HOPF ALGEBRAS

1. Algebras and coalgebras

1.1. **Algebras.** We start by formulating a familiar definition in a possibly unfamiliar way:

Definition. A k-*algebra* is a k-vector space with two linear maps

$$m : A \otimes_k A \to A \quad \text{and} \quad u : k \to A$$

satisfying the following conditions hold. These respectively encode associativity and the unit element:
(a) the diagram

$$\begin{tikzcd}
A \otimes A \otimes A \arrow[r, "m\otimes id"] \arrow[d, "id\otimes m"'] & A \otimes A \arrow[d, "m"] \\
A \otimes A \arrow[r, "m"] & A
\end{tikzcd}$$

is commutative;
and (b) the diagram

$$\begin{tikzcd}
 & A \otimes A \arrow[dd, "m"] & \\
k \otimes A \arrow[ur, "u\otimes id"] \arrow[dr, "s"'] & & A \otimes k \arrow[ul, "id\otimes u"'] \arrow[dl, "s"] \\
 & A &
\end{tikzcd}$$

(where s denotes scalar multiplication) is commutative.

We get 1_A as $u(1_k)$ via the second diagram.

1.2. **Coalgebras.** To define these, we reverse the arrows in (7.1):

Definition. A k-*coalgebra* is a k-vector space, C, with two k-linear maps, Δ (*comultiplication* or *coproduct*) and ε (*counit*), with

$$\Delta : C \to C \otimes C \quad \text{and} \quad \varepsilon : C \to k,$$

such that the following conditions, respectively called the coassociativity and the counit axioms, hold:

a) the diagram

$$\begin{tikzcd}
C\otimes C\otimes C & C\otimes C \arrow[l, "\Delta\otimes id"'] \\
C\otimes C \arrow[u, "id\otimes\Delta"] & C \arrow[l, "\Delta"] \arrow[u, "\Delta"']
\end{tikzcd}$$

commutes;

b) the diagram

$$\begin{tikzcd}
& C\otimes C \arrow[dl, "\varepsilon\otimes id"'] \arrow[dr, "id\otimes\varepsilon"] & \\
k\otimes C & & C\otimes k \\
& C \arrow[ul, "1\otimes\_"] \arrow[uu, "\Delta"] \arrow[ur, "\_\otimes 1"'] &
\end{tikzcd}$$

commutes, where $1\otimes\_$ is the map $x\mapsto 1\otimes x$.

1.3. **Morphisms.**

Definition. Let A and B be k-algebras. A linear map $\theta : A\to B$ is a *k-algebra homomorphism* if the diagrams

$$\begin{tikzcd}
A \arrow[r, "\theta"] & B \\
A\otimes A \arrow[u, "m_A"] \arrow[r, "\theta\otimes\theta"'] & B\otimes B \arrow[u, "m_B"']
\end{tikzcd}$$

and

$$\begin{tikzcd}
A \arrow[r, "\theta"] & B \\
k \arrow[u, "u_A"] \arrow[r, equal] & k \arrow[u, "u_B"']
\end{tikzcd}$$

commute.

Definition. Let C and D be k-coalgebras. A linear map $f : C\to D$ is a *k-coalgebra morphism* if the diagrams

$$\begin{tikzcd}
C \arrow[r, "f"] \arrow[d, "\Delta_c"'] & D \arrow[d, "\Delta_D"] \\
C\otimes C \arrow[r, "f\otimes f"] & B\otimes B
\end{tikzcd}$$

and

$$\begin{tikzcd}
C \arrow[r, "f"] \arrow[d, "\varepsilon_C"'] & D \arrow[d, "\varepsilon_D"] \\
k \arrow[r, equal] & k
\end{tikzcd}$$

commute.

1.4. **Example.** Let V be a k-vector space with basis $\mathcal{B}$. Then V is a coalgebra if we set

$$\begin{aligned}\Delta(V) &= v \otimes v \quad \forall v \in \mathcal{B}\\ \varepsilon(V) &= 1 \quad \forall v \in \mathcal{B}\end{aligned}$$

(extended linearly). V is called the (group-like) *coalgebra on the set* $\mathcal{B}$.

2. Bialgebras

2.1. The definition.

Definition. A *bialgebra* A is a k-vector space, $A = (A, m, u, \Delta, \varepsilon)$ where (A, m, u) is an algebra; and (A, Δ, ε) is a coalgebra; and such that either (and hence both) of the following two conditions hold:-

(1) Δ and ε are algebra homomorphisms; and
(2) m and u are coalgebra homomorphisms.

Notes. 1. If A and B are two k-algebras then so is $A \otimes B$ if we define $(a \otimes b)(c \otimes d) = ac \otimes db$. Expressed as a diagram this is:

$$A \otimes B \otimes A \otimes B \xrightarrow{id \otimes \tau \otimes id} A \otimes A \otimes B \otimes B \xrightarrow{m_A \otimes m_B} A \otimes B$$

where $\tau : B \otimes A \to A \otimes B$ is the flip: $\tau(b \otimes a) = a \otimes b$. The unit $u_{A \otimes B}$ of $A \otimes B$ is given by

$$k \cong k \otimes k \xrightarrow{u_A \otimes u_B} A \otimes B \ .$$

Similarly, if C and D are coalgebras then so is $C \otimes D$ with $\Delta_{C \otimes D}$ given by

$$C \otimes D \xrightarrow{\Delta_C \otimes \Delta_D} C \otimes C \otimes D \otimes D \xrightarrow{id \otimes \tau \otimes id} C \otimes D \otimes C \otimes D$$

and counit

$$C \otimes D \xrightarrow{\varepsilon_C \otimes \varepsilon_D} k \otimes k \cong k \ .$$

In particular this applies when $A = B$ and when $C = D$.

2. (1) $\Leftrightarrow$ (2) in the definition follows by drawing the diagrams to express the conditions that Δ and ε are algebra morphisms; we find the diagrams are the same as the ones to give (2); see Exercises 2.4(1).

3. A morphism of bialgebras $f : A \to B$ is a linear map which is both an algebra and a coalgebra homomorphism.

2.2. **Test Lemmas.**

Lemma 1. *Suppose that A is an algebra and we have algebra homomorphisms $\Delta : A \to A \otimes A$ and $\varepsilon : A \to k$. If A is generated as an algebra by a set $\mathcal{B}$, to prove that A is a bialgebra we only need to check the diagrams in 1.2 with input from $\mathcal{B}$.*

Proof. All the maps in the diagrams are algebra homomorphisms given our hypothesis. So commutativity in general follows at once from commutativity on the generators. □

If $f : A \to B$ is a bialgebra homomorphism, then ker$f$ is called a *biideal*: this means that ker$f$ is an ideal and a coideal (ie the kernel of a coalgebra homomorphism). See Ex1.5(3) where we check that $I \subseteq A$ is a *coideal* if $\varepsilon(I) = 0$ and $\Delta(I) \subseteq C \otimes I + I \otimes C$.

Lemma 2. *When I is a biideal of a bialgebra A, then the operatins on A induce a structure of bialgebra on A/J.*

2.3. **Examples of bialgebras.** Here are the first few examples. We will add to this list once we have defined Hopf algebras.

(1) **Group algebras**: Let G be any group and let kG be the group algebra. It is a bialgebra if we define $\Delta : kG \to kG \otimes kG$ by $\Delta(g) = g \otimes g$ for $g \in G$, and $\varepsilon(g) = 1$ for $g \in G$; see Exercise 2.4(2).

(2) **Tensor algebras**: Let V be a vector space and form $T(V)$, the tensor algebra, so

$$T(V) = \bigoplus_{n \geq 0} (V^{\otimes n});$$

multiplication of tensors is given by juxtaposition, extended linearly. Then $T(V)$ is a bialgebra if we define

$$\Delta(V) = v \otimes 1 + 1 \otimes v \in T(V) \otimes T(V)$$

and $\varepsilon(V) = 0$ for $v \in V$.

Proof. $T(V)$ is the free k-algebra on generators $\{v_i : i \in I\}$, a basis of V. So Δ and ε extend uniquely to algebra homomorphisms, to $T(V)$ and to k respectively. So we can apply Lemma (2.2)(1) and see that we only need to check commutativity of the diagrams in 1.2 for input $\{v_i\}$ a basis element. This is easy. □

(3) **Enveloping algebras of Lie algebras**: A *Lie algebra* $\mathfrak{g}$ is a vector space over a field k with an operation

$$[\ ,\ ] : \mathfrak{g} \times \mathfrak{g} \to \mathfrak{g}$$

which is bilinear, antisymmetric and satifies the *Jacobi identity*, namely for all $x, y, z \in \mathfrak{g}$,

$$[x, [y, z]] = [[x, y], z] + [y, [x, z]].$$

For example, if A is any associative k-algebra then A is a Lie algebra if we define

$$[a,b] = ab - ba$$

for all $a, b \in A$. In particular, when $A = M_n(k)$, we write this as $\mathfrak{gl}(n,k)$.

The *universal enveloping algebra* of the Lie algebra $\mathfrak{g}$ is the factor algebra of the tensor algebra $T(\mathfrak{g})$ by the ideal

$$I(\mathfrak{g}) =< [x,y] - xy + yx : x, y \in \mathfrak{g} >$$

There is a bijective correspondence between left $U(\mathfrak{g})$-modules and representations of the Lie algebra $\mathfrak{g}$, where the latter are - by definition - Lie algebra homomorphisms

$$\rho : \mathfrak{g} \to \operatorname{End}(V)$$

for k-vector spaces V.

Special case (A): Let $n \geq 1$, $\mathfrak{g} = \sum_{i=1}^{n} {}^{\oplus} k x_i$ with $[x_i, x_j] = 0$ for all i, j. Then

$$U(\mathfrak{g}) \cong k[x_1, \ldots, x_n],$$

the commutative polynomial algebra.

