

Math564: Representation theory of \mathfrak{sl}_2

Talk 4: Universal enveloping algebra I - the PBW theorem

Mariya Stamatova
University of Zürich

April 6, 2019

Abstract

Today we are going to introduce the notion of the universal enveloping algebra $\mathfrak{U}(\mathfrak{g})$ as well as the PBW theorem, which allows us to construct a basis for $\mathfrak{U}(\mathfrak{g})$.

1 Some preliminaries and notations

Before we start with the construction of the universal enveloping algebra, we need to recall some algebraic structures and set notations that we are going to use throughout the entire talk.

Recall that an associative unital algebra over a field \mathbb{K} is a pair (A, \cdot) , consisting of a vector space A , together with a bilinear multiplication $\cdot : A \times A \rightarrow A$, $a, b \mapsto ab$, which is associative, i.e. for any $a, b, c \in A$ we have $(ab)c = a(bc)$. Unital means that there is an element $1 \in A$, such that $a1 = 1a = a$ for any $a \in A$. An algebra homomorphism is a linear map $\varphi : A \rightarrow B$, $xy \mapsto \varphi(xy) = \varphi(x)\varphi(y)$ for A, B associative algebras and $x, y \in A$.

Each associative algebra (A, \cdot) can be turned into a Lie algebra by replacing the multiplication with the commutator, i.e. for any two elements $a, b \in A$ we have $[a, b] = ab - ba$. We shall denote this Lie algebra as $A^{(-)}$.

Consider the case if V is a vector space, then the space of all endomorphisms of V has the natural structure of an associative unital algebra with multiplication being the composition of linear operators on V . Denote this associative algebra $\mathfrak{L}(V)$ and its underlying Lie algebra as $\mathfrak{L}(V)^{(-)}$.

To define an \mathfrak{sl}_2 -module we need a Lie algebra homomorphism from \mathfrak{sl}_2 to $\mathfrak{L}(V)^{(-)}$, that is a linear map $\varphi : \mathfrak{sl}_2 \rightarrow \mathfrak{L}(V)$, which satisfies:

$$\varphi([x, y]) = [\varphi(x), \varphi(y)] = \varphi(x)\varphi(y) - \varphi(y)\varphi(x) \text{ for all } x, y \in \mathfrak{sl}_2.$$

Using the notation from the first talk, we get $H = \varphi(\mathbf{h})$, $F = \varphi(\mathbf{f})$ and $E = \varphi(\mathbf{e})$.

This is a general construction, i.e. replacing \mathfrak{sl}_2 with any Lie algebra \mathfrak{g} gives the notion of a module over any Lie algebra. The homomorphism φ is usually called a representation of the Lie algebra. As we discussed in the first talk, we use module and representation interchangeably, since they are equivalent definitions.

2 Construction of the universal enveloping algebra

There is an issue with the Lie algebra homomorphism $\varphi : \mathfrak{sl}_2 \rightarrow \mathfrak{L}(V)^{(-)}$, namely in the non-trivial cases the image of φ is not closed with respect to composition but it is closed only with respect to taking the commutator of the linear operators. To fix this problem we have to look for external algebraic objects whose properties are related to \mathfrak{g} (sometimes not obviously). We shall define an associative algebra $\mathfrak{U}(\mathfrak{g})$, called the *universal enveloping algebra of \mathfrak{g}* and show that it has the following properties:

- The Lie algebra \mathfrak{g} is a canonical subalgebra of $\mathfrak{U}(\mathfrak{g})^{(-)}$;
- Any \mathfrak{g} -action on any vector space canonically extends to a $\mathfrak{U}(\mathfrak{g})$ -action on the same vector space;
- The extension and the restriction from $\mathfrak{U}(\mathfrak{g})$ to \mathfrak{g} are mutually inverse isomorphisms between the categories $\mathfrak{g}\text{-mod}$ and $\mathfrak{U}(\mathfrak{g})\text{-mod}$.

The last property is very important, since it says that there is a one-to-one correspondence between \mathfrak{g} -modules and $\mathfrak{U}(\mathfrak{g})$ -modules. Thus, any \mathfrak{g} -module corresponds to a morphism of associative algebras $\psi : \mathfrak{U}(\mathfrak{g}) \rightarrow \mathfrak{L}(V)$ and the image of this morphism is always closed with respect to composition of operators. This implies that one should study the internal structure of $\mathfrak{U}(\mathfrak{g})$. A disadvantage of the universal enveloping algebra is that in any non-trivial case it is infinite-dimensional, while the Lie algebra \mathfrak{g} is finite dimensional.

