\mathrm{ad} : \mathfrak{g} \to \mathrm{Lie}(\mathrm{GL}(\mathfrak{g})) = \mathfrak{gl}(\mathfrak{g})$. We claim that $\mathfrak{g}$ together with $[x,y] = \mathrm{ad}(x)(y)$ is a Lie algebra.

Example 2.8.3. Let $G = \mathrm{GL}(n)$. We wish to verify that our functorial definition of $\mathrm{ad} : \mathfrak{gl}_n \to \mathfrak{gl}(\mathfrak{gl}_n)$ agrees with the elementary definition $\mathrm{ad}(x)(y) = [x,y]$. Start with the action of $\mathrm{GL}(n)$ on $\mathfrak{gl}_n$. For any k-algebra A, this is the action by conjugation of $\mathrm{GL}_n(A) \subset \mathrm{GL}_n(A[\varepsilon])$ on $\mathfrak{gl}_n(A) = \ker(\mathrm{GL}_n(A[\varepsilon]) \to \mathrm{GL}_n(A))$. This is because

$$g \cdot (1+\varepsilon x)(g^{-1}) = 1 + \varepsilon\, \mathrm{ad}(g)(x).$$

So the functorial and elementary definitions of $\mathrm{ad} : \mathrm{GL}(n) \to \mathrm{GL}(\mathfrak{gl}_n)$ agree.

Now let's differentiate $\mathrm{ad} : \mathrm{GL}(n) \to \mathrm{GL}(\mathfrak{gl}_n)$. For $A \in \mathsf{Alg}_k$, we have a commutative diagram:

$$\begin{tikzcd}
\mathfrak{gl}_n(A) \arrow[r, hook] \arrow[d, "\mathrm{ad}"] & \mathrm{GL}_n(A[\varepsilon]) \arrow[r, two heads] \arrow[d, "\mathrm{ad}"] & \mathrm{GL}_n(A) \arrow[d, "\mathrm{ad}"] \\
\mathfrak{gl}(\mathfrak{gl}_n)(A) \arrow[r, hook] & \mathrm{GL}(\mathfrak{gl}_n \otimes A[\varepsilon]) \arrow[r, two heads] & \mathrm{GL}(\mathfrak{gl}_n \otimes A)
\end{tikzcd}$$

All that remains is the simple computation

$$\begin{aligned} \mathrm{ad}(1+\varepsilon x)(y) &= (1+\varepsilon x) y (1 - \varepsilon x) \\ &= y + [x,y]\varepsilon \end{aligned}$$

So as an endomorphism of $\mathfrak{gl}_n \otimes A[\varepsilon]$, $\mathrm{ad}(1+\varepsilon x)$ is of the form $1 + \varepsilon[x,-]$. So when we identify $1+\varepsilon x$ with x, we get that $\mathrm{ad}(x) = [x,-]$ as desired. See [SGA 3_{I}, II 4.8] for a proof in much greater generality. ▷

This example yields the general fact that $\mathrm{Lie}(G)$ is a Lie algebra. Choose an embedding $G \hookrightarrow \mathrm{GL}(n)$. By construction, the Lie functor is limit-preserving, so $\mathfrak{g} \hookrightarrow \mathfrak{gl}_n$. The bracket on $\mathfrak{g}$ (as a subspace of $\mathfrak{gl}_n$ is induced by the bracket on $\mathfrak{gl}_n$. We have seen that the functorial definition of the bracket on $\mathfrak{gl}_n$ matches the elementary definition, so $\mathfrak{gl}_n$ is a Lie algebra and $\mathfrak{g}$ is a Lie subalgebras of $\mathfrak{gl}_n$.

Does $\mathrm{Lie}(G)$ determine G? The answer is an easy no! For example, $\mathrm{SO}(n)$ and $\mathrm{O}(n)$ both have Lie algebra $\mathfrak{so}_n$. Also $\mathrm{SL}(n)$ and $\mathrm{PSL}(n)$ both have Lie algebra $\mathfrak{sl}_n$. There is are the easy example $\mathrm{Lie}(\mathbf{G}_{\mathrm{a}}) = \mathrm{Lie}(\mathbf{G}_{\mathrm{m}}) = \mathfrak{gl}_1$. Finally, $\mathrm{Lie}(G) = \mathrm{Lie}(G^\circ)$, so $\mathrm{Lie}(G)$ does not depend on the group $\pi_0(G) = G/G^\circ$ of connected components of G. However, given a semisimple Lie algebra $\mathfrak{g}$, there is a unique split connected, simply-connected semisimple algebraic group G with $\mathrm{Lie}(G) = \mathfrak{g}$.

Example 2.8.4. Let's go over the Lie bracket on $\mathrm{GL}(n)$ in a more elementary manner. We have

$$\mathfrak{gl}_n = \ker\left(\mathrm{GL}_n(k[\varepsilon]) \to \mathrm{GL}_n(k)\right) = \{1 + \varepsilon x : x \in \mathrm{M}_n(k)\} \xrightarrow{\sim} \mathrm{M}_n(k).$$

We'll write elements of $\mathrm{M}_n(k[\varepsilon])$ as $x + y\varepsilon$; these should be thought of as a "point" x together with an "infinitesimal direction" y. The adjoint map is the homomorphism $\mathrm{ad} : \mathrm{GL}(n) \to \mathrm{GL}(\mathfrak{gl}_n)$, defined on A-points as the map $\mathrm{GL}_n(A) \to \mathrm{GL}(\mathfrak{gl}_n(A))$ given by $\mathrm{ad}(g)(x) = gxg^{-1}$. So for $A = k[\varepsilon]$, the group $\mathrm{GL}_n(k[\varepsilon])$ acts on $\mathrm{M}_n(k[\varepsilon])$ by conjugation. Take any $1 + \varepsilon b \in \mathrm{GL}_n(k[\varepsilon])$, and any $x + \varepsilon y \in \mathrm{M}_n(k[\varepsilon])$. We compute:

$$\begin{aligned}(1+\varepsilon b)(x+\varepsilon y)(1-\varepsilon b)^{-1} &= (x + \varepsilon y + \varepsilon bx)(1 - \varepsilon b) \\ &= x + \varepsilon y + \varepsilon(bx - xb) \\ &= x + \varepsilon y + \varepsilon[b, x] \\ &= (1 + \varepsilon[b, -])(x + \varepsilon y).\end{aligned}$$

Thus $\mathrm{ad}(1 + \varepsilon b) = 1 + \varepsilon[b, -]$ as an element of $\mathrm{End}_k(\mathfrak{gl}_n) = \mathfrak{gl}(\mathfrak{gl}_n)$. Summing it all up, we have a commutative diagram:

$$\begin{tikzcd} \mathfrak{gl}_n \arrow[r, "\mathrm{ad}"] \arrow[d, "\wr"] & \mathfrak{gl}(\mathfrak{gl}_n) \arrow[d, "\wr"] \\ \mathrm{M}_n \arrow[r, "\mathrm{ad}"] & \mathrm{End}(\mathrm{M}_n) \end{tikzcd}$$

so that $\mathrm{ad}(x)(y) = [x, y]$. ▷

As we have already seen, $\mathrm{Lie}(G)$ does not determine G. Even worse, the functor Lie is neither full nor faithful. It's not faithful because, for example, if Γ is a finite group and G a connected group, then $\mathrm{Aut}(\Gamma) \hookrightarrow \mathrm{Aut}(\Gamma \times G)$, but since $(G \times \Gamma)^\circ \subset G$, any automorphism of Γ acts trivially on $\mathrm{Lie}(\Gamma \times G)$. To see that Lie is not faithful, note that $\hom(\mathfrak{gl}_1, \mathfrak{gl}_1)$ is a one-dimensional vector space, while $\hom(\mathbf{G}_{\mathrm{m}}, \mathbf{G}_{\mathrm{m}}) = \mathbf{Z}$.

Theorem 2.8.5. *Let k be a field of characteristic zero, $G_{/k}$ a linear algebraic group. Let $\mathfrak{g} = \mathrm{Lie}(G)$. The map $H \mapsto \mathrm{Lie}(H)$ from connected closed subgroups of G to Lie subalgebras of $\mathfrak{g}$ is injective and preserves inclusions.*

Proof. If $H_1 \subset H_2$, use the functoriality of forming Lie algebras to see that $\mathrm{Lie}(H_1) \subset \mathrm{Lie}(H_2)$ as subalgebras of $\mathfrak{g}$. The nontrivial part is to show that $\mathrm{Lie}(H)$, as a subalgebra of $\mathfrak{g}$, determines H. Let H_1, H_2 be be two closed connected subgroups of G such that $\mathfrak{h} = \mathrm{Lie}(H_1) = \mathrm{Lie}(H_2)$. Then $H_3 = (H_1 \cap H_2)^\circ$ is a closed connected subgroup of G. Since fiber products are computed pointwise and the Lie functor is exact, we have $\mathrm{Lie}(H_3) = \mathfrak{h}$. By Theorem 2.8.7, the H_i are all smooth, so $\dim(H_i) = \dim \mathfrak{h}$. But the only way $H_3 \subset H_1$ can both be smooth and irreducible with the same dimension is for $H_1 = H_3$. Similarly $H_2 = H_3$, so $H_1 = H_2$. □

Example 2.8.6. The subgroup $\mathbf{G}_{\mathrm{m}} \simeq \left\{\begin{pmatrix} a & \\ & a^{-1}\end{pmatrix}\right\}$ and $\mathbf{G}_{\mathrm{a}} \simeq \begin{pmatrix} 1 & * \\ & 1\end{pmatrix}$ of $\mathrm{GL}(2)$ have Lie algebras that are abstractly isomorphic, but distinct as subalgebras of $\mathfrak{gl}_2$. Thus $\mathrm{Lie}(H)$, seen as an abstract Lie algebra, does not determine H as a subgroup of G. ▷

Theorem 2.8.5 fails in positive characteristic. Also, surjectivity need not hold, see e.g. $\mathrm{GL}(5)$. If we instead work in the category of smooth manifolds and Lie groups, then *every* Lie subalgebra comes from a subgroup.

Theorem 2.8.7 (Cartier)**.** *Let k be a field of characteristic zero, $G_{/k}$ a linear algebraic group. Then G is smooth.*

Proof. The idea is that for $k = \mathbf{C}$, $G(\mathbf{C})$ must be smooth at "most" points g. But any two points in $G(\mathbf{C})$ have diffeomorphic neighborhoods, so $G(\mathbf{C})$ itself is smooth. For a careful proof in much greater generality, see [SGA 3_{I}, VI_{B} 1.6]. Even SGA assumes that G is locally of finite type, but this is not necessary. See `http://mathoverflow.net/questions/22553` for some discussion and references. □

Example 2.8.8. Consider $\boldsymbol{\mu}_p = \ker(\mathbf{G}_{\mathrm{m}} \xrightarrow{p} \mathbf{G}_{\mathrm{m}})$ over $k = \mathbf{F}_p$. That is, $\boldsymbol{\mu}_p(A) = \{a \in A : a^p = 1\}$. The coordinate ring of $\boldsymbol{\mu}_p$ is $k[x]/(x^p - 1)$. Note that

$$\begin{aligned} \mathrm{Lie}(\boldsymbol{\mu}_p)(A) &= \{1 + \varepsilon x : x \in A \text{ and } (1+\varepsilon x)^p = 1\} \\ &= \{1 + \varepsilon x : 1 + (\varepsilon x)^p = 1\} \\ &= A. \end{aligned}$$

In other words, $\boldsymbol{\mu}_p \subset \mathrm{GL}(1)$ has Lie algebra $\mathfrak{gl}_1$. Since $\boldsymbol{\mu}_p$ is connected over $\mathbf{F}_p$, this provides a counterexample to Theorem 2.8.5 in characteristic p. Moreover, $\boldsymbol{\mu}_p(\overline{\mathbf{F}_p}) = 1$, so "$\boldsymbol{\mu}_p$ has no points." ▷

If, on the other hand, the base field has characteristic not p, then $(1+\varepsilon x)^p = 1 + p\varepsilon x$, which is 1 exactly when $x = 0$. So $\mathrm{Lie}(\boldsymbol{\mu}_p) = 0$ as expected.

3 Solvable groups, unipotent groups, and tori

Recall that if $G_{/k}$ is an algebraic group, there is a canonical filtration

$$1 \supset \mathcal{R}_{\mathrm{u}} G \subset \mathcal{R} G \subset G^\circ \subset G.$$

Each subgroup in the filtration is normal in G. The *neutral component* G° of G, is defined as a functor on k-schemes by

$$G^\circ(S) = \{g : S \to G : g(|S|) \subset |G|^\circ\},$$

where $|G|^\circ$ is the connected component of 1 in the topological space underlying G. By [SGA 3_{I}, VI_{A} 2.3.1, 2.4], the functor G° represents an open, geometrically irreducible, subgroup scheme of G.By [SGA 3_{I}, VI_{A} 5.5.1], the quotient $\pi_0(G) = G/G^\circ$ is étale over k.

One calls $\mathcal{R}G$ the *radical* of G, an $\mathcal{R}_{\mathrm{u}}G$ the *unipotent radical.* All possible quotients in the filtration have names:

- G°/G is *finite*
- $G^\circ/\mathcal{R}G$ is *semisimple*
- $G^\circ/\mathcal{R}_{\mathrm{u}}G$ is *reductive*
- $\mathcal{R}G/\mathcal{R}_{\mathrm{u}}G$ is a *torus*
- $\mathcal{R}_{\mathrm{u}}G$ is *unipotent* .

3.1 One-dimensional groups

For simplicity, assume k is algebraically closed. Let $G_{/k}$ be a one-dimensional smooth connected linear algebraic group. Currently, we have two candidates for G, the additive group $\mathbf{G}_{\mathrm{a}}$ and the multiplicative group $\mathbf{G}_{\mathrm{m}}$, given by

$$\mathbf{G}_{\mathrm{a}}(A) = (A, +)$$
$$\mathbf{G}_{\mathrm{m}}(A) = A^\times$$

for all k-algebras A.

Theorem 3.1.1. *Any one-dimensional connected smooth linear algebraic group over an algebraically closed field is isomorphic to a unique member of* $\{\mathbf{G}_{\mathrm{a}}, \mathbf{G}_{\mathrm{m}}\}$.

Proof. As a variety over k, G is smooth and one-dimensional. Thus there is a unique smooth proper curve $C_{/k}$ with an open embedding $G \hookrightarrow C$. The set $S = C(k) \smallsetminus G(k)$ is finite. Take $g \in G(k)$. Then $\phi_g : G \xrightarrow{\sim} G$ given by $x \mapsto g \cdot x$ is an automorphism of curves. We can think of ϕ_g as a rational map $C \to C$; by Zariski's main theorem, this extends uniquely to an automorphism $\phi_g : C \xrightarrow{\sim} C$. We obtain a group homomorphism $\phi : G(k) \hookrightarrow \mathrm{Aut}(C)$.

Let g be the genus of C (if $k = \mathbf{C}$, this is just the number of "holes" in the closed surface $C(\mathbf{C})$). By [Har77, IV ex 5.2], if $g \geqslant 2$, then $\mathrm{Aut}(C)$ is finite. It follows that $g \leqslant 1$. Since S is finite, there is an infinite subgroup $H \subset G(k)$ that acts trivially on S. Write $\mathrm{Aut}(C, S)$ for the group of automorphisms of C that are trivial on S; there is an injection $H \hookrightarrow \mathrm{Aut}(C, S)$. If $g = 1$, then $\mathrm{Aut}(C, S)$ is finite [Har77, IV cor 4.7].

We've reduced to the case $g = 0$. We can assume $G \subset C = \mathbf{P}^1_{/k} = \mathbf{A}^1_{/k} \cup \{\infty\}$. It is known that $\mathrm{Aut}(\mathbf{P}^1) = \mathrm{PGL}(2)$ as schemes, so in particular $\mathrm{Aut}(\mathbf{P}^1_{/k}) = \mathrm{PGL}_2(k)$ [Har77, p. IV 7.1.1]. The action of $\mathrm{PGL}_2(k)$ is via fractional linear transformations:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} x = \frac{ax+b}{cx+d}.$$

For any distinct $\alpha, \beta, \gamma \in \mathbf{P}^1(k)$, there is a unique $g \in \mathrm{PGL}_2(k)$ such that $g(\alpha) = 0$, $g(\beta) = 1$, and $g(\gamma) = \infty$ [this is equivalent to $M_{0,3} = *$, it can be verified by a direct computation]. If $\# S \geqslant 3$, then this shows that $\mathrm{Aut}(\mathbf{P}^1_{/k}, S) = 1$, which doesn't work. We now get two cases, $\# S \in \{1, 2\}$. So without loss of generality, $G = \mathbf{P}^1_{/k} \smallsetminus \{\infty\}$ or $G = \mathbf{P}^1_{/k} \smallsetminus \{0, \infty\}$. So as a variety, $G = \mathbf{G}_\mathrm{a}$ or $\mathbf{G}_\mathrm{m}$.

We'll treat the case $G = \mathbf{P}^1_{/k} \smallsetminus \{0, \infty\}$. We can assume $1 \in \mathbf{P}^1$ is the identity of G. Pick $g \in G(k) \subset k^\times$; then $\phi_g : x \mapsto gx$ must be of the form $x \mapsto \frac{ax+b}{cx+d}$. Moreover, $\phi_g\{0, \infty\} = \{0, \infty\}$. Either $\phi_g(x) = ax$ for $a \in k^\times$, or $\phi_g(x) = a/x$. In the latter case, ϕ_g has a fixed point, namely $\sqrt{a}$. But translation has no fixed points, so $\phi_g(x) = ax$. Since $g = \phi_g(1) = a$, it follows that $G = \mathbf{G}_\mathrm{m}$. $\square$

The group $\mathbf{G}_\mathrm{m}$ is reductive (better, a torus), and $\mathbf{G}_\mathrm{a}$ is unipotent. For a general (i.e., not necessarily linnear) connected one-dimensional algebraic group, there are many possibilities, namely elliptic curves. Even over $\mathbf{C}$, the collection of elliptic curves is one-dimensional when interpreted as a variety in the appropriate sense.

3.2 Solvable groups

Let $G_{/k}$ be an algebraic group, and let $\mathfrak{g} = \mathrm{Lie}(G)$. It turns out that $\mathrm{Lie}(G^\circ) = \mathfrak{g}$. There is a canonical sub-Lie algebra $\mathrm{rad}(\mathfrak{g}) \subset \mathfrak{g}$; in characteristic zero, this will determine a connected linear algebraic subgroup $\mathcal{R}G \subset G$.

For the moment, let $\mathfrak{g}$ be an arbitrary k-Lie algebra. Let $\mathcal{D}\mathfrak{g} = [\mathfrak{g}, \mathfrak{g}]$ be the subspace of $\mathfrak{g}$ generated by $\{[x, y] : x, y \in \mathfrak{g}\}$. The subspace $\mathcal{D}\mathfrak{g}$ is actually an ideal, and the quotient $\mathfrak{g}/\mathcal{D}\mathfrak{g}$ is commutative. Moreover, $\mathcal{D}\mathfrak{g}$ is the smallest ideal in $\mathfrak{g}$ with this property.

Every Lie algebra comes with a canonical descending filtration $\mathcal{D}^\bullet\mathfrak{g}$, called the *derived series*. It is defined by

$$\begin{aligned} \mathcal{D}^1\mathfrak{g} &= \mathcal{D}\mathfrak{g} \\ \mathcal{D}^{n+1}\mathfrak{g} &= \mathcal{D}(\mathcal{D}^n\mathfrak{g}). \end{aligned}$$

Definition 3.2.1. *A Lie algebra $\mathfrak{g}$ is* solvable *if the filtration $\mathcal{D}^\bullet\mathfrak{g}$ is separated, that is if $\mathcal{D}^n\mathfrak{g} = 0$ for some n.*

Lemma 3.2.2. *A Lie algebra $\mathfrak{g}$ is solvable if and only if there exists a decreasing filtration $\mathfrak{g} = \mathfrak{g}_0 \supset \cdots \supset \mathfrak{g}_n = 0$ with each $\mathfrak{g}_{i+1}$ an ideal in $\mathfrak{g}_i$, and with $\mathfrak{g}_i/\mathfrak{g}_{i+1}$ commutative.*

Proof. $\Rightarrow$. This follows from the fact that $\mathcal{D}^i\mathfrak{g}/\mathcal{D}^{i+1}\mathfrak{g}$ is abelian for each i.

$\Leftarrow$. Since $\mathfrak{g}_0/\mathfrak{g}_1$ is commutative, we get $\mathcal{D}\mathfrak{g} \supset \mathfrak{g}_1$. More generally, we get $\mathcal{D}^i\mathfrak{g} \supset \mathfrak{g}_i$ by induction, so $\mathfrak{g}_i = 0$ for $i \gg 0$ implies $\mathcal{D}^i\mathfrak{g} = 0$ for $i \gg 0$. □

Lemma 3.2.3. *Let $\mathfrak{g}$ be a finite-dimensional Lie algebra. Then $\mathfrak{g}$ has a unique maximal solvable ideal; it is called the* radical *of $\mathfrak{g}$, and denoted* $\operatorname{rad}(\mathfrak{g})$.

Proof. Let $\mathfrak{a}$ be an ideal of $\mathfrak{g}$ that is solvable, and has $\dim(\mathfrak{a})$ maximal. Let $\mathfrak{b}$ be any solvable ideal. Then $\mathfrak{a}+\mathfrak{b}$ is an ideal and $(\mathfrak{a}+\mathfrak{b})/\mathfrak{a}$ is solvable. From the general fact that solvable Lie algebras are closed under extensions, we get that $\mathfrak{a}+\mathfrak{b}$ is solvable, so $\mathfrak{a}+\mathfrak{b} = \mathfrak{a}$, whence $\mathfrak{b} \subset \mathfrak{a}$. □

Definition 3.2.4. *A Lie algebra k is* semisimple *if* $\operatorname{rad}(\mathfrak{g}) = 0$.

Example 3.2.5. Consider the Lie algebra

$$\mathfrak{b}_n = \{x \in \mathfrak{gl}_n : x_{i,j} = 0 \text{ for all } i > j\}.$$

We claim that $\mathfrak{b}_n$ is solvable. This follows from the fact that

$$\mathcal{D}^r\mathfrak{b}_n = \{x \in \mathfrak{gl}_n : x_{i,j=0} \text{ for all } i > j - r\}.$$

To see that this is true, note that it is trivially true for $r = 0$, so assume it is true for some r, and let $x, y \in \mathcal{D}^r\mathfrak{b}_n$. Note that

$$\begin{aligned} [x,y]_{i,j} &= \sum_k (x_{i,k}y_{k,j} - y_{i,k}x_{k,j}) \\ &= \sum_{i-r\leqslant k\leqslant j+r} (x_{i,k}y_{k,j} - y_{i,k}x_{k,j}) \end{aligned} \tag{$*$}$$

Moreover, when $i > j+r+1$, then all of the terms in ($*$) are zero, whence the result. In some sense, $\mathfrak{b}_n$ is the "only" example of a solvable Lie algebra over an algebraically closed field. ▷

Theorem 3.2.6 (Lie-Kolchin)**.** *Let k be an algebraically closed field, $\mathfrak{g}$ a finite-dimensional solvable k-Lie algebra. Then there is an injective Lie homomorphism $\mathfrak{g} \hookrightarrow \mathfrak{b}_n$ for some n.*

Proof. In characteristic zero, this follows directly from Corollary 2 of [$\text{Lie}_{1\text{–}3}$, I §5.3] applied to the adjoint representation. □

Example 3.2.7. One can check that:

$$\begin{aligned} \operatorname{rad}(\mathfrak{gl}_2) &= \left\langle \begin{pmatrix} 1 & \\ & 1 \end{pmatrix} \right\rangle \\ \mathcal{D}^n(\mathfrak{gl}_2) &= \mathfrak{sl}_2 && \text{for all } n \geqslant 1 \end{aligned}$$

This is because $\mathfrak{sl}_2$ is simple (has no non-trivial ideals). ▷

Definition 3.2.8. *Let $G_{/k}$ be a linear algebraic group. We say G is* solvable *if there is a sequence of algebraic subgroups $G = G_0 \supset G_1 \supset \cdots \supset G_n = 1$ such that*

1. *each G_{i+1} is normal in G_i,*
2. *each G_i/G_{i+1} is commutative.*

Example 3.2.9. Let $G = B(n) \subset \mathrm{GL}(n)$ be the subgroup of upper-triangular matrices (the letter B represents "Borel"). This is solvable, as is witnessed by the filtration

$$\begin{aligned} G_1 &= \{g \in \mathrm{GL}(n) : g_{ii} = 1 \text{ for all } i\} \\ G_r &= \{g \in B(n)_2 : g_{ij} = 0 \text{ for all } i < j + r\} && r \geqslant 1. \end{aligned}$$

The map $G_0 \to \mathbf{G}_\mathrm{m}^n$ defined by $(a_{ij}) \mapsto (a_{11}, \dots, a_{nn})$ induces an isomorphism $G_0/G_1 \xrightarrow{\sim} \mathbf{G}_\mathrm{m}^n$. Similarly $G_1 \to \mathbf{G}_\mathrm{a}^{n-1}$ defined by $(a_{ij}) \mapsto (a_{1,2}, \dots, a_{n-1,n})$ induces an isomorphism $G_1/G_2 \xrightarrow{\sim} \mathbf{G}_\mathrm{a}^{n-1}$. In general, for $i \geqslant 0$, we have $G_i/G_{i+1} \xrightarrow{\sim} \mathbf{G}_\mathrm{a}^{n-i}$.

We could have chosen our filtration in such a way that $G_i/G_{i+1} \in \{\mathbf{G}_\mathrm{a}, \mathbf{G}_\mathrm{m}\}$. ▷

Definition 3.2.10. *Let $G_{/k}$ be a linear algebraic group. The* derived *group $\mathcal{D}G$ (or G', or G^{der}) is the smallest normal subgroup $\mathcal{D}G$ of G such that $G/\mathcal{D}G$ is commutative.*

The basic idea is that $\mathcal{D}G$ is the algebraic group generated by $\{xyx^{-1}y^{-1} : x, y \in G\}$.

Theorem 3.2.11. *Let $G_{/k}$ be a smooth linear algebraic group. Then $\mathcal{D}G$ exists and is smooth, and if G is connected then so is $\mathcal{D}G$.*

Proof. This essentially follows from [SGA 3_I, $\mathrm{VI_B}$ 7.1]. □

Just as for Lie algebras, we can define a filtration

$$\begin{aligned} \mathcal{D}^1 G &= \mathcal{D}G \\ \mathcal{D}^{n+1} G &= \mathcal{D}(\mathcal{D}^n G). \end{aligned}$$

Theorem 3.2.12. *A linear algebraic group G is solvable if and only if $\mathcal{D}^n G = 1$ for some n.*

Example 3.2.13. If $G \subset B(n) \subset \mathrm{GL}(n)$, then G is solvable. Indeed, this follows from $\mathcal{D}^\bullet G \subset \mathcal{D}^\bullet B(n)$. ▷

Theorem 3.2.14 (Lie-Kolchin)**.** *Suppose k is algebraically closed. Let $G \subset \mathrm{GL}(n)_{/k}$ be a connected solvable algebraic group. Then there exists $x \in \mathrm{GL}_n(k)$ such that $xGx^{-1} \subset B(n)$.*

Proof. Let $V = k^{\oplus n}$, and consider V as a representation of G via the inclusion $G \hookrightarrow \mathrm{GL}(V)$. It is sufficient to prove that V contains a one-dimensional subrepresentation, for then we could induct on $\dim(V)$. For simplicity, we assume G is smooth. If G is commutative, then the set $G(k)$ is a family of mutually commuting endomorphisms of V. It is known that such sets are mutually triangularisable, i.e. can be conjugated to lie within $B(n)$. (This follows from the Jordan decomposition.)

In the general case, we may assume the claim is true for $\mathcal{D}G$. Recall that $\mathrm{X}^*(\mathcal{D}G) = \hom(\mathcal{D}G, \mathbf{G}_\mathrm{m})$ is the group of *characters* of $\mathcal{D}G$. The group G acts on $\mathrm{X}^*(\mathcal{D}G)$ by conjugation:

$$(g \cdot \chi)(h) = \chi(ghg^{-1}).$$

Even better, we can define $\mathrm{X}^*(\mathcal{D}G)$ as a group functor:

$$\mathrm{X}^*(\mathcal{D}G)(A) = \hom_{\mathsf{Grp}_{/A}}((\mathcal{D}G)_{/A}, (\mathbf{G}_\mathrm{m})_{/A}).$$

By [SGA 3_{II}, 11.4.2], this is represented by a smooth separated scheme over k. We define a subscheme

$$\Delta(A) = \{\chi \in \mathrm{X}^*(\mathcal{D}G)(A) : \chi \text{ factors through } G_{/A} \hookrightarrow \mathrm{GL}(V)_{/A}\}.$$

Note that Δ is finite and nonempty, and G is connected. Thus the induced action of G on Δ is trivial, so G fixes some $\chi \in \Delta(k)$. Let V_χ be the suprepresentation of V generated by all χ-typical vectors, i.e.

$$V_\chi(A) = \langle v \in V_{/A} : g \cdot v = \chi(g)v \text{ for all } g \in G(A)\}.$$

After replacing V by V_χ, we may assume $\mathcal{D}G$ acts on V by a character χ. That is, as a subgroup of $\mathrm{GL}(n)$, $\mathcal{D}G \subset \mathbf{G}_\mathrm{m}$. Since the determinant map kills commutators, $\mathcal{D}G \subset \mathbf{G}_\mathrm{m} \cap \mathrm{SL}(n) = \boldsymbol{\mu}_n$, so $\mathcal{D}G$ is finite. Since G connected, Theorem 3.2.11 tells us that $\mathcal{D}G = 1$, so G is abelian, and we're done. $\square$

Example 3.2.15. If k is algebraically closed and $G_{/k} \subset \mathrm{GL}(n)_{/k}$ is solvable, then there exists a filtration $G = G_0 \supset \cdots \supset G_n = 1$ such that $G_0/G_1 \simeq \mathbf{G}_\mathrm{m}^r$, and all higher $G_i/G_{i+1} \simeq \mathbf{G}_\mathrm{a}$. We will see that this property determines G_1. We know there is $v \in k^{\oplus n}$ which is a common eigenvector of all $g \in \mathcal{D}G(k)$. This gives us a character $\chi : \mathcal{D}G \to \mathbf{G}_\mathrm{m}$. $\triangleright$

Example 3.2.16. This shows that Theorem 3.2.14 does not hold over non-algebraically closed fields. Let

$$G_{/\mathbf{R}} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \right\} \subset \mathrm{GL}(2)_{/\mathbf{R}}.$$

Note that $G(\mathbf{R}) \simeq \mathbf{C}^\times$ (in fact, $G = \mathrm{R}_{\mathbf{C}/\mathbf{R}}\, \mathbf{G}_\mathrm{m}$) via

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \leftrightarrow a + bi.$$

The group G is commutative (hence solvable), but it is not conjugate to $B(2)$ by an element of $\mathrm{GL}_2(\mathbf{R})$. Indeed, note that $\begin{pmatrix} & -1 \\ 1 & \end{pmatrix}$ is not diagonalizable in $\mathrm{GL}_2(\mathbf{R})$ because it has eigenvalues $\pm i$. $\triangleright$

For a general group, we'll have a subgroup $\mathcal{R}G$, the *radical* of G. It will be the largest connected normal solvable subgroup of G. It will turn out that $\mathrm{rad}(\mathfrak{g}) = \mathrm{Lie}(\mathcal{R}G)$.

