Counting Arithmetic Objects

Contents

CHAPTER 1

Algebraic groups, representations and invariant theory

Eyal Z. Goren

1. Introduction

We provide a quick introduction to the theory of linear algebraic groups and their structure. The text follows closely the original lectures that consisted of 3 hours, justifying its brevity and omission of many important topics. The choice of topics was influenced by the aspects of the theory of algebraic groups used in other lectures of the summer school.

The theory of algebraic groups is a vast area of algebraic geometry. The reader interested in expanding their knowledge is advised to consult any of the references appearing in the bibliography; in particular, the excellent books by Borel [Bor2], Fulton & Harris [FH], Humphries [Hum1] and Springer [Spr]. In preparing this talk we made an extensive use of Borel's article [Bor1].

In the interest of simplifying the exposition *we assume throughout that k is a field of characteristic 0 and $\bar{k}$ is an algebraic closure of k.* The conventions of algebraic geometry that we use are as in Hartshorne [Har].

2. Algebraic groups

The most fundamental linear algebraic group is $\mathrm{GL}_n(\bar{k})$. This is the algebraic group of invertible $n \times n$ matrices (x_{ij}) with entries in $\bar{k}$ such that $\det(x_{ij}) \neq 0$. It is an affine variety with coordinate ring $\bar{k}[y, x_{ij} : 1 \leq i, j \leq n]/(y \cdot \det(x_{ij}) - 1)$.

2.1. Definition. A *linear algebraic group* G is a Zariski closed subgroup of $\mathrm{GL}_n(\bar{k})$ for some n.

It follows from the definition, by Yoneda's lemma, that the multiplication and inverse morphisms of $\mathrm{GL}_n(\bar{k})$ induce morphisms of the subgroup G. Thus, by definition, the multiplication morphism $m : G \times G \to G$, the inverse morphism $i : G \to G$ and the zero point, viewed as a morphism $e : \mathbb{A}^0 \to G$ where $\mathbb{A}^0$ is the one pointed space with coordinate ring $\bar{k}$, all induced from GL_n, are morphisms of varieties and respect the group structure at the same time. More precisely, they satisfy the following commutative diagrams:

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{id \times m} & G \times G \\ \downarrow{\scriptstyle m \times id} & & \downarrow{\scriptstyle m} \\ G \times G & \xrightarrow{m} & G, \end{array} \qquad \begin{array}{ccc} \mathbb{A}^0 \times G & \xrightarrow{m \circ (e \times id)} & G \\ \downarrow{\scriptstyle p_2} & \nearrow{\scriptstyle id} & \\ G, & & \end{array} \qquad \begin{array}{ccc} G & \xrightarrow{i \times id} & G \times G \\ \downarrow & & \downarrow{\scriptstyle m} \\ \mathbb{A}^0 & \xrightarrow{e} & G. \end{array}$$

Passing to coordinate rings, one finds the following homomorphisms of $\bar{k}$-algebras (and that they are multiplicative as well is a *key* fact):

$$m^* : \bar{k}[G] \to \bar{k}[G] \otimes_{\bar{k}} \bar{k}[G], \quad e^* : \bar{k}[G] \to \bar{k}, \quad i^* : \bar{k}[G] \to \bar{k}[G],$$

with commutative diagrams induced from those above. Such a structure is called a *Hopf algebra*. We will not make much use of it apart from using it to analyze the so-called characters of algebraic groups. The book [Wat] is a good introduction to affine group schemes.

2.2. Examples. We have, of course, the example of $\mathrm{GL}_n(\bar{k})$ itself, whose coordinate ring is $\bar{k}[y, \{x_{ij}\}_{1\le i,j\le n}]/(y\cdot\det(x_{ij})-1)$. The co-multiplication morphism is given by expressing the ij coordinate of the product of two matrices in terms of the entries of the matrices. Namely, m^* is determined by $m^*(x_{k\ell}) = \sum_i x_{ki} \otimes x_{i\ell}$ and $m^*(y) = y \otimes y$, which expresses the fact that the determinant is a multiplicative function. Standard subgroups of $\mathrm{GL}_n(\bar{k})$ are given by the following subgroups B, N and T that are examples of a Borel subgroup, a unipotent subgroup and a torus, respectively.

$$B = \{(x_{ij}) \in \mathrm{GL}_n(\bar{k}) : x_{ij} = 0 \text{ for } i < j\} = \left\{ \begin{pmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ & x_{22} & \dots & x_{2n} \\ & & \ddots & \\ & & & x_{nn} \end{pmatrix} : x_{ij} \in \bar{k}, x_{11}x_{22}\cdots x_{nn} \neq 0 \right\},$$

$$U = \{(x_{ij}) \in B : x_{ii} = 1, 1 \le i \le n\} = \left\{ \begin{pmatrix} 1 & x_{12} & \dots & x_{1n} \\ & 1 & \dots & x_{2n} \\ & & \ddots & \\ & & & 1 \end{pmatrix} : x_{ij} \in \bar{k} \right\},$$

and

$$T = \{(x_{ij}) \in \mathrm{GL}_n(\bar{k}) : x_{ij} = 0 \text{ for } i \neq j\} = \left\{ \begin{pmatrix} x_{11} & & & \\ & x_{22} & & \\ & & \ddots & \\ & & & x_{nn} \end{pmatrix} : x_{ii} \in \bar{k}, x_{11}x_{22}\cdots x_{nn} \neq 0 \right\}.$$

In this case, all these subgroups are defined by linear conditions. Another subgroup of $\mathrm{GL}_n(\bar{k})$ is $\mathrm{SL}_n(\bar{k})$, the matrices of determinant 1.

Let q be a quadratic form in n variables and let $q(x, y)$ be the associated bilinear form: $q(x, y) : \bar{k}^n \times \bar{k}^n \to \bar{k}$, $q(x, y) = q(x + y) - q(x) - q(y)$, which we identify with an $n \times n$ matrix (q_{ij}), $q_{ij} = q(e_i, e_j)$, where e_i is the standard i-th basis vector of $\bar{k}^n$. We then have $2q(x) = q(x, x)$. In terms of coordinates

$$q(x, y) = {}^t x(q_{ij})y$$

(we use column vectors throughout). One lets

$$\mathrm{SO}_q = \{M \in \mathrm{SL}_n(\bar{k}) : {}^t M(q_{ij})M = (q_{ij})\}.$$

It is an algebraic group defined by quadratic equations.

As a particular case, take $q(x, y) = \sum_{i=1}^n x_i y_{n-i+1}$. The matrix corresponding to q is

$$\begin{pmatrix} & & & 1 & 1 \\ & & \iddots & & \\ & 1 & 1 & & \\ 1 & & & & \end{pmatrix}.$$

We then define two subgroups T_1 and B_1 of SO_q, by $B_1 = B \cap \mathrm{SO}_q, T_1 = T \cap \mathrm{SO}_q$. Note that T_1 consists of diagonal matrices of the form $\mathrm{diag}(t_1, \dots, t_n)$ for which $t_i t_{n-i+1} = 1$ for all i and $\prod_{i=1}^n t_i = 1$; the first condition follow from preserving q, while the second follows from the determinant condition (and is a consequence of the first condition when n is even).

2.3. Homomorphisms and characters. A *homomorphism* $f : G \to H$ *of algebraic groups* over $\bar{k}$ is a morphism of varieties over $\bar{k}$ that is also a homomorphism of groups. Since G and H are affine, giving f is equivalent to giving a homomorphism of $\bar{k}$ algebras $f^* : \bar{k}[H] \to \bar{k}[G]$ satisfying the extra condition that the following diagram commutes:

$$\begin{array}{ccc} \bar{k}[G] & \xleftarrow{\quad f^* \quad} & \bar{k}[H] \\ \downarrow{\scriptstyle m^*} & & \downarrow{\scriptstyle m^*} \\ \bar{k}[G] \otimes_{\bar{k}} \bar{k}[G] & \xleftarrow{f^* \otimes f^*} & \bar{k}[H] \otimes_{\bar{k}} \bar{k}[H]. \end{array}$$

A case of particular interest are the homomorphisms $G \to \mathbb{G}_m$, where $\mathbb{G}_m$ is another notation for $\mathrm{GL}_1(\bar{k}) = \bar{k}^\times$, the multiplicative group of non-zero elements of $\bar{k}$. Such homomorphisms are called *characters* of G. As $\bar{k}[\mathbb{G}_m] = \bar{k}[x, x^{-1}]$ with $m^*(x) = x \otimes x$, giving a character $\chi : G \to \mathbb{G}_m$ is equivalent to providing an invertible element $f = \chi^*(x)$ in $\bar{k}[G]$ that satisfies

$$m_G^*(f) = f \otimes f.$$

Such elements f are called *group-like elements* of $\bar{k}[G]$. One denotes the set of characters $\chi : G \to \mathbb{G}_m$ of G by $X^*(G)$. They form an abelian group under multiplication, where $(\chi_1 \chi_2)(g) := \chi_1(g) \cdot \chi_2(g)$, and are functorial in G in a contravariant manner.

