LECTURE 6

Frobenius kernels, Kempf's vanishing theorem, distributions algebras and theorem of Curtis (21 and 24/2/2025)

Let k be a field of characteristic $p > 0$. Denote by $\overline{k}$ an algebraic closure of k.

10. Frobenius kernels, Frobenius twists

Since we are only interested in split reductive groups, which are defined over the prime field, it suffices to define the Frobenius morphism as follows.

Definition 10.1 (Frobenius morphism). Let A be k-algebra, coming by base change from a $\mathbb{F}_p$-algebra A_0, i.e. $A = A_0 \otimes_{\mathbb{F}_p} k$, and let $X = \mathrm{Spec}(A)$. Then the Frobenius morphism $\mathrm{Fr}_X : X \to X$ is the endomorphism induced by the morphism of k-algebras $A \to A$ defined by $a_0 \otimes z \mapsto a_0^p \otimes z$.

If A_0 is finitely generated, hence a quotient of a polynomial ring $\mathbb{F}_p[X_1, \dots, X_n]$ and if we regard X as a closed subscheme of affine space $\mathbb{A}^n_k$, then $\mathrm{Fr}_X(R)$ sends an arbitrary R-point $(x_1, \dots, x_n)$ of $X(R)$ to $(x_1^p, \dots, x_n^p)$, for any k-algebra R.

Definition 10.2 (Frobenius kernels). With the previous notation, suppose that A_0 is a Hopf algebra with comultiplication Δ_0 and augmentation $\varepsilon_0 : A_0 \to \mathbb{F}_p$. Then $G_0 = \mathrm{Spec}(A_0)$ is a group scheme over $\mathbb{F}_p$ and $G = \mathrm{Spec}(A)$ is the k-group scheme obtained by base change. For any $a_0 \in A_0$ one has $\Delta_0(a_0^p) = \Delta_0(a_0)^p$ and $\varepsilon_0(a_0^p) = \varepsilon_0(a_0)^p = \varepsilon_0(a_0)$, since Δ_0, ε_0 are morphisms of algebras and since ε_0 takes values in $\mathbb{F}_p$. Thus, Fr_G is a morphism of k-group schemes.

Its kernel will be denoted by G_1 and called the first Frobenius kernel of G. The kernel of the composed morphism $\mathrm{Fr}_G^n = \mathrm{Fr}_G \circ \cdots \circ \mathrm{Fr}_G$ (n times) will be denoted by G_n and called the n-th Frobenius kernel of G.

Examples 10.3. (1) Let $G = \mathbb{G}_{m,k} = \mathrm{Spec}(k[T, T^{-1}])$. The Frobenius morphism is given by $T \mapsto T^p$ hence $G_1 = \mu_p$ is the spectrum of $k[T]/(T^p - 1) \simeq k[T]/(T-1)^p$. It is non-reduced and has only one point: one says that is is an *infinitesimal group scheme*. For any $n \in \mathbb{N}^*$, the n-th Frobenius kernel is $G_n = \mu_{p^n}$.

More generally, for any finitely generated abelian group M, if $G = \mathrm{Spec}\, k[M]$ is the corresponding diagonalisable group, then $G_n = \mathrm{Spec}(k[M/p^n M])$ is the diagonalisable group corresponding to $M/p^n M$.

(2) Let $G = \mathbb{G}_{a,k} = \mathrm{Spec}(k[X])$. The Frobenius morphism is given by $X \mapsto X^p$ hence for any $n \in \mathbb{N}^*$ the n-th Frobenius kernel G_n is the k-group scheme $\alpha_{p^n} = \mathrm{Spec}(k[X]/(X^p))$.

(3) Let $G = \mathrm{SL}_{2,k}$. It is $\mathrm{Spec}(A_0 \otimes k)$ where $A_0 = \mathbb{F}_p[a, b, c, d]/(ad - bc - 1)$. By abuse of notation, denote by the same letters a, b, c, d the entries of a "generic" matrix of SL_2. Then the Frobenius morphism is given by

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \mapsto \begin{pmatrix} a^p & c^p \\ b^p & d^p \end{pmatrix}$$

hence for any $n \in \mathbb{N}^*$ the n-th Frobenius kernel is the closed subgroup of $\mathrm{SL}_{2,k}$ defined by the equations: $b^{p^n} = 0 = c^{p^n}$, $a^{p^n} = 1 = d^{p^n}$ (and of course $ad = 1 + bc$). Again, it is non-reduced and infinitesimal (this is a general fact).

[0]Preliminary version of Feb. 28

One can prove the following proposition:

PROPOSITION 10.4. *Suppose our k-group scheme G is smooth (i.e. $G \otimes \overline{k}$ is reduced). Then $\mathrm{Fr}_G : G \to G$ is a finite, locally free morphism of rank $p^{\dim G}$. In particular, it is faithfully flat, hence so is Fr_G^n for every $n \in \mathbb{N}^*$, and one has an exact sequence of k-group schemes:*

$$1 \longrightarrow G_n \longrightarrow G \xrightarrow{\mathrm{Fr}_G^n} G \longrightarrow 1. \tag{10.1}$$

EXAMPLES 10.5. (1) For $G = \mathbb{G}_{m,k}$, the Frobenius morphism corresponds to the inclusion $k[T^p, T^{-p}] \subset k[T, T^{-1}]$ and the larger ring is a free module of rank p over the smaller ring, with basis $\{1, T, \ldots, T^{p-1}\}$.

(2) For $G = \mathbb{G}_{a,k}$, the Frobenius morphism corresponds to the inclusion $k[X^p] \subset k[X]$ and the larger ring is a free module of rank p over the smaller ring, with basis $\{1, X, \ldots, X^{p-1}\}$.

(3) Let $G = \mathrm{SL}_{2,k} = \mathrm{Spec}(A)$, with A as in Example 10.3 above. The Frobenius morphism corresponds to the inclusion $B \subset A$, where B denotes the k-subalgebra generated by the elements a^p, b^p, c^p, d^p. Note that G is covered by the two principal open subsets given by $a \neq 0$ and $b \neq 0$. Over the principal open set given by $a \neq 0$, one has $A_a \simeq k[a, a^{-1}] \otimes k[b, c]$ and this is free of rank p^3 over the subring $k[a^p, a^{-p}] \otimes k[b^p, c^p]$. Similarly, over the open subset $b \neq 0$ one has $A_b \simeq k[b, b^{-1}] \otimes k[a, d]$ and this is free of rank p^3 over the subring $k[b^p, b^{-p}] \otimes k[a^p, d^p]$. So we see that A is a locally free B-module of rank p^3.

DEFINITION 10.6 (Frobenius twist of a G-module). Let V be a G-module. For each $r \in \mathbb{N}^*$, its Frobenius twist $V^{[r]}$ is the vector space V regarded as G-module through $\mathrm{Fr}_G^n : G \to G$.

EXAMPLES 10.7. (1) Let $G = T$ a d-dimensional split torus, let $\lambda \in X(T)$ and let $V = k_\lambda$ be the corresponding 1-dimensional T-module. Then $V^{[r]}$ is the vector space k on which every $t \in T(R)$ acts by $t *_r 1 = t^{p^r} \cdot 1 = \lambda(t^{p^r})1 = (p^r\lambda)(t)1$, i.e. one has $V^{[r]} \simeq k_{p^r\lambda}$.

(2) Let V be the natural representation of $\mathrm{SL}_{2,k}$, with its basis $\{x, y\}$. Note that V is the simple module $L(1) = H^0(1)$. Then $V^{[1]}$ has a basis that we denote by $\{x^{[1]}, y^{[1]}\}$, on which a matrix

$$g = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

acts by sending $x^{[1]}$ to $a^p x^{[1]} + b^p y^{[1]}$ and $y^{[1]}$ to $c^p x^{[1]} + d^p y^{[1]}$. Thus, $L(1)^{[1]}$ is isomorphic to the G-submodule of $H^0(p)$ spanned by x^p and y^p, which is exactly the simple submodule $L(p)$.

