

ALGEBRAIC GROUPS, LIE ALGEBRAS, AND THEIR REPRESENTATIONS

1. ALGEBRAIC GROUPS

1.1. Recap of bits of Algebraic geometry. Let \mathbb{F} be an algebraically closed field.

- Definition 1.1.**
- (1) By an *embedded affine variety*, we mean a subset $X \subset \mathbb{A}^n$ for some n , defined by polynomial equations.
 - (2) Let $X \subset \mathbb{A}^m$ and $Y \subset \mathbb{A}^n$ be embedded affine varieties. A map $\varphi : X \rightarrow Y$ is called *polynomial* (a.k.a. a morphism) if it is a restriction of a map $\mathbb{A}^m \rightarrow \mathbb{A}^n$ given by polynomials.
 - (3) The *algebra of polynomial functions*, $\mathbb{F}[X]$, by definition, consists of all polynomial maps $X \rightarrow \mathbb{A}^1$ with the usual addition and multiplication of functions.

Now we list a few standard facts.

- (i) Let A be a commutative \mathbb{F} -algebra, and let $I \subset A$ be an ideal. Recall that the *radical* of I , denoted by \sqrt{I} , by definition, consists of all $a \in A$ such that $a^n \in I$ for some n . This is also an ideal. We say that I is *radical* if $I = \sqrt{I}$. For every subset $X \subset \mathbb{A}^n$, the subset $I_X := \{f \in \mathbb{F}[x_1, \dots, x_n] \mid f(x) = 0 \text{ for all } x \in X\}$ is a radical ideal in $\mathbb{F}[x_1, \dots, x_n]$. Hilbert's Nullstellensatz implies that the assignment $X \mapsto I_X$ gives a bijection between the embedded affine varieties in \mathbb{A}^n and the radical ideals of $\mathbb{F}[x_1, \dots, x_n]$. Moreover, $\mathbb{F}[X] \cong \mathbb{F}[x_1, \dots, x_n]/I_X$. It is a finitely generated \mathbb{F} -algebra with a distinguished collection of generators $x_i \in \mathbb{F}[X]$ for $i = 1, \dots, n$. Since I_X is radical, the algebra $\mathbb{F}[X]$ contains no nonzero nilpotent elements.
- (ii) Let $\varphi : X \rightarrow Y$ be a morphism and let $f \in \mathbb{F}[Y]$. Define a function $\varphi^*(f) = f \circ \varphi : X \rightarrow \mathbb{F}$. This function is polynomial, hence an element of $\mathbb{F}[X]$. We get a homomorphism $\varphi^* : \mathbb{F}[Y] \rightarrow \mathbb{F}[X]$. The assignment $\varphi \mapsto \varphi^*$ defines a bijection between morphisms $X \rightarrow Y$ and algebra homomorphisms $\mathbb{F}[Y] \rightarrow \mathbb{F}[X]$. Moreover, this assignment is functorial: if $\varphi : X \rightarrow Y$ and $\psi : Y \rightarrow Z$ are morphisms, then $(\psi \circ \varphi)^* = \varphi^* \circ \psi^*$.
- (iii) (ii) allows us to talk about abstract affine varieties X . They correspond to finitely generated \mathbb{F} -algebras with no nilpotent elements. The choice of generators corresponds to an embedding of X into some \mathbb{A}^n , but we view X irrespective of an embedding. The notion of a morphism still makes sense in this setting.

Here are two useful constructions:

- (a) Let X be an affine variety. If $f \in \mathbb{F}[X]$, then $X_f = \{x \in X \mid f(x) \neq 0\}$ is an affine variety with $\mathbb{F}[X_f] \cong \mathbb{F}[X][f^{-1}]$.
- (b) Let X, Y be affine varieties. Then $X \times Y$ is also an affine variety with $\mathbb{F}[X \times Y] \cong \mathbb{F}[X] \otimes_{\mathbb{F}} \mathbb{F}[Y]$. Namely, if $f : X \rightarrow \mathbb{A}^1$ and $g : Y \rightarrow \mathbb{A}^1$ are polynomial maps, then $f \otimes g : X \times Y \rightarrow \mathbb{A}^1$ defined by $(f \otimes g)(x, y) = f(x)g(y)$ is also a polynomial map.

Remark 1.2. Subsets in an affine variety X defined by polynomial equations are called *Zariski closed*; they are indeed closed subsets in a topology called the *Zariski topology*. A subset in X is called *Zariski open* if its complement is Zariski closed. Note that a Zariski

closed subset, say Y , of X is again an affine variety (this may fail for open subvarieties). For a closed subvariety $Y \subset X$, the homomorphism $\mathbb{F}[X] \rightarrow \mathbb{F}[Y]$ corresponding to the inclusion $Y \subseteq X$ is surjective.

1.2. Definition and examples of algebraic groups. Consider the group $\mathrm{GL}_n(\mathbb{F})$ of all non-degenerate $n \times n$ matrices with coefficients in \mathbb{F} . Relatedly, if V is an n -dimensional vector space over \mathbb{F} , then we can talk about the group $\mathrm{GL}(V)$ of all invertible linear operators $V \rightarrow V$. Choosing a basis in V identifies $\mathrm{GL}(V)$ with $\mathrm{GL}_n(\mathbb{F})$. Note that $\mathrm{GL}_n(\mathbb{F}) = \{A \in \mathrm{Mat}_{n \times n}(\mathbb{F}) \mid \det(A) \neq 0\}$ is an affine variety with $\mathbb{F}[\mathrm{GL}_n(\mathbb{F})] = \mathbb{F}[x_{ij}, \det(x_{ij})^{-1}]$, where x_{ij} for $i, j = 1, \dots, n$ are the matrix coefficients.

Definition 1.3. By an *algebraic group*, we mean a subgroup $G \subseteq \mathrm{GL}_n(\mathbb{F})$ that is Zariski closed (see Remark 1.2), i.e., given by polynomial equations.

Example 1.4. (1) $\mathrm{SL}_n(\mathbb{F}) = \{A \in \mathrm{GL}_n(\mathbb{F}) \mid \det(A) = 1\}$ is the *special linear group*.

- (2) Assume $\mathrm{char}(\mathbb{F}) \neq 2$. Set $\mathrm{O}_n(\mathbb{F}) = \{A \in \mathrm{GL}_n(\mathbb{F}) \mid A^T A = I\}$, here the superscript “ T ” stands for the matrix transpose and I is the identity matrix. More conceptually, let B be a non-degenerate symmetric form on a vector space V of dimension n (all such forms have an orthonormal basis, so there is no real difference between them). Then we can consider

$$\mathrm{O}(V, B) = \{g \in \mathrm{GL}(V) \mid B(gu, gv) = B(u, v), \forall u, v \in V\}.$$

A choice of an orthonormal basis for B identifies $\mathrm{O}(V, B)$ with $\mathrm{O}_n(\mathbb{F})$. The group $\mathrm{O}_n(\mathbb{F})$ is called the *orthogonal group*. Note that $\mathrm{SO}_n(\mathbb{F}) = \{A \in \mathrm{O}_n(\mathbb{F}) \mid \det(A) = 1\}$ is also an algebraic group, the *special orthogonal group*.

- (3) Similarly, for a non-degenerate skew-symmetric form ω on a finite-dimensional vector space V , where automatically $\dim(V)$ is even, we can consider the *symplectic group*

$$\mathrm{Sp}(V, \omega) = \{g \in \mathrm{GL}(V) \mid \omega(gu, gv) = \omega(u, v) \forall u, v \in V\}.$$

One can find a basis v_1, \dots, v_{2n} of V such that $\omega(e_i, e_j) = \delta_{i, 2n-j+1}$. Let J be the matrix of ω in this basis. Then $\mathrm{Sp}(V, \omega)$ gets identified with $\{A \in \mathrm{GL}_{2n}(\mathbb{F}) \mid A^T JA = J\}$.

- (4) The subgroups of upper triangular, upper uni-triangular (with 1's on the diagonal), and diagonal matrices in $\mathrm{GL}_n(\mathbb{F})$ are algebraic.
(5) The *multiplicative group* $\mathbb{G}_m = \mathrm{GL}_1(\mathbb{F})$ and the *additive group* $\mathbb{G}_a = (\mathbb{F}, +)$ are algebraic. Note that the former can be thought of as $\mathrm{GL}_1(\mathbb{F})$, while the latter is identified with the subgroup of upper uni-triangular matrices in $\mathrm{GL}_2(\mathbb{F})$.

The groups in Examples (1)-(3) are called the *classical groups*. They are extremely important.

Exercise 1.5. If G_1 and G_2 are algebraic groups, then so is their product. Hint: $\mathrm{GL}_n(\mathbb{F}) \times \mathrm{GL}_m(\mathbb{F})$ embeds into $\mathrm{GL}_{n+m}(\mathbb{F})$ as the subgroup of block diagonal matrices).

Note that every algebraic group G is Zariski closed in an affine variety $\mathrm{GL}_n(\mathbb{F})$, hence is an affine variety itself. Moreover, the multiplication map $\mathrm{GL}_n(\mathbb{F}) \times \mathrm{GL}_n(\mathbb{F}) \rightarrow \mathrm{GL}_n(\mathbb{F})$ and the inversion map $\mathrm{GL}_n(\mathbb{F}) \rightarrow \mathrm{GL}_n(\mathbb{F})$ are given by polynomials in the matrix coefficients and \det^{-1} (the latter is only needed for the inversion). Hence they are morphisms. So, we can give a more conceptual definition of an algebraic group.

Definition 1.6. By an (affine) algebraic group we mean a group G equipped with an affine variety structure such that the multiplication map $G \times G \rightarrow G$ and the inversion map $G \rightarrow G$ are morphisms.

