Lec 3: algebraic groups & Lie algebras III

1) Distribution algebras

1) Distribution algebras

1.0) Introduction.

Let $\mathbb{F}$ be an algebraically closed field, $G\subset GL_n(\mathbb{F})$ algebraic subgroup & $\mathfrak{g}=T_eG\subset Mat_n(\mathbb{F})$, the tangent space at the unit e. We want to understand additional structures on $\mathfrak{g}$. In Lec 2, Sec 2, we stated:

Thm: 1) $\mathfrak{g}$ is closed under $[\cdot,\cdot]$: $\xi,\eta\in\mathfrak{g}\Rightarrow[\xi,\eta]=\xi\eta-\eta\xi\in\mathfrak{g}$.

1') If $\operatorname{char}\mathbb{F}=p>0$, then $\mathfrak{g}$ is also closed under $\xi\mapsto\xi^p$.

Let $H\subset GL_m$ be another algebraic subgroup & $\Phi: G\to H$ be an algebraic group homomorphism & $\varphi=T_e\Phi$. Then

2) $[\varphi(\xi),\varphi(\eta)]=\varphi([\xi,\eta])\ \forall\ \xi,\eta\in\mathfrak{g}$.

2') If $\operatorname{char}\mathbb{F}=p>0$, then $\varphi(\xi^p)=\varphi(\xi)^p\ \forall\ \xi\in\mathfrak{g}$.

Today we prove this theorem. First, to G we assign an associative algebra $(\mathcal{D}(G),*)$ of "distributions on G supported at e" in a functorial way (meaning, in particular, that Φ gives rise to an algebra homomorphism $\Phi_*:\mathcal{D}(G)\to\mathcal{D}(H)$) & s.t. $\mathfrak{g}$ is naturally a subspace in $\mathcal{D}(G)$. Then we show that for $\xi,\eta\in\mathfrak{gl}_n\subset\mathcal{D}(GL_n)$, we have $\xi*\eta-\eta*\xi=[\xi,\eta]$, $\xi^{*p}=\xi^p\in\mathfrak{gl}_n$.

This observation, the functoriality of $\mathcal{D}(G)$ & a few other things will allow us to prove the theorem.

1.1) Space of distributions

First we consider a general situation: X is an affine variety over $\mathbb{F}$, $A=\mathbb{F}[X]$, $\alpha\in X$, $\mathfrak{m}_\alpha=\{f\in A \mid f(\alpha)=0\}$, the max. ideal of α.

By a distribution on X supported at α we mean any element $\delta\in A^*$ s.t. $\exists\, k>0 \mid \delta(\mathfrak{m}_\alpha^k)=0$, i.e. $\delta\in(A/\mathfrak{m}_\alpha^k)^*\subset A^*$

All distributions supported at α form the subspace

$$D_\alpha(X):=\bigcup_{k\geqslant 0}\underbrace{(A/\mathfrak{m}_\alpha^k)^*}\subset A \quad \text{ascending chain of subspaces}$$

In particular, $T_\alpha X=\{\delta\in A^* \mid \delta(1)=\delta(\mathfrak{m}_\alpha^2)=0\}\subset D_\alpha(X)$.

Example: $X=\mathbb{F}$, $\alpha=0$. Then $A=\mathbb{F}[x]$, $\mathfrak{m}_\alpha=(x)$, $A/\mathfrak{m}_\alpha^k=\operatorname{Span}_{\mathbb{F}}(1,\dots x^{k-1})$

The space $D_0(\mathbb{F})=\bigcup_{k\geqslant 0}(A/\mathfrak{m}_\alpha^k)^*$ has basis $\delta^{(i)}, i\in\mathbb{Z}_{\geqslant 0}$, given by

$$\delta^{(i)}(x^j)=\delta_{i,j} \text{ (Kronecker symbol)}$$

Now let $\varphi: X\to Y$ be a morphism, $\varphi^*:\mathbb{F}[Y]\to\mathbb{F}[X]$ be the corresponding homomorphism & $\varphi_*:\mathbb{F}[X]^*\to\mathbb{F}[Y]^*$ be its dual map.

