Several proofs of PBW theorem

0. Notation

Also true for inf. dim.

$\mathfrak{g}$ (fin dim) Lie alg $/\mathbb{K}$. char $\mathbb{K} \neq 2,3$.

- T Tensor algebra of $\mathfrak{g}$, $\quad T^m = \{x_1\otimes\cdots\otimes x_m : x_i \in \mathfrak{g}\}$, $T_m = \bigoplus_{i=0}^m T^i$
- I ideal of T gen by $x\otimes y - y\otimes x$ $\quad \sigma : T \to T/I$
- J ideal of T gen by $x\otimes y - y \otimes x - [x,y]$ $\quad \pi : T \to T/J$
- S Symmetric algebra of $\mathfrak{g}$ $\quad S^m = \sigma(T^m)$, $S = \bigoplus_{m\in\mathbb{N}} S^m$, $S_m = \bigoplus_{i=0}^m S^i$
- $\mathcal{U}$ universal enveloping alg of $\mathfrak{g}$, $\quad \mathcal{U}_m = \pi(T_m)$

$$\mu_m : \mathcal{U}_m \to \mathcal{U}_m/\mathcal{U}_{m-1} =: G^m, \quad G = \bigoplus_{m\in\mathbb{N}} G^m$$

I. The universal enveloping algebra

Def. The universal enveloping algebra of $\mathfrak{g}$ is a pair $(\mathcal{U}, i)$, where $\mathcal{U}$ is an ass alg with 1, $i : \mathfrak{g} \to \mathcal{U}$ is a Lie alg homom (ass alg induces a Lie alg structure) and the following holds:

For any ass alg A with 1 and Lie alg homom $j : \mathfrak{g} \to A$, there exists a unique alg homom $\phi : \mathcal{U} \to A$ s.t.
$$\begin{tikzcd} \mathfrak{g} \arrow[r, "j"] \arrow[dr, "i"'] & A \\ & \mathcal{U} \arrow[u, dashed, "\phi"'] \end{tikzcd}$$
commutes.

Existence of $\mathcal{U}(\mathfrak{g})$: Consider the two-sided ideal $J \subseteq T(\mathfrak{g})$ generated by $x\otimes y - y \otimes x - [x,y]$

Define $\mathcal{U} = T(\mathfrak{g})/J$, then it is plain to show that $\mathcal{U}$ satisfies the universal property.

Uniqueness of $\mathcal{U}(\mathfrak{g})$: If $(\mathcal{U}, i)$, $(\mathcal{U}', i')$ are two universal enveloping alg of $\mathfrak{g}$, then

$\exists!\, \phi, \phi'$ s.t.
$$\begin{tikzcd} & \mathcal{U} \arrow[d, dashed, shift left, "\phi"] \\ \mathfrak{g} \arrow[ur, "i"] \arrow[dr, "i'"'] & \mathcal{U}' \arrow[u, dashed, shift left, "\phi'"] \end{tikzcd}$$
commutes. By uniqueness of ϕ & ϕ', $\begin{cases} \phi\circ\phi' = id_{\mathcal{U}'} \\ \phi'\circ\phi = id_{\mathcal{U}} \end{cases}$

Thus $\mathcal{U}(\mathfrak{g})$ unique up to isom.

II. PBW Theorem

Define $\phi_m : T^m \xrightarrow{\pi} \mathcal{U}_m \xrightarrow{\mu_m} G^m = \mathcal{U}_m/\mathcal{U}_{m-1}$, then $\phi = \bigoplus_{m\in\mathbb{N}} \phi_m : T = \bigoplus_{m\in\mathbb{N}} T^m \to \bigoplus_{m\in\mathbb{N}} G^m = G$

- ϕ is a surjective alg homo

product in G is induced by product in T.

pf. $\forall x \in T^p$, $y \in T^q$, $\phi(x)\phi(y) = \phi_p(x)\,\phi_q(y) = \phi_{p+q}(xy) = \phi(xy)$

$\forall s \in \mathcal{U}_m \setminus \mathcal{U}_{m-1}$, there exists $t \in T^m \setminus T^{m-1}$ s.t. $\pi(t) = s$. (Otherwise $s \in \mathcal{U}_{m-1}$).