3.3 Quotients

Let $G_{/k}$ be an algebraic group, $N \subset G$ a sub-algebraic group. As functors of points, $N(A)$ is a normal subgroup of $G(A)$ for all k-algebras A.

Example 3.3.1. Let $k = \mathbf{R}$, and consider $\boldsymbol{\mu}_2 = \ker(\mathbf{G}_\mathrm{m} \xrightarrow{(-)^2} \mathbf{G}_\mathrm{m})$ over k. Should we consider the sequence

$$1 \to \boldsymbol{\mu}_2 \to \mathbf{G}_\mathrm{m} \xrightarrow{2} \mathbf{G}_\mathrm{m} \to 1$$

to be exact? On $\mathbf{C}$-points, this is the sequence

$$1 \to \{\pm 1\} \to \mathbf{C}^\times \xrightarrow{2} \mathbf{C}^\times \to 1$$

which is certainly exact. So we will write $\mathbf{G}_\mathrm{m} = \mathbf{G}_\mathrm{m}/\boldsymbol{\mu}_2$. Note however that the sequence for $\mathbf{R}$-points is $1 \to \{\pm 1\} \to \mathbf{R}^\times \xrightarrow{2} \mathbf{R}^\times$, which is *not* exact on the right. ▹

In general, if $1 \to N \to G \to H \to 1$ is an "exact sequence" of algebraic groups, we will not necessarily have surjections from the A-points of G to the A-points of H.

Definition 3.3.2. *Let $N_{/k} \subset G_{/k}$ be a sub-algebraic group. A* quotient *of G by N is a homomorphism $G \xrightarrow{q} Q$ of algebraic groups over k with kernel N, such that if $G \xrightarrow{\phi} G'$ vanishes on N, then there is a unique $\psi : Q \to G'$ such that the following diagram commutes:*

$$\begin{tikzcd} 1 \arrow[r] & N \arrow[r] & G \arrow[r, "q"] \arrow[dr, "\phi"] & Q \arrow[d, dashed, "\psi"] \\ & & & G' \end{tikzcd}$$

Theorem 3.3.3. *Quotients exist in the category of (possibly non-smooth) affine group schemes of finite type over k.*

Proof. This is [Mil14, 10.16]. □

If G/H is the quotient of G by a subgroup H, it is generally true that $(G/H)(\bar{k}) = G(\bar{k})/H(\bar{k})$.

⋆ There is a more abstract, but powerful approach to defining quotients. Let Sch_k be the category of schemes over $\operatorname{Spec}(k)$. We can regard any scheme over k as an fppf sheaf on Sch_k via the Yoneda embedding. If $H \subset G$ is a closed subgroup-scheme, we write G/H for the quotient sheaf of $S \mapsto G(S)/H(S)$ in the fppf topology. By [SGA 3_I, VI_A 3.2], this quotient sheaf is representable. By general nonsense, it will satisfy more elementary definition of quotient. ⋆

3.4 Unipotent groups

Recall that for the moment, $B(n) \subset \mathrm{GL}(n)$ is the subgroup of upper triangular matrices and $U(n) \subset B(n)$ is the subgroup of *strictly* upper-triangular matrices.

Recall that in our filtration of $B(n) \subset \mathrm{GL}(n)$, we had $B(n)/U(n) \simeq \mathbf{G}_{\mathrm{m}}^n$, and all further quotients were $\mathbf{G}_{\mathrm{a}}^r$ for varying r. We'd like to generalize this to an arbitrary connected solvable groups over algebraically closed fields. For the moment though, k need not be algebraically closed.

Definition 3.4.1. *Let $G_{/k}$ be an algebraic group. We say G is* unipotent *if it admits a filtration $G = G_0 \supset \cdots \supset G_n = 1$ of closed subgroups defined over k such that*

1. *each G_{i+1} is normal in G_i,*
2. *each G_i/G_{i+1} is isomorphic to a closed subgroup of $\mathbf{G}_{\mathrm{a}}$.*

Clearly, unipotent groups are solvable. If k has characteristic zero, we can assume $G_i/G_{i+1} \simeq \mathbf{G}_{\mathrm{a}}$. If k has characteristic $p > 0$, then we have to worry about things like $\boldsymbol{\alpha}_p = \ker(\mathbf{G}_{\mathrm{a}} \xrightarrow{p} \mathbf{G}_{\mathrm{a}})$. Fortunately, by [SGA 3_{II}, XVII 1.5], the only possible closed subgroups of $\mathbf{G}_{\mathrm{a}}$ over a field of characteristic p are 0, $\mathbf{G}_{\mathrm{a}}$ and extensions of $(\mathbf{Z}/p)^r$ by $\boldsymbol{\alpha}_{p^e}$.

Theorem 3.4.2. *Let $G_{/k}$ be a connected linear algebraic group. Then G is unipotent if and only if it is isomorphic to a closed subgroup of some $U(n)_{/k}$.*

Proof. This follows directly from [SGA 3_{II}, XVII 3.5]. □

If $G_{/k}$ is unipotent and $\rho : G \to \mathrm{GL}(V)$ is a representation, then for all $g \in G(\bar{k})$, the matrix $\rho(g)$ is unipotent, i.e. $(\rho(g) - 1)^n = 0$ for some $n \geqslant 1$. Indeed, by [SGA 3_{II}, XVII 3.4], for any such representation, there is a G-stable filtration $\mathrm{fil}^\bullet V$ for which the action of G on $\mathrm{gr}^\bullet(V)$ is trivial. In other words, ρ is conjugate to a representation which factors through some $U(n)$, and elements of $U(n)(k)$ are all unipotent. Conversely, by [SGA 3_{II}, XVII 3.8], if k is algebraically closed and every element of $G(k) \subset \mathrm{GL}_n(k)$ is unipotent, then G is unipotent when considered as an algebraic group.

Theorem 3.4.3. *Let $G_{/k}$ be a connected solvable smooth group over a perfect field k. Then there exists a unique connected normal $G_{\mathrm{u}} \subset G$ such that*

1. *G_{u} is unipotent,*
2. *G/G_{u} is of multiplicative type .*

Proof. This is [Mil14, XVII 17.23]. □

Recall that an algebraic group $G_{/k}$ is *of multiplicative type* if it is locally (in the fpqc topology) the form $A \mapsto \hom(M, A^\times)$, for M an (abstract) abelian group [SGA 3_{II}, IX 1.1]. Over a perfect field, any group of multiplicative type is locally of this form after an étale base change. In particular, if k has characteristic zero, G/G_{u} will be a torus. If moreover $k = \bar{k}$, then $G/G_{\mathrm{u}} \simeq \mathbf{G}_{\mathrm{m}}^r$. In general, G/G_{u} will be a closed subgroup of a torus.

Example 3.4.4. If $G = B(n) \subset \mathrm{GL}(n)$, then $G_{\mathrm{u}} = U(n)$, the subgroup of strictly upper-triangular matrices. ▷

3.5 Review of canonical filtration

For this section, assume k is a perfect field.

Let $G_{/k}$ be a smooth connected linear algebraic group. In [cite], we defined $\mathcal{R}G$, the radical of G, to be the largest normal subgroup of G that is connected and solvable.

The *unipotent radical* $\mathcal{R}_{\mathrm{u}}G$ of G, is by definition $(\mathcal{R}G)_{\mathrm{u}}$. As in subsection 1.6, we have a diagram

$$\begin{array}{l}
\begin{array}{lll} \phantom{\text{connected}} & G & \\ & \cup & \text{finite} \end{array}\\
\left.\begin{array}{lll} \text{connected} & G^\circ & \\ & \cup & \text{semisimple} \\ \text{solvable} & \mathcal{R}G & \\ & \cup & \text{torus} \\ \text{unipotent} & \mathcal{R}_{\mathrm{u}}G & \end{array}\right\}\text{reductive}\\
\begin{array}{lll} \phantom{\text{connected}} & \cup & \\ & 1 & \end{array}
\end{array}$$

So the group $\mathcal{R}_{\mathrm{u}}G$ is unipotent, $\mathcal{R}G$ is solvable. The quotient $\mathcal{R}G/\mathcal{R}_{\mathrm{u}}G$ is a torus (we could define a torus to be a solvable group with trivial unipotent radical.)

The quotient $G/\mathcal{R}G$ is *semisimple*, and $G/\mathcal{R}_{\mathrm{u}}G$ is *reductive*. There is a good structure theory for semisimple groups.

Definition 3.5.1. *Let k be a perfect field. A connected linear algebraic group $G_{/k}$ is* reductive *if $\mathcal{R}_{\mathrm{u}}G = 1$.*

Over a non-perfect field k, we say $G_{/k}$ is reductive if $\mathcal{R}_{\mathrm{u}}(G_{\bar{k}}) = 1$. If k is perfect, then $\mathcal{R}_{\mathrm{u}}(G_{\bar{k}})$ descends uniquely to a group $\mathcal{R}_{\mathrm{u}}G$ defined over k, but this is not true in general. Over a non-perfect field, one calls G *pseudo-reductive* if we only have $\mathcal{R}_{\mathrm{u}}G = 1$. The main example of a pseudo-reductive group which is not reductive is any group of the form $\mathrm{R}_{K/k}\,G$, where K/k is purely inseparable and $G_{/K}$ is reductive. There is a reasonably satisfying structure theory for pseudo-reductive groups, worked out in [CGP10].

Example 3.5.2. The group $\mathrm{GL}(n)$ is reductive, even though $\mathcal{R}\,\mathrm{GL}(n) = \mathbf{G}_{\mathrm{m}}$ is nontrivial. ▷

Definition 3.5.3. *A connected linear algebraic group G is* semisimple *if $\mathcal{R}G = 1$.*

Example 3.5.4. The group $\mathrm{SL}(n)$ is semisimple. The subgroup $\boldsymbol{\mu}_n = \mathrm{Z}(\mathrm{SL}_n)$ is a solvable normal subgroup, but it's not connected (or not smooth, if the base characteristic divides n). ▷

3.6 Jordan decomposition

To begin with, let k be an algebraically closed field, V a finite-dimensional k-vector space. Let $x \in \mathfrak{gl}(V)$. Then we can consider the action of a polynomial ring $k[x]$ on V via x. By the fundamental theorem of finitely generated modules over a principal ideal domain [$\text{Alg}_{4\text{–}7}$, VII §2.2 thm.1], we have $V = \bigoplus_\lambda V_\lambda$, where for $\lambda \in k$, we define

$$V_\lambda = \{v \in V : (x-\lambda)^n v = 0 \text{ for some } n \geqslant 1\}.$$

The λ for which $V_\lambda \neq 0$ are called *eigenvalues* of x, and $\dim(V_\lambda)$ is the *multiplicity* of λ. By a further application of the fundamental theorem for modules over a PID, we get that each $V_\lambda \simeq \bigoplus_i k[x]/(x-\lambda)^{n_i}$.

The k-vector space $k[x]/(t-\lambda)^n$ has basis $\{v_i = (t-\lambda)^{n-i}\}_{i=1}^n$. Moreover,

$$\begin{aligned} tv_1 &= \lambda v_1 \\ tv_2 &= \lambda v_2 + v_2 \ \cdots \end{aligned}$$

When we write x with respect to this basis, we get the $n \times n$ matrix $J_n(\lambda)$ which is λ along the diagonal, 1 just above the diagonal, and zeros everywhere else.

For a general endomorphism $x \in \mathfrak{gl}(V)$, we end up with a direct sum decomposition (with respect to some basis) $g = \bigoplus J_{n_i}(\lambda_i)$.

In all of this, we used $k = \bar{k}$. Over a general field k, we'll be able to write a matrix x as the sum of a diagonal matrix and a strictly upper triangular (hence nilpotent) matrix. Suppose we have written $x = x_{\mathrm{ss}} + x_{\mathrm{n}}$, where x_{ss} is diagonal and x_{n} is nilpotent. It turns out that x_{ss} is uniquely determined, and is a polynomial in x. That is, there exists a polynomial $f \in k[x]$, possibly depending on x, such that $x_{\mathrm{ss}} = f(x)$, and similarly for x_{n}.

For the remainder of this section, let k be an arbitrary perfect field, V a finite-dimensional k-vector space.

Definition 3.6.1. *An element $x \in \mathfrak{gl}(V)$ is* semisimple *if it is diagonalizable after base-change to an extension of k.*

Definition 3.6.2. *An element $x \in \mathfrak{gl}(V)$ is* nilpotent *if $x^n = 0$ for some $n \geqslant 1$.*

Definition 3.6.3. *An element $x \in \mathrm{GL}(V)$ is* unipotent *if $x - 1$ is nilpotent.*

Theorem 3.6.4 (Additive Jordan decomposition)**.** *For any $x \in \mathfrak{gl}(V)$, there exists unique elements $x_{\mathrm{ss}} \in \mathrm{GL}(V)$, $x_{\mathrm{n}} \in \mathfrak{gl}(V)$, such that*

1. $x = x_{\mathrm{ss}} + g_{\mathrm{n}}$,
2. x_{ss} *is semisimple,*
3. x_{n} *is nilpotent, and*
4. $[x_{\mathrm{ss}}, x_{\mathrm{n}}] = 0$.

Moreover, there exist polynomials $f, g \in k[x]$ such that $x_{\mathrm{ss}} = f(x)$ and $x_{\mathrm{n}} = g(x)$.

Proof. Case 1: the eigenvalues of x lie in k. Then by the theory of Jordan normal form, we get existence of a decomposition. Suppose $x = x_{\mathrm{ss}} + x_{\mathrm{n}} = y_{\mathrm{ss}} + y_{\mathrm{n}}$ are two distinct decompositions. Then $y_{\mathrm{ss}} - y_{\mathrm{ss}} = -y_{\mathrm{n}} + h_{\mathrm{n}}$, and x_{ss}, x_{n} commute with t_{ss}, t_{n}. This is because x_{ss} and x_{n} are polynomials in x. It follows that $-x_{\mathrm{n}} + y_{\mathrm{n}}$ is nilpotent. The matrices x_{ss}, y_{ss} commute, so they are simultaneously diagonalizable. So $x_{\mathrm{ss}} - y_{\mathrm{ss}}$ is still semisimple. But $x_{\mathrm{ss}} - y_{\mathrm{ss}}$ is also nilpotent, so $x_{\mathrm{ss}} = y_{\mathrm{ss}}$.

Case 2: the eigenvalues of x may not lie in k. Take a Galois extension K/k containing all the eigenvalues of x. (For example, we could let K be the extension of k generated by the eigenvalues of x.) We can write $x = x_{\mathrm{ss}} + x_{\mathrm{n}}$, where $x_{\mathrm{ss}}, x_{\mathrm{n}} \in \mathfrak{gl}(V) \otimes K$. For any $\sigma \in \mathrm{Gal}(K/k)$, we have $\sigma(x) = x$, because $x \in \mathfrak{gl}(V)$. But then $x = \sigma(x_{\mathrm{ss}}) + \sigma(x_{\mathrm{n}})$, and this is another additive Jordan decomposition of x. By uniqueness in the first case, we see that x_{ss} and x_{n} are fixed by σ. Since σ was arbitrary, x_{ss} and x_{n} lie in $\mathfrak{gl}(V)$. □

For a more careful proof, see [$\mathrm{Alg}_{4\text{–}7}$, VII §5.8 thm.1].

Example 3.6.5. This shows that the perfectness hypothesis on k is necessary. Let $k = \mathbf{F}_2(t)$. Consider the matrix $x = \begin{pmatrix} & 1 \\ t & \end{pmatrix}$. This has characteristic polynomial $x^2 - t$, so its only eigenvalue is $\sqrt{2}$ appearing with multiplicity two. So the only way we could give x a Jordan decomposition is $\begin{pmatrix} \sqrt{t} & \\ & \sqrt{t} \end{pmatrix} + \begin{pmatrix} -\sqrt{t} & 1 \\ t & -\sqrt{t} \end{pmatrix}$. The problem is, this doesn't work after a separable base change. More concretely, this doesn't descend back to k. ▷

Theorem 3.6.6 (Multiplicative Jordan decomposition)**.** *Let k be a perfect field, V a finite-dimensional k-vector space. For any $g \in \mathrm{GL}(V)$, there exists unique $g_{\mathrm{ss}}, g_{\mathrm{u}} \in \mathrm{GL}(V)$ such that*

1. $g = g_{\mathrm{ss}} g_{\mathrm{u}}$*,*
2. g_{ss} *is semisimple,*
3. g_{u} *is unipotent, and*
4. g_{ss} *and* g_{u} *commute.*

Proof. Recall that we can write $g = g_{\mathrm{ss}} + g_{\mathrm{n}}$. Just rewrite it as $g_{\mathrm{ss}}(1 + g_{\mathrm{ss}}^{-1} g_{\mathrm{n}})$, and note that $g_{\mathrm{ss}}^{-1} g_{\mathrm{n}}$ is nilpotent because g_{n} is nilpotent and g_{ss} commutes with g_{n}. So $g_{\mathrm{u}} = 1 + g_{\mathrm{ss}}^{-1} g_{\mathrm{n}}$. Uniqueness is similarly easy. □

We'd like to connect the theory of Jordan decomposition with algebraic groups. Let $G_{/k}$ be a linear algebraic group, $\rho : G \to \mathrm{GL}(n)$ a representation. For $g \in G(k)$, we can write $\rho(g) = h_{\mathrm{ss}} h_{\mathrm{u}}$. It is a beautiful fact that $h_{\mathrm{ss}} = \rho(g_{\mathrm{ss}})$, $h_{\mathrm{u}} = \rho(g_{\mathrm{u}})$ for uniquely determined $g_{\mathrm{ss}}, g_{\mathrm{u}} \in G(k)$.

Similarly, let $\mathfrak{g}$ be a k-Lie algebra, $\rho : \mathfrak{g} \to \mathfrak{gl}(V)$ a faithful representation. For $x \in \mathfrak{g}$, the decomposition $\rho(x) = \rho(x)_{\mathrm{ss}} + \rho(x)_{\mathrm{n}}$ comes from a uniquely determined decomposition $x = x_{\mathrm{ss}} + x_{\mathrm{n}}$. However, the decomposition $x = x_{\mathrm{ss}} + x_{\mathrm{n}}$ is not functorial – the decomposition may be different for a different embedding $\mathfrak{g} \hookrightarrow \mathfrak{gl}(V)$.

Let $f : G \to H$ be a homomorphism of linear algebraic groups defined over a perfect field k. Let $g \in G(k)$. Then $f(g)_{\mathrm{ss}} = f(g_{\mathrm{ss}})$ and $f(g)_{\mathrm{u}} = f(g_{\mathrm{u}})$. In other words, the Jordan decomposition is functorial. It follows that if $G_{/k}$ is an affine algebraic group (without a choice of embedding $G \hookrightarrow \mathrm{GL}(n)$), then the multiplicative Jordan decomposition within G is well-defined, independent of any choice of embedding.

3.7 Diagonalizable groups

Let k be a field; recall that we are working in the category of fppf sheaves on Sch_k. The affine line $\mathbf{A}^1(S) = \Gamma(S, \mathscr{O}_S)$ is such a sheaf. We have already written $\mathbf{G}_{\mathrm{a}}$ for the affine line considered as an algebraic group. Since $\Gamma(S, \mathscr{O}_S)$ is naturally a commutative ring, we can consider $\mathbf{A}^1$ as a *ring scheme*, i.e. a commutative ring object in the category of schemes. We will write $\mathscr{O}$ for $\mathbf{A}^1$ so considered.

Thus if $G_{/k}$ is an affine algebraic group, the coordinate ring of G is

$$\mathscr{O}(G) = \hom(G, \mathbf{A}^1).$$

We will be interested in

$$\mathrm{X}^*(G) = \hom_{\mathsf{Grp}_{/k}}(G, \mathbf{G}_{\mathrm{m}}) \subset \mathscr{O}(G),$$

the set of *characters* of G.

Lemma 3.7.1. *The set* $\mathrm{X}^*(G)$ *is linearly independent in* $\mathscr{O}(G)$.

Proof. We may assume k is algebraically closed. Let $\chi_1, \dots, \chi_n$ be distinct characters of G, and suppose there is some relation $\sum c_i \chi_i = 0$ in $\mathscr{O}(G)$ with the $c_i \in k$. If $n = 1$, there is nothing to prove. In the general case, we may assume $c_1 \neq 0$. There exists a k-algebra A and $h \in G(A)$ such that $\chi_1(h) \neq \chi_n(h)$. Note that

$$\sum c_i \chi_n(h) \chi_i(g) = \sum c_i \chi_i(h) \chi_i(g) = 0,$$

for all $g \in G$. This implies

$$\sum_{i=1}^{n-1} c_i(\chi_n(h) - \chi_i(h))\chi_i(g) = 0$$

for all $g \in G(B)$ for A-algebras B. Thus $\chi_1, \dots, \chi_{n-1}$ are linearly dependent in $\mathscr{O}(G) \otimes_k A$. The only way this can happen is for $\chi_1, \dots, \chi_{n-1}$ to be linearly dependent in $\mathscr{O}(G)$. Induction yields a contradiction. □

The set $\mathrm{X}^*(G)$ naturally has the structure of a group, coming from the group law on $\mathbf{G}_{\mathrm{m}}$. If $\chi_1, \chi_2 \in \mathrm{X}(G)$, then

$$(\chi_1 + \chi_2)(g) = \chi_1(g)\chi_2(g).$$

Warning: this notation is confusing, because the group law in $\mathbf{G}_{\mathrm{m}}$ is written multiplicatively. But the group law on $\mathrm{X}^*(G)$ will always be written additively.

Example 3.7.2. As an exercise, check that $\mathrm{X}^*(\mathbf{G}_\mathrm{a}) = 0$. ▷

Example 3.7.3. One has $\mathrm{X}^*(\mathrm{SL}_2) = 0$. More generally, $\mathrm{X}^*(\mathrm{SL}_n) = 0$ for all n. ▷

Example 3.7.4. Let's compute $\mathrm{X}^*(\mathbf{G}_\mathrm{m}) = \hom_{\mathsf{Grp}}(\mathbf{G}_\mathrm{m}, \mathbf{G}_\mathrm{m})$. We claim that $\mathrm{X}^*(\mathbf{G}_\mathrm{m}) \simeq \mathbf{Z}$ as a group, with $n \in \mathbf{Z}$ corresponding to the character $t \mapsto t^n$. Indeed, $\mathscr{O}(\mathbf{G}_\mathrm{m}) = k[t^{\pm 1}]$, so we have to classify elements $f \in k[t^{\pm 1}]$ such that $\Delta(f) = f \otimes f$. It is easy to check that these are precisely the powers of t. Alternatively, use the fact that $\mathscr{O}(G)$ has a basis consisting of the obvious characters; by linear independence of characters, these are the only ones. ▷

It is easy to check that $\mathrm{X}^*(G_1 \times G_2) = \mathrm{X}^*(G_1) \oplus \mathrm{X}^*(G_2)$. Thus $\mathrm{X}^*(\mathbf{G}_\mathrm{m}^n) = \mathbf{Z}^n$. A tuple $a = (a_1, \dots, a_n) \in \mathbf{Z}^n$ corresponds to the character $(t_1, \dots, t_n) \mapsto \prod t_i^{a_i}$.

Example 3.7.5. There is a canonical isomorphism $\mathrm{X}^*(\boldsymbol{\mu}_n) = \mathbf{Z}/n$, even if n is not invertible in k. There is an obvious inclusion $\mathbf{Z}/n \hookrightarrow \mathrm{X}(\boldsymbol{\mu}_n)$ sending $a \in \mathbf{Z}/n$ to the character $t \mapsto t^a$. This inclusion is an isomorphism. ▷

In classical texts, if the base field has characteristic $p > 0$, then $\mathrm{X}(\boldsymbol{\mu}_p) = 0$ because they only treat $\bar{k}$-points. In fact, in such texts, they have "$\boldsymbol{\mu}_p = 1$."

From Example 3.7.4 and Example 3.7.5, we see that all finitely generated abelian groups arise as $\mathrm{X}(G)$ for some G.

Theorem 3.7.6. *Let $G_{/k}$ be a linear algebraic group. Then the following are equivalent:*

1. *G is isomorphic to a closed subgroup of some $\mathbf{G}_\mathrm{m}^n$.*
2. *$\mathrm{X}^*(G)$ is a finitely generated abelian group, and forms a k-basis for $\mathscr{O}(G)$.*
3. *Any representation $\rho : G \to \mathrm{GL}(n)$ is a direct sum of one-dimensional representations.*

Proof. $1 \Rightarrow 2$. An embedding $G \hookrightarrow \mathbf{G}_\mathrm{m}^n$ induces a surjection $\mathscr{O}(\mathbf{G}_\mathrm{m}^n) \twoheadrightarrow \mathscr{O}(G)$. The image in $\mathscr{O}(G)$ of a character $\chi \in \mathscr{O}(\mathbf{G}_\mathrm{m}^n)$ is a character, and $\mathscr{O}(\mathbf{G}_\mathrm{m}^n)$ has a basis consisting of characters. The image of a basis is a generating set, so we're done. Alternatively, see [Mil14, 14.8].

$2 \Rightarrow 3$. This is [Mil14, 14.11].

$3 \Rightarrow 1$. By Theorem 2.6.1, there exists an embedding $G \hookrightarrow \mathrm{GL}(n)$, and by 3, we can assume the image of G lies in the subgroup of diagonal matrices, which is isomorphic to $\mathbf{G}_\mathrm{m}^n$. □

Definition 3.7.7. *Let G be a linear algebraic group. If G satisfies any of the equivalent conditions of Theorem 3.7.6, we say that G is* diagonalizable*.*

It is possible to classify diagonalizable groups. Let M be a finitely generated abelian group, whose group law is written multiplicatively. The basic idea is to construct an algebraic group $\mathrm{D}(M)$ such that there is a natural isomorphism $\mathrm{X}^*(\mathrm{D}(M)) = M$. We first define $\mathrm{D}(M)$ as a functor $\mathsf{Alg}_k \to \mathsf{Grp}$ by

$$\mathrm{D}(M)(A) = \hom_{\mathsf{Grp}}(M, A^\times).$$

This is representable, with coordinate ring the group ring

$$k[M] = \left\{ \sum_{m\in M} c_m \cdot m : c_m \neq 0 \text{ for only finitely many } m \right\}.$$

In other words, $k[M]$ is the free k-vector space on M. Addition is formal, and multiplication is defined by $(c_1 m_1)(c_2 m_2) = c_1 c_2 (m_1 m_2)$, the multiplication $m_1 m_2$ taking place in M. It is easy to check that $\mathrm{D}(M)(A) = \hom(k[M], A)$.

There is a canonical isomorphism $\mathrm{X}^*(\mathrm{D}(M)) = M$. Given $m \in \mathrm{X}^*(\mathrm{D}(M))$, we get a character $\chi_m : \mathrm{D}(M) \to \mathbf{G}_{\mathrm{m}}$ defined on A-points by

$$\chi_m(\phi) = \phi(m) \qquad (\phi : M \to A^\times).$$

We will see that this is an isomorphism.

The operation "take $\mathrm{D}(-)$" is naturally a contravariant functor from the category of finitely generated abelian groups to the category of diagonalizable groups over k. By [SGA 3_{II}, VIII 1.6], it induces an (anti-) equivalence of categories

$$\mathrm{D} : \{\text{f.g. ab. groups}\} \rightleftarrows \{\text{diagonalizable gps. over } k\} : \mathrm{X}^*.$$

So diagonalizable groups are exactly those of the form $\mathrm{D}(M)$ for a finitely generated abelian group M. More concretely, every diagonalizable group will be of the form

$$\mathbf{G}_{\mathrm{m}}^n \times \boldsymbol{\mu}_{n_1} \times \cdots \times \boldsymbol{\mu}_{n_r}.$$

3.8 Tori

Let k be a field. Recall that we have an equivalence of categories:

$$\mathrm{X}^* : \{\text{diagonalizable groups } /k\} \rightleftarrows \{\text{f.g. ab. groups}\} : \mathrm{D}.$$

Here $\mathrm{X}^*(G) =^* \hom(G, \mathbf{G}_{\mathrm{m}})$ and $\mathrm{D}(M)(A) = \hom(M, A^\times)$.