Lemma: $\varphi_*(D_\alpha(X))\subset D_{\varphi(\alpha)}(Y)$

Proof: as we've seen in the proof of Lemma in Sec. 1.2 of Lec 2, $\varphi^*(\mathfrak{m}_{\varphi(\alpha)}^k)\subset\mathfrak{m}_\alpha^k$. So for ξ vanishing on $\mathfrak{m}_\alpha^k$ we have $\langle\varphi_*(\xi),f\rangle=\langle\xi,\varphi^*(f)\rangle=0\ \ \forall f\in\mathfrak{m}_{\varphi(\alpha)}^k$. $\square$

1.2) Group case

Now let G be an algebraic group & $\alpha=e\in G$. Write $D(G)$ for $D_e(G)$. There's a map $*: D(G)\times D(G)\to D(G)$ defined as follows. Let $\mu: G\times G\to G$ denote the product map. It gives rise to the

pullback homomorphism $\mu^*: \mathbb{F}[G] \to \mathbb{F}[G\times G] = \mathbb{F}[G]\otimes\mathbb{F}[G]$.
For $\delta_1, \delta_2 \in \mathcal{D}(G)$ define their convolution $\delta_1 * \delta_2 \in \mathbb{F}[G]^*$ by
$$[\delta_1 * \delta_2](f) = [\delta_1 \otimes \delta_2](\mu^*(f)),$$
here $\delta_1\otimes\delta_2 : \mathbb{F}[G]\otimes\mathbb{F}[G] \to \mathbb{F}$ is described by $[\delta_1\otimes\delta_2](f_1\otimes f_2) = \delta_1(f_1)\delta_2(f_2)$.

Example cont'd: Let $G = \mathbb{G}_a\ (=(\mathbb{F},+)) \Rightarrow \mu(x,y) = x+y$. Identifying $\mathbb{F}[G\times G]$ w. $\mathbb{F}[x_1,x_2]$ (w. $x_1 = x\otimes 1$ & $x_2 = 1\otimes x$), we have $\mu^*(f) = f(x_1+x_2)$ $\forall f\in\mathbb{F}[G] = \mathbb{F}[x]$. We want to compute $\delta^{(i)} * \delta^{(j)}$.

$\delta^{(i)} * \delta^{(j)}(x^k) = \delta^{(i)}\otimes\delta^{(j)}(\mu^*(x^k)) = \delta^{(i)}\otimes\delta^{(j)}((x_1+x_2)^k) = [\text{coeff. of } x_1^i x_2^j\ (= x^i\otimes x^j) \text{ in } (x_1+x_2)^k] = \delta_{i+j,k}\binom{i+j}{i} \Rightarrow \delta^{(i)} * \delta^{(j)} = \binom{i+j}{i}\delta^{(i+j)}$.

This computation allows to realize $\mathcal{D}(\mathbb{G}_a)$ as follows: consider the subgroup $B = \mathrm{Span}_{\mathbb{Z}}(\delta^i/i!) \subset \mathbb{Q}[\delta]$. It's a subring. We identify $\mathcal{D}(\mathbb{G}_a)$ w. $\mathbb{F}\otimes_{\mathbb{Z}} B$ via $\delta^{(i)} \leftrightarrow 1\otimes(\delta^i/i!)$. In particular, if char $\mathbb{F} = 0$, then $\mathcal{D}(\mathbb{G}_a) \simeq \mathbb{Q}[\delta]$, while in case of char p we get a more complicated, in fact, infinitely generated algebra.

Note that $\mathfrak{g} = \mathbb{F}$ embeds into $\mathcal{D}(\mathbb{G}_a)$ as $\mathbb{F}\delta^{(1)}$.

Premium exercise/example. Here we compute $\mathcal{D}(\mathbb{G}_m)$. Consider the subring $C = \mathrm{Span}_{\mathbb{Z}}(\binom{\delta}{i} \mid i\geqslant 0) \subset \mathbb{Q}[\delta]$, where $\binom{\delta}{i} = \frac{\delta(\delta-1)\dots(\delta-i+1)}{i!}$.
Then $\mathcal{D}(\mathbb{G}_m) \xrightarrow{\sim} \mathbb{F}\otimes_{\mathbb{Z}} C$. Hint: $\mathcal{D}(\mathbb{G}_m)$ has basis δ_i ($i\in\mathbb{Z}$), where $\delta_i((x-1)^j) = \delta_{ij}$. Then $\delta_i \longleftrightarrow 1\otimes\binom{\delta}{i}$.

Here's a general result about $\mathcal{D}(G)$ that we are going to use in the proof of the main theorem.