Special case (B): Let $n \geq 2$, and let $\mathfrak{sl}(n,k)$ be the space of all $n \times n$ matrices of trace 0. This is a Lie algebra called the *special linear Lie algebra.*

Special case (C): $\mathfrak{sl}(2,k)$ is 3-dimensional, with usual basis

$$e = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, f = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, h = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Check: $[h,e] = 2e, [h,f] = -2f, [e,f] = h$, so

$$I(\mathfrak{sl}(2,k)) =< he - e(h+2), hf - f(h-2), ef - fe - h > .$$

It's easy to check that $U(\mathfrak{sl}(2,k))$ has k-basis

$$\{e^i h^j f^t : i, j, t \geq 0\}.$$

This is a special case of the

Theorem (Poincaré-Birkhoff-Witt). *If $\mathfrak{g}$ is a Lie algebra with k-basis $\{x_1, \ldots, x_n\}$ then $U(\mathfrak{g})$ has k-basis $\{x_1^{t_1} x_2^{t_2} \cdots x_n^{t_n} : t_i \geq 0\}$.*

Fact. $U(\mathfrak{g})$ is a bialgebra for all Lie algebras $\mathfrak{g}$, with

$$\triangle(x) = x \otimes 1 + 1 \otimes X$$

and

$$\varepsilon(x) = 0$$

for all $x \in \mathfrak{g}$.

Proof. We know $U(\mathfrak{g}) = T(\mathfrak{g})/I(\mathfrak{g})$, and $T(\mathfrak{g})$ is a bialgebra with the same definitions of $\triangle$ and ε. So we only need to check (thanks to Lemma 2.2(2)) that $I(\mathfrak{g})$ is a biideal, that is

$$\triangle(t) \in T(\mathfrak{g}) \otimes I(\mathfrak{g}) + I(\mathfrak{g}) \otimes T(\mathfrak{g})$$

for all $t \in I(\mathfrak{g})$ and that $\varepsilon(t) = 0$ for all $t \in I(\mathfrak{g})$. Because the maps are algebra homomorphisms, we only need to do the check for t a generator of $I(\mathfrak{g})$. It's easy to do this. □

(4) **Opposite algebras and coalgebras**: If A is any k-algebra, the *opposite algebra* of A, denoted A^{op}, is the same vector space as A but with new multiplication

$$a \cdot b = ba$$

for all $a, b \in A$. Similarly, if C is a coalgebra, the *opposite coalgebra*, C^{cop}, is the same k-vector space as C, but with

$$\triangle_{C^{\mathrm{cop}}} := \tau \circ \triangle_C,$$

where $\tau =$ is the flip. If B is a bialgebra, then it's easy to check that B^{op}, B^{cop} and B^{opcop} are all bialgebras.

Definition. A co- or bialgebra A is called *cocommutative* if $A^{\mathrm{cop}} = A$, that is, if

$$\triangle = \tau \circ \triangle.$$

So all the bialgebras so far introduced are cocommutative.

2.4. **Sweedler notation.** Let C be a coalgebra. For $c \in C$, we write

$$\triangle(c) = \sum c_1 \otimes c_2.$$

Consider associativity: expressed using the above, it says

$$(\mathrm{id} \otimes \triangle) \circ \triangle(c) = (\mathrm{id} \otimes \triangle)\left(\sum c_1 \otimes c_2\right) = \sum c_1 \otimes c_{21} \otimes c_{22}$$

should equal

$$\sum c_{11} \otimes c_{12} \otimes c_2.$$

So, we write both of the above simply as

$$\sum c_1 \otimes c_2 \otimes c_3. \tag{1}$$

Applying coassociativity to (1), we find that the three expressions

$$\sum \triangle(c_1) \otimes c_2 \otimes c_3, \sum c_1 \otimes \triangle(c_2) \otimes c_3 \text{ and } \sum c_1 \otimes c_2 \otimes \triangle(c_3)$$

are all equal in $C \otimes C \otimes C \otimes C$. We write this as

$$\sum c_1 \otimes c_2 \otimes c_3 \otimes c_4.$$

We use $\triangle_{n-1}$ to denote the iterated application of $\triangle$ as above, so

$$\triangle_{n-1} : C \to C^{\otimes n}.$$

Using Sweedler notation, the second axiom in (1.2) says that for all $c \in C$,

$$c = \sum \varepsilon(c_1)c_2 = \sum c_1\varepsilon(c_2).$$

And C is *cocommutative* $\Leftrightarrow \triangle(c) = \sum c_2 \otimes c_1$ for all $c \in C$.

3. Hopf algebras

3.1. **Definition.** Let $A = (A, m, u, \triangle, \varepsilon)$ be a bialgebra. Then a linear endomorphism S from A to A is an *antipode* for A if the diagram

$$\begin{tikzcd}
A \otimes A \arrow[r, "m"] & A & A \otimes A \arrow[l, "m"] \\
A \otimes A \arrow[u, "\mathrm{id}\otimes S"] & A \arrow[l, "\triangle"] \arrow[r, "\triangle"] \arrow[u, "u\circ\varepsilon"] & A \otimes A \arrow[u, "S\otimes\mathrm{id}"]
\end{tikzcd}$$

commutes. In Sweedler notation, this says that for all $a \in A$,

$$\varepsilon(a) = \sum a_1 S(a_2) = \sum S(a_1)a_2. \tag{2}$$

A *Hopf algebra* is a bialgebra with an antipode. *Morphisms* of Hopf algebras are just bialgebra maps “preserving the antipode” (Exercise 3.5(3)).

Example: Let G be any group, k any field. Then kG is a Hopf algebra if we define

$$S(g) = g^{-1}$$

for all $g \in G$. Since S is linear, it’s enough to check (2) on G: it says that

$$1 = \varepsilon(g) = gg^{-1} = g^{-1}g$$

for all $g \in G$.

3.2. **Convolution product.** Let $A = (A, m, u)$ be an algebra and $C = (C, \Delta, \varepsilon)$ be a coalgebra, over k. Then we can define a product on

$$\mathrm{Hom}_k(C, A)$$

called the *convolution product*, $*$, by: for $f, g \in \mathrm{Hom}_k(C, A)$ and $c \in C$

$$(f * g)(c) = \Sigma f(c_1)g(c_2). \tag{3}$$

Proposition. *With the above notation* $(\mathrm{Hom}_k(C, A), *, u \circ \varepsilon)$ *is an algebra.*

Proof. Associativity of $*$ follows from associativity of the coproduct:

$$\begin{aligned} ((f * g) * h)(c) &= \Sigma f(c_1)g(c_2)h(c_3) \\ &= (f * (g * h))(c). \end{aligned}$$

And $u \circ \varepsilon$ is a left identity element, because for $f \in \mathrm{Hom}_k(C, A)$ and $c \in C$

$$\begin{aligned} ((u \circ \varepsilon) * f)(c) &= \Sigma\varepsilon(c_1)f(c_2) \\ &= (f * (g * h))(c) \\ &= f(c). \end{aligned}$$

Similarly it's a right identity. □

Applying the above when $C = A$ is a bialgebra we get that $(\mathrm{End}_k(A), *, u \circ \varepsilon)$ is an algebra. Comparing Definition 3.1 with (3) we get the first part of

Corollary. *(1) Suppose A is a bialgebra. An antipode S for A is an inverse for $id\,|_A$ in $(\mathrm{End}_k(A), *, u \circ \varepsilon)$.*

(2) If a bialgebra does have an antipode then that antipode is uniquely determined.

Proof. (2) Uniqueness of inverses. □

Corollary. *If $C = (C, \Delta, \varepsilon)$ is any k-coalgebra, then*

$$C^* = \mathrm{Hom}_k(C, k)$$

is an algebra, with

$$(f * g)(c) = \Sigma f(c_1)g(c)_2.$$

So C^* is commutative if and only if C is cocommutative.

Remark. We might expect that given an algebra $A = (A, m, u)$ we can dually get a coalgebra structure on A^*. Indeed we might define, for $f, g \in A^*$

$$\varepsilon(f) = f(1_A)\ (= u^*(f))$$

and

$$\Delta(f) \in A^* \otimes A^*$$

given by

$$\Delta(f)(x \otimes y)) = f(xy).$$

But notice that this gives us $\Delta(f) \in (A \otimes A)^*$ and if $\dim_k A = \infty$ then $A^* \otimes A^* \subsetneqq (A \otimes A)^*$. However, everything works if $\dim_k A < \infty$, and it can be repaired in general, as we'll discuss later.

3.3. **Properties of the antipode.**

Theorem. *Let $H = (H, m, \Delta, u, \varepsilon, S)$ be a Hopf algebra. Then S is a bialgebra homomorphism from H to H^{opcop}. That is, for all $x, y \in H$*

$$S(x, y) = S(y)S(x), \qquad S(1) = 1 \tag{4}$$

and

$$(S \otimes S) \circ \Delta = S, \qquad \varepsilon \circ S = \varepsilon; \tag{5}$$

that is, $\Delta S(x_2) \otimes S(x_1) = \Sigma (Sx)_1 (Sx)_2$.

Proof. Note that $H \otimes H$ is a coalgebra by 2.1, Note (1) with

$$\Delta_{H \otimes H}(x \otimes y) = \Sigma (x_1 \otimes y_1) \otimes (x_2 \otimes y_2). \tag{6}$$

So by proposition 3.2, $\mathrm{Hom}_k(H \otimes H, H)$ is an algebra. Define maps ν and ρ in $\mathrm{Hom}_k(H \otimes H, H)$ by

$$\begin{aligned} \mu(x \otimes y) &= S(y)S(x) \\ \rho(x \otimes y) &= S(xy). \end{aligned}$$

We shall show that $\mu = \rho$ by proving that

$$\rho * m = m * \mu = u \circ \varepsilon \tag{7}$$

where m is multiplication in H. This will do it! Well, take $x, y \in H$. Then

$$\begin{aligned} \rho * m(x \otimes y) &= \Sigma \rho((x \otimes y)_1) m((x \otimes y)_2) \\ &= \Sigma \rho(x_1 \otimes y_1) m(x_2 \otimes y_2) \\ &= \Sigma (x_1 y_1) x_2 y_2 \\ &= \Sigma S((xy)_1)(xy)_2 \qquad \text{since } \Delta \text{ is an algebra homomorphism} \\ &= u \circ \varepsilon(x \otimes y), \end{aligned}$$

noting that ε on $H \otimes H$ is just $\varepsilon \otimes \varepsilon$. Similarly

$$\begin{aligned} (m * \mu)(x \otimes y) &= \Sigma m((x \otimes y)_1) \mu((x \otimes y)_2) \\ &= \Sigma x_1 y_1 S(y_2) S(x_2) \qquad \text{by (6) and definition of } \mu \\ &= \Sigma x_1 (\Sigma y_1 S(y_2)) S(x_2) \\ &= \Sigma S((xy)_1)(xy)_2 \\ &= u \circ \varepsilon(x \otimes y). \end{aligned}$$

This proves (7). If we apply corollary 3.2 (1) to $id * S = u \circ \varepsilon$, giving in particular, $S(1) = 1$.
(5) is proved similarly - Exercise 3.5 (1). □

Definition. A map of rings $\theta : R \to S$ which satisfies $\theta(rt) = \theta(t)\theta(r)$ for all $r, t \in R$ is called an *anti-homomorphism.*

Analogous to lemma 1 we now have

Corollary. *Let* $A = k < \mathcal{B} >$ *be a bialgebra. Let* $S : A \to A^{op}$ *be an algebra homomorphism. To check that* S *is an antipode for* A*, it's enough to check (2) for* $a \in \mathcal{B}$*.*

Proof. Exercise (3.5)(2). □

3.4. **More examples of Hopf algebras.** 1. **The tensor algebra** $T(V)$ Define Δ, ε as in 2.3 (2). Define an antihomomorphism

$$\begin{array}{rcl} S : T(V) & \longrightarrow & T(V) \\ v & \longmapsto & -v. \end{array}$$

For $v \in V$, $\varepsilon(v) = 0$ while

$$\Sigma v_1 S(v_2) = v \cdot 1 + 1 \cdot (-v) = v - v = 0 = \varepsilon(v).$$

Same for $\Sigma S(v_1)v_2$. So $T(V)$ is a Hopf algebra.