For example, a character of $\mathbb{G}_m$ itself is just an endomorphism of $\mathbb{G}_m$ given by a polynomial $f(x, x^{-1}) = \sum_{-N \le n \le N} a_n x^n \in \bar{k}[x, x^{-1}]$ that satisfies $m^*(f) = f \otimes f$. That gives the identity $\sum_n a_n x^n \otimes x^n = (\sum_n a_n x^n) \otimes (\sum_n a_n x^n)$, from which one concludes that $f(x) = x^n$ for some unique $n \in \mathbb{Z}$. Thus, $X^*(\mathbb{G}_m) \cong \mathbb{Z}$ canonically. It is not hard to boot-strap this argument to conclude that $X^*(T) \cong \mathbb{Z}^n$ canonically, where T is the standard torus of GL_n. The idea is that given a character χ of T, for every fixed i, the character of $\mathbb{G}_m$ provided by the composition $\mathbb{G}_m \to T \to \mathbb{G}_m$, $t \mapsto \mathrm{diag}(1, \dots, t, \dots 1)$ (inclusion into the i-th coordinate), is raising to some power $a_i(\chi)$. One concludes a homomorphism $X^* \to \mathbb{Z}^n$, $\chi \mapsto (a_1(\chi), \dots, a_n(\chi))$, which is the desired isomorphism. Another consequence is that

$$\mathrm{Aut}(T) = \mathrm{Aut}(\mathbb{G}_m^n) \cong \mathrm{GL}_n(\mathbb{Z}).$$

Indeed, given an automorphism $f \colon T \to T$ let f_{ij} be the projection on the i-th coordinate of the restriction of f to the j-th coordinate. Then f_{ij} is a character corresponding to an integer a_{ij}. The matrix corresponding to f is non-other than $(a_{ij})_{1 \le i,j \le n}$. In turn, such a matrix (a_{ij}) defines the automorphism taking a matrix $\mathrm{diag}(t_1, \dots, t_n)$ to $\mathrm{diag}(s_1, \dots, s_n)$ where $s_j = t_1^{a_{j1}} t_2^{a_{j2}} \cdots t_n^{a_{jn}}$.

As another example of a homomorphism between groups, fix an element g of G. Then,

$$\mathrm{Int}_g \colon G \to G, \quad \mathrm{Int}_g(x) = gxg^{-1},$$

is an automorphism of G, and, in fact, $g \mapsto \mathrm{Int}_g$ is a homomorphism $G \to \mathrm{Aut}(G)$.

3. Non-abelian cohomology and forms

3.1. Non-abelian cohomology. Let G be a topological group, acting continuously from the left on a discrete possibly non-commutative group M. The action of $g \in G$ on $m \in M$ is denoted ${}^g m$. We let

$$H^0(G, M) = M^G := \{m \in M : {}^g m = m, \forall g \in G\},$$

be the subgroup of fixed points of G. We also define

$$H^1(G, M) := \{\zeta : G \to M : \zeta(ab) = \zeta(a) \cdot {}^a\zeta(b)\}/\sim .$$

In this definition we take continuous functions $\zeta : G \to M$ only; the equivalence relation $\sim$ is defined as follows: $\zeta \sim \xi$ if there exists an $m \in M$ such that $\zeta(a) = m^{-1} \cdot \xi(a) \cdot {}^a m, \forall a \in G$. Here, H^0 and H^1 are called the *zeroth* and *first cohomology* of G with values in M, respectively. The functions in H^1 are called *cocyles*. We remark that although M^G is a group, unless M is abelian $H^1(G, M)$ is typically not a group but merely a pointed set, that is, a set equipped with a distinguish element, which is just the class of the constant function 1_G.

We remark that there are different conventions in the literature as to the rule relating $\zeta(ab)$ to $\zeta(a)$ and $\zeta(b)$ and, accordingly, the definition of $\sim$. They all produce the same cohomology pointed sets, so these differences are inessential.

If $0 \to A \to B \to C \to 0$ is an exact sequence of G-groups, there is a long exact sequence

$$0 \to A^G \to B^G \to C^G \xrightarrow{\delta} H^1(G, A) \to H^1(G, B) \to H^1(G, C) (\to H^2(G, A)).$$

Some explanations are necessary. The first arrows are group homomorphisms, but as soon as we get to the pointed sets, the statement is that the image of the previous map is the collection of elements going under the next map to the distinguished element. For instance, the image of $H^1(G, A)$ in $H^1(G, B)$ are precisely the elements of $H^1(G, B)$ mapping to the trivial cocycle of $H^1(G, C)$. Furthermore, if A is contained in the centre of B (and, in particular, A is commutative) one can define an abelian group $H^2(G, A)$ and the exact sequence can be prolonged as indicated above. To keep the exposition brief we do not define H^2 here, although we shall use some of its properties - the interested reader can consult [Ser1, Ser2] for details. The maps in the exact sequence are all "obvious", except for the map δ (and the map to H^2, if relevant). It is defined as follows: given $c \in C^G$ choose some $b \in B$ mapping to it and let $\zeta(g) = b^{-1} \cdot {}^g b$. The equivalence relation defined on cocycles shows that this is independent of the choice of b.

3.2. Forms of linear algebraic groups. Let G be a linear algebraic group over $\bar{k}$ and assume that G is defined as a variety over k. That is, the ideal defining G as a sub variety of $\mathrm{GL}_n(\bar{k})$ can be generated using polynomials with coefficients in k. A *k-form* of G is an algebraic group H defined over k such that H is isomorphic to G as an algebraic group over $\bar{k}$. Namely, there is an isomorphism of varieties $H \cong G$, defined over $\bar{k}$, that is also a group homomorphism $H(\bar{k}) \cong G(\bar{k})$. Let $\Gamma = \mathrm{Gal}(\bar{k}/k)$ be the absolute Galois group of k. It is a topological group with a topology determined by decreeing all subgroups $\mathrm{Gal}(\bar{k}/F)$, $[F : k] < \infty$, to be open.

Let H be a k-form of G and $f : G \to H$ an isomorphism over $\bar{k}$. For every $\sigma \in \Gamma$ we have another group isomorphism ${}^\sigma f : G \to H$, simply obtained by applying σ to

the polynomial formulas defining f. Clearly, $f^{-1}\circ{}^{\sigma}f \in \mathrm{Aut}_{\bar{k}}(G)$ (automorphisms as an algebraic group!). That way, H produces a cocycle,

$$\zeta_H\colon \Gamma \to \mathrm{Aut}_{\bar{k}}(G), \quad \zeta_H(\sigma) = f^{-1}\circ{}^{\sigma}f;$$

That is,

$$\zeta_H \in H^1(\Gamma, \mathrm{Aut}_{\bar{k}}(G)).$$

Theorem 1. *There is a natural bijection between the k-forms of G, considered up to k-isomorphism, and the cohomology group $H^1(\Gamma, \mathrm{Aut}_{\bar{k}}(G))$. Under this correspondence, if H corresponds to a cocyle ζ then $H(k) = G(\bar{k})^{\Gamma}$, where Γ acts on $G(\bar{k})$ as ${}^{\tau}g = \zeta(\tau)(g)$.*

Using this, we define the *compact real form* of $\mathrm{GL}_n(\mathbb{C})$. We let $\Gamma = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$, with $\boldsymbol{c}$ denoting complex conjugation and define $\zeta\colon \Gamma \to \mathrm{Aut}_{\mathbb{C}}(\mathrm{GL}_n(\mathbb{C}))$ by $\zeta(1) = \mathrm{id}, \zeta(\boldsymbol{c}) = \{g \mapsto {}^t\bar{g}^{-1}\}$ (a so-called Cartan involution). Let U_n be the group corresponding to this cocyle. Then,

$$U_n(\mathbb{R}) = \{g \in \mathrm{GL}_n(\mathbb{C}) : g = {}^t\bar{g}^{-1}\} = \{g : gg^* = 1\},$$

which is indeed the unitary group over $\mathbb{R}$ (and so our notation is good!). Note that $U_n(\mathbb{R})$ is a compact space in the complex topology, explaining the terminology.

A general theorem asserts that any real reductive group G has a unique real compact form; see, e.g., [OV, Theorem 12, p. 247].

3.3. Examples.

3.3.1. Take the one dimensional torus $T = \mathbb{G}_m$. As an automorphism of $\mathbb{G}_m$ is an invertible character, we conclude that $\mathrm{Aut}(T) = \{\pm 1\}$, where -1 stands for the automorphism $t \mapsto t^{-1}$. Let $\Gamma = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. It is not hard to check, using that Γ acts trivially on $\mathrm{Aut}(T)$, that $H^1(\Gamma, \{\pm 1\})$ is a group with two elements; the non-trivial cocycle takes $\boldsymbol{c}$ (complex conjugation) to -1. We then conclude that T has two forms over $\mathbb{R}$. One is $\mathbb{G}_m = \mathrm{GL}_1$ and the other one is U_1 (the compact real form).

3.3.2. We consider the exact sequence of algebraic groups over k,

$$1 \to \mathbb{G}_m \to \mathrm{GL}_n \to \mathrm{PGL}_n \to 1,$$

where $\mathrm{PGL}_n(\bar{k}) = \mathrm{GL}_n(\bar{k})/\bar{k}^{\times}$ ($\bar{k}^{\times}$ embedded as the scalar matrices). While not obvious, one can show that $\mathrm{PGL}_n(\bar{k})$ is a linear algebraic group, defined over k. Taking Galois cohomology we find the sequence

$$\begin{aligned}(1)\quad 1 \to k^{\times} \to \mathrm{GL}_n(k^{\times}) \to \mathrm{PGL}_n(\bar{k})^{\Gamma} \\ \to H^1(\Gamma, \bar{k}^{\times}) \to H^1(\Gamma, \mathrm{GL}_n(\bar{k})) \to H^1(\Gamma, \mathrm{PGL}_n(\bar{k})) \\ \to H^2(\Gamma, \bar{k}^{\times}).\end{aligned}$$