Definition 3.8.1. *An algebraic group $G_{/k}$ has* multiplicative type *if $G_{\bar{k}}$ is diagonalizable.*

⋆ The general definition is in [SGA 3_{III}, IX 1.1]. An affine group scheme $G_{/S}$ is said to be of multiplicative type if there is an fpqc cover $\widetilde{S} \to S$ such that $G_{\widetilde{S}}$ is diagonalizable. One says G is *isotrivial* if $\widetilde{S} \to S$ may be taken to be a finite étale cover. By [SGA 3_{II}, X 5.16], all groups of multiplicative type over a field are isotrivial. So if $G_{/k}$ is of multiplicative type, there exists a finite separable extension K/k such that G_K is diagonalizable. ⋆

Definition 3.8.2. *An algebraic group $G_{/k}$ is a* split torus *if $G \simeq \mathbf{G}_{\mathrm{m}}^n$ for some n. The group G is a* torus *if $G_{\bar{k}}$ is a split torus over k.*

⋆ As above, the general definition in [SGA 3_{II}, IX 1.3] is that $G_{/S}$ is a torus if there is an fpqc cover $\widetilde{S} \to S$ such that $G_{\widetilde{S}} \simeq \mathbf{G}_{\mathrm{m}/\widetilde{S}}^n$. As with groups of multiplicative type, if $T_{/k}$ is a torus, then there is a finite separable extension K/k such that $T_K \simeq \mathbf{G}_{\mathrm{m}/K}^n$. ⋆

Example 3.8.3 (Nonsplit tori)**.** Recall that if K/k is a field extension and $G_{/K}$ is an algebraic group, then the *Weil restriction* $\mathrm{R}_{K/k} G$ is the algebraic group representing the functor $A \mapsto G(A \otimes_k K)$ on k-algebras A. Consider $G = \mathrm{R}_{K/k} \mathbf{G}_\mathrm{m}$. For any k-algebra A, we have (by definition) $G(A) = (A \otimes_k K)^\times$. Note that $G(A)$ acts on K_A via multiplication, so there is an embedding $\mathrm{R}_{K/k} \mathbf{G}_\mathrm{m} \hookrightarrow \mathrm{GL}(K)_{/k}$. If K/k is Galois, there is a canonical isomorphism of k-algebras $K \otimes_k K \xrightarrow{\sim} \prod_\Gamma K$, where $\Gamma = \mathrm{Gal}(K/k)$. It sends $x \otimes y$ to the tuple $(x\gamma(y))_\gamma$. Now for $A \in \mathsf{Alg}_K$, we compute

$$\begin{aligned} G(A \otimes_k K) &= G(A \otimes_K (K \otimes_k K)) \\ &= G\left(A \otimes_K \prod_\Gamma K\right) \\ &= \prod_\Gamma G(A). \end{aligned}$$

Thus $(\mathrm{R}_{K/k} \mathbf{G}_\mathrm{m})_K = \prod_\Gamma \mathbf{G}_{\mathrm{m}/K}$, hence $\mathrm{R}_{K/k} \mathbf{G}_\mathrm{m}$ is a torus. But $\mathrm{R}_{K/k} \mathbf{G}_\mathrm{m}$ is not diagonalizable. If it were, by Theorem 3.7.6 the representation $\mathrm{R}_{K/k} \mathbf{G}_\mathrm{m} \hookrightarrow \mathrm{GL}(K)_{/k}$ would factor through the diagonal, whence all coordinates of the image of $(\mathrm{R}_{K/k} \mathbf{G}_\mathrm{m})(k) = K^\times$ would be in k, which is clearly false. ▷

Example 3.8.4. A specific case of Example 3.8.3 that is of special interest is when the field extension is $\mathbf{C}/\mathbf{R}$. One writes $\mathbf{S} = \mathrm{R}_{\mathbf{C}/\mathbf{R}} \mathbf{G}_\mathrm{m}$, and calls a representation $\rho : \mathbf{S} \to \mathrm{GL}(V)$ a *Hodge structure* on V. The natural embedding $\mathrm{R}_{\mathbf{C}/\mathbf{R}} \mathbf{G}_\mathrm{m} \hookrightarrow \mathrm{GL}(\mathbf{C})_{/\mathbf{R}}$ can be made explicit via

$$\begin{aligned} \mathbf{S}(A) &= (A \otimes_\mathbf{R} \mathbf{C})^\times \\ &= \{((a,b) \in A \times A : a^2 + b^2 \in A^\times\} \\ &\simeq \left\{\begin{pmatrix} a & -b \\ b & a \end{pmatrix}\right\} \subset \mathrm{GL}_2(A). \end{aligned}$$

See §2 of Deligne's paper [Del71] for more on Hodge structures. ▷

Just as we have a nice classification of diagonalizable groups, we'd like to have a classification theorem for tori (or, more generally, groups of multiplicative type). For general groups $G_{/k}$, we define

$$\mathrm{X}^*(G) = \hom_{\mathsf{Grp}_{/k^\mathrm{sep}}} \left(G_{k^\mathrm{sep}}, \mathbf{G}_{\mathrm{m}/k^\mathrm{sep}}\right).$$

This is an abelian group, and naturally has an action of $\Gamma_k = \mathrm{Gal}(k^\mathrm{sep}/k)$. Indeed, for $\gamma \in \Gamma_k$, let $\gamma : \mathrm{Spec}(k^\mathrm{sep}) \to \mathrm{Spec}(k^\mathrm{sep})$ be the induced map. The pullback $\gamma^* G$ is defined on k^sep-algebras A by

$$(\gamma^* G)(A) = G(A \otimes_\gamma k^\mathrm{sep}).$$

In other words, A is viewed as a k^sep-algebra via γ, so that $x \cdot a = \gamma(x)a$. If $\chi \in \mathrm{X}^*(G)$, the character $\gamma\chi$ is defined by the commutative diagram, in which the outer squares are pullbacks:

$$\begin{tikzcd} G_{k^{\mathrm{sep}}} \arrow[r] \arrow[d] & \gamma^* G_{k^{\mathrm{sep}}} \arrow[r, "\gamma^*\chi"] \arrow[d] & \gamma^* \mathbf{G}_{\mathrm{m}/k^{\mathrm{sep}}} \arrow[r] \arrow[d] & \mathbf{G}_{\mathrm{m}/k^{\mathrm{sep}}} \arrow[d] \\ k^{\mathrm{sep}} \arrow[r, "\gamma^{-1}"] & k^{\mathrm{sep}} \arrow[r, equal] & k^{\mathrm{sep}} \arrow[r, "\gamma"] & k^{\mathrm{sep}} \end{tikzcd} \tag{$*$}$$

Here we have written k^{sep} instead of $\mathrm{Spec}(k^{\mathrm{sep}})$ in order to save space. On k^{sep}-points, this map is $(\gamma\chi)(g) = \gamma(\chi(\gamma^{-1}g))$.

Example 3.8.5. Let K/k be a finite Galois extension with $\Gamma = \mathrm{Gal}(K/k)$. We have seen in Example 3.8.3 that there is a natural isomorphism $X^*(\mathrm{R}_{K/k}\, \mathbf{G}_{\mathrm{m}}) = \mathbf{Z}[\Gamma]$ of abelian groups. It is a good exercise to check that this isomorphism respects the Γ-action, i.e. that $X^*(\mathrm{R}_{K/k}\, \mathbf{G}_{\mathrm{m}}) = \mathbf{Z}[\Gamma]$ as Γ-modules. ▷

Example 3.8.6. Let $\mathbf{S}$ be the group in Example 3.8.4. Then over $\mathbf{R}$, all characters are powers of

$$\det : \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mapsto a^2 + b^2.$$

But over $\mathbf{C}$, there are two characters,

$$z : \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mapsto a + bi$$
$$\bar{z} : \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \mapsto a - bi.$$

The group $\mathrm{X}^*(G_{\mathbf{C}})$ has some extra structure, namely an action of the group $\mathrm{Gal}(\mathbf{C}/\mathbf{R}) = \langle c \rangle$. The generator c interchanges z and $\bar{z}$. So under the obvious isomorphism $\mathrm{X}^*(G) \simeq \mathbf{Z}^2$, the action of $\mathrm{Gal}(\mathbf{C}/\mathbf{R})$ is $c \cdot (n_1, n_2) = (n_2, n_1)$. Moreover, $\mathrm{H}^0(\mathbf{R}, \mathrm{X}^*(G)) = \det^{\mathbf{Z}}$, and the kernel of det on G is

$$\mathbf{S}^{\det=1} = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} : a^2 + b^2 = 1 \right\} \subset \mathrm{GL}(2)_{/\mathbf{R}}.$$

The group $\mathbf{S}^{\det=1}$ fits inside a short exact sequence $1 \to \mathbf{S}^{\det=1} \to \mathbf{S} \to \mathbf{G}_{\mathrm{m}} \to 1$, so on the level of characters, we have a short exact sequence of $\mathbf{Z}[\mathrm{Gal}(\mathbf{C}/\mathbf{R})]$-modules

$$0 \to \mathrm{X}^*(\mathbf{G}_{\mathrm{m}}) \to \mathrm{X}^*(\mathbf{S}) \to \mathrm{X}^*(\mathbf{S}^{\det=1}) \to 0.$$

Complex conjugation c acts on the quotient $\mathrm{X}^*(\mathbf{S}^{\det=1})$ as multiplication by -1. ▷

Theorem 3.8.7. *Let k be a field, $\Gamma = \mathrm{Gal}(k^{\mathrm{sep}}/k)$. Then the functor X^* induces an exact anti-equivalence of categories*

$$\{\textit{groups of mult. type over } k\} \xrightarrow{\sim} \{\textit{f.g. ab. groups with cont. } \Gamma\textit{-action}\}.$$

Proof. This is [SGA 3_{II}, X 1.4]. □

In general, we call the action of a profinite group Γ on a discrete set X *continuous* if the map $\Gamma \times X \to X$ is continuous. Equivalently, for each $x \in X$, the stabilizer $\mathrm{Stab}_\Gamma(x)$ is open. The action of Γ on $\mathrm{X}^*(G)$ is as given in ($*$).

$\star$ In the proof of Theorem 3.2.14, we saw that it is possible to view $\mathrm{X}^*(G)$ as a group scheme. This makes it possible to recover the Galois action on $\mathrm{X}^*(G)$ in a more natural manner. It is a basic fact (see [SGA 1, V 8.1]) that the category of finite sets with continuous Γ_k-action is equivalent to the category of finite étale covers of $\mathrm{Spec}(k)$. Thus the category of sets with continuous Γ_k-action is equivalent to the category of sheaves on $k_{\text{ét}}$.

In light of this, we construct $\mathrm{X}^*(G)$ as a scheme; its restriction to $k_{\text{ét}}$ recovers the usual definition of $\mathrm{X}^*(G)$. Put

$$\mathrm{X}^*(G)(A) = \hom_{\mathsf{Grp}_{/A}}\left(G_A, \mathbf{G}_{\mathrm{m}/A}\right).$$

If G is of multiplicative type, then by [SGA 3_{II}, XI 4.2], the group functor $\mathrm{X}^*(G)$ is represented by a smooth separated k-scheme. The restriction of this scheme to $k_{\text{ét}}$ recovers the usual definition of $\mathrm{X}^*(G)$. $\star$

Example 3.8.8. Let k be a field of characteristic $\neq 2$. The Kummer theory tells us that quadratic extensions K/k are all of the form $k(\sqrt{d})/k$ for $d \in k^\times/2 = \mathrm{H}^1(k, \boldsymbol{\mu}_2)$. Since $2 \in k^\times$, we have $\boldsymbol{\mu}_2 = \mathbf{Z}/2 = \mathrm{Aut}(\mathbf{G}_\mathrm{m})$. Thus k-forms of $\mathbf{G}_\mathrm{m}$ are classified by $\mathrm{H}^1(k, \mathbf{Z}/2) = k^\times/2$. We can work this out explicitly. For $c \in \mathrm{H}^1(k, \boldsymbol{\mu}_2)$, let k_c/k be the corresponding quadratic extension, and let $c^*\mathbf{G}_\mathrm{m}$ be defined by

$$c^*\mathbf{G}_\mathrm{m} = \ker\left(\mathrm{R}_{k_c/k}\,\mathbf{G}_\mathrm{m} \hookrightarrow \mathrm{GL}(k_c)_{/k} \xrightarrow{\det} \mathbf{G}_\mathrm{m}\right).$$

The group $c^*\mathbf{G}_\mathrm{m}$ can be written explicitly as

$$\left\{\begin{pmatrix} a & bc \\ b & a \end{pmatrix} : a^2 - cb^2 = 1\right\} \subset \mathrm{GL}(2)_{/k}.$$

The isomorphism type of $c^*\mathbf{G}_\mathrm{m}$ depends only on the class of c in $k^\times/2$. Moreover, $\mathrm{X}^*(c^*\mathbf{G}_\mathrm{m}) \simeq \mathbf{Z}$, with the action of Γ_k factoring through $\mathrm{Gal}(k_c/k)$ and being multiplication by -1 on the unique generator of $\mathrm{Gal}(k_c/k)$. ▹

Note that general tori can be extremely difficult to classify. For example, when $k = \mathbf{Q}$, the category of tori over $\mathbf{Q}$ is anti-equivalent to the category of finitely generated abelian groups with $\Gamma_\mathbf{Q}$-action. The group $\Gamma_\mathbf{Q}$ can be recovered from its finite quotients, but it is still very mysterious.

Example 3.8.9. Over $\mathbf{R}$, if we have an involution c acting on a lattice $\mathbf{Z}^n$, then with respect to some basis, c wiill have the form

$$(1)^{\oplus a} \oplus (-1)^{\oplus b} \oplus \begin{pmatrix} & 1 \\ 1 & \end{pmatrix}^{\oplus c}$$

So any torus over $\mathbf{R}$ breaks up as a product of copies of $\mathbf{G}_\mathrm{m}$, copies of $\mathbf{S}$, and copies of $\mathbf{S}^{\det=1}$. ▹

Over a general field, any torus is a quotient of products of $\mathrm{R}_{K/k}\,\mathbf{G}_\mathrm{m}$ for varying K/k.

If T is a diagonalizable group and $\rho : T \to \mathrm{GL}(V)$ a representation of T, then we have a direct sum decomposition

$$V = \bigoplus_{\chi \in \mathrm{X}^*(T)} V_\chi,$$

where $V_\chi = \{v \in V : \rho(g)v = \chi(g)v \text{ for all } g\}$. The χ for which $V_\chi \neq 0$ will be called the *weights* of V. To summarize, every representation of a split torus is semisimple, the direct sum of a bunch of characters.

For T of multiplicative type, all representations are semisimple. The irreducible representations are given by Galois orbits in $\mathrm{X}^*(T)$.

Tori have strong rigidity properties which will be useful later. Recall that if T_2, T_2 are tori, we write $\hom(T_1, T_2)$ for the scheme over k whose functor of points is

$$\hom(T_1, T_2)(S) = \hom_{\mathsf{Grp}_{/S}}(T_{1S}, T_{2S}).$$

By [SGA 3_{II}, XI 4.2], this is represented by a smooth scheme over k. If $X_{/k}$ is a scheme, a *family of homomorphisms* from T_1 to T_2 parameterized by X is just a morphism $X \to \hom(T_1, T_2)$. By general nonsense, it is equivalent to give a morphism $\phi : X \times T_1 \to T_2$ such that for all $x \in X(S)$, the map $T_{1S} \to T_{2S}$ given by $t \mapsto \phi(x, t)$ is a homomorphism. We say a family of homomorphisms $\phi : X \to \hom(T_1, T_2)$ is *constant* if the morphism ϕ is constant, i.e. if $\phi(x)$ does not depend on x. Alternatively, the morphism $X \times T_1 \to T_2$ factors as $X \times T_1 \twoheadrightarrow T_1 \xrightarrow{\phi} T_2$.

Theorem 3.8.10 (Rigidity of tori)**.** *Let k be a field, $T_{/k}$ a torus, $X_{/k}$ a connected variety. Any family $X \to \hom(T, T)$ of homomorphisms is constant.*

Proof. We'll use two facts.

1. For $n \geqslant 1$, let ${}_nT = \ker(T \xrightarrow{n} T)$. Then $\{{}_nT\}$ is dense in T [SGA 3_{II}, IX 4.7].

2. For each $n \geqslant 1$ invertible in k, the scheme ${}_nT$ is finite étale over k. (This follows from étale descent.)

The family $X \to \hom(T, T)$ induces, for each n invertible in k, a family $X \to \hom({}_nT, {}_n)$, which by [SGA 3_{II}, X 4.2] is finite étale. Since X is connected, each $X \to \hom({}_nT, {}_nT)$ is constant. By the first fact, we obtain that X is constant. □

Example 3.8.11. This shows that Theorem 3.8.10 fails for groups that are not tori. Let $G = \mathrm{SL}(2)$. Then the map $G \times G \to G$ given by $(g, h) \mapsto ghg^{-1}$ is a perfectly good family of homomorphisms that is not constant. One has $\mathrm{PSL}(2) \hookrightarrow \mathrm{Aut}(\mathrm{SL}_2)$, with image of index two. The other coset is generated by $g \mapsto {}^{\mathrm{t}}g^{-1}$. ▹

4 Semisimple groups

Let k be an algebraically closed field of characteristic zero. Let $G_{/k}$ be a reductive algebraic group. That is, G is connected and $\mathcal{R}_{\mathrm{u}}G = 1$. We will associate to G some combinatorial data, called the *root datum*. The root datum of G will characterize G up to isomorphism, will not depend on the field k, and will completely determine the representation theory of G. Much of the theory will depend on the notions of *maximal torus* and *Borel subgroup*. To prove basic properties of these, we need to be able to take quotients, and it is to this that we now turn. The theory of quotients requires quite a bit of, sophistication, and may safely be skipped at first reading.

4.1 Quotients revisited ⋆

The "morally correct" place to take quotients is in the category of fppf sheaves.

Definition 4.1.1. *A finite family $\{f_i : X_i \to X\}$ of morphisms of schemes is an* fppf cover *if it is jointly surjective (on points), and each $X_i \to X$ is flat, of finite presentation, and quasi-finite.*

We write fppf for the topology generated by fppf covers. Recall that a topology is called *subcanonical* if each representable functor is a sheaf. Also, a *sieve* on X is a subfunctor of $h_X = \hom(-, X)$. We reproduce the following theorem from SGA.

Theorem 4.1.2.

1. *A sieve S on X is a cover for the fppf topology if and only if there is an open affine cover $\{X_i\}$ of X together with affine fppf covers $\{X_{ij} \to X_i\}$ such that each $X_{ij} \to X$ is in S.*
2. *A presheaf F on* Sch *is an fppf sheaf if and only if:*
   - *(a) F is a Zariski sheaf.*
   - *(b) For each fppf cover $X \to Y$, where X and Y are affine, the following diagram is an equalizer:*

$$F(X) \longrightarrow F(Y) \rightrightarrows F(Y \times_X Y).$$

3. *The fppf topology is subcanonical.*
4. *If $\{X_i \to X\}$ is jointly surjective and each $X_i \to X$ is faithfully flat and of finite presehtation, then $\{X_i \to X\}$ is an fppf cover.*

Proof. This is [SGA 3_{I}, IV 6.3.1]. □

A good general source for topologies and sheaves is the book [MLM94]. From it, we get that the category $\mathrm{Sh}_{\mathrm{fppf}}(\mathsf{Sch}_S)$ is a *topos*. That is, limits, colimits and more exist in the category of sheaves on Sch_S. However, it can be quite tricky to check whether a given colimit of schemes (taken in the fppf topology) is actually represented by a scheme.

Let k be a field. For the remainder, we'll work in the category of fppf sheaves on Sch_k. We'll call such sheaves *spaces*.

Definition 4.1.3. *Let G be a k-group space. A k-space X is called a G-*space *if it is equipped with a morphism $G \times X \to X$, such that for each $S \in \mathsf{Sch}_k$, the map $G(S) \times X(S) \to X(S)$ gives an action of the group $G(S)$ on the set $X(S)$.*

If $G_{/k}$ is an algebraic group and $X_{/k}$ is a variety, we call X a *G-variety*, or *variety with G-action*. (Recall that for us, a *variety* over k is a separated scheme of finite type over k.) The representability of quotients $G\backslash X$ is a subtle one, but fortunately we only need to take quotients G/H, where $H \subset G$ is an algebraic subgroup.

Theorem 4.1.4. *Let $G_{/k}$ be an algebraic group, $H \subset G$ an algebraic subgroup. Then the fppf quotient G/H is a variety over k. If G is smooth, so is G/H, and if H is normal, then G/H has a unique structure of a group scheme for which $G \to G/H$ is a homomorphism.*

Proof. This is [SGA 3_{I}, VI_{A} 3.2]. □

A major theorem whose proof uses quotients is the Borel fixed point theorem. To state it, we need some terminology. Following [EGA 2, II 5.4.1], we say a morphism $f : X \to Y$ of schemes is *proper* if it is separated, of finite type, and if for all $Y' \to Y$, the induced morphism $X_{Y'} \to Y$ is closed. We call a variety $X_{/k}$ proper if the structure map $X \to \operatorname{Spec}(k)$ is proper. There is a valuative criterion for properness [EGA 2, II 7.3.8]. One considers pairs (A, K), where A is a valuation ring with morphism $\operatorname{Spec}(A) \to Y$, and K is the field of fractions of Y. A morphism $X \to Y$ is proper if and only if for all such pairs, the map $X_{/Y}(A) \to X_{/Y}(K)$ is a bijection. If $f : X \to Y$ is a morphism of varieties over $\mathbf{C}$, then by [SGA 1, XII 3.2], f is proper if and $f : X(\mathbf{C}) \to Y(\mathbf{C})$ is proper in the topological sense. (Following [$\mathrm{Top}_{1\text{–}4}$, I §10.2 th.1], a map $f : X \to Y$ between Hausdorff spaces is proper if it is closed, and the preimage of any compact set is compact.)

Theorem 4.1.5. *Let k be an algebraically closed field, $G_{/k}$ a connected solvable group, and $X_{/k}$ a proper non-empty G-variety. Then $X^G \neq \varnothing$.*

Proof. We induct on the dimension of G. If G is one-dimensional, then G is one of $\{\mathbf{G}_{\mathrm{a}}, \mathbf{G}_{\mathrm{m}}\}$, so neither G nor any of its nontrivial quotients are proper. For $x \in X(k)$, let $G_x = \operatorname{Stab}_G(x)$. Either $G_x = G$, in which case $x \in X^G(k)$, or G_x is finite, in which case we have an embedding $G/G_x \hookrightarrow X$ given by $g \mapsto gx$. By passing to the closure of the image of this map, we may assume the image of G/G_x in X is dense. Thus $X \smallsetminus G/G_x$ is a G-stable finite nonempty (because G isn't proper) variety on which G acts, hence $X^G \supset X \smallsetminus G/G_x$.

In the general case, choose a one-dimensional normal subgroup $H \subset G$. By induction, $X^H \neq \varnothing$, and by the first part of the proof, $X^G = (X^H)^{G/H} \neq \varnothing$.

For a more careful proof, see [Mil14, 18.1]. □

Checking the valuative (or topological) criteria for properness can be pretty difficult. There is a special class of morphisms, called *projective morphisms*, that are automatically proper. Let S be a base scheme, and $\mathscr{E}$ a quasi-coherent sheaf on S. Define a functor $\mathbf{P}(\mathscr{E})$ on Sch_S by

$$\mathbf{P}(\mathscr{E})(X) = \{(\mathscr{L}, \varphi) : \mathscr{L} \text{ is invertible and } \varphi : \mathscr{E}_X \twoheadrightarrow \mathscr{L}\}/\simeq .$$

That is, $\mathbf{P}(\mathscr{E})(X)$ is the set of isomorphism classes of pairs $(\mathscr{L}, \varphi)$, where $\mathscr{L}$ is a line bundle on X and $\varphi : \mathscr{E}_X \twoheadrightarrow \mathscr{L}$ is a surjection. By [EGA 2, II 4.2.3], this functor is representable. Following [EGA 2, II 5.5.2], a morphism $f : X \to Y$ is called *projective* if it factors as $X \hookrightarrow \mathbf{P}(\mathscr{E}) \twoheadrightarrow Y$, where $\mathscr{E}$ is a coherent $\mathscr{O}_Y$-module, $X \hookrightarrow \mathbf{P}(\mathscr{E})$ is a closed immersion and $\mathbf{P}(\mathscr{E}) \twoheadrightarrow Y$ is the canonical morphism. Equivalently, X is isomorphic to $\operatorname{Proj}(\mathscr{A})$ for some sheaf $\mathscr{A} = \mathscr{A}_\bullet$ of graded $\mathscr{O}_Y$-algebras, which is generated as an $\mathscr{O}_Y$-algebra by $\mathscr{A}_1$, and for which $\mathscr{A}_1$ is coherent. By [EGA 2, II 5.5.3], projective morphisms are proper. In particular, if we work over a base field k, all closed subschemes of $\mathbf{P}(V)$ for a finite-dimensional k-vector space V are proper.

You need to be careful when taking quotients. As motivation, suppose $G_{/k}$ is an algebraic group and $Z \subset \mathrm{Z}(G)$ is a central subgroup. For any k-algebra A, we have a long exact sequence

$$1 \to Z(A) \to G(A) \to (G/Z)(A) \to \mathrm{H}^1_{\mathrm{fppf}}(A, Z) \to \cdots$$

So $(G/Z)(A)$ is "easy" to understand when Z is "cohomologically trivial" in some sense. Conversely, when Z has nontrivial cohomology, G/Z tends to be trickier to study directly.

Example 4.1.6. Consider the algebraic group $\mathrm{PGL}(n) = \mathrm{GL}(n)/\mathbf{G}_\mathrm{m}$. See [Con, 1.6.3] for a careful construction. It is well-known that $\mathrm{H}^1(A, \mathbf{G}_\mathrm{m}) = \mathrm{Pic}(A)$, the group of isomorphism classes of invertible A-modules. Thus if A is a Dedekind domain with non-trivial class group, the map $\mathrm{GL}_n(A)/A^\times \to \mathrm{PGL}_n(A)$ is *not* surjective. But since $\mathrm{Pic}(k) = 0$ for all fields K, one has $\mathrm{PGL}_n(k) = \mathrm{GL}_n(k)/k^\times$. ▷

Example 4.1.7. This problem presents itself even earlier with $\mathrm{PSL}(n) =$"$\mathrm{SL}(n)/\boldsymbol{\mu}_n$." The problem is, by Kummer theory, $\mathrm{H}^1(k, \boldsymbol{\mu}_n) = k^\times/n$ whenever n is invertible in k. So, for example, $\mathrm{SL}_2(\mathbf{R}) \to \mathrm{PSL}_2(\mathbf{R})$ should not be surjective, because it has cokernel $\mathrm{H}^1(\mathbf{R}, \boldsymbol{\mu}_2) = \mathbf{Z}/2$. It turns out that the quotient sheaf $\mathrm{SL}(n)/\boldsymbol{\mu}_n$ is actually $\mathrm{PGL}(n)$. For this reason, we will only use notation $\mathrm{PSL}(n)$ when taking its k-valued points. See `http://mathoverflow.net/questions/16145/` for more discussion of this. ▷

4.2 Centralizers, normalizers, and transporter schemes

Here we define some constructions scheme-theoretically that will be used extensively in the structure theory of reductive groups. Fix a base scheme S, and let $G_{/S}$ be a group scheme. If $X, Y \subset G$ are subschemes, the *transporter scheme* $\mathrm{Transp}_G(X, Y)$ and the *strict transporter scheme* $\mathrm{stTransp}_G(X, Y)$ are given by their functors of points:

$$\begin{aligned}
\mathrm{Transp}_G(X,Y)(T) &= \{g \in G(T) : \mathrm{ad}(g)(X_T) \subset Y_T\} \\
&= \{g \in G(T) : gX(T')g^{-1} \subset Y(T') \text{ for all } T' \to T\} \\
\mathrm{stTransp}_G(X,Y)(T) &= \{g \in G(T) : \mathrm{ad}(g)(X_T) = Y_T\}.
\end{aligned}$$

Similarly, if $u, v : X \to G$ are morphisms, one defines

$$\mathrm{Transp}_G(u,v)(T) = \{g \in G(T) : \mathrm{ad}(g) \circ u_T = v_V\}.$$

This enables us to define, for a subgroup-scheme $H \subset G$,

$$\begin{aligned}
\mathrm{C}_G(H) &= \mathrm{Transp}_G(H \hookrightarrow G, H \hookrightarrow G) && \text{(the \textit{centralizer})} \\
\mathrm{N}_G(H) &= \mathrm{stTransp}_G(H,H) && \text{(the \textit{normalizer})}.
\end{aligned}$$

We reproduce the following theorem from SGA.

Theorem 4.2.1. *Let k be a field, $G_{/k}$ a group scheme of finite type.*

1. *If $X, Y \subset G$ are closed subschemes, then* $\mathrm{Transp}_G(X,Y)$ *and* $\mathrm{stTransp}_G(X,Y)$ *are represented by closed subschemes of G.*

2. *If $u, v : X \to G$ are two morphisms of schemes over k, then* $\mathrm{Transp}_G(u,v)$ *is represented by a closed subscheme of G.*

Proof. This is essentially [SGA 3_{I}, VI_{B} 6.2.5]. □

Corollary 4.2.2. *Let k be a field, $G_{/k}$ a group scheme of finite type, and $H \subset G$ a closed subgroup scheme. Then* $\mathrm{C}_G(H)$ *and* $\mathrm{N}_G(H)$ *are represented by closed subgroup schemes of G*

Clearly $\mathrm{C}_G(H) \subset \mathrm{N}_G(H)$.

4.3 Borel subgroups

For this section, k is an algebraically closed field of characteristic zero.

Definition 4.3.1. *Let $G_{/k}$ be a linear algebraic group. A* Borel subgroup *of G is a connected solvable subgroup $B \subset G$ that is maximal with respect to those properties.*

Theorem 4.3.2. *Let $G_{/k}$ be a linear algebraic group. Then all Borel subgroups of G are conjugate.*

Proof. Let B_1, B_2 be two Borel subgroups. By [Mil14, 18.11.a], the variety G/B_1 is proper. By Theorem 4.1.5, the left-action of B_2 on G/B_1 admits a fixed point gB_1. One has $B_2 \subset \mathrm{ad}(g)(B_1)$; by maximality $B_2 = \mathrm{ad}(g)(B_1)$. □

In general, one calls the quotient G/B of G by a Borel subgroup B the *flag variety* of G.