Further, regarding $L(1) = H^0(1)$ as a subspace of the symmetric algebra $\bigoplus_{n\in\mathbb{N}} H^0(n) = k[x, y]$, one sees that the p-th power map φ induces a k-semilinear isomorphism from $L(1)^{[1]}$ to the G-submodule of $H^0(p)$ spanned by x^p and y^p, which is exactly the simple submodule $L(p)$.

One can prove the following proposition:

PROPOSITION 10.8. *Suppose that we have an exact sequence of k-group schemes:*

$$1 \longrightarrow N \longrightarrow G \xrightarrow{\pi} G' \longrightarrow 1. \tag{10.2}$$

i.e. π is faithfully flat and $N = \mathrm{Ker}(\pi)$. Then:

1. *If V is a G-module on which N acts trivially, the structure of G-module on V factors uniquely through a structure of G'-module, which we denote by $\pi_*(V)$.*
2. *If V' if a G'-module and if one denotes by $V = \pi^*(V')$ the G-module obtained by restriction via π, then N acts trivially on V and the resulting G'-module $\pi_*(V)$ is the original module G'-module V'.*

11. Properties of the induction functors Ind_H^G

Recall that k is a field. One can prove the following theorem, see [**SGA3**$_1$], Exp. VI$_A$, §3 and Exp. VI$_B$, §11 for (i) and [**Ja03**], Prop. I.5.12 for (ii).

THEOREM 11.1. *Let G be an affine k-group scheme, H a closed subgroup of G. Then:*

(i) *The quotient G/H exists in the category of schemes. Further, if H is a normal subgroup then G/H is an affine k-group scheme and $k[G/H] = k[G]^H$.*

(ii) *Every H-module M gives rise to an H-equivariant quasi-coherent sheaf $\mathcal{L}(M)$ on G/H and there is a natural isomorphism $R^i\mathrm{Ind}_H^G(M) \simeq H^i(G/H, \mathcal{L}(M))$ for every $i > 0$.*

(iii) *In particular, if H is normal in G, then $H^i(G/H, \mathcal{L}(M)) = 0$ since G/H is affine, hence the subgroup H is exact in G, i.e. $R^i\mathrm{Ind}_H^G = 0$ for $i > 0$.*

We deduce from this the following corollary:

COROLLARY 11.2. *Suppose that we have an exact sequence of k-group schemes:*

$$1 \longrightarrow N \longrightarrow G \xrightarrow{\pi} G' \longrightarrow 1.$$

Let H' be a closed subgroup of G' and H be its inverse image in G; so that $H/N \simeq H'$. Then, for any H'-module M, one has natural isomorphisms of G-modules:

$$\pi_G^*\big(R^i\mathrm{Ind}_{H'}^{G'}(M)\big) \simeq R^i\mathrm{Ind}_H^G\big(\pi_H^*(M)\big) \tag{11.1}$$

where π_G^* and π_H^* denote restriction via π for G'-modules and H'-modules respectively.

PROOF. Consider the H-module $V = \pi_H^*(M) \otimes k[G]$. Then V^N is a $H/N = H'$-module and $V^H = (V^N)^{H'}$. But N acts trivially on $\pi_H^*(M)$ hence one has:

$$V^N = \pi_H^*(M) \otimes k[G]^N = \pi_H^*(M) \otimes k[G']$$

and its structure of H'-module is precisely that of $M \otimes k[G']$, whereas its structure of G-module is that of $\pi_G^*(M \otimes k[G'])$. So we obtain that

$$\mathrm{Ind}_H^G\big(\pi_H^*(M)\big) = V^H = (V^N)^{H'} = \pi_G^*\big((M \otimes k[G'])^{H'}\big) = \pi_G^*\big(\mathrm{Ind}_{H'}^{G'}(M)\big). \tag{11.2}$$

This proves the assertion for $i = 0$. Now, consider the functor $F = \pi_G^* \circ \mathrm{Ind}_{H'}^{G'} = \mathrm{Ind}_H^G \circ \pi_H^*$. Since π_G^* is exact, one has $R^iF = \pi_G^* \circ R^i\mathrm{Ind}_{H'}^{G'}$ for all $i \geq 0$. Further, π_H^* is also exact, so if we prove that it takes injective H'-modules to H-modules which are acyclic for Ind_H^G, we will obtain that $R^iF = R^i\mathrm{Ind}_H^G \circ \pi_H^*$ and this will prove (11.1).

We have seen in Lect. 3 that every injective H'-module is a direct summand of an induced module $\mathrm{Ind}_e^{H'}(J)$ for some k-vector space J. So it suffices to prove that $\pi_H^*\big(\mathrm{Ind}_e^{H'}(J)\big)$ is acyclic. By (11.2) applied to the pairs $H \supset N$ and $H' \supset e$ instead of $G \supset H$ and $G' \supset H'$, we have:

$$\pi_H^*\big(\mathrm{Ind}_e^{H'}(J)\big) = \mathrm{Ind}_N^H\big(\pi_N^*(J)\big) = \mathrm{Ind}_N^H(J_{\mathrm{triv}}) \tag{11.3}$$

where J_{triv} denotes J regarded as a trivial N-module.

Now, one has $\mathrm{Ind}_N^G = \mathrm{Ind}_H^G \circ \mathrm{Ind}_N^H$ and since N is exact in H and in G (since H/N and G/N are affine) we obtain that, for $i > 0$:

$$0 = R^i\mathrm{Ind}_N^G(J_{\mathrm{triv}}) = R^i\mathrm{Ind}_H^G\big(\mathrm{Ind}_N^H(J_{\mathrm{triv}})\big).$$

This proves that $\pi_H^*\big(\mathrm{Ind}_e^{H'}(J)\big) = \mathrm{Ind}_N^H(J_{\mathrm{triv}})$ is acyclic for Ind_H^G and this completes the proof of the corollary. □

12. Kempf's vanishing theorem

Let us come back to a split reductive k-group G, with maximal torus T and root datum $\mathcal{R}(G,T) = (X(T), X_*(T), R, R^\vee)$. Let Δ be a base of the root system and B the Borel subgroup containing T and corresponding to the set $-R^+$ of *negative* roots. Let

$$X(T)^+ = \{\lambda \in X(T) \mid \langle \lambda, \alpha^\vee \rangle \in \mathbb{N} \quad \forall \alpha \in \Delta\}$$

be the set of dominant weights. For every B-module M we write $H^i(G/B, M)$ or simply $H^i(M)$ instead of $R^i\mathrm{Ind}_B^G(M)$. And when $M = k_\lambda$ for $\lambda \in X(T)$ regarded as a character of B, we write simply λ instead of k_λ. We want to prove the following:

THEOREM 12.1 (Kempf's vanishing theorem). *For $\lambda \in X(T)^+$ one has $H^i(G/B, \lambda) = 0$ for all $i > 0$.*

The proof uses as a technical tool the dominant "weight" $\rho = \frac{1}{2}\sum_{\beta \in R^+} \beta$, which satisfies $\langle \rho, \alpha^\vee \rangle = 1$ for all $\alpha \in \Delta$. Here we put "weight" in quotes because if, for example, $G = \mathrm{PGL}_2$ then ρ does not belong to $X(T)$. However, this is not a serious problem, as we explain below.

REMARK 12.2. The derived subgroup $G_0 = \mathcal{D}(G)$ of G is a split semi-simple k-group of type R and $T_0 = T \cap G_0$ is a maximal torus of G_0. The radical $R(G)$ of G is a central torus S contained in T, and $C = S \cap G_0$ is a finite diagonalisable subgroup of S. We have isomorphisms

$$T \simeq (T_0 \times S)/C \qquad \text{and} \qquad G \simeq (G_0 \times S)/C.$$

Thus, $X(T)$ is the subgroup of $X(T_0) \times X(S)$ consisting of pair of characters (λ, χ) which coincide on C and for any such pair, the simple G-module $L(\lambda, \chi)$ is $L(\lambda) \otimes k_\chi$, where $L(\lambda)$ is the corresponding simple G_0-module.