Definition 2.1. Let $R\langle e, f, h \rangle$ be the free associative algebra with generators e, f and h and quotient it by the ideal I , generated by the relations $ef - fe = h, he - eh = 2e, hf - fh = -2f$. We call the quotient $R\langle e, f, h \rangle/I$ the universal enveloping algebra of a Lie algebra \mathfrak{g} and denote it as $\mathfrak{U}(\mathfrak{g})$.

Remark 2.2. We will identify the elements of $R\langle e, f, h \rangle$ with their images in $\mathfrak{U}(\mathfrak{g})$.

Lemma 2.3. (a) *There is a unique linear map $\epsilon : \mathfrak{g} \rightarrow \mathfrak{U}(\mathfrak{g})$ satisfying:*

$$\epsilon(\mathbf{e}) = e, \quad \epsilon(\mathbf{f}) = f, \quad \epsilon(\mathbf{h}) = h.$$

(b) *The map is a linear homomorphism of Lie algebras $\epsilon : \mathfrak{g} \rightarrow \mathfrak{U}(\mathfrak{g})^{(-)}$.*

Proof. (a) Clear, since generators are mapped to generators.

(b) Follows from the definition of $\mathfrak{U}(\mathfrak{g})$ and ϵ preserving the Lie bracket. \square

Remark 2.4. The map ϵ is called canonical embedding of \mathfrak{g} into $\mathfrak{U}(\mathfrak{g})^{(-)}$. This map is injective, which will be proved later.

The main result of this section is the following universal property of $\mathfrak{U}(\mathfrak{g})$:

Theorem 2.5. *Let A be any associative algebra and $\varphi : \mathfrak{g} \rightarrow A^{(-)}$ be any homomorphism of Lie algebras. There exists a unique homomorphism $\bar{\varphi} : \mathfrak{U}(\mathfrak{g}) \rightarrow A$ of associative algebras, such that the diagram commutes:*

$$\begin{array}{ccc}
\mathfrak{g} & \xrightarrow{\varphi} & A \\
\epsilon \downarrow & \nearrow \exists! \bar{\varphi} & \\
\mathfrak{U}(\mathfrak{g}) & &
\end{array}$$

i.e. we have $\bar{\varphi} \circ \epsilon = \varphi$.

Proof. We need to prove the existence and uniqueness of $\bar{\varphi}$. We shall begin with the existence. Consider the discussed free associative algebra $R\langle e, f, h \rangle$. For any associative algebra A we have the unique homomorphism $\psi : R \rightarrow A$, defined via

$$\psi(e) = \varphi(\mathbf{e}), \quad \psi(f) = \varphi(\mathbf{f}), \quad \psi(h) = \varphi(\mathbf{h}) \quad (2.1)$$

Consider the natural projection $\pi : R \twoheadrightarrow \mathfrak{U}(\mathfrak{g}) \cong R\langle e, f, h \rangle/I$. Let $K = \text{Ker}(\pi)$. Then we have:

$$\begin{aligned}
\psi(e f - f e) &= \psi(e)\psi(f) - \psi(f)\psi(e) \\
&= \varphi(\mathbf{e})\varphi(\mathbf{f}) - \varphi(\mathbf{f})\varphi(\mathbf{e}) \\
&= [\varphi(\mathbf{e}), \varphi(\mathbf{f})] = \varphi([\mathbf{e}, \mathbf{f}]) \\
&= \varphi(\mathbf{h}) = \psi(h).
\end{aligned}$$

This means that $\psi(e f - f e - h) = 0$. Similarly, $\psi(h e - e h - 2e) = 0$ and $\psi(h f - f h + 2f) = 0$. This implies that the image of the kernel $\psi(K)$ is trivial. Therefore, ψ factors through $R\langle e, f, h \rangle/K \cong \mathfrak{U}(\mathfrak{g})$.

Denote by $\bar{\varphi}$ the homomorphism $\bar{\varphi} : \mathfrak{U}(\mathfrak{g}) \rightarrow A$, then the composition $\varphi = \bar{\varphi} \circ \epsilon$ follows.