In fact, this definition is equivalent to Definition 1.3, see [OV, §3.1.6, Theorem 8].

Remark 1.7. Definition 1.6 is parallel to the definition of a Lie group: we replace C^∞ -manifolds there with affine algebraic varieties. In fact, every algebraic group over \mathbb{C} is a complex analytic Lie group, see Remark 2.11.

Note also that we can drop the condition of being affine from the definition of an algebraic group getting a broader class of groups (including, for example, abelian varieties). However, from the group and representation theory perspective affine algebraic groups are still the most interesting. In fact, the Chevalley structure theorem states that every algebraic group in the general sense contains a unique maximal normal affine algebraic subgroup and the quotient is an abelian variety, [BSU, Theorem 1.1.1]. In particular, the derived subgroup of any algebraic group is affine.

1.3. Homomorphisms and Representations.

Definition 1.8. Let G and H be algebraic groups. By an (algebraic group) *homomorphism* $G \rightarrow H$, we mean a group homomorphism that is also a morphism of varieties.

Let V be a finite-dimensional vector space. By a *rational representation* of G in V we mean an algebraic group homomorphism $G \rightarrow \mathrm{GL}(V)$. We will elaborate on why the term “rational” is used later. In other words, a rational representation of G is one whose matrix coefficients in $\mathbb{F}[G]$.

Example 1.9.

- (i) The groups $\mathrm{GL}_n(\mathbb{F})$, $\mathrm{SL}_n(\mathbb{F})$, $O_n(\mathbb{F})$, and $\mathrm{Sp}_{2m}(\mathbb{F})$ (for even n in the last case) are embedded into $\mathrm{GL}_n(F)$, hence come with a rational representation in $V = \mathbb{F}^n$, called the *tautological representation*.
- (ii) If V is a rational representation of G , then so are its subrepresentations and quotient representations. (This is left as an exercise; look at the matrix coefficients.)
- (iii) If V and W are rational representations of G , then so are $V \oplus W$, $V \otimes W$ and $\mathrm{Hom}(V, W)$ (exercise).

Example 1.10. Suppose $\mathrm{char}(\mathbb{F}) = p > 0$. In this case, the map $x \mapsto x^p$ is an automorphism of \mathbb{F} (recall that we assume \mathbb{F} to be algebraically closed) called the *Frobenius automorphism*. The map $\mathrm{Fr} : \mathrm{GL}_n(\mathbb{F}) \rightarrow \mathrm{GL}_n(\mathbb{F})$, defined by applying $x \mapsto x^p$ to the entries of a matrix, is therefore an algebraic group homomorphism. It’s an automorphism of an abstract group but not of an algebraic group, as $x \mapsto x^{1/p}$ is not a polynomial.

Now let $G \subset \mathrm{GL}_n(\mathbb{F})$ be defined by polynomials with coefficients in \mathbb{F}_p and not just in \mathbb{F} . For example, this is the case for the groups in (1)-(4) of Example 1.4. Then Fr restricts to G , giving us the *Frobenius homomorphism* $\mathrm{Fr} : G \rightarrow G$. Again, this is an abstract group automorphism, but not an algebraic group automorphism.

Remark 1.11. For the group $\mathrm{GL}_n(\mathbb{F})$, a representation being rational means its matrix coefficients are polynomials in the matrix entries x_{ij} and \det^{-1} , a special class of rational functions on G , hence the name. One also considers *polynomial representations*, where the matrix coefficients are polynomials just in the x_{ij} ’s. For example, the tautological representation, its tensor powers, etc., are polynomial, while its dual is not polynomial.

1.4. Big picture and connections. As part of the general ideology, we care about the structure and representation theory of simple algebraic groups and their relatives (semisimple and reductive groups). The reason is two-fold: these theories are extremely rich and interesting, and appear in numerous areas of Mathematics, from Differential geometry to Combinatorics to Number theory. Here's the definition of a simple group in the algebraic context.

Definition 1.12. An algebraic group G is *simple* if the following conditions hold:

- G is connected in the Zariski topology,
- all normal algebraic subgroups of G are finite,
- and G is not commutative.

Example 1.13. The groups $\mathrm{SL}_n(\mathbb{F})$ for $n \geq 2$, $\mathrm{SO}_n(\mathbb{F})$ for $n \geq 3$, and $\mathrm{Sp}_{2n}(\mathbb{F})$ for $n \geq 1$ are simple. In a way, there are just five more examples, the exceptional groups G_2 , F_4 , E_6 , E_7 , and E_8 . We'll discuss more on this later.

Simple algebraic groups give the most important kind of symmetry in Mathematics. They are also the most central object in representation theory. Most things considered in Representation theory are related to simple algebraic groups in one way or another. For example, S_n appears in at least three ways when we study $\mathrm{SL}_n(\mathbb{K})$ (for a suitable field \mathbb{K}) and its representations.

One manifestation of this central role is a connection to finite simple groups. Let G be a simple algebraic group over $\mathbb{F} := \overline{\mathbb{F}}_p$. As in Example 1.4, G embeds into some $\mathrm{GL}_n(\mathbb{F})$ as a subgroup defined by polynomial equations with coefficients in \mathbb{F}_p . So by Example 1.10, we get the Frobenius endomorphism $\mathrm{Fr} : G \rightarrow G$. Pick $k \geq 1$ and set $\Phi = \mathrm{Fr}^k$. Let $G(\mathbb{F}_{p^k})$ be the fixed point group. Note that $\mathrm{GL}_n(\mathbb{F})^\Phi = \mathrm{GL}_n(\mathbb{F}_{p^k})$ because Φ acts entry-wise. In particular, $G(\mathbb{F}_{p^k})$ is a finite group (e.g., for $G = \mathrm{SL}_n(\mathbb{F})$, we get $G^\Phi = \mathrm{SL}_n(\mathbb{F}_{p^k})$).

The groups G^Φ are “almost simple”: we can produce finite simple groups out of them. This construction can be generalized; one can replace Fr^k with its twisted versions. In fact, most finite simple groups are produced this way.

2. LIE ALGEBRAS OF ALGEBRAIC GROUPS

Algebraic (or Lie) groups are defined by nonlinear equations, so are nonlinear objects. A basic paradigm to study such objects is to linearize them. In the context of Lie groups, this was applied already by Sophus Lie leading to the notion of Lie algebras. If the base field has characteristic 0, the study of the structure and representation theory of algebraic groups reduces (to a large extent) to these for the Lie algebras. In characteristic p , the representations of algebraic groups and of their Lie algebras are still related, but the relation is more subtle.

2.1. Tangent spaces. Let \mathbb{F} be an algebraically closed field and X be an affine algebraic variety. Recall that we write $\mathbb{F}[X]$ for the algebra of polynomial functions on X . Pick $\alpha \in X$.

Definition 2.1. An α -derivation of $\mathbb{F}[X]$ is an \mathbb{F} -linear map $\delta : \mathbb{F}[X] \rightarrow \mathbb{F}$ satisfying the following version of Leibniz identity:

$$\delta(fg) = f(\alpha)\delta(g) + g(\alpha)\delta(f).$$

Note that the α -derivations form a vector subspace in the space $\mathbb{F}[X]^*$ of all linear functions $\mathbb{F}[X] \rightarrow \mathbb{F}$. The space of α -derivations is denoted by $T_\alpha X$ and is called the *tangent space* of X at α .

Exercise 2.2. Let $\alpha \in X$, and $\mathfrak{m}_\alpha \subset \mathbb{F}[X]$ denote the maximal ideal of α . Show that every α -derivation vanishes on 1 and on \mathfrak{m}_α^2 defining a linear map $T_\alpha X \rightarrow (\mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2)^*$. Further, show that this map is an isomorphism.

Now let Y be another affine variety and $\varphi : X \rightarrow Y$ be a morphism giving the pullback algebra homomorphism $\varphi^* : \mathbb{F}[Y] \rightarrow \mathbb{F}[X]$.

Exercise 2.3. If δ is an α -derivation for $\alpha \in X$, then $\delta \circ \varphi^* : \mathbb{F}[Y] \rightarrow \mathbb{F}$ is a $\varphi(\alpha)$ -derivation. The map $\delta \mapsto \delta \circ \varphi^*$ is a linear map $T_\alpha X \rightarrow T_{\varphi(\alpha)} Y$.

Definition 2.4. The map $\delta \mapsto \delta \circ \varphi^*$ is called the *tangent map* of φ at α and is denoted by $T_\alpha \varphi$.

Example 2.5. Suppose first $X = \mathbb{A}^n$ so that $\mathbb{F}[X] = \mathbb{F}[x_1, \dots, x_n]$. Then an α -derivation δ is uniquely determined by its values on x_1, \dots, x_n yielding an isomorphism $T_\alpha X \xrightarrow{\sim} \mathbb{F}^n$, $\delta \mapsto (\delta(x_1), \dots, \delta(x_n))$.

More generally, take an arbitrary affine variety X and embed X into some \mathbb{A}^n , let ι denote the embedding. Let f_1, \dots, f_m denote generators of the ideal $\ker \iota^*$, they give equations defining X inside \mathbb{A}^n . Since $\iota^* : \mathbb{F}[x_1, \dots, x_n] \rightarrow \mathbb{F}[X]$ is surjective, $T_\alpha \iota$ is injective for all $\alpha \in X$ and identifies $T_\alpha X$ with

$$\{\delta \in T_\alpha \mathbb{A}^n \mid \delta(f_i) = 0, \forall i = 1, \dots, m\} = \{(a_1, \dots, a_n) \in \mathbb{F}^n \mid \sum_{j=1}^n a_n \frac{\partial f_i}{\partial x_j}(\alpha) = 0, \forall i = 1, \dots, m\}.$$

Exercise 2.6. Let X, Y be affine varieties, and $\alpha \in X, \beta \in Y$. Let π^X, π^Y denote the projections from $X \times Y$ to X and Y , respectively. Show that $(d_\alpha \pi^X, d_\beta \pi^Y)$ is an isomorphism $T_{(\alpha, \beta)}(X \times Y) \rightarrow T_\alpha X \oplus T_\beta Y$ (hint: use the identification $\mathbb{F}[X \times Y] \cong \mathbb{F}[X] \otimes \mathbb{F}[Y]$).