Example 4.3.3. If $G = \mathrm{GL}(n)$, then by Theorem 3.2.14, the subgroup B of upper-triangular matrices is a Borel subgroup. We will see that G/B is proper. Indeed, we will work in much greater generality. Let S be a base scheme and $\mathscr{E}$ a locally free $\mathscr{O}_S$-module. If $X_{/S}$ is a scheme, write $\mathscr{E}_X$ for the pullback of $\mathscr{E}$ to X. Write $\mathrm{GL}(\mathscr{E})$ for the functor $X \mapsto \mathrm{Aut}_{\mathscr{O}_X}(\mathscr{E}_X)$. This is an open subscheme of $\mathbf{V}(\mathscr{E}^\vee \otimes \mathscr{E})$, so it is representable.

Let $n = \mathrm{rk}(\mathscr{E})$; for $r < n$, let $\mathrm{Gr}(\mathscr{E}, r)$ be the functor given by

$$\mathrm{Gr}(\mathscr{E}, r)(X) = \{\mathscr{E}_X \twoheadrightarrow \mathscr{F} : \mathscr{F} \text{ is a locally free } \mathscr{O}_X\text{-module of rank } r\}/\simeq .$$

By [Nit05, ex.2], this is representable. note that $\mathrm{Gr}(\mathscr{E}, 1) = \mathbf{P}(\mathscr{E})$, so $\mathrm{Gr}(\mathscr{E}, 1)$ is projective. More generally, for each r the operation "take r-th wedge power" gives a closed embedding $\mathrm{Gr}(\mathscr{E}, r) \hookrightarrow \mathbf{P}(\bigwedge^r \mathscr{E})$, so all the $\mathrm{Gr}(\mathscr{E}, r)$ are projective. Put $\mathrm{Gr}(\mathscr{E}) = \prod_{r<n} \mathrm{Gr}(\mathscr{E}, r)$; this is projective via the Segre embedding [EGA 2, II 4.3.3]

$$\mathbf{P}(\mathscr{E}) \times \cdots \times \mathbf{P}(\textstyle\bigwedge^{n-1} \mathscr{E}) \hookrightarrow \mathbf{P}(\mathscr{E} \otimes \cdots \otimes \textstyle\bigwedge^{n-1} \mathscr{E}).$$

Suppose $\mathscr{E}$ admits a descending filtration $\mathrm{fil}^\bullet \mathscr{E}$ such that each quotient $\mathscr{E}_r = \mathscr{E}/\mathrm{fil}^r$ has rank r. Define a closed subgroup of $\mathrm{GL}(\mathscr{E})$ by

$$B(X) = \{g \in \mathrm{GL}(\mathscr{E})(X) : g \text{ preserves } \mathrm{fil}^\bullet\}.$$

This is a Borel subgroup of $\mathrm{GL}(\mathscr{E})$. We will realize the relative flag variety G/B as a closed subscheme of $\mathrm{Gr}(\mathscr{E})$. If $X_{/S}$ is a scheme, a *flag (relative to $\mathscr{E}$)* on X is a diagram $\mathscr{E}_X = \mathscr{V}_n \twoheadrightarrow \cdots \twoheadrightarrow \mathscr{V}_0 = 0$ of locally free quotients of $\mathscr{E}_X$, where each $\mathscr{V}_r$ has rank r. Write $\mathscr{V}_\bullet$ for such a flag. Define a functor $\mathrm{Fl}(\mathscr{E})$ by

$$\mathrm{Fl}(\mathscr{E})(X) = \{\text{flags relative to } \mathscr{E} \text{ on } X\}/\simeq .$$

The rule $\mathscr{V}_\bullet \mapsto (\mathscr{V}_r)_r$ gives a closed embedding $\mathrm{Fl}(\mathscr{E}) \hookrightarrow \mathrm{Gr}(\mathscr{E})$. See [DG80, I §2 6.3] for a proof when $S = \mathrm{Spec}(\mathbf{Z})$ and $\mathscr{E} = \mathbf{Z}^n$.

Our filtration $\mathrm{fil}^\bullet \mathscr{E}$ induces an element of $\mathrm{Fl}(\mathscr{E})(S)$, namely $\{\mathscr{E} \twoheadrightarrow \mathscr{E}/\mathrm{fil}^r\}_r$. The action of $\mathrm{GL}(\mathscr{E})$ on $\mathscr{E}$ induces a right action of $\mathrm{GL}(\mathscr{E})$ on $\mathrm{Fl}(\mathscr{E})$, in which an element $g \in \mathrm{GL}(\mathscr{E})(X)$ acts on a flag $\mathscr{E} \twoheadrightarrow \mathscr{V}_\bullet$ by $\mathscr{E} \xrightarrow{g} \mathscr{E} \twoheadrightarrow \mathscr{V}_\bullet$. Moreover, $B \subset \mathrm{GL}(\mathscr{E})$ acts trivially. Assume S is locally noetherian. Then by [SGA 3_{I}, V 10.1.1], the quotient $\mathrm{GL}(\mathscr{E})/B$ exists and comes with an embedding $\mathrm{GL}(\mathscr{E})/B \hookrightarrow \mathrm{Fl}(\mathscr{E})$. We claim that this map is surjective, hence an isomorphism. Indeed, Zariski-locally, it comes down to checking that $\mathrm{GL}(A^n)/B(A) \to \mathrm{Fl}(A^n)$ is surjective, which is a basic fact from linear algebra. Thus $\mathrm{GL}(\mathscr{E})/B \xrightarrow{\sim} \mathrm{Fl}(\mathscr{E})$. ▷

We will be mainly interested in when $S = \mathrm{Spec}(k)$ and $V = k^n$. In this case, we write $\mathrm{Gr}(n, r) = \mathrm{Gr}(k^n, r)$ and $\mathrm{Fl}(n) = \mathrm{Fl}(k^n)$. Thus $\mathrm{GL}(n)/B \xrightarrow{\sim} \mathrm{Fl}(n) \hookrightarrow \mathrm{Gr}(n)$. More generally, we have the following fact.

Theorem 4.3.4. *Let G be a linear algebraic group, $B \subset G$ a Borel subgroup. Then G/B is a projective variety.*

Definition 4.3.5. *Let G be a linear algebraic group. A closed subgroup $P \subset G$ is* parabolic *if G/P is proper.*

Theorem 4.3.6. *A subgroup $P \subset G$ is parabolic if and only if P contains a Borel subgroup of G.*

Proof. $\Leftarrow$. Suppose P contains a Borel subgroup B. Then the inclusion $B \subset P$ induces a map $G/B \twoheadrightarrow G/P$. Since G/B is proper, by [EGA 2, II 5.4.3], so is G/P. Alternatively, see [SGA 3_{II}, XVI 2.5] for a proof over a general base.

$\Rightarrow$. Consider the action of B on the proper variety G/P. By Theorem 4.1.5, there is a fixed point gP. One obtains $\operatorname{ad}(g^{-1})(B) \subset P$, so P contains a Borel subgroup. □

In light of this result, we could have defined a Borel subgroup to be a minimal parabolic subgroup.

4.4 Maximal tori

For this section, k is an algebraically closed field of characteristic zero. Let $G_{/k}$ be a linear algebraic group. A *maximal torus* in G is a subgroup scheme $T \subset G$ that is a torus, and is maximal with respect to this property. In our setting, any torus in G is contained in a maximal torus.

Example 4.4.1. Let $G = \mathrm{GL}(n)$. Then we can choose T to be the subgroup consisting of diagonal matrices. This is a maximal torus because all tori are diagonalizable, so any torus in $\mathrm{GL}(n)$ is conjugate to a subgroup of T. A Borel subgroup consists of upper-triangular matrices. ▷

Theorem 4.4.2. *Let $G_{/k}$ be a linear algebraic group. Then all maximal tori are conjugate.*

Proof. If G is solvable, this is [Mil14, 17.40]. Essentially, one uses the fact that $G = T \ltimes \mathcal{R}_{\mathrm{u}} G$ for any maximal torus T.

If G is a general group, then different maximal tori T_1, T_2 will live in Borel subgroups B_1, B_2. By Theorem 4.3.2, the subgroups B_1 and B_2 are conjugate, so we may as well assume T_1 and T_2 are maximal tori in the same Borel subgroup B. But then we can use the fact that the theorem holds for solvable groups. □

Example 4.4.3. Let $\rho : G \to \mathrm{GL}(V)$ be a representation, where G is a connected solvable group. Then G acts on $\mathbf{P}(V)$ via $\mathrm{GL}(V)$, so Theorem 4.1.5 tells us that G fixes a vector, i.e. that V contains a G-invariant line. ▷

Lemma 4.4.4. *Let $T \subset G$ be a torus. Then the quotient $\mathrm{W}_G(T) = \mathrm{C}_G(T)^\circ = \mathrm{N}_G(T)^\circ$, hence the quotient $\mathrm{N}_G(T)/\mathrm{C}_G(T)$ is finite étale.*

Proof. There is an obvious family $\mathrm{N}_G(T)^\circ \times T \to T$ given by $(y,t) \mapsto yty^{-1}$. By Theorem 3.8.10, this is constant, hence $\mathrm{N}_G(T)^\circ \subset \mathrm{C}_G(T)$. □

One calls $\mathrm{W}_G(T)$ the *Weyl group* of the pair (G,T). It is finite étale over k.

Lemma 4.4.5. *Let $G_{/k}$ be a connected reductive group. Then $\mathcal{R}G = \mathrm{Z}(G)^\circ$.*

Proof. Note that $\mathcal{R}G$ is a torus. Since $\mathcal{R}G$ is normal in G, there is a family $G \times \mathcal{R}G \to \mathcal{R}G$ given by $(y, t) \mapsto yty^{-1}$. Again by Theorem 3.8.10, this is trivial, hence $\mathcal{R}G \subset \mathrm{Z}(G)$. The result follows. □

Lemma 4.4.6. *Let G be a connected linear algebraic group that admits a faithful irreducible representation $\rho : G \hookrightarrow \mathrm{GL}(V)$. Then G is reductive.*

Proof. We may assume that $G \subset \mathrm{GL}(V)$. Let $H = \mathcal{R}_{\mathrm{u}}G$; the space V^H is nonzero since H is unipotent. In fact, since H is normal in G, V^H is a subrepresentation of V. Since V is simple, $V^H = V$. But $G \subset \mathrm{GL}(V)$, so $H = 1$. □

Corollary 4.4.7. *The groups* $\mathrm{GL}(n)$, $\mathrm{SL}(n)$, $\mathrm{SO}(2n)$ *and* $\mathrm{Sp}(2n)$ *are reductive.*

Proof. Apply Lemma 4.4.6 to the standard representations. For SO and Sp, use the fact that the group preserves a nondegenerate bilinear form. □

Theorem 4.4.8. *Let k be a field, $G_{/k}$ a reductive group. If $T \subset G$ is a torus, then $\mathrm{C}_G(T)$ is reductive. If T is maximal, then $\mathrm{C}_G(T) = T$.*

Proof. This is [SGA 3_{III}, XIX 1.6]. □

4.5 Root systems

Let k be a field, $G_{/k}$ a reductive group, $\mathfrak{g} = \mathrm{Lie}(G)$. In subsection 2.8, we defined a canonical representation $\mathrm{ad} : G \to \mathrm{GL}(\mathfrak{g})$. Let $T \subset G$ be a maximal torus. We are interested in the representation $\mathrm{ad}|_T : T \to \mathrm{GL}(\mathfrak{g})$. For simplicity, assume T is diagonalizable (i.e. , a *split* torus). By Theorem 3.7.6, there is a decomposition

$$\mathfrak{g} = \bigoplus_{\alpha \in \mathrm{X}^*(T)} \mathfrak{g}_\alpha,$$

where for $\alpha \in \mathrm{X}^*(T)$, the space $\mathfrak{g}_\alpha = \{x \in \mathfrak{g} : tg = \alpha(t)g \text{ for all } t \in T\}$. Let $\mathrm{R}(G, T) = \{\alpha \in \mathrm{X}^*(T) \smallsetminus 0 : \mathfrak{g}_\alpha \neq 0\}$. Then we have a decomposition

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \bigoplus_{\alpha \in \mathrm{R}(G,T)} \mathfrak{g}_\alpha.$$

We call $\mathrm{R}(G, T) \subset \mathrm{X}^*(G)$ the set of *roots* of G. This is a finite set.

Let V be the span of $\mathrm{R}(G, T)$ in $\mathrm{X}^*(T)_{\mathbf{R}} = \mathrm{X}^*(T) \otimes \mathbf{R}$. The finite set $\mathrm{R}(G, T)$ sitting inside the real vector space V is an example of a "root system." General root systems break up into irreducibles, and there is a combinatorial classification of irreducible root systems into types $\mathrm{A}_n, \mathrm{B}_n, \mathrm{C}_n, \mathrm{D}_n, \mathrm{G}_2, \mathrm{F}_4, \mathrm{E}_6, \mathrm{E}_7, \mathrm{E}_8$. The root system $\mathrm{R}(G, T) \subset V$ will recover $G/\mathrm{Z}(G)$.

Example 4.5.1. We will work out the root datum of $\mathrm{SL}(n+1)$ for $n \geqslant 1$. We choose the maximal torus

$$
\begin{aligned}
T &= \left\{\operatorname{diag}(a_1, \dots, a_{n+1}) : a_i \in \mathbf{G}_{\mathrm{m}} \text{ and } \prod a_i = 1\right\} \\
&= \begin{pmatrix} * & & \\ & \ddots & \\ & & * \end{pmatrix} \subset \mathrm{SL}(n+1).
\end{aligned}
$$

Define $\chi_i : T \to \mathbf{G}_{\mathrm{m}}$ by $\chi_i(\operatorname{diag}(a_1, \dots, a_{n+1})) = a_i$. Then $(\chi_1, \dots, \chi_n)$ induces an isomorphism between T and the subgroup of $\mathbf{G}_{\mathrm{m}}^{n+1}$ consisting of $(a_1, \dots, a_{n+1})$ with $a_1 \cdots a_{n+1}) = 1$. Thus $\mathrm{X}^*(T) = \{\sum a_i \chi_i : \sum a_i = 0\}$.

The Lie algebra $\mathfrak{sl}(n+1)$ is spanned by $\mathfrak{t} = \mathrm{Lie}(T)$ and the set

$$\{E_{i,j} = (\delta_{i,a}\delta_{j,b})_{a,b}\} \subset \mathfrak{sl}(n+1).$$

Moreover, one can check that

$$\operatorname{ad}\left(\operatorname{diag}(a_1, \dots, a_{n+1})\right)(E_{i,j}) = \frac{a_i}{a_j} E_{i,j}.$$

Thus, the root decomposition of $\mathfrak{sl}(n+1)$ is

$$\mathfrak{sl}(n+1) = \mathfrak{t} \oplus \bigoplus_{i \neq j} \langle E_{i,j} \rangle.$$

So $\mathrm{R}(\mathrm{SL}_{n+1}, T) = \{\chi_i - \chi_j : i \neq j\}$. We think of $\mathrm{R}(\mathrm{SL}_{n+1})$ as a subset of the real vector space $\{\sum a_i \chi_i : a_i \in \mathbf{R} \text{ and } \sum a_i = 0\}$. ▷

With this example in mind, we move towards the general definition of a root system. Fix a finite-dimensional $\mathbf{R}$-vector space V. For $\alpha \in V \smallsetminus 0$, a *reflection* on V with vector α is a linear map $s : V \to V$ such $s(\alpha) = -\alpha$, and for which there exists a decomposition $V = \mathbf{R}\alpha \oplus U$ such that $\alpha|_U = 1$. Note that if s is a reflection with vector α, then $s(v) - v \in \mathbf{R}\alpha$ for all $v \in V$.

Lemma 4.5.2. *Let V be a finite-dimensional $\mathbf{R}$-vector space, $R \subset V$ a finite set which spans V, and $\alpha \in V \smallsetminus 0$. There exists at most one reflection s of V with vector α such that $s(R) = R$.*

Proof. This is [$\text{Lie}_{4\text{–}6}$, VI §1.1 lem.1]. Suppose s, s' are two such reflections. Define $u = s(s')^{-1}$. Note that $u(\alpha) = \alpha$. Moreover, u induces the identity on V/α. This implies u is unipotent. But $u(R) = R$, so $u^n = 1$ for some $n \geqslant 1$. This means that u is semisimple. The only way an operator can be both unipotent and semisimple is for $u = 1$. □

Definition 4.5.3. *Let V be a finite-dimensional $\mathbf{R}$-vector space. A subset $R \subset V \smallsetminus 0$ is a* root system *in V if the following hold:*

1. *R is finite and spans V.*

2. *For each $\alpha \in R$, there is a (unique) reflection s_α with vector α such that $s_\alpha(R) = R$.*

3. *For each $\alpha, \beta \in R$, $s_\alpha(\beta) - \beta \in \mathbf{Z}\alpha$.*

Often, we will speak of "a root system R," and tacitly assume that the vector space V has been given. One calls the elements of R *roots* of R.

Let $R \subset V$ be an arbitrary root system. For any root $\alpha \in R$, the reflection s_α acts on α by -1, that is, $s_\alpha(\alpha) = -\alpha$. Thus $\alpha \in R \Rightarrow -\alpha \in R$.

Definition 4.5.4. *A root system R is* reduced *if whenever $c\alpha \in R$ for some $c \in \mathbf{R}$, $\alpha \in R$, then $c = \pm 1$.*

Definition 4.5.5. *Let R be a root system. The* Weyl group *of R is the subgroup $W = \mathrm{W}(R)$ of $\mathrm{GL}(V)$ generated by $\{s_\alpha : \alpha \in R\}$.*

Since each s_α preserves R, the group W preserves R. Moreover, since R spans V, an element $w \in W$ is determined by its restriction $w|_R \in \mathrm{Perm}(R)$. Thus $W \hookrightarrow \mathrm{Perm}(R)$, so W is finite with cardinality $\leqslant (\#R)!$.

For an arbitrary root system $R \subset V$, there always exists a nondegenerate inner product $\langle \cdot, \cdot \rangle : V \times V \to \mathbf{R}$ that is W-invariant in the sense that $\langle wu, wv \rangle = \langle u, v \rangle$ for all $w \in W$. Existence of such an inner product follows from the "unitary trick." If G is an arbitrary compact group acting continuously on a Hilbert space V, define a new inner product by

$$\langle u, v \rangle_G = \int_G \langle gu, gv \rangle \, \mathrm{d}g.$$

Then $\langle \cdot, \cdot \rangle_G$ is G-invariant.

Fix a W-invariant inner product $\langle \cdot, \cdot \rangle$ on V. For $\alpha \in R$, we can write $V = \mathbf{R}\alpha \oplus (\mathbf{R}\alpha)^\perp$. One has

$$s_\alpha(v) = v - 2\frac{\langle v, \alpha \rangle}{\langle \alpha, \alpha \rangle}\alpha.$$

Condition 3 in the definition of a root system comes down to requiring that $2\frac{\langle \beta, \alpha \rangle}{\langle \alpha, \alpha \rangle} \in \mathbf{Z}$ for all $\alpha, \beta \in R$. For the remainder, put $n(\beta, \alpha) = 2\frac{\langle \beta, \alpha \rangle}{\langle \alpha, \alpha \rangle}$.

Example 4.5.6. Let $V = \mathbf{R}$, and $R = \{\pm\alpha\}$ for some $\alpha \neq 0$. This is the unique one-dimensional reduced root system, up to isomorphism. ▷

Definition 4.5.7. *Let $R_1 \subset V_1$, $R_2 \subset V_2$ be root systems. The* direct sum *of R_1 and R_2 has vector space $V_1 \oplus V_2$, with root system $\{R_1 \times 0\} \sqcup \{0 \times R_2\}$.*

We call a root system *reducible* if it can be written as the direct sum of two nonzero root systems, and *irreducible* otherwise. From [$\mathrm{Lie}_{4\text{–}6}$, VI §1.2 prop.5], we see that a root system $R \subset V$ is reducible if and only if V is reducible as a W-module. Moreover, the decomposition of a root system into irreducibles is determined by the decomposition of V into irreducible W-modules.

Definition 4.5.8. *A subset $S \subset R$ is a* base *if*

1. *S is a basis of V*
2. *For any $\beta \in R$, write $\beta = \sum_{\alpha\in S} m_\alpha \alpha$. Then either all $m_\alpha \geqslant 0$ or all $m_\alpha \leqslant 0$.*

Let $S \subset R$ be a base; one calls the $\alpha \in S$ *simple roots*. Let $R^+ \subset R$ be the collection of $\beta \in R$ such that in the decomposition $\beta = \sum_{\alpha\in S} m_\alpha \alpha$, one has all $m_\alpha \geqslant 0$. If we put $R^- = -R^+$, then by [Lie$_{4-6}$, VI §1.6 th.3], one has $R = R^+ \sqcup R^-$.

Theorem 4.5.9. *Let R be a root system.*

1. *A base for R exists.*
2. *If $S_1, S_2 \subset R$ are bases, then there exists $w \in W$ such that $w(S_1) = S_2$.*
3. *$R = \bigcup_{w\in W} w(S)$.*
4. *W is generated by $\{s_\alpha : \alpha \in S\}$.*

Proof. These all follow from various results in [Lie$_{4-6}$, VI §1.5]. Namely, 1 and 4 follow from parts (ii) and (vii) of Theorem 2. The claim 3 follows from Proposition 15, and 2 follows from the corollary to that proposition. □

Let $R \subset V$ be a reduced root system, $W = \mathrm{W}(R)$, and $\langle\cdot,\cdot\rangle$ a W-invariant inner product on V. Fix $\alpha, \beta \in R$ that are linearly independent. Let ϕ be the angle between α and β, determined by $\langle\alpha,\beta\rangle = |\alpha|\cdot|\beta|\cos\phi$. We have $n(\beta,\alpha) = 2\frac{|\beta|}{|\alpha|}\cos\phi \in \mathbf{Z}$. Moreover, $n(\alpha,\beta)n(\beta,\alpha) = 4\cos^2\phi \in \{0,1,2,3,4\}$, so the possibilities for ϕ are very limited. In fact, we can write them all down:

$n(\alpha,\beta)$	$n(\beta,\alpha)$	ϕ	$\lvert\beta\rvert/\lvert\alpha\rvert$
0	0	$\pi/2$	?
1	1	$\pi/3$	1
-1	-1	$2\pi/3$	1
1	2	$\pi/4$	$\sqrt{2}$
-1	-2	$3\pi/4$	$\sqrt{2}$
1	3	$\pi/6$	$\sqrt{3}$
-1	-3	$5\pi/6$	$\sqrt{3}$

Even with this finite list, classifying reduced root systems directly is tricky. We will classify them via a type of graph (with extra data) called a *Dynkin diagram*. The following definition is from [Lie$_{4-6}$, VI §4.2].

Definition 4.5.10. *A* Dynkin graph *is a pair (Γ, f), where Γ is an undirected graph and*

$$f : \{(\gamma_1,\gamma_2) \in \Gamma\times\Gamma : \gamma_1 \text{ and } \gamma_2 \text{ are connected by an edge}\} \to \mathbf{R}$$

satisfies $f(\gamma_1,\gamma_2)f(\gamma_2,\gamma_1) = 1$ whenever the expression is defined.

If $R \subset V$ is a reduced root system, we define a Dynkin graph $(Df), = \operatorname{Dyn}(R)$ as follows. Choose a base S of R. The vertices of D are elements of S. Given $\alpha \neq \beta \in S$, put $f(\alpha,\beta) = \frac{n(\alpha,\beta)}{n(\beta,\alpha)}$. For any two vertices $\alpha, \beta \in R$, after possibly switching α and β, we will have $f(\alpha,\beta) \in \mathbf{Z}$. In $\operatorname{Dyn}(R)$, there are $|f(\alpha,\beta)$ edges between α and β. From the above table, we see that there are at most 3 edges.

By [Lie$_{4\text{–}6}$, VI §4.2], the Dynkin diagram $\operatorname{Dyn}(R)$ only depends on R, in the sense that the choice of another basis yields a Dynkin graph that is canonically isomorphic to the first one. Moreover, $\operatorname{Dyn}(-)$ induces an injection from the set of isomorphism classes of reduced root systems to the set of isomorphism classes of Dynkin graphs. Moreover, R is irreducible if and only if $\operatorname{Dyn}(R)$ is connected, the decomposition of R into irreducibles matches the decomposition of $\operatorname{Dyn}(R)$ into connected components, and $\operatorname{Aut}(R)/\operatorname{W}(R) \xrightarrow{\sim} \operatorname{Aut}(\operatorname{Dyn} R)$.

4.6 Classification of root systems

We begin with what will turn out to be a complete list of examples of reduced root systems, following [Lie$_{4\text{–}6}$, VI §4]. For some of the more complicated root systems (e.g. E_8) we only give the associated Dynkin diagram. When drawing Dynkin diagrams, if $f(i,j) > 1$, we place an inequality sign $>$ over the arrows from i to j. For example, if $f(i,j) = 2$, we put $i \Rightarrow j$.

Example 4.6.1 (type A_n, $n \geqslant 1$)**.** Let $n \geqslant 1$. Let $V = \{x \in \mathbf{R}^{n+1} : \sum x_i = 0\}$, and give $\mathbf{R}^{n+1}$ the standard basis $e_1, \dots, e_{n+1}$ and standard inner product $\langle \cdot, \cdot \rangle$. The root system $\mathrm{A}_n \subset V$ is

$$\mathrm{A}_n = \{e_i - e_j : i \neq j\}.$$

Clearly A_n is finite and spans V. For each root α, put

$$s_\alpha(v) = v - 2\frac{\langle v, \alpha\rangle}{\langle \alpha, \alpha\rangle}\alpha = v - \langle v, \alpha\rangle \alpha.$$

If $i < j$, then it is easy to check that

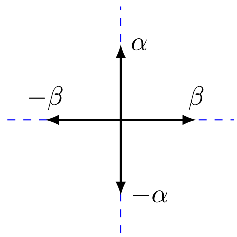
$$s_{e_i - e_j}(a_1, \dots, a_{n+1}) = (a_1, \dots, a_j, \dots, a_i, \dots, a_{n+1}) \qquad (a_i \text{ and } a_j \text{ swapped})$$

For all $\alpha, \beta \in \mathrm{A}_n$, one has $s_\alpha(\beta) - \beta = -\langle \beta, \alpha\rangle \alpha$, and $\langle \beta, \alpha \rangle \in \{0, \pm 1, \pm 2\}$, so A_n is indeed a root system. It is clearly reduced. The group $\operatorname{W}(\mathrm{A}_n)$ is generated by all linear transformations of the form "swap ith and jth coordinates." Thus we can identify $\operatorname{W}(\mathrm{A}_n)$ with the set of permutation matrices in $\operatorname{GL}(V)$. Note that the standard inner product $\langle \cdot, \cdot \rangle$ on V is W-invariant. The Dynkin diagram of A_n is

$$\bullet \;\text{———}\; \bullet \;\text{———}\; \cdots \;\text{———}\; \bullet \;\text{———}\; \bullet \qquad (n \text{ vertices}).$$

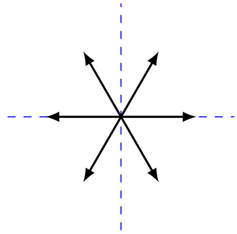
$\triangleright$

Example 4.6.2 (type $\mathrm{A}_1 \times \mathrm{A}_1$)**.** This root system lives inside $V = \mathbf{R}^2$ and $R = \{\pm(\alpha, 0), \pm(0, \beta)\}$. We draw it as:



The Dynkin diagram of $\mathrm{A}_1 \times \mathrm{A}_1$ is a disjoint union of two points. ▷

Example 4.6.3 (type A_2)**.** This root system can be drawn as living in $\mathbf{R}^2$ with the standard metric. It looks like:



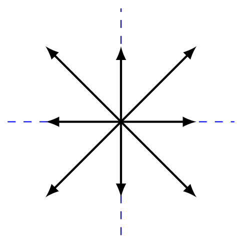
The roots lie on the unit circle and at multiples of the angle $\pi/3$. The Dynkin diagram is $\bullet \longrightarrow\!\!\!\!\!- \bullet$. ▷

Example 4.6.4 (type B_n, $n \geqslant 2$)**.** Let $V = \mathbf{R}^n$ and the roots be $\{\pm e_i\} \cup \{\pm e_i \pm e_j : i < j\}$. The Dynkin diagram of B_n is

$$\bullet \;\text{——}\; \bullet \;\text{——}\; \cdots \;\text{——}\; \bullet \;\text{——}\; \bullet \Longrightarrow \bullet \qquad (n \text{ vertices}).$$

▷

Example 4.6.5 (type B_2)**.** This root system lives in $\mathbf{R}^2$, and looks like



The Dynkin diagram $\mathrm{Dyn}(\mathrm{B}_2)$ is $\bullet \Longrightarrow \bullet$. ▷

Example 4.6.6 (type C_n, $n \geqslant 2$)**.** The ambient vector space is $V = \mathbf{R}^n$, and the set of roots is $\{\pm 2e_i\} \cup \{\pm e_i \pm e_j : i < j\}$. The Dynkin diagram is

$$\bullet \;\text{——}\; \bullet \;\text{——}\; \cdots \;\text{——}\; \bullet \;\text{——}\; \bullet \Longleftarrow \bullet \qquad (n \text{ vertices}).$$

▷

Example 4.6.7 (type D_n, $n \geqslant 4$)**.** The ambient vector space is $V = \mathbf{R}^n$, and the set of roots is $\{e_i\} \cup \{\pm e_i \pm e_j : i < j\}$. The Dynkin diagram is

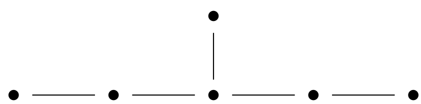
(n vertices).