Now we prove the uniqueness of $\bar{\varphi}$. Since ψ is unique, as we already said, then it implies the uniqueness of φ , since $\varphi = \bar{\varphi} \circ \epsilon$ gives the formulas 2.1. \square

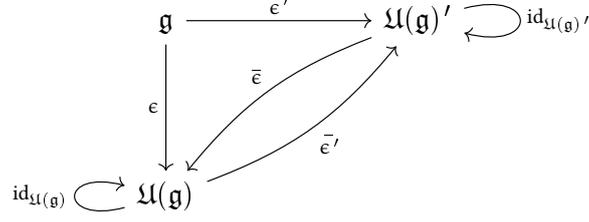
Similarly as for many algebraic objects, the universal enveloping algebra is defined uniquely up to isomorphism.

Proposition 2.6. *Let $\mathfrak{U}(\mathfrak{g})'$ be another associative algebra such that there exists a fixed homomorphism $\epsilon' : \mathfrak{g} \rightarrow (\mathfrak{U}(\mathfrak{g})')^{(-)}$ of Lie algebras having the universal property. Then we have that $\mathfrak{U}(\mathfrak{g})$ is canonically isomorphic to $\mathfrak{U}(\mathfrak{g})'$.*

Proof. Set $A = \mathfrak{U}(\mathfrak{g})$ and $\varphi = \epsilon$. We obtain $\bar{\varphi} = \text{id}_{\mathfrak{U}(\mathfrak{g})}$ and we know that the identity map is unique.

Take $\mathfrak{U}(\mathfrak{g})' = A$ and $\varphi = \epsilon'$. From the universal property in Theorem 2.5 we get a homomorphism $\bar{\epsilon}' : \mathfrak{U}(\mathfrak{g}) \rightarrow \mathfrak{U}(\mathfrak{g})'$. Similarly, the universal property of $\mathfrak{U}(\mathfrak{g})'$ gives another homomorphism $\bar{\epsilon} : \mathfrak{U}(\mathfrak{g})' \rightarrow \mathfrak{U}(\mathfrak{g})$.

As next, consider the compositions $\bar{\epsilon}' \circ \bar{\epsilon} = \text{id}_{\mathfrak{U}(\mathfrak{g})}$, and $\bar{\epsilon} \circ \bar{\epsilon}' = \text{id}_{\mathfrak{U}(\mathfrak{g})}$, which gives the claim.



□

The universal property allows us to find some relations between the \mathfrak{g} -modules and $\mathfrak{U}(\mathfrak{g})$ -modules.

Remark 2.7. If A and B are associative algebras and $\psi : A \rightarrow B$ a homomorphism of algebras, then $\psi : A^{(-)} \rightarrow B^{(-)}$ is a homomorphism of Lie algebras.

Proposition 2.8. (a) Let V be a \mathfrak{g} -module defined via the Lie algebra homomorphism $\varphi : \mathfrak{g} \rightarrow \mathfrak{L}(V)^{(-)}$. Then the homomorphism $\bar{\varphi} : \mathfrak{U}(\mathfrak{g}) \rightarrow \mathfrak{L}(V)$, given by the universal property, endows V with the canonical structure of a $\mathfrak{U}(\mathfrak{g})$ -module.

(b) Let V be a $\mathfrak{U}(\mathfrak{g})$ -module given by $\psi : \mathfrak{U}(\mathfrak{g}) \rightarrow \mathfrak{L}(V)$. Then the composition $\psi \circ \epsilon$ is a Lie algebra homomorphism from \mathfrak{g} to $\mathfrak{L}(V)^{(-)}$, which endows V with the canonical structure of a \mathfrak{g} -module.

(c) Let V and W be two \mathfrak{g} -modules with the induced structures of $\mathfrak{U}(\mathfrak{g})$ -modules, given by (a). Then $\text{Hom}_{\mathfrak{g}}(V, W) = \text{Hom}_{\mathfrak{U}(\mathfrak{g})}(V, W)$.

(d) Let V and W be two $\mathfrak{U}(\mathfrak{g})$ -modules with the induced structures of \mathfrak{g} -modules given by (b). Then we have $\text{Hom}_{\mathfrak{U}(\mathfrak{g})}(V, W) = \text{Hom}_{\mathfrak{g}}(V, W)$.

(e) The operations in (a) and (b) are mutually inverse to each other.