Then $\forall\, s+\mathcal{U}_{m-1} \in G^m \setminus \{0\}$, $\phi(t) = s+\mathcal{U}_{m-1}$. Thus surjective.

- $\phi(I) = 0$ $\quad (I = \langle x\otimes y - y\otimes x\rangle \subseteq T)$

pf. $\forall x,y \in \mathfrak{g}$, $\phi(x\otimes y - y\otimes x) = \phi_2(x\otimes y - y\otimes x) = \mu_2\circ\pi(x\otimes y - y\otimes x) = \mu_2([y,x]+J) = 0$. $\quad \mathcal{U}_1$

- By universal property of quotient: ϕ induces an surj alg homom $\omega: S \twoheadrightarrow G$

$$\begin{tikzcd} S \arrow[r, two heads, "\omega"] \arrow[d, equal] & G \\ T/I & T \arrow[l] \arrow[u, "\phi"'] \end{tikzcd}$$

pf. Follows from the surjectivity of ϕ.

only a linear map!

- $\omega|_{S^m}: S^m \to G^m$ is surjective and makes

$$\begin{tikzcd} S^m \arrow[rr, "\omega|_{S^m}"] & & G^m \\ & T^m \arrow[ul, "\sigma|_{S^m}"] \arrow[ur, "\phi_m"'] & \end{tikzcd}$$

commute

pf. By definition, the diagram commutes.

Since $\sigma|_{S^m}$ and ϕ_m are both surjective, $\omega|_{S^m}$ is surjective.

Explicitly:

$$\begin{tikzcd} & S^m \arrow[dr] & \\ T^m \arrow[ur] \arrow[dr] & G & G^m \\ & \mathcal{U}_m \arrow[ur] & \end{tikzcd}$$

Theorem [Poincáre–Birkhoff–Witt] $\omega: S \to G$ is an isomorphism of algebras.

Another version: Let $(x_1, \cdots, x_n)$ be an ordered basis of $\mathfrak{g}$, then the elements $x_{i_1}\cdot x_{i_2}\cdots x_{i_m}$, $m\in\mathbb{N}_{>0}$, $i_1 \le i_2 \le \cdots \le i_m$, along with 1, form a basis of $\mathcal{U}(\mathfrak{g})$.

For simplicity, for each sequence $\Sigma = (i_1, \cdots, i_m)$, $i_j \in [\![1,n]\!]$,

- Denote $x_{i_1}\otimes\cdots\otimes x_{i_m} \in T$ by t_Σ
- Denote $x_{i_1}\otimes\cdots\otimes x_{i_m} + I \in S$ by $z_{i_1}\cdots z_{i_m}$ or z_Σ and $1+I \in S^0$ by z_ϕ.
- Denote $x_{i_1}\cdots x_{i_m} \in \mathcal{U}$ by x_Σ. and $\overline{x_\Sigma} := x_{i_1}\cdots x_{i_m} + \mathcal{U}_{m-1} \in G$
- Say Σ increasing if $i_1 \le \cdots \le i_m$. Technically, say ϕ increasing.
- $l(\Sigma) = m$ the length of Σ

pf. "$\Rightarrow$" Let $W = \operatorname{span}\{t_\Sigma : \Sigma \nearrow\} \subset T$. Note that $\{z_\Sigma = \sigma(t_\Sigma) : \Sigma\nearrow\}$ is a basis of S.

Thus, $\{\phi_m(t_\Sigma) : \Sigma\nearrow, l(\Sigma) = m\} = \{\omega|_{S^m}(z_\Sigma) : \Sigma\nearrow, l(\Sigma) = m\}$ is a basis of G^m, which follows from the bijectivity of $\omega|_{S^m}$.

Hence $\{x_\Sigma = \pi(t_\Sigma) : \Sigma\nearrow, l(\Sigma) = m\} \subseteq \mathcal{U}_m \setminus \mathcal{U}_{m-1}$. Then it can be proved by induction

linearly independent set

that $\{x_\Sigma : \Sigma\nearrow, l(\Sigma) \le m\}$ is a basis of $\mathcal{U}_m$. Our statement follows.

