Cpt 2. Integrals and semisimplicity

Cpt 2.3. comm. s.s. hopf algs and restricted enveloping algs.

1. lemma:

① If A is a f.d. separable $\mathbb{K}$-alg

then $A \cong \bigoplus_i M_{n_i}(D_i)$, where $\{D_i\}$ are division algs s.t.

$\{Z(D_i)\}$ are separable extensions of $\mathbb{K}$.

② In particular, if A is a f.d. commu. separable $\mathbb{K}$-alg,

then $A = \bigoplus_i E_i$, where $\{E_i\}$ are separable extensions of $\mathbb{K}$

2. Theorem

①. Let H be a f.d. comm. s.s. hopf alg. over $\mathbb{K}$.

then there exists a separable extension E of $\mathbb{K}$

s.t. $H \otimes E \cong E^{(n)}$, where $n = \dim_{\mathbb{K}} H$

pf: (1) by 2.2.2, H is separable over $\mathbb{K}$.

Hence $H = \bigoplus_{i=1}^{r} E_i$, where $\{E_i\}$ are separable extensions of $\mathbb{K}$.

(2) let $E_i = \mathbb{K}[x]/f_i(x)$, for some irreducible polynomial f_i, $i = 1, \cdots, m$

We may take E to be a common extension of E_i

then $E_i \otimes_{\mathbb{K}} E = (\mathbb{K}[x]/f_i(x)) \otimes_{\mathbb{K}} E$ ∂ extension

$= E[x]/f_i(x)$

(3). Since $E_i/\mathbb{K}$ is a separable extension, f_i has distinct roots,

Write $f_i(x) = \prod_{j=1}^{m_i}(x - a_j)$, where $m_i = \deg f_i = \dim_{\mathbb{K}} E_i$

by Chinese Remainder Thm, we have

$$E[x]/f_i(x) = E[x]/\prod_j (x - a_j) \cong \bigoplus_{j=1}^{m_i} E/(x - a_j) \cong E^{(m_i)}$$

Hence $H \otimes_{\mathbb{K}} E \cong E^{(n)}$ is a direct sum of field E.

where $n = \dim_{\mathbb{K}} H = \sum m_i$

② let $H = \mathbb{K}^{(n)}$ be a Hopf algebra, then $H^* \cong (\mathbb{K}G)$ as hopf algs for some group G.

pf:

let $\{p_i\}_{i=1}^n$ be a basis of orthogonal idempotents in H

and let $\{g_i\}_{i=1}^n$ be its dual basis in H^*

Since $g_i(p_j \cdot p_k) = \delta_{jk} \cdot g_i(p_j) = \delta_{ij} \cdot \delta_{jk} = g_i(p_j) \cdot g_i(p_k)$

we have $g_i \in Alg(H, \mathbb{K})$, hence $g_i \in G(H^*)$

Since grouplike elements are linearly independent,

the set G of all g_i is a group.

Thus $H^* \cong \mathbb{K}G$

③ Thm: If H is a f.d. commu. S.S. hopf algebras,

then there exists a finite separable extensions E of $\mathbb{K}$,

and a finite group G s.t. $H \otimes E \cong (\mathbb{K}G)^*$

3. restricted enveloping alg.

① let $\mathbb{K}$ have characteristic $p \neq 0$. A Lie algebra over $\mathbb{K}$

is restricted if $\exists$ $[p]: \mathfrak{g} \to \mathfrak{g}$, $x \mapsto x^{[p]}$, s.t. for all $x, y \in \mathfrak{g}$, $\alpha \in \mathbb{K}$,

the following holds:

(1) $(\alpha \cdot x)^{[p]} = \alpha^p \cdot x^{[p]}$

(2) $(x+y)^{[p]} = x^{[p]} + y^{[p]} + \sum_{i=1}^{p-1} \frac{S_i(x,y)}{i}$

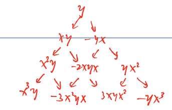
where $S_i(x,y)$ is the coefficient of t^{i-1} in $ad(tx+y)^{p-1} \cdot (x)$

