13. **The Poincaré-Birkhoff-Witt theorem**

13.1. **The statement of the Poincaré-Birkhoff-Witt theorem.** Let $\mathfrak{g}$ be a Lie algebra over a field $\mathbf{k}$. Recall from Example 12.8 that we have a surjective algebra homomorphism

$$\phi : S\mathfrak{g} \to \mathrm{gr}U(\mathfrak{g}).$$

Theorem 13.1. *(Poincaré-Birkhoff-Witt theorem) The homomorphism ϕ is an isomorphism.*

We will prove Theorem 13.1 in Subsection 13.2. Now let us discuss its reformulation in terms of a basis and corollaries.

Given a basis $\{x_i\}$ of $\mathfrak{g}$, fix an ordering on this basis and consider ordered monomials $\prod_i x_i^{n_i}$, where the product is ordered according to the ordering of the basis. The statement that ϕ is surjective is equivalent to saying that ordered monomials span $U(\mathfrak{g})$. This is also easy to see directly: any monomial can be ordered using the commutation relations at the cost of an error of lower degree, so proceeding recursively, we can write any monomial as a linear combination of ordered ones. Thus the PBW theorem can be formulated as follows:

Theorem 13.2. *The ordered monomials are linearly independent, hence form a basis of $U(\mathfrak{g})$.*

For instance, if $\mathbf{k} = \mathbb{R}$ or $\mathbb{C}$ and $\mathfrak{g} = \mathrm{Lie}(G)$ where G is a Lie group, this theorem is easy to deduce from Exercise 12.12 (do this!).

Corollary 13.3. *The map $\rho : \mathfrak{g} \to U(\mathfrak{g})$ is injective. Thus $\mathfrak{g} \subset U(\mathfrak{g})$.*

Remark 13.4. Let $\mathfrak{g}$ be a vector space equipped with a bilinear map $[,] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$. Then one can define the algebra $U(\mathfrak{g})$ as above. However, if the map $\rho : \mathfrak{g} \to U(\mathfrak{g})$ is injective then we clearly must have $[x, x] = 0$ for $x \in \mathfrak{g}$ and the Jacobi identity, i.e., $\mathfrak{g}$ has to be a Lie algebra. Thus the PBW theorem and even Corollary 13.3 fail without the axioms of a Lie algebra.

Corollary 13.5. *Let $\mathfrak{g}_i$, $1 \le i \le n$, be Lie subalgebras of $\mathfrak{g}$ such that $\mathfrak{g} = \oplus_i \mathfrak{g}_i$ as a vector space (but $[\mathfrak{g}_i, \mathfrak{g}_j]$ need not be zero). Then the multiplication map $\otimes_i U(\mathfrak{g}_i) \to U(\mathfrak{g})$ in any order is a linear isomorphism.*

Proof. The corollary follows immediately from the PBW theorem by choosing a basis of each $\mathfrak{g}_i$. □

Remark 13.6. 1. Corollary 13.5 applies to the case of infinitely many $\mathfrak{g}_i$ if we understand the tensor product accordingly: the span of tensor products of elements of $U(\mathfrak{g}_i)$ where almost all of these elements are equal to 1.

2. Note that if $\dim \mathfrak{g}_i = 1$, this recovers the PBW theorem itself, so Corollary 13.5 is in fact a generalization of the PBW theorem.

Let $\mathrm{char}(\mathbf{k}) = 0$. Define the **symmetrization map** $\sigma : S\mathfrak{g} \to U(\mathfrak{g})$ given by

$$\sigma(y_1 \otimes ... \otimes y_n) = \frac{1}{n!} \sum_{s \in S_n} y_{s(1)} ... y_{s(n)}.$$

It is easy to see that this map commutes with the adjoint action of $\mathfrak{g}$.

Corollary 13.7. *σ is an isomorphism.*

Proof. It is easy to see that $\mathrm{gr}\sigma$ (the induced map on the associated graded algebra) coincides with ϕ, so the result follows from the PBW theorem. ☐

Let $Z(U(\mathfrak{g}))$ denote the center of $U(\mathfrak{g})$.

