CHAPTER 4

The Infinitesimal Theory

1. Integrals and Fourier Transforms

Assume for this chapter that $\mathbb{K}$ is a field.

Lemma 4.1.1. Let $C$ be a finite dimensional coalgebra. Every right $C$-comodule $M$ is a left $C^*$-module by $c^*m = \sum m_i(c^*, m_{(1)})$ and conversely by $\delta(m) = \sum c_i^* m \otimes c_i$ where $\sum c_i^* \otimes c_i$ is the dual basis.

Proof. We check that $M$ becomes a left $C^*$-module

\[(c^* c^*)m = \sum m_{(M)}(c^* c^*, m_{(1)}) = \sum m_{(M)}(c^*, m_{(1)}) \langle c^*, m_{(2)} \rangle = c^* \sum m_{(M)}(c^*, m_{(1)}) = c^*(c^* m).\]

It is easy to check that the two constructions are inverses of each other. In particular assume that $M$ is a right $C$-comodule. Choose $m_i$ such that $\delta(m) = \sum m_i \otimes c_i$. Then $c^*_j m = \sum m_i \langle c^*_j, c_i \rangle = m_j$ and $\sum c_i^* m \otimes c_i = \sum m_i \otimes c_i = \delta(m)$. \qed

Definition 4.1.2. 1. Let $A$ be an algebra with augmentation $\varepsilon : A \to \mathbb{K}$, an algebra homomorphism. Let $M$ be a left $A$-module. Then $A M = \{m \in M | am = \varepsilon(a)m \}$ is called the space of left invariants of $M$.

This defines a functor $A^\cdot : A \to \text{Mod}$.

2. Let $C$ be a coalgebra with a group-like element $1 \in C$. Let $M$ be a right $C$-comodule. Then $M^{\text{co}C} := \{m \in M | \delta(m) = m \otimes 1 \}$ is called the space of right coinvariants of $M$.

This defines a functor $-^{\text{co}C} : \text{Comod-C} \to \text{Vec}$.

Lemma 4.1.3. Let $C$ be a finite dimensional coalgebra with a group like element $1 \in C$. Then $A := C^*$ is an augmented algebra with augmentation $\varepsilon : C^* \ni a \mapsto \langle a, 1 \rangle \in \mathbb{K}$. Let $M$ be a right $C$-comodule. Then $M$ is a left $C^*$-module and we have

$C^* M = M^{\text{co}C}$.

Proof. Since $1 \in C$ is group-like we have $\varepsilon_A(ab) = \langle ab, 1 \rangle = \langle a, 1 \rangle \langle b, 1 \rangle = \varepsilon_A(a)\varepsilon_A(b)$ and $\varepsilon_A(1_A) = \langle 1_A, 1_C \rangle = \varepsilon_C(1_C) = 1$.

We have $m \in M^{\text{co}H}$ iff $\delta(m) = \sum m_{(M)} \otimes m_{(1)} = m \otimes 1$ iff $\sum m_{(M)} \langle a, m_{(1)} \rangle = m \langle a, 1 \rangle$ for all $a \in A = C^*$ and by identifying $C^* \otimes C = \text{Hom}(C^*, C^*)$ iff $am = \varepsilon_A(a)m$ iff $m \in A M$. \qed

Remark 4.1.4. The theory of Fourier transforms contains the following statements. Let $H$ be the (Schwartz) space of infinitely differentiable functions $f : \mathbb{R} \to \mathbb{C}$,
such that \( f \) and all derivatives rapidly decrease at infinity. \(( f \) decreases rapidly at infinity if \( |x|^m f(x) \) is bounded for all \( m \).\) This space is an algebra (without unit) under the multiplication of values. There is a second multiplication on \( H \), the convolution

\[
(f \ast g)(x) = (2\pi)^{-1/2} \int_{-\infty}^{+\infty} f(t)g(x-t)dt.
\]

The Fourier transform is a homomorphism \( \hat{\cdot} : H \to H \) defined by

\[
\hat{f}(x) = (2\pi)^{-1/2} \int_{-\infty}^{+\infty} f(t)e^{-itx} dt.
\]

It satisfies the identity \(( f \ast g) = \hat{f}\hat{g} \) hence it is an algebra homomorphism. We want to find an analogue of this theory for finite quantum groups.

A similar example is the following. Let \( G \) be a locally compact topological group. Let \( \mu \) be the (left) Haar measure on \( G \) and \( \int f := \int_G f(x) d\mu(x) \) be the Haar integral.

The Haar measure is left invariant in the sense that \( \mu(gE) = \mu(E) \) for all \( g \in G \) and all compact subsets \( E \) of \( G \). The Haar measure exists and is unique up to a positive factor. The Haar integral is translation invariant i.e. for all \( y \in G \) we have

\[
\int f(yx) d\mu(x) = \int f(x) d\mu(x).
\]

If \( \mu \) is a left-invariant Haar measure then there is a continuous homomorphism \( \text{mod} : G \to (\mathbb{R}^+, \cdot) \) such that \( \int f(xy^{-1}) d\mu(x) = \text{mod} (y) \int f(x) d\mu(x) \). The homomorphism \( \mu \) does not depend on \( f \) and is called the modulus of \( G \). The group \( G \) is called unimodular if the homomorphism \( \text{mod} \) is the identity.

If \( G \) is a compact, or discrete, or Abelian group, or a connected semisimple or nilpotent Lie group, then \( G \) is unimodular.

Let \( G \) be a quantum group (or a quantum monoid) with function algebra \( H \) an arbitrary Hopf algebra. We also use the algebra of linear functionals \( H^* = \text{Hom}(H, \mathbb{K}) \) (called the bialgebra of \( G \) in the French literature). The operation \( H^* \otimes H \ni a \otimes f \mapsto \langle a, f \rangle \in \mathbb{K} \) is nondegenerate on both sides. We denote the elements of \( H \) by \( f, g, h \in H \), the elements of \( H^* \) by \( a, b, c \in H^* \), the (non existing) elements of the quantum group \( G \) by \( x, y, z \in G \).

**Remark 4.1.5.** In 2.4.8 we have seen that the dual vector space \( H^* \) of a finite dimensional Hopf algebra \( H \) is again a Hopf algebra. The Hopf algebra structures are connected by the evaluation bilinear form

\[
\text{ev} : H^* \otimes H \ni a \otimes f \mapsto \langle a, f \rangle \in \mathbb{K}
\]

as follows:

\[
\langle a \otimes b, \sum_i f_i(1) \otimes f_i(2) \rangle = \langle ab, f \rangle, \quad \langle \sum a_{1(1)} \otimes a_{1(2)}, f \otimes g \rangle = \langle a, fg \rangle, \quad \langle a, 1 \rangle = \varepsilon(a), \quad \langle 1, f \rangle = \varepsilon(f), \quad \langle a, S(f) \rangle = \langle S(a), f \rangle.
\]

**Definition 4.1.6.** 1. The linear functionals \( a \in H^* \) are called generalized integrals on \( H \) ([Riesz-Nagy] S.123).
2. An element \( \int \in H^* \) is called a left (invariant) integral on \( H \) if
\[
a \int = \langle a, 1_H \rangle \int
\]
or \( a \int = \varepsilon_{H^*}(a) \int \) for all \( a \in H^* \).

3. An element \( \delta \in H \) is called a left integral in \( H \) if
\[
f \delta = \varepsilon(f) \delta
\]
for all \( f \in H \).

4. The set of left integrals in \( H \) is denoted by \( \text{Int}_l(H) \), the set of right integrals by \( \text{Int}_r(H) \). The set of left (right) integrals on \( H \) is \( \text{Int}_l(H^*) (\text{Int}_r(H^*)) \).

5. A Hopf algebra \( H \) is called unimodular if \( \text{Int}_l(H) = \text{Int}_r(H) \).

**Lemma 4.1.7.** The left integrals \( \text{Int}_l(H^*) \) form a two sided ideal of \( H^* \). If the antipode \( S \) is bijective then \( S \) induces an isomorphism \( S : \text{Int}_l(H^*) \rightarrow \text{Int}_r(H^*) \).

**Proof.** For \( \int \) in \( \text{Int}_l(H^*) \) we have \( a \int = \varepsilon(a) \int \in \text{Int}_l(H^*) \) and \( a \int b = \varepsilon(a) \int b \) hence \( \int b \in \text{Int}_l(H^*) \). If \( S \) is bijective then the induced map \( S : H^* \rightarrow H^* \) is also bijective and satisfies \( S(\int) b = S(\int) S(S^{-1}(b)) = S(S^{-1}(b) \int) = S(\int) \varepsilon(b) \) hence \( S(\int) \in \text{Int}_r(H^*) \).

**Remark 4.1.8.** Maschke’s Theorem has an extension to finite dimensional Hopf algebras: \( \varepsilon(\int) \neq 0 \) iff \( H^* \) is semisimple.

**Corollary 4.1.9.** Let \( H \) be a finite dimensional Hopf algebra. Then \( H^* \) is a left \( H^* \)-module by the usual multiplication, hence a right \( H \)-comodule. We have
\[
(H^*)^{coH} = \text{Int}_l(H^*).
\]

**Proof.** By definition we have \( \text{Int}_l(H^*) = H^* H^* \).

**Example 4.1.10.** Let \( G \) be a finite group. Let \( H := \text{Map}(G, \mathbb{K}) \) be the Hopf algebra defined by the following isomorphism
\[
\mathbb{K}^G = \text{Map}(G, \mathbb{K}) \cong \text{Hom}(\mathbb{K} G, \mathbb{K}) = (\mathbb{K} G)^*.
\]
This isomorphism between the vector space \( \mathbb{K}^G \) of all set maps from the group \( G \) to the base ring \( \mathbb{K} \) and the dual vector space \( (\mathbb{K} G)^* \) of the group algebra \( \mathbb{K} G \) defines the structure of a Hopf algebra on \( \mathbb{K}^G \).

We regard \( H := \mathbb{K}^G \) as the function algebra on the set \( G \). In the sense of algebraic geometry this is not quite true. The algebra \( \mathbb{K}^G \) represents a functor from \( \text{K-cAlg} \) to \( \text{Set} \) that has \( G \) as value for all connected algebras \( A \) in particular for all field extensions of \( \mathbb{K} \).

As before we use the map \( \text{ev} : \mathbb{K} G \otimes \mathbb{K}^G \rightarrow \mathbb{K} \). The multiplication of \( \mathbb{K}^G \) is given by pointwise multiplication of maps since \( \langle x, ff' \rangle = \left( \sum x_{(1)} \otimes x_{(2)}, f \otimes f' \right) = \langle x \otimes x, f \otimes f' \rangle = \langle x, f \rangle \langle x, f' \rangle \) for all \( f, f' \in \mathbb{K}^G \) and all \( x \in G \). The unit element \( 1_{\mathbb{K}^G} \) of \( \mathbb{K}^G \) is the map \( \varepsilon : \mathbb{K} G \rightarrow \mathbb{K} \) restricted to \( G \), hence \( \varepsilon(x) = 1 = \langle x, 1_{\mathbb{K}^G} \rangle \) for all \( x \in G \). The antipode of \( f \in \mathbb{K}^G \) is given by \( S(f)(x) = \langle x, S(f) \rangle = f(x^{-1}) \).
4. THE INFINITESIMAL THEORY

The elements of the dual basis \((x^* | x \in G)\) with \(\langle x, y^* \rangle = \delta_{x,y}\) considered as maps from \(G\) to \(\mathbb{K}\) form a basis of \(\mathbb{K}^G\). They satisfy the conditions

\[ x^* y^* = \delta_{x,y} x^* \quad \text{and} \quad \sum_{x \in G} x^* = 1_{\mathbb{K}^G} \]

since \(\langle z, x^* y^* \rangle = \langle z, x^* \rangle \langle z, y^* \rangle = \delta_{x,z} \delta_{x,y} = \delta_{x,y} \langle z, x^* \rangle \) and \(\langle z, \sum_{x \in G} x^* \rangle = 1 = \langle z, 1_{\mathbb{K}^G} \rangle\).

Hence the dual basis \((x^* | x \in G)\) is a decomposition of the unit into a set of minimal orthogonal idempotents and the algebra of \(\mathbb{K}^G\) has the structure

\[ \mathbb{K}^G = \bigoplus_{x \in G} \mathbb{K} x^* \cong \mathbb{K} \times \ldots \times \mathbb{K}. \]

In particular \(\mathbb{K}^G\) is commutative and semisimple.