Moreover, by the classification theory in terms of root data, we know that there exists a split, simply connected, semi-simple k-group G_1 of type R with split maximal torus T_1 and a surjective (faithfully flat) morphisms of split groups $(G_1, T_1) \to (G_0, T_0)$ and hence of $\widetilde{G} = G_1 \times S$ onto G. Thus, setting $\widetilde{T} = T_1 \times S$, one sees that $X(T)$ is a subgroup of $X(\widetilde{T}) = X(T_1) \times X(S)$, one has $X(T)^+ \subset X(\widetilde{T})^+$ and the representation theory of G is completely determined by that of $\widetilde{G}$.

Further, the Borel subgroup $\widetilde{B}$ of $\widetilde{G}$ containing $\widetilde{T}$ and corresponding to the negative roots maps onto B and one has an isomorphism $\widetilde{G}/\widetilde{B} \simeq G/B$. Thus, for any $\lambda \in X(T)^+$ one has $H^i(G/B, \lambda) = H^i(\widetilde{G}/\widetilde{B}, \lambda)$. Thus, it suffices to prove Kempf's vanishing theorem when G is semi-simple and simply-connected; in this case ρ belongs to $X(T)$, which is the weight lattice $P(R)$.

Therefore, from now on we shall assume that G is a split, simply connected semi-simple k-group with root system R. We assume further that $\mathrm{char}(k) = p > 0$.

NOTATION 12.3. As said above, one sets $\rho = \frac{1}{2}\sum_{\beta \in R^+} \beta$. It is the unique element of $P(R)$ such that $\langle \rho, \alpha^\vee \rangle = 1$ for every $\alpha \in \Delta$.

Further, for each $r \in \mathbb{N}^*$ we consider the r-th Steinberg weight $\sigma_r = (p^r - 1)\rho$ and the r-th Steinberg module $\mathrm{St}_r = L(\sigma_r)$.[1]

Denote by G_rB the inverse image of the B via the Frobenius morphism $\mathrm{Fr}^r : G \to G$; it is a closed subgroup of G. We may regard St_r as a G_rB-module by restriction, and since we have a non-zero B-module map $\mathrm{St}_r \to k_{\sigma_r}$ we get by Frobenius reciprocity a non-zero morphism of G_rB-modules $\mathrm{St}_r \to \mathrm{Ind}_B^{G_rB}(\sigma_r)$.

One crucial property of St_r is the following proposition, whose proof will be given in the next lecture.

[1] Steinberg introduced this module in a different manner in the context of representations of the finite group $G(\mathbb{F}_{p^r})$ and proved as part of his construction that $\dim_k \mathrm{St}_r = p^{rN}$ where $N = |R^+|$. We will give a different proof below.

PROPOSITION 12.4. *The above map* $\mathrm{St}_r \to \mathrm{Ind}_B^{G_rB}(\sigma_r)$ *is an isomorphism of* G_rB*-modules.*

PROOF OF TH. 12.1. Assuming this result, we can now give the Haboush-Andersen proof of Kempf's vanishing theorem. Let $\lambda \in X(T)^+$. We saw earlier that the r-th Frobenius twist of the 1-dimensional B-module k_λ is $k_{p^r\lambda}$. Now, apply (11.1) to $G' = G$, $H' = B$ and $\pi = \mathrm{Fr}^r$. Then $H = G_rB$ and we obtain an isomorphism of G-modules:

$$H^i(G/B,\lambda)^{[r]} \simeq R^i\mathrm{Ind}_{G_rB}^G(p^r\lambda).$$

Tensor this with the G-module St_r and applying the generalised tensor identity on the right hand-side, we obtain:

$$H^i(G/B,\lambda)^{[r]} \otimes \mathrm{St}_r \simeq R^i\mathrm{Ind}_{G_rB}^G(p^r\lambda) \otimes \mathrm{St}_r \simeq R^i\mathrm{Ind}_{G_rB}^G(p^r\lambda \otimes \mathrm{St}_r). \tag{12.1}$$

Further, $\mathrm{St}_r \simeq \mathrm{Ind}_B^{G_rB}(\sigma_r)$. Thus, applying the tensor identity to the G_rB-module $p^r\lambda$ one obtains that

$$p^r\lambda \otimes \mathrm{St}_r \simeq \mathrm{Ind}_B^{G_rB}(p^r\lambda \otimes \sigma_r) = \mathrm{Ind}_B^{G_rB}(p^r(\lambda+\rho)-\rho).$$

Thus, (12.1) gives

$$H^i(G/B,\lambda)^{[r]} \otimes \mathrm{St}_r \simeq R^i\mathrm{Ind}_{G_rB}^G\big(\mathrm{Ind}_B^{G_rB}(p^r(\lambda+\rho)-\rho)\big). \tag{12.2}$$

Further, one has an isomorphism of schemes $G_rB/B \simeq G_r/(B\cap G_r) = G_r/B_r$ and the latter scheme is a finite affine k-scheme because G_r is so (see the next lecture).

Therefore, $R^j\mathrm{Ind}_B^{G_rB} = 0$ for $j > 0$ and this gives that the right-hand side of (12.2) is $R^i\mathrm{Ind}_B^G\big(p^r(\lambda+\rho)-\rho\big)$. Thus we obtain:

$$H^i(G/B,\lambda)^{[r]} \otimes \mathrm{St}_r \simeq H^i\big(G/B, p^r(\lambda+\rho)-\rho\big) = H^i\big(G/B, \mathcal{L}(\lambda+\rho)^{p^r} \otimes \mathcal{L}(-\rho)\big). \tag{12.3}$$

Now, for any $\lambda \in X(T)^+$ one knows that the line bundle $\mathcal{L}(\lambda+\rho)$ is ample on the projective variety G/B and hence the right-hand side is 0 for r large enough. This implies that $H^i(G/B,\lambda)^{[r]} = 0$ for some r, hence $H^i(G/B,\lambda) = 0$. □

REMARK 12.5. The k-group schemes G and B come from base change from flat (and smoooth) $\mathbb{Z}$-group schemes $G_\mathbb{Z}$ and $B_\mathbb{Z}$. Denoting the derived functors $R^i\mathrm{Ind}_{B_\mathbb{Z}}^{G_\mathbb{Z}}$ by $H^i_\mathbb{Z}$ and similarly if we replace $\mathbb{Z}$ by an arbitrary field K one can prove the following universal coefficient theorem: for any field K and $\lambda \in X(T)$ (not necessarily dominant) there is a short exact sequence of G_K-modules (see [**Ja03**], Prop. I..4.18)

$$0 \longrightarrow H^i_\mathbb{Z}(\lambda) \otimes K \longrightarrow H^i_\mathbb{K}(\lambda) \longrightarrow \mathrm{Tor}_1^\mathbb{Z}(K, H^{i+1}_\mathbb{Z}(\lambda)) \longrightarrow 0. \tag{12.4}$$

Therefore, Kempf's theorem implies that over our base field k, one has $H^0(\lambda) \simeq H^0_\mathbb{Z}(\lambda) \otimes k$ for $\lambda \in X(T)^+$.

On the other hand, since induction commutes with flat base change, one has $H^0_\mathbb{Z}(\lambda) \otimes \mathbb{C} \simeq H^0_\mathbb{C}(\lambda)$ and one knows that this is a simple $G_\mathbb{C}$ module with highest weight λ, whose character is given by Weyl's character formula.

To prove the crucial proposition 12.4, we need a new tool, the algebra of distributions at the origin of an affine k-group scheme, which we introduce in the next section.

