The Enveloping Algebra

Let $\mathfrak{g} = \mathrm{Lie}(G)$ and let $\mathcal{U}(\mathfrak{g})$ be the universal enveloping algebra. We fix an embedding

$$(*) \qquad \mathfrak{g} \hookrightarrow \mathcal{U}(\mathfrak{g})$$

once and for all.

We're interested in the centre $Z = Z(\mathcal{U}(\mathfrak{g}))$ of the universal enveloping algebra. Let $\mathrm{ad}: \mathcal{U}(\mathfrak{g}) \to GL(\mathcal{U}(\mathfrak{g}))$ be the usual adjoint rep. of $\mathcal{U}(\mathfrak{g})$. Then $\mathfrak{g}$ acts on $\mathcal{U}(\mathfrak{g})$ via this rep and we have

$$Z = \mathcal{U}(\mathfrak{g})^{\mathfrak{g}}.$$

The Harish-Chandra Centre

As for the translations we have a linear action $\rho: G(k) \to GL(k[G])$ given by conjugation. This defines a linear action $\mathrm{Ad}: G(k) \to GL(\mathfrak{g})$, the adjoint representation. Its differential is $\mathrm{ad}: \mathfrak{g} \to GL(\mathfrak{g})$.

By the universal property Ad extends uniquely to a homomorphism

$$\mathrm{Ad}: G(k) \to \mathrm{Aut}_{k\text{-alg}}(\mathcal{U}(\mathfrak{g}))$$

The fixed points $\mathcal{U}(\mathfrak{g})^{G(k)} \subseteq \mathcal{U}(\mathfrak{g})^{\mathfrak{g}}$ give a central subalgebra of the enveloping algebra called the Harish-Chandra centre.

The p-centre

Assume $\mathrm{char}(k) = p > 0$. Recall we have two Lie algebra embeddings

$$\mathcal{U}(\mathfrak{g}) \hookleftarrow \mathfrak{g} \xhookrightarrow{\phi} \mathcal{D}_G$$

Recall that for $X \in \mathfrak{g}$ we have $X^{[p]} \in \mathfrak{g}$ is the unique element satisfying $\phi(X^{[p]}) = \phi(X)^p$. We let X^p be the p^{th} power as an element of $\mathcal{U}(\mathfrak{g})$. In general $X^{[p]} \neq X^p$.

Moreover $X^{[p]} - X^p \in Z(\mathcal{U}(\mathfrak{g}))$ because

$$\mathrm{ad}(X^{[p]} - X^p) = \mathrm{ad}(X)^p - \mathrm{ad}(X)^p = 0$$

We call $Z_p = Z_p(\mathcal{U}(\mathfrak{g})) = \langle X^{[p]} - X^p \mid X \in \mathfrak{g} \rangle$ the *p-centre* of $\mathcal{U}(\mathfrak{g})$.

Veldkamp's Theorem

We now assume $k = \bar{k}$ is a field with $\mathrm{char}(k) = p > 0$. In addition we assume G is connected reductive. Recall that G satisfies the *standard hypotheses* if:

(H1) the derived subgroup $G_{der} \leq G$ is simply connected,
(H2) p is good for G,
(H3) there exists a nondegenerate $G(k)$-invariant bilinear form on $\mathfrak{g}$.

Theorem

If G is con. red. and satisfies the standard hypotheses then the following hold:

(i) The natural product map

$$Z_p \bigotimes_{Z_p^{G(k)}} \mathcal{U}(\mathfrak{g})^{G(k)} \xrightarrow{\sim} Z$$

is an isomorphism.

(ii) Z is a free Z_p-module of rank $p^{\mathrm{rk}(\mathfrak{g})}$, where $\mathrm{rk}(\mathfrak{g})$ is the dimension of a maximal toral subalgebra.

Remark: This is proved in several places. For details see:

- K.A. Brown and I. Gordon, "The ramification of centres: Lie algebras in positive characteristic and quantised enveloping algebras", Math Z. (238), 733–779 (2001)
- R. Tange, "The Zassenhaus Variety of a reductive Lie algebra in positive characteristic", Adv. Math (224), 340–354 (2010).

Also the included references. This result is false when $G = SL_n$ and $p \mid n$. See a paper by A. Braun, J. of Alg. (504), 217–290 (2018).

One can actually give a basis of Z as a Z_p-module. Fix $T \leq G$ a max. torus and let $\mathfrak{t} = \mathrm{Lie}(T)$. It is known that we have an isomorphism

$$\Phi : \mathcal{U}(\mathfrak{g})^{G(k)} \longrightarrow S(\mathfrak{t})^{W}.$$

If $r = \dim(\mathfrak{t})$ then choose $u_1, \dots, u_r$ s.t. $\Phi(u_1), \dots, \Phi(u_r)$ are alg. independent homogeneous generators. Then

$$(u_1^{a_1} \cdots u_r^{a_r} \mid 0 \leq a_i < p)$$

gives a basis of Z as a free Z_p-module.