Exercise 2.7. Let ι be a closed embedding $Y \hookrightarrow X$ of affine varieties. Then $d_y \iota : T_y Y \rightarrow T_{\iota(y)} X$ is injective.

Now we discuss smooth points of varieties. Let X be an affine variety and $\alpha \in X$. Let \mathfrak{m}_α denote the maximal ideal of α in $\mathbb{F}[X]$. Note that the multiplication on $\mathbb{F}[X]$ gives rise to a linear map

$$(1) \quad S^k(\mathfrak{m}_\alpha/\mathfrak{m}_\alpha^2) \rightarrow \mathfrak{m}_\alpha^k/\mathfrak{m}_\alpha^{k+1}$$

The following definition follows [D, §1.7.4]. It has an advantage of being self-contained and not referring to the dimensions (it is equivalent to the usual definition, see [D, §2.4.7]).

Definition 2.8. We say that α is a *smooth point* of X if (1) is an isomorphism for each k .

We will need the following result from [D, §2.4.7].

Theorem 2.9. Let X be an affine algebraic variety. The locus of smooth points in X is open and dense with respect to the Zariski topology.

Exercise 2.10. Every algebraic group is smooth as a variety meaning that every point is smooth (hints: every variety has a smooth point and the action of G on itself is by variety automorphisms).

Remark 2.11. It follows that every algebraic group over \mathbb{C} is also a complex analytic Lie group.

2.2. Examples for algebraic groups. We want to compute the spaces $T_1 G$ for the classical groups G , i.e., $G = \mathrm{GL}_n(\mathbb{F})$, $\mathrm{SL}_n(\mathbb{F})$, $\mathrm{O}_n(\mathbb{F})$, $\mathrm{Sp}_n(\mathbb{F})$ (in the latter case n is even). Here and below we write 1 for the unit element in G .

Example 2.12. Let $G = \mathrm{GL}_n(\mathbb{F})$. We claim that $T_1 G$ is identified with $\mathrm{Mat}_n(\mathbb{F})$. First, suppose X is a general affine variety, $f \in \mathbb{F}[X]$, and $\alpha \in X_f$. We observe that $T_\alpha(X_f)$ is identified with $T_\alpha X$ via the $T_\alpha \iota$, where $\iota : X_f \hookrightarrow X$ is the inclusion. Apply this to $X = \mathrm{Mat}_n(\mathbb{F})$ and $f = \det$ to get $T_1 \mathrm{GL}_n(\mathbb{F}) \xrightarrow{\sim} T_1 \mathrm{Mat}_n(\mathbb{F})$. The latter is identified with $\mathrm{Mat}_n(\mathbb{F})$. One commonly uses the notation $\mathfrak{gl}_n(\mathbb{F})$ for $T_1 \mathrm{GL}_n(\mathbb{F})$.

To handle the other three classical groups, $G = \mathrm{SL}_n(\mathbb{F})$, $\mathrm{O}_n(\mathbb{F})$, $\mathrm{Sp}_n(\mathbb{F})$, we first observe that all of them are Zariski closed in $\mathrm{GL}_n(\mathbb{F})$. As in Example 2.5, this allows to identify $T_1 G$ with a subspace in $\mathfrak{gl}_n(\mathbb{F})$. To describe these subspaces, we will need the following version of the regular value theorem.

Fact 2.13. Let U be an affine variety that is open in some \mathbb{F}^m , and $\varphi : U \rightarrow \mathbb{F}^k$ be a morphism. Let $\alpha \in U$ be such that $T_\alpha \varphi : T_\alpha U \rightarrow T_{\varphi(\alpha)} \mathbb{F}^k$ is surjective. Then $T_\alpha \varphi^{-1}(\varphi(\alpha)) = \ker T_\alpha \Phi$.

We do not provide a proof, see [H2, Sec. 5.5] for a related statement.

We will apply this to $U = \mathrm{GL}_n(\mathbb{F})$. In all cases we care about, $G = \varphi^{-1}(\beta)$ for suitable $\varphi : U \rightarrow \mathbb{F}^k$, $\beta \in \mathbb{F}^k$.

Example 2.14. Let $\varphi : \mathrm{GL}_n(\mathbb{F}) \rightarrow \mathbb{G}_m$ be given by $g \mapsto \det(g)$. For $\xi \in T_1 \mathrm{GL}_n(\mathbb{F}) = \mathfrak{gl}_n(\mathbb{F})$, we have $T_1 \varphi(\xi) = \mathrm{tr}(\xi)$ (we just formally differentiate $\det(1 + s\xi)$ at $s = 0$). The map $\mathrm{tr} : \mathfrak{gl}_n(\mathbb{F}) \rightarrow \mathbb{F}$ is surjective. From Fact 2.13 we conclude $T_1 G = \ker \mathrm{tr}$, the subspace of matrices with trace 0 usually denoted by $\mathfrak{sl}_n(\mathbb{F})$.

Example 2.15. Assume $\mathrm{char} \mathbb{F} \neq 2$. Set $G := \mathrm{O}_n(\mathbb{F})$. Let $Y \subset \mathrm{Mat}_n(\mathbb{F})$ be the subspace of all symmetric matrices. Consider the morphism $\varphi : \mathrm{GL}_n(\mathbb{F}) \rightarrow Y$, $g \mapsto gg^T$, so that $G = \varphi^{-1}(1)$. We have $T_1 \varphi(\xi) = \xi + \xi^T$, this is a surjective map $\mathfrak{gl}_n(\mathbb{F}) \rightarrow Y$. So, $T_1 G = \ker T_1(\varphi)$. This is the space of skew-symmetric matrices, commonly denoted by $\mathfrak{so}_n(\mathbb{F})$.

We also could (and should) view this subspace basis-free, in the notation of Example 1.4, dealing with $\mathrm{O}(V, B)$ instead of $\mathrm{O}_n(\mathbb{F})$. We get

$$T_1 \mathrm{O}(V, B) = \{\xi \in \mathfrak{gl}(V) \mid B(\xi u, v) + B(u, \xi v) = 0, \forall u, v \in V\}.$$

This subspace is denoted by $\mathfrak{so}(V, B)$ (or just $\mathfrak{so}(V)$ when B is understood).

Exercise 2.16. $T_1 \mathrm{Sp}(V, \beta) = \{\xi \in \mathfrak{gl}(V) \mid \omega(\xi u, v) + \omega(u, \xi v) = 0, \forall u, v \in V\}$. This subspace is usually denoted by $\mathfrak{sp}(V, \omega)$ (or just $\mathfrak{sp}(V)$).

2.3. Bracket on the Tangent Space at 1 of an Algebraic Group. One can ask how the group structure on an algebraic group G reflects upon the tangent spaces $T_\alpha G$. A natural candidate to carry an additional structure is $T_1 G$, where we write 1 for the identity element of G . At the first glance, the group structure does not equip $T_1 G$ with any additional structure, as evidenced by the following exercise.

Exercise 2.17. Let $m : G \times G \rightarrow G$ denote the multiplication map, and $i : G \rightarrow G$ be the inversion map. Show that

- (1) Under the identification of $T_{(1,1)}(G \times G)$ with $T_1 G \oplus T_1 G$, see Exercise 2.6, we have $d_1 m(\xi_1, \xi_2) = \xi_1 + \xi_2$.
- (2) We have $d_1 i(\xi) = -\xi$.

Hint: handle the case $G = \mathrm{GL}_n(\mathbb{F})$ first; in the general case, embed G into some $\mathrm{GL}_n(\mathbb{F})$.

Nevertheless, $T_1 G$ does come with a well-defined additional bilinear operation, usually denoted by $[\cdot, \cdot]$. For $\xi, \eta \in \mathfrak{gl}_n(\mathbb{F})$, let $[\xi, \eta]$ denote the matrix commutator $\xi\eta - \eta\xi$. As mentioned in Section 2.2, $T_1 G$ is a subspace of $\mathfrak{gl}_n(\mathbb{F})$. In what follows we will write \mathfrak{g} for $T_1 G$.

Theorem 2.18. (1) \mathfrak{g} is closed under the bracket operation.

(2) Suppose H is another algebraic group, and $\Phi : G \rightarrow H$ is an algebraic group homomorphism. Set $\mathfrak{h} := T_1 H$, $\varphi := T_1 \Phi : \mathfrak{g} \rightarrow \mathfrak{h}$. Then $\phi([\xi, \eta]) = [\phi(\xi), \phi(\eta)]$ for all $\xi, \eta \in \mathfrak{g}$.

Exercise 2.19. Check (1) explicitly for $\mathfrak{g} = \mathfrak{sl}_n, \mathfrak{so}_n$, or $\mathfrak{sp}_n \subset \mathfrak{gl}_n(\mathbb{F})$.

Proof. Step 1: Here we produce a bilinear map $[\cdot, \cdot]' : \mathfrak{g} \times \mathfrak{g} \rightarrow \mathbb{F}[G]^*$. Recall that $\xi_1, \xi_2 \in \mathfrak{g}$ can be viewed as linear functions $\mathbb{F}[G] \rightarrow \mathbb{F}$. So $\xi_1 \otimes \xi_2$ is a linear function on $\mathbb{F}[G] \otimes \mathbb{F}[G] \rightarrow \mathbb{F}$.