2. Let $\mathfrak{g}$ be a Lie algebra and recall that $U(\mathfrak{g}) := T(\mathfrak{g})/I(\mathfrak{g})$ as in 2.3 (3). For $x, y \in \mathfrak{g}$, we see that

$$\begin{array}{rcl} S([x,y] - xy + yx) & = & -[x,y] - (-y)(-x) + (-x)(-y) \\ & = & -([x,y] + yx - xy) \in I(\mathfrak{g}). \end{array}$$

So S induces an antiautomorphism of $U(\mathfrak{g})$ satisfying definition 3.1. So $U(\mathfrak{g})$ is a Hopf algebra.

3. **A finite dimensional noncommutative, non cocommutative Hopf Algebra.** Assume char$k \neq 2$. Let $< g >$ be a cyclic group of order 2. Take $R = k[x]/ < x^2 >$ and let $g \in \mathrm{Aut}_{k-alg}(R)$ by $g(x) = -x$. Form $H = R* < g >$, the skew group ring. So $gx = -xg$. So:
(i) $\dim_k H = 4$, with basis $\{1, g, x, xg\}$.
(ii) H is the factor of the free algebra $F = k < \hat{g}, \hat{x} >$ by the ideal $< \hat{g}^2 - 1, \hat{x}^2, \hat{g}\hat{x} + \hat{x}\hat{g} >= I$.
(iii) H is a bialgebra with

$$\begin{array}{rcll} \Delta(g) & = & g \otimes g, & \varepsilon(g) = 1, \\ \Delta(x) & = & x \otimes 1 + g \otimes x, & \varepsilon(g) = 0. \end{array}$$

Proof. (iii): Freeness of F allows us to define

$$\hat{\Delta} : F \to H \otimes H, \qquad \text{and} \qquad \hat{\varepsilon} : F \to k$$

by lifting the definitions of Δ and ε. Check routinely that $\hat{\Delta}(I) = 0 = \hat{\varepsilon}(I)$, so the maps factor through H. The diagrams in Definition 1.2 are easy to check. □

(iv) H is a Hopf algebra, if we define

$$S(g) = g, \qquad S(x) = -gx \quad \text{and} \qquad S(xg) = S(g)S(x) = g(-gx) = -x.$$

Proof. Define $\hat{S} : F \to H^{op}$ by lifting our proposed definitions for $S(g)$, $S(x)$ to $\hat{S}(\hat{g})$, $\hat{S}(\hat{x})$. Check that $\hat{S}(I) = 0$, so we get antihomomorphism $H \to H$ as we want. Finally

$$\begin{aligned}
m \circ (S \otimes id) \circ \Delta(x) &= m \circ (S \otimes id)(x \otimes 1 + g \otimes x) \\
&= m(-gx \otimes 1 + g \otimes x) \\
&= -gx + gx \\
&= 0 \\
&= \varepsilon(0).
\end{aligned}$$

□

Notes. (1) S has order 4 in this example.

(2) Taft generalised Example 3 to give an infinite series H_n of Hopf algebras of dimension n^2, $(n \geq 2)$ in 1971. See Exercise (3.5)(7).

3.5. **Further properties of the antipode.** In general, the antipode S is *not* bijective, for a Hopf algebra H - there are examples due to Takeuchi (1971). But there are positive cases:

(a) If $\dim_k H < \infty$, then S is bijective [Larson and Sweedler, 1971];

(a′) [Larson, 1976] In fact, if $\dim_k H < \infty$ then S has finite order (but there does not exist a global bound on possible orders (see Exercises(3.6)(7)));

(b) If H is commutative or cocommutative, then $S^2 = \mathrm{id}_H$;

(c) [Skryabin, 2006] If H is noetherian and is either semiprime or satisfies a polynomial identity then S is bijective.

Conjecture (Skryabin)**.** *If H is noetherian then S is bijective.*

We'll prove (b):

Theorem. *Let H be a Hopf algebra. Then the following are equivalent:*

(i) $S^2 = id$;

(ii) for all $x \in H, \sum S(x_2)x_1 = \varepsilon(x)1_H$;

(iii) for all $x \in H, \sum x_2 S(x_1) = \varepsilon(x)1_H$.

Proof. (ii) ⇒ (i): Suppose (ii). It's enough to prove that S^2 is right convolution inverse to S, by Corollary 3.2A(i). Let $x \in H$. Then

$$\begin{aligned}
S * S^2(x) &= \sum S(x_1)S^2(x_2) = S\left(\sum S(x_2)x_1\right) \qquad \text{by Theorem 3.3(1)} \\
&= S(\varepsilon(x)1_H) = \varepsilon(x)1_H \qquad \text{by Theorem 3.3(2).}
\end{aligned}$$

So $S^2 = \mathrm{id}_H$.

(i) ⇒ (ii): Suppose $S^2 = \mathrm{id}_H$. Let $x \in H$. Then

$$\begin{aligned}
\sum S(x_2)x_1 &= S^2\left(\sum S(x_2)x_1\right) = S\left(\sum S(x_1)S^2(x_2)\right) \qquad 3.3(1) \\
&= S\left(\sum S(x_1)x_2\right) = S(\varepsilon(x)1_h) \qquad \text{by definition of antipode} \\
&= \varepsilon(x)1_H \qquad \text{by 3.3(2).}
\end{aligned}$$

(i) $\Leftrightarrow$ (iii) Similar. □

Corollary (A)**.** *If H is commutative or cocommutative, then $S^2 = id_H$.*

Corollary (B)**.** *Let $H = (H, m, u, \Delta, \varepsilon, S)$ be a Hopf algebra. Then*

(i) $H^{opcop} = (H, m_{op}, u, \Delta^{op}, \varepsilon, S)$ is another Hopf algebra;

(ii) $S : H \to H^{opcop}$ is a Hopf algebra morphism;

(iii) Suppose S is bijective. Then $H^{op} = (H, m_{op}, u, \Delta, \varepsilon, S^{-1})$ and $H^{cop} = (H, m, u, \Delta^{op}, \varepsilon, S^{-1})$ are isomorphic Hopf algebras, the isomorphism being given by S.

Proof. (i) In (2.3)(4) we saw that H^{opcop} is a bialgebra. 3.1(1) translated into statements about H^{opcop} ensures that S is an antipode for H^{opcop}.
(ii) From Theorem 3.3.
(iii) We know that H^{op} and H^{cop} are bialgebras, isomorphic via S thanks to Theorem 3.3.

For $a \in H^{\mathrm{op}}$ (writing $\cdot$ for m_{op}, $\times$ for m),

$$\sum a_1 \cdot S^{-1}(a_2) = \sum S^{-1}(a_2) \times a_1.$$

Applying S to the right hand side, we get

$$\sum S(a_1) \times a_2,$$

which is $\varepsilon(a)1_A$ by 3.1(1). So

$$\sum a_1 \cdot S^{-1}(a_2) = \varepsilon(a)1_A.$$

Similarly,

$$\sum S^{-1}(a_1) \cdot a_2 = \varepsilon(a)1_A.$$

For H^{cop}, the argument is similar. □

3.6. **The Hopf dual.** Our aim here is to obtain a dual result to Corollary B of (3.2). The key definition is:

Definition. Let A be any k-algebra. The *finite dual* or *restricted dual* of A is

$$A^{\mathrm{o}} = \{f \in A^* : f(I) = 0 \text{ for some } I \lhd A \text{ with } \dim_k(A/I) < \infty\}.$$

In Chapter 5 we'll prove:

Theorem. *Let $A = (A, m, u)$ be a k-algebra.*

(i) A^o is a coalgebra with coproduct $m^* = \Delta$. That is, for $f \in A^o, x, y \in A$,

$$\Delta(f)(x \otimes y) := f(xy).$$

The counit of A^o is $\varepsilon = u^*$ - that is,

$$\varepsilon(f) = f(1_A).$$

(ii) If $B = (B, m, u, \Delta, \varepsilon)$ is a bialgebra, then so is B^o,

$$B^o = (B^o, \Delta^*, \varepsilon^*, m^*, u^*);$$

(so e.g. $\Delta^* : B^o \otimes B^o \to B^o : f \otimes g \mapsto f \cdot g$, where

$$f \cdot g(x) = \sum f(x_1)g(x_2).$$

(iii) If additionally B is a Hopf algebra with antipode S, then B^o is a Hopf algebra with antipode S^* (so $S^*(f) = f \circ S$).

Of course, if B is commutative, then $B^{\rm o}$ is cocommutative and if B is cocommutative, then $B^{\rm o}$ is commutative. Are the converses of these statements true?

Example. Let k be any field and G any finite group. Then

$$(kG)^* = kG^{\rm o} = \mathrm{Hom}_k(kG, k).$$

We can take as k-basis for $kG^{\rm o}$ the dual basis $\{\rho_g : g \in G\}$, so

$$\rho_g(h) = \delta_{g,h}, \qquad g, h, \in G.$$

Then

$$\Delta(\rho_g) = \sum_{uw=g} \rho_u \otimes \rho_w \qquad \text{where } u, w \in G,$$

and for $f, h \in kG^{\rm o}$ and $x \in G$,

$$(fh)(x) = f(x)h(x).$$

So we find that $\rho_g \rho_h = \delta_{g,h}\rho_g$ and as a k-algebra, $kG^{\rm o}$ is the direct sum of $|G|$ copies of k.