Proof. **(a)** Follows immediately from the universal property.

(b) $\psi \circ \epsilon$ is a Lie algebra homomorphism. This is what Remark 2.7 implies.

(c) and **(d)** hold true, since for any \mathfrak{g} -module and the associated $\mathfrak{U}(\mathfrak{g})$ -module V the image of \mathfrak{g} in $\mathfrak{L}(V)^{(-)}$ is generated by the same elements as the image of $\mathfrak{U}(\mathfrak{g})$ in $\mathfrak{L}(V)$.

(e) Follows from the definition of ϵ and its uniqueness. □

Let $\mathfrak{g}\text{-mod}$ be the category of all left \mathfrak{g} -modules and $\mathfrak{U}(\mathfrak{g})\text{-mod}$ be the category of all left $\mathfrak{U}(\mathfrak{g})$ -modules. The next corollary defines this very important relation.

Corollary 2.9. The operations defined in Proposition 2.8 **(a)** and **(b)** are mutually inverse isomorphisms between the categories $\mathfrak{g}\text{-mod}$ and $\mathfrak{U}(\mathfrak{g})\text{-mod}$, i.e. there is a functor $F : \mathfrak{g}\text{-mod} \rightarrow \mathfrak{U}(\mathfrak{g})\text{-mod}$, another functor $G : \mathfrak{U}(\mathfrak{g})\text{-mod} \rightarrow \mathfrak{g}\text{-mod}$ and two natural isomorphisms $\delta : F \circ G \Rightarrow \text{Id}_{\mathfrak{U}(\mathfrak{g})\text{-mod}}$ and $\eta : G \circ F \Rightarrow \text{Id}_{\mathfrak{g}\text{-mod}}$.

Remark 2.10. The equivalence of the categories defined above allows us to use the notions of a \mathfrak{g} -module and $\mathfrak{U}(\mathfrak{g})$ -module interchangeably.

If V is a \mathfrak{g} -module with $v \in V$ and $u \in \mathfrak{U}(\mathfrak{g})$, then we denote the action of u on v by $u(v)$. In particular, $e(v) = E(v)$, $f(v) = F(v)$, $h(v) = H(v)$.

Remark 2.11. There is another way to construct $\mathfrak{U}(\mathfrak{g})$.

First, define the tensor algebra $T(\mathfrak{g})$ of a Lie algebra \mathfrak{g} as follows:

$$T^0 := \mathbb{C}, T^1 := \mathfrak{g}, T^2 := \mathfrak{g} \otimes \mathfrak{g}, \text{ more generally } T^n := \underbrace{\mathfrak{g} \otimes \mathfrak{g} \otimes \cdots \otimes \mathfrak{g}}_{n \text{ times}}.$$

Then, the tensor algebra is the associative unital algebra $T(\mathfrak{g}) := T^0 \oplus T^1 \oplus T^2 \oplus \dots$ with multiplication given by concatenation of tensor words and the empty word for a unit element. Let J denote the two-sided ideal of $T(\mathfrak{g})$, generated by all elements of the form $x \otimes y - y \otimes x - [x, y]$, where $x, y \in \mathfrak{g}$. Then the universal algebra $\mathfrak{U}(\mathfrak{g})$ is constructed by taking the quotient of the tensor algebra by the ideal J , namely $T(\mathfrak{g})/J$.

3 The PBW theorem

The definition of $\mathfrak{U}(\mathfrak{g})$ doesn't give us enough information about this algebra, for instance we don't know if it is finite-dimensional or infinite-dimensional. It is not even clear yet that e is injective.

This part of the talk will be focussed on the construction of an explicit basis of $\mathfrak{U}(\mathfrak{g})$.

Theorem 3.1 (Poincaré-Birkhoff-Witt). *The set $\{f^i h^j e^k : i, j, k \in \mathbb{N}_0\}$ is a basis of $\mathfrak{U}(\mathfrak{g})$.*

Remark 3.2. The theorem is usually called the PBW theorem. The monomials $f^i h^j e^k$ are called standard monomials. They form a basis of the polynomial algebra $\mathbb{C}[f, h, e]$, which is commutative, unlike $\mathfrak{U}(\mathfrak{g})$.

Before we prove Theorem 3.1 we need two intermediate results.