▷

Example 4.6.8 (type E_6)**.** The space V is the subspace of $\mathbf{R}^8$ consisting of vectors x such that $x_6 = x_7 = -x_8$. The roots are $\{\pm e_i \pm e_j : i < j \leqslant 5\}$, together with all

$$\pm\frac{1}{2}\left(e_8 - e_7 - e_6 + \sum_{i=1}^{5}(-1)^{\nu(i)} e_i\right),$$

where $\sum \nu(i)$ is even. The Dynkin diagram is

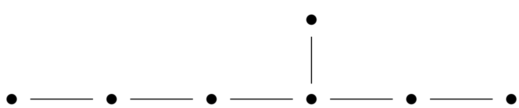


▷

Example 4.6.9 (type E_7)**.** Here V is the hyperplane in $\mathbf{R}^8$ orthogonal to $e_7 + e_8$. The set of roots is $\{\pm e_i \pm e_j : i < j \leqslant 6\} \cup \{\pm(e_7 - e_8)\}$, together with all

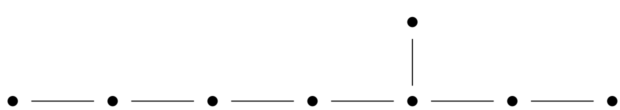
$$\pm\frac{1}{2}\left(e_7 - e_8 + \sum_{i=1}^{6}(-1)^{\nu(i)} e_i\right),$$

where $\sum \nu(i)$ is odd. The Dynkin diagram is



▷

Example 4.6.10 (type E_8)**.** The vector space is $\mathbf{R}^8$, and the set of roots consists of $\{\pm e_i \pm e_j : i < j\}$, together with all $\frac{1}{2}\sum_{i=1}^{8}(-1)^{\nu(i)} e_i$ for which $\sum \nu(i)$ is even. The Dynkin diagram is



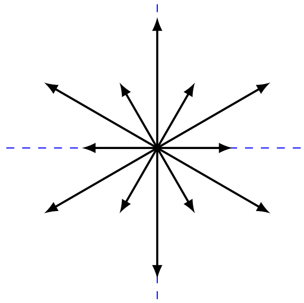
▷

Example 4.6.11 (type F_4)**.** The space is $\mathbf{R}^4$, the set of roots is $\{\pm e_i\} \cup \{\pm e_i \pm e_j : e < i\}$, together with $\frac{1}{2}(\pm e_1 \pm e_2 \pm e_3 \pm e_4)$. The Dynkin diagram is

$$\bullet \longrightarrow \bullet \Longrightarrow \bullet \longrightarrow \bullet$$

$\triangleright$

Example 4.6.12 (type G_2)**.** This is one of the exceptional root systems. It lives inside $\mathbf{R}^2$ and looks like:



The inner collection of roots is a copy of A_2. The outer collection has radius $\sqrt{3}$, and is rotated by $\pi/6$. The Dynkin diagram of G_2 is $\bullet \Rrightarrow \bullet$. $\triangleright$

It is possible to classify the Dynkin diagrams of irreducible reduced root systems.

Theorem 4.6.13. *Let R be an irreducible reduced root system, $D = \mathrm{Dyn}(R)$. Then D is a unique one of:*

- A_n *($n \geqslant 1$)*
- B_n *($n \geqslant 2$)*
- C_n *($n \geqslant 3$)*
- D_n *($n \geqslant 4$)*
- E_6*,* E_7*,* E_8
- F_4
- G_2

Proof. This is [$\mathrm{Lie}_{4\text{–}6}$, VI §4.2 th.3]. $\square$

From the examples in [Mil14, Ch.23], we see that we can obtain all the infinite families of root systems from algebraic groups:

group	root system
$\mathrm{SL}(n+1)$	A_n
$\mathrm{SO}(2n+1)$	B_n
$\mathrm{Sp}(2n)$	C_n
$\mathrm{SO}(2n)$	D_n

Automorphisms of a reductive group will be classified by automorphisms of the corresponding root system. So we will make use of the following table:

root system	outer automorphisms
A_1	1
A_n $(n \geqslant 2)$	$\mathbf{Z}/2$
B_n	1
C_n	1
D_4	S_3
D_n $(n \geqslant 5)$	$\mathbf{Z}/2$
E_6	$\mathbf{Z}/2$
E_7, E_8, F_4, G_2	1

4.7 Orthogonal and symplectic groups

In Example 4.5.1, we showed that the root system of $\mathrm{SL}(n+1)$ has type A_n. Here, we work out the root systems of $\mathrm{Sp}(2n)$ and $\mathrm{SO}(2n)$. Our computations will work over any field k of characteristic zero, so we will tacitly exclude k from the notation.

Example 4.7.1 (Orthogonal)**.** Write 1_n for the identity $n \times n$ matrix, and let $J = \begin{pmatrix} & 1_n \\ 1_n & \end{pmatrix}$. We define

$$\begin{aligned} \mathrm{O}(2n) &= \{g \in \mathrm{GL}(2n) : {}^{\mathrm{t}}gJg = J\} \\ \mathrm{SO}(2n) &= \mathrm{O}(2n) \cap \mathrm{SL}(2n). \end{aligned}$$

This is not the same as our definition in Example 1.4.3, in which we used the pairing $\langle x, y\rangle = \sum x_i y_i$. The problem is, the definition in that example does not give a split group, i.e. there is no split maximal torus. The basis

$$\left\{ \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}}\right), \left(\frac{1}{\sqrt{-2}}, -\frac{1}{\sqrt{-2}}\right) \right\}$$

realizes an isomorphism between $\mathrm{SO}(2n)$ and $\{g \in \mathrm{SL}(2n) : {}^{\mathrm{t}}g \cdot g = 1\}$, but only after base change to the field $\mathbf{Q}(\sqrt{2}, \sqrt{-2})$.

It is easy to verify that

$$\mathfrak{so}_{2n} = \left\{ \begin{pmatrix} a & b \\ c & -{}^{\mathrm{t}}a \end{pmatrix} : a, b, c \in \mathrm{M}_n \text{ and } {}^{\mathrm{t}}b = -b, {}^{\mathrm{t}}c = -c \right\}.$$

For a tuple $\lambda = (\lambda_1, \dots, \lambda_n) \in \mathbf{G}_{\mathrm{m}}^n$, write

$$\mathrm{diag}^*(\lambda) = \mathrm{diag}(\lambda_1, \dots, \lambda_n, \lambda_1^{-1}, \dots, \lambda_n^{-1}).$$

Let $T = \{\mathrm{diag}^* \lambda : \lambda \in \mathbf{G}_{\mathrm{m}}^n\}$; since $\mathrm{Z}_{\mathrm{SO}(2n)}(T) = T$, this is a maximal torus. Clearly $\mathrm{X}^*(T) = \bigoplus \mathbf{Z}\chi_i$, where each character χ_i is defined by $\chi_i(\mathrm{diag}^*(\lambda)) = \lambda_i$.

Let $\mathfrak{t} = \mathrm{Lie}(T)$. For any i, j, let $e_{i,j}$ be the matrix with a 1 in the (i, j) entry and 0 elsewhere. For $t \in T$ and $x \in \mathfrak{so}_{2n}$, we compute:

$$\mathrm{ad}(t)(x) = \begin{cases} x & \text{if } x \in \mathfrak{t} \\ (\chi_i - \chi_j)(t) \cdot x & \text{if } x = \begin{pmatrix} e_{ii} & \\ & -e_{ii} \end{pmatrix} \text{ and } i \neq j \\ (\chi_i + \chi_j)(t) \cdot x & \text{if } x = \begin{pmatrix} & e_{ij} - e_{ji} \\ & \end{pmatrix} \text{ and } i < j \\ (-\chi_i - \chi_j)(t) \cdot x & \text{if } x = \begin{pmatrix} & \\ e_{ij} - e_{ji} & \end{pmatrix} \text{ and } i < j \end{cases}$$

Thus the set of roots is $\{\pm\chi_i \pm \chi_j : i \neq j\} \subset \mathrm{X}^*(T)_{\mathbf{R}}$. This recovers the root system $\mathrm{D}_n = \{\pm e_i \pm e_j : i \neq j\} \subset \mathbf{R}^n$ of Example 4.6.7. A basis of D_n is $\{e_1 - e_2, \ldots, e_{n-2} - e_{n-1}, e_{n-1} - e_n, e_{n-1} + e_n\}$. ▷

Example 4.7.2 (Symplectic)**.** This time, let $J = \begin{pmatrix} & 1 \\ -1 & \end{pmatrix}$. Recall the definitions:

$$\begin{aligned} \mathrm{GSp}(2n) &= \{g \in \mathrm{GL}(2n) : {}^{\mathrm{t}}gJg = J\} \\ \mathrm{Sp}(2n) &= \mathrm{GSp}(2n) \cap \mathrm{SL}(2n). \end{aligned}$$

One can check that

$$\begin{aligned} \mathfrak{sp}(2n) = \mathrm{Lie}(\mathrm{Sp}_{2n}) &= \{x \in \mathfrak{gl}(2n) : {}^{\mathrm{t}}xJ + J\,{}^{\mathrm{t}}x = 0\} \\ &= \left\{ \begin{pmatrix} a & b \\ c & -\,{}^{\mathrm{t}}a \end{pmatrix} : a, b, c \in \mathrm{M}_n \text{ and } {}^{\mathrm{t}}b = b \right\}. \end{aligned}$$

If we define diag^* as in Example 4.7.1, then the group $\mathrm{Sp}(2n)$ has a maximal torus $T = \{\mathrm{diag}^*(\lambda) : \lambda \in \mathbf{G}_{\mathrm{m}}^n\}$. The group $\mathrm{X}^*(T)$ has basis $\{\chi_1, \ldots, \chi_n\}$, where $\chi_i(\mathrm{diag}^*(\lambda)) = \lambda_i$. Put $\mathfrak{t} = \mathrm{Lie}(T)$. For $t \in T$, $x \in \mathfrak{sp}_{2n}$, we have

$$\mathrm{ad}(t)(x) = \begin{cases} x & \text{if } x \in \mathfrak{t} \\ (\chi_i - \chi_j)(t) \cdot x & \text{if } x = \begin{pmatrix} e_{ii} & \\ & -e_{ii} \end{pmatrix} \text{ and } i \neq j \\ (\chi_i + \chi_j)(t)\dot{x} & \text{if } x = \begin{pmatrix} & e_{ij} + e_{ji} \\ & \end{pmatrix} \text{ and } i \leqslant j \\ (-\chi_i - \chi_j)(t) \cdot x & \text{if } x = \begin{pmatrix} & \\ e_{ij} + e_{ji} & \end{pmatrix} \text{ and } i \leqslant j \end{cases}$$

It follows that the set of roots is

$$\{\pm\chi_i \pm \chi_j : i \neq j\} \cup \{\pm 2\chi_i\} \subset \mathrm{X}^*(T).$$

This recovers the root system $\mathrm{C}_n = \{\pm e_i \pm e_j : i \neq j\} \cup \{\pm 2e_i\} \subset \mathbf{R}^n$ of Example 4.6.6. A base for C_n is $\{e_1 - e_2, \ldots, e_{n-1} - e_n, 2e_n\}$. ▷

⋆ Both $\mathrm{SO}(2n)$ and $\mathrm{Sp}(2n)$ are special cases of a more general construction that starts with an arbitrary algebra with involution. We follow [Ber10, VIII.21]. Let k be an arbitrary field of characteristic not 2. An *algebra with involution* over k is a (possibly non-commutative) k-algebra R together with an anti-involution $\sigma : R \to R$. The main examples are $R = \mathrm{M}_{2n}(k)$ and $\sigma(x) = \theta\,{}^{\mathrm{t}}x\theta^{-1}$ for some invertible matrix θ, especially θ either $\begin{pmatrix} & 1_n \\ 1_n & \end{pmatrix}$ or $\begin{pmatrix} & 1_n \\ -1_n & \end{pmatrix}$.

Let (R, σ) be an algebra with involution. The group of *similitudes* of R is the functor $\mathrm{Sim}(R)$ from k-algebras to groups, defined by

$$\mathrm{Sim}(R,\sigma)(A) = \{r \in (R \otimes_k A)^\times : r\sigma(r) \in A^\times\}.$$

Similarly, the group of *isometries* of R is the functor

$$\mathrm{Iso}(R,\sigma)(A) = \{r \in (R \otimes_k A)^\times : r\sigma(r) = 1\}.$$

Substituting in $\mathrm{M}_n(k)$ with an orthogonal or symplectic involution recovers the special orthogonal and symplectic groups. ⋆

4.8 Classification of split semisimple groups

Let k be a field of characteristic zero. Recall that an algebraic group $G_{/k}$ is said to be *split* if there is a maximal torus $T \subset G$ which is split. We will use our classification of root systems to classify split semisimple groups over k.

Definition 4.8.1. *A homomorphism $f : G \to H$ of algebraic groups is an* isogeny *if*

1. *f is surjective, and*
2. $\ker(f)$ *is finite.*

In characteristic p, one has to be very careful, as a lot of nice properties of isogenies fail to hold. For example, in characteristic zero $\ker(f)$ is a finite normal subgroup of G, hence G acts on $\ker(f)$ by conjugation. If G is connected, this action must be trivial, so $\ker(f) \subset \mathrm{Z}(G)$. Thus, in characteristic zero, all isogenies are central.

Definition 4.8.2. *Two semisimple groups $G_{/k}$, $H_{/k}$ are* isogenous *if there is a semisimple group $J_{/k}$ with isogenies $J \twoheadrightarrow G$, $J \twoheadrightarrow H$.*

It is not obvious, but "being isogenous" is an equivalence relation.

Theorem 4.8.3. *Let k be an algebraically closed field of characteristic zero. Then $G \mapsto \mathrm{R}(G,T)$ induces a bijection between the set of isogeny classes of connected semisimple groups and isomorphism classes of reduced root systems.*

Proof. This follows from [Mil14, 23.14-15]. □

Unfortunately, we cannot substitute "isomorphism" for "isogeny" in the statement of this theorem.

Example 4.8.4. Work in characteristic zero, and let $\mathrm{PGL}(n) = \mathrm{GL}(n)/\mathrm{Z}(\mathrm{GL}(n))$. Then $\mathrm{PGL}(n)$ and $\mathrm{SL}(n)$ have the same root systems. Moreover, the sequence $1 \to \boldsymbol{\mu}_n \to \mathrm{SL}(n) \to \mathrm{PGL}(n) \to 1$ is exact. So $\mathrm{SL}(n)$ and $\mathrm{PGL}(n)$ are isogenous but one can check that they are not isomorphic. ▹

The way we have defined "isogenous" as a relation on semisimple groups, it is not obvious that the relation is transitive. It turns out that the isogeny class of G contains two distinguished groups denoted G^{ad} and G^{sc}. The first, $G^{\mathrm{ad}} = G/\mathrm{Z}(G)$ is obviously isogenous to G via the quotient map $G \twoheadrightarrow G^{\mathrm{ad}}$. By [Mil14, 21.38], there is also an initial isogeny $G^{\mathrm{sc}} \to G$. One calls G^{ad} the *adjoint form* of G, and G^{sc} the *simply connected form* of G. They (tautologically) fit into a sequence $G^{\mathrm{sc}} \twoheadrightarrow G \twoheadrightarrow G^{\mathrm{ad}}$ of isogenies. So we could have said that two semisimple groups G and H are isogenous if and only if $G^{\mathrm{sc}} \simeq H^{\mathrm{sc}}$.

If we want to classify connected semisimple groups up to isomorphism, we need a finer invariant than the root system, namely the *root datum*. We'll cover root data in more detail in subsection 5.1. For now, all we need is that a root datum can be given by a reduced root system $R \subset V$ together with a group $Q(R) \subset X \subset P(R)$. Recall that if $R \subset V$, we define

$$Q(R) = \mathbf{Z} \cdot R \subset V \qquad \text{(root lattice)}$$

$$P(R) = \left\{ x \in V : \frac{2\langle x, \alpha\rangle}{\langle \alpha, \alpha\rangle} \in \mathbf{Z} \text{ for all } \alpha \in R \right\} \qquad \text{(weight lattice).}$$

The letter P for "weight lattice" is possibly inspired by the French word *poid* for "weight."

Let G be a semisimple group, $T \subset G$ a maximal torus. Let $R = \mathrm{R}(G, T) \subset \mathrm{X}^*(T)$. The inclusion $R \subset \mathrm{X}^*(T)_{\mathbf{R}}$ is a root system. Put $X = \mathrm{X}^*(T)$; then $Q(R) \subset X \subset P(R)$. The quotient group $P(R)/Q(R)$ is finite, so there are only finitely many possibilities for X.

The group G is simply connected if and only if $X = P(R)$, and adjoint if and only if $X = Q(R)$. We already know that each isogeny class has a unique simply connected simply connected (resp. adjoint) group. Intermediate quotients $G^{\mathrm{sc}} \twoheadrightarrow G \twoheadrightarrow G^{\mathrm{ad}}$ will correspond to quotients of the group $\pi_1^{\mathrm{al}}(G^{\mathrm{ad}}) = P(R)/Q(R)$.

Example 4.8.5. Start with $\mathrm{Sp}(2n)$. Let T be as in Example 4.7.2. Recall that $\mathrm{X}^*(T)$ has basis $\{\chi_1, \ldots, \chi_n\}$, where $\chi_i(\mathrm{diag}^*(\lambda)) = \lambda_i$. We showed that the set of roots is

$$\{\pm\chi_i \pm \chi_j : i \neq j\} \cup \{\pm 2\chi_i\} \subset \mathrm{X}^*(T).$$

Now let $G = \mathrm{Sp}(2n)/\{\pm 1\}$; this contains a maximal torus $T/\{\pm 1\}$. Note that $\mathrm{X}^*(T/\pm 1) \hookrightarrow \mathrm{X}^*(T)$; the image consists of those $\alpha \in \mathrm{X}^*(T) : \alpha(-1) = 1\}$. This is $\mathbf{Z} \cdot R$, so $\mathrm{Sp}(2n)/\{\pm 1\} = \mathrm{Sp}(2n)^{\mathrm{ad}}$, as we already knew from $\mathrm{Z}(\mathrm{Sp}_{2n}) = \boldsymbol{\mu}_2$. It turns out that $\mathrm{Sp}(2n)$ is simply connected. ▹

The following table is a complete list of the possible isomorphism classes of almost simple algebraic groups over an algebraically closed field of characteristic zero. Recall that an algebraic group is *almost simple* if its only normal proper subgroups are finite.

R	P/Q	G^{sc}	G^{ad}	groups in between
A_n $(n \geqslant 1)$	$\mathbf{Z}/(n+1)$	SL_{n+1}	$\text{SL}_{n+1}/\boldsymbol{\mu}_{n+1}$	$\text{SL}_{n+1}/\boldsymbol{\mu}_d$, $d \mid n+1$
B_n $(n \geqslant 2)$	$\mathbf{Z}/2$	Spin_{2n+1}	SO_{2n+1}	
C_n $(n \geqslant 3)$	$\mathbf{Z}/2$	Sp_{2n}	$\text{Sp}_{2n}/\boldsymbol{\mu}_2$	
D_n (n odd)	$\mathbf{Z}/4$	Spin_{2n}	$\text{SO}_{2n}/\boldsymbol{\mu}_2$	SO_{2n}
D_n (n even)	$\mathbf{Z}/2 \times \mathbf{Z}/2$	Spin_{2n}	$\text{SO}_{2n}/\boldsymbol{\mu}_2$	SO_{2n}, HSpin_{2n}
G_2	1	G_2	G_2	
F_4	1	F_4	F_4	
E_6	$\mathbf{Z}/3$	$(\text{E}_6)^{\text{sc}}$	$(\text{E}_6)^{\text{ad}}$	
E_7	$\mathbf{Z}/2$	$(\text{E}_7)^{\text{sc}}$	$(\text{E}_7)^{\text{ad}}$	
E_8	1	E_8	E_8	

Let G be a simply connected semisimple group over k. Then $G \simeq \prod G_i$, where each G_i is simply connected and almost simple. Each of the G_i will be one of:

$$\text{SL}(n+1), \text{Spin}(n), \text{Sp}(2n), \text{G}_2, \text{F}_4, (\text{E}_6)^{\text{sc}}, (\text{E}_7)^{\text{sc}}, \text{E}_8.$$

Here, we call an algebraic group G *almost simple* if all closed normal subgroups N are either trivial (in the sense that $N = 1$ or $N = G$) or finite. Similarly, if G is an adjoint group, then $G \simeq \prod G_i$ in which each G_i is a simple adjoint group.

Example 4.8.6. The group $G = \text{SL}(2) \times \text{SL}(2)$ has an (obvious) decomposition into almost simple factors. We have $\text{Z}(G) = \boldsymbol{\mu}_2 \times \boldsymbol{\mu}_2$. So the quotients of G are:

$$G, G/(\boldsymbol{\mu}_2 \times 1), G/(1 \times \boldsymbol{\mu}_2), G/\Delta(\boldsymbol{\mu}_2), G/(\boldsymbol{\mu}_2 \times \boldsymbol{\mu}_2).$$

The group $\text{SL}(2) \times (\text{SL}(2)/\boldsymbol{\mu}_2)$ is neither adjoint nor simply connected. Here $\Delta(\boldsymbol{\mu}_2) = \{(x,x) : x \in \boldsymbol{\mu}_2\}$. The group $G/\Delta(\boldsymbol{\mu}_2)$ does not have a product factorization. It is (obviously) a quotient of $\text{SL}(2) \times \text{SL}(2)$, but is not directly isomorphic to any $H_1 \times H_2$ for positive-dimensional H_i. ▷

Example 4.8.7. Let A be a finite abelian group. We can write $A = \mathbf{Z}/d_1 \oplus \cdots \oplus \mathbf{Z}/d_n$. Then $G_A = \text{SL}(d_1) \times \cdots \times \text{SL}(d_n)$ has $\text{Z}(G_A) \simeq A$. So all finite abelian groups arise as centers of semisimple algebraic groups. ▷

5 Reductive groups

Let k be an algebraically closed field of characteristic zero. Let $G_{/k}$ be a reductive group, i.e. $\mathcal{R}_{\text{u}} G = 1$. A good example is $\text{GL}(n)$. We could like to determine G up to isomorphism via some combinatorial data. Let $T \subset G$ be a maximal torus. Better, let $G_{/k}$ be a split reductive group and k arbitrary of characteristic zero. Let $X = \text{X}^*(T)$. We have the adjoint representation $\text{ad} : G \to \text{GL}(\mathfrak{g})$. Just as before, we can write

$$\mathfrak{g} = \mathfrak{g}_0 \oplus \bigoplus_{\alpha \in R} \mathfrak{g}_\alpha,$$

where $\mathfrak{g}_\alpha = \{x \in \mathfrak{g} : tx = \alpha(t)x \text{ for all } t\}$ and $R = \{\alpha \in X \smallsetminus 0 : \mathfrak{g}_\alpha \neq 0\}$.

Note that $R \subset X_{\mathbf{R}}$ need not be a root system, since R may only span a proper subspace of $X_{\mathbf{R}}$. For example, if G is itself a torus, then $R = \varnothing$. However, $R \subset V \subset X_{\mathbf{R}}$, where $V = \mathbf{R} \cdot R$, is a root system, and it determines the semisimple group $G/\mathcal{R}G$ up to isogeny. The datum "$R \subset X$" is not in general enough to determine G.

Let $\mathrm{X}_*(T) = \hom(\mathbf{G}_{\mathrm{m}}, T)$. There is a perfect pairing (composition) $\mathrm{X}^*(T) \times \mathrm{X}_*(T) \to \mathbf{Z} = \hom(\mathbf{G}_{\mathrm{m}}, \mathbf{G}_{\mathrm{m}})$. Here $\langle \alpha, \beta \rangle$ is the integer n such that $\alpha \circ \beta$ is $(-)^n$. From G we'll construct a root datum, which will be an ordered quadruple $(\mathrm{X}^*(T), \mathrm{R}(G,T), \mathrm{X}_*(T), \check{\mathrm{R}}(G,T))$. Before doing this, we'll define root data in general.

5.1 Root data

The following definitions are from [SGA 3_{III}, XXI]. A *dual pair* is an ordered pair $(X, \check{X})$, where X and $\check{X}$ are finitely generated free abelian groups, together with a pairing $\langle \cdot, \cdot \rangle : X \times \check{X} \to \mathbf{Z}$ that induces an isomorphism $\check{X} \simeq X^\vee = \hom(X, \mathbf{Z})$. Let $(X, \check{X})$ be a dual pair, and suppose we have two elements $\alpha \in X$, $\check{\alpha} \in \check{X}$. Define the *reflections* s_α and $s_{\check{\alpha}}$ by

$$s_\alpha(x) = x - \langle x, \check{\alpha} \rangle \alpha$$
$$s_{\check{\alpha}}(x) = x - \langle \alpha, x \rangle \check{\alpha}.$$

Definition 5.1.1. *A* root datum *consists of an ordered quadruple $(X, R, \check{X}, \check{R})$, such that*

- *$(X, \check{X})$ is a dual pair.*
- *$R \subset X$ and $\check{R} \subset \check{X}$ are finite sets,*
- *There is a specified mapping $\alpha \mapsto \check{\alpha}$ from R to $\check{R}$.*

These data are required to satisfy the following conditions:

1. *For each $\alpha \in R$, $\langle \alpha, \check{\alpha} \rangle = 2$.*
2. *For each $\alpha \in R$, $s_\alpha(R) \subset R$ and $s_{\check{\alpha}}(\check{R}) \subset \check{R}$.*

It turns out that $\alpha \mapsto \check{\alpha}$ is a bijection, and that R and $\check{R}$ are closed under negation. If $\mathscr{R} = (X, R, \check{X}, \check{R})$ is a root datum, the *Weyl group* of $\mathscr{R}$ is the group $\mathrm{W}(\mathscr{R}) \subset \mathrm{GL}(X)$ generated by $\{s_\alpha : \alpha \in R\}$. By [SGA 3_{III}, XXI 1.2.8], the Weyl group of a root datum is finite.

Definition 5.1.2. *Let $\mathscr{R}_1 = (X_1, R_1, \check{X}_1, \check{R}_1)$ and $\mathscr{R}_2 = (X_2, R_2, \check{X}_2, \check{R}_2)$ be root data. A* morphism *$f : \mathscr{R}_1 \to \mathscr{R}_2$ consists of a linear map $f : X_1 \to X_2$ such that*

1. *f induces a bijection $R_1 \xrightarrow{\sim} R_2$,*
2. *The dual map $f^\vee : \check{X}_2 \to \check{X}_1$ induces a bijection $\check{R}_2 \xrightarrow{\sim} \check{R}_1$.*

Definition 5.1.3. *Let $\mathscr{R} = (X, R, \check{X}, \check{R})$ be a root datum. We say $\mathscr{R}$ is* reduced *if for any $\alpha \in R$, the only multiples of α in R are $\pm\alpha$.*

Just as with root systems, there is a notion of a base for root data. If $N \subset \mathbf{Q}$ and $S \subset X$, we write $N \cdot S$ for the subset of $X_{\mathbf{Q}}$ generated as a monoid by $\{ns : (n,s) \in N \times S\}$. We call a root $\alpha \in R$ *indivisible* if there does not exist any $\beta \in R$ for which $\alpha = n\beta$ for some $n > 1$, i.e. $\mathbf{Q}^+ \cdot \alpha \cap R = \{\alpha\}$.

Definition 5.1.4. *Let $\mathscr{R} = (X, R, \check{X}, \check{R})$ be a root system. A subset $\Delta \subset R$ is a* base *if it satisfies any of the following conditions (reproduced from [SGA 3_{III}, XXI 3.1.5]):*

1. *All $\alpha \in \Delta$ are indivisible, and $R \subset \mathbf{Q}^+ \cdot \Delta \cup \mathbf{Q}^- \cdot \Delta$.*
2. *The set Δ is linearly independent, and $R \subset \mathbf{N} \cdot \Delta \cup \mathbf{Z}^- \cdot \Delta$.*
3. *Each $\alpha \in R$ can be written uniquely as $\sum_{\beta \in R} m_\beta \beta$, where all $m_\beta \in \mathbf{Z}$ and have the same sign.*

If $\Delta \subset R$ is a base, write $R^+ = \mathbf{N} \cdot \Delta$ for the set of *positive roots* and $R^- = \mathbf{Z}^- \cdot \Delta$ for the set of *negative roots*. One has $R = R^+ \sqcup R^-$, and $R^- = -R^+$.

Write RtDt for the category of root data. There is a contravariant functor $\check{\cdot} : \mathsf{RtDt} \to \mathsf{RtDt}$ which sends a root datum $\mathscr{R} = (X, R, \check{X}, \check{R})$ to $\check{\mathscr{R}} = (\check{X}, \check{R}, X, R)$. This is clearly an anti-equivalence of categories. We will use this later to define the *dual* of a split reductive group. If $G_{/k}$ is a split reductive group, then $\check{G}$ will be a split reductive group scheme over $\mathbf{Z}$, whose root datum is $\mathscr{R}(G,T)^\vee$.

We'll write $\mathsf{RtDt}^{\mathrm{red}}$ for the category of reduced root data.

Example 5.1.5. Let $R \subset V$ be a root system. As in subsection 4.8, we have lattices $Q(R) \subset V(R) \subset V$. Choose a W-invariant inner product $\langle \cdot, \cdot \rangle$ on V. Given $Q \subset X \subset P$, we can define a root datum as follows:

$$\begin{aligned}
X &= X \\
R &= R \\
\check{X} &= \{v \in V : \langle \alpha, v \rangle \in \mathbf{Z} \text{ for all } \alpha \in R\} \\
\check{R} &= \left\{ \frac{2\alpha}{\langle \alpha, \alpha \rangle} : \alpha \in R \right\}.
\end{aligned}$$

It is easy to check that this satisfies the required properties. ▷

For a classification of "reduced simply connected root systems," see [SGA 3_{III}, XXI 7.4.6].