A classical theorem of Hilbert ("Hilbert's 90") asserts that $H^1(\Gamma, \bar{k}^{\times}) = \{1\}$. This already gives the conclusion that

$$1 \to k^{\times} \to \mathrm{GL}_n(k) \to \mathrm{PGL}_n(\bar{k})^{\Gamma} \to 1$$

is exact and consequently

$$\mathrm{PGL}_n(\bar{k})^{\Gamma} = \mathrm{GL}_n(k)/k^{\times}.$$

(This conclusion is in fact a subtle point. It fails for $\mathrm{PSL}_2 = \mathrm{SL}_2/\{\pm I_2\}$ for example.) A generalization of Hilbert's 90, gives $H^1(\Gamma, \mathrm{GL}_n(\bar{k})) = \{1\}$ (see [Ser1, §X]) and thus we have an exact sequence

$$1 \to H^1(\Gamma, \mathrm{PGL}_n(\bar{k})) \to H^2(\Gamma, \bar{k}^\times).$$

Now, as it turns out, $H^2(\Gamma, \bar{k}^\times)$ is a famous construction; it is the Brauer group of the field k and classify central simple algebras over k up Brauer equivalence: two central simple algebras D_1, D_2, over k are equivalent if for some positive m, n we have an isomorphism of k-algebras $M_m(D_1) \cong M_n(D_2)$. It so happens that also the group $H^1(\Gamma, \mathrm{PGL}_n(\bar{k}))$ has a nice interpretation. The action of $\mathrm{GL}_n(\bar{k})$ on $M_n(\bar{k})$ by conjugation induces an isomorphism

$$\mathrm{PGL}_n(\bar{k}) \cong \mathrm{Aut}(M_n(\bar{k})),$$

where the automorphisms are as a k-algebras. Thus, $H^1(\Gamma, \mathrm{PGL}_n(\bar{k}))$ classifies forms of the algebra $M_n(\bar{k})$. That is, it classifies central simple algebras over k, of rank n^2.

4. Structure of algebraic groups

4.1. Jordan decomposition. This is a seemingly technical property of elements of a linear algebraic group. However, it turns out to play an absolutely crucial part in many arguments.

Any matrix $g \in \mathrm{GL}_n(\bar{k})$ has a unique decomposition, called the *Jordan decomposition*,

$$g = g_s \cdot g_u, \quad g_s g_u = g_u g_s,$$

where g_s is semisimple (that is, diagonalizable) and g_u is unipotent (that is, $(g_u - I_n)^n = 0$). To understand what this decomposition is, we may by conjugating the matrix restrict our attention to a matrix in Jordan canonical form. An easy argument gives that it is enough then to examine the case of a single Jordan block; the overall decomposition is obtained by putting together the compositions of the blocks. But for a matrix M of the form $\lambda I_a + U$, where I_a is the identity matrix of size a and where U is a matrix all whose entries are zero except that $U_{i,i+1} = 1, i = 1, 2, \ldots, n-1$, we easily check that the decomposition is $\lambda I_a \cdot (\lambda^{-1} M)$.

The key fact about the Jordan decomposition is that it is "very persistent". The following holds:

Proposition 2. *Let H be a subgroup of $\mathrm{GL}_n(\bar{k})$. If $g \in H$ so are g_s and g_u. Let $f\colon G \to H$ be a homomorphism of algebraic groups. Then $f(g)_s = f(g_s)$ and $f(g)_u = f(g_u)$.*

4.2. Tori. A *torus* T over k is a form of $\mathbb{G}_m^n$ for some n. Thus, tori are classified by

$$H^1(\Gamma, \mathrm{GL}_n(\mathbb{Z})) = \mathrm{Hom}(\Gamma, \mathrm{GL}_n(\mathbb{Z}))/\sim \text{conjugation}.$$

However, there is a more effective mechanism to describe tori. Consider

$$X^*(T \otimes_k \bar{k}) := \mathrm{Hom}(T \otimes_k \bar{k}, \mathbb{G}_m) \cong \mathrm{Hom}(\mathbb{G}_m^n, \mathbb{G}_m) \cong \mathbb{Z}^n.$$

It carries a Galois action. For $\sigma \in \Gamma, \chi \in X^*(T)$,

$$({}^\sigma\chi)(t) = \sigma(\chi({}^{\sigma^{-1}}t)).$$

Thus T provides us with a free rank n Galois module, namely, $X^*(T)$. By pull-back, a homomorphism of tori $f\colon T_1 \to T_2$ defined over k induces a Galois equivariant homomorphism $f^*\colon X^*(T_2) \to X^*(T_1)$. It turns out that this captures completely the category of tori. More precisely,

Theorem 3. *(Cf.* [Bor2, §III.8.12]*) There is an anti-equivalence of categories between tori over k and free $\mathbb{Z}$-modules of finite rank equipped with a continuous Galois action.*

Note that the elements of $\mathbb{G}_m^n$ are diagonal and commuting. Thus, by properties of the Jordan decomposition, their images under any linear representation of $\mathbb{G}_m^n$, say $\rho\colon \mathbb{G}_m^n \to \mathrm{GL}(V)$ are simultaneously diagonalizable. The same holds for any torus T, only that the decomposition is taking place over $\bar{k}$. That is,

$$V = \oplus_{\alpha \in X^*(T)} V_\alpha, \tag{2}$$

where $V_\alpha := \{v \in V : \rho(t)(v) = \alpha(t) \cdot v\}$, for all $t \in T$. The subspaces V^α are only defined over $\bar{k}$ in general. If V and ρ are defined over k then we have an induced Galois action: $\sigma(V_\alpha) = V_{\sigma\alpha}$.

Example. Consider the Deligne torus $\mathbb{S}$. This is a rank 2 torus over $\mathbb{R}$, with the property $\mathbb{S}(\mathbb{R}) \cong \mathbb{C}^\times, \mathbb{S}(\mathbb{C}^\times) \cong \mathbb{C}^\times \times \mathbb{C}^\times$; more precisely, $\mathbb{S}(A) = (\mathbb{C} \otimes_{\mathbb{R}} A)^\times$ for any $\mathbb{R}$-algebra A. The inclusion $(\mathbb{R} \otimes_{\mathbb{R}} A)^\times \subseteq (\mathbb{C} \otimes_{\mathbb{R}} A)^\times$ shows an injection $\mathbb{G}_m \to \mathbb{S}$, corresponding to a surjection $X^*(T) \to X^*(\mathbb{G}_m) = \mathbb{Z}$ (where the Galois action on $\mathbb{Z}$ is trivial). This shows that the action of complex conjugation on $X^*(T)$ must be given by a matrix whose characteristic polynomial is $x^2 - 1$. Up to conjugation by $\mathrm{GL}_2(\mathbb{Z})$ such a matrix is either $\left(\begin{smallmatrix} 1 & \\ & -1 \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} & 1 \\ 1 & \end{smallmatrix}\right)$. The first leads to a split torus $\mathbb{G}_m \times U_1$ (see §3.3.1) and so T must correspond to the lattice $\mathbb{Z}^2$ with $\boldsymbol{c}$ acting by $\left(\begin{smallmatrix} & 1 \\ 1 & \end{smallmatrix}\right)$. Given now a representation $\rho\colon T \to \mathrm{GL}_n(\mathbb{R})$, we can decompose $V = \sum_{(p,q)\in\mathbb{Z}^2} V^{(p,q)}$, where we think about (p, q) as a character of T. The Galois action induces an isomorphism $\overline{V^{(p,q)}} = V^{(q,p)}$. This structure appears in the theory of Hodge structures.

Theorem 4. *All maximal tori in G are conjugate in G over $\bar{k}$. Their common dimension is called the rank of G and denoted here* $\mathrm{rk}(G)$.

For example, $\mathrm{rk}(\mathrm{GL}_n(\bar{k})) = n$ and $\mathrm{rk}(\mathrm{SO}_{2n+1}) = \mathrm{rk}(\mathrm{SO}_{2n}) = n$. Examples of maximal tori for these groups were given in §2.2.

4.3. Solvable groups. A linear algebraic group G is called *solvable* if there is a series of algebraic subgroups $\{1\} \subseteq G_1 \subseteq \cdots \subseteq G_t = G$, such that G_{i-1} is normal in G_i and the quotients G_i/G_{i-1}, that exist by a general theorem for quotients of linear algebraic groups, are abelian.

The standard example is provided by the group B of upper triangular matrices in $\mathrm{GL}_n(\bar{k})$, given in §2.2. In fact, as $B = T \ltimes U$ in the notation of loc. cit., B is solvable if and only if U is solvable. One considers the subgroups of the form

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & * & * & \cdots & * \\ & 1 & 0 & & 0 & * & \cdots & * \\ & & \ddots & & & \ddots & & \\ & & & 1 & 0 & \cdots & 0 & * \\ & & & & 1 & & & 0 \\ & & & & & \ddots & & \\ & & & & & & & 1 \end{pmatrix}.$$

They provide us with a series of subgroups with abelian quotients. In a sense B is the most general example. More precisely:

Theorem 5 (Kolchin-Lie). *Let G be a solvable subgroup of $\mathrm{GL}_n(\bar{k})$ then G can be conjugated into B.*

We say that G *acts on a variety* V if we have a morphism $G \times V \to V$ that satisfies the expected diagrams for a group action (the details are left to the reader). It is not hard to check that the Kolchin-Lie theorem is equivalent to the following statement: *A solvable algebraic group acting on a projective space has a fixed point.* Borel's theorem generalizes this fact.

Theorem 6 (Borel). *Let G be a connected solvable algebraic group acting on a complete algebraic non-empty variety V, then G has a fixed point in V.*

Definition. Let G be a linear algebraic group. A maximal connected solvable subgroup of G is called a *Borel subgroup* of G.

We have given examples of Borel subgroups - the subgroups denoted by B and B_1 - in §2.2. Here are two important facts about Borel subgroups.