13. Distribution algebras

Let $G = \mathrm{Spec}(A)$ be an affine k-group scheme, where $A = k[G]$. Let I be the augmentation ideal of A, i.e. the kernel of the augmentation map $\varepsilon : A \to k$ (since we assume that k is a field, I is a maximal ideal). Denote by A^* the dual vector space.

DEFINITION 13.1. Let $\mathrm{Dist}(G) = \{\phi \in A^* \mid \phi(I^{n+1}) = 0 \text{ for some } n \in \mathbb{N}\}$. It is the increasing union of the finite dimensional subspaces

$$\mathrm{Dist}_n(G) = \{\phi \in A \mid \phi(I^{n+1}) = 0\} \simeq (A/I^{n+1})^*.$$

Note that $\mathrm{Dist}_0(G)$ is 1-dimensional and spanned by the augmentation map ε. For $\phi, \psi \in \mathrm{Dist}(G)$, define their product $\phi\psi$ as the linear form $m_k \circ (\phi \otimes \psi) \circ \Delta : A \to k$, where Δ is the comultiplication of A and m_k the multiplication $k \otimes k \to k$. Then $\phi\psi$ belongs to $\mathrm{Dist}(G)$ because for any $n \in \mathbb{N}^*$ one has

$$\Delta(I^n) \subset \sum_{j=0}^{n} I^r \otimes I^{n-j} \tag{13.1}$$

hence if ϕ vanishes on I^{r+1} and ψ on I^{s+1} then $\phi \otimes \psi$ vanishes on a term $I^u \otimes I^v$ unless $u \leq r$ and $v \leq s$ hence $\phi\psi$ vanishes on I^n unless $n \leq r + s$. This shows that we have

$$\mathrm{Dist}_r(G)\mathrm{Dist}_s(G) \subset \mathrm{Dist}_{r+s}(G). \tag{13.2}$$

The associativity of the product follows from the axiom of coassociativity $(\Delta \circ \mathrm{id}_A) \circ \Delta = (\mathrm{id}_A \circ \Delta) \circ \Delta$. Further, the axiom

$$(\varepsilon \otimes \mathrm{id}) \circ \Delta = \mathrm{id}_A = (\mathrm{id} \otimes \varepsilon) \circ \Delta \tag{13.3}$$

shows that ε is the unit for the multiplication. One calls $\mathrm{Dist}(G)$ the algebra of distributions on G (with support at the origin).[2]

Set $\mathrm{Dist}^+(G) = \{\phi \in \mathrm{Dist}(G) \mid \phi(1) = 0\}$. Then

$$\mathrm{Dist}(G) = k\varepsilon \oplus \mathrm{Dist}^+(G). \tag{13.4}$$

Moreover, since $\Delta(1) = 1 \otimes 1$ one sees that $\mathrm{Dist}^+(G)$ is a two-sided ideal of $\mathrm{Dist}(G)$.

Further, recalling that

$$A \otimes A = k\,(1 \otimes 1) \oplus I \otimes k1 \oplus k1 \otimes I \oplus I \otimes I,$$

the axiom (13.3) implies that for any $a \in I$ one has

$$\Delta(a) \in a \otimes 1 + 1 \otimes a + I \otimes I$$

from which one deduces that, for any $n \geq 2$ and $a_1, \ldots, a_n \in I$, one has:

$$\Delta(a_1 \cdots a_n) \in \prod_{i=1}^{n}(a_i \otimes 1 + 1 \otimes a_i) + \sum_{j=1}^{n} I^j \otimes I^{n+1-j}. \tag{13.5}$$

Thus, if $\phi \in \mathrm{Dist}_r(G)$ and $\psi \in \mathrm{Dist}_r(G)$ with $r, s \geq 1$ and $n = r + s$, then both $\phi\phi$ and $\psi\phi$ vanish on the last sum, whereas $\phi\psi - \psi\phi$ vanish on the product, which is invariant under the swap $a \otimes b \leftrightarrow b \otimes a$. Thus $\phi\psi - \psi\phi$ vanish on I^n and hence belong to Dist_{r+s-1}.

This proves that the filtered algebra $(\mathrm{Dist}_n(G))_{n\geq 0}$ is *almost commutative*, i.e. the associated graded algebra is commutative.

Further, for $r = s = 1$, we obtain that $\mathrm{Dist}_1(G)$ and its subspace $\mathrm{Dist}_1^+(G)$ are Lie algebras for the bracket $[\phi, \psi] = \phi\psi - \psi\phi$. Note that

$$\mathrm{Dist}_1^+(G) \simeq (I/I^2)^*$$

i.e. $\mathrm{Dist}_1^+(G)$ identifies with the tangent space to G at the origin, namely $\mathrm{Lie}(G)$.[3] One can show that the structure of Lie algebra on $\mathrm{Dist}_1^+(G)$ is the same as the structure of Lie algebra on $\mathrm{Lie}(G)$, regarded as the Lie algebra of left-invariant derivations of $A = k[G]$.

[2]This terminology was introduced by Laurent Schwartz when the Bourbaki group was writing the part of his treatise on Lie algebras.

[3]Since $\mathrm{Dist}_1(G) = k\varepsilon \oplus \mathrm{Dist}_1^+(G)$ and since ε is the unit element of the algebra, hence central, one obtains that as Lie algebra $\mathrm{Dist}_1(G)$ is the direct sum of $\mathrm{Lie}(G)$ and the trivial Lie algebra k.

REMARK 13.2. Suppose that $\mathrm{char}(k) = p > 0$ and hat G is smooth over k, of dimension d. Let $r \in \mathbb{N}^*$. The previous definition applies also to the r-th Frobenius kernel G_r of G. In this case, we have seen that $\mathrm{Fr} : G \to G$ is a locally free morphism of rank p^d. It follows that Fr^r is locally free of rank p^{rd}.

(1) Since G_r is the fiber product:

$$\begin{array}{ccc} G_r & \longrightarrow & \mathrm{Spec}(k) \\ \downarrow & & \downarrow e \\ G & \xrightarrow{\mathrm{Fr}^r} & G \end{array}$$

where e is the unit section of G, we see that G_r is a finite k-group scheme of rank p^{rd}, i.e. its coordinate algebra $A = k[G_r]$ is finite dimensional, of dimension p^{rd}.

(2) Since A is finite dimensional, $H = \mathrm{Dist}(G_r)$ is actually the full linear dual A^* hence the transpose of multiplication map $A \otimes A \to A$ induces a linear map $\Delta_H : H \to H \otimes H$ which makes H into a Hopf algebra. It is called the *dual Hopf algebra* of A. Taking the dual again, one obtains that A is the Hopf dual of H: we say that A and H are *dual Hopf algebras*. We will use this property in a later section.

REMARK 13.3. Let $\mathrm{char}(k)$ be arbitrary again. Denote by $\mathfrak{g}$ the Lie algebra of G and by $U(\mathfrak{g})$ the enveloping algebra of $\mathfrak{g}$. The isomorphism of Lie algebras $\mathfrak{g} \xrightarrow{\sim} \mathrm{Dist}_1^+(G)$ induces a unique morphism of associative algebras:

$$\phi : U(\mathfrak{g}) \to \mathrm{Dist}(G).$$

Clearly, its image is the subalgebra of $\mathrm{Dist}(G)$ generated by $\mathfrak{g}$. One can prove the following:

(a) If $\mathrm{char}(k) = 0$ then ϕ is an isomorphism.