Proposition: 0) $\mathcal{D}(G)*\mathcal{D}(G)\subset\mathcal{D}(G)$

1) $(\mathcal{D}(G),*)$ is an associative unital algebra w. unit ε given by $\varepsilon|_{\mathfrak{m}_e}=0$ & $\varepsilon(1)=0$.

2) If $\varphi: G\longrightarrow H$ is an algebraic group homomorphism, then φ_*: $\mathcal{D}(G)\to\mathcal{D}(H)$ is a unital algebra homomorphism.

Proof: Set $A=\mathbb{F}[G]$, $\mathfrak{m}=\mathfrak{m}_e\subset A$

0) Let $\delta_i\in(A/\mathfrak{m})^{k_i}$ $(i=1,2)$. We claim $[\delta_1*\delta_2](f)=0$ $\forall f\in\mathfrak{m}^{k_1+k_2}$, this will imply 0). By definition, $[\delta_1*\delta_2](f)=[\delta_1\otimes\delta_2](\mu^*(f))$. Note that $\delta_1\otimes\delta_2$ vanishes on $\mathfrak{m}^{k_1}\otimes A$ & $A\otimes\mathfrak{m}^{k_2}$ so it's enough to show that $\mu^*(f)\in\mathfrak{m}^{k_1}\otimes A+A\otimes\mathfrak{m}^{k_2}$. Since $\mu(e,e)=e$, $\mu^*(\mathfrak{m})\subset\mathfrak{m}_{(e,e)}$. We observe that $\mathfrak{m}_{(e,e)}=\mathfrak{m}\otimes A+A\otimes\mathfrak{m}$ (exercise. hint: have $\supset$ & $A\otimes A=\mathbb{F}\cdot1\oplus(\mathfrak{m}\otimes A+A\otimes\mathfrak{m})$ b/c $\forall f_1\otimes f_2\in$ r.h.s.). So $\mu^*(\mathfrak{m}^{k_1+k_2})\subset\mu^*(\mathfrak{m})^{k_1+k_2}\subset(\mathfrak{m}\otimes A+A\otimes\mathfrak{m})^{k_1+k_2}\subset$[binomial formula] $\mathfrak{m}^{k_1}\otimes A+A\otimes\mathfrak{m}^{k_2}$. $\square$ of 0).

1) We'll deduce the associativity of $*$ from that of the product in G, which amounts to the claim that the following diagram is commutative:

$$\begin{tikzcd} G\times G\times G \arrow[r, "\mu\times id"] \arrow[d, "id\times\mu"] & G\times G \arrow[d, "\mu"] \\ G\times G \arrow[r, "\mu"'] & G \end{tikzcd}$$

Equivalently, the diagram of pullbacks is commutative:

$$\begin{tikzcd} A\otimes A\otimes A & A\otimes A \arrow[l, "(\mu\times id)^*=\mu^*\otimes id"'] \\ A\otimes A \arrow[u, "(id\times\mu)^*=id\otimes\mu^*"] & A \arrow[l, "\mu^*"'] \arrow[u, "\mu^*"'] \end{tikzcd}$$

$a\otimes b\mapsto\mu^*(a)\otimes b$

Now $[(\delta_1*\delta_2)*\delta_3](f)=[(\delta_1*\delta_2)\otimes\delta_3](\mu^*(f))=$

$$[\delta_1\otimes\delta_2\otimes\delta_3]([\mu^*\otimes id](\mu^*(f)))$$ reverse computation

commut. diagram $\;\; \overset{\|}{([id\otimes\mu^*](\mu^*(f))]} = [\delta_1 * (\delta_2 * \delta_3)](f)$

The proof that ε is a unit is left as exercise $\square$ of 1).

2) similar to 1) using the commutative diagram

$$\begin{tikzcd} G\times G \arrow[r, "\mu_G"] \arrow[d, "\varphi\times\varphi"] & G \arrow[d, "\varphi"] \\ H\times H \arrow[r, "\mu_H"] & H \end{tikzcd}$$

$$[\varphi_*(\delta_1*\delta_2)](f) = [\delta_1*\delta_2](\varphi^*(f)) = [\delta_1\otimes\delta_2](\mu_G^*\circ\varphi^*(f))$$

$$\| $$

$$[\varphi_*(\delta_1)*\varphi_*(\delta_2)](f) = [\varphi_*(\delta_1)\otimes\varphi_*(\delta_2)](\mu_H^*(f)) = [\delta_1\otimes\delta_2]((\varphi^*\otimes\varphi^*)\circ\mu_H^*(f))$$

$\square$ of 2).