The diagonal of \(\mathbb{K}^G\) is

\[ \Delta(x^*) = \sum_{y \in G} y^* \otimes (y^{-1} x)^* = \sum_{y,z \in G, y = x} y^* \otimes z^* \]

since

\[ \langle z \otimes u, \Delta(x^*) \rangle = \langle zu, x^* \rangle = \delta_{z,u} \delta_{z^{-1} u} = \sum_{y \in G} \delta_{y,z} \delta_{y^{-1} u} = \sum_{y \in G} \langle z, y^* \rangle \langle u, (y^{-1} x)^* \rangle = \langle z \otimes u, \sum_{y \in G} y^* \otimes (y^{-1} x)^* \rangle. \]

Let \(a \in \mathbb{K}G\). Then \(a\) defines a map \(\tilde{a} : G \to \mathbb{K} \in \mathbb{K}^G\) by \(a = \sum_{x \in G} \tilde{a}(x)x\). For arbitrary \(f \in \mathbb{K}^G\) and \(a \in \mathbb{K}G\) this gives

\[ \langle a, f \rangle = f(\sum_{x \in G} \tilde{a}(x)x) = \sum_{x \in G} \tilde{a}(x)f(x). \]

The counit of \(\mathbb{K}^G\) is given by \(\varepsilon(x^*) = \delta_{x,e}\) where \(e \in G\) is the unit element.

The antipode is, as above, \(S(x^*) = (x^{-1})^*\).

We consider \(H = \mathbb{K}^G\) as the function algebra on the finite group \(G\) and \(\mathbb{K}G\) as the dual space of \(H = \mathbb{K}^G\) hence as the set of distributions on \(H\).

Then

\[ (1) \quad \int := \sum_{x \in G} x \in H^* = \mathbb{K}G \]

is a (two sided) integral on \(H\) since \(\sum_{x \in G} yx = \sum_{x \in G} x = \varepsilon(y)\sum_{x \in G} x = \sum_{x \in G} yx\).

We write

\[ \int f(x)dx := \langle \int, f \rangle = \sum_{x \in G} f(x). \]

We have seen that there is a decomposition of the unit \(1 \in \mathbb{K}^G\) into a set of primitive orthogonal idempotents \(\{x^* | x \in G\}\) such that every element \(f \in \mathbb{K}^G\) has a unique representation \(f = \sum f(x)x^*\). Since \(\int y^* = \sum_{x \in G} \langle x, y^* \rangle\) we get \(\int f y^* = \sum_{x \in G} \langle x, f y^* \rangle = \sum_{x \in G} f(x)y^*(x) = f(y)\) hence

\[ f = \sum \left( \int f(x)y^*(x)dx \right)y^*. \]
Problem 4.1.1. Describe the group valued functor $\mathbb{K}\text{-cAlg}(\mathbb{K}^G, -)$ in terms of sets and their group structure.

Definition and Remark 4.1.11. Let $\mathbb{K}$ be an algebraically closed field and let $G$ be a finite abelian group (replacing $\mathbb{R}$ above). Assume that the characteristic of $\mathbb{K}$ does not divide the order of $G$. Let $H = \mathbb{K}^G$. We identify $\mathbb{K}^G = \text{Hom}(\mathbb{K}G, \mathbb{K})$ along the linear expansion of maps as in Example 2.1.10.

Let us consider the set $\hat{G} := \{ \chi : G \to \mathbb{K}^* | \chi \text{ group homomorphism} \}$. Since $\mathbb{K}^*$ is an abelian group, the set $\hat{G}$ is an abelian group by pointwise multiplication.

The group $\hat{G}$ is called the character group of $G$.

Obviously the character group is a multiplicative subset of $\mathbb{K}^G = \text{Hom}(\mathbb{K}G, \mathbb{K})$. Actually it is a subgroup of $\mathbb{K}\text{-cAlg}(\mathbb{K}G, \mathbb{K}) \subset \text{Hom}(\mathbb{K}G, \mathbb{K})$ since the elements $\chi \in \hat{G}$ expand to algebra homomorphisms: $\chi(ab) = \chi(\sum \alpha_x \sum \beta_y) = \sum \alpha_x \beta_y \chi(xy) = \chi(a)\chi(b)$ and $\chi(1) = \chi(e) = 1$. Conversely an algebra homomorphism $f \in \mathbb{K}\text{-cAlg}(\mathbb{K}G, \mathbb{K})$ restricts to a character $f : G \to \mathbb{K}^*$. Thus $\hat{G} = \mathbb{K}\text{-cAlg}(\mathbb{K}G, \mathbb{K})$, the set of rational points of the affine algebraic group represented by $\mathbb{K}G$.

There is a more general observation behind this remark.

Lemma 4.1.12. Let $H$ be a finite dimensional Hopf algebra. Then the set Gr($H^*$) of group like elements of $H^*$ is equal to $\mathbb{K}\text{-Alg}(H, \mathbb{K})$.

Proof. In fact $f : H \to \mathbb{K}$ is an algebra homomorphism iff $\langle f \otimes f, a \otimes b \rangle = \langle f, a \rangle \langle f, b \rangle = \langle f, ab \rangle = \langle \Delta(f), a \otimes b \rangle$ and $1 = \langle f, 1 \rangle = \varepsilon(f)$.

Hence there is a Hopf algebra homomorphism $\varphi : \hat{G} \to \mathbb{K}^G$ by 2.1.5.

Proposition 4.1.13. The Hopf algebra homomorphism $\varphi : \hat{G} \to \mathbb{K}^G$ is bijective.

Proof. We give the proof by several lemmas.


Proof. Assume there is a linearly dependent set $\{x_0, x_1, \ldots, x_n\}$ of group like elements in $H$. Choose such a set with $n$ minimal. Obviously $n \geq 1$ since all elements are non zero. Thus $x_0 = \sum_{i=1}^n \alpha_i x_i$ and $\{x_1, \ldots, x_n\}$ linearly independent. We get

$$\sum_{i,j} \alpha_i \alpha_j x_i \otimes x_j = x_0 \otimes x_0 = \Delta(x_0) = \sum_i \alpha_i x_i \otimes x_i.$$  

Since all $\alpha_i \neq 0$ and the $x_i \otimes x_j$ are linearly independent we get $n = 1$ and $\alpha_1 = 1$ so that $x_0 = x_1$, a contradiction.

Corollary 4.1.15. (Dedekind’s Lemma) Any set of characters in $\mathbb{K}^G$ is linearly independent.
Thus \( \varphi : \mathbb{K} \hat{G} \to \mathbb{K}^G \) is injective. Now we prove that the map \( \varphi : \mathbb{K} \hat{G} \to \mathbb{K}^G \) is surjective.

**Lemma 4.1.16.** *(Pontryagin duality)* The evaluation \( \hat{G} \times G \to \mathbb{K}^* \) is a non-degenerate bilinear map of abelian groups.

**Proof.** First we observe that \( \text{Hom}(C_n, \mathbb{K}^*) \cong C_n \) for a cyclic group of order \( n \) since \( \mathbb{K} \) has a primitive \( n \)-th root of unity (\( \text{char}(\mathbb{K}) \neq |G| \)). Since the direct product and the direct sum coincide in \( \text{Ab} \) we can use the fundamental theorem for finite abelian groups \( G \cong C_{n_1} \times \cdots \times C_{n_t} \) to get \( \text{Hom}(G, \mathbb{K}^*) \cong G \) for any abelian group \( G \) with \( \text{char}(\mathbb{K}) \neq |G| \). Thus \( \hat{G} \cong G \) and \( \hat{G} = G \). In particular \( \chi(x) = 1 \) for all \( x \in G \) iff \( \chi = 1 \). By the symmetry of the situation we get that the bilinear form \( \langle \cdot , \cdot \rangle : \hat{G} \times G \to \mathbb{K}^* \) is non-degenerate. \( \square \)

Thus \( |\hat{G}| = |G| \) hence \( \dim(\mathbb{K} \hat{G}) = \dim(\mathbb{K}^G) \). This proves Proposition 2.1.13. \( \square \)

**Definition 4.1.17.** Let \( H \) be a Hopf algebra. A \( \mathbb{K} \)-module \( M \) that is a right \( H \)-module by \( \rho : M \otimes H \to M \) and a right \( H \)-comodule by \( \delta : M \to M \otimes H \) is called a **Hopf module** if the diagram

\[
\begin{array}{ccc}
M \otimes H & \xrightarrow{\rho} & H \\
\delta \otimes \Delta & \downarrow & \delta \otimes \rho \\
M \otimes H \otimes H \otimes H & \overset{1 \otimes \tau \otimes 1}{\longrightarrow} & M \otimes H \otimes H \otimes H
\end{array}
\]

commutes, i.e. if \( \delta(mh) = \sum m(M)h_{(1)} \otimes m(1)h_{(2)} \) holds for all \( h \in H \) and all \( m \in M \).

Observe that \( H \) is an Hopf module over itself. Furthermore each module of the form \( V \otimes H \) is a Hopf module by the induced structure. More generally there is a functor \( \text{Vec} \ni V \mapsto V \otimes H \in \text{Hopf-Mod}-H. \)

**Proposition 4.1.18.** The two functors \( \cdot \otimes H : \text{Hopf-Mod}-H \to \text{Vec} \) and \( - \otimes H : \text{Vec} \ni V \mapsto V \otimes H \in \text{Hopf-Mod}-H \) are inverse equivalences of each other.

**Proof.** Define natural isomorphisms

\[ \alpha : M^{\co H} \otimes H \ni m \otimes h \mapsto mh \in M \]

with inverse map

\[ \alpha^{-1} : M \ni m \mapsto \sum m(M)S(m(1)) \otimes m(2) \in M^{\co H} \otimes H \]

and

\[ \beta : V \ni v \mapsto v \otimes 1 \in (V \otimes H)^{\co H} \]

with inverse map

\[ (V \otimes H)^{\co H} \ni v \otimes h \mapsto v \varepsilon(h) \in V. \]
1. INTEGRALS AND FOURIER TRANSFORMS

Obviously these homomorphisms are natural transformations in $M$ and $V$. Furthermore $\alpha$ is a homomorphism of $H$-modules. $\alpha^{-1}$ is well-defined since

$$
\delta(\sum m_{(M)}S(m(1))) = \sum m_{(M)}S(m(3)) \otimes m(1)S(m(2))
$$

(since $M$ is a Hopf module)

$$
= \sum m_{(M)}S(m(2)) \otimes \eta(m(1))
$$

$$
= \sum m_{(M)}S(m(1)) \otimes 1
$$

hence $\sum m_{(M)}S(m(1)) \in M^{\text{co}H}$. Furthermore $\alpha^{-1}$ is a homomorphism of comodules since

$$
\delta \alpha^{-1}(m) = \delta(\sum m_{(M)}S(m(1)) \otimes m(2)) = \sum m_{(M)}S(m(1)) \otimes m(2) \otimes m(3)
$$

$$
= \sum \alpha^{-1}(m_{(M)}) \otimes m(1) = (\alpha^{-1} \otimes 1)\delta(m).
$$

Finally $\alpha$ and $\alpha^{-1}$ are inverse to each other by

$$
\alpha \alpha^{-1}(m) = \alpha(\sum m_{(M)}S(m(1)) \otimes m(2)) = \sum m_{(M)}S(m(1))m(2) = m
$$

and

$$
\alpha^{-1}(m \otimes h) = \alpha^{-1}(mh) = \sum m_{(M)}h_{(1)}S(m(1)h(2)) \otimes m(2)h(3)
$$

$$
= \sum mh_{(1)}S(h(2)) \otimes h(3) \quad \text{(by $\delta(m) = m \otimes 1$)} = m \otimes h.
$$

Thus $\alpha$ and $\alpha^{-1}$ are mutually inverse homomorphisms of Hopf modules.

The image of $\beta$ is in $(V \otimes H)^{\text{co}H}$ by $\delta(v \otimes 1) = v \otimes \Delta(1) = (v \otimes 1) \otimes 1$. Both $\beta$ and $\beta^{-1}$ are $\mathbb{K}$-linear maps. Furthermore we have

$$
\beta^{-1}(v) = \beta^{-1}(v \otimes 1) = v \varepsilon(1) = v
$$

and

$$
\beta \beta^{-1}(\sum v_i \otimes h_i) = \beta(\sum v_i \varepsilon(h_i)) = \sum v_i \varepsilon(h_i) \otimes 1 = \sum v_i \otimes \varepsilon(h_i) 1
$$

$$
= \sum v_i \otimes \varepsilon(h_{i(1)})h_{i(2)} \quad \text{(since $\sum v_i \otimes h_i \in (V \otimes H)^{\text{co}H}$)} = \sum v_i \otimes h_i.
$$

Thus $\beta$ and $\beta^{-1}$ are mutually inverse homomorphisms. \hfill \square

Since $H^* = \text{Hom}(H, \mathbb{K})$ and $S : H \rightarrow H$ is an algebra antihomomorphism, the dual $H^*$ is an $H$-module in four different ways:

$$
\langle (f \rightarrow a), g \rangle := \langle a, gf \rangle, \quad \langle (a \leftarrow f), g \rangle := \langle a, fg \rangle,
$$

$$
\langle (f \rightarrow a), g \rangle := \langle a, S(f)g \rangle, \quad \langle (a \leftarrow f), g \rangle := \langle a, gS(f) \rangle.
$$

If $H$ is finite dimensional then $H^*$ is a Hopf algebra. The equality $\langle (f \rightarrow a), g \rangle = \langle a, gf \rangle = \sum \langle a_{(1)}, g \rangle \langle a_{(2)}, f \rangle$ implies

$$
(f \rightarrow a) = \sum a_{(1)} \langle a_{(2)}, f \rangle.
$$

Analogously we have

$$
(a \leftarrow f) = \sum \langle a_{(1)}, f \rangle a_{(2)}.
$$

**Proposition 4.1.19.** Let $H$ be a finite dimensional Hopf algebra. Then $H^*$ is a right Hopf module over $H$. 

PROOF. $H^*$ is a left $H^*$-module by left multiplication hence by 2.1.1 a right $H$-comodule by $\delta (a) = \sum_i b_i^* a \otimes b_i$. Let $f, g \in H$ and $a, b \in H^*$. The (left) multiplication of $H^*$ satisfies

$$ab = \sum b_{(H^*)}\langle a, b_{(1)} \rangle.$$ 

We use the right $H$-module structure

$$(a \triangleright f) = \sum a_{(1)} \langle S(f), a_{(2)} \rangle.$$ 

on $H^* = \text{Hom}(H, K)$.