(b) If $\mathrm{char}(k) = p$ then $\mathrm{Im}(\phi)$ is the subalgebra $\mathrm{Dist}(G_1)$ of $\mathrm{Dist}(G)$. Further, for any $D \in \mathfrak{g}$, regarded as a left-invariant derivation of $A = k[G]$, the composed map $D^p = D \circ \cdots \circ D$ (p times) is again a left-invariant derivation of A hence it coincides with some element $D^{[p]}$ of $\mathfrak{g}$. This defines an endomorphism $x \mapsto x^{[p]}$ of $\mathfrak{g}$ which is semilinear, i.e. $(zx)^{[p]} = z^p x^{[p]}$ for every $z \in k$. Then one has the following result: ϕ induces an isomorphism

$$U(\mathfrak{g})/J \xrightarrow{\sim} \mathrm{Dist}_1(G)$$

where J is the two-sided ideal of $U(\mathfrak{g})$ generated by the elements $x^p - x^{[p]}$, for $x \in \mathfrak{g}$. (These elements are central in $U(\mathfrak{g})$ hence the left ideal that they generate is already equal to J.)

The importance of the algebras $\mathrm{Dist}(G)$ comes from the following:

PROPOSITION 13.4. *Let V be a G-module, i.e. a right A-comodule $\mu : V \to V \otimes A$. Then V has a structure of left $\mathrm{Dist}(G)$-module,*[4] *given for any $\phi \in \mathrm{Dist}(G)$ and $v \in V$ by $\phi \cdot v = (\mathrm{id}_V \otimes \phi)(\mu(v))$.*

Further, if G is a finite k-group scheme, i.e. if $\dim_k(A) < \infty$, then any $\mathrm{Dist}(G)$-module V has a natural structure of A-comodule, i.e. a structure of G-module.,[5]

PROOF. (1) Recall that ε is the unit 1 of $\mathrm{Dist}(G)$. Then the axiom $(\mathrm{id}_V \otimes \varepsilon) \circ \mu = \mathrm{id}_V$ gives that $1 \cdot v = v$ for all $v \in V$.

[4]Conversely, under various hypotheses on G that will be described later, every finite dimensional $\mathrm{Dist}(G)$-module is a G-module.

[5]One can prove that this is also true if G is a split semi-simple, simply connected k-group and V is finite dimensional, but this requires more work.

Further, let $\phi, \psi \in \mathrm{Dist}(G)$ and $v \in V$ and write $\mu(v) = \sum_i v_i \otimes a_i$ and $\mu(v_i) = \sum_j v_{ij} \otimes a_{ij}$ for all i. Then one has

$$\phi \cdot (\psi \cdot v) = \phi \cdot \sum_i \psi(a_i) v_i = \sum_{i,j} \psi(a_i)\phi(a_{ij}) v_{ij} = (\mathrm{id}_V \otimes \phi \otimes \psi) \circ (\mu \otimes \mathrm{id}_A) \circ \mu(v).$$

But $(\mu \otimes \mathrm{id}_A) \circ \mu = (\mathrm{id}_V \otimes \Delta) \circ \mu$ hence the expression above is $(\phi\psi) \cdot v$. This proves the first assertion.

(2) Suppose that $\dim_k(A) < \infty$. Then, as remarked above, A and $H = \mathrm{Dist}(G)$ are dual Hopf algebras. If V is a left H-module, given by a k-linear map $\lambda : H \otimes V \to V$, we have natural isomorphisms (the second one since $\dim_k(h) < \infty$):

$$\mathrm{Hom}_k(H \otimes V, V) = \mathrm{Hom}_k(V, \mathrm{Hom}_k(H, V)) = \mathrm{Hom}_k(V, V \otimes H^*) = \mathrm{Hom}_k(V, V \otimes A)$$

and one checks without difficulty that the resulting map $\mu : V \to V \otimes A$ is a coaction. □

Example 13.5 (The additive group). Let $G = \mathbb{G}_{a,k}$. Then $A = k[X]$ and $I = (X)$. For any $i \in \mathbb{N}$, let γ_i be the linear form on A defined by $\gamma_i(X^n) = \delta_{i,n}$ (Kronecker symbol). Then $\{\gamma_i \mid i \in \mathbb{N}\}$ is a basis of $\mathrm{Dist}(\mathbb{G}_{a,k})$ and $\gamma_0 = vep$ is the unit element. Let us compute the multiplication table. One has

$$\Delta(X) = X \otimes 1 + 1 \otimes X$$

and hence, for any $n \geq 1$,

$$\Delta(X^n) = \sum_{i=0}^{n} X^i \otimes X^{n-i}.$$

It folllows that for any $r, s \geq 1$, one has $\gamma_r \gamma_s = \binom{r+s}{r} \gamma_{r+s}$. In particular, for $s = 1$ one obtains $\gamma_r \gamma_1 = (r+1)\gamma_{r+1}$ and by induction one obtains that $r!\gamma_1^r = \gamma_r$. For this reason, we will denote γ_1 by γ and γ_r for $r \geq 2$ by the symbol $\gamma^{(r)}$: if $\mathrm{char}(k) = 0$ one has $\gamma^{(r)} = \gamma^r / r!$ and $\mathrm{Dist}(\mathbb{G}_{a,\mathbb{Q}})$ is isomorphic to the polynomial ring $\mathbb{Q}[\gamma]$.[6]

Further, let V be a $\mathbb{G}_{a,k}$-module, given by a coaction $\mu : V \to V \otimes A$. For any $v \in V$, one can write uniquely:

$$\mu(v) = \sum_{n \in \mathbb{N}} v_n \otimes X^n$$

with $v_n = 0$ for all but a finite number of indices n. Then, for each $r \in \mathbb{N}$ one has

$$\gamma^{(r)} v = (\mathrm{id}_V \otimes \gamma^{(r)})(\mu(v)) = v_r$$

hence we can write:

$$\mu(v) = \sum_{n \in \mathbb{N}} \gamma^{(n)} v \otimes X^n. \tag{13.6}$$

Thus, if U_α is a root subgroup in a split semi-simple group G and if we have chosen an isomorphism $\exp_\alpha : \mathbb{G}_{a,k} \xrightarrow{\sim} U_\alpha$, $z \mapsto \exp_\alpha(z)$ and if V is a U_α-module then for any $v \in V$ one has

$$\mu(v) = \sum_{n \in \mathbb{N}} \gamma_\alpha^{(n)} v \otimes X^n$$

and hence, for every $z \in k$:

$$\exp_\alpha(z) v = \sum_{n \in \mathbb{N}} z^n \, \gamma_\alpha^{(n)} v \tag{13.7}$$

which is in accordance with the formula $\exp_\alpha(z) = \sum_{n \in \mathbb{N}} z^n \dfrac{\gamma_\alpha^n}{n!}$ in characteristic 0.

[6] But note that if $\mathrm{char}(k) = p > 0$, the algebra $\mathrm{Dist}(\mathbb{G}_{a,k})$ is not finitely generated: it is generated by the γ_{p^r} for $r \in \mathbb{N}$.

EXAMPLE 13.6 (The multiplicative group). Let $G = \mathbb{G}_{m,k}$. Then $A = k[T, T^{-1}]$ and $I = (T-1)$. For any $n \in \mathbb{N}$, a k-basis of the quotient A/I^{n+1} is given by the images of the $(T-1)^j$ for $j = 0, \dots, n$. So, for each $n \in \mathbb{N}$ let δ_n be the linear form which vanishes on I^{n+1} and on $(T-i)^j$ for $j < n$ but takes the value 1 on $(T-1)^n$. Then $\{\gamma_n \mid n \in \mathbb{N}\}$ is a basis of $\mathrm{Dist}(\mathbb{G}_{m,k})$ and $\delta_0 = vep$ is the unit element. Let us compute the multiplication table. Setting $u = T - 1$

$$\Delta(T) = T \otimes T \quad \text{and hence} \quad \Delta(u) = (u \otimes u) + (u \otimes 1) + (1 \otimes u).$$

Therefore, for any $n \in \mathbb{N}^*$, one has

$$\Delta(u^n) = \sum_{\substack{a,b,c \in \mathbb{N} \\ a+b+c=n}} \frac{n!}{a!b!c!}\, u^{a+b} \otimes u^{a+c}.$$