(3) $ad\, x^{[p]} = (ad\, x)^p$

② Example: Let A be any algebra over a field $\mathbb{K}$ with char $p \neq 0$, then $[A]$ is restricted via $[p]: a \mapsto a^p$

pf: (1) is trivial

(3). $\mathrm{ad}\,x(y) = xy - yx$,



if $\mathrm{ad}\,x^n(y) = \sum_{k=0}^{n} \binom{n}{k} \cdot (-1)^k \cdot x^{n-k} y \cdot x^k$, $n < p$

then $\mathrm{ad}\,x^{n+1}(y) = \mathrm{ad}\,x\left(\sum_{k=0}^{n} \binom{n}{k} \cdot (-1)^k \cdot x^{n-k} y \cdot x^k \right)$

$$= \sum_{k=0}^{n} \binom{n}{k} \cdot (-1)^k \left(x^{n-k+1} y \cdot x^k - x^{n-k} y \cdot x^{k+1} \right)$$

$$= \sum_{k=0}^{n} \binom{n}{k} \cdot (-1)^k \cdot x^{n-k+1} y \cdot x^k + \overset{\downarrow\, k \to k+1}{\sum_{k=1}^{n+1}} \binom{n}{k-1} (-1)^k \cdot x^{n+1-k} \cdot y \cdot x^k$$

$$= x^{n+1} y + y x^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k} + \binom{n}{k-1} \right) \cdot (-1)^k \cdot x^{n+1-k} \cdot y \cdot x^k$$

$$= \sum_{k=0}^{n+1} \binom{n+1}{k} (-1)^k \cdot x^{n+1-k} \cdot y \cdot x^k$$

by induction, $(\mathrm{ad}\,x)^p(y) = \sum_{k=0}^{p} \binom{p}{k} (-1)^k \cdot x^{p-k} \cdot y \cdot x^p$

$$= x^p y - y \cdot x^p$$

$$= \mathrm{ad}\,x^p(y)$$

(2) Remark: The second condiction is difficult to check in general. In the case that A is commutative, the second axiom applied to A is exactly the binomial theorem in characteristic p. i.e. $(a+b)^p = a^p + b^p$.

let $W = \{$words in x and y of length $p\}$, then $(x+y)^p = \sum_{w \in W} w$

by (3),

$$(\mathrm{ad}\, tx+y)^{p-1}(x) = \sum_{k=0}^{p-1} \binom{p-1}{k} \cdot (-1)^k \cdot (tx+y)^{p-1-k} \cdot x \cdot (tx+y)^k$$

$$= \sum_{k=0}^{p-1} (tx+y)^{p-1-k} \cdot x \cdot (tx+y)^k$$

the second equal sign holds, since $\binom{p-1}{k} \cdot (-1)^k \equiv 1 \pmod p$, $\forall\, 0 \le k < p$

Fix a word $w \in W$ with j x's, where $1 \le j \le p-1$. we would like to know how many times this word is counted in the given sum.

w is a summand of the expansion of $(tx+y)^{p-1-k} \cdot x \cdot (tx+y)^k$ iff w has an x in the $(p-k)$-th position. hence w is counted in $(\mathrm{ad}\, tx+y)^{p-1}(x)$ exactly j times. #

Note: $\binom{p-1}{0}=1$, $\binom{p-1}{k} \equiv \binom{p}{k}-\binom{p-1}{k-1} \equiv -\binom{p-1}{k-1} \mod p$, $\forall\, k<p$

Note 2: $p=2$, $(x+y)^2 = x^2+y^2+xy+yx$

$$(\mathrm{ad}\, tx+y)(x) = t\cdot x^2+yx-(t\cdot x^2+xy)$$
$$= yx+xy$$

Hence $s_1(x,y) = yx+xy$

$p=3$: $(x+y)^3 = x^3+y^3+xy^2+x^2y+xyx+x^2y+xy^2+yxy$

$$(\mathrm{ad}\, tx+y)^2(x) = (tx+y)^2\cdot x + (tx+y)\cdot x\cdot(tx+y) + x\cdot(tx+y)^2$$
$$= t^2\cdot 3\cdot x^3 + y^2x+yxy+xy^2$$
$$+ t\cdot(xyx+yx^2+x^2y+yx^2+x^2y+xyx)$$

Hence $s_1(x,y) = y^2x+yxy+xy^2$

$$s_2(x,y) = \tfrac{1}{2}(xyx+yx^2+x^2y+yx^2+x^2y+xyx)$$
$$= xyx+yx^2+x^2y$$

③ another example.

