Lecture $10\frac{1}{3}$: $(x+y)^p-x^p-y^p$

0) Introduction.
1) Free Lie algebra
2) Primitive elements.

0) The goal of this note is to prove part 3 of Thm in Sec. 1.2 of Lec 10: if $\mathbb{F}$ is a characteristic p field, A is an associative (unital) $\mathbb{F}$-algebra & $x,y\in A$, then $(x+y)^p-x^p-y^p$ is a Lie polynomial in x,y that is "universal" - independent of x,y,A.

Example: $p=2$: $(x+y)^2-x^2-y^2=xy+yx=[x,y]$

$p=3$: $(x+y)^3-x^3-y^3=x^2y+xyx+yx^2+xy^2+yxy+y^2x=[x,[x,y]]+[y,[y,x]]$.

Our strategy is as follows:

1: we introduce the free Lie algebra on the alphabet $x_i, i\in I$. The universal enveloping algebra of this Lie algebra is the free associative algebra. Our problem becomes to show that for the free Lie algebra $\mathcal{L}_2$ w. generators x,y the element $(x+y)^p-x^p-y^p$ of $\mathcal{U}(\mathcal{L}_2)=\mathbb{F}\langle x,y\rangle$ is in $\mathcal{L}_2$. This is Section 1.

2: We have $(x+y)^p-x^p-y^p\in\mathcal{U}(\mathcal{L}_2)_{\leq p-1}$. For an arbitrary Lie algebra $\mathfrak{g}$ over $\mathbb{F}$, $\mathfrak{g}$ is recovered inside $\mathcal{U}(\mathfrak{g})_{\leq p-1}$ as the subspace of "primitive elements." This is Section 2.

1) Free Lie algebras.

The construction: Pick an alphabet x_i, $i\in I$. Consider the free (non-assoc've) $\mathbb{F}$-algebra Free_I: it's basis consists of finite bracketed monomials in the alphabet x_i, e.g. $(x_1x_2)x_3 \neq x_1(x_2x_3)$, and the product of basis elements is given by $a\cdot b=(a)(b)$.

The free Lie algebra $\mathcal{L}_I$ is the quotient of Free_I by the 2-sided ideal spanned by the elements $[a,a]$, $[[a,b],c]+[b,[c,a]]+[c,[a,b]]$ for $a,b,c\in \mathrm{Free}_I$. It's universal property: for all Lie algebras $\mathfrak{g}$ and elements $a_i\in\mathfrak{g}$, $i\in I$, $\exists!$ Lie algebra homomorphism $\mathcal{L}_I\to\mathfrak{g}$ w. $x_i\mapsto a_i$.

Now we describe $\mathcal{U}(\mathcal{L}_I)$.

Lemma: We have an associative algebra isomorphism $\mathcal{U}(\mathcal{L}_I)\xrightarrow{\sim}\mathbb{F}\langle x_i\rangle_{i\in I}$ (the free associative algebra) w. $x_i\leftrightarrow x_i$.

Proof: To give a homomorphism $\mathcal{U}(\mathcal{L}_I)\longrightarrow\mathbb{F}\langle x_i\rangle$ of associative algebras is the same as to give a homomorphism $\mathcal{L}_I\to\mathbb{F}\langle x_i\rangle$ of Lie algebras. Now we use the universal property of $\mathcal{L}_I$ and get the unique homomorphism $\mathcal{U}(\mathcal{L}_I)\longrightarrow\mathbb{F}\langle x_i\rangle$ w. $x_i\mapsto x_i$. The homomorphism in the opposite direction comes from the universal property of $\mathbb{F}\langle x_i\rangle$. $\square$

2) Primitive elements

2.1) Hopf algebra structure on $\mathcal{U}(\mathfrak{g})$ & primitive elements.

Here $\mathbb{F}$ is an arbitrary field.