4. Modules and comodules

4.1. To dualise it, we quickly recall the definition of a left *module* M over a k-algebra A: it's a k-vector space with a k-linear map $\lambda : A \otimes M \to M$ such that

$$\begin{tikzcd}
A \otimes A \otimes M \arrow[r, "\mathrm{id}\otimes\lambda"] \arrow[d, "m\otimes\mathrm{id}_M"'] & A \otimes M \arrow[d, "\lambda"] \\
A \otimes M \arrow[r, "\lambda"'] & M
\end{tikzcd}$$

and

$$\begin{tikzcd}
k \otimes M \arrow[r, "u\otimes\mathrm{id}"] \arrow[dr, "s"'] & A \otimes M \arrow[d, "\lambda"] \\
& M
\end{tikzcd}$$

commute, where s is scalar multiplication.

4.2. Comodules. Let C be a coalgebra. A *right comodule* M over C is a k-vector space M and a linear map $\rho : M \to M \otimes C$ such that

$$\begin{tikzcd} M \arrow[r, "\rho"] \arrow[d, "\rho"'] & M \otimes C \arrow[d, "\mathrm{id}_M \otimes \Delta"] \\ M \otimes C \arrow[r, "\rho \otimes \mathrm{id}"'] & M \otimes C \otimes C \end{tikzcd}$$

and

$$\begin{tikzcd} M \arrow[r, "\rho"] \arrow[dr, "- \otimes 1"'] & M \otimes C \arrow[d, "\mathrm{id} \otimes \varepsilon"] \\ & M \end{tikzcd}$$

commute.

Left comodules are defined analogously.

A morphism of right comodules $f : M \to N$ over C is a linear map such that

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "\rho_M"'] & N \arrow[d, "\rho_N"] \\ M \otimes C \arrow[r, "f \otimes \mathrm{id}"'] & N \otimes C \end{tikzcd}$$

commutes.

4.3. Duality.

Proposition. *(i) Let M be a right comodule for the coalgebra C. Then M is a left module for C^*.*

(ii) Let A be an algebra and M a left A-module. Then M is a right A^o-comodule (in the sense that $A \to A^{o*}$ and part (1) coupled with restriction retrieves M) $\Leftrightarrow$ for all $m \in M$, $dim_k(Am) < \infty$.

Proof. (i) Let $\rho : M \to M \otimes C$ be the comodule map, so

$$\rho(m) = \sum m_0 \otimes m_1,$$

where $m \in M, m_0 \in M, m_1 \in C$. Let $f \in C^*$ and define

$$f \cdot m = \sum \langle f, m_1 \rangle m_0,$$

where we write $\langle f, m_1 \rangle$ for $f(m_1)$.

Thus, if $g, f \in C^*$ and $m \in M$, we have

$$g \cdot (f \cdot m) = g \cdot \left(\sum \langle f, m_1 \rangle m_0 \right) = \sum \langle f, m_2 \rangle \langle g, m_1 \rangle m_0;$$

whereas, using 4.2(1),

$$(g * f) \cdot m = \sum \langle g * f, m_1 \rangle m_0 = \sum \langle g, m_1 \rangle \langle f, m_2 \rangle m_0.$$

And $\varepsilon \cdot m = \sum \varepsilon(m_1) m_0 = m$ by 4.2(2).

(ii) $\Leftarrow$: Suppose M is a left A-module such that $\dim_k(Am) < \infty$, for all $m \in M$. For $m \in M$, choose a k-basis $m_1, m_2, \ldots, m_n$ for Am. Define $f_i \in A^*$ for $i = 1, \ldots, n$ by the rule

$$a \cdot m = \sum_{i=1}^{n} f_i(a) m_i.$$

The kernel I of the algebra homomorphism $A \to \mathrm{End}_k(Am)$ has finite codimension in A, and $f(I) = 0$ for all $i = 1, \ldots, n$. So $f_i \in A^{\mathrm{o}}$ for all i.

Define a right coaction $\rho : M \to M \otimes A^{\mathrm{o}}$ by

$$\rho(m) = \sum_{i=1}^{n} m_i \otimes f_i. \tag{8}$$

One checks that (8) is independent of the choices made and makes M into a right A^{o}-comodule. To see this, note that for *any* left A-module $\hat{M}$, we have a well-defined linear map

$$\hat{\rho} : \hat{M} \hookrightarrow \mathrm{Hom}_k(A, \hat{M});$$

where $\hat{\rho}(\hat{m})(a) := a \cdot \hat{m}$. And

$$\hat{M} \otimes A^{\mathrm{o}} \subseteq \mathrm{Hom}_k(A, \hat{M}),$$

via $(\hat{m} \otimes a^{\mathrm{o}})(a) = \langle a^{\mathrm{o}}, a \rangle \hat{m}$. The condition that $\dim_k A \cdot m < \infty$ for all $m \in \hat{M}$ simply ensures that $\mathrm{im}\, \hat{\rho} \subseteq \hat{M} \otimes A^{\mathrm{o}}$, so ρ in (8) is the same as $\hat{\rho}$ and is thus well-defined.

$\Rightarrow$: This follows from what we've done, because if M is a right A^{o}-comodule via $\rho(m) = \sum m_0 \otimes m_1$, then $A \cdot m$ is spanned by the $\{m_0\}$. □

Definition. An A-module M with $\dim_k Am < \infty$ for all $m \in M$ is called *rational.*

4.4. Examples of modules and comodules. (1) If C is any coalgebra, then C is a right (or left) comodule, using Δ.

(2) Let G be a group, $C = kG$. A k-vector space, M is a right kG-module if and only if M is a G-graded vector space. (Exercise 4.6 (2)).

(3) Let C be a coalgebra, so C is a right C-comodule by (1). Proposition 4.3(1) tells us that C is a *left C^*-module* with, for $f \in C^*$, $c \in C$,

$$f \rightharpoonup c = \Sigma \langle f, c_2 \rangle c_1.$$

This is often called the *left hit action* of C^* on C. The *right hit action* is

$$c \leftharpoonup f = \Sigma \langle f, c_1 \rangle c_2.$$

These are (respectively) the transposes of right and left multiplication in C^*, (Exercise 4.6(3)).

(4) Analogously to (3), if A is any k-algebra, we can define a left action of A on A^*, which is the transpose of right multiplication on A. That is, for $a \in A$ and $f \in A^*$, $a \rightharpoonup f$ is defined for $b \in A$ by

$$\langle a \rightharpoonup f, b \rangle = \langle f, ba \rangle.$$

Similarly for $f \leftharpoondown a$.

Suppose $f \in A^o$. Then by Theorem 3.6 (still to be proved), A^o is a coalgebra, so Δf makes sense for f and

$$\begin{aligned} \langle a \rightharpoonup f, b\rangle &= \langle f_1, ba\rangle \\ &= \Sigma\langle f_1, b\rangle\langle f_2, a\rangle. \end{aligned}$$

So $a \rightharpoonup f = \Sigma\langle f_2, a\rangle f_1$.

4.5. Tensor products and hom spaces. (1) **Tensor products of modules:** Let A be a bialgebra, and let V and W be left A-modules. Then $V \otimes W$ is a left A-module via

$$a.(v \otimes w) = \sum a_1 v \otimes a_2 w.$$

If X is a third module for A, then coassociativity ensures that

$$(V \otimes W) \otimes X \cong V \otimes (W \otimes X).$$

Also we have the trivial left A-module, k (given by $a.v = \varepsilon(a)v$ for $a \in A$ and $v \in k$), and

$$V \otimes k \cong V \cong k \otimes V.$$

as left A-modules.

If A is cocommutative then obviously

$$V \otimes W \cong W \otimes V$$

as left A-modules, with the isomorphism given by the flip $\tau : v \otimes w \mapsto w \otimes v$. But if A is not cocommutative, this will fail in general.

Example. Let $A = (kG)^*$ where G is any non-abelian finite group. By (3.7)

$$\begin{aligned} (kG)^* &= \sum_{g\in G}^{\oplus} kp_g \\ &= k \oplus \cdots \oplus k \end{aligned}$$

($|G|$ copies of k), as k-algebras, with

$$\Delta p_g = \sum_{u,v \;\; uv=g} p_u \otimes p_v \tag{9}$$

A has exactly $|G|$ simple modules $\{V_g \cong k : g \in G\}$ where for $g, h \in G$ and $v \in V_g$

$$p_h v = \delta_{g,h} v.$$

Now take $g, h \in G$, and form

$$V_g \otimes V_h;$$

using (9) we see that

$$V_g \otimes V_h \cong V_{gh}$$

so if $gh \neq hg$ then

$$V_g \otimes V_h \ncong V_h \otimes V_g.$$

(2) **Homomorphisms of modules:** Let H be a Hopf algebra and let V and W be left H-modules. Then

$$\operatorname{Hom}_k(V, W)$$

is a left H-module with action

$$(h.f)(v) = \sum h_1 f((Sh_2)v)$$

for $h \in H, f \in \operatorname{Hom}_k(V, W)$ (Exercise 4.6 (6)). An important case is when W is the trivial module k, which yields a left H-module structure on V^*, namely

$$h.f = f(S(h)).$$

(3) **Tensor products of comodules:** If B is a bialgebra and V and W are right B-comodules, then $V \otimes W$ is a right comodule via

$$v \otimes w \mapsto \sum v_0 \otimes w_0 \otimes v_1 w_1.$$

Check that this works. If B is commutative then $V \otimes W \cong W \otimes V$ as comodules, via the flip map (Ex 4.6(7)).

5. The Hopf dual

5.1. In Chapter 5 we prove Theorem 3.6, which said

(i) (A, m, u) an algebra $\Rightarrow (A^{\text{o}}, m^*, \varepsilon = u^*)$ is a coalgebra;

(ii) B a bialgebra, $\Rightarrow B^{\text{o}}$ is a bialgebra

(iii) H a Hopf algebra $\Rightarrow H^{\text{o}}$ is a Hopf algebra.