The p-enveloping algebra

Continue to assume $p > 0$. The p-restricted structure on $\mathfrak{g}$ remembers information about G. For instance as Lie algebras we have $\mathrm{Lie}(\mathbb{G}_a) \cong \mathrm{Lie}(\mathbb{G}_m)$ but these are not isomorphic as p-restricted Lie algebras.

The *p-enveloping algebra* of $\mathfrak{g}$ is defined to be:

$$\mathcal{U}^{[p]}(\mathfrak{g}) = \mathcal{U}(\mathfrak{g}) / Z_p.$$

This is universal with respect to homomorphisms $\mathfrak{g} \to A$ of p-Lie algebras, where A is a k-alg. equipped with its natural p-restricted structure.

The algebra $\mathcal{U}^{[p]}(\mathfrak{g})$ has a k-basis given by 1 and the monomials

$$X_{i_1}^{a_1} \cdots X_{i_r}^{a_r}, \quad \text{with } i_1 < \dots < i_r \text{ and } 0 < a_i < p,$$

where $(X_j)_{j \in J}$ is a totally ordered k-basis of $\mathfrak{g}$.

The Distribution Algebra

The Lie algebra is a first order approximation of G. More generally the distribution algebra takes into account higher order approximations of G. One can consider distributions as a generalisation of derivations to more general differential operators.

For a k-module V let $V^* = \mathrm{Hom}_k(V,k)$ be the dual.

As before $\mathfrak{m} = \ker(\varepsilon_G) = \{f \in k[G] \mid f(1) = 0\}$ is the augmentation ideal. The distributions of order $\leq n$ are

$$\begin{aligned}\mathrm{Dist}_n(G) &= \{\mu : k[G] \to k \mid \mu(\mathfrak{m}^{n+1}) = 0\} \\ &\cong \left(k[G]/\mathfrak{m}^{n+1}\right)^*\end{aligned}$$

We call $\mathrm{Dist}(G) = \bigcup_{n \geq 0} \mathrm{Dist}_n(G)$ the distribution algebra of G.

Exercise

Show that $\mathrm{Dist}(G)$ is a subalgebra of $k[G]^*$ equipped with the product

$$\begin{tikzcd} k[G] \otimes k[G] \arrow[r, "\mu \otimes \nu"] & k \otimes k \arrow[d, "\wr"] \\ k[G] \arrow[u, "\Delta"] \arrow[r, dashed, "\mu\nu"] & k \end{tikzcd}$$

Example

$G = \mathbb{G}_a \rightsquigarrow k[G] = k[T]$

$\rightsquigarrow \mathfrak{m} = \langle T \rangle$

$\rightsquigarrow k[G]/\mathfrak{m}^{n+1} = \bigoplus_{i=0}^{n} kS^i$ with $S = T + \mathfrak{m}^{n+1}$

Let $\gamma_r \in k[T]^*$ be such that $\gamma_r(T^s) = \delta_{rs}$ (the Kronecker delta). Then

$$\mathrm{Dist}(G) = \bigoplus_{r \geq 0} k\gamma_r \quad \text{and} \quad \mathrm{Dist}_n(G) = \bigoplus_{r=0}^{n} k\gamma_r .$$

For the product recall that $\Delta(T) = T \otimes 1 + 1 \otimes T$. So,

$\Delta(T^n) = \sum_{r=0}^{n} \binom{n}{r} T^r \otimes T^{n-r}$. It follows that

$$\gamma_n \gamma_m = \binom{n+m}{n} \gamma_{n+m} \Rightarrow \gamma_1^n = n!\, \gamma_n .$$

Assume $k = \mathbb{Z}$. If K is another ring then $K[G_K] \cong K \otimes_{\mathbb{Z}} k[G]$ and

$$\mathrm{Hom}_K(K[G_K], K) \cong K \otimes_{\mathbb{Z}} \mathrm{Hom}(k[G], k).$$

One similarly checks that $\mathrm{Dist}(G_K) \cong K \otimes_{\mathbb{Z}} \mathrm{Dist}(G)$. Now $\mathrm{Dist}(G_{\mathbb{C}}) \cong \mathbb{C}[\gamma_1]$ is a poly. ring and we can identify $\mathrm{Dist}(G)$ with the lattice

$$\mathrm{Span}_{\mathbb{Z}}\{ \gamma_1^n / n! \mid n \geq 1 \} \subseteq \mathrm{Dist}(G_{\mathbb{C}}).$$

Example

$G = \mathbb{G}_m \rightsquigarrow k[G] = k[T, T^{-1}]$

$\rightsquigarrow \mathfrak{m} = \langle T - 1 \rangle$

$\rightsquigarrow k[G]/\mathfrak{m}^{n+1} = \bigoplus_{i=0}^{n} kS$ with $S = T - 1 + \mathfrak{m}^{n+1}$

There is a unique $\beta_r \in \mathrm{Dist}(G)$ with

$$\beta_r((T-1)^s) = \delta_{rs}$$

Expanding $T^n = ((T-1)+1)^n$ we get $\beta_r(T^n) = \binom{n}{r}$ for all $n \in \mathbb{Z}$ and $r \in \mathbb{N}$.