Let g be any abelian Lie alg over $\mathbb{K}$, with char $p \neq 0$.

g is a restricted Lie algebra via $x^{[p]}=0$

pf: (1) $(a\cdot x)^{[p]}=0=a^p\cdot x^{[p]}$

(3) $\mathrm{ad}_{x^{[p]}}(y)=0=\mathrm{ad}\, x^p(y)$, since g is abelian.

(2) $(\mathrm{ad}\, tx+y)^{p-1}(y)=0$, $(x+y)^{[p]}=0$ #

4. enveloping alg.

① If g is restricted and $U(g)$ the the usual enveloping algebra, let B be the ideal in $U(g)$ generated by $\{x^p - x^{[p]} \mid x\in g\}$, and define $u(g) = U(g)/B$.

$u(g)$ is called the restricted enveloping alg. or u-alg. of g.

② Since $g\cap B=0$, g imbedds into $[u(g)]$.

A version of PBW theorem holds for $u(g)$, i.e.

let $\{x_i \mid i \in I\}$ be a basis of $\mathfrak{g}$ and "$<$" a total order on I. then $\{x_{i_1}^{r_1} \cdots x_{i_n}^{r_n} \mid i_1 < i_2 < \cdots < i_n,\ n \in \mathbb{Z}_+,\ r_n \le p-1\}$ is a basis of $u(\mathfrak{g})$. Consequently if $\dim \mathfrak{g} = n$, then $\dim u(\mathfrak{g}) = p^n$

③ $u(\mathfrak{g})$ becomes a Hopf alg. since B is a hopf ideal of $U(\mathfrak{g})$.

pf:

Since $\Delta(x^p) = \sum_{k=0}^{p} \binom{p}{k} x^k \otimes x^{p-k} = x^p \otimes 1 + 1 \otimes x^p$

$\{x^p \mid x \in \mathfrak{g}\}$ are also primitive elements of $U(\mathfrak{g})$

Thus B is a coideal of $U(\mathfrak{g})$ and $S(B) = -B \subseteq B$

i.e. B is a hopf ideal of $U(\mathfrak{g})$.

5. Thm.

① let V, W be modules over field $\mathbb{K}$, $f: V \to W$ is a semi-linear map if the following holds

(1) $f(v+v') = f(v) + f(v')$, $\forall v, v' \in V$

(2) $f(\lambda \cdot v) = \lambda^\theta \cdot f(v)$, $\forall v \in V$, $\alpha \in \mathbb{K}$. where θ is an automorphism of $\mathbb{K}$.

② If $\dim_{\mathbb{K}} V = \dim_{\mathbb{K}} W < \infty$, then f is surjective $\Leftrightarrow$ f is injective

pf: let $\{v_i\}$ be a basis of V. $w_i = f(v_i) \in W$, $\forall i$

then $\mathrm{Im} f = \mathbb{K}.\{w_i\}$

$\Rightarrow$: If f is surjective, then $\{w_i\}$ is a basis of W.

$v = \sum_i k_i v_i \in V$ s.t. $f(v) = 0 \Rightarrow \sum_i k_i^\theta w_i = 0$

$\Rightarrow k_i^\theta = 0,\ \forall i$

Thus f is injective

$\Leftarrow$: Conversely, assume that f is injective

$\forall k_i \in \mathbb{K}$ s.t. $\sum_i k_i w_i = 0 \Rightarrow f(\sum_i k_i^{\theta^{-1}} v_i) = 0$

$\Rightarrow \sum_i k_i^{\theta^{-1}} v_i = 0$

$\Rightarrow k_i \equiv 0,\ \forall i$

Thus $\{w_i\}$ are linearly independent, and $\dim \mathrm{Im} f = \dim V = \dim W$ #