The key step is (i) and here we need to show that if $f \in A^{\text{o}}$ then

$$m^* f \in A^{\text{o}} \otimes A^{\text{o}}$$

where

$$m^* f(x \otimes y) = f(xy)$$

for $x, y \in A$. For this we need

Lemma 3. *Let (A, m, u) be a k-algebra, $f \in A^*$. Then the following are equivalent:*
(a) $f(I) = 0$ for some $I \lhd_r A$, $\dim_k(A/I) < \infty$;
(b) $f(I) = 0$ for some $I \lhd_l A$, $\dim_k(A/I) < \infty$;
(c) $f(I) = 0$ for some $I \lhd A$, $\dim_k(A/I) < \infty$;
(d) $\dim_k(A \rightharpoonup f) < \infty$;
(e) $\dim_k(f \leftharpoonup A) < \infty$;
(f) $\dim_k(A \rightharpoonup f \leftharpoonup A) < \infty$;
(g) $m^* f \in A^* \otimes A^*$.

Proof. (Sketch) Recall $(a \rightharpoonup f)(b) = f(ba)$, $(f \leftharpoonup a)(b) = f(ab)$ for $a, b \in A, f \in A^*$.

(a)$\Rightarrow$(d): Supppose (a), with $\langle f, I\rangle = 0$, $I \lhd_r A$. For all $a \in A$,

$$\langle a \rightharpoonup f, I\rangle = \langle f, Ia\rangle \subseteq \langle f, I\rangle = 0.$$

Thus $A \rightharpoonup f \subseteq (A/I)^*$ and so (d) holds.

(d)⇒(a): Suppose $\dim_k(A \rightharpoonup f) < \infty$. Set $I = \{b \in A : \langle A \rightharpoonup f, b\rangle = 0\}$. If $a \in A$ and $b \in I$ then

$$\begin{aligned} \langle A \rightharpoonup f, ba\rangle &= \langle aA \rightharpoonup f, b\rangle \\ &\subseteq \langle A \rightharpoonup f, b\rangle = 0 \end{aligned}$$

So $I \lhd_r A$. Since I is the kernel of the restriction map from A to $(A \rightharpoonup f)^*$, $\dim_k(A/I) < \infty$. Since $f(I) = 0$ we are done.

(b)⇔(e) and (c)⇔(f) are similar. (c)⇒(a) and (c)⇒(b) are trivial.

(b)⇒(c): Let $f(I) = 0$, $I \lhd_l A, \dim_k(A/I) < \infty$. There is an algebra homomorphism $\rho : A \to \mathrm{End}_k(A/I)$ whose kernel J has finite dimension since $\dim_k \mathrm{End}_k(A/I) < \infty$. And $J = \{a \in A : aA \subset I\} \subseteq \{a \in A : a1 \in I\} = I$. Thus $f(J) = 0$ and so (c) holds. Similarly (a)⇒(c), so (a)-(f) are equivalent.

(d)⇒(g): Suppose (d) and fix a basis $\{g_1, \dots, g_n\}$ for $A \rightharpoonup f$. So, for $a \in A$,

$$a \rightharpoonup f = \sum_{i=1}^{n} h_i(a) g_i,$$

where one checks easily that $h_i \in A^*$, $1 \le i \le n$. Now for $b \in A$,

$$\begin{aligned} \langle m^* f, b \otimes a\rangle &= \langle f, ba\rangle \\ &= \langle a \rightharpoonup f, b\rangle \\ &= \sum_{i=1}^{n} h_i(a) g_i(b). \end{aligned}$$

Therefore

$$m^* f = \sum_{i=1}^{n} g_i \otimes h_i \in A^* \otimes A^*.$$

(g)⇒(d): If (g) holds, there exist $g_i, h_i \in A^*$ with $m^* f = \sum_{i=1}^{n} g_i \otimes h_i$. The calculation just done shows that for all $a \in A$,

$$a \rightharpoonup f = \sum_{i=1}^{n} h_i(a) g_i \in \sum_{i=1}^{n} k g_i$$

so $\dim_k(A \rightharpoonup f) < \infty$. □

5.2. Proof of 3.6(i). Assume (A, m, u) is an algebra. We prove that

$$m^* A^{\circ} \subseteq A^{\circ} \otimes A^{\circ}.$$

This will prove that A° is a coalgebra. Let $f \in A^{\circ}$ so there exists $I \lhd A$ with $\dim_k(A/I) < \infty$ such that $f(I) = 0$. Then

$$I \otimes A + A \otimes I$$

is an ideal of $A \otimes A$ and it has finite codimension, because it's the kernel of the algebra homomorphism $\pi : A \otimes A \to A/I \otimes A/I$. Now if α is any element of $I \otimes A + A \otimes I$, then

$$m^* f(\alpha) = 0.$$

This shows that $m^*f \in (A \otimes A)^{\mathrm{o}}$. Indeed m^*f factors through $A/I \otimes A/I$:

$$\begin{tikzcd}
A \otimes A \arrow[rr, "m^*f"] \arrow[dr, "\pi"'] & & k . \\
& A/I \otimes A/I \arrow[ur, "\overline{m * f}"'] &
\end{tikzcd}$$

Otherwise put, we can write m^*f as $\sum_{i=1}^n g_i \otimes h_i$, where $g_i, h_i \in A^*$ and $I \subseteq \ker g_i$ and $I \subseteq \ker h_i$, for all i. Thus $m^*f \in A^{\mathrm{o}} \otimes A^{\mathrm{o}}$. Now coassociativity follows by restriction of the commutative diagram

$$\begin{tikzcd}
A^* \arrow[r, "m^*"] \arrow[d, "m^*"'] & (A \otimes A)^* \arrow[d, "(id \otimes m)^*"] \\
(A \otimes A)^* \arrow[r, "(m \otimes id)^*"] & (A \otimes A \otimes A)^*
\end{tikzcd}$$

which is itself commutative because it's the dual of associativity in A. And one easily checks that $\varepsilon = u^*$ satisfies the counit property.

5.3. Proof of 3.6 (ii),(iii). Suppose first that

$$B = (B, m, u, \Delta, \varepsilon)$$

is a bialgebra. By (3.2) Corollary B,

$$(B^*, \Delta^*, \varepsilon^*)$$

is an algebra. And

$$(B^{\mathrm{o}}, m^*, u^*) \text{ is a coalgebra.} \tag{10}$$

by Theorem 3.6(i), just proved. We claim:

$$B^{\mathrm{o}} \textit{ is a subalgebra of } B^*. \tag{11}$$

Well, take $f, g \in B^{\mathrm{o}}$, so that Lemma 5.1 ensures

$$\dim_k(B \rightharpoonup f) < \infty, \ \ dim_k(B \rightharpoonup g) < \infty. \tag{12}$$

Now let $x, y \in B$. Then $fg \in B^*$ (convolution product), and

$$\begin{aligned}
\langle x \rightharpoonup fg, y\rangle &= \langle fg, yx\rangle \\
&= \sum \langle f, (yx)_1\rangle\langle g, (yx)_2\rangle \\
&= \sum \langle f, y_1x_1\rangle\langle g, y_2x_2\rangle \text{ since } \Delta \text{ is an algebra hom,} \\
&= \sum \langle x_1 \rightharpoonup f, y_1\rangle\langle x_2 \rightharpoonup g, y_2\rangle \\
&= \sum \langle (x_1 \rightharpoonup f)(x_2 \rightharpoonup g), y\rangle. \qquad (13)
\end{aligned}$$

So (12) and (13) imply that

$$\dim_k(B \rightharpoonup fg) \leq dim_k(B \rightharpoonup f)(B \rightharpoonup f) < \infty,$$

proving (11). Also, $\varepsilon \in B^{\circ}$, since $\dim_k(B/\ker\varepsilon) = 1$. So

$$(B^{\circ}, \Delta^*, \varepsilon^*) \text{ is an algebra.} \tag{14}$$

Now (ii) follows from (10) and (14) after we check the bialgebra commutative diagrams; these follow at once by dualizing the ones for B (Exercise 5.4(3)).

Suppose finally that S is an antipode for $B = H$. So $S^* : H^* \to H^*$ exists; we have to check that

$$S^* H^{\circ} \subseteq H^{\circ}.$$

Well, let $a \in H$ and $f \in H^*$. Then, for $b \in H$,

$$\begin{aligned}
\langle a \rightharpoonup S^* f, b\rangle &= \langle S^* f, ba\rangle \\
&= \langle f, S(ba)\rangle \\
&= \langle f, S(a)S(b)\rangle \\
&= \langle f \leftharpoonup S(a), S(b)\rangle \\
&= \langle S^*(f \leftharpoonup S(a)), b\rangle.
\end{aligned}$$

Thus

$$H \rightharpoonup S^* f = S^*(f \leftharpoonup SH) \subseteq S^*(f \leftharpoonup H);$$

so if $f \in H^{\circ}$, Lemma 5.1 gives $\dim_k(f \leftharpoonup H) < \infty$, and so Lemma 5.1 again ensures

$$S^* f \in H^{\circ}.$$

Finally, S^* is the convolution inverse for $id_{H^{\circ}}$, as follows easily by dualizing the corresponding property for S and $id|_H$ (Exercise 5.4(4)).

6. Primer on affine algebraic geometry

In order to discuss Hopf algebras arising as the coordinate rings of algebraic groups, we need to recall some basic definitions and ideas from algebraic geometry. We do this in this chapter. Throughout, k will be an algebraically closed field.

6.1. Algebraic sets. For a positive integer n, the set $k^n = \{(a_1, \dots, a_n) : a_i \in k\}$ is called affine n-space, denoted ${\mathbb{A}_k}^n$, or $\mathbb{A}^n$ for short. Elements of $\mathbb{A}^n$ are *points*, the a_i are *coordinates*.

The objects of study are the sets of zeros in $\mathbb{A}^n$ of collections of polynomials. So, for

$$T \subseteq R_n := k[X_1, X_2, \dots, X_n]$$

we write

$$Z(T) = \{\underline{a} \in \mathbb{A}^n : f(\underline{a}) = 0 \ \forall \ f \in T\}.$$

Notice that if $\langle T\rangle$ is the ideal of R_n generated by T, then

$$Z(T) = Z(\langle T\rangle).$$

By the Hilbert Basis Theorem, there is a finite set $f_1, \ldots, f_r$ of polynomials in T such that

$$\langle T \rangle = \sum_{i=1}^{r} f_i R_n,$$

so

$$Z(T) = Z(\{f_1, \ldots, f_r\}).$$

Definition. An *algebraic subset* of $\mathbb{A}^n$ is a subset $Y \subseteq \mathbb{A}^n$ such that $Y = Z(T)$ for some set T of polynomials in R_n.

