Algebraic groups and all in characteristic p.

0) Reminder

$\mathbb{F}$ char p field, G alg. group$/\mathbb{F}$

$\rightsquigarrow \mathfrak{g} = Lie(G)$, $\mathcal{U} := \mathcal{U}(\mathfrak{g})$

Last time, we introduced the p (th power) map

$x \mapsto x^{[p]} : \mathfrak{g} \to \mathfrak{g}$ w. following properties:

i) - defining property: under identification $\mathfrak{g} \xrightarrow{\sim} Vect(G)^G$ ($Vect(G)$ $= \mathcal{D}_G$ in Jay's notation), $x^{[p]} := x^p$ as map $\mathbb{F}[G] \longrightarrow \mathbb{F}[G]$.

ii) - functoriality: if $\Phi : G \to H$ is alg. group homomorphism & $\varphi := d_1\Phi : \mathfrak{g} \to \mathfrak{h}$, then $\varphi(x)^{[p]} = \varphi(x^{[p]})$

Exercise: for $G = GL_n$, have $x^{[p]} = x^p$ as a matrix.

iii) $\Leftarrow$ ii) & Exercise: for $G \subset GL_n$, $x^{[p]} = x^p$ as a matrix.

iv) —. —. —. —. —: $ad(x^{[p]}) = ad(x)^p$

v) easy: $(ax)^{[p]} = a^p x^{[p]}$ $\forall a \in \mathbb{F}$

Fact: in the free algebra $\mathbb{F}\langle x,y\rangle$, the element $(x+y)^p - x^p - y^p$ is a Lie polynomial in x,y. Denote it by $L(x,y)$.

vi) $\Leftarrow$ Fact: $(x+y)^{[p]} = x^{[p]} + y^{[p]} + L(x,y)$.

Definition : A p-Lie algebra over $\mathbb{F}$ is a Lie algebra together w. a p-map $\bullet^{[p]}$ satisfying properties (iv)-(vi)

Example: An associative algebra A together w. $a^{[p]} := a^p$ is a p-Lie algebra.

1) Center & central reductions of $\mathcal{U}(\mathfrak{g})$.

Consider $\iota: \mathfrak{g} \longrightarrow \mathcal{U}$, $\iota(x) = x^p - x^{[p]}$

filtration deg p deg 1

Exercise: Use (iv) & (vi) to show that:

$\iota(x)$ is central

$\iota(x+y) = \iota(x) + \iota(y)$.

$+$ ι is semilinear: $\iota(ax) = a^p \iota(x)$. Assume from now on: $\mathbb{F}$ is perfect. Can twist $\mathbb{F}$-mult'n on $\mathfrak{g}$ by autom $a \mapsto a^{1/p}$ of $\mathbb{F}$, so ι becomes $\mathbb{F}$-linear. Resulting space is denoted by $\mathfrak{g}^{(1)}$ (Frobenius twist).

So have $\mathbb{F}$-linear $\iota: \mathfrak{g}^{(1)} \longrightarrow$ center of $\mathcal{U}$

$$\begin{tikzcd}
\mathfrak{g}^{(1)} \arrow[rr] \arrow[dr] & & \text{center of } \mathcal{U} \\
& S(\mathfrak{g}^{(1)}) \arrow[ur, "\iota"'] &
\end{tikzcd}$$

Exercise (on PBW): ι is injective & makes $\mathcal{U}$ into free $S(\mathfrak{g}^{(1)})$-module w. basis $x_1^{d_1} \dots x_n^{d_n}$ w. $d_i \in \{0, .. p-1\}$ (here $x_1, .. x_n$ is a basis in $\mathfrak{g}$).

Def'n: $\iota(S(\mathfrak{g}^{(1)}))$ is called the p-center.