5.2 Classification of reductive groups

Let k be a field of characteristic zero, $G_{/k}$ a (connected) split reductive group. Let $T \subset G$ be a split maximal torus. The *rank* of G is the integer $r = \mathrm{rk}(G) = \dim(T)$. Let $\mathfrak{g} = \mathrm{Lie}(G)$. As we have seen many times before, we can decompose $\mathfrak{g}$ as a representation of T:

$$\mathfrak{g} = \mathfrak{t} \oplus \bigoplus_{\alpha \in R} \mathfrak{g}_\alpha,$$

where $\mathfrak{t} = \mathrm{Lie}(T)$, $R = \mathrm{R}(G, T)$ is the set of *roots* of G, and $\mathfrak{g}_\alpha$ is the α-typical component of $\mathfrak{g}$. Recall that the *Weyl group* of G is $\mathrm{W}(G, T) = \mathrm{N}_G(T)/\mathrm{C}_G(T)$. By [SGA 3_{II}, XII 2.1], the Weyl group is finite.

A good source for what follows is [Jan03, II.1]. Let $\alpha : T \to \mathbf{G}_\mathrm{m}$ be a root, and put $T_\alpha = (\ker \alpha)^\circ$; this is a closed $(r-1)$-dimensional subgroup of T. Let $G_\alpha = \mathrm{C}_G(T_\alpha)$; by Theorem 4.4.8, this is reductive. One has $\mathrm{Z}(G_\alpha)^\circ = T_\alpha$. From the embedding $G_\alpha \hookrightarrow G$, we get an embedding of Lie algebras $\mathrm{Lie}(G_\alpha) \hookrightarrow \mathfrak{g}$. By [SGA 3_{III}, IX 3.5], one has

$$\mathrm{Lie}(G_\alpha) = \mathfrak{t} \oplus \mathfrak{g}_\alpha \oplus \mathfrak{g}_{-\alpha}$$

and $\mathfrak{g}_\alpha, \mathfrak{g}_{-\alpha}$ are both one-dimensional. In classical Lie theory, we could define $U_\alpha = \exp(\mathfrak{g}_\alpha)$. Since the exponential map does not make sense in full generality, we need the following result. Recall that we interpret the Lie algebra of an algebraic group as a new algebraic group.

Theorem 5.2.1. *Let T act on G via conjugation. Then there is a unique T-equivariant closed immersion $u_\alpha : \mathfrak{g}_\alpha \hookrightarrow G$ which is also a group homomorphism.*

Proof. This is [SGA 3_{III}, XXII 1.1.i]. □

We let U_α be the image of u_α. Since $\mathfrak{g}_\alpha$ is one-dimensional, it is isomorphic to $\mathbf{G}_\mathrm{a}$ as a group scheme. So we will generally write $u_\alpha : \mathbf{G}_\mathrm{a} \xrightarrow{\sim} U_\alpha \subset G$. The fact that u_α is T-equivariant comes down to:

$$t u_\alpha(x) t^{-1} = u_\alpha(\alpha(t)x) \qquad t \in T, x \in \mathbf{G}_\mathrm{a}.$$

The group G_α is generated by T, $U_{\pm\alpha}$ by Lie algebra considerations. So the group G is generated by T and $\{U_\alpha : \alpha \in R\}$.

Example 5.2.2 (type A_n)**.** Inside $\mathrm{SL}(n+1)$, the maximal torus T consists of diagonal matrices $\mathrm{diag}(t) = \mathrm{diag}(t_1, \dots, t_{n+1})$ for which $t_1 \cdots t_{n+1} = 1$. The group $\mathrm{X}^*(T)$ is generated by the characters $\chi_i(\mathrm{diag}(t)) = t_i$. The roots are $\{\chi_i - \chi_j : i \neq j\}$. For such a root, one can verify that $G_\alpha = \mathrm{C}_G(T_\alpha)$ consists of matrices of the form (g_{ab}) for which $g_{ab} = \delta_{ab}$ unless $a = b = i$, $a = b = j$, or $(a, b) = (i, j)$. So $G_\alpha \simeq \mathrm{SL}(2)$. It follows that $U_\alpha = 1 + \mathbf{G}_\mathrm{a} e_{ij}$. Note that indeed, $\mathrm{SL}(n+1)$ is generated by $\{U_\alpha : \alpha \in R\}$ and T. ▷

Back to our general setup $T \subset G_\alpha \subset G$. We can consider the "small Weyl group" $\mathrm{W}(G_\alpha, T) \subset \mathrm{W}(G, T)$. Since $\mathrm{rk}(G_\alpha/\mathrm{Z}(G_\alpha)^\circ) = 1$, we have $\mathrm{W}(G_\alpha, T) = \mathbf{Z}/2$. Let s_α be the unique generator of $\mathrm{W}(G_\alpha, T)$. It is known that $W = \mathrm{W}(G, T)$ is generated by $\{s_\alpha : \alpha \in R\}$. The group W acts on $\mathrm{X}^*(T)$. Indeed, if $w \in W$, we have $w = \dot{n}$ for some $n \in \mathrm{N}_G(T)$. Define $(w \cdot \chi)(t) = \chi(\dot{n}^{-1} t \dot{n})$.

Recall that $\mathrm{X}_*(T) = \hom(\mathbf{G}_\mathrm{m}, T)$. There is a natural pairing $\mathrm{X}^*(T) \times \mathrm{X}_*(T) \to \mathbf{Z}$, for which $\langle \alpha, \beta \rangle$ is the unique n such that $\alpha\beta$ is $t \mapsto t^n$. That is, $\alpha(\beta(t)) = t^{\langle \alpha, \beta \rangle}$. This pairing induces an isomorphism $\mathrm{X}_*(T) \simeq \mathrm{X}^*(T)^\vee$.

Theorem 5.2.3. *Let $\alpha \in R$. Then there exists a unique $\check{\alpha} \in \mathrm{X}_*(T)$ such that $s_\alpha(x) = x - \langle x, \check{\alpha} \rangle \alpha$ for all $x \in \mathrm{X}^*(T)$. Moreover, $\langle \alpha, \check{\alpha} \rangle = 2$.*

Proof. This is [SGA 3_{III}, XXII 1.1.ii]. □

Equivalently, $s_\alpha(\alpha) = -\alpha$. We put $\check{\mathrm{R}}(G,T) = \{\check{\alpha} : \alpha \in R\}$. The quadruple

$$\mathscr{R}(G,T) = (\mathrm{X}^*(T), \mathrm{R}(G,T), \mathrm{X}_*(T), \check{\mathrm{R}}(G,T))$$

is the *root datum* of G; it will determine G up to isomorphism (not just isogeny).

In defining coroots, we could also have used the fact that $\mathrm{Z}(G_\alpha)^\circ = T_\alpha$, which implies $T/T_\alpha \hookrightarrow G_\alpha/T_\alpha$ is a maximal torus of dimension 1. So the group G_α/T_α is semisimple, and has one-dimensional maximal torus. Its Dynkin diagram has type A_1, so G_α/T_α is either SL(2) or PGL(2).

Definition 5.2.4. *Let k be a field, $G_{/k}$ a split reductive group. A* pinning *of G consists of the following data:*

1. *A maximal torus $T \subset G$.*
2. *An isomorphism $T \xrightarrow{\sim} \mathrm{D}(M)$ for some free abelian group M.*
3. *A base $\Delta \subset \mathrm{R}(G,T)$.*
4. *For each $\alpha \in \Delta$, a non-zero element $X_\alpha \in \mathfrak{g}_\alpha$.*

If G_1, G_2 are pinned reductive groups, a morphism $f : G_1 \to G_2$ is said to be *compatible with the pinnings* if $f(T_1) = f(T_2)$, f induces a bijection (written f_*) $R_1 \xrightarrow{\sim} R_2$, and such that

$$f(u_\alpha(X_{1,\alpha})) = u_{f_*\alpha}(X_{2,f_*\alpha}).$$

Let $\mathsf{RdGp}^{\mathrm{pinn}}_{/k}$ be the category of split reductive groups over k with pinnings. We can define a pinning of a root system $\mathscr{R} = (X, R, \check{X}, \check{R})$ to be the choice of a base $\Delta \subset R$. Let $\mathsf{RtDt}^{\mathrm{red,pinn}}$ be the category of pinned reduced root data. The following combines the "existence and uniqueness theorems" in the classification of reductive groups.

Theorem 5.2.5. *The operation $G \mapsto \mathscr{R}(G,T)$ induces an equivalence of categories*

$$\mathsf{RdGp}^{\mathrm{pinn}}_{/k} \xrightarrow{\sim} \mathsf{RtDt}^{\mathrm{red,pinn}}.$$

Proof. See [SGA 3_{III}, XXIII 4.1] for a proof that $\mathscr{R}$ is fully faithful, [SGA 3_{III}, XXV 2] for a proof of essential surjectivity. □

5.3 Chevalley-Demazure group schemes

In Theorem 5.2.5, we classified split reductive groups over an arbitrary field. It turns out that the classification works over an arbitrary (non-empty) base scheme. More precisely, let S be a scheme, $G_{/S}$ a smooth affine group scheme of finite type. We say G is *reductive* if each geometric fiber $G_{\bar{s}}$ is reductive. A *maximal torus* in G is a subgroup scheme $T \subset G$ of multiplicative type such that for all $s \in S$, the geometric fiber $T_{\bar{s}} \subset G_{\bar{s}}$ is a maximal torus. Suppose there exists an abelian group M with an embedding $\mathrm{D}(M)_{/S} \hookrightarrow G$ whose image is a maximal torus. Just as before, there is a decomposition $\mathfrak{g} = \mathfrak{t} \oplus \bigoplus \mathfrak{g}_\alpha$, except now $\mathfrak{g}$ (and the $\mathfrak{g}_\alpha$) is a locally free sheaf on S. We say that G is *split* if the following conditions hold:

1. Each $\mathfrak{g}_\alpha$ is a free $\mathscr{O}_S$-module.
2. Each root α (resp. each coroot $\check{\alpha}$) is constant, i.e. induced by an element of M (resp. $M^\vee$).

Given the obvious notion of "pinned reductive group over S," the classification result in Theorem 5.2.5 actually gives an equivalence of categories

$$\mathsf{RdGp}_{/S}^{\mathrm{pinn}} \xrightarrow{\sim} \mathsf{RtDt}^{\mathrm{red,pinn}}.$$

In particular, for each reduced root datum $\mathscr{R}$, there is a reductive group scheme $G_{\mathscr{R}/\mathbf{Z}}$ with root datum $\mathscr{R}$, such that for any scheme S, the unique (up to isomorphism) reductive group scheme with root datum $\mathscr{R}$ is the base-change $G_{\mathscr{R}/S} = (G_{\mathscr{R}/\mathbf{Z}})_S$. In particular, if k is a field, the unique split reductive k-group with root datum $\mathscr{R}$ is $G_{\mathscr{R}/k}$. One calls $G_{\mathscr{R}/\mathbf{Z}}$ the *Chevalley-Demazure group scheme of type $\mathscr{R}$*.

6 Special topics

6.1 Borel-Weil theorem[1]

Let k be a field of characteristic zero, $G_{/k}$ an algebraic group. We write $\mathsf{Mod}(G)$ for the category whose objects are (not necessarily finite-dimensional) vector spaces V together with $\rho : G \to \mathrm{GL}(V)$. Here, $\mathrm{GL}(V)$ is the fppf sheaf (not representable unless V is finite-dimensional) $S \mapsto \mathrm{GL}(V_{\mathscr{O}(S)})$. The action action of G on itself by multiplication induces an action of G on the (k-vector spaces) $\mathscr{O}(G)$, which is not finite-dimensional unless G is finite. By [Jan03, I 3.9], the category $\mathsf{Mod}(G)$ has enough injectives; this enables us to define derived functors in the usual way.

Let $H \subset G$ be an algebraic subgroup. There is an obvious functor $\mathrm{res}_H^G : \mathsf{Mod}(G) \to \mathsf{Mod}(H)$ which sends $(V, \rho : G \to \mathrm{GL}(V))$ to $(V, \rho|_H)$. It has a right adjoint, the *induction functor*, determined by

$$\hom_G(V, \mathrm{ind}_H^G U) = \hom_H(\mathrm{res}_H^G V, U).$$

We are especially interested in this when U is finite-dimensional, in which case we have

$$\mathrm{ind}_H^G U = \{f : G \to \mathbf{V}(U) : f(gh) = h^{-1} f(g) \text{ for all } g \in G\}.$$

Since the induction functor is a right adjoint, it is left-exact, so it makes sense to talk about its derived functors $\mathrm{R}^\bullet \mathrm{ind}_H^G$. It turns out that these can be computed as the sheaf cohomology of certain locally free sheaves on the quotient G/H. Let

[1]Balazs Elek

$\pi : G \twoheadrightarrow G/H$ be the quotient map; for a representation V of H, define an $\mathscr{O}_{G/H}$-module $\mathscr{L}(V)$ by
$$\mathscr{L}(V)(U) = (V \otimes \mathscr{O}(\pi^{-1}U))^G.$$

By [Jan03, I 5.9], the functor $\mathscr{L}(-)$ is exact, and sends finite-dimensional representations of H to coherent $\mathscr{O}_{G/H}$-modules. Moreover, by [Jan03, I 5.12] there is a canonical isomorphism

$$\mathrm{R}^\bullet \operatorname{ind}_H^G V = \mathrm{H}^\bullet(G/H, \mathscr{L}(V)). \tag{$*$}$$

In general, both the vector spaces in ($*$) will not be finite-dimensional. However, if G/H is proper, then finiteness theorems for proper pushforward [EGA 3_{I}, 3.2.1] tell us that $\mathrm{H}^\bullet(G/H, \mathscr{F})$ is finite-dimensional whenever $\mathscr{F}$ is coherent. So we can use $\mathrm{R}^i \operatorname{ind}_H^G$ to produce finite-dimensional representations of G from finite-dimensional representations of H.

Note: for the remainder of this section, "representation" means *finite-dimensional* representation, while "module" means possibly infinite-dimensional representation.

Let $G_{/k}$ be a split reductive group, $B \subset G$ a Borel subgroup and $T \subset B$ a maximal torus. Let $N = \mathcal{R}_{\mathrm{u}} B$; one has $B \simeq T \ltimes N$. In particular, we can extend $\chi \in \mathrm{X}^*(T)$ to a one-dimensional representation of B by putting $\chi(tn) = \chi(t)$ for $t \in T$, $n \in N$.

Theorem 6.1.1. *Every irreducible representation of G is a quotient of $\operatorname{ind}_B^G \chi$ for a unique $\chi \in \mathrm{X}^*(T)$.*

Proof. Let V be an irreducible representation of G. The group B acts on the projective variety $\mathbf{P}(V)$; by 4.1.5 there is a fixed point v, i.e. $\operatorname{res}_B^G V$ contains a one-dimensional subrepresentation. This corresponds to a B-equivariant map $\chi \hookrightarrow \operatorname{res}_B^G V$ for some $\chi \in \mathrm{X}^*(T)$. By the definition of induction functors, we get a nonzero map $\operatorname{ind}_B^G \chi \to V$. Since V is simple, it must be surjective. Uniqueness of χ is a bit trickier. $\square$

One calls χ the *highest weight* of V. A natural question is: for which χ is $\operatorname{ind}_B^G \chi$ irreducible? By [Jan03, II 2.3], $\operatorname{ind}_B^G \chi$ (if nonzero) contains a unique simple subrepresentation, which we denote by $L(\chi)$.

Recall that our choice of Borel $B \subset T$ induces a base $S \subset \mathrm{R}(G, T) \subset \mathrm{X}^*(T)$. We put an ordering on $\mathrm{X}^*(T)$ by saying that $\lambda \leqslant \mu$ if $\mu - \lambda \in \mathbf{N} \cdot S$. It is known that there exists $w_0 \in W = \mathrm{W}(G, T)$ such that $w_0(R^+) = R^-$. Finally, the set of *dominant weights* is:

$$\mathrm{X}^*(T)_+ = \{\chi \in \mathrm{X}^*(T) : \langle \chi, \check{\alpha} \rangle \geqslant 0 \text{ for all } \alpha \in R^+\}.$$

We can now classify irreducible representations of G.

Theorem 6.1.2. *Any irreducible representation of G is of the form $L(\chi)$ for a unique $\chi \in \mathrm{X}^*(T)_+$.*

Proof. This is [Jan03, II 2.7]. $\square$

The Borel-Weil theorem completely describes $\mathrm{R}^\bullet \operatorname{ind}_B^G(\chi)$ for dominant χ. First we need some definitions. If $w \in W$, the *length* of w, denoted $l(w)$, is the minimal n such that w can be written as a product $s_1 \cdots s_n$ of simple reflections. Let S be a set of simple roots, $\rho = \frac{1}{2}\sum_{\alpha \in R^+} \alpha$. The "dot action" of W on character is:

$$w \bullet \chi = w(\chi + \rho) - \rho.$$

Define

$$C = \{\chi \in \mathrm{X}^*(T) : \langle \chi + \rho, \check{\alpha}\rangle \text{ for all } \alpha \in R^+\}.$$

It turns out that all $\chi \in \mathrm{X}^*(T)$ are of the form $w \bullet \chi_1$ for some $\chi_1 \in C$. Thus the following theorem describes $\mathrm{R}^\bullet \operatorname{ind}_B^G \chi$ for all χ.

Theorem 6.1.3 (Borel-Weil)**.** *Let $\chi \in C$. If $c \notin \mathrm{X}^*(T)_+$, then* $\mathrm{R}^\bullet \operatorname{ind}_B^G(w \bullet \chi) = 0$ *for all $w \in W$. If $\chi \in \mathrm{X}^*(T)_+$, then for all $w \in W$,*

$$\mathrm{R}^i \operatorname{ind}_B^G(w \bullet \chi) = \begin{cases} L(\chi) & i = l(w) \\ 0 & \textit{otherwise} \end{cases}$$

Proof. This is [Jan03, II 5.5]. □

Putting $w = 1$, we see that $\operatorname{ind}_B^G(\chi) = L(\chi)$.

6.2 Tannakian categories

Throughout, k is an arbitrary field of characteristic zero. We will work over k, so all maps are tacitly assumed to be k-linear and all tensor product will be over k. Consider the following categories.

For $G_{/k}$ an algebraic group, the category $\mathsf{Rep}(G)$ has as objects pairs (V, ρ), where V is a finite-dimensional k-vector space and $\rho : G \to \mathrm{GL}(V)$ is a homomorphism of k-groups. A morphism $(V_1, \rho_1) \to (V_2, \rho_2)$ in $\mathsf{Rep}(G)$ is a k-linear map $f : V_1 \to V_2$ such that for all k-algebras A and $g \in G(A)$, one has $f\rho_1(g) = \rho_2(g)f$, i.e. the following diagram commutes:

$$\begin{tikzcd} V_1 \otimes A \arrow[r, "f"] \arrow[d, "\rho_1(g)"] & V_2 \otimes A \arrow[d, "\rho_2(g)"] \\ V_1 \otimes A \arrow[r, "f"] & V_2 \otimes A. \end{tikzcd}$$

Example 6.2.1 (Representations of a Hopf algebra)**.** Let H be a co-commutative Hopf algebra. The category $\mathsf{Rep}(H)$ has as objects H-modules that are finite-dimensional over k, and morphisms are k-linear maps. The algebra H acts on a tensor product $U \otimes V$ via its comultiplication $\Delta : H \to H \otimes H$. ▷

Example 6.2.2 (Representations of a Lie algebra)**.** Let $\mathfrak{g}$ be a Lie algebra over k. The category $\mathsf{Rep}(\mathfrak{g})$ has as objects $\mathfrak{g}$-representations that are finite-dimensional as a k-vector space. There is a canonical isomorphism $\mathsf{Rep}(\mathfrak{g}) = \mathsf{Rep}(\mathcal{U}\mathfrak{g})$, where $\mathcal{U}\mathfrak{g}$ is the universal enveloping algebra of $\mathfrak{g}$. ▷

Example 6.2.3 (Continuous representations of a compact Lie group)**.** Let K be a compact Lie group. The category $\mathsf{Rep}_{\mathbf{C}}(K)$ has as objects pairs (V, ρ), where V is a finite-dimensional complex vector space and $\rho : K \to \mathrm{GL}(V)$ is a continuous (hence smooth, by Cartan's theorem) homomorphism. Morphisms $(V_1, \rho_1) \to (V_2, \rho_2)$ are K-equivariant $\mathbf{C}$-linear maps $V_1 \to V_2$. ▷

Example 6.2.4 (Graded vector spaces)**.** Consider the category whose objects are finite-dimensional k-vector spaces V together with a direct sum decomposition $V = \bigoplus_{n\in\mathbf{Z}} V_n$. Morphisms $U \to V$ are k-linear maps $f : U \to V$ such that $f(U_n) \subset V_n$. ▷

Example 6.2.5 (Hodge structures)**.** Let V be a finite-dimensional $\mathbf{R}$-vector space. A *Hodge structure* on V is a direct sum decomposition $V_{\mathbf{C}} = \bigoplus V_{p,q}$ such that $\overline{V_{p,q}} = V_{q,p}$. If U, V are vector spaces with Hodge structures, a morphism $U \to V$ is a $\mathbf{R}$-linear map $f : U \to V$ such that $f(U_{p,q}) \subset V_{p,q}$. Write Hdg for the category of vector spaces with Hodge structure. ▷

Let $\mathsf{Vect}(k)$ be the category of finite-dimensional k-vector spaces. For $\mathcal{C}$ any of the categories above, there is a faithful functor $\omega : \mathcal{C} \to \mathsf{Vect}(k)$. In our examples, it is just the forgetful functor. The main theorem will be that for $\pi = \mathrm{Aut}(\omega)$, the functor ω induces an equivalence of categories $\mathcal{C} \xrightarrow{\sim} \mathsf{Rep}(\pi)$. We proceed to make sense of the undefined terms in this theorem.

Our definitions follow [DM82]. As before, k is an arbitrary field of characteristic zero.

Definition 6.2.6. *A* k-linear category *is an abelian category* $\mathcal{C}$ *such that each* V_1, V_2, *the group* $\hom(V_1, V_2)$ *has the structure of a* k*-vector space in such a way that the composition map* $\hom(V_2, V_3) \otimes \hom(V_1, V_2) \to \hom(V_1, V_3)$ *is* k*-linear. For us, a* rigid k-linear tensor category *is a* k*-linear category* $\mathcal{C}$ *together with the following data:*

1. *An exact faithful functor* $\omega : \mathcal{C} \to \mathsf{Vect}(k)$.
2. *A bi-additive functor* $\otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$.
3. *Natural isomorphisms* $\omega(V_1 \otimes V_2) \xrightarrow{\sim} \omega(V_1) \otimes \omega(V_2)$.
4. *Isomorphisms* $V_1 \otimes V_2 \xrightarrow{\sim} V_2 \otimes V_1$ *for all* $V_i \in \mathcal{C}$.
5. *Isomorphisms* $(V_1 \otimes V_2) \otimes V_3 \xrightarrow{\sim} V_1 \otimes (V_2 \otimes V_3)$

These data are required to satisfy the following conditions:

1. *There exists an object* $1 \in \mathcal{C}$ *such that* $\omega(1)$ *is one-dimensional and such that the natural map* $k \to \hom(1, 1)$ *is an isomorphism.*
2. *If* $\omega(V)$ *is one-dimensional, there exists* $V^{-1} \in \mathcal{C}$ *such that* $V \otimes V^{-1} \simeq 1$.
3. *Under* ω*, the isomorphisms 3 and 4 are the obvious ones.*

By [DM82, Pr. 1.20], this is equivalent to the standard (more abstract) definition. Note that all our examples are rigid k-linear tensor categories. One calls the functor ω a *fiber functor.*

Let $(\mathcal{C}, \otimes)$ be a rigid k-linear tensor category. In this setting, define a functor $\mathrm{Aut}(\omega)$ from k-algebras to groups by setting:

$$\begin{aligned}\mathrm{Aut}^{\otimes}(\omega)(A) &= \mathrm{Aut}^{\otimes}(\omega : \mathcal{C} \otimes A \to \mathsf{Rep}(A)) \\ &= \left\{ (g_V) \in \prod_{V \in \mathcal{C}} \mathrm{GL}(\omega(V) \otimes A) : \begin{array}{c} g_{V_1 \otimes V_2} = g_{V_1} \otimes g_{V_2}, \text{ and} \\ f g_{V_1} = g_{V_1} f \text{ for all } f, V_1, V_2 \end{array} \right\}.\end{aligned}$$

In other words, an element of $\mathrm{Aut}(\omega)(A)$ consists of a collection (g_V) of A-linear automorphisms $g_V : \omega(V) \otimes A \xrightarrow{\sim} \omega(V) \otimes A$, where V ranges over objects in $\mathcal{C}$. This collection must satisfy:

1. $g_1 = 1_{\omega(1)}$
2. $g_{V_1 \otimes V_2} = g_{V_1} \otimes g_{V_2}$ for all $V_1, V_2 \in \mathcal{C}$, and
3. whenever $f : V_1 \to V_2$ is a morphism in $\mathcal{C}$, the following diagram commutes:

$$\begin{tikzcd} \omega(V_1)_A \arrow[r, "f"] \arrow[d, "g_{V_1}"] & \omega(V_2)_A \arrow[d, "g_{V_2}"] \\ \omega(V_1)_A \arrow[r, "f"] & \omega(V_2)_A. \end{tikzcd}$$

Typically one only considers affine group schemes $G_{/k}$ that are *algebraic*, i.e. whose coordinate ring $\mathscr{O}(G)$ is a finitely generated k-algebra, or equivalently that admit a finite-dimensional faithful representation. Let $G_{/k}$ be an arbitrary affine group scheme, V an arbitrary representation of G over k. By [DM82, Cor. 2.4], one has $V = \varinjlim V_i$, where V_i ranges over the finite-dimensional subrepresentations of V. Applying this to the regular representation $G \to \mathrm{GL}(\mathscr{O}(G))$, we see that $\mathscr{O}(G) = \varinjlim \mathscr{O}(G_i)$, where G_i ranges over the algebraic quotients of G. That is, an arbitrary affine group scheme $G_{/k}$ can be written as a filtered projective limit $G = \varprojlim G_i$, where each G_i is an affine algebraic group over k. So we will speak of pro-algebraic groups instead of arbitrary affine group schemes.

If V is a finite-dimensional k-vector space and $G = \varprojlim G_i$ is a pro-algebraic k-group, representations $G \to \mathrm{GL}(V)$ factor through some algebraic quotient G_i. That is, $\hom(G, \mathrm{GL}(V)) = \varinjlim \hom(G_i, \mathrm{GL}(V))$. As a basic example of this, let Γ be a profinite group, i.e. a projective limit of finite groups. If we think of Γ as a pro-algebraic group, then algebraic representations $\Gamma \to \mathrm{GL}(V)$ are exactly those representations that are continuous when V is given the discrete topology.

First, suppose $\mathcal{C} = \mathsf{Rep}(G)$ for a pro-algebraic group G, and that $\omega : \mathsf{Rep}(G) \to \mathsf{Vect}(k)$ is the forgetful functor. Then the Tannakian fundamental group $\mathrm{Aut}^{\otimes}(\omega)$ carries no new information [DM82, Pr. 2.8]:

Theorem 6.2.7. *Let $G_{/k}$ be a pro-algebraic group, $\omega : \mathsf{Rep}(G) \to \mathsf{Vect}(k)$ the forgetful functor. Then $G \xrightarrow{\sim} \mathrm{Aut}^{\otimes}(G)$.*

The main theorem is the following, taken essentially verbatim from [DM82, Th. 2.11].

Theorem 6.2.8. *Let $(\mathcal{C}, \otimes, \omega)$ be a rigid k-linear tensor category. Then $\pi = \mathrm{Aut}^{\otimes}(\omega)$ is represented by a pro-algebraic group, and $\omega : \mathcal{C} \to \mathsf{Rep}(\pi)$ is an equivalence of categories.*

Often, the group $\pi_1(\mathcal{C})$ is "too large" to handle directly. For example, if $\mathcal{C}$ contains infinitely many simple objects, probably $\pi_1(\mathcal{C})$ will be infinite-dimensional. For $V \in \mathcal{C}$, let $\mathcal{C}(V)$ be the Tannakian subcategory of $\mathcal{C}$ generated by V. One puts $\pi_1(\mathcal{C}/V) = \pi_1(\mathcal{C}(V))$. It turns out that $\pi_1(\mathcal{C}/V) \subset \mathrm{GL}(\omega V)$, so $\pi_1(\mathcal{C}/V)$ is finite-dimensional. One has $\pi_1(\mathcal{C}) = \varprojlim \pi_1(\mathcal{C}/V)$.

Example 6.2.9 (Pro-algebraic groups)**.** If $G_{/k}$ is a pro-algebraic group, then Theorem 6.2.7 tells us that if $\omega : \mathsf{Rep}(G) \to \mathsf{Vect}(k)$ is the forgetful functor, then $G = \mathrm{Aut}^{\otimes}(G)$. That is, $G = \pi_1(\mathsf{Rep} G)$. ▷

Example 6.2.10 (Hopf algebras)**.** Suppose H is a co-commutative Hopf algebra over k. Then $\pi_1(\mathsf{Rep} H) = \mathrm{Spec}(H^\circ)$, where H° is the *reduced dual* defined in [Car07]. Namely, for any k-algebra A, A° is the set of k-linear maps $\lambda : A \to k$ such that $\lambda(\mathfrak{a}) = 0$ for some two-sided ideal $\mathfrak{a} \subset A$ of finite codimension. The key fact here is that $(A \otimes B)^\circ = A^\circ \otimes B^\circ$, so that we can use multiplication $m : H \otimes H \to H$ to define comultiplication $m^* : H^\circ \to (H \otimes H)^\circ = H^\circ \otimes H^\circ$. From [DG80, II §6 1.1], if G is a linear algebraic group over an algebraically closed field k of characteristic zero, we get an isomorphism $\mathscr{O}(G)^\circ = k[G(k)] \otimes \mathcal{U}(\mathfrak{g})$. Here $k[G(k)]$ is the usual group algebra of the abstract group $G(k)$, and $\mathcal{U}(\mathfrak{g})$ is the universal enveloping algebra of $\mathfrak{g} = \mathrm{Lie}(G)$, both with their standard Hopf structures. ▷

[Note: one often calls $\mathscr{O}(G)^\circ$ the "space of distributions on G." If instead G is a real Lie group, then one often writes $\mathscr{H}(G)$ for the space of distributions on G. Let $K \subset G$ be a maximal compact subgroup, $M(K)$ the space of finite measures on K. Then convolution $D \otimes \mu \mapsto D * \mu$ induces an isomorphism $\mathcal{U}(\mathfrak{g}) \otimes M(K) \xrightarrow{\sim} \mathscr{H}(G)$. In the algebraic setting, $k[G(k)]$ is the appropriate replacement for $M(K)$.]