The gymnastics of algebraic sets starts with

Lemma. *(i) If $T_1 \subseteq T_2 \subseteq R_n$, then*

$$Z(T_2) \subseteq Z(T_1).$$

(ii) The union of two algebraic sets in $\mathbb{A}^n$ is an algebraic set.

(iii) The intersection of any collection of algebraic subsets of $\mathbb{A}^n$ is an algebraic set.

(iv) ϕ and $\mathbb{A}^n$ are algebraic sets.

Proof. (i) is obvious.

(ii) Let $U = Z(T_1)$, $W = Z(T_2)$. Then one checks that $U \cup W = Z(T_1T_2)$, where $T_1T_2 = \{fg : f \in T_1, g \in T_2\}$.]

(iii) Let $U_j = Z(T_j)$ for $j \in \mathcal{I}$. Then

$$\bigcap_j U_j = Z\Big(\bigcup_j T_j\Big).$$

(iv) $\phi = Z(1), \mathbb{A}^n = Z(\{0\})$.

□

6.2. The Zariski topology. In view of the above lemma, we make the

Definition. Define the *Zariski topology* on $\mathbb{A}^n$ by taking the closed sets to be the algebraic sets.

Example. Algebraic subsets of $\mathbb{A}^1$: $R_1 = k[X]$ is a P.I.D., so every closed set in $\mathbb{A}^1$ is the set of zeros of a single polynomial f. Since $k = \overline{k}$, $f = c(X_1 - a_1) \cdots (X_n - a_n)$, $a_i \in k$. Thus the algebraic sets in $\mathbb{A}^1$ are $\phi, \mathbb{A}^1$ and all finite subsets of $\mathbb{A}^1$. Thus any two non-empty open sets have non-empty intersection. In particular $\mathbb{A}^1$ is not Hausdorff.

6.3. Ideals versus algebraic sets (I). We are aiming for a bijection between closed subsets of $\mathbb{A}^n$ and ideals of R_n. But this fails since - for instance - the ideals $\langle X \rangle$ and $\langle X^2 \rangle$ of $k[X] = R$ both define the set $\{0\}$. To fix this, we make the

Definition. An ideal I of a ring R is *semiprime* if whenever an ideal J of R satisfies $J^2 \subseteq I$, then $J \subseteq I$.

Remarks. (i) If R is commutative, then $I \lhd R$ is semiprime $\Leftrightarrow \forall f \in R, \forall t \geq 1, f^t \in I$ only if $f \in I$.

(ii) *Radical* is sometimes used rather than semiprime.

If I is any ideal of a commutative ring R, we define

$$\sqrt{I} = \{g \in R : g^t \in I, \text{ some } t \geq 1\}.$$

Then $\sqrt{I} \lhd R$, with $I \subseteq \sqrt{I}$. Moreover, if $R = R_n$ for some $n \geq 1$, $Z(I) = Z(\sqrt{I})$. For $Z(\sqrt{I}) \subseteq Z(I)$ and if $\underline{a} \in Z(I)$ and $g \in \sqrt{I}$, then

$$g^t(\underline{a}) = g(\underline{a})^t = 0,$$

for some $t \geq 1$, and so $g(\underline{a}) = 0$. Hence $\underline{a} \in Z(\sqrt{I})$.

Now define, for a set Y of points in $\mathbb{A}^n$, the subset

$$\mathcal{I}(Y) = \{f \in R_n : f(y) = 0 \; \forall y \in Y\}.$$

We have the following obvious facts:

Lemma. *(i) $Y \subseteq \mathbb{A}^n \Rightarrow \mathcal{I}(Y) \lhd R_n$, in fact $\mathcal{I}(Y)$ is a semiprime ideal of R_n (using our discussion above);*

(ii) If $Y_1 \subseteq Y_2 \subseteq \mathbb{A}^n$, then $\mathcal{I}(Y_2) \subseteq \mathcal{I}(Y_1)$;

(iii) If $U, W \subseteq \mathbb{A}^n$, then $\mathcal{I}(U \cup W) = \mathcal{I}(U) \cup \mathcal{I}(W)$;

(iv) If $Y \subseteq \mathbb{A}^n$, then $Y \subseteq Z(\mathcal{I}(Y))$;

(v) If $I \lhd R^n$, then $\sqrt{I} \subseteq \mathcal{I}(Z(I))$.

Proof. Easy. □

6.4. Ideals versus algebraic sets (II). In fact, (v) of the lemma is an equality and (iv) is also an equality if we restrict to *closed* sets Y. To see this, we need

Theorem (Hilbert's Nullstellensatz)**.** *Let $I \lhd R_n$ for some $n \geq 1$. Suppose $f \in \mathcal{I}(Z(I))$. Then $f \in \sqrt{I}$ - that is, $f^t \in I$ for some $t \geq 1$.*

Corollary. *Let $n \geq 1$. The correspondences*

$$\begin{tikzcd} \{\textit{algebraic subsets of } \mathbb{A}^n\} \arrow[r, shift left, "\mathcal{I}(-)"] & \{\textit{semiprime ideals of } R_n\} \arrow[l, shift left, "Z(-)"] \end{tikzcd}$$

are 1-1 and order reversing.

Proof. If I is a semiprime ideal, then

$$\mathcal{I}(Z(I)) = I \text{ by Lemma 6.3(v) and the Nullstellensatz.}$$

Let Y be an algebraic subset of $\mathbb{A}^n$. By 6.3(iv),

$$Y \subseteq Z(\mathcal{I}(Y)). \tag{15}$$

But Y is algebraic, so $Y = Z(J)$ for some ideal J of R_n. Then $J \subseteq \mathcal{I}(Y)$, so Lemma 6.1(i) implies

$$Y = Z(J) \supseteq Z(\mathcal{I}(Y)). \tag{16}$$

Thus (15) and (16) give equality. □

Corollary. *Let $n \geq 1$. The maximal ideals of R_n correspond bijectively to the points of $\mathbb{A}^n$. Namely,*

$$\underline{a} = (a_1, \dots, a_n) \rightleftarrows \underline{m}_a = \langle X_1 - a_1, \dots, X_n - a_n \rangle$$

Proof. Clearly, every ideal of the form $\underline{m}_a$ is maximal, since $R_n/\underline{m}_a \cong k$, a field. Conversely, let $\underline{m}$ be *any* maximal ideal of R_n. Apply the Nullstellensatz to $\underline{m}$: we get $\mathcal{I}(Z(\underline{m})) = \underline{m}$. So $Z(\underline{m})$ cannot be the empty set in $\mathbb{A}^n$, so there exists $\underline{a} = (a_1, a_2, \dots, a_n) \in Z(\underline{m})$. Therefore,

$$\langle X_1 - a_1, \dots, X_n - a_n \rangle = \mathcal{I}(\underline{a}) \supseteq \mathcal{I}(Z(\underline{m})) = \underline{m}.$$

Since $\underline{m}$ is a maximal ideal, we conclude $\underline{m} = \underline{m}_a$. □

Otherwise put, this says in particular that each point of $\mathbb{A}^n$ is closed.

Corollary. *Let $I \lhd R_n$, some $n \geq 1$. Then I is semiprime $\Leftrightarrow$ I is the intersection of the maximal ideals in which it is contained.*

Proof. $\Leftarrow$ Easy - Exercise (6.)(5).

$\Rightarrow$ Let $I \lhd R_n$, I semiprime, and set

$$J = \bigcap \{\underline{m} \lhd R_n : \underline{m} \text{ maximal, } I \subseteq \underline{m}\} = \bigcap \{\underline{m}_a : \underline{a} \in Z(I)\} \text{ by Corollary 2.}$$

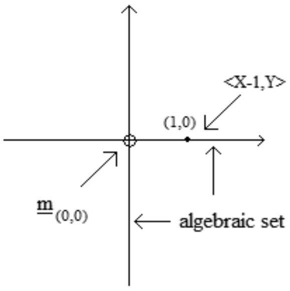
But $J = \mathcal{I}(Z(I))$, which equals I by Corollary 1. So $J = I$. □

Example. The algebraic subsets of ${\mathbb{A}_{\mathbb{C}}}^2$: Here $R_2 = \mathbb{C}[X,Y]$, which is a U.F.D. We have:

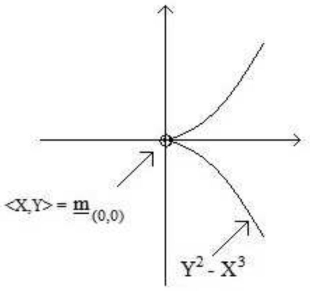
$$\begin{array}{rcl}
\underline{\text{semiprime ideals of}}\ \mathbb{C}[X,Y] & \longleftrightarrow & \underline{\text{algebraic subsets of}}\ \mathbb{A}^2_{\mathbb{C}} \\
\{0\} & \longleftrightarrow & \mathbb{A}^2_{\mathbb{C}} \\
\left\{ \begin{array}{c} \text{finite intersections of maximal ideals,} \\ \bigcap_{i=1}^{t} \underline{m}_{a_i} \end{array} \right\} & \longleftrightarrow & \{\underline{a}_1, \underline{a}_2, \dots, \underline{a}_t\} \\
\mathbb{C}[X,Y] & \longleftrightarrow & \phi \\
\left\{ \begin{array}{c} < f >: f = \prod_{i=1}^{n} f_i, \\ f_i \ \text{irreducible,} \\ f_i \ \text{not an associate of } f_j \ \text{for } i \neq j \end{array} \right\} & \longleftrightarrow & \begin{array}{c} \text{finite } \cup \text{s of irreducible curves,} \\ Y_1 \cup \cdots \cup Y_r \end{array}
\end{array}$$

There are also, of course, the algebraic sets we get by taking the union of finitely many curves with a finite set of points. Two typical examples of (unions of) curves in $\mathbb{A}^2_{\mathbb{C}}$ are shown overleaf.