In the right-hand side, consider only the terms for which $a + b = 1$, that is, $c = n - 1$ and $a = 1, b = 0$ or $a = 0, b = 1$. This gives

$$\Delta(u^n) = nu \otimes u^n + nu \otimes u^{n-1} + \text{ other terms.}$$

For arbitrary $r \in \mathbb{N}^*$ one deduces that

$$\delta_1\delta_r(u^n) = \begin{cases} r & \text{if } r = n; \\ r+1 & \text{if } r = n-1, \text{ i.e. } n = r+1; \\ 0 & \text{otherwise.} \end{cases}$$

Thus one has $\delta_1\delta_r = r\delta_r + (r+1)\delta_{r+1}$, hence $(\delta_1 - r)\delta_r = (r+1)\delta_{r+1}$. By induction one obtains that $r!\delta_r = \delta_1(\delta_1 - 1)\cdots(\delta_1 - r + 1)$. Thus, if $\mathrm{char}(k) = 0$ one obtains that δ_r is the "binomial polynomial"

$$\binom{\delta_1}{r} = \frac{\delta_1(\delta_1 - 1)\cdots(\delta_1 - r + 1)}{r!}$$

(and $\mathrm{Dist}(\mathbb{G}_{m,\mathbb{Q}})$ is isomorphic to the polynomial ring $\mathbb{Q}[\delta_1]$). For this reason, we will denote δ_1 by δ and δ_r for $r \geq 2$ by the symbol $\binom{\delta}{r}$.

Observe that, since $T^n = (T - 1 + 1)^n = \sum_{i=0}^n \binom{n}{i}(T-1)^i$ for $n \geq 0$, we have for all $r, n \in \mathbb{N}$:

$$\binom{\delta}{r}(T^n) = \begin{cases} \binom{n}{r} & \text{if } n \geq r; \\ 0 & \text{otherwise.} \end{cases} \tag{13.8}$$

(Note also that the second case is contained in the first, since $\binom{n}{r} = 0$ when $0 \leq n < r$.) Further, setting $u = T - 1$ we have for every $n > 0$, the following equality in the completion $k[[u]]$ of the local ring of of A at the unit element 1:

$$T^{-1} = \frac{1}{1+u} = \sum_{r \geq 0} (-1)^r u^r$$

and hence, by differentiating, for every $n \geq 2$

$$T^{-n} = \frac{1}{(1+u)^n} = \frac{1}{(n-1)!} \sum_{j \geq 0} (-1)^j (j+n-1)\cdots(j+1)u^j = \sum_{j \geq 0} (-1)^j \binom{j+n-1}{n-1} u^j.$$

Since $(-1)^j\binom{j+n-1}{n-1} = (-1)^j\binom{j+n-1}{j} = \binom{-n}{j}$ (also for $n = 1$) we obtain that $\binom{\delta}{r}(T^{-n}) = \binom{-n}{r}$ for every $r \geq 0$ and $n > 0$.

Therefore, if V is a $\mathbb{G}_{m,k}$-module given by a coaction $\mu : V \to V \otimes A$ and if v is a weight vector of weight $n \in \mathbb{Z}$, i.e. if

$$\mu(v) = v \otimes T^n$$

then $\binom{\delta}{r}v = \binom{n}{r}v$. If $\mathrm{char}(k) = 0$, this is obtained more easily by noting that the generator δ of $\mathrm{Lie}(\mathbb{G}_{m,k})$ acts on v by $\delta v = -nv$ and hence

$$\binom{\delta}{r}v = \frac{\delta(\delta-1)\cdots(\delta-r+1)}{r!}v = \frac{-n(-n-1)\cdots(-n-r+1)}{r!}v.$$

REMARK 13.7. Denote temporarily the augmentation ideal I by $\mathfrak{m}$, to emphasize that it is a maximal ideal. The localized ring $A_{\mathfrak{m}}$ is the local ring $\mathcal{O}_{G,e}$ at the unit elements and for every $n \in \mathbb{N}$ we have isomorphisms of vector spaces

$$A/\mathfrak{m}^{n+1} \simeq \mathcal{O}_{G,e}/(\mathfrak{m}\mathcal{O}_{G,e})^{n+1}.$$

Thus we see that as k vector space, $\mathrm{Dist}(G)$ depends only on the local ring $\mathcal{O}_{G,e}$ hence is determined by any affine open neighbourhood of e. We will apply this in the case where G is a split semi-simple group over k.

PROPOSITION 13.8. *Let G be a split semi-simple, simply connected group over k, with maximal torus T and root system R. Let $\mathfrak{g}$ and $\mathfrak{t}$ be the Lie algebras of G and T. Fix a base $\Delta = \{\alpha_1, \ldots, \alpha_\ell\}$ of R and a numbering $\beta_1, \ldots, \beta_N$ of R^+ such that $\beta_i = \alpha_i$ for $i = 1, \ldots, \ell$. Then:*

(1) *Since G is simply-connected, the elements $\alpha_i^\vee$ form a $\mathbb{Z}$-basis of $X_*(T)$ and their differentials H_i form a k-basis of $\mathfrak{t} = X_*(T) \otimes k$. Further, for $j = 1, \ldots, N$ denote by H_j the differential of $\beta_j^\vee$; it is a combination with coefficients in $\mathbb{N}$ of the H_i's for $i = 1, \ldots, \ell$.*

(2) *For $j = 1, \ldots, N$, choose generators X_j and Y_j of $\mathfrak{g}_{\beta_j}$ and $\mathfrak{g}_{-\beta_j}$ respectively, such that $[Y_j, X_j] = H_j$. Then the elements*

$$Y_N^{(a_n)} \cdots Y_1^{(a_1)} \binom{H_1}{b_1} \cdots \binom{H_\ell}{b_\ell} X_1^{(c_1)} \cdots X_N^{(c_N)} \tag{13.9}$$

with the $a_j, c_j, b_i \in \mathbb{N}$, form of k-basis of $\mathrm{Dist}(G)$. Further, if $\mathrm{char}(k) = p$, then these elements with $0 \le a_j, c_j, b_i < p^r$ form a k-basis of $\mathrm{Dist}(G_r)$.

(3) *If V is a T-module and $v \in V$ a vector of weight $\mu \in X(T)$, then for $i = 1, \ldots, \ell$ and $b \in \mathbb{N}$ one has*

$$\binom{H_i}{b}v = \binom{\langle \mu, \alpha_i^\vee \rangle}{b}v. \tag{13.10}$$

PROOF. (1) For $T = \mathbb{G}_{m,k}$ one has $X_*(T) = \mathbb{Z}\omega$ where ω is the identity map from $\mathbb{G}_{m,k}$ to T. Identifying $\mathrm{Lie}(\mathbb{G}_{m,k})$ with k and $\mathrm{Hom}_k(k, \mathrm{Lie}(T)) = \mathrm{Lie}(T)$, we obtain that the differential $d\omega$ is a generator of $\mathrm{Lie}(T)$.[7] In the general case, one has $X_*(T) = \bigoplus_{\alpha\in\Delta} \mathbb{Z}\alpha^\vee$ and accordingly T is isomorphic to the direct product of the $\alpha^\vee(\mathbb{G}_{m,k})$. The first assertion follows. The second assertion (which we wrote only to introduce the H_j's) follows from the fact that $\Delta^\vee$ is a base of the root system $R^\vee$.

(2) The multiplication map

$$U_{-\beta_N} \times \cdots \times U_{-\beta_1} \times T \times U_{\beta_1} \times \cdots \times U_{\beta_N} \to G$$

is an isomorphism from the left-hand side onto an open neighbourhood Ω of the unit element e. The result then follows from the previous remark and the description of $\mathrm{Dist}(\mathbb{G}_{a,k})$ and $\mathrm{Dist}(\mathbb{G}_{m,k})$.