Lemma: There are unique algebra homomorphisms:

- $\Delta: \mathcal{U}(\mathfrak{g}) \longrightarrow \mathcal{U}(\mathfrak{g}) \otimes \mathcal{U}(\mathfrak{g})$ w. $\Delta(x) = x \otimes 1 + 1 \otimes x$,
- $S: \mathcal{U}(\mathfrak{g}) \to \mathcal{U}(\mathfrak{g})^{opp}$, $S(x) = -x$,
- $\eta: \mathcal{U}(\mathfrak{g}) \to \mathbb{F}$, $\eta(x) = 0$,

for $x \in \mathfrak{g}$. They equip $\mathcal{U}(\mathfrak{g})$ w. a Hopf algebra structure.

Definition: An element $a \in \mathcal{U}(\mathfrak{g})$ is *primitive* if $\Delta(a) = a \otimes 1 + 1 \otimes a$.

Example: $\mathfrak{g}$ consists of primitive elements.

Exercise: if char $\mathbb{F} = p$, and $a \in \mathcal{U}(\mathfrak{g})$ is primitive, then so is a^p.

2.2) Primitive elements in $\mathcal{U}(\mathfrak{g})_{\leq p-1}$

Thm: Let char $\mathbb{F} = p$. The only primitive elements in $\mathcal{U}(\mathfrak{g})_{\leq p-1}$ are in $\mathfrak{g}$.

Rem: if char $\mathbb{F} = 0$, then the claim holds for the entire $\mathcal{U}(\mathfrak{g})$.

Here's an important observation for the proof of the theorem.

As was mentioned in Lecture 8.5, Section 1, the subspaces $\mathcal{U}(\mathfrak{g})_{\leq d}$ $(d \geq 0)$ form an algebra filtration. We have a natural algebra homomorphism $S(\mathfrak{g}) \longrightarrow \operatorname{gr} \mathcal{U}(\mathfrak{g})$ and by the PBW theorem, it's an isomorphism.

Proof of Thm: Pick a degree $i \leq p-1$ element $a \in U(\mathfrak{g})$ and let $\bar{a} := a + U(\mathfrak{g})_{\leq d-1} \in \operatorname{gr} U(\mathfrak{g}) = S(\mathfrak{g})$, a degree d homogeneous element in $S(\mathfrak{g})$. Assume the contrary: $a \notin \mathfrak{g}$. Next, assume $d > 1$.

Pick a basis $x_i, i \in I$, in $\mathfrak{g}$ and equip it with a total order. Then $U(\mathfrak{g})$ has a basis of ordered monomials in x_i's.

Consider $\Delta(a) \in U(\mathfrak{g}) \otimes U(\mathfrak{g})$. It has the form (exercise) $\Delta(a) = a \otimes 1 + 1 \otimes a + \sum_{i \in I} x_i \otimes a_i + \ldots$, where $\ldots$ stands for the sum of tensor monomials with the first factor of degree j w.r.t. x_i's, where $2 \leq j \leq d-1$. Clearly if $\Delta(a) = a \otimes 1 + 1 \otimes a$, then $a_i = 0$ $\forall i$.

Exercise: • Show that $a_i + U(\mathfrak{g})_{<d-1} = \frac{\partial \bar{a}}{\partial x_i}$. Deduce $d=1$.

• The primitive elements in $U(\mathfrak{g})_{\leq 1}$ are in $\mathfrak{g}$.

$\square$

2.3) Completion of proof.

We set $\mathfrak{g} = \mathcal{L}_2$. By Exercise in Section 2.1, $(x+y)^p - x^p - y^p$ is primitive. Thx to Thm in Sec 2.2, we'll be done if we show $(x+y)^p - x^p - y^p \in U(\mathfrak{g})_{\leq p-1}$. But $\operatorname{gr} U(\mathfrak{g})$ is commutative so $(x+y)^p - x^p - y^p + U(\mathfrak{g})_{\leq p-1} = 0$ in $\operatorname{gr} U(\mathfrak{g}) \Leftrightarrow (x+y)^p - x^p - y^p \in U(\mathfrak{g})_{\leq p-1}$.

This finally shows $(x+y)^p - x^p - y^p \in \mathcal{L}_2$. This is the Lie polynomial we need.