Corollary 13.8. *The map σ defines a filtered vector space isomorphism $\sigma_0 : (S\mathfrak{g})^{\mathrm{ad}\mathfrak{g}} \to Z(U(\mathfrak{g}))$ whose associated graded is the algebra isomorphism $\phi|_{(S\mathfrak{g})^{\mathrm{ad}\mathfrak{g}}} : (S\mathfrak{g})^{\mathrm{ad}\mathfrak{g}} \to \mathrm{gr}Z(U(\mathfrak{g}))$.*

In the case when $\mathfrak{g} = \mathrm{Lie}G$ for a connected Lie group G, we thus obtain a filtered vector space isomorphism of the center of $U(\mathfrak{g})$ with $(S\mathfrak{g})^{\mathrm{Ad}G}$.

Remark 13.9. The map σ_0 is not, in general, an algebra homomorphism; however, a nontrivial theorem of M. Duflo says that if $\mathfrak{g}$ is finite dimensional then there exists a canonical filtered *algebra isomorphism* $\eta : Z(U(\mathfrak{g})) \to (S\mathfrak{g})^{\mathrm{ad}\mathfrak{g}}$ (a certain twisted version of σ_0) whose associated graded is $\phi|_{Z(U(\mathfrak{g}))}$. A construction of the Duflo isomorphism can be found in [CR].

Example 13.10. Let $\mathfrak{g} = \mathfrak{sl}_2 = \mathfrak{so}_3$. Then $\mathfrak{g}$ has a basis x, y, z with $[x, y] = z$, $[y, z] = x$, $[z, x] = y$, and $G = SO(3)$ acts on these elements by ordinary rotations of the 3-dimensional space. So the only G-invariant polynomials of x, y, z are polynomials of $r^2 = x^2 + y^2 + z^2$. Thus we get that $Z(U(\mathfrak{g})) = \mathbb{C}[x^2 + y^2 + z^2]$. In terms of e, f, h, we have

$$x^2 + y^2 + z^2 = -fe - \frac{h^2 + 2h}{4} = -\frac{C}{2},$$

where C is the Casimir element.

13.2. **Proof of the PBW theorem.** The proof of Theorem 13.1 is based on the following key lemma.

Lemma 13.11. *There exists a unique linear map $\varphi : T\mathfrak{g} \to S\mathfrak{g}$ such that*

(i) for an **ordered** *monomial $X := x_{i_1}...x_{i_m} \in \mathfrak{g}^{\otimes m}$ one has $\varphi(X) = X$;*

(ii) one has $\varphi(I) = 0$; in other words, φ descends to a linear map $\overline{\varphi} : U(\mathfrak{g}) \to S\mathfrak{g}$.

Remark 13.12. The map φ is not canonical and depends on the choice of the ordered basis x_i of $\mathfrak{g}$.

Note that Lemma 13.11 immediately implies the PBW theorem, since by this lemma the images of ordered monomials under φ are linearly independent in $S\mathfrak{g}$, implying that these monomials themselves are linearly independent in $U(\mathfrak{g})$.

Proof. It is clear that φ is unique if exists since ordered monomials span $U(\mathfrak{g})$. We will construct φ by defining it inductively on $F_nT\mathfrak{g}$ for $n \geq 0$.

Suppose φ is already defined on $F_{n-1}T\mathfrak{g}$ and let us extend it to $F_nT\mathfrak{g} = F_{n-1}T\mathfrak{g} \oplus \mathfrak{g}^{\otimes n}$. So we should define φ on $\mathfrak{g}^{\otimes n}$. Since φ is already defined on ordered monomials X (by $\varphi(X) = X$), we need to extend this definition to all monomials.