③. let g be a f.d. restricted Lie algebra over field $\mathbb{K}$ of char $p \neq 0$

$u(g)$ is semisimple $\Leftrightarrow$ g is abelian and $g = \mathbb{K} g^p$

g^p is not necessarily equal to $\mathbb{K} g^p$

pf:

(1) let E be the algebraic closure of $\mathbb{K}$, Since

$u(g \otimes E) \cong u(g) \otimes E$ is semisimple $\Leftrightarrow$ $u(g)$ is semisimple, and

$(g \otimes E)^p = g \otimes E \Leftrightarrow g^p = g$, we may assume that $\mathbb{K}$ is algebraic closed.

(2) $\Leftarrow$: When g is abelian, $H = u(g)$ is commutative, hence

$(x+y)^p = x^p + y^p$, $(x \cdot y)^p = x^p \cdot y^p$

$\mathbb{K}$ is algebraic closed $\Rightarrow$ $\mathbb{K}$ is perfect

$\Rightarrow \mathbb{K} \to \mathbb{K}^p$ is an automorphism

$\Rightarrow$ the p-map is semilinear

Since $(x \cdot y)^p = x^p \cdot y^p$, H^p is a subalgebra of H generated

by $g^p = g$. Thus $H^p = H$, p is surjective hence injective.

Hence H has no non-zero nilpotent elements so is semisimple.

$\Rightarrow$: (pass).

⑥. let g be a Lie algebra (resp. restricted Lie algebra)

of char $p \neq 0$. If $f \in U(g)^{\circ}$ (resp. $u(g)^{\circ}$) is an algebra

morphism, then $f^p = \epsilon$

pf: It is enough to show that $f^p(1) = 1$, $f^p(x) = 0$, $\forall x \in g$

(1) $f^p(1) = 1$ is trivial, since f is algebraic.

(2) If $f^n(x) = n f(x)$, $n < p$, then $f^{n+1}(x) = f * f^n(x)$

$= f(1) \cdot f^n(x) + f^n(1) \cdot f(x) = (n+1) f(x)$

Hence $f^p(x) = p \cdot f(x) = 0$ #

⑤. let g be a f.d. restricted Lie algebra of char $p \neq 0$ s.t.

$u(g)$ is semisimple. Then for some finite separable field extension $E \supseteq \mathbb{K}$, $u(g) \otimes E \cong (EG)^*$, where $G \cong (\mathbb{Z}_p)^n$

pf: By ③, $H = u(g)$ is commutative.

By 2.①, $u(g) \otimes E \cong (EG)^*$ for $E \supseteq \mathbb{K}$ as desired.

Moreover $|G| = \dim u(g) = p^n$.

By ④, since $G(H^*) = Alg(H, \mathbb{K})$, every non-identity element of G has order p. Thus $G \cong (\mathbb{Z}_p)^n$

Cpt 2.4. cosemisimplicity and integrals on H

0. dual version of Maschke's thm.

1. definition

① let C be a coalgebra,

(1) C is simple (cosimple) if it has no proper subcoalgebra.

(2) C is cosemisimple if it is a direct sum of simple subcoalgebras.

Note: (1) A is simple if it has no proper ideal.

(2) A is semisimple if it is a direct sum of simple ideals

Remark: Cpt5: when C is f.d., C is a co.s.s. coalgebra $\Leftrightarrow$ C^* is a s.s. algebra. Moreover, C is cosimple $\Leftrightarrow$ C^* is simple.

Example: $C = \mathbb{K}G$ is cosemisimple since $C = \bigoplus_{g \in G} \mathbb{K}g$ is a direct sum of cosimple coalgebra. C^* is semisimple since $C^* \cong \mathbb{K}^{(n)}$

②. let M be a right C-comodule, then

(1). M is simple (cosimple) if it has no proper submodules

(2) M is completely reducible if it is a direct sum of simple submodules.

2. C is cosemisimple iff every right (left) C-comodule is completely reducible.

Ref: Sweedler 14.0.1

3. let H be a Hopf algebra, An element $T \in H^*$ is a left integral on H if for all $h^* \in H^*$, $h^* T = h^*(1_H) T$.