<u>Restricted</u> universal enveloping:

$$\mathcal{U}^0(\mathfrak{g}) = \mathcal{U}(\mathfrak{g}) \otimes_{S(\mathfrak{g}^{(1)})} \mathbb{F}_0 = \mathcal{U}(\mathfrak{g}) / (x^p - x^{[p]} \mid x \in \mathfrak{g}).$$

basis: $x_1^{d_1} \dots x_n^{d_n}$, $d_i \in \{0, .. p-1\}$. $S(\mathfrak{g}^{(1)})$-module on $\mathbb{F}$ w. $\mathfrak{g}^{(1)*} \curvearrowright$ by 0.

Universal property: If A is assoc. algebra (hence p-Lie algebra), then any p-Lie algebra homom. $\mathfrak{g} \to A$ uniquely factors through <u>assoc. alg.</u> homom'm $\mathcal{U}^0(\mathfrak{g}) \to A$.

Remark*: Full center: $G \curvearrowright \mathcal{U} \rightsquigarrow$ subalgebra $\mathcal{U}^G \subset \mathcal{U}^{\mathfrak{g}}$, which is the center. $\mathcal{U}^G$ is called <u>Harish-Chandra center</u> $\mathcal{U}^G \xrightarrow{\sim} \mathbb{F}[\mathfrak{h}^*]^{(W,\cdot)}$. Under modest restrictions on p & on G have Veldkamp's thm:

$$\text{center of } \mathcal{U} \xleftarrow{\sim} \mathcal{U}^G \otimes_{S(\mathfrak{g}^{(1)})^G} S(\mathfrak{g}^{(1)})$$

2) Distribution algebra.

Motivation for why we care: care about rat'l rep's of G

Have forgetful functor $Rat_{fd}(G) \longrightarrow \mathcal{U}(\mathfrak{g})\text{-mod}_{fd}$

fin. dim rational reps

But over $\mathbb{F}$ (alg. closed char p field) this functor is far from equivalence. It's neither essentially surjective (one can show we land in $\mathcal{U}^0(\mathfrak{g})\text{-mod}_{fd}$) nor full:

e.g.: $G = \mathbb{G}_m$, rep'n $V \simeq \mathbb{F}$, $t.v = t^p v$, the corresp'g $\mathfrak{g}$-module is trivial.

Goal: replace $\mathcal{U}(\mathfrak{g})$ w. a diff't algebra, $Dist(G)$, w. "forgetful" functor $Rat_{fd}(G) \to Dist(G)\text{-mod}_{fd}$ which is "closer" to being an equivalence. In fact, $\mathcal{U}^0(\mathfrak{g}) \hookrightarrow Dist(G)$ & the functor $Rat_{fd}(G) \to Dist(G)\text{-mod}_{fd}$ lifts $Rat_{fd}(G) \to \mathcal{U}^0(\mathfrak{g})\text{-mod}_{fd}$.

2.1) Definition of Dist(G).

Setting: k comm've Noetherian ring, G affine group scheme over k (i.e. $k[G]$ is fin. gen'd comm've Hopf algebra)

$\mathfrak{m} = \ker \varepsilon_G = \{f \in k[G] \mid f(1) = 0\}$

$V \in k\text{-Mod} \rightsquigarrow V^* = \mathrm{Hom}_k(V, k)$

(care about $k = \mathbb{Z}, \mathbb{Q}, \mathbb{F}$).

Assume $k[G]$ is free over k.

$k[G]^*$ is assoc. algebra w.r.t. Δ^*, where $\Delta: k[G] \to k[G] \otimes k[G]$.

Definition: 1) For $n \geq 0$, define $\mathrm{Dist}_{\leq n}(G)$ as $(k[G]/\mathfrak{m}^n)^*$ $\subset k[G]^*$, the modules of distributions of order $\leq n$.

Note $\mathrm{Dist}_{\leq n}(G) \subset \mathrm{Dist}_{\leq n+1}(G)$

2) $\mathrm{Dist}(G) := \bigcup_n \mathrm{Dist}_{\leq n}(G)$.

Claim: $\mathrm{Dist}(G)$ is a Hopf algebra.