(3) This follows from the discussion in Example 13.6 and the fact that $T \simeq \prod_{i=1}^{\ell} \alpha_i^\vee(\mathbb{G}_{m,k})$. □

[7] That is, we use the identification $\mathrm{Hom}_k(k, \mathrm{Lie}(T)) = \mathrm{Lie}(T)$ to identify $d\omega$ with its value at the generator 1_k of k.

REMARK 13.9. It follows from point (2) that we have isomorphisms

$$\text{Dist}(G) \simeq \text{Dist}(U) \otimes \text{Dist}(B^+) \qquad \text{and} \qquad \text{Dist}(G_r) \simeq \text{Dist}(U_r) \otimes \text{Dist}(B_r^+) \tag{13.11}$$

of $(\text{Dist}(U), \text{Dist}(B^+)$-bimodules and $(\text{Dist}(U_r), \text{Dist}(B_r^+)$-bimodules, respectively.

Let us introduce another notation and definition. Since we assumed that our split semi-simple group G is simply-connected, the set of simple coroots $\{\alpha_1^\vee, \dots, \alpha_\ell^\vee\}$ form a $\mathbb{Z}$-basis of the cocharacter group $X_*(T)$.

NOTATION 13.10. We denote by $(\omega_1, \dots, \omega_\ell)$ the dual basis of the character group $X(T)$, i.e. one has $\langle \omega_i, \alpha_j^\vee \rangle = \delta_{ij}$ (Kronecker symbol). The ω_i are called the *fundamental weights*.

DEFINITION 13.11. Suppose that $\text{char}(k) = p > 0$. For any $r \in \mathbb{N}^*$, the set of r-restricted dominant weights is:

$$X_r(T) = \{\lambda \in X(T)^+ \mid 0 \leq \langle \lambda, \alpha^\vee \rangle < p^r, \quad \forall \alpha \in \Delta\}.$$

Thus, $X_r(T) = \{\sum_{i=1}^\ell a_i \omega_i \mid a_i \in \mathbb{N}, \quad a_i < p^r\}$.

Now, one has the following useful lemma, see e.g. [**Hu72**], Lemma 26.2.

LEMMA 13.12. *For $j = 1, \dots, N$, one has for every $a, b \in \mathbb{N}$ the commutation formula:*

$$X_j^{(a)} Y_j^{(b)} = \sum_{i=0}^{\min(a,b)} Y_j^{(b-i)} \binom{H_j - a - b + 2i}{i} X_j^{(a-i)}.$$

Before stating and proving a more general result, let us mention the following easy proposition.

PROPOSITION 13.13. *Assume that $\text{char}(k) = p > 0$ and that $G = \text{SL}_2$. Then for $n = 0, \dots, p-1$, the induced module $H^0(n)$ is simple as a G_1-module, a fortiori as a G-module. In particular, one has $H^0(n) = L(n)$ for $n = 0, \dots, p-1$.*

PROOF. Denote by $Y^{(a)}$, $X^{(c)}$ and $\binom{H}{b}$ the standard generators of $\text{Dist}(U)$, $\text{Dist}(U^+)$ and $\text{Dist}(T)$, as given in Prop. 13.8. On the other hand, let $\{x, y\}$ be the standard basis of $V = k^2$. We have seen that $H^0(n) = S^n(V) =$ the space of homogeneous polynomials in x, y of degree n. For any k-algebra R and $r \in R$, one has

$$\begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix} x^n = (x + zy)^n = \sum_{i=0}^n \binom{n}{i} r^i x^{n-i} y^i.$$

If we regard $H^0(n)$ as a U-module and identify $k[U]$ to a polynomial ring in one variable $k[w]$, it follows that the corresponding coaction $\nu : H^0(n) \to H^0(n) \otimes k[Z]$ satisfies

$$\nu(x^n) = \sum_{i=0}^n \binom{n}{i} x^{n-i} y^i \otimes w^i$$

and hence the elements $Y^{(r)}$ of $\text{Dist}(U)$ act on x^n by:

$$Y^{(r)} x^n = \begin{cases} \binom{n}{r} x^{n-r} y^r & \text{for } r = 0, \dots, n; \\ 0 & \text{if } r > n. \end{cases} \tag{13.12}$$

This is true for any $n \in \mathbb{N}$. Further, under the assumption that $n < p$ all coefficients $\binom{n}{r}$ for $r = 0, \dots, n$ are non-zero in k. Therefore for $n < p$ we obtain, firstly, that $H^0(n)$ is generated as $\text{Dist}(U_1)$-module, a fortiori as $\text{Dist}(G_1)$-module, by the vector x^n.

Now, let $w \neq 0$ be arbitrary in $H^0(n)$. By (13.12) we can written uniquely

$$w = \sum_{i=0}^{d} z_i Y^{(i)} x^n$$

for some $d \in \{0, \ldots, n\}$, the z_i in k and $z_d \neq 0$. Now observe that $X^{(j)}x^n = 0$ for all $j > 0$ because, if non-zero, $X^{(j)}jx^n$ would have weight $n+2j$. This, combined with the previous lemma and Example 13.6, gives:

$$X^{(d)}w = z_d \binom{H}{d} x^n = z_d \binom{n}{d} x^n$$

As $z_d \neq 0$ by assumption and $\binom{n}{d} \neq 0$ since $0 \leq d \leq n < p$, this shows that the $\mathrm{Dist}(G_1)$-submodule generated by w contains x^n, hence equals $H^0(n)$ by our first observation above. This proves that $H^0(n)$ is simple as a $\mathrm{Dist}(G_1)$-module, i.e. as a G_1-module, hence a fortiori as a G-module. □

14. Curtis-Humphreys' theorem

We want to prove the following theorem, due to Curtis [**Cu60**] in the case $r = 1$ and generalised to $r \geq 1$ by Humphreys [**Hu77**].

THEOREM 14.1. *Let G be a split semisimple, simply connected group over k, with* $\mathrm{char}(k) = p > 0$. *Let $r \in \mathbb{N}^*$ and $\lambda \in X_r(T)$. Then, regarded as G_r-module, $L(\lambda)$ is simple.*

PROOF. The proof will be in several steps. Recall that $\overline{k}$ denotes an algebraic closure of k. Firstly, one has the following lemma:

LEMMA 14.2. *Let H be an algebraic group over k such that $H \otimes \overline{k}$ is reduced. Let M be a H-module and N a subspace of M such that $G(\overline{k})(N \otimes \overline{k}) \subset N \otimes \overline{k}$. Then N is a sub-H-module of M.*

PROOF. For simplicity of notation, suppose that $\dim_k(M) < \infty$. Let $(v_1, \ldots, v_r)$ be a k-basis of N, extend it to a k-basis $(v_1, \ldots, v_m)$ of M. Let $A = k[H]$ and $\mu : M \to M \otimes A$ the coaction. For $j = 1, \ldots, r$, one can write uniquely

$$\mu(v_j) = \sum_{i=1}^{m} v_i \otimes a_{ij} \tag{14.1}$$

with $a_{ij} \in A$. Then, for a fixed j and for any $g \in G(\overline{k})$ one has in $M \otimes \overline{k}$ the equality:

$$g \cdot (v_j \otimes 1) = \sum_{i=1}^{m} v_i \otimes g(a_{ij}).$$

By hypothesis, this is an element of $N \otimes \overline{k}$ and it follows that for each $i > r$ one has $g(a_{ij}) = 0$ for all $g \in G(\overline{k})$. But $A \otimes \overline{k}$ is a finitely generated $\overline{k}$-algebra, hence a Jacobson algebra, i.e. the intersection of all its maximal ideals $\mathrm{Ker}(g)$, for $g \in G(\overline{k})$, is the nilradical of A, which is 0 by assumption. It follows that $a_{ij} = 0$ for all $j = 1, \ldots, r$ and $i > r$, and hence (14.1) shows that N is a subcomodule of M. □