Recall, (b) in Section 1.1, that $\mathbb{F}[G] \otimes \mathbb{F}[G]$ is identified with $\mathbb{F}[G \times G]$. Consider the multiplicative commutator map $C : G \times G \rightarrow G$ given by $(g_1, g_2) \mapsto g_1 g_2 g_1^{-1} g_2^{-1}$. Since multiplication and inversion maps are morphisms, the same is true for C . So we have the pullback homomorphism $C^* : \mathbb{F}[G] \rightarrow \mathbb{F}[G \times G]$. Set

$$[\xi_1, \xi_2]' = (\xi_1 \otimes \xi_2) \circ C^*.$$

The map $[\cdot, \cdot]'$ is indeed bilinear.

Step 2: We compute $[\cdot, \cdot]'$ for $G = \mathrm{GL}_n(\mathbb{F})$. For $f \in \mathbb{F}[G]$, we have

$$\begin{aligned} [\xi_1, \xi_2]'(f) &= (\xi_1 \otimes \xi_2) \circ C^*(f) \\ &= \partial_{s_1} \partial_{s_2} f((1 + \xi_1 s_1)(1 + \xi_2 s_2)(1 + \xi_1 s)^{-1}(1 + \xi_2 s)^{-1})|_{s_1=s_2=0} \end{aligned}$$

Note that the expression inside of f expanded as a power series in s_1, s_2 equals $1 + s_1 s_2 ([\xi_1, \xi_2] + \text{h.o.t.})$, where “h.o.t.” stands for higher order – at least cubic – terms in s_1, s_2 . Hence its derivative with respect to s_1 and s_2 equals $[\xi_1, \xi_2](f)$. We conclude that $[\xi_1, \xi_2]' = [\xi_1, \xi_2]$ (the left hand side is an element in $\mathbb{F}[G]^*$, while the right hand side is an element of \mathfrak{g} that is a subspace in $\mathbb{F}[G]^*$).

Step 3: In the notation of part 2) of the theorem, we claim that the following diagram is commutative:

$$(2) \quad \begin{array}{ccc} \mathfrak{g} \times \mathfrak{g} & \xrightarrow{\varphi \times \varphi} & \mathfrak{h} \times \mathfrak{h} \\ \downarrow [\cdot, \cdot]' & & \downarrow [\cdot, \cdot]' \\ \mathbb{F}[G]^* & \xrightarrow{? \circ \Phi^*} & \mathbb{F}[H]^* \end{array}$$

Indeed, recall that Φ is a group homomorphism, so

$$\Phi \circ C_G = C_H \circ (\Phi \times \Phi) \Leftrightarrow C_G^* \circ \Phi^* = (\Phi \otimes \Phi)^* \circ C_H^*,$$

where C_G, C_H denote the commutator maps for G, H , respectively. Then

$$\begin{aligned} [\varphi(\xi_1), \varphi(\xi_2)]' &= (\varphi(\xi_1) \otimes \varphi(\xi_2)) \circ C_H = (\xi_1 \otimes \xi_2) \circ (\Phi \otimes \Phi)^* \circ C_H^* = \\ &(\xi_1 \otimes \xi_2) \circ C_G^* \circ \Phi^* = [\xi_1, \xi_2]' \circ \Phi^*. \end{aligned}$$

So (2) is indeed commutative.

Step 4: Here we establish 1) of Proposition. Consider commutative diagram (2) for the inclusion $\Phi : G \hookrightarrow H := \mathrm{GL}_n(\mathbb{F})$. Then $\Phi^* : \mathbb{F}[H] \rightarrow \mathbb{F}[G]$ is a surjection, hence $\mathbb{F}[G]^* \hookrightarrow \mathbb{F}[H]^*$. Also $\mathfrak{h} \subset \mathbb{F}[H]^*$. We claim that $\mathfrak{g} = \mathfrak{h} \cap \mathbb{F}[G]^*$. Indeed, \mathfrak{g} consists of all elements $\delta \in \mathbb{F}[G]^*$ that satisfy the Leibniz identity: $\delta(fg) = f(1)\delta(g) + g(1)\delta(f)$ for all functions $f, g \in \mathbb{F}[G]$, or equivalently, all functions $f, g \in \mathbb{F}[H]$. Note that \mathfrak{h} as a subspace of $\mathbb{F}[H]^*$ admits a similar description. These descriptions imply $\mathfrak{g} = \mathfrak{h} \cap \mathbb{F}[G]^*$. Recall that $[\xi_1, \xi_2]' = [\xi_1, \xi_2] \in \mathfrak{h}$ for all $\xi_1, \xi_2 \in \mathfrak{h}$, thanks to Step 2. From here and Step 2 we conclude that \mathfrak{g} is stable with respect to $[\cdot, \cdot]$.

Step 5: Now we establish 2) of Proposition. By Step 4, $\mathrm{im}[\cdot, \cdot]' \subset T_1 G$ for any G . The claim of 2) now follows from the commutativity of (2). \square

Remark 2.20. Here is a slightly alternative way to construct $[\cdot, \cdot]' : \mathfrak{g} \times \mathfrak{g} \rightarrow \mathbb{F}[G]^*$ that will be useful in what follows: we set $[\xi_1, \xi_2]' := (\xi_1 \otimes \xi_2 - \xi_2 \otimes \xi_1) \circ m^*$, where $m : G \times G \rightarrow G$ is the product map. To show that this is equivalent to the construction in Step 1 of the proof of Theorem 2.18 is left as an exercise.

2.4. Bonus: Equivalent definitions of the bracket. There are other equivalent definitions of the bracket on \mathfrak{g} that we are going to sketch now.

For an affine variety X , we can talk about *vector fields* on X . By definition, these are derivations $\mathbb{F}[X] \rightarrow \mathbb{F}[X]$, i.e., \mathbb{F} -linear maps satisfying Leibniz identity:

$$\delta(fg) = f\delta(g) + g\delta(f).$$

Denote the space of derivations by $\mathrm{Der}(X)$. It comes with a bracket: for $\delta_1, \delta_2 \in \mathrm{Der}(X)$, the map $\mathbb{F}[X] \rightarrow \mathbb{F}[X]$ defined by

$$[\delta_1, \delta_2](f) := \delta_1(\delta_2(f)) - \delta_2(\delta_1(f))$$

for $f \in \mathbb{F}[X]$ is a derivation.

Now let $X = G$ be an algebraic group. The group G acts on $\mathrm{Der}(G)$, say via the action of G on itself on the right, and the action respects the bracket. So, the subspace $\mathrm{Der}(G)^G$ of invariant vector fields is stable under the bracket. Similarly to the case of Lie groups, restricting a vector field to the identity element $1 \in G$ gives an isomorphism $\mathrm{Der}(G)^G \xrightarrow{\sim} \mathfrak{g}$ intertwining the brackets. The functoriality (part 2 of the theorem) is then harder to establish; see [H2, Sec. 9.2].

One can also adapt an approach from [OV, Sec. 1.2] to the algebraic setting as follows. For this, we assume that the reader is familiar with the language of schemes.

For $k \in \mathbb{Z}_{>0}$, consider the algebra $\mathbb{F}[\epsilon]/(\epsilon^{k+1})$ of truncated polynomials. For an algebraic group G , we consider its group of $\mathbb{F}[\epsilon]/(\epsilon^{k+1})$ -points. A naïve definition is as follows. The group G is defined inside $\mathrm{GL}_n(\mathbb{F})$ by some polynomial equations. Consider the subset of $\mathrm{GL}_n(\mathbb{F}[\epsilon]/(\epsilon^{k+1}))$, the group of invertible matrices with entries in $\mathbb{F}[\epsilon]/(\epsilon^{k+1})$, given by the same polynomial equations. It's a subgroup. A more conceptual way is to view this group as the group of scheme morphisms $\mathrm{Spec}(\mathbb{F}[\epsilon]/(\epsilon^{k+1})) \rightarrow G$, that should be viewed as curves up to order k in G . Denote the resulting group by G_k . Note that for $k < \ell$, we have a homomorphism of abstract groups $G_\ell \rightarrow G_k$. An exercise is to check that the kernel of $G_{k+1} \rightarrow G_k$ is identified with \mathfrak{g} , with its additive group structure, for all k .

Now, an algebraic group homomorphism $\varphi : G \rightarrow H$ gives rise to a group homomorphism $\varphi_k : G_k \rightarrow H_k$ for all k , given by the same polynomials. This is especially easy to see if we identify G_k and H_k with the groups of morphisms from $\text{Spec}(\mathbb{F}[\epsilon]/(\epsilon^{k+1}))$ to G and H , respectively; to get φ_k we post-compose with φ . For each k , the diagram

$$(3) \quad \begin{array}{ccc} G_\ell & \xrightarrow{\varphi_\ell} & H_\ell \\ \downarrow & & \downarrow \\ G_k & \xrightarrow{\varphi} & H_k \end{array}$$

is commutative. The induced homomorphism

$$\mathfrak{g} = \ker(G_{k+1} \rightarrow G_k) \rightarrow \ker(H_{k+1} \rightarrow H_k) = \mathfrak{h}$$

coincides with $T_1\Phi$ for any k . Since the kernels in question are abelian, the commutator map for the group $\ker(G_3 \rightarrow G_1)$ descends to a map

$$\ker(G_2 \rightarrow G_1) \times \ker(G_2 \rightarrow G_1) \rightarrow \ker(G_3 \rightarrow G_2).$$

Under the identification of these kernels with \mathfrak{g} , we recover the bracket on \mathfrak{g} , the reader interested in proving this case can try to reduce it to the case of $G = \text{GL}_n(\mathbb{F})$. From here and commutative diagram (3) we deduce that $T_1\Phi$ intertwines the brackets.