Theorem 7. *Over $\bar{k}$, every torus is contained in a Borel subgroup. If G is reductive, all Borel subgroups are conjugate.*

We will soon get to the definition of reductive group. The linear groups $\mathrm{GL}_n, \mathrm{SL}_n, \mathrm{SO}_n, U_n, \mathrm{Sp}_{2n}$ (the last group, called the symplectic group, is the subgroup of GL_{2n} preserving the standard bilinear alternating pairing on $\bar{k}^{2n}$ given by the matrix $\left(\begin{smallmatrix} 0_n & I_n \\ -I_n & 0_n \end{smallmatrix}\right)$) are all reductive, as is any torus. A product of reductive groups, or, more generally, an extension of reductive groups, is reductive.

4.4. Radicals, semisimple and reductive groups. We define here the notions of semisimple and reductive groups. The reductive groups are a more general class than the semisimple groups and it is the class of algebraic groups for which one can develop an elegant theory of their linear representations (often by reduction to the semisimple case). It is perhaps a good place to remind the reader our standing assumption that the base field k has characteristic 0. In this case, a group is reductive, in the sense defined below, if and only if it is *linearly reductive*, that is, any linear representation of the group is a direct sum of irreducible representations; over a field of positive characteristic the representation theory of a reductive group is not as easy and one needs to distinguish between a reductive group and a linearly reductive group. In fact, by a theorem of Nagata, a connected algebraic group over a field of positive characteristic is linearly reductive if and only if it is a torus (cf. [Koh]).

Definition. For a linear algebraic group G we let $R(G)$, the *radical* of G, denote the maximal connected-normal-solvable-subgroup of G. We let $R_u(G)$, the *unipotent radical* of G, denote the maximal connected-normal-unipotent-subgroup of G. A connected linear algebraic group G is called *semi simple* if $R(G) = \{1\}$. It is called *reductive* if $R_u(G) = \{1\}$.

Of course, behind those definitions are a series of lemmas without which the definition would not make sense. For example, that the product of two connected (resp. normal, resp. solvable) subgroups of G is a connected (resp. normal, resp. solvable) subgroup of G. The groups $\mathrm{SL}_n, \mathrm{SO}_n, \mathrm{Sp}_{2n}$ are semisimple, while the

group GL_n as well as any nontrivial torus are reductive but not semisimple. The Borel subgroup B of GL_n, $n > 1$, is not reductive as its unipotent radical is U.

Any linear algebraic group G has a decomposition

$$G = H \ltimes R_u(G),$$

where H is a maximal reductive subgroup of G - see [Bor1, §5.1] for this fact and other properties of reductive groups stated below. This particular statement uses once more our assumption that $\mathrm{char}(k) = 0$. The group $G/R_u(G)$ is reductive and the group $G/R(G)$ is semisimple. Further, if G is reductive and $Z(G)$ denotes its centre, then $G/Z(G)$ is semisimple. In that case the connected component of $Z(G)$ is a torus. And so, morally speaking, for connected algebraic groups, the difference between reductive and semisimple is just a central torus.

From the point of view of representation theory, the reductive groups are precisely the linear algebraic groups for which the representation theory is managable. To see the problem, consider the unipotent group U of $\mathrm{GL}_2(\bar{k})$ acting naturally on $\bar{k}^2$. This representation is not a sum of irreducible representations, but rather a non-split extension $0 \to \bar{k} \to \bar{k}^2 \to \bar{k} \to 0$, where the action on both kernel and quotient is the trivial representation. Without presuming to offer here a serious discussion, we can appreciate the complications arising from such a phenomenon where a representation cannot be captured by a decomposition into irreducible representations, or even a filtration by such. The main difference is the following fundamental result:

Theorem 8. *Let G be a reductive group and $\rho\colon G \to \mathrm{GL}(V) \cong \mathrm{GL}_n(\bar{k})$ a finite dimensional representation of G. Then $\bar{k}[\rho(G)]$, the sub-algebra of the algebra of $n \times n$ matrices $M_n(\bar{k})$, is a semisimple algebra. Consequently, the representation V decomposes into a direct sum of irreducible representations of G.*

Conversely, if G is a connected linear algebraic group that is linearly reductive then G is reductive.

4.5. Parabolic subgroups. Let G be a connected linear algebraic group. A subgroup P of G is called *parabolic* if G/P is a projective variety. A basic result is

Theorem 9. *P is a parabolic subgroup of G if and only if P contains a Borel subgroup of G.*

Example. A *flag* F in $\bar{k}^n$ is a sequence of subspaces

$$F = (\{0\} \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots \subsetneq F_a \subsetneq \bar{k}^n).$$

Let $\underline{d} = (d_1, \ldots, d_a), d_i = \dim(F_i)$. We call $\underline{d}$ the type of F. The space of all flags of type $\underline{d}$ is a complete algebraic variety $\mathcal{F}_{\underline{d}}$. This is a classical result in algebraic geometry; the basic example being the case of a single subspace, that is $\underline{d} = (d_1)$ for some integer $0 < d_1 < n$. The resulting space is called the Grassmann variety $G(d_1, n)$ (and, still specializing, the case $d_1 = 1$ is nothing else than the projective space $\mathbb{P}^{n-1}$). The general case could be understood as a closed subset of $G(d_1, n) \times G(d_2, n) \times \cdots \times G(d_a, n)$, a so-called incidence variety. At any rate, the group $\mathrm{GL}_n(\bar{k})$ acts transitively on $\mathcal{F}_{\underline{d}}$ and so the stabilizer of a given point is a parabolic subgroup. For example, taking $F_i = \mathrm{Span}\{e_1, \ldots, e_{d_i}\}$, where e_i are the

standard basis elements, we find the parabolic

$$\begin{pmatrix} \boxed{M_1} & * & \cdots & * \\ & \boxed{M_2} & \cdots & * \\ & & \ddots & \\ & & & \boxed{M_{a+1}} \end{pmatrix},$$

where $M_i \in \mathrm{GL}_{d_i - d_{i-1}}(\bar{k})$ (put $d_0 = 0$ and $d_{a+1} = n$ for convenience). Note that taking the maximal type $\underline{d} = (1, 2, \ldots, n-1)$ gives us the standard Borel subgroup.

Now consider $V = \bar{k}^n$ with the bilinear form $q = \begin{pmatrix} & & & 1 & 1 \\ & & \iddots & & \\ & 1 & 1 & & \\ 1 & 1 & & & \end{pmatrix}$ as in §2.2. An *isotropic flag* is a sequence of subspaces of $\bar{k}^n$,

$$F = (\{0\} \subsetneq F_1 \subsetneq F_2 \subsetneq \cdots \subsetneq F_a),$$

such that each F_i is isotropic, that is, the restriction of q to $F_i \times F_i$ is identically zero. The type is defined in the same way. Let $\mathcal{F}^\circ_{\underline{d}}$ be the flag variety of isotropic flags. As before, $\mathcal{F}^\circ_{\underline{d}}$ is a complete algebraic variety and SO_q acts transitively on $\mathcal{F}^\circ_{\underline{d}}$ by Witt's extension theorem. Thus, the stabilizer of a point is a parabolic subgroup of SO_q. If we let $F_i = \mathrm{Span}\{e_1, \ldots, e_{d_i}\}$ (where $d_i \leq n/2$ necessarily) then F_i is isotropic and we get an isotropic flag. The fact that a linear transformation T in SO_q preserves q implies that if it preserves F_i it must preserve $F_i^\perp = \mathrm{Span}\{e_1, \ldots, e_{n-d_i}\}$ and if T acts on F_i by the matrix A_i, it acts on $\bar{k}^n / F_i^\perp = \mathrm{Span}\{e_{n-d_i+1}, \ldots, e_n\}$ by the matrix $\tilde{A}_i := J^t A_i^{-1} J$, where J is the matrix $\begin{pmatrix} & & & 1 & 1 \\ & & \iddots & & \\ & 1 & 1 & & \\ 1 & 1 & & & \end{pmatrix}$ of the same size as A_i. Putting it together, we get a parabolic subgroup

$$\begin{pmatrix} \boxed{M_1} & * & \cdots & & & & * \\ & \boxed{M_2} & * & \cdots & & & * \\ & & \ddots & & & & \\ & & & \boxed{R} & & & \vdots \\ & & & & \ddots & & \\ & & & & & \boxed{\tilde{M}_2} & * \\ & & & & & & \boxed{\tilde{M}_1} \end{pmatrix};$$

the M_i are arbitrary invertible matrices of size $d_i - d_{i-1}$ and $R \in \mathrm{SO}(W)$, where W is the span of $\{e_{d_a+1}, \ldots, e_{n-d_a}\}$.

The example we just gave may mislead the reader to think that pullback of parabolic subgroups are often parabolic (in this case, the pullback from GL_n). This is *rarely* the case. Indeed, we have the following theorem.

Theorem 10 (Chevalley, cf. [DMOS, Proposition 3.1, p. 40]**).** *Let G be a linear reductive group and H a linear algebraic subgroup of G. Then there is an embedding $G \to \mathrm{GL}_n$ such that $H = G \cap P$, where P is a parabolic subgroup of GL_n.*

5. Roots and parabolic subgroups

We define here the root system of a reductive algebraic group G. We explain how the root system gives a detailed map of all parabolic subgroups of G.

5.1. Lie algebra. Let G be a linear algebraic group over $\bar{k}$. Left multiplication by an element of $g \in G$, $\ell_g(x) = gx$, is an automorphism of G that induces an automorphism of the tangent bundle, $\ell_{g,*} \colon T_G \to T_G$ (taking the tangent space at a point x to the tangent space at the point gx). The Lie algebra of G, $\mathrm{Lie}(G)$ is initially the tangent space $T_{G,1}$ to G at the identity; due to the structure above, elements of $T_{G,1}$, viewed as derivation at the point 1, can be extended to left invariant derivations of G, that is, to a section of T_G that is invariant under the map $\ell_{g,*}$ for any $g \in G$.