"$\Leftarrow$" Since x_Σ is a basis of $\mathcal{U}$, $\{x_\Sigma : \Sigma\nearrow, l(\Sigma) \le m\}$ is a basis of $\mathcal{U}_m$

Then $\{\overline{x_\Sigma} : \Sigma\nearrow, l(\Sigma) = m\}$ is a basis of $G^m = \mathcal{U}_m/\mathcal{U}_{m-1}$.

Note that $\omega|_{S^m}(z_\Sigma) = \phi(t_\Sigma) = \overline{x_\Sigma}$, that is, ω maps a basis of S^m to a basis of G^m. Thus, ω is an isom.

III. Proof of PBW thm (Jacobson)

$\{x_\Sigma, \Sigma \text{ increasing}\}$ span $\mathcal{U}$:

Induce on m: $\{x_\Sigma : \Sigma \nearrow, l(\Sigma) \leq m\}$ span $\mathcal{U}_m$

If $m=0$, it is trivial.

Suppose it holds for m. $\quad \exists \text{ elt} \in S^{m+1}$ s.t. $\omega(\text{elt}) = \mu_{m+1}(x_\Sigma)$

Let $x_\Sigma \in \mathcal{U}_{m+1} \setminus \mathcal{U}_m$, Note that ω surj $\Rightarrow$ $\omega|_{S^{m+1}}: S^{m+1} \to G^{m+1}$ surj.

$\Rightarrow \exists \Sigma_i, i \in [\![1,k]\!], l(\Sigma') = m+1$ s.t. $\omega(\sum_{i=1}^{k} z_{\Sigma_i}) = \mu_{m+1}(x_\Sigma)$.

Then $\mu_{m+1}(x_\Sigma - \sum_{i=1}^{k} x_{\Sigma_i}) = \omega(\sum_{i=1}^{k} z_{\Sigma_i}) - \sum_{i=1}^{k} \phi(t_{\Sigma_i}) = \omega(\sum_{i=1}^{k} z_{\Sigma_i}) - \sum_{i=1}^{k} \omega(z_{\Sigma_i}) = 0$

$\Rightarrow x_\Sigma = \sum x_{\Sigma_i} + x_{\Sigma'}$, where $l(\Sigma_i) = m+1$, $x_{\Sigma'} \in \mathcal{U}_m$.

$\{x_\Sigma : \Sigma \text{ increasing}\}$ linearly independent:

Idea: Construct rep $\rho: \mathfrak{g} \to \mathfrak{gl}(S)$ s.t. the action x_i on z_Σ is similar to x_i acts on x_Σ $\quad$ spanned by z_Σ.

- Define the action of x_i on z_Σ recursively on $l(\Sigma)$.

0. $\quad x_i z_\phi = z_i$

1. $\quad x_i z_j = \begin{cases} z_{(i,j)} & , i \leq j \\ z_{(j,i)} + \sum_k C_{ij}^k z_k & , j < i \end{cases}$ $\quad$ $x_j z_i + [x_i, x_j] z_\phi$, $\quad [x_i, x_j] = \sum_k C_{ij}^k x_k$

----

2. $\quad$ For increasing seq Σ, $l(\Sigma) = m$, let $\Sigma = (j, \Sigma')$,

$$x_i z_\Sigma = \begin{cases} z_{(i,\Sigma)} & , i \leq j \\ x_j x_i z_{\Sigma'} + \sum_k C_{ij}^k x_k z_{\Sigma'} & , j < i \end{cases}$$

Note that $x_k z_{\Sigma'}$ and $x_i z_{\Sigma'}$ are well-defined ($l(\Sigma') = m-1$).

For $x_j(x_i z_{\Sigma'})$, we can define it recursively, since 1 is the minimal index.

- Now check it a well-defined rep:

T.B.A.

- If $\sum_{\Sigma\nearrow} C_\Sigma x_\Sigma = 0$, then $\sum_{\Sigma\nearrow} C_\Sigma x_\Sigma z_\phi = \sum_{\Sigma\nearrow} C_\Sigma z_\Sigma = 0$

Since z_Σ is a basis of V, $C_\Sigma = 0$ for all Σ.

$$\begin{tikzcd} & T^m \arrow[dl, "\sigma"'] \arrow[dr, "\phi_m"] & \\ S^m \arrow[rr, dashed, "\omega|_{S^m}"] & & G^m \end{tikzcd}$$

IV. Proof of PBW thm (Bourbaki)

It suffices to show $\omega|_{S^m}$ is injective, i.e. $\forall s \in S^m$, $\omega(s)=0 \Rightarrow \sigma^{-1}(s) \subseteq I$

that is, $\forall t \in T^m$, $\phi_m(t)=0 \Rightarrow t \in I$

that is, $\forall t \in T^m$, $\pi(t) \in \mathcal{U}_{m-1} \Rightarrow t \in I$

Construct a rep $\rho: \mathfrak{g} \to \mathfrak{gl}(S)$ the same as the rep above.