2.5. Definition and basic examples of Lie algebras. Let \mathbb{F} be a field.

Definition 2.21. A *Lie algebra* over \mathbb{F} is an \mathbb{F} -vector space \mathfrak{g} equipped with a bilinear map $[\cdot, \cdot] : \mathfrak{g} \times \mathfrak{g} \rightarrow \mathfrak{g}$ (called the *Lie bracket* or *commutator*) satisfying the following two properties:

(SS) *Skew-symmetry*: For all $x \in \mathfrak{g}$,

$$[x, x] = 0.$$

(JI) *Jacobi identity*: For all $x, y, z \in \mathfrak{g}$,

$$[x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0.$$

Note that (SS) implies $[x, y] = -[y, x]$ for all $x, y \in \mathfrak{g}$ and, assuming $\text{char } \mathbb{F} \neq 2$, is equivalent to that condition (while for $\text{char } \mathbb{F} = 2$, (SS) is stronger than $[x, y] = -[y, x]$). Modulo (SS), (JI) is equivalent to:

$$[x, [y, z]] = [[x, y], z] + [y, [x, z]].$$

Definition 2.22. Let $\mathfrak{g}, \mathfrak{h}$ be Lie algebras. An \mathbb{F} -linear map $\varphi : \mathfrak{g} \rightarrow \mathfrak{h}$ is called a *Lie algebra homomorphism* if:

$$\varphi([x, y]) = [\varphi(x), \varphi(y)] \quad \text{for all } x, y \in \mathfrak{g}.$$

Definition 2.23. Let \mathfrak{h} be a Lie algebra. A subspace $\mathfrak{g} \subset \mathfrak{h}$ is called a *Lie subalgebra* if it is closed under $[\cdot, \cdot]$. Then the restriction of $[\cdot, \cdot]$ to \mathfrak{g} is also a Lie bracket, and the inclusion map $\mathfrak{g} \hookrightarrow \mathfrak{h}$ is a Lie algebra homomorphism.

Now we give some basic examples of Lie algebras.

Example 2.24 (Abelian Lie algebra). An *abelian* Lie algebra \mathfrak{g} is one in which $[x, y] = 0$ for all $x, y \in \mathfrak{g}$.

Example 2.25. Let A be an associative algebra. Then, for $a, b \in A$, define $[a, b] := ab - ba$. This operation satisfies (SS) and (JI), hence is a Lie bracket. An important special case is $A = \text{Mat}_n(\mathbb{F})$ or $\text{End}(V)$ for an \mathbb{F} -vector space V . The resulting Lie algebra is denoted by $\mathfrak{gl}_n(\mathbb{F})$ or $\mathfrak{gl}(V)$. Note that it is the tangent space $T_1 \text{GL}(V)$, see Example 2.12.

Example 2.26. Let \mathbb{F} be algebraically closed, and G be an algebraic group. Then, as we have seen in (1) of Theorem 2.18, $\mathfrak{g} := T_1 G$ is a Lie subalgebra in $\mathfrak{gl}_n(\mathbb{F})$. Moreover, according to (2) of Theorem 2.18, for an algebraic group homomorphism $\Phi : G \rightarrow H$, its tangent map $\varphi := T_1 \Phi : \mathfrak{g} \rightarrow \mathfrak{h}$ is a Lie algebra homomorphism.

2.6. Representations of Lie algebras. In Example 2.25 we have assigned the general linear Lie algebra $\mathfrak{gl}(V)$ to an \mathbb{F} -vector space V . As usual, this allows us to talk about representations of Lie algebras: by definition, a *representation* of a Lie algebra \mathfrak{g} in a vector space V is a Lie algebra homomorphism $\mathfrak{g} \rightarrow \mathfrak{gl}(V)$. One source of these representations is the rational representations of algebraic groups: if V is a finite dimensional vector space, and $\Phi : G \rightarrow \mathrm{GL}(V)$ is a rational representation of G , then $\varphi := T_1 \Phi : \mathfrak{g} \rightarrow \mathfrak{gl}(V)$ is a representation of \mathfrak{g} .

Now we give some examples and constructions of representations.

Example 2.27. For $x \in \mathfrak{g}$, let $\mathrm{ad}_x : \mathfrak{g} \rightarrow \mathfrak{g}$ denote the operator given by $\mathrm{ad}_x(y) = [x, y]$ for all $y \in \mathfrak{g}$. The map $x \mapsto \mathrm{ad}_x : \mathfrak{g} \rightarrow \mathfrak{gl}(\mathfrak{g})$ is a representation called the *adjoint representation*.

Suppose now G is an algebraic group and \mathfrak{g} is its Lie algebra. Then there is a rational representation of G in \mathfrak{g} , also called the adjoint representation and denoted by $\mathrm{Ad} : G \rightarrow \mathrm{GL}(\mathfrak{g})$. It is constructed as follows. Consider the conjugation action of G on itself: $a_g(g') := gg'g^{-1}$. Note that $1 \in G$ is invariant under this action. For Ad_g we take the linear map $T_1 a_g \in \mathrm{End}(T_1 G)$.

Lemma 2.28. *The map $g \mapsto \mathrm{Ad}_g : G \rightarrow \mathrm{End}(T_1 G)$ is a rational representation of G . Moreover, we have $T_1 \mathrm{Ad} = \mathrm{ad}$.*

Proof. First, we observe that Ad is an abstract group representation. Indeed, the functoriality of T_1 (also known as the chain rule) shows $\mathrm{Ad}_{g_1 g_2} = \mathrm{Ad}_{g_1} \circ \mathrm{Ad}_{g_2}$. Since $\mathrm{Ad}_1 = \mathrm{id}$, we see that Ad is indeed a group representation.

Now we show that Ad is a rational representation. Embed G into $\mathrm{GL}_n(\mathbb{F})$ for some n . Then a_g is the matrix conjugation, hence for $\xi \in \mathfrak{g} (\subset \mathfrak{gl}_n(\mathbb{F}))$ and $g \in G$, we have $\mathrm{Ad}_g(\xi) = g\xi g^{-1}$. This manifestly defines a rational representation of G in \mathfrak{g} .

The formula $\mathrm{Ad}_g(\xi) = g\xi g^{-1}$ also implies that $T_1 \mathrm{Ad}(\eta)(\xi) = \eta\xi - \xi\eta = [\eta, \xi]$ for all $\eta, \xi \in \mathfrak{g}$. Hence $T_1 \mathrm{Ad} = \mathrm{ad}$. \square

Example 2.29. Let V and W be representations of a Lie algebra \mathfrak{g} . Then $V \otimes W$ has a unique structure of a representation of \mathfrak{g} , defined by

$$\xi.(v \otimes w) = (\xi.v) \otimes w + v \otimes (\xi.w), \forall \xi \in \mathfrak{g}, v \in V, w \in W.$$

Exercise 2.30. 1) Check that this is indeed a representation.

2) Let G be an algebraic group with Lie algebra \mathfrak{g} and let V, W be rational representations of G and hence representations of \mathfrak{g} . Then the representation of \mathfrak{g} in $V \otimes W$ arises from the representation of G in $V \otimes W$.

Example 2.31. If V is a representation of \mathfrak{g} , then so is V^* , the dual space of V . The structure of a \mathfrak{g} -representation on V^* is given by

$$(\xi.\alpha)(v) = -\alpha(\xi.v), \forall \xi \in \mathfrak{g}, \alpha \in V^*, v \in V.$$

This is the *dual representation*. The motivation is similar to 2) of Exercise 2.30.

Example 2.32. The *trivial representation* of \mathfrak{g} in \mathbb{F} is the representation where all $\xi \in \mathfrak{g}$ act by the zero.

2.7. Correspondence between Algebraic Groups and Lie Algebras. Recall that over the real or complex numbers there is an equivalence between:

- The category of finite dimensional Lie algebras (with Lie algebra homomorphisms),

- and the category of simply connected Lie groups (with Lie group homomorphisms),

see, e.g., [OV, §1.2.6, 1.2.8, 6.2]. For algebraic groups, even over the complex numbers, this correspondence is more subtle. This is what we are going to briefly discuss in this section.

First, recall that every algebraic group G is smooth as a variety, see Exercise 2.10. Note that for a smooth variety being irreducible is equivalent to being connected in the Zariski topology. Now suppose the base field \mathbb{F} is the complex numbers. We can consider any algebraic variety as a complex analytic space. If the resulting manifold is connected in the usual topology, then the initial variety is connected in the Zariski topology. The converse is also true, but is harder. For algebraic groups, the converse is relatively easy though, see [OV, §3.3.1].

Example 2.33. The groups $\mathrm{GL}_n(\mathbb{F})$, $\mathrm{SL}_n(\mathbb{F})$, $\mathrm{SO}_n(\mathbb{F})$, and $\mathrm{Sp}_n(\mathbb{F})$ are connected (in the Zariski topology). To see this, one can argue similarly to [OV, §1.3.1]. On the other hand, $\mathrm{O}_n(\mathbb{F})$ is not connected.

In characteristic 0, one has the following uniqueness results.

Theorem 2.34. Suppose G is connected and $\mathrm{char}(\mathbb{F}) = 0$. Let $\Phi, \Psi : G \rightarrow H$ be algebraic group homomorphisms and $\varphi, \psi : \mathfrak{g} \rightarrow \mathfrak{h}$ the corresponding Lie algebra homomorphisms. If $\varphi = \psi$, then $\Phi = \Psi$.