Thinking of $X, Y \in \mathrm{Lie}(G)$ as derivations allows us to define the bracket of X and Y, namely $[X,Y] := X \circ Y - Y \circ X$, which is a again a left-invariant derivation. This makes the $\bar{k}$ vector space $\mathrm{Lie}(G)$ into a Lie algebra. Namely, besides the fact that $[X,Y]$ is bilinear and alternating also the Jacobi identity holds: $[X,[Y,Z]] + [Z,[X,Y]] + [Y,[Z,X]] = 0$.

The association $G \to \mathrm{Lie}(G)$ is functorial. In particular, a homomorphism of algebraic groups $f \colon G \to H$ induces a homomorphism $\mathrm{Lie}(f) \colon \mathrm{Lie}(G) \to \mathrm{Lie}(H)$ of Lie algebras. In particular, the conjugation homomorphism $\mathrm{Int}_g(x) = gxg^{-1}$ induces an automorphism $\mathrm{Lie}(\mathrm{Int}_g) \colon \mathrm{Lie}(G) \to \mathrm{Lie}(G)$, commonly denoted

$$\mathrm{Ad}(g) \colon \mathrm{Lie}(G) \to \mathrm{Lie}(G).$$

In particular $\mathrm{Ad}(g)$ is a linear map and the resulting homomorphism into the automorphisms of $\mathrm{Lie}(G)$, viewed merely as a vector space,

$$G \to \mathrm{Aut}(\mathrm{Lie}(G)) \cong \mathrm{GL}_n(\bar{k}), \quad g \mapsto \mathrm{Ad}(g),$$

is called the *adjoint representation* of G on its Lie algebra ($n = \dim(G)$). Passing to the Lie algebras, we get a homomorphism of Lie algberas

$$\mathfrak{ad} : \mathrm{Lie}(G) \to \mathrm{End}(\mathrm{Lie}(G)). \tag{3}$$

5.1.1. *The Lie algebra of* $\mathrm{GL}_n(\bar{k})$. This is the fundamental example. One can show that the Lie Algebra of $\mathrm{GL}_n(\bar{k})$, customarily denoted $\mathfrak{gl}_n$, can be canonically identified with the vector space $M_n(\bar{k})$ of $n \times n$ matrices, endowed with the bracket $[X,Y] = XY - YX$. The adjoint representation is simply

$$\mathrm{Ad}(g)(X) = gXg^{-1},$$

and its derivative is

$$\mathfrak{ad}(g)(X) = gX - Xg.$$

5.1.2. *The Lie algebra of a general linear group.* Let $H \subset \mathrm{GL}_n(\bar{k})$ be a linear algebraic group. There is an easy method to calculate the Lie algebra of H as a sub Lie algebra of $\mathfrak{gl}_n$; one develops the equations defining H to first order around the identity and takes the resulting linear equations as defining a subspace of $\mathfrak{gl}_n$. This subspace can be proven to be $\mathrm{Lie}(H)$. Note that this gives a quick way to calculate $\dim(H)$ as it is equal to $\dim_{\bar{k}}(\mathrm{Lie}(H))$. We illustrate this in a few examples.

(1) **The group** $\mathrm{SL}_n(\bar{k})$**.** The group SL_n is determined by the condition $\det(M) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) \prod_{i=1}^n m_{\sigma(i),i} = 1$ for a matrix $M = (m_{ij})$. Write $M = I_n + X$ and $X = (x_{ij})$. Writing the formula for $1 - \det(M) = 0$ and ignoring any terms in the square of the maximal ideal, namely terms

in the ideal $(\{x_{ij}x_{kl} : 1 \leq i,j,k,l \leq n\})$ we find that only one term survives. This is the term $\sum_i x_{ii} = 0$ coming from the product $\prod_i (1 + x_{ii})$. Consequently,

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

In particular, $\dim(\mathrm{GL}_n) = n^2$ and $\dim(\mathrm{SL}_n) = n^2 - 1$.

(2) **The group $\mathrm{O}_n(\bar{k})$.** Let q be the bilinear form defined by the identity matrix I_n. Then O_q, denoted in this case O_n, is the group of matrices $\{M \in \mathrm{GL}_n(\bar{k}) : {}^tM \cdot M = I_n\}$. Again, writing $M = I_n + X$ we find that $I_n = {}^t(I_n + X)(I_n + X) = I_n + {}^tX + X + {}^tXX$. Modulo the square of the maximal ideal we get that $X = -{}^tX$. We find that $\mathfrak{o}_q = \mathrm{Lie}(\mathrm{O}_q)$ is given by

$$\mathfrak{o}_q = \{M \in \mathfrak{gl}_n : M = -{}^tM\}.$$

Note that the Lie algebra $\mathfrak{so}_n$ of SO_n is the same; we have that the determinant 1 condition is translated into the trace being zero, but that is a consequence of $M = -{}^tM$. This is of course expected, the orthogonal group is disconnected with SO_n being the connected component of the identity. The tangent space at the identity depends, of course, only on the identity component. We conclude also that $\dim(\mathrm{O}_n) = \dim(\mathrm{SO}_n) = \binom{n}{2}$.

(3) **The group $\mathrm{Sp}_{2n}(\bar{k})$.** The group $\mathrm{Sp}_{2n}(\bar{k})$ is defined as the subgroup of $\mathrm{GL}_{2n}(\bar{k})$ that preserves the alternating bilinear form given by the matrix $\left(\begin{smallmatrix} & I_n \\ -I_n & \end{smallmatrix}\right)$. Writing such a matrix around the identity as $I_{2n} + \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$ we find the conditions $B = {}^tB, C = {}^tC, {}^tA = -D$ and $\dim(\mathrm{Sp}_{2n}) = 2n^2 + n$.

(4) **The maximal torus T of $\mathrm{GL}_n(\bar{k})$.** The same reasoning as above allows us to identify the Lie algebra $\mathfrak{h}$ of T as the diagonal matrices of size n.

Let G be a *semisimple* algebraic group with a maximal torus T and let $\mathfrak{h}$ be the Lie algebra of T. Via the adjoint representation Ad, T acts on the Lie algebra $\mathfrak{g}$ of G. The properties of the Jordan decomposition guarantee that the elements of T are "universally semisimple" and commuting, it follows that we can decompose $\mathfrak{g}$ canonically as

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{g}_\alpha,$$

where $\Phi = \{\alpha \in X^*(T) - \{0\} : \mathfrak{g}_\alpha \neq 0\}$ and $\mathfrak{g}_\alpha = \{x \in \mathfrak{g} : \mathrm{Ad}(t)(x) = \alpha(t) \cdot x, \forall t \in T\}$ is the eigenspace of T corresponding to the character α.

The set Φ is finite. It is contained in the real vector space $X^*(T) \otimes_{\mathbb{Z}} \mathbb{R}$ of dimension equal to the rank of G. This real vector space is endowed with a canonical inner product $(\cdot, \cdot)$ called the *Killing form*. To begin with, the Killing form is a bilinear symmetric form on $\mathfrak{g}$ given by

$$B(x, y) = \mathrm{Tr}(\mathfrak{ad}(x) \circ \mathfrak{ad}(y)).$$

We can restrict this bilinear form to $\mathfrak{h}$ and then one finds that (cf. [FH, §14.2])

$$B(x, y) = \sum_{\alpha \in \Phi} \alpha(x)\alpha(y).$$

Here we implicitly identify the roots for the action of T on $\mathfrak{g}$ with the roots for the action of its Lie algebra $\mathfrak{h}$ on $\mathfrak{g}$. The restriction of Killing form to $\mathfrak{h}$ is thus non-degenerate and consequently, it provides an isomorphism of the dual vector space

$\mathfrak{h}^*$ with $\mathfrak{h}$ and in particular every root α is assigned a particular element $T_\alpha \in \mathfrak{h}$. By definition, the inner product on the roots of T is

$$(\alpha, \beta) = B(T_\alpha, T_\beta).$$

See the references above and also [GW, §§2.4-2.5] for more details. In it an interesting theorem that if the Killing form is non-degenerate then G is semisimple (see [GW, Theorem 2.5.11]). We will not discuss the Killing form further except to provide it for GL_n below.

The set Φ is a *root system* of $X^*(T) \otimes_{\mathbb{Z}} \mathbb{R}$, which means that (i) it is finite and spans $X^*(T) \otimes_{\mathbb{Z}} \mathbb{R}$, (ii) Φ doesn't contain 0 and $\Phi = -\Phi$, (iii) for all $\alpha \in \Phi, s_\alpha(\Phi) = \Phi$, where $s_\alpha(v) = v - \frac{2(v,\alpha)}{(\alpha,\alpha)} \cdot \alpha$, and (iv) for all $\alpha, \beta \in \Phi$, $s_\alpha(\beta) - \beta$ is an integral multiple of α (equivalently, $\frac{2(\beta,\alpha)}{(\alpha,\alpha)} \in \mathbb{Z}$).

A *Weyl chamber* $\mathcal{W}$ is a connected component of $(X^*(T) \otimes_{\mathbb{Z}} \mathbb{R}) \setminus \cup_{\alpha \in \Phi} \alpha^\perp$. It is an open polyhedral cone in $X^*(T) \otimes_{\mathbb{Z}} \mathbb{R}$ with finitely many faces. A Weyl chamber $\mathcal{W}$ determines an ordering of the roots: one says that α is *positive* if $(\alpha, v) > 0, \forall v \in \mathcal{W}$ and extends this notion to Φ by saying that $\alpha > \beta$ if $\alpha - \beta$ is positive. A positive root α is called *simple* if it not the sum of positive roots in $\Phi - \{\alpha\}$ with positive integer coefficients. Let $\Delta \subset \Phi$ be the set of simple roots.