Example 6.2.11 (Lie algebras)**.** Let $\mathfrak{g}$ be a semisimple Lie algebra over k. Then by [Mil07], $G = \pi_1(\mathsf{Rep}\mathfrak{g})$ is the unique connected, simply connected algebraic group with $\mathrm{Lie}(G) = \mathfrak{g}$. If $\mathfrak{g}$ is not semisimple, e.g. $\mathfrak{g} = k$, then things get a lot nastier. See the above example. ▷

Example 6.2.12 (Compact Lie groups)**.** By definition, the *complexification* of a real Lie group K is a complex Lie group $K_{\mathbf{C}}$ such that all morphisms $K \to \mathrm{GL}(V)$ factor uniquely through $K_{\mathbf{C}} \to \mathrm{GL}(V)$. It turns out that $K_{\mathbf{C}}$ is a complex algebraic group, and so $\pi_1(\mathsf{Rep} K) = K_{\mathbf{C}}$. ▷

Example 6.2.13 (Graded vector spaces)**.** To give a grading $V = \bigoplus_{n \in \mathbf{Z}} V_n$ on a vector space is equivalent to giving an action of the split rank-one torus $\mathbf{G}_{\mathrm{m}}$. On each V_n, $\mathbf{G}_{\mathrm{m}}$ acts via the character $g \mapsto g^n$. Thus $\pi_1(\text{graded vector spaces}) = \mathbf{G}_{\mathrm{m}}$. ▷

Example 6.2.14 (Hodge structures)**.** Let $\mathbf{S} = \mathrm{R}_{\mathbf{C}/\mathbf{R}}\, \mathbf{G}_{\mathrm{m}}$; this is defined by $\mathbf{S}(A) = (A \otimes \mathbf{C})^\times$ for $\mathbf{R}$-algebras A. One can check that the category Hdg of Hodge structures is equivalent to $\mathsf{Rep}_{\mathbf{R}}(\mathbf{S})$. Thus $\pi_1(\mathsf{Hdg}) = \mathbf{S}$. ▷

6.3 Automorphisms of semisimple Lie algebras[2]

Let k be a field of characteristic zero, $\mathfrak{g}$ a split semisimple Lie algebra over k. We want to describe the group $\mathrm{Aut}(\mathfrak{g})$. It turns out $\mathrm{Aut}(\mathfrak{g}) = \mathrm{Aut}(G^{\mathrm{sc}})$, where G^{sc} is the unique simply connected semisimple group with Lie algebra $\mathfrak{g}$. We can give $\mathrm{Aut}(\mathfrak{g})$ the structure of a linear algebraic group by putting

$$\mathrm{Aut}(\mathfrak{g})(A) = \mathrm{Aut}(\mathfrak{g}_A).$$

Clearly $\mathrm{Aut}(\mathfrak{g}) \subset \mathrm{GL}(\mathfrak{g})$. Let $\mathfrak{t} \subset \mathfrak{g}$ be a maximal abelian subalgebra. Let $R \subset \mathfrak{t}^\vee$ be the set of roots, $S \subset R$ a base of Δ. We can define some subgroups of $\mathrm{Aut}(\mathfrak{g})$:

$$\mathrm{Aut}(\mathfrak{g}, \mathfrak{t}) = \{\theta \in \mathrm{Aut}(\mathfrak{g}) : \theta(\mathfrak{t}) = \mathfrak{t}\}$$
$$\mathrm{Aut}(\mathfrak{g}, \mathfrak{t}, S) = \{\theta \in \mathrm{Aut}(\mathfrak{g}, \mathfrak{t}) : {}^{\mathrm{t}}\theta(S) = S\}.$$

Lemma 6.3.1. *If* $\theta \in \mathrm{Aut}(\mathfrak{g}, \mathfrak{t})$*, then* ${}^{\mathrm{t}}\theta(R) = R$*.*

Proof. The definition of R is invariant under automorphisms of $\mathfrak{t}$. □

Let $\mathrm{Aut}(R)$ be the set of automorphisms of the Dynkin diagram associated to R.

Lemma 6.3.2. *The natural map* $\varepsilon : \mathrm{Aut}(\mathfrak{g}, \mathfrak{t}, S) \to \mathrm{Aut}(R)$ *is surjective.*

Proof. Choose, for each $\alpha \in R$, a non-zero element $x_\alpha \in \mathfrak{g}_\alpha$. The existence theorem [Lie_{7-9}, VIII §4.4 th.2] tells us that to each automorphism φ of the Dynkin diagram of R, there exists a unique $\tilde{\varphi} \in \mathrm{Aut}(\mathfrak{g}, \mathfrak{t}, S, \{x_\alpha\})$ inducing φ. Thus $\varepsilon : \mathrm{Aut}(\mathfrak{t}, \mathfrak{t}, S) \to \mathrm{Aut}(R)$ splits. □

We want to describe the kernel of ε. Since $\mathfrak{g}$ is semisimple, the adjoint map $\mathfrak{g} \to \mathrm{Der}(\mathfrak{g}) = \mathrm{Lie}(\mathrm{Aut}\,\mathfrak{g})$ is an embedding, and thus $\mathfrak{t} \xrightarrow{\sim} \mathrm{ad}(\mathfrak{t})$. Let $T \subset \mathrm{Inn}(\mathfrak{g})$ be the subgroup with Lie algebra $\mathrm{ad}(\mathfrak{t})$.

Lemma 6.3.3. $\ker(\varepsilon) = T$*.*

Proof. Clearly $T \subset \ker(\varepsilon)$. Let $\theta \in \ker(\varepsilon)$. For any $\alpha \in R$, we have $\theta x_\alpha \in \mathfrak{g}_\beta$ for some β. For $t \in \mathfrak{t}$, we compute:

$$\begin{aligned}[t, \theta x_\alpha] &= [\theta t, \theta x_\alpha] \\ &= \theta[t, x_\alpha] \\ &= \alpha(t)\theta x_\alpha,\end{aligned}$$

so $\alpha = \beta$. Moreover, θ acts on $\mathfrak{g}$ exactly like an element of $\mathfrak{t}$, so $\theta \in T$. □

Lemma 6.3.4. $\mathrm{Aut}(\mathfrak{g}) = \mathrm{Aut}(\mathfrak{g}, \mathfrak{t}, S) \cdot \mathrm{Inn}(\mathfrak{g})$*.*

Proof. Use the well-known facts that all Cartan subalgebras of $\mathfrak{g}$ are conjugate, and that moreover the Weyl group acts transitively on sets of simple roots. □

We have arrived at the main result.

Theorem 6.3.5. $\mathrm{Aut}(\mathfrak{g}) = \mathrm{Inn}(\mathfrak{g}) \rtimes \mathrm{Aut}(R)$*. In particular,* $\mathrm{Out}(\mathfrak{g}) = \mathrm{Aut}(R)$*.*

This allows us to recover the table of automorphisms in subsection 4.6.

[2]Sasha Patotski

6.4 Exceptional isomorphisms[3]

Terence Tao's blog post at http://terrytao.wordpress.com/2011/03/11/ is an excellent reference for this section. From Theorem 4.8.3, we know that the set of isogeny classes of split semisimple algebraic groups is the same as the set of isomorphism classes of Dynkin diagrams. In Theorem 4.6.13, we classified the Dynkin diagrams. In this classification, we just included, e.g. D_n for $n \geqslant 4$. If we include all the D_n etc., the classification is no longer unique – we have to account for the "exceptional isomorphisms"

$$\begin{aligned}
&\mathrm{A}_1 \simeq \mathrm{B}_1 \simeq \mathrm{C}_1 \simeq \mathrm{D}_2 \simeq \mathrm{E}_1 \\
&\mathrm{B}_2 \simeq \mathrm{C}_2 \\
&\mathrm{D}_3 \simeq \mathrm{A}_3 \\
&\mathrm{D}_2 \simeq \mathrm{A}_1 \times \mathrm{A}_1.
\end{aligned}$$

The Dynkin diagram for D_2 and $\mathrm{A}_1 \times \mathrm{A}_1$ is disconnected – it is a disjoint union of two points. We'll explicitly construct the induced isogenies between algebraic groups of different types.

Example 6.4.1 ($\mathrm{A}_1 \simeq \mathrm{C}_1$)**.** Since $\mathrm{Sp}(2) = \mathrm{SL}(2)$, there is nothing to prove. ▷

Example 6.4.2 ($\mathrm{A}_1 \simeq \mathrm{B}_1$)**.** Define a pairing on $\mathfrak{sl}_2$ by $\langle x, y\rangle = \mathrm{tr}(xy)$ (the *Killing form*). One easily verifies that the adjoint action of $\mathrm{SL}(2)$ on $\mathfrak{sl}_2$ preserves this form. Moreover, a general theorem of linear algebra tells us that any non-degenerate bilinear symmetric pairing on a three-dimensional vector space is isomorphic to the orthogonal pairing. It follows that $\mathrm{Aut}(\mathfrak{sl}_2, \langle\cdot,\cdot\rangle) \simeq \mathrm{O}(3)$, at least over an algebraically closed field. Since $\mathrm{SL}(2)$ is connected, $\mathrm{ad}(\mathrm{SL}(2)) \supset \mathrm{SO}(3)$. A dimension count tells us that $\mathrm{SL}(2)/\boldsymbol{\mu}_2 \simeq \mathrm{SO}(3)$. Again, this only works over an algebraically closed field. ▷

Example 6.4.3 ($\mathrm{D}_2 \simeq \mathrm{A}_1 \times \mathrm{A}_1$)**.** We need to show that $\mathrm{SO}(4)$ and $\mathrm{SL}(2) \times \mathrm{SL}(2)$ are isogenous. Let $\mathrm{std} : \mathrm{SL}(2) \hookrightarrow \mathrm{GL}(2)$ be the standard representation, and consider the representation $\mathrm{std} \boxtimes \mathrm{std}$ of $\mathrm{SL}(2) \times \mathrm{SL}(2)$. There is an obvious bilinear form form:

$$\langle u_1 \otimes u_2, v_1 \otimes v_2\rangle = \omega(u_1, v_1)\omega(u_2, v_2),$$

where ω is the determinant pairing $k^2 \times k^2 \to \bigwedge^2 k^2 \simeq k$ given by $(x, y) \mapsto x \wedge y$. The group $\mathrm{SL}(2) \times \mathrm{SL}(2)$ acts on $\mathrm{std} \boxtimes \mathrm{std}$ by $(g, h)(v \otimes w) = (gv) \otimes (gw)$. Thus we have a representation $\mathrm{SL}(2) \times \mathrm{SL}(2) \to \mathrm{GL}(4)$. The image preserves $\langle\cdot,\cdot\rangle$, hence (by linear algebra) lies inside $\mathrm{O}(4)$, By connectedness and a dimension count, we see that this is an isogeny $\mathrm{SL}(2) \times \mathrm{SL}(2) \twoheadrightarrow \mathrm{SO}(4)$. ▷

6.5 Constructing some exceptional groups[4]

We roughly follow [SV00]. Let k be a field of characteristic not 2 or 3. Recall that if V is a k-vector space and $\langle\cdot,\cdot\rangle : V \times V \to k$ is a symmetric bilinear form, we can

[3] Theodore Hui
[4] Gautam Gopal

define a quadratic form $q : V \to k$ by $q(v) = \langle v, v\rangle$. This correspondence is bijective; we can go backwards via the familiar identity

$$\langle u, v\rangle = \frac{1}{2}(q(u+v) - q(u) - q(v)).$$

Definition 6.5.1. *A* composition algebra *is a pair (C, q), where C is a unital, not-necessarily associative k-algebra and q is a multiplicative non-degenerate quadratic on C.*

In other words, we require $q(xy) = q(x)q(y)$ for all $x, y \in C$. Since by [SV00, 1.2.4], q is determined by the multiplicative strucure of C, we will just refer to "a composition algebra C." Write e for the unit of C. Every composition algebra comes with a natural involution $x \mapsto \bar{x}$, defined by $\bar{x} = \langle x, e\rangle - x$.

Theorem 6.5.2. *Let C be a composition algebra. Then* $\dim(C) \in \{1, 2, 4, 8\}$.

Proof. This is [SV00, 1.6.2]. □

We call an 8-dimensional composition algebra an *octobian algebra*. If C is an octonian k-algebra, we define an algebraic group $\mathrm{Aut}(C)$ by putting

$$\mathrm{Aut}(C)(A) = \{g \in \mathrm{GL}(C \otimes A) : g \text{ is a morphism of normed } A\text{-algebras}\},$$

for all (commutative, unital) k-algebras A. There is an obvious embedding $\mathrm{Aut}(C) \hookrightarrow \mathrm{O}(C, q)$.

Theorem 6.5.3. *Let C be an octonian k-algebra. Then* $\mathrm{Aut}(C)$ *is a connected algebraic group of type* G_2.

Proof. We mean that after base-change to an algebraic closure of k, $\mathrm{Aut}(C)$ becomes isomorphic to G_2. This is [SV00, 2.3.5]. □

If C is a composition algebra and $\gamma = (\gamma_1, \gamma_2, \gamma_3) \in (k^\times)^3$, we define a new algebra $H_{C,\gamma}$ to be as a set the collection of matrices

$$\begin{pmatrix} z_1 & c_3 & \gamma_1^{-1}\gamma_3\bar{c}_2 \\ \gamma_2^{-1}\gamma_1\bar{c}_3 & z_2 & c_1 \\ c_2 & \gamma_3^{-1}\gamma_2\bar{c}_1 & z_3 \end{pmatrix} \qquad c_i \in k^\times \text{ and } z_i \in k.$$

Give $H_{C,\gamma}$ the product $xy = \frac{1}{2}(x \cdot y + y \cdot x)$ and quadratic form $q(x) = \frac{1}{2}\operatorname{tr}(x^2)$.

Definition 6.5.4. *An* Albert algebra *is a commutative, non-unital, associative k-algebra A such that $A \otimes \bar{k}$ is isomorphic to a $\bar{k}$-algebra of the form $H_{C,\gamma}$ for some octobian algebra C and $\gamma \in \bar{k}^\times$.*

If A is an Albert algebra, we can define an algebraic group $\mathrm{Aut}(A)$ just as above.

Theorem 6.5.5. *If A is an Albert algebra, then* $\mathrm{Aut}(A)$ *is a connected simple algebraic group of type* F_4.

Proof. Put $G = \mathrm{Aut}(A)$. Call an element $u \in A$ *idempotent* if $u2 = u$. It turns out that if u is idempotent, then either $u \in \{0, e\}$, or $q(u) \in \{1/2, 1\}$. Call the idempotents with $q(u) = 1/2$ *primitive*. Let $V \subset A$ be the set of primitive idempotents; this is naturally a variety over k. It turns out that V is 16-dimensional closed and irreducible and has a transitive G-action. For some $v \in V$, the group $G_v = \mathrm{Stab}_G(v)$ is the spin group of a nine-dimensional quadratic form, so $\dim(G_v) = 36$. It follows that $\dim(G) = 16 + 36 = 52$. Since G_v and V are irreducible, G is connected. From the action of G on $e^\perp \subset A$, we see that G is semisimple algebraic. The only 52-dimensional semisimple algebraic group over an algebraically closed field is F_4. For a more careful proof, see [SV00, 7.2.1]. □

It turns out that any group of type F_4 can be obtained as $\mathrm{Aut}(A)$ for some Albert algebra A. Consider the cubic form

$$\det(x) = z_1 z_2 z_3 - \gamma_3^{-1}\gamma_2 z_1 q(c_1) - \gamma_2^{-1}\gamma_3 z_2 q(c_2) - \gamma_2^{-1}\gamma_1 z_3 q(c_3) + \langle c_1 c_2, \bar{c}_3 \rangle.$$

Let $\mathrm{GL}(A, \det)$ be the subgroup of $\mathrm{GL}(A)$ consisting of those linear maps which preserve det.

Theorem 6.5.6. *Let A be an Albert algebra. Then* $\mathrm{GL}(A, \det)$ *is a connected simple algebraic group of type* E_6*.*

Proof. This is [SV00, 7.3.2]. □

Unlike the case with groups of type F_4, not all groups of type E_6 can be obtained this way.

6.6 Spin groups[5]

The motivation for spin groups is as follows. Recall that up to isogeny, the simple algebraic groups are $\mathrm{SL}(n)$, $\mathrm{Sp}(2n)$, $\mathrm{SO}(n)$, or one of the exceptional groups. Recall that each isogeny class has two distinguished elements, the simply connected and adjoint. For $\mathrm{SO}(n)$, we should expect there to be a simply connected group $\mathrm{Spin}(n) = (\mathrm{D}_n)^{\mathrm{sc}}$, which is a double cover of $\mathrm{SO}(n)$.

Work over a field k of characteristic not 2. Let V be a k-vector space, q a quadratic form on V. The *Clifford algebra* $\mathrm{Cl}(V, q)$ is the quotient of the tensor algebra $T(V)$ by the ideal generated by $\{v \otimes v - q(v) : v \in V\}$. There is an obvious injection $V \hookrightarrow \mathrm{Cl}(V, q)$, and k-linear maps $f : V \to A$ into associative k-algebras lift to $\tilde{f} : \mathrm{Cl}(V, q) \to A$ if and only if $f(v)f(v) = q(v)$ for all $v \in V$. This univeral property clearly characterizes $\mathrm{Cl}(V, q)$. For brevity, write $\mathrm{Cl}(V) = \mathrm{Cl}(V, q)$.

Example 6.6.1. Let $V = \mathbf{R}^4$, q be the indefinite form of signature $(3, 1)$, i.e. $q(v) = -v_1^2 + v_2^2 + v3^2 + v_4^2$. We write $\mathrm{Cl}_{(1,3)}(\mathbf{R})$ for the Clifford algebra $\mathrm{Cl}(V, q)$; it has presentation

$$\mathrm{Cl}_{(1,3)}(\mathbf{R}) = \mathbf{R}\langle e_1, e_2, e_3, e_4 \rangle / (e_1^2 = -1, e_2^2 = e_3^2 = e_4^2 = 1).$$

[5]Benjamin ?

This is used in the Dirac equation, which unifies special relativity and quantum mechanics. ▷

There is a clear action $\mathrm{O}(V,q) \to \operatorname{Aut}\mathrm{Cl}(V)$. In particular, the involution $\alpha(v) = -v$ induces an involution (also denoted α) of $\mathrm{Cl}(V)$. This induces a grading $\mathrm{Cl}(V) = \mathrm{Cl}^0(V) \oplus \mathrm{Cl}^1(V)$, where

$$\mathrm{Cl}^0(V) = \{x \in \mathrm{Cl}(V) : \alpha(x) = x\}$$
$$\mathrm{Cl}^1(V) = \{x \in \mathrm{Cl}(V) : \alpha(x) = -x\}.$$

We define some algebraic groups via their functors of points:

$$\mathrm{Pin}(V,q)(A) = \{g \in \mathrm{Cl}(V,q)_A : q(g) \in \boldsymbol{\mu}_2(A)\}$$
$$\mathrm{Spin}(V,q) = \mathrm{Pin}(V,q) \cap \mathrm{Cl}^0(V).$$

There is a "twisted adjoint map" $\tilde{\mathrm{ad}} : \mathrm{Pin}(V,q) \to \mathrm{O}(V,q)$, given by $\tilde{\mathrm{ad}}(g)(v) = \alpha(g)vg^{-1}$.

Theorem 6.6.2. *There is a natural exact sequence*

$$1 \to \boldsymbol{\mu}_2 \to \mathrm{Spin}(V,q) \to \mathrm{SO}(V,q) \to 1.$$

Proof. This is [Ber10, IV.10.21]. □

6.7 Differential Galois theory[6]

A good source for differential Galois theory is [PS03]. Recall that if A is a ring, a *derivation* on A is an additive map $\partial : A \to A$ satisfying the *Liebniz rule*: $\partial(ab) = a\partial(b) + \partial(a)b$. We write $\mathrm{Der}(A)$ for the group of derivations $A \to A$.

Definition 6.7.1. *A* differential ring *is a pair* (R, Δ)*, where* $\Delta \subset \mathrm{Der}(R)$ *is such that* $\partial_1\partial_2 = \partial_2\partial_1$ *for all* $\partial_1, \partial_2 \in \Delta$.

If $\Delta = \{\partial\}$, we write $r' = \partial r$ for $r \in R$. The ring $C = \{c \in R : \partial c = 0 \text{ for all } \partial \in \Delta\}$ is called the *ring of constants*. If R is a field, we call (R, Δ) a *differential field*.

Example 6.7.2. Let $R = C^\infty(\mathbf{R}^n)$ and $\Delta = \{\frac{\partial}{\partial x_i} : 1 \leqslant i \leqslant n\}$. Then (R, Δ) is a differential ring with $\mathbf{R}$ as ring of constants. ▷

Example 6.7.3. Let k be a field, $R = k(x_1, \ldots, x_n)$, and $\Delta = \{\frac{\partial}{\partial x_i} : 1 \leqslant i \leqslant n\}$. Then (R, Δ) is a differential field with field of constants k. ▷

We are interested in solving *matrix differential equations*, that is, equations of the form $y' = Ay$ for $A \in \mathrm{M}_n(k)$. A solution would be a tuple $y = (y_1, \ldots, y_n) \in k^n$ such that $(y_1', \ldots, y_n') = Ay$. To a matrix differential equation we will associate two objects: a Picard-Vessiot ring R, and a linear algebraic group $\mathrm{DGal}(R/k)$.

[6] Ian Pendleton

Definition 6.7.4. *Let (k, ∂) be a differential field, (R, ∂) a differential k-algebra (so $\partial_R|_k = \partial_k$). Let $A \in \mathrm{M}_n(k)$. A* fundamental solution matrix *to the equation $y' = Ay$ is an element $Z \in \mathrm{GL}_n(R)$ such that $Z' = AZ$.*

It is easy to construct a (universal) fundamental solution matrix for the equation $y' = Ay$. Let $S = \mathscr{O}(\mathrm{GL}_n) = k[y_{ij}, \det(y_{ij})^{-1}]$, and define a differential $\partial : S \to S$ by $\partial(y_{ij}) = (Ay)_{ij}$. It is easy to see that S represents the functor that sends a differential k-algebra R to the set of fundamental solution matrices in R.

If (R, Δ) is a differential ring, a *differential ideal* is an ideal $\mathfrak{a} \subset R$ such that $\partial(\mathfrak{a}) \subset \mathfrak{a}$ for all $\partial \in \Delta$. If $\mathfrak{a}$ is a differential ideal, then $R/\mathfrak{a}$ naturally has the structure of a differential ring. Call a differential ring *simple* if it has no nontrivial differential ideals. Note that simple differential rings need not be fields, e.g. $(k[t], \frac{\partial}{\partial t})$.

Definition 6.7.5. *Let $A \in \mathrm{M}_n(k)$. A* Picard-Vessiot ring *for the equation $y' = Ay$ is pair (R, Z), where R is a simple differential k-algebra which has a fundamental solution matrix Z for $y' = Ay$, such that R is generated as a k-algebra by the entries of Z and $\frac{1}{\det Z}$.*

It is easy to prove that Picard-Vessiot rings exist. Let S be the differential ring constructed above. For any maximal differential ideal $\mathfrak{m} \subset S$, the quotient $R = S/\mathfrak{m}$ is a Picard-Vessiot ring. By [PS03, 1.20], Picard-Vessiot rings (for a given equation $y' = Ay$) are unique.

Definition 6.7.6. *Let (k, ∂) be a differential field, $A \in \mathrm{M}_n(k)$. The* differential Galois group *of the equation $y' = Ay$ is $\mathrm{DGal}(R/k) = \mathrm{Aut}_{(k,\partial)}(R)$ for any Picard-Vessiot ring R (for the equation $y' = Ay$).*

Lemma 6.7.7. *The group $\mathrm{DGal}(R/k)$ is linear algebraic.*

Proof. See [PS03, 1.26]. □

Example 6.7.8. If $k = \mathbf{C}(x)$ and we consider the equation $y' = \frac{\alpha}{x} y$ for $\alpha = \frac{n}{m} \in \mathbf{Q}$, then the Picard-Vessiot ring is $R = \mathbf{C}(x^{n/m})$ and $\mathrm{DGal}(R/k) = \mathbf{Z}/m$. ▷

It is shown in [TT79] that over $\mathbf{C}$, all linear algebraic groups arise as differential Galois groups. The "modern" approach to differential Galois theory uses $\mathscr{D}$-modules and Tannakian categories.

6.8 Universal enveloping algebras and the Poincaré-Birkhoff-Witt theorem[7]

Let k be a field, Lie be the category of Lie algebras over k, and Ass be the category of unital associative k-algebras. There is an easy functor $\mathcal{L} : \mathsf{Ass} \to \mathsf{Lie}$, that sends a k-algebra A to the Lie algebra $\mathcal{L}A$ whose underlying vector space is A, with bracket

$$[a, b] = a \cdot b - b \cdot a.$$

[7] Daoji Huang

This has a left adjoint, denoted $\mathcal{U}$. That is, for each Lie algebra $\mathfrak{g}$, there is an associative algebra $\mathcal{U}\mathfrak{g}$ with a k-linear map $i : \mathfrak{g} \to \mathcal{U}\mathfrak{g}$ satisfying $i[x,y] = [i(x), i(y)]$, such that for any algebra A and linear map $f : \mathfrak{g} \to A$ satisfying $f[x,y] = [f(x), f(y)]$, there is a unique extension $\tilde{f} : \mathcal{U}\mathfrak{g} \to A$ such that $f = \tilde{f} \circ i$.

We can construct the universal enveloping algebra $\mathcal{U}\mathfrak{g}$ directly. Let $\mathcal{T}\mathfrak{g} = \bigoplus_{n \geqslant 0} \mathfrak{g}^{\otimes n}$ be the tensor algebra of $\mathfrak{g}$. It is easy to see that $\mathcal{U}\mathfrak{g}$ is the quotient of $\mathcal{T}\mathfrak{g}$ by the relations $\{x \otimes y - y \otimes x - [x,y] : x, y \in \mathfrak{g}\}$.

There is an obvious filtration on $\mathcal{T}\mathfrak{g}$, for which $\mathcal{T}_m\mathfrak{g} = \bigoplus_{m \geqslant n} \mathfrak{g}^{\otimes m}$. It induces a filtration on $\mathcal{U}\mathfrak{g}$. The Poincaré-Birkhoff-Witt theorem is an explicit description of the graded ring $\operatorname{gr} \mathcal{U}(\mathfrak{g})$.

Define a map $\varphi : \mathcal{T}\mathfrak{g} \to \operatorname{gr}(\mathcal{U}\mathfrak{g})$ by the obvious surjections

$$\mathcal{T}^m\mathfrak{g} = \mathfrak{g}^{\otimes m} \to \mathcal{U}^m\mathfrak{g} \twoheadrightarrow \operatorname{gr}^m \mathcal{U}(\mathfrak{g}).$$

This is a homomorphism of graded k-algebras. Moreover, since, for $x \in \mathcal{U}_2\mathfrak{g}$, we have

$$U_2 \ni x \otimes y - y \otimes x = [x,y] \in U_1,$$

it follows that the map φ factors through the symmetric algebra $\mathcal{S}\mathfrak{g}$.

Theorem 6.8.1 (Poincaré-Birkhoff-Witt)**.** *Let $\mathfrak{g}$ be a Lie algebra over k. The map $\varphi : \mathcal{S}(\mathfrak{g}) \to \operatorname{gr} \mathcal{U}(\mathfrak{g})$ is an isomorphism of graded k-agebras.*

Proof. This is [Lie_{1-3}, I §2.7 th.1]. □

More concretely, suppose $\mathfrak{g}$ has a basis $x_1, \ldots, x_n$ of $\mathfrak{g}$. The PBW theorem tells us that every element of $\mathcal{U}\mathfrak{g}$ can be written uniquely as a sum

$$\sum_{\boldsymbol{i}} \lambda_{\boldsymbol{i}} x^{e_{\boldsymbol{i}}},$$

where $\boldsymbol{i}$ ranges over all tuples $(i_1, \ldots, i_r)$ for which $1 \leqslant i_1 < \cdots < i_r \leqslant n$. Here we write

$$x^{e_{\boldsymbol{i}}} = x_{i_1}^{e_1} \cdots x_{i_r}^{e_r}.$$

The PBW theorem is used in many places – one application is a simpler (though less transparent) construction of free Lie algebras than the one in [Lie_{1-3}, II §2].

6.9 Forms of algebraic groups[8]

We start by defining non-abelian cohomology, following [Ber10, II.3]. Let Γ be a profinite group, G a (possibly nonabelian) discrete group on which G acts continuously by automorphisms. The pointed set of 1-*cocycles*, denoted $Z^1(\Gamma, G)$, consists of functions $c : \Gamma \to G$, written $\sigma \mapsto c_\sigma$, such that

$$c_{\sigma\tau} = c_\sigma \sigma(c_\tau)$$

[8] Tao Ran Chen

for all $\sigma, \tau \in \Gamma$. The distinguished 1-cocycle is $\sigma \mapsto 1$. We put an equivalence relation on $Z^1(\Gamma, G)$, namely $c \sim c'$ if there exists $g \in G$ such that

$$c'_\sigma = g c_\sigma \sigma(g^{-1})$$

for all $\sigma \in \Gamma$. Write $\mathrm{H}^1(\Gamma, G) = Z^1(\Gamma, G)/\sim$ be the set of equivalence classes of 1-cocycles.