Now we check the Hopf module property. Let $a, b \in H^*$ and $f, g \in H$. We apply $H^* \otimes H$ to its dual $H \otimes H^*$ and get

$$\delta(a \triangleright f)(g \otimes b) = \sum \langle (a \triangleright f)(H^*), g \rangle \langle b, (a \triangleright f)_{(1)} \rangle = \langle b(a \triangleright f), g \rangle$$

$$= \sum \langle b, g_{(1)} \rangle \langle (a \triangleright f), g_{(2)} \rangle = \sum \langle b, g_{(1)} \rangle \langle a, g_{(2)} S(f) \rangle$$

$$= \sum \langle (f_{(2)} \mapsto b)a, S(f_{(1)}) \rangle = \sum \langle (f_{(2)} \mapsto b) (a \triangleright f), g \rangle$$

$$= \sum \langle (a_{(H^*)}(f_{(2)} \mapsto b), a_{(1)}) \rangle \langle f_{(1)}, g \rangle = \sum \langle (a_{(H^*)} \triangleright f_{(1)})(f_{(2)} \mapsto b), a_{(1)} \rangle, g \rangle = \sum \langle (a_{(H^*)} \triangleright f_{(1)})(f_{(2)} \mapsto b), a_{(1)} f_{(2)} \rangle, g \rangle$$

hence $\delta(a \triangleright f) = \sum (a_{(H^*)} \triangleright f_{(1)}) \otimes a_{(1)} f_{(2)}$. 

\[\square\]

**Theorem 4.1.20.** Let $H$ be a finite dimensional Hopf algebra. Then the antipode $S$ is bijective, the space of left integrals $\text{Int}_l(H^*)$ has dimension 1, and the homomorphism

$$H \ni f \mapsto (f \mapsto f) = \sum \langle f_{(1)}, f_{(2)} \rangle \ni H^*$$

is bijective for any $0 \neq f \in \text{Int}_l(H^*)$.

**PROOF.** By Proposition 2.1.19 $H^*$ is a right Hopf module over $H$. By Proposition 2.1.18 there is an isomorphism $\alpha : (H^*)^{coH} \otimes H \ni a \otimes f \mapsto (a \mapsto f) = (S(f) \mapsto a) \in H^*$. Since $(H^*)^{coH} \cong \text{Int}_l(H^*)$ by 2.1.9 we get

$$\text{Int}_l(H^*) \otimes H \cong H^*$$

as right $H$-Hopf modules by the given map. This shows $\dim(\text{Int}_l(H^*)) = 1$. So we get an isomorphism $H \ni f \mapsto (f \mapsto f) \in H^*$ that is a composition of $S$ and $f \mapsto (f \mapsto f)$. Since $H$ is finite dimensional both of these maps are bijective. 

\[\square\]

If $G$ is a finite group then every generalized integral $a \in \mathbb{K}G$ can be written with a uniquely determined $g \in H = \mathbb{K}^G$ as

$$(5) \quad \langle a, f \rangle = \int f(x) S(g)(x)dx = \sum_{x \in G} f(x) g(x^{-1})$$

for all $f \in H$. 

If $G$ is a finite Abelian group then each group element (rational integral) $y \in G \subseteq \mathbb{K}G$ can be written as

$$y = \sum_{x \in G} \sum_{\chi \in G} \beta_{\chi}(x^{-1}, \chi) x$$

since

$$\langle y, f \rangle = \langle \left( \int G \beta_{\chi}(x^{-1}, \chi) f(x) dx \right), f \rangle = \langle \int G S(\sum_{\chi \in G} \beta_{\chi}(x^{-1}, \chi)) f(x) dx, f \rangle = \sum_{x \in G} \sum_{\chi \in G} \beta_{\chi}(x, S(\chi)) \langle x^{-1}, x, f \rangle = \sum_{x \in G} \sum_{\chi \in G} \beta_{\chi}(x^{-1}, \chi) x, f \rangle.$$ 

In particular the matrix $(\langle x^{-1}, \chi \rangle)$ is invertible.

Let $H$ be finite dimensional. Since $\langle f, f \rangle = \langle \left( \int f \right), f \rangle$ as a functional on $g$ is a generalized integral, there is a unique $\nu(f) \in H$ such that

$$\langle f, f \rangle = \langle f, \nu(f) \rangle$$

or

$$\int f(x) g(x) dx = \int g(x) \nu(f)(x) dx.$$

Although the functions $f, g \in H$ of the quantum group do not commute under multiplication, there is a simple commutation rule if the product is integrated.

**Proposition and Definition 4.1.21.** The map $\nu : H \rightarrow H$ is an algebra automorphism, called the Nakayama automorphism.

**Proof.** It is clear that $\nu$ is a linear map. We have $\int f \nu(gh) = \int gh f = \int h f \nu(g) = \int f \nu(g) \nu(h)$ hence $\nu(gh) = \nu(g) \nu(h)$ and $\int f \nu(1) = \int f$ hence $\nu(1) = 1$. Furthermore if $\nu(g) = 0$ then $0 = \langle f, \nu(g) \rangle = \langle f, g f \rangle = \langle (f \rightarrow f), f g \rangle$ for all $f \in H$ hence $\langle a, g \rangle = 0$ for all $a \in H^*$ hence $g = 0$. So $\nu$ is injective hence bijective. \qed

**Corollary 4.1.22.** The map $H \ni f \mapsto (\int \rightarrow f) \in H^*$ is an isomorphism.

**Proof.** We have

$$\langle (\int \rightarrow f), g \rangle = \langle \int, f g \rangle = \langle \int, \nu(f) \rangle = \langle (\nu(f) \rightarrow f), g \rangle.$$ This implies the corollary. \qed

If $G$ is a finite group and $H = \mathbb{K}G$ then $H$ is commutative hence $\nu = \text{id}$.

**Definition 4.1.23.** An element $\delta \in H$ is called a Dirac $\delta$-function if $\delta$ is a left invariant integral in $H$ with $\langle f, \delta \rangle = 1$, i.e. if $\delta$ satisfies

$$f \delta = \varepsilon(f) \delta \quad \text{and} \quad \int \delta(x) dx = 1$$

for all $f \in H$. If $H$ has a Dirac $\delta$-function then we write

$$\langle f \rangle := \int \delta(x) dx = \int a := \langle a, \delta \rangle.$$ 

**Proposition 4.1.24.**
1. If $H$ is finite dimensional then there exists a unique Dirac $\delta$-function $\delta$.
2. If $H$ is infinite dimensional then there exists no Dirac $\delta$-function.

PROOF. 1. Since $H \ni f \mapsto (f \mapsto f) \in H^*$ is an isomorphism there is a $\delta \in H$ such that $(\delta \mapsto f) = \varepsilon$. Then $(f \delta \mapsto f) = (f \mapsto (\delta \mapsto f)) = (f \mapsto \varepsilon) = \varepsilon(f)\varepsilon = \varepsilon(f)(\delta \mapsto f)$ which implies $f\delta = \varepsilon(f)\delta$. Furthermore we have $(f, \delta) = \langle f, 1_H \delta \rangle = \langle (\delta \mapsto f), 1_H \rangle = \varepsilon(1_H) = 1_K$.

2. is [Sweedler] exercise V.4. □

**Lemma 4.1.25.** Let $H$ be a finite dimensional Hopf algebra. Then $f \in H^*$ is a left integral iff

\[(\sum a f(1) \otimes S(f(2))) = (\sum a f(1) \otimes S(f(2))) a \]

iff

\[\sum S(a) f(1) \otimes f(2) = \sum f(1) \otimes a f(2) \]

iff

\[\sum f(1) \langle f, f(2) \rangle = \langle f, f \rangle 1_H. \]

PROOF. Let $f$ be a left integral. Then

\[\sum a f(1) \otimes S(f(2)) S(a(2)) = \sum a f(1) \otimes S(a f(2)) = \varepsilon(a) (\sum f(1) \otimes S(f(2))) \]

for all $a \in H$. Hence

\[\sum f(1) \otimes S(f(2)) a = \sum \varepsilon(a(1)) (f(1) \otimes S(f(2))) a(2) = \sum a(1) f(1) \otimes S(f(2)) S(a(2)) a(3) = \sum a(1) f(1) \otimes S(f(2)) \varepsilon(a(2)) = a(\sum f(1) \otimes S(f(2))). \]

Conversely $a(\sum f(1) \varepsilon(S(f(2)))) = (\sum f(1) \varepsilon(S(f(2))) a) = \varepsilon(a)(\sum f(1) \varepsilon(S(f(2))))$, hence $f = \sum f(1) \varepsilon(S(f(2)))$ is a left integral.

Since $S$ is bijective the following holds

\[\sum S(a) f(1) \otimes f(2) = \sum S(a) f(1) \otimes S^{-1}(S(f(2))) = \sum f(1) \otimes S^{-1}(S(f(2)) S(a)) = \sum f(1) \otimes a f(2). \]

The converse follows easily.

If $f \in \text{Int}_1(H)$ is a left integral then $\sum \langle a, f(1) \rangle \langle f, f(2) \rangle = \langle a f, f \rangle = \langle a, 1_H \rangle \langle f, f \rangle$.

Conversely if $\lambda \in H^*$ with (11) is given then $\langle a \lambda, f \rangle = \sum \langle a, f(1) \rangle \langle \lambda, f(2) \rangle = \langle a, 1_H \rangle \langle \lambda, f \rangle$ hence $a \lambda = \varepsilon(a) \lambda$. □

If $G$ is a finite group then

\[\delta(x) = \begin{cases} 0 & \text{if } x \neq e; \\ 1 & \text{if } x = e. \end{cases} \]
In fact since $\delta$ is left invariant we get $f(x)\delta(x) = f(\epsilon)\delta(x)$ for all $x \in G$ and $f \in \mathbb{K}^G$. Since $G \subset H^* = \mathbb{K}G$ is a basis, we get $\delta(x) = 0$ if $x \neq \epsilon$. Furthermore $\int \delta(x) dx = \sum_{x \in G} \delta(x) = 1$ implies $\delta(\epsilon) = 1$. So we have $\delta = \epsilon^*$. 

If $G$ is a finite Abelian group we get $\delta = \alpha \sum_{\chi \in G} \chi$ for some $\alpha \in \mathbb{K}$. The evaluation gives $1 = \langle f, \delta \rangle = \alpha \sum_{\chi \in G} \chi \langle \chi, x \rangle$. Now let $\lambda \in \hat{G}$. Then $\sum_{\chi \in G} \chi \langle \chi, x \rangle = \langle \lambda, x \rangle \sum_{\chi \in G} \chi$. Since for each $x \in G \setminus \{\epsilon\}$ there is a $\lambda$ such that $\langle \lambda, x \rangle \neq 1$ and we get

$$\sum_{\chi \in G} \chi = |G| \delta_{\epsilon, x}.$$ 

Hence $\sum_{\chi \in G, \chi \in G} \chi \langle \chi, x \rangle = |G| = \alpha^{-1}$ and

$$\delta = |G|^{-1} \sum_{\chi \in G} \chi. \tag{13}$$

Let $H$ be finite dimensional for the rest of this section. In Corollary 1.22 we have seen that the map $H \ni f \mapsto (\int \leftarrow f) \in H^*$ is an isomorphism. This map will be called the Fourier transform.