Then, by universal property of $\mathcal{U}$, ρ can be extend to a rep of $\mathcal{U} \to \mathfrak{gl}(S)$.

Consider $\hat{\rho}: T \xrightarrow{\pi} \mathcal{U} \xrightarrow{\rho} \mathfrak{gl}(V)$

Lemma. Let ρ be the rep above, $\rho(x_i) z_\Sigma \equiv z_{(i,\Sigma)}$ mod S_m if Σ has length m.

Pf. Show it by induction on the length Σ and the index i.

If $\Sigma = 0$ or 1, it is trivial. Suppose this holds for $(l(\Sigma)<m$, all $x_j)$ ① and $(l(\Sigma)=m$, x_j with $j<i)$ ②. Then for any $\Sigma=(k,\Sigma')$ with $l(\Sigma)=m$,

if $i \le k$, $x_i \cdot z_\Sigma = z_{(i,\Sigma)}$;

if $i>k$, $x_i \cdot z_\Sigma = x_k x_i z_{\Sigma'} + [x_i, x_k] z_{\Sigma'}$

by hypo ① $\quad \equiv x_k z_{(i,\Sigma')} + \sum C_{ik}^j z_{(j,\Sigma')}$ mod S_{m-1}

by hypo ② $\quad \equiv z_{(k,i,\Sigma')} = z_{(i,k,\Sigma')}$ mod S_m $\square$

Let $t \in T^m$ and $\pi(t) \in \mathcal{U}_{m-1}$. Denote $t = \sum \alpha_i t_{\Sigma_i}$ for some Σ_i of length m.

Since $\pi(t) \in \mathcal{U}_{m-1}$, there exists $t' \in T^{m-1}$ s.t. $\pi(t)=\pi(t')$

By lemma above, $\hat{\rho}(t)\cdot z_\phi = \sum \alpha_i \rho(x_{\Sigma_i})\cdot z_\phi \equiv \sum \alpha_i z_{\Sigma_i}$ mod S_m

But $\hat{\rho}(t) z_\phi = \rho\circ\pi(t)\cdot z_\phi = \rho\circ\pi(t') z_\phi \equiv 0$ mod S_m

Hence, it means $\sigma(t) = \sum \alpha_i z_{\Sigma_i} = 0$, that is, $t \in I$ as desired.

V. Proof of PBW thm (Dimond Lemma)

Actually it's NOT necessary, so this method adapts to inf-dim Lie alg as well.

As long as, X has a order!

Def. Let $A = \langle X \mid R \rangle$ be a fin presentation of an ass alg. X has an order with minimal condition.

alphabet relation

Denote the sets of all word by $X^* = \{x_1 \cdots x_k \in \mathbb{K}\langle X\rangle : x_i \in X\}$.

For any $f \in \mathbb{K}\langle X \rangle$, $f = \alpha_1 w_1 + \cdots + \alpha_k w_k$, where $w_i \in X^*$, $\alpha_i \in \mathbb{K}^*$. Let w_j be the maxi word w.r.t the lexi order. Then call w_j the leading monomial of f, denoted by $\bar{f}$.

Rmk. For $A = \langle X \mid R \rangle$, if $f \in R$, then $\bar{f} = \omega_j = \sum_{i \neq j} \frac{\alpha_i}{\alpha_j} w_i$. Thus $\bar{f}$ can be writen as a linear comb of smaller words in A.