5.2. Parabolic subgroups and roots. The basic theorem in this business is the following.

Theorem 11. *A choice of a Borel subgroup $B \supseteq T$ corresponds to a choice of Weyl chamber $\mathcal{W}$ and thus to an ordering of the roots. This correspondence is such that if $\mathfrak{b} = \mathrm{Lie}(B)$ then*

$$\mathfrak{b} = \sum_{\alpha \geq 0} \mathfrak{g}_\alpha.$$

This Lie algebra contains a Lie subalgebra $\mathfrak{u} = \sum_{\alpha > 0} \mathfrak{g}_\alpha$. There is a corresponding decomposition $B = TU$, where U is the unipotent radical of B; $\mathfrak{u} = \mathrm{Lie}(U)$.

Given a subset $\Theta \subseteq \Delta$, let S_Θ be the connected component of $\cap_{\alpha \in \Theta} \mathrm{Ker}(\alpha)$, which is a torus of rank $\mathrm{rk}(G) - \sharp\Theta$. Let $Z(S_\Theta)$ be the centralizer of S_Θ in G and let

$$P_\Theta = Z(S_\Theta) \cdot U.$$

We call such a group a standard parabolic group. *There is a bijection between conjugacy classes of parabolic subgroups of G and standard parabolic subgroups. The set of standard parabolic subgroups has cardinality $2^{\sharp\Delta}$.*

5.2.1. *Example: parabolic subgroups of* GL_n. We take $G = \mathrm{GL}_n(\bar{k})$, with the maximal torus $T = \{t = \mathrm{diag}(t_1, \ldots, t_n) : \prod t_i \neq 0\}$. Let

$$\lambda_i(t) = t_i.$$

Then

$$X^*(T) = \oplus_{i=1}^n \mathbb{Z} \cdot \lambda_i.$$

The Lie algebra $\mathfrak{g} = \mathfrak{gl}_n$ can be identified with the $n \times n$ matrices with entries in $\bar{k}$ and has a basis consisting of the elementary matrices $\{E_{ij} : 1 \leq i, j \leq n\}$, where E_{ij} has ij entry equal to 1 and all its other entries are zero. An easy calculation gives $t \cdot E_{ij} \cdot t^{-1} = \frac{t_i}{t_j} \cdot E_{ij} = (\lambda_i - \lambda_j)(t) \cdot E_{ij}$. Hence,

$$\Phi = \{\lambda_i - \lambda_j : 1 \leq i, j \leq n, i \neq j\},$$

and

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{g}_\alpha,$$

where if $\alpha = \lambda_i - \lambda_j$, $\mathfrak{g}_\alpha = \bar{k} \cdot E_{ij}$, and $\mathfrak{h}$ comprised the diagonal matrices with entries in $\bar{k}$. For the action of $\mathfrak{h}$ we find again that the matrices E_{ij} are a basis of eigenvectors: for $t = \mathrm{diag}(t_1, \ldots, t_n) \in \bar{k}^n$, let $\pi_i(t) = t_i$, then $\mathfrak{ad}(t)(E_{ij}) = (\pi_i - \pi_j)(t)E_{ij}$, but where now, as a result of passing from T to its Lie algebra $\mathfrak{h}$, subtraction is really subtraction. That is, $(\pi_i - \pi_j)(t) = t_i - t_j$. From this it is an exercise in matrices to conclude that the Killing form on $\mathfrak{gl}_n$ is $B(x, y) = 2n \cdot \mathrm{Tr}(x \circ y) - 2 \cdot \mathrm{Tr}(x)\mathrm{Tr}(y)$ (where, recall, x, y are $n \times n$ matrices). If $x = \mathrm{diag}(x_1, \ldots, x_n), y = \mathrm{diag}(y_1, \ldots, y_n)$ then

$$B(x, y) = 2n(\sum_i x_i y_i) - 2(\sum x_i)(\sum y_i).$$

The functional $\pi_{ij} := \pi_i - \pi_j$ (or λ_{ij}, if you will) corresponds to the diagonal matrix $T_{ij} = \frac{1}{2n}(E_{ii} - E_{jj})$, and one may now proceed to calculate the inner product on $X^*(T)$.

Choosing the upper diagonal matrices B as a Borel subgroup containing T, we get

$$\mathfrak{b} = \mathrm{Lie}(B) = \left\{ \begin{pmatrix} t_{11} & \cdots & t_{1n} \\ & \ddots & \vdots \\ & & t_{nn} \end{pmatrix} : t_{ij} \in \bar{k} \right\} = \mathrm{Span}(\{E_{ij} : i \leq j\}),$$

and thus the induced order is that $\lambda_i \geq \lambda_j \Leftrightarrow i \leq j$. Use the notation $\lambda_{ij} = \lambda_i - \lambda_j$. We have

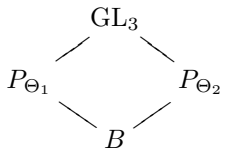
$$\Phi^+ := \{\lambda_{ij} : i < j\} \supseteq \Delta := \{\lambda_{12}, \lambda_{23}, \ldots, \lambda_{n-1,n}\},$$

and Δ are the simple roots.

Note that generally if $\Theta = \emptyset$ then $S_\Theta = T = Z(T)$ and $P = B$, while, on the other extreme, if $\Theta = \Delta$ then S_Θ is a central torus and so $Z(S_\Theta) = G$ and also $P = G$, the maximal parabolic subgroup.

For $n = 2$, these two extremal choices for Θ exhaust all possible choices and we conclude that the standard parabolics are just GL_2 and B; every parabolic subgroup is conjugate to one of those.

For $n = 3$ there are two more choices. First, taking $\Theta_1 = \{\lambda_1 - \lambda_2\}$ we get $S_{\Theta_1} = \{\mathrm{diag}(t_{11}, t_{11}, t_{33})\}$ and $P_{\Theta_1} = \left\{ \left(\begin{array}{c|c} \mathrm{GL}_2 & \begin{smallmatrix} * \\ * \end{smallmatrix} \\ \hline & \mathrm{GL}_1 \end{array} \right) \right\}$. Secondly, taking $\Theta_2 = \{\lambda_2 - \lambda_3\}$ we get $P_{\Theta_2} = \left\{ \left(\begin{array}{c|cc} \mathrm{GL}_1 & * & * \\ \hline & \multicolumn{2}{c}{\mathrm{GL}_2} \end{array} \right) \right\}$. Every parabolic subgroup of GL_3 is conjugate to exactly one of the standard parabolic subgroups $\mathrm{GL}_3, P_{\Theta_1}, P_{\Theta_2}$ and B, whose inclusion relation is



6. Representations and Hilbert's invariants theorem

We discuss briefly the representation theory of a semisimple group G, using weights and the notion of highest vector. Some examples are given in the context

of quadratic forms. We apply the theory to prove Hilbert's theorem about the finite generation of rings of invariant polynomials.

6.1. Representations and weights. Let G be a semisimple group over $\bar{k}$ and fix $T \subseteq B$, a maximal torus and a Borel subgroup of G. Let $\rho\colon G \to \mathrm{GL}(V)$ be a finite dimensional linear representation of G. That is, after fixing a basis for V, we have a homomorphism $\rho\colon G \to \mathrm{GL}_n$, $n = \dim(V)$, that is a homomorphism of algebraic groups. As the elements of T are semisimple, they are mapped to semisimple elements of GL_n and consequently we have a decomposition

$$V = \oplus_{\alpha \in X^*(T)} V_\alpha, \qquad V_\alpha = \{v \in V : \rho(t)v = \alpha(t) \cdot v, \forall t \in T\}.$$

The *weights* of ρ are the set $\{\alpha : V_\alpha \neq 0\}$. The *weight lattice* Λ_w of G is the minimal subgroup of $X^*(T)$ containing all weights of all linear representations of G. On the other hand, the *root lattice* Λ_r of G, is the $\mathbb{Z}$-span of the roots Φ in the group $X^*(T)$; namely, the span of the weights of the adjoint representation of G. Evidently, $\Lambda_w \supseteq \Lambda_r$ and it is a theorem that the index is finite.

Fix an ordering on the roots of G, equivalently, a Weyl chamber $\mathcal{W}$. One of the most fundamental results concerning representations of G is the following: let V be an irreducible representation of G, $\rho\colon G \to \mathrm{GL}(V)$. There exists a unique maximal weight α among the weights of ρ; furthermore, α determines the representation ρ up to isomorphism. Let us use then the notation $V \cong U_\alpha$, where we fix some arbitrary representation U_α of G of highest weight α (in particular, $U_0 = \bar{k}$ is the trivial representation). It is known that the set of α appearing as highest weight vectors is $\Lambda_w \cap \mathcal{W}$. The weights that appear in U_α have the property that they are congruent to α mod Λ_r.

Given any finite dimensional linear representation W of G one can decompose W into an irreducible sum "by hand". For example, starting with a given representation V, we often want to decompose $V^{\otimes n} \otimes (V^*)^{\otimes m}, \wedge^a V, \mathrm{Sym}^a(V)$ and so on, where V^* is the dual vector space on which G acts by $\rho^*(g)$; if we fix a basis for V and take the dual basis for V^* then $\rho^*(g) = {}^t\rho(g)^{-1}$. Find then a maximal weight α_1 appearing in W. Then, as a semisimple group is reductive, $W = U_{\alpha_1} \oplus W'$ for some linear representation W'. We now repeat the process for W'. Of course, as such, it is easier said than done. However, this is indeed quite easy to do in any given case if one has a good method to find all the weights appearing in U_α; that determines the weights of W', without any need to calculate W' itself, and thus one can proceed rather smoothly. There is indeed a rather elegant theory for determining the weights in U_α, but we will not describe it here.