**Theorem 4.1.26.** The Fourier transform $H \ni f \mapsto \tilde{f} \in H^*$ is bijective with

$$\tilde{f} = (\int \leftarrow f) = \sum \langle f^{(1)}; \tilde{f} \rangle f^{(2)} \tag{14}$$

The inverse Fourier transform is defined by

$$\tilde{a} = \sum S^{-1}(\delta^{(1)}) \langle a, \delta^{(2)} \rangle. \tag{15}$$

Since these maps are inverses of each other the following formulas hold

$$\langle \tilde{f}, g \rangle = \int f(x)g(x) dx \quad \langle a, \tilde{b} \rangle = \int S^{-1}(a)(x)b(x) dx$$

$$f = \sum S^{-1}(\delta^{(1)}) \langle \tilde{f}, \delta^{(2)} \rangle \quad a = \sum \langle f^{(1)}; \tilde{a} \rangle f^{(2)}. \tag{16}$$

**Proof.** We use the isomorphisms $H \rightarrow H^*$ defined by $\tilde{f} := \tilde{f} = (\int \leftarrow f) = \sum \langle f^{(1)}; f \rangle f^{(2)}$ and $H^* \rightarrow H$ defined by $\tilde{a} := (a \leftarrow \delta) = \sum \delta^{(1)}(a, \delta^{(2)})$. Because of

$$\langle a, \tilde{b} \rangle = \langle a, (b \leftarrow \delta) \rangle = \langle ab, \delta \rangle \tag{17}$$

and

$$\langle \tilde{f}, g \rangle = \langle (\int \leftarrow f), g \rangle = \langle \tilde{f}, fg \rangle \tag{18}$$

we get for all $a \in H^*$ and $f \in H$

$$\langle a, \tilde{f} \rangle = \langle a \tilde{f}, \delta \rangle = \sum \langle a, \delta^{(1)} \rangle \langle \tilde{f}, \delta^{(2)} \rangle = \sum \langle a, \delta^{(1)} \rangle \langle f, f \delta^{(2)} \rangle \quad (\text{by Lemma 1.25})$$

$$= \sum \langle a, S(f) \delta^{(1)} \rangle \langle f, \delta^{(2)} \rangle = \langle a, S(f) \rangle \langle \tilde{f}, \delta \rangle = \langle a, S(f) \rangle. \tag{19}$$
This gives \( \hat{f} = S(f) \). So the inverse map of \( H \rightarrow H^* \) with \( \hat{f} = (f \leftarrow f) = \hat{f} \) is \( H^* \rightarrow H \) with \( S^{-1}(\hat{a}) = \sum S^{-1}(\delta(1)) \langle a, \delta(2) \rangle = \hat{a} \). Then the given inversion formulas are clear.

We note for later use \( \langle a, \hat{b} \rangle = \langle a, S^{-1}(\hat{b}) \rangle = \langle S^{-1}(a), \hat{b} \rangle = \langle S^{-1}(a)b, \delta \rangle \).

If \( G \) is a finite group and \( H = \mathbb{K}^G \) then
\[
\hat{f} = \sum_{x \in G} f(x)x.
\]
Since \( \Delta(\delta) = \sum_{x \in G} x^{-1} \otimes x^* \) where the \( x^* \in \mathbb{K}^G \) are the dual basis to the \( x \in G \), we get
\[
\tilde{a} = \sum_{x \in G} \langle a, x^* \rangle x^*.
\]

If \( G \) is a finite Abelian group then the groups \( G \) and \( \hat{G} \) are isomorphic so the Fourier transform induces a linear automorphism \( \tilde{\cdot} : \mathbb{K}^G \rightarrow \mathbb{K}^G \) and we have
\[
\tilde{a} = |G|^{-1} \sum_{\chi \in \hat{G}} \langle a, \chi \rangle \chi^{-1}
\]
By substituting the formulas for the integral and the Dirac \( \delta \)-function (1) and (13) we get
\[
\hat{f} = \sum_{x \in G} f(x)x, \quad \hat{a} = |G|^{-1} \sum_{\chi \in \hat{G}} a(\chi) \chi^{-1}, \quad f = |G|^{-1} \sum_{\chi \in \hat{G}} \hat{f}(\chi) \chi^{-1}, \quad a = \sum_{x \in G} \hat{a}(x)x.
\]
This implies
\[
\hat{f}(\chi) = \sum_{x \in G} f(x)\chi(x) = \int f(x)\chi(x)dx
\]
with inverse transform
\[
\tilde{a}(x) = |G|^{-1} \sum_{\chi \in \hat{G}} \chi(a)\chi^{-1}(x).
\]

**Corollary 4.1.27.** The Fourier transforms of the left invariant integrals in \( H \) and \( H^* \) are
\[
\tilde{\delta} = \varepsilon \nu^{-1} \in H^* \quad \text{and} \quad \hat{f} = 1 \in H.
\]

**PROOF.** We have \( \langle \tilde{\delta}, f \rangle = \langle f, \delta f \rangle = \langle f, \nu^{-1}(f) \delta \rangle = \varepsilon \nu^{-1}(f) \langle f, \delta \rangle = \varepsilon \nu^{-1}(f) \rangle = \varepsilon \nu^{-1}(f) \) hence \( \tilde{\delta} = \varepsilon \nu^{-1} \). From \( \hat{1} = (f \leftarrow 1) = f \) we get \( \hat{f} = 1 \). \( \Box \)

**Proposition 4.1.28.** Define a convolution multiplication on \( H^* \) by
\[
\langle a * b, f \rangle := \sum \langle a, S^{-1}(\delta(1)) f \rangle \langle b, \delta(2) \rangle.
\]
Then the following transformation rule holds for \( f, g \in H \):
\[
\widehat{fg} = \widehat{f} \ast \widehat{g}.
\]

In particular \( H^* \) with the convolution multiplication is an associative algebra with unit \( \widehat{1_H} = \widehat{f} \), i.e.
\[
\widehat{f} \ast a = a \ast \widehat{f} = a.
\]

**Proof.** Given \( f, g, h \in H^* \). Then
\[
\langle \widehat{fg}, h \rangle = \langle \widehat{f}, fgh \rangle = \langle \widehat{f}, fS^{-1}(1_H)gh \rangle \langle \widehat{f}, \delta \rangle = \sum \langle \widehat{f}, fS^{-1}(\delta_{(1)})gh \rangle \langle \widehat{f}, \delta_{(2)} \rangle = \sum \langle \widehat{f}, S^{-1}(\delta_{(1)})h \rangle \langle \widehat{f}, g\delta_{(2)} \rangle = \langle \widehat{f} \ast \widehat{g}, h \rangle.
\]

From (22) we get \( \widehat{1_H} = \widehat{f} \). So we have \( \widehat{f} = \widehat{1_f} = \widehat{1} \ast \widehat{f} = \widehat{f} \ast \widehat{f} \). \( \square \)

If \( G \) is a finite Abelian group and \( a, b \in H^* = \mathbb{K}^\hat{G} \). Then
\[
(a \ast b)(\mu) = |G|^{-1} \sum_{\chi, \lambda \in \hat{G}, \chi \lambda = \mu} a(\lambda) b(\chi).
\]

In fact we have
\[
(a \ast b)(\mu) = \langle a \ast b, \mu \rangle = \sum \langle a, S^{-1}(\delta_{(1)}) \mu \rangle \langle b, \delta_{(2)} \rangle = |G|^{-1} \sum_{\chi, \lambda \in \hat{G}, \chi \lambda = \mu} a(\lambda) b(\chi).
\]

One of the most important formulas for Fourier transforms is the Plancherel formula on the invariance of the inner product under Fourier transforms. We have

**Theorem 4.1.29.** *(The Plancherel formula)*

\[ (a, f) = \langle \widehat{f}, \nu(\widehat{a}) \rangle. \]

**Proof.** First we have from (16)
\[
\langle a, f \rangle = \sum \langle f_{(1)}, \widehat{a} \rangle \langle f_{(2)}, S^{-1}(\delta_{(1)}) \rangle \langle \widehat{f}, \delta_{(2)} \rangle = \sum \langle \widehat{f}, aS^{-1}(\delta_{(1)}) \rangle \langle \widehat{f}, \delta_{(2)} \rangle = \sum \langle f, S^{-1}(\delta_{(1)}) \nu(\widehat{a}) \rangle \langle \widehat{f}, \delta_{(2)} \rangle = \sum \langle f, S^{-1}(\delta_{(1)}) \rangle \langle \widehat{f}, \nu(\widehat{a}) \delta_{(2)} \rangle = \sum \langle f, S^{-1}(\delta_{(2)}) \rangle \langle \widehat{f}, \nu(\widehat{a}) \rangle S(\delta_{(2)}) = \langle \widehat{f}, S^{-1}(\delta) \rangle \langle \widehat{f}, \nu(\widehat{a}) \rangle \langle S^{-1}(\delta), \delta_{(2)} \rangle.
\]

Apply this to \( \langle f, \delta \rangle \). Then we get
\[
1 = \langle f, \delta \rangle = \langle f, S^{-1}(\delta) \rangle \langle \delta, \nu(\widehat{f}) \rangle = \langle f, S^{-1}(\delta) \rangle \nu(1) \langle \widehat{f}, S^{-1}(\delta) \rangle = \langle \widehat{f}, S^{-1}(\delta) \rangle \nu(1) = \langle \widehat{f}, S^{-1}(\delta) \rangle.
\]

Hence we get \( \langle a, f \rangle = \langle \widehat{f}, \nu(\widehat{a}) \rangle \). \( \square \)

**Corollary 4.1.30.** If \( H \) is unimodular then \( \nu = S^2 \).
4. THE INFINITESIMAL THEORY

PROOF. $H$ unimodular means that $\delta$ is left and right invariant. Thus we get

$$\langle a, f \rangle = \int \tilde{a}(x) f(x) dx = \int S^{-1}(a(x)) \tilde{f}(x) dx.$$

Hence $S^2 = \nu$.  

We also get a special representation of the inner product $H^* \otimes H \rightarrow \mathbb{K}$ by both integrals:

**Corollary 4.1.31.**

(26)

$$\langle a, f \rangle = \int \tilde{a}(x) f(x) dx = \int S^{-1}(a(x)) \tilde{f}(x) dx.$$

**Proof.** We have the rules for the Fourier transform. From (18) we get $\langle a, f \rangle = \int \tilde{a} f dx = \int a(x) f(x) dx$ and from (17) $\langle a, f \rangle = \langle S^{-1}(a) \tilde{f}, \delta \rangle = \int S^{-1}(a(x)) \tilde{f}(x) dx$.

The Fourier transform leads to an interesting integral transform on $H$ by double application.

**Proposition 4.1.32.** The double transform $\hat{f} := (\delta \mapsto (\tilde{f} \leftarrow f))$ defines an automorphism $H \rightarrow H$ with

$$\hat{f}(y) = \int f(x) \delta(xy) dx.$$

**Proof.** We have

$$\langle y, \hat{f} \rangle = \langle y, (\delta \mapsto (\tilde{f} \leftarrow f)) \rangle = \langle (\tilde{f} \leftarrow f) y, \delta \rangle$$

$$= \sum \langle (\tilde{f} \leftarrow f), \delta(1) \rangle \langle y, \delta(2) \rangle = \sum \langle (\tilde{f} \leftarrow f), \delta(1) \rangle \langle y, \delta(2) \rangle$$

$$= \sum \langle (\tilde{f}(1), f) \langle \tilde{f}(2), \delta(1) \rangle \langle y, \delta(2) \rangle = \sum \langle f(1), f \rangle \langle f(2), y, \delta \rangle$$

$$= \sum \langle f(1), f \rangle \langle f(2), y \leftarrow \delta \rangle = \langle f, f(y \leftarrow \delta) \rangle$$

since $\langle x, (y \leftarrow \delta) \rangle = \langle xy, \delta \rangle$.  

2. Derivations

**Definition 4.2.1.** Let $A$ be a $\mathbb{K}$-algebra and $A M_A$ be an $A$-$A$-bimodule (with identical $\mathbb{K}$-action on both sides). A linear map $D : A \to M$ is called a *derivation* if

$$D(ab) = aD(b) + D(a)b.$$ 

The set of derivations $\text{Der}_\mathbb{K}(A, A M_A)$ is a $\mathbb{K}$-module and a functor in $A M_A$.

By induction one sees that $D$ satisfies

$$D(a_1 \ldots a_n) = \sum_{i=1}^{n} a_1 \ldots a_{i-1} D(a_i) a_{i+1} \ldots a_n.$$ 

Let $A$ be a commutative $\mathbb{K}$-algebra and $A M$ be an $A$-module. Consider $M$ as an $A$-$A$-bimodule by $ma := am$. We denote the set of derivations from $A$ to $M$ by $\text{Der}_\mathbb{K}(A, M)$.\[\text{c.}]

**Proposition 4.2.2.** 1. Let $A$ be a $\mathbb{K}$-algebra. Then the functor $\text{Der}_\mathbb{K}(A, -) : A\text{-Mod}-A \to \text{Vec}$ is representable by the module of differentials $\Omega_A$.