Lemma 3.3. *The standard monomials generate $\mathfrak{U}(\mathfrak{g})$.*

Proof. Recall the free algebra $R\langle e, f, h \rangle$. Its basis is given by arbitrary monomials $x_1 x_2 \dots x_k$ where $k \in \mathbb{N}_0$ and $x_i \in \{e, f, h\}$ for all $i = 1, \dots, k$.

We need to prove that each such monomial can be written as a linear combination of standard monomials.

We shall use induction on k :

- $k = 1$: nothing to prove;
- For $k > 1$ consider some monomial $x_1 x_2 \dots x_k$ as above.
We call a pair of indices (i, j) , $1 \leq i < j \leq k$ an *inversion*, of one of the following situations holds true:

$$\begin{cases} x_i = h \\ x_j = f, \end{cases} \quad \begin{cases} x_i = e \\ x_j = f, \end{cases} \quad \begin{cases} x_i = e \\ x_j = h. \end{cases}$$

Proceed by induction on the number of inversions in $x_1 x_2 \dots x_k$. If the monomials are already ordered, i.e. there are no inversions, we get $x_1 x_2 \dots x_k$, which is standard.

Otherwise, fix an inversion $(i, i + 1)$:

$$x_1 \dots x_{i-1} \boxed{x_i x_{i+1}} x_{i+2} \dots x_k = x_1 \dots x_{i-1} \boxed{x_{i+1} x_i} \dots x_k + x_1 \dots x_{i-1} [x_i, x_{i+1}] x_{i+2} \dots x_k.$$

We notice that the bracket $[x_i, x_{i+1}]$ can take values in the set $\{\pm h, \pm 2e, \pm 2f\}$, the second summand is of degree $k - 1$. The first summand has one inversion less than $x_1 x_2 \dots x_k$, hence the claim holds true for any k .

□

Remark 3.4. Consider the vector space $\mathbb{C}[a, b, c]$. By using the induction on the degree of a monomial, we can describe the actions of E, F and H on V :

$$F(a^i b^j c^k) = a^{i+1} b^j c^k, \quad (3.1)$$

$$H(a^i b^j c^k) = \begin{cases} b^{j+1} c^k, & \text{if } i = 0 \\ F(H(a^{i-1} b^j c^k)) - 2a^i b^j c^k, & \text{otherwise} \end{cases} \quad (3.2)$$

$$E(a^i b^j c^k) = \begin{cases} c^{k+1}, & \text{if } i, j = 0 \\ H(E(b^{j-1} c^k)) - 2E(b^{j-1} c^k), & \text{otherwise} \\ F(E(a^{i-1} b^j c^k)) + H(a^{i-1} b^j c^k) & \text{if } i \neq 0, \end{cases} \quad (3.3)$$

where $i, j, k \in \mathbb{N}_0$.

We can modify a little the last two equations above to get:

$$H(a^i b^j c^k) = \begin{cases} b^{j+1} c^k, & \text{if } i = 0 \\ F(H(a^{i-1} b^j c^k)) + [H, F] a^{i-1} b^j c^k, & \text{otherwise;} \end{cases} \quad (3.2^*)$$

$$E(a^i b^j c^k) = \begin{cases} c^{k+1}, & \text{if } i, j = 0 \\ H(E(b^{j-1} c^k)) + [E, H](b^{j-1} c^k), & \text{if } i = 0, j \neq 0, \\ F(E(a^{i-1} b^j c^k)) + [E, F](a^{i-1} b^j c^k) & \text{if } i \neq 0, \end{cases} \quad (3.3^*)$$

where $i, j, k \in \mathbb{N}_0$.

Lemma 3.5. *The equations (3.1)-(3.3) from the remark above define on V the structure of a \mathfrak{g} -module.*

Proof. We have to check the three relations for the \mathfrak{g} -structure.

- We begin with the relation $[H, F] = -2F$.

For $i, j, k \in \mathbb{N}_0$ we have:

$$\begin{aligned} H(F(a^i b^j c^k)) &\stackrel{(3.1)}{=} H(a^{i+1} b^j c^k) \stackrel{(3.2)}{=} \\ &= F(H(a^i b^j c^k)) - 2a^{i+1} b^j c^k \stackrel{(3.1)}{=} F(H(a^i b^j c^k)) - 2F(a^i b^j c^k), \end{aligned}$$

which implies that $[H, F] = -2F$.