Exercise: $\mathrm{Dist}(G) \subset k[G]^*$ is a subalgebra.

Coproduct on $\mathrm{Dist}(G)$: mult'n $\mu: k[G] \otimes k[G] \to k[G] \rightsquigarrow$

$\mu: k[G]/\mathfrak{m}^n \otimes k[G]/\mathfrak{m}^n \longrightarrow k[G]/\mathfrak{m}^n \rightsquigarrow$

$\mu^*: \mathrm{Dist}_{\leq n}(G) \longrightarrow \mathrm{Dist}_{\leq n}(G) \otimes \mathrm{Dist}_{\leq n}(G)$

$\rightsquigarrow$ coproduct $\mathrm{Dist}(G) \longrightarrow \mathrm{Dist}(G) \otimes \mathrm{Dist}(G)$.

Exercise: Define antipode on $\mathrm{Dist}(G)$ and show it's a Hopf algebra

Exercise: (functoriality) $\varphi: G \to H$ alg. gr'p homom'm
$\rightsquigarrow \varphi^*: k[H] \to k[G] \rightsquigarrow \varphi_*: Dist(G) \to Dist(H)$ is a Hopf algebra homom'm.

Exercise: (base change) if k' is k-algebra, then
$Dist(G_{k'}) = k' \otimes_k Dist(G_k)$

Connection between $\mathcal{U}(\mathfrak{g})$ & $Dist(G)$
$\mathcal{U}(\mathfrak{g})$ = left invariant differential operators on G
$\subseteq End_k(k[G])$
Define a map $\mathcal{U}(\mathfrak{g}) \xrightarrow{\eta} k[G]^*$, $a \in \mathcal{U}(\mathfrak{g}) \rightsquigarrow$
$[\eta(a)](f) = (a.f)(1)$, $\operatorname{im} \eta \subset Dist(G)$ & $\eta: \mathcal{U}(\mathfrak{g}) \to Dist(G)$ respects filtrations. Moreover, η is alg. homom'm.

Facts: • if k is char 0 field, then $\eta: \mathcal{U}(\mathfrak{g}) \xrightarrow{\sim} Dist(G)$.
• if k is char p field, then η factors through $\mathcal{U}^0(\mathfrak{g}) \hookrightarrow Dist(G)$

2.2) 1-dimensional examples.
• $G = \mathbb{G}_a$, $k[G] = k[t]$, $\Delta(t) = t \otimes 1 + 1 \otimes t$, $\mathfrak{m} = (t)$
For $r \geq 0 \rightsquigarrow \gamma_r \in k[G]^*$: $\gamma_r(t^n) = \delta_{r,n}$ so $\gamma_r \in Dist_{\leq r}(G)$
So $\gamma_0, \gamma_1, \ldots, \gamma_r, \ldots$ form a basis in $Dist(G)$
$$\gamma_r * \gamma_s(t^n) = \gamma_r \otimes \gamma_s(\Delta(t^n)) = \gamma_r \otimes \gamma_s\left(\sum_{i=0}^{n} \binom{n}{i} t^i \otimes t^{n-i}\right)$$
$$= \begin{cases} \binom{n}{r}, & \text{if } n = r+s \\ 0, & \text{else} \end{cases}$$

so $\gamma_r * \gamma_s = \binom{r+s}{s}\gamma_{r+s}. \Rightarrow \gamma_1^n = n!\gamma_n$

$\mathrm{Dist}(G_{\mathbb{Z}}) = \mathrm{Span}_{\mathbb{Z}}\left(\frac{\gamma_1^i}{i!} \mid i \geq 0\right) \subset \mathrm{Span}_{\mathbb{Q}}(\gamma_1^i) = \mathrm{Dist}(G_{\mathbb{Q}}).$

infinitely generated.