Theorem 2.35. Let V and W be rational representations of G . If a linear map $\eta : V \rightarrow W$ is G -linear, then η is \mathfrak{g} -linear. If G is connected and $\mathrm{char}(\mathbb{F}) = 0$, then the converse is true as well.

Over $\mathbb{F} = \mathbb{C}$, both theorems can be proved by using the exponential map $\exp : \mathfrak{g} \rightarrow G$, cf. [OV, §1.2.7]. Namely, embed G into $\mathrm{GL}_n(\mathbb{C})$ for some n . The image of \mathfrak{g} under the usual matrix exponential map $\mathfrak{gl}_n(\mathbb{C}) \rightarrow \mathrm{GL}_n(\mathbb{C})$ is contained in G , the resulting map $\exp : \mathfrak{g} \rightarrow G$ does not depend on the choice of the embedding. Both theorems can be deduced from this independence, this is left as an exercise. One can emulate these constructions over general algebraically closed characteristic 0 fields using formal groups.

For other results relating algebraic groups and their Lie algebras over characteristic 0 fields we refer the reader to [OV, Sec. 3.3].

Remark 2.36. Both theorems are false when $\mathrm{char}(\mathbb{F}) = p \neq 0$. For Theorem 2.34, consider groups $G = H = \mathbb{G}_m$, $\Phi(g) = 1$, $\Psi(g) = g^p$, so that both φ and ψ are zero maps. This also serves as a counterexample to Theorem 2.35.

3. UNIVERSAL ENVELOPING ALGEBRAS

3.1. Definition. The universal enveloping algebras play the same role for Lie algebras as the group algebras do for (finite) groups.

Definition 3.1. Let \mathbb{F} be a field, and \mathfrak{g} be a Lie algebra over \mathbb{F} . Define the *universal enveloping algebra* $U(\mathfrak{g})$ as

$$U(\mathfrak{g}) = T(\mathfrak{g}) / (x \otimes y - y \otimes x - [x, y] | x, y \in \mathfrak{g})$$

where $T(\mathfrak{g})$ is the tensor algebra of \mathfrak{g} . Here we mod out the two-sided ideal generated by the elements in the brackets.

The composition map $\iota : \mathfrak{g} \rightarrow T(\mathfrak{g}) \rightarrow U(\mathfrak{g})$ is a Lie algebra homomorphism. It is universal in the following sense.

Lemma 3.2. *Let A be an associative algebra (hence a Lie algebra). Let $\varphi : \mathfrak{g} \rightarrow A$ be a Lie algebra homomorphism. Then, there is a unique associative algebra homomorphism $\tilde{\varphi} : U(\mathfrak{g}) \rightarrow A$ such that $\varphi = \tilde{\varphi} \circ \iota$.*

The proof is left as an exercise.

Example 3.3. If \mathfrak{g} is an abelian Lie algebra, then $U(\mathfrak{g}) = S(\mathfrak{g})$, the symmetric algebra on \mathfrak{g} . Indeed, these two algebras are just given by the same generators and relations.

3.2. Poincare-Birkhoff-Witt (PBW) Theorem. Let \mathfrak{g} be a Lie algebra. Our goal is to present a basis in $U(\mathfrak{g})$. Assume for simplicity that \mathfrak{g} is finite-dimensional. Let x_1, \dots, x_n be a basis of \mathfrak{g} . We can view x_1, \dots, x_n as elements of $U(\mathfrak{g})$ via the homomorphism $\iota : \mathfrak{g} \rightarrow U(\mathfrak{g})$.

Theorem 3.4. *The ordered monomials $x_1^{d_1} \cdots x_n^{d_n}$ with $d_1, \dots, d_n \in \mathbb{Z}_{\geq 0}$ form a basis in $U(\mathfrak{g})$.*

An easy part is that these elements span $U(\mathfrak{g})$. A stronger claim is true: for $d \geq 0$, let $U(\mathfrak{g})_{\leq d}$ denote the span of all monomials in x_1, \dots, x_n of degree $\leq d$.

Lemma 3.5. *The ordered monomials $x_1^{d_1} \cdots x_n^{d_n}$ with $d_1 + \dots + d_n \leq d$ span $U(\mathfrak{g})_{\leq d}$.*

Proof. We apply induction on d , using the observation that for $i < j$, we have $x_j x_i = x_i x_j - [x_i, x_j]$. Note that the second summand is a linear combination of x_1, \dots, x_n . The finish the proof is left as an exercise. \square

The linear independence is more subtle (see [Bo, Ch. I, Sec. 2] or [H1, Sec. 17.8]). The idea is to construct a representation of \mathfrak{g} with basis $x_1^{d_1} \cdots x_n^{d_n}$ for $d_1, \dots, d_n \in \mathbb{Z}_{\geq 0}$ and the action given by left multiplication. One needs to write the product $x_\ell x_1^{d_1} \cdots x_n^{d_n}$ as the linear combination of ordered monomials, using the identity $[x_i, x_j] = x_i x_j - x_j x_i$. The existence of such a representation is automatic once we know the theorem (this is just $U(\mathfrak{g})$), but the point is that the existence can be verified independently, although the check is unpleasant. We will prove the theorem in Section 4.3 for Lie algebras of algebraic groups in the case when $\text{char } \mathbb{F} = 0$. The two ingredients in the proof are filtrations and gradings (to be covered in Section 3.3) and Hopf algebra structures to be covered in Section 4.

3.3. Filtered and graded algebras. The goal of this section is to observe an additional structure – an ascending algebra filtration – on $U(\mathfrak{g})$ and interpret Theorem 3.4 as a statement about the associated graded algebra (a construction we are also going to define).

Definition 3.6. Let V be a vector space over \mathbb{F} . By a *vector space grading* on V we mean a vector space decomposition $V = \bigoplus_{i \in \mathbb{Z}} V_i$. An element of V_i will be called *homogeneous of degree i* . We refer to the subspaces V_i as the *graded components* of V .

Let $U = \bigoplus_i U_i, V = \bigoplus_i V_i$ be two graded vector spaces. We say that a linear map $\varphi : U \rightarrow V$ is *graded* if $\varphi(U_i) \subset V_i$.

Example 3.7. Let U, V be vector spaces with gradings $U = \bigoplus_i U_i$ and $V = \bigoplus_j V_j$. Then their tensor product $U \otimes V$ is graded with $(U \otimes V)_k = \bigoplus_i U_i \otimes V_{k-i}$ for all $k \in \mathbb{Z}$.

We now proceed to graded algebras.

Definition 3.8. Let A be an \mathbb{F} -algebra (not necessarily associative or unital). By an *algebra grading on A* (by \mathbb{Z}) we mean a vector space grading $A = \bigoplus_{i \in \mathbb{Z}} A_i$ such that $A_i A_j \subset A_{i+j}$ for all $i, j \in \mathbb{Z}$, equivalently, the product map $A \otimes A \rightarrow A$ is a graded linear map.

We note that if A is associative and unital, then necessarily $1 \in A_0$ (because the projection of 1 to A_0 is the unit).

Example 3.9. Let V be a vector space. Then the tensor, symmetric, and exterior algebras $A = T(V), S(V), \Lambda(V)$ admit unique gradings with $A_1 = V$.

Now we proceed to filtrations.

Definition 3.10. Let V be a vector space. By an *ascending vector space filtration* (or, more precisely, \mathbb{Z} -filtration) on V we mean a collection of subspaces $V_{\leq j} \subset V$ such that $V_j \subset V_{j+1}$ for all $j \in \mathbb{Z}$. We say that the filtration is *exhaustive* if $V = \bigcup_{j \in \mathbb{Z}} V_{\leq j}$ and *separated* if $\bigcap_j V_j = \{0\}$. We refer to the subspaces $V_{\leq j}$ as the *filtered pieces* of V .

We can talk about filtered linear maps, similarly to graded ones: a *filtered* linear map $\varphi : U \rightarrow V$ is one satisfying $\varphi(U_{\leq j}) \subset V_{\leq j}$ for all j . One subtlety is the notion of an isomorphism: if $\varphi : U \rightarrow V$ is a filtered linear map that is bijective, then φ^{-1} may fail to be filtered if U and V are infinite dimensional. Below, when we talk about filtered isomorphisms φ we always assume that $\varphi(U_{\leq j}) = V_{\leq j}$ for all j , then φ^{-1} is a filtered linear map.

Similarly to graded vector spaces, the tensor product of two filtered spaces U and V carries a natural filtration with

$$(U \otimes V)_{\leq k} = \sum_i U_i \otimes V_{k-i}, \forall k \in \mathbb{Z}.$$

Definition 3.11. Let A be an associative unital \mathbb{F} -algebra equipped with a vector space filtration with pieces $V_{\leq j}$:

- (a) $A_{\leq i} A_j \subset A_{i+j}$ for all $i, j \in \mathbb{Z}$,
- (b) $1 \in A_{\leq 0}$.

Note that (a) is equivalent to the condition that the product map $A \otimes A \rightarrow A$ is filtered.

Now we give constructions of exhaustive ascending algebra filtrations.

Example 3.12. Let $A = \bigoplus_{i \in \mathbb{Z}} A_i$ be a graded algebra. Set $A_{\leq j} := \bigoplus_{i \leq j} A_i$. This defines an exhaustive ascending algebra filtration.

Example 3.13. Let A be an associative unital algebra with generators x_i , where i runs over some indexing set I . Let $A_{\leq j}$ denote the span of monomials $x_{i_1} \dots x_{i_j}$ with $i_1, \dots, i_j \in I$. Then the subspaces $A_{\leq j}$ define an exhaustive ascending algebra filtration on A . Note that this algebra is filtered by $\mathbb{Z}_{\geq 0}$ meaning that $A_{\leq j} = \{0\}$ for $j < 0$.