2. Let $A$ be a commutative $\mathbb{K}$-algebra. Then the functor $\text{Der}_\mathbb{K}(A, -) : A\text{-Mod} \to \text{Vec}$ is representable by the module of commutative differentials $\Omega^c_A$.

**Proof.** 1. Represent $A$ as a quotient of a free $\mathbb{K}$-algebra $A := \mathbb{K}\langle X_i | i \in J \rangle / I$ where $B = \mathbb{K}\langle X_i | i \in J \rangle$ is the free algebra with generators $X_i$. We first prove the theorem for free algebras.

a) A representing module for $\text{Der}_\mathbb{K}(B, -)$ is $(\Omega_B, d : B \to \Omega_B)$ with $\Omega_B := B \otimes F(dX_i | i \in J) \otimes B$ where $F(dX_i | i \in J)$ is the free $\mathbb{K}$-module on the set of formal symbols \{dX_i | i \in J\} as a basis.

We have to show that for every derivation $D : B \to M$ there exists a unique homomorphisms $\varphi : \Omega_B \to M$ of $B$-$B$-bimodules such that the diagram

$$\begin{array}{ccc}
B & \xrightarrow{d} & \Omega_B \\
\downarrow{D} & & \downarrow{\varphi} \\
M & & \\
\end{array}$$

commutes. The module $\Omega_B$ is a $B$-$B$-bimodule in the canonical way. The products $X_1 \ldots X_n$ of the generators $X_i$ of $B$ form a basis for $B$. For any product $X_1 \ldots X_n$ we define $d(X_1 \ldots X_n) := \sum_{i=1}^{n} X_1 \ldots X_{i-1} \otimes dX_i \otimes X_{i+1} \ldots X_n$ in particular $d(X_i) = 1 \otimes dX_i \otimes 1$. To see that $d$ is a derivation it suffices to show this on the basis elements:

$$d(X_1 \ldots X_k X_{k+1} \ldots X_n)$$

$$= \sum_{j=1}^{k} X_1 \ldots X_{j-1} \otimes dX_j \otimes X_{j+1} \ldots X_k X_{k+1} \ldots X_n$$

$$+ \sum_{j=k+1}^{n} X_1 \ldots X_k X_{k+1} \ldots X_{j-1} \otimes dX_j \otimes X_{j+1} \ldots X_n$$

$$= d(X_1 \ldots X_k) X_{k+1} \ldots X_n + X_1 \ldots X_k d(X_{k+1} \ldots X_n)$$
Now let $D : B \to M$ be a derivation. Define $\varphi$ by $\varphi(1 \otimes dX_i \otimes 1) := D(X_i)$. This map obviously extends to a homomorphism of $B$-$B$-bimodules. Furthermore we have

$$
\varphi d(X_1 \ldots X_n) = \varphi(\sum_j X_1 \ldots X_{j-1} \otimes dX_j \otimes X_{j+1} \ldots X_n) = \sum_j X_1 \ldots X_{j-1} \varphi(1 \otimes dX_j \otimes 1) X_{j+1} \ldots X_n = D(X_1 \ldots X_n)
$$

hence $\varphi d = D$.

To show the uniqueness of $\varphi$ let $\psi : \Omega_B \to M$ be a bimodule homomorphism such that $\psi d = D$. Then $\psi(1 \otimes dX_i \otimes 1) = \psi d(X_i) = D(X_i) = \varphi(1 \otimes dX_i \otimes 1)$. Since $\psi$ and $\varphi$ are $B$-$B$-bimodules homomorphisms this extends to $\psi = \varphi$.

b) Now let $A := \mathbb{K}(X_i | i \in J)/I$ be an arbitrary algebra with $B = \mathbb{K}(X_i | i \in J)$ free. Define

$$
\Omega_A := \Omega_B/(I \Omega_B + \Omega_B I + Bd_B(I) + d_B(I)B).
$$

We first show that $I \Omega_B + \Omega_B I + Bd_B(I) + d_B(I)B$ is a $B$-$B$-subbimodule. Since $\Omega_B$ and $I$ are $B$-$B$-bimodules the terms $I \Omega_B$ and $\Omega_B I$ are bimodules. Furthermore we have $bd_B(i)b = bd_B(bi) - bd_B(b') \in Bd_B(I) + I \Omega_B$ hence $I \Omega_B + \Omega_B I + Bd_B(I) + d_B(I)B$ is a subbimodule.

Now $\Omega_B$ and $\Omega_B I$ are subbimodules of $I \Omega_B + \Omega_B I + Bd_B(I) + d_B(I)B$. Hence $A = B/I$ acts on both sides on $\Omega_A$ so that $\Omega_A$ becomes an $A$-$A$-bimodule.

Let $\nu : \Omega_B \to \Omega_A$ and also $\nu : B \to A$ be the residue homomorphisms. Since $\nu d_B(i) \in \nu d_B(I) = 0 \subseteq \Omega_A$ we get a unique factorization map $d_A : A \to \Omega_A$ such that

$$
\begin{array}{ccc}
B & \xrightarrow{d_B} & \Omega_B \\
\downarrow \nu & & \downarrow \nu \\
A & \xrightarrow{d_A} & \Omega_A \\
\end{array}
$$

commutes. Since $d_A(\bar{b}) = \overline{d_B(b)}$ it is clear that $d_A$ is a derivation.

Let $D : A \to M$ be a derivation. The $A$-$A$-bimodule $M$ is also a $B$-$B$-bimodule by $bm = \overline{b}m$. Furthermore $D\nu : B \to A \to M$ is again a derivation. Let $\varphi_B : \Omega_B \to M$ be the unique factorization map for the $B$-derivation $D\nu$. Consider the following diagram

$$
\begin{array}{ccc}
B & \xrightarrow{d_B} & \Omega_B \\
\downarrow \nu & & \downarrow \nu \\
A & \xrightarrow{d_A} & \Omega_A \\
\downarrow D & & \downarrow \varphi \\
M & & \\
\end{array}
$$

We want to construct $\psi$ such that the diagram commutes. Let $i\omega \in I \Omega_B$. Then $\varphi(i\omega) = \overline{\varphi(\omega)} = 0$ and similarly $\varphi(\omega i) = 0$. Let $bd_B(i) \in Bd_B(I)$ then $\varphi(bd_B(i)) = \overline{\varphi(d_B(i))} = \overline{\varphi(d_B(i))} = 0$ and similarly $\varphi(d_B(i)b) = 0$. Hence $\varphi$ vanishes on $I \Omega_B + \Omega_B I +$
2. DERIVATIONS

$Bd_B(I) + d_B(I)B$ and thus factorizes through a unique map $\psi : \Omega_A \to M$. Obviously $\psi$ is a homomorphism of $A$-$A$-bimodules. Furthermore we have $D\nu = \varphi d_B = \psi d_B = \psi d_{A\nu}$ and, since $\nu$ is surjective, $D = \psi d_A$. It is clear that $\psi$ is uniquely determined by this condition.

2. If $A$ is commutative then we can write $A = \mathbb{K}[X_i | i \in J]/I$ and $\Omega_B = B \otimes F(dX_i)$. With $\Omega_A = \Omega_B/(I^\circ B + Bd_B(I))$ the proof is analogous to the proof in the noncommutative situation. \qed

**Remark 4.2.3.** 1. $\Omega_A$ is generated by $d(A)$ as a bimodule, hence all elements are of the form $\sum_i a_i d(a'_i a''_i)$. These elements are called **differentials**.

2. If $A = \mathbb{K}(X_i)/I$, then $\Omega_A$ is generated as a bimodule by the elements $\{d(X_i)\}$.

3. Let $f \in B = \mathbb{K}(X_i)$. Let $B^{op}$ be the algebra opposite to $B$ (with opposite multiplication). Then $\Omega_B = B \otimes F(dX_i) \otimes B$ is the free $B \otimes B^{op}$ left module over the free generating set $\{d(X_i)\}$. Hence $d(f)$ has a unique representation

$$d(f) = \sum_i \frac{\partial f}{\partial x_i} d(x_i)$$

with uniquely defined coefficients

$$\frac{\partial f}{\partial x_i} \in B \otimes B^{op}.$$

In the commutative situation we have unique coefficients

$$\frac{\partial f}{\partial x_i} \in \mathbb{K}[X_i].$$

4. We give the following examples for part 3:

$$\frac{\partial x_i}{\partial x_j} = \delta_{ij},$$

$$\frac{\partial x_1 x_2}{\partial x_1} = 1 \otimes x_2,$$

$$\frac{\partial x_1 x_2}{\partial x_2} = x_1 \otimes 1,$$

$$\frac{\partial x_1 x_2 x_3}{\partial x_2} = x_1 \otimes x_3,$$

$$\frac{\partial x_1 x_3 x_2}{\partial x_2} = x_1 x_3 \otimes 1.$$

This is obtained by direct calculation or by the **product rule**

$$\frac{\partial f g}{\partial x_i} = (1 \otimes g) \frac{\partial f}{\partial x_i} + (f \otimes 1) \frac{\partial g}{\partial x_i}.$$
The product rule follows from
\[ d(fg) = d(f)g + fd(g) = \sum ((1 \otimes g) \frac{\partial f}{\partial X_i} + (f \otimes 1) \frac{\partial g}{\partial X_i}) d(X_i). \]

Let \( A = \mathbb{K}(X_i)/I \). If \( f \in I \) then \( \overline{d(f)} = d_A(\overline{f}) = 0 \) hence
\[ \sum \frac{\partial f}{\partial X_i} d_A(\overline{X_i}) = 0. \]

These are the defining relations for the \( A \)-\( A \)-bimodule \( \Omega_A \) with the generators \( d_A(\overline{X_i}) \).

For motivation of the quantum group case we consider an affine algebraic group \( G \) with representing commutative Hopf algebra \( A \). Recall that \( \text{Hom}(A, R) \) is an algebra with the convolution multiplication for every \( R \in \mathbb{K} \text{-cAlg} \) and that \( G(R) = \mathbb{K} \text{-cAlg}(A, R) \subseteq \text{Hom}(A, R) \) is a subgroup of the group of units of the algebra \( \text{Hom}(A, R) \).

**Definition and Remark 4.2.4.** A linear map \( T : A \to A \) is called left translation invariant, if the following diagram functorial in \( R \in \mathbb{K} \text{-cAlg} \) commutes:

\[
\begin{array}{c}
G(R) \times \text{Hom}(A, R) \xrightarrow{\ast} \text{Hom}(A, R) \\
1 \otimes \text{Hom}(T, R) \downarrow \quad \downarrow \text{Hom}(T, R) \\
G(R) \times \text{Hom}(A, R) \xrightarrow{\ast} \text{Hom}(A, R)
\end{array}
\]

i. e. if we have
\[
\forall g \in G(R), \forall x \in \text{Hom}(A, R) : g \ast (x \circ T) = (g \ast x) \circ T.
\]

This condition is equivalent to
\[
(27)\quad \Delta_A \circ T = (1_A \otimes T) \circ \Delta_A.
\]

In fact if (27) holds then \( g \ast (x \circ T) = \nabla_R(g \otimes x)(1_A \otimes T) \Delta_A = \nabla_R(g \otimes x) \Delta_A T = (g \ast x) \circ T. \)

Conversely if the diagram commutes, then take \( R = A, g = 1_A \) and we get
\[
\nabla_A(1_A \otimes x)(1_A \otimes T) \Delta_A = 1_A \ast (x \circ T) = (1_A \ast x) \circ T = \nabla_A(1_A \otimes x) \Delta_A T
\]
for all \( x \in \text{Hom}(A, A) \). To get (27) it suffices to show that the terms \( \nabla_A(1_A \otimes x) \) can be cancelled in this equation. Let \( \sum_{i=1}^n a_i \otimes b_i \in A \otimes A \) be given such that \( \nabla_A(1_A \otimes x)(\sum a_i \otimes b_i) = 0 \) for all \( x \in \text{Hom}(A, A) \) and choose such an element with a shortest representation (\( n \) minimal). Then \( \sum a_i x(b_i) = 0 \) for all \( x \). Since the \( b_i \) are linearly independent in such a shortest representation, there are \( x_i \) with \( x_i(b_i) = \delta_{ij} \). Hence \( a_j = \sum a_i x_j(b_i) = 0 \) and thus \( \sum a_i \otimes b_i = 0 \). From this follows (27).

**Definition 4.2.5.** Let \( H \) be an arbitrary Hopf algebra. An element \( T \in \text{Hom}(H, H) \) is called left translation invariant if it satisfies
\[
\Delta_H T = (1_H \otimes T) \Delta_H.
\]
2. DERIVATIONS

**Proposition 4.2.6.** Let $H$ be an arbitrary Hopf algebra. Then $\Phi : H^* \to \text{End}(H)$ with $\Phi(f) := \text{id} * u_H f$ is an algebra monomorphism satisfying

$$\Phi(f * g) = \Phi(f) \circ \Phi(g).$$

The image of $\Phi$ is precisely the set of left translation invariant elements $T \in \text{End}(H)$.