6.1.1. *Example: representations of* SL_2. We have seen that the root system of GL_2 is $\mathbb{Z} \cdot (\lambda_1 - \lambda_2)$. The maximal torus of SL_2 is the sub-torus $S = \{\mathrm{diag}(t, t^{-1}) : t \in \bar{k}^\times\}$ of the maximal torus we have used for GL_2. On this sub-torus we have $(\lambda_1 - \lambda_2)(\mathrm{diag}(t, t^{-1})) = t^2$. If we use $\chi(\mathrm{diag}(t, t^{-1})) = t$ as a basis for the characters of S, we have $X^*(S) = \mathbb{Z} \cdot \chi$ and $\Lambda_r = 2\mathbb{Z} \cdot \chi$. The character 2χ appears as a highest weight vector in the Adjoint representation of SL_2 on its Lie algebra, which is a 3-dimensional vector space, identified with the 2×2-matrices of trace 0. The adjoint representation is irreducible simply because it has a unique positive root, although irreducibility can be check "by hand" too. The roots are $\pm 2\chi$.

Of course, the group SL_2 has an even simpler representation - its action on the two dimensional vector space $V = \bar{k}^2$. The natural basis e_1, e_2 span the weight spaces, $V = \bar{k} \cdot e_1 \oplus \bar{k} \cdot e_2 = V_\chi \oplus V_{-\chi}$. It follows that $[\Lambda_w : \Lambda_r] = 2$ in this

case. Note that $\mathrm{Sym}^2(V)$ is a 3-dimensional space containing the weights $\pm 2\chi, 0$. It follows that $\mathrm{Sym}^2(V)$ is isomorphic to the adjoint representation. $\mathrm{Sym}^3(V)$ is a 4 dimensional representation containing the weights $\pm 3\chi, \pm\chi$, where a basis for the eigenspaces is $\{e_1\otimes e_1\otimes e_1, e_2\otimes e_2\otimes e_2, e_1\otimes e_1\otimes e_2, e_2\otimes e_2\otimes e_1\}$. We know that there is an irreducible sub representation $U_{3\chi}$ containing $e_1\otimes e_1\otimes e_1$ as highest weight vector. Applying $\left(\begin{smallmatrix} & 1\\ -1 & \end{smallmatrix}\right)$ we see that $U_{3\chi}$ also contains $e_2\otimes e_2\otimes e_2$. Applying $\left(\begin{smallmatrix} 1 & \epsilon\\ & 1\end{smallmatrix}\right)$, we see that it contains also $(e_1+\epsilon e_2)\otimes(e_1+\epsilon e_2)\otimes(e_1+\epsilon e_2)$ and thus $\epsilon\cdot e_1\otimes e_1\otimes e_2+\epsilon^2\cdot e_2\otimes e_2\otimes e_1$. Taking $\epsilon\in\{\pm 1\}$ we conclude that $U_{3\chi}=\mathrm{Sym}^3(V)$ and that, in particular, $\mathrm{Sym}^3(V)$ is irreducible. In fact, for every $n\geq 0$, $\mathrm{Sym}^n(V)$ is an irreducible representation of SL_2 and its highest weight is $n\cdot\chi$; conversely, every irreducible representation of SL_2 arises as $\mathrm{Sym}^n(V)$ for a unique n determined by the highest weight (or the dimension of the representation, $\dim(\mathrm{Sym}^n(V))=n+1$); cf. [FH, §11.1].

6.2. Hilbert's invariants theorem. As above, let G be a reductive group and $\rho\colon G\to \mathrm{GL}(V)$ a finite dimensional linear representation. Let M be a $\bar{k}$-vector space, $\mathrm{Sym}(M)=\oplus_{n=0}^{\infty}M^{\otimes n}/J$, where $M^{\otimes 0}:=\bar{k}, M^{\otimes 1}=M$ and in general $M^{\otimes n}=M^{\otimes n-1}\otimes_{\bar{k}}M$; here J is the ideal generated in the non-commutative tensor algebra $\oplus_{n=0}^{\infty}M^{\otimes n}$ by $\{a\otimes b-b\otimes a : a,b\in M\}$. It is thus the minimal ideal we can mod out by to get a commutative $\bar{k}$-algebra. The image of $M^{\otimes a}$ in $\mathrm{Sym}(M)$ is denoted $\mathrm{Sym}^a(M)$.

Consider then symmetric algebra $\mathrm{Sym}(V^*)$. It has a rather concrete interpretation as the ring of polynomial functions on V. Indeed, fix a basis $\{v_1,\dots,v_n\}$ for V; the dual basis $\lambda_1,\dots,\lambda_n$ gives us the linear functions on V

$$\sum_i x_i v_i \overset{\lambda_j}{\mapsto} x_j,\quad j=1,\dots,n.$$

On the other hand, one can show that $\mathrm{Sym}(V^*)$ is nothing but the $\bar{k}$-algebra of finite sums $\{\sum_I a_I\lambda^I : a_I\in\bar{k}\}$, where I is a multi-index $I=(i_1,\dots,i_n)\in\mathbb{N}^n$ and $\lambda^I:=\lambda_1^{i_1}\cdots\lambda_n^{i_n}$. Indeed, there is a natural identification of $\sum_{\{I:|I|:=i_1+\cdots+i_n=a\}}a_I\lambda^I$ with the image of $\mathrm{Sym}^a(V^*)$ in $\mathrm{Sym}(V^*)$. Thus, $\mathrm{Sym}(V^*)\cong\bar{k}[x_1,\dots,x_n]$, the polynomial ring in n variables.

To ease notation, let $R=\mathrm{Sym}(V^*)$. G acts on R linearly by substitutions:

$$(g*f)(v):=f(g^{-1}v),\qquad g\in G, f\in R.$$

The fundamental problem of classical invariant theory is to give a presentation for the $\bar{k}$-algebra R^G - the G-invariant elements of R; that is, to give a presentation of the algebra of G-invariant polynomial functions on V.

Theorem 12 (Hilbert's theorem). *R^G is a finitely-generated $\bar{k}$-algebra.*

The heuristic meaning of this theorem is that there are finitely many "basic invariants" for the group G from which all other invariants can be constructed (in a polynomial fashion). Prior to Hilbert's work this was not known; the setting in which such questions were asked is similar to our following example. Hilbert's theorem did somewhat of a disservice to that area of mathematics. The theorem provides no method to construct such "basic invariants" - this remains a hard problem to this day; yet, the *a priori* knowledge that such are guaranteed to exist took some of the enthusiasm out of the subject for many years.

6.2.1. *Example: binary quadratic forms.* Let $G = \mathrm{SL}_2(\bar{k})$. It acts on vector space symmetric bilinear forms $q = \left(\begin{smallmatrix} a & b \\ b & d \end{smallmatrix}\right)$ over $\bar{k}$ by conjugation; if $g \in G$ then

$$g * q := g\, q\, {}^t g.$$

If we write $q(x, y) = ax^2 + 2bxy + dy^2$ and $g = \left(\begin{smallmatrix} \alpha & \beta \\ \gamma & \delta \end{smallmatrix}\right)$ then the quadratic form $g * q$ is obtained by substituting for x the quantity $\alpha x + \beta y$ and for y the quantity $\gamma x + \delta y$. We note that

$$\det(q) = ad - b^2,$$

which is -4 times the usual discriminant of the form $ax^2 + 2bxy + dy^2$, is invariant under the action of G. At this point, natural questions arise: (i) Is $\det(q)$ the only basic invariant in the sense that every other invariant is a polynomial in $\det(q)$ with $\bar{k}$-coefficients? Is the ring of invariants R^G in this case sufficient to classify (i.e., separate) the orbits for the action of G? Namely, is it the case that two symmetric quadratic forms are equivalent under $\mathrm{SL}_2(\bar{k})$ if and only if they have the same determinant? What is the nature of the map

$$\mathrm{Spec(R)} \to \mathrm{Spec}(R^G),$$

that corresponds to $V \mapsto V/\!\!/G$? In this case classical results in linear algebra answer all these questions. Every quadratic form over a field of characteristic 0 (or just different than 2) can be diagonalized and, furthermore, over an algebraically closed field it can be brought into the form $\mathrm{diag}(0,0), \mathrm{diag}(1,0)$ or $\mathrm{diag}(1,d)$. As $\mathrm{diag}(0,0)$ is in the closure of the orbit of $\mathrm{diag}(1,0)$, we see that the orbits of $\mathrm{diag}(0,0)$ and $\mathrm{diag}(1,0)$ can not be separated by the value of any invariant function. However, the orbits of all the non-zero forms are classified by the determinant. It is then not hard to prove that $R^G = \bar{k}[\det(q)]$ and in particular is a free polynomial ring. We get a morphism

$$V \text{ “}=\text{” } \mathrm{Spec}(R) \to \mathbb{A}^1_{\bar{k}} = \mathrm{Spec}(\bar{k}[t]),$$

corresponding to the ring homomorphism $t \mapsto ad - b^2$. It is a surjective flat morphism whose fibres are the quadratic surfaces $ad - b^2 = t$. The fibres over non-zero points t are non-singular surfaces that are single orbits corresponding to quadratic forms with discriminant t; The fibre over zero is a cone consisting of two orbits; one orbit consists of quadratic forms q whose matrix has rank 1, the other to those of rank 0 (namely, the zero matrix) and is the singular point of the cone.

Pretty much the same considerations apply to the action of $\mathrm{SL}_n(\bar{k})$ on quadratic forms in n-variables. Once more there is only "one" invariant; it is just the determinant of the matrix defining the quadratic form, or, up to a constant, the discriminant of the quadratic form. Let $R = \bar{k}[\{x_{ij} : 1 \le i, j \le n\}]/(\{x_{ij} - x_{ji}\})$. The morphism

$$\mathrm{Spec}(R) \to \mathbb{A}^1_{\bar{k}}$$

is flat has a fibre over d that consist of a single orbit - the forms of discriminant d - if $d \neq 0$. While the fibre over 0 consists of n-orbits, each of which corresponds to degenerate quadratic forms of a given rank. In any case, the fibre is a degree n surface in $\mathbb{A}^{n(n+1)/2}_{\bar{k}}$.