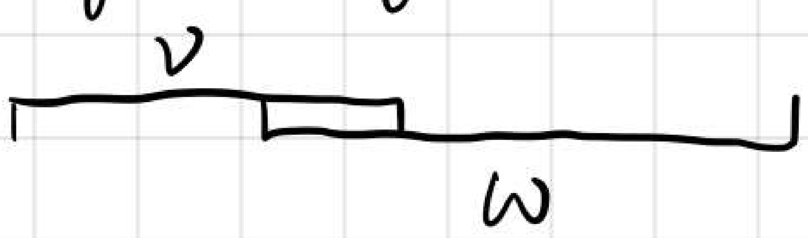
Def A word $w \in X^*$ is reducible if it contains some $\bar{f}$, $f \in R$, as a subword. i.e. $\omega = \omega' \bar{f} \omega''$. $\omega', \omega'' \in X^*$. Otherwise, ω is called irreducible.

Prop Irreducibles span A.

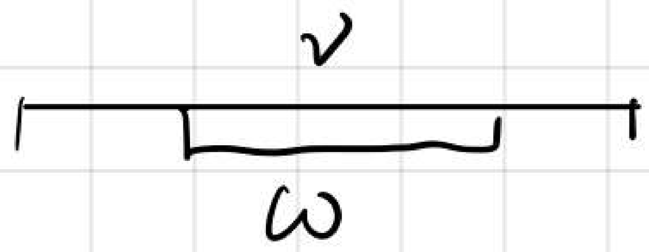
Pf. From the Remark above, it is easy to show this by induction on the order.

Def Given words v & $w \in X^*$, we say v, w admit a composition if

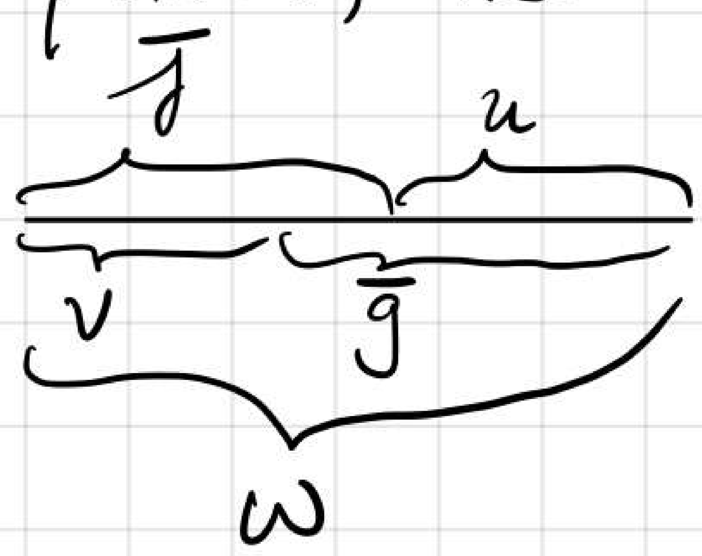
1° the end of one of words is the beginning of the other.



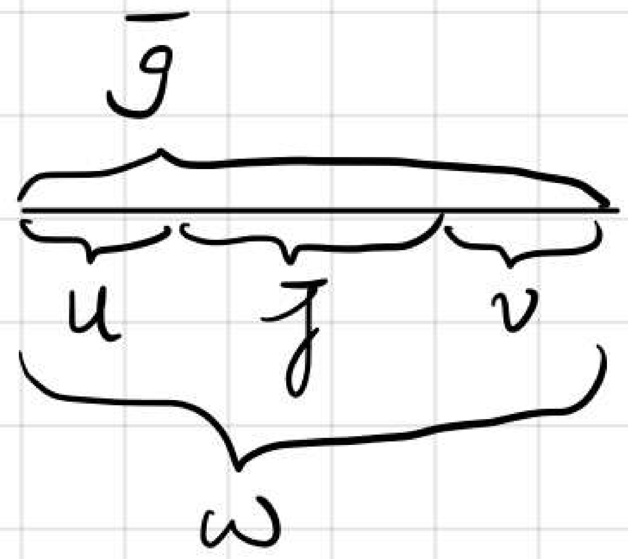
2° One of these words is a subword of the other.



Def Let $f, g \in F\langle X \rangle$. The coef at $\bar{f}, \bar{g}$ resp are equal to 1. Suppose that $\bar{f}, \bar{g}$ admit a composition, i.e.



or



The element $(f,g)_w = fu - vg$ (or $ufv - g$) is called the composition of f & g. w.r.t the word w.