**Proof.** For $f \in \text{Hom}(H, \mathbb{K})$ we have $u_H f \in \text{End}(H)$ hence $\text{id} * u_H f \in \text{End}(H)$. Thus $\Phi$ is a well-defined homomorphism. Observe that

$$\Phi(f)(a) = (\text{id}_H * u_H f)(a) = \sum a_{(1)} f(a_{(2)}).$$

$\Phi$ is injective since it has a retraction $\text{End}(H) \ni g \mapsto \epsilon_H \circ g \in \text{Hom}(H, \mathbb{K})$. In fact we have $(\epsilon \Phi(f))(a) = \epsilon(\sum a_{(1)} f(a_{(2)})) = \sum \epsilon(a_{(1)}) f(a_{(2)}) = f(\sum \epsilon(a_{(1)}) a_{(2)}) = f(a)$ hence $\epsilon \Phi(f) = f$.

The map $\Phi$ preserves the algebra unit since $\Phi(1_H) = \Phi(\epsilon_H) = \text{id}_H * u_H \epsilon_H = \text{id}_H$.

The map $\Phi$ is compatible with the multiplication: $\Phi(f * g)(a) = \sum a_{(1)}(f * g)(a_{(2)}) = \sum a_{(1)} f(a_{(2)}) g(a_{(3)}) = \sum (\text{id} * u_H f)(a_{(1)}) g(a_{(2)}) = \Phi(f)(\sum a_{(1)} g(a_{(2)})) = \Phi(f) \Phi(g)(a)$ so that $\Phi(f * g) = \Phi(f) \circ \Phi(g)$.

For each $f \in H^*$ the element $\Phi(f)$ is left translation invariant since $\Delta \Phi(f)(a) = \Delta(\sum a_{(1)} f(a_{(2)})) = \sum a_{(1)} \otimes a_{(2)} f(a_{(3)}) = (1 \otimes \Phi(f)) \Delta(a)$.

Let $T \in \text{End}(H)$ be left translation invariant then $S * T = \nabla_H(S \otimes 1)(1 \otimes T) \Delta_H = \nabla_H(S \otimes 1) \Delta_H T = u_H \epsilon_H T$. Thus $\Phi(\epsilon T) = \text{id} * u_H \epsilon_H T = \text{id} * S * T = T$, so that $T$ is in the image of $\Phi$. \qed

**Proposition 4.2.7.** Let $d \in \text{Hom}(H, \mathbb{K})$ and $\Phi(d) = D \in \text{Hom}(H, H)$ be given. The following are equivalent:

1. $d : H \to \epsilon \mathbb{K}_e$ is a derivation.
2. $D : H \to H H$ is a (left translation invariant) derivation.

In particular $\Phi$ induces an isomorphism between the set of derivations $d : H \to \epsilon \mathbb{K}_e$ and the set of left translation invariant derivations $D : H \to H H$.

**Proof.** Assume that 1. holds so that $d$ satisfies $d(ab) = \epsilon(a) d(b) + d(a) \epsilon(b)$. Then we get $D(ab) = \Phi(d)(ab) = \sum a_{(1)} b_{(1)} d(a_{(2)} b_{(2)}) = \sum a_{(1)} b_{(1)} \epsilon(a_{(2)}) d(b_{(2)}) + \sum a_{(1)} b_{(1)} d(a_{(2)}) \epsilon(b_{(2)}) = a D(b) + D(a) b$. Conversely assume that $D(ab) = a D(b) + D(a) b$. Then $d(ab) = \epsilon D(ab) = \epsilon(a) \epsilon D(b) + \epsilon D(a) \epsilon(b) = \epsilon(a) d(b) + d(a) \epsilon(b)$. \qed
3. The Lie Algebra of Primitive Elements

Lemma 4.3.1. Let $H$ be a Hopf algebra and $H^o$ be its Sweedler dual. If $d \in \text{Der}_K(H, eK_e) \subseteq \text{Hom}(H, K)$ is a derivation then $d$ is a primitive element of $H^o$. Furthermore every primitive element $d \in H^o$ is a derivation in $\text{Der}_K(H, eK_e)$.

Proof. Let $d : H \to K$ be a derivation and let $a, b \in H$. Then $(b \to d)(a) = d(ab) = \varepsilon(a)d(b) + d(a)\varepsilon(b) = (d(b)\varepsilon + \varepsilon(b)d)(a)$ hence $(b \to d) = d(b)\varepsilon + \varepsilon(b)d$. Consequently we have $Hd = (H \to d) \subseteq \mathfrak{k} \varepsilon + \mathfrak{K}d$ so that $\dim Hd \leq 2 < \infty$. This shows $d \in H^o$. Furthermore we have $\langle \Delta d, a \otimes b \rangle = \langle d(ab) = d(ab) = d(a)\varepsilon(b) + \varepsilon(a)d(b) = (d \otimes \varepsilon, a \otimes b) + \langle \varepsilon \otimes d, a \otimes b \rangle = 1_{H^o} \otimes d + d \otimes 1_{H^o}, a \otimes b \rangle$ hence $\Delta(d) = d \otimes 1_{H^o} + 1_{H^o} \otimes d$ so that $d$ is a primitive element in $H^o$.

Conversely let $d \in H^o$ be primitive. then $d(ab) = \langle \Delta(d), a \otimes b \rangle = d(a)\varepsilon(b) + \varepsilon(a)d(b)$.

Proposition and Definition 4.3.2. Let $H$ be a Hopf algebra. The set of primitive elements of $H$ will be denoted by $\text{Lie}(H)$ and is a Lie algebra. If $\text{char}(K) = p > 0$ then $\text{Lie}(H)$ is a restricted Lie algebra or a $p$-Lie algebra.

Proof. Let $a, b \in H$ be primitive elements. Then $\Delta([a, b]) = \Delta(ab - ba) = (a \otimes 1 + 1 \otimes a)(b \otimes 1 + 1 \otimes b) - (b \otimes 1 + 1 \otimes b)(a \otimes 1 + 1 \otimes a) = (ab - ba) \otimes 1 + 1 \otimes (ab - ba)$ hence $\text{Lie}(H) \subseteq H^L$ is a Lie algebra. If the characteristic of $K$ is $p > 0$ then we have $(a \otimes 1 + 1 \otimes a)^p = a^p \otimes 1 + 1 \otimes a^p$. Thus $\text{Lie}(H)$ is a restricted Lie subalgebra of $H^L$ with the structure maps $[a, b] = ab - ba$ and $a^{[p]} = a^p$.

Corollary 4.3.3. Let $H$ be a Hopf algebra. Then the set of left translation invariant derivations $D : H \to H$ is a Lie algebra under $[D, D'] = DD' - D'D$. If $\text{char} = p$ then these derivations are a restricted Lie algebra with $D^{[p]} = D^p$.

Proof. The map $\Psi : H^o \to H^* \otimes \text{End}(H)$ is a homomorphism of algebras by 4.2.6. Hence $\Psi(d \ast d' - d' \ast d) = \Phi(d \ast d' - d' \ast d) = \Phi(d)\Phi(d') - \Phi(d')\Phi(d)$. If $d$ is a primitive element in $H^o$ then by 4.2.7 and 4.3.1 the image $D := \Psi(d)$ in $\text{End}(H)$ is a left translation invariant derivation and all left translation invariant derivations are of this form. Since $[d, d'] = d \ast d' - d' \ast d$ is again primitive we get that $[D, D'] = DD' - D'D$ is a left translation invariant derivation so that the set of left translation invariant derivations $\text{Der}_K^H(H, H)$ is a Lie algebra resp. a restricted Lie algebra.

Definition 4.3.4. Let $H$ be a Hopf algebra. An element $c \in H$ is called cocommutative if $\tau \Delta(c) = \Delta(c)$, i. e. if $\sum c_{(1)} \otimes c_{(2)} = \sum c_{(2)} \otimes c_{(1)}$. Let $C(H) := \{c \in H | c$ is cocommutative $\}$.

Let $G(H)$ denote the set of group like elements of $H$.

Lemma 4.3.5. Let $H$ be a Hopf algebra. Then the set of cocommutative elements $C(H)$ is a subalgebra of $H$ and the group like elements $G(H)$ form a linearly independent subset of $C(H)$. Furthermore $G(H)$ is a multiplicative subgroup of the group of units $U(C(H))$. 

3. The Lie Algebra of Primitive Elements

Proof. It is clear that \( C(H) \) is a linear subspace of \( H \). If \( a, b \in C(H) \) then
\[
\Delta(ab) = \Delta(a)\Delta(b) = (\tau\Delta)(a)(\tau\Delta)(b) = \tau(\Delta(a)\Delta(b)) = \tau\Delta(ab) \quad \text{and} \quad \Delta(1) = 1 \otimes 1 = \tau\Delta(1).
\]
Thus \( C(H) \) is a subalgebra of \( H \).

The group like elements obviously are cocommutative and form a multiplicative group, hence a subgroup of \( U(C(H)) \). They are linearly independent by Lemma 2.1.14. \( \square \)

Proposition 4.3.6. Let \( H \) be a Hopf algebra with \( S^2 = \text{id}_H \). Then there is a left module structure
\[
C(H) \otimes \text{Lie}(H) \ni c \otimes a \mapsto c \cdot a \in \text{Lie}(H)
\]
with \( c \cdot a := \nabla_H(\nabla_H \otimes 1)(1 \otimes \tau)(1 \otimes S \otimes 1)(\Delta \otimes 1)(c \otimes a) = \sum c_{(1)}aS(c_{(2)}) \) such that
\[
c \cdot [a, b] = \sum [c_{(1)} \cdot a, c_{(2)} \cdot b].
\]

In particular \( G(H) \) acts by Lie automorphisms on \( \text{Lie}(H) \).

Proof. The given action is clearly the action \( H \otimes H \rightarrow H \) with \( h \cdot a = \sum h_{(1)}aS(h_{(2)}) \), the so-called adjoint action.

We first show that the given map has image in \( \text{Lie}(H) \). For \( c \in C(H) \) and \( a \in \text{Lie}(H) \) we have
\[
\Delta(c \cdot a) = \Delta(\sum c_{(1)}aS(c_{(2)})) = \sum \Delta(c_{(1)})(a \otimes 1 + 1 \otimes a)\Delta(S(c_{(2)})) = \sum \Delta(c_{(1)})(a \otimes 1)\Delta(S(c_{(2)})) + \sum \Delta(c_{(2)})(1 \otimes a)\Delta(S(c_{(1)})) = \sum c_{(1)}aS(c_{(4)}) \otimes c_{(2)}S(c_{(5)}) + \sum c_{(3)}S(c_{(6)}) \otimes c_{(4)}aS(c_{(7)}) \in c \cdot a \otimes 1 + 1 \otimes c \cdot a \text{ since } c \text{ is cocommutative, } S^2 = \text{id}_H \text{ and } a \text{ is primitive.}
\]

We show now that \( \text{Lie}(H) \) is a \( C(H) \)-module. \( (cd) \cdot a = \sum c_{(1)}d_{(1)}aS(c_{(2)}d_{(2)}) = \sum c_{(1)}d_{(1)}aS(c_{(2)})S(c_{(3)}) = c \cdot (d \cdot a) \). Furthermore we have \( 1 \cdot a = 1aS(1) = a \).

To show the given formula let \( a, b \in \text{Lie}(H) \) and \( c \in C(H) \). Then \( c \cdot [a, b] = \sum c_{(1)}(ab - ba)S(c_{(2)}) = \sum c_{(1)}aS(c_{(2)})c_{(3)}bS(c_{(4)}) - \sum c_{(1)}bS(c_{(2)})c_{(3)}aS(c_{(4)}) = \sum [c_{(1)}a, c_{(2)}b] \) again since \( c \in C(H) \) is cocommutative.

Now let \( g \in G(H) \). Then \( g \cdot a = gaS(g) = gag^{-1} \) since \( S(g) = g^{-1} \) for any group like element. Furthermore \( g \cdot [a, b] = [g \cdot a, g \cdot b] \) hence \( g \) defines a Lie algebra automorphism of \( \text{Lie}(H) \). \( \square \)

Problem 4.3.2. Show that the adjoint action \( H \otimes H \ni h \otimes a \mapsto \sum h_{(1)}aS(h_{(2)}) \in H \) makes \( H \) an \( H \)-module algebra.

Definition and Remark 4.3.7. The algebra \( K(\delta) = K[\delta]/(\delta^2) \) is called the algebra of dual numbers. Observe that \( K(\delta) = K \oplus K\delta \) as a \( K \)-module.

We consider \( \delta \) as a "small quantity" whose square vanishes.

The maps \( p : K(\delta) \rightarrow K \) with \( p(\delta) = 0 \) and \( j : K \rightarrow K(\delta) \) are algebra homomorphisms satisfying \( pj = \text{id} \).