1.3) Case of GL_n

Proposition:

For $A, B\in \mathfrak{gl}_n \subset D(GL_n)$, we have: $A*B - B*A = [A,B]\in\mathfrak{gl}_n$ & in the case when char $\mathbb{F} = p$, we have $A^{*p} = A^p \in \mathfrak{gl}_n$

Proof: • Case of commutator

We interpret the e-derivation A as $f\mapsto \frac{1}{t}(f(I+At) - f(I))|_{t=0}$ (Rem. ii) in Sec 1.1 of Lec 2), equivalently

$A(f) = $ [coefficient of t in (the Taylor expansion of) $f(I+tA)$]

So for $F\in\mathbb{F}[GL_n\times GL_n]$, we have

(1) $[A\otimes B](F) = $ [coefficient of ts in $F(I+tA, I+sB)$]

Indeed, (1) holds for F of the form $f_1\otimes f_2$, hence in general.

Note that $[\mu^*(f)](I+tA, I+sB) = f((I+tA)(I+sB)) =$

$= f(I + tA + sB + ts\,AB)$. So (1) for $F = \mu^*(f)$ is the sum of 2 terms.

(i) The contribution of tA, sB. It's equal

$$\sum_{i,j,k,e=1}^{n} \frac{\partial^2 f}{\partial x_{ij}\,\partial x_{ke}}(I)\, A_{ij} B_{ke},$$

where the notation is as follows: we write $C \in Mat_n(\mathbb{F})$ as (C_{ij}) & x_{ij} denote the variable corresponding to the matrix entry ij (so that $C_{ij} = x_{ij}(C)$ & f is a function of the variables x_{ij}).

(ii) The contribution of $ts\,AB$ is $\sum_{i,j=1}^{n} \frac{\partial f}{\partial x_{ij}}(AB)_{ij}$, which is $AB \in Mat_n(\mathbb{F}) = T_e GL_n \subset \mathcal{D}(GL_n)$.

To finish the proof note that (i) doesn't change if we swap A & B, hence in the difference $[A*B - B*A](f)$ these terms cancel out & we get $A*B - B*A = [A,B]$.

• Case of pth power. Here char $\mathbb{F} = p$. We want to show that the coefficient of $t_1 \dots t_p$ in (the Taylor expansion of)

(2) $f\left(\prod_{i=1}^{p}(I + t_i A)\right) = f\left(\sum_{S \subset \{1,..p\}} t_S A^{|S|}\right)$, where $t_S := \prod_{s \in S} t_s$

This coefficient is equal to:

(3) $\sum \frac{\partial^k f}{\partial x_{i_1 j_1} \dots \partial x_{i_k j_k}}(I) \prod_{e=1}^{k} (A^{|S_e|})_{i_e j_e}$

where the sum is taken over the following indexing set

$Ind = \{(S_1, \dots S_k, (i_1, j_1), \dots (i_k, j_k)) \mid 1 \le k \le p,\ 1 \le i_e, j_e \le n,\ \{1,..p\} = S_1 \sqcup \dots \sqcup S_k\}$

(where S_i's correspond to taking the summands in the r.h.s. of (2)).
The symmetric group $\mathfrak{S}_p$ acts on Ind by permuting $\{1,..p\}$ - and so changing S_i's but not their cardinalities. So the summands in (3) corresponding to the indexes in the same orbit are equal. The number of elements in the orbit of $(S_1, \dots S_k, \dots)$ is $p!/|S_1|! \dots |S_k|!$

– so divisible by p unless $k=1$, where the number is 1 & the corresponding summands are $\frac{\partial f}{\partial x_{ij}}(A^p)_{ij}$ $(1\leq i,j\leq n)$. The orbits whose cardinalities are divisible by p contribute multiples of p, i.e. 0 b/c char $\mathbb{F}$ $=p$. So $(3)=\sum_{i,j=1}^{n}\frac{\partial f}{\partial x_{ij}}(A^p)_{ij}$, which is $A^p\in \mathrm{Mat}_n(\mathbb{F})\subset \mathcal{D}(GL_n)$ $\square$