- Now we have to prove the relation $[E, F] = -2F$. For $i, j, k \in \mathbb{N}_0$ we have:

$$E(F(a^i b^j c^k)) \stackrel{(3.1)}{=} E(a^{i+1} b^j c^k) \stackrel{(3.3)}{=} F(E(a^i b^j c^k)) - H(a^i b^j c^k),$$

and the relation is proved.

- As next, we prove the relation $[H, E] = 2E$, which we rewrite as $EH - HE = -2E$. For any $j, k \in \mathbb{N}_0$ and $i = 0$ we have:

$$E(H(b^j c^k)) = E(b^{j+1} c^k) \stackrel{(3.3)}{=} H(E(b^j c^k)) - 2E(b^j c^k)$$

and the relation $[H, E] = 2E$ is proved on monomials of the form $b^j c^k$.

The part with the proof of this relation for monomials $a^i b^j c^k$, where $i \in \mathbb{N}$ and $j, k \in \mathbb{N}_0$ is more complicated.

For this we use induction on i :

1. The case $i = 0$ is done.
2. For the case $i \geq 1$, write the relation $[H, E] = 2E$ as $HE - EH - 2E = 0$. Apply $HE - EH - 2E$ to the monomial $a^i b^j c^k$, use the equations (3.1)-(3.3), together with the modified equations (3.2*) and (3.3*) to obtain:

$$\begin{aligned} (HE - EH - 2E)(a^i b^j c^k) &= \\ &= (HFE + H[E, F] - EFH - E[H, F] - 2FE - 2[E, F])(a^{i-1} b^j c^k). \end{aligned} \quad (3.4)$$

By induction we have $-2FE = F[E, H]$, using $[H, F] = -2F$, we have:

$$\begin{aligned} H[E, F] &= HEF - HFE, \\ E[H, F] &= EHF - EFH, \\ -2[E, F] &= [E, [H, F]]. \end{aligned}$$

Applying these relations to (3.4) gives us:

$$(HE - EH - 2E)(a^i b^j c^k) = ([F, [E, H]] + [E, [H, F]])(a^{i-1} b^j c^k). \quad (3.5)$$

We know that $[E, F] = H$, so we can add the zero term $0 = [H, H] = -[H, H] = -[H, [E, F]] = [H, [F, E]]$ to the equation (3.5) and get:

$$\begin{aligned} (HE - EH - 2E)(a^i b^j c^k) &= \\ &= \underbrace{([F, [E, H]] + [E, [H, F]] + [H, [F, E]])}_{\text{Jacobi identity for } \mathfrak{L}(V)^{(-)}}(a^{i-1} b^j c^k). \end{aligned}$$

Hence, the last relation is satisfied.

□

Now we are ready to prove the PBW theorem.

Proof. To prove that the standard monomials form a basis in $\mathfrak{U}(\mathfrak{g})$ we need to show:

- They generate $\mathfrak{U}(\mathfrak{g})$;
- They are linearly independent.

The first part was proved in Lemma 3.3.

What is left to prove is the linear independency.

Consider now the $\mathfrak{U}(\mathfrak{g})$ -module V from Lemma 3.5.

Then for all $i, j, k \in \mathbb{N}_0$ for the constant polynomial $1 \in V$ we have:

$$F^i H^j K^k(1) = a^i b^j c^k.$$

The elements $a^i b^j c^k \in V$ are linearly independent.

Hence, the linear operators $F^i H^j E^k$ are linearly independent as well.

These linear operators are exactly the images of the standard monomials under the homomorphism, defining the $\mathfrak{U}(\mathfrak{g})$ -structure on V , it follows that the standard monomials are linearly independent and this proves the statement of the theorem. □

Corollary 3.6. *The canonical embedding $\epsilon : \mathfrak{g} \hookrightarrow \mathfrak{U}(\mathfrak{g})^{(-)}$ is injective.*

Proof. We know that the elements \mathbf{e} , \mathbf{f} and \mathbf{h} form a basis of \mathfrak{g} and that the elements $\epsilon(\mathbf{e}) = \mathbf{e}$, $\epsilon(\mathbf{f}) = \mathbf{f}$ and $\epsilon(\mathbf{h}) = \mathbf{h}$ are linearly independent in $\mathfrak{U}(\mathfrak{g})$ by PBW. □

This means we can identify \mathfrak{g} with $\epsilon(\mathfrak{g})$.