The space of left integrals on H will be denoted by I_H^l.

Right integrals are defined similarly.

Prop: when H is finite-dimensional, an integrals on H is an integral in H^*. Since $T \in \int_{H^*}^l \Leftrightarrow h^* T = \epsilon_{H^*}(h^*) \cdot T = h^*(1_H) \cdot T$, $\forall h^* \in H^*$

4. Example. (motivating influence for the terminology "integral".)

Let G be a compact topological group, and let $H = R_{\mathbb{C}}(G)$ be the hopf algebra of continuous complex-valued representative functions. i.e. $H = \{ f \in R_{\mathbb{C}}(G) \mid f: G \to \mathbb{C}$ is continuous $\}$. The Harr integral is an integral in the sense of 2.4.4.

5. dual Maschke Thm: The following are equivalent.

(1) H is cosemisimple (as a coalgebra)

(2) There exists a left integral T on H s.t. $T(1_H) = 1$ (i.e. $\epsilon_{H^*}(T) = 1$)

Remark: 1. ref: sweedler 14.0.3.

2. when $\dim H < \infty$, this is equivalent to Maschke's Thm.

3. If $\mathbb{K}$ has charateristic 0, and H is commutative, then H is cosemisimple $\Leftrightarrow$ $I_H \neq 0$

Cpt 2.5. Kaplansky's conjecture and the order of the antipode.

Thm: let H be a f.d. hopf alg, then the antipode S has finite order.

Remark: 1. S^4 has a very special form: $S^{-4} = (\mathrm{ad}\, a) \circ (\mathrm{ad}\, \alpha)^*$

2. Kaplansky conjectured that the antipode of any f.d. cosemisimple Hopf algebra has order 2.

3. [La. R] (a): If $\mathrm{char}\, \mathbb{K} = 0$, then f.d. cosemisimple Hopf algebras are semisimple.

(2) f.d. co.s.s and s.s. Hopf algebras over a field $\mathbb{K}$ of char 0 or char $p > (\dim H)^2$. Then $S^2 = id$.

Cpt 2.3 - 2.5 summary

Cpt 2.3.

1. comm. s.s. hopf alg.

① A is a f.d. separable $\mathbb{K}$-alg. $\Leftrightarrow A \cong \bigoplus_i M_{n_i}(D_i)$, where D_i are division alg. s.t. $Z(D_i)/\mathbb{K}$ are separable field extension.

② If H is a f.d. comm. s.s. hopf alg. over $\mathbb{K}$, then $\exists$ separable extension E of $\mathbb{K}$ s.t. $H \otimes E \cong E^{(n)} \cong (EG)^*$ for some group G.

2. restricted lie algebra and its enveloping algebra.

① Let $\mathfrak{g}$ be a f.d. restricted lie algebra over field $\mathbb{K}$ of char $p \neq 0$, then $u(\mathfrak{g})$ is s.s. $\Leftrightarrow$ $\mathfrak{g}$ is abelian and $\mathfrak{g} = \mathbb{K}\mathfrak{g}^p$

②. $f \in Alg(U(\mathfrak{g})^\circ, \mathbb{K}) \Rightarrow f^p = \epsilon$

$f \in Alg(u(\mathfrak{g})^\circ, \mathbb{K}) \Rightarrow f^p = \epsilon$

1+2 : $\mathfrak{g}$ is defined as above $\Rightarrow u(\mathfrak{g}) \otimes E \cong (EG)^*$, where $G = (\mathbb{Z}_p)^n$, $n = \dim_{\mathbb{K}} H$

Cpt 2.4.

1. cosemisimplicity, integrals on H

2. dual Maschke's Thm : cosemisimple $\Leftrightarrow$ $\exists$ an integrals T s.t. $\epsilon_{H^*}(T) \neq 0$.

Cpt 2.5.

1. Kaplansky's conjecture: f.d. co.s.s. Hopf alg. $\Rightarrow S^2 = Id$.

2. some results by [La. R]