Let X be a Γ-set with (equivariant) G-action, such that the map $G \times X \to X \times X$ given by $(g, x) \mapsto (gx, x)$ is a bijection. (Such X are called *G-torsors* in the category of Γ-sets.) Choose $x_0 \in X$ and define $c : \Gamma \to G$ by $\sigma(x_0) = c_\sigma^{-1} \cdot x_0$. One can check that c_σ is a 1-cocycle that only depends on the isomorphism class of X as a Γ-equivariant G-set. The "right perspective" here is that G is a group object in the category of Γ-sets, and that $\mathrm{H}^1(\Gamma, G)$ classifies G-torsors in that category. More generally, let G be a group object in an arbitrary topos $\mathcal{T}$. A *G-torsor* is a G-object $X \in \mathcal{T}$ such that $X \to 1$ is an isomorphism, and such that the obvious morphism $G \times X \to X \times X$ is an isomorphism. As in [Joh77, §8.3], one can *define* $\mathrm{H}^1(\mathcal{T}, G)$ to be the (pointed) set of isomorphism classes of G-torsors in $\mathcal{T}$. If $N \subset G$ is a normal subgroup in $\mathcal{T}$, there is a "short long exact sequence" of pointed sets:

$$\begin{tikzcd} 1 \arrow[r] & \mathrm{H}^0(\mathcal{T}, N) \arrow[r] & \mathrm{H}^0(\mathcal{T}, G) \arrow[r] & \mathrm{H}^0(\mathcal{T}, G/N) \arrow[dll, rounded corners] \\ & \mathrm{H}^1(\mathcal{T}, N) \arrow[r] & \mathrm{H}^1(\mathcal{T}, G) \arrow[r] & \mathrm{H}^1(\mathcal{T}, G/N). \end{tikzcd}$$

Our main example is: $\Gamma = \mathrm{Gal}(\bar{k}/k)$ for k a field, in which case the category of Γ-sets is equivalent to $\mathrm{Sh}(k_{\text{ét}})$. We will write $\mathrm{H}^1(k, G)$ instead of $\mathrm{H}^1(k_{\text{ét}}, G)$ for $G \in \mathrm{Sh}(k_{\text{ét}})$. Suppose X is an "object we want to classify." Let $G = \operatorname{Aut} X$ (internal automorphisms object in the category $\mathrm{Sh}(k_{\text{ét}})$). If X' is another object and $\varphi : X'_{k^{\text{sep}}} \to X_{k^{\text{sep}}}$ is an isomorphism, we can define a cocycle $c : \Gamma = \mathrm{Gal}(k^{\text{sep}}/k) \to G(k^{\text{sep}})$ by $c_\sigma = \sigma(\varphi) \circ \varphi^{-1}$. This gives a map $\{k\text{-forms of } X\} \to \mathrm{H}^1(k, G)$, which will generally be injective. We are interested in the case where X is an algebraic group over k.

Let k be a field, $G_{/k}$ an algebraic group. A *k-form of G* is an algebraic group $G'_{/k}$ such that $G'_{k^{\text{sep}}} \simeq G_{k^{\text{sep}}}$. Two k-forms G', G'' are equivalent if $G' \simeq G''$ over k.

Example 6.9.1. Let K/k be a finite Galois extension, $G_{/k}$ an algebraic group. We defined in Example 3.8.3 the *Weil restriction* of an algebraic group; here we apply it to G_K. That is, we write $\mathrm{R}_{K/k} G$ for the algebraic group over k defined by

$$(\mathrm{R}_{K/k} G)(A) = G(A \otimes_k K),$$

for any k-algebra A. By [BLR90, §7.6], $\mathrm{R}_{K/k} G$ is actually an algebraic group. Since $K \otimes_k K \simeq \prod_\Gamma K$, where $\Gamma = \mathrm{Gal}(K/k)$, we have $(\mathrm{R}_{K/k} G)_K \simeq \prod_\Gamma G_K$, i.e. $\mathrm{R}_{K/k} G$ is a k-form of $\prod_K \Gamma$. Interesting k-forms of G can often be obtained by taking appropriate subgroups of $\mathrm{R}_{K/k} G$. ▷

Example 6.9.2. Apply the previous general construction to the extension $\mathbf{C}/\mathbf{R}$. The group $\mathbf{S} = \mathrm{R}_{\mathbf{C}/\mathbf{R}}\,\mathbf{G}_{\mathrm{m}}$ comes with a *norm map* $\mathrm{N} : \mathbf{S} \to \mathbf{G}_{\mathrm{m}}$, coming from the "usual norm" $\mathrm{N} : \mathbf{C} \to \mathbf{R}$. Then $\mathbf{S}^{\mathrm{N}=1}$ is a $\mathbf{R}$-form of $\mathbf{G}_{\mathrm{m}}$. ▷

Example 6.9.3. Let k be a field. A *central simple algebra* over k is a (possibly non-commutative) k-algebra R that is simple and has $\mathrm{Z}(R) = k$. The obvious examples are $\mathrm{M}_n(k)$, but there are others, for example any division algebra D with $\mathrm{Z}(D) = k$. If R is any central simple algebra, then $R_{k^{\mathrm{sep}}} \simeq \mathrm{M}_n(k^{\mathrm{sep}})$ for some n. There is a norm map $\mathrm{N} : R \to k$, which we can use to define a group $\mathrm{SL}(R)$ by

$$\mathrm{SL}(R)(A) = \ker\left((R \otimes_k A)^\times \xrightarrow{\mathrm{N}} A^\times\right),$$

for all k-algebras A. Since R splits over k^{sep}, we have $\mathrm{SL}(R)_{k^{\mathrm{sep}}} \simeq \mathrm{SL}(n)_{k^{\mathrm{sep}}}$. ▷

When $k = \mathbf{R}$, it is well-known that there is only one division algebra, the quaternions $\mathbf{H}$. So the only obvious forms of $\mathrm{SL}(2)_{\mathbf{R}}$ are $\mathrm{SL}(2)$ and $\mathrm{SL}(\mathbf{H})$. It turns out that these are the only ones, but this is far from obvious.

It turns out that the set of k-forms of an algebraic group G can be described using Galois cohomology. Write $\mathrm{Aut}(G)$ for the functor on k-schemes defined by

$$\mathrm{Aut}(G)(S) = \mathrm{Aut}_S(G_S).$$

This is a sheaf for the canonical topology. In particular, we can take $\mathrm{H}^1(k, \mathrm{Aut}\, G) = \mathrm{H}^1(\mathrm{Gal}(\bar{k}/k), \mathrm{Aut}_{k^{\mathrm{sep}}}(G))$. Let G' be a k-form of G. Choose an isomorphism $\phi : G'_{k^{\mathrm{sep}}} \xrightarrow{\sim} G_{k^{\mathrm{sep}}}$, and define $c : \mathrm{Gal}(k^{\mathrm{sep}}/k) \to \mathrm{Aut}_{k^{\mathrm{sep}}}(G)$ by $c_\sigma = \sigma(\phi) \circ \phi^{-1}$. It turns out that the class of c in $\mathrm{H}^1(k, \mathrm{Aut}\, G)$ does not depend on the choice of ϕ. In fact, we have the following result.

Theorem 6.9.4. *Let k be a field, $G_{/k}$ an algebraic group. Then the correspondence defined above induces a natural bijection between the set of equivalence classes of k-forms of G and the pointed set $\mathrm{H}^1(k, \mathrm{Aut}\, G)$.*

Proof. This is Lemma 7.1.1 in [Con]. □

Example 6.9.5. As above, let $k = \mathbf{R}$, $G = \mathrm{SL}(2)$. Then $\mathrm{Aut}\, G = \mathrm{PSL}_2$ and $\mathrm{Gal}(\mathbf{C}/\mathbf{R}) = \mathbf{Z}/2$. So the set of $\mathbf{R}$-forms of $\mathrm{SL}(2)$ is in bijection with $\mathrm{H}^1(\mathbf{R}, \mathrm{PSL}_2) \simeq \mathrm{H}^2(\mathbf{R}, \boldsymbol{\mu}_2)[2]$, which classifies quaternion algebras over $\mathbf{R}$. It is well-known that there are only two such algebras, namely $\mathrm{M}_2(\mathbf{R})$ and $\mathbf{H}$. So our list above is complete. ▷

6.10 Arithmetic subgroups[9]

In what follows, we focus on arithmetic subgroups of real Lie groups. Margulis proved his arithmeticity and hyperrigidity theorems in much greater generality, e.g. for groups like $\mathrm{GL}_n(\mathbf{Z}[\frac{1}{p}]) \subset \mathrm{GL}_n(\mathbf{R}) \times \mathrm{GL}_n(\mathbf{Q}_p)$.

Definition 6.10.1. *Let G be an abstract group, H_1, H_2 subgroups of G. We say H_1 and H_2 are* commensurable *if $H_1 \cap H_2$ has finite index in both H_1 and H_2.*

[9] Ryan McDermott

As an exercise, check that commensurability is an equivalence relation on the set of subgroups of G.

Definition 6.10.2. *Let $G_{/\mathbf{Q}}$ be an algebraic group. A subgroup $\Gamma \subset G(\mathbf{R})$ is* arithmetic *if for some (hence any) embedding $G \hookrightarrow \mathrm{GL}(n)_{\mathbf{Q}}$, the group $G(\mathbf{Q}) \cap \mathrm{GL}_n(\mathbf{Z})$ is commensurable with Γ.*

Clearly $\mathrm{SL}_n(\mathbf{Z})$ is an arithmetic subgroup of $\mathrm{SL}_n(\mathbf{R})$.

Lemma 6.10.3. *Let $G_{/\mathbf{Q}}$ be an algebraic group. If $\Gamma \subset G(\mathbf{R})$ is arithmetic, then Γ is discrete in the induced (analytic) topology.*

Proof. The group Γ is a finite union of cosets of a subgroup of $G(\mathbf{Q}) \cap \mathrm{GL}_n(\mathbf{Z})$, so it suffices to prove that $\mathrm{GL}_n(\mathbf{Z})$ is a discrete subgroup of $\mathrm{GL}_n(\mathbf{R})$. But $\mathrm{GL}_n(\mathbf{Z}) \subset \mathrm{M}_n(\mathbf{Z}) \subset \mathrm{M}_n(\mathbf{R})$, and clearly $\mathrm{M}_n(\mathbf{Z})$ is a discrete subgroup of $\mathrm{M}_n(\mathbf{R})$. $\square$

It is well-known (see for example [Int $\mathrm{II}_{7\text{–}9}$, VII §1.2 th.1]) that any locally compact group G admits a unique (up to scalar) left-invariant Borel measure, called the *Haar measure* on G. We say G is *unimodular* if this measure is also right-invariant. Left-invariant and right-invariant Haar measures are related via a continuous homomorphism $\Delta : G \to \mathbf{R}^+$, known as the *modulus* [Int $\mathrm{II}_{7\text{–}9}$, VII §1.3]. If G is a Lie group, one has $\Delta(g) = (\det \mathrm{ad}\, g)^{-1}$ by [$\mathrm{Lie}_{1\text{–}3}$, III §3.16], so in particular G is unimodular. If G is a general unimodular group and $\Gamma \subset G$ is discrete, then by [Int $\mathrm{II}_{7\text{–}9}$, VII §2.6 cor.2], there is a unique (up to scalar) G-invariant measure on the quotient space $\Gamma \backslash G$.

Definition 6.10.4. *Let G be a unimodular locally compact group, $\Gamma \subset G$ a discrete subgroup. Then Γ is a* lattice *if $\mathrm{vol}(\Gamma \backslash G) < \infty$.*

Definition 6.10.5. *If $G = V$ is a real vector space and $\Gamma = \Lambda \subset V$ is a discrete abelian subgroup with $\mathrm{rk}(\Lambda) = \dim(V)$, then $V/\Lambda \simeq (S^1)^n$ for some n. This is compact, hence it has finite volume.*

We can give a more general version of the definition of arithmetic subgroups.

Definition 6.10.6. *Let $H_{/\mathbf{R}}$ be an almost-simple algebraic group. A subgroup $\Gamma \subset H(\mathbf{R})$ is* arithmetic *if there exists an algebraic group $G_{/\mathbf{Q}}$, a surjection $\phi : G_{\mathbf{R}} \twoheadrightarrow H$ with compact kernel, and an arithmetic subgroup (in the old sense) $\Gamma' \subset G(\mathbf{R})$ such that $\phi(\Gamma)$ is commensurable with Γ.*

As before, arithmetic subgroups are discrete. Moreover, Γ' is discrete in $G(\mathbf{R})$, so $\Gamma' \cap \ker \phi(R)$ is finite. In other words, all arithmetic subgroups (in the new sense) are finite quotients of arithmetic subgroups (in the old sense). Even this new definition is a special case of the much more general one in [Mar91, IX §1].

Define two quadratic forms, one on $\mathbf{R}^{n+1}$ and the other on $\mathbf{C}^{n+1}$:

$$q_1(x) = x_1^2 + \cdots + x_n^2 - x_{n+1}^2$$
$$q_2(z) = |z_1|^2 + \cdots + |z_n|^2 - |z_{n+1}|^2.$$

From this, we define the associated "orthogonal groups:"

$$\mathrm{SO}(1,n) = \{g \in \mathrm{SL}_{n+1}(\mathbf{R}) : q_1(gx) = q_1(x) \text{ for all } x \in \mathbf{R}^{n+1}\}$$
$$\mathrm{SU}(1,n) = \{g \in \mathrm{SL}_{n+1}(\mathbf{C}) : q_2(gz) = q_2(z) \text{ for all } x \in \mathbf{C}^{n+1}\}.$$

Note that $\mathrm{SO}(1,n)$ and $\mathrm{SU}(1,n)$ can be interpreted as the real points of simple algebraic groups over $\mathbf{R}$, but we will not do this.

Theorem 6.10.7 (Margulis)**.** *Let $H_{/\mathbf{R}}$ be a simple algebraic group such that $H(\mathbf{R})$ is not compact, $\Gamma \subset H(\mathbf{R})$ a lattice. Then Γ is arithmetic unless H is isogenous to* $\mathrm{SO}(1,n)$ *or* $\mathrm{SU}(1,n)$.

Proof. This is a special case of the "Theorem A" from [Mar91, IX §1]. □

Since $\mathrm{SL}_2(\mathbf{R})$ is isogenous to $\mathrm{SO}(1,2)$, the theorem doesn't apply to $\mathrm{SL}_2(\mathbf{R})$. In fact, it doesn't hold in this setting. For, there are only countably many arithmetic subgroups of $\mathrm{SL}_2(\mathbf{R})$. However, every compact Riemann surface of genus $g \geqslant 2$ is the quotient of the upper half-plane $\mathfrak{H} = \{z \in \mathbf{C} : \Im z > 0\}$ by a discrete subgroup of $\mathrm{SL}_2(\mathbf{R})$. Since the "space of genus-g compact Riemann surfaces," denoted M_g, is itself $(3g-3)$-dimensional variety over $\mathbf{C}$, there are uncountably many isomorphism-classes of lattices in $\mathrm{SL}_2(\mathbf{R})$. By cardinality considerations, there are non-arithmetic lattices in $\mathrm{SL}_2(\mathbf{R})$.

6.11 Finite simple groups of Lie type

Consider for a moment how we might try to use algebraic geometry to construct simple abstract groups. Clearly, if $G_{/S}$ is a group scheme, then $G(X)$ is an abstract group for any $X_{/S}$. If $x \in X$ is a point, then there is a natural homomorphism $G(X) \to G(k(x))$, probably with nontrivial kernel, so it makes sense to only study $G(k)$ for k a field and $G_{/k}$ an algebraic group. The unipotent radical $\mathcal{R}G$ is normal in G, so we may as well require that $\mathcal{R}G = 1$, i.e. that G be semisimple. Simple factors of G yield big normal subgroups, so we finally arrive at the case where G is a simple algebraic group. One would think that we should look at $G^{\mathrm{ad}}(k)$, where $G^{\mathrm{ad}} = G/\mathrm{Z}(G)$, but from the long exact sequence

$$1 \to Z(k) \to G^{\mathrm{sc}}(k) \to G^{\mathrm{ad}}(k) \to \mathrm{H}^1(k,Z) \to \cdots,$$

we see that $G^{\mathrm{ad}}(k)$ will have an abelian quotient, namely (a subgroup of) $\mathrm{H}^1(k,Z)$. Thus, it makes sense to consider

$$\mathrm{im}(G^{\mathrm{sc}}(k) \to G^{\mathrm{ad}}(k)).$$

If R is a root system, write $G^{\mathrm{sc}}_{R/\mathbf{Z}}$ (resp. $G^{\mathrm{ad}}_{R/\mathbf{Z}}$) for the unique simply connected (resp. adjoint) Chevalley-Demazure group scheme over $\mathbf{Z}$ with root system of type R. If q is a prime power, we define

$$R(q) = \mathrm{im}\left(G^{\mathrm{sc}}_{R/\mathbf{Z}}(\mathbf{F}_q) \to G^{\mathrm{ad}}_{R/\mathbf{Z}}(\mathbf{F}_q)\right).$$

Note that $R(q)$ is *not* the $\mathbf{F}_q$-points of an algebraic group. We will use this construction to give a complete (up to finitely many) list of all finite simple groups.

Theorem 6.11.1 (Classification theorem)**.** *Every finite simple group is one of the following:*

- *cyclic:* $\mathbf{Z}/p$
- *alternating:* A_n $(n \geqslant 5)$
- *Chevalley groups:*
  - $\mathrm{A}_n(q)$, $n \geqslant 1$
  - $\mathrm{B}_n(q)$, $n \geqslant 2$
  - $\mathrm{C}_n(q)$, $n \geqslant 2$
  - $\mathrm{D}_n(q)$, $n \geqslant 3$
  - $\mathrm{E}_6(q)$, $\mathrm{E}_7(q)$, $\mathrm{E}_8(q)$, $\mathrm{F}_4(q)$, *and* $\mathrm{G}_2(q)$
- *Steinberg groups:*
  - ${}^2\mathrm{A}_n(q^2)$, $n \geqslant 2$
  - ${}^2\mathrm{D}_n(q^2)$, $n \geqslant 2$
  - ${}^2\mathrm{E}_6(q^2)$, ${}^3\mathrm{D}_4(q^3)$
- *Suzuki groups:* ${}^2\mathrm{B}_2(2^{2n+1})$, $n \geqslant 1$
- *Ree groups:* ${}^2\mathrm{F}_4(2^{2n+1})$, $n \geqslant 1$ *and* ${}^2\mathrm{G}_2(3^{2n+1})$, $n \geqslant 1$.
- *Tits group:* ${}^2\mathrm{F}_4(2)^1$.
- *The* 26 *sporadic groups.*

Here, q ranges over all primes powers.

See the table in Chapter 1 of [GLS94] for a complete list that includes all the sporadics. The "groups of Lie type" which are not simple are All of these groups are simple, except $\mathrm{A}_1(2)$, $\mathrm{A}_1(3)$, $\mathrm{B}_2(2)$, $\mathrm{G}_2(2)$, and ${}^3\mathrm{A}_2(2^2)$.

Example 6.11.2 (type A_n)**.** One has $\mathrm{A}_n(q) = \operatorname{im}(\mathrm{SL}_{n+1}(\mathbf{F}_q) \to \mathrm{PGL}_{n+1}(\mathbf{F}_q))$. This group is often written $\mathrm{PSL}_n(q)$, but as we have discussed elsewhere, this notation is misleading. For example, $\mathrm{A}_n(2^f) = \mathrm{SL}_{n+1}(\mathbf{F}_{2^f})$. ▷

Example 6.11.3 (type D_n)**.** Recall that the simply-connected form of D_n is $\mathrm{Spin}(2n)$, and the adjoint form is $\mathrm{SO}(2n)/\boldsymbol{\mu}_2$. Thus $\mathrm{D}_n(q)$ is an index-two subgroup of $\mathrm{SO}_{2n}(\mathbf{F}_q)/\{\pm 1\}$. ▷

Example 6.11.4 (type ${}^2\mathrm{A}_n$)**.** These are constructed via "unitary groups." Recall that $\mathrm{SL}(n+1)$ has Dynkin diagram

$$\bullet \text{———} \bullet \text{———} \cdots \text{———} \bullet \text{———} \bullet \qquad (n \text{ vertices}).$$

This has an automorphism (flip accross vertical axis). The induced outer automorphism of $\mathrm{SL}(n+1)$ is $g \mapsto {}^{\mathrm{t}}g^{-1}$. One puts

$$\mathrm{SU}(n) = \{g \in \mathrm{SL}_n(\mathbf{C}) : \bar{g} = {}^{\mathrm{t}}g^{-1}\}.$$

For a finite field $\mathbf{F}_q$, the appropriate analogue of complex conjugation is the unique nontrivial element $\sigma \in \mathrm{Gal}(\mathbf{F}_{q^2}/\mathbf{F}_q)$. Put

$${}^2\mathrm{A}_n(q^2) = \{g \in \mathrm{SL}_{n+1}(\mathbf{F}_{q^2}) : \sigma(g) = {}^{\mathrm{t}}g^{-1}\}/(\text{center}).$$

$\triangleright$

One obtains the other Steinberg groups similarly: they are of the form

$$\{g \in R(q^2) : \sigma(g) = \phi(g)\},$$

where ϕ is an automorphism of $\mathrm{Dyn}(R)$ of order 2. For ${}^3\mathrm{D}_4(q)$, one chooses a generator $\sigma \in \mathrm{Gal}(\mathbf{F}_{q^3}/\mathbf{F}_q)$ and an outer automorphism ϕ of D_4 of order 3. Essentially the same construction can be done with σ and ϕ.

The Suzuki and Ree groups come from the so-called "special isogenies" in characteristics 2 and 3. Roughly, these come from the fact that in characteristic p, a directed multi-arrow in a Dynkin diagram should be replaced with p undirected edges. Thus in characteristic 2, the Dynkin diagram for B_2 is $\bullet = \bullet$, which has a nontrivial automorphism. Similarly, in characteristic 2, The Dynkin diagram of type F_4 should be $\bullet - \bullet = \bullet - \bullet$, which also has an automorphism. Finally, in characteristic 3, $\mathrm{Dyn}(\mathrm{G}_2)$ should be $\bullet \equiv \bullet$.

Finite simple groups of exceptional Lie type can be quite large. For example, $\#\mathrm{E}_8(2) \approx 3.3 \cdot 10^{74}$. In contrast, the Monster group has cardinality $\approx 8.1 \cdot 10^{53}$.

References

[Ber10] Grégory Berhuy. *An introduction to Galois cohomology and its applications*. Vol. 377. London Mathematical Society Lecture Note Series. With a foreword by Jean-Pierre Tignol. Cambridge University Press, 2010.

[Bor91] Armand Borel. *Linear algebraic groups*. Vol. 126. Graduate Texts in Mathematics. Springer-Verlag, 1991.

[BW05] James Borger and Ben Wieland. "Plethystic algebra". In: *Adv. Math.* 194.2 (2005), p. 246.

[BLR90] Siegfried Bosch, Werner Lütkebohmert, and Michel Raynaud. *Néron models*. Vol. 21. Ergebnisse der Mathematik und ihrer Grenzgebiete. Springer-Verlag, 1990.

[Alg_{4-7}] Nicolas Bourbaki. *Algebra. II. Chapters 4–7*. Elements of Mathematics. Translated from the French by P. M. Cohn and J. Howie. Springer-Verlag, 1990.

[Top_{1-4}] Nicolas Bourbaki. *General topology. Chapters 1–4*. Elements of mathematics. Translated from the French, Reprint of the 1989 English translation. Springer-Verlag, 1998.

[Lie_{1-3}] Nicolas Bourbaki. *Lie groups and Lie algebras. Chapters 1–3*. Elements of Mathematics. Translated from the French, Reprint of the 1989 English translation. Berlin: Springer-Verlag, 1998.

[Lie_{4-6}] Nicolas Bourbaki. *Lie groups and Lie algebras. Chapters 4–6*. Elements of Mathematics. Translated from the 1968 French original by Andrew Pressley. Berlin: Springer-Verlag, 2002.

[Int II_{7-9}] Nicolas Bourbaki. *Integration. II. Chapters 7–9*. Elements of Mathematics. Translated from the 1963 and 1969 French originals by Sterling K. Berberian. Springer-Verlag, 2004.

[Lie_{7-9}] Nicolas Bourbaki. *Lie groups and Lie algebras. Chapters 7–9*. Elements of Mathematics. Translated from the 1975 and 1982 French originals by Andrew Pressley. Berlin: Springer-Verlag, 2005.

[Car07] Pierre Cartier. "A primer of Hopf algebras". In: *Frontiers in number theory, physics, and geometry. II.* Springer, 2007, pp. 537–615.

[Con] Brian Conrad. "Reductive group schemes". Available at `http://math.stanford.edu/~conrad/papers/luminysga3.pdf`. Notes from a summer school on SGA 3 in 2011.

[CGP10] Brian Conrad, Ofer Gabber, and Gopal Prasad. *Pseudo-reductive groups*. Vol. 17. New Mathematical Monographs. Cambridge University Press, 2010.

[DM82] P. Deligne and J.S. Milne. "Tannakian categories". In: *Hodge cycles, motives and Shimura varieties*. Vol. 900. Lecture Notes in Mathematics. Corrected and revised version available at http://www.jmilne.org/math/xnotes/tc.pdf. Springer, 1982, pp. 101–228.

[Del71] Pierre Deligne. "Théorie de Hodge. II". In: *Inst. Hautes Études Sci. Publ. Math.* 40 (1971), pp. 5–57.

[DG80] Michel Demazure and Peter Gabriel. *Introduction to algebraic geometry and algebraic groups*. Vol. 39. North-Holland Mathematical Studies. Translated from the French by J. Bell. North-Holland Publishing Co., 1980.

[EGA 2] Jean Dieudonné and Alexandre Grothendieck. *Éléments de géométrie algébrique. II. Étude globale élémentaire de quelques classes de morphismes*. 8. 1961.

[EGA 3_{I}] Jean Dieudonné and Alexandre Grothendieck. *Éléments de géométrie algébrique. III. Étude cohomologique des faisceaux cohérents, Première partie*. 11. 1961.

[GLS94] Daniel Gorenstein, Richard Lyons, and Ronald Solomon. *The classification of the finite simple groups*. Vol. 40. Mathematical Surveys and Monographs. American Mathematical Society, 1994.

[SGA 1] Alexandre Grothendieck, ed. *Revêtements étales et groupe fondamentale (SGA 1)*. Vol. 224. Lecture Notes in Mathematics. Augmenté de deux exposés de M. Raynaud. Springer-Verlag, 1971.

[SGA 3_{I}] Alexandre Grothendieck and Michel Demazure, eds. *Schémas en groupes (SGA 3). Tome I. Propriétés générales des schémas en groupes*. Vol. 151. Lecture Notes in Mathematics. Springer-Verlag, 1970.

[SGA 3_{II}] Alexandre Grothendieck and Michel Demazure, eds. *Schémas en groupes (SGA 3). Tome II. Groupes de type multiplicatif, et structure des schémas en groupes généraux*. Vol. 152. Lecture Notes in Mathematics. Springer-Verlag, 1970.

[SGA 3_{III}] Alexandre Grothendieck and Michel Demazure, eds. *Schémas en groupes (SGA 3). Tome III. Structure des schémas en groupes réductifs*. Vol. 153. Lecture Notes in Mathematics. Springer-Verlag, 1970.

[Har77] Robin Hartshorne. *Algebraic geometry*. Springer-Verlag, 1977.

[Hum75] James Humphreys. *Linear algebraic groups*. Graduate Texts in Mathematics 21. Springer-Verlag, 1975.

[Jac79] Nathan Jacobson. *Lie algebras*. Republication of the 1962 original. New York: Dover Publ. Inc., 1979.

[Jan03] Jens Carsten Jantzen. *Representations of algebraic groups*. Second. Vol. 107. Mathematical Surveys and Monographs. American Mathematical Society, 2003.

[Joh77] P. T. Johnstone. *Topos theory*. Vol. 10. London Mathematical Society Monographs. Academic Press, 1977.

[MLM94] Saunders Mac Lane and Ieke Moerdijk. *Sheaves in geometry and logic*. Universitext. Corrected reprint of the 1992 edition. Springer-Verlag, 1994.

[Mar91] Gregory Margulis. *Discrete subgroups of semisimple Lie groups*. Vol. 17. Ergebnisse der Mathematik und ihrer Grenzgebiete (3). Springer-Verlag, 1991.

[Mil07] J. S. Milne. *Semisimple algebraic groups in characteristic zero*. May 9, 2007. arXiv: 0705.1348.

[Mil14] James Milne. *Algebraic groups*. Online. 2014. URL: http://www.jmilne.org/math/CourseNotes/iAG.pdf (visited on 10/02/2014).

[Nit05] Nitin Nitsure. “Construction of Hilbert and Quot schemes”. In: *Fundamental algebraic geometry*. Vol. 123. Math. Surveys Monogr. Amer. Math. Soc., 2005, pp. 105–137.

[PS03] Marius van der Put and Michael Singer. *Galois theory of linear differential equations*. Vol. 328. Grundlehren der Mathematischen Wissenschaften. Springer-Verlag, 2003.

[Spr09] T. Springer. *Linear algebraic groups*. Second. Modern Mirkhäuser Classics. Birkhäuser Boston, 2009.

[SV00] Tonny Springer and Ferdinand Veldkamp. *Octonions, Jordan algebras and exceptional groups*. Springer Monographs in Mathematics. Springer-Verlag, 2000.

[TT79] Carol Tretkoff and Marvin Tretkoff. “Solution of the inverse problem of differential Galois theory in the classical case”. In: *Amer. J. Math.* 101.6 (1979), pp. 1327–1332.

[Voj07] Paul Vojta. “Jets via Hasse-Schmidt derivations”. In: *Diophantine geometry*. Vol. 4. CRM Series. Pisa: Ed. Norm., 2007, pp. 335–361.

[Wat79] William Waterhouse. *Introduction to affine group schemes*. Vol. 66. Graduate Texts in Mathematics. New York-Berlin: Springer-Verlag, 1979.