- $G = \mathbb{G}_m$, $k[G] = k[t^{\pm 1}]$, $m = (t-1)$, $\Delta(t) = t \otimes t$

Define $\beta_r \in k[G]^*$ by $\beta_r((t-1)^n) = \delta_{n,r}$

β_i, $i \geq 0$, form (k-basis) in $\mathrm{Dist}(G)$

$\beta_r(t^n) = \binom{n}{r}$

Exercise: $\forall n \Rightarrow n!\beta_n = \beta_1(\beta_1 - 1)\ldots(\beta_1 - (n-1))$ so β_n "=" $\binom{\beta_1}{n}$.

So $\mathrm{Dist}(G_{\mathbb{Z}}) = \mathrm{Span}_{\mathbb{Z}}\left(\binom{\beta_1}{i} \mid i \geq 0\right) \subset \mathbb{Q}[\beta_1] = \mathrm{Dist}(G_{\mathbb{Q}}).$

2.3) Dist(G) for s/simple G.

Assume also G is simply connected, want $\mathrm{Dist}(G_{\mathbb{Z}}) \subset \mathrm{Dist}(G_{\mathbb{Q}}) = \mathcal{U}(\mathfrak{g}_{\mathbb{Q}})$.

Notation: $\Pi \subset \Phi_+$ simple & positive roots

$N^-, T, N \subset G$, max. unipotents & max. torus

$\alpha \in \Phi_+ \rightsquigarrow \mathbb{G}_a^{\pm\alpha} \hookrightarrow N^{\pm}$, $\beta \in \Pi \rightsquigarrow \mathbb{G}_m^{\beta} \hookrightarrow T$

$T = \prod_{\beta \in \Pi} \mathbb{G}_m^{\beta}$ as an alg. group, $N^{\pm} = \prod_{\alpha \in \Phi_+} \mathbb{G}_a^{\pm\alpha}$ as a scheme.

Open Bruhat cell

$$\prod_{\alpha \in \Phi_+} \mathbb{G}_a^{-\alpha} \times \prod_{\beta \in \Pi} \mathbb{G}_m^{\beta} \times \prod_{\alpha \in \Phi_+} \mathbb{G}_a^{\alpha} \xleftarrow{\sim} N^- \times T \times N \subset G \qquad (*)$$

contains 1.

$\mathbb{G}_a^{\pm\alpha} \hookrightarrow G \rightsquigarrow \mathrm{Dist}(\mathbb{G}^{\pm\alpha}_{a,\mathbb{Z}}) \hookrightarrow \mathrm{Dist}(G_{\mathbb{Z}})$

$\gamma_1 \longmapsto e_{\pm\alpha}$

$\mathbb{G}_m^{\beta} \hookrightarrow G \rightsquigarrow \mathrm{Dist}(\mathbb{G}^{\beta}_{m,\mathbb{Z}}) \hookrightarrow \mathrm{Dist}(G_{\mathbb{Z}})$

$\beta_1 \longmapsto \beta^\vee$

(*) $\rightsquigarrow$ tensor product (over $\mathbb{Z}$) decomp'n of $\mathrm{Dist}(G_{\mathbb{Z}}) \rightsquigarrow$

Theorem: $\mathrm{Dist}(G_{\mathbb{Z}}) \subset U(\mathfrak{g}_{\mathbb{Q}})$ has following additive basis:

some order

$$\prod_{\alpha\in\Phi_+} \frac{e_{-\alpha}^{k_\alpha}}{k_\alpha!} \prod_{\beta\in\Pi} \binom{\beta}{m_\beta} \prod_{\alpha\in\Phi_+} \frac{e_\alpha^{n_\alpha}}{n_\alpha!}$$

where $k_\alpha, n_\alpha, m_\beta \in \mathbb{Z}_{\geqslant 0}$

Notation: $e_\alpha^{(n)} = \frac{e_\alpha^n}{n!}$ (divided power)

3) Frobenius.