PROPOSITION 14.3. *Let $r \in \mathbb{N}^*$ and $\lambda \in X_r(T)$. Let kv_λ be the unique line of weight λ in $L(\lambda)$. Then $L(\lambda)$ is generated by v_λ as a G_r-module, and even as a U_r-module.*

PROOF. Let us prove the firsrt assertion. Let $N = \mathrm{Dist}(G_r)v_\lambda$ be the G_r-submodule of $L(\lambda)$ generated by v_λ. Let us prove that N is a G-submodule. By the previous lemma, it suffices to prove that $N \otimes \overline{k}$ is stable by $G(\overline{k})$. So, to abbreviate notation, we may assume in the sequel of

the proof that $k = \overline{k}$. Since G_r is a normal subgroup, $\mathrm{Dist}(G_r)$ is stable by the adjoint action of $G(k)$ hence for any $g \in G(k)$ we have:

$$gN = \mathrm{Dist}(G_r)gv_\lambda \tag{14.2}$$

so it suffices to prove that $gv_\lambda \in N$ for every $g \in G(k)$. One knows that $G(k)$ is generated by $B^+(k)$ and the elements n_α of $N_G(T)(k)$, for $\alpha \in \Delta$. For $b \in B^+(k)$ the results is clear since $bv_\lambda = \lambda(b)v_\lambda$.

So let $\alpha \in \Delta$. Then n_α induces a linear isomorphism between the weight spaces $L(\lambda)_\lambda$ and $L(\lambda)_{s_\alpha(\lambda)}$, both 1-dimensional. Further, setting $d = \langle \lambda, \alpha^\vee \rangle$, one has

$$s_\alpha(\lambda) = \lambda - d\alpha$$

and $0 \leq d < p^r$ since $\lambda \in X_r(T)$. Hence the element $Y_\alpha^{(d)}$ belongs to $\mathrm{Dist}(G_r)$, as well as $X_\alpha^{(d)}$. Further, $Y_\alpha^{(d)}v_\lambda$ is of weight $\lambda - d\alpha$, and it is non-zero because by Lemma 13.12 combined with point (3) of Prop. prop-nota-sssc one has

$$X_\alpha^{(d)}Y_\alpha^{(d)}v_\lambda = \binom{H_\alpha}{d}v_\lambda = \binom{d}{d}v_\lambda = v_\lambda.$$

Therefore, $n_\alpha v_\lambda$ is a non-zero multiple of $Y_\alpha^{(d)}v_\lambda$ and hence belongs to $N = \mathrm{Dist}(G_r)$.

This completes the proof that $N = \mathrm{Dist}(G_r)$ is stable by $G(\overline{k})$ and is hence a G-submodule of $L(\lambda)$. Since the latter is a simple G-module, it follows that $L(\lambda) = \mathrm{Dist}(G_r)$. This proves the first assertion.

Finally, since $\mathrm{Dist}(G_r) = \mathrm{Dist}(U_r) \otimes \mathrm{Dist}(B_r^+)$ and $\mathrm{Dist}(B_r^+)v_\lambda = kv_\lambda$, we obtain that $\mathrm{Dist}(G_r)v_\lambda = \mathrm{Dist}(U_r)v_\lambda$. □

By a duality argument, detailed in the next section, one obtains the following dual proposition:

Proposition 14.4. *Let $r \in \mathbb{N}^*$ and $\lambda \in X_r(T)$. Then $L(\lambda)^{U_r^+}$ is the line kv_λ, whereas $L(\lambda)^{U_r}$ is the line $L(\lambda)_{w_0\lambda}$.*

Assuming this, we can finish the proof of Th. 14.1. Let V be a non-zero G_r submodule of $L(\lambda)$. Since U_r^+ is a unipotyent group, one has $V^{U_r^+} \neq 0$ hence V contains the line kv_λ. Since $\mathrm{Dist}(U_r)v_\lambda = L(\lambda)$, one obtains $V = L(\lambda)$. □

Consider now the Steinberg module $\mathrm{St}_r = L(\sigma_r)$, where $\sigma_r = (p^r - 1)\rho$. Note that σ_r belongs to $X_r(T)$ hence St_r is simple as G_r module. Further, its lowest weight is $w_0\sigma_r = -\sigma_r$ and hence one the difference $\sigma_r - w_0\sigma_r = 2\sigma_r$ equals $(p^r - 1)\sum_{\beta \in R^+} \beta$.

Observe that since B_r is a normal subgroup of B, it is normalised by T, and this induces an action by conjugation of T on $\mathrm{Dist}(U_r)$ One has the following proposition:

Proposition 14.5. *Let $r \in \mathbb{N}^*$. Since*

1. *$\mathrm{Dist}(U_r)$ has a unique minimal non-zero left ideal S, which is the line spanned by the monomial $Y_N^{(p-1)} \cdots Y_1^{(p-1)}$ (it is also a right ideal). Further, T acts on this line by the weight $-2\sigma_r$, and all other weights are $> -2\sigma_r$.*
2. *For any $\lambda \in X_r(T)$, the surjective map $\phi : \mathrm{Dist}(U_r) \to L(\lambda)$, $x \mapsto xv_\lambda$ is T-equivariant.*
3. *For $\lambda = \sigma_r$, this surjective map is injective, hence an isomorphism of $\mathrm{Dist}(U_r)$-modules. In particular, one has $\dim_k \mathrm{St}_r = p^{rN}$.*

Proof. (1) For the first part, we refer to [**Ja03**], §§I.8.6-7 or Prop. II.3.8 a). The second part follows easily from the fact that the T-weight of a monomial $Y_N^{(a_N)} \cdots Y_1^{(a_1)}$ is $-\sum_{i=1}^n a_i\beta_i$.

(2) is clear. Let us prove (3). Since ϕ is surjective (by the proof of Prop. 14.3), there exist a non-zero element $x \in \mathrm{Dist}(U)$ such that xv_{σ_r} is the lowest weight vector $v_{-\sigma_r}$. Since ϕ is

T-equivariant we may assume that x has weight $-\sigma_r$, and hence x is a generator of the line S. Since this is the unique minimal non-zero left ideal of $\mathrm{Dist}(U_r)$, it follows that ϕ is injective. It is therefore bijective. In particular, one has $\dim_k \mathrm{St}_r = \dim_k \mathrm{Dist}(U_r) = p^{rN}$. □

We can now finish the proof of Kempf's vanishing theorem 12.1 by proving Prop. 12.4, which we repeat below

PROPOSITION 14.6. *The non-zero morphism of G_rB-modules $\phi_r : \mathrm{St}_r \to \mathrm{Ind}_B^{G_rB}(\sigma_r)$ is an isomorphism.*

PROOF. One has $B \cap G_r = B_r$ and hence the inclusion $B \hookrightarrow G_rB$ induces an isomorphism of schemes $G_rB/B \simeq G_r/B_r$. By duality, the isomorphism

$$\mathrm{Dist}(G_r) \simeq \mathrm{Dist}(U_r^+) \otimes \mathrm{Dist}(B_r)$$

implies that one has an isomorphism $k[G_r] \simeq k[U_r^+] \otimes k[B_r]$ of (U_r^+, B_r)-modules and it follows that for any B_r-module M the induced module

$$\mathrm{Ind}_B^{G_rB}(M) = (k[G_r] \otimes M)^{B_r}$$

is isomorphic to $k[U_r^+] \otimes M$ as k-vector space. In particular, when $M = k_\lambda$ for some $\lambda \in X(T)$ one obtains that $\mathrm{Ind}_B^{G_rB}(\lambda)$ has dimension p^{rN}.

Now, ϕ_r is non-zero hence injective since St_r is a simple G_r-module. Further, both modules have dimension p^{rN}. It follows that ϕ_r is an isomorphism. □

15. Invariants and coinvariants for finite group schemes

To be written soon. Next lecture will be: Steinberg's Tensor Product Theorem and a brief survey of alcove geometry.