Let \( K(\delta, \delta') := K[\delta, \delta']/(\delta^2, \delta'^2) \). Then \( K(\delta, \delta') = K \oplus K\delta \oplus K\delta' \oplus K\delta\delta' \). The map \( K(\delta) \ni \delta \mapsto \delta \delta' \in K(\delta, \delta') \) is an injective algebra homomorphism. Furthermore for every \( \alpha \in K \) we have an algebra homomorphism \( \varphi_\alpha : K(\delta) \ni \delta \mapsto \alpha \delta \in K(\delta) \).

These algebra homomorphisms induce algebra homomorphisms \( H \otimes K(\delta) \rightarrow H \otimes K(\delta, \delta') \) for every Hopf algebra \( H \).
Proposition 4.3.8. The map 
\[ e^\delta : \text{Lie}(H) \rightarrow H \otimes \mathbb{K}(\delta) \subseteq H \otimes \mathbb{K}(\delta, \delta') \]
with \( e^\delta a := 1 + a \otimes \delta = 1 + \delta a \) is called the exponential map and satisfies 
\[ e^{\delta(a+b)} = e^{\delta a} e^{\delta b}, \]
\[ e^{\delta a} = \varphi_a(e^\delta), \]
\[ e^{\delta b} = e^{\delta b} e^{\delta a} - 1(e^{\delta b})^{-1}. \]
Furthermore all elements \( e^\delta a \in H \otimes \mathbb{K}(\delta) \) are group like in the \( \mathbb{K}(\delta) \)-Hopf algebra \( H \otimes \mathbb{K}(\delta) \).

**Proof.**
1. \( e^{\delta(a+b)} = (1 + \delta(a + b)) = (1 + \delta a)(1 + \delta b) = e^{\delta a} e^{\delta b}. \)
2. \( e^{\delta a} = 1 + \delta a a = \varphi_a(1 + \delta a) = \varphi_a(e^\delta). \)
3. Since \((1 + \delta a)(1 - \delta a) = 1\) we get \( e^{\delta a} = 1 - \delta a. \) So we get \( e^{\delta [a, b]} = 1 + \delta [a, b] = 1 + \delta(a - a) + \delta'(b - b) + \delta'(ab - ab - ba + ab) = (1 + \delta a)(1 + \delta' b)(1 - \delta a)(1 - \delta' b) = e^{\delta a} e^{\delta' b} e^{\delta a} - 1(e^{\delta b})^{-1}. \)
4. \( \Delta_{\mathbb{K}(\delta)}(e^\delta a) = \Delta(1 + a \otimes \delta) = 1 \otimes_{\mathbb{K}(\delta)} 1 + (a \otimes 1 + 1 \otimes a) \otimes \delta = 1 \otimes_{\mathbb{K}(\delta)} 1 + \delta a \otimes_{\mathbb{K}(\delta)} 1 + 1 \otimes_{\mathbb{K}(\delta)} \delta a + \delta a \otimes_{\mathbb{K}(\delta)} \delta a = (1 + \delta a) \otimes_{\mathbb{K}(\delta)} (1 + \delta a) = e^{\delta a} \otimes_{\mathbb{K}(\delta)} e^{\delta a} \) and \( \varepsilon_{\mathbb{K}(\delta)}(e^\delta a) = \varepsilon_{\mathbb{K}(\delta)}(1 + \delta a) = 1 + \delta \varepsilon(a) = 1 \). \( \square \)

Corollary 4.3.9. \( (\text{Lie}(H), e^\delta) \) is the kernel of the group homomorphism \( p : G_{\mathbb{K}(\delta)}(H \otimes \mathbb{K}(\delta)) \rightarrow G(H). \)

**Proof.** \( p = 1 \otimes p : H \otimes \mathbb{K}(\delta) \rightarrow H \otimes \mathbb{K} = H \) is a homomorphism of \( \mathbb{K} \)-algebras. We show that it preserves group like elements. Observe that group like elements in \( H \otimes \mathbb{K}(\delta) \) are defined by the Hopf algebra structure over \( \mathbb{K}(\delta) \). Let \( g \in G_{\mathbb{K}(\delta)}(H \otimes \mathbb{K}(\delta)) \). Then \( (\Delta_H \otimes 1)(g) = g \otimes_{\mathbb{K}(\delta)} g \) and \( (\varepsilon_H \otimes 1)(g) = 1 \in \mathbb{K}(\delta) \).

Since \( p : \mathbb{K}(\delta) \rightarrow \mathbb{K} \) is an algebra homomorphism the following diagram commutes 
\[
(H \otimes \mathbb{K}(\delta)) \otimes_{\mathbb{K}(\delta)} (H \otimes \mathbb{K}(\delta)) \twoheadrightarrow H \otimes H \otimes \mathbb{K}(\delta)
\]
\[
\begin{array}{ccc}
(1 \otimes p) \otimes (1 \otimes p) & \downarrow & 1 \otimes p \\
(1 \otimes p) \otimes (1 \otimes p) & \downarrow & H \otimes H \otimes \mathbb{K}.
\end{array}
\]
We identify elements along the isomorphisms. Thus we get \( (\Delta_H \otimes 1_{\mathbb{K}})(1_H \otimes p)(g) = (1_H \otimes p)(\Delta_H \otimes 1_{\mathbb{K}})(g) = (1_H \otimes p)(1_{\mathbb{K}} \otimes g) = (1_H \otimes p)(g) \otimes (1_H \otimes p)(g) \) so that \( 1_H \otimes p : G_{\mathbb{K}(\delta)}(H \otimes \mathbb{K}(\delta)) \rightarrow G(H) \). Now we have \( (1_H \otimes p)(gg') = (1_H \otimes p)(g)(1_H \otimes p)(g') \) so that \( 1_H \otimes p \) is a group homomorphism.

Now let \( g = g_0 \otimes 1 + g_1 \otimes \delta \in G_{\mathbb{K}(\delta)}(H \otimes \mathbb{K}(\delta)) \subseteq H \otimes \mathbb{K} \oplus H \otimes \mathbb{K}(\delta) \). Then we have \( (1_H \otimes p)(g) = 1 \) iff \( g_0 = 1 \) iff \( g = 1_H \otimes 1_{\mathbb{K}(\delta)} + g_1 \otimes \delta \). Furthermore we have
\[
\Delta_H \otimes_{\mathbb{K}(\delta)}(g) = g \otimes_{\mathbb{K}(\delta)} g \iff 1_H \otimes 1_H \otimes 1_{\mathbb{K}(\delta)} + \Delta_H(g_1) \otimes \delta = (1_H \otimes 1_{\mathbb{K}(\delta)} + g_1 \otimes \delta) \otimes_{\mathbb{K}(\delta)} (1_H \otimes 1_{\mathbb{K}(\delta)} + g_1 \otimes \delta)
\]
\[
= 1_H \otimes 1_H \otimes 1_{\mathbb{K}(\delta)} + (g_1 \otimes 1_H + 1_H \otimes g_1) \otimes \delta \iff \Delta_H(g_1) = g_1 \otimes 1_H + 1_H \otimes g_1.
\]
Similarly we have $\varepsilon_{3\delta_3}(g) = 1$ iff $1 \otimes 1 + \varepsilon(g_1) \otimes \delta = 1$ iff $\varepsilon(g_1) = 0$. \hfill \Box
4. Derivations and Lie Algebras of Affine Algebraic Groups

Lemma and Definition 7.4.1. Let \( \mathcal{G} : \mathbb{K} \text{-cAlg} \to \text{Set} \) be a group valued functor. The kernel \( \text{Lie}(\mathcal{G})(R) \) of the sequence

\[
0 \to \text{Lie}(\mathcal{G})(R) \to \mathcal{G}(R(\delta)) \xrightarrow{\mathcal{G}(p)} \mathcal{G}(R) \to 0
\]

is called the Lie algebra of \( \mathcal{G} \) and is a group valued functor in \( R \).

Proof. For every algebra homomorphism \( f : R \to S \) the following diagram of groups commutes

\[
\begin{array}{cccccc}
0 & \to & \text{Lie}(\mathcal{G})(R) & \to & \mathcal{G}(R(\delta)) & \xrightarrow{\mathcal{G}(p)} & \mathcal{G}(R) & \to & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & \text{Lie}(\mathcal{G})(S) & \to & \mathcal{G}(S(\delta)) & \xrightarrow{\mathcal{G}(p)} & \mathcal{G}(S) & \to & 0 \\
\end{array}
\]

\[\Box\]

Proposition 4.4.2. Let \( \mathcal{G} : \mathbb{K} \text{-cAlg} \to \text{Set} \) be a group valued functor with multiplication \( \ast \). Then there are functorial operations

\[
\mathcal{G}(R) \times \text{Lie}(\mathcal{G})(R) \ni (g, x) \mapsto g \cdot x \in \text{Lie}(\mathcal{G})(R)
\]

\[
R \times \text{Lie}(\mathcal{G})(R) \ni (a, x) \mapsto ax \in \text{Lie}(\mathcal{G})(R)
\]

such that

\[
\begin{align*}
g \cdot (x + y) &= g \cdot x + g \cdot y, \\
h \cdot (g \cdot x) &= (h * g) \cdot x, \\
a(x + y) &= ax + ay, \\
(ab)x &= a(bx), \\
g \cdot (ax) &= a(g \cdot x).
\end{align*}
\]

Proof. First observe that the composition \( + \) on \( \text{Lie}(\mathcal{G})(R) \) is induced by the multiplication \( \ast \) of \( \mathcal{G}(R(\delta)) \) so it is not necessarily commutative.

We define \( g \cdot x := \mathcal{G}(j)(g) \ast x \ast \mathcal{G}(j)(g)^{-1} \). Then \( \mathcal{G}(p)(g \cdot x) = \mathcal{G}(p)\mathcal{G}(j)(g) \ast \mathcal{G}(p)(x) \ast \mathcal{G}(p)\mathcal{G}(j)(g)^{-1} = g \ast 1 \ast g^{-1} = 1 \) hence \( g \cdot x \in \text{Lie}(\mathcal{G})(R) \).

Now let \( a \in R \). To define \( a : \text{Lie}(\mathcal{G})(R) \to \text{Lie}(\mathcal{G})(R) \) we use \( u_a : R(\delta) \to R(\delta) \) defined by \( u_a(\delta) := a\delta \) and thus \( u_a(b + c\delta) := b + ac\delta \). Obviously \( u_a \) is a homomorphism of \( R \)-algebras. Furthermore we have \( pu_a = p \) and \( u_a \cdot j = j \). Thus we get a commutative diagram

\[
\begin{array}{cccccc}
0 & \to & \text{Lie}(\mathcal{G})(R) & \to & \mathcal{G}(R(\delta)) & \xrightarrow{\mathcal{G}(p)} & \mathcal{G}(R) & \to & 0 \\
\downarrow a & & \downarrow \mathcal{G}(u_a) & & \downarrow \mathcal{G}(p) & & \downarrow \text{id} & & \downarrow 0 \\
0 & \to & \text{Lie}(\mathcal{G})(R) & \to & \mathcal{G}(R(\delta)) & \xrightarrow{\mathcal{G}(p)} & \mathcal{G}(R) & \to & 0
\end{array}
\]
that defines a group homomorphism \( a : \mathcal{L}ie(\mathcal{G})(R) \to \mathcal{L}ie(\mathcal{G})(R) \) on the kernel of the exact sequences. In particular we have then \( a(x + y) = ax + ay \).

Furthermore we have \( u_{ab} = u_a u_b \) hence \( (ab)x = a(bx) \).

The next formula follows from \( g \cdot (x + y) = \mathcal{G}(j(g)) * x * y = \mathcal{G}(j(g)) \).

We also see \( (h * g) * x = \mathcal{G}(j(h)) * \mathcal{G}(j(g)) * x = \mathcal{G}(j(h)) * (h * g) \).

Finally we have \( g \cdot (ax) = \mathcal{G}(j(g)) * u_a(x) \).

\( \square \)

**Proposition 4.4.3.** Let \( \mathcal{G} = KcAlg(H, -) \) be an affine algebraic group. Then \( \mathcal{L}ie(\mathcal{G})(K) \cong \mathcal{L}ie(H^o) \) as additive groups. The isomorphism is compatible with the operations given in 4.4.3 and 4.3.6.

**Proof.** We consider the following diagram

\[
\begin{array}{ccc}
0 & \longrightarrow & \mathcal{L}ie(\mathcal{G})(K) \\
\varepsilon & \quad & \mathcal{L}ie(\mathcal{G})(H^o, K(\delta)) \quad p \quad \mathcal{L}ie(\mathcal{G})(H, K) \quad \longrightarrow \quad 0 \\
\wedge & \quad & \mathcal{L}ie(H^o) \quad \mathcal{L}ie(H^o) \quad \longrightarrow \quad G_{K(\delta)}(H^o \otimes K(\delta)) \quad \longrightarrow \quad G(H^o) \\
0 & \longrightarrow & G(H^o) \\
\end{array}
\]

We know by definition that the top sequence is exact. The bottom sequence is exact by Corollary 4.3.9.