3.1) Frobenius homomorphism:

$\mathbb{F}$ perfect char p field, A fin. gen'd comm've $\mathbb{F}$-algebra $\rightsquigarrow X = \mathrm{Spec}(A)$

Basic observation: $f \mapsto f^p : A \to A$, ring endomorphism. Can make it $\mathbb{F}$-linear if we twist $\mathbb{F}$-mult'n on source by $a \mapsto a^{1/p}$ ($a \in \mathbb{F}$). Denote resulting algebra by $A^{(1)}$. So $f \mapsto f^p : A^{(1)} \longrightarrow A$ is an $\mathbb{F}$-algebra homomorphism.

$\longleftrightarrow Fr : X \longrightarrow X^{(1)}$ ($Fr^*(f) = f^p$)

Exercise: if A is defined over $\mathbb{F}_p$, then $A^{(1)} \xrightarrow{\sim} A$ isom'c as $\mathbb{F}$-algebras.

Suppose A is Hopf algebra. Then $f \mapsto f^p$ is Hopf algebra homom'm. Let $G = Spec(A)$ - alg'c group. Then

$Fr: G \to G^{(1)}$ is an alg. group homom'm.

Example: $G = GL_n \Rightarrow G^{(1)} = GL_n$; $Fr: GL_n \to GL_n$

$$Fr((a_{ij})) = (a_{ij}^p).$$

3.2) Fr vs distribution algebra.

$$Fr: G \to G^{(1)} \rightsquigarrow Fr_*: Dist(G) \longrightarrow Dist(G^{(1)})$$

Example 1: $G = \mathbb{G}_a (= G^{(1)})$, $Dist(G_{\mathbb{F}}) = Span_{\mathbb{F}}(\gamma_i)$, w. $\gamma_i(t^n) = \delta_{i,n}$.

$[Fr_*(\gamma_i)](t^n) = \gamma_i(Fr^*(t^n)) = \gamma_i(t^{np})$ so

$$Fr_*(\gamma_i) = \begin{cases} \gamma_{i/p}, & \text{if } i \text{ divisible by } p \\ 0, & \text{else} \end{cases}$$

Example 2: $G = \mathbb{G}_m (= G^{(1)})$ $Dist(G_{\mathbb{F}}) = Span_{\mathbb{F}}(\beta_i)$ w.

$\beta_i((t-1)^n) = \delta_{in}$

Then $$Fr_*(\beta_i) = \begin{cases} \beta_{i/p} & \text{if } i \text{ is divisible by } p \\ 0 & \text{else.} \end{cases}$$

Example 3: G is semisimple & simply connected

$$\begin{array}{ccc} \mathbb{G}_a^\alpha & \hookrightarrow & G \\ {\scriptstyle Fr}\downarrow & & \downarrow{\scriptstyle Fr} \\ \mathbb{G}_a^{\alpha(1)} & \hookrightarrow & G^{(1)} \\ \wr\| & & \wr\| \\ \mathbb{G}_a^\alpha & & G \end{array} \quad \rightsquigarrow \quad \begin{array}{ccc} Dist(\mathbb{G}_a^\alpha) & \longrightarrow & Dist(G) \\ \downarrow{\scriptstyle Fr_*} & & \downarrow{\scriptstyle Fr_*} \\ Dist(G_a^{\alpha(1)}) & \longrightarrow & Dist(G^{(1)}) \end{array}$$

So $Fr_*\left(\prod_{\alpha\in\Phi_+} e_{-\alpha}^{(k_\alpha)} \prod_{\beta\in\Pi} \binom{\beta^\vee}{m_\beta} \prod_{\alpha\in\Phi_+} e_\alpha^{(n_\alpha)}\right)$

$$= \begin{cases} \prod e_{-\alpha}^{(k_\alpha/p)} \prod \binom{\beta^\vee}{m_\beta/p} \prod e_\alpha^{(n_\alpha/p)} & \text{if } p \text{ divides } \underline{\text{all}}\ k_\alpha, m_\beta, n_\alpha \\ 0 & \text{else.} \end{cases}$$

9