1. $f = XY$



2. $f = Y^2 - X^3$



6.5. Irreducible components versus prime ideals. Comparing the two examples above: both are connected, but $Z(XY)$ appears to have two "components", $(X^2 - Y^3)$ only one. To make this precise, we need the

Definition. A non-empty subset Y of a topological space X is *irreducible* if, whenever

$$Y = Y_1 \cup Y_2$$

with Y_i closed in Y, $i = 1, 2$, then $Y = Y_1$ or $Y = Y_2$. [i.e. "Y can't be expressed as the union of 2 proper closed subsets"]

Examples. (i) $\mathbb{A}^1$ is irreducible since every proper closed subset is finite.
(ii) Any non-empty open subset of an irreducible space is irreducible and dense (Exercise (6.11)(6))

A Zorn's lemma argument shows that any topological space is the union of its maximal irreducible subspaces (which are always closed by Ex (6.11)(7)). To make this union finite, we need:-

Definition. A topological space X is *noetherian* if it has ACC on open sets (equivalently, DCC on closed sets).

Example. $\mathbb{A}^n$ with the Zariski topology is noetherian, since DCC for closed subsets of $\mathbb{A}^n$ is equivalent to ACC for (semiprime) ideals of $R_n = k[X_1, \ldots, X_n]$ which we get from Hilbert's basis theorem. Of course the same then applies to all algebraic sets.

Proposition. *A noetherian topological space X has only finitely many maximal irreducible subspaces. These are closed and their union in X.*

Proof. Let $\mathcal{A}$ be the collection of finite unions of closed irreducible subsets of X. So e.g. $\emptyset \in \mathcal{A}$.

Suppose $X \notin \mathcal{A}$. Then use the noetherian property to find a closed subset Y of X, *minimal* among closed sets not in $\mathcal{A}$. Clearly, Y is neither $\emptyset$ nor irreducible. So $Y = Y_1 \cup Y_2$ where Y_1, Y_2 are proper closed subsets. Minimality of Y forces each Y_i to be in $\mathcal{A}$, but then $Y \in \mathcal{A}$, a contradiction.

Write

$$X = X_1 \cup X_2 \cup \ldots \cup X_n,$$

X_i irreducible closed subspaces. Let Y be *any* maximal closed irreducible subspace. Then

$$Y = \bigcup_i (Y \cap X_i),$$

so $Y = Y \cap X_i$ for some i, since Y is irreducible. That is, $Y \subseteq X_i$, and then Y maximal forces $Y = X_i$. □

The maximal irreducible subspaces of the noetherian space X are called *irreducible components.*

How do we recognise the irreducible algebraic sets algebraically?

Definition. An ideal P of a ring R is *prime* if and only if, for all ideals A and B of R, $AB \subseteq P \Rightarrow A \subseteq P$ or $B \subseteq P$.

So if R is commutative then P is prime if and only if R/P is an integral domain. Thus P prime $\Rightarrow$ P semiprime.

Lemma. *An algebraic subset Y in $\mathbb{A}^n$ is irreducible if and only if $\mathcal{I}(Y)$ is a prime ideal of R_n.*

Proof. $\Rightarrow$: Suppose Y is irreducible, and let $f, g \in R_n$ with $fg \in \mathcal{I}(Y)$. So if $y \in Y$, $f(y) = 0$ or $g(y) = 0$. Hence

$$Y = (Y \cap Z(f)) \cup (Y \cap Z(g))$$

is a union of closed sets. So Y irreducible forces Y to equal one of these sets, and so

$$Y \subseteq Z(f)$$

say. That is, $f \in \mathcal{I}(Y)$.
$\Leftarrow$: Suppose $Y = A \cup B$, A, B proper closed subsets of Y. Thus there exist $f, g \in R_n$

with $f \in \mathcal{I}(A)$, $f \notin \mathcal{I}(Y)$ and $g \in \mathcal{I}(B)$, $g \notin \mathcal{I}(Y)$. Hence $\mathcal{I}(Y)$ is *not* a prime ideal of R_n. □

Notice that the above lemma and proposition translate to the ring theoretic statement:

If I is any semiprime ideal of R_n, then there are finitely many prime ideals of R_n which are minimal with respect to containing I, say $P_1, P_2, \ldots, P_t$, and then

$$I = P_1 \cap P_2 \cap \cdots \cap P_t$$

e.g. $I = \langle XY \rangle \lhd k[X, Y]$, then

$$P_1 = \langle X \rangle, \;\; P_2 = \langle Y \rangle.$$

Note that $\mathbf{m} = \langle X, Y \rangle$ is the only maximal ideal containing both P_1 and P_2.

In fact, this statement is valid in *any* (not necessarily commutative) noetherian ring.

We can now state

Definition. An *an affine algebraic variety* is an irreducible algebraic subset of $\mathbb{A}^n$ for some n.

6.6. Morphisms. Since our category consists of objects defined by *polynomial* equations, we naturally define the morphism in the category to be polynomial maps. For brevity and simplicity we adopt here a “naive” approach - but really the theory can and should be developed in a way which avoids specific embeddings of varieties in the ambient space $\mathbb{A}^n$ - See e.g. [Hartshorne] or [Humphreys].

Definition (A)**.** Let $X \subseteq \mathbb{A}^n$ be an affine algebraic set. The *(affine) coordinate ring* of X (or *ring of regular functions* on X) is the factor algebra $\mathcal{O}(X) := R_n/\mathcal{I}(X)$ of R_n.

Remarks. (i) $\mathcal{O}(X)$ is the image of R_n under the restriction map from $\mathbb{A}^n$ to X.
(ii) If we give k the Zariski topology then $\mathcal{O}(X)$ consists of continuous maps from X to k. (Exercise (6.11)(11)).

Definition (B)**.** Let $X \subseteq \mathbb{A}^n$, $Y \subseteq \mathbb{A}^m$ be algebraic sets. A *morphism*

$$\phi : X \to Y$$

is a map given by

$$\phi(\mathbf{x}) = (\psi_1(\mathbf{x}), \psi_2(\mathbf{x}), \ldots, \psi_m(\mathbf{x}))$$

for $\mathbf{x} \in X$, where $\psi_i \in \mathcal{O}(X)$ for $i = 1, \ldots, m$.

Remarks. (i) Morphisms $X \to \mathbb{A}^1$ are the same as polynomial functions on X.
(ii) A morphism $\phi : X \to Y$ is continuous for the Zariski topologies on X and Y (Exercise (6.11)(12)).

If $\phi : X \to Y$ is a morphism of algebraic sets, we define its *comorphism* $\phi^* : \mathcal{O}(Y) \to \mathcal{O}(X)$ given by

$$\phi^*(f) = f \circ \phi$$

for $f \in \mathcal{O}(Y)$. We record the key facts:

Lemma. *(i) $\phi^*(f) \in \mathcal{O}(X)$ for $f \in \mathcal{O}(Y)$;*
(ii) ϕ^* is a k-algebra homomorphism;
(iii) $(id)^* = id$;
(iv) $(\phi \circ \psi)^* = \psi^* \circ \phi^*$ if ψ is a morphism of algebraic sets from Z to X;
(v) Every k-algebra homomorphism form $\mathcal{O}(Y)$ to $\mathcal{O}(X)$ arises as the comorphism of a morphism from X to Y.

Proof. (i) By definition, $\phi^*(f) = f \circ X : X \to k$ where f is the restriction to Y of $\hat{f} \in k[Y_1, \dots, Y_m]$. So

$$\phi^*(f)(\mathbf{x}) = f(\psi_1(\mathbf{x}), \psi_2(\mathbf{x}), \dots, \psi_m(\mathbf{x}))$$

which is in $\mathcal{O}(X)$ as required.
(ii) Check the definitions. (Exercise (6.11)(13))
(iii), (iv) Clear
(v) Suppose that $\theta : \mathcal{O}(Y) \to \mathcal{O}(X)$ is a k-algebra homomorphism. Let $\pi : k[Y_1, \dots, Y_m] \twoheadrightarrow \mathcal{O}(Y)$ be the canonical epimorphism given by restriction of maps from $\mathbb{A}^m$. So

$$\mathcal{O}(Y) = k\langle y_1, \dots, y_m \rangle,$$

where $Y_i = \pi(Y_i)$, $i = i, \dots, m$. Now θ lifts to a homomorphism form $k[Y_1, \dots, Y_m]$ to $\mathcal{O}(X)$:

$$\begin{tikzcd}
\mathcal{O}(Y) \arrow[r, "\theta"] & \mathcal{O}(X) , \\
k[Y_1, \dots, Y_m] \arrow[u, two heads, "\pi"] \arrow[ur, "\hat{\theta}"'] &
\end{tikzcd}$$

where $\hat{\theta} : Y_i \mapsto \theta(y_i)$. Define $\hat{\theta}(Y_j)(= \theta(y_j)) =: \psi_j \in \mathcal{O}(X)$ for $j = 1, \dots, m$. Set

$$\tau : X \to \mathbb{A}^m : \mathbf{x} \mapsto (\psi_1(\mathbf{x}), \dots, \psi_m(\mathbf{x})).$$

Since

$$\begin{aligned} \tau^* : k[Y_1, \dots, Y_m] &\to \mathcal{O}(X) \\ : Y_j &\mapsto Y_j \circ \tau = \psi_j, \end{aligned}$$

we see that

$$\tau^* = \hat{\theta},$$

so that $\mathrm{im}\tau \subseteq Y$ and taking $\tau : X \to Y$ we get $\tau^* = \theta$ as required. □

The proof of (v) shows that we can recover any morphism $\phi : X \to Y$ from knowledge of its comorphism ϕ^*. So in effect we have proved

Theorem. *The functor $X \to \mathcal{O}(X)$ defines a contravariant equivalence of categories.*

$$\left\{\begin{array}{c}\textit{algebraic sets /k}\\ \textit{and their morphisms}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\textit{affine semiprime commutative}\\ \textit{k-algebras and algebra homomorphisms}\end{array}\right\}$$

6.7. Product varieties. Suppose that X and Y are algebraic sets, say $X \subseteq \mathbb{A}^n$ and $Y \subseteq \mathbb{A}^m$. Then the cartesian product $X \times Y$ is again an algebraic set: first $\mathbb{A}^n \times \mathbb{A}^m = \mathbb{A}^{n+m}$, and $X \times Y$ is a closed subset of $\mathbb{A}^{n+m}$. For if $X = Z(\{f_i \in k[T_1, \dots, T_n]\})$ and $Y = Z(\{g_j \in k[U_1, \dots, U_m]\})$ then $X \times Y = Z(\{f_i\} \cup \{g_j\})$, where we think of f_i and g_j as in $k[T_1, \dots, T_n, U_1, \dots, U_m]$. You should convince yourself that

$$\mathcal{O}(X \times Y) \cong \mathcal{O}(X) \otimes_k \mathcal{O}(Y). \qquad (1)$$