Example 3.14. Let A, B be two filtered associative unital algebras with filtered pieces $A_{\leq i}, B_{\leq j}$. Then $A \otimes B$ with the tensor product filtration as above is a filtered algebra.

We can apply Example 3.13 to $A = U(\mathfrak{g})$ and $\{x_i\}$ being the set of all elements of \mathfrak{g} (or just the elements of a chosen basis). The j th filtered piece is the subspace $U(\mathfrak{g})_{\leq j}$ from Section 3.2. This is the so called *PBW filtration*.

Now we proceed to the associated graded space of a filtered vector space.

Definition 3.15. Let V be a filtered vector space with filtered pieces $V_{\leq j}$. Form the space $\text{gr } V := \bigoplus_{i \in \mathbb{Z}} V_{\leq i} / V_{\leq i-1}$. This space is called the *associated graded space* of V , it is graded with i th

graded component $V_{\leq i}/V_{\leq i-1}$. Note that if A is a filtered algebra, then $\text{gr } A$ has a unique associative product satisfying $(a + A_{\leq i-1})(b + A_{\leq j-1}) = ab + A_{\leq i+j-1}$ for all $i, j, a \in A_{\leq i}, b \in A_{\leq j}$ turning $\text{gr } A$ into a graded algebra.

Here is a basic tool to get some understanding of associated graded algebras. Let \tilde{A} be an algebra equipped with an ascending filtration $\tilde{A}_{\leq j}$. Let $I \subset \tilde{A}$ be a two-sided ideal. Then $A := \tilde{A}/I$ inherits an ascending filtration from \tilde{A} : if $\pi : \tilde{A} \rightarrow \tilde{A}/I$ is the quotient epimorphism, then for the filtered pieces we take $\pi(\tilde{A}_{\leq j})$. Now suppose that \tilde{A} is graded and the filtration arises as in Example 3.12. For a nonzero element $a \in \tilde{A}$ with $a = \sum_i a_i$ for $a_i \in A_i$ we write $\text{top}(a)$ for the nonzero a_i with maximal possible i . For $a = 0$, we set $\text{top}(a) = 0$. Note that $\text{top}(I) := \text{Span}_{\mathbb{F}}\{\text{top}(a) | a \in I\}$ is an ideal, and it is graded meaning that $\text{top}(I) = \bigoplus_{i \in \mathbb{Z}} (\text{top}(I) \cap \tilde{A}_i)$. The algebra $\tilde{A}/\text{top}(I)$ inherits a grading from \tilde{A} .

Exercise 3.16. Construct a graded algebra epimorphism $\tilde{A} \rightarrow \text{gr } A$ and show that its kernel is $\text{top}(I)$.

We apply this construction to $\tilde{A} = T(\mathfrak{g})$ and the two-sided ideal I generated by the elements $x \otimes y - y \otimes x - [x, y]$. The quotient $A = \tilde{A}/I$ is the universal enveloping algebra $U(\mathfrak{g})$. Consider the two-sided ideal $I_0 \subset T(\mathfrak{g})$ generated by the elements $x \otimes y - y \otimes x$ with $x, y \in \mathfrak{g}$. The quotient $T(\mathfrak{g})/I_0$ is nothing else but the symmetric algebra $S(\mathfrak{g})$. Note that $I_0 \subset \text{top}(I)$. This yields the epimorphism $S(\mathfrak{g}) \rightarrow \text{gr } U(\mathfrak{g})$. The PBW theorem (Theorem 3.4) is equivalent to the claim that this epimorphism is an isomorphism.

Next exercise studies the compatibility of taking the associated graded algebra with tensor products.

Exercise 3.17. Let U, V be as in Example 3.14, so that $U \otimes V$ carries a natural filtration. Construct a natural homomorphism $(\text{gr } U) \otimes (\text{gr } V) \rightarrow \text{gr}(U \otimes V)$, where the right hand side is equipped with a grading as in Example 3.7. Show that it is an isomorphism. Moreover, if U, V are filtered algebras then the isomorphism above is that of graded algebras.

We finish this section with a remark.

Remark 3.18. Sometimes it is convenient to talk about descending vector space (and algebra) filtrations. These are obtained from ascending ones by reversing the index: $V_{\geq i} := V_{\leq -i}$. Here is an important example of a descending filtration: let A be an associative unital algebra and $I \subset A$ be a two-sided ideal. Then for $i \geq 0$ we can set $A_{\geq i} := I^i$.

4. HOPF ALGEBRAS

4.1. Introduction. Questions about affine varieties (or schemes) usually get translated to the language of algebras of functions. So we can ask how an algebraic group structure on G is reflected on its algebra of functions.

To have an algebraic group structure means to have

- the product morphism $m : G \times G \rightarrow G$,
- the unit element that can be viewed as a morphism $\mathbf{1} : \text{pt} \rightarrow G$,
- and the inversion morphism $i : G \rightarrow G$.

The axioms m , $\mathbf{1}$, and i should satisfy are exactly those of a group, i.e.:

- m is associative, equivalently, we have the following commutative diagram:

$$\begin{array}{ccc} G \times G \times G & \xrightarrow{m \times \text{id}} & G \times G \\ \downarrow \text{id} \times m & & \downarrow m \\ G \times G & \xrightarrow{m} & G \end{array}$$

- The unit axiom, which is the following commutative diagram (and its analog, where we swap pt and G , and $\mathbf{1}$ and id):

$$\begin{array}{ccc} \text{pt} \times G & \xrightarrow{\mathbf{1} \times \text{id}} & G \times G \\ & \searrow \cong & \downarrow m \\ & & G \end{array}$$

- The inverse axiom, which is the following commutative diagram:

$$\begin{array}{ccccc} G & \xrightarrow{(\text{id}, i)} & G \times G & & \\ \downarrow & \searrow (i, \text{id}) & \downarrow m & & \\ G \times G & \xrightarrow{\mathbf{1}} & G & & \end{array}$$

Now consider the pullback homomorphisms $m^* : \mathbb{F}[G] \rightarrow \mathbb{F}[G] \otimes \mathbb{F}[G]$, $\mathbf{1}^* : \mathbb{F}[G] \rightarrow \mathbb{F}$, and $i^* : \mathbb{F}[G] \rightarrow \mathbb{F}[G]$. The diagrams above translate to the corresponding diagrams for m^* , $\mathbf{1}^*$, and i^* when we replace the varieties with their algebras of functions and reverse all arrows.

4.2. Definition: Hopf Algebra. Let \mathbb{F} be a field and A be an associative unital \mathbb{F} -algebra. We write $\mu : A \otimes A \rightarrow A$ for the multiplication map, $\mu(a \otimes b) = ab$, and $\eta : \mathbb{F} \rightarrow A$ for the unit map $\eta(1) = 1_A$.

Definition 4.1. By a *Hopf algebra structure* on A , we mean a triple of algebra homomorphisms:

- The *coproduct* $\Delta : A \rightarrow A \otimes A$.
- The *counit* $\epsilon : A \rightarrow \mathbb{F}$.
- The *antipode* $S : A \rightarrow A^{opp}$ (the algebra with opposite product).

satisfying the following axioms:

- The coproduct is co-associative, i.e., the following diagram is commutative:

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes A \\ \Delta \downarrow & & \downarrow \Delta \otimes \text{id} \\ A \otimes A & \xrightarrow{\text{id} \otimes \Delta} & A \otimes A \otimes A \end{array}$$

- ϵ satisfies the counit axiom, i.e., the following diagram is commutative (and its analog, where $\epsilon \otimes \text{id}$ is replaced with $\text{id} \otimes \epsilon$ is commutative):

$$\begin{array}{ccc} A & \xrightarrow{\Delta} & A \otimes A \\ & \searrow \text{id} & \downarrow \epsilon \otimes \text{id} \\ & & A \end{array}$$

- S satisfies the antipode axiom, meaning that the following diagram is commutative:

$$\begin{array}{ccccc} A & \xrightarrow{\Delta} & A \otimes A & & \\ \downarrow \Delta & \swarrow \epsilon & \downarrow \mu \circ (S \otimes \text{id}) & & \\ A \otimes A & \xrightarrow{\mu \circ (\text{id} \otimes S)} & A & & \end{array}$$

Remark 4.2. A vector space C equipped with linear maps $\Delta : C \rightarrow C \otimes C$ satisfying the coassociativity axiom and $\epsilon : C \rightarrow \mathbb{F}$ satisfying the counit axiom, is called, not surprisingly, a coassociative counital *coalgebra*. So a Hopf algebra is an associative unital algebra and a coassociative counital coalgebra such that Δ, ϵ are algebra homomorphisms (such a structure is called a *bialgebra*) and an antipode exists (if so, it is recovered uniquely from the other structures, see, e.g., [EGNO, Proposition 5.3.5]).

Example 4.3. Let G be an algebraic group. Then $\mathbb{F}[G]$ is a Hopf algebra with $\Delta = m^*, \epsilon = 1^*, S = i^*$, cf. the end of Section 4.1.

Example 4.4. Let G be a group. Then the group algebra $\mathbb{F}G$ is a Hopf algebra with unique coproduct, counit and antipode maps satisfying

$$\Delta(g) = g \otimes g, \quad \epsilon(g) = 1, \quad S(g) = g^{-1}, \forall g \in G \subset \mathbb{F}G.$$

To check the axioms is an exercise.

Example 4.5. Let \mathfrak{g} be a Lie algebra. Then the universal enveloping algebra $U(\mathfrak{g})$ has the unique Hopf algebra structure such that

$$\Delta(x) = x \otimes 1 + 1 \otimes x, \epsilon(x) = 0, S(x) = -x, \forall x \in \mathfrak{g} \subset U(\mathfrak{g}).$$

In particular, the symmetric algebra $S(V)$ of a vector space V (viewed as an abelian Lie algebra) is a Hopf algebra.