Thm. $A = \mathbb{K}\langle X \mid R \rangle$, irreducibles are a basis of A $\Longleftrightarrow$ For any two relations $f, g \in R$ that admit a composition, all their compositions $(f,g)_w$ reduce to 0.

Pf. "$\Rightarrow$" If there exists one reduction not 0, then it is a nontrivial linear comb of irreducible words. Since $f, g \in R$, $(f,g)_w = 0$ in A. Thus, this linear comb $= 0$.

"$\Leftarrow$" Claim that $\forall f \in id(R) \setminus \{0\}$, the leading monomial $\bar{f}$ is reducible.

If this holds, every nontrivial linear combination of irreducibles g, $\bar{g}$ irreducible. $\Rightarrow g \notin id(R)$, that is, all irreducibles in A are linearly independent. By Rmk above, they are a basis.

So it suffices to show the claim: Denote $f \in \mathrm{id}(R)\setminus\{0\}$ by $\sum_i \alpha_i u_i \overline{r_i} v_i$, where $\alpha_i \in \mathbb{K}$, $u_i, v_i \in X^*$, $r_i \in R\setminus\{0\}$. Note that $\overline{u_i \overline{r_i} v_i} = u_i \overline{r_i} v_i$ (u_i, v_i are monomials)
Let $\omega = \max\{\overline{u_i r_i v_i} : i\}$. If ω occurs in one summand, then $\overline{f} = \omega$, which is reducible; if ω occurs more than once, we prove it by induction on the order of ω.

quite difficult and a more detailed discussion is needed. :(!

Ex. $A = \langle x, y \mid y^2x - xyx \rangle$.

1° $x<y$. then y^2x does not admit a comp with itself. Thus, thm works.

2° $x>y$. then $\omega = x\underbrace{y\overbrace{xyx}}$, and

$$(-xyx+y^2x, -xyx+y^2x)_\omega = y^2\underline{xyx} - xy^3x = y^4x - xy^3x$$

Irreducibles

Thus, irreducibles are not linearly independent!

$\sum C_{ij}^k x_k$

Cor. The universal enveloping alg $\mathcal{U} = \mathbb{K}\langle x_1, x_2, \cdots, x_n \mid x_ix_j - x_jx_i - [x_i, x_j] \rangle$ has a basis $\{x_{i_1}\cdots x_{i_m} : i_1 < \cdots < i_m,\ i_j \in [\![1,n]\!]\}$

pf. Step 1. The set R is closed w.r.t compositions:

Consider relations
$$f = x_ix_j - x_jx_i - [x_i, x_j]$$
$$g = x_jx_k - x_kx_j - [x_j, x_k]$$
, $k<j<i$

$\omega = x_ix_jx_k$,

$$\begin{aligned}
(f,g)_\omega &= -x_jx_ix_k - [x_i,x_j]x_k + x_ix_kx_j + x_i[x_j,x_k] \\
&= -x_j(x_kx_i + [x_i,x_k]) - [x_i,x_j]x_k + (x_kx_i + [x_i,x_k])x_j + x_i[x_j,x_k] \\
&= -x_jx_kx_i - x_j[x_i,x_k] - [x_i,x_j]x_k + x_kx_ix_j + [x_i,x_k]x_j + x_i[x_j,x_k] \\
&= -(x_kx_j + [x_j,x_k])x_i - x_j[x_i,x_k] - [x_i,x_j]x_k + x_k(x_jx_i + [x_i,x_j]) + \\
&\quad [x_i,x_k]x_j + x_i[x_j,x_k] \\
&= -[x_j,x_k]x_i + x_i[x_j,x_k] - x_j[x_i,x_k] + [x_i,x_k]x_j - [x_i,x_j]x_k + x_k[x_i,x_j] \\
&= [x_i,[x_j,x_k]] + [x_j,[x_k,x_i]] + [x_k,[x_i,x_j]] \\
&= 0.
\end{aligned}$$

Step 2. All irreducibles are $x_{i_1}\cdots x_{i_m}$, $m \in \mathbb{N}^*$, $i_1 \le \cdots \le i_m$ & 1.

Note that for any relation f, say $f = x_ix_j - x_jx_i - [x_i,x_j]$, $i<j$, the leading monomial $\overline{f} = x_jx_i$. Thus, a word in X^* is reducible iff it has a x_jx_i as subword where $j>i$. Then our claim follows.