When V is replaced by an arbitrary variety (or even a scheme) and G is a general reductive group (scheme), the study of the quotient $V \to V/\!\!/G$ (including its precise definition) is the subject of geometric invariant theory. We have the following fundamental result:

Theorem 13 (Chevalley-Iwahori-Nagata, cf. [DC]). *For any action of a reductive group G on an affine algebraic variety $V = \mathrm{Spec}(A)$, the fibres of $V \to V^G := \mathrm{Spec}(A^G)$ are union of orbits of G; the set of orbits always surjects onto V^G. We have a bijection between the set of orbits and the points of V^G if and only if each orbit is Zariski closed.*

Remark: It is rather clear from the definitions that the fibres are unions of orbits and that every fibre is a closed set (remember that we doing classical algebraic geometry, where points means $\bar{k}$-points). The difficult parts are to show that every point of V^G is obtained as the image of an orbit and that if an orbit is closed then there are "enough invariant functions" to separate it from other orbits.

Going back to our example, we see that the fibres over $d \neq 0$ are the closed Zariski sets of quadratic forms of discriminant d, while the fibre over 0 is a union of orbits $C_0, \ldots, C_{n-1}$, one for every rank less than n, and in fact the Zariski closure of C_r is $C_0 \cup C_1 \cup \cdots \cup C_r$.

The study of geometric invariant theory in great generality was carried out by D. Mumford in [Mum] in 1965, in a work that had revolutionized the subject.

We now turn to the proof of Hilbert's theorem, following [GW, §5.1.1]. We write

$$R = \mathrm{Sym}(V^*) = \bigoplus_{d \geq 0} \mathrm{Sym}^d(V^*),$$

where $\mathrm{Sym}^d(V^*)$ can be thought of as homogenous polynomials of degree d. Note that $\mathrm{Sym}^d(V^*)$ is a finite dimensional space preserved by the action of G. Since G is reductive, we can decompose $\mathrm{Sym}^d(V^*)$ into a sum of irreducible representations of G. Letting d vary now, we can collect like linear representations. That is, we have two decompositions:

$$R = \bigoplus_{d \geq 0} R[d], \quad R = \bigoplus_{\alpha \in \Lambda_r} R_\alpha,$$

where $R[d] = \mathrm{Sym}^d(V^*)$ and R_α is the isotypical component of R type α. That is, R_α is the sum of all irreducible sub representations of $\mathrm{Sym}(V^*)$ that are isomorphic to U_α, in the notation of §6.1. Note that these decompositions are compatible in the sense that

$$R[d] = \oplus_\alpha (R[d] \cap R_\alpha), \quad R_\alpha = \oplus_d (R[d] \cap R_\alpha).$$

In particular, if $f \in R_\alpha$ then f can be written as a sum of homogenous polynomials each of which lies in R_α. Therefore, taking a polynomial $f \in R$, we may write

$$f = \sum_\alpha f_\alpha, \quad f_\alpha \in R_\alpha, \tag{4}$$

where each f_α is a sum of homogenous polynomials lying in R_α; furthermore, if f itself is homogenous of degree d then each f_α is homogenous of degree d.

We define the *Raynolds operator* $f \mapsto f^\natural$, where $f^\natural$ is the trivial representation component in the decomposition (4); if you wish, using previous notation, we can also say that $f^\natural = f_0 \in U_0$. This operator is clearly $\bar{k}$-linear map. Its crucial property is the following.

Lemma 14. *The Raynolds operator satisfies*

$$(\varphi f)^\natural = \varphi f^\natural, \qquad \forall \varphi \in R^G.$$

That is, $f \mapsto f^\natural$ is a homomorphism of R^G-modules.

PROOF. Using linearity, it is enough to prove the lemma for $f \in R[d]_\alpha$ and it is therefore enough to show that multiplication by φ preserves $R[d]_\alpha$. We have an isomorphism $\bar{k} \cdot \varphi \otimes_{\bar{k}} R[d]_\alpha \cong \varphi \cdot R[d]_\alpha$ by $\varphi \otimes f \mapsto \varphi \cdot f$. This is easily checked to be an isomorphism of G-modules: $g * (\varphi \otimes f) = \varphi \otimes (g * f)$ which is mapped to the function $v \mapsto \varphi(v) \cdot f(g^{-1}v)$. As $\varphi(v) \cdot f(g^{-1}v) = \varphi(g^{-1}v) \cdot f(g^{-1}v) = (\varphi f)(g^{-1}v) = (g*(\varphi f))(v)$, the equivariance of the map follows. But, $\bar{k} \cdot \varphi \otimes_{\bar{k}} R[d]_\alpha \cong \bar{k} \otimes_{\bar{k}} R[d]_\alpha = R[d]_\alpha$ as G-modules and so is clearly of type α □

Let $R^G_+ = \sum_{d>0} R[d]^G$ and consider the ideal $R \cdot R^G_+$ of R. R is a polynomial ring in finitely many variables over $\bar{k}$. Thus, by Hilbert's basis theorem, the ideal $R \cdot R^G_+$ is finitely generated. Thus, there are $f_1, \ldots, f_N \in R^G_+$ such that $R \cdot R^G_+ = \langle f_1, \ldots, f_N \rangle_R$ and, as we may replace each f_i by the set of its homogenous parts, we may assume each f_i is homogenous of some positive degree. We show that $R^G = \bar{k}[f_1, \ldots, f_N]$.

Let $\varphi \in R^G$. To show $\varphi \in \bar{k}[f_1, \ldots, f_N]$ we may assume that φ is homogenous, and we argue by induction on its degree; the case of degree 0 being obvious. Now, write $\varphi = \sum_i a_i f_i$, $a_i \in R$. By homogeneity, we may assume that each a_i is homogenous and $\deg(a_i f_i) = \deg(\varphi)$. Then $\varphi = \varphi^\natural = \sum_i a_i^\natural f_i$. We may replace $a_i^\natural$ by their suitable homogenous part so that still $\varphi = \sum_i a_i^\natural f_i$ and now, if $a_i^\natural \neq 0$, $\deg(a_i^\natural f_i) = \deg(\varphi)$. However, this implies that for all i, either $a_i^\natural = 0$ or $\deg(a_i^\natural) < \deg(\varphi)$. Thus, by the induction hypothesis, for all i, $a_i^\natural \in \bar{k}[f_1, \ldots, f_N]$ and so is φ. This completes the proof of the theorem.

Acknowledgement. I would like to thank Dylan Attwell-Duval and Andrew Fiori for their helpful comments.

Bibliography

[Bor1] Borel, Armand: Linear algebraic groups. 1966 Algebraic Groups and Discontinuous Subgroups (Proc. Sympos. Pure Math., Boulder, Colo., 1965) pp. 3-19 Amer. Math. Soc., Providence, R.I.

[Bor2] Borel, Armand: Linear algebraic groups. Second edition. Graduate Texts in Mathematics, 126. Springer-Verlag, New York, 1991.

[DMOS] Deligne, Pierre; Milne, James S.; Ogus, Arthur; Shih, Kuang-yen: Hodge cycles, motives, and Shimura varieties. Lecture Notes in Mathematics, 900. Springer-Verlag, Berlin-New York, 1982.

[DC] Dieudonné, Jean A.; Carrell, James B.: Invariant theory, old and new. Advances in Math. 4, 1-80 (1970).

[FH] Fulton, William; Harris, Joe: Representation theory. A first course. Graduate Texts in Mathematics, 129. Springer-Verlag, New York, 1991.

[GW] Goodman, Roe; Wallach, Nolan R.: Symmetry, representations, and invariants. Graduate Texts in Mathematics, 255. Springer, Dordrecht, 2009.

[Har] Hartshorne, Robin: Algebraic geometry. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[Hum1] Humphreys, James E.: Linear algebraic groups. Graduate Texts in Mathematics, No. 21. Springer-Verlag, New York-Heidelberg, 1975.

[Hum2] Humphreys, James E.: Introduction to Lie algebras and representation theory. Second printing, revised. Graduate Texts in Mathematics, 9. Springer-Verlag, New York-Berlin, 1978.

[Koh] Kohls, Martin: A user friendly proof of Nagata's characterization of linearly reductive groups in positive characteristics. Linear Multilinear Algebra 59 (2011), no. 3, 271–278.

[Mum] Mumford, D.; Fogarty, J.; Kirwan, F.: Geometric invariant theory. Third edition. Ergebnisse der Mathematik und ihrer Grenzgebiete (2), 34. Springer-Verlag, Berlin, 1994.

[OV] Onishchik, A. L.; Vinberg, E. B.: Lie groups and algebraic groups. Translated from the Russian and with a preface by D. A. Leites. Springer Series in Soviet Mathematics. Springer-Verlag, Berlin, 1990.

[Ser1] Serre, Jean-Pierre: Local fields. Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979.

[Ser2] Serre, Jean-Pierre: Galois cohomology. Corrected reprint of the 1997 English edition. Springer Monographs in Mathematics. Springer-Verlag, Berlin, 2002.

[Spr] Springer, T. A.: Linear algebraic groups. Reprint of the 1998 second edition. Modern Birkhuser Classics. Birkhuser Boston, Inc., Boston, MA, 2009.

[Wat] Waterhouse, William C.: Introduction to affine group schemes. Graduate Texts in Mathematics, 66. Springer-Verlag, New York-Berlin, 1979.