Namely, let X be an ordered monomial of degree n, and let us define φ on monomials of the form $s(X)$ for $s \in S_n$, where

$$s(y_1...y_n) := y_{s(1)}...y_{s(n)}.$$

To this end, fix a decomposition D of s into a product of transpositions of neighbors:

$$s = s_{j_r}...s_{j_1},$$

and define $\varphi(s(X))$ by the formula

$$\varphi(s(X)) := X + \Phi_D(s, X),$$

where

$$\Phi_D(s, X) := \sum_{m=0}^{r-1} \varphi([,]_{j_{m+1}}(s_{j_m}...s_{j_1}(X))),$$

and

$$[,]_j(y_1...y_jy_{j+1}...y_n) := y_1...[y_j, y_{j+1}]...y_n.$$

We need to show that $\varphi(s(X))$ is well defined, i.e., $\Phi_D(s, X)$ does not really depend on the choice of D and s but only on $s(X)$. We first show that $\Phi_D(s, X)$ is independent on D.

To this end, recall that the symmetric group S_n is generated by $s_j, 1 \leq j \leq n-1$ with defining relations

$$s_j^2 = 1;\ s_js_k = s_ks_j, |j-k| \geq 2;\ s_js_{j+1}s_j = s_{j+1}s_js_{j+1}.$$

Thus any two decompositions of s into a product of transpositions of neighbors can be related by a sequence of applications of these relations somewhere inside the decomposition.

Now, the first relation does not change the outcome by the identity $[x, y] = -[y, x]$.

For the second relation, suppose that $j < k$ and we have two decompositions D_1, D_2 of s given by $s = ps_js_kq$ and $s = ps_ks_jq$, where q is a product of m transpositions of neighbors. Let $q(X) = YabZcdT$ where $a, b, c, d \in \mathfrak{g}$ stand in positions $j, j+1, k, k+1$. Let $\Phi_1 := \Phi_{D_1}(s, X)$, $\Phi_2 := \Phi_{D_2}(s, X)$. Then the sums defining Φ_1 and Φ_2 differ only in the m-th and $m+1$-th term, so we get

$$\Phi_1 - \Phi_2 =$$

$$\varphi(YabZ[c, d]T) + \varphi(Y[a, b]ZdcT) - \varphi(Y[a, b]ZcdT) - \varphi(YbaZ[c, d]T),$$

which equals zero by the induction assumption.

For the third relation, suppose that we have two decompositions D_1, D_2 of s given by $s = ps_js_{j+1}s_jq$ and $s = ps_{j+1}s_js_{j+1}q$, where q is a product of k transpositions of neighbors. Let $q(X) = YabcZ$ where $a, b, c \in \mathfrak{g}$ stand in positions $j, j+1, j+2$. Let $\Phi_1 := \Phi_{D_1}(s, X)$, $\Phi_2 := \Phi_{D_2}(s, X)$. Then the sums defining Φ_1 and Φ_2 differ only in the k-th, $k+1$-th, and $k+2$-th terms, so we get

$$\Phi_1 - \Phi_2 =$$

$$(\varphi(Y[a, b]cZ) + \varphi(Yb[a, c]Z) + \varphi(Y[b, c]aZ)) -$$
$$(\varphi(Ya[b, c]Z) + \varphi(Y[a, c]bZ) + \varphi(Yc[a, b]Z)).$$

So the Jacobi identity

$$[[b, c], a] + [b, [a, c]] + [[a, b], c] = 0$$

combined with property (ii) in degree $n-1$ implies that $\Phi_1 - \Phi_2 = 0$, i.e., $\Phi_1 = \Phi_2$, as claimed. Thus we will denote $\Phi_D(s, X)$ just by $\Phi(s, X)$.

It remains to show that $\Phi(s, X)$ does not depend on the choice of s and only depends on $s(X)$. Let $X = x_{i_1}...x_{i_n}$; then $s(X) = s'(X)$ if and only if $s = s't$, where t is the product of transpositions s_k for which $i_k = i_{k+1}$. Thus, it suffices to show that $\Phi(s, X) = \Phi(ss_k, X)$ for such k. But this follows from the the fact that $[x, x] = 0$.

Now, it follows from the construction of φ that for any monomial X of degree n (not necessarily ordered), $\varphi(s_j(X)) = \varphi(X) + \varphi([,]_j(X))$. Thus φ satisfies property (ii) in degree n. This concludes the proof of Lemma 13.11 and hence Theorem 13.1. □

18.745 Lie Groups and Lie Algebras I
Fall 2020