Let \( f \in KcAlg(H, K) \). Since \( \text{Ker}(f) \) is an ideal of codimension 1 we get \( f \in H^o \).

The map \( f \) is an algebra homomorphism iff \( \langle f, ab \rangle = \langle f, f, a \otimes b \rangle \) and \( \langle f, 1 \rangle = 1 \) iff \( \Delta_{H^o}(f) = f \otimes f \) and \( \varepsilon_{H^o}(f) = 1 \) iff \( f \in G(H^o) \). Hence we get the right hand vertical isomorphism \( KcAlg(H, K) \cong G(H^o) \).

Consider an element \( f \in KcAlg(H, K(\delta)) \subseteq \text{Hom}(H, K(\delta)) \). It can be written as \( f = f_0 + f_1 \delta \) with \( f_0, f_1 \in \text{Hom}(H, K) \). The linear map \( f \) is an algebra homomorphism iff \( f_0 : H \to K \) is an algebra homomorphism and \( f_1 \) satisfies \( f_1(1) = 0 \) and \( f_1(ab) = f_0(a)f_1(b) + f_1(a)f_0(b) \). In fact we have \( f_1(1) = f_0(1) + f_1(1)\delta = 1 \) iff \( f_0(1) = 1 \) and \( f_1(1) = 0 \) (by comparing coefficients). Furthermore we have \( f_0(ab) = f_0(f(b)) \).

Since \( f_0 \) is an algebra homomorphism we have as above \( f_0 \in H^o \). For \( f_1 \) we have \( (b \rightarrow f_1)(a) = f_1(ab) = f_0(a)f_1(b) + f_1(a)f_0(b) = (f_1(b)f_0 + f_0(b)f_1)(a) \) hence \( (b \rightarrow f_1) = f_1(b)f_0 + f_0(b)f_1 \in Kf_0 + Kf_1 \), a two dimensional subspace. Thus \( f_1 \in H^o \).

In the following computations we will identify \( (H^o \otimes K(\delta)) \otimes K(\delta)(H^o \otimes K(\delta)) \) with \( H^o \otimes H^o \otimes [K(\delta)] \).

Let \( f = f_0 + f_1 \delta = f_0 \otimes 1 + f_1 \otimes \delta \in H^o \otimes H^o \delta = H^o \otimes K(\delta) \). Then \( f \) is a homomorphism of algebras iff \( f(ab) = f(a)f(b) \) and \( f(1) = 1 \) iff \( f_0(ab) = f_0(a)f_0(b) \) and \( f_1(ab) = f_0(a)f_1(b) + f_1(a)f_0(b) \) and \( f_0(1) = 1 \) and \( f_1(1) = 0 \) iff \( \Delta_{H^o}(f_0) = f_0 \otimes f_0 \) and \( \Delta_{H^o}(f_1) = f_0 \otimes f_1 + f_1 \otimes f_0 \) and \( \varepsilon_{H^o}(f_0) = 1 \) and \( \varepsilon_{H^o}(f_1) = 0 \) iff \( \Delta_{H^o} \otimes \text{id}_{K(\delta)}((f_0 \otimes 1 + f_1 \otimes \delta) = f_0 \otimes f_0 \otimes 1 + f_0 \otimes f_1 \otimes \delta + f_1 \otimes f_0 \otimes \delta = (f_0 \otimes 1 + f_1 \otimes \delta) \otimes K(\delta)(f_0 \otimes 1 + f_1 \otimes \delta) \)
and $(\varepsilon \otimes \text{id}_{\mathbb{K}(\delta)})(f_0 \otimes 1 + f_1 \otimes \delta) = 1 \otimes 1$ iff $(\Delta \otimes \text{id}_{\mathbb{K}(\delta)})(f) = f \otimes_{\mathbb{K}(\delta)} f$ and $(\varepsilon \otimes \text{id}_{\mathbb{K}(\delta)})(f) = 1$ iff $f \in G_{\mathbb{K}(\delta)}(H^o \otimes \mathbb{K}(\delta))$.

Hence we have a bijective map $\omega : \mathbb{K} \text{-cAlg}(H, \mathbb{K}(\delta)) \ni f = f_0 + f_1 \delta \mapsto f_0 \otimes 1 + f_1 \otimes \delta \in G_{\mathbb{K}(\delta)}(H^o \otimes \mathbb{K}(\delta))$. Since the group multiplication in $\mathbb{K} \text{-cAlg}(H, \mathbb{K}(\delta)) \subseteq \text{Hom}(H, \mathbb{K}(\delta))$ is the convolution $*$ and the group multiplication in $G_{\mathbb{K}(\delta)}(H^o \otimes \mathbb{K}(\delta)) \subseteq H^o \otimes \mathbb{K}(\delta)$ is the ordinary algebra multiplication, where the multiplication of $H^o$ again is the convolution, it is clear that $\omega$ is a group homomorphism. Furthermore the right hand square of the above diagram commutes. Thus we get an isomorphism $e : \text{Lie}(H^o) \to \text{Lie}(G(\mathbb{K}))$ on the kernels. This map is defined by $e(d) = 1 + d \delta \in \mathbb{K} \text{-cAlg}(H, \mathbb{K}(\delta))$.

To show that this isomorphism is compatible with the actions of $\mathbb{K}$ resp. $G(H^o)$ let $\alpha \in \mathbb{K}$, $a \in H$, and $d \in \text{Lie}(H^o)$. We have $e(\alpha d)(a) = e(\alpha) + \alpha d(a) \delta = u_\alpha(e(a)) + d(a) \delta = (u_\alpha \circ (1 + d \delta))(a) = (u_\alpha \circ e(d))(a) = (\alpha e(d))(a)$ hence $e(\alpha d) = \alpha e(d)$.

Furthermore let $g \in G(H^o) = \mathbb{K} \text{-cAlg}(H, \mathbb{K})$, $a \in H$, and $d \in \text{Lie}(H^o)$. Then we have $e(g \cdot d)(a) = e(g dg^{-1})(a) = e(a) + g dg^{-1}(a) \delta = \sum g(a_{(1)}) e(a_{(2)}) g S(a_{(3)}) + \sum g(a_{(1)}) d(a_{(2)}) g S(a_{(3)}) \delta = \sum g(a_{(1)}) e(d)(a_{(2)}) g S(a_{(3)}) = (g \circ e(d))(a) = e(g \cdot d)(a)$ hence $e(g \cdot d) = g \cdot e(d)$.

**Proposition 4.4.4.** Let $H$ be a Hopf algebra and let $I := \text{Ker}(\varepsilon)$. Then $\text{Der}_\varepsilon(H, -) : \text{Vec} \to \text{Vec}$ is representable by $I/I^2$ and $d : H \xrightarrow{\varepsilon} I \xrightarrow{\nu} I/I^2$, in particular

$$
\text{Der}_\varepsilon(H, -) \cong \text{Hom}(I/I^2, -) \quad \text{and} \quad \text{Lie}(H^o) \cong \text{Hom}(I/I^2, \mathbb{K}).
$$

**Proof.** Because of $\varepsilon(\text{id} - u \varepsilon)(a) = \varepsilon(a) - u \varepsilon(a) = 0$ we have $\text{Im}(\text{id} - \varepsilon) \subseteq I$. Let $i \in I$. Then we have $i = i - \varepsilon(i) = (\text{id} - \varepsilon)(i)$ hence $\text{Im}(\text{id} - \varepsilon) = \text{Ker}(\varepsilon)$. We have $I^2 \supseteq (\text{id} - \varepsilon)(a)(\varepsilon - \varepsilon)(b) = ab - \varepsilon(a)b - a\varepsilon(b) + \varepsilon(a)\varepsilon(b) = (\text{id} - \varepsilon)(ab) - \varepsilon(a)(\text{id} - \varepsilon)(b) - (\text{id} - \varepsilon)(a)\varepsilon(b)$. Hence we have in $I/I^2$ the equation $(\text{id} - \varepsilon)(ab) = \varepsilon(a)(\text{id} - \varepsilon)(b) + (\text{id} - \varepsilon)(a)\varepsilon(b)$ so that $\nu(\text{id} - \varepsilon) : H \to I \to I/I^2$ is an $\varepsilon$-derivation.

Now let $D : H \to M$ be an $\varepsilon$-derivation. Then $D(1) = D(1)1 = D(1) + D(1)1$ hence $D(1) = 0$. It follows $D(a) = D(\text{id} - \varepsilon)(a)$. From $\varepsilon(I) = 0$ we get $D(I) \subseteq \varepsilon(I)D(I) + D(I)\varepsilon(I) = 0$ hence there is a unique factorization

$$
\begin{array}{c}
H \xrightarrow{\varepsilon - \nu} I/I^2 \\
D \downarrow \quad \downarrow \nu \quad \downarrow D \\
M.
\end{array}
$$

**Corollary 4.4.5.** Let $H$ be a Hopf algebra that is finitely generated a s an algebra. Then $\text{Lie}(H^o)$ is finite dimensional.

**Proof.** Let $H = \mathbb{K}(a_1, \ldots, a_n)$. Since $H = \mathbb{K} \oplus I$ we can choose $a_1 = 1$ and $a_2, \ldots, a_n \in I$. Thus any element in $i \in I$ can be written as $\sum \alpha_j a_{j_1} \ldots a_{j_k}$ so that $I/I^2 = \mathbb{K} a_2 + \ldots + a_n$. This gives the result.
Proposition 4.4.6. Let $H$ be a commutative Hopf algebra and $\_HM$ be an $H$-module. Then we have $\Omega\_H \cong H \otimes I/I^2$ and $d : H \rightarrow H \otimes I/I^2$ is given by $d(a) = \sum a_{(1)} \otimes (\id - \varepsilon)(a_{(2)})$.

Proof. Consider the algebra $B := H \oplus M$ with $(a, m)(a', m') = (aa', am' + a'm)$. Let $\mathcal{G} = \mathbb{K} - \text{cAlg}(H, -)$. Then we have $\mathcal{G}(B) \subseteq \text{Hom}(H, B) \cong \text{Hom}(H, H) \oplus \text{Hom}(H, M)$. An element $(\varphi, D) \in \text{Hom}(H, B)$ is in $\mathcal{G}(B)$ iff $(\varphi, D)(1) = (\varphi(1), D(1)) = (1, 0)$, hence $\varphi(1) = 1$ and $D(1) = 0$, and $(\varphi(ab), D(ab)) = (\varphi, D)(ab) = (\varphi, D)(a)(\varphi, D)(b) = (\varphi(a), D(a))(\varphi(b), D(b)) = (\varphi(a), D(b) + D(a)\varphi(b))$, hence $\varphi(ab) = \varphi(a)\varphi(b)$ and $D(ab) = \varphi(a)D(b) + D(a)\varphi(b)$. So $(\varphi, D)$ is in $\mathcal{G}(B)$ iff $\varphi \in \mathcal{G}(H)$ and $D$ is a $\varphi$-derivation. The *-multiplication in $\text{Hom}(H, B)$ is given by $(\varphi, D) * (\varphi', D') = (\varphi * \varphi', \varphi * D' + D * \varphi')$ by applying this to an element $a \in H$. Since $(\varphi, 0) \in \mathcal{G}(B)$ and $(u\varepsilon, D) \in \mathcal{G}(B)$ for every $\varepsilon$-derivation $D$, there is a bijective $\text{Der}_\varepsilon(H, M) \cong \{(u\varepsilon, D) \in \mathcal{G}_e(B)\} \cong \{(1_H, D) \in \mathcal{G}_e(B)\} \cong \text{Der}_\varepsilon(H, M)$ by $(u\varepsilon, D) \mapsto (1, 0) * (u\varepsilon, D) = (1, 1 * D) \in \mathcal{G}_e(B)$ with inverse map $(1, D) \mapsto (S, 0) * (1, D) = (u\varepsilon, S * D) \in \mathcal{G}_e(B)$. Hence we have isomorphisms $\text{Der}_\varepsilon(H, M) \cong \text{Der}_e(H, M) \cong \text{Hom}(I/I, M) \cong \text{Hom}_H(H \otimes I/I^2, M)$.

The universal $\varepsilon$-derivation for vector spaces is $\id - \varepsilon : A \rightarrow I/I^2$. The universal $\varepsilon$-derivation for $H$-modules is $D_e(a) = 1 \otimes (\id - \varepsilon)(a) \in A \otimes I/I^2$. The universal $1$-derivation for $H$-modules is $1 * D_e$ with $(1 * D_e)(a) = \sum a_{(1)} \otimes (\id - \varepsilon)(a_{(2)}) \in A \otimes I/I^2$. 

\[ \square \]