If $k = \mathbb{C}$ we get

$$\mathrm{Dist}(G) = \bigoplus_{r \geq 0} k\beta_r \quad \text{and} \quad \mathrm{Dist}_n(G) = \bigoplus_{r=0}^{n} k\beta_r .$$

As $\Delta(T) = T \otimes T$ we get that

$$\Delta(T-1) = (T-1) \otimes (T-1) + (T-1) \otimes 1 + 1 \otimes (T-1).$$

From this we can show that

$$\beta_r \beta_s = \sum_{i=0}^{\min\{r,s\}} \frac{(r+s-i)!}{(r-i)!\,(s-i)!\,i!} \beta_{r+s-i} .$$

As a special case $\beta_1\beta_r = (r+1)\beta_{r+1} + r\beta_r$ so $(\beta_1 - r)\beta_r = (r+1)\beta_{r+1}$. By induction

$$r!\,\beta_r = \beta_1(\beta_1-1)\cdots(\beta_1-r+1)$$

so $\beta_r = \binom{\beta_1}{r}$. Thus $\mathrm{Dist}(G) \cong k[\beta_1]$ is again a poly. ring.

Now assume $k=\mathbb{Z}$. For any ring K we have $\mathrm{Dist}(G_K) \cong K \otimes_{\mathbb{Z}} \mathrm{Dist}(G)$ and we can identify $\mathrm{Dist}(G)$ with the lattice

$$\mathrm{Span}_{\mathbb{Z}}\left\{ \binom{\beta_1}{n} \mid n \geq 0 \right\} \subseteq \mathrm{Dist}(G_{\mathbb{C}}).$$

The Reductive Case

Now let G be a split con. red. alg. $\mathbb{Z}$-group scheme. We will assume k is a field (or more generally an integral domain). The base change G_k is con. red.

Let $T \leq G$ be a split max. torus and $\Phi \subset X(T)$ the roots. To each root $\alpha \in \Phi$ we fix a root hom. $x_\alpha : \mathbb{G}_{a,\mathbb{Z}} \to G$. We have:

- $t x_\alpha(c) t^{-1} = x_\alpha(\alpha(t)c)$ for all $\mathbb{Z}$-alg. A, $t \in T(A)$, and $c \in A$,
- x_α is an iso. onto its image $U_\alpha \leq G$, the functor $U_\alpha(A) = x_\alpha(A)$,
- $\mathrm{Lie}(U_\alpha) = \mathrm{Lie}(G)_\alpha$ the root space of the Lie alg.

For $\alpha \in \Phi$ we let

$$X_\alpha = (dx_\alpha)(1) \in \mathrm{Lie}(G)_\alpha.$$

Choose a basis $\varphi_1, \dots, \varphi_r$ of $\check{X}(T)$ and set

$$H_i = (d\varphi_i)(1) \in \mathrm{Lie}(T).$$

Lemma

We have $(H_i, X_\alpha \mid 1 \leq i \leq r \text{ and } \alpha \in \Phi)$ is a basis of $\mathrm{Lie}(G)$.

Remark
We have $\mathrm{Lie}(G_k) \cong k \otimes_{\mathbb{Z}} \mathrm{Lie}(G)$ so their canonical images give a basis of $\mathrm{Lie}(G_k)$. Moreover, let

$$H_\alpha = (d\check{\alpha})(1).$$

Then $H_\alpha = [X_\alpha, X_{-\alpha}]$. If G is adjoint then the elements H_α, X_α form a Chevalley basis of $\mathrm{Lie}(G_{\mathbb{C}})$.

For the distribution algebra we have

$$\mathrm{Dist}(G_k) \cong k \otimes_{\mathbb{Z}} \mathrm{Dist}(G).$$

The discussion of $\mathbb{G}_a$ shows that the divided powers $X_\alpha^{(n)} = X_\alpha^n / n!$ form a basis of

$$\mathrm{Dist}(U_\alpha) \subset \mathrm{Dist}(U_{\alpha,\mathbb{C}}).$$

Similarly we have all

$$\binom{H_1}{m_1} \cdots \binom{H_r}{m_r}$$

form a basis of

$$\mathrm{Dist}(T) \subset \mathrm{Dist}(T_{\mathbb{C}}).$$

We get the following PBW type result for $\mathrm{Dist}(G_k)$.

Proposition
Fix a system of positive roots $\Phi^+ \subset \Phi$. Then all terms

$$\prod_{\alpha \in \Phi^+} X_\alpha^{(n_\alpha)} \prod_{i=1}^{r} \binom{H_i}{m_i} \prod_{\alpha \in \Phi^+} X_{-\alpha}^{(n_{-\alpha})}$$

form a basis of $\mathrm{Dist}(G_k)$.

Remark
If G is semisimple and simply connected then one gets that $\mathrm{Dist}(G)$ is Kostant's $\mathbb{Z}$-form of $\mathcal{U}(\mathrm{Lie}(G_{\mathbb{C}}))$.