6.8. Principal open subsets. Let X be an affine variety, and let $0 \neq f \in \mathcal{O}(X)$. The *principal open subset* of X defined by f is

$$X_f := \{\underline{x} \in X : f(\underline{x}) \neq 0\}.$$

Clearly, X_f is open in X. Notice two important facts:

- Every non-empty open subset of X is a finite union of principal open sets. This follows from Hilbert's basis theorem. So the principal open sets form a basis for the Zariski topology on X;
- X_f is itself an affine algebraic variety. For, let R be the subalgebra of the quotient field of $\mathcal{O}(X)$ generated by $\mathcal{O}(X)$ and f^{-1}; i.e. $R = \mathcal{O}(X)[f^{-1}]$. Since

  $$R \cong \mathcal{O}(X)[Y]/ < Yf - 1 >,$$

  R is an affine commutative domain, so it is $\mathcal{O}(Y)$ for some affine variety Y. In fact, $Y = X_f$, because the space of maximal ideals of R is homeomorphic to X_f via the map

  $$Y \to X_f : \underline{m} \mapsto \underline{m} \cap \mathcal{O}(X).$$

7. Algebraic groups and commutative Hopf algebras

7.1. Algebraic groups. Let G be an algebraic set which also has the structure of a group. That is, we have maps

$$m : G \times G \to G : (x, y) \mapsto xy,$$

and

$$\tau : G \to G : x \mapsto x^{-1}.$$

Definition. (i) If $G \times G$ is made into an algebraic set as in (6.7) and m and τ are morphisms of algebraic sets, then G is an *algebraic group* over k.

(ii) A *morphism of algebraic groups* is a morphism of algebraic sets which is also a group homomorphism.

Examples (i) The *additive group* $G_{\underline{a}}(k)$ is $k = \mathbb{A}^1$ with the usual addition in k. So $m(x, y) = x + y$, $\tau(x) = -x$.

(ii) The *multiplicative group* $G_{\underline{m}}(k)$ is just the open subset $k \setminus \{0\}$ of $\mathbb{A}^1$, with the multiplication from k. So by (6.8),

$$\mathcal{O}(G_{\underline{m}}(k)) = k[X, X^{-1}] \cong k[X, Y]/ < XY = 1 > .$$

In fact, it can be shown that (i) and (ii) are the only irreducible one-dimensional algebraic groups over k, but this is nontrivial [Humphreys, Theorem (20.5)].

(iii) *The special linear groups:* For $n \geq 1$, $SL_n(k) = \{A \in M_n(k) : \det(A) = 1\}$ is an algebraic group. For, $M_n(k)$ is clearly a variety, namely $\mathbb{A}^{n^2}$, so its coordinate ring is

$$\mathcal{O}(M_n(k)) = k[X_{ij} : 1 \leq i, j \leq n].$$

Then $SL_n(k)$ is the closed subset of $M_n(k)$ defined as the zeros of the single polynomial

$$\det(X_{ij}) - 1.$$

The formulae for matrix multiplication and inversion now make it clear that $SL_n(k)$ is an algebraic group.

(iv) *The general linear groups:* Let $n \geq 1$, $GL_n(k) = \{A \in M_n(k) : \det(A) \neq 0\}$ is a principal open subset in $M_n(k)$ and hence by (6.8) has coordinate ring

$$\begin{aligned} \mathcal{O}(GL_n(k)) &= \mathcal{O}(M_n(k))[\det(X_{ij})^{-1}] \\ &= k[X_{ij} : 1 \leq i, j \leq n][\det(X_{ij})^{-1}]. \end{aligned}$$

(v) *Any closed subgroup of an algebraic group is an algebraic group.* This is clear, and it means that e.g.

$$\begin{aligned} T(n, k) &= \{\text{upper triangular matrices in } GL_n(k)\}; \\ U(n, k) &= \{\text{strictly upper triangular matrices in } GL_n(k)\}; \\ D(n, k) &= \{\text{diagonal matrices in } GL_n(k)\} \end{aligned}$$

are all algebraic groups.

(vi) All finite groups are algebraic (over any algebraically closed field k). This is clear because every finite group has a faithful $k-$linear representation - the regular representation, for instance; and finite subsets of algebraic sets are algebraic, as we have seen in Chapter 6.

7.2. Hopf algebras. Let G be an algebraic group over k. It's almost obvious that $\mathcal{O}(G)$ is a Hopf algebra if we transpose the multiplication and inverse operations from G to $\mathcal{O}(G)$. That is, recalling (6.7)(1), we define

$$\Delta : \mathcal{O}(G) \to \mathcal{O}(G) \otimes \mathcal{O}(G) \cong \mathcal{O}(G \times G)$$

by defining $\Delta(f)$ to be the function from $G \times G$ to k given by

$$\Delta(f)((x, y)) = f(xy),$$

for $x, y \in G$; and $\varepsilon : \mathcal{O}(G) \to k$ is given by $f \mapsto f(1_G)$. Finally, let $S : \mathcal{O}(G) \to \mathcal{O}(G)$ be given by

$$(Sf)(x) = f(x^{-1}).$$

It is a routine exercise to check that all the Hopf algebra axioms are satisfied.

Conversely, if $\mathcal{O}(X)$ is the coordinate ring of an algebraic set X *and* $\mathcal{O}(X)$ is a Hopf algebra, then X is in fact an algebraic group.

For, recall that we can and should think of X as the set Maxspec($\mathcal{O}(X)$) of maximal ideals of $\mathcal{O}(X)$, made into a topological space with the Zariski topology. Now every such maximal ideal $\underline{m}_x$ determines a homomorphism of k-algebras

$$ev_{\underline{m}_x} : \mathcal{O}(X) \to k : f \mapsto f + \underline{m}_x.$$

[I'm calling the map $ev_{\underline{m}_x}$ to stand for "evaluation at x", since under our correspondence

$$X \longleftrightarrow \mathrm{Maxspec}\mathcal{O}(X),$$

we have

$$x \longleftrightarrow \underline{m}_x = \{g \in \mathcal{O}(X) : g(x) = 0\},$$

and so $f + \underline{m}_x$ is just $f(x)$.]

Conversely, if $\pi : \mathcal{O}(X) \to k$ is a k-algebra homomorphism, π is determined by its kernel, a maximal ideal. Thus X identifies with the set of k-algebra homomorphisms from $\mathcal{O}(X)$ to k, and this is a group: namely, if a, b are k-algebra homomorphisms, define

$$ab := (a \otimes b) \circ \Delta;$$

so $\varepsilon : \mathcal{O}(X) \to k$ is an identity element for this multiplication; and

$$a^{-1} := a \circ S$$

yields an inverse for a.

Moreover, it's easy to see that these operations are continuous maps for the Zariski topology, so that X is an algebraic group as claimed.

Summing up, we have, as a specialisation of Theorem 6.6

Theorem. *The functor $G \to \mathcal{O}(G)$ defines a contravariant equivalence of categories*

$$\left\{ \begin{array}{c} \textit{affine algebraic groups over } k \\ \textit{and their morphisms} \end{array} \right\} \longleftrightarrow \left\{ \begin{array}{c} \textit{affine commutative semiprime} \\ \textit{Hopf } k-\textit{algebras and} \\ \textit{Hopf algebra morphisms} \end{array} \right\}$$

7.3. Examples. We should note what the Hopf maps are for some of our examples in (7.1).

(i) $G_{\underline{a}}(k) = k$, so $\mathcal{O} = k[X]$ with $X(a) = a$ for $a \in k$. Thus

$$\varepsilon(X) = X(0) = 0;$$

and

$$\Delta(X) = X \otimes 1 + 1 \otimes X.$$

Finally, $S(X)(a) = X(-a) = -a$, so that

$$S(X) = -X.$$

(ii) $G_{\underline{m}}(k) = k \setminus 0 \subseteq \mathbb{A}^1$,so, noting (6.8), $\mathcal{O} = k[X, X^{-1}]$. And

$$\varepsilon(X) = X(1) = 1;$$

while

$$\Delta(X)(a \otimes b) = X(ab) = ab,$$

so that

$$\Delta(X) = X \otimes X.$$

Finally $S(X)(a) = X(a^{-1}) = a^{-1} = (X(a))^{-1} = X^{-1}(a)$, so that

$$S(X) = X^{-1}.$$

(iii), (iv) First, $\mathcal{O}(M_n(k))$ is a *bialgebra*, with

$$\varepsilon(X_{ij}) = X_{ij}(I_n) = \delta_{ij},$$

and

$$\Delta(X_{ij})((A, B)) = (ij)^{th} \textit{ entry of } AB,$$

so that

$$\Delta(X_{ij}) = \sum_{k=1}^{n} X_{ik} \otimes X_{kj}.$$

Notice that this is *not* cocommutative. For $GL_n(k)$ and $SL_n(k)$ the antipode is given by the formula for matrix inverse:

$$(SX_{ij})(A) = X_{ij}(A^{-1}) = (ij)^{th} \textit{ entry of } A^{-1}.$$

7.4. Supplements to Theorem (7.2). 1. The restriction to *affine* $k-$algebras in the theorem is not very important: *every* commutative Hopf algebra is a union of affine Hopf algebras [Waterhouse, Theorem (3.3)]. Expressed group-theoretically, this says:

every affine algebraic group scheme over k is the
inverse limit of algebraic affine group schemes.

2. The key example in (7.3) is $GL_n(k)$. Indeed,

every affine algebraic group scheme over k is a
closed subgroup of $GL_n(k)$ for some k.

This is [Waterhouse, Theorem (3.4)].

3. In characteristic 0, the adjective "semiprime" can be removed from Theorem (7.2):

Theorem. *(Cartier) let k be a field of characteristic 0, and let H be a commutative Hopf $k-$algebra. Then H is semiprime; (that is, H has no non-zero nilpotent elements).*

For a proof, see [Waterhouse, Theorem 11.4].

Note that this is false in positive characteristic: for example let k have characteristic $P > 0$, let G be any non-trivial finite $p-$group, and let H be the group algebra kG. If $1 \neq x \in G$ with $x^p = 1$, then $(x-1)^p = 0$ in H.

4. In fact, we can extend Theorem (7.2) to *all* commutative Hopf algebras in arbitrary characteristic by replacing "group" by "affine group scheme" - for the details, see e.g. [Waterhouse].