Example 4.6. Here is a construction with Hopf algebras. Let A be a Hopf algebra, and I an ideal satisfying the following conditions:

- $\Delta(I) \subset I \otimes A + A \otimes I$,
- $S(I) \subset I$,
- $\epsilon(I) = 0$.

In this case we say I is a *Hopf ideal*. Note that the quotient A/I acquires a natural Hopf structure uniquely characterized by the condition that the projection $A \twoheadrightarrow A/I$ is a Hopf algebra homomorphism.

There are further examples: the cohomology algebra of a Lie group that was studied by Hopf, or the distribution algebra of an algebraic group, and perhaps the most interesting class, the quantum groups (q-deformed versions of universal enveloping algebras).

Remark 4.7. The definition of a Hopf algebra is “self-dual”. More precisely, let A be a finite-dimensional Hopf algebra with operations $\mu, \eta, \Delta, \epsilon, S$. One can check that A^* (the dual vector space) is also a Hopf algebra with operations $\Delta^*, \epsilon^*, \mu^*, \eta^*, S^*$. For example, for a finite group G and $A = \mathbb{F}G$, we have that $A^* = \mathbb{F}[G]$ (the algebra of functions on G). To check that $\mathbb{F}[G]$ is dual to $\mathbb{F}G$ is also an exercise.

Remark 4.8. Let A be a Hopf algebra over a field \mathbb{F} , and U, V be A -modules with corresponding homomorphisms $\rho_U : A \rightarrow \text{End}(U), \rho_V : A \rightarrow \text{End}(V)$. This gives an algebra homomorphism

$$A \otimes A \rightarrow \text{End}(U) \otimes \text{End}(V) \rightarrow \text{End}(U \otimes V)$$

making $U \otimes V$ an $A \otimes A$ -module. Thanks to the homomorphism $\Delta : A \rightarrow A \otimes A$, we can view $U \otimes V$ as an A -module. In other words, the tensor product of two A -modules is naturally an A -module. Similarly, \mathbb{F} becomes an A -module via ϵ (the trivial module), while U^* (which is naturally a right A -module) becomes a (left) A -module via S . For $A = \mathbb{F}G$ (resp., $A = U(\mathfrak{g})$) this recovers tensor product, trivial and dual group (resp., Lie algebra) representations.

4.3. Graded and filtered Hopf algebras. In this section we investigate analogs of constructions from Section 3.3 for Hopf algebras and prove a special case of Theorem 3.4.

Definition 4.9. Let A be a Hopf algebra equipped with an associative unital algebra filtration with filtered pieces $A_{\leq i}$. Then $A \otimes A$ is filtered as well, see Example 3.14. We say that the filtration on A is a *Hopf algebra filtration* if the coproduct, the counit and the antipode are filtered algebra homomorphisms. Similarly, we can talk about graded Hopf algebras.

Example 4.10. Let V be a vector space, so that the symmetric algebra $S(V)$ has a natural Hopf algebra structure, see Example 4.5. The natural grading on $S(V)$ makes it into a graded Hopf algebra.

Example 4.11. Let \mathfrak{g} be a Lie algebra, and $A := U(\mathfrak{g})$. Then $U(\mathfrak{g})$ is a filtered Hopf algebra with respect to the PBW filtration.

Exercise 4.12. Let $A = \mathbb{F}[G]$ and let \mathfrak{m}_1 is the maximal ideal of 1 in $\mathbb{F}[G]$. It gives rise to the descending filtration on $\mathbb{F}[G]$ as in Remark 3.18. Show that it is a Hopf algebra filtration. Hint: observe that $\mathbb{F}[G] \otimes \mathfrak{m}_1 + \mathfrak{m}_1 \otimes \mathbb{F}[G]$ is the maximal ideal of $(1, 1) \in G \times G$. Deduce from here that, for the product map $m : G \times G \rightarrow G$, we have $m^*(\mathfrak{m}_1^k) \subset \sum_{i=0}^k \mathfrak{m}_1^i \otimes \mathfrak{m}_1^{k-i}$.

Suppose now that A is a filtered Hopf algebra. In this case $\text{gr } A$ acquires the structure of a graded Hopf algebra by taking the top degree terms of Δ, S, ϵ , cf. Definition 3.15.

With this preparation we are ready to establish a special case of Theorem 3.4.

Proposition 4.13. Suppose that \mathbb{F} is an algebraically closed field with $\text{char}(\mathbb{F}) = 0$. Let G be an algebraic group. Then the epimorphism $S(\mathfrak{g}) \rightarrow \text{gr } U(\mathfrak{g})$ from Section 3.3 is an isomorphism.

Proof. The proof is in several steps.

Step 1. Let I denote the kernel of the epimorphism $S(\mathfrak{g}) \twoheadrightarrow \text{gr } U(\mathfrak{g})$. Note that I is graded, meaning that $I = \bigoplus_{j=0}^{\infty} I_j$, where $I_j = I \cap S^j(\mathfrak{g})$. Also note that $S(\mathfrak{g}) \twoheadrightarrow \text{gr } U(\mathfrak{g})$ is a Hopf

algebra homomorphism (left as an exercise). It follows that I is a Hopf ideal in the sense of Example 4.6.

Step 2. We claim that the only Hopf ideal in $A := S(\mathfrak{g})$ with $I_0 = I_1 = \{0\}$ is the zero ideal. Assume the contrary. Let m be the minimal number with $I_m \neq \{0\}$. Choose a nonzero element $f \in I_m$ and consider $\Delta(f)$. This is a homogeneous element of degree m in $A \otimes A$, so $\Delta(f) \in \bigoplus_{i=0}^m A_i \otimes A_{m-i} \subset A \otimes A$. On the other hand, I is a Hopf ideal, so $\Delta(f) \in I \otimes A + A \otimes I$. Since m is the minimal possible degree of a homogeneous element in I , we have $\Delta(f) \in 1 \otimes I_m \oplus I_m \otimes 1$. Now we claim that the component of $\Delta(f)$ in $A_1 \otimes A_{m-1}$ is nonzero leading to a contradiction hence proving the claim in the beginning of the step. Choose a basis x_1, \dots, x_n in \mathfrak{g} . We leave it as an exercise to show that the component of $\Delta(f)$ in $A_1 \otimes A_{n-1}$ is $\sum_{i=1}^n x_i \otimes \frac{\partial f}{\partial x_i}$. Since $\text{char } \mathbb{F} = 0$, the latter element cannot be zero for $f \neq 0$.

Step 3. It remains to show that for the ideal I in Step 1, we have $I_0 = I_1 = \{0\}$. This is equivalent to the condition that the elements $1, x_1, \dots, x_n \in U(\mathfrak{g})$ are linearly independent. Thanks to the universal property of $U(\mathfrak{g})$, Lemma 3.2, it suffices to find a representation ρ of \mathfrak{g} in a vector space V such that $\text{id}_V, \rho(x_1), \dots, \rho(x_n)$ are linearly independent elements of $\text{End}(V)$. Recall that G embeds into $\text{GL}_n(\mathbb{F})$ for some n as a closed subgroup, let Φ denote the embedding. By Exercise 2.7, $d_1\Phi$ is injective. For ρ we take the direct sum of $d_1\Phi$ and the one-dimensional trivial representation. To check that $\text{id}_V, \rho(x_1), \dots, \rho(x_n)$ are linearly independent is an exercise. \square

We note that if $\text{char } \mathbb{F} = p > 0$, then the claim of Step 2 is false: for any $f \in S(\mathfrak{g})$, the ideal (f^p) is a Hopf ideal. However, we have the following important exercise that will be used in a subsequent chapter.

Exercise 4.14. Let \mathbb{F} be an algebraically closed field of characteristic p , and let G be an algebraic group over \mathbb{F} . Let x_1, \dots, x_n be a basis of \mathfrak{g} . Then the elements $x_1^{d_1} \dots x_n^{d_n}$ with $\sum_{i=1}^n d_i < p$ are linearly independent in $U(\mathfrak{g})$. Moreover, if an element $z \in U(\mathfrak{g})_{\leq p-1}$ satisfies $\Delta(z) = z \otimes 1 + 1 \otimes z$, then $z \in \mathfrak{g}$.

REFERENCES

- [Bo] N. Bourbaki, *Lie groups and Lie algebras. Chapters 1–3*. Translated from the French. Reprint of the 1975 edition. Elem. Math. (Berlin) Springer-Verlag, Berlin, 1989.
- [BSU] M. Brion, P. Samuel, V. Uma, *Lectures on the structure of algebraic groups and geometric applications*. CMI Lecture Series in Mathematics 1, Hindustan Book Agency, 2013.
- [D] V. Danilov, *Algebraic varieties and schemes*. Encyclopaedia Math. Sci., 23 Springer-Verlag, Berlin, 1994, 167–297.
- [EGNO] P. Etingof, S. Gelaki, D. Nikshych, V. Ostrik, *Tensor categories*. Math. Surveys Monogr., 205, American Mathematical Society, Providence, RI, 2015, xvi+343 pp.
- [H1] J. Humphreys, *Introduction to Lie algebras and representation theory*. GTM 9, Springer-Verlag, New York-Berlin, 1972.
- [H2] J. Humphreys, *Linear algebraic groups*. GTM 21, Springer-Verlag, New York-Berlin, 1995.
- [OV] A. Onishchik, E. Vinberg, *Lie groups and algebraic groups*. Springer Ser. Soviet Math. Springer-Verlag, Berlin